Hewlett Packard
Enterprise

HPE Integrated Lights-Out Security Technology Brief

Abstract

HPE Integrated Lights-Out (iLO) has been widely accepted as the standard for remotely managing servers in data centers. With security a key concern of all aspects of data center—including remote management, this paper describes the firmware and hardware methods iLO uses to protect against the risks of unauthorized access. Additionally, this paper describes utilities and services providing access points into iLO and its host system, and offers recommendations for configuring iLO security parameters and iLO connectivity options. Not all features and utilities are available to all of iLO.

Part Number: 808974-002
Published: October 2016
Edition: 1

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

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

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

Acknowledgments

Contents

1 Introduction

HPE iLO is an autonomous management processor built into the server that simplifies server setup, offers server health monitoring, allows power and thermal optimization, and facilitates remote server administration. This wide latitude of control is available independent of the server's operating system and even the state of the server hardware. Thus, we have designed iLO to ensure that it's powerful functionality is protected against unauthorized users.

IMPORTANT: Data center managers are responsible for the physical security of their facilities. Anyone with physical access to a server can potentially alter the iLO setup through the Security Override switch discussed later in this paper. It is assumed that anyone with access to the inside of a server chassis is a super-user or administrator.

iLO lets you deploy your ProLiant servers without concern. It uses strong authentication, highly configurable user privileges with strong authorization processes, and encryption of data, keystrokes, and security keys. The hardware design protects keys and sensitive password information, and lets you separate iLO management traffic from all server traffic.

FIPS mode and Common Criteria

HPE iLO 3 firmware v1.50 is FIPS 140–2 Level 1 validated. For more information, see this document on the NIST website at **http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp2173.pdf**. HPE iLO 3 firmware v1.50 is also Common Criteria EAL 4+ certified. For more information, see this document on the Common Criteria website: **https://www.commoncriteriaportal.org/files/epfiles/383-4-209%20CR%20v1.0e.pdf**.

The cryptographic module in HPE iLO 4 firmware v2.50 is FIPS 140–2 Level 1 validated. For more information, see this document on the NIST website at **http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp2574.pdf**.

2 Firmware-based protection

iLO employs firmware-based mechanisms that offer protection from unauthorized access and phlashing.

Unauthorized access

Access through an iLO portal involves a multi-layer security process that includes authentication, authorization, data integrity, and security keys. iLO firmware is digitally signed with a private key that prohibits unauthorized code from executing.

Authentication	Determines who is at the other end of the network connection using identity verification methods such as Kerboros. Authentication can be performed locally, or through directory services using authentication methods such as Active Directory and SSO.
Authorization	Determines whether the user attempting to perform a specific action has the right to do it. Using local accounts, you can define separate iLO users and vary their server access rights. Using directory services, you maintain network user accounts and security policies in a central, scalable database that supports thousands of users and system management roles.
Data integrity	Verifies that no one has altered incoming commands or data. iLO uses digital signatures and trusted .NET, Java, and iLO mobile applets available for Android and iOS.
Security keys	Manages confidentiality of sensitive data and transactions. iLO protects privacy through TLS encryption of web pages and the RC4 or AES encryption of remote console and virtual serial port data. iLO can be configured to allow only the highest cryptographic methods (like AES) to be used. iLO uses layers of security and industry-standard methods to secure access to the server. For example, iLO cryptographic keys use a minimum key length of 128 bits and conform to industry standards. When high encryption modes are not used, iLO may negotiate less than 128 bit key lengths.

Phlashing

Phlashing is a permanent denial of service (PDOS) attack. A PDOS attack could theoretically take advantage of vulnerabilities during updates of network-based firmware. Rogue firmware installed through a PDOS attack could lead to unauthorized server access or permanent hardware damage.

iLO offers following protections:

- Authorized firmware updates – iLO firmware images are digitally signed with a 2048-bit private key. The boot block checks the digital signature every time iLO comes out of reset. iLO checks the digital signature before allowing a firmware update to proceed. Remote flashing requires login authentication and authorization, including optional two-factor authentication.
- Unencrypted ports – iLO clearly defines the port encryption status. You can disable access to any non-encrypted ports (such as telnet). Access to iLO requires a password unless you decide to disable the password.
- Authentication and audit trails – iLO creates a log of SSH authentication failures and successes. SSH-key authentication makes successful brute force attacks even less likely. For additional protection, iLO 3 creates a second session key for remote access, and iLO 4 uses 2048-bit DSA or RSA keys.

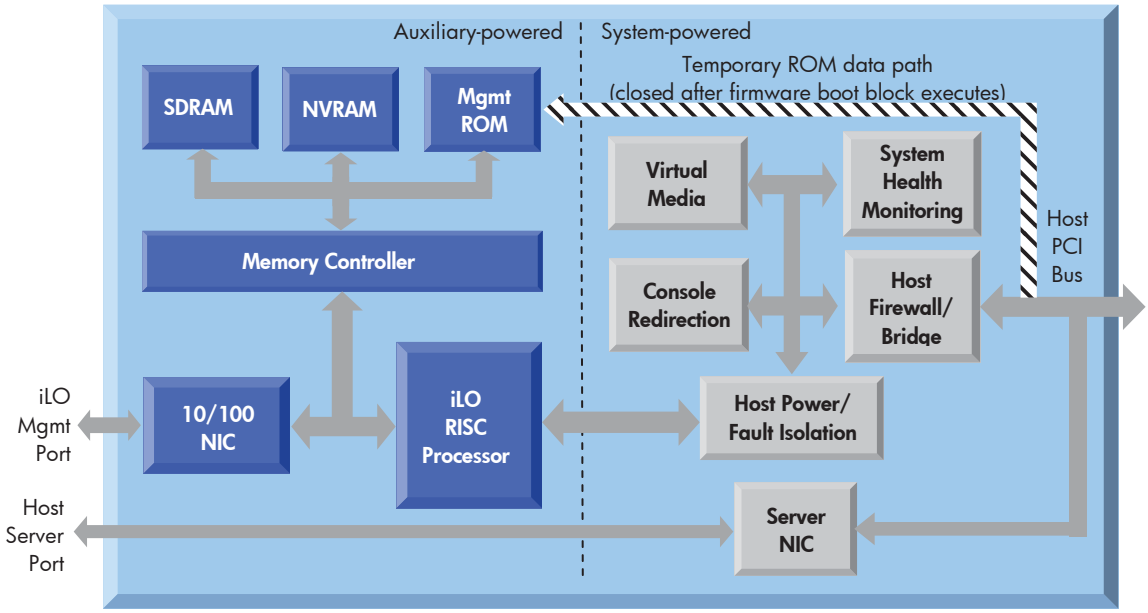
- Unsuccessful Login delays – iLO captures all login activity. It uses a progressive timed delay during unsuccessful login attempts to impede brute force and dictionary attacks.
- Restricted access and modification of critical security parameters – iLO logs many security parameter changes such as user accounts, log changes, and certificates. This allows tracing potential unauthorized information access attempts.

We address these security topics in more detail later in this technology brief.

3 Hardware-based protection

The iLO subsystem includes a 32-bit, iLO RISC processor core with separate instruction and data caches, a memory controller, SDRAM, NVRAM, management ROM, and NIC. The iLO subsystem also involves other elements such as System Health Monitoring, Console Redirection, Host/Firewall Bridge, the Server NIC, and Virtual Media. As shown in Figure 1, iLO consists of system-powered functions (available only while the server is powered up) and auxiliary powered functions (available as long as the server has power applied).

Figure 1 Block diagram of iLO processor



Management ROM

There are two types of signature checking of the iLO firmware image. There is the validation of a new image before it is programed into iLO's flash device and there is the integrity check of this image as iLO boots.

Image Validation

The entire image is hashed with SHA256 and signed using Hewlett Packard Enterprise's RSA 2048-bit private key. This signature block is pre-pended to the firmware binary image.

When performing a firmware update, the hash is decrypted by the currently executing iLO firmware with Hewlett Packard Enterprise's public key. This hash is compared with a hash of the entire image. If they match, the firmware update is allowed to proceed. The signature block is discarded.

The iLO boot block is not overwritten unless a new boot block is required.

Boot-Time Integrity Check

At boot time, each piece has its signature validated before it is allowed to execute. Subsequent pieces are checked by the previous ones until iLO is fully booted.

If an image becomes corrupt to the point that it will not boot, a new image can be applied by running the iLO firmware Smart Component locally in direct mode. This requires that the Security Override switch on the server's motherboard be set. In direct mode, the Smart Component writes directly to the iLO flash device through the PCI bus (see Figure 1).

Individual parts, such as the kernel, of the iLO firmware image are also signed. These integrity signatures are not discarded during the flash process.

Protected PCI bus

iLO includes firewall and bridge logic to control information flow between the server and the management console (Figure 1). The firewall logic protects against unauthorized access through the server's PCI bus. It shields keys and data stored in memory and firmware, and does not allow direct access to keys via the PCI bus.

Host Access Configuration Lock

iLO access from the host operating system can be locked to prevent configuration changes with a Host Access Configuration Lock. Set the lock using one of the following methods:

- Use the RIBCL `MOD_GLOBAL_SETTINGS` command (LOCK_CONFIGURATION parameter) or script
- Enter the IPMI `set system interface configuration parameters` command.

When using RIBCL or IPMI, the system will respond with an insufficient privilege level error for commands while the lock is enabled (note that for IPMI, any commands require a session login and it is possible to set the maximum privilege level that can be accepted when the lock is enabled.) The unlock sequence can only be done across the system interface.

Network and management ports

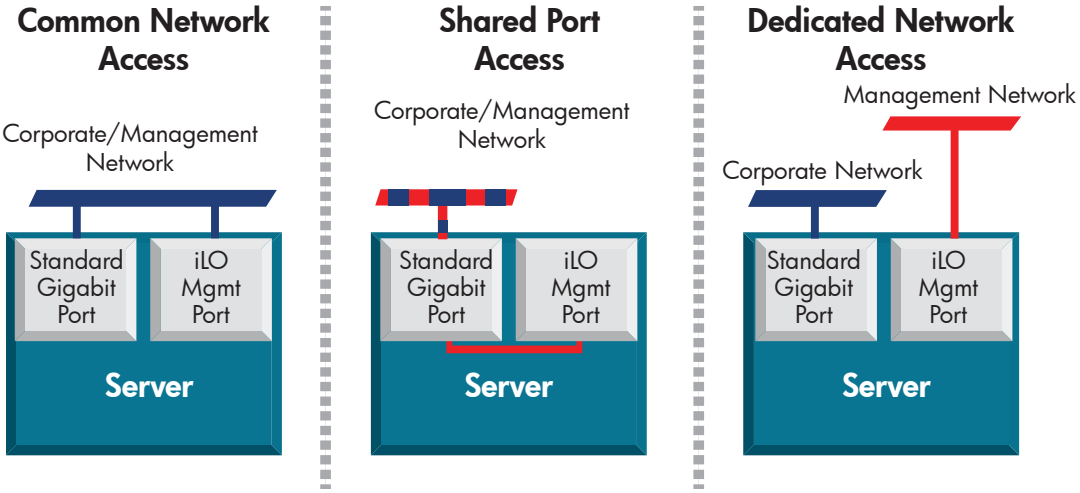
iLO's firewall and bridge logic prevent any connection between the iLO management port and the server Ethernet port (Figure 1). Even by using the shared network port (SNP), iLO cannot bridge traffic between its 10/100 Ethernet port and the server Ethernet port. Therefore, attacks on the server network cannot compromise iLO and vice-versa.

Shared network port

Most ProLiant ML and DL servers with iLO support SNP. Consult the server documentation to determine whether your ProLiant server supports SNP. Hewlett Packard Enterprise does not support SNP on HPE BladeSystem server blades.

The SNP lets iLO management traffic use a sideband connection on the server NIC rather than dedicating a second port to iLO management traffic (Figure 2). Although the iLO traffic shares a port with the server OS traffic, both iLO and the server NIC have their own MAC and IP address. This ensures that other devices can independently address iLO. This is an advantage if you want to install and maintain a single network infrastructure for handling both management and productivity traffic.

Figure 2 Traffic paths of shared and dedicated networks



Shared network port with Virtual LAN

Implementing Virtual LAN (VLAN) tags enhances iLO SNP security. When you enable VLAN Tags, the iLO SNP becomes part of a Virtual LAN. The VLAN is a logical network that isolates network traffic to segments. It increases security because established rules keep traffic on one segment from entering another segment. All network devices with the same Virtual LAN tag appear to be on a separate LAN even if they are physically connected to the same LAN. The SNP NIC checks the Ethernet frame for a VLAN ID and compares it against its configured value. If they match, then the SNP strips the frame of the VLAN tag and forwards it to iLO. If they do not match, the SNP forwards the frame to the server. The SNP NIC inserts a VLAN tag into any outgoing Ethernet frames.

Security Override switch

You can disable all of iLO's security authorization checks by turning on the Security Override switch. This gives you access to the following tasks:

- Reconfigure iLO through ROM-Based Setup (RBSU) even if RBSU is disabled
- Direct flash for disaster recovery, allowing you to flash from the host
- Log into iLO without credentials

Trusted Platform Module and Trusted Modules

Trusted Platform Modules and Trusted Modules are computer chips that securely store artifacts used to authenticate the platform. These artifacts can include passwords, certificates, or encryption keys. You can also use a TPM or TM to store platform measurements to make sure that the platform remains trustworthy. On a supported system, ROM decodes the TPM or TM record and

passes the configuration status to iLO, the RESTful interface, the command line processor (CLP), and the XML interface. The iLO Overview page displays the following TPM status information:

- **Not Supported**—A TPM or TM is not supported.
- **Not Present**—A TPM or TM is not installed.
- **Present** (Gen8 servers)—This indicates one of the following statuses:
  - A TPM or TM is installed and disabled.
  - A TPM or TM is installed and enabled.
  - A TPM is installed and enabled, and Expansion ROM measuring is enabled.

    On servers with a TPM: If Option ROM Measuring is enabled, the **Update Firmware** page displays a warning message when you click **Upload**.
- Present-Enabled (Gen9 Servers)—A TPM is installed and enabled.

  On servers with a TPM: If Option ROM Measuring is enabled, the **Update Firmware** page displays a warning message when you click **Upload**.

4 Configuring iLO security settings

You can configure the iLO access options by using the iLO interfaces, iLO RBSU, or the iLO 4 Configuration Utilities.

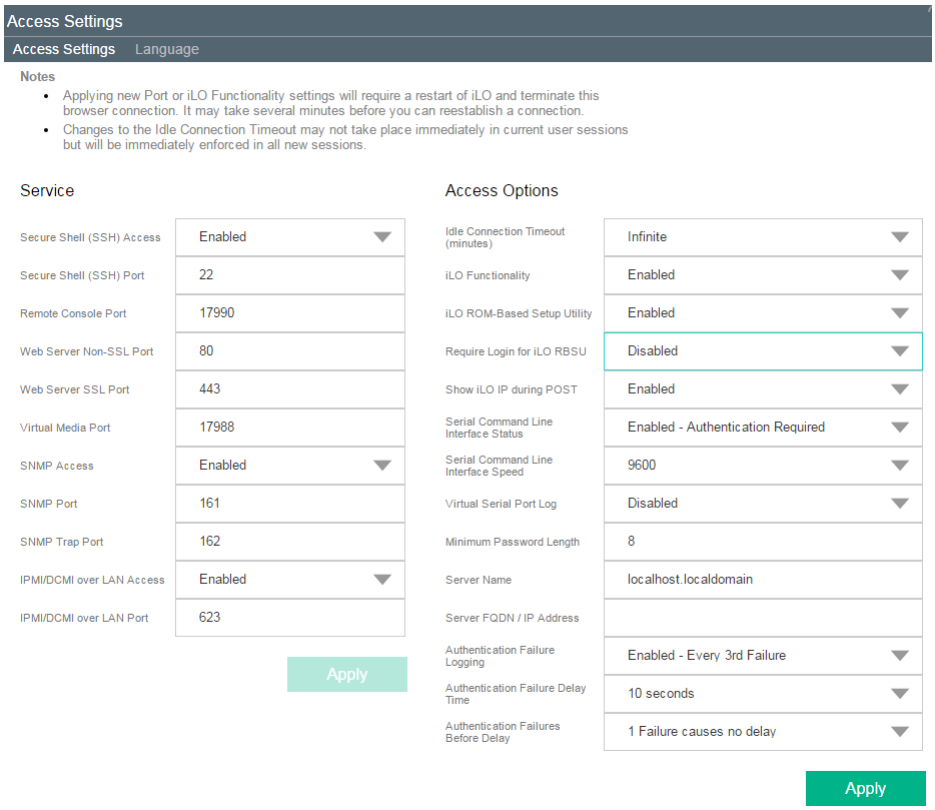
Configuring access options using the iLO interface

The **Access Options** section of the **Access Settings** page are described in Appendix A. To apply your new settings, end your browser connection and restart iLO. It might take several minutes before you can re-establish a connection.

You can also modify access options for the Intelligent Platform Management Interface (IPMI) and the Data Center Management Interface (DCMI).

The values you enter on the Access Settings (Figure 3) page apply to all iLO users. You must have the Configure iLO Settings privilege to modify access settings.

Figure 3 Access Settings page



For greater security, HPE recommends the following settings:

- **iLO Functionality**

  This setting specifies whether iLO functionality is available. Set it to **Enabled** (the default). This makes the iLO network available and communications with operating system drivers active.

- **iLO ROM-Based Setup Utility**

  This setting enables or disables the iLO RBSU or the iLO 4 Configuration Utility. Set it to **Enabled** (the default). On servers that support the iLO RBSU, pressing **F8** during POST starts the iLO RBSU. On servers that support UEFI, the iLO 4 Configuration Utility is available when you access the UEFI System Utilities.

  This setting cannot be set to **Enabled** if option ROM prompting is disabled in the system BIOS.

NOTE: This option is called **iLO 4 Configuration Utility** in the UEFI System Utilities.

- **Require Login for iLO RBSU**

  This setting determines whether a user-credential prompt is displayed when a user accesses the iLO RBSU or the iLO 4 Configuration Utility. Set it to **Enabled**. A login dialog box opens when a user accesses the iLO RBSU or the iLO 4 Configuration Utility.

Operating in FIPS mode:

Operating in FIPS approved mode with iLO firmware that has been FIPS 140–2 validated requires the following steps:

- Clear the **Enable IPMI/DCMI over LAN on Port 623** in the IPMI/DCMI section of the Access Settings page and then click **Apply**.

  Server-side IPMI/DCMI applications are still functional when IPMI/DCMI over LAN is disabled.
- In the **Service** section of the **Access Settings** page, change **SNMP Access** to **Disabled**.

  iLO continues to operate, and the information displayed in the iLO web interface is updated, but no alerts are generated and SNMP access is not permitted. When **SNMP Access** is set to **Disabled**, most of the boxes on the **Administration→Management→SNMP Settings** page are unavailable and will not accept input.
- Navigate to the **Administration→Security→Encryption**page and enable **FIPS mode** under **Encryption Enforcement Settings**.
- After iLO reboots, change the default Administrator credentials.
- Replace the iLO self-signed certificate with a trusted certificate.

Authentication Failure Logging using a Secure Shell client

When a user logs in to iLO by using an SSH client, the number of login name and password prompts displayed by iLO matches the value of the **Authentication Failure Logging** option (3 if it is disabled). The number of prompts might also be affected by your SSH client configuration. SSH clients also implement delays after login failure.

For example, to generate an SSH authentication failure log with the default value (**Enabled-Every 3rd Failure**), assuming that the SSH client is configured with the number of password prompts set to 3, three consecutive login failures occur as follows:

1. Run the SSH client and log in with an incorrect login name and password.

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

   You receive three password prompts. After the third incorrect password, the connection ends and the second login failure is recorded. The SSH login failure counter is set to 2.
3. Run the SSH client and log in with an incorrect login name and password.

   You receive three password prompts. After the third incorrect password, the connection ends and the third login failure is recorded. The SSH login failure counter is set to 3.

The iLO firmware records an SSH failed login log entry, and sets the SSH login failure counter to 0.

Service settings

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

configurable, which enables compliance with any site requirements or security initiatives for port settings. These settings do not affect the host system.

Changing these settings usually requires configuration of the web browser used for standard and SSL communication. When these settings are changed, iLO initiates a reset to activate the changes. Update the settings depicted in Table 1 as needed.

Table 1 Service settings

Service setting	Default value
Secure Shell (SSH) Access	Enables you to specify whether the SSH feature on iLO is enabled or disabled. SSH provides encrypted access to the iLO CLP. The default is Enabled
Secure Shell (SSH) Port	22
Remote Console Port	17990
Web Server Non-SSL Port (HTTP)	80
Web Server SSL Port (HTTPS)	443
Virtual Media Port	17988
SNMP Access	Specifies whether iLO should respond to external SNMP requests. The default setting is **Enabled**.
SNMP Port	The industry-standard (default) SNMP port is 161 for SNMP access.
SNMP Trap Port	The industry-standard (default) SNMP trap port is 162 for SNMP alerts (or traps). **NOTE:** If you customize the SNMP Trap Port value, some SNMP monitoring applications (such as HPE SIM) might not work correctly with iLO unless those applications support the use of a nonstandard SNMP trap port.

Security configuration guidelines and procedures

NOTE: The following sections provide general guidelines and procedures for configuring iLO security parameters. For more detailed information about configuring iLO security refer to the iLO 4 user guide.

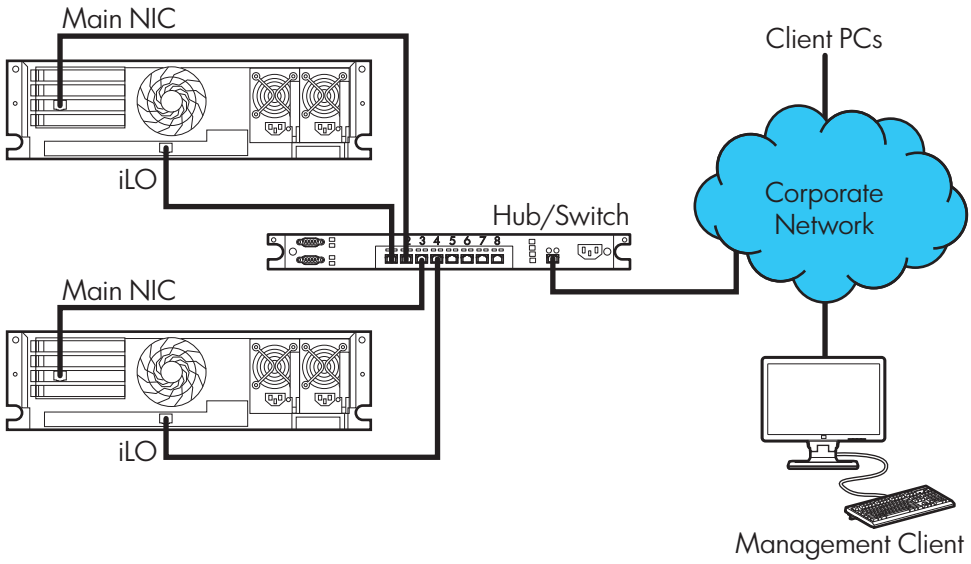
Configuring iLO involves the following security strategies:

- Network connection type
- Infrastructure authentication/directory server authentication
- iLO RBSU and Configuration Utility security
- SSH key and/or SSL certificate administration

Connecting iLO to a network

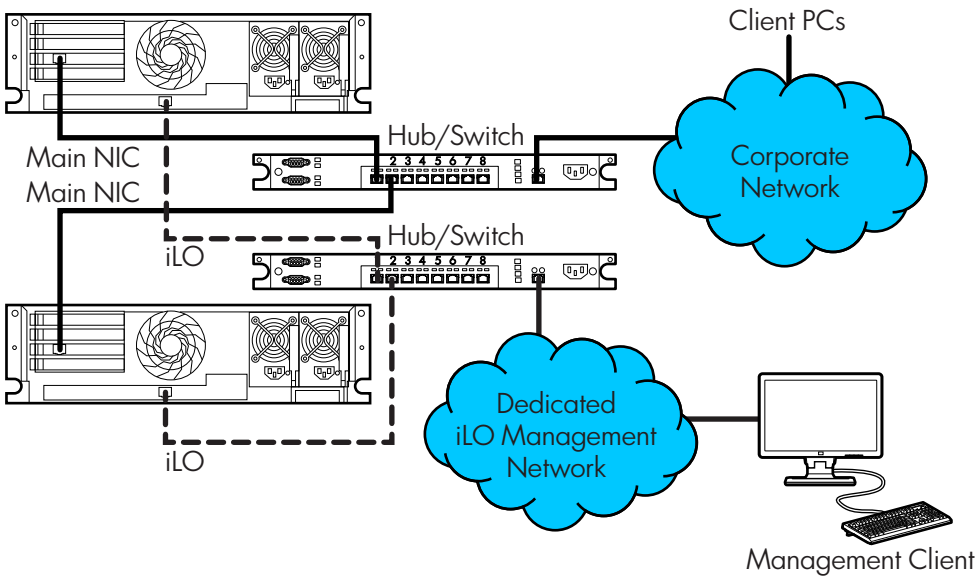
You can connect iLO to a corporate network or a dedicated management network (recommended). In a corporate network, the server has two network port types (server NICs and one iLO NIC) connected to the corporate network, as shown in Figure 4.

Figure 4 Corporate network diagram



We recommend using a dedicated management network, where the iLO port is on a separate network and not directly connected to the internet, as shown in Figure 5.

Figure 5 Dedicated management network diagram



Passwords

Hewlett Packard Enterprise recommends that you follow these password guidelines:

- Passwords should:
  - Never be written down or recorded
  - Never be shared with others

- Not be words found in a dictionary
- Not be obvious words, such as the company name, product name, user name, or login name

- Passwords should have at least three of the following characteristics:
  - One numeric character
  - One special character
  - One lowercase character
  - One uppercase character

Depending on the Minimum Password Length setting on the Access Settings page, the password can have a minimum of zero characters (no password) and a maximum of 39 characters. The default Minimum Password Length is eight characters.

IMPORTANT: We do not recommend setting the Minimum Password Length to fewer than eight characters unless you have a physically secure management network that does not extend outside a secure data center.

iLO RBSU and iLO 4 Configuration Utility security

iLO RBSU and the iLO 4 Configuration Utility enable you to view and modify the iLO configuration. You can configure iLO RBSU and iLO Configuration Utility access settings by using iLO RBSU, the iLO 4 Configuration Utility, the iLO web interface, or Remote Insight Board Command Language (RIBCL) scripts.

IMPORTANT: If the system maintenance switch is set to disable iLO security, any user can access iLO RBSU or the iLO 4 Configuration Utility regardless of the configured access settings.

iLO RBSU has the following security levels:

- **Login Not Required** (default): Anyone who has access to the host during POST can enter iLO RBSU to view and modify configuration settings. This is an acceptable setting if host access is controlled. If host access is not controlled, any user can make changes by using the active configuration menus.
- **Login Required** (more secure); If iLO RBSU login is required, the active configuration menus are controlled by the authenticated user access rights.
- **Disabled**(most secure): If iLO RBSU is disabled, user access is prohibited. This prevents modification by using the iLO RBSU.

To change the security level for RBSU, use the iLO web interface, the iLO RBSU, or the iLO 4 Configuration Utility to edit the **Require Login for iLO RBSU** or **Require Login for iLO Configuration Utility** (Host Access Configuration Lock) setting (the name of the setting varies based on your server capabilities).

Security levels can also be changed using the HPE RESTful Interface Tool.

iLO Security Override Switch administration

The iLO Security Override Switch (sometimes referred to as the iLO System Maintenance Switch) allows the administrator full access to the iLO processor. Disabling iLO security allows login

access with all privileges, without a user ID and password. Such access might be necessary for any of the following conditions:

- iLO has been disabled and must be re-enabled.
- All user accounts that have the Administer User Accounts privilege are locked out.
- An invalid configuration prevents iLO from being displayed on the network, and iLO RBSU or the iLO 4 Configuration Utility is disabled.
- The iLO firmware image is corrupt.
- The iLO NIC is turned off, and running iLO RBSU or the iLO 4 Configuration Utility to turn it back on is not possible or convenient.
- Only one user name is configured, and the password is forgotten.

The ramifications of setting the iLO Security Override Switch include the following:

- All security authorization verifications are disabled when the switch is set. In other words, all authentication will succeed.
- iLO RBSU or the iLO 4 Configuration Utility runs if the host server is reset.
- iLO is not disabled and might be displayed on the network as configured.
- iLO, if disabled when the switch is set, does not log out the user and complete the disable process until the power is cycled on the server.
- The firmware can be updated from a Smart Component in direct mode. However, the Hewlett Packard Enterprise signature is not updated.
- A warning message is displayed on iLO web interface pages, indicating that the switch is currently in use.
- An iLO log entry records the use of the switch.

When iLO boots after you set or clear the iLO Security Override Switch, an SNMP alert is sent if an SNMP Alert Destination is configured. Setting the iLO Security Override Switch enables you to flash the iLO firmware image in direct mode. Hewlett Packard Enterprise does not anticipate that you will need to update the boot block. However, if an update is required, you must be physically present at the server to reprogram the firmware and reset iLO. You must open the server enclosure to access the iLO Security Override Switch.

To set the iLO Security Override Switch:

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

Reverse this procedure to clear the iLO Security Override Switch. The iLO Security Override Switch uses switch #1 on the DIP switch panel. For information about accessing the iLO Security Override Switch, see the server documentation or use the diagrams on the server access panel.

User accounts and access

iLO supports the configuration of up to 12 local user accounts. Each account can be managed through the following features:

- Privileges
- Login security

You can configure iLO to use a directory to authenticate and authorize its users. This configuration enables an unlimited number of users and easily scales to the number of iLO devices in an enterprise. The directory also provides a central point of administration for iLO devices and users,

and the directory can enforce a stronger password policy. iLO enables you to use local users, directory users, or both. The following directory configuration options are available:

- An LDAP directory extended with HPE schema
- An LDAP directory default schema
- Kerberos authentication service

User privileges

iLO allows you to control user account access to iLO features through the use of privileges. When a user attempts to use a feature, iLO verifies that the user has the proper privilege to use that feature. You can control access to iLO features by using the following privileges: Administer User Accounts, Remote Console Access, Virtual Power and Reset, Virtual Media, and Configure iLO Settings. User privileges are configured on the **Administration→User Administration** page.

NOTE: User accounts can also be configured by using iLO RBSU or the iLO 4 Configuration Utility.

Login security

iLO provides several login security features. iLO can be configured to impose a delay after a configured number of failed login attempts. Each subsequent failed attempt increases the delay by the configured number of seconds. A message is displayed during each delay; this continues until a valid login occurs. This feature helps to prevent dictionary attacks against the browser login port. You can configure the login delay and other login settings on the **Administration→Access Settings** page.

iLO saves a detailed log entry for failed login attempts. You can configure the Authentication Failure Logging frequency on the **Administration→Access Settings** page.

Administering Secure Shell keys

The **Secure Shell Key** page displays the hash of the SSH public key associated with each user. Each user can have only one key assigned. Use this page to view, add, or delete SSH keys. You must have the Configure User Accounts privilege to add and delete any SSH keys but your own.

About SSH keys

When you add an SSH key to iLO the file must contain the user-generated public key. The iLO firmware associates each key with the selected local user account. If a user is removed after an SSH key is authorized for that user, the SSH key is removed. The following SSH key formats are supported:

- RFC 4716
- OpenSSH key format—this format must be one line only.
- iLO legacy format—OpenSSH keys surrounded by BEGIN/END headers needed for RIBCL. This format must be one line between the BEGIN and END.

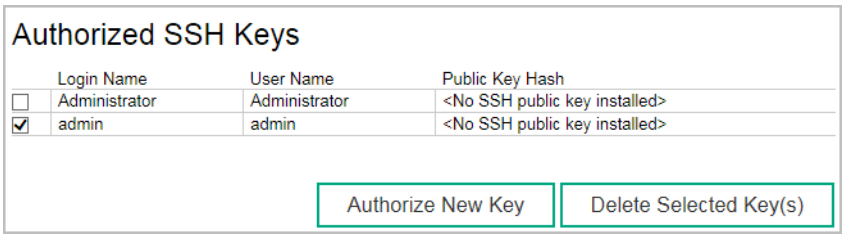
Note the following when working with SSH keys:

- The previously listed sample formats are supported with the iLO web interface and the CLI. Only the iLO legacy format is supported with RIBCL scripts.
- Any SSH connection authenticated through the corresponding private key is authenticated as the owner of the key and has the same privileges.

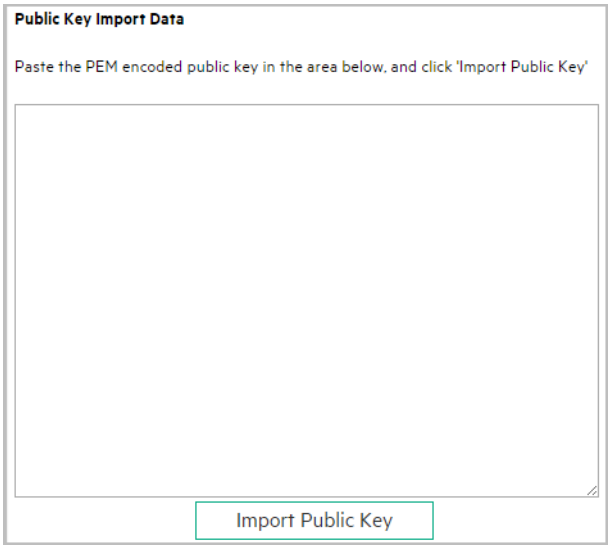
- The iLO firmware provides storage to accommodate SSH keys that have a length of 1366 bytes or less. If the key is larger than 1366 bytes, the authorization might fail. If this occurs, use the SSH client software to generate a shorter key.
- If you use the iLO web interface to enter the public key, you select the user associated with the public key. If you use the CLI to enter the public key, the public key is linked to the user name that you entered to log in to iLO. If you use HPQLOCFG to enter the public key, you append the iLO user name to the public key data. The public key is stored with that user name.

Authorizing a new key by using the iLO web interface

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



5. Select the check box to the left of the user for which you want to add an SSH key.
6. Click **Authorize New Key**.
7. Copy and paste the public key into the Public Key Import Data box.



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

8. Click **Import Public Key**.

Authorizing a new key by using the CLI

1. Generate a DSA or RSA SSH key by using ssh-keygen, `puttygen.exe`, or another SSH key utility.
2. Create the `key.pub` file.

3. Verify that **Secure Shell (SSH) Access** is enabled on the **Access Settings** page.
4. Use `Putty.exe` to open an SSH session using port 22.
5. Change (`cd`) to the `/Map1/Config1` directory.
6. Enter the following command:

   oemhp_loadSSHkey -source *<protocol://username:password@hostname:port/filename>*

When you use this command:

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

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

Example 1 Authorizing a new key.pub file

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

Deleting SSH keys

1. Navigate to the **Administration→Security** page.
2. Click the **Secure Shell Key** tab.
3. Select the check box to the left of the user for which you want to delete an SSH key.
4. Click **Delete Selected Key(s)**.The selected SSH key is removed from iLO. When an SSH key is deleted from iLO, an SSH client cannot authenticate to iLO by using the corresponding private key.

Authorizing keys from an HPE SIM server

The `mxagentconfig` utility enables you to authorize SSH keys from SIM server.

- SSH must be enabled on iLO before you use `mxagentconfig` to authorize a key.
- The user name and password entered in `mxagentconfig` must correspond to an iLO user who has the Configure iLO Settings privilege. The user can be a directory user or a local user.
- The key is authorized on iLO and corresponds to the user name specified in the `mxagentconfig` command.

For more information about `mxagentconfig`, refer to the *iLO 4 Scripting and Command Line Guide*.

Administering Secure Sockets Layer certificates

Secure Sockets Layer (SSL) is a standard for encrypting data so that it cannot be viewed or modified while in transit on the network. SSL uses a key to encrypt and decrypt the data; the longer the key, the better the encryption. A certificate is a public document that describes the server. It contains the name of the server and the server's public key. Because only the server has the corresponding private key, this is how the server is authenticated.

A certificate must be signed to be valid. If it is signed by a certificate authority (CA) and that CA is trusted, all certificates signed by the CA are also trusted. A self-signed certificate is one in which the owner of the certificate acts as its own CA. Self-signed certificates are the default for Hewlett Packard Enterprise management products, though they do support certificates signed by certifying authorities. The iLO firmware enables you to create a certificate request, import a

certificate, and view information associated with a stored certificate. Certificate information is encoded in the certificate by the CA and is extracted by iLO.

IMPORTANT: By default, iLO creates a self-signed certificate for use in SSL connections. This certificate enables iLO to work without additional configuration steps. **However, you must import a trusted certificate to enhance iLO security.** Users who have the Configure iLO Settings privilege can customize and import a trusted certificate.

Viewing certificate information

To view certificate information, navigate to the **Administration→Security→SSL Certificate** page. The following certificate details are displayed:

- **Issued To—**The entity to which the certificate was issued
- **Issued By—**The CA that issued the certificate
- **Valid From—**The first date that the certificate is valid
- **Valid Until—**The date that the certificate expires
- **Serial Number—**The serial number that the CA assigned to the certificate

Obtaining and importing a certificate

Users who have the Configure iLO Settings privilege can customize and import a trusted certificate. A certificate works only with the keys generated with its corresponding certificate signing request (CSR). If iLO is reset to factory defaults, or another CSR is generated before the certificate that corresponds to the previous CSR is imported, the certificate does not work. In that case, a new CSR must be generated and used to obtain a new certificate from the CA. To obtain and import a certificate:

1. Navigate to the **Administration→Security→SSL Certificate**
2. Click **Customize Certificate**.

   The **SSL Certificate Customization** page opens.
3. Enter the following information in the **Certificate Signing Request Information** section:
   - **Country (C)—**The two-character country code that identifies the country where the company or organization that owns this iLO subsystem is located. Enter the two-letter abbreviation in capital letters.
   - **State (ST)—**The state where the company or organization that owns this iLO subsystem is located.
   - **City or Locality (L)—**The city or locality where the company or organization that owns this iLO subsystem is located.
   - **Organization Name (O)—**The name of the company or organization that owns this iLO subsystem.
   - **Organizational Unit (OU)—**(Optional) The unit within the company or organization that owns this iLO subsystem.
   - **Common Name (CN)—**The FQDN of this iLO subsystem.

   The FQDN is entered automatically in the **Common Name (CN)** box.

   TIP: You must configure the **Domain Name** on the **Network General Settings** page to enable iLO to enter the FQDN into the CSR.
4. Click **Generate CSR**.

   A message notifies you that a certificate is being generated and that the process might take up to 10 minutes.

5. After a few minutes (up to 10), click **Generate CSR** again.

   The CSR is displayed.

   The CSR contains a public and private key pair that validates communications between the client browser and iLO. Key sizes up to 2,048 bits are supported. This is restricted to 2048–bit only in FIPS mode or in later versions of iLO firmware. The generated CSR is held in memory until a new CSR is generated, or iLO is reset to factory default settings, or a certificate is imported.

   NOTE: iLO supports certificates with key sizes up to 2048 bits, which can include any supported signature algorithm, including signatures based on SHA-2 (SHA-256, SHA-384, SHA-512)

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

   When you submit the CSR to the CA, your environment might require the specification of Subject Alternative Names (SAN). This information is typically included in the **Additional Attributes** box. If required, enter the iLO DNS short name and IP address in the **Additional Attributes** box by using the following syntax:

   `san:dns=10.10.20.95&dns=server1.ilo.example.com.`

   The CA generates a certificate in PKCS #10 format.
9. After you obtain the certificate, make sure that:
   - The CN matches the iLO FQDN.

     This is listed as the **iLO Hostname** on the **Information→Overview** page.
   - The certificate is a Base64–encoded X.509 certificate.
   - The first and last lines are included in the certificate.
10. Return to the **SSL Certificate Customization** page in the iLO web interface.
11. Click the **Import Certificate** button.

    The **Import Certificate** window opens.
12. Paste the certificate into the text box, and then click **Import**.

    iLO supports SSL certificates that are up to 3 KB in size (including the 609 or 1,187 bytes used by the private key, for 1,024–bit and 2,048–bit certificates, respectively).
13. Reset iLO.

Directory authentication and authorization

The iLO firmware supports Microsoft Active Directory for user authentication and authorization. You can configure iLO to authenticate and authorize users by using the HP Extended Schema directory integration or the schema-free directory integration. The HP Extended Schema works only with Microsoft Windows. The iLO firmware connects to directory services by using SSL connections to the directory server LDAP port. The default secure LDAP port is 636.

Locally stored user accounts (listed on the User Administration page) can be active when iLO directory support is enabled. This enables both local-based and directory-based user access. Typically, you can delete local user accounts (with the possible exception of an emergency access account) after iLO is configured to access the directory service. You can also disable access to these accounts when directory support is enabled. You must have the Configure iLO Settings privilege to change directory settings. This feature and many others are part of an iLO licensing package. For more information about iLO licensing, see the following website: **http://www.hpe.com/info/ilo/licensing**.

Configuring the authentication and directory server settings is one step in the process of configuring iLO to use a directory or Kerberos authentication.

Prerequisites

- Your iLO user account has the Configure iLO Settings privilege.
- An iLO license that supports this feature is installed. For more information, see the following website: **http://www.hpe.com/info/ilo/licensing**.
- The environment is configured to support Kerberos authentication or directory integration.
- The Kerberos keytab file is available (Kerberos authentication only).

Configuring Kerberos authentication settings in iLO

1. Navigate to the **Administration→Security→Directory** page.
2. Select the **Enabled** option for **Kerberos Authentication**.
3. Select the **Enabled** option for **Local User Accounts** if you want to use local user accounts at the same time as Kerberos authentication.
4. Enter the **Kerberos Realm** name.
5. Enter the **Kerberos KDC Server Address**.
6. Enter the **Kerberos KDC Server Port**.
7. To add the Kerberos Keytab file, click **Browse** (Internet Explorer or Firefox) or **Choose File** (Chrome), and then follow the onscreen instructions.
8. Click **Apply Settings**.

Kerberos settings

- **Kerberos Authentication**—This setting enables or disables Kerberos login. If Kerberos login is enabled and configured correctly, the **Zero Sign In** button appears on the login page.
- **Kerberos Realm**—The name of the Kerberos realm in which the iLO processor operates. This value can be up to 128 characters. The realm name is usually the DNS name converted to uppercase letters. Realm names are case-sensitive.
- **Kerberos KDC Server Address**—The IP address or DNS name of the KDC server. This value can be up to 128 characters. Each realm must have at least one KDC that contains an authentication server and a ticket grant server. These servers can be combined.
- **Kerberos KDC Server Port**—The TCP or UDP port number on which the KDC is listening. The default value is 88.
- **Kerberos Keytab**—A binary file that contains pairs of service principal names and encrypted passwords. In the Windows environment, you use the `ktpass` utility to generate the keytab file.

Configuring schema-free directory settings in iLO

1. Navigate to the **Administration→Security→Directory** page.
2. Select the **Use Directory Default Schema** option for **LDAP Directory Authentication**.
3. Select the **Enabled** option for **Local User Accounts** if you want to use local user accounts at the same time as directory integration.
4. Enter the FQDN or IP address of a directory server in the **Directory Server Address** box.
5. Enter the directory server port number in the **Directory Server LDAP Port** box.
6. Enter valid search contexts in one or more of the **Directory User Context** boxes.
7. Click **Apply Settings**.
8. To test the communication between the directory server and iLO, click **Test Settings**.

9. Optional: To configure directory groups, click **Administer Groups** to navigate to the **User Administration** page.

Schema-free directory settings

- **Use Directory Default Schema**—Selects directory authentication and authorization by using user accounts in the directory. Select this option when the directory is not extended with the HPE Extended Schema. User accounts and group memberships are used to authenticate and authorize users.
- **Directory Server Address**—Specifies the network DNS name or IP address of the directory server. The directory server address can be up to 127 characters.

  If you enter the FQDN, ensure that the DNS settings are configured in iLO.

  Hewlett Packard Enterprise recommends using DNS round-robin when you define the directory server.
- **Directory Server LDAP Port**—Specifies the port number for the secure LDAP service on the server. The default value is 636. If your directory service is configured to use a different port, you can specify a different value. Make sure that you enter a secured LDAP port. iLO cannot connect to an unsecured LDAP port.
- **Directory User Contexts**—These boxes enable you to specify common directory subcontexts so that users do not need to enter their full DNs at login. Directory user contexts can be up to 128 characters.

Configuring HPE extended schema directory settings in iLO

1. Navigate to the **Administration→Security→Directory** page.
2. Select the **Use Extended Schema** option for **LDAP Directory Authentication**.
3. Select the **Enabled** option for **Local User Accounts** if you want to use local user accounts at the same time as directory integration.
4. Enter the FQDN or IP address of a directory server in the **Directory Server Address** box.
5. Enter the directory server port number in the **Directory Server LDAP Port** box.
6. Enter the location of this iLO instance in the directory tree in the **LOM Object Distinguished Name** box.
7. Enter valid search contexts in one or more of the **Directory User Context** boxes.
8. Click **Apply Settings**.
9. To test the communication between the directory server and iLO, click **Test Settings**.
10. Optional: To configure directory groups, click **Administer Groups** to navigate to the **User Administration** page.

HPE Extended Schema directory settings

- **Use HPE Extended Schema**—Selects directory authentication and authorization by using directory objects created with the HPE Extended Schema. Select this option when the directory has been extended with the HPE Extended Schema. The HPE extended schema works only with Microsoft Windows.
- **Directory Server Address**—Specifies the network DNS name or IP address of the directory server. The directory server address can be up to 127 characters.

  If you enter the FQDN, ensure that the DNS settings are configured in iLO.

  Hewlett Packard Enterprise recommends using DNS round-robin when you define the directory server.
- **Directory Server LDAP Port**—Specifies the port number for the secure LDAP service on the server. The default value is 636. If your directory service is configured to use a different

port, you can specify a different value. Make sure that you enter a secured LDAP port. iLO cannot connect to an unsecured LDAP port.

- **LOM Object Distinguished Name**—Specifies where this iLO instance is listed in the directory tree (for example, `cn=Mail Server,ou=Management Devices,o=ab`). This option is available when **Use HPE Extended Schema** is selected.

  User search contexts are not applied to the LOM object DN when iLO accesses the directory server.

- **Directory User Contexts**—These boxes enable you to specify common directory subcontexts so that users do not need to enter their full DNs at login. Directory user contexts can be up to 128 characters.

Directory user contexts

You can identify the objects listed in a directory by using unique DNs. However, DNs can be long, users might not know their DNs, or users might have accounts in different directory contexts. When you use user contexts, iLO attempts to contact the directory service by DN, and then applies the search contexts in order until login is successful.

- **Example 1**—If you enter the search context **`ou=engineering,o=ab`**, you can log in as **`user`** instead of logging in as `cn=user,ou=engineering,o=ab`.
- **Example 2**—If the Information Management, Services, and Training departments manage a system, the following search contexts would enable users in these departments to log in by using their common names:

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

  If a user exists in both the `IM` organizational unit and the `Training` organizational unit, login is first attempted as `cn=user,ou=IM,o=ab`.

- **Example 3 (Active Directory only)**—Microsoft Active Directory allows an alternate user credential format. A user can log in as `user@domain.example.com`. Entering the search context **`@domain.example.com`** allows the user to log in as `user`. Only a successful login attempt can test search contexts in this format.

Local user accounts with Kerberos authentication and directory integration

Local user accounts can be active when you configure iLO to use a directory or Kerberos authentication. In this configuration, you can use local and directory-based user access.

Consider the following:

- When local user accounts are enabled, configured users can log in by using locally stored user credentials.
- When local accounts are disabled, user access is limited to valid directory credentials.
- Do not disable local user access until you have validated access through Kerberos or a directory.
- When you use Kerberos authentication or directory integration, Hewlett Packard Enterprise recommends enabling local user accounts and configuring a user account with administrator privileges. This account can be used if iLO cannot communicate with the directory server.
- Access through local user accounts is enabled when directory support is disabled or an iLO license is revoked.

About directory tests

Directory tests enable you to validate the configured directory settings. The directory test results are reset when directory settings are saved, or when directory tests are started.

For the directory test procedure, see “Running directory tests” in the *iLO 4 User Guide*.

Using encryption

iLO provides enhanced security for remote management in distributed IT environments. SSL encryption protects web browser data. SSL encryption of HTTP data ensures that the data is secure as it is transmitted across the network.

If enabled, iLO enforces the use of these enhanced ciphers (both AES and 3DES) over the secure channels, including secure HTTP transmissions through the browser, SSH port, and XML port. When AES/3DES encryption is enabled, you must use a cipher strength equal to or greater than AES/3DES to connect to iLO through these secure channels. The AES/3DES encryption enforcement setting does not affect communications and connections over less-secure channels. By default, Remote Console data uses 128-bit RC4 bidirectional encryption. The HPQLOCFG utility uses 168-bit 3DES with RSA, and a SHA1 MAC cipher to securely send RIBCL scripts to iLO over the network. iLO firmware supports Federal Information Processing Standard (FIPS) Mode.

NOTE: The term *FIPS Mode* is used in this document and in iLO to describe the feature, not its validation status.

iLO supports the following ciphers when **FIPS Mode** or **Enforce AES/3DES Encryption** is enabled and iLO is restricted to TLS version 1.2.

- 256-bit AESGCM with RSA, ECDH, and a AEAD MAC (ECDHE-RSA-AES256-GCM-SHA384)
- 256-bit AES with RSA, ECDH, and a SHA384 MAC (ECDHE-RSA-AES256-SHA384)
- 256-bit AESGCM with RSA, DH, and a AEAD MAC (DHE-RSA-AES256-GCM-SHA384)
- 256-bit AES with RSA, DH, and a SHA256 MAC (DHE-RSA-AES256-SHA256)
- 256-bit AESGCM with RSA, and a AEAD MAC (AES256-GCM-SHA384)
- 256-bit AES with RSA, and a SHA256 MAC (AES256-SHA256)
- 128-bit AESGCM with RSA, ECDH, and a AEAD MAC (ECDHE-RSA-AES128-GCM-SHA256)
- 128-bit AES with RSA, ECDH, and a SHA256 MAC (ECDHE-RSA-AES128-SHA256)
- 128-bit AESGCM with RSA, DH, and a AEAD MAC (DHE-RSA-AES128-GCM-SHA256)
- 128-bit AES with RSA, DH, and a SHA256 MAC (DHE-RSA-AES128-SHA256)
- 128-bit AESGCM with RSA, and a AEAD MAC (AES128-GCM-SHA256)
- 128-bit AES with RSA, and a SHA256 MAC (AES128-SHA256)

FIPS is a set of standards mandated for use by United States government agencies and contractors. FIPS Mode in iLO 4 firmware v2.50 meets the requirements of FIPS 140-2 level 1.
.

Viewing encryption enforcement settings

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

The **Encryption Settings** page displays the cipher in use, and allows you to configure **FIPS Mode** or **Enforce AES/3DES Encryption**.

Figure 6 Security-Encryption Settings page

The -**Encryption Settings** page displays the current encryption settings for iLO.

- **Current Negotiated Cipher**—The cipher in use for the current browser session. After you log in to iLO through the browser, the browser and iLO negotiate a cipher setting to use during the session.
- **Encryption Enforcement Settings**—The current encryption settings for iLO:
  - **FIPS Mode**—Indicates whether FIPS Mode is enabled or disabled for this iLO system.
  - **Enforce AES/3DES Encryption**—Indicates whether AES/3DES encryption is enforced for this iLO system.

    When enabled, iLO accepts only those connections through the browser and SSH interface that meet the minimum cipher strength. A cipher strength of at least AES or 3DES must be used to connect to iLO when this setting is enabled.

IMPORTANT: Once FIPS is enabled, it cannot be disabled with this switch. It must be disabled by restoring the iLO to factory defaults as described elsewhere in this document.

Modifying the AES/DES encryption setting

You must have the Configure iLO Settings privilege to change the encryption settings. To modify the AES/DES encryption setting:

1. Navigate to the **Administration→Security→Encryption** page.
2. Change the **Enforce AES/3DES Encryption** setting to **Enabled** or **Disabled**.
3. To end your browser connection and restart iLO, click **Apply**.

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

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

Connecting to iLO by using AES or 3DES encryption

After you enable the Enforce AES/3DES Encryption setting, iLO requires that you connect through secure channels (web browser, SSH connection, or XML channel) by using a cipher strength of at least AES or 3DES.

- Web browser—You must configure the browser with a cipher equal to or greater than AES/3DES. If the browser is not using AES or 3DES ciphers, iLO displays an error message. The error text varies depending on the installed browser.

  Different browsers use different methods for selecting a negotiated cipher. For more information, see your browser documentation. You must log out of iLO through the current browser before changing the browser cipher setting. Any changes made to the browser

cipher setting while you are logged in to iLO might enable the browser to continue using a non-AES/3DES cipher.

- SSH connection—For instructions on setting the cipher strength, see the SSH utility documentation.
- XML channel—HPQLOCFG uses a secure 3DES cipher by default. For example, HPQLOCFG displays the following cipher strength in the XML output:

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

Enabling FIPS Mode

Prerequisites

- Configure iLO Settings privilege
- Install a trusted certificate for iLO. The default issued SSL certificate is not allowed in FIPS mode.

IMPORTANT: Some interfaces to iLO, such as supported versions of IPMI and SNMP, are not FIPS compliant and cannot be made FIPS compliant.

- Change the default password.
- Turn off SNMP and IPMI

To enable FIPS Mode for iLO:

1. Optional: Capture the current iLO configuration by using HPONCFG. For more information, refer to the iLO 4 scripting and command line guide.
2. Navigate to the **Administration→Security→Encryption** page.
3. Set FIPS Mode to **Enabled**.

CAUTION: Enabling FIPS Mode resets iLO to the factory default settings, and clears all user and license data.

4. Click **Apply**.

   iLO prompts you to confirm the request.
5. To confirm the request to enable FIPS mode, click **OK**

   iLO reboots in FIPS mode. Wait at least 90 seconds before attempting to re-establish a connection.
6. (Optional) Restore the iLO configuration by using HPONCFG. For more information, see the iLO 4 scripting and command line guide.

TIP: You can use the Login Security Banner feature to notify iLO users that a system is using FIPS Mode.

7. Reapply the Advanced Pack license if applicable.

Disabling FIPS Mode

If you want to disable FIPS Mode for iLO (for example, if a server is decommissioned), you must set iLO to the factory default settings. You can perform this task by using RIBCL scripts, iLO RBSU, or the iLO 4 Configuration Utility.

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

5 HPE Single Sign-On

HPE Single Sign-On (SSO) enables you to browse directly from an HPE SSO-compliant application (such as HPE SIM and HPE OneView) to iLO, bypassing an intermediate login step. To use SSO, you must have a supported version of an SSO-compliant application, and you must configure the iLO processor to trust the SSO-compliant application. This feature and many others are part of an iLO licensing package. For more information about iLO licensing, go to **http://www.hpe.com/info/ilo/licensing**.

iLO contains support for SSO applications to determine the minimum SSO certificate requirements. Some SSO-compliant applications automatically import trust certificates when they connect to iLO. For applications that do not do this automatically, use the HPE SSO page to configure the SSO settings through the iLO web interface. You must have the Configure iLO Settings privilege to change these settings.

Configuring iLO for HPE SSO

Prerequisites

- Configure iLO Settings privilege
- An iLO license that supports this feature is installed. For more information, see the following website: **http://www.hpe.com/info/ilo/licensing**.

Configuring HPE SSO

1. Navigate to the **Administration→Security→HPE SSO** page.
2. Configure the **Single Sign-On Trust Mode** by selecting **Trust by Certificate**, **Trust by Name**, or **Trust All**.

   The iLO firmware supports configurable trust modes, which enables you to meet your security requirements. The trust mode affects how iLO responds to SSO requests. If you enable support for SSO, Hewlett Packard Enterprise recommends using the **Trust by Certificate** mode. The available modes follow:

   - **Trust None (SSO disabled)** (default)—Rejects all SSO connection requests
   - **Trust by Certificate** (most secure)—Enables SSO connections from an SSO-compliant application by matching a certificate previously imported to iLO
   - **Trust by Name**—Enables SSO connections from an SSO-compliant application by matching a directly-imported IP address or DNS name.
   - **Trust All** (least secure)—Accepts any SSO connection initiated from any SSO-compliant application.
3. Configure iLO privileges for each role in the **Single Sign-On Settings** section.

   When you log in to an SSO-compliant application, you are authorized based on your SSO-compliant application role assignment. The role assignment is passed to iLO when SSO is attempted.

   SSO attempts to receive only the privileges assigned in this section. iLO directory settings do not apply. Default privilege assignments are as follows:

   - **User**—Login only
   - **Operator**—Login, Remote Console, Power and Reset, and Virtual Media
   - **Administrator**—Login, Remote Console, Power and Reset, Virtual Media, Configure iLO, and Administer Users
4. Click **Apply** to save the SSO settings.

5. If you selected **Trust by Certificate** or **Trust by Name**, add the trusted certificate or DNS name to iLO.
6. After you configure SSO in iLO, log in to an SSO-compliant application and browse to iLO. For example, log in to HPE SIM, navigate to the **System** page for the iLO processor, and then click the iLO link in the **More Information** section.

NOTE: Although a system might be registered as a trusted server, SSO might be refused because of the current trust mode or certificate status. For example, if HPE SIM server name is registered, and the trust mode is **Trust by Certificate**, but the certificate is not imported, SSO is not allowed from that server. Likewise, if HPE SIM server certificate is imported, but the certificate has expired, SSO is not allowed from that server. The list of trusted servers is not used when SSO is disabled. iLO does not enforce SSO server certificate revocation.

Adding trusted certificates

iLO users who have the Configure iLO Settings privilege can install trusted certificates or add direct DNS names. The Base64-encoded X.509 certificate data resembles the following:

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

To add trusted SSO records by using the iLO web interface:

1. Navigate to the **Administration→Security→HP SSO** page.
2. Use one of the following methods to add a trusted certificate:
   - To directly import a trusted certificate, copy the Base64-encoded certificate X.509 data, paste it into the text box above the **Import Certificate** button, and then click the button.
   - To indirectly import a trusted certificate, type the DNS name or IP address in the text box above the **Import Certificate from URL** button, and then click the button. iLO contacts the SSO-compliant application over the network, retrieves the certificate, and then saves it.

You can use one the following links to extract HPE SIM certificates:

- For HPE SIM versions earlier than 7.0:

  ```
  http://<HP SIM name or network address>:280/GetCertificate
  https://<HP SIM name or network address>:50000/GetCertificate
  ```

- For HPE SIM 7.0 or later:

  ```
  http://<HP SIM name or networkaddress>:280/GetCertificate?certtype=sso
  https://<HP SIM name or networkaddress>:50000/GetCertificate?certtype=sso
  ```

NOTE: All request parameters are case-sensitive. If you capitalize the lowercase certtype parameter, the parameter will not be read, and HPE SIM will return the default HPE SIM server certificate instead of a trust certificate.

- Export the certificate from HPE SIM:
  - For HPE SIM versions earlier than 7.0:

    Select **Options→Security→Certificates→Server Certificate**.
  - For HPE SIM 7.0 or later:

    Select **Options→Security→HP Systems Insight Manager Server Certificate**, and then click **Export**.
- Use the HPE SIM command-line tools. For example, using the alias `tomcat` for the HPE SIM certificate, enter **`mxcert -l tomcat`**.

For more information, see the SIM documentation.

Viewing trusted certificates

The Manage Trusted Certificates table on the Single Sign-On Settings page displays the status of the trusted certificates configured to use SSO with the current iLO management processor.

- **Status**—The status of the record (if any are installed).
- **Certificate**—Indicates that the record contains a stored certificate. Move the cursor over the icon to view the certificate details, including subject, issuer, and dates.
- **Description**—The server name (or certificate subject).

Removing trusted certificates

1. Navigate to the **Administration→Security→HP SSO** page.
2. Select one or more records in the **Manage Trusted Certificates and Records** table.

   Click **Delete**. iLO prompts you to confirm that you want to delete the certificate or record.

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

3. Click **Yes**.

6 Configuring Remote Console security settings

Use the Remote Console security settings to control the Remote Console Computer Lock settings and the Integrated Remote Console Trust settings.

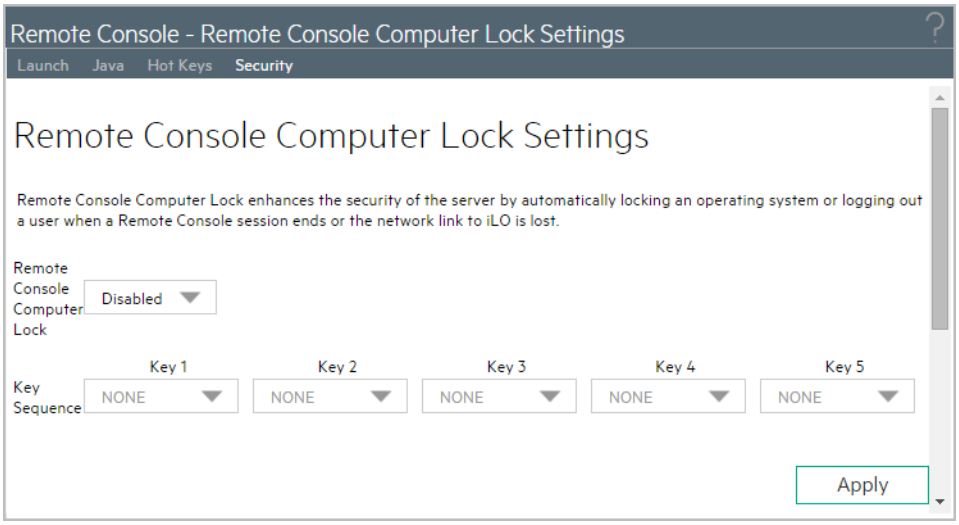
Prerequisites

Configure iLO Settings privilege

Configuring Remote Console Computer Lock settings

Remote Console Computer Lock enhances the security of an iLO-managed server by automatically locking an operating system or logging out a user when a Remote Console session ends or the network link to iLO is lost. If you open a .NET IRC or Java IRC window when this feature is configured, the operating system will be locked when you close the window.

1. Navigate to the **Remote Console→Security** page.



2. Select from the following **Remote Console Computer Lock** settings:
   - **Windows**—Use this option to configure iLO to lock a managed server running a Windows operating system. The server automatically displays the **Computer Locked** dialog box when a Remote Console session ends or the iLO network link is lost.
   - **Custom**—Use this option to configure iLO to use a custom key sequence to lock a managed server or log out a user on that server. You can select up to five keys from the list. The selected key sequence is sent automatically to the server operating system when a Remote Console session ends or the iLO network link is lost.
   - **Disabled**(default)—Use this option to disable the Remote Console Computer Lock feature. Terminating a Remote Console session or losing an iLO network link will not lock the operating system on the managed server.
3. Select a computer lock key sequence.
4. Click **Apply** to save the changes.

Valid Remote Console Computer Lock keys

You can create a Remote Console Computer Lock key sequence by using the keys listed in Table 2 (page 33):

Table 2 Remote Console Computer Lock keys

ESC	SCRL LCK	1	g
L_ALT	SYS RQ	2	h
R_ALT	F1	3	i
L_SHIFT	F2	4	j
R_SHIFT	F3	5	k
L_CTRL	F4	6	l
R_CTRL	F5	7	m
L_GUI	F6	8	n
R_GUI	F7	9	o
INS	F8	;	p
DEL	F9	=	q
HOME	F10	[	r
END	F11	\	s
PG_UP	F12	]	t
PG_DN	" " (space)	'	u
ENTER	'	a	v
TAB	,	b	w
BREAK	-	c	x
BACKSPACE	.	d	y
NUM PLUS	/	e	z
NUM MINUS	0	f	

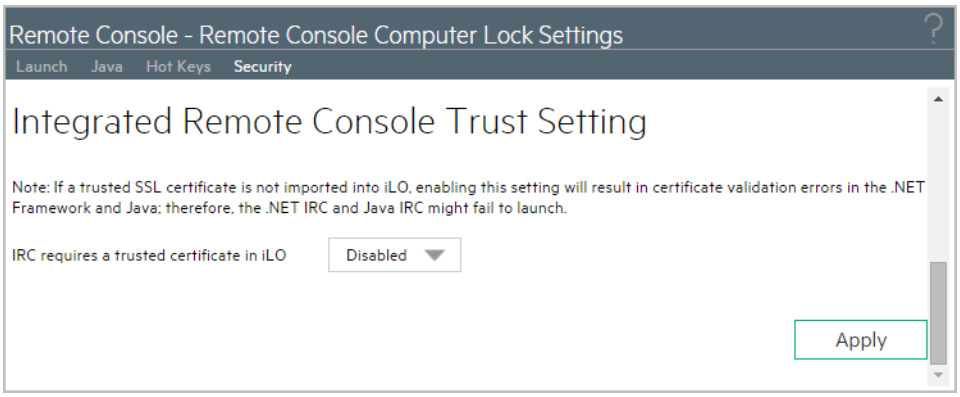
Configuring Integrated Remote Console Trust settings (.NET IRC)

The .NET IRC is launched through Microsoft ClickOnce, which is part of the Microsoft .NET Framework. ClickOnce requires that any application installed from an SSL connection be from a trusted source. If a browser is not configured to trust an iLO processor, and the Integrated Remote Console Trust setting is set to **Enabled**, ClickOnce displays the following error message:

```
Cannot Start Application – Application download did not succeed...
```

To specify whether all clients that browse to this iLO require a trusted iLO certificate to run the .NET IRC:

1. Navigate to the **Remote Console→Security** page.



2. Select one of the following in the **Integrated Remote Console Trust Setting** section:
   - **Enabled**—The .NET IRC is installed and runs only if this iLO certificate and the issuer certificate have been imported and are trusted.
   - **Disabled**(default)—When you launch the .NET IRC, the browser installs the application from a non-SSL connection. SSL is still used after the .NET IRC starts to exchange encryption keys.
3. Click **Apply**.

7 Configuring the Login Security Banner

The Login Security Banner feature allows you to configure the security banner displayed on the iLO login page. For example, you could enter a message indicating that an iLO system uses FIPS Mode.

Prerequisites

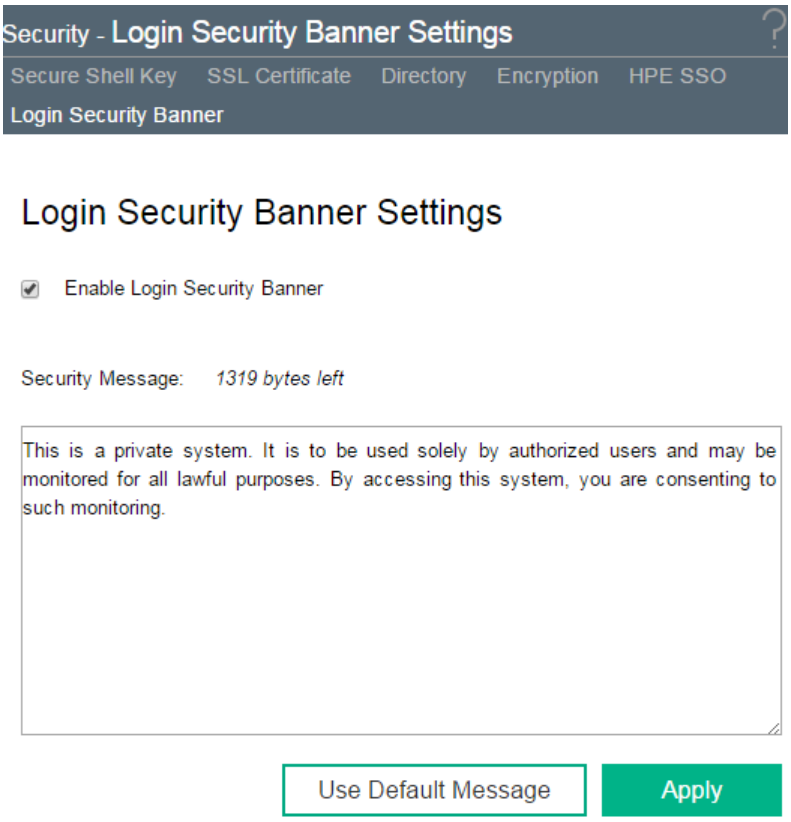
Configure iLO Settings privilege

Enabling the Login Security Banner

1. Navigate to the **Administration→Security→Login Security Banner** page.
2. Select the **Enable Login Security Banner** check box.

   iLO uses the following default text for the Login Security Banner:

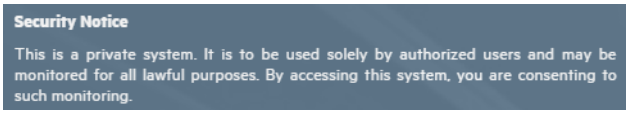
   ```
   This is a private system. It is to be used solely by authorized
   users and may be monitored for all lawful purposes. By accessing
   this system, you are consenting to such monitoring.
   ```
3. Optional: To customize the security message, enter a custom message in the **Security Message** text box.



The byte counter above the text box indicates the remaining number of bytes allowed for the message. The maximum is 1,500 bytes.

TIP: Click **Use Default Message** to restore the default text.

4. Click **Apply**.
   The security message is displayed at the next login.



8 IT infrastructure security considerations

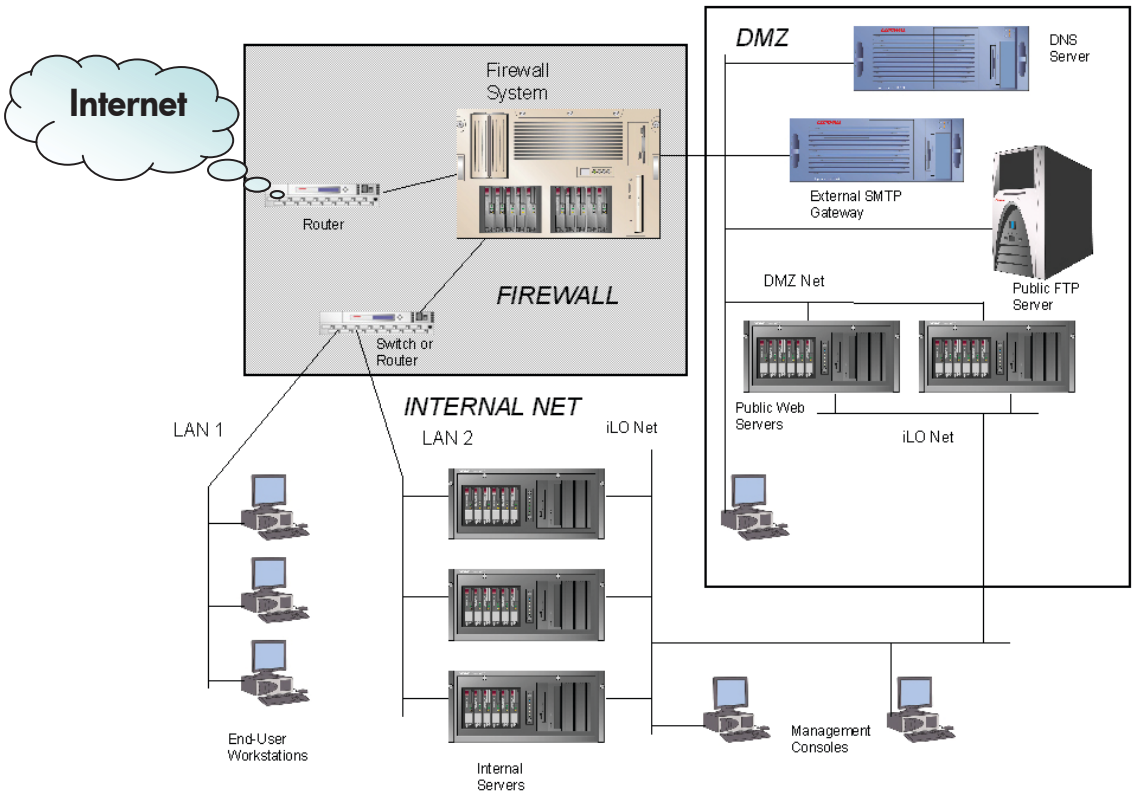
The following sections describe iLO security in two particular IT environments:

- When operating in the infrastructure between an external firewall and an internal network (DMZ)
- When operating in a server blade environment

Operating iLO servers in the DMZ

An Internet-connected architecture typically has a more secure, de-militarized zone (DMZ). The DMZ zone lies between the corporate servers and the Internet. It usually has firewalls that restrict traffic flow between the corporate/Internet areas. This architecture lets you access servers that provide publicly available Internet services through a firewall, but you cannot access these services on the internal network. This more secure zone provides an area isolated from the internal network and hardened against external attack (Figure 7 (page 37)). The security challenges in the DMZ require a careful balance between critical security requirements and the need to effectively manage and maintain the systems.

Figure 7 Example configuration of a DMZ



iLO can exist on a separate, secondary network (iLO Net in Figure 14) parallel to the primary or production network. This dual-network architecture segregates management traffic from production network traffic. It allows system-wide server management activities, including servers inside the DMZ, while maintaining maximum security by limiting access to the production network.

Figure 7 (page 37) shows a packet-filtering router that acts as an initial line of defense. Behind this router is a firewall system. There is no direct connection from the Internet or the external router to the internal network. All traffic to or from the internal network must pass through the

firewall system. An additional router filters packets destined for the public services in the DMZ and protects the internal network from public access.

The firewall is a multi-targeted server that you can configure to evaluate traffic according to different rules based on the traffic source and destination:

- From the Internet to the DMZ
- From the DMZ to the Internet
- From the Internet to the internal network
- From the internal network to the internet
- From the DMZ to the internal network
- From the internal network to the DMZ

Servers inside the DMZ and on the internal network can use iLO processors. There is no possibility for data to flow between the DMZ network and the iLO network because the network connection to iLO is completely isolated from the network ports on the server. Even if the DMZ network were compromised, the iLO network would remain secure. This lets you use iLO on servers located in the DMZ or in the internal network without compromising sensitive data. Administrators create this separation by using a dedicated NIC or the SNP with its VLAN (see the section “Shared network port” (page 9)).

For best protection of the servers operating inside the DMZ, set the SNMP trap destinations to the loop back address and enable the SNMP pass-thru in iLO to route traps onto the iLO network. This SNMP pass-thru option does not activate all management functions. However, it does pass status, inventory, and fault information to HPE SIM or another SNMP-capable management application. This option is very secure because the OS does not recognize the iLO product as a NIC.

The Rapid Deployment Pack Deployment Server Console provides secure access to the management functions of iLO and Remote Insight Lights-Out Edition (RILOE).

The ProLiant Integration Module includes:

- Intelligent Provisioning Scripting Toolkit
- Configuration Events for industry-standard operating systems
- Sample unattended files
- ProLiant Support Packs containing software drivers and management agents

Administrators can deploy servers through scripting using the Intelligent Provisioning Scripting Toolkit. HPE Rapid Deployment Pack is a part of HPE Insight Control Management Software. See the Hewlett Packard Enterprise website **http://www.hpe.com/servers/rdp-we** for more information about Insight Control Management Software.

Communication between iLO and server blades

The HPE BladeSystem architecture uses a single enclosure to hold multiple servers. A separate power subsystem provides power to all servers in that enclosure. ProLiant c-Class server blades use iLO to send alerts and management information throughout the server blade infrastructure.

There is a strict communication hierarchy among ProLiant c-Class server components. The Onboard Administrator (OA) management module communicates with the iLO processor on each server blade. The OA module provides independent IP addresses for each server blade. The iLO device on a server blade also maintains an independent IP address. The iLO firmware exclusively controls any communication from iLO to the OA module. There is no path from an iLO processor on one server blade to the iLO processor on another blade. There is no connection from the iLO processor or OA module to the server NICs. The iLO processor only has information about the presence of other server blades in the infrastructure and whether enough amperage

is available from the power subsystem to boot the iLO server blade. A single, physical port on the rear of the BladeSystem enclosure provides access to the iLO network connections on the server blade. This simplifies and reduces cabling.

Security audits

A company's policy may mandate periodic security audits. iLO maintains an event log containing date- and time-stamped information pertaining to events that occurred in the iLO configuration and operation. You can manually access this log through the System Status tab of the iLO browser interface. You can also use XML commands to set up an automated examination and extraction process that parses the event log by date/time and by authenticated user for accessing information about security events.

Security Vulnerability Scanners and iLO

Security Vulnerability Scanners are tools commonly used in server environments to probe for weaknesses that need to be investigated and addressed. The iLO team uses Security Vulnerability Scanners in our quality labs for every release of iLO firmware. There are known issues and best practices associated with the use of Security Vulnerability Scanners.

A best practice is to test new versions of Security Vulnerability Scanners in a lab environment before deploying to a production environment. By definition the Security Vulnerability Scanner is probing interfaces for known or suspected vulnerabilities. In effect, the scanner is attempting to hack the interface being tested. This operation may have a negative impact on the stability of the system being scanned. Therefore, it makes sense to start on a small scale and then move to a wider scale and production environment.

There are some known issues that most Security Vulnerability Scanners will identify. These items are listed in the following sections, and include remediation recommendations.

The referenced documents can be found using the following links:

- HPE iLO 4 user guide: **http://www.hpe.com/support/ilo4_ug_en**
- HPE iLO scripting and command line user guide: **http://www.hpe.com/support/ilo4_cli_gde_en**

X.509 Certificate Subject CN Does Not Match the Entity Name

The customer needs to replace the default, self-signed SSL certificate with a certificate signed by a Certificate Authority. When iLO left the factory, the customer, DNS name/IP address of the server was not known. Therefore, iLO uses a self-signed certificate. iLO firmware provides the capability to create a Certificate Signing Request (CSR) that the customer can use to request/create a signed certificate that matches their system. This signed certificate can then be imported back into the iLO.

This is documented in the HPE iLO 4 user guide.

The CSR process can also be executed using iLO's XML scripting. The specific commands are in the iLO scripting and command line user guide.

IPMI 2.0 RAKP RMCP+ Authentication HMAC Password Hash Exposure

The IPMI handshake that is required in the IPMI specification should be more secure. For customers who are not actively using IPMI, Hewlett Packard Enterprise recommends disabling the IPMI over LAN interface. Instead, Hewlett Packard Enterprise recommends that you use the HPE RESTful programmatic interface and the industry-standard "Redfish" project as a replacement for IPMI over LAN capabilities.

The Security Bulletin for this issue may be found at **http://www.hpe.com/support/iLO234-SB-CVE-2013-4786**

Enabling/Disabling IPMI is documented in the iLO 4 user guide.

Enabling/Disabling IPMI can also be executed using iLO's XML scripting and is documented in the iLO scripting and command line user guide.

Untrusted TLS/SSL server X.509 certificate

The resolution to this issue is the same as the first item. The customer needs to use the CSR process and import a CA-signed certificate.

IPMI 1.5 GetChannelAuth Response Information Disclosure

iLO is not actually susceptible to this vulnerability. It is an assumed vulnerability based on our support of the IPMI protocol. The vulnerability report can be suppressed by disabling IPMI as described in the RAKP vulnerability above.

TCP Sequence Number Approximation Vulnerability

iLO is not actually susceptible to this vulnerability. iLO does use TCP sequence number randomization and is resistant to these attacks.

IPMI 2.0 RAKP RMCP+ Authentication Username Disclosure

The IPMI specification enables a pre-authenticated client to confirm the existence of a configured username. We recommend changing the default username. Additionally, for customers who are not actively using IPMI, we recommend disabling the interface as described in the RAKP vulnerability above.

Weak Cryptographic Key

This vulnerability may be addressed by enabling the "*Enforce AES/3DES"* setting. This will require iLO to use the higher grade ciphers.

This is documented in the iLO 4 user guide.

The CSR process can also be executed using iLO's XML scripting. The specific commands are documented in the iLO scripting and command line user guide.

This vulnerability will also be reported if the default SSL certificate is used. This is addressed, as documented above, by creating a Certificate Signing Request and importing a CA-signed certificate.

TCP timestamp response

This is a standard TCP behavior. The theory is that this can be used to estimate the uptime of the system, which could then be used for further attacks. This has a very low CVE vulnerability rating of 1.

9 Security best practices

iLO mitigates many of the inherent security risks of a networked environment through strong authorization, authentication, and encryption. You can further decrease the chance of attacks by following security recommendations, being aware of access points to the iLO devices and their servers, and configuring their networks to eliminate unnecessary services.

Hewlett Packard Enterprise recommends that you observe the following security practices:

- Use a separate management network. We recommend that you establish a private management network separate from your data network and that only administrators have access to that management network.
- If you connect iLO devices to a shared network, consider the iLO devices as separate servers and include them in security and network audits.
- Do not connect iLO directly to the Internet. The iLO processor is a management and administration tool, not an Internet gateway. Connect to the Internet using a corporate VPN that provides firewall protection.
- Change passwords frequently if using local accounts. Change the default iLO password immediately to a more relevant password. You should change the iLO management passwords with the same frequency and according to the same guidelines as the server administrative passwords. Passwords should include at least three of these four character types; numeric, special, lowercase, and uppercase
- Implement directory services. This allows authentication and authorization using the same login process throughout the network. It provides a way to control multiple iLO devices simultaneously. Directories provide role-based access to iLO with very specific roles and privileges based on time and location.
- Implement two-factor authentication. This provides additional security, especially when you can make connections remotely or outside the local network.
- Protect SNMP traffic. Reset the community strings according to the same guidelines as the administrative passwords. Also set firewalls or routers to accept only specific source and destination addresses. Disable SNMP at the server if you don’t need it. You can also disable the iLO SNMP pass-thru.
- Replace the default self-signed certificate with one from a trusted CA.
- Enable the universal data center lock, where available.
- Enable AES/3DES encryption or better. For even stronger protection, enable FIPS mode.
- Disable IPMI.
- Decide whether to disable F8 BIOS access. Customers who want to secure iLO against host administrators may want to enable the **Require Login for iLO RBSU** setting.

IPMI/DCMI settings

iLO supports IPMI 2.0 and DCMI industry standard protocols. IPMI is an industry standard protocol, developed by Intel and supported by over two hundred vendors, such as Hewlett Packard Enterprise, IBM, Dell, Cisco, NEC, Fujitsu-Siemens, and Supermicro. For more information on IPMI, visit Intel’s website at **http://www.intel.com/content/www/us/en/servers/ipmi/ipmi-home.html**

iLO enables you to send industry-standard IPMI and DCMI commands over the LAN. The IPMI/DCMI port is set to 623 and is not configurable. To enable or disable IPMI/DCMI, select or clear the **Enable IPMI/DCMI over LAN on Port 623** check box on the **Access Settings** page of the iLO interface. IPMI/DCMI is enabled by default and allows you to send IPMI/DCMI

commands over the LAN by using a client-side application. When this settings is disabled (cleared), however, server-side IPMI/DCMI applications are still functional.

When using IPMI over LAN, the following guidelines are suggested:

- Segment IPMI traffic from the rest of the network. If using a shared NIC connection, a VLAN for iLO can be used to accomplish this separation. Isolate the IPMI/Management subnet using a firewall and limit access to authorized administrators.
- Do not allow IPMI traffic from outside the network.
- iLO supports IPMI 2.0 which uses stronger encryption than IPMI 1.5. Hewlett Packard Enterprise recommends cipher suites 3 and 17.

Resolved vulnerabilities

In July 2013, the US-CERT issued an alert (TA13–207A)Risks of Using the Intelligent Platform Management Interface (IPMI) (**https://www.us-cert.gov/ncas/alerts/TA13-207A**).

Hewlett Packard Enterprise addressed the vulnerabilities as follows:

- Cipher 0 is an option that allows authentication to be bypassed. iLO addressed this by not allowing cipher 0 to be selected by an IPMI client.
- In the IPMI specification, user ID 1 is used to support anonymous logins. iLO does not support anonymous logins using user ID 1.
- In the IPMI specification, disabled user ID's are configured with usernames and passwords. Often, this is preconfigured in manufacturing to well known user ID's and passwords. iLO does not retain disabled user ID usernames and passwords. iLO has one username preconfigured with a unique password in manufacturing. Hewlett Packard Enterprise suggests that the customer reconfigure this default user immediately per the aforementioned guidelines in this brief.
- While the IPMI specification allows for NULL passwords, iLO does not support the setting of a user password to NULL.
- The IPMI specification requires support for RAKP authentication, which allows remote attackers to obtain password hashes and conduct offline password guessing attacks. As this is part of the IPMI protocol itself, Hewlett Packard Enterprise recommends that IPMI over LAN be disabled if not in use or that the IPMI management subnet be isolated, as discussed above.

Viewing customer advisories, bulletins, and notices

1. Go to **http://www.hpe.com/support/iLO4**.
2. On the left side of the page, under **Knowledge base options**, click one of the following:
   - **Top issues**
   - **Advisories, bulletins & notices**

   .

   The the chosen information appears in tabular format.
3. To narrow the list of Advisories, bulletins and notices, enter iLO4 in the box at the top right.

10 Support and other resources

Accessing Hewlett Packard Enterprise Support

- For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website:

  www.hpe.com/assistance

- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website:

  www.hpe.com/support/hpesc

Information to collect

- Technical support registration number (if applicable)
- Product name, model or version, and serial number
- Operating system name and version
- Firmware version
- Error messages
- Product-specific reports and logs
- Add-on products or components
- Third-party products or components

Accessing updates

- Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method.
- To download product updates, go to either of the following:
  - Hewlett Packard Enterprise Support Center **Get connected with updates** page:

    www.hpe.com/support/e-updates

  - Software Depot website:

    www.hpe.com/support/softwaredepot

- To view and update your entitlements, and to link your contracts, Care Packs, and warranties with your profile, go to the Hewlett Packard Enterprise Support Center **More Information on Access to Support Materials** page:

  www.hpe.com/support/AccessToSupportMaterials

IMPORTANT: Access to some updates might require product entitlement when accessed through the Hewlett Packard Enterprise Support Center. You must have an HP Passport set up with relevant entitlements.

Websites

Website	Link
Hewlett Packard Enterprise Information Library	**www.hpe.com/info/enterprise/docs**
Hewlett Packard Enterprise Support Center	**www.hpe.com/support/hpesc**

Website	Link
Contact Hewlett Packard Enterprise Worldwide	**www.hpe.com/assistance**
Subscription Service/Support Alerts	**www.hpe.com/support/e-updates**
Software Depot	**www.hpe.com/support/softwaredepot**
Customer Self Repair	**www.hpe.com/support/selfrepair**
Insight Remote Support	**www.hpe.com/info/insightremotesupport/docs**
Serviceguard Solutions for HP-UX	**www.hpe.com/info/hpux-serviceguard-docs**
Single Point of Connectivity Knowledge (SPOCK) Storage compatibility matrix	**www.hpe.com/storage/spock**
Storage white papers and analyst reports	**www.hpe.com/storage/whitepapers**

Customer self repair

Hewlett Packard Enterprise customer self repair (CSR) programs allow you to repair your product. If a CSR part needs to be replaced, it will be shipped directly to you so that you can install it at your convenience. Some parts do not qualify for CSR. Your Hewlett Packard Enterprise authorized service provider will determine whether a repair can be accomplished by CSR.

For more information about CSR, contact your local service provider or go to the CSR website:

www.hpe.com/support/selfrepair

Remote support

Remote support is available with supported devices as part of your warranty, Care Pack Service, or contractual support agreement. It provides intelligent event diagnosis, and automatic, secure submission of hardware event notifications to Hewlett Packard Enterprise, which will initiate a fast and accurate resolution based on your product's service level. Hewlett Packard Enterprise strongly recommends that you register your device for remote support.

For more information and device support details, go to the following website:

www.hpe.com/info/insightremotesupport/docs

Documentation feedback

Hewlett Packard Enterprise is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (**docsfeedback@hpe.com**). When submitting your feedback, include the document title, part number, edition, and publication date located on the front cover of the document. For online help content, include the product name, product version, help edition, and publication date located on the legal notices page.

A Access Options

Table 3 Access options

Option	Default value	Description
Idle Connection Timeout (minutes)	30	This setting specifies how long a user can be inactive, in minutes, before the session ends automatically. Valid settings are: 15, 30, 60, 120 minutes, or Infinite. Inactive users are not logged out when this value is set to Infinite. Failure to log out of iLO can produce an idle connection. The iLO firmware supports a finite number of iLO connections. Use of the Infinite timeout option might make iLO inaccessible to other users.
iLO Functionality	Enabled	The iLO network and communications with operating system drivers are terminated when iLO functionality is disabled. If iLO functionality is disabled, you must use the server Security Override Switch to enable iLO. The iLO functionality cannot be disabled on blade servers.
iLO ROM-Based Setup Utility or iLO 4 Configuration Utility (UEFI)	Enabled	The name of this setting depends on whether your system supports the iLO ROM-Based Setup Utility or the HPE UEFI System Utilities. This setting enables or disables iLO RBSU or the iLO 4 Configuration Utility. On servers that support iLO RBSU, the iLO Option ROM prompts you to press F8 to start iLO RBSU. If this option is set to Disabled, the prompt is not displayed. On servers that support the UEFI System Utilities, if this option is set to Disabled, the iLO 4 Configuration Utility menu item is not available when you access the utilities.
Require Login for iLO RBSU or Require Login for iLO 4 Configuration Utility (UEFI)	Disabled	The name of this setting depends on whether your system supports the iLO ROM-Based Setup Utility or the UEFI System Utilities. This setting determines whether a user-credential prompt is displayed when a user accesses iLO RBSU or the iLO 4 Configuration Utility. If this setting is Enabled, a login dialog box opens when you access the iLO RBSU or the iLO 4 Configuration Utility.
Show iLO IP during POST	Enabled	This setting enables the display of the iLO network IP address during host server POST.
Serial Command Line Interface Status	Enabled-Authentication Required	This setting enables you to change the login model of the CLI feature through the serial port. The following settings are valid: Enabled-Authentication Required Serial Command Line Interface Status Enabled-Authentication Required—Enables access to the iLO CLP from a terminal connected to the host serial port. Valid iLO user credentials are required. Enabled-No Authentication—Enables access to the iLO CLP from a terminal connected to the host serial port. iLO user credentials are not required. Disabled—Disables access to the iLO CLP from the host serial port. Use this option if you are planning to use physical serial devices.
Serial Command Line Interface Speed	9600	This setting enables you to change the speed of the serial port for the CLI feature. The following speeds (in bits per second) Serial Command Line 9600 Interface Speed are valid: 9600, 19200, 38400, 57600, and 115200. The serial port configuration must be set to no parity, 8 data bits, and 1 stop bit (N/8/1) for correct operation. The serial port speed set by this option should match the speed of the serial port configured in the iLO RBSU or the iLO 4 Configuration Utility. **NOTE:** The 38400 speed is not currently supported by the iLO RBSU or the iLO 4 Configuration Utility.
Virtual Serial Port Log	Disabled	This setting enables or disables logging of the Virtual Serial Port. When enabled, Virtual Serial Port activity is logged to Virtual Serial Port Log Disabled a 150-page circular buffer in the iLO memory, and can be viewed using the CLI command vsp log. The Virtual Serial Port buffer size is 128 KB. This feature and many others are part of an iLO licensing package.
Minimum Password Length	8	This setting specifies the minimum number of characters allowed when a user password is set or changed. The character length must be a value from 0 to 39.

Table 3 Access options *(continued)*

Option	Default value	Description
Server Name		This setting enables you to specify the host server name. You can assign this value manually, but it might be overwritten by the host software when the operating system loads. Server Name — You can enter a server name that is up to 49 bytes. To force the browser to refresh, save this setting, and then press F5.
Server FQDN/IP Address		This setting enables you to specify the server FQDN or IP address. You can assign this value manually, but it might be Server FQDN/IP Address — overwritten by the host software when the operating system loads. You can enter an FQDN or IP address that is up to 255 bytes. To force the browser to refresh, save this setting, and then press F5.
Authentication Failure Logging	Enabled-Every 3rd Failure	This setting enables you to configure logging criteria for failed authentications. All login types are supported; each login type works independently. The following are valid settings: Enabled-Every 3rd Failure Authentication Failure Logging Enabled-Every Failure—A failed login log entry is recorded after every failed login attempt. Enabled-Every 2nd Failure—A failed login log entry is recorded after every second failed login attempt. Enabled-Every 3rd Failure—A failed login log entry is recorded after every third failed login attempt. Enabled-Every 5th Failure—A failed login log entry is recorded after every fifth failed login attempt. Disabled—No failed login log entry is recorded
Authentication Failure Delay Time—	10 seconds	Enables you to configure the duration of the iLO login delay after a failed login attempt. The following values are valid: 2, 5, 10, and 30 seconds.
Authentication Failures Before Delay	1	Enables you to configure the number of failed login attempts that are allowed before iLO imposes a login delay. The following values are valid: 1, 3, 5, or every failed login attempt.

B SSH2 support

Table 4 iLO SSH feature support

	SSH2 Standard	iLO 3 SSH	iLO 4 2.20
Encryption (same set supported both ways)			
3des-cbc	Required	Supported	Supported
blowfish-cbc	Recommended	Not supported	Not supported
twofish256-cbc	Optional	Not supported	Not supported
twofish192-cbc	Optional	Not supported	Not supported
twofish128-cbc	Recommended	Not supported	Not supported
aes256-cbc	Optional	Supported	Supported
aes192-cbc	Optional	Supported	Not supported
aes128-cbc	Recommended	Supported	Supported
serpent256-cbc	Optional	Not supported	Not supported
serpent192-cbc	Optional	Not supported	Not supported
serpent128-cbc	Optional	Not supported	Not supported
Arcfour	Optional	Not supported	Not supported
idea-cbc	Optional	Not supported	Not supported
cast128-cbc	Optional	Not supported	Not supported
None	Optional, but not recommended	Not supported	Not supported
Hashing algorithm			
Hmac-sha1	Required	Supported	Supported
Hmac-sha1-96	Recommended	Not supported	Not supported
Hmac-md5	Optional	Not supported	Supported[1]
Hmac-md5-96	Optional	Not supported	Not supported
None	Optional	Not supported	Not supported
Compression			
Zlib	Optional	Not supported	Not supported
None	Required	Supported	Supported
Language			
English (same as current Telnet)		Supported	Supported
Key exchange			
Diffe-Hellman-group1-sha1	Required	Supported	Supported[1]
Diffe-Hellman-group14-sha1	Not supported	Not supported	Supported
Public Key algorithms			
ssh-dss	Required	Supported	Supported

Table 4 iLO SSH feature support *(continued)*

	SSH2 Standard	iLO 3 SSH	iLO 4 2.20
ssh-rsa	Recommended	Not supported	Supported
X509v3-sign-rsa (certificates)	Optional	Not supported	Not supported
X509v3-sign-dss (certificates)	Optional	Not supported	Not supported
Spki-sign-rsa (certificates)	Optional	Not supported	Not supported
Spki-sign-dss (certificates)	Optional	Not supported	Not supported
Pgp-sign-rsa (certificates)	Optional	Not supported	Not supported
Pgp-sign-dss (certificates)	Optional	Not supported	Not supported
Client/User Authentication Method			
None	Must not be listed		
Public key	Required	Supported	Supported
Server based	Optional	Not Supported	Not Supported
Password		Supported	Supported
Client/User authentication parameters			
Default authentication timeout	10 minutes recommended	Hardcoded to 10 minutes	Hardcoded to 10 minutes
Default SSH port	Default 22	Configurable. Defaults to 22.	Configurable. Defaults to 22.
Default number of attempts	20 recommended	Hardcoded to 3	Hardcoded to 3
User initiated key generation		Not supported	Not supported

[1] Not supported in FIPS mode or Forced AES mode)