NEC

iLO 5
User's Guide

NEC Express Server

Express5800 Series

2017/10

Notices

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

Confidential computer software. Valid license from NEC Corporation 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 NEC Corporation website. NEC Corporation has no control over and is not responsible for information outside the NEC Corporation website.

Acknowledgments

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

Java® and Oracle® are registered trademarks of Oracle and/or its affiliates. Google™ is a

trademark of Google Inc.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Red Hat® is a registered trademark of Red Hat, Inc. in the United States and other countries.

SD is a trademark or registered trademark of SD-3C in the United States, other countries or both.

VMware® is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions.

Redfish® is a registered trademark of Distributed Management Task Force.

Contents

1.iLO

iLO 5 is a remote server management processor embedded on the system boards of NEC Express servers. iLO enables the monitoring and controlling of servers from remote locations. iLO management is a powerful tool that provides multiple ways to configure, update, monitor, and repair servers remotely. iLO (Standard) comes preconfigured on servers without an additional cost or license.

Features that enhance server administrator productivity and additional new security features are licensed.

iLO key features

- **Server health monitoring**—iLO monitors temperatures in the server and sends corrective signals to the fans to maintain proper server cooling. iLO also monitors installed firmware and software versions and the status of fans, memory, the network, processors, power supplies, storage, and devices installed on the system board.
- **Agentless Management**—With Agentless Management, the management software (SNMP) operates within the iLO firmware instead of the host OS. This configuration frees memory and processor resources on the host OS for use by server applications. iLO monitors all key internal subsystems, and can send SNMP alerts directly to a central management server, even with no host OS installed.
- **Integrated Management Log**—View server events and configure notifications through SNMP alerts, remote syslogs, and email alerts.
- **Active Health System Log**—Download the Active Health System log. You can send the log file to NEC Corporation when you have an open support case.
- **iLO Federation management**—Use the iLO Federation features to discover and manage multiple servers at a time.
- **Integrated Remote Console**—If you have a network connection to the server, you can access a secure high-performance console to manage the server from any location.
- **Virtual Media**—Remotely mount high-performance Virtual Media devices to the server.
- **Power management**—Securely and remotely control the power state of the managed server.
- **Deployment and provisioning**—Use Virtual Power and Virtual Media for tasks such as the automation of deployment and provisioning.
- **Power consumption and power settings**—Monitor the server power consumption, configure server power settings, and configure power capping on supported servers.
- **User access**—Use local or directory-based user accounts to log in to iLO.
- **Two-factor authentication**—Two-factor authentication is supported with Kerberos.
- **iLO interface controls**—For enhanced security, enable or disable selected iLO interfaces and features.
- **Firmware management**—Save components to the iLO Repository and use SUM to configure install sets and manage the installation queue.
- **iLO Service Port**—Use a supported USB Ethernet adapter to connect a client to the iLO

Service Port to access the server directly. You can also connect a USB key to download the Active Health System Log.

- **IPMI**—The iLO firmware provides server management based on the IPMI version 2.0 specification.
- **iLO RESTful API and RESTful Interface Tool (iLOrest)**—iLO 5 includes the iLO RESTful API, which is Redfish API conformant
- **iLO Backup & Restore**—Back up the iLO configuration and then restore it on a system with the same hardware configuration when replacing the motherboard etc.

ROM-based configuration utility

You can use the BMC Configuration Utility in the UEFI System Utilities to configure network parameters, global settings, and user accounts.

The BMC Configuration Utility is designed for the initial iLO setup, and is not intended for continued iLO administration. You can start the utility when the server is booted, and you can run it remotely with the Remote Console.

You can configure iLO to require users to log in when they access the BMC Configuration Utility, or you can disable the utility for all users. These settings can be configured on the **Access Settings** page.
Disabling the BMC Configuration Utility prevents reconfiguration from the host unless the system maintenance switch is set to disable iLO security.

To access the BMC Configuration Utility, press **F9** during POST to start the UEFI System Utilities. Click **System Configuration**, and then click **BMC Configuration Utility**.

iLO RESTful API

iLO includes the iLO RESTful API, which is Redfish API conformant. The iLO RESTful API is a management interface that server management tools can use to perform configuration, inventory, and monitoring tasks by sending basic HTTPS operations (GET, PUT, POST, DELETE, and PATCH) to the iLO web server.

RESTful Interface Tool

The RESTful Interface Tool (iLOrest) is a scripting tool that allows you to automate Express server management tasks. It provides a set of simplified commands that take advantage of the iLO RESTful API.

You can install the tool on your computer for remote use or install it locally on a server with a Windows or Linux Operating System. The RESTful Interface Tool offers an interactive mode, a scriptable mode, and a file-based mode to help decrease automation times.

iLO scripting and command line

You can use the iLO scripting tools to configure multiple servers, to incorporate a standard configuration into the deployment process, and to control servers and subsystems.

The iLO scripting and CLI guide describes the syntax and tools available for using iLO through a command line or scripted interface.

2.Setting up iLO

Preparing to set up iLO

Before setting up an iLO management processor, you must decide how to handle networking and security. The following questions can help you configure iLO:

Procedure

1. **How will iLO connect to the network?**
2. **Will NIC Teaming be used with the Shared Network Port configuration?**
3. **How will iLO acquire an IP address?**
4. **What access security is required, and what user accounts and privileges are needed?**
5. **What tools will you use to configure iLO?**

iLO network connection options

Typically, iLO is connected to the network through a dedicated management network or a shared connection on the production network.

Dedicated management network

In this configuration, the iLO port is on a separate network. A separate network improves performance and security because you can physically control which workstations are connected to the network. A separate network also provides redundant access to the server when a hardware failure occurs on the production network. In this configuration, iLO cannot be accessed directly from the production network. The Dedicated management network is the preferred iLO network configuration.

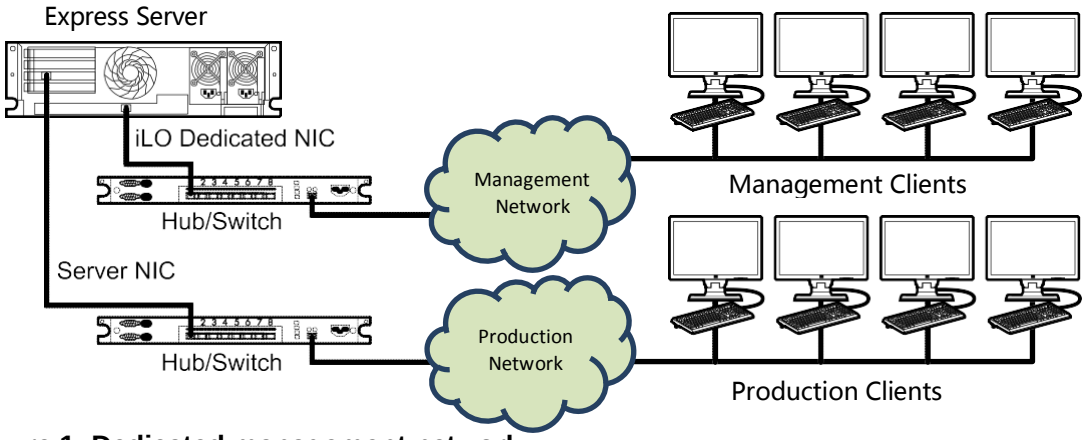


Figure 1: Dedicated management network

Production network

In this configuration, both the NIC and the iLO port are connected to the production network. In iLO, this type of connection is called the Shared Network Port configuration. Certain NEC Corporation embedded NICs and add-on cards provide this capability. This connection enables access to iLO from anywhere on the network and reduces the amount of networking hardware and infrastructure required to support iLO.

- There are some drawbacks to using this configuration.
- With a shared network connection, traffic can hinder iLO performance.
- During the server boot process and when the OS NIC drivers are loading and unloading, there are brief periods of time (2–8 seconds) when iLO cannot be reached from the network. After these short periods, iLO communication is restored and iLO will respond to network traffic.

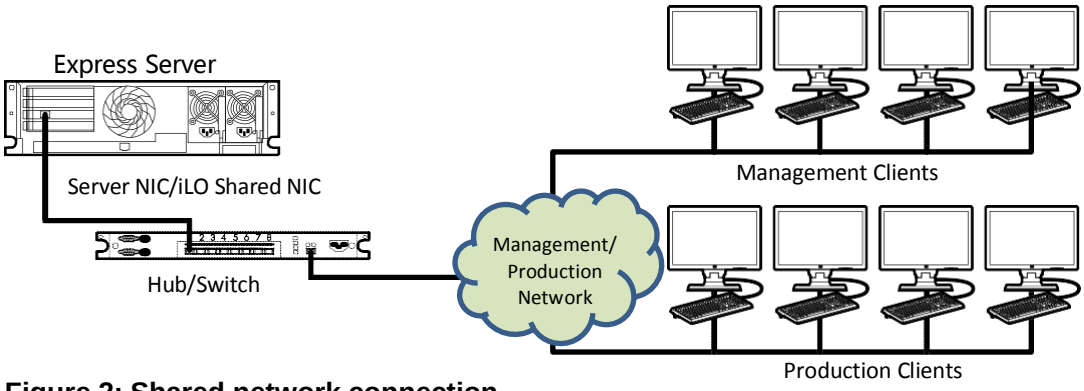


Figure 2: Shared network connection

NIC teaming with Shared Network Port configurations

NIC teaming is a feature you can use to improve server NIC performance and reliability.

NIC teaming constraints

When you select a teaming mode to use when iLO is configured to use the Shared Network Port:

- iLO network communications will be blocked in the following conditions:
  - The selected NIC teaming mode causes the switch that iLO is connected with to ignore traffic from the server NIC/port that iLO is configured to share.
  - The selected NIC teaming mode sends all traffic destined for iLO to a NIC/port other than the one that iLO is configured to share.
- Because iLO and the server transmit and receive on the same switch port, the selected NIC teaming mode must allow the switch to tolerate traffic with two different MAC addresses on the same switch port. Some implementations of LACP (802.3ad) will not tolerate multiple MAC addresses on the same link.

NIC teaming modes

If your server is configured to use NIC teaming, observe the following guidelines.

Network Fault Tolerance

The server transmits and receives on only one NIC (the primary adapter). The other NICs (secondary adapters) that are part of the team do not transmit server traffic and they ignore received traffic. This mode allows the iLO Shared Network Port to function correctly.

Select the NIC/port iLO uses as the **Preferred Primary Adapter**.

Transmit Load Balancing

The server transmits on multiple adapters but receives only on the primary adapter. This mode allows the iLO Shared Network Port to function correctly.

Select the NIC/port iLO uses as the **Preferred Primary Adapter**.

Switch Assisted Load Balancing

In this mode, there is no concept of primary and secondary adapters. All adapters are considered equal for the purposes of sending and receiving data. This mode is the most problematic for iLO Shared Network Port configurations because traffic destined for iLO can be received on only one of the server NIC/ports. To determine the constraints that your switch vendor places on their implementation of switch assisted load balancing, see the switch vendor documentation.

iLO IP address acquisition

To enable iLO access after it is connected to the network, the iLO management processor must acquire an IP address and subnet mask. You can use a dynamic address or a static address.

Dynamic IP address

A dynamic IP address is set by default. iLO obtains the IP address and subnet mask from DNS or DHCP servers. This method is the simplest.

If you use DHCP:

- The iLO management port must be connected to a network that is connected to a DHCP server, and iLO must be on the network before power is applied. DHCP sends a request soon after power is applied. If the DHCP request is not answered when iLO first boots, it will reissue the request at 90-second intervals.
- The DHCP server must be configured to provide DNS and WINS name resolution.

Static IP address

If DNS or DHCP servers are not available on the network, a static IP address is used. A static IP address can be configured by using the BMC Configuration Utility.

If you plan to use a static IP address, you must have the IP address before starting the iLO setup process.

iLO access security

You can use the following methods to manage access to iLO:

Local accounts

Up to 12 user accounts can be stored in iLO. This configuration is ideal for small environments such as labs and small-sized or medium-sized businesses.

Login security with local accounts is managed through the iLO Access Settings and user privileges.

Directory services

Up to six directory groups can be configured in iLO. Use a directory to authenticate and authorize iLO access. This configuration enables an unlimited number of users and easily scales to the number of iLO devices in an enterprise.

If you plan to use directory services, consider enabling at least one local administrator account for alternate access.

A directory provides a central point of administration for iLO devices and users, and the directory can enforce a strong password policy.

iLO configuration tools

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

iLO web interface

Use the iLO web interface when you can connect to iLO on the network by using a web browser. You can also use this method to reconfigure an iLO management processor.

ROM-based setup

Use the BMC Configuration Utility when the system environment does not use DHCP, DNS, or WINS. Other configuration options not discussed in this guide follow:

EXPRESSBUILDER

To start EXPRESSBUILDER, press **F10** during POST.

iLO RESTful API

A management interface that server management tools can use to perform configuration, inventory, and monitoring of a supported server through iLO.

Scripting

You can use scripting to set up multiple iLO management processors. You can use scripts to configure iLO on the network during initial deployment or from a deployed host.

- **SMASH CLP**—A command-line protocol that can be used when a command line is accessible through SSH or the physical serial port.

Initial setup steps: Process overview

The iLO default settings enable you to use most features without additional configuration. However, the configuration flexibility of iLO enables customization for multiple enterprise environments. This chapter discusses the initial iLO setup steps.

Procedure

1. **Connect iLO to the network.**
2. If you are not using dynamic IP addressing, use the ROM-based setup utilities to **configure a static IP address**.
3. If you will use the local accounts feature, use the ROM-based setup utilities to **configure user accounts**.
4. **Configure a time zone to iLO.** iLO 5 Firmware Version 1.15 Aug 17 2017 needs a time zone configuration to display a correct date and time.
5. Optional: **Install an iLO license**.
6. **If necessary, install the iLO drivers.**

Connecting iLO to the network

Connect iLO to the network through a production network or a dedicated management network.

iLO uses standard Ethernet cabling, which includes CAT 5 UTP with RJ-45 connectors. Straight-through cabling is necessary for a hardware link to a standard Ethernet hub or switch.

For more information about setting up your hardware, see the server user guide.

More Information

iLO network connection options

Setting up iLO by using the BMC Configuration Utility

NEC Corporation recommends using the BMC Configuration Utility to set up iLO for the first time and to configure iLO network parameters for environments that do not use DHCP, DNS, or WINS.

NOTE:

If you can connect to iLO on the network by using a web browser, you can also use the iLO web interface to configure iLO. Access iLO from a remote network client by using a supported browser and providing the default DNS name, user name, and password.

Configuring a static IP address (BMC Configuration Utility)

This step is required only if you want to use a static IP address. When you use dynamic IP addressing, the DHCP server automatically assigns an IP address for iLO.

To simplify installation, NEC Corporation recommends using DNS or DHCP with iLO.

Procedure

1. Optional: If you access the server remotely, start an iLO remote console session.
2. Restart or power on the server.
3. Press **F9** in the server POST screen.

   The UEFI System Utilities start.
4. Click **System Configuration**.
5. Click **BMC Configuration Utility**.
6. Disable DHCP:
   a. Click Network Options.
   b. Select OFF in the DHCP Enable menu.

      The **IP Address**, **Subnet Mask**, and **Gateway IP Address** boxes become editable. When DHCP Enable is set to ON, you cannot edit these values.
7. Enter values in the **IP Address**, **Subnet Mask**, and **Gateway IP Address** boxes.
8. To save the changes and exit, press **F12**.
9. The BMC Configuration Utility prompts you to confirm that you want to save the pending configuration changes.
10. To save and exit, click **Yes - Save Changes**.
11. The BMC Configuration Utility notifies you that iLO must be reset in order for the changes to take effect.
12. Click **OK**.

    iLO resets, and the iLO session is automatically ended. You can reconnect in approximately 30 seconds.
13. Resume the normal boot process:
    a. Start the iLO remote console.
       The BMC Configuration Utility is still open from the previous session.
    b. Press **ESC** several times to navigate to the **System Configuration** page.
    c. To exit the System Utilities and resume the normal boot process, click **Exit and resume system boot**.

Managing local user accounts with the BMC Configuration Utility

Adding user accounts (BMC Configuration Utility)

Procedure

1. Optional: If you access the server remotely, start an iLO remote console session.

2. Restart or power on the server.
3. Press **F9** in the server POST screen.

   The UEFI System Utilities start.
4. Click **System Configuration**, click **BMC Configuration Utility**, click **User Management**, and then click **Add User**.
5. Select the privileges for the new user.

   To assign a privilege, select **YES** in the menu next to the privilege name. To remove a privilege, select **NO**.

   The **Login** privilege is assigned to every user by default, so it is not listed in the BMC Configuration Utility.

   You cannot assign the **Recovery Set** privilege through the BMC Configuration Utility, so it is not available in the list.
6. Enter the user name and login name in the **New User Name** and **Login Name** boxes.
7. Enter the password.
   a. Move the cursor to the **Password** box, and then press **Enter**.

      The **Enter your new password** box opens.
   b. Type the password, and then press **Enter**.

      The **Confirm your new password** box opens.
   c. Type the password again to confirm, and then press **Enter**.
8. The BMC Configuration Utility confirms the new account creation.
9. To close the confirmation dialog box, click **OK**.
10. Create as many user accounts as needed, and then press **F12** to save the changes and exit the system utilities.
11. When prompted to confirm the changes, click **Yes - Save Changes** to exit the utility and resume the boot process.

More Information

iLO user privileges

iLO user account options

Editing user accounts (BMC Configuration Utility)

Procedure

1. Optional: If you access the server remotely, start an iLO remote console session.
2. Restart or power on the server.
3. Press **F9** in the server POST screen.

The UEFI System Utilities start.

4. Click **System Configuration**, click **BMC Configuration Utility**, click **User Management**, and then click **Edit/Remove User**.
5. In the **Action** menu for the user you want to edit or remove, select **Edit**.

   The account properties are displayed.
6. Update the **Login Name**.
7. Update the **Password**.
   a. Move the cursor to the **Password** box, and then press **Enter**.

      The **Enter your new password** box opens.
   b. Type the password, and then press **Enter**.

      The **Confirm your new password** box opens.
   c. Type the password again to confirm, and then press **Enter**.
8. Modify the user account privileges.

   To assign a privilege, select YES in the menu next to the privilege name. To remove a privilege, select NO.

   The Login privilege is assigned to every user by default, so it is not available in the BMC Configuration Utility.

   You cannot assign the Recovery Set privilege through the BMC Configuration Utility, so it is not available in the list.
9. Update as many user accounts as needed, and then press F12 to save the changes and exit the system utilities.
10. When prompted to confirm the changes, click Yes - Save Changes to exit the utility and resume the boot process.

More Information

iLO user privileges

iLO user account options

Removing user accounts (BMC Configuration Utility)

Procedure

1. Optional: If you access the server remotely, start an iLO remote console session.
2. Restart or power on the server.
3. Press **F9** in the server POST screen.

   The System Utilities start.
4. Click **System Configuration**, click **BMC Configuration Utility**, click **User Management**, and then

click **Edit/Remove User**.

5. In the **Action** menu for the user you want to remove, select **Delete**.

   The user name is marked to be deleted when you save the changes on this page.

6. If needed, mark other user accounts to delete, and then press **F12** to save the changes and exit the system utilities.

7. When prompted to confirm the changes, click **Yes - Save Changes** to exit the utility and resume the boot process.

Logging in to iLO for the first time

Procedure

1. **Enter** https://<iLO hostname or IP address>**.**

   HTTPS (HTTP exchanged over an SSL encrypted session) is required for accessing the iLO web interface.

2. Enter the default user credentials, and then click **Log In**.

iLO default credentials

The iLO firmware is configured with a default user name, password, and DNS name. The default information is on the serial label pull tab attached to the server that contains the iLO management processor. Use these values to access iLO remotely from a network client by using a web browser.

- **User name**—Administrator
- **Password**—A random eight-character string
- **DNS name**—BMCXXXXXXXXXXXX, where the **X** characters represent the server serial number.

IMPORTANT:

NEC Corporation recommends changing the default password after you log in to iLO for the first time.

If you reset iLO to the factory default settings, use the default iLO account credentials to log in after the reset.

iLO licensed features

iLO (Standard) is preconfigured on Express servers without an additional cost or license. Features that enhance productivity are licensed.

To activate iLO licensed features, **install an iLO license**.

iLO drivers

iLO is an independent microprocessor running an embedded operating system. The architecture ensures that most iLO functionality is available, regardless of the host operating system. The iLO driver enables software such as the Agentless Management Service to communicate with iLO. The installed OS and system configuration determine the installation requirements.

The iLO drivers will be applied automatically when you install using EXPRESSBUILDER and Starter Pack.

iLO time zone

Configure time zone to iLO . Login to iLO Web Interface using an user has Configure iLO Settings privilege. Click iLO Dedicated Network Port and Click SNTP when iLO is using iLO Dedicated Network Port. Click iLO Shared Network Port and Click SNTP when iLO is using iLO Shared Network Port.

If you would like to sync a date and time between iLO and SNTP server, **configure iLO SNTP settings**.

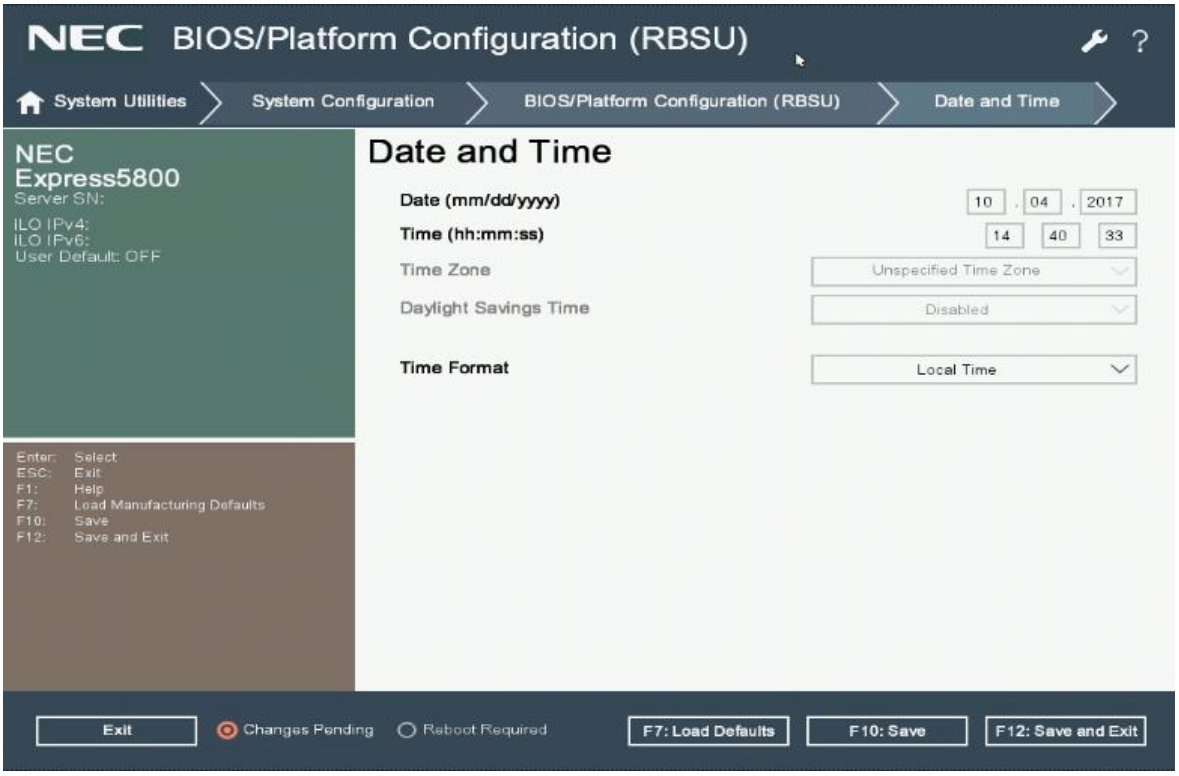
If you won't use time syncing function with SNTP server, configure following parameters.
Use DHCPv4 Supplied Time Settings – Disable
Use DHCPv6 Supplied Time Settings – Disable
Primary Time Server – Blank
Secondary Time Server – Blank
Time Zone – Refer next page.

IMPORTANT:

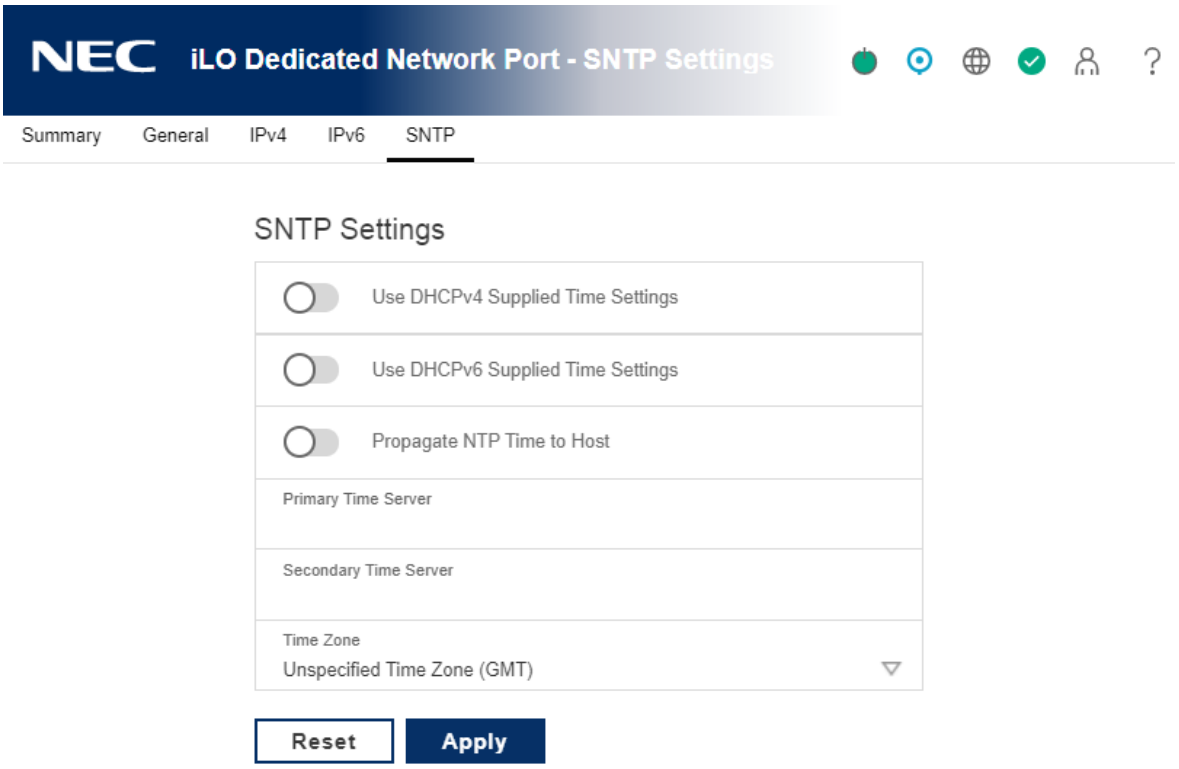
The Time Zone setting is required to display correct time by iLO5 Firmware Version 1.15 Aug 17 2017 even granting that you won't use time syncing function with SNTP server.

If Time Format on BIOS/Platform Configuration(RBSU) is Local time, set Unspecified Time Zone (GMT) to iLO Time Zone.

BIOS/Platform Configuration(RBSU) :

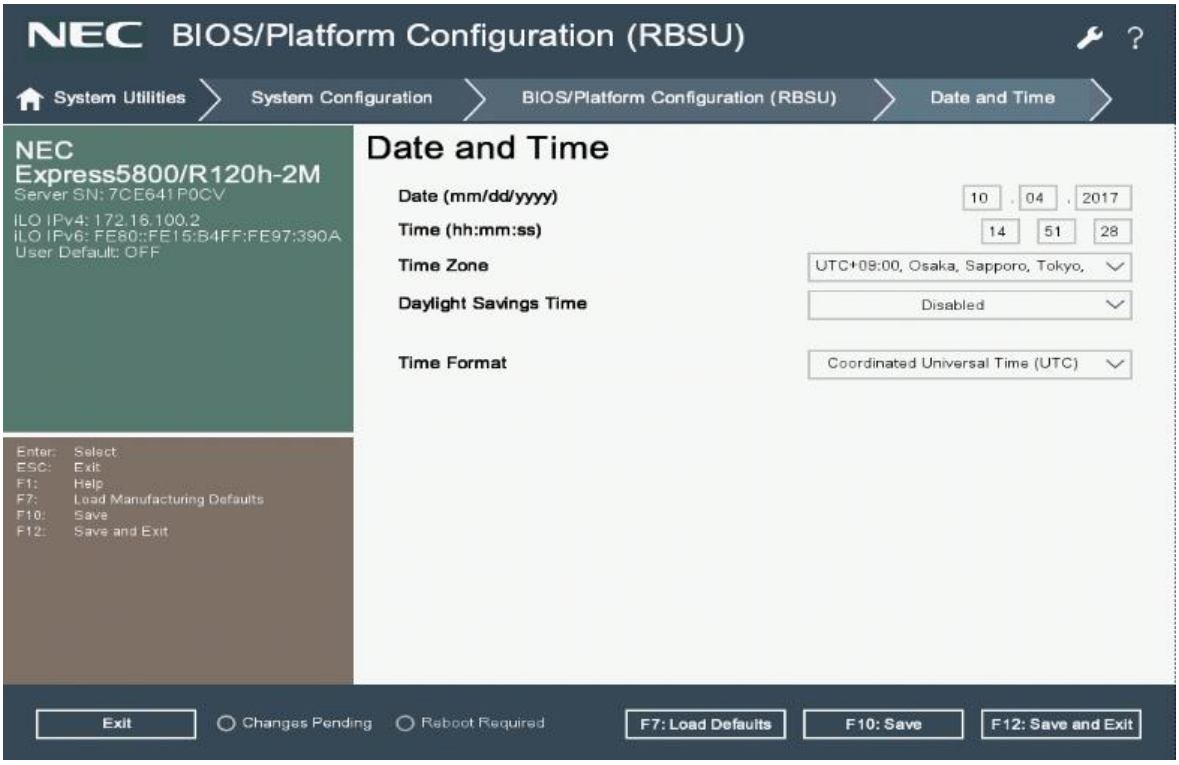


iLO Web Interface:

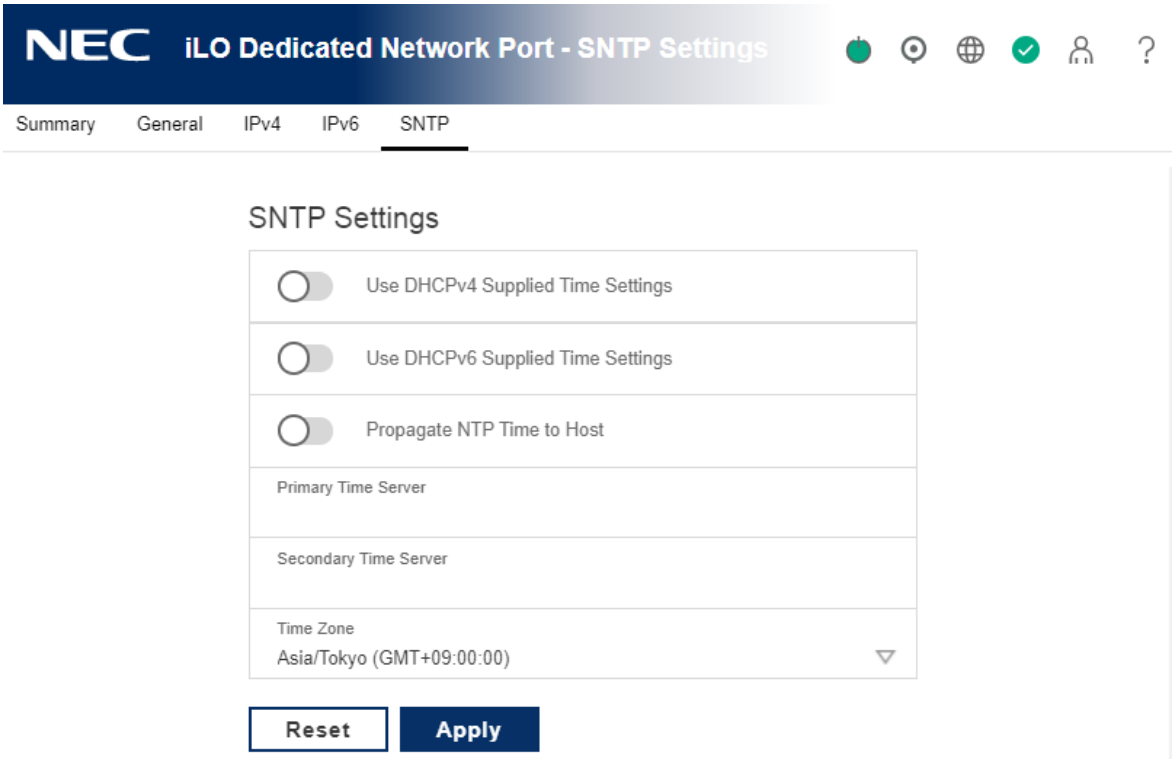


If Time Format on BIOS/Platform Configuration(RBSU) is Coordinated Universal Time (UTC), set same time zone parameter to iLO Time Zone.

BIOS/Platform Configuration(RBSU) :



iLO Web Interface:



After setting, Click Apply and Click Reset. iLO will restart to apply the settings.

3.Using the iLO web interface

iLO web interface

You can use the iLO web interface to manage iLO. You can also use a Remote Console, SMASH CLP, or the iLO RESTful API.

Supported browsers

iLO 5 supports the latest versions of the following browsers:

- Microsoft Edge
- Mozilla Firefox
- Google Chrome mobile and desktop
- Microsoft Internet Explorer 11

Browser requirements

The iLO web interface requires a browser that meets the following requirements:

- **JavaScript**—The iLO web interface uses client-side JavaScript extensively.

  This setting is not enabled by default in all versions of Internet Explorer. To check or change this setting, see **Configuring the Internet Explorer JavaScript setting**.
- **Cookies**—Cookies must be enabled for certain features to function correctly.
- **Pop-up windows**—Pop-up windows must be enabled for certain features to function correctly. Verify that pop-up blockers are disabled.
- **TLS**—To access the iLO web interface, you must enable TLS 1.0 or later in your browser.

Configuring the Internet Explorer JavaScript setting

Some versions of Internet Explorer have JavaScript disabled by default. Use the following procedure to enable JavaScript.

Procedure

1. Start Internet Explorer.
2. Select **Tools** > **Internet options**.
3. Click **Security**.
4. Click **Custom level**.
5. In the **Scripting** section, set **Active scripting** to **Enable**.
6. Click **OK**.
7. Refresh your browser window.

Logging in to the iLO web interface

Procedure

1. **Enter** https://<iLO host name or IP address>**.**

   When you access the iLO web interface, you must use HTTPS (HTTP exchanged over an SSL encrypted session).

   The iLO login page opens. If a **login security banner** is configured, the banner text is displayed in the **NOTICE** section.

2. Do one of the following:

   - On the login page, enter a directory or local user account name and password, and then click **Log In**.
   - Click the **Zero Sign In** button.

     If iLO is configured for Kerberos network authentication, the **Zero Sign In** button is displayed below the **Log In** button. You can use the **Zero Sign In** button to log in without entering a user name and password.

More Information

iLO default credentials

Cookie sharing between browser instances and iLO

When you browse to iLO and log in, one session cookie is shared with all open browser windows that share the iLO URL in the browser address bar. As a consequence, all open browser windows share one user session. Logging out in one window ends the user session in all the open windows. Logging in as a different user in a new window replaces the session in the other windows.

This behavior is typical of browsers. iLO does not support multiple users logged in from two different browser windows in the same browser on the same client.

Shared instances

When the iLO web interface opens another browser window or tab (for example, a help file), this window shares the connection to iLO and the session cookie.

When you are logged into the iLO web interface, and you open a new browser window manually, a duplicate instance of the original browser window opens. If the domain name in the address bar matches the original browser session, the new instance shares a session cookie with the original browser window.

Cookie order

During login, the login page builds a browser session cookie that links the window to the appropriate session in the iLO firmware. The firmware tracks browser logins as separate sessions

listed on the **Session List** page.

For example, when User1 logs in, the web server builds the initial frames view, with User1 listed as the active user, menu items in the navigation pane, and page data in the right pane. When User1 clicks from link to link, only the menu items and page data are updated.

While User1 is logged in, if User2 opens a browser window on the same client and logs in, the second login overwrites the cookie generated in the User1 session. Assuming that User2 is a different user account, a different current frame is built, and a new session is granted. The second session appears on the **Session List** page as User2.

The second login has effectively orphaned the first session by overriding the cookie generated during the User1 login. This behavior is the same as closing the User1 browser without clicking the **Log Out** button. The User1 orphaned session is reclaimed when the session timeout expires.

Because the current user frame is not refreshed unless the browser is forced to refresh the entire page, User1 can continue navigating by using the browser window. However, the browser is now operating by using the User2 session cookie settings, even though it might not be readily apparent.

If User1 continues to navigate in this mode (User1 and User2 sharing a process because User2 logged in and reset the session cookie), the following might occur:

- User1 session behaves consistently with the privileges assigned to User2.
- User1 activity keeps User2 session alive, but User1 session can time out unexpectedly.
- Logging out of either window causes both sessions to end. The next activity in the other window can redirect the user to the login page as if a session timeout or premature timeout occurred.
- Clicking Log Out from the second session (User2) results in the following warning message:

  ```
  Logging out: unknown page to display before redirecting the user to the login page.
  ```

- If User2 logs out and then logs back in as User3, User1 assumes the User3 session.
- If User1 is at login, and User2 is logged in, User1 can alter the URL to redirect to the index page. It appears as if User1 has accessed iLO without logging in.

These behaviors continue as long as the duplicate windows are open. All activities are attributed to the same user, using the last session cookie set.

Displaying the current session cookie

After logging in, you can force the browser to display the current session cookie by entering the following in the URL navigation bar:

```
javascript:alert(document.cookie)
```

The first field visible is the session ID. If the session ID is the same among the different browser

windows, these windows are sharing iLO session.

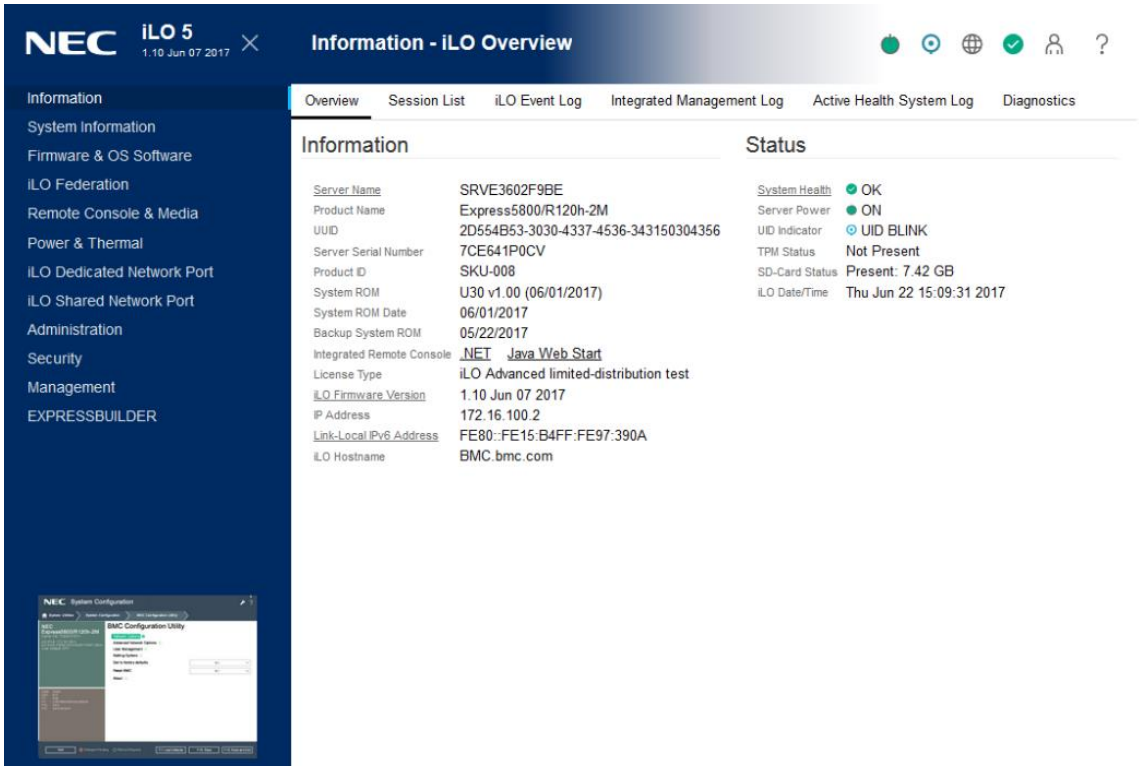
You can force the browser to refresh and reveal your true identity by pressing **F5**, selecting **View** > **Refresh**, or clicking the **Refresh** button.

Best practices for preventing cookie-related issues

- Start a new browser for each login by double-clicking the browser icon or shortcut.
- To close an iLO session before you close the browser window, click the **Log Out** button.

iLO web interface

The iLO web interface groups similar tasks for easy navigation and workflow. The interface is organized with a navigation tree in the left pane. To use the web interface, click an item in the navigation tree, and then click the name of the tab you want to view.



Using the iLO controls

iLO control icons

When you log in to the iLO web interface, the iLO controls are available from any iLO page.

- **Power icon**—Click this icon to access the Virtual Power Button features.
- **UID icon**—Click this icon to turn the UID LED on and off.
- **Language**—Click this icon to select a language for the current iLO web interface session.

- To view or modify the language settings, click the language icon, and then select **Settings**.
- **Health icon**—Click this icon to view the overall health status for the server fans, temperature sensors, and other monitored subsystems. For all components except the Agentless Management Service (AMS), click a component to view additional details.
- **User icon**—Click this icon to do the following:
  - To log out of the current iLO web interface session, click the user icon, and then select **Logout**.
  - To view the active iLO sessions, click the user icon, and then select **Sessions**.
  - To view or modify iLO user accounts, click the user icon, and then select **Settings**.
- **Help icon**—Click this icon to view online help for the current iLO web interface page.
- **Ellipsis icon**—This icon is displayed on the **Firmware & OS Software** page when the browser window is too small to show the full page. To access the **Update Firmware** and **Upload to iLO Repository** options, click this icon. These options are available on all **Firmware & OS Software** tabs.

iLO navigation pane

iLO has a collapsible navigation pane that is accessible from each page.

- To toggle between showing and hiding the navigation pane, click the icon in the top left corner of the iLO web interface.

- To hide the navigation pane, click the X icon.
- To show the navigation pane, click the icon in the top left corner of the iLO web interface.
- The navigation pane shows a thumbnail of the Remote Console. To start a Remote Console, click the thumbnail and select a console option from the menu.
- For servers with monitors, click the Remote Console thumbnail in the navigation pane, and then select **Wake-Up Monitor** to wake up a monitor that is in sleep mode.

Changing the language from the login page

If a language pack is installed, use the language menu on the login screen to select the language for the iLO session. This selection is saved in a browser cookie for future use.

Prerequisites

A language pack is installed.

Procedure

1. Navigate to the iLO **Login** page.
2. Select a language from the **Language** menu.


login name
password
Log In
en - English
en - English
ja - 日本語

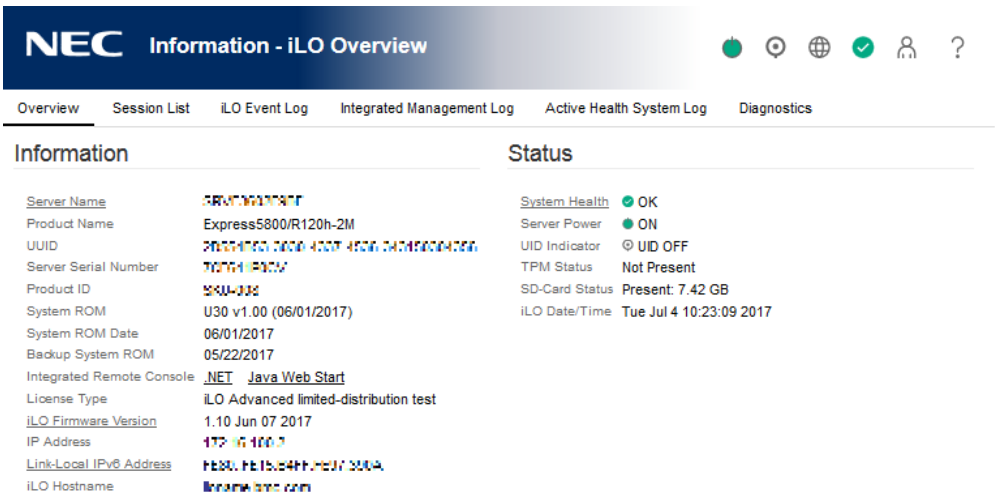
4.Viewing iLO information and logs

Viewing iLO overview information

Procedure

1. Navigate to the **Information** page.

   The **iLO Overview** page displays high-level details about the server and the iLO subsystem, as well as links to commonly used features.



System information details

- **Server Name**—The server name defined by the host operating system. To navigate to the **Access Settings** page, click the **Server Name** link.
- **Product Name**—The product with which this iLO processor is integrated.
- **UUID**—The universally unique identifier that software uses to identify this host. This value is assigned when the system is manufactured.
- **UUID (Logical)**—The system UUID that is presented to host applications. This value is displayed only when set by other software. This value might affect operating system and application licensing. The **UUID (Logical)** value is set as part of the logical server profile that is assigned to the system. If the logical server profile is removed, the system **UUID** value reverts from the **UUID (Logical)** value to the **UUID** value. If no **UUID (Logical)** value is set, this item is not displayed.
- **Server Serial Number** —The server serial number, which is assigned when the system is manufactured. You can change this value by using the ROM-based system utilities during POST.
- **Serial Number (Logical)**—The system serial number that is presented to host applications. This value is displayed only when set by other software. This value might affect operating system and application licensing. The **Serial Number (Logical)** value is set as part of the

logical server profile that is assigned to the system. If the logical server profile is removed, the serial number value reverts from the **Serial Number (Logical)** value to the **Server Serial Number** value. If no **Serial Number (Logical)** value is set, this item is not displayed.

- **Chassis Serial Number**—The serial number of the chassis that contains the server node.
- **Product ID**—This value distinguishes between different systems with similar serial numbers. The product ID is assigned when the system is manufactured. You can change this value by using the UEFI system utilities during POST.
- **System ROM**—The version of the active system ROM.
- **System ROM Date**—The date of the active system ROM.
- **Backup System ROM**—The version of the backup system ROM. If a system ROM update fails or is rolled back, the backup system ROM is used. This value is displayed only if the system supports a backup system ROM.
- **Integrated Remote Console**—Provides links to start the .NET IRC or Java IRC for remote, out-of- band communication with the server console.

  For information about the available remote console options, see **iLO Integrated Remote Console**.
- **License Type**—The level of licensed iLO firmware functionality.
- **iLO Firmware Version**—The version and date of the installed iLO firmware. To navigate to the **Firmware Update** page, click the **iLO Firmware Version** link.
- **IP Address**—The network IP address of the iLO subsystem.
- **Link-Local IPv6 Address**—The SLAAC link-local address of the iLO subsystem. To navigate to the **Network Summary** page, click the **Link-Local IPv6 Address** link. This value is displayed only for iLO Dedicated Network Port configurations.
- **iLO Hostname**—The fully qualified network name assigned to the iLO subsystem. By default, the hostname is **BMC**, followed by the system serial number and the current domain name. This value is used for the network name and must be unique.

System status details

- **System Health**—The server health indicator. This value summarizes the condition of the monitored subsystems, including overall status and redundancy (ability to handle a failure). Lack of redundancy in any subsystem at startup will not degrade the system health status. To navigate to the **Health Summary** page, click the **System Health** link.
- **Server Power**—The server power state (**ON** or **OFF**). To access the Virtual Power Button features, click the **Server Power** icon.
- **UID Indicator**—The state of the UID LED. The UID LED helps you identify and locate a server, especially in high-density rack environments. The possible states are **UID ON**, **UID OFF**, and **UID BLINK**.

If the iLO Service Port is in use, **UID BLINK** status includes the Service Port status. The possible values are **UID BLINK (Service Port Busy)**, **UID BLINK (Service Port Error)**, and **UID BLINK (Service Port Finished)**.

To turn the UID LED on or off, click the UID Indicator icon, click the UID control at the top of the iLO web interface window, or use the UID buttons on the server chassis.

When the UID is blinking, and then it stops blinking, the status reverts to the previous value (**UID ON** or **UID OFF**). If a new state is selected while the UID LED is blinking, that state takes effect when the UID LED stops blinking.

CAUTION:

The UID LED blinks automatically to indicate that a critical operation is underway on the host, such as Remote Console access or a firmware update. Do not remove power from a server when the UID LED is blinking.

- **TPM Status** or **TM Status**—The status of the TPM or TM socket or module. The possible values are **Not Supported**, **Not Present**, or **Present-Enabled**.

  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 iLO RESTful API, and the CLP.
- **Module Type**—The TPM or TM type and specification version. The possible values are **TPM 1.2**, **TPM 2.0**, **TM 1.0**, **TPM Module 2.0 (Intel PTT)**, **Not Specified**, and **Not Supported**. This value is displayed when a TPM or TM is present on a server.
- **SD-Card Status**—The status of the internal SD card. If present, the number of blocks in the SD card is displayed.
- **Access Panel Status**—The state of the access panel. The possible states are **OK** (the access panel is installed) and **Intrusion** (the access panel is open). This value is displayed only on servers that are configured for chassis intrusion detection.
- **iLO Date/Time**—The internal clock of the iLO subsystem.

Managing iLO sessions

Prerequisites

Administer User Accounts privilege

Procedure

1. Navigate to the **Information** page, and then click the **Session List** tab. The **Session List** page displays information about the active iLO sessions.
2. Optional: To disconnect one or more sessions, click the check box next to each session you want to disconnect, and then click **Disconnect Session**.

Session list details

iLO displays the following details in the **Current Session** and **Session List** tables:

- **User**—The iLO user account name.
- **IP**—The IP address of the computer used to log in to iLO.
- **Login Time**—The date and time that the iLO session started.
- **Access Time**—The date and time that iLO was last active in the session.
- **Expires**—The date and time that the session will end automatically.
- **Source**—The session source (for example, Remote Console, web interface, ROM-based setup utility, iLO RESTful API, or SSH).
- **Privilege icons** (current user only)—The **privileges** assigned to the current user account.

iLO Event Log

The event log provides a record of significant events recorded by the iLO firmware.

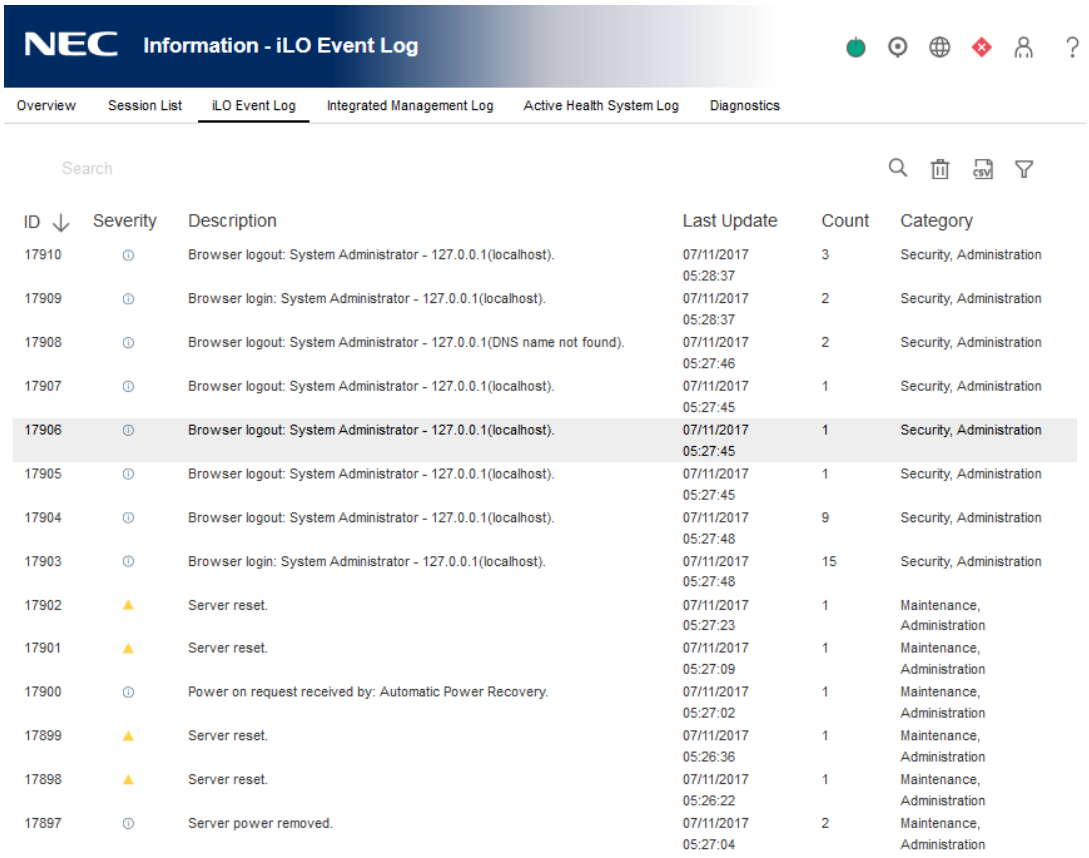
Logged events include major server events such as a server power outage or a server reset, and iLO events such as unauthorized login attempts. Other logged events include successful or unsuccessful browser and Remote Console logins, virtual power and power-cycle events, clearing the log, and some configuration changes, such as creating or deleting a user.

iLO provides secure password encryption, tracking all login attempts and maintaining a record of all login failures. The **Authentication Failure Logging** setting allows you to configure logging criteria for failed authentications. The event log captures the client name for each logged entry to improve auditing capabilities in DHCP environments, and records the account name, computer name, and IP address.

Viewing the event log

Procedure

1. Click **Information** in the navigation tree, and then click the **iLO Event Log** tab.
2. Optional: Use the event log sort, search, and filter features to customize the log view.
3. Optional: To view the event details pane, click an event.



Event log details

- **ID**—The event ID number. Events are numbered in the order in which they are generated. By

default, the event log is sorted by the ID, with the most recent event at the top.

- **Severity**—The importance of the detected event.
- **Description**—The description identifies the component and detailed characteristics of the recorded event. If the iLO firmware is rolled back to an earlier version, the description `UNKNOWN EVENT TYPE` might be displayed for events recorded by the newer firmware. You can resolve this issue by updating the firmware to the latest supported version, or by clearing the event log.
- **Last Update**—The date and time when the latest event of this type occurred. This value is based on the date and time stored by the iLO firmware.

  If the iLO firmware did not recognize the date and time when an event was updated, `[NOT SET]` is displayed.
- **Count**—The number of times this event has occurred (if supported).

  In general, important events generate an event log entry each time they occur. They are not consolidated into one event log entry.

  When less important events are repeated, they are consolidated into one event log entry, and the **Count** and **Last Update** values are updated. Each event type has a specific time interval that determines whether repeated events are consolidated or a new event is logged.
- **Category**—The event category.

Event log icons

iLO uses the following icons to indicate event severity:

- **Critical**—The event indicates a service loss or imminent service loss. Immediate attention is needed.
- **Caution**—The event is significant but does not indicate performance degradation.
- **Informational**—The event provides background information.
- **Unknown**—The event severity could not be determined.

Event log event pane details

- **Initial Update**—The date and time when the first event of this type occurred. This value is based on the date and time stored by the iLO firmware.

  If iLO did not recognize the date and time when the event was first created, [NOT SET] is displayed.
- **Event Code**—A unique identifier for an event within a given event class displayed in hexadecimal format.

Customizing the event log view

Sorting events

Click a column heading to sort the event log table by that column.

To change the display to ascending or descending order, click the column heading again.

Event filters

To access the event log filters, click  .

- To filter by severity, select a severity level from the **Severity** menu.
- To filter by event category, select a value in the **Category** menu.
- To change the displayed date and time for events, select a value in the **Time** menu. Choose from the following:
  - **Show Default**—Display UTC time.
  - **Show Local Time**—Display the iLO web interface client time.
  - **Show ISO Time**—Display UTC time in ISO 8601 format.

  In iLO 5 Firmware Version 1.10 Jun 07 2017, when SNTP setting is not configured or when it is not used in an environment where can be synchronized with the time server, the following times are displayed.

  ✓ If Show Default and Show ISO Time are selected, the following is displayed.

  System time(UTC±Time Zone) displayed in BIOS/Platform Configuration(RBSU)

  ✓ If Show Local Time is selected, the following is displayed.

  Added to the System time(UTC±Time Zone) displayed in BIOS/Platform Configuration(RBSU) and the time zone of the environment of the client connected to iLO.

  In iLO 5 Firmware Version 1.15 Aug 17 2017, when SNTP setting is not configured and Time Format on BIOS/Platform Configuration(RBSU) is Local Time, the following times are displayed.

  ✓ If Show Default and Show ISO Time are selected, the following is displayed.

  System time(UTC±Time Zone) displayed in BIOS/Platform Configuration(RBSU)

  ✓ If Show Local Time is selected, the following is displayed.

  Added to the System time(UTC±Time Zone) displayed in BIOS/Platform Configuration(RBSU) and the time zone of the environment of the client connected to iLO.
- To filter by the last update date, select a value in the Last Update menu.

  Based on the time displayed in Show Default, the filter will be applied.
- To set the filters back to the default values, click Reset filters.

Searching for an event

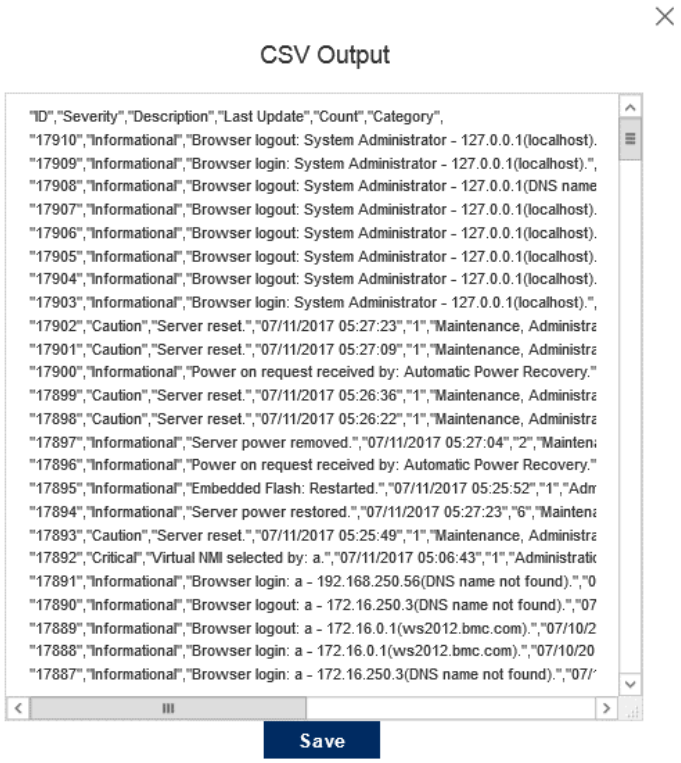
To search for events based on dates, event ID, or description text, click, and then enter text in the search box.

Saving the event log to a CSV file

Use a supported browser to export the event log to a CSV file.

Procedure

1. Click **Information** in the navigation tree, and then click the **iLO Event Log** tab.
2. Click the CSV icon
3. In the **CSV Output** window, click **Save**, and then follow the browser prompts to save or open the file.



Clearing the event log

Prerequisites

Configure iLO Settings privilege

Procedure

1. Click **Information** in the navigation tree, and then click the **iLO Event Log** tab.
2. Click .
3. When prompted to confirm the request, click **OK**.

The event log is cleared of all previously logged information and an event is recorded in the log.

Integrated Management Log

The IML provides a record of historical events that have occurred on the server. Events are generated by the system ROM and by services such as the iLO driver. Logged events include all server-specific events recorded by the iLO driver, including operating system information and ROM-based POST codes.

Entries in the IML can help you diagnose issues or identify potential issues. Preventative action might help to avoid disruption of service.

iLO manages the IML, which you can access through a supported browser, even when the server is off. The ability to view the log when the server is off can be helpful when troubleshooting remote host server issues.

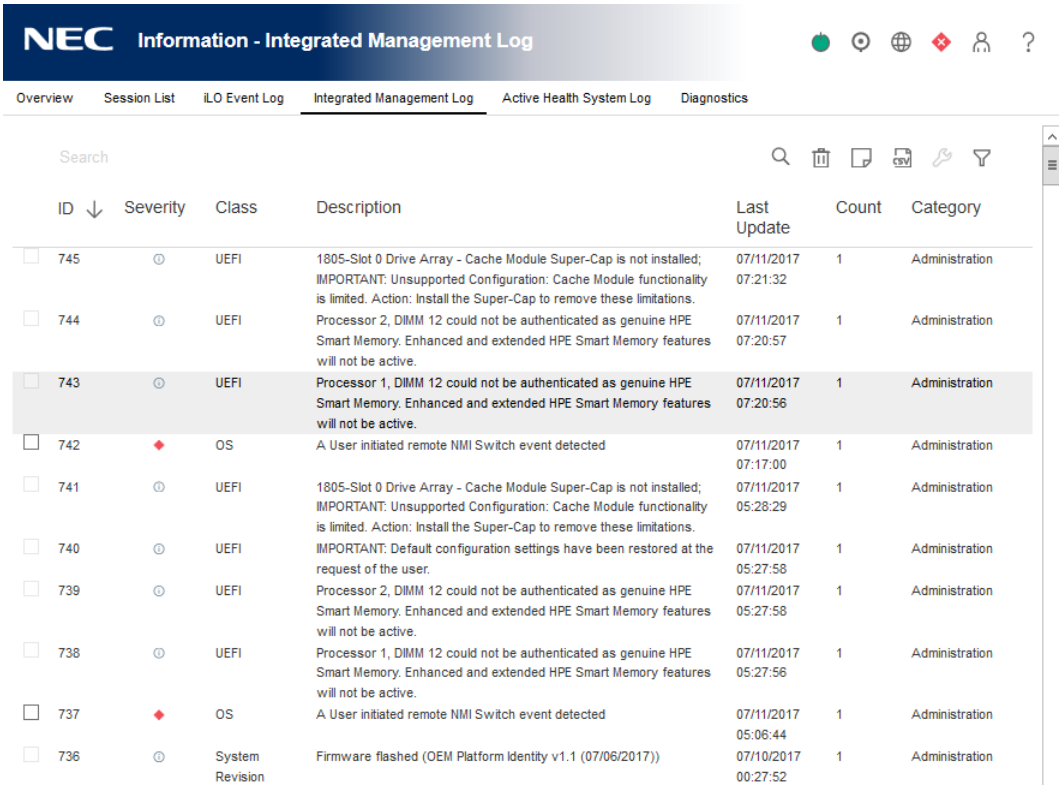
Examples of the types of information recorded in the IML follow:

- Fan inserted
- Fan removed
- Fan failure
- Fan degraded
- Fan repaired
- Fan redundancy lost
- Fans redundant
- Power supply inserted
- Power supply removed
- Power supply failure
- Power supplies redundancy lost
- Power supplies redundant
- Temperature over threshold
- Temperature normal
- Automatic shutdown started
- Automatic shutdown canceled
- Drive failure

Viewing the IML

Procedure

1. Click **Information** in the navigation tree, and then click the **Integrated Management Log** tab.
2. Optional: Use the IML sort, search, and filter features to customize the log view.
3. Optional: To view the event details pane, click an event.



IML details

- The first column on the left side of the web interface displays an active check box next to each event with Critical or Caution status. Use this check box to select an event to mark as repaired.
- **ID**—The event ID number. Events are numbered in the order in which they are generated.

  By default, the IML is sorted by the ID, with the most recent event at the top. A factory reset will reset the counter.
- **Severity**—The importance of the detected event.
- **Class**—Identifies the type of event that occurred, for example, network, maintenance, or system revision.
- **Description**—The description identifies the component and detailed characteristics of the recorded event.

  If the iLO firmware is rolled back, the description UNKNOWN EVENT TYPE might be displayed for events recorded by the newer firmware. You can resolve this issue by updating the firmware to the latest supported version, or by clearing the log.
- **Last Update**—The date and time when the latest event of this type occurred. This value is based on the date and time stored by the iLO firmware.

  If iLO did not recognize the date and time when an event was updated, [NOT SET] is displayed.
- **Count**—The number of times this event has occurred (if supported).

In general, important events generate an IML entry each time they occur. They are not consolidated into one event log entry.

When less important events are repeated, they are consolidated into one IML entry, and the **Count** and **Last Update** values are updated. Each event type has a specific time interval that determines whether repeated events are consolidated or a new event is logged.

- **Category**—The event category. For example, Hardware Failure, Firmware Failure, Power, or Administration.

IML icons

iLO uses the following icons to indicate IML event severity:

- **Critical**—The event indicates a service loss or an imminent service loss. Immediate attention is needed.
- **Caution**—The event is significant but does not indicate performance degradation.
- **Informational**—The event provides background information.
- **Repaired**—An event has undergone corrective action.
- **Unknown**—The event severity could not be determined.

IML event pane details

- **Initial Update**—The date and time when the first event of this type occurred. This value is based on the date and time stored by the iLO firmware.

  If iLO did not recognize the date and time when the event was first created, [NOT SET] is displayed.
- **Event Code**—A unique identifier for an event within a given event class (displayed in hexadecimal format).
- **Recommended Action**— A short description of the recommended action for a failure condition.

Customizing the IML view

Sorting events

Click a column heading to sort the IML table by that column.

To change the display to ascending or descending order, click the arrow next to the column heading.

Event filters

To access the event log filters, click .

- To filter by severity, select a severity level from the **Severity** list.

- To filter by class, select a class from the **Class** list.
- To filter by event category, select a value in the **Category** list.
- To change the displayed date and time for events, select a value in the **Time** menu. Choose from the following:
  - **Show Default**—Display UTC time.
  - **Show Local Time**—Display the iLO web interface client time.
  - **Show ISO Time**—Display UTC time in ISO 8601 format.

  In iLO 5 Firmware Version 1.10 Jun 07 2017, when SNTP setting is not configured or when it is not used in an environment where can be synchronized with the time server, the following times are displayed.

  ✓ If Show Default and Show ISO Time are selected, the following is displayed.

  System time(UTC±Time Zone) displayed in BIOS/Platform Configuration(RBSU)

  ✓ If Show Local Time is selected, the following is displayed.

  Added to the System time(UTC±Time Zone) displayed in BIOS/Platform Configuration(RBSU) and the time zone of the environment of the client connected to iLO.

  In iLO 5 Firmware Version 1.15 Aug 17 2017, when SNTP setting is not configured and Time Format on BIOS/Platform Configuration(RBSU) is Local Time, the following times are displayed.

  ✓ If Show Default and Show ISO Time are selected, the following is displayed.

  System time(UTC±Time Zone) displayed in BIOS/Platform Configuration(RBSU)

  ✓ If Show Local Time is selected, the following is displayed.

  Added to the System time(UTC±Time Zone) displayed in BIOS/Platform Configuration(RBSU) and the time zone of the environment of the client connected to iLO.
- To filter by the **Last Update** date, select a value in the **Last Update** menu.

  Based on the time displayed in **Show Default**, the filter will be applied.
- To set the filters back to the default values, click **Reset filters**.

Searching for an event

To search for events based on dates, event IDs, or description text, click 🔍, and then enter text in the search box.

Marking an IML entry as repaired

Use this feature to change the status of an IML entry from **Critical** or **Caution** to **Repaired**.

Prerequisites

Configure iLO Settings privilege

Procedure

1. Investigate and repair the issue.
2. Click **Information** in the navigation tree, and then click the **Integrated Management Log** tab.
3. Select the log entry.

   To select an IML entry, click the check box next to the entry in the first column of the IML table. If a check box is not displayed next to an IML entry, that entry cannot be marked as repaired.

4. Click .

   The iLO web interface refreshes, and the selected log entry status changes to **Repaired**.

Adding a maintenance note to the IML

Use maintenance notes to create log entries about maintenance activities such as upgrades, system backups, periodic system maintenance, or software installations.

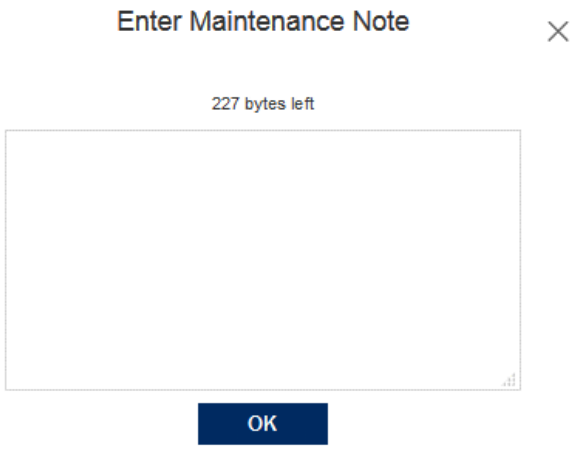
Prerequisites

Configure iLO Settings privilege

Procedure

1. Click **Information** in the navigation tree, and then click the **Integrated Management Log** tab.
2. Click .

   The **Enter Maintenance Note** window opens.



3. Enter the text that you want to add as a log entry, and then click **OK**.

   You can enter up to 227 bytes of text. You cannot submit a maintenance note without entering some text.

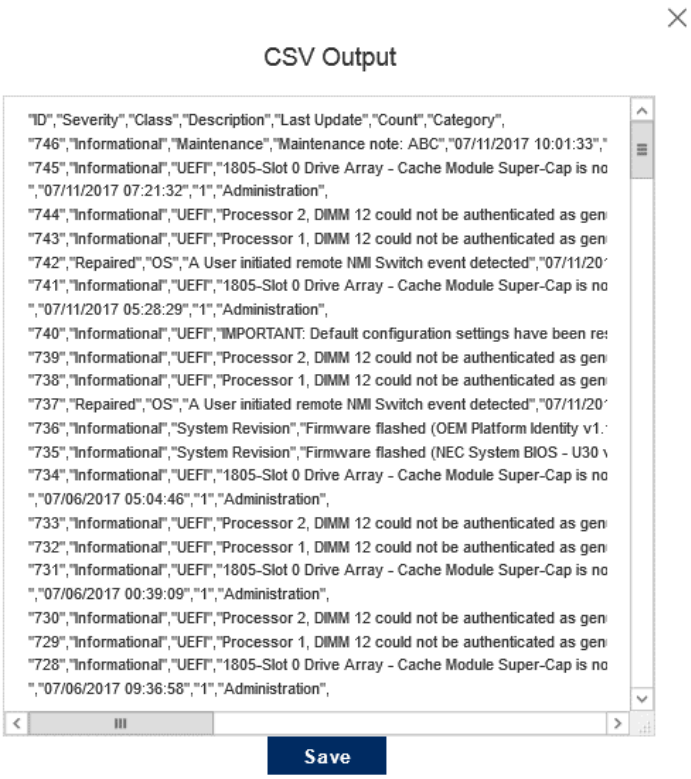
   An **Informational** log entry with the class **Maintenance** is added to the IML.

Saving the IML to a CSV file

Use a supported browser to export the IML to a CSV file.

Procedure

1. Click **Information** in the navigation tree, and then click the **Integrated Management Log** tab.
2. Click the CSV icon .
3. In the **CSV Output** window, click **Save**, and then follow the browser prompts to save or open the file.



Clearing the IML

Prerequisites

Configure iLO Settings privilege

Procedure

1. Click **Information** in the navigation tree, and then click the **Integrated Management Log** tab.
2. Click 🗑.
3. When prompted to confirm the request, click **OK**.

The IML is cleared of all previously logged information and an event is recorded in the IML.

Active Health System

The Active Health System monitors and records changes in the server hardware and system configuration.

The Active Health System provides:

- Continuous health monitoring of over 1600 system parameters
- Logging of all configuration changes
- Consolidated health and service alerts with precise time stamps
- Agentless monitoring that does not affect application performance

Active Health System data collection

The Active Health System does not collect information about your operations, finances, customers, employees, or partners.

Examples of information that is collected:

- Server model and serial number
- Processor model and speed
- Storage capacity and speed
- Memory capacity and speed
- Firmware/BIOS and driver versions and settings

The Active Health System does not parse or change OS data from third-party error event log activities (for example, content created or passed through the OS).

Active Health System Log

The data collected by the Active Health System is stored in the Active Health System Log. The data is logged securely, isolated from the operating system, and separate from customer data.

When the Active Health System Log is full, new data overwrites the oldest data in the log.

When you download and send Active Health System data to NEC Corporation, you agree to have the data used for analysis, technical resolution, and quality improvements.

Downloading the Active Health System Log for a date range

Procedure

1. Click **Information** in the navigation tree, and then click the **Active Health System Log** tab.

   The Active Health System Log is inaccessible when it is being used by System Utilities, EXPRESSBUILDER, or the iLO Service Port.

2. Enter the range of days to include in the log. The default value is seven days.
   a. Click the **From** box.

      A calendar is displayed.
   b. Select the range start date on the calendar.
   c. Click the **To** box.

      A calendar is displayed.
   d. Select the range end date on the calendar.

   To reset the range to the default values, click the **Reset** icon↺.
3. Optional: Enter the following information to include in the downloaded file:
   - Support case number
   - Contact name
   - Phone number
   - Email address
   - Company name

   This information is not written to the log data stored on the server.
4. Click **Download**.
5. Save the file.

Downloading the entire Active Health System Log

It might take a long time to download the entire Active Health System Log. If you must upload the Active Health System Log for a technical issue, NEC Corporation recommends downloading the log for the specific range of dates in which the problem occurred.

Procedure

1. Click **Information** in the navigation tree, and then click **Active Health System Log**.

   The Active Health System Log is inaccessible when it is being used by System Utilities, EXPRESSBUILDER, or the iLO Service Port.
2. Click **Show Advanced Settings**.
3. Optional: Enter the following information to include in the downloaded file:
   - Support case number
   - Contact name
   - Phone number
   - Email address

- Company name

This information is not written to the log data stored on the server.

4. Click **Download Entire Log**.
5. Save the file.

Clearing the Active Health System Log

If the log file is corrupted, or if you want to clear and restart logging, use the following procedure to clear the Active Health System Log.

Prerequisites

Configure iLO Settings privilege

Procedure

1. Click **Information** in the navigation tree, and then click the **Active Health System Log** tab.

   The Active Health System Log is inaccessible when it is being used by EXPRESSBUILDER, the Active Health System download CLI tool, or the iLO Service Port.
2. Click **Show Advanced Settings**.
3. Scroll to the **Clear Log** section, and then click **Clear**.
4. When prompted to confirm the request, click **OK**.

   iLO notifies you that the log is being cleared.
5. Reset iLO.

   Resetting iLO is required because some Active Health System data is recorded to the log only during iLO startup. Performing this step ensures that a complete set of data is available in the log.
6. Reboot the server.

   Rebooting the server is required because some information, such as the operating system name and version, is logged at server startup. Performing this step ensures that a complete set of data is available in the log.

Viewing iLO self-test results

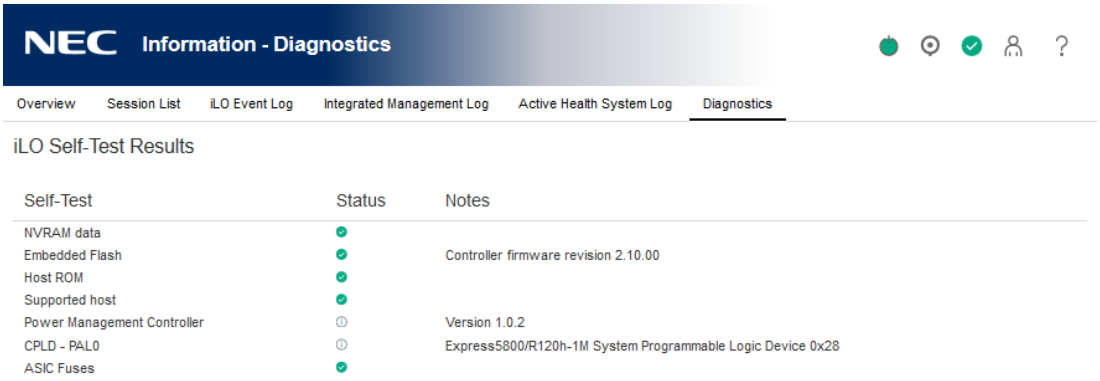
The iLO Self-Test Results section displays the results of internal iLO diagnostic tests, including the test name, status, and notes.

The tests that are run are system-dependent. Not all tests are run on all systems. To see the tests that are performed on your system, view the list on the **Diagnostics** page.

If a status is not reported for a test, the test is not listed.

Procedure

1. Click **Information** in the navigation tree, and then click the **Diagnostics** tab.



iLO self-tests

Self-test details

Self-Test

The tested function.

Status

The test status.

- Pass—The test was successful.
- Fail—The test detected a problem. A reboot, firmware or software update, or service might be required.
- Informational—Supplemental data about the tested system is provided in the Notes column.

Notes

A test might include supplemental information in the Notes column.

For some tests, this column displays the versions of other system programmable logic, such as the System Board PAL or the Power Management Controller.

iLO self-test types

The tests that are run are system-dependent. Not all tests are run on all systems. The possible tests include:

- **Cryptographic**—Tests security features.
- **NVRAM**—Tests the subsystem that retains nonvolatile configuration data, logs, and settings.
- **Embedded Flash**—Tests the state of the system that can store configuration, provisioning, and service information.
- **Power Management**—Tests functions related to power measurement, power capping, and power management.
- **CPLD**—Tests the programmable hardware in the server.
- **Host ROM**—Checks the BIOS to determine whether it is out-of-date compared to the management processor.
- **Supported Host**—Checks the management processor firmware to determine whether it is out of date for the server hardware.
- **EEPROM**— Tests the hardware that stores basic iLO properties that are assigned during the manufacturing process.

5. Viewing general system information

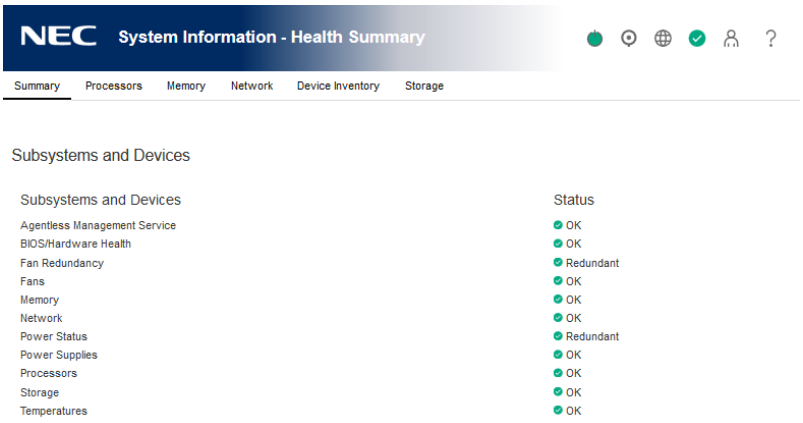
Viewing health summary information

The Health Summary page displays the status of monitored subsystems and devices. Depending on the server configuration, the information on this page varies.

If the server is powered off, the system health information on this page is current as of the last power off. Health information is updated only when the server is powered on and POST is complete.

Procedure

1. Click **System Information** in the navigation tree.



Redundancy status

Redundancy status is displayed for the following:

- **Fan Redundancy**
- **Power Status**

Subsystem and device status

Summarized status information is displayed for the following:

- **Agentless Management Service**
- **BIOS/Hardware Health**
- **Fans**
- **Memory**
- **Network**
- **Power Supplies**
- **Processors**
- **Storage**
- **Temperatures**
- **Smart Storage Battery Status** (supported servers only)

Subsystem and device status values

The **Health Summary** page uses the following status values:

- **Redundant**—There is a backup component for the device or subsystem.
- **OK**—The device or subsystem is working correctly.
- **Not Redundant**—There is no backup component for the device or subsystem.
- **Not Available**—The component is not available or not installed.
- **Degraded**—The device or subsystem is operating at a reduced capacity.

  iLO displays the power supply status as **Degraded** when mismatched power supplies are installed.

  If you power on a server with nonredundant fans or power supplies, the system health status is listed as **OK**. However, if a redundant fan or power supply fails while the system is powered on, the system health status is listed as **Degraded** until you replace the fan or power supply.
- **Failed Redundant**—The device or subsystem is in a nonoperational state.
- **Failed**—One or more components of the device or subsystem are nonoperational.]
- **Other**—For more information, navigate to the **System Information** page of the component that is reporting this status.
- **Link Down**—The network link is down.
- **Unknown**—The iLO firmware has not received data about the device status. If iLO was reset when the server was powered off, some subsystems display the status **Unknown** because the status cannot be updated when the server is powered off.
- **Not Installed**—The subsystem or device is not installed.

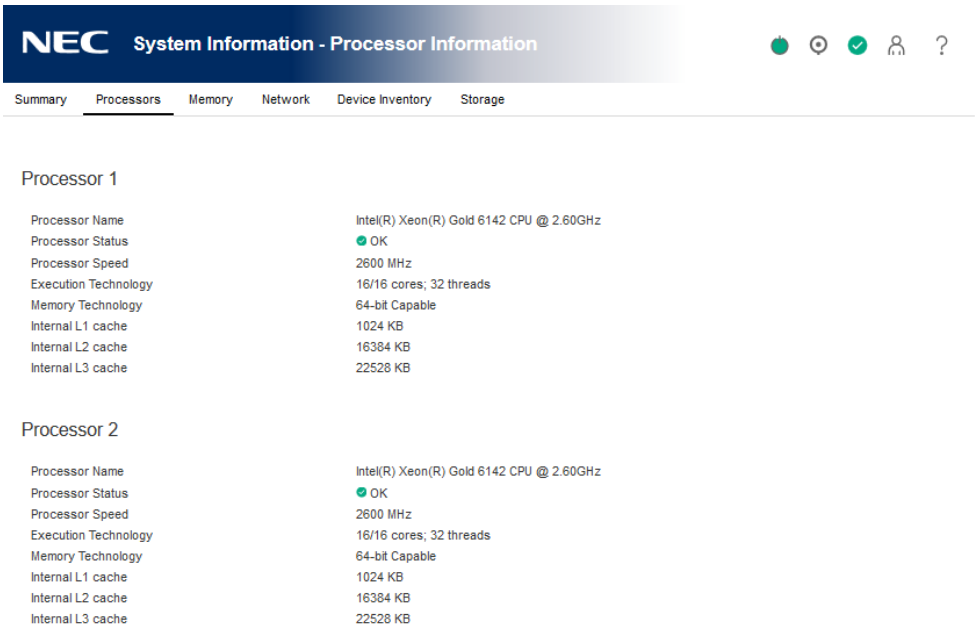
Viewing processor information

The **Processor Information** page displays the available processor slots, the type of processor installed in each slot, and a summary of the processor subsystem.

If the server is powered off, the system health information on this page is current as of the last power off. Health information is updated only when the server is powered on and POST is complete.

Procedure

(ア) Click **System Information** in the navigation tree, and then click the **Processors** tab.



Processor details

The following information is displayed for each processor:

- **Processor Name**—The name of the processor.
- **Processor Status**—The health status of the processor.
- **Processor Speed**—The speed of the processor.
- **Execution Technology**—Information about the processor cores and threads.
- **Memory Technology**—The processor memory capabilities.
- **Internal L1 cache**—The L1 cache size.
- **Internal L2 cache**—The L2 cache size.
- **Internal L3 cache**—The L3 cache size.

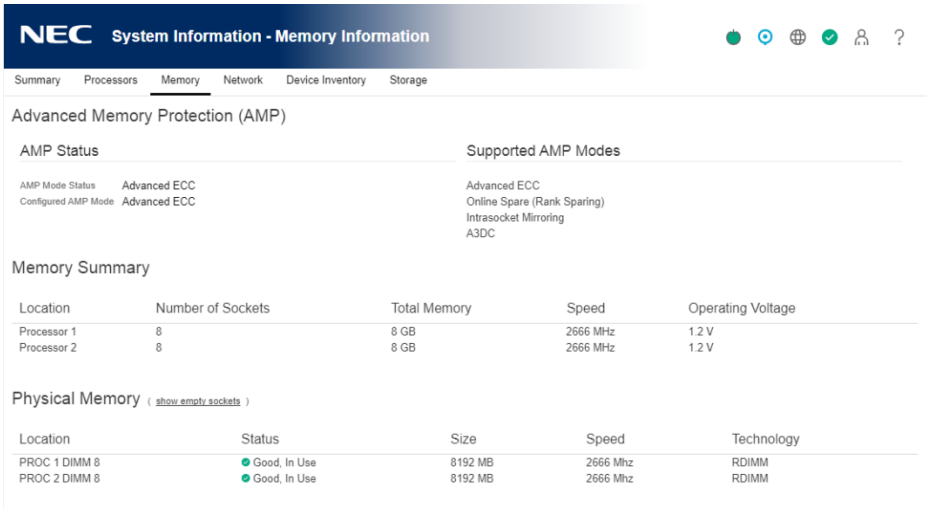
Viewing memory information

The Memory Information page displays a summary of the system memory. When server power is off, AMP data is unavailable, and only memory modules present at POST are displayed.

If the server is powered off, the system health information on this page is current as of the last power off. Health information is updated only when the server is powered on and POST is complete.

Procedure

1. Click **System Information** in the navigation tree, and then click the **Memory** tab. The **Memory** page displays details for the following:
   - **Advanced Memory Protection**
   - **Memory Summary**
   - **Memory Details**
2. Optional: By default, empty memory sockets are hidden in the **Memory Details** table. To view the empty memory sockets, click **show empty sockets**. When empty memory sockets are displayed, click **hide empty sockets** to hide them.



Advanced Memory Protection details

AMP Mode Status

The status of the AMP subsystem.

- **Other/Unknown**—The system does not support AMP, or the management software cannot determine the status.
- **Not Protected**—The system supports AMP, but the feature is disabled.
- **Protected**—The system supports AMP. The feature is enabled but not engaged.
- **Degraded**—The system was protected, but AMP is engaged. Therefore, AMP is no longer available.
- **DIMM ECC**—The system is protected by DIMM ECC only.
- Mirroring—The system is protected by AMP in the mirrored mode. No DIMM faults have been detected.

- **Degraded Mirroring**—The system is protected by AMP in the mirrored mode. One or more DIMM faults have been detected.
- **On-line Spare**—The system is protected by AMP in the hot spare mode. No DIMM faults have been detected.
- **Degraded On**-line Spare—The system is protected by AMP in the hot spare mode. One or more DIMM faults have been detected.
- **RAID-XOR**—The system is protected by AMP in the XOR memory mode. No DIMM faults have been detected.
- **Degraded RAID-XOR**—The system is protected by AMP in the XOR memory mode. One or more DIMM faults have been detected.
- **Advanced ECC**—The system is protected by AMP in the Advanced ECC mode.
- **Degraded Advanced ECC**—The system is protected by AMP in the Advanced ECC mode. One or more DIMM faults have been detected.
- **LockStep**—The system is protected by AMP in the LockStep mode.
- **Degraded LockStep**—The system is protected by AMP in the LockStep mode. One or more DIMM faults have been detected.

Configured AMP Mode

The active AMP mode. The following modes are supported:

- **None/Unknown**—The management software cannot determine the AMP fault tolerance, or the system is not configured for AMP.
- **On-line Spare**—A single spare bank of memory is set aside at boot time. If enough ECC errors occur, the spare memory is activated and the memory that is experiencing the errors is disabled.
- **Mirroring**—The system is configured for mirrored memory protection. All memory banks are duplicated in mirrored memory, as opposed to only one for online spare memory. If enough ECC errors occur, the spare memory is activated and the memory that is experiencing the errors is disabled.
- **RAID-XOR**—The system is configured for AMP with the XOR engine.
- **Advanced ECC**—The system is configured for AMP with the Advanced ECC engine.
- **LockStep**—The system is configured for AMP with the LockStep engine.
- **Online Spare (Rank Sparing)**—The system is configured for Online Spare Rank AMP.
- **Online Spare (Channel Sparing)**—The system is configured for Online Spare Channel AMP.
- **Intersocket Mirroring**—The system is configured for mirrored intersocket AMP between the memory of two processors or boards.
- **Intrasocket Mirroring**—The system is configured for mirrored intrasocket AMP between the memory of a single processor or board.

Supported AMP Modes

- **RAID-XOR**—The system can be configured for AMP using the XOR engine.
- **Dual Board Mirroring**—The system can be configured for mirrored advanced memory protection in a dual memory board configuration. The mirrored memory can be swapped with memory on the same memory board or with memory on the second memory board.
- **Single Board Mirroring**—The system can be configured for mirrored advanced memory

protection in a single memory board.

- **Advanced ECC**—The system can be configured for Advanced ECC.
- **Mirroring**—The system can be configured for mirrored AMP.
- **On-line Spare**—The system can be configured for online spare AMP.
- **LockStep**—The system can be configured for LockStep AMP.
- **Online Spare (Rank Sparing)**—The system can be configured for Online Spare Rank AMP.
- **Online Spare (Channel Sparing)**—The system can be configured for Online Spare Channel AMP.
- **Intersocket Mirroring**—The system can be configured for mirrored intersocket AMP between the memory of two processors or boards.
- **Intrasocket Mirroring**—The system can be configured for mirrored intrasocket AMP between the memory of a single processor or board.
- **None**—The system cannot be configured for AMP.

Memory Summary

The **Memory Summary** section shows a summary of the memory that was installed and operational at POST.

Location

The slot or processor on which the memory board, cartridge, or riser is installed. Possible values follow:

- **System Board**—There is no separate memory board slot. All DIMMs are installed on the motherboard.
- **Board <Number>**—There is a memory board slot available. All DIMMs are installed on the memory board.
- **Processor <Number>**—The processor on which the memory DIMMs are installed.
- **Riser <Number>**—The riser on which the memory DIMMs are installed.

Number of Sockets

The number of present memory module sockets.

Total Memory

The capacity of the memory, including memory recognized by the operating system and memory used for spare, mirrored, or XOR configurations.

Operating Frequency

The frequency at which the memory operates.

Operating Voltage

The voltage at which the memory operates.

Physical Memory Details

The **Physical Memory Details** section shows the physical memory modules on the host that were installed and operational at POST. Unpopulated module positions are also listed. Various resilient memory configurations can change the actual memory inventory from what was sampled at POST. In systems that have a high number of memory modules, all module positions might not be listed.

Location

The slot or processor on which the memory module is installed.

Status

The memory module status and whether the module is in use.

Size

The size of the memory module, in MB.

Speed

The memory module speed.

Technology

The memory module technology. Possible values follow:

- Unknown—Memory technology cannot be determined.
- N/A—Not present.
- Synchronous
- RDIMM
- UDIMM
- LRDIMM
- NVDIMM
- NVDIMM-N
- R-NVDIMM

Logical Memory Details

This section shows the NEC Scalable Persistent Memory devices that were configured and operational at POST.

Location

The processor and/or the region for the logical device. For example, PROC 1,2 Spanned Logical NVDIMM, or PROC 1 Logical NVDIMM 1.

Status

The logical memory status.

Size

The size of the logical memory, in MB.

Speed

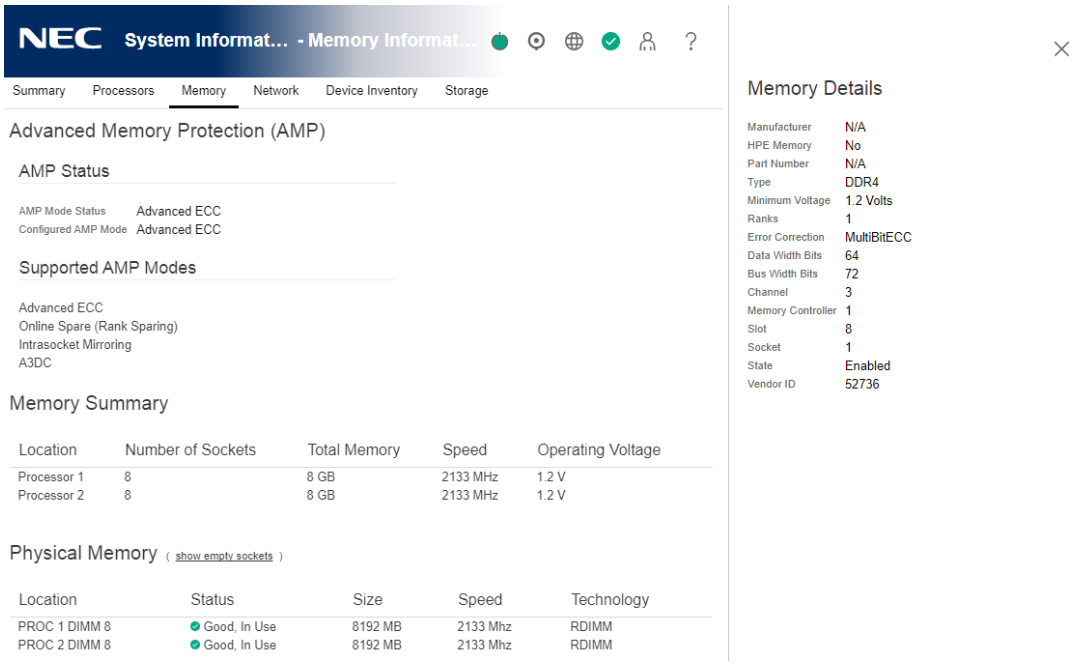
The logical memory speed.

Technology

The logical memory technology. Possible values follow:

- **NVDIMM**
- **NVDIMM-N**
- **R-NVDIMM**

Memory Details pane



Physical Memory

Manufacturer

The memory module manufacturer.

Type

The type of memory installed. Possible values follow:

- **Other**—Memory type cannot be determined.
- **Board**—Memory module is permanently mounted (not modular) on a system board or memory expansion board.
- **DDR4**
- **N/A**—Memory module is not present.

Minimum Voltage

The minimum voltage at which the memory module can operate.

Ranks

The number of ranks in the memory module.

Error Correction

The type of error correction used by the memory module.

Data Width Bits

The memory module data width in bits.

Bus Width Bits

The memory module bus width in bits.

Channel

The channel number in which the memory module is connected.

Memory Controller

The memory controller number.

Slot

The memory module slot number.

Socket

The memory module socket number.

State

The memory state.

Vendor ID

The memory vendor ID.

Armed

The current backup-ready status of the NVDIMM-N, if available.

Last Operation

The status of the last operation.

Media Life

The percentage of media life left.

Logical Memory

Name

The memory module product name.

Manufacturer

The memory module manufacturer.

Power Backup Unit Bays

The number of battery backed unit bays that provide backup power to the logical DIMM.

Type

The type of memory installed.

The only possible value for logical memory is **Logical**.

Minimum Voltage

The minimum voltage at which the memory module can operate.

Ranks

The number of ranks in the memory module.

Error Correction

The type of error correction used by the memory module.

Data Width Bits

The memory module data width in bits.

Bus Width Bits

The memory module bus width in bits.

Memory Media

The proprietary media source of the memory module. For example, NAND or Proprietary.

State

The memory state.

Armed

The current backup-ready status of an NVDIMM-N, if available.

Last Operation

The status of the last operation.

Media Life

The percentage of media life left.

Viewing network information

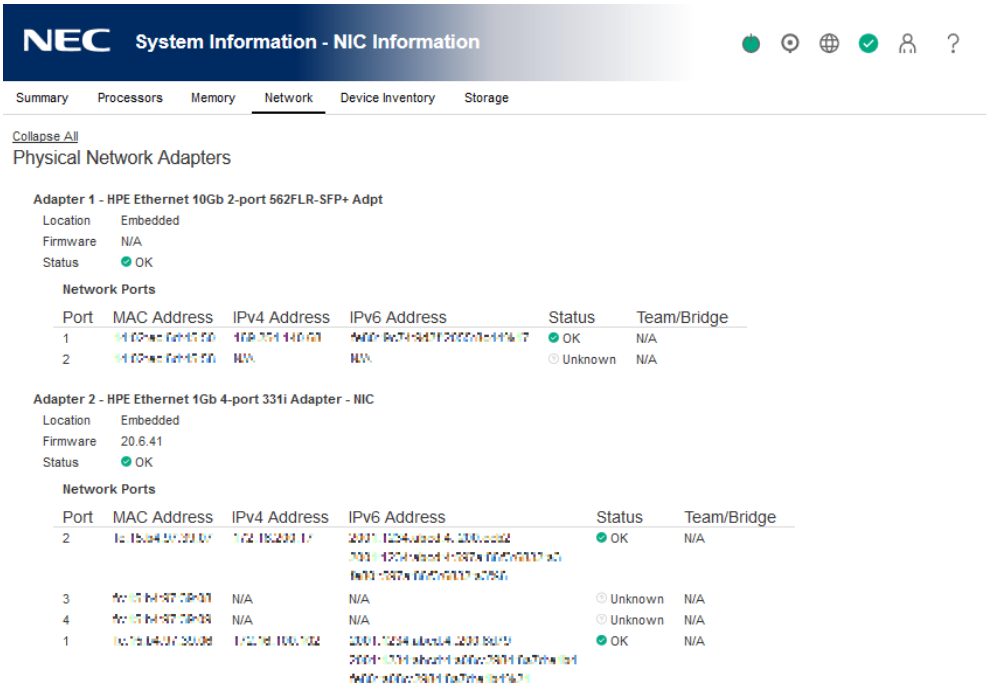
If the server is powered off, the health status information on this page is current as of the last power off. Health information is updated only when the server is powered on and POST is complete.

To view a full set of data on this page, ensure that AMS is installed and running. The server IP address, add in network adapters, and the server NIC status are displayed only if AMS is installed and running on the server.

The information on this page is updated when you log in to iLO. To refresh the data, log out of iLO, and then log back in.

Procedure

1. Click System Information in the navigation tree, and then click the Network tab.
2. Optional: To expand or collapse the information on this page, click Expand All or Collapse All, respectively.



Physical Network Adapters

Integrated and add-in NICs and Fibre Channel adapters

This section displays the following information about the integrated and add-in NICs and Fibre Channel adapters in the server:

- **Adapter number**—The adapter number, for example, **Adapter 1** or **Adapter 2**.
- **Location**—The location of the adapter on the system board.
- **Firmware**—The version of the installed adapter firmware, if applicable. This value is displayed for system NICs (embedded and stand-up) only.
- **Status**—The NIC status.

- On Windows servers:
  If the NIC has never been plugged in to a network, iLO displays the status **Unknown**.
  If the NIC has been plugged in to a network, and is now unplugged, iLO displays the status **Link Down**.
- On Linux servers:
  If NetworkManager is used to manage the NIC, the default status is **Up** and the link status is displayed in iLO.
  If Linux legacy utilities are used to manage the NIC, iLO displays the link status only if the NIC is configured by an administrator. If the NIC is not configured, iLO displays the status **Unknown**.
- On VMware servers:
  If iLO cannot communicate with the NIC port, it displays the status **Unknown**. If the NIC driver reports the status `link_down`, iLO displays the status **Down**.
  If the NIC driver reports the status `link_up`, iLO displays the status **Up**.

- **Port**—The configured network port. This value is displayed for system NICs (embedded and stand-up) only.
- **MAC Address**—The port MAC address.
- **IPv4 Address**—For iLO adapters, the iLO IPv4 address. For system NICs (embedded and stand-up), the server IP address (if available).
- **IPv6 Address**—For iLO adapters, the iLO IPv6 address. For system NICs (embedded and stand-up), the server IP address (if available).
- **Status**—The port status.
- **Team/Bridge**—If a port is configured for NIC teaming, the name of the configured link between the physical ports that form a logical network adapter. This value is displayed for system NICs (embedded and stand-up) only.

Fibre Channel host bus adapters or converged network adapters

The following information is displayed for Fibre Channel host bus adapters or converged network adapters:

- **Physical Port**—The physical network port number.
- **WWNN**—The port world-wide node name.
- **WWPN**—The world-wide port name.
- **Status**—The port status.

Boot progress and boot targets

The following information about the boot progress and boot targets is displayed when DCI connectivity is available:

- **Port**—The configured virtual port number.
- **Boot Progress**—The current boot status.
- **Boot Targets**
  - **WWPN**—The world-wide port name.
  - **LUN ID**—The logical unit number ID.

Logical Network Adapters

This section displays the following information about network adapters that use NIC teaming to combine two or more ports into a single logical network connection:

Adapter name—The name of the configured link between the physical ports that form the logical network adapter.

- **MAC Address**—The logical network adapter MAC address.
- **IP Address**—The logical network adapter IP address.
- **Status**—The logical network adapter status.

The following information is displayed for the ports that form each logical network adapter:

- **Members**—A sequential number assigned to each port that forms the logical network adapter.
- **MAC Address**—The MAC address of the physical adapter port.
- **Status**—The status of the physical adapter port.

Viewing the device inventory

The **Device Inventory** page displays information about devices installed on the system board. Some examples of the devices listed on this page include installed adapters, PCI devices, SATA controllers, and Smart Storage batteries.

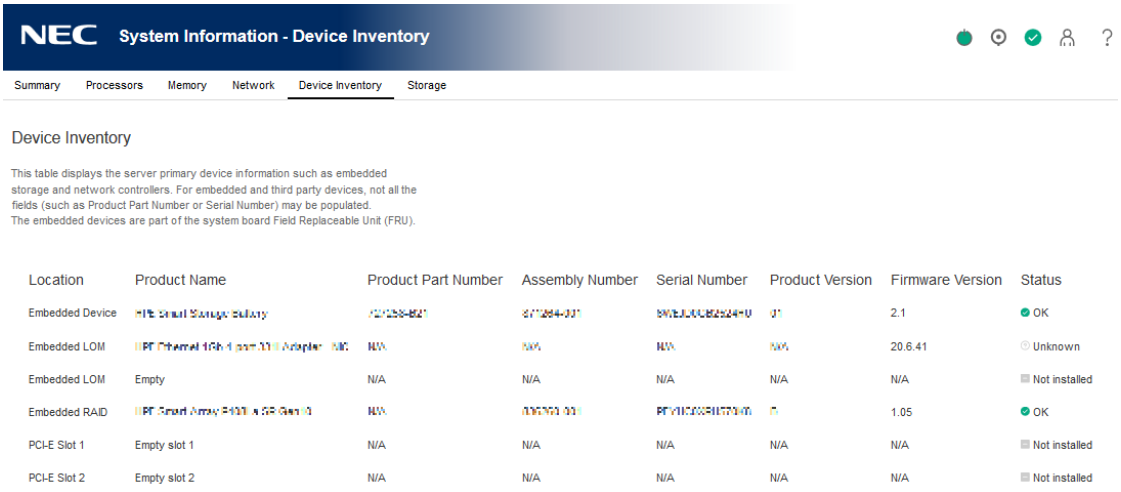
If the server is powered off, the health status information on this page is current as of the last power on. Health information is updated only when the server is powered on and POST is complete.

The following information is displayed only if AMS is installed and running on the server: Firmware version and status of add-in network adapters, network-attached storage details, and Smart Storage Battery status.

If the iLO firmware cannot retrieve the network adapter product name or part number directly from the device, it attempts to collect that information from AMS.

Procedure

1. Click **System Information** in the navigation tree, and then click the **Device Inventory** tab.



Device Inventory details

- **Location**—The device install location.
- **Product Name**—The device product name.
- **Product Part Number**—The device part number.
  This column displays the value **Various** when the actual part number of the listed device depends on internally installed graphics devices that differ by server model.
- **Assembly Number**—The device part number (NEC Corporation devices) or the EEPROM Board Info data (third-party devices).
- **Serial Number**—The device serial number.
- **Product Version**—The device product version.
- **Firmware Version**—The installed device firmware version.
- **Status**—The device status.

Device status values

The **Device Inventory** page uses the following status values:

- **OK**—The device is working correctly.
- **Other**—The device status could not be determined.
- **No Supporting CPU**—The CPU that supports the device slot is not installed.
- **Not Installed**—A device is not installed.
- **Link Down**—The network link is down.
- **Failed**—One or more components of the device are nonoperational.
- **Degraded**—The device is operating at a reduced capacity.
- **Unknown**—The iLO firmware has not received data about the device status.

Viewing PCI slot details

Procedure

1. Click **System Information** in the navigation tree, and then click the **Device Inventory** tab.
2. Move the cursor over the **Location** column for a listed PCI slot.

PCI slot tooltip details

- **Type**—The PCI slot type.
- **Bus Width**—The PCI slot bus width.
- **Length**—The PCI slot length.
- **Characteristics 1**—Information about the PCI slot, for example, voltage and other support information.
- **Characteristics 2**—Information about the PCI slot, for example, voltage and other support information.

Viewing storage information

If the server is powered off, the system health information on this page is current as of the last power off. Health information is updated only when the server is powered on and POST is complete.

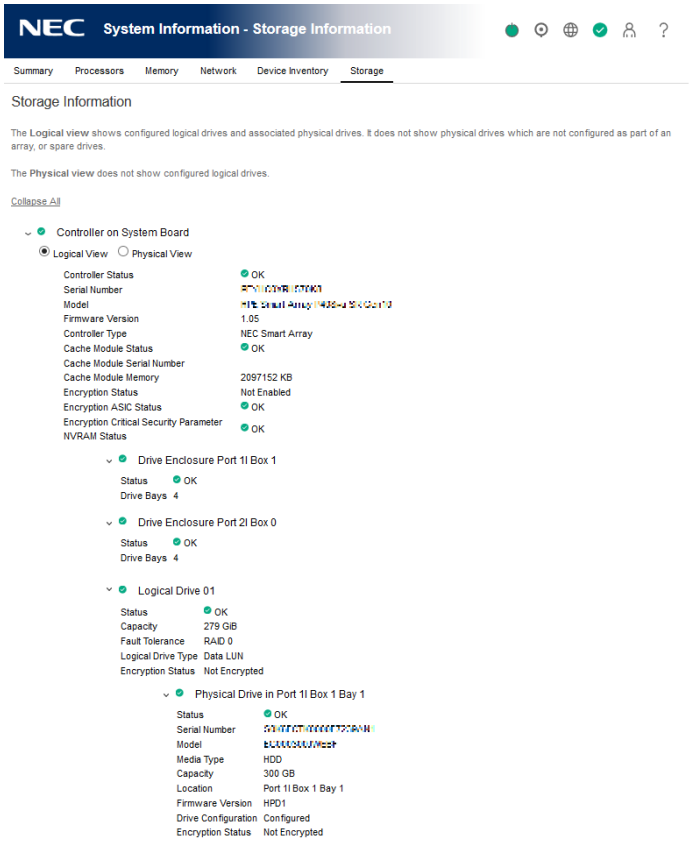
To view a full set of data on this page, ensure that AMS is installed and running. SAS/SATA controller information is displayed only if AMS is installed and running on the server.

The information displayed on this page depends on your storage configuration. Some storage configurations will not display information for every category.

Fibre Channel adapters are not listed on this page. To view information about Fibre Channel adapters, click **System Information** in the navigation tree, and then click the **Network** tab.

Procedure

1. Click **System Information** in the navigation tree, and then click the Storage tab.
2. Optional: To expand or collapse the data, click Expand All or Collapse All, respectively.
3. Smart Array controllers only: For the controller you want to view, select one of the following options:
   - **Logical View**—View configured logical drives and associated physical drives. This view does not show physical drives that are not configured as part of an array, or spare drives.
   - **Physical View**—View physical drives. This view does not show logical drives.



Supported storage components

The **Storage Information** page displays information about the following storage components:

- Smart Array controllers, drive enclosures, the attached logical drives, and the physical drives that constitute the logical drives.
- NEC and third-party storage controllers that manage direct-attached storage, and the attached physical drives.

  iLO 5 supports the following products:
  - M.2 SSD Enablement Kit
  - 12G SAS Expander
  - Dual 8GB MicroSD EM USB Kit
  - NVMe drives

Smart Array controllers are listed first on the page, followed by other NEC Corporation and third-party storage controllers.

Smart Array details

iLO displays information controllers, enclosures, logical drives, and physical drives.

iLO can monitor 256 physical drives total and 256 logical drives total.

Controllers

This section provides the following details for each Smart Array controller.

- **Controller location**—Slot number or system board
- **Top-level controller status** (displayed on the left of the controller location)—A combination of the controller hardware status and the status of cache modules, enclosures, and physical, logical, and spare drives associated with the controller. If the controller hardware status is **OK**, and any associated hardware has a failure, the top-level controller status changes to **Major Warning** or **Degraded**, depending on the failure type. If the controller hardware has a **Failed** status, the top-level controller status is **Failed**.
- **Controller Status**—Controller hardware status (**OK** or **Failed**)
- **Serial Number**
- **Model**
- **Firmware Version**
- **Controller Type**
- **Cache Module Status**
- **Cache Module Serial Number**
- **Cache Module Memory**
- **Encryption Status**—Indicates whether encryption is enabled in the controller.
  The following values are possible:
  - **Enabled**
  - **Not Enabled**
  - **Enabled—Local Mode**—This value is displayed when you do not use a remote key

management server.

- **Encryption ASIC Status**—Indicates whether the ASIC encryption self tests for the controller passed or failed. A failed status indicates that the controller is not encrypted.
- **Encryption Critical Security Parameter NVRAM Status**—Indicates whether the controller successfully detected the critical security parameter NVRAM. A failed status means that the controller is not encrypted.

The encryption settings for a Smart Array controller can be configured by using the Smart Storage Administrator software.

Drive enclosures

This section provides the following information about the drive enclosures attached to a Smart Array controller.

- **Enclosure port and box numbers**
- **Status**
- **Drive Bays—**The number of drive bays
- **Serial Number**
- **Model**
- **Firmware Version**

Some enclosures do not have all the listed properties, and some storage configurations do not have drive enclosures.

Logical drives

When the **Logical View** option is selected, the following information is listed for the logical drives attached to a Smart Array controller.

- **Logical drive number**
- **Status**
- **Capacity**
- **Fault Tolerance**
- **Logical Drive Type**
- **Encryption Status**

Logical drives must be configured through the Smart Storage Administrator software before they can be displayed on this page.

Physical drives

The information listed in this section depends on whether the **Logical View** or **Physical View** option is selected. In the **Logical View**, physical drives that are configured as part of an array are listed. In the **Physical View**, all physical drives are listed.

When a physical drive has a **Failed** status, this status does not affect the overall storage health status. Only logical drives affect the storage health status.

The following information is listed for the physical drives attached to a Smart Array controller:

- **Physical drive port, box, and bay numbers**

- **Status**
- **Serial Number**
- **Model**
- **Media Type**
- **Capacity**
- **Location**
- **Firmware Version**
- **Drive Configuration**
- **Encryption Status**

Direct-attached storage details

Controllers

This section provides the following information about the NEC Corporation and third-party storage controllers that manage direct-attached storage.

- **Controller location**
- **Top-level controller status**—The top-level controller status (displayed on the left of the controller location) is a combination of the controller hardware status and the status of the enclosures, physical drives, and spare drives associated with the controller. If the controller hardware status is OK, and any associated hardware has a failure, the top-level controller status changes to Major Warning or Degraded, depending on the failure type. If the controller hardware has a Failed status, the top-level controller status is Failed.
- **Controller Statu**s—Controller hardware status (OK or Failed)
- **Serial Number**
- **Model**
- **Firmware Version**
- **Controller Typ**e

Physical Drives

This section provides information about physical drives attached to NEC Corporation and third-party storage controllers.

When a physical drive has a **Failed** status, this status does not affect the overall storage health status. Only logical drives affect the storage health status.

- **Physical drive location**
- **Status**
- **Serial Number**
- **Model**
- **Media Type**
- **Capacity**
- **Location**
- **Firmware Version**
- **Drive Configuration**
- **Encryption Status**

6. Managing firmware, software, and language packs

Firmware updates

Firmware updates enhance server and iLO functionality with new features, improvements, and security updates.

You can update firmware by using an online or offline firmware update method.

Online firmware update

When you use an online method to update firmware, you can perform the update without shutting down the server operating system. Online firmware updates can be performed in-band or out-of-band.

In-band

Firmware is sent to iLO from the server host operating system.

The iLO 5 Channel Interface Driver is required for in-band firmware updates.

During a host-based firmware update, it does not verify user credentials or privileges because the host-based utilities require a root (Linux and VMware) or Administrator (Windows) login.

The iLO Online ROM Flash Component is examples of online in-band firmware update methods.

Out-of-band

Firmware is sent to iLO over a network connection. Users with the Configure iLO Settings privilege can update firmware by using an out-of-band method. If the system maintenance switch is set to disable iLO security, any user can update firmware with an out-of-band method.

The iLO web interface, the iLO RESTful API, and SMASH CLP are examples of online out-of-band firmware update methods.

Online firmware update methods

In-band firmware updates

- **Online ROM Flash Component**—Use an executable file to update firmware while the server is running. The executable file contains the installer and the firmware package.

  You can download online ROM flash components for iLO and server firmware at the following website: **http://www.nec.com/express/**.

  This option is supported when iLO is configured to use the Production security state.

Out-of-band firmware updates

- **iLO web interface**—Download a supported firmware file and install it by using the iLO web interface. You can update firmware for a single server or an iLO Federation group.
- **iLO RESTful API**—Use the iLO RESTful API and a REST client such as the RESTful Interface Tool to update firmware.
- **SMASH CLP**—Access SMASH CLP through the SSH port, and use standard commands to view firmware information and update firmware.

Offline firmware update

When you use an offline method to update the firmware, you must reboot the server by using an offline utility.

The SPP, SUM are examples of offline firmware update methods.

Offline firmware update methods

You can use the following offline firmware update methods:

Starter Pack

Use the StarterPack to install firmware.

SUM

SUM is a tool for firmware, driver, and software maintenance on supported servers and other nodes.

You can use SUM together with iLO to access the iLO repository and manage install sets and the installation queue.

Viewing and updating firmware from the iLO web interface

The iLO web interface supports the following firmware and software management features:

- Viewing **installed firmware**.
- Viewing **installed software**.
- Using the **Flash Firmware** controls to install firmware on the local managed server.
- Using the **Group Firmware Update** feature to install firmware on multiple servers in an iLO Federation group.
- Accessing the iLO with integrated Smart Update features. This version of iLO supports the following actions:
  - Manage the **iLO Repository** and add saved components to the installation queue.
  - View and remove **install sets** and add them to the installation queue.
  - Use SUM to configure install sets.
    The best practice is to use SUM to manage the installation queue. You can use the iLO web interface to update the queue by adding or removing an individual component.

You can access the iLO Repository and the **Flash Firmware** controls from all tabs on the **Firmware & OS Software** page.

Updating iLO or server firmware by using the Flash Firmware feature

You can update firmware from any network client by using the iLO web interface. A signed file is required. You can also initiate a component update from the **iLO Repository** page.

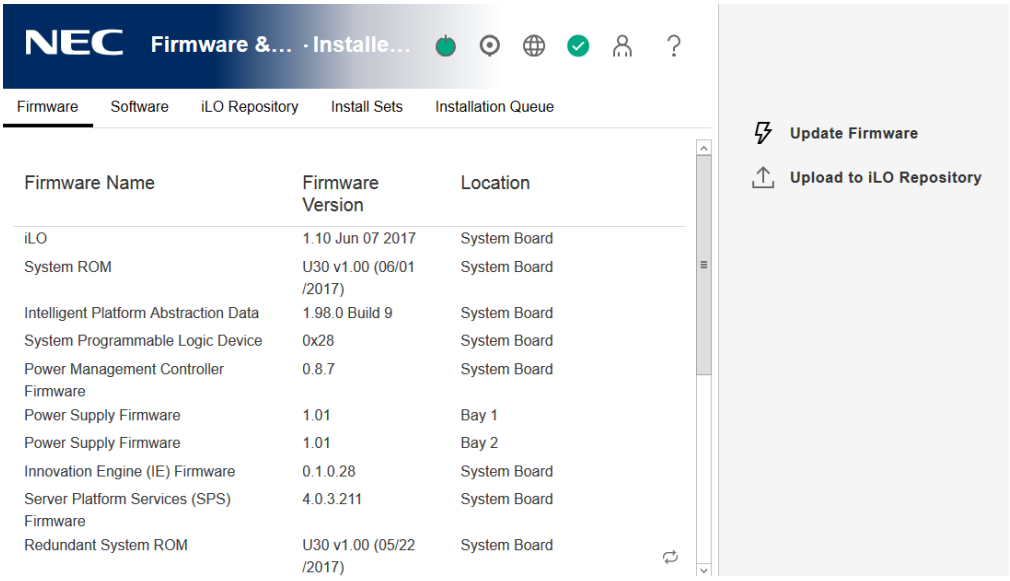
Prerequisites

Configure iLO Settings privilege

Procedure

1. Obtain an **iLO firmware** or **server firmware** file.
2. Click **Firmware & OS Software** in the navigation tree, and then click **Update Firmware**.

   If the **Update Firmware** option is not displayed, click the ellipsis icon in the top right corner of the iLO web interface, then click **Update Firmware**.



3. Select the **Local file** or **Remote file** option.
4. Depending on the option you selected, do one of the following:
   - In the **Local binary file** box, click **Browse** (Internet Explorer or Firefox) or **Choose Files** (Chrome), and then specify the location of the firmware component.
   - In the **Remote binary file URL** box, enter the URL for a firmware component on an accessible web server.
5. Optional: To save a copy of the component to the iLO Repository, select the **Also store in iLO Repository** check box.
6. To start the update process, click **Flash**.
   Depending on the server configuration, iLO notifies you that:
   - When you update the iLO firmware, iLO will reboot automatically.
     Some types of server firmware might require a server reboot, but the server will not reboot automatically.
   - A TPM or TM is installed in this server. Before you initiate a system ROM or iLO firmware

update, suspend or back up any software that stores information on the TPM or TM. For example, if you use drive encryption software, suspend it before initiating a firmware update. Failure to follow these instructions might result in losing access to your data.

7. Do one of the following:
   - If a TPM or TM message was not displayed, click **OK**.
   - If a TPM or TM message was displayed, verify that any software that stores data on the TPM or TM is suspended or backed up, and then click **OK**.

   The iLO firmware receives, validates, and then flashes the firmware image.
   When you update the iLO firmware, iLO reboots and closes your browser connection. It might take several minutes before you can re-establish a connection.
8. For iLO firmware updates only: To start working with the new firmware, clear your browser cache, and then log in to iLO.
9. For server firmware updates only: If the firmware type requires a system reset or server reboot for the new firmware to take effect, take the appropriate action. For more information, see **Requirements for firmware update to take effect** .
10. Optional: To confirm that the new firmware is active, check the firmware version on the **Installed Firmware** page.

    You can also check the iLO firmware version on the **Overview** page.

Supported firmware types

Many types of firmware update are supported, depending on the server platform. These types include:

- iLO
- System ROM/BIOS
- Chassis
- Power Management Controller
- Programmable Logic (CPLD)
- Backplane
- Language Packs

Requirements for firmware update to take effect

- iLO firmware or language pack—Requires an iLO reset, which is triggered automatically.
- System ROM (BIOS)—Requires a server reboot.
- Chassis firmware (Power Management)—Take effect immediately.
- System Programmable Logic Device (CPLD)—Requires a server reboot.
- Power Management Controller and NVMe Backplane Firmware—Do not require a server reboot or a system reset.

  The NVMe firmware version will be displayed in the iLO web interface after the next server reboot.

Obtaining the iLO firmware image file

You can download an iLO firmware image file and use it to update a single server or multiple servers in an iLO Federation group.

The BIN file from the iLO Online ROM Flash Component is required for updating the iLO firmware with the

Flash Firmware and **Group Firmware Update** features.

Procedure

1. Navigate to the following website: **http://www.nec.com/express/.**
2. To locate and download the iLO Online ROM Flash Component file, follow the onscreen instructions.

   Download a Windows or Linux component.
3. Extract the BIN file.
   - For Windows components: Double-click the downloaded file, and then click the **Extract** button. Select a location for the extracted files, and then click **OK**.
   - For Linux components: Depending on the file format, enter one of the following commands:
     - `#sh ./CP00XXXX.scexe –unpack=/tmp/`
     - `#rpm2cpio <firmware_file_name>.rpm | cpio -id`

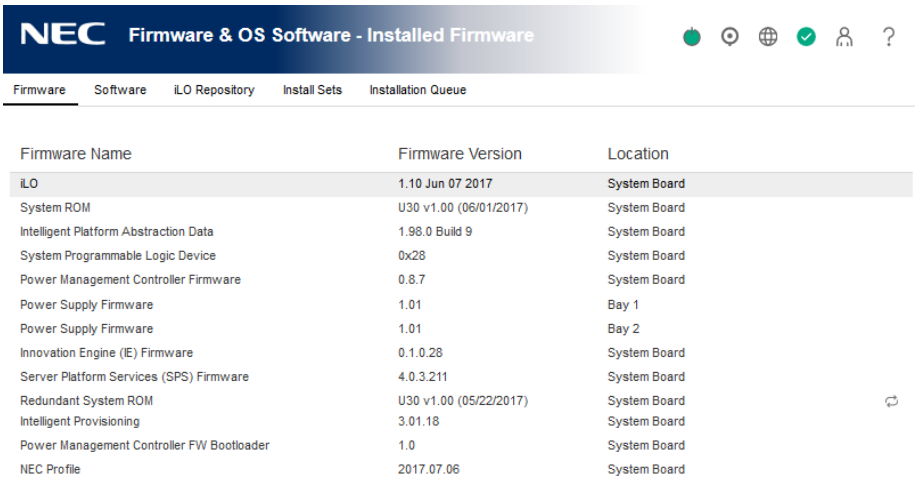
   The name of the iLO firmware image file is similar to `iLO 5_<yyy>.bin`, where `<yyy>` represents the firmware version.

Viewing installed firmware information

Procedure

1. Click **Firmware & OS Software** in the navigation tree.

   The **Installed Firmware** page displays firmware information for various server components. If the server is powered off, the information on this page is current as of the last power off. Firmware information is updated only when the server is powered on and POST is complete.



Firmware types

The firmware types listed on the **Installed Firmware** page vary based on the server model and configuration.

For most servers, the system ROM and iLO firmware are listed. Other possible firmware options include the following:

- Power Management Controller
- Server Platform Services Firmware
- Smart Array
- Intelligent Platform Abstraction Data
- Smart Storage Battery
- TPM or TM firmware
- SAS Programmable Logic Device
- System Programmable Logic Device
- EXPRESSBUILDER
- Networking adapters
- NVMe Backplane firmware
- Innovation Engine (IE) firmware
- Drive firmware
- Power Supply firmware

Firmware details

The **Installed Firmware** page displays the following information for each listed firmware type:

- **Firmware Name**—The name of the firmware.
- **Firmware Version**—The version of the firmware.
- **Location**—The location of the component that uses the listed firmware.

Replacing the active system ROM with the redundant system ROM

Prerequisites

- The server supports redundant system ROM.
- Virtual Power and Reset privilege

Procedure

1. Click **Firmware & OS Software** in the navigation tree.
2. On the **Firmware** tab, click the swap icon ⟲ next to the **Redundant System ROM** details. iLO prompts you to confirm the request.
3. Click **OK**.

   The change will take effect after the next server reboot.

iLO Repository

The iLO Repository is a secure storage area in the nonvolatile flash memory embedded on the system board. This flash memory is called the iLO NAND. Use SUM or iLO to manage signed software and firmware components in the iLO Repository.

iLO, the UEFI BIOS, SUM, and other client software can retrieve these components and apply them to supported servers. Use SUM to organize the stored components into install sets and SUM or iLO to manage the installation queue.

Adding a component to the iLO Repository

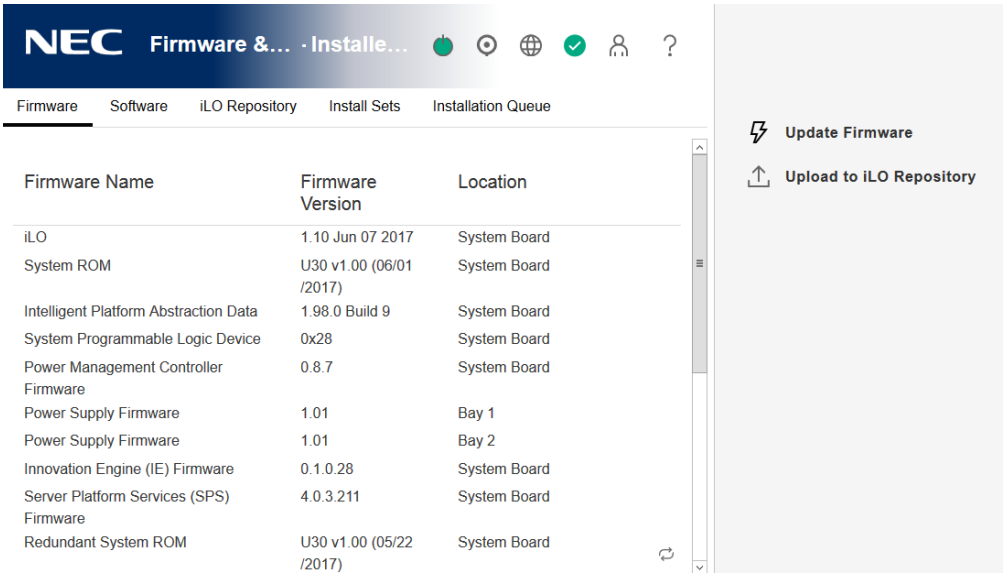
Prerequisites

Configure iLO Settings privilege

Procedure

1. Click **Firmware & OS Software** in the navigation tree, and then click Upload to **iLO Repository**.

   If the **Upload to iLO Repository** option is not displayed, click the ellipsis icon in the top right corner of the iLO web interface, then click **Upload to iLO Repository**.



2. Select the Local file or Remote file option.
3. Depending on the option you selected, do one of the following:
   - In the **Local binary file** box, click **Browse** (Internet Explorer or Firefox) or **Choose Files** (Chrome), and then specify the location of the firmware component.
   - In the **Remote binary file URL** box, enter the URL for a firmware component on an accessible web server.
4. For firmware components specified by multiple files only: Select the **I have a component signature file** check box.
5. If you selected the check box in the previous step, do one of the following:

- In the **Local component signature file** box, click **Browse** (Internet Explorer or Firefox) or **Choose Files** (Chrome), and then specify the location of the component signature file.
- In the **Remote component signature file URL** box, enter the URL for a component signature file on an accessible web server.

6. Click **Upload**.

   iLO notifies you that uploading a component with the same name as an existing component will replace the existing component. Components that are part of the Recovery Set are protected and cannot be replaced by uploading a new component with the same name. To replace a Recovery Set component, log in with an account that has the Recovery Set privilege, and then delete the recovery install set.

7. Click **OK**.

   The upload starts. The upload status is displayed at the top of the iLO web interface.

Installing a component from the iLO Repository

You can add a component to the installation queue from the **iLO Repository** page.

When you add a component to the installation queue, it is added to the end of the queue. After other queued items are complete, the added component is installed when the software that initiates updates for the component type detects the installation request. To determine the software that can initiate an update, check the component details on the **iLO Repository** and **Installation Queue** pages.

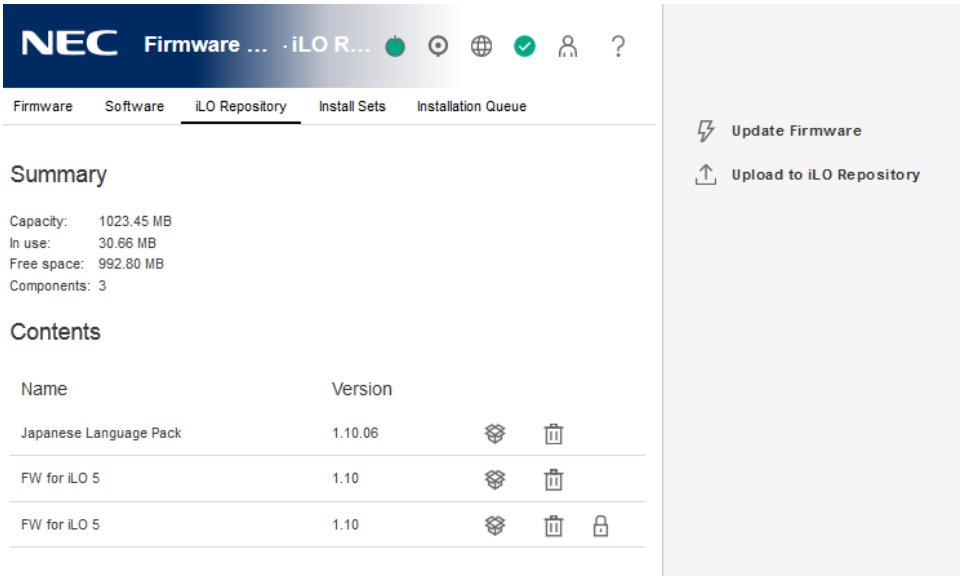
If a component in a previously queued task is waiting to start or finish, a new queued component might be delayed indefinitely. For example, if a queued update must wait until the UEFI BIOS detects it during server POST, but the server is not restarted, then the updates that follow in the queue will not be installed.

Prerequisites

Configure iLO Settings privilege

Procedure

1. Click **Firmware & OS Software** in the navigation tree, and then click **iLO Repository**.



2. Click the install component icon next to the component you want to install.

   iLO notifies you that the component will be added to the end of the installation queue, and prompts you to confirm the request.

3. Click **Yes, add to the end of the queue.**

   If the installation queue is empty, and iLO can initiate the component installation, the button is labeled **Yes, install now.**

   The update is initiated after existing queued tasks finish and the software that initiates installation for the selected component type detects a pending installation. If the installation queue is empty and iLO can initiate the update, the update begins immediately.

Removing a component from the iLO Repository

Prerequisites

- Configure iLO Settings privilege
- The component is not in an install set.
- The component is not part of a queued task.

Procedure

1. Click **Firmware & OS Software** in the navigation tree, and then click the **iLO Repository** tab.
2. Click the remove component icon . iLO prompts you to confirm the request.
3. Click **Yes, remove**.
   The component is removed.

Viewing iLO Repository summary and component details

Procedure

1. Click **Firmware & OS Software** in the navigation tree, and then click the **iLO Repository** tab.
2. Optional: To view detailed component information, click an individual component.

iLO Repository details

iLO Repository storage details

The **Summary** section of the iLO Repository page displays the following details about the iLO Repository storage use:

- **Capacity**—Total iLO Repository storage capacity
- **In Use**—Used storage
- **Free Space**—Available iLO Repository storage
- **Components**—Number of saved components in the iLO Repository

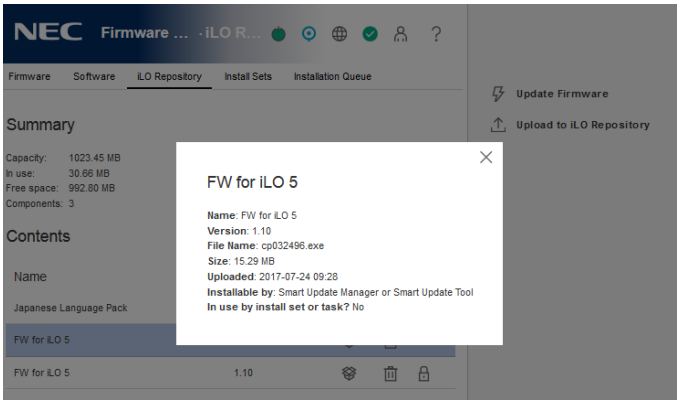
iLO Repository contents

The **Contents** section of the **iLO Repository** page displays the following details about each firmware or software component:

- **Name**
- **Version**

iLO Repository individual component details

When you click an individual component, the following details are displayed:



- **Name**—Component name
- **Version**—Component version
- **File Name**—Component file name
- **Size**—Component size
- **Uploaded**—Upload date and time
- **Installable by**—The software that can initiate an update with the component.
- **In use by install set or task?**—Whether the component is part of an install set.

Install Sets

An install set is a group of components that can be applied to supported servers with a single command. Use SUM to create install sets. You can use iLO to view existing install sets in the iLO web interface.

Saving an install set when you deploy from SUM keeps all the components on the iLO system for immediate use at a later time to restore or roll back a component version without needing to find the original SPP.

Installing an install set

You can add an install set to the installation queue from the Install Sets page.

When you add an install set to the installation queue, iLO adds a task to the end of the installation queue for each component or command in the install set. After other queued items are complete, the install set contents are installed when the software that initiates updates for each component type detects the installation request. To determine the software that can initiate an update, check the component details.

If a component in a previously queued task is waiting to start or finish, a new queued component might be delayed indefinitely. For example, if a queued update must wait until the UEFI BIOS detects it during server POST, but the server is not restarted, then the updates that follow in the queue will not be installed.

Prerequisites

- Configure iLO Settings privilege
- No components in the install set are queued as part of another installation task.

Procedure

1. Click **Firmware & OS Software** in the navigation tree, and then click **Install Sets**.
2. Click the install icon  next to the install set you want to install.

iLO notifies you that the contents of the install set will be added to the end of the installation queue, and prompts you to confirm the request.

3. **Click** Yes, add to the end of the queue..

If the installation queue is empty, and iLO can initiate the updates in the install set, the button is labeled **Yes, install now**.

The updates are initiated after existing queued tasks finish and the software that initiates installation for the selected component types detects a pending installation.

If the installation queue is empty and iLO can initiate the requested updates, the update begins immediately.

Removing an Install Set

Prerequisites

- Configure iLO Settings privilege for unprotected install sets.
- Recovery Set privilege for removing the protected install set.

Procedure

1. Click **Firmware & OS Software** in the navigation tree, and then click **Install Sets**.
2. Click the remove install set icon .

   iLO prompts you to confirm the request.
3. Click **Yes, remove**.

   The install set is removed.

Viewing Install Sets

Procedure

1. Click **Firmware & OS Software** in the navigation tree, and then click the **Install Sets** tab.
2. Optional: Click an install set to view detailed information.

Install Set details

Install Set summary details

The **Install Sets** tab displays the following details about each install set:

- **Name**—The install set name.
- **Components/Commands**—The components and commands in the install set.

Use the install set icons to **add an install set to the installation queue** or to **remove an install set**. The protected install set is displayed with a lock icon.

Individual install set details

When you click an individual install set, the following details are displayed:

- **Name**—The install set name.
- **Created**—The creation date and time.
- **Description**—A description of the install set.
- **Component/Commands**—The components and commands in the install set.
  System Recovery Set?—Indicates whether the install set can be edited or deleted. This status is used for the **system recovery set**. Only one system recovery set can exist at a time.

System recovery set

By default, a system recovery install set is included with every server. User accounts with the **Recovery Set** privilege can configure this install set.

The following firmware components are included in the default system recovery set:

- System ROM (BIOS)
- iLO firmware
- System Programmable Logic Device (CPLD)
- Innovation Engine
- Server Platform Services (SPS) Firmware

If the default system recovery set is deleted, a user with the **Recovery Set** privilege can use SUM to create an install set, and then designate it as the system recovery set by using the iLO RESTful API. For instructions, see the SUM user guide. Only one system recovery install set can exist at a time.

Installation Queue

The installation queue is an ordered list of components that were added to the queue individually or as parts of an install set. Use SUM to manage the queue. You can view queued tasks and add single components to the queue from the iLO web interface.

When you add a component to the installation queue, it is added to the end of the queue. After other queued items are complete, the added component is installed when the software that initiates updates for the component type detects the installation request. To determine the software that can initiate an update, check the component details on the **iLO Repository** and **Installation Queue** pages.

If a component in a previously queued task is waiting to start or finish, a new queued component might be delayed indefinitely. For example, if a queued update must wait until the UEFI BIOS detects it during server POST, but the server is not restarted, then the updates that follow in the queue will not be installed.

To learn more about how iLO, SUM, and the BIOS software work together to manage software and firmware, see the SUM documentation.

Viewing the Installation Queue

Procedure

1. Click **Firmware & OS Software** in the navigation tree, and then click the **Installation Queue** tab.
2. Optional: To view detailed information, click an individual task.

Queued task details

Task summary details

The **Installation Queue** tab displays the following details about each task:

State

Status of the task. The possible values follow:

- **In progress**—The task is being processed.
- **Expired**—The task is expired. Subsequent tasks will not run until this task is removed from the queue.
- **Exception**—The task could not complete. Subsequent tasks will not run until this task is removed from the queue.
- **Complete**—The task completed successfully.
- **Pending**—The task will run when the software that initiates updates for the component type detects the installation request.

Name

The task name.

Starts

The task start date and time.

Expires

The task expiration date and time.

Individual task details

When you click an individual task, the following details are displayed:

- **Name**—The task name.
- **State**—Task status.
- **Result**—Task results, if available.
- **Installable by**—The software that can initiate an update with the selected component.
- **Start time**—The task start date and time.
- **Expiration**—The task expiration date and time.

Removing a task from the Installation Queue

Prerequisites

Configure iLO Settings privilege

Procedure

1. Click **Firmware & OS Software** in the navigation tree, and then click **Installation Queue**.
2. Click the remove component icon 🗑.

   iLO prompts you to confirm the request.
3. Click **Yes, remove**.

   The component is removed.

Installing language packs

Prerequisites

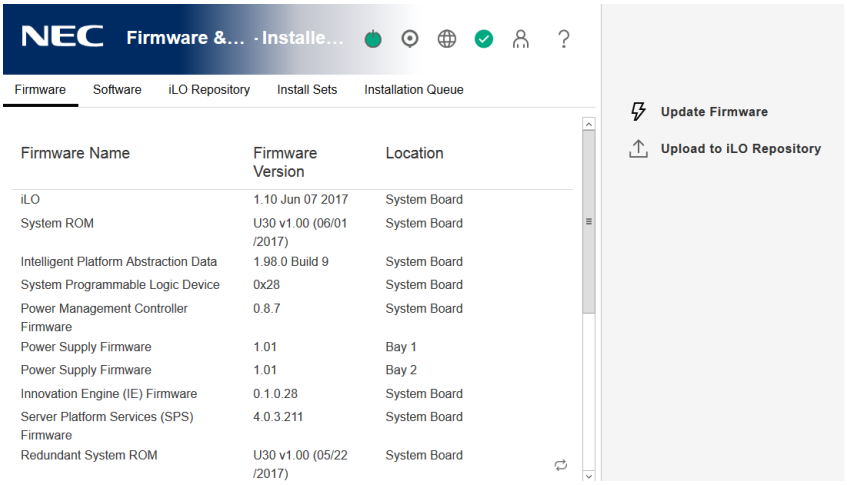
Configure iLO Settings privilege

Procedure

1. Download a language pack from the following website: **http://www.nec.com/express/**.
2. To extract the contents, double-click the downloaded file.

   The language pack file name is similar to the following: lang_<language>_<version>.lpk.
3. Click **Firmware & OS Software** in the navigation tree, and then click **Update Firmware**.

   The **Flash Firmware** controls appear.



4. Click **Browse** (Internet Explorer or Firefox) or **Choose Files** (Chrome).
5. Select a language pack, and then click **Open**.
6. Optional: To save a copy of the language pack file to the iLO Repository, select the **Also store in iLO Repository** check box.
7. Click **Flash**.

   iLO prompts you to confirm the installation request.
8. Click **OK**.

   iLO installs the selected language pack, reboots, and closes your browser connection. It might take several minutes before you can re-establish a connection.

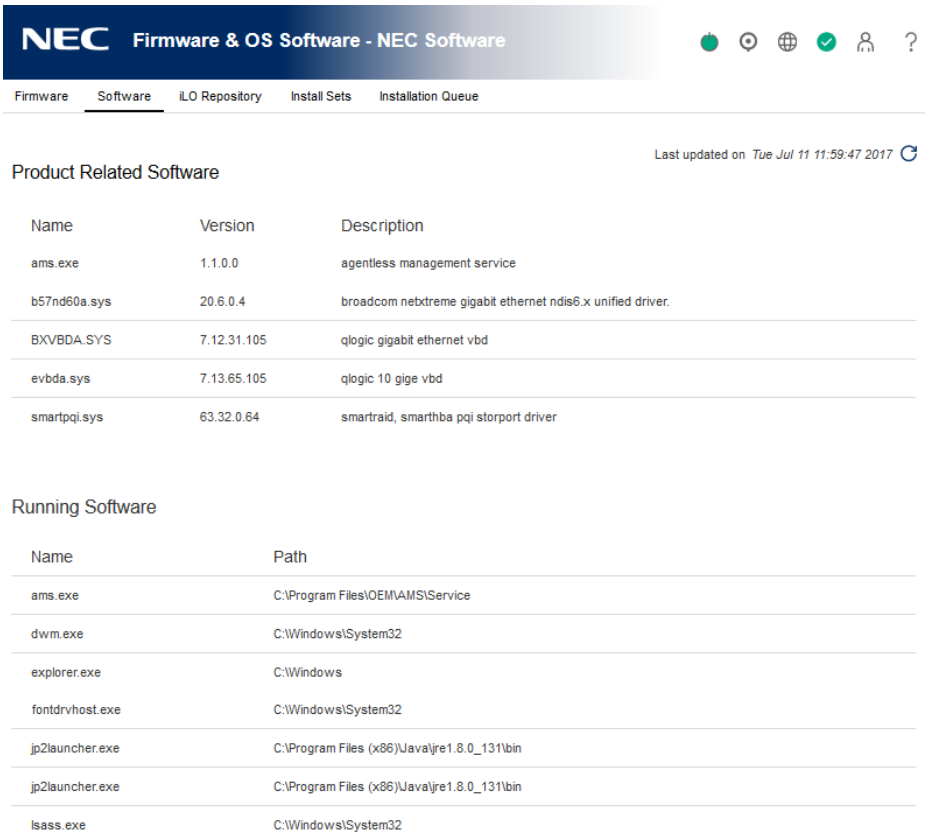
Viewing software information

Prerequisites

To display a complete set of data on this page, AMS must be installed.

Procedure

1. Click **Firmware & OS Software** in the navigation tree, and then click the **Software** tab.



2. Optional: To update the software information data, click ↻.

   The information on this page is cached in the browser, and iLO displays the date and time of the last update. If 5 minutes or more have passed since the page was updated, click ↻ to update the page with the latest information.

Product-related Software details

This section lists all the product-related software on the managed server. The list includes NEC Corporation and NEC-recommended third-party software that was added manually or by using the SPP.

- **Name**—The name of the software.
- **Version**—The software version.

The versions of the displayed firmware components indicate the firmware versions available in the firmware flash components that are saved on the local operating system. The displayed version might not match the firmware running on the server.

- **Description**—A description of the software.

Running Software details

This section lists all the software that is running or available to run on the managed server.

- **Name**—The name of the software.
- **Path**—The file path of the software.

Installed Software details

The **Installed Software** list displays the name of each installed software program.

7.Configuring and using iLO Federation

iLO Federation

iLO Federation enables you to manage multiple servers from one system using the iLO web interface.

When configured for iLO Federation, iLO uses multicast discovery and peer-to-peer communication to enable communication between the systems in an iLO Federation group.

When an iLO Federation page loads, a data request is sent from the iLO system running the web interface to its peers, and from those peers to other peers until all data for the selected iLO Federation group is retrieved.

iLO supports the following features:

- Group health status—View server health and model information.
- Group Virtual Media—Connect scripted media for access by the servers in an iLO Federation group.
- Group power control—Manage the power status of the servers in an iLO Federation group.
- Group power capping—Set dynamic power caps for the servers in an iLO Federation group.
- Group firmware update—Update the firmware of the servers in an iLO Federation group.
- Group license installation—Enter a license key to activate iLO licensed features on the servers in an iLO Federation group.
- Group configuration—Add iLO Federation group memberships for multiple iLO systems.

Any user can view information on iLO Federation pages, but a license is required for using the following features: Group Virtual Media, Group power control, Group power capping, Group configuration, and Group firmware update.

Configuring iLO Federation

Prerequisites for using the iLO Federation features

Procedure

- **The network configuration meets the iLO Federation requirements.**
- **The multicast options are configured for each iLO system that will be added to an iLO Federation group.**

  If you use the default multicast option values, configuration is not required.
- **iLO Federation group memberships are configured.**

  All iLO systems are automatically added to the DEFAULT group.

iLO Federation network requirements

- Servers that will be used with iLO Federation must use the iLO Dedicated Network Port configuration. The iLO Federation features cannot be used with the iLO Shared Network Port configuration.
- Optional: iLO Federation supports both IPv4 and IPv6. If both options have valid configurations, you can configure iLO to use IPv4 instead of IPv6. To configure this setting, clear the iLO Client Applications use IPv6 first check box on the iLO Dedicated Network Port - IPv6 Settings page.
- Configure the network to forward multicast traffic if you want to manage iLO systems in multiple locations.
- Ensure that multicast traffic is enabled if the switches in your network include the option to enable or disable it. This configuration is required for iLO Federation and other NEC Corporation products to discover the iLO systems on the network.
- For iLO systems that are separated by Layer 3 switches, configure the switches to forward SSDP multicast traffic between networks.
- Configure the network to allow multicast traffic (UDP port 1900) and direct HTTP (TCP default port 80) communication between iLO systems.
- For networks with multiple VLANs, configure the switches to allow multicast traffic between the VLANs.
- For networks with Layer 3 switches:
  - For IPv4 networks: Enable PIM on the switch and configure it for PIM Dense Mode.
  - For IPv6 networks: Configure the switch for MLD snooping.

Configuring the multicast options for one iLO system at a time

Use the following procedure to configure the multicast options for each iLO system that will be added to an iLO Federation group. If you use the default values, configuration is not required.

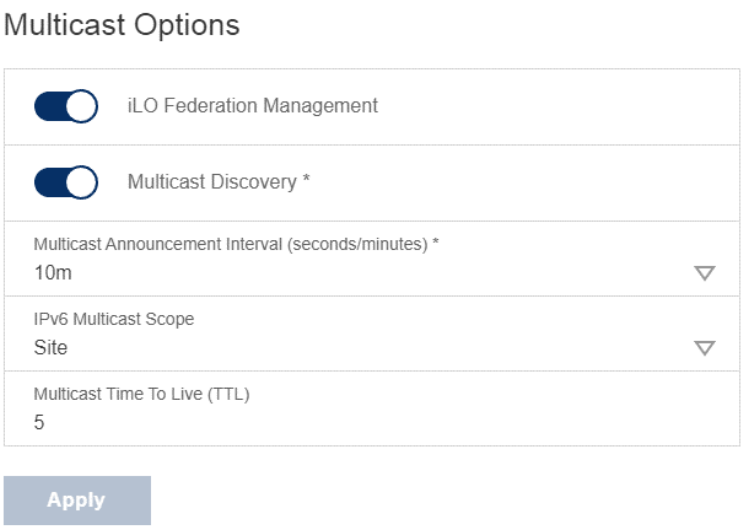
You can use the iLO RESTful API to view and configure multicast options for multiple iLO systems.

Prerequisites

Configure iLO Settings privilege

Procedure

1. Click **iLO Federation** in the navigation tree. The **Setup** tab is displayed.



2. For **iLO Federation Management**, select **Enabled** or **Disabled**.
3. For **Multicast Discovery**, select **Enabled** or **Disabled**.
4. Enter a value for **Multicast Announcement Interval (seconds/minutes)**.
5. Select a value for **IPv6 Multicast Scope**.

   To ensure that multicast discovery works correctly, make sure that all iLO systems in the same group use the same value for **IPv6 Multicast Scope**.
6. Enter a value for **Multicast Time To Live (TTL)**.

   To ensure that multicast discovery works correctly, make sure that all iLO systems in the same group use the same value for **Multicast Time to Live (TTL)**.
7. Click **Apply**.

   Network changes and changes you make on this page take effect after the next multicast announcement.

Multicast options

- **iLO Federation Management**—Enables or disables the iLO Federation features. The default setting is **Enabled**. Selecting **Disabled** disables the iLO Federation features for the local iLO system.
- **Multicast discovery**—Enables or disables multicast discovery. The default setting is **Enabled**. Selecting **Disabled** disables the iLO Federation features for the local iLO system.
- **Multicast Announcement Interval (seconds/minutes)**—Sets the frequency at which the iLO system announces itself on the network. Each multicast announcement is approximately 300 bytes. Select a value of 30 seconds to 30 minutes. The default value is 10 minutes. Selecting **Disabled** disables the iLO Federation features for the local iLO system.
- **IPv6 Multicast Scope**—The size of the network that will send and receive multicast traffic. Valid values are **Link**, **Site**, and **Organization**. The default value is **Site**.
- **Multicast Time To Live (TTL)**—Specifies the number of switches that can be traversed before multicast discovery stops. The default value is 5.

iLO Federation groups

iLO Federation group memberships for local iLO systems

When you configure group memberships for a local iLO system, you specify the privileges that members of a group have for configuring the local managed server.

For example, if you add the local iLO system to **group1** and assign the Virtual Power and Reset privilege, the users of other iLO systems in **group1** can change the power state of the managed server.

If the local iLO system does not grant the Virtual Power and Reset privilege to **group1**, the users of other iLO systems in **group1** cannot use the group power control features to change the power state of the managed server.

If the system maintenance switch is set to disable iLO security on the local iLO system, the users of other iLO systems in **group1** can change the state of the managed server, regardless of the assigned group privileges.

Group memberships for the local iLO system are configured on the **iLO Federation** page **Setup** tab. You can perform the following tasks for a local iLO system:

- View group memberships.
- Add and edit group memberships.
- Remove group memberships.

iLO Federation group memberships for a set of iLO systems

When you add group memberships for multiple iLO systems at one time, you specify the privileges that members of the group have for configuring the other members of the group.

For example, if you configure **group2** based on the **DEFAULT** group, and you assign the Virtual Power and Reset privilege, the users of iLO systems in **group2** can change the power state of all the servers in the group.

You can add group memberships for multiple iLO systems on the **Group Configuration** page. You can perform the following tasks for a group of iLO systems:

- Create a group with the same members as an existing group, but with different privileges.
- Create a group with members that you select by using the iLO Federation filters.

iLO Federation group privileges

When an iLO system added to a group, the group can be granted the following privileges:

- **Login**— Group members can log in to iLO.
- **Remote Console**—Group members can remotely access the managed server Remote Console, including video, keyboard, and mouse control.
- **Virtual Power and Reset**—Group members can power-cycle or reset the host system.

These activities interrupt the system availability.

- **Virtual Media**—Group members can use scripted Virtual Media with the managed server.
- **Host BIOS**—Group members can configure the host BIOS settings by using the UEFI System Utilities.
- **Configure iLO Settings**—Group members can configure most iLO settings, including security settings, and can remotely update firmware.
- **Administer User Accounts**—Group members can add, edit, and delete iLO user accounts.
- **Host NIC**—Group members can configure the host NIC settings.
- **Host Storage**—Group members can configure the host storage settings.
- **Recovery Set**—Group members can manage the recovery install set.

This privilege is not available if you start a session when the system maintenance switch is set to disable iLO security.

iLO Federation group characteristics

- All iLO systems are automatically added to the **DEFAULT** group, which is granted the Login privilege for each group member. You can edit or delete the **DEFAULT** group membership.
- iLO Federation groups can overlap, span racks and data centers, and can be used to create management domains.
- An iLO system can be a member of up to 10 iLO Federation groups.
- There is no limit on the number of iLO systems that can be in a group.
- You must have the Configure iLO Settings privilege to configure group memberships.
- You can use the iLO web interface to configure group memberships for a local iLO system or a group of iLO systems.
- You can use the iLO RESTful API to configure group memberships.
- NEC Corporation recommends installing the same version of the iLO firmware on iLO systems that are in the same iLO Federation group.

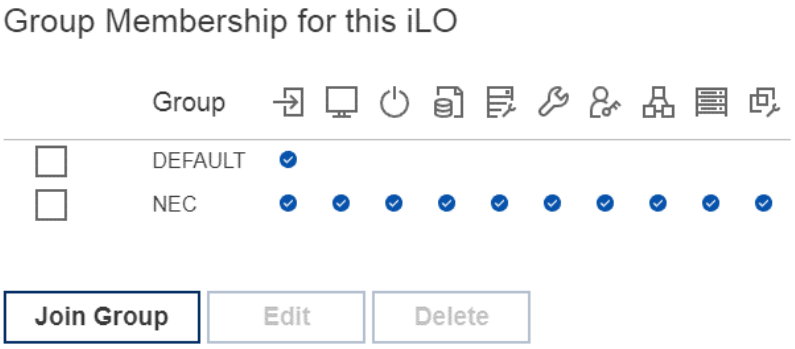
Managing iLO Federation group memberships (local iLO system)

Viewing iLO Federation group memberships (local iLO system)

Procedure

1. Click **iLO Federation** in the navigation tree.

   The **Group Membership for this iLO** table lists the name of each group that includes the local iLO system, and the privileges granted to the group by the local iLO system.



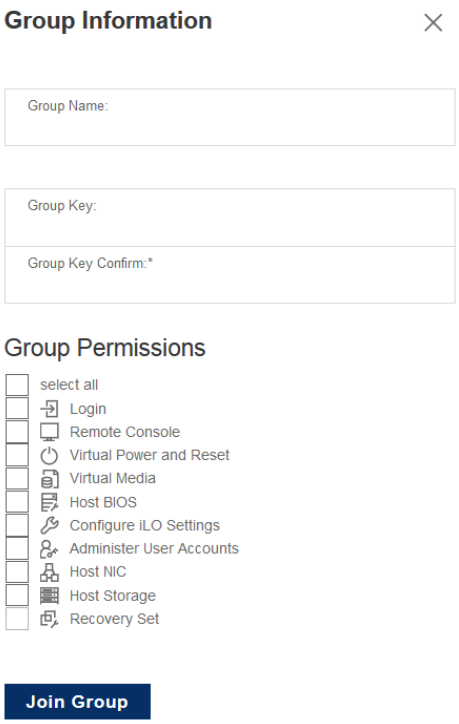
Adding iLO Federation group memberships

Prerequisites

Configure iLO Settings privilege

Procedure

1. Click **iLO Federation** in the navigation tree. The **Setup** tab is displayed.
2. Click **Join Group**.



3. Enter the following information:
   - **Group Name**—The group name, which can be 1 to 31 characters long.
   - **Group Key**—The group password, which can be from the configured minimum password length to 31 characters long.
   - **Group Key Confirm**—Confirm the group password.

   If you enter the name and key for an existing group, the local iLO system is added to that group. If you enter the name and key for a group that does not exist, the group is created and the local iLO system is added to the new group.

4. Select from the following privileges:
   - **Login**
   - **Remote Console**
   - **Virtual Power and Reset**
   - **Virtual Media**
   - **Host BIOS**
   - **Configure iLO Settings**
   - **Administer User Accounts**
   - **Host NIC**
   - **Host Storage**
   - **Recovery Set**

   The privileges granted to the group by the local iLO system control the tasks that users of other iLO systems in the group can perform on the managed server.

5. Click **Join Group**.

Editing iLO Federation group memberships

Prerequisites

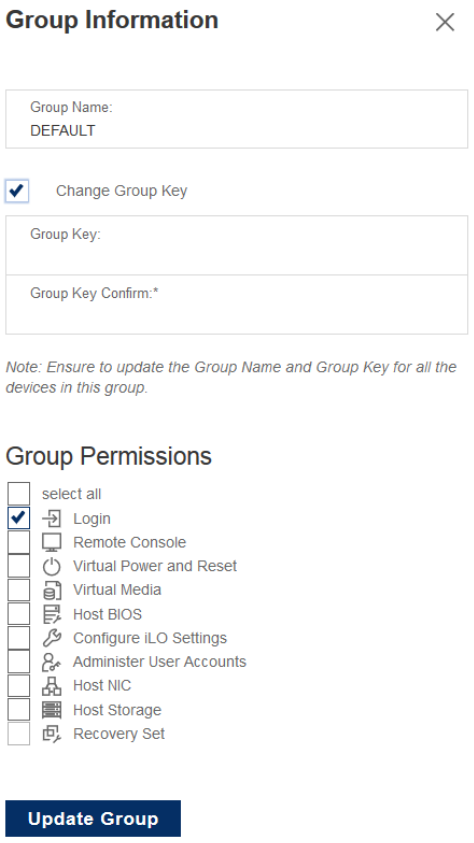
Configure iLO Settings privilege

Procedure

1. Click **iLO Federation** in the navigation tree.

   The **Setup** tab displays the existing group memberships for the local iLO system.

2. Select a group membership, and then click **Edit**.



3. To change the group name, enter a new name in the **Group Name** box.

   The group name can be 1 to 31 characters long.

4. To change the group key, select the **Change Group Key** check box, then enter a new value in the **Group Key** and **Group Key Confirm** boxes.

   The group key can be from the configured minimum password length to 31 characters long.

5. Select or clear the check boxes for the privileges you want to update.

   The privileges granted to the group by the local iLO system control the tasks that users of other iLO systems in the group can perform on the managed server.

6. For more information about the available privileges, see **iLO Federation group privileges** .

7. Click **Update Group**.

8. If you updated the group name or group key, update them on the other systems in the affected group.

Removing a local iLO system from an iLO Federation group

Prerequisites

Configure iLO Settings privilege

Procedure

1. Click **iLO Federation** in the navigation tree.

   The **Setup** tab shows the group membership for the local iLO system.
2. Select the check box next to the group membership that you want to delete.
3. Click **Delete**.
4. When prompted to confirm the request, click **OK**.

Adding iLO Federation group memberships (multiple iLO systems)

Adding an iLO Federation group based on an existing group

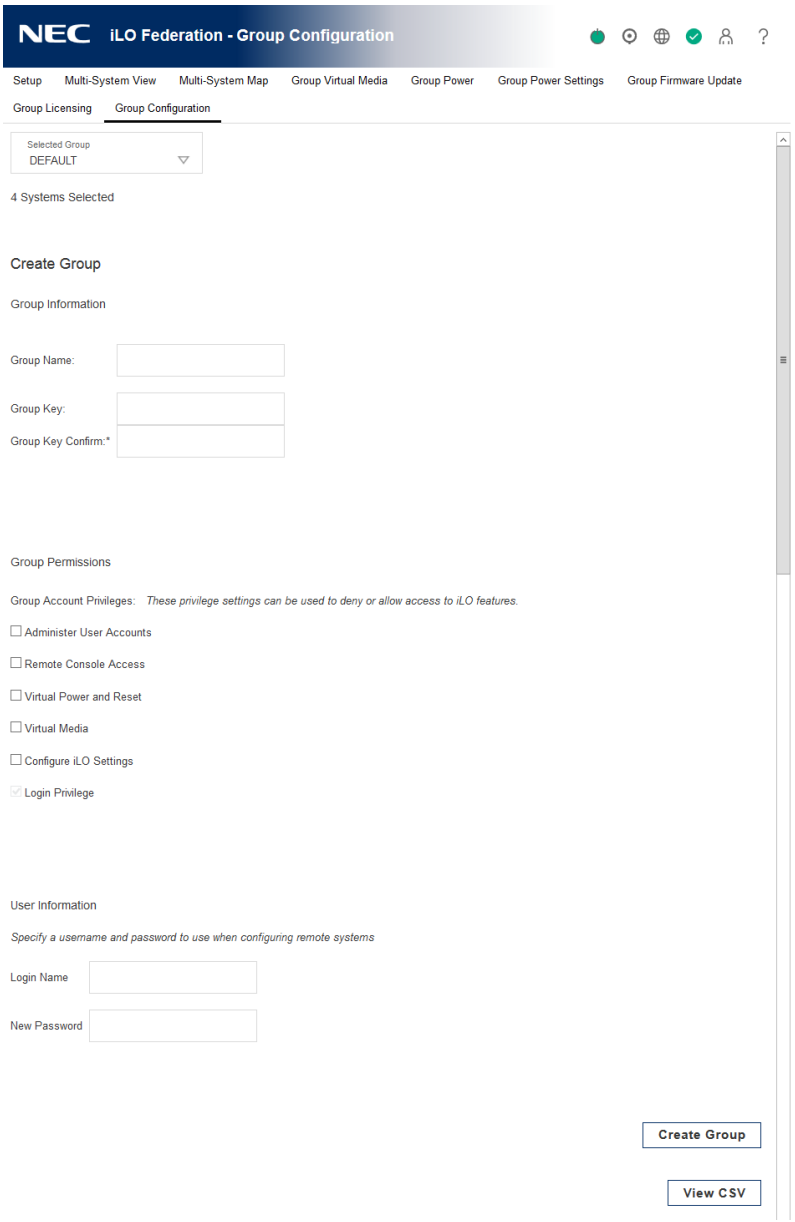
Use this procedure to create an iLO Federation group with the same members as an existing group. For example, you might want to create a group that contains the same systems that are in the DEFAULT group, but with different privileges.

Prerequisites

- Configure iLO Settings privilege
- An iLO license that supports this feature is installed.

Procedure

1. Click **iLO Federation** in the navigation tree, and then click the **Group Configuration** tab.



If no iLO Federation groups exist, this page displays the following message: `There are no configured groups`. Use the **iLO Federation Setup** page to create a group.

2. Select a group from the **Selected Group** menu.

   All of the systems in the selected group will be added to the group you create on this page.

3. Enter the following information:
   - **Group Name**—The group name, which can be 1 to 31 characters long.
   - **Group Key**—The group password, which can be from the configured minimum password length to 31 characters long.
   - **Group Key Confirm**—Confirm the group password.

   If you enter the name of a group that exists, iLO prompts you to enter a unique group name.

4. Select from the following privileges:
   - **Administer User Accounts**
   - **Remote Console Access**
   - **Virtual Power and Reset**
   - **Virtual Media**
   - **Configure iLO Settings**
   - **Login Privilege**

   This step defines the privileges that members of the group have for configuring the other members of the group.

5. Optional: Enter the **Login Name** and **Password** for a user account on the remote systems you want to manage.

   This information is required if the selected group does not have the Configure iLO Settings privilege on the remote systems you want to manage.

   To enter credentials for multiple remote systems, create a user account with the same login name and password on each system.

6. Click **Create Group**.

   The group creation process takes a few minutes. The group will be fully populated within the amount of time configured for the Multicast Announcement Interval.

Creating a group from a filtered set of servers

Use this procedure to create an iLO Federation group from a list of filtered servers. For example, you might want to create a group that contains all servers with a specific version of the iLO firmware.

When you create a group from a list of filtered servers, only the servers listed in the **Affected Systems** list at the time the group is created are added to the group. If you configure servers that meet the filter criteria after the group is created, they are not added to the group.

Prerequisites

- Configure iLO Settings privilege
- An iLO license that supports this feature is installed.

Procedure

1. Create a set of systems by using the filters on the **iLO Federation** pages.
2. Click **iLO Federation** in the navigation tree, and then click the **Group Configuration** tab.

   The filters you apply when you create a set of systems are listed at the top of the page. To remove a filter, click the filter name.

   If no iLO Federation groups exist, this page displays the following message: `There are no configured groups`. Use the **Setup** page to create a group.
3. Select a group from the **Selected Group** menu.

   All of the systems in the selected group that meet the selected filter criteria will be added to the new group.
4. Enter the following information:
   - **Group Name**—The group name, which can be 1 to 31 characters long.
   - **Group Key**—The group password, which can be from the configured minimum password length to 31 characters long.
   - **Group Key Confirm**—Confirm the group password.
5. Select from the following privileges:
   - **Administer User Accounts**
   - **Remote Console Access**
   - **Virtual Power and Reset**
   - **Virtual Media**
   - **Configure iLO Settings**
   - **Login Privilege**

   For more information about the available privileges, see **iLO Federation group privileges**.

   This step defines the privileges that members of the group have for configuring the other members of the group.
6. Optional: Enter the **Login Name** and **Password** for a user account on the remote systems you want to manage.

   This information is required if the selected group does not have the Configure iLO Settings privilege on the remote systems you want to manage.

   To enter credentials for multiple remote systems, create a user account with the same login name and password on each system.
7. To save the configuration, click **Create Group**.

   The group creation process takes a few minutes. The group will be fully populated within the amount of time configured for the **Multicast Announcement Interval**.

Servers affected by a group membership change

The **Affected Systems** section on the **Group Configuration** page provides the following details about the servers affected when you make a group membership change:

- **Server Name**—The server name defined by the host operating system.
- **Server Power**—The server power state (**ON** or **OFF**).
- **UID Indicator**—The state of the UID LED. The UID LED helps you identify and locate a server, especially in high-density rack environments. The possible states are **UID ON**, **UID OFF**, and **UID BLINK**.
- **iLO Hostname**—The fully qualified network name assigned to the iLO subsystem. To open the iLO web interface for the server, click the link in the **iLO Hostname** column.
- **IP Address**—The network IP address of the iLO subsystem. To open the iLO web interface for the server, click the link in the **IP Address** column.

Click **Next** or **Previous** (if available) to view more servers in the list.

More Information

Exporting iLO Federation information to a CSV file

Using the iLO Federation features

Selected Group list

All of the iLO Federation pages except for **Setup** have a **Selected Group** list. When you select a group from the **Selected Group** list:

- The servers affected by a change on the **Group Virtual Media**, **Group Power**, **Group Firmware Update**, **Group Licensing**, and **Group Configuration** pages are listed in the **Affected Systems** table.
- The information displayed on iLO Federation pages applies to all the servers in the selected group.
- The changes you make on iLO Federation pages apply to all the servers in the selected group.
- The selected group is saved in a cookie and remains persistent, even when you log out of iLO.

After you select a group, you can filter the servers in the list to view server information or perform actions on a subset of the servers in the group.

Selected Group list filters

When you filter the list of servers:

- The information displayed on iLO Federation pages applies to all the servers in the selected group that meet the filter criteria.
- The changes you make on iLO Federation pages apply to all the servers in the selected group that meet the filter criteria.
- The filter settings are saved in a cookie and remain persistent, even when you log out of iLO.

Selected Group list filter criteria

You can use the following criteria to filter the servers in a group:

- **Health status**—Click a health status link to select servers with a specific health status.
- **Model**—Click a server model number link to select servers matching the selected model.
- **Server name**—Click a server name to filter by an individual server.
- **Firmware Information**—Click a firmware version or flash status to select servers matching the selected firmware version or status.
- **TPM or TM Option ROM Measuring**—Click an Option ROM Measuring status to include or exclude servers matching the selected Option ROM Measuring status.
- **License usage**—If an error message related to a license key is displayed, click the license key to select servers that use that license key.
- **License type**—Click a license type to select servers with the selected license type installed.
- **License status**—Click a license status to select servers with an installed license matching the selected status.

Exporting iLO Federation information to a CSV file

The following **iLO Federation** pages allow you to export information to a CSV file:

- **Multi-System View**
- **Multi-System Map**
- **Group Virtual Media**
- **Group Power**
- **Group Firmware Update**
- **Group Licensing**
- **Group Configuration**

Procedure

1. Navigate to a page that supports the file export feature.
2. Click **View CSV**.
3. In the **CSV Output** window, click **Save**, and then follow the browser prompts to save or open the file.

   If multiple pages of servers are included in the list, the CSV file will contain only the servers that are currently displayed on the iLO web interface page.

   If a query error occurred, the systems that did not respond to the query are excluded from the iLO web interface page and the CSV file.

iLO Federation information export options

You can export the following information from the **iLO Federation** pages:

Systems with critical or degraded status

Export this list from the **Multi-System View** page.

iLO peers list

Export this list from the **Multi-System Map** page.

Affected systems list

Export the list of systems affected by an iLO Federation action on the following pages:

- **Group Virtual Media**
- **Group Power**
- **Group Firmware Update**
- **Group Licensing**
- **Group Configuration**

The export feature is not supported on the **Group Power Settings** page.

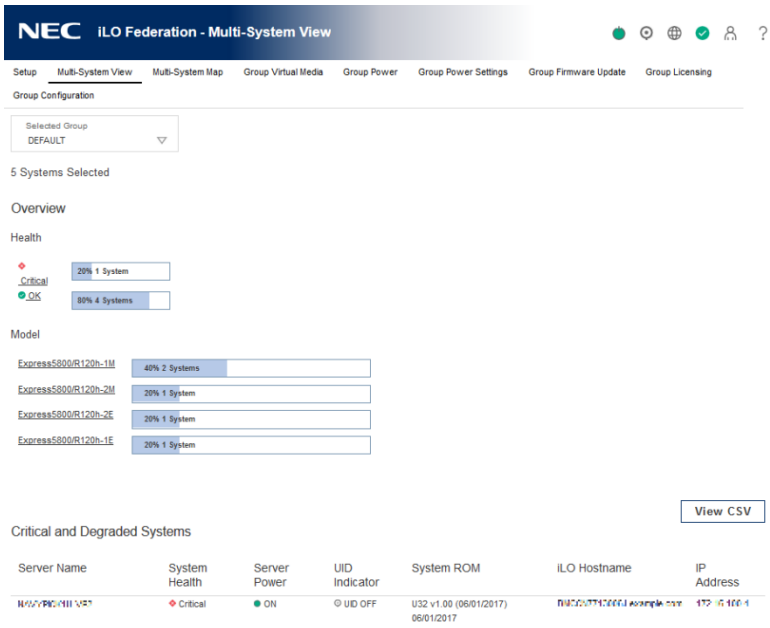
iLO Federation Multi-System view

The **Multi-System View** page provides a summary of the server models, server health, and critical and degraded systems in an iLO Federation group.

Viewing server health and model information

Procedure

1. Click **iLO Federation** in the navigation tree, and then click the **Multi-System View** tab.
2. Select a group from the **Selected Group** menu.
3. Optional: To filter the list of servers, click a health status, server model, or server name link.



Server health and model details

- **Health**—The number of servers in each listed health status. The percentage of the total number of servers in each listed health status is also displayed.
- **Model**—The list of servers, grouped by model number. The percentage of the total number of servers for each model number is also displayed.
- **Critical and Degraded Systems**—The list of servers in the critical or degraded state.

Viewing servers with critical and degraded status

Procedure

1. Click **iLO Federation** in the navigation tree, and then click the **Multi-System View** tab.
2. Select a group from the **Selected Group** menu.
3. Optional: To filter the list of servers, click a health status, server model, or server name link.
4. Click **Next** or **Previous** (if available) to view more servers in the **Critical and Degraded**

Systems list.

More Information

Exporting iLO Federation information to a CSV file

Critical and degraded server status details

- **Server Name**—The server name defined by the host operating system.
- **System Health**—The server health status.
- **Server Power**—The server power status (**ON** or **OFF**).
- **UID Indicator**—The state of the server UID LED. The UID LED helps you identify and locate a server, especially in high-density rack environments. The possible states are **UID ON**, **UID OFF** , and **UID BLINK**.
- **System ROM**—The installed System ROM version.
- **iLO Hostname**—The fully qualified network name assigned to the iLO subsystem. To open the iLO web interface for the server, click the link in the **iLO Hostname** column.
- **IP Address**—The network IP address of the iLO subsystem. To open the iLO web interface for the server, click the link in the **IP Address** column.

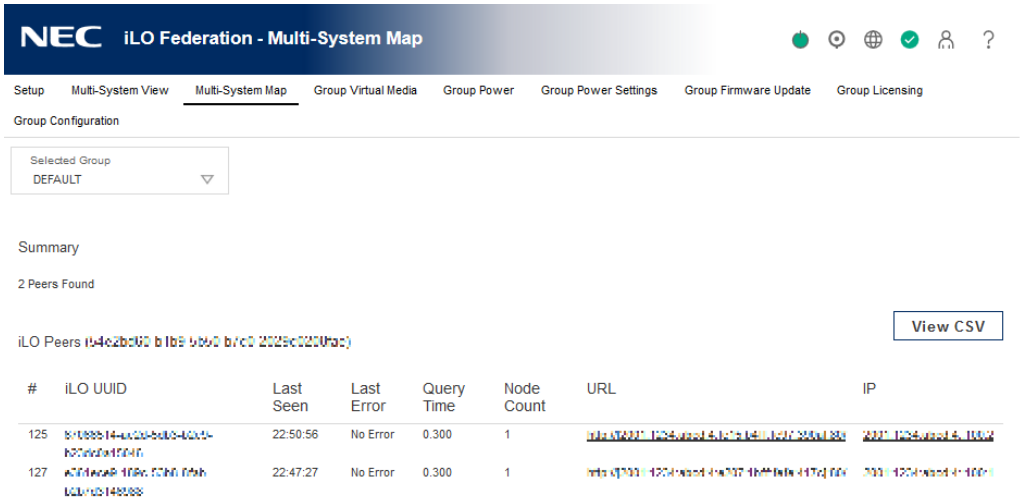
Viewing the iLO Federation Multi-System Map

The **Multi-System Map** page displays information about the peers of the local iLO system. The local iLO system identifies its peers through multicast discovery.

When an iLO Federation page loads, a data request is sent from the iLO system running the web interface to its peers, and from those peers to other peers until all the data for the selected group is retrieved.

Procedure

1. Click **iLO Federation** in the navigation tree, and then click the **Multi-System Map** tab.
2. Select a group from the **Selected Group** menu.



More Information

Exporting iLO Federation information to a CSV file

iLO peer details

- **#**—The peer number.
- **iLO UUID**—The iLO system UPnP UUID.
- **Last Seen**—The time stamp of the last communication from the server.
- **Last Error**—A description of the most recent communication error between the listed peer and the local iLO system.
- **URL**—The URL for starting the iLO web interface for the listed peer.
- **IP**—The peer IP address.

iLO Federation Group Virtual Media

Group Virtual Media enables you to connect scripted media for access by the servers in an iLO Federation group.

- Scripted media only supports 1.44 MB floppy disk images (IMG) and CD/DVD-ROM images (ISO). The image must be on a web server on the same network as the grouped iLO systems.
- Only one of each type of media can be connected to a group at the same time.
- You can view, connect, and eject scripted media, and you can boot from CD/DVD-ROM disk images.

  When you use scripted media, you save a floppy disk or CD/DVD-ROM disk image to a web server and connect to the disk image by using a URL. iLO accepts URLs in HTTP or HTTPS format. iLO does not support FTP.
- Before you use the Virtual Media feature, review the Virtual Media operating system considerations.

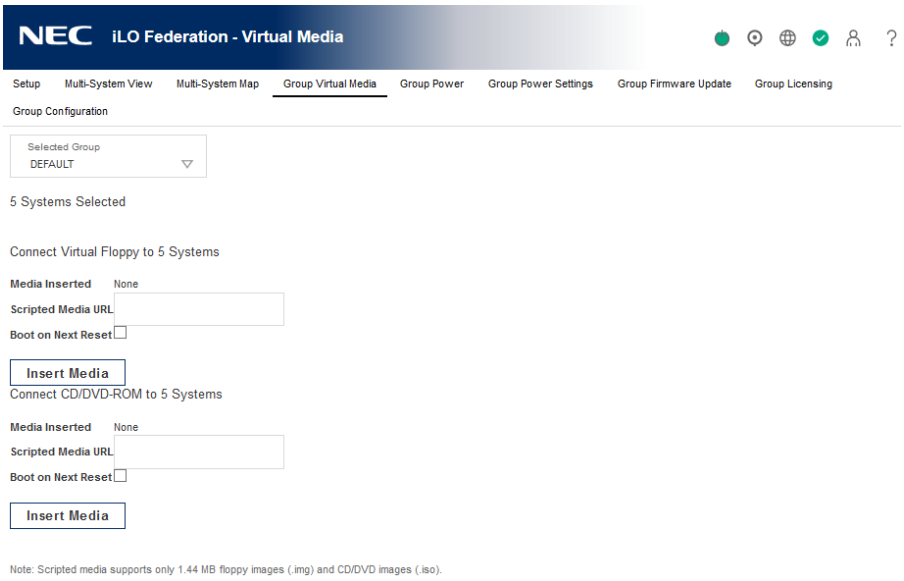
Connecting scripted media for groups

Prerequisites

- An iLO license that supports this feature is installed.
- Each member of the selected iLO Federation group has granted the Virtual Media privilege to the group.

Procedure

1. Click **iLO Federation** in the navigation tree, and then click the **Group Virtual Media** tab.



2. Select a group from the **Selected Group** menu.

   The scripted media you connect will be available to all systems in the selected group.
3. Enter the URL for the scripted media disk image in the **Scripted Media URL** box in the **Connect Virtual Floppy** section (IMG files) or the **Connect CD/DVD-ROM** section (ISO files).
4. Select the **Boot on Next Reset** check box if you want the servers in the group to boot to

this disk image only on the next server reboot.

The image will be ejected automatically on the second server reboot so that the servers do not boot to it twice.

If this check box is not selected, the image remains connected until it is manually ejected, and the servers boot to it on all subsequent server resets, if the system boot options are configured accordingly.

If a server in the group is in POST when you enable the **Boot on Next Reset** check box, an error occurs because you cannot modify the server boot order during POST. Wait for POST to finish, and then try again.

5. Click **Insert Media**.

   iLO displays the command results.

Viewing scripted media status for groups

Procedure

1. Click **iLO Federation** in the navigation tree, and then click the **Group Virtual Media** tab.

Scripted media details

When scripted media is connected to the systems in an iLO Federation group, the following details are listed in the **Virtual Floppy Status** section and **Virtual CD/DVD-ROM Status** section:

- **Media Inserted**—The Virtual Media type that is connected. **Scripted Media** is displayed when scripted media is connected.
- **Connected**—Indicates whether a Virtual Media device is connected.
- **Image URL**—The URL that points to the connected scripted media.

The **Virtual Floppy Status** and **Virtual CD/DVD-ROM Status** sections are displayed only when media is connected.

Ejecting a scripted media device

Prerequisites

- An iLO license that supports this feature is installed.
- Each member of the selected iLO Federation group has granted the Virtual Media privilege to the group.

Procedure

1. Click **iLO Federation** in the navigation tree, and then click the **Group Virtual Media** tab.
2. Select a group from the **Selected Group** menu.
   The scripted media device that you eject will be disconnected from all the systems in the selected group.
3. Click **Eject Media** in the **Virtual Floppy Status** section or the **Virtual CD/DVD-ROM Status** section.

Servers affected by a Group Virtual Media action

The **Affected Systems** section provides the following details about the servers affected when you initiate a Group Virtual Media action:

- **Server Name**—The server name defined by the host operating system.
- **Server Power**—The server power state (**ON** or **OFF**).
- **UID Indicator**—The state of the UID LED. The UID LED helps you identify and locate a server, especially in high-density rack environments. The possible states are **UID ON**, **UID OFF**, and **UID BLINK**.
- **iLO Hostname**—The fully qualified network name assigned to the iLO subsystem. To open the iLO web interface for the server, click the link in the **iLO Hostname** column.
- **IP Address**—The network IP address of the iLO subsystem. To open the iLO web interface for the server, click the link in the **IP Address** column.

Click **Next** or **Previous** (if available) to view more servers in the list.

More Information

Exporting iLO Federation information to a CSV file

iLO Federation Group Power

The Group Power feature enables you to manage the power of multiple servers from a system running the iLO web interface. Use this feature to do the following:

- Power off, reset, or power-cycle a group of servers that are in the ON or Reset state.
- Power on a group of servers that are in the OFF state.
- View the list of servers that will be affected when you click a button in the Virtual Power Button section of the Group Power page.

Changing the power state for a group of servers

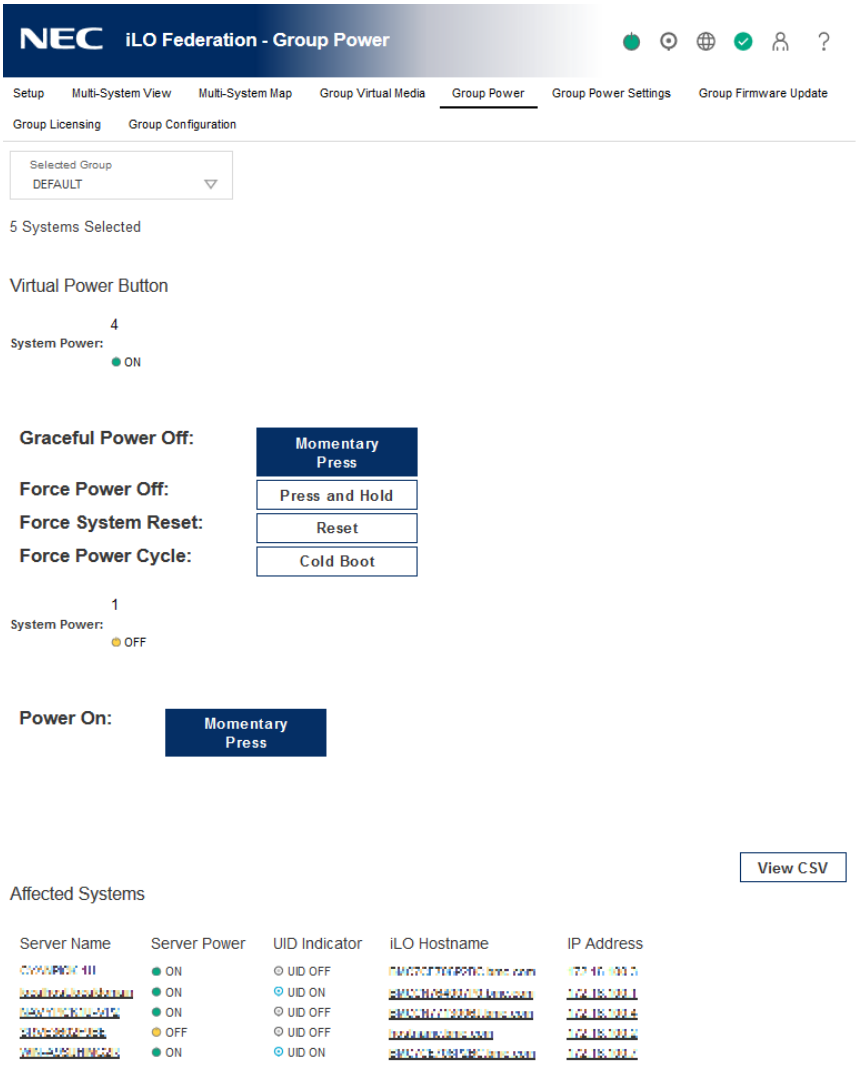
The **Virtual Power Button** section on the **Group Power** page summarizes the current power state of the servers in a group. The summary information includes the total number of servers that are in the **ON**, **OFF**, or **Reset** state. The **System Power** summary indicates the state of the server power when the page is first opened. Use the browser refresh feature to update the **System Power** information.

Prerequisites

- An iLO license that supports this feature is installed.
- Each member of the selected iLO Federation group has granted the Virtual Power and Reset privilege to the group.

Procedure

1. Click **iLO Federation** in the navigation tree, and then click the **Group Power** tab.



2. Select a group from the **Selected Group** menu.

   iLO displays the grouped servers by power state with a counter that shows the total number of servers in each state.

3. To change the power state of a group of servers, do one of the following:
   - For servers that are in the **ON** or **Reset** state, click one of the following buttons:
     - **Momentary Press**
     - **Press and Hold**
     - **Reset**
     - **Cold Boot**
   - For servers that are in the **OFF** state, click the **Momentary Press** button.
     The **Press and Hold**, **Reset**, and **Cold Boot** options are not available for servers that are in the **OFF** state.

4. When prompted to confirm the request, click **OK**.

   iLO displays a progress bar while the grouped servers respond to the Virtual Power Button action. The progress bar indicates the number of servers that successfully processed the command.

The **Command Results** section displays the command status and results, including error messages related to the power state change.

Virtual Power Button options

- **Momentary Press**—The same as pressing the physical power button.
  Some operating systems might be configured to initiate a graceful shutdown after a momentary press, or to ignore this event. NEC Corporation recommends using system commands to complete a graceful operating system shutdown before you attempt to shut down by using the Virtual Power Button.
- **Press and Hold**—The same as pressing the physical power button for 5 seconds and then releasing it.
  The servers in the selected group are powered off as a result of this operation. Using this option might circumvent a graceful operating system shutdown.
  This option provides the ACPI functionality that some operating systems implement. These operating systems behave differently, depending on a short press or long press.
- **Reset**—Forces the servers in the selected group to warm-boot: CPUs and I/O resources are reset. Using this option circumvents a graceful operating system shutdown.
- **Cold Boot**—Immediately removes power from the servers in the selected group. Processors, memory, and I/O resources lose main power. The servers will restart after approximately 6 seconds. Using this option circumvents a graceful operating system shutdown.

Servers affected by the Virtual Power Button

The **Affected Systems** list provides the following details about the servers affected when you initiate a Virtual Power Button action:

- **Server Name**—The server name defined by the host operating system.
- **Server Power**—The server power state (**ON** or **OFF**).
- **UID Indicator**—The state of the UID LED. The UID LED helps you identify and locate a server, especially in high-density rack environments. The possible states are **UID ON**, **UID OFF**, and **UID BLINK**.
- **iLO Hostname**—The fully qualified network name assigned to the iLO subsystem. To open the iLO web interface for the server, click the link in the **iLO Hostname** column.
- **IP Address**—The network IP address of the iLO subsystem. To open the iLO web interface for the server, click the link in the **IP Address** column.

Click **Next** or **Previous** (if available) to view more servers in the list.

More Information

Exporting iLO Federation information to a CSV file

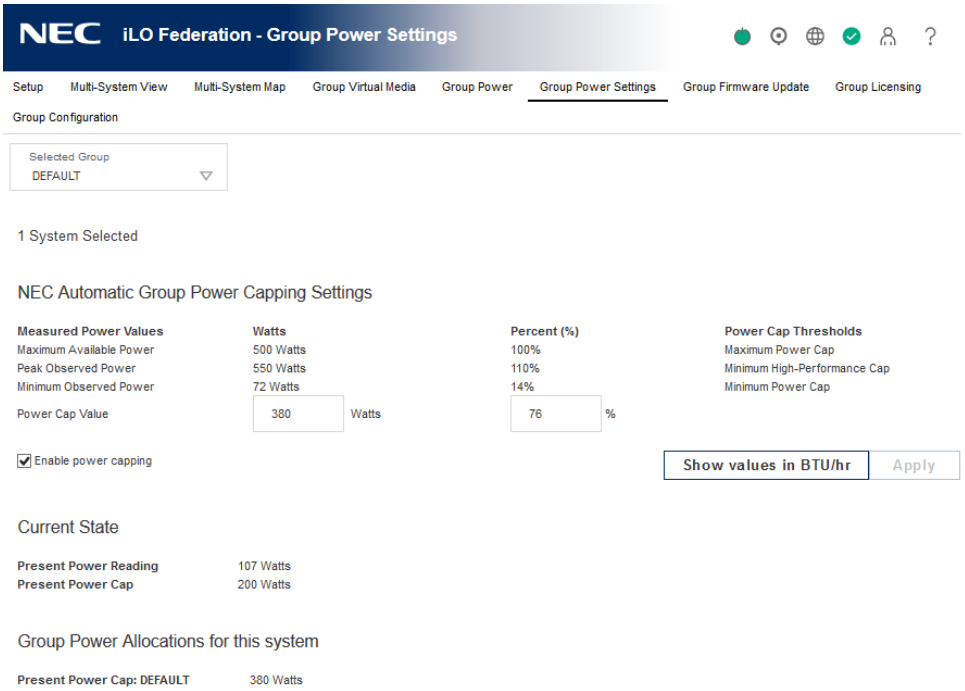
Configuring group power capping

Prerequisites

- An iLO license that supports this feature is installed.
- Each member of the selected iLO Federation group has granted the Configure iLO Settings privilege to the group.

Procedure

1. Click **iLO Federation** in the navigation tree, and then click the **Group Power Settings** tab.



2. Select a group from the **Selected Group** menu.

   Changes you make on this page affect all systems in the selected group.

3. Select the **Enable power capping** check box.
4. Enter the **Power Cap Value** in watts, BTU/hr, or as a percentage.

   The percentage is the difference between the maximum and minimum power values. The power cap value cannot be set lower than the server minimum power value.

5. Optional: When values are displayed in watts, click **Show values in BTU/hr** to change the display to BTU/hr. When values are displayed in BTU/hr, click **Show values in Watts** to change the display to watts.
6. Click **Apply**.

Group power capping considerations

The Group Power Settings feature enables you to set dynamic power caps for multiple servers from a system running the iLO web interface.

- When a group power cap is set, the grouped servers share power to stay below the power

cap. More power is allocated to busy servers and less power is allocated to servers that are idle.

- The power caps that you set for a group operate concurrently with the power caps that you can set on the **Power Settings** page for an individual server.
- If a power cap configured at the enclosure or individual server level or by another iLO Federation group affects a server, other group power caps might allocate less power to that server.
- When a power cap is set, the average power reading of the grouped servers must be at or below the power cap value.
- During POST, the ROM runs two power tests that determine the peak and minimum observed power values.
  Consider the values in the **Automatic Group Power Capping Settings** table when determining your power capping configuration.
  - **Maximum Available Power**—The total power supply capacity for all servers in a group. This value is the **Maximum Power Cap** threshold. The servers in a group must not exceed this value.
  - **Peak Observed Power**—The maximum observed power for all servers in a group. This value is the **Minimum High-Performance Cap** threshold, and it represents the maximum power that the servers in a group use in their current configuration. A power cap set to this value does not affect server performance.
  - **Minimum Observed Power**—The minimum observed power for all servers in a group. This value is the **Minimum Power Cap** threshold, and it represents the minimum power that the servers in a group use. A power cap set to this value reduces the server power usage to the minimum, which results in server performance degradation.
- Power capping is not supported on all servers. For more information, check the server user's guide.

Viewing group power capping information

Prerequisites

An iLO license that supports this feature is installed.

Procedure

1. Click **iLO Federation** in the navigation tree, and then click the **Group Power Settings** tab.
2. Select a group from the **Selected Group** menu.
3. Optional: When values are displayed in watts, click **Show values in BTU/hr** to change the display to BTU/hr. When values are displayed in BTU/hr, click **Show values in Watts** to change the display to watts.

Power capping details

- **Automatic Group Power Capping Settings**—This section shows the following details:
  - **Measured Power Values**—The maximum available power, peak observed power, and minimum observed power.

    - **Power Cap Value**—The power cap value, if one is configured.
- **Current State**—This section includes the following details:
    - **Present Power Reading**—The current power reading for the selected group.
    - **Present Power Cap**—The total amount of power allocated to the selected group. This value is 0 if a power cap is not configured.
- **Group Power Allocations for this system**—The group power caps that affect the local iLO system, and the amount of power allocated to the local iLO system by each group power cap. If a power cap is not configured, the allocated power value is 0.

iLO Federation Group Firmware Update

The Group Firmware Update feature enables you to view firmware information and update the firmware of multiple servers from a system running the iLO web interface. The following firmware types are supported with iLO Federation:

- iLO firmware
- System ROM (BIOS)
- Chassis firmware (Power Management)
- Power Management Controller
- System Programmable Logic Device (CPLD)
- NVMe Backplane Firmware
- Language packs

Updating the firmware for multiple servers

Prerequisites

- Each member of the selected iLO Federation group has granted the Configure iLO Settings privilege to the group.
- An iLO license that supports this feature is installed.

Procedure

1. Download the supported firmware from the NEC Corporation website: **http://www.nec.com/express/.**
2. Save the firmware file to a web server.
3. Click **iLO Federation** in the navigation tree, and then click the **Group Firmware Update** tab.
4. Select a group from the **Selected Group** menu.

   All of the systems in the selected group will be affected when you initiate a firmware update on this page.
5. Optional: To filter the list of affected systems, click a firmware version, flash status, or TPM or TM Option ROM Measuring status link.

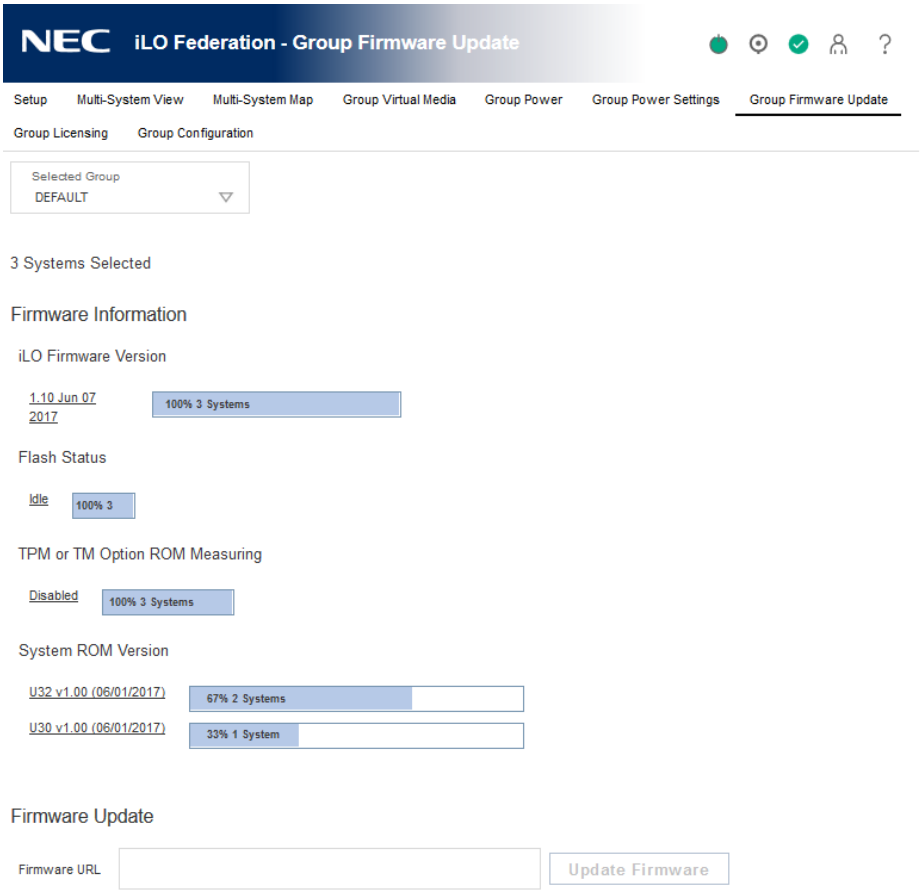
   CAUTION:

   If you attempt to perform a system ROM or iLO firmware update on a server with a TPM or TM installed, iLO prompts you to suspend or back up any software that stores information on the TPM or TM. For example, if you use drive encryption software, suspend it before initiating a firmware update. Failure to follow these instructions might result in losing access to your data.
6. In the **Firmware Update** section, enter the URL to the firmware file on your web server, and then click **Update Firmware**.

   Each selected system downloads the firmware image and attempts to flash it.

The **Flash Status** section is updated and iLO notifies you that the update is in progress. When the update is complete, the **Firmware Information** section is updated.

If a firmware image is not valid for a system or has a bad/missing signature, iLO rejects the image and the **Flash Status** section shows an error for the affected system.



7. Some firmware update types might require a system reset, iLO reset, or a server reboot for the new firmware to take effect.

More Information

Obtaining the iLO firmware image file

Obtaining supported server firmware image files

Viewing group firmware information

Procedure

1. Click **iLO Federation** in the navigation tree, and then click the **Group Firmware Update** tab.
2. Select a group from the **Selected Group** menu.
3. Optional: To filter the list of displayed systems, click a firmware version, flash status, or TPM or TM Option ROM Measuring status link.

Firmware details

The **Firmware Information** section displays the following information:

- The number of servers with each supported iLO firmware version. The percentage of the total number of servers with the listed firmware version is also displayed.
- The flash status for the grouped servers. The percentage of the total number of servers with the listed status is also displayed.
- The TPM or TM Option ROM Measuring status for the grouped servers. The percentage of the total number of servers with the listed status is also displayed.
- The number of servers with each system ROM version. The percentage of the total number of servers with the listed system ROM version is also displayed.

Servers affected by a Group Firmware Update

The **Affected Systems** list provides the following details about the servers affected by a firmware update:

- **Server Name**—The server name defined by the host operating system.
- **System ROM**—The installed System ROM (BIOS).
- **iLO Firmware Version**—The installed iLO firmware version.
- **iLO Hostname**—The fully qualified network name assigned to the iLO subsystem. To open the iLO web interface for the server, click the link in the **iLO Hostname** column.
- **IP Address**—The network IP address of the iLO subsystem. To open the iLO web interface for the server, click the link in the **IP Address** column.

Click **Next** or **Previous** (if available) to view more servers in the list.

More Information

Exporting iLO Federation information to a CSV file

Installing license keys (iLO Federation group)

IMPORTANT:

Do not use this function.

8.iLO Integrated Remote Console

The iLO Integrated Remote Console is a graphical remote console that can be used to control the display, keyboard, and mouse of the host server. The Integrated Remote Console provides access to the remote file system and network drives.

With Integrated Remote Console access, you can observe POST messages as the server starts, and initiate ROM-based setup activities to configure the server hardware. When you install operating systems remotely, the Integrated Remote Console (if licensed) enables you to view and control the host server monitor throughout the installation process.

Integrated Remote Console access options

- **.NET IRC**—Provides access to the system KVM, allowing control of Virtual Power and Virtual Media from a single console through a supported browser on a Windows client. In addition to the standard features, the .NET IRC supports Console Capture, Shared Console, Virtual Folder, and Scripted Media.
- **Java Web Start and Java Applet**—Provide access to the system KVM, allowing control of Virtual Power and Virtual Media. In addition to the standard features, the Java IRC includes the iLO disk image tool and Scripted Media.

Integrated Remote Console usage information and tips

- Users with the Remote Console privilege can use the .NET IRC and the Java IRC.
- A license must be installed to use the Integrated Remote Console after the OS is started. To determine whether a license is installed, click **Administration** in the navigation tree, and then click the **Licensing** tab.
- When you use Windows or Linux with the Oracle Java Runtime Environment, the Java IRC is a Java Web Start application that is launched from the iLO web interface. The application runs in a separate window outside of the web browser. At launch, a blank secondary window opens. Do not close this window after the Java IRC loads.
- When you use Linux with the OpenJDK Java Runtime Environment, the Java IRC is a Java applet that is launched from the iLO web interface. The applet runs in a separate window.
- Java IRC with OpenJDK only: When you refresh or close the iLO web interface window, the Remote Console connection is closed. When the Remote Console connection is closed, you lose access to Virtual Media devices that were connected through the Java IRC, except for devices that were connected by using scripted media.
- Do not run the Integrated Remote Console from the host operating system on the server that contains the iLO processor.
- NEC Corporation recommends that users who log in to a server through the Integrated Remote Console logout before closing the console.
- Pop-up blockers prevent the .NET IRC or Java IRC applet from running, so you must disable them before starting an Integrated Remote Console session. In some cases, you can bypass the pop-up blocker by **Ctrl+clicking** the remote console launch button. This limitation does not apply to the Java IRC Web Start application.
- Some browsers do not support the Java plug-in. The following alternatives are available:

- Windows users: Use the Java IRC Java Web Start application.
- Linux users with Oracle JRE: Use the Java IRC Java Web Start application.
- Linux users with OpenJDK JRE: Use the Java IRC applet.

- The UID LED blinks when an Integrated Remote Console session is active.
- When you finish using the Integrated Remote Console, close the window or click the browser **Close** button (X) to exit.
- The **Idle Connection Timeout** specifies how long a user can be inactive before an Integrated Remote Console session ends automatically. This value does not affect Integrated Remote Console sessions when a virtual media device is connected.
  For more information about the **Idle Connection Timeout**, see **Access Settings**.
- When the mouse is positioned over the Integrated Remote Console window, the console captures all keystrokes, regardless of whether the console window has focus.

.NET IRC requirements

Microsoft .NET Framework

The .NET IRC requires one of the following versions of the .NET Framework:

- .NET Framework 3.5 Full (SP1 recommended)
- .NET Framework 4.0 Full
- .NET Framework 4.5
- .NET Framework 4.6

For Windows 7, 8, 8.1, and 10, a supported version of the .NET Framework is included in the OS.

The .NET Framework is also available at the Microsoft Download Center: **http://www.microsoft.com/download**.

The .NET Framework versions 3.5 and 4.0 have two deployment options: Full and Client Profile. The Client Profile is a subset of the Full framework. The .NET IRC is supported with the Full framework only; the Client Profile is not supported. Versions 4.5 and later of the .NET Framework do not have the Client Profile option.

Microsoft ClickOnce

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

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

- Mozilla Firefox requires an add-on to launch .NET applications. You can launch the .NET IRC from a supported version of Firefox by using a ClickOnce add-on such as the Microsoft .NET Framework Assistant. You can download the .NET Framework Assistant from http://addons.mozilla.org/.
- Previous versions of Google Chrome could run the .NET IRC with an NPAPI plug-in that

supported ClickOnce. Google Chrome 42 and later does not support NPAPI-based plug-ins. As a workaround, use one of the following:

- The .NET IRC with a different browser.
- The Java IRC.

Starting the Integrated Remote Console

Starting the .NET IRC

Prerequisites

- Remote Console privilege
- The Remote Console feature is enabled on the **Access Settings** page.
- An iLO license that supports this feature is installed.
- Your system meets the requirements for using the .NET IRC.

Procedure

1. Click **Remote Console & Media** in the navigation tree.

   The **Launch** tab displays the Remote Console launch options.

2. Click the **Launch** button.

Starting the .NET IRC from the Overview page

Prerequisites

- Remote Console privilege
- The Remote Console feature is enabled on the **Access Settings** page.
- An iLO license that supports this feature is installed.
- Your system meets the requirements for using the .NET IRC.

Procedure

1. Click **Information** in the navigation tree, and then click the **Overview** tab.
2. Click the **.NET** link.

Starting the Java IRC (Oracle JRE)

Use this procedure to start the Java IRC in environments with Windows or Linux and the Oracle JRE.

Prerequisites

- Remote Console privilege
- The Remote Console feature is enabled on the **Access Settings** page.
- An iLO license that supports this feature is installed.
- Your system meets the requirements for using the Java IRC.

Procedure

1. Click **Remote Console & Media** in the navigation tree.

   The **Launch** tab displays the Remote Console launch options.

2. Click the **Web Start** button.
   - Internet Explorer: The browser prompts you to open the Java IRC JNLP file.
   - Firefox: The browser prompts you to save the Java IRC JNLP file.

- Chrome: The browser downloads the Java IRC JNLP file.

3. Open the JNLP file.
   - Internet Explorer: Click the open prompt.
   - Firefox: Save and open the downloaded JNLP file.
   - Chrome: Open the downloaded JNLP file.
4. If you are prompted to confirm that you want to run the application, click **Run**.

   If you do not click **Run**, the Java IRC will not start.
5. If a **Security Warning** dialog box is displayed, click **Continue**.

   If you do not click **Continue**, the Java IRC will not start.

Starting the Java IRC (OpenJDK JRE)

Use this procedure to start the Java IRC in environments with Linux and the OpenJDK JRE.

Prerequisites

- Remote Console privilege
- The Remote Console feature is enabled on the **Access Settings** page.
- An iLO license that supports this feature is installed.
- Your system meets the requirements for using the Java IRC.

Procedure

1. Click **Remote Console & Media** in the navigation tree.

   The **Launch** tab displays the Remote Console launch options.
2. Click the **Applet** button.
3. If a **Security Warning** dialog box or a confirmation dialog box appears, follow the on-screen instructions to continue.

Starting the Java IRC from the Overview page

Prerequisites

- Remote Console privilege
- The Remote Console feature is enabled on the **Access Settings** page.
- An iLO license that supports this feature is installed.
- Your system meets the requirements for using the Java IRC.

Procedure

1. Click **Information** in the navigation tree, and then click the **Overview** tab.
2. Click the **Java Web Start** link.

   Depending on your web browser, you might need to open the downloaded file to start the Java IRC.

Acquiring the Remote Console

If another user is working in the Remote Console, you can acquire it from that user.

Prerequisites

- Remote Console privilege
- The Remote Console feature is enabled on the **Access Settings** page.
- An iLO license that supports this feature is installed.

Procedure

1. Click **Remote Console & Media** in the navigation tree.

   The **Launch** tab displays the Remote Console launch options.

2. Click the button for the Remote Console you want to use.

   iLO notifies you that another user is working in the Remote Console.

3. Click **Acquire**.

   The other user is prompted to approve or deny permission to acquire the Remote Console. If there is no response in 10 seconds, permission is granted.

Using the Remote Console power switch

Use the Remote Console power switch menu to access the iLO Virtual Power Button features.

Prerequisites

- Remote Console privilege
- The Remote Console feature is enabled on the **Access Settings** page.
- An iLO license that supports this feature is installed.

Procedure

1. Click **Remote Console & Media** in the navigation tree.
2. The **Launch** tab displays the Remote Console launch options.
3. Start the .NET IRC or the Java IRC.
4. Select one of the following options from the Remote Console **Power Switch** menu.
   - **Momentary Press**
   - **Press and Hold**
   - **Cold Boot**
   - **Reset**

   The **Press and Hold**, **Reset**, and **Cold Boot** options are not available when the server is powered off.

Virtual Power Button options

- **Momentary Press**—The same as pressing the physical power button. If the server is powered off, a momentary press will turn on the server power.

  Some operating systems might be configured to initiate a graceful shutdown after a momentary press, or to ignore this event. NEC Corporation recommends using system commands to complete a graceful operating system shutdown before you attempt to shut down by using the Virtual Power button.

- **Press and Hold**—The same as pressing the physical power button for 5 seconds and then releasing it.

  The server is powered off as a result of this operation. Using this option might circumvent the graceful shutdown features of the operating system.

  This option provides the ACPI functionality that some operating systems implement. These operating systems behave differently depending on a short press or long press.

- **Reset**—Forces the server to warm-boot: CPUs and I/O resources are reset. Using this option circumvents the graceful shutdown features of the operating system.

- **Cold Boot**—Immediately removes power from the server. Processors, memory, and I/O resources lose main power. The server will restart after approximately 6 seconds. Using this option circumvents the graceful shutdown features of the operating system.

Using iLO Virtual Media from the Remote Console

For instructions on using the Virtual Media feature from the Remote Console, see **Remote Console Virtual Media**.

Shared Remote Console (.NET IRC only)

Shared Remote Console allows the connection of multiple sessions on the same server. This feature can be used for activities such as training and troubleshooting.

The first user to initiate a Remote Console session connects to the server normally and is designated as the session leader. Any subsequent user who requests Remote Console access initiates an access request for a satellite client connection. A dialog box for each access request opens on the session leader desktop, identifying the requester user name and DNS name (if available) or IP address. The session leader can grant or deny access. If there is no response, permission is denied.

Shared Remote Console does not support passing the session leader designation to another user, or reconnecting a user after a failure. To allow user access after a failure, restart the Remote Console session.

During a Shared Remote Console session, the session leader has access to all Remote Console features, whereas all other users can access only the keyboard and mouse. Satellite clients cannot control Virtual Power or Virtual Media.

iLO encrypts Shared Remote Console sessions by authenticating the client first, and then the session leader determines whether to allow new connections.

Joining a Shared Remote Console session

Prerequisites

- Remote Console privilege
- The Remote Console feature is enabled on the **Access Settings** page.
- An iLO license that supports this feature is installed.

Procedure

1. Click **Remote Console & Media** in the navigation tree.

   The **Launch** tab displays the Remote Console launch options.

2. Click **Launch** in the **.NET Integrated Remote Console (.NET IRC)** section.

   A message notifies you that the .NET IRC is already in use.

3. Click **Share**.

   The session leader receives your request to join the .NET IRC session.

   If the session leader clicks **Yes**, you are granted access to the .NET IRC session with access to the keyboard and mouse.

Console Capture (.NET IRC only)

Console Capture allows you to record and play back video streams of events such as startup, and sensed operating system faults. iLO automatically captures the Server Startup and Server Prefailure sequences. You can manually start and stop the recording of console video.

- Console Capture is supported with the .NET IRC; it is not supported with the Java IRC.
- Console Capture is available only through the .NET IRC. It cannot be accessed through the CLP.
- The Server Startup and Server Prefailure sequences are not captured automatically during firmware updates or while the Remote Console is in use.
- Server Startup and Server Prefailure sequences are saved automatically in iLO memory. They will be lost during firmware updates, iLO reset, and power loss. You can save the captured video to your local drive by using the .NET IRC.
- The Server Startup file starts capturing when server startup is detected, and stops when it runs out of space. This file is overwritten each time the server starts.
- The Console Capture control buttons are on the bottom of the .NET IRC session window. The following controls are available:
  - **Skip to Start**—Restarts playback from the beginning of the file.
  - **Pause**—Pauses the playback.
  - **Play**—Starts playback if the currently selected file is not playing or is paused.
  - **Record**—Records your .NET IRC session.
  - **Progress Bar**—Shows the progress of the video session.

  Move the cursor over the controls to identify each button.

Viewing Server Startup and Server Prefailure sequences

Prerequisites

- Remote Console privilege
- The Remote Console feature is enabled on the **Access Settings** page.
- An iLO license that supports this feature is installed.

Procedure

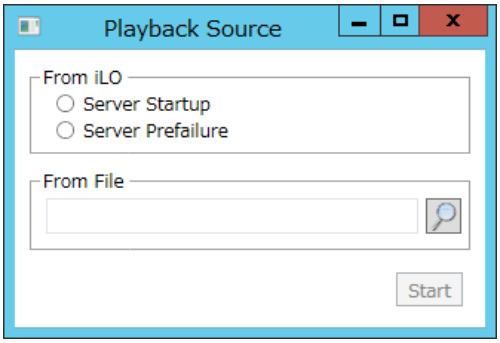
1. Click **Remote Console & Media** in the navigation tree.

   The **Launch** tab displays the Remote Console launch options.

2. Start the .NET IRC.

3. Press the **Play** button.

   The **Playback Source** dialog box opens.



4. Select **Server Startup** or **Server Prefailure**.
5. Click **Start**.

Saving Server Startup and Server Prefailure video files

Prerequisites

- Remote Console privilege
- The Remote Console feature is enabled on the **Access Settings** page.
- An iLO license that supports this feature is installed.

Procedure

1. Click **Remote Console & Media** in the navigation tree.

   The **Launch** tab displays the Remote Console launch options.
2. Start the .NET IRC.
3. Press the **Play** button.

   The **Play** button has a green triangle icon, and it is located in the toolbar at the bottom of the Remote Console window.
4. Select **Server Startup** or **Server Prefailure**.
5. Click **Start**.
6. Press the **Play** button again to stop playback.

Capturing video files

Use this procedure to capture video files of sequences other than Server Startup and Server Prefailure.

Prerequisites

- Remote Console privilege
- The Remote Console feature is enabled on the **Access Settings** page.
- An iLO license that supports this feature is installed.

Procedure

1. Click **Remote Console & Media** in the navigation tree.

The **Launch** tab displays the Remote Console launch options.

2. Start the .NET IRC.
3. Click the **Record** button.

   The **Save Video** dialog box opens.
4. Enter a file name and save location, and then click **Save**.
5. When you are finished recording, press the **Record** button again to stop recording.

Viewing saved video files

Prerequisites

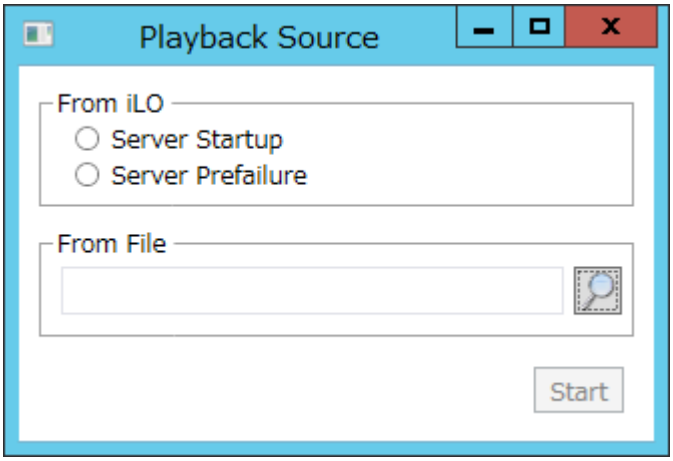
- Remote Console privilege
- The Remote Console feature is enabled on the **Access Settings** page.
- An iLO license that supports this feature is installed.

Procedure

1. Click **Remote Console & Media** in the navigation tree.

   The **Launch** tab displays the Remote Console launch options.
2. Start the .NET IRC.
3. Press the **Play** button.

   The **Playback Source** dialog box opens.



4. Click the magnifying glass icon next to the **From File** box.
5. Navigate to a video file, and then click **Open**.

   Video files captured in the Remote Console use the iLO file type.
6. Click **Start**.

Remote Console hot keys

The **Program Remote Console Hot Keys** page allows you to define up to six hot keys to use during Remote Console sessions. Each hot key represents a combination of up to five keys that are sent to the host server when the hot key is pressed. Hot keys are active during Remote Console sessions that use the .NET IRC, Java IRC, and the text-based Remote Console.

If a hot key is not set—for example, **Ctrl+V** is set to **NONE**, **NONE**, **NONE**, **NONE**, **NONE**—this hot key is disabled. The server operating system will interpret **Ctrl+V** as it usually does (paste, in this example). If you set **Ctrl+V** to use another combination of keys, the server operating system will use the key combination set in iLO (losing the paste functionality).

Example 1: If you want to send **Alt+F4** to the remote server, but pressing that key combination closes your browser, you can configure the hot key **Ctrl+X** to send the **Alt+F4** key combination to the remote server. After you configure the hot key, press **Ctrl+X** in the Remote Console window when you want to send **Alt+F4** to the remote server.

Example 2: If you want to create a hot key to send the international **AltGR** key to the remote server, use **R_ALT** in the key list.

Creating hot keys

Prerequisites

Configure iLO Settings privilege

Procedure

1. Click **Remote Console & Media** in the navigation tree, and then click the **Hot Keys** tab.
2. For each hot key that you want to create, select the key combination to send to the remote server.

   To configure hot keys to generate key sequences from international keyboards, select the key on a U.S. keyboard that is in the same position as the desired key on the international keyboard. **Keys for configuring Remote Console computer lock keys and hot keys** lists the keys you can use when you configure hot keys.
3. Click **Save Hot Keys**.

   iLO confirms that the hot key settings were updated successfully.

Keys for configuring Remote Console computer lock keys and hot keys

The following keys are supported when you configure Remote Console hot keys and Remote Console computer lock keys.

Table 1: Keys for configuring hot keys

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

Resetting hot keys

Resetting the hot keys clears all current hot key assignments.

Prerequisites

Configure iLO Settings privilege

Procedure

1. Click **Remote Console & Media** in the navigation tree, and then click the **Hot Keys** tab.
2. Click **Reset Hot Keys**.

iLO prompts you to confirm the request.

3. Click **OK**.

   iLO notifies you that the hot keys were reset.

Viewing configured remote console hot keys (Java IRC only)

Prerequisites

- Remote Console privilege
- The Remote Console feature is enabled on the **Access Settings** page.
- An iLO license that supports this feature is installed.

Procedure

1. Click **Remote Console & Media** in the navigation tree.

   The **Launch** tab displays the Remote Console launch options.

2. Start the Java IRC.
3. Select **Keyboard** > **View Hot Keys**.

Configuring Remote Console Computer Lock settings

This feature locks the OS or logs a user out 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.

Prerequisites

Configure iLO Settings privilege

Procedure

1. Click **Remote Console & Media** in the navigation tree, and then click the **Security** tab.
2. Select from the following **Remote Console Computer Lock** settings: **Windows**, **Custom**, and **Disabled.**
3. Select a computer lock key sequence.
4. To save the changes, click **Apply**.

Remote Console Computer Lock options

- **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. When a Remote Console session ends or the iLO network link is lost, the operating system on the managed server is not locked.

More Information

Keys for configuring Remote Console computer lock keys and hot keys

Configuring the Integrated Remote Console Trust setting (.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 must be from a trusted source. If a browser is not configured to trust an iLO processor, and this setting is enabled, ClickOnce notifies you that the application cannot start.

NEC Corporation recommends installing a trusted SSL certificate and enabling the **IRC requires a trusted certificate in iLO** setting. In this configuration, the .NET IRC is launched by using an HTTPS connection. If the **IRC requires a trusted certificate in iLO** setting is disabled, the .NET IRC is launched by using a non-SSL connection, and SSL is used after the .NET IRC starts to exchange encryption keys.

Prerequisites

Configure iLO Settings privilege

Procedure

1. Click **Remote Console & Media** in the navigation tree, and then click the **Security** tab.
2. To enable or disable the **IRC requires a trusted certificate in iLO** setting, click the toggle switch.
3. To save the changes, click **Apply**.

9.Using a text-based Remote Console

iLO supports a true text-based Remote Console. Video information is obtained from the server, and the contents of the video memory are sent to the iLO management processor, compressed, encrypted, and forwarded to the management client application. iLO uses a screen-frame buffer that sends the characters (including screen positioning information) to text-based client applications. This method ensures compatibility with standard text-based clients, good performance, and simplicity. However, you cannot display non-ASCII or graphical information, and screen positioning information (displayed characters) might be sent out of order.

iLO uses the video adapter DVO port to access video memory directly. This method increases iLO performance significantly. However, the digital video stream does not contain useful text data, and text- based client applications such as SSH cannot render this data.

Using the iLO Virtual Serial Port

You can access a text-based console from iLO using a standard license and the iLO Virtual Serial Port.

The iLO Virtual Serial Port provides a bidirectional data flow with a server serial port. Using the remote console, you can operate as if a physical serial connection exists on the remote server serial port.

The iLO Virtual Serial Port is displayed as a text-based console, but the information is rendered through graphical video data. iLO displays this information through an SSH client when the server is in a pre- operating-system state, enabling an unlicensed iLO system to observe and interact with the server during POST.

By using the iLO Virtual Serial Port, the remote user can perform operations such as the following:

- Interact with the server POST sequence and the operating system boot sequence.
  To start the UEFI System Utilities during a Virtual Serial Port session, enter the key combination **ESC**+ **shift 9** or **Esc** + **(.**
- Establish a login session with the operating system, interact with the operating system; and execute and interact with applications on the operating system.
- For an iLO system running Linux in a graphical format, you can configure getty()on the server serial port, and then use the iLO Virtual Serial Port to view a login session to the Linux OS.
- Use the EMS Console through the iLO Virtual Serial Port. EMS is useful for debugging Windows boot issues and kernel-level issues.

More Information

Configuring Windows for use with the iLO Virtual Serial Port
Configuring Linux to use the iLO Virtual Serial Port
Windows EMS Console with iLO Virtual Serial Port

Configuring the iLO Virtual Serial Port in the UEFI System Utilities

The following procedure describes the settings you must configure before you can use the iLO Virtual Serial Port. This procedure is required for both Windows and Linux systems.

Procedure

1. Access the UEFI System Utilities.
   a. Optional: If you access the server remotely, start an iLO remote console session.
   b. Restart or power on the server.
   c. Press **F9** in the server POST screen.
      The UEFI System Utilities start.
2. Set the Virtual Serial Port COM port.
   a. Click **System Configuration**, then click **BIOS/Platform Configuration (RBSU)**.
   b. Click **System Options**, then click **Serial Port Options**.
   c. In the **Virtual Serial Port** menu, select the COM port you want to use.
3. Set the BIOS serial console and EMS properties.
   a. At the top of the **Serial Port Options** page, click **BIOS Serial Console and EMS**.
   b. In the **BIOS Serial Console Port** menu, select the COM port you want to use.
   c. In the **BIOS Serial Console Baud Rate** menu, select **115200**.

   NOTE: The iLO Virtual Serial Port does not use a physical UART, so the **BIOS Serial Console Baud Rate** value has no effect on the speed the iLO Virtual Serial Port uses to send and receive data.

   d. For Windows users only: In the **EMS Console** menu, select the COM port that matches the selected **Virtual Serial Port** COM port.
5. To save the changes and exit, press **F12**.
6. When prompted to confirm the request, click **Yes - Save Changes**.
7. The UEFI System Utilities notify you that a system reboot is required.
8. Click **Reboot**.

Configuring Linux to use the iLO Virtual Serial Port

You can manage Linux servers remotely using console redirection. To configure Linux to use console redirection, you must configure the Linux boot loader (GRUB). The boot-loader application loads from the bootable device when the server system ROM finishes POST. Define the serial interface as the default interface so that if no input arrives from the local keyboard within 10 seconds (the default timeout value), the system will redirect output to the serial interface (iLO Virtual Serial Port).

Configuring Linux 6 to use the iLO Virtual Serial Port

Procedure

1. Configure GRUB based on the following configuration examples.

   NOTE:

   In the following configuration examples, ttyS0 and unit 0 are for com1 and ttyS1 and unit 1 are for com2.

   The following configuration example uses Red Hat Enterprise Linux 6 and com1:

   ```
   serial -unit=0 -speed=115200 terminal -timeout=10 serial console
   default=0

   timeout=10

   #splashimage=(hd0,2)/grub/splash.xpm.gz title Red Hat Linux (2. 6.18-
   164.e15) root (hd0,2)

   9

   kernel /vmlinux-2.6.18-164.e15 ro root=/dev/sda9 console=tty0

   console=ttyS0,115200

   initrd /initrd-2.6.18-164.e15.img
   ```

   If com2 was selected, the configuration example would be as follows:

   ```
   serial -unit=1 -speed=115200 terminal -timeout=10 serial console
   default=0

   timeout=10

   #splashimage=(hd0,2)/grub/splash.xpm.gz title Red Hat Linux (2. 6.18-
   164.e15) root (hd0,2)

   9

   kernel /vmlinux-2.6.18-164.e15 ro root=/dev/sda9 console=tty0
   console=ttyS1,115200

   initrd /initrd-2.6.18-164.e15.img
   ```

   After Linux is fully booted, a login console can be redirected to the serial port.

   If configured, the `/dev/ttyS0` and `/dev/ttyS1` devices enable you to obtain serial TTY sessions through the iLO Virtual Serial Port.

2. To begin a shell session on a configured serial port, add the following line to the `/etc/inittab` file to start the login process automatically during system boot:

   The following example initiates the login console on `/dev/ttyS0`:
   `S0:2345:respawn:/sbin/agetty 115200 ttyS0 vt100` The following example initiates the login console on `dev/ttys1`:

   ```
   S1:2345:respawn:/sbin/agetty 115200 ttyS1 vt100
   ```

3. Use SSH to connect to iLO, and then use the iLO CLP command `start /system1/oemNEC_vsp1` to view a login session to the Linux operating system.

Configuring Red Hat Enterprise Linux 7 to use the iLO Virtual Serial Port

Procedure

1. Open `/etc/sysconfig/grub` with a text editor. This configuration example uses `ttys0`.
   - At the end of the line `GRUB_CMD_LINELINUX`, enter **`console=ttys0`**.
   - Remove `rhgb quiet`.
   - Enter the following parameters:

     ```
     GRUB_TIMEOUT=5

     GRUB_DEFAULT=saved GRUB_DISABLE_SUBMENU=true
     GRUB_TERMINAL_OUTPUT="console"

     GRUB_CMDLINE_LINUX="crashkernel=auto rd.lvm.lv=rhel/root
     rd.lvm.lv=rhel/ swap console=ttyS0,115200n8"

     GRUB_DISABLE_RECOVERY="true"
     ```

2. Enter the following command to create the `grub.cfg` file:

   ```
   grub2-mkconfig -o /boot/efi/EFI/redhat/grub.cfg
   ```

3. Enable a `getty` login service for the serial port.

   For example:

   ```
   systemctl enable serial-getty@ttyS0.service
   ```

4. Configure `getty` to listen on the serial port.

   For example:

   ```
   systemctl start getty@ttyS0.service
   ```

5. To begin a shell session on a configured serial port, add the following line to the `/etc/inittab` file to start the login process automatically during system boot:

   The following example initiates the login console on `/dev/ttyS0`:
   `S0:2345:respawn:/sbin/agetty 115200 ttyS0 vt100`

6. Use SSH to connect to iLO, and then use the iLO CLP command `start /system1/oemNEC_vsp1` to view a login session to the Linux operating system.

Windows EMS Console with iLO Virtual Serial Port

iLO enables you to use the Windows EMS Console over the network through a web browser. EMS enables you to perform emergency management services when video, device drivers, or other OS features prevent normal operation and normal corrective actions from being performed.

When using the Windows EMS Console with iLO:

- The Windows EMS console must be configured in the OS before you can use the iLO Virtual Serial Port. For information about how to enable the EMS console, see your OS documentation. If the EMS console is not enabled in the OS, iLO displays an error message when you try to access the iLO Virtual Serial Port.
- The Windows EMS serial port must be enabled through the UEFI System Utilities. The configuration options allow you to enable or disable the EMS port, and select the COM port. iLO automatically detects whether the EMS port is enabled or disabled, and detects the selection of the COM port.
- You can use the Windows EMS Console and the iLO Remote Console at the same time.
- To display the SAC>prompt, you might have to press **Enter** after connecting through the iLO Virtual Serial Port.

More Information

Configuring the iLO Virtual Serial Port in the UEFI System Utilities

Configuring Windows for use with the iLO Virtual Serial Port

Enter **`bcdedit /?`** for syntax help when you complete these steps.

Procedure

1. Open a command window.
2. To edit the boot configuration data, enter the following command:

   ```
   bcdedit /ems on
   ```

3. Enter the following command to configure the EMSPORT and EMSBAUDRATE values:

   ```
   bcdedit /emssettings EMSPORT:1 EMSBAUDRATE:115200
   ```

   NOTE:

   EMSPORT:1 is COM1, and EMSPORT:2 is COM2.

4. To enable or disable emergency management services for a boot application, enter the following command:

   ```
   bcdedit /bootems on
   ```

5. Reboot the operating system.

More Information

Configuring the iLO Virtual Serial Port in the UEFI System Utilities

Starting an iLO Virtual Serial Port session

Prerequisites

- The iLO Virtual Serial Port settings are configured in the UEFI System Utilities.
- The Windows or Linux operating system is configured for use with the iLO Virtual Serial Port.

Procedure

1. Start an SSH session.

   For example, you could enter **`ssh Administrator@<iLO IP address>`** or connect through port 22 with `putty.exe`.

2. When prompted, enter your iLO account credentials.
3. At the `</>iLO->` prompt, enter **`VSP`**, and press **Enter**.
4. For Windows systems only: At the `<SAC>` prompt, enter **`cmd`** to create a command prompt channel.
5. For Windows systems only: to switch to the channel specified by the channel numberEnter **`ch - si`**

   `<#>`**`.`**

6. When prompted, enter the OS login credentials.

More Information

Configuring the iLO Virtual Serial Port in the UEFI System Utilities
Configuring Windows for use with the iLO Virtual Serial Port
Windows EMS Console with iLO Virtual Serial Port

Viewing the iLO Virtual Serial Port log

If the iLO Virtual Serial Port log is enabled, you can view iLO Virtual Serial Port activity by using the `vsp log` command.

Virtual Serial Port activity is logged to 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.

Prerequisites

An iLO license that supports this feature is installed.

Procedure

1. Enable Secure Shell (SSH) and Virtual Serial Port Log on the Security - Access Settings page.
2. Connect to the CLI through SSH.
3. Use the `vsp` command to view iLO Virtual Serial Port activity.
4. Enter `ESC (` to exit.
5. To view the iLO Virtual Serial Port log, enter `vsp log`.

More Information

Configuring iLO access options

10. Using iLO Virtual Media

iLO Virtual Media

iLO Virtual Media provides a virtual device that can be used to boot a remote host server from standard media anywhere on the network. Virtual Media devices are available when the host system is booting. Virtual Media devices connect to the host server by using USB technology.

When you use Virtual Media, note the following:

- An iLO license key is required to use some forms of Virtual Media.
- You must have the Virtual Media privilege to use this feature.
- Only one of each type of virtual media can be connected at a time.
- The Virtual Media feature supports ISO images of up to 8 TB. The maximum ISO image file size also depends on factors such as the single file size limit for the file system where the ISO image is stored and the SCSI commands the server OS supports.
- In an operating system, an iLO Virtual Floppy/USB key or Virtual CD/DVD-ROM behaves like any other drive. When you use iLO for the first time, the host operating system might prompt you to complete a New Hardware Found wizard.
- When virtual devices are connected, they are available to the host server until you disconnect them. When you are finished using a Virtual Media device and you disconnect it, you might receive an "unsafe device removal" warning message from the host OS. You can avoid this warning by using the operating system feature to stop the device before disconnecting it.
- The iLO Virtual CD/DVD-ROM is available at server boot time for supported operating systems. Booting from a Virtual CD/DVD-ROM enables you to perform tasks such as deploying an operating system from network drives and performing disaster recovery of failed operating systems.
- If the host server OS supports USB mass storage devices or secure digital devices, the iLO Virtual Floppy/USB key is available after the host server OS loads.
    - You can use the Virtual Floppy/USB key when the host server OS is running to upgrade drivers, create an emergency repair disk, and perform other tasks.
    - Having the Virtual Floppy/USB key available when the server is running can be useful if you must diagnose and repair the NIC driver.
    - The Virtual Floppy/USB key can be the physical floppy disk, USB key, or secure digital drive on which the web browser is running, or an image file stored on a local hard drive or network drive.
    - For optimal performance, NEC Corporation recommends using image files stored on the hard drive of your client PC or on a network drive accessible through a high-speed network link.
- If the host server operating system supports USB mass storage devices, the iLO Virtual CD/DVD- ROM is available after the host server operating system loads.
    - You can use the Virtual CD/DVD-ROM when the host server operating system is running to upgrade device drivers, install software, and perform other tasks.

- Having the Virtual CD/DVD-ROM available when the server is running can be useful if you must diagnose and repair the NIC driver.
- The Virtual CD/DVD-ROM can be the physical CD/DVD-ROM drive on which the web browser is running, or an image file stored on your local hard drive or network drive.
- For optimal performance, NEC Corporation recommends using image files stored on the hard drive of your client PC or on a network drive accessible through a high-speed network link.

- You can use the .NET IRC to mount a Virtual Folder to access and copy files between a client and a managed server.
- You can also access the Virtual Media feature by using the .NET IRC or Java IRC, the iLO RESTful API, or the SMASH CLP.
- If the Virtual Floppy/USB key or Virtual CD/DVD-ROM capability is enabled, you cannot typically access the floppy drive or CD/DVD-ROM drive from the client operating system.

CAUTION:

To prevent file and data corruption, do not try to access the local media when you are using it as an iLO Virtual Media device.

Virtual Media operating system information

This section describes the operating system requirements to consider when you are using the iLO Virtual Media features.

Operating system USB requirement

To use Virtual Media devices, your operating system must support USB devices, including USB mass storage devices. For more information, see your operating system documentation.

During system boot, the ROM BIOS provides USB support until the operating system loads. Because MS- DOS uses the BIOS to communicate with storage devices, utility diskettes that boot DOS will also function with Virtual Media.

Operating system considerations: Virtual Floppy/USB key

- **Boot process and DOS sessions**—During the boot process and DOS sessions, the virtual floppy device appears as a standard BIOS floppy drive (drive A). If a physically attached floppy drive exists, it is unavailable at this time. You cannot use a physical local floppy drive and a virtual floppy drive simultaneously.
- **Windows Server 2008 or later**—Virtual Floppy/USB key drives appear automatically after Windows recognizes the USB device. Use the virtual device as you would use a locally attached device.
  To use a Virtual Floppy as a driver diskette during a Windows installation, disable the integrated diskette drive in the host RBSU, which forces the virtual floppy disk to appear as drive A.
  To use a virtual USB key as a driver diskette during a Windows installation, change the boot order of the USB key drive. NEC Corporation recommends placing the USB key drive first in the boot order.
- **Red Hat Enterprise Linux**—Linux supports the use of USB diskette and key drives.

Changing diskettes

When you are using a Virtual Floppy/USB key on a client machine with a physical USB disk drive, disk- change operations are not recognized. For example, if a directory listing is obtained from a floppy disk, and then the disk is changed, a subsequent directory listing shows the directory listing for the first disk. If disk changes are necessary when you are using a Virtual Floppy/USB key, make sure that the client machine contains a non-USB disk drive.

Operating system considerations: Virtual CD/DVD-ROM

MS-DOS

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

Windows

The Virtual CD/DVD-ROM appears automatically after Windows recognizes the mounting of the device. Use it as you would use a locally attached CD/DVD-ROM device.

Linux

The requirements for Red Hat Enterprise Linux follow:

- **Red Hat Enterprise Linux**—On servers that have a locally attached CD/DVD-ROM, the Virtual CD/DVD-ROM device is accessible at /dev/cdrom1. However, on servers that do not have a locally attached CD/DVD-ROM, the Virtual CD/DVD-ROM is the first CD/DVD-ROM accessible at /dev/cdrom.

  You can mount the Virtual CD/DVD-ROM as a normal CD/DVD-ROM device by using the following command:

  ```
  mount /mnt/cdrom1
  ```

Mounting a USB Virtual Media CD/DVD-ROM on Linux systems

Procedure

1. Log in to iLO through the web interface.
2. Start the .NET IRC or Java IRC.
3. Select the **Virtual Drives** menu.
4. Select the CD/DVD-ROM to use.
5. Mount the drive by using the following commands:
   - For Red Hat Enterprise Linux:

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

Operating system considerations: Virtual Folder

- **Boot process and DOS sessions**—The Virtual Folder device appears as a standard BIOS floppy drive (drive A). If a physically attached floppy drive exists, it is unavailable at this time. You cannot use a physical local floppy drive and the Virtual Folder simultaneously.
- **Windows**—A Virtual Folder appears automatically after Windows recognizes the mounting of the virtual USB device. You can use the folder the same way that you use a locally attached device. Virtual Folders are nonbootable. Attempting to boot from the Virtual Folder might prevent the server from starting.
- **Red Hat Enterprise Linux**—Linux supports the use of the Virtual Folder feature, which uses a FAT 16 file system format.

Using Virtual Media from the iLO web interface

The **Virtual Media** page allows you to perform the following tasks:

- View or eject local media, including locally stored image files, floppy disks, USB keys, CDs/DVD- ROMs, and virtual folders.
- View, connect, eject, or boot from scripted media. Scripted media refers to connecting images hosted on a web server by using a URL. iLO will accept URLs in HTTP or HTTPS format. FTP is not supported.

Viewing Virtual Media status and port configuration

Use the **Virtual Media** page to view the Virtual Media feature status and port configuration. You can configure these settings on the **Access Settings** page.

Procedure

1. Navigate to the **Remote Console & Media** page, and then click the **Virtual Media** tab.

   The Virtual Media feature status and configured port are displayed.

2. Optional: To configure the Virtual Media feature status, click the **Virtual Media Status** link.

   The **Access Settings** page is displayed.

3. Optional: To configure the Virtual Media port, click the **Virtual Media Port** link.

   The **Access Settings** page is displayed.

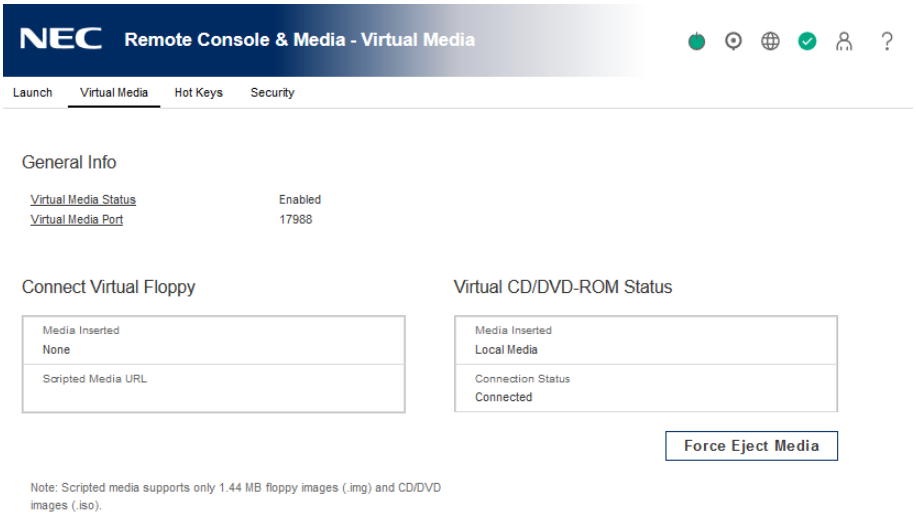
Viewing connected local media

Prerequisites

- Virtual Media privilege
- The Virtual Media feature is enabled on the **Access Settings** page.

Procedure

1. To view the connected local media devices, click **Remote Console & Media** in the navigation tree, and then click the **Virtual Media** tab.



Local media details

When local Virtual Media is connected, the details are listed in the following sections:

Virtual Floppy/USB Key/Virtual Folder Status

- **Media Inserted**—The Virtual Media type that is connected.
  Local Media is displayed when local media is connected.
- **Connected**—Indicates whether a Virtual Media device is connected.

Virtual CD/DVD-ROM Status

- **Media Inserted**—The Virtual Media type that is connected.
  Local Media is displayed when local media is connected.
- **Connected**—Indicates whether a Virtual Media device is connected.

Ejecting a local media device

Prerequisites

- Virtual Media privilege
- The Virtual Media feature is enabled on the **Access Settings** page.

Procedure

1. Click **Remote Console & Media** in the navigation tree, and then click the **Virtual Media** tab.
2. Click the **Force Eject Media** button in the **Virtual Floppy/USB Key/Virtual Folder Status** or **Virtual CD/DVD-ROM Status** section.

Connecting scripted media

You can connect scripted media from the **Virtual Media** page. Use the .NET IRC or Java IRC, or the iLO CLI to connect other types of Virtual Media. The **Virtual Media** page supports the connection of 1.44 MB floppy images (IMG) and CD/DVD-ROM images (ISO). The image must be on a web server on the same network as iLO.

Prerequisites

- Virtual Media privilege
- The Virtual Media feature is enabled on the **Access Settings** page.

Procedure

1. Click **Remote Console & Media** in the navigation tree, and then click the **Virtual Media** tab.
2. Enter the URL for the scripted media in the **Scripted Media URL** box in the **Connect Virtual Floppy** (IMG files) or **Connect CD/DVD-ROM** section (ISO files).
3. For CD/DVD-ROM only: Select the **Boot on Next Reset** check box if you want the server to boot to this image only on the next server reboot.

   The image will be ejected automatically on the second server reboot so that the server does not boot to this image twice.

   If this check box is not selected, the image remains connected until it is manually ejected, and the server boots to it on all subsequent server resets, if the system boot options are configured accordingly.

   An error occurs if you try to enable the **Boot on Next Reset** check box when the server is in POST because you cannot modify the boot order during POST. Wait for POST to finish, and then try again.
4. Click **Insert Media**.
5. Optional: To boot to the connected image now, reboot the server.

Viewing connected scripted media

Prerequisites

- Virtual Media privilege
- The Virtual Media feature is enabled on the **Access Settings** page.

Procedure

1. Click **Remote Console & Media** in the navigation tree, and then click the **Virtual Media** tab.

Scripted media details

When scripted Virtual Media is connected, the details are listed in the **Virtual Floppy/Virtual Folder Status** or **Virtual CD/DVD-ROM Status** section:

- **Media Inserted**—The Virtual Media type that is connected.
- **Scripted Media** is displayed when scripted media is connected.
- **Connected**—Indicates whether a Virtual Media device is connected.
- **Image URL**—The URL that points to the connected scripted media.

Ejecting scripted media

Prerequisites

- Virtual Media privilege
- The Virtual Media feature is enabled on the **Access Settings** page.

Procedure

1. Click **Remote Console & Media** in the navigation tree, and then click **Virtual Media**.
2. To eject scripted media devices, click the **Force Eject Media** button in the **Virtual Floppy/Virtual Folder Status** or **Virtual CD/DVD-ROM Status** section.

Remote Console Virtual Media

You can access Virtual Media on a host server by using the Remote Console, the iLO web interface, the iLO RESTful API, and the CLP. This section describes how to use the Virtual Media feature with the .NET IRC or Java IRC.

Virtual Drives

The Virtual Drive feature supports the use of a physical floppy disk or CD/DVD-ROM, a USB key drive, an image file, or an image file through a URL.

Using a physical drive on a client PC

Prerequisites

- Remote Console privilege
- The Remote Console feature is enabled on the **Access Settings** page.
- An iLO license that supports this feature is installed.
- If you are using the remote console with the Windows operating system, you have Windows administrator rights, which are required for mounting a physical drive.

Procedure

1. Click **Remote Console & Media** in the navigation tree.

   The **Launch** tab displays the Remote Console launch options.

2. Start the .NET IRC or Java IRC.
3. Click the **Virtual Drives** menu, and then select the drive letter of a floppy disk, CD/DVD-ROM, or USB key drive on your client PC.

   The virtual drive activity LED will show virtual drive activity.

Using an image file

Prerequisites

- Remote Console privilege
- The Remote Console feature is enabled on the **Access Settings** page.
- An iLO license that supports this feature is installed.

Procedure

1. Click **Remote Console & Media** in the navigation tree.

   The **Launch** tab displays the Remote Console launch options.

2. Start the .NET IRC or Java IRC.
3. Click the **Virtual Drives** menu, and then select **Image File Removable Media** (IMG) or **Image File CD-ROM/DVD** (ISO).

   The .NET IRC or Java IRC prompts you to select a disk image.

4. Enter the path or file name of the image file in the **File name** text box, or browse to the image file location, and then click **Open**.

   The virtual drive activity LED will show virtual drive activity.

Using an image file through a URL (IIS/Apache)

You can connect scripted media by using the .NET IRC or Java IRC. Scripted media supports only 1.44 MB floppy disk images (IMG) and CD/DVD-ROM images (ISO).

Prerequisites

- Remote Console privilege
- The Remote Console feature is enabled on the **Access Settings** page.
- An iLO license that supports this feature is installed.
- The image file you want to use is on a web server on the same network as iLO.

Procedure

1. Click **Remote Console & Media** in the navigation tree.

   The **Launch** tab displays the Remote Console launch options.

2. Start the .NET IRC or Java IRC.
3. Depending on the image type you will use, select **Virtual Drives** > **URL Removable Media** (IMG) or **Virtual Drives** > **URL CD-ROM/DVD** (ISO).

   The **Image file at URL** dialog box opens.

4. Enter the URL for the image file that you want to mount as a virtual drive, and then click **Connect**. The virtual drive activity LED does not show drive activity for URL-mounted virtual media.

Create Media Image feature (Java IRC only)

When you use Virtual Media, performance is fastest when image files are used instead of physical disks. You can use industry-standard tools like DD to create image files or to copy data from a disk image file to a physical disk. You can also use the Java IRC to perform these tasks.

Creating a disk image file

The Create Media Image feature enables you to create disk image files from data in a file or on a physical disk. You can create an ISO-9660 disk image file (IMG or ISO).

Prerequisites

- Remote Console privilege
- The Remote Console feature is enabled on the **Access Settings** page.
- An iLO license that supports this feature is installed.

Procedure

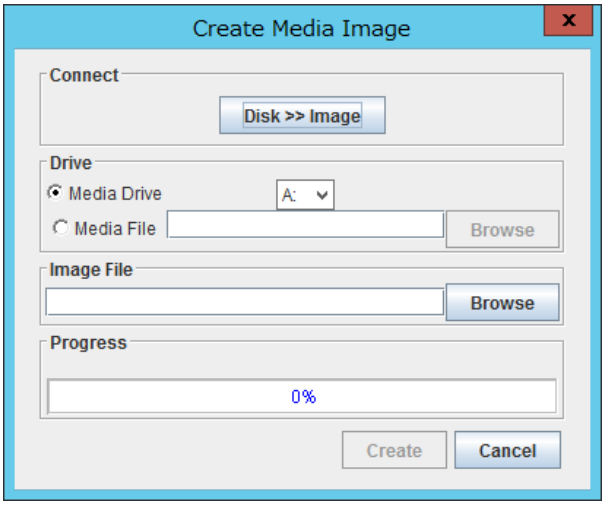
1. Click **Remote Console & Media** in the navigation tree.

   The **Launch** tab displays the Remote Console launch options.

2. Start the Java IRC.

3. Select **Virtual Drives** > **Create Disk Image**.

   The **Create Media Image** dialog box opens.



4. Verify that the **Disk>>Image** button is displayed. If the button label is **Image>>Disk**, click the button to change it to **Disk>>Image**.

5. Do one of the following:
   - If you will use a file, select **Media File**, and then click **Browse** and navigate to the file you want to use.
   - If you will use physical media, select **Media Drive**, and then select the drive letter of the floppy disk, USB key, or CD-ROM in the **Media Drive** menu.

6. Enter the path and file name for the image file in the **Image File** text box.

7. Click **Create**.

   iLO notifies you when the image creation is complete.

8. Click **Close**.

9. Confirm that the image was created in the specified location.

Copying data from an image file to a physical disk

The Create Media Image feature enables you to copy the data from a disk image file to a floppy disk or USB key. Only IMG disk image files are supported. Copying data to a CD-ROM is not supported.

You can copy disk image data to a floppy disk or USB key.

Prerequisites

- Remote Console privilege
- The Remote Console feature is enabled on the **Access Settings** page.
- An iLO license that supports this feature is installed.

Procedure

1. Click **Remote Console & Media** in the navigation tree.

   The **Launch** tab displays the Remote Console launch options.

2. Start the Java IRC.
3. Select **Virtual Drives** > **Create Disk Image**.

   The **Create Media Image** dialog box opens.

4. In the **Create Media Image** window, click **Disk>>Image**.

   The **Create Media Image** changes to the **Image>>Disk** option.

5. Select the drive letter of the floppy disk or USB key in the **Media Drive** menu.
6. Enter the path and file name for the existing image file in the **Image File** text box.

   iLO notifies you when the disk creation is complete.

7. Click **Close**.
8. Confirm that the files were copied to the specified location.

Using a Virtual Folder (.NET IRC only)

Prerequisites

- Remote Console privilege
- The Remote Console feature is enabled on the **Access Settings** page.
- An iLO license that supports this feature is installed.

Procedure

1. Click **Remote Console & Media** in the navigation tree.

   The **Launch** tab displays the Remote Console launch options.

2. Start the .NET IRC.
3. Select **Virtual Drives** > **Folder**.

4. In the **Browse For Folder** window, select the folder you want to use, and then click **OK**. The Virtual Folder is mounted on the server with the name **iLO Folder**.

Virtual folders

Virtual folders enable you to access, browse to, and transfer files from a client to a managed server. You can mount and dismount a local or networked directory that is accessible through the client. After you create a virtual image of a folder or directory, the server connects to the image as a USB storage device. You can browse to the server and transfer the files from the virtual image to the server.

This feature and many others are part of a licensing package.

The Virtual Folder is nonbootable and read-only; the mounted folder is static. Changes to the client folder are not replicated in the mounted folder.

11. Using the power and thermal features

Server power-on

If an AC power loss occurs on a Express server with iLO 5, approximately 30 seconds must elapse before the server can power on again. If the power button is pressed during that time, it will blink, indicating a pending request.

This delay is a result of the iLO firmware loading, authenticating, and booting. iLO processes pending power-button requests when initialization is complete. If the server does not lose power, there is no delay. A 30-second delay occurs only during an iLO reset. The power button is disabled until iLO is ready to manage power.

The iLO firmware monitors and configures power thresholds to support managed-power systems (for example, using power capping technology). Multiple system brownout, blackout, and thermal overloads might result when systems are allowed to boot before iLO can manage power. The managed-power state is lost because of AC power loss, so iLO must first boot to a restore state and allow power-on.

Brownout recovery

A brownout condition occurs when power to a running server is lost momentarily. Depending on the duration of the brownout and the server hardware configuration, a brownout might interrupt the operating system, but does not interrupt the iLO firmware.

iLO detects and recovers from power brownouts. If iLO detects that a brownout has occurred, server power is restored after the power-on delay unless **Auto Power-On** is set to **Always Remain Off**. After the brownout recovery, the iLO firmware records a Brown-out recoveryevent in the iLO Event Log.

Graceful shutdown

The ability of the iLO processor to perform a graceful shutdown requires cooperation from the operating system. To perform a graceful shutdown, the iLO driver and ESMPRO/ServerAgentService or Agentless Management Service must be loaded. iLO communicates with the driver and above service and uses the appropriate operating system method of shutting down the system safely to ensure that data integrity is preserved.

If the driver and above service is not loaded, the iLO processor attempts to use the operating system to perform a graceful shutdown through the power button. iLO emulates a physical power-button press (iLO momentary press) to prompt the operating system to shut down gracefully. The behavior of the operating system depends on its configuration and settings for a power-button press.

The Thermal Shutdown option in the UEFI System Utilities allows you to disable the automatic shutdown feature. This configuration allows the disabling of automatic shutdown except in the

most extreme conditions when physical damage might result.

More Information
iLO drivers

Power efficiency

iLO enables you to improve power usage by using High Efficiency Mode(HEM). HEM improves the power efficiency of the system by placing the secondary power supplies in step-down mode. When the secondary supplies are in step-down mode, the primary supplies provide all DC power to the system. The power supplies are more efficient because there are more DC output watts for each watt of AC input.

When the system draws more than 70% of the maximum power output of the primary supplies, the secondary supplies return to normal operation (exit step-down mode). When power use drops below 60% capacity of the primary supplies, the secondary supplies return to step-down mode. HEM enables you to achieve power consumption equal to the maximum power output of the primary and secondary power supplies, while maintaining improved efficiency at lower power-usage levels.

HEM does not affect power redundancy. If the primary supplies fail, the secondary supplies immediately begin supplying DC power to the system, preventing any downtime.

Use the UEFI System Utilities to configure HEM. You cannot configure these settings through iLO. For more information, see the Server Maintenance guide.

The configured HEM settings are displayed on the **Power Information** page.

Managing the server power

The **Virtual Power Button** section on the **Server Power** page displays the current power state of the server, as well as options for remotely controlling server power. **System Power** indicates the state of the server power when the page is first opened. The server power state can be **ON**, **OFF**, or **Reset**. Use the browser refresh feature to view the current server power state. The server is rarely in the **Reset** state.

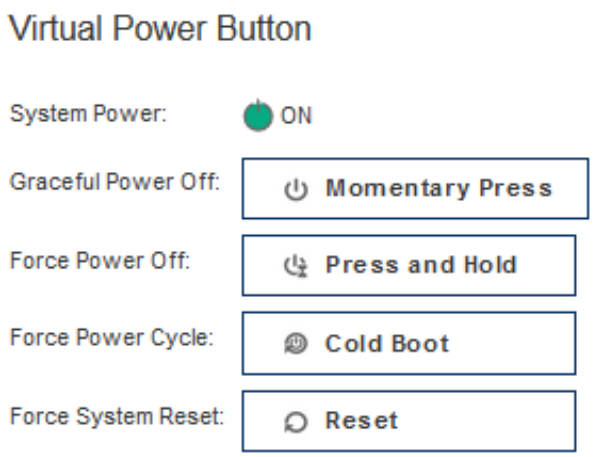
Prerequisites

Virtual Power and Reset privilege

Procedure

1. Click **Power & Thermal** in the navigation tree.

   The page opens with the **Server Power** tab selected.



2. Click one of the following buttons:
   - **Momentary Press**
   - **Press and Hold**
   - **Reset**
   - **Cold Boot**

   The **Press and Hold**, **Reset**, and **Cold Boot** options are not available when the server is powered off.
3. When prompted to confirm the request, click **OK**.

Virtual Power Button options

- **Momentary Press**—The same as pressing the physical power button. If the server is powered off, a momentary press will turn on the server power.
  Some operating systems might be configured to initiate a graceful shutdown after a momentary press, or to ignore this event. NEC Corporation recommends using system commands to complete a graceful operating system shutdown before you attempt to shut down by using the Virtual Power button.
- **Press and Hold**—The same as pressing the physical power button for 5 seconds and then releasing it.
  The server is powered off as a result of this operation. Using this option might circumvent the graceful shutdown features of the operating system.
  This option provides the ACPI functionality that some operating systems implement. These operating systems behave differently depending on a short press or long press.
- **Reset**—Forces the server to warm-boot: CPUs and I/O resources are reset. Using this option circumvents the graceful shutdown features of the operating system.
- **Cold Boot**—Immediately removes power from the server. Processors, memory, and I/O resources lose main power. The server will restart after approximately 6 seconds. Using this option circumvents the graceful shutdown features of the operating system.

Configuring the System Power Restore Settings

The **System Power Restore Settings** section enables you to control system behavior after power is lost. You can also configure these settings by using the UEFI System Utilities during POST.

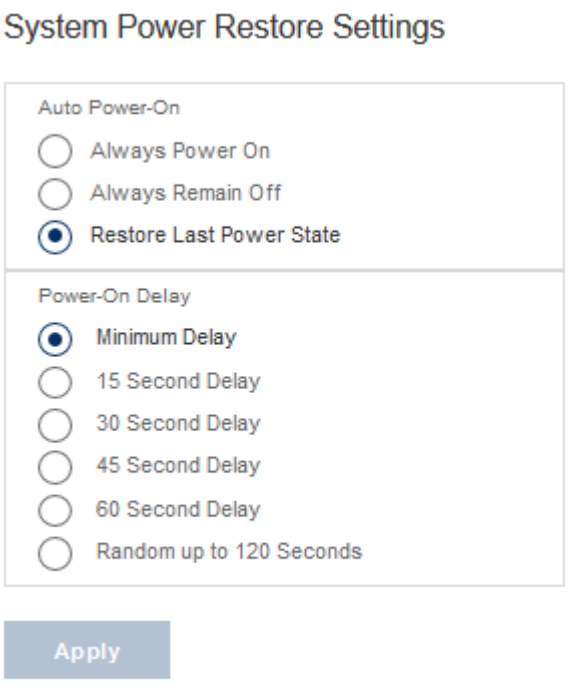
Prerequisites

Configure iLO Settings privilege

Procedure

1. Click **Power & Thermal** in the navigation tree.

   The page opens with the **Server Power** tab selected.



2. Select an **Auto Power-On** value.

   Changes to the **Auto Power On** value might not take place until after the next server reboot.

3. Select a **Power-On Delay** value.

   This value is not available if the **Auto Power-On** option is set to **Always Remain Off**.

4. Click **Apply**.

Auto Power-On

The Auto Power-On setting determines how iLO behaves after power is restored—for example, when the server is plugged in or when a UPS is activated after a power outage. This setting is not supported with micro-UPS systems.

Choose from the following Auto Power-On settings:

- **Always Power On**—Power on the server after the power-on delay.

- **Always Remain Off**—The server remains off until directed to power on.
- **Restore Last Power State**—Returns the server to the power state when power was lost. If the server was on, it powers on; if the server was off, it remains off.
  This option is the default setting.

Power-On Delay

The Power-On Delay setting staggers server automatic power-on in a data center. It determines the amount of time that iLO waits before powering on a server after iLO startup is complete. This setting is not supported with micro-UPS systems.

On supported servers, choose from the following Power-On Delay settings:

- **Minimum Delay**—Power-on occurs after iLO startup is complete.
- **15 Second Delay**—Power-on is delayed by 15 seconds.
- **30 Second Delay**—Power-on is delayed by 30 seconds.
- **45 Second Delay**—Power-on is delayed by 45 seconds.
- **60 Second Delay**—Power-on is delayed by 60 seconds.
- **Random up to 120 seconds**—The power-on delay varies and can be up to 120 seconds.

Viewing server power usage

Power meter graphs display recent server power usage. Power history information is not collected when the server is powered off. When you view a graph that includes periods in which the server was powered off, the graph displays a gap to indicate that data was not collected.

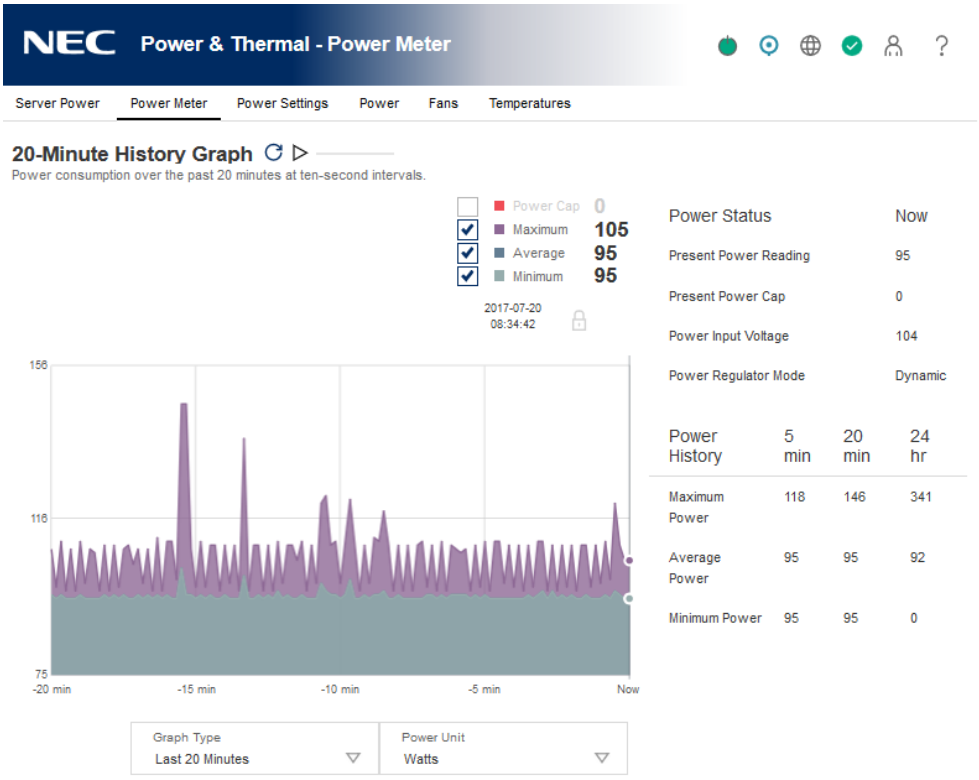
The graph data is cleared when iLO is reset or the server is power cycled. For example, the data is cleared when you use the **Virtual Power Button** Reset or Cold Boot actions, but it is not cleared when you use the Momentary Press or Press and Hold actions.

Prerequisites

An iLO license that supports this feature is installed.

Procedure

1. Click **Power & Thermal** in the navigation tree, and then click the **Power Meter** tab.



2. Select a graph type in the **Graph Type** menu.

   You can view a graph of the last 20 minutes or the last 24 hours.

   To view data for the measured values, move the cursor from side to side within the graph.

3. Optional: To customize the graph display, select or clear the following check boxes:
   - **Power Cap**
   - **Maximum**
   - **Average**
   - **Minimum**

4. Optional: Choose how to refresh data on this page.

   By default, the page data is not refreshed after you open the page.
   - To refresh the page immediately, click the refresh icon ↻.
   - To start refreshing the page automatically, click the triangle icon next to the refresh icon. Depending on the selected graph type, the page refreshes at ten-second or five minute intervals until you click the stop icon or navigate to another page.

5. Optional: To change the power reading display to watts or BTU/hr, select a value from the **Power Unit** menu.

6. Optional: To lock the displayed data at a specific point on the graph, move the cursor to the desired point, and then click.

   To unlock the cursor, click in the graph again or click the lock icon.

Power meter graph display options

Graph Type

- **Last 20 Minutes**—Displays the power usage of the server over the last 20 minutes. The iLO firmware collects power usage information for this graph every 10 seconds.
- **Last 24 hours**—Displays the power usage of the server over the last 24 hours. The iLO firmware updates power usage information for this graph every 5 minutes.

Chart data

Use the following check boxes to customize the data included in power meter graphs.

- **Power Cap**—The configured power cap during the sample. Power cap data is displayed in red in power meter graphs.
  - A power cap limits average power draw for extended periods of time.
  - Power caps are not maintained during server reboots, resulting in temporary spikes during boot.
  - Power caps set for less than 50% of the difference between maximum power and idle power might become unreachable because of changes in the server. NEC Corporation does not recommend configuring power caps for less than 20%. Configuring a power cap that is too low for the system configuration might affect system performance.
- **Maximum**—The highest instantaneous power reading during the sample. iLO records this value on a subsecond basis. Maximum power data is displayed in purple in power meter graphs.
- **Average**—The mean power reading during the sample. Average power data is displayed in blue in power meter graphs.
- **Minimum**—The minimum value observed during a measurement period. The 20-minute graph displays a minimum value that matches the lowest average reading every 10 seconds. The 24-hour graph displays minimum values lower than the 5-minute average value. Minimum power data is displayed in gray in power meter graphs.

Refreshing power meter graphs

- To refresh the page immediately, click the refresh icon ↻.
- To start refreshing the page automatically, click the start icon ▷ next to the refresh icon. The page refreshes automatically until you click the stop icon □ or navigate to another page.

Power unit display

To change the power reading display to watts or BTU/hr, select a value from the **Power Unit** list.

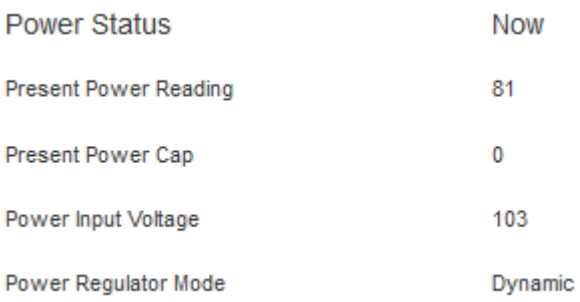
Power meter lock icon

- When automatic refresh is not running, click the lock icon or click a point on the graph to lock the display on a specific point on the graph.
- When automatic refresh is running, use the lock feature to show a data point that falls under a specific historical point along the x-axis. For example, on the 20 minute graph you could lock the display at -10 minutes, and every time the chart refreshes the values that occurred 10 minutes ago are displayed.

Viewing the current power state

Procedure

1. Click **Power & Thermal** in the navigation tree, and then click the **Power Meter** tab. The **Power Status** section displays the current power state details.



Power Status	Now
Present Power Reading	81
Present Power Cap	0
Power Input Voltage	103
Power Regulator Mode	Dynamic

Current power state details

The values displayed in the **Power Status** section vary depending on the server type. The following values are possible:

- **Present Power Reading**—The current power reading from the server. This value is displayed for all servers.
- **Present Power Cap**—The configured power cap for the server. This value is 0 if the power cap is not configured.
- **Power Input Voltage**—The supplied input voltage to the server.
  This value is displayed for ML and DL servers.
- **Power Regulator Mode**—The configured mode. For information about the possible settings, see **Power settings**.

Viewing the server power history

Procedure

1. Click **Power & Thermal** in the navigation tree, and then click the **Power Meter** tab.

   The **Power History** section displays the server power history details.

Power history details

The **Power History** table shows power readings from three time periods: 5 minutes, 20 minutes, and 24 hours.

- **Maximum Power**—The maximum power reading from the server for the specified time period. If the server has not been running for the specified time period, the value is the maximum of all readings since the server booted.
- **Average Power**—The average of the power readings for the specified time period. If the server has not been running for the specified time period, the value is the average of all

readings since the server booted.

- **Minimum Power**—The minimum power reading from the server for the specified time period. If the server has not been running for the specified time period, the value is the minimum of all readings since the server booted.

When multiple power supplies are removed from the server at the same time, there is a short time period in which iLO will not display information in the Power History section or in the Power Meter graphs. This information will be displayed again after iLO collects information about the remaining installed power supplies.

Power settings

The **Power Settings** page enables you to view and control the power management features of the server. The power management features on this page vary based on the server configuration.

Configuring the Power Regulator settings

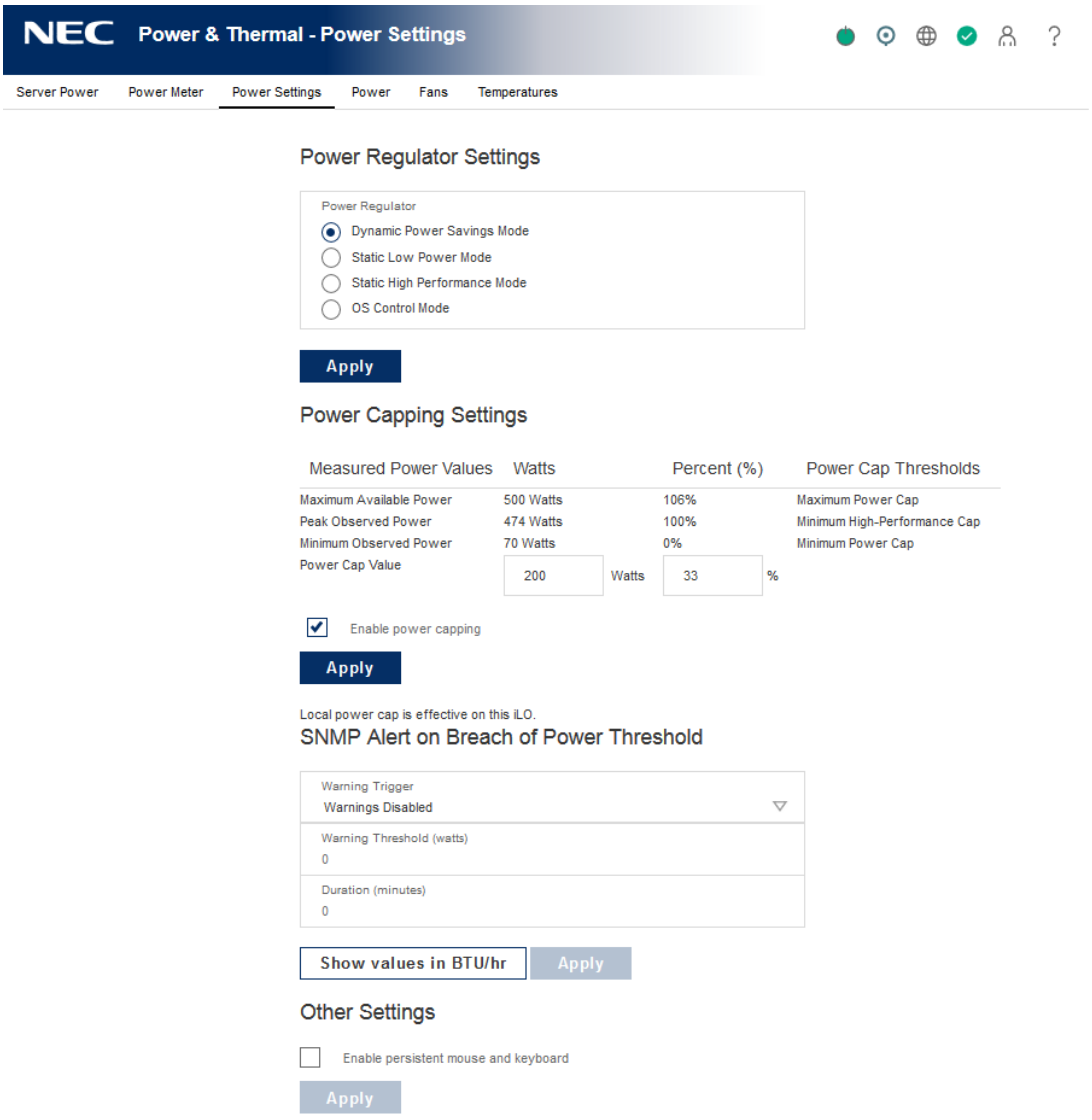
The Power Regulator feature enables iLO to modify processor frequency and voltage levels based on operating conditions to provide power savings with minimal effect on performance.

Prerequisites

Configure iLO Settings privilege

Procedure

1. Click **Power & Thermal** in the navigation tree, and then click the **Power Settings** tab.



2. Select a Power Regulator mode.
3. Click **Apply**.

If the server is off or in POST, the changes will not take effect until POST is complete.

For the Dynamic Power Savings Mode, Static Low Power Mode, and Static High Performance Mode settings, iLO notifies you that the Power Regulator settings changed.

For the OS Control Mode setting, iLO notifies you that you must reboot the server to complete the Power Regulator settings change.

When you change from OS Control Mode to any other mode, you must reboot the server to complete the Power Regulator Settings change.

4. If a reboot is required to complete the change, reboot the server.

Power Regulator modes

Choose from the following modes when you configure the Power Regulator settings:

- **Dynamic Power Savings Mode**—Automatically varies processor speed and power usage based on processor utilization. This option allows the reduction of overall power consumption with little or no impact to performance. It does not require OS support.
- **Static Low Power Mode**—Reduces processor speed and power usage. This option guarantees a lower maximum power usage value for the system.
- **Static High Performance Mode**—Processors will run at maximum power and performance at all times, regardless of the OS power management policy.
- **OS Control Mode**—Processors will run at maximum power and performance at all times, unless the OS enables a power management policy.

Configuring power caps

Prerequisites

- Configure iLO Settings privilege
- An iLO license that supports this feature is installed.
- The server model supports power capping.

See the server user's guide for support information.

Procedure

1. Click **Power & Thermal** in the navigation tree, and then click the **Power Settings** tab.
2. Select the **Enable power capping** check box.
3. Enter the **Power Cap Value** in watts, BTU/hr, or as a percentage.

   The percentage is the difference between the maximum and minimum power values. The power cap value cannot be set lower than the server minimum power value.
4. Optional: When values are displayed in watts, click **Show values in BTU/hr** to change the display to BTU/hr. When values are displayed in BTU/hr, click **Show values in Watts** to change the display to watts.
5. Click **Apply**.

iLO notifies you that the change was successful.

Power capping considerations

- During POST, the ROM runs two power tests that determine the peak and minimum observed power values.

  Consider the values in the **Power Capping Settings** table when determining your power capping configuration.

  - **Maximum Available Power**—The **Maximum Power Cap** threshold. The server must not exceed this value. This value is the power supply capacity.
  - **Peak Observed Power**—The maximum observed power for the server. This value is the **Minimum High-Performance Cap** threshold, and it represents the maximum power that the server uses in the current configuration. A power cap set to this value does not affect server performance.
  - **Minimum Observed Power**—The minimum observed power for the server. This value is the **Minimum Power Cap** threshold, and it represents the minimum power that the server uses. A power cap set to this value reduces the server power usage to the minimum, which results in server performance degradation.
- When a power cap is set, the average power reading of the server must be at or lower than the power cap value.
- Power capping is not supported on all servers. For more information, check the server user's guide.

Configuring SNMP alert on breach of power threshold settings

The **SNMP Alert on Breach of Power Threshold** feature enables the sending of an SNMP alert when power consumption exceeds a defined threshold.

Prerequisites

Configure iLO Settings privilege

Procedure

1. Click **Power & Thermal** in the navigation tree, and then click the **Power Settings** tab.
2. Select a value in the **Warning Trigger** list.
3. If you selected **Peak Power Consumption** or **Average Power Consumption**, enter the following:
   - **Warning Threshold**
   - **Duration**
4. Optional: To change the **Warning Threshold** display to Watts or BTU/hr, click **Show values in Watts** or **Show values in BTU/hr.**

5. Click **Apply**.

SNMP Alert on breach of power threshold options

- **Warning Trigger**—Determines whether warnings are based on peak power consumption, average power consumption, or if they are disabled.
- **Warning Threshold**—Sets the power consumption threshold, in watts. If power consumption exceeds this value for the specified time duration, an SNMP alert is triggered.
- **Duration**—Sets the length of time, in minutes, that power consumption must remain above the warning threshold before an SNMP alert is triggered. When an SNMP alert is generated, it is based on the power consumption data sampled by iLO. It is not based on the exact date and time that the Duration value was changed. The maximum duration is 240 minutes, and the duration must be a multiple of 5.

Configuring the persistent mouse and keyboard

The **Other Settings** section on the **Power Settings** page allows you to enable or disable the persistent keyboard and mouse feature.

When this feature is enabled, the iLO virtual keyboard and mouse are always connected to the iLO UHCI USB controller. When this feature is disabled, the iLO virtual keyboard and mouse are connected dynamically to the iLO UHCI controller only when a Remote Console application is open and connected to iLO. Disabling the feature allows some servers to increase power savings by 15 watts when the server OS is idle and no virtual USB keyboard and mouse are connected.

For example, the power savings for a 24-hour period might be 15 watts x 24 hours, or 360 watt hours (.36 kilowatt-hours).

Prerequisites

Configure iLO Settings privilege

Procedure

1. Click **Power & Thermal** in the navigation tree, and then click the **Power Settings** tab.
2. Select or clear the **Enable persistent mouse and keyboard** check box.

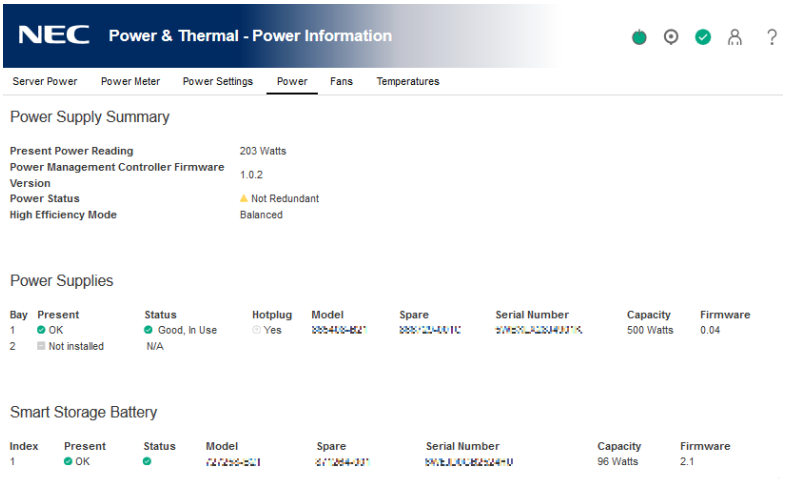
   The persistent mouse and keyboard feature is disabled by default.
3. Click **Apply**.

   iLO notifies you that the change was successful.

Viewing power information

Procedure

1. Click **Power & Thermal** in the navigation tree, and then click the **Power** tab.



The information displayed on the **Power Information** page varies depending on the server type. The following sections are possible:

- **Power Supply Summary**
- **Power Supplies**
- **Smart Storage Battery**

If the server is powered off, the system health information on this page is current as of the last power off. Health information is updated only when the server is powered on and POST is complete.

Power Supply Summary details

Present Power Reading

When Common Slot Power Supplies are present, the most recent power reading from the server is displayed. Other power supplies do not provide this data.

Although this value is typically equal to the sum of all active power supply outputs, there might be some variance as a result of reading the individual power supplies. This value is a guideline value and is not as accurate as the values presented on the **Power Meter** page. For more information, see **Viewing server power usage**.

Power Management Controller Firmware Version

The firmware version of the power management controller. The server must be powered on for the iLO firmware to determine this value. This feature is not available on all servers.

Power Status

The overall status of the power supplied to the server. This section displays the status of the

internal server power supplies.

Possible **Power Status** values follow:

- **Redundant**—Indicates that the power supplies are in a redundant state.
- **Not Redundant**—Indicates that at least one of the power supplies is not providing power to the server. The most common reason for this status is a loss of input power to the power supply.
- **OK**—A Common Slot Power Supply is not installed. The installed power supply is working correctly.
- **N/A**—Only one power supply is installed. Redundancy is not applicable in this configuration.

High Efficiency Mode

The redundant power supply mode that will be used when redundant power supplies are configured. The possible values follow:

- **N/A**—Not applicable.
- **Balanced Mode**—Delivers power equally across all installed power supplies.
- **High Efficiency Mode (Auto)**—Delivers full power to one of the power supplies, and places the other power supplies on standby at a lower power-usage level. A semi-random distribution is achieved because the **Auto** option chooses between the odd or even power supply based on the server serial number.
- **High Efficiency Mode (Even Supply Standby)**—Delivers full power to the odd-numbered power supplies, and places the even-numbered power supplies on standby at a lower power-usage level.
- **High Efficiency Mode (Odd Supply Standby)**—Delivers full power to the even-numbered power supplies, and places the odd-numbered power supplies on standby at a lower power-usage level.
- **Not Supported**—The installed power supplies do not support High Efficiency Mode.

Power Supplies list

Some power supplies do not provide information for all the values in this list. If a power supply does not provide information for a value, **N/A** is displayed.

- **Bay**—The power supply bay number.
- **Present**—Indicates whether a power supply is installed. The possible values are **OK** and **Not Installed**.
- **Status**—The power supply status. The displayed value includes a status icon (**OK**, **Degraded**, **Failed**, or **Other**), and text that provides more information. The possible values follow:
  - **Unknown**
  - **Good, In Use**
  - **Good, Standby**
  - **General Failure**
  - **Over Voltage Failure**
  - **Over Current Failure**

    - **Over Temperature Failure**
    - **Input Voltage Lost**
    - **Fan Failure**
    - **High Input A/C Warning**
    - **Low Input A/C Warning**
    - **High Output Warning**
    - **Low Output Warning**
    - **Inlet Temperature Warning**
    - **Internal Temperature Warning**
    - **High Vaux Warning**
    - **Low Vaux Warning**
    - **Mismatched Power Supplies**
- **Hotplug**—Whether the power supply bay supports swapping the power supply when the server is powered on. If the value is **Yes**, and the power supplies are redundant, the power supply can be removed or replaced when the server is powered on.
- **Model**—The power supply model number.
- **Spare**—The spare power supply part number.
- **Serial Number**—The power supply serial number.
- **Capacity**—The power supply capacity (watts).
- **Firmware**—The installed power supply firmware version.

Smart Storage Battery details

The following details are displayed on servers that support the Smart Storage Battery.

- **Index**—The battery index number.
- **Present**—Whether a battery is installed. The possible values are **OK** and **Not Installed**.
- **Status**—The battery status. The possible values are **OK**, **Degraded**, **Failed**, or **Other**.
- **Model**—The battery model number.
- **Spare**—The part number of the spare battery.
- **Serial Number**—The battery serial number.
- **Capacity**—The battery capacity.
- **Firmware**—The installed battery firmware version.

Power monitoring

iLO monitors the power supplies in the server to ensure the longest available uptime of the server and operating system. Brownouts and other electrical conditions might affect power supplies, or AC cords might be unplugged accidentally. These conditions result in a loss of redundancy if redundant power supplies are configured, or result in a loss of operation if redundant power supplies are not used. If a power supply hardware failure is detected or the AC power cord is disconnected, events are recorded in the IML and LED indicators are used.

High Efficiency Mode

High Efficiency Mode improves the power efficiency of the server by placing the secondary power supplies in standby mode. When the secondary power supplies are in standby mode, primary power provides all DC power to the system. The power supplies are more efficient (more DC output watts for each watt of AC input) at higher output levels, and the overall power efficiency improves.

High Efficiency Mode does not affect power redundancy. If the primary power supplies fail, the secondary power supplies immediately begin supplying DC power to the system, preventing any downtime. You can configure redundant power supply modes only through the UEFI System Utilities. You cannot modify these settings through the iLO firmware.

If High Efficiency Mode is configured to use an unsupported mode, you might experience decreased power supply efficiency.

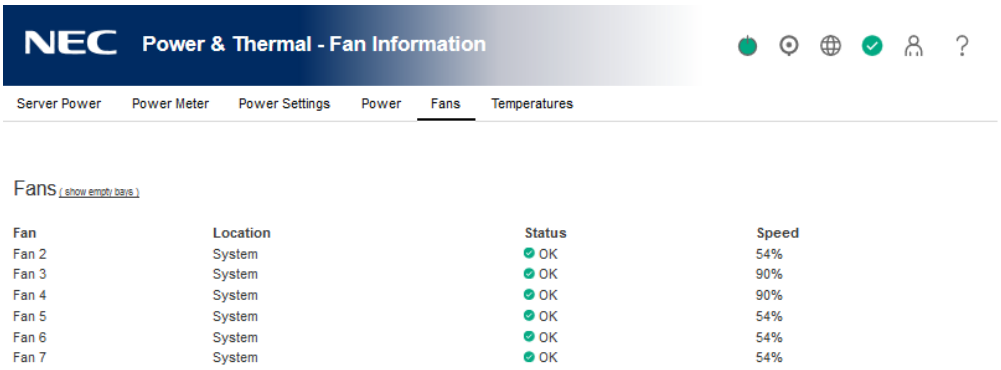
Viewing fan information

The information displayed on the **Fan Information** page varies depending on the server configuration.

If the server is powered off, the system health information on this page is current as of the last power off. Health information is updated only when the server is powered on and POST is complete.

Procedure

1. Click **Power & Thermal** in the navigation tree, and then click the **Fans** tab.



2. Optional: On servers that support fan redundancy, empty fan bays are hidden. To view the empty fan bays, click **show empty bays**. When empty fan bays are displayed, click **hide empty bays** to hide them.

Fan details

The following details are displayed for each fan:

- **Fan**—The fan name.
- **Location**—This value depends on the server type.

The location in the server chassis is listed.

- **Status**—The fan health status.
- **Speed**—The fan speed (percent).

Fans

The iLO firmware, in conjunction with the hardware, controls the operation and speed of the fans. Fans provide essential cooling of components to ensure reliability and continued operation. The fans react to the temperatures monitored throughout the system to provide sufficient cooling with minimal noise.

Monitoring the fan subsystem includes the sufficient, redundant, and non-redundant fan configurations. If one or more fans fail, the server still provides sufficient cooling to continue operation.

Fan operation policies might differ from server to server based on fan configuration and cooling demands. Fan control monitors the internal temperature of the system, increasing the fan speed

to provide more cooling, and decreasing the fan speed when cooling is sufficient. If a fan failure occurs, fan operation policies might increase the speed of the other fans, record the event in the IML, or turn on LED indicators.

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

Temperature information

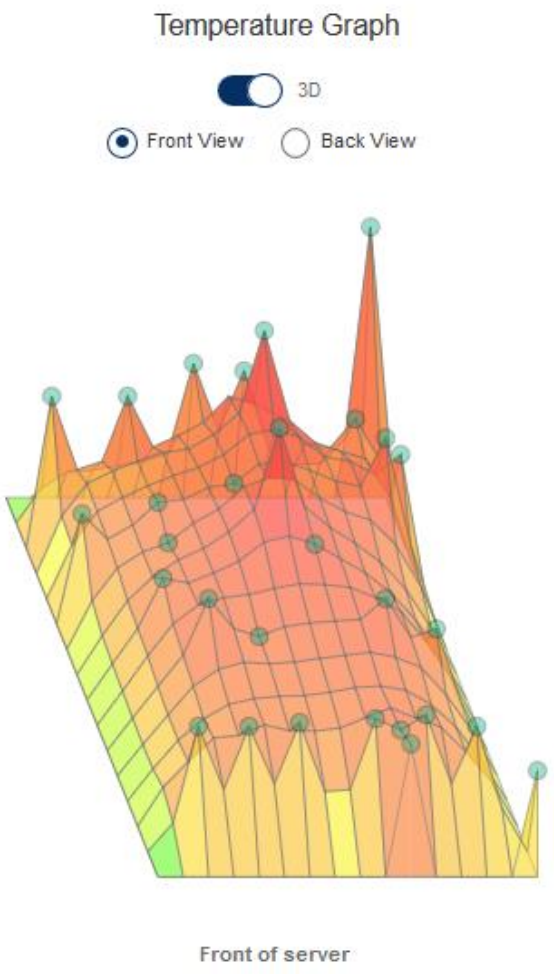
The **Temperature Information** page includes a temperature graph and a table that displays the location, status, temperature, and threshold settings of temperature sensors in the server chassis.

If the server is powered off, the system health information on this page is current as of the last power off. Health information is updated only when the server is powered on and POST is complete.

Viewing the temperature graph

Procedure

1. Click **Power & Thermal** in the navigation tree, and then click the **Temperatures** tab.



2. Optional: Customize the graph display.
   - To display a three-dimensional graph, select the **3D** check box.
   - To display a two-dimensional graph, clear the **3D** check box.
   - To display the sensors at the front or back of the server, select **Front View** or **Back View**.
3. Optional: To view individual sensor details, move the mouse over a circle on the graph. The sensor ID, status, and temperature reading are displayed.

Temperature graph details

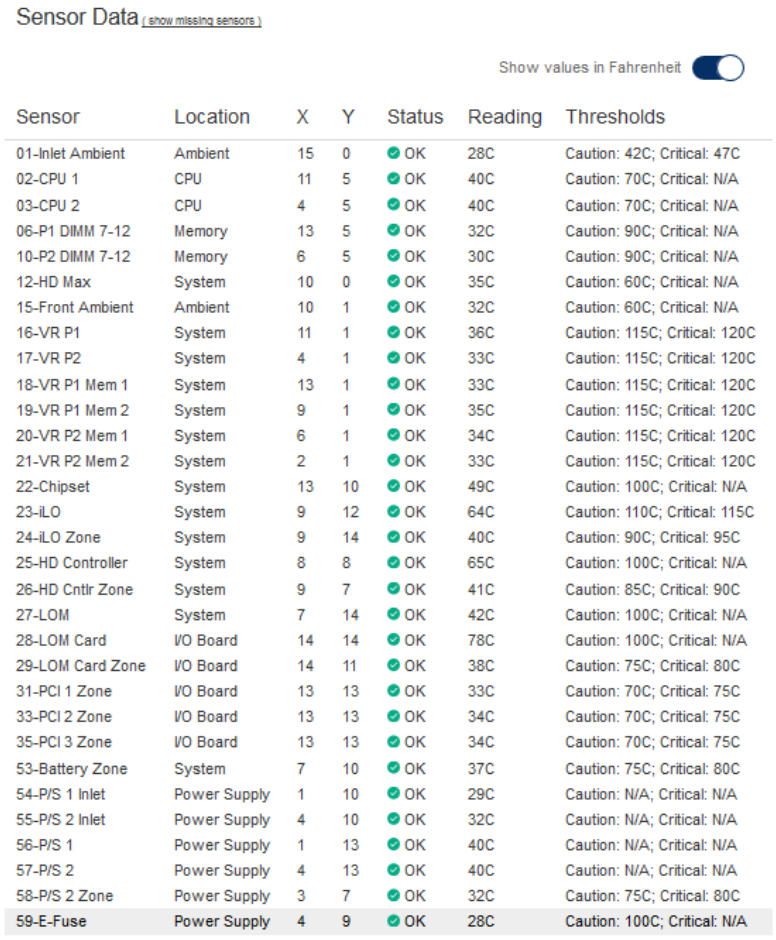
When you view the temperature graph, the circles on the graph correspond to the sensors listed in the **Sensor Data** table.

The color on the graph is a gradient that ranges from green to red. Green represents a temperature of 0°C and red represents the critical threshold. As the temperature of a sensor increases, the graph color changes from green to amber, and then to red if the temperature approaches the critical threshold.

Viewing temperature sensor data

Procedure

1. Click **Power & Thermal** in the navigation tree, and then click the **Temperatures** tab.



Sensor Data (show missing sensors)

Show values in Fahrenheit

Sensor	Location	X	Y	Status	Reading	Thresholds
01-Inlet Ambient	Ambient	15	0	OK	28C	Caution: 42C; Critical: 47C
02-CPU 1	CPU	11	5	OK	40C	Caution: 70C; Critical: N/A
03-CPU 2	CPU	4	5	OK	40C	Caution: 70C; Critical: N/A
06-P1 DIMM 7-12	Memory	13	5	OK	32C	Caution: 90C; Critical: N/A
10-P2 DIMM 7-12	Memory	6	5	OK	30C	Caution: 90C; Critical: N/A
12-HD Max	System	10	0	OK	35C	Caution: 60C; Critical: N/A
15-Front Ambient	Ambient	10	1	OK	32C	Caution: 60C; Critical: N/A
16-VR P1	System	11	1	OK	36C	Caution: 115C; Critical: 120C
17-VR P2	System	4	1	OK	33C	Caution: 115C; Critical: 120C
18-VR P1 Mem 1	System	13	1	OK	33C	Caution: 115C; Critical: 120C
19-VR P1 Mem 2	System	9	1	OK	35C	Caution: 115C; Critical: 120C
20-VR P2 Mem 1	System	6	1	OK	34C	Caution: 115C; Critical: 120C
21-VR P2 Mem 2	System	2	1	OK	33C	Caution: 115C; Critical: 120C
22-Chipset	System	13	10	OK	49C	Caution: 100C; Critical: N/A
23-iLO	System	9	12	OK	64C	Caution: 110C; Critical: 115C
24-iLO Zone	System	9	14	OK	40C	Caution: 90C; Critical: 95C
25-HD Controller	System	8	8	OK	65C	Caution: 100C; Critical: N/A
26-HD Cntlr Zone	System	9	7	OK	41C	Caution: 85C; Critical: 90C
27-LOM	System	7	14	OK	42C	Caution: 100C; Critical: N/A
28-LOM Card	I/O Board	14	14	OK	78C	Caution: 100C; Critical: N/A
29-LOM Card Zone	I/O Board	14	11	OK	38C	Caution: 75C; Critical: 80C
31-PCI 1 Zone	I/O Board	13	13	OK	33C	Caution: 70C; Critical: 75C
33-PCI 2 Zone	I/O Board	13	13	OK	34C	Caution: 70C; Critical: 75C
35-PCI 3 Zone	I/O Board	13	13	OK	34C	Caution: 70C; Critical: 75C
53-Battery Zone	System	7	10	OK	37C	Caution: 75C; Critical: 80C
54-P/S 1 Inlet	Power Supply	1	10	OK	29C	Caution: N/A; Critical: N/A
55-P/S 2 Inlet	Power Supply	4	10	OK	32C	Caution: N/A; Critical: N/A
56-P/S 1	Power Supply	1	13	OK	40C	Caution: N/A; Critical: N/A
57-P/S 2	Power Supply	4	13	OK	40C	Caution: N/A; Critical: N/A
58-P/S 2 Zone	Power Supply	3	7	OK	32C	Caution: 75C; Critical: 80C
59-E-Fuse	Power Supply	4	9	OK	28C	Caution: 100C; Critical: N/A

2. Optional: When temperatures are displayed in Celsius, click the **Show values in Fahrenheit** switch to change the display to Fahrenheit. When temperatures are displayed in Fahrenheit, click the **Show values in Celsius** switch to change the display to Celsius.
3. Optional: By default, sensors that are not installed are hidden. To view the missing sensors, click **show missing sensors**. When missing sensors are displayed, click **hide missing sensors** to hide them.

Temperature sensor details

- **Sensor**—The ID of the temperature sensor, which also gives an indication of the sensor location.
- **Location**—The area where the temperature is being measured. In this column, Memory refers to the following:
  - Temperature sensors on physical memory DIMMs.
  - Temperature sensors located close to the memory DIMMs, but not on the DIMMs. These sensors are located further down the airflow cooling path, near the DIMMs, to provide additional temperature information.

  The ID of the temperature sensor in the Sensor column helps to pinpoint the location, providing detailed information about the DIMM or memory area.
- **X**—The x-coordinate of the temperature sensor.
- **Y**—The y-coordinate of the temperature sensor.
- **Status**—The temperature status.
- **Reading**—The temperature recorded by the temperature sensor. If a temperature sensor is not installed, the Reading column shows the value N/A.
- **Thresholds**—The temperature thresholds for the warning for overheating conditions. The two threshold values are Caution and Critical. If a temperature sensor is not installed, the **Thresholds** column shows the value **N/A**.

Temperature monitoring

The following temperature thresholds are monitored:

- **Caution**—The server is designed to maintain a temperature lower than the caution threshold. If the temperature exceeds the caution threshold, the fan speeds are increased to maximum.

  If the temperature exceeds the caution threshold for 60 seconds, a graceful server shutdown is attempted.
- **Critical**—If temperatures are uncontrollable or rise quickly, the critical temperature threshold prevents system failure by physically shutting down the server before the high temperature causes an electronic component failure.

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

Additional policies are implemented after an excessive temperature condition is corrected, including returning the fan speed to normal, recording the event in the IML, turning off the LED indicators, and canceling shutdowns in progress (if applicable).

12. Configuring iLO network settings

iLO network settings

iLO provides the following options for network connection:

- **iLO Dedicated Network Port**—Uses an independent NIC that is dedicated to iLO network traffic only. When supported, this port uses an RJ-45 jack (labeled iLO) on the back of the server.
- **Shared Network Port LOM**—Uses a permanently installed NIC that is built into the server. This NIC normally handles server network traffic, and it can be configured to handle iLO network traffic at the same time through a common LAN connector.
- **Shared Network Port FlexibleLOM**—Uses an optional NIC that plugs into a special slot on the server. This NIC normally handles server network traffic, and it can be configured to handle iLO network traffic at the same time through a common LAN connector.

To access the network settings, select the active NIC in the navigation tree, and then view or edit the network settings on the following pages:

- **Network Summary**
- **Network General Settings**
- **IPv4 Settings**
- **IPv6 Settings**
- **SNTP Settings**

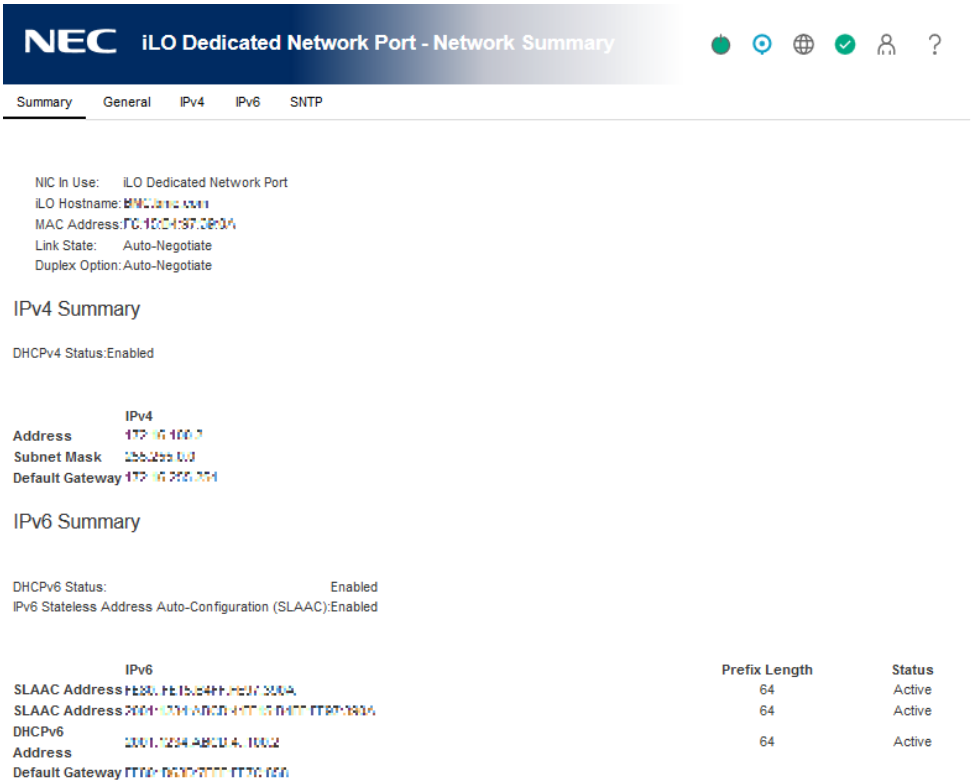
If you select the inactive NIC, a message notifies you that iLO is not configured to use that NIC.

Viewing the network configuration summary

Procedure

1. Depending on your network configuration, click **iLO Dedicated Network Port** or **iLO Shared Network Port** in the navigation tree.

   The **Network Summary** tab is displayed.



Network configuration summary details

- **NIC in Use**—The name of the active iLO network interface (iLO Dedicated Network Port or iLO Shared Network Port).
- **iLO Hostname**—The fully qualified network name assigned to the iLO subsystem. By default, the hostname is **ILO**, followed by the system serial number and the current domain name. This value is used for the network name and must be unique.
- **MAC Address**—The MAC address of the selected iLO network interface.
- **Link State**—The current link speed of the selected iLO network interface. The default value is Auto- Negotiate.
- **Duplex Option**—The current link duplex setting for the selected iLO network interface. The default value is Auto-Negotiate.

You can configure the iLO hostname and NIC settings on the **Network General Settings** page.

IPv4 Summary details

- **DHCPv4 Status**—Indicates whether DHCP is enabled for IPv4.
- **Address**—The IPv4 address currently in use. If the value is 0.0.0.0, the IPv4 address is not configured.
- **Subnet Mask**—The subnet mask of the IPv4 address currently in use. If the value is 0.0.0.0, no address is configured.
- **Default Gateway**—The default gateway address in use for the IPv4 protocol. If the value is 0.0.0.0, the gateway is not configured.

IPv6 Summary details

This section is displayed only for the iLO Dedicated Network Port.

- **DHCPv6 Status**—Indicates whether DHCP is enabled for IPv6. The following values are possible:
  - **Enabled**—Stateless and Stateful DHCPv6 are enabled.
  - **Enabled (Stateless)**—Only Stateless DHCPv6 is enabled.
  - **Disabled**—DHCPv6 is disabled.
- **IPv6 Stateless Address Auto-Configuration (SLAAC)**—Indicates whether SLAAC is enabled for IPv6. When SLAAC is disabled, the SLAAC link-local address for iLO is still configured because it is required.
- **Address list**—This table shows the currently configured IPv6 addresses for iLO. It provides the following information:
  - **Source**—The address type.
  - **IPv6**—The IPv6 address.
  - **Prefix Length**—The address prefix length.
  - **Status**—The address status. The possible values are **Active** (the address is in use by iLO), **Pending** (Duplicate Address Detection is in progress), or **Failed** (Duplicate Address Detection failed. The address is not in use by iLO).
- **Default Gateway**—The default IPv6 gateway address that is in use. For IPv6, iLO keeps a list of possible default gateway addresses. The addresses in this list originate from router advertisement messages and the IPv6 **Static Default Gateway** setting.
  The **Static Default Gateway** setting is configured on the IPv6 page.

General network settings

Use the iLO Dedicated Network Port or iLO Shared Network Port **Network General Settings** page to configure the iLO Hostname and NIC settings.

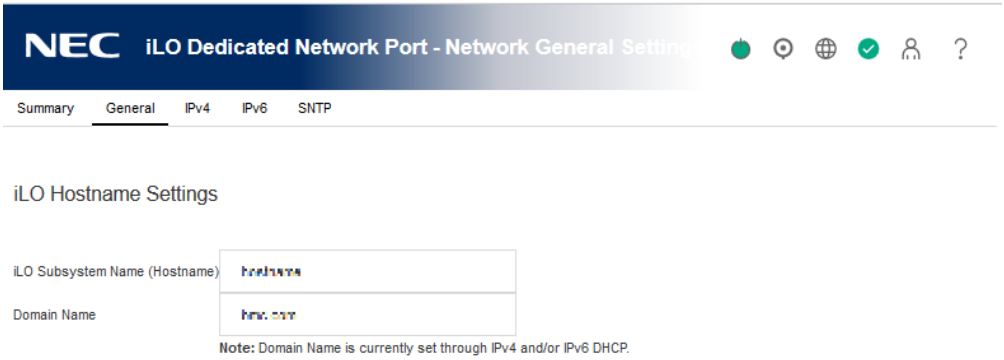
Configuring the iLO Hostname Settings

Prerequisites

Configure iLO Settings privilege

Procedure

1. Click **iLO Dedicated Network Port** or **iLO Shared Network Port** in the navigation tree.
2. Click the **General** tab.



3. Enter the **iLO Subsystem Name (Hostname).**

   The hostname is the DNS name of the iLO subsystem (for example, `ilo` instead of `ilo.example.com`). This name can be used only if DHCP and DNS are configured to connect to the iLO subsystem name instead of the IP address.

4. Enter the iLO Domain Name if DHCP is not configured.

   To use a static domain name when the iLO Dedicated Network port is selected, disable the **Use DHCPv4 Supplied Domain Name** and **Use DHCPv6 Supplied Domain Name** settings on the **IPv4** and **IPv6 Network General Settings** tabs.

   To use a static domain name when the iLO Shared Network port is selected, disable the **Use DHCPv4 Supplied Domain Name** setting on the **IPv4 Network General Settings** tab.

5. Click **Submit**.
6. If you are finished configuring the iLO network settings on the General, IPv4, IPv6, and SNTP tabs, click Reset to restart the iLO processor.

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

iLO hostname and domain name limitations

When you configure the **iLO Hostname Settings**, note the following:

- **Name service limitations**—The subsystem name is used as part of the DNS name.
  - DNS allows alphanumeric characters and hyphens.
  - Name service limitations also apply to the **Domain Name**.
- **Namespace issues**—To avoid these issues:
  - Do not use the underscore character.
  - Limit subsystem names to 15 characters.
  - Verify that you can ping the iLO processor by IP address and by DNS/WINS name.
  - Verify that NSLOOKUP resolves the iLO network address correctly and that no namespace conflicts exist.
  - If you are using both DNS and WINS, verify that they resolve the iLO network address correctly.
  - Flush the DNS name if you make any namespace changes.

NIC settings

Enable the iLO Dedicated Network Port or the iLO Shared Network Port and configure the associated NIC settings in the **NIC Settings** section of the **Network General Settings** tab.

Enabling the iLO Dedicated Network Port through the iLO web interface

Prerequisites

Configure iLO Settings privilege

Procedure

1. Connect the iLO Dedicated Network Port to a LAN from which the server is managed.
2. Click **iLO Dedicated Network Port** in the navigation tree.
3. Click the **General** tab.
4. Select the **Use iLO Dedicated Network Port** check box.
5. Select a **Link State**.

   The link state setting controls the speed and duplex settings of the iLO network transceiver.
6. To save the changes, click **Submit**.
7. If you are finished configuring the iLO network settings on the **General**, **IPv4**, **IPv6**, and **SNTP** tabs, click **Reset** to restart iLO.

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

Link State values

Choose from the following **Link State** values when you enable the iLO Dedicated Network Port:

- **Automatic** (default)—Enables iLO to negotiate the highest supported link speed and duplex

settings when connected to the network.

- **1000BaseT, Full-duplex**—Forces a 1 Gb connection that uses full duplex (supported servers only).
- **1000BaseT, Half-duplex**—Forces a 1 Gb connection that uses half duplex (supported servers only).
- 1000BaseT, Half-duplex is not a standard setting, and few switches support it. If you use this setting, ensure that the switch is configured to support 1000BaseT, Half-duplex.
- **100BaseT, Full-duplex**—Forces a 100 Mb connection using full duplex
- **100BaseT, Half-duplex**—Forces a 100 Mb connection using half duplex
- **10BaseT, Full-duplex**—Forces a 10 Mb connection using full duplex
- **10BaseT, Half-duplex**—Forces a 10 Mb connection using half duplex

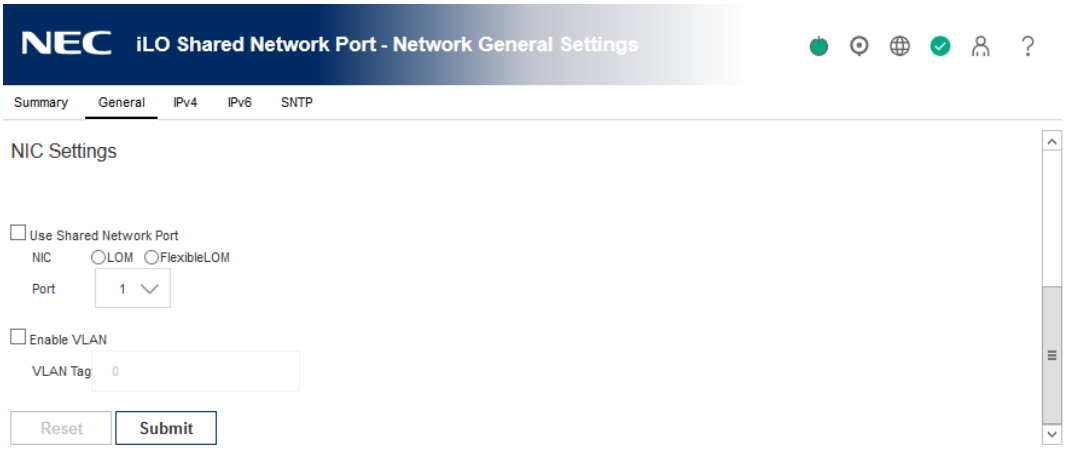
Enabling the iLO Shared Network Port through the iLO web interface

Prerequisites

Configure iLO Settings privilege

Procedure

1. Connect the Shared Network Port LOM or FlexibleLOM port to a LAN.
2. Click **iLO Shared Network Port** in the navigation tree, and then click the **General** tab.



3. Select the **Use Shared Network Port** check box.
4. Depending on the server configuration, select **LOM**, or **FlexibleLOM**.
5. Select a value from the **Port** menu.

   Selecting a port number other than port 1 works only if the server and the network adapter both support this configuration. If you enter an invalid port number, port 1 is used.
6. To use a VLAN, select the **Enable VLAN** check box.

   When the Shared Network Port is active and VLAN is enabled, the iLO Shared Network Port becomes part of a VLAN. All network devices with different VLAN tags will appear to be on separate LANs, even if they are physically connected to the same LAN.

7. If you enabled VLAN, enter a **VLAN Tag**. All network devices that you want to communicate with each other must have the same VLAN tag. The VLAN tag can be any number between 1 and 4094.
8. To save the changes, click **Submit**.
9. If you are finished configuring the iLO network settings on the **General**, **IPv4**, **IPv6**, and **SNTP** tabs, click **Reset** to restart iLO.

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

   After iLO resets, the Shared Network Port is active. Any network traffic going to or originating from iLO is directed through the Shared Network Port LOM or FlexibleLOM port.

iLO network port configuration options

The iLO subsystem provides the following options for network connection:

- **iLO Dedicated Network Port**—Uses an independent NIC that is dedicated to iLO network traffic only. When supported, this port uses an RJ-45 jack (labeled iLO) on the back of the server.
- **Shared Network Port LOM**—Uses a permanently installed NIC that is built into the server. This NIC normally handles server network traffic, and it can be configured to handle iLO network traffic at the same time through a common RJ-45 connector.
- **Shared Network Port FlexibleLOM**—Uses an optional NIC that plugs into a special slot on the server. This NIC normally handles server network traffic, and it can be configured to handle iLO network traffic at the same time through a common RJ-45 connector.

For information about the NICs your server supports, see the server system configuration guide at the following website: **http://www.nec.com/express/**.

iLO network connection considerations

- Only one of the Dedicated Network Port or Shared Network Port options can be enabled at a time because iLO supports only one active NIC connection.
- By default, the iLO Shared Network Port uses port 1 on the server NIC. Depending on the server configuration, this NIC might be a LOM or FlexibleLOM adapter. The port number corresponds to the label on the NIC, which might be different from the numbering in the operating system.
  If both the server and the NIC support port selection, the iLO firmware allows you to select a different port number. If a port other than port 1 is selected for Shared Network Port use, and your server does not support that configuration, iLO switches back to port 1 when it starts.
- Access to iLO through IPv6 is not currently supported when the Shared Network Port is enabled.
- On servers that do not have a Dedicated Network Port, the standard hardware configuration provides iLO network connectivity only through the iLO Shared Network Port connection.

On these servers, the iLO firmware defaults to the Shared Network Port.

- Due to server auxiliary-power budget limitations, some 1Gb/s copper network adapters used for iLO Shared Network Port functionality might run at 10/100 speed when the server is powered off. To avoid this issue, NEC Corporation recommends configuring the switch that the iLO Shared Network Port is connected to for auto-negotiation.
  If the switch port that iLO is connected to is configured for 1Gb/s, some copper iLO Shared Network Port adapters might lose connectivity when the server is powered off. Connectivity will return when the server is powered back on.
- Disabling the iLO Shared Network Port does not completely disable the system NIC—server network traffic can still pass through the NIC port. When the iLO Shared Network Port is disabled, any traffic going to or originating from iLO will not pass through the Shared Network Port.
- If the Shared Network Port is enabled, you cannot modify the link state or duplex options. When using Shared Network Port configurations, these settings must be managed in the operating system.

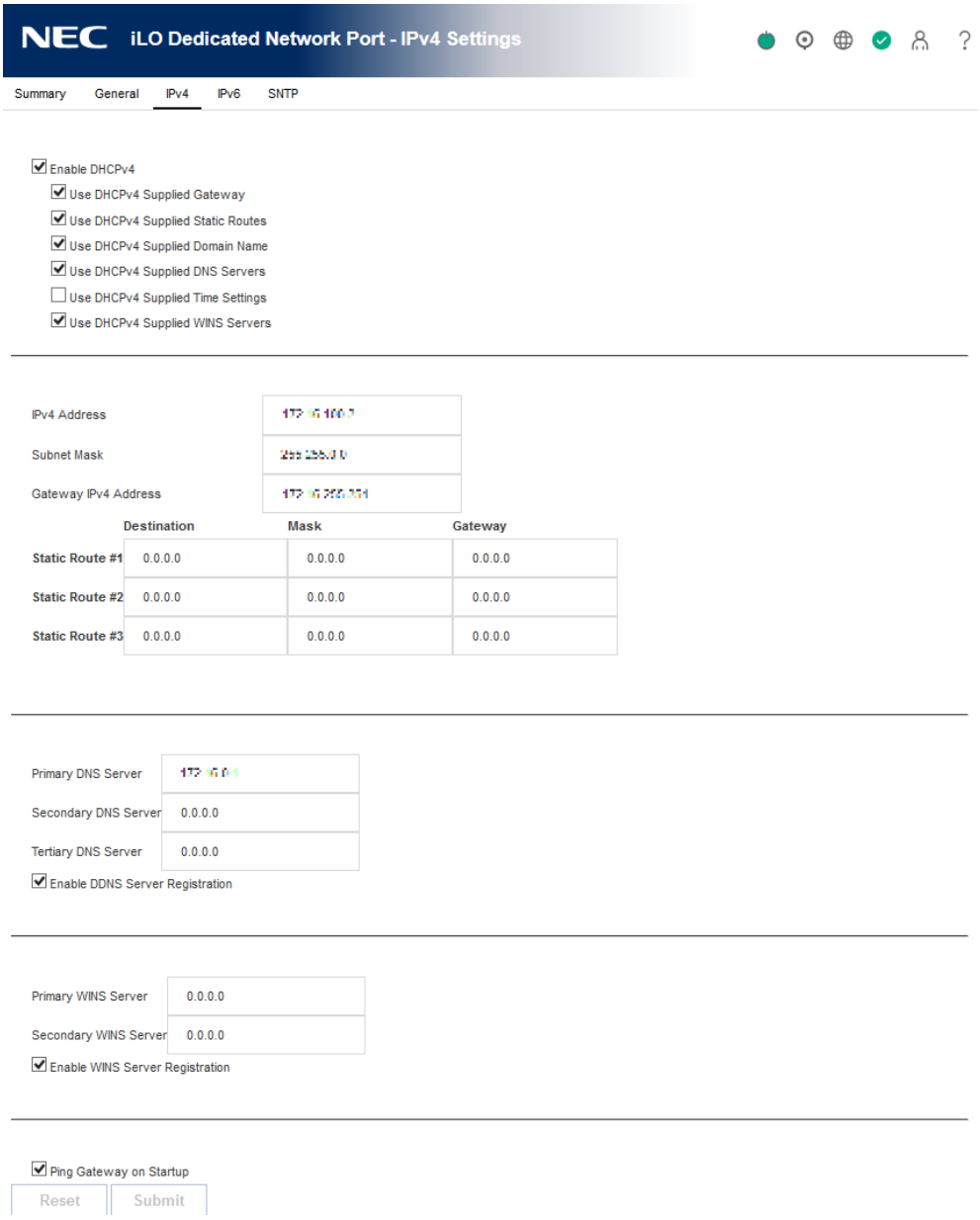
Configuring IPv4 settings

Prerequisites

Configure iLO Settings privilege

Procedure

1. Click **iLO Dedicated Network Port** or **iLO Shared Network Port** in the navigation tree, and then click the **IPv4** tab.



2. Configure the DHCPv4 settings.
3. Configure the general IPv4 settings.
4. Configure the DNS server information.
5. Configure the WINS server information.

6. Configure the **Ping Gateway on Startup** setting.
7. To save the changes you made on the **IPv4 Settings** page, click **Submit**.
8. If you are finished configuring the iLO network settings on the **General**, **IPv4**, **IPv6**, and **SNTP** tabs, click **Reset** to restart iLO.

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

DHCPv4 settings

- **Enable DHCPv4**—Enables iLO to obtain its IP address (and many other settings) from a DHCP server.
- **Use DHCPv4 Supplied Gateway**—Specifies whether iLO uses the DHCP server-supplied gateway. If DHCP is not used, enter a gateway address in the **Gateway IPv4 Address** box.
- **Use DHCPv4 Supplied Static Routes**—Specifies whether iLO uses the DHCP server-supplied static routes. If not, enter the static route destination, mask, and gateway addresses in the **Static Route #1**, **Static Route #2**, and **Static Route #3** boxes.
- **Use DHCPv4 Supplied Domain Name**—Specifies whether iLO uses the DHCP server-supplied domain name. If DHCP is not used, enter a domain name in the **Domain Name** box on the **Network General Settings** page.
- **Use DHCPv4 Supplied DNS Servers**—Specifies whether iLO uses the DHCP server-supplied DNS server list. If not, enter the DNS server addresses in the **Primary DNS Server**, **Secondary DNS Server**, and **Tertiary DNS Server** boxes.
- **Use DHCPv4 Supplied Time Settings**—Specifies whether iLO uses the DHCPv4-supplied NTP service locations.
- **Use DHCPv4 Supplied WINS Servers**—Specifies whether iLO uses the DHCP server-supplied WINS server list. If not, enter the WINS server addresses in the **Use DHCPv4 Supplied WINS Servers**, **Primary WINS Server** , and **Secondary WINS Server** boxes.

General IPv4 settings

- **IPv4 Address**—The iLO IP address. If DHCP is used, the iLO IP address is supplied automatically. If DHCP is not used, enter a static IP address.
- **Subnet Mask**—The subnet mask of the iLO IP network. If DHCP is used, the subnet mask is supplied automatically. If DHCP is not used, enter a subnet mask for the network.
- **Gateway IPv4 Address**—The iLO gateway IP address. If DHCP is used, the iLO gateway IP address is supplied automatically. If DHCP is not used, enter the iLO gateway IP address.
- **Static Route #1**, **Static Route #2**, and **Static Route #3**—The iLO static route destination, mask, and gateway addresses. If **Use DHCPv4 Supplied Static Routes** is used, these values are supplied automatically. If not, enter the static route values.

IPv4 DNS server settings

- **Primary DNS Server**—If **Use DHCPv4 Supplied DNS Servers** is enabled, this value is supplied automatically. If not, enter the Primary DNS Server address.
- **Secondary DNS Server**—If **Use DHCPv4 Supplied DNS Servers** is enabled, this value is supplied automatically. If not, enter the Secondary DNS Server address.

- **Tertiary DNS Server**—If **Use DHCPv4 Supplied DNS Servers** is enabled, this value is supplied automatically. If not, enter the Tertiary DNS Server address.
- **Enable DDNS Server Registration**—Select or clear this check box to specify whether iLO registers its IPv4 address and name with a DNS server.

WINS server settings

- **Primary WINS Server**—If **Use DHCPv4 Supplied WINS Servers** is enabled, this value is supplied automatically. If not, enter the Primary WINS Server address.
- **Secondary WINS Server**—If **Use DHCPv4 Supplied WINS Servers** is enabled, this value is supplied automatically. If not, enter the Secondary WINS Server address.
- **Enable WINS Server Registration**—Specifies whether iLO registers its name with a WINS server.

Ping Gateway on Startup setting

This setting causes iLO to send four ICMP echo request packets to the gateway when the iLO processor initializes. This activity ensures that the ARP cache entry for iLO is up-to-date on the router responsible for routing packets to and from iLO.

Configuring IPv6 settings

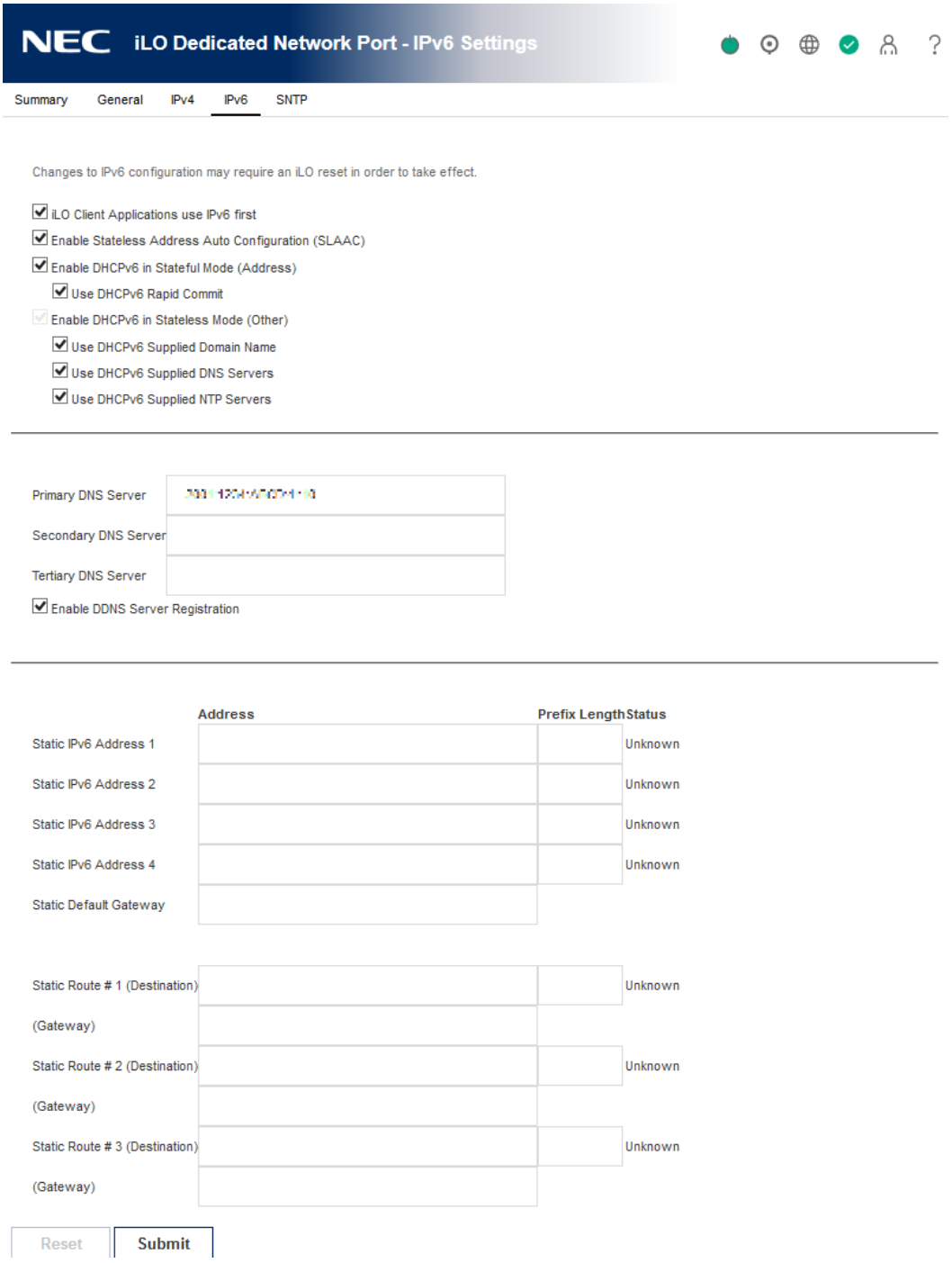
Use the iLO Dedicated Network Port **IPv6 Settings** page to configure the iLO IPv6 settings. IPv6 is not supported in the Shared Network Port configuration.

Prerequisites

Configure iLO Settings privilege

Procedure

1. Click **iLO Dedicated Network Port** in the navigation tree, and then click the **IPv6** tab.



2. Configure the DHCPv6 settings.

3. Configure the DNS server settings.
4. Configure the general IPv6 settings.
5. To save the changes you made on the **IPv6 Settings** page, click **Submit**.
6. If you are finished configuring the iLO network settings on the **General**, **IPv4**, **IPv6**, and **SNTP** tabs, click **Reset** to restart iLO.

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

DHCPv6 settings

iLO Client Applications use IPv6 first

When both IPv4 and IPv6 service addresses are configured for iLO client applications, this option specifies which protocol iLO tries first when accessing a client application. This setting also applies to lists of addresses received from the name resolver when using FQDNs to configure NTP.

- Select this check box if you want iLO to use IPv6 first.
- Clear this check box if you want iLO to use IPv4 first.

If communication fails using the first protocol, iLO automatically tries the second protocol.

Enable Stateless Address Auto Configuration (SLAAC)

Select this check box to enable iLO to create IPv6 addresses for itself from router advertisement messages.

iLO creates its own link-local address even when this option is not selected.

Enable DHCPv6 in Stateful Mode (Address)

Select this check box to allow iLO to request and configure IPv6 addresses provided by a DHCPv6 server.

- **Use DHCPv6 Rapid Commit**—Select this check box to instruct iLO to use the Rapid Commit messaging mode with the DHCPv6 server. This mode reduces DHCPv6 network traffic, but might cause problems when used in networks where more than one DHCPv6 server can respond and provide addresses.

Enable DHCPv6 in Stateless Mode (Other)

Select this check box to enable iLO to request settings for NTP and DNS service location from the DHCPv6 server.

- **Use DHCPv6 Supplied Domain Name**—Select this check box to use the DHCPv6 server-supplied domain name.
- **Use DHCPv6 Supplied DNS Servers**—Select this check box to use IPv6 addresses provided by the DHCPv6 server for DNS server locations. This setting can be enabled at the same time as the IPv4 DNS server location options.
- **Use DHCPv6 Supplied NTP Servers**—Select this check box to use IPv6 addresses provided by the DHCPv6 server for NTP server locations. This setting can be enabled at

the same time as the IPv4 NTP server location options.

When **Enable DHCPv6 in Stateful Mode (Address)** is selected, **Enable DHCPv6 in Stateless Mode (Other)** is always selected by default because it is implicit in the DHCPv6 Stateful messages that are required between iLO and the DHCPv6 server.

IPv6 DNS server settings

- **Primary DNS Server**, **Secondary DNS Server**, and **Tertiary DNS Server**—Enter the IPv6 addresses for the DNS service.
  When DNS server locations are configured on both the IPv4 and IPv6 pages, both sources are used. Preference is given according to the iLO Client Applications use IPv6 first configuration option, primary sources, then secondary, and then tertiary.
- **Enable DDNS Server Registration**—Specify whether iLO registers its IPv6 address and name with a DNS server.

General IPv6 settings

- **Static IPv6 Address 1**, **Static IPv6 Address 2**, **Static IPv6 Address 3**, and **Static IPv6 Address 4**— Enter up to four static IPv6 addresses and prefix lengths for iLO. Do not enter link-local addresses.
- **Static Default Gateway**—Enter a default IPv6 gateway address for cases in which no router advertisement messages are present in the network.
- **Static Route #1**, **Static Route #2**, and **Static Route #3**—Enter static IPv6 route destination prefix and gateway address pairs. Specify the prefix length for the destination. Link-local addresses are not allowed for the destination, but are allowed for the gateway.

iLO features that support IPv6

iLO 5 supports IPv6 in the iLO Dedicated Network Port configuration. It is not supported with the Shared Network Port configuration.

The IETF introduced IPv6 in response to the ongoing depletion of the IPv4 address pool. In IPv6, addresses are increased to 128 bits in length, to avoid an address shortage problem. iLO supports the simultaneous use of both protocols through a dual-stack implementation.

The following features support the use of IPv6:

- IPv6 Static Address Assignment
- IPv6 SLAAC Address Assignment
- IPv6 Static Route Assignment
- IPv6 Static Default Gateway Entry
- DHCPv6 Stateful Address Assignment
- DHCPv6 Stateless DNS, Domain Name, and NTP Configuration
- Integrated Remote Console
- NEC Single Sign-On
- Web Server
- SSH Server
- SNTP Client

- DDNS Client
- SNMP
- AlertMail
- Remote Syslog
- WinDBG Support
- Scriptable Virtual Media
- CLI key import over an IPv6 connection
- Authentication using LDAP and Kerberos over IPv6
- iLO Federation
- IPMI

Configuring iLO SNTP settings

In iLO 5 Firmware Version 1.10 Jun 07 2017, when SNTP setting is not configured or when it is not used in an environment where can be synchronized with the time server, the following times are displayed.

- ✓ If Show Default and Show ISO Time are selected, the following is displayed.

  System time(UTC±Time Zone) displayed in BIOS/Platform Configuration(RBSU)

- ✓ If Show Local Time is selected, the following is displayed.

  Added to the System time(UTC±Time Zone) displayed in BIOS/Platform Configuration(RBSU) and the time zone of the environment of the client connected to iLO.

In iLO 5 Firmware Version 1.15 Aug 17 2017, when SNTP setting is not configured and Time Format on BIOS/Platform Configuration(RBSU) is Local Time, the following times are displayed.

- ✓ If Show Default and Show ISO Time are selected, the following is displayed.

  System time(UTC±Time Zone) displayed in BIOS/Platform Configuration(RBSU)

- ✓ If Show Local Time is selected, the following is displayed.

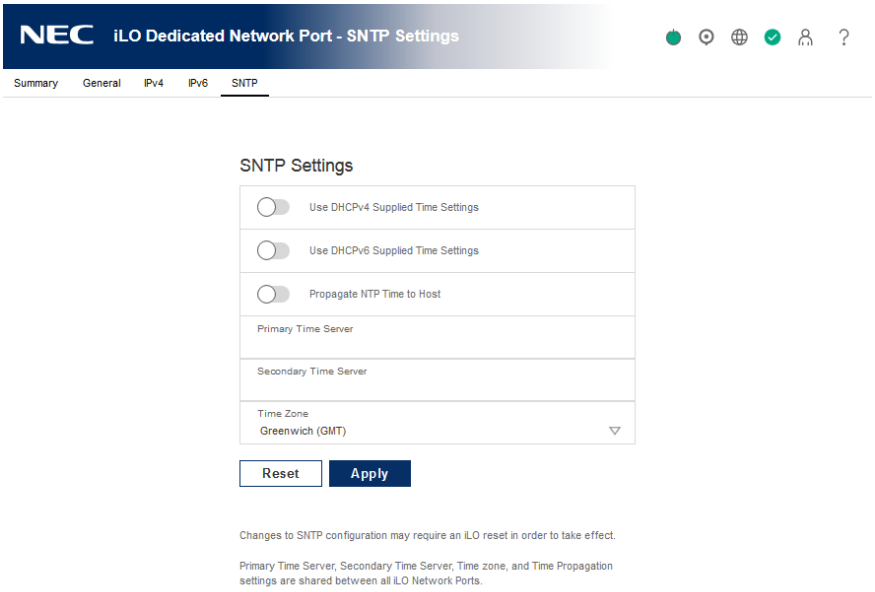
  Added to the System time(UTC±Time Zone) displayed in BIOS/Platform Configuration(RBSU) and the time zone of the environment of the client connected to iLO.

Prerequisites

- Configure iLO Settings privilege
- At least one NTP server is available on your management network.
- If you will use a DHCPv4-provided NTP service configuration, DHCPv4 is enabled on the IPv4 tab.
- If you will use a DHCPv6-provided NTP service configuration, DHCPv6 Stateless Mode is enabled on the IPv6 tab.
- For DHCPv6 time settings configurations only: The server is configured to use the iLO Dedicated Network Port. IPv6 is not supported in the Shared Network Port configuration.

Procedure

1. Click **iLO Dedicated Network Port** or **iLO Shared Network Port** in the navigation tree.
2. Click the **SNTP** tab.



3. Do one of the following:
   - To use DHCP-provided NTP server addresses, enable **Use DHCPv4 Supplied Time** Settings, **Use DHCPv6 Supplied Time** Settings, or both.
   - Enter NTP server addresses in the Primary Time Server and Secondary Time Server boxes.
4. If you selected only **Use DHCPv6 Supplied Time** Settings, or if you entered a primary and secondary time server, select the server time zone from the **Time Zone** list.
5. To save the changes you made on the **SNTP Settings** page, click **Apply**.
6. If you are finished configuring the iLO network settings on the **General**, **IPv4**, **IPv6**, and **SNTP** tabs, click Reset to restart iLO.

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

SNTP options

Use DHCPv4 Supplied Time Settings

Configures iLO to use a DHCPv4-provided NTP server address.

Use DHCPv6 Supplied Time Settings

Configures iLO to use a DHCPv6-provided NTP server address.

NTP time propagation setting

The name of this setting differs depending on the server type.

- **Propagate NTP Time to Host**—Determines whether the server time is synchronized with the iLO time during the first POST after AC power is applied or iLO is reset to the default settings.

IMPORTANT:

For iLO 5 Firmware Version 1.15 Aug 17 2017 or earlier：Does not enable this option and leave it as default.

Primary Time Server

Configures iLO to use a primary time server with the specified address. You can enter the server address by using the server FQDN, IPv4 address, or IPv6 address.

Secondary Time Server

Configures iLO to use a secondary time server with the specified address. You can enter the server address by using the server FQDN, IPv4 address, or IPv6 address.

Time Zone

Determines how iLO adjusts UTC time to obtain the local time, and how it adjusts for Daylight Savings Time (Summer Time). In order for the entries in the iLO Event Log and IML to display the correct local time, you must specify the server location time zone, and select **Show Local Time** in the iLO Event Log and IML display filters.

If you want iLO to use the time the SNTP server provides, without adjustment, select a time zone that does not apply an adjustment to UTC time. In addition, that time zone must not apply a Daylight Savings Time (Summer Time) adjustment. There are several time zones that fit this requirement. One example that you can select in iLO is **Greenwich (GMT)**. If you select this time zone, the iLO web interface pages and log entries display the exact time provided by the SNTP server.

NOTE:

Configure the NTP servers to use Coordinated Universal Time (UTC).

iLO clock synchronization

SNTP allows iLO to synchronize its clock with an external time source. Configuring SNTP is optional because the iLO date and time can also be synchronized from the following sources:

- System ROM (during POST only)

Primary and secondary NTP server addresses can be configured manually or through DHCP servers. If the primary server address cannot be contacted, the secondary address is used.

DHCP NTP address selection

When you use DHCP servers to provide NTP server addresses, the **iLO Client Applications use IPv6 first** setting on the **IPv6** page controls the selection of the primary and secondary NTP values. When **iLO Client Applications use IPv6 first** is selected, a DHCPv6-provided NTP service

address (if available) is used for the primary time server and a DHCPv4-provided address (if available) is used for the secondary time server.

To change the protocol-based priority behavior to use DHCPv4 first, clear the **iLO Client Applications use IPv6 first** check box.

If a DHCPv6 address is not available for the primary or secondary address, a DHCPv4 address (if available) is used.

iLO NIC auto-selection

iLO NIC auto-selection enables iLO to choose between the iLO Dedicated Network Port and the iLO Shared Network port. At startup, iLO searches for network activity on the available ports, and automatically selects one for use based on network activity.

This feature enables you to use a common preconfiguration for your Express servers. For example, if you have several servers, some might be installed in a data center where iLO is contacted through the iLO Dedicated Network Port. Other servers might be installed in a data center where iLO is contacted through the Shared Network Port. When you use iLO NIC auto-selection, you can install a server in either data center and iLO will select the correct network port.

By default, NIC auto-selection is disabled.

More Information
Enabling iLO NIC auto-selection

NIC auto-selection support

- iLO 5 can be configured to search both Shared Network Ports on servers that support this configuration.
- iLO 5 supports NIC failover. When enabled, iLO automatically begins searching for a NIC connection when the current connection fails. NIC auto-selection must be enabled to use this feature.

iLO startup behavior with NIC auto-selection enabled

When NIC auto-selection is enabled:

- If iLO was just connected to power, it tests the iLO Dedicated Network Port first.
- If iLO was just reset, it tests the last used iLO network port first.
- When testing a network port, if iLO detects network activity, then that port is selected for use. If network activity is not found after approximately 100 seconds, iLO switches to the opposite network port and begins testing there. iLO alternates testing between the iLO Dedicated Network Port and the
  iLO Shared Network Port until network activity is detected. An iLO reset occurs each time iLO switches between network ports for testing purposes.

CAUTION:

If any of the physical NICs are connected to an unsecured network, unauthorized access attempts might occur when iLO is alternating between the iLO network ports. NEC Corporation strongly recommends that whenever iLO is connected to any network:

- Use strong passwords for iLO access.
- Never connect the iLO Dedicated Network Port to an unsecured network.
- If the iLO Shared Network Port is connected to an unsecured network, use VLAN

tagging on the iLO portion of the shared NIC, and make sure that the VLAN is connected to a secure network.

- When iLO searches for an active network port, the server UID LED is illuminated. If iLO is reset during the search, the UID LED flashes for 5 seconds and then is illuminated until an active port is selected or iLO is reset.
- When a server supports both LOM and FlexibleLOM Shared Network Port connections to iLO, iLO will test only the option that was selected during configuration. It will not alternate testing between LOM and FlexibleLOM options.
- If NIC auto-selection is configured to search for DHCP address assignment activity, but only one of the iLO network ports has DHCP enabled, iLO tests for received data packet activity on the port that is not configured for DHCP.

Enabling iLO NIC auto-selection

Procedure

1. Configure both iLO network ports.

   Before enabling and using the NIC auto-selection feature, both iLO network ports must be configured for their respective network environments.

2. Use the CLI command `oemNEC_nicautosel` to configure NIC auto-selection.
3. Arrange server cabling as desired, and then reset iLO.

   The change to NIC auto-selection does not take effect until iLO is reset.

Configuring NIC failover

Procedure

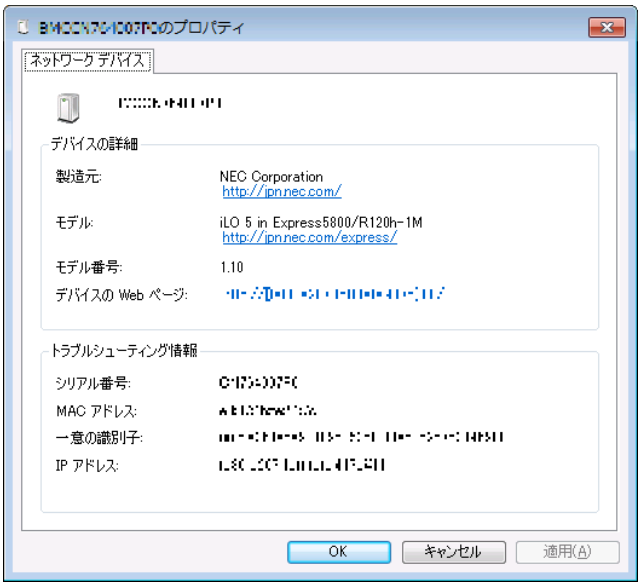
1. Configure iLO NIC auto-selection.
2. Use the CLI command `oemNEC_nicfailover` to configure NIC failover.

Viewing iLO systems in the Windows Network folder

If UPnP is configured, iLO systems on the same network as a Windows system are displayed in the Windows **Network** folder.

Procedure

- To start the web interface for an iLO system, right-click the icon in the Windows **Network** folder, and then select **View device webpage**.
- To view the properties of an iLO system, right-click the icon in the Windows **Network** folder, and then select **Properties**.



The **Properties** window includes the following:

- **Device Details**—iLO manufacturer and version information. To start the iLO web interface, click the **Device webpage** link.
- **Troubleshooting Information**—The serial number, MAC address, UUID, and IP address.

13. Using the iLO administration features

iLO user accounts

iLO enables you to manage user accounts stored locally in secure memory.

You can create up to 12 local user accounts with custom login names and advanced password encryption. Privileges control individual user settings, and can be customized to meet user access requirements.

You can use directories to support more than 12 user accounts. iLO supports up to six directory groups.

More Information
Directory authentication and authorization

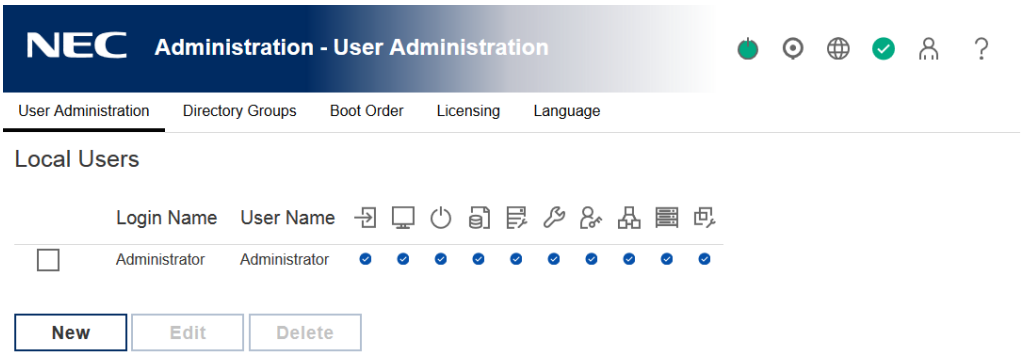
Adding local user accounts

Prerequisites

Administer User Accounts privilege

Procedure

1. Click **Administration** in the navigation tree. The **User Administration** tab is displayed.



2. Click **New**.
3. Enter the following details:
   - **Login Name**
   - **User Name**
   - **New Password** and **Confirm Password**
4. Select from the following privileges:
   - **Login**
   - **Remote Console**
   - **Virtual Power and Reset**
   - **Virtual Media**
   - **Host BIOS**
   - **Configure iLO Settings**

- **Administer User Accounts**
- **Host NIC**
- **Host Storage**
- **Recovery Set**

To select all available user privileges, click the **select all** check box.

5. To save the new user, click **Add User**.

Editing local user accounts

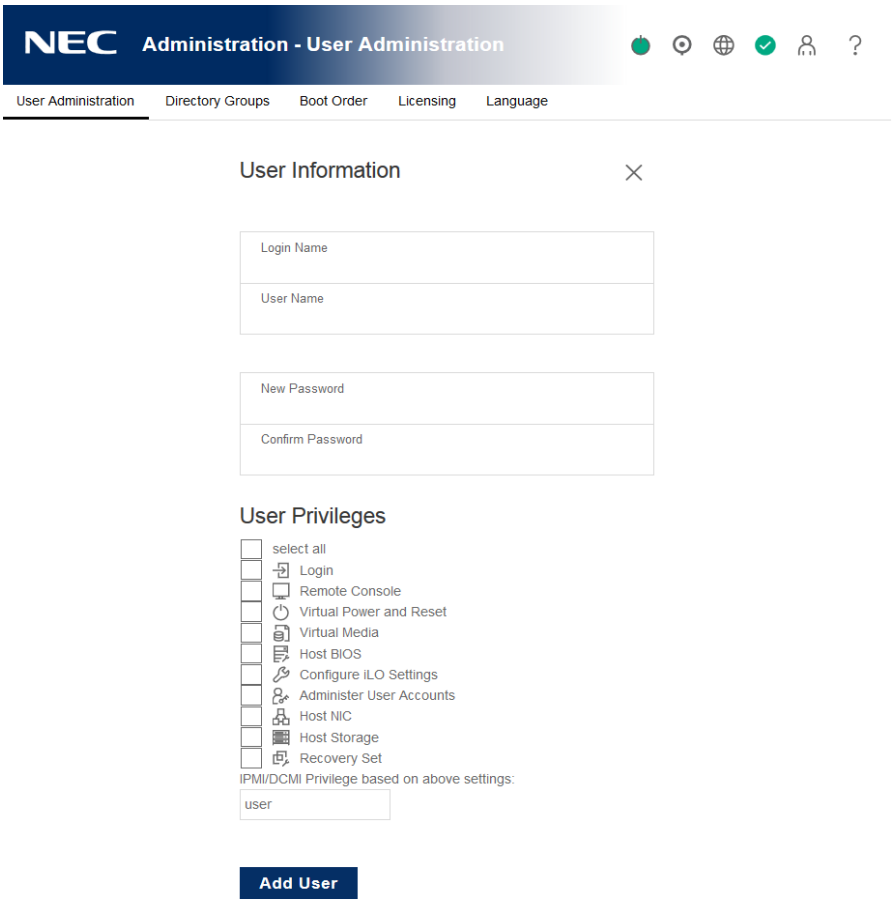
Prerequisites

Administer User Accounts privilege

Procedure

1. Click **Administration** in the navigation tree.

   The **User Administration** tab is displayed.



2. Select a user, and then click **Edit**.
3. Update the following values on the **Add/Edit Local User** page, as needed:
   - **Login Name**
   - **User Name**
4. To change the password, click the **Change password** check box, and then update the **New**

Password and **Confirm Password** values.

5. Select from the following privileges:
   - **Login**
   - **Remote Console**
   - **Virtual Power and Reset**
   - **Virtual Media**
   - **Host BIOS**
   - **Configure iLO Settings**
   - **Administer User Accounts**
   - **Host NIC**
   - **Host Storage**
   - **Recovery Set**
6. To select all available user privileges, click the **select all** check box.
7. To save the user account changes, click **Update User**.

Deleting a user account

Prerequisites

Administer User Accounts privilege

Procedure

1. Click **Administration** in the navigation tree. The **User Adminisration** tab is displayed.
2. Select the check box next to one or more user accounts that you want to delete.
3. Click **Delete**.
4. When prompted to confirm the request, click **OK**.

iLO user account options

- **User Name** appears in the user list on the **User Administration** page. It does not have to be the same as the **Login Name**. The maximum length for a user name is 39 characters. The **User Name** must use printable characters. Assigning descriptive user names can help you to identify the owner of each login name.
- **Login Name** is the name you use when logging in to iLO. It appears in the user list on the **User Administration** page, on the **iLO Overview** page, and in logs. The **Login Name** does not have to be the same as the **User Name**. The maximum length for a login name is 39 characters. The login name must use printable characters.
- **Password** and **Password Confirm** set and confirm the password that is used for logging in to iLO.

iLO user privileges

The following privileges apply to user accounts:

- **Login**— Enables a user to log in to iLO.
- **Remote Console**—Enables a user to access the host system Remote Console, including video, keyboard, and mouse control.
  Users with this privilege can access the BIOS, and therefore might be able to perform host-based BIOS, iLO, storage, and network configuration tasks.
- **Virtual Power and Reset**—Enables a user to power-cycle or reset the host system. These activities interrupt the system availability. A user with this privilege can diagnose the system by using the **Generate NMI to System** button.
- **Virtual Media**—Enables a user to use the Virtual Media feature on the host system.
- **Host BIOS**—Enables a user to configure the host BIOS settings by using the UEFI System Utilities.
- **Configure iLO Settings**—Enables a user to configure most iLO settings, including security settings, and to update the iLO firmware. This privilege does not enable local user account administration.
  After iLO is configured, revoking this privilege from all users prevents reconfiguration with the web interface, iLO RESTful API, or the CLI. Users who have access to the UEFI System Utilities can still reconfigure iLO. Only a user who has the Administer User Accounts privilege can enable or disable this privilege.
- **Administer User Accounts**—Enables a user to add, edit, and delete local iLO user accounts.
  A user with this privilege can change privileges for all users. If you do not have this privilege, you can view your own settings and change your own password.
- **Host NIC**—Enables a user to configure the host NIC settings.
- **Host Storage**—Enables a user to configure the host storage settings.
- **Recovery Set**—Enables a user to manage the recovery install set.
  By default, this privilege is assigned to the default Administrator account. To assign this privilege to another account, log in with an account that already has this privilege.
  This privilege is not available if you start a session when the system maintenance switch is set to disable iLO security.

The following privileges are not available through the CLI: Host NIC, Host Storage, Recovery Set, Host BIOS, and Login.

The following privileges are not available through the UEFI System Utilities BMC Configuration Utility: Login and Recovery Set.

The Host BIOS, Host NIC, and Host Storage privileges apply when you configure the BIOS, Storage, or Network settings through the iLO web interface or the iLO RESTful API. These privileges do not affect configuration through host-based utilities.

Password guidelines

NEC Corporation recommends that you follow these password guidelines when you create and edit user accounts.

- When working with passwords:

- Do not write down or record passwords.
- Do not share passwords with others.
- Do not use passwords that are made up of words found in a dictionary.
- Do not use passwords that contain obvious words, such as the company name, product name, user name, or login name.

- Use passwords with at least three of the following characteristics:
  - One numeric character
  - One special character
  - One lowercase character
  - One uppercase character
- The minimum length for an iLO user account password is set on the **Access Settings** page. Depending on the configured **Minimum Password Length** value, 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:

NEC Corporation does 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 the secure data center.

More Information
Configuring iLO access options

IPMI/DCMI users

The iLO firmware follows the IPMI 2.0 specification. When you add IPMI/DCMI users, the login name must be a maximum of 16 characters, and the password must be a maximum of 20 characters.

When you select iLO user privileges, the equivalent IPMI/DCMI user privilege is displayed in the **IPMI/ DCMI Privilege based on above settings** box.

- **User**—A user has read-only access. A user cannot configure or write to iLO, or perform system actions.
- For IPMI User privileges: Disable all privileges. Any combination of privileges that does not meet the Operator level is an IPMI User.
- **Operator**—An operator can perform system actions, but cannot configure iLO or manage user accounts.
- For IPMI Operator privileges: Enable Remote Console Access, Virtual Power and Reset, and Virtual Media. Any combination of privileges greater than Operator that does not meet the Administrator level is an IPMI Operator.
- **Administrator**—An administrator has read and write access to all features. For IPMI

Administrator privileges: Enable all privileges.

Viewing local user accounts

Procedure

1. Click **Administration** in the navigation tree. The **User Administration tab** is displayed.

   The **Local Users** table shows the login names, user names, and assigned privileges of each configured user.

2. Optional: To view a privilege name, move the cursor over a privilege icon.

iLO directory groups

iLO enables you to manage directory group accounts. Use MMC to manage directory- based user accounts.

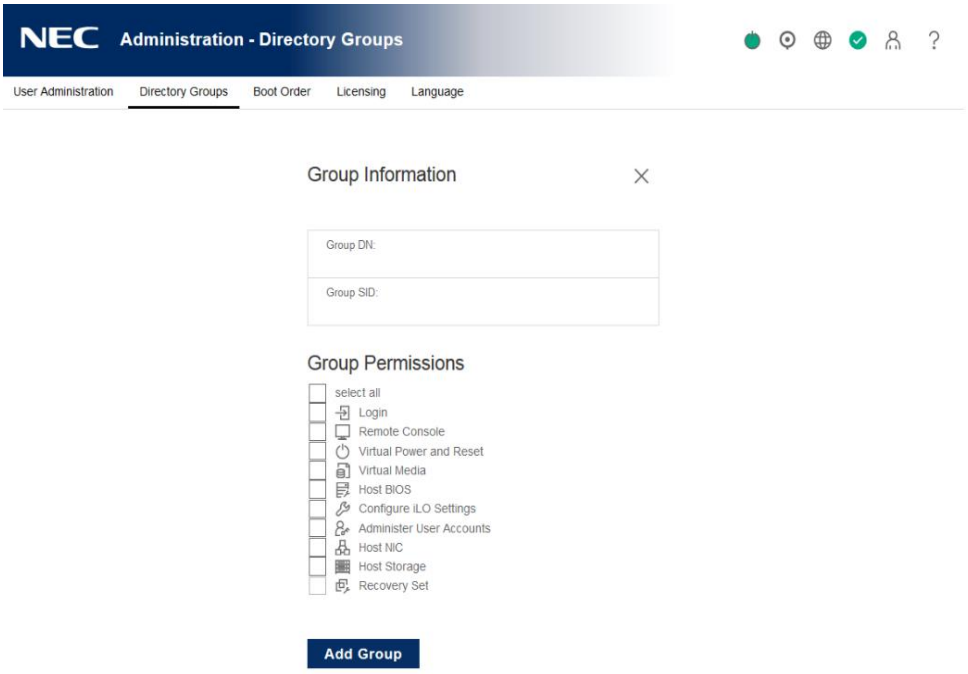
Adding directory groups

Prerequisites

- Configure iLO Settings privilege
- An iLO license that supports this feature is installed.

Procedure

1. Click **Administration** in the navigation tree, and then click the **Directory Groups** tab.



2. Click **New**.
3. Provide the following details in the **Group Information** section:
   - **Group DN**
   - **Group SID** (Kerberos authentication and Active Directory integration only)
4. Select from the following privileges:
   - **Login**
   - **Remote Console**
   - **Virtual Power and Reset**
   - **Virtual Media**
   - **Host BIOS**
   - **Configure iLO Settings**
   - **Administer User Accounts**
   - **Host NIC**
   - **Host Storage**

- **Recovery Set**

5. To save the new directory group, click **Add Group**.

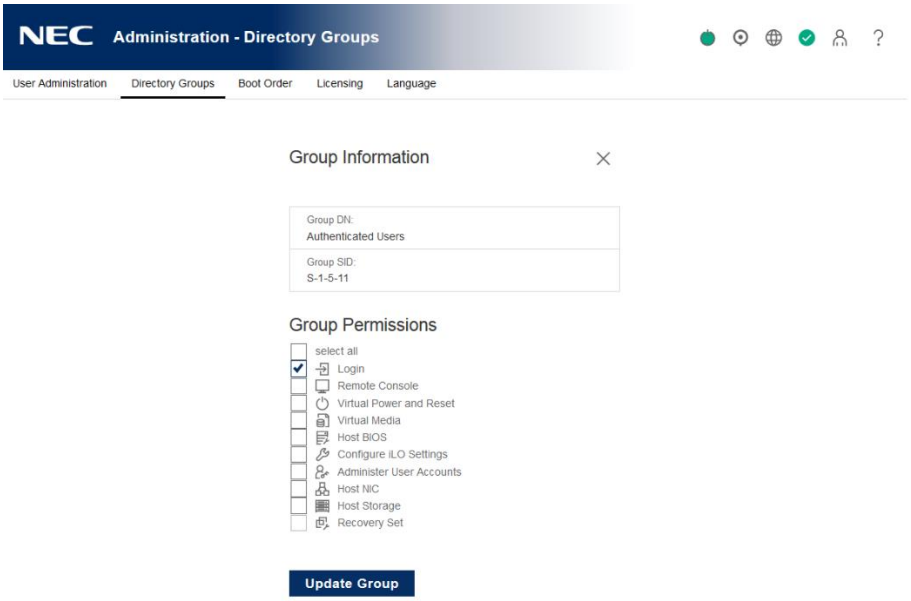
Editing directory groups

Prerequisites

- Configure iLO Settings privilege
- An iLO license that supports this feature is installed.

Procedure

1. Click **Administration** in the navigation tree, and then click the **Directory Groups** tab.



2. Select a group in the **Directory Groups** section, and then click **Edit**.
3. Provide the following details in the **Group Information** section:
   - **Group DN**
   - **Group SID** (Kerberos authentication and Active Directory integration only)
4. Select from the following privileges:
   - **Login**
   - **Remote Console**
   - **Virtual Power and Reset**
   - **Virtual Media**
   - **Host BIOS**
   - **Configure iLO Settings**
   - **Administer User Accounts**
   - **Host NIC**
   - **Host Storage**
   - **Recovery Set**
5. To save the directory group changes, click **Update Group**.

Deleting a directory group

Prerequisites

- Configure iLO Settings privilege
- An iLO license that supports this feature is installed.

Procedure

1. Click **Administration** in the navigation tree, and then click the **Directory Groups** tab.
2. Select the check box next to the directory group that you want to delete.
3. Click **Delete**.
4. When prompted to confirm the request, click **OK**.

Directory group options

Each directory group includes a DN, SID, and account privileges. For Kerberos login, the SIDs of groups are compared to the SIDs for directory groups configured for iLO. If a user is a member of multiple groups, the user account is granted the privileges of all the groups.

You can use global and universal groups to set privileges. Domain local groups are not supported. When you add a directory group to iLO, configure the following values:

- **Group DN** (Security Group DN)—Members of this group are granted the privileges set for the group. The specified group must exist in the directory, and users who need access to iLO must be members of this group. Enter a DN from the directory (for example, CN=Group1, OU=Managed Groups, DC=domain, DC=extension).

  Shortened DNs are also supported (for example, Group1). The shortened DN is not a unique match. NEC Corporation recommends using the fully qualified DN.
- **Group SID (**Security ID)—Microsoft Security ID is used for Kerberos and directory group authorization. This value is required for Kerberos authentication. The required format is S-1-5-2039349. This value does not apply to OpenLDAP servers.

Directory group privileges

The following privileges apply to directory groups:

- **Login**— Enables directory users to log in to iLO.
- **Remote Console**—Enables directory users to access the host system Remote Console, including video, keyboard, and mouse control.
  Users with this privilege can access the BIOS, and therefore might be able to perform host-based BIOS, iLO, storage, and network configuration tasks.
- **Virtual Power and Reset**—Enables directory users to power-cycle or reset the host system. These activities interrupt the system availability. A user with this privilege can diagnose the system by using the Generate NMI to System button.
- **Virtual Media**—Enables directory users to use the Virtual Media feature on the host system.
- **Host BIOS**—Enables directory users to configure the host BIOS settings by using the UEFI

System Utilities.

- **Configure iLO Settings**—Enables directory users to configure most iLO settings, including security settings, and to update the iLO firmware. This privilege does not enable local user account administration.
  After iLO is configured, revoking this privilege from all users prevents reconfiguration with the iLO web interface, iLO RESTful API, or the CLI. Users who have access to the UEFI System Utilities can still reconfigure iLO. Only a user who has the Administer User Accounts privilege can enable or disable this privilege.
- **Administer User Accounts**—Enables directory users to add, edit, and delete local iLO user accounts.
- **Host NIC**—Enables directory users to configure the host NIC settings.
- **Host Storage**—Enables directory users to configure the host storage settings.
- **Recovery Set**—Enables directory users to manage the critical recovery install set.
  By default, this privilege is assigned to the default Administrator account. To assign this privilege to another account, log in with an account that already has this privilege.
  This privilege is not available if you start a session when the system maintenance switch is set to disable iLO security.

The Host BIOS, Host NIC, and Host Storage privileges apply when you configure the BIOS, Storage, or Network settings through the iLO web interface or the iLO RESTful API. These privileges do not affect configuration through host-based utilities.

Viewing directory groups

Procedure

1. Click **Administration** in the navigation tree, and then click the **Directory Groups** tab.

   The **Directory Groups** table shows the group DN, group SID, and the assigned privileges for the configured groups.

2. Optional: To view a privilege name, move the cursor over a privilege icon.

Boot Order

The Boot Order feature enables you to set the server boot options.

Changes made to the boot mode, boot order, or one-time boot status might require a server reset. iLO notifies you when a reset is required.

An error occurs if you try to change the server boot order when the server is in POST. You cannot modify the boot order during POST. If this error occurs, wait for POST to finish, and then try again.

Configuring the server boot mode

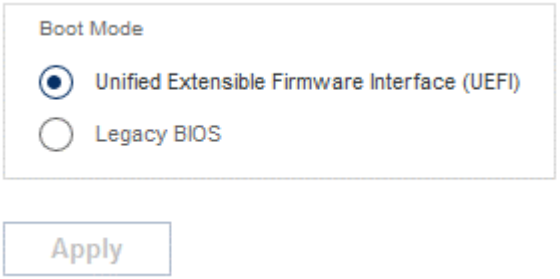
Use the **Boot Mode** setting to define how the server looks for OS boot firmware. You can select UEFI or the Legacy BIOS.

Prerequisites

Configure iLO Settings privilege

Procedure

1. Click **Administration** in the navigation tree, and then click the **Boot Order** tab.
2. **Select** Unified Extensible Firmware Interface (UEFI) **or** Legacy BIOS**.**



3. Click **Apply**.

   iLO prompts you to confirm the change. When you change this setting, you cannot make additional changes on the **Boot Order** page until you reset the server.
4. Click **OK**.
5. Reset the server.

Configuring the server boot order

Prerequisites

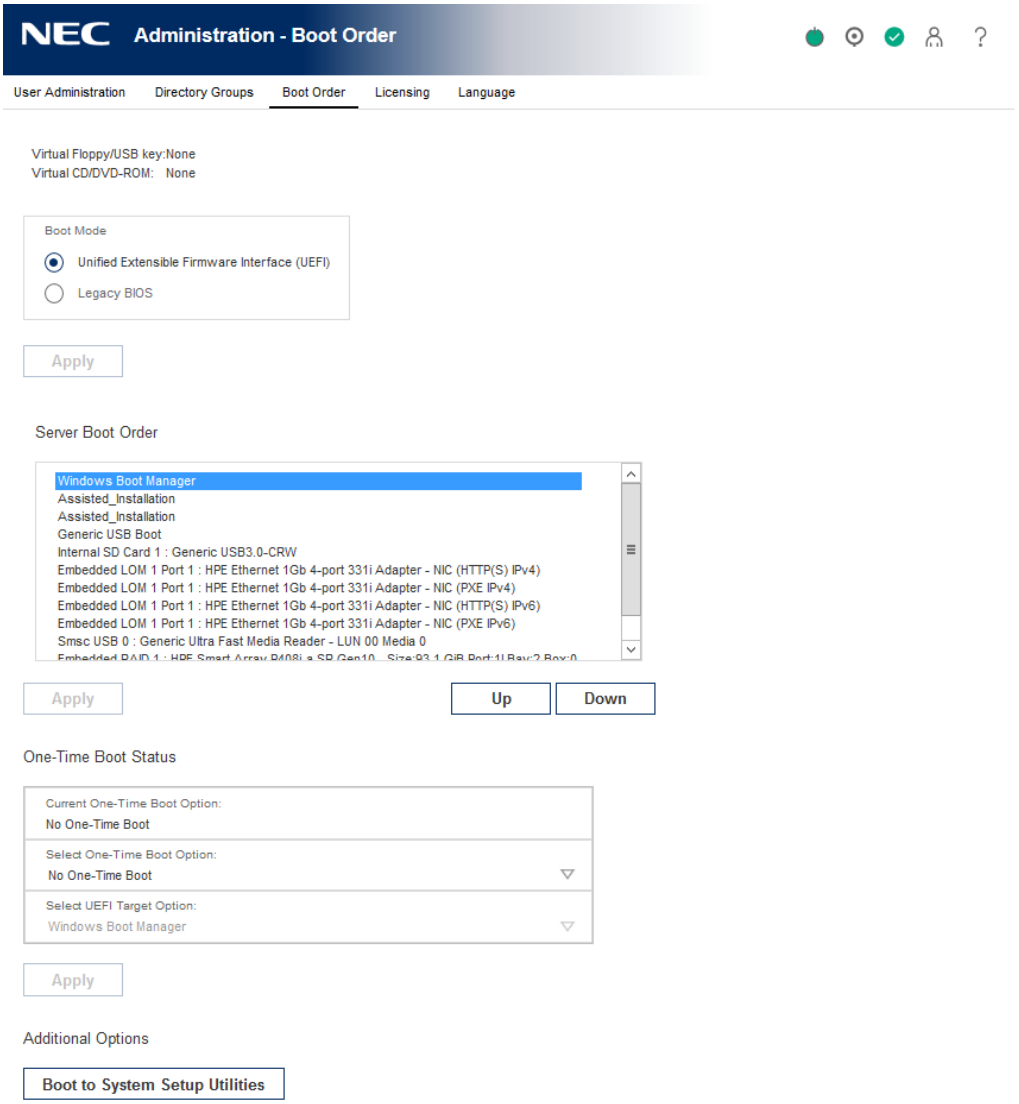
Configure iLO Settings privilege

Procedure

1. Click **Administration** in the navigation tree, and then click the **Boot Order** tab.

   When Virtual Media is connected, the iLO web interface displays the Virtual Media type next

to the **Virtual Floppy/USB key** and **Virtual CD/DVD-ROM** text at the top of the page.



2. To move a device up or down in the boot order, select the device in the **Server Boot Order** list, and then click **Up** or **Down**.

   In Legacy BIOS mode, select from the following devices:

   - **CD/DVD Drive**
   - **USB Storage Device**
   - **Hard Disk Drive**
   - **Network Device <number>**, where the server Ethernet card and additional NIC/FlexibleLOM cards are Network Device 1, Network Device 2, Network Device 3, and so on.

   In UEFI mode, select an option from the list of available boot devices.

3. Click **Apply**.

   iLO confirms that the boot order was updated successfully.

Changing the one-time boot status

Use the one-time boot status feature to set the type of media to boot on the next server reset, without changing the predefined boot order. The procedure to use depends on whether the server uses Legacy BIOS mode or UEFI mode.

Prerequisites

Configure iLO Settings privilege

Changing the one-time boot status in Legacy BIOS mode

Procedure

1. Click **Administration** in the navigation tree, and then click the **Boot Order** tab.
2. Select an option from the **Select One-Time Boot Option** list.

The following options are available:

- **No One-Time Boot**
- **CD/DVD Drive**
- **USB Storage Device**
- **Hard Disk Drive**
- **Network Device <number>**, where the server Ethernet card is Network Device 1, and additional NIC/FlexibleLOM cards are Network Device 2, Network Device 3, and so on.
- **Intelligent Provisioning** – When you select this option, the server boots the EXPRESSBUILDER.
- **Embedded UEFI Shell**—When you select this option, the server boots to an embedded shell environment that is separate from the UEFI System Utilities.

3. Click **Apply**.
4. iLO confirms that the one-time boot option was updated successfully.
5. The **Current One-Time Boot Option** value is updated to show the selection.

Changing the one-time boot status in UEFI mode

Procedure

1. Click **Administration** in the navigation tree, and then click the **Boot Order** tab.
2. Select an option from the **Select One-Time Boot Option** list. The following options are available:
   - **No One-Time Boot**
   - **CD/DVD Drive**
   - **USB Storage Device**
   - **Hard Disk Drive**
   - **Network Device <number>** , where the server Ethernet card is Network Device 1, and additional NIC/FlexibleLOM cards are Network Device 2, Network Device 3, and so on.
   - **Intelligent Provisioning** – When you select this option, the server boots the EXPRESSBUILDER.
   - **HTTP Boot**—When you select this option, if the HTTP Boot feature is enabled and a URI to a bootable image is defined in the ROM-based system utility, the server boots to an HTTP URI.
   - **UEFI Target**—When you select this option, you can select from the list of available boot devices in the **Select UEFI Target Option** list.
   - **Embedded UEFI Shell**—When you select this option, the server boots to an embedded shell environment that is separate from the UEFI System Utilities.
3. If you selected **UEFI Target** in the **Select One-Time Boot Option** list, select a boot device from the **Select UEFI Target Option** list.

   For example, you might have a hard drive with two bootable partitions, and you can use this option to select the bootable partition to use on the next server reset.
4. Click **Apply**.

   iLO confirms that the one-time boot option was updated successfully.

   The **Current One-Time Boot Option** value is updated to show the selection.

Using the additional Boot Order page options

The **Additional Options** section on the **Boot Order** page provides buttons for resetting the server and booting to the system setup utilities.

Prerequisites

- The Virtual Media and Configure iLO Settings privileges are required for the Boot to System Setup Utilities features.
- The Virtual Power and Reset privilege is required for the Server Reset feature.

Procedure

1. Click **Administration** in the navigation tree, and then click the **Boot Order** tab.

2. To use the additional options, do one of the following:
   - To load the ROM-based setup utility on the next server reset, click **Boot to System Setup Utilities**.
   - To reboot the server, click **Server Reset**.
     If a one-time boot option is specified, this setting takes precedence over the **Server Boot Order** value.

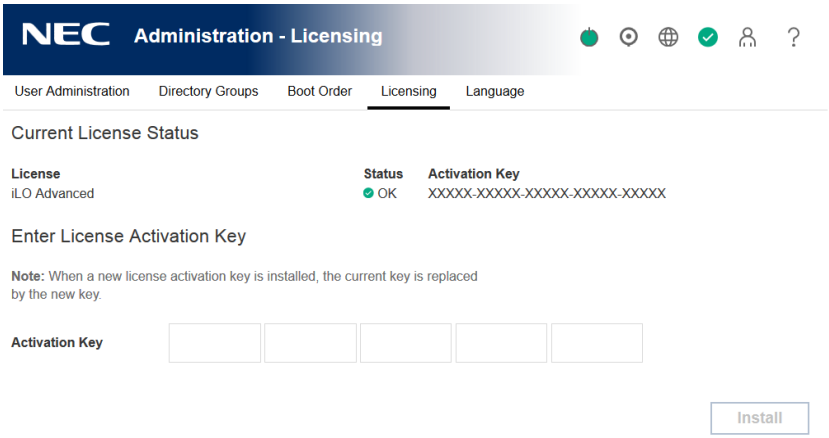
Installing a license key by using a browser

Prerequisites

Configure iLO Settings privilege

Procedure

1. Click **Administration** in the navigation tree, and then click the **Licensing** tab.



2. Enter a license key in the **Activation Key** box.

   To move between segments, press the **Tab** key or click inside a segment of the **Activation Key** box. The cursor advances automatically when you enter data into the segments of the **Activation Key** box.

3. Click **Install**.

4. The EULA confirmation opens.

   The EULA details are available in the License Pack option kit.

5. Click **OK**.

   The license key is now enabled.

Viewing license information

Procedure

1. Click **Administration** in the navigation tree, and then click the **Licensing** tab.

License details

- **License**—The license name
- **Status**—The license status
- **Activation Key**—The installed key

iLO licensing

iLO standard features are included with every server to simplify server setup, perform health

monitoring, monitor power and thermal control, and facilitate remote administration.

iLO licenses activate functionality such as graphical Remote Console with multiuser collaboration, video record/playback, and many more features.

License key information

- One iLO license is required for each server on which the product is installed and used. Licenses are not transferable.
- Please you keep a license key carefully not to lose because it cannot be reissued.

Language packs

Language packs enable you to change the iLO web interface from English to a supported language of your choice. Language packs provide translations for the iLO web interface, .NET IRC, and Java IRC.

Consider the following when using language packs:

- The following language packs are available: Japanese(It is applied from the time of shipment).
- The language packs cannot be uninstalled.
- You can install multiple language packs.

  If a language pack is installed, installing a newer language pack of the same language replaces the installed language pack.
- The Java IRC and .NET IRC use the language of the current iLO session.
- For localization support with the Java IRC on Windows systems, you must select the correct language in the Regional and Language Options Control Panel.
- For localization support with the Java IRC on Linux systems, make sure that the fonts for the specified language are installed and available to the JRE.
- If an installed language pack does not include the translation for a text string, the text is displayed in English.
- When you update the iLO firmware, NEC Corporation recommends downloading the latest language pack to ensure that the language pack contents match the iLO web interface.

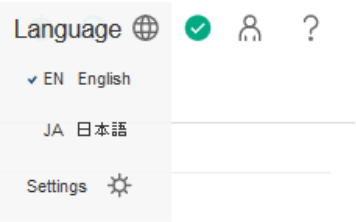
Selecting a language pack

Use one of the following methods to select an installed language pack:

Procedure

- Navigate to the login page, and then select a language in the Language menu.

- Click the Language menu in the toolbar on the bottom right side of the browser window, and then select a language.



- Click Administration in the navigation tree, and then click the Language tab. Click a language in the Installed Languages list.

Configuring the default language settings

Use this procedure to configure the default language for the users of this instance of the iLO firmware.

Prerequisites

Configure iLO Settings privilege

Procedure

1. Click **Administration** in the navigation tree, and then click the **Language** tab.
2. Select a value in the **Default Language** menu.

   The available languages are English and any other language for which a language pack is installed.
3. Click **Apply**.

   iLO notifies you that the default language was changed.

   In subsequent iLO web interface sessions, if there is no browser cookie from a previous session, and the browser or OS language is not supported, the iLO web interface uses the configured default language.

Configuring the current iLO web interface session language

Procedure

1. Click **Administration** in the navigation tree, and then click the **Language** tab.
2. Click the name of a language in the **Installed Languages** list.

   The iLO web interface for the current browser session changes to the selected language.

Uninstalling a language pack

Prerequisites

Configure iLO Settings privilege

Procedure

1. Click **Administration** in the navigation tree, and then click the **Language** tab.
2. Click the trash can icon next to the language you want to remove.
3. When prompted to confirm the request, click **Yes, remove**.

   iLO removes the selected language pack, reboots, and closes your browser connection. It might take several minutes before you can re-establish a connection.

How iLO determines the session language

iLO uses the following process to determine the language of a web interface session:

1. If you previously logged in to the iLO web interface on the same computer using the same browser, and you have not cleared the cookies, the language setting of the last session with that iLO processor is used.
2. If there is no cookie, the current browser language is used if iLO supports it and the required language pack is installed.
3. **Internet Explorer only**: If the browser language is not supported, then the OS language is used if iLO supports it and the required language pack is installed.
4. If there is no cookie, and the browser or OS language is not supported, iLO uses the configured default language. For more information, see **Configuring the default language settings**.

iLO Backup & Restore

The Backup & Restore feature allows you to restore the iLO configuration on a system with the same hardware configuration as the system that was backed up when replacing the motherboard etc. This feature is not meant to duplicate a configuration and apply it to a different iLO system.

In general, it is not expected that you will need to perform an iLO restore operation. However, there are cases in which having a backup of the configuration eases and expedites the return to a normal operating environment.

As with any computer system, backing up your data is a recommended practice to minimize the impact from failures. NEC Corporation recommends performing a backup each time that you update the iLO firmware.

You might want to restore the iLO configuration in the following situations:

Battery failure or removal

Various configuration parameters are stored in the battery-powered SRAM. Although rare, the battery can fail. In some situations, battery removal and replacement might be required. To avoid the loss of configuration information, restore the iLO configuration from a backup file after the battery is replaced.

Reset to factory defaults

In some cases, you might need to reset iLO to the factory default settings to erase settings external to iLO. Resetting iLO to the factory default settings erases the iLO configuration. To recover the iLO configuration quickly, restore the configuration from a backup file after the reset to the factory default settings is complete.

Accidental or incorrect configuration change

In some cases, the iLO configuration might be changed incorrectly, causing important settings to be lost. This situation might occur if iLO is set to the factory default settings or user accounts are deleted.

To recover the original configuration, restore the configuration from a backup file.

System board replacement

If a system board replacement is required to address a hardware issue, you can use this feature to transfer the iLO configuration from the original system board to the new system board.

Lost license key

If a license key is accidentally replaced, or you reset iLO to the factory default settings, and you are not sure which key to install, you can restore the license key and other configuration settings from a backup file.

What information is restored?

The iLO configuration includes many categories such as Power, Network, Security, the User Database, and License Keys. Most configuration information is stored in the battery-powered SRAM memory device, and it can be backed up and restored.

Information that is not restored

Some information is not suitable to be restored. The information that cannot be restored is not part of the iLO configuration, but instead is related to the iLO or server system state.
The following information is not backed up or restored:

Security state

Allowing a restore operation to change the iLO security state would defeat the principles of security and enforcement of security.

Integrated Management Log

To preserve information about events that occurred between the backup and the time or event that required the restore, this information is not restored.

iLO Event Log

To preserve information about events that occurred between the backup and the time or event that required the restore, this information is not restored.

Active Health System data

To preserve the information recorded during the backup and restore process, this information is not restored.

Server state information

- Server power state (ON/OFF)
- Server UID LED states
- iLO and server clock settings

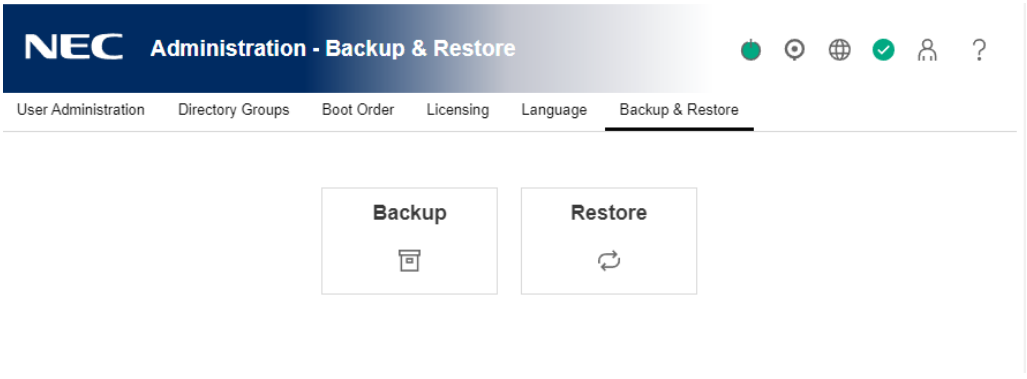
Backing up the iLO configuration

Prerequisites

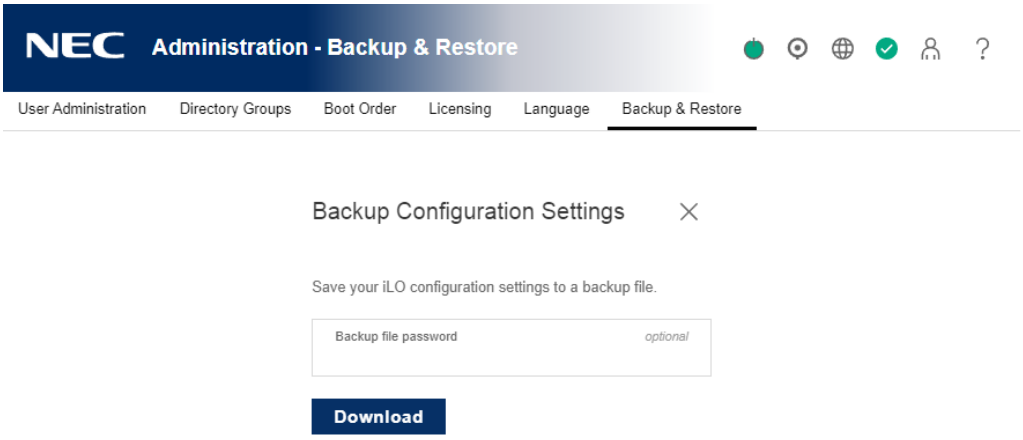
Configure iLO Settings privilege

Procedure

1. Click Administration in the navigation tree, and then click Backup & Restore.



2. Click Backup.



3. Optional: To password protect the backup file, enter a password in the Backup file password box.
4. Click Download.
   The file is downloaded and this activity is recorded in the event log.
   The file name uses the following format:
   <server serial number>_<YYYYMMDD>_<HHMM>.bak.

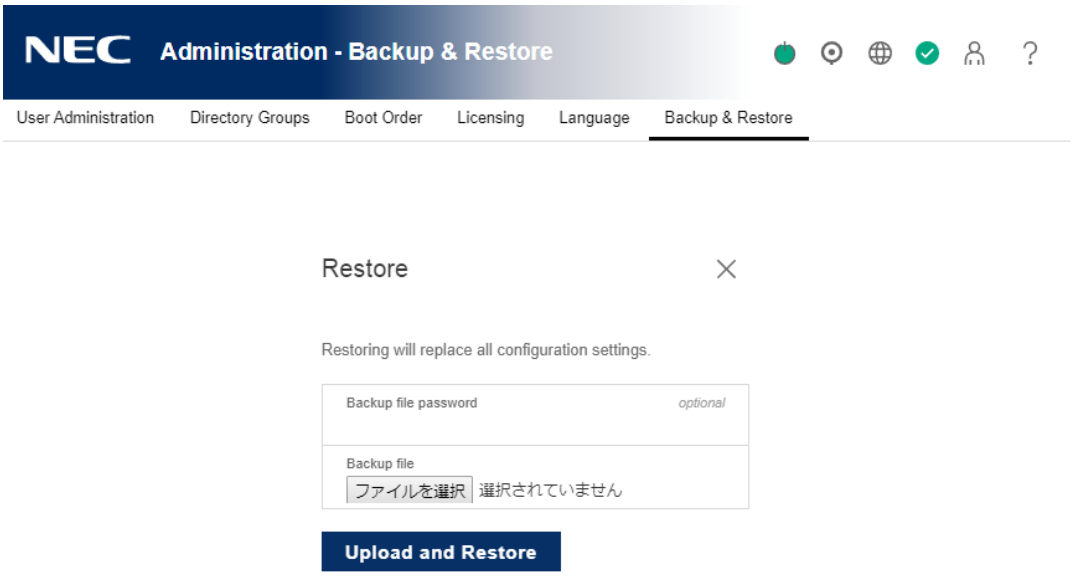
Restoring the iLO configuration

Prerequisites

- Configure iLO Settings privilege
- Administer iLO User Accounts privilege
- An iLO backup file exists.
- The default iLO account credentials are available if you previously reset iLO to the factory default settings.

Procedure

1. Click Administration in the navigation tree, and then click Backup & Restore.
2. Click Restore.



3. Depending on your browser, click Browse or Choose File, and then navigate to the backup file.
4. If the backup file is password protected, enter the password.
5. Click Upload and Restore.

iLO prompts you to confirm the request.

6. Click Restore.
   iLO reboots and closes your browser connection. It might take several minutes before you can reestablish a connection.

Restoring the iLO configuration after system board replacement

When you replace a system board, you can restore the configuration from the replaced system board.

Prerequisites

- Configure iLO Settings privilege
- Administer iLO User Accounts privilege
- An iLO backup file exists.
- The default iLO account credentials are available if you previously reset iLO to the factory default settings.

Procedure

1. Replace the system board and transfer the hardware components from the old system board to the new system board.
2. Power on the system and ensure that all components are working correctly.
3. Log in to iLO with the default user credentials for the new system board.
4. Restore the configuration from the backup file.

14. Using the iLO security features

iLO security

To access the security features that you can configure with the iLO web interface, click Security in the navigation tree.

General security guidelines

When you set up and use iLO, consider the following guidelines for maximizing security:

- Configure iLO on a separate management network.
- Do not connect iLO directly to the Internet.
- Install an SSL certificate.
- Change the password for the default user account.
- Use an authentication service (for example, Active Directory or OpenLDAP), preferably with two-factor authentication.
- Disable protocols that you do not use (for example, SNMP or IPMI over LAN).
- Disable features that you do not use (for example, Remote Console or Virtual Media).
- Use HTTPS for the Integrated Remote Console.

Key security features

Configure iLO security features on the following web interface pages.

Access Settings

- Enable or disable iLO interfaces and features.
- Customize the TCP/IP ports iLO uses.
- Configure authentication failure logging and delays.
- Secure the BMC Configuration Utility.

iLO Service Port

Configure iLO Service Port availability, authentication, and supported devices.

Secure Shell Key

Add SSH keys to iLO user accounts to provide stronger security.

SSL Certificate

Install X.509 CA signed certificates to enable encrypted communications.

Directory

Configure Kerberos authentication and Directory integration.

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 strong password policy.

Encryption

Implement a higher security environment by changing the iLO security state from the default Production level to a stronger setting.

NEC SSO

Configure supported tools for single-sign-on with iLO.

Login Security Banner

Add a security notice to the iLO login page.

More Information

Administering SSL certificates
Directory authentication and authorization
iLO access settings
Connecting iLO to the network
Editing local user accounts
Configuring encryption settings
Configuring the Integrated Remote Console Trust setting (.NET IRC)

iLO access settings

You can modify iLO access settings, including service settings and access options. The values you enter on the Access Settings page apply to all iLO users.

The default access settings values are suitable for most environments. The values you can modify on the Access Settings page allow customization of the iLO external access methods for specialized environments.

You can configure the following iLO security features on this page: ports, iLO interface and feature access, password length, and iLO login security.

Configuring iLO service settings

The TCP/IP ports used by iLO are configurable, which enables compliance with site requirements and security initiatives for port settings. These settings do not affect the host system. The range of valid port values in iLO is from 1 to 65535. If you enter the number of a port that is in use, iLO prompts you to enter a different value.

In addition to customizing the TCP/IP ports, you can also enable or disable iLO features in the **Service** section of the **Access Settings** page.

Changing these settings usually requires configuration of the web browser used for standard and SSL communication. When these settings are changed, an iLO reset is required to activate the changes.

Prerequisites

Configure iLO Settings privilege

Procedure

1. Click **Security** in the navigation tree.

   The **Access Settings** page is displayed.

2. Update the service settings as needed.

   When you disable a service setting, iLO notifies you that the features that depend on the service setting will be unavailable if you apply the changes.

3. Click **Apply**.

   iLO prompts you to confirm that you want to apply the changes and reset iLO.

4. To apply the changes and reset iLO now, click **OK**.

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

Service settings

You can configure the following settings in the **Service** section on the **Access Settings** page.

Secure Shell (SSH)

Allows you to enable or disable the SSH feature. SSH provides encrypted access to the iLO CLP.

Secure Shell (SSH) Port

Sets the SSH port. The default value is 22.

Web Server

Allows you to enable or disable access through the iLO web server.

If you set this value to disabled, iLO will not listen for communication on the Web Server Non-SSL Port or the Web Server SSL port. The following features will not work when the web server is disabled: iLO RESTful API, remote console, iLO Federation, and the iLO web interface.

When **Web Server** is disabled, the ports configured for the **Web Server Non-SSL Port (HTTP)** and **Web Server SSL Port (HTTPS)** are not detected in a security audit that uses a port scanner to scan for security vulnerabilities.

Web Server Non-SSL Port (HTTP)

Sets the HTTP port. The default value is 80.

Web Server SSL Port (HTTPS)

Sets the HTTPS port. The default value is 443.

Remote Console

Allows you to enable or disable access through the iLO remote consoles.

When this option is disabled, the .NET IRC, Java IRC, standalone remote console, and text-based remote console are disabled. The configured remote console port is not detected in a security audit that uses a port scanner to scan for security vulnerabilities.

Remote Console Port

Sets the remote console port. The default value is 17990.

Virtual Media

Allows you to enable or disable the iLO Virtual Media feature.

When this option is disabled, virtual media and scripted virtual media are disabled. The configured virtual media port is not detected in a security audit that uses a port scanner to scan for security vulnerabilities.

Virtual Media Port

The port that iLO uses to listen for incoming local Virtual Media connections. The default value is 17988.

SNMP

Specifies whether iLO responds to external SNMP requests.

If you disable **SNMP** access, iLO continues to operate, and the information displayed in the iLO web interface is updated. In this state, no alerts are generated and SNMP access is not

permitted.

When **SNMP** access is disabled, most of the boxes on the **SNMP Settings** page are unavailable and will not accept input.

SNMP Port

Sets the SNMP port. The industry-standard (default) SNMP port is 161 for SNMP access.

If you customize the **SNMP Port** value, some SNMP clients might not work correctly with iLO unless those clients support the use of a nonstandard SNMP port.

SNMP Trap Port

Sets the SNMP trap port. The industry-standard (default) SNMP trap port is 162 for SNMP alerts (or traps).

If you customize the **SNMP Trap Port** , some SNMP monitoring applications might not work correctly with iLO unless those applications support the use of a nonstandard SNMP trap port.

IPMI/DCMI over LAN

Allows you to send industry-standard IPMI and DCMI commands over the LAN. This setting is disabled by default.

When IPMI/DCMI over LAN is disabled, iLO disables IPMI/DCMI over the LAN. Server-side IPMI/ DCMI applications are still functional when this feature is disabled.

When IPMI/DCMI over LAN is enabled, iLO allows you to use a client-side application to send IPMI/ DCMI commands over the LAN.

When **IPMI/DCMI over LAN** is disabled, the configured **IPMI/DCMI over LAN Port** is not detected in a security audit that uses a port scanner to scan for security vulnerabilities.

IPMI/DCMI over LAN Port

Sets the IPMI/DCMI port number. The default value is 623.

Configuring iLO access options

Prerequisites

Configure iLO Settings privilege

Procedure

1. Click **Security** in the navigation tree, and then click the **Access Settings** tab.
2. Update the access options as needed.
3. Click **Apply**.

   If you changed a value that does not require a reset, iLO completes the change and refreshes the page.

   If you changed a value that requires a reset to take effect, iLO prompts you to confirm that

you want to apply the changes and reset iLO.

4. If iLO prompted you to confirm a settings change and reset, click **OK** to end your browser connection and reset iLO.

Access options

You can configure the following settings in the **Access Options** section on the **Access Settings** page.

Idle Connection Timeout (minutes)

Specifies how long a user can be inactive before an iLO web interface or Remote Console session ends automatically.

The iLO web interface and the Remote Console track idle time separately because each connection is a separate session. This setting has no effect on a Remote Console session if a Virtual Media device is connected.

The following values are valid:

- **15**, **30**, **60**, or **120** minutes—The default value is 30 minutes.
- **Infinite**—Inactive users are not logged out.

Failure to log out of iLO by either browsing to a different site or closing the browser also results in an idle connection. The iLO firmware supports a finite number of connections. Misuse of the **Infinite** timeout option might make iLO inaccessible to other users. Idle connections are recycled after they expire.

This setting applies to local and directory users. Directory server timeout settings might pre-empt the iLO setting.

Changes to the setting might not take effect immediately in current user sessions, but will be enforced immediately in all new sessions.

iLO Functionality

Specifies whether iLO functionality is available.

When this setting is enabled (default), the iLO network is available and communications with operating system drivers are active.

When this setting is disabled, the iLO network and communications with operating system drivers are terminated.

To re-enable iLO functionality, use the UEFI System Utilities. For more information, see the server maintenance guide.

iLO Web Interface

Specifies whether the iLO web interface can be used to communicate with iLO. This setting is enabled by default.

iLO ROM-Based Setup Utility

Enables or disables the iLO configuration options in the UEFI System Utilities.

When this setting is enabled (default), the iLO configuration options are available when you access the UEFI System Utilities.

When this setting is disabled, the iLO configuration options are not available when you access the UEFI System Utilities.

This setting cannot be enabled if option ROM prompting is disabled in the system BIOS. This option is called **BMC Configuration Utility** in the UEFI System Utilities.

Require Login for iLO RBSU

Determines whether a user credential prompt is displayed when a user accesses the iLO configuration options in the UEFI System Utilities.

When this setting is disabled (default), login is not required when a user accesses the iLO configuration options in the UEFI System Utilities.

When this setting is enabled, a login dialog box opens when a user accesses the iLO configuration options in the UEFI System Utilities.

This option is called **Require user login and configuration privilege for BMC Configuration** in the UEFI System Utilities.

Show iLO IP during POST

Enables the display of the iLO network IP address during host server POST.

When this setting is enabled (default), the iLO IP address is displayed during POST. When this setting is disabled, the iLO IP address is not displayed during POST.

Virtual Serial Port Log

Enables or disables logging of the Virtual Serial Port.

When this setting is enabled, Virtual Serial Port activity is logged to a 150-page circular buffer in the iLO memory. Use the CLI command `vsp log` to view the logged information. The Virtual Serial Port buffer size is 128 KB.

When this setting is disabled (default), Virtual Serial Port activity is not logged.

This feature is part of a licensing package.

XML Reply

Controls the XML object iLO provides in response to an anonymous request for basic system information. When this setting is enabled (default), other software is allowed to discover and identify an iLO system on the network. To view the XML response that iLO provides, click **View**.

When this option is disabled, iLO responds to requests with an empty XML object.

Serial Command Line Interface Status

Enables you to change the login model of the CLI feature through the serial port. The following settings are valid:

- **Enabled-Authentication Required** (default)—Enables access to the SMASH CLP command line from a terminal connected to the host serial port. Valid iLO user credentials are required.
- **Enabled-No Authentication**—Enables access to the SMASH CLP command line from a terminal connected to the host serial port. iLO user credentials are not required.
- **Disabled**—Disables access to the SMASH CLP command line from the host serial port. Use this option if you are planning to use physical serial devices.

Serial Command Line Interface Speed

Enables you to change the speed of the serial port for the CLI feature. The following speeds (in bits per second) are valid:

- **9600 (default)**
- **19200**
- **38400—**The iLO configuration options in the UEFI System Utilities do not support this value.
- **57600**
- **115200**

The serial port configuration must be set to no parity, eight data bits, and one stop bit (N/8/1) for correct operation.

Set this value to match the serial port speed configured in the UEFI System Utilities.

Minimum Password Length

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 characters long. The default value is 8.

Server Name

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.

You can enter a server name that is up to 49 bytes.

To force the browser to refresh and display the new value, save this setting, and then press F5.

Server FQDN/IP Address

Enables you to specify the server FQDN or IP address. You can assign this value manually, but it might be 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 and display the new value, save this setting, and then press F5.

Authentication Failure Logging

Enables you to configure logging criteria for failed authentications. The following settings are valid:

- **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 (default)**—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

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.

The default value is 10 seconds.

Authentication Failures Before Delay

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.

The default setting is 1, which means that a login delay is not imposed until the second failed login attempt.

iLO login with an SSH client

When you log in to iLO with an SSH client, the number of displayed login prompts matches the value of the **Authentication Failure Logging** option (3 if it is disabled). Your SSH client configuration might affect the number of prompts, because SSH clients also implement delays after a login failure.

For example, to generate an SSH authentication failure log with the default value (**Enabled-Every 3rd Failure**), if the SSH client is configured with the number of password prompts set to three, 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.

iLO Service Port

The Service Port is a USB port with the label iLO on the front of Express servers.

When you have physical access to a server, you can use the Service Port to do the following:

Download the Active Health System Log to a supported USB flash drive.

- When you use this feature, the connected USB flash drive is not accessible by the host operating system.
- Connect a client (such as a laptop) with a supported USB to Ethernet adapter to access the iLO web interface, remote console, CLI, or iLO RESTful API.

When you use the iLO Service Port:

- Actions are logged in the iLO Event Log.
- The server UID blinks to indicate the Service Port status.
  You can also retrieve the status by using a REST client and the iLO RESTful API.
- You cannot use the Service Port to boot any device within the server, or the server itself.
- You cannot access the server by connecting to the Service Port.
- You cannot access the connected device from the server.

Downloading the Active Health System Log through the iLO Service Port

Prerequisites

The **iLO Service Port** and **USB flash drives** options are enabled on the iLO Service Port page.

Procedure

1. Create a text file named command.txtwith the **required content** for downloading the Active Health System Log.
2. Save the file to the root directory of a **supported USB flash drive**.
3. Connect the USB flash drive to the iLO Service Port (the USB port labeled **iLO**, on the front of the server).

   The file system is mounted and the command.txtfile is read and executed.

   The iLO Service Port status changes to Busy, and the UID flashes at a rate of four medium flashes then off for one second.

   If the command is successful, the iLO Service Port status changes to Complete, and the UID flashes at a rate of one fast flash then off for three seconds.

   If the command is not successful, the iLO Service Port status changes to Error, and the UID flashes at a rate of eight fast flashes then off for one second.

   The file system is unmounted.
4. Remove the USB flash drive.

   The iLO Service Port status changes to Ready, and the UID stops flashing or flashes to indicate another state such as Remote Console access or a firmware update in progress.

Connecting a client to iLO through the iLO Service Port

Prerequisites

- The iLO Service Port and USB Ethernet adapters options are enabled on the iLO Service Port page.
- The client NIC is configured to support the Service Port feature.
- You have physical access to the server.

Procedure

1. Use a supported USB to Ethernet adapter to connect a client to the Service Port (the USB port labeled **iLO**, on the front of the server).

   The client NIC is assigned a link-local address. This process might take several seconds.

2. Connect to iLO through a browser, the CLI, or a scripting utility by using the following IPv4 address:

   169.254.1.2.

   The same IP address is used when you connect a client to any server through the Service Port. You cannot change this address.

   The Service Port status changes to Busy, and the UID flashes at a rate of four medium flashes then off for one second.

3. When you are finished, disconnect the client from the Service Port.

   The Service Port status changes to Ready, and the UID stops flashing or flashes to indicate a state such as Remote Console access or a firmware update in progress.

Configuring the iLO Service Port settings

Prerequisites

Configure iLO Settings privilege

Procedure

1. Click **Security** in the navigation tree, and then click the **iLO Service Port** tab.
2. Configure the following settings:
   - **iLO Service Port**
   - **USB flash drives**
   - **Require authentication**
   - **USB Ethernet adapters**
3. Click **Apply**.

   The updated settings take effect immediately, and information about the configuration change is logged in the iLO Event Log.

iLO Service Port options

- **iLO Service Port**—Allows you to enable or disable the iLO Service Port. The default setting is enabled. When this feature is disabled, you cannot configure the features in the **Mass Storage Options** or **Networking Options** sections on this page.
  Do not disable the iLO Service Port when it is in use. If you disable the port when data is being copied, the data might be corrupted.
- **USB flash drives**—Allows you to connect a USB flash drive to the iLO Service Port to download the Active Health System Log. The default setting is enabled.
  Do not disable this setting when the iLO Service Port is in use. If you disable USB flash drives when data is being copied, the data might be corrupted.
  If you insert a USB flash drive in the iLO Service Port when this setting is disabled, the device is ignored.
- **Require authentication**—Requires you to enter an iLO user name and password in the command.txtfile when you use the iLO Service Port to download the Active Health System Log. The default setting is disabled.
  User credentials are not required when the system maintenance switch is set to disable iLO security.
- **USB Ethernet adapters**—Allows you to use a USB to Ethernet adapter to connect a laptop to the iLO Service Port to access the Integrated Remote Console. The default setting is enabled.
  If you connect a laptop when this setting is disabled, the device is ignored.

Configuring a client to connect through the iLO Service Port

Procedure

1. Configure the client NIC to obtain an IPv4 autoconfiguration address automatically. For more information, see your operating system documentation.
2. Do one of the following:
   - Add a proxy exception. Use one of the following formats:
     - Edge, Chrome, Internet Explorer: 169.254.*
     - Firefox: 169.254.0.0/16
   - Disable web proxy settings on the client.

   For more information about proxy settings, see your operating system documentation.

iLO Service Port supported devices

Mass storage devices

The iLO Service Port supports USB keys with the following characteristics:

- High-speed USB 2.0 compatibility.
- FAT32 format, preferably with 512 byte blocks.
- One LUN.
- One partition with a maximum size of 127 GB and sufficient free space for the Active Health

System Log download.

- Valid FAT32 partition table.
- Not read-protected.
- Not bootable.

Mass storage devices are not supported on servers that do not have a NAND.

USB Ethernet adapters

The iLO Service Port supports USB Ethernet adapters that contain one of the following chips by ASIX Electronics Corporation:

- AX88772
- AX88772A
- AX88772B
- AX88772C

Sample text file for Active Health System Log download through iLO Service Port

When you use the iLO Service Port to download the Active Health System Log, you create a text file called `command.txt` and save the file to a **supported USB device**. When you connect the USB device to a server, the `command.txt` file runs and downloads the log file.

`command.txt` file template

Use the following example as a template for your `command.txt` file:

```
{
   "/ahsdata/" : {
     "POST" : {
       "downloadAll"  : "0",
       "from"         : "2016-08-25",
       "to"           : "2016-08-26",
       "case_no"      : "ABC0123XYZ",
       "UserName"     : "my_username",
       "Password"     : "my_password"
     }
   }
}
```

`command.txt` file parameters

You can customize the following values:

- `downloadAll`—Controls the download scope. To download the log for a range of dates, enter 0. To download the entire log, enter 1.
- `from`—The start date when you download the log for a range of dates.
- `to`—The end date when you download the log for a range of dates.
- `case_no` (optional)—The case number for an open support case. This value can be up to 14 characters long. If you enter this value, it is included in the downloaded file.
- `UserName`—If iLO is configured to require authentication for iLO Service Port actions on mass storage devices, enter an iLO account user name. A user name is not required when

the system maintenance switch is set to disable iLO security.

- `Password`—If iLO is configured to require authentication for iLO Service Port actions on mass storage devices, enter the password the iLO user name you entered. A password is not required when the system maintenance switch is set to disable iLO security.

`command.txt` file requirements

- The file must be in valid JSON format.
  NEC Corporation recommends using an online JSON formatter to verify the file syntax. A free utility is available at the following website: **http://www.freeformatter.com/json-formatter.html**.
- Do not include comments in the file.
- The text in the file is case-sensitive.
- The file supports plain text only. Do not create the file with an application that embeds additional formatting properties.

Administering SSH 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.

Authorizing a new SSH key by using the web interface

Prerequisites

Administer User Accounts privilege

Procedure

1. Generate a 2,048-bit DSA or RSA key by using ssh-keygen, puttygen.exe, or another SSH key utility.
2. Create the key.pubfile.
3. Click **Security** in the navigation tree, and then click the **Secure Shell Key** tab.
4. Select the check box to the left of the user to which you want to add an SSH key.
5. Click **Authorize New Key**.
6. Copy and paste the public key into the **Public Key Import Data** box.

   The key must be a 2,048-bit DSA or RSA key.
7. Click **Import Public Key**.

Authorizing a new SSH key by using the CLI

Prerequisites

Administer User Accounts privilege

Procedure

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. 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 to the `cd /Map1/Config1` directory.
6. Enter the following command: **`load sshkey type "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.
- `oemNEC_loadSSHkey` is case-sensitive.

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

```
oemNEC_loadSSHkey -source http://192.168.1.1/images/path/sshkey.pub
```

Deleting SSH keys

Use the following procedure to delete SSH keys from one or more user accounts.

When an SSH key is deleted from iLO, an SSH client cannot authenticate to iLO by using the corresponding private key.

Prerequisites

Administer User Accounts privilege

Procedure

1. Click **Security** in the navigation tree, and then click the **Secure Shell Key** tab.
2. In the **Authorized SSH Keys** list, select the check box to the left of one or more user accounts.
3. Click **Delete Selected Key(s)**.

   The selected SSH keys are removed from iLO.

SSH keys

When you add an SSH key to iLO, you paste the SSH key file into 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.

Supported SSH key formats

- RFC 4716
- OpenSSH key format
- iLO legacy format

Working with SSH keys

- The supported SSH key formats are supported with the iLO web interface and the CLI.
- 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 1,366 bytes or less. If the key is larger than 1,366 bytes, the authorization might fail. If a failure 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 iLO RESTful API to enter the public key, the user name is provided with the public key in the POST body.
- 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.

Supported SSH key format examples

RFC 4716

```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "Administrator"
AAAAB3NzaC1kc3MAAACAT27C04Dy2zr7fWhUL7TwHDKQdEdyuAlNLIivLFP3IoKZ
ZtzF0VInP5x2VFVYmTvdVjSupD92CTlxxAtarOPON2qUqoOajKRtBWLmxcfqsLCT3wI
3ldxQvPYnhTYyhPQuoeJ/vYhoam+y0zi8D03pDv9KaeNA3H/zEL5mf9Ktgts8/UA
AAAVAJ4efo8ffq0hg4a/eTGEuHPCb3INAAAAgCbnhADYXu+Mv4xuXccXWP0Pcj47 7YiZgos3jt/
Z0ezFX6/cN/RwwZwPC1HCsMuwsVBIqi7bvn1XczFPKOt06gVWcjFt eBY3/
bKpQkn61SGPC8AhSu8ui0KjyUZrxL4LdBrtp/K2+lm1fqXHnzDIEJ0RHg8Z
JazhY920PpkD4hNbAAAAgDN3lba1qFVl0UlRjj21MjXgr6em9TETSOO5b7SQ8hX/ Z/axobbrHCj/
2s66VA/554chkVimJT2IDRRKVkcV8OVC3nb4ckpfFEZvKkAWYaiF
DLqRbHhh4qyRBIfBKQpvvhDj1aecdFbaO2UvZltMir4n8/E0hh19nfi3tjXAtSTV
---- END SSH2 PUBLIC KEY ----
```

OpenSSH key format

```
ssh-dss AAAAB3NzaC1kc3MAAACAYjEd8Rk8HLCLqDIlI
+RkA1UXjVS28hNSk8YDljTaJpw1VOlBirrLGPdSt0avNSz0DNQuU7gTPfjj/8c
XyHe3y95Oa3Rics1fARyLiNFGqFjr7w2ByQuoYUaXBzzghIYMQcmpc/W/
kDMC0dVOf2XnfcLpcVDIm3ahVPRkxFV9WKkAAAAVAI 3J61F
+oVKrbNovhoHh8pFfUa9LAAAAgA8pU5/M9F0s5QxqkEWPD6+FVz9cZ0GfwIbiuAI/
9ARsizkbwRtpAlxAp6eDZKFvj3ZIy
NjcQODeYYqOvVU45AkSkLBMGjpF05cVtnWEGEvrW7mAvtG2zwMEDFSREw/V526/jR9TKzSNXTH/
wqRtTc/oLotHeyV2jFZFGpxD
OvNWAAAAgFf6pvWaco3CDELmH0jT3yUkRSaDztpqtoo4D7ev7VrNPPjnKKKmpzHPmAKRxz3g5S80S
fWSnWM3n/pekBa9QI9lH1r 3Lx4JoOVwTpkbwb0by4eZ2cqDw20KQ0A5J84iQE9TbPNecJ0HJtZH/
K8YnFNwwYy2NSJyjLwA0TSmQEOW Administrator
```

iLO legacy format

This format must be one line between the BEGIN SSH KEY and END SSH KEY text.

```
-----BEGIN SSH KEY-----
ssh-dss AAAAB3NzaC1kc3MAAACBANA45qXo9cM1asav6ApuCREt1UvP7qcMbw
+sTDrx9lV22XvonwijdFiOM/0VvuzVhM9oKdGMC7sCGQr
FV3zWDMJcIb5ZdYQSDt44X6bvlsQcAR0wNGBN9zHL6YsbXvNAsXN7uBM7jXwHwrApWVuGAI0QnwUY
vN/dsE8fbEYtGZCRAAAAFQ
DofA47q8pIRdr6epnJXSNrwJRvaQAAAIBY7MKa2uH82I0KKYTbNMi0o5mOqmqy+tg5s9GC+HvvYy/
S7agpIdfJzqkpHF5EPhm0j KzzVxmsanO+pjju7lrE3xUxojevlokTERSCM xLa
+OVVbNcgTe0xpvc/cF6ZvsHs0UWz6gXIMCQ9Pk118VMOw/tyLp42YXOaLZzG
fi5pKAAAAIEAl7FsO7sDbPj02a5jO3qFXa762lWvu5iPRZ9cEt5WJEYwMO/
ICaJVDWVOpqF9spoNb53Wl1pUARJg1ss8Ruy7YBv 8Z1urWWAF3fYy7R/
SlQqrsRYDPLM5eBkkLO28B8C6++HjLuc+hBvj90tsqeNVhpCfO9qrjYomYwnDC4m1IT4= ASmith
-----END SSH KEY-----
```

Administering SSL certificates

SSL protocol is a standard for encrypting data so that it cannot be viewed or modified while in transit on the network. This protocol uses a key to encrypt and decrypt the data. Generally, the longer the key, the better the encryption.

A certificate is a small data file that connects an SSL key to a server. The certificate contains the server name and the server public key. Only the server has the corresponding private key, and this is how it 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.

By default, iLO creates a self-signed certificate for use in SSL connections. This certificate enables iLO to work without additional configuration steps.

IMPORTANT:

Using a self-signed certificate is less secure than importing a trusted certificate. NEC Corporation recommends importing a trusted certificate to protect the security of the iLO processor.

Viewing SSL certificate information

Procedure

To view certificate information, click Security in the navigation tree, and then click the **SSL Certificate** tab.

SSL certificate details

- **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 an SSL certificate

iLO allows you to create a Certificate Signing Request that you can send to a Certificate Authority to obtain a trusted SSL certificate to import into iLO.

An SSL certificate works only with the keys generated with its corresponding CSR. If iLO is reset to the factory default settings, 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 a CA.

Prerequisites

Configure iLO Settings privilege

Procedure

1. **Obtain a trusted certificate from a Certificate Authority (CA).**
2. **Import the trusted certificate into iLO.**

Obtaining a trusted certificate from a CA

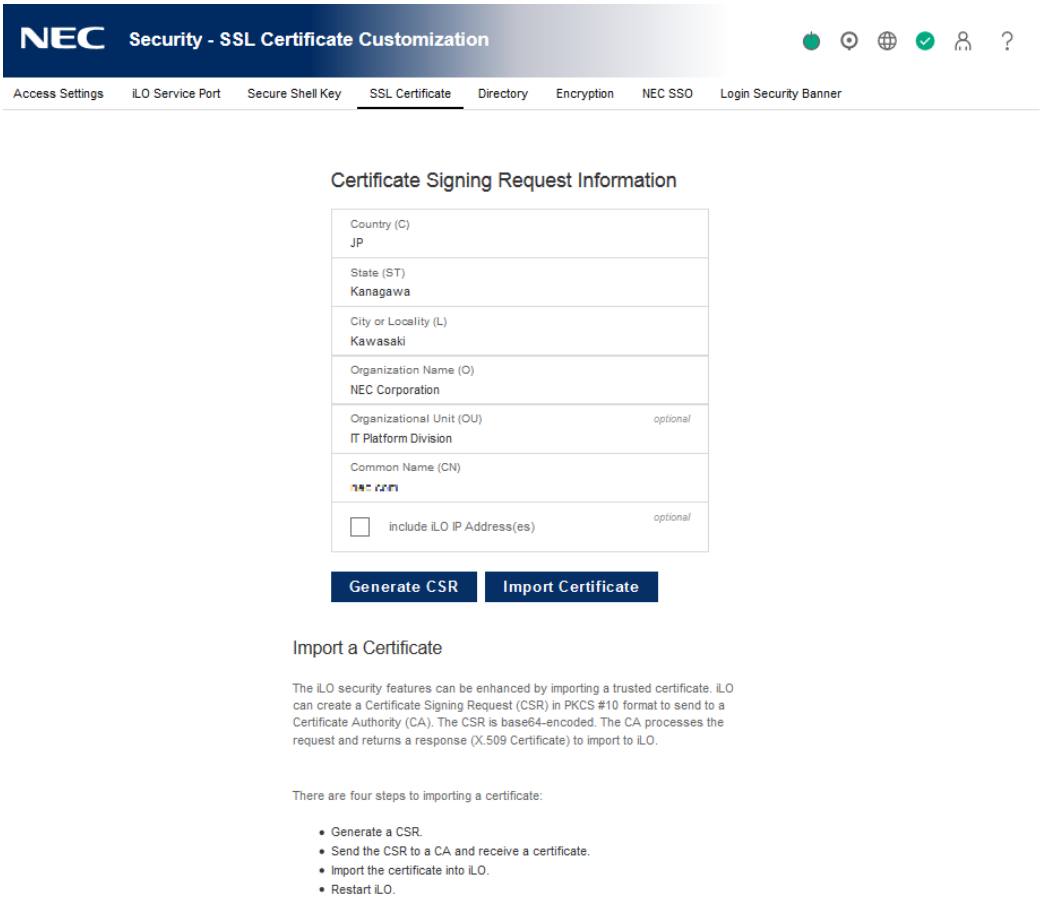
Prerequisites

Configure iLO Settings privilege

Procedure

1. Click **Security** in the navigation tree, and then click the **SSL Certificate** tab.

2. Click **Customize Certificate**.



3. On the **SSL Certificate Customization** page, enter the following:
   - **Country (C)**
   - **State (ST)**
   - **City or Locality (L)**

- **Organization Name (O)**
- **Organizational Unit (OU)**
- **Common Name (CN)**

For more information, see **CSR input details**.

4. If you want the iLO IP addresses included in the CSR, select the **include iLO IP Address(es)** check box.

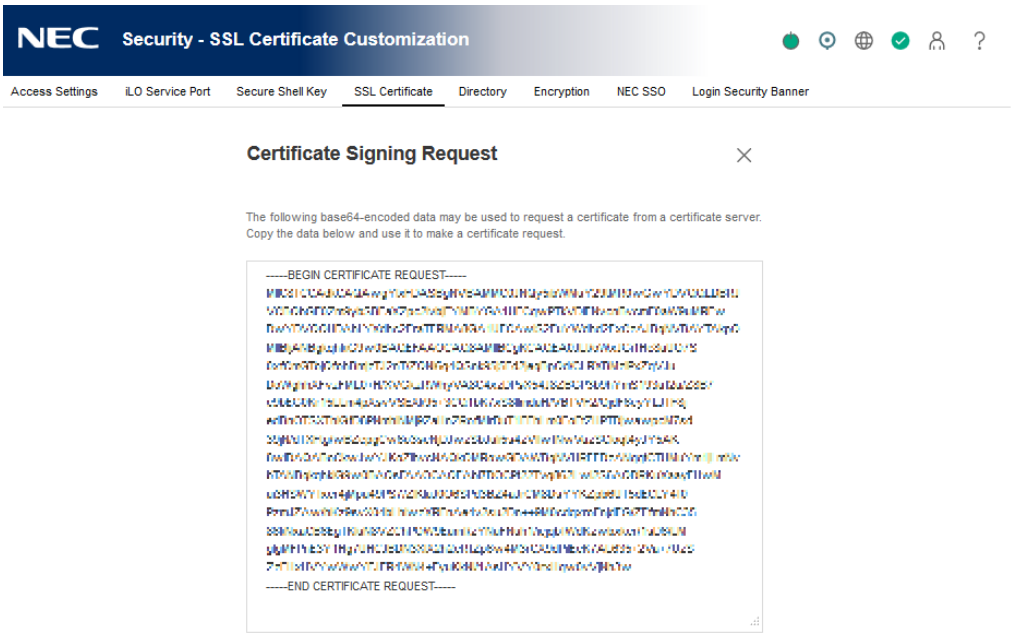
   This option is disabled by default because some CAs cannot use this input.

5. Click **Generate CSR**.

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

6. 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. The generated CSR is held in memory until a new CSR is generated, iLO is reset to the factory default settings, or a certificate is imported.



7. Select and copy the CSR text.
8. Open a browser window and navigate to a third-party CA.
9. 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 necessary, enter the iLO DNS short name and IP address in the **Additional Attributes** box by using the following syntax: san:dns=<IP address>&dns=<server name>.

   The CA generates a certificate in PKCS #10 format.

10. After you obtain the certificate, make sure that:
    - The CN matches the iLO FQDN. This value is listed as the **iLO Hostname** on the **Overview** page.
    - The certificate is a Base64-encoded X.509 certificate.
    - The first and last lines are included in the certificate.

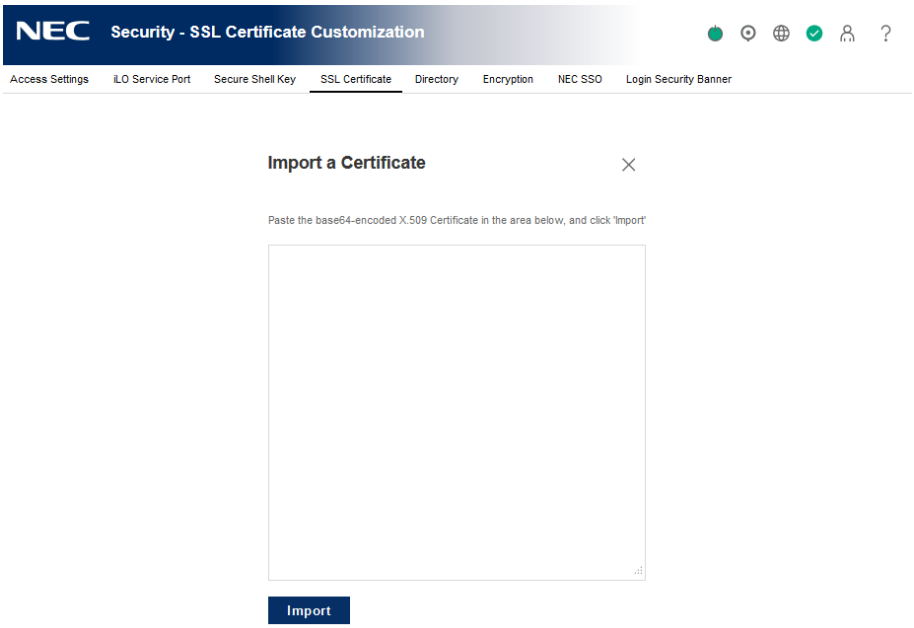
Importing a trusted certificate

Prerequisites

Configure iLO Settings privilege

Procedure

1. Click **Security** in the navigation tree, and then click the **SSL Certificate** tab.



2. Click **Customize Certificate**.
3. Click **Import Certificate**.
4. In the **Import Certificate** window, paste the certificate into the text box, and then click **Import**.

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

CSR input details

Enter the following details when you create a CSR:

- **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.

  To enable iLO to enter the FQDN into the CSR, configure the **Domain Name** on the **Network General Settings** page.

Directory authentication and authorization

The iLO firmware supports Kerberos authentication with Microsoft Active Directory. It also supports directory integration with an Active Directory or OpenLDAP directory server.

When you configure directory integration, you can use the schema-free option. The iLO firmware connects to directory services by using SSL connections to the directory server LDAP port.

You can enable the directory server certificate validation option for schema-free by importing a CA certificate. This feature ensures that iLO connects to the correct directory server during LDAP authentication.

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

Prerequisites for configuring authentication and directory server settings

Procedure

1. Verify that your iLO user account has the Configure iLO Settings privilege.
2. Install an iLO license that supports this feature.
3. Configure your environment to support Kerberos authentication or directory integration.
4. The Kerberos keytab file is available (Kerberos authentication only).

Configuring Kerberos authentication settings in iLO

Prerequisites

Your environment meets the **prerequisites** for using this feature.

Procedure

1. Click **Security** in the navigation tree, and then click the **Directory** tab.
2. Enable **Kerberos Authentication**.
3. Set **Local User Accounts** to enabled 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**—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 Key Distribution Center (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

Prerequisites

Your environment meets the **prerequisites** for using this feature.

Procedure

1. Click **Security** in the navigation tree, and then click the **Directory** tab.
2. Select **Use Directory Default Schema** from the **LDAP Directory Authentication** menu.
3. Set **Local User Accounts** to enabled if you want to use local user accounts at the same time as directory integration.
4. OpenLDAP users only: Enable **Generic LDAP**.
5. This setting is available only if **Use Directory Default Schema** is selected.
6. Enter the FQDN or IP address of a directory server in the **Directory Server Address** box.
7. Enter the directory server port number in the **Directory Server LDAP Port** box.
8. Optional: Import a new CA certificate.
   a. Click **Import** in the **Certificate Status** box.
   b. Paste the Base64-encoded X.509 certificate data into the **Import Certificate** window, and then click **Import**.
9. Optional: Replace an existing CA certificate.
   a. Click **View** in the **Certificate Status** text box.
   b. Click **New** in the **Certificate Details** window.
   c. Paste the Base64-encoded X.509 certificate data into the **Import Certificate** window,

and then click **Import**.

10. Enter valid search contexts in one or more of the **Directory User Context** boxes.
11. Click **Apply Settings**.
12. To **test the communication** between the directory server and iLO, click **Test Settings**.
13. Optional: To **configure directory groups**, click **Administer Groups** to navigate to the **Directory Groups** page.

Schema-free directory settings

- **Generic LDAP**—Specifies that this configuration uses the OpenLDAP supported BIND method.
- **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.
  NEC Corporation 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.
- **Certificate Status**—Specifies whether a directory server CA certificate is loaded.
  If the status is **Loaded**, click **View** to display the CA certificate details. If no CA certificate is loaded, the status **Not Loaded** is displayed. iLO supports SSL certificates up to 4 KB in size.

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 IM, Services, and Training departments manage a system, the following search contexts 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 IMorganizational unit and the Trainingorganizational 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.

- **Example 4 (OpenLDAP user)**—If a user has the DN UID=user,ou=people,o=ab, and you enter the search context **ou=people,o=ab**, the user can log in as **user**instead of entering the DN.

Directory Server CA Certificate

During LDAP authentication, iLO validates the directory server certificate if the CA certificate is already imported. For successful certificate validation, make sure that you import the correct CA certificate. If certificate validation fails, iLO login is denied and an event is logged. If no CA certificate is imported, the directory server certificate validation step is skipped.

To verify SSL communication between the directory server and iLO, click Test Settings.

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:

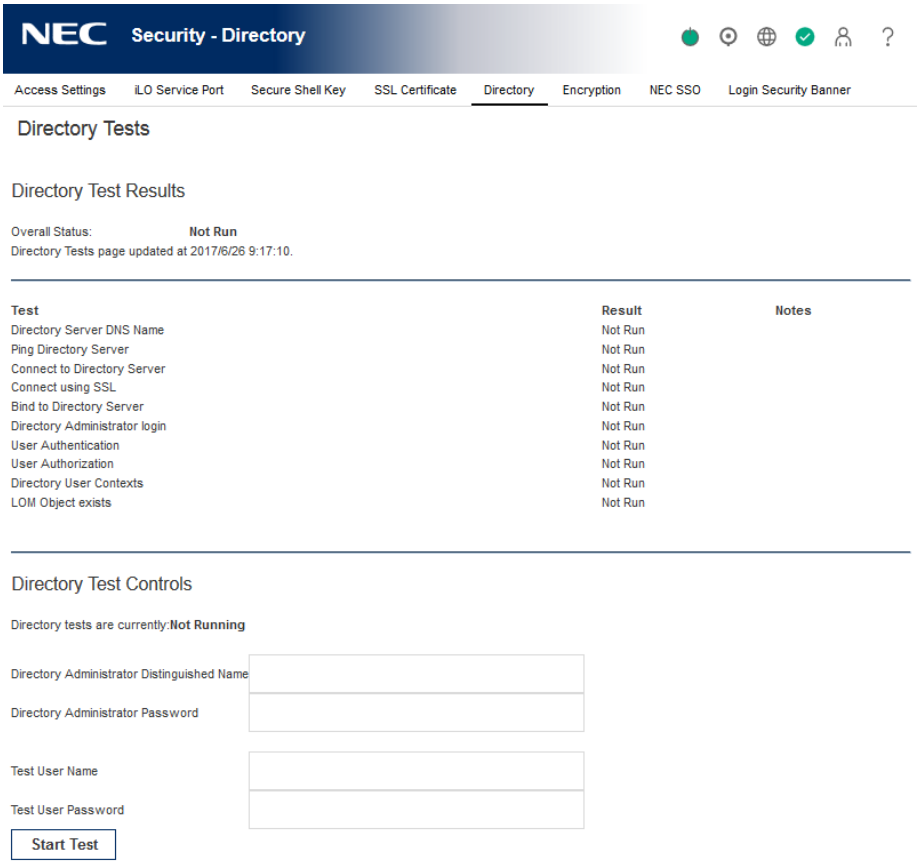
- When local user accounts are enabled, configured users can log in by using locally stored user credentials.
- When local accounts are disabled, user access is limited to valid directory credentials.
- Do not disable local user access until you have validated access through Kerberos or a directory.
- When you use Kerberos authentication or directory integration, NEC Corporation 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.

Running 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 the directory tests are started.

Procedure

1. Click **Security** in the navigation tree, and then click the **Directory** tab.



2. At the bottom of the **Directory** page, click **Test Settings**.

   iLO displays the results of a series of simple tests designed to validate the directory settings. After your directory settings are configured correctly, you do not need to rerun these tests. The **Directory Tests** page does not require you to log in as a directory user.

3. In the **Directory Test Controls** section, enter the DN and password of a directory administrator in the **Directory Administrator Distinguished Name** and **Directory Administrator Password** boxes.

   NEC Corporation recommends that you use the same credentials that you used when creating the iLO objects in the directory. iLO does not store these credentials; they are used to verify the iLO object and user search contexts.

4. In the **Directory Test Controls** section, enter a test user name and password in the **Test User Name** and **Test User Password** boxes.

5. Click **Start Test**.

   Several tests begin in the background, starting with a network ping of the directory user by establishing an SSL connection to the server and evaluating user privileges.

   While the tests are running, the page refreshes periodically. You can stop the tests or manually refresh the page at any time.

Directory test input values

Enter the following values when you run directory tests:

- **Directory Administrator Distinguished Name**—Searches the directory for iLO objects, roles, and search contexts. This user must have the right to read the directory.
- **Directory Administrator Password**—Authenticates the directory administrator.
- **Test User Name** and **Test User Password**—Tests login and access rights to iLO. This name does not need to be fully distinguished because user search contexts can be applied. This user must be associated with a role for this iLO.

Typically, this account is used to access the iLO processor being tested. It can be the directory administrator account, but the tests cannot verify user authentication with a superuser account. iLO does not store these credentials.

Directory test status values

iLO displays the following status values for directory tests:

- **In Progress**—Indicates that directory tests are currently being performed in the background. Click **Stop Test** to cancel the current tests, or click **Refresh** to update the contents of the page with the latest results. Using the **Stop Test** button might not stop the tests immediately.
- **Not Running**—Indicates that directory tests are current, and that you can supply new parameters to run the tests again. Use the **Start Test** button to start the tests and use the current test control values. Directory tests cannot be started after they are already in progress.
- **Stopping**—Indicates that directory tests have not yet reached a point where they can stop. You cannot restart tests until the status changes to **Not Running**. Use the **Refresh** button to determine whether the tests are complete.

Directory test results

The **Directory Test Results** section shows the directory test status with the date and time of the last update.

- **Overall Status**—Summarizes the results of the tests.
  - **Not Run**—No tests were run.
  - **Inconclusive**—No results were reported.
  - **Passed**—No failures were reported.
  - **Problem Detected**—A problem was reported.
  - **Failed**—A specific subtest failed. To identify the problem, check the onscreen log.
  - **Warning**—One or more of the directory tests reported a **Warning** status.
- **Test**—The name of each test.
- **Result**—Reports status for a specific directory setting or an operation that uses one or more directory settings. These results are generated when a sequence of tests is run. The results

stop when the tests run to completion, when a test failure prevents further progress, or when the tests are stopped. Test results follow:
    - **Passed**—The test ran successfully. If more than one directory server was tested, all servers that ran this test were successful.
    - **Not Run**—The test was not run.
    - **Failed**—The test was unsuccessful on one or more directory servers. Directory support might not be available on those servers.
    - **Warning**—The test ran and reported a warning condition, for example, a certificate error. Check the **Notes** column for suggested actions to correct the warning condition.
- **Notes**—Indicates the results of various phases of the directory tests. The data is updated with failure details and information that is not readily available, like the directory server certificate subject and which roles were evaluated successfully.

iLO directory tests

Directory Server DNS Name

If the directory server is defined in FQDN format (directory.company.com), iLO resolves the name from FQDN format to IP format, and queries the configured DNS server.

If the test is successful, iLO obtained an IP address for the configured directory server. If iLO cannot obtain an IP address for the directory server, this test and all subsequent tests fail.

If the directory server is configured with an IP address, iLO skips this test.

Ping Directory Server

iLO initiates a ping to the configured directory server.

The test is successful if iLO receives the ping response; it is unsuccessful if the directory server does not reply to iLO.

If the test fails, iLO will continue with the subsequent tests.

Connect to Directory Server

iLO attempts to negotiate an LDAP connection with the directory server. If the test is successful, iLO was able to initiate the connection.

If the test fails, iLO was not able to initiate an LDAP connection with the specified directory server. Subsequent tests will stop.

Connect using SSL

iLO initiates SSL handshake and negotiation and LDAP communications with the directory server through port 636.

If the test is successful, the SSL handshake and negotiation between iLO and the directory server were successful.

LDAP server certificate validation errors are reported in the results for this test.

Bind to Directory Server

This test binds the connection with the user name specified in the test controls. If no user is specified, iLO does an anonymous bind.

If the test is successful, the directory server accepted the binding.

Directory Administrator Login

If **Directory Administrator Distinguished Name** and **Directory Administrator Password** were specified, iLO uses these values to log in to the directory server as an administrator. Providing these values is optional.

User Authentication

iLO authenticates to the directory server with the specified user name and password. If the test is successful, the supplied user credentials are correct.

If the test fails, the user name and/or password is incorrect.

User Authorization

This test verifies that the specified user name is part of the specified directory group, and is part of the directory search context specified during directory services configuration.

Directory User Contexts

If **Directory Administrator Distinguished Name** was specified, iLO tries to search the specified context.

If the test is successful, iLO found the context by using the administrator credentials to search for the container in the directory.

User login is the only way that you can test contexts that begin with the @ symbol. A failure indicates that the container could not be located.

LOM Object Exists

This test searches for the iLO object in the directory server by using the **LOM Object Distinguished Name** configured on the **Security** - **Directory** page.

If the test is successful, iLO found the object that represents itself.

Configuring encryption settings

IMPORTANT:

For iLO 5 Firmware Version 1.15 Aug 17 2017 or earlier：Does not use encryption settings and leave it as default. If you change encryption settings, Express report service and Product Info Collection Utility etc. will not work.

SSH cipher, key exchange, and MAC support

iLO provides enhanced encryption through the SSH port for secure CLP transactions. Based on the configured security state, iLO supports the following:

- AES256-CBC, AES128-CBC, 3DES-CBC, and AES256-CTR ciphers
- diffie-hellman-group14-sha1 and diffie-hellman-group1-sha1 key exchange
- hmac-sha1 or hmac-sha2-256 MACs

SSL cipher and MAC support

SSL cipher and MAC support

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

When you log in to iLO through a browser, the browser and iLO negotiate a cipher setting to use during the session. The negotiated cipher is displayed on the **Encryption** page.

Based on the configured security state, iLO supports the following:

Production

- 256-bit AES-GCM with RSA, ECDH, and an AEAD MAC (ECDHE-RSA-AES256-GCM-SHA384)
- 256-bit AES with RSA, ECDH, and a SHA384 MAC (ECDHE-RSA-AES256-SHA384)
- 256-bit AES with RSA, ECDH, and a SHA1 MAC (ECDHE-RSA-AES256-SHA)
- 256-bit AES-GCM with RSA, DH, and an AEAD MAC (DHE-RSA-AES256-GCM-SHA384)
- 256-bit AES with RSA, DH, and a SHA256 MAC (DHE-RSA-AES256-SHA256)
- 256-bit AES with RSA, DH, and a SHA1 MAC (DHE-RSA-AES256-SHA)
- 256-bit AES-GCM with RSA, and an AEAD MAC (AES256-GCM-SHA384)
- 256-bit AES with RSA, and a SHA256 MAC (AES256-SHA256)
- 256-bit AES with RSA, and a SHA1 MAC (AES256-SHA)
- 128-bit AES-GCM with RSA, ECDH, and an AEAD MAC (ECDHE-RSA-AES128-GCM-SHA256)
- 128-bit AES with RSA, ECDH, and a SHA256 MAC (ECDHE-RSA-AES128-SHA256)
- 128-bit AES with RSA, ECDH, and a SHA1 MAC (ECDHE-RSA-AES128-SHA)
- 128-bit AES-GCM with RSA, DH, and an AEAD MAC (DHE-RSA-AES128-GCM-SHA256)
- 128-bit AES with RSA, DH, and a SHA256 MAC (DHE-RSA-AES128-SHA256)

- 128-bit AES with RSA, DH, and a SHA1 MAC (DHE-RSA-AES128-SHA)
- 128-bit AES-GCM with RSA, and an AEAD MAC (AES128-GCM-SHA256)
- 128-bit AES with RSA, and a SHA256 MAC (AES128-SHA256)
- 128-bit AES with RSA, and a SHA1 MAC (AES128-SHA)
- 168-bit 3DES with RSA, ECDH, and a SHA1 MAC (ECDHE-RSA-DES-CBC3-SHA)
- 168-bit 3DES with RSA, DH, and a SHA1 MAC (EDH-RSA-DES-CBC3-SHA)
- 168-bit 3DES with RSA, and a SHA1 MAC (DES-CBC3-SHA)

NEC SSO

NEC SSO enables you to browse directly from an NEC SSO-compliant application to iLO, bypassing an intermediate login step.

To use this feature:

- You must have a supported version of an NEC SSO-compliant application.
- Configure iLO to trust the SSO-compliant application.

There is no application currently compatible with NEC SSO.

Configuring the Login Security Banner

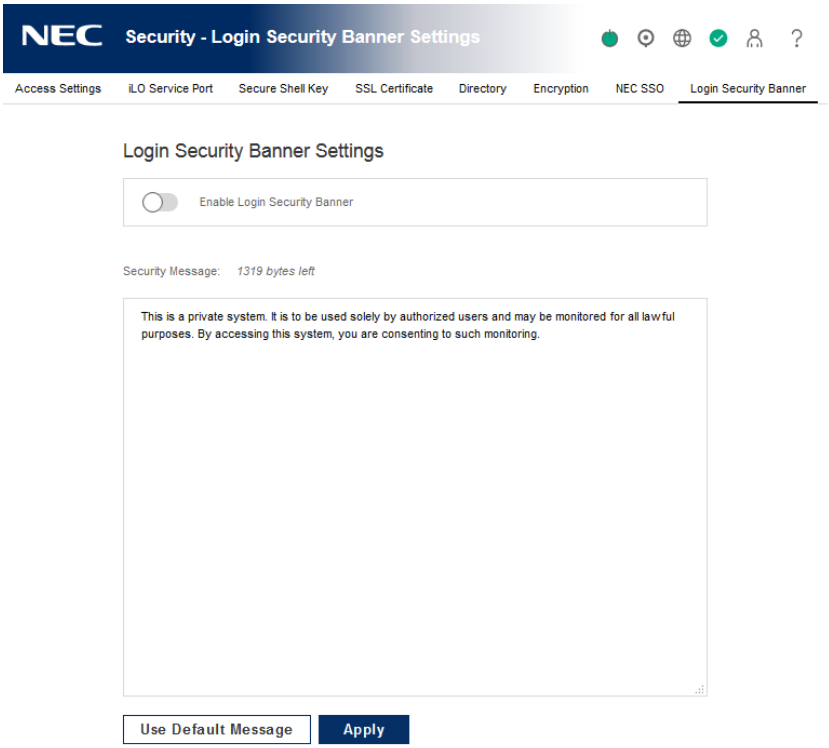
The Login Security Banner feature allows you to configure the security banner displayed on the iLO login page. For example, you could enter a message with contact information for the owner of the server.

Prerequisites

Configure iLO Settings privilege

Procedure

1. Click **Security** in the navigation tree, and then click **Login Security Banner**.



2. Enable the **Enable Login Security Banner** setting.

   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.

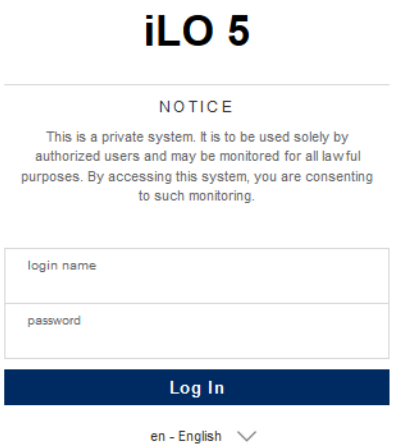
   The byte counter above the text box indicates the remaining number of bytes allowed for the message. The maximum is 1,500 bytes.

   TIP:

   To restore the default text, click **Use Default Message**.

4. Click **Apply**.

5. The security message is displayed at the next login.



iLO security with the system maintenance switch

The iLO security setting on the system maintenance switch provides emergency access to an administrator who has physical control over the server system board. Disabling iLO security allows login access with all privileges, without a user ID and password, provided that iLO is configured to use the **Production** security state.

The system maintenance switch is inside the server and cannot be accessed without opening the server enclosure. When you work with the system maintenance switch, ensure that the server is powered off and disconnected from the power source. Set the switch to enable or disable iLO security, and then power on the server. For detailed information about enabling and disabling iLO security with the system maintenance switch, see the maintenance and service guide for your server.

The system maintenance switch position that controls iLO security is sometimes called the iLO Security Override switch.

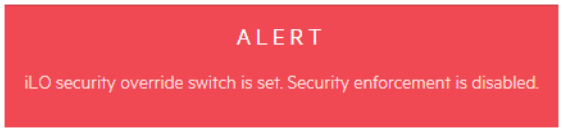
Reasons to disable iLO security

- 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 the ROM-based configuration utility is disabled.
- The iLO NIC is turned off, and it is not possible or convenient to run the ROM-based configuration utility to turn it back on.
- Only one user name is configured, and the password is forgotten.

Effects of disabling iLO security

When iLO is set to use the Production security state, and you disable iLO security:

- All security authorization verifications are disabled.
- If the host server is reset, the ROM-based configuration utility runs.
- iLO is not disabled and might be displayed on the network as configured.
- If iLO functionality is disabled, iLO does not log out active users and complete the disable process until the power is cycled on the server.
- A warning message is displayed on iLO web interface pages, indicating that iLO security is disabled:



- An iLO log entry is added to record the iLO security change.
- If an SNMP Alert Destination is configured, an SNMP alert is sent when iLO starts after you use the system maintenance switch to enable or disable iLO security.

15. Configuring iLO management settings

Agentless Management and AMS

Agentless Management uses out-of-band communication for increased security and stability. With Agentless Management, health monitoring and alerting is built into the system and begins working the moment a power cord is connected to the server. This feature runs on the iLO hardware, independent of the operating system and processor.

To collect information from devices and components that cannot communicate directly with iLO, install the Agentless Management Service (AMS).

Table 2: Information provided by Agentless Management with and without AMS

Component	Agentless Management without AMS	Additional information provided when AMS is installed
Server health	• Fans • Temperatures • Power supplies • Memory • CPU • NVDIMM	• N/A
Storage	• Smart Array • SMART Drive Monitoring (connected to Smart Array) • Internal and external drives connected to Smart Array • Smart Storage battery monitoring	• SMART Drive Monitoring (connected • to Smart Array, Smart HBA, and AHCI) • iSCSI (Windows) • NVMe drives
Network	• MAC addresses for embedded NICs that support NC-SI over MCTP • Physical link connectivity and link up/ link down traps for NICs that support NC-SI over MCTP • Fibre Channel adapters that	• MAC and IP address for standup and embedded NICs • Link up/link down traps • NIC teaming and bridging information (Windows and Linux) • Supported Fibre Channel adapters
Other	• iLO data • Firmware inventory • Device inventory	• OS information (host SNMP MIB) • Driver/service inventory • Logging events to OS logs[1, 2]
Prefailure warranty alerts	• Memory • Drives (physical and logical)	• N/A

[1] *AMS-based OS logging for Linux (`/var/log/messages`).*

[2] *Smart Array logging is supported.*

Configuring SNMP settings

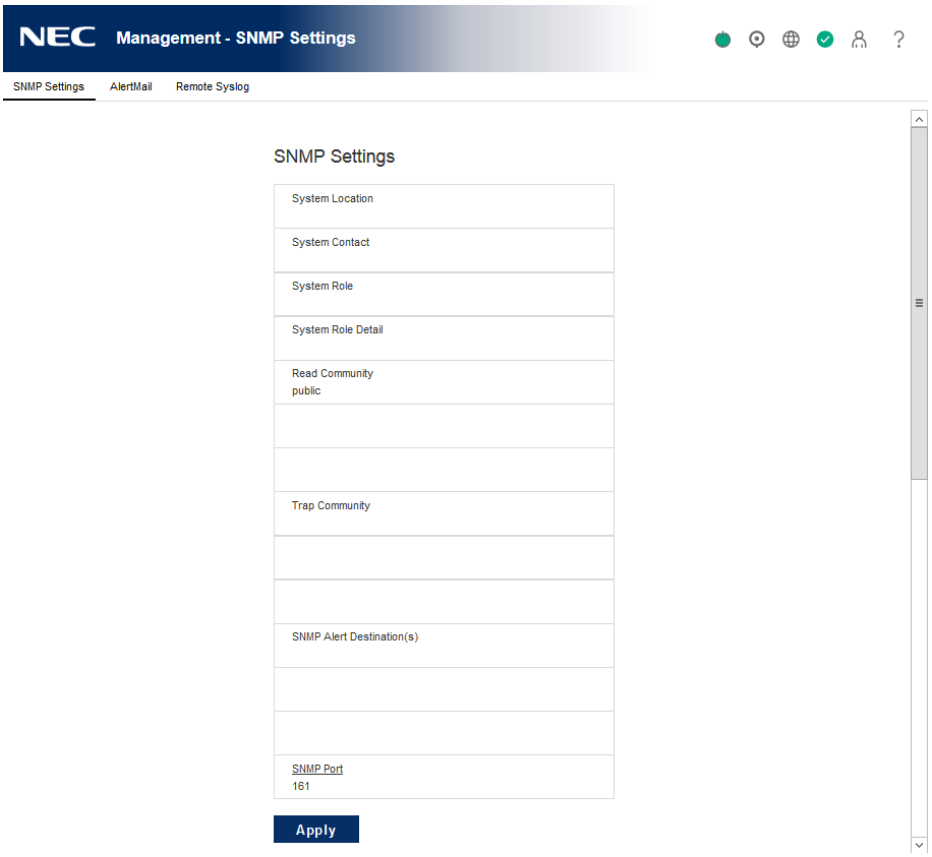
The settings you configure on this page are for the default Agentless Management and AMS configuration. If you use the System Management Assistant and an OS-based SNMP service, similar settings must be configured on the host.

Prerequisites

Configure iLO Settings privilege

Procedure

1. Click **Management** in the navigation tree. The **SNMP Settings** page is displayed.



2. Enter the following values in the **SNMP Settings** section:
   - **System Location**
   - **System Contact**
   - **System Role**
   - **System Role Detail**
   - **Read Community**
   - **Trap Community**
   - **SNMP Alert Destination(s)**

   The **SNMP Port** value is read-only on this page. You can change this value on the **Access Settings** page.

3. To save the configuration, click **Apply**.

SNMP options

- **System Location**—A string of up to 49 characters that specifies the physical location of the server.
- **System Contact**—A string of up to 49 characters that specifies the system administrator or server owner. The string can include a name, email address, or phone number.
- **System Role**—A string of up to 64 characters that describes the server role or function.
- **System Role Detail**—A string of up to 512 characters that describes specific tasks that the server might perform.
- **Read Community**—The configured SNMP read-only community string.
  The following formats are supported:
  - A community string (for example, public).
  - A community string followed by an IP address or FQDN (for example, public 192.168.0.1).
    Use this option to specify that SNMP access will be allowed from the specified IP address or FQDN.
    You can enter an IPv4 address, an IPv6 address, or an FQDN.
- **Trap Community**—The configured SNMP trap community string.
- **SNMP Alert Destination(s)**—The IP addresses or FQDNs of up to three remote management systems that will receive SNMP alerts from iLO.
  When SNMP Alert Destinations are configured using FQDNs, and DNS provides both IPv4 and IPv6 addresses for the FQDNs, iLO sends traps to the address specified by the **iLO Client Applications use IPv6 first** setting on the **IPv6** page. If **iLO Client Applications use IPv6 first** is enabled, traps will be sent to IPv6 addresses (when available). When **iLO Client Applications use IPv6 first** is disabled, traps will be sent to IPv4 addresses (when available).
- **SNMP Port**—The port used for SNMP communications. This value is read-only, but can be modified on the **Access Settings** page.
  To navigate to the **Access Settings** page, click the **SNMP Port** link. For more information, see **Access options**.

SNMPv3 authentication

The following SNMPv3 security features enable secure data collection from iLO SNMP agents:

- Message integrity prevents tampering during packet transmission.
- Encryption prevents packet snooping.
- Authentication ensures that packets are from a valid source.

By default, SNMPv3 supports the User-based Security Model. With this model, security parameters are configured at both the SNMP agent level (iLO) and the SNMP manager level (client system). Messages exchanged between the SNMP agent and the manager are subject to a data integrity check and data origin authentication.

iLO supports three user profiles in which you can set the SNMPv3 USM parameters.

Configuring SNMPv3 users

Prerequisites

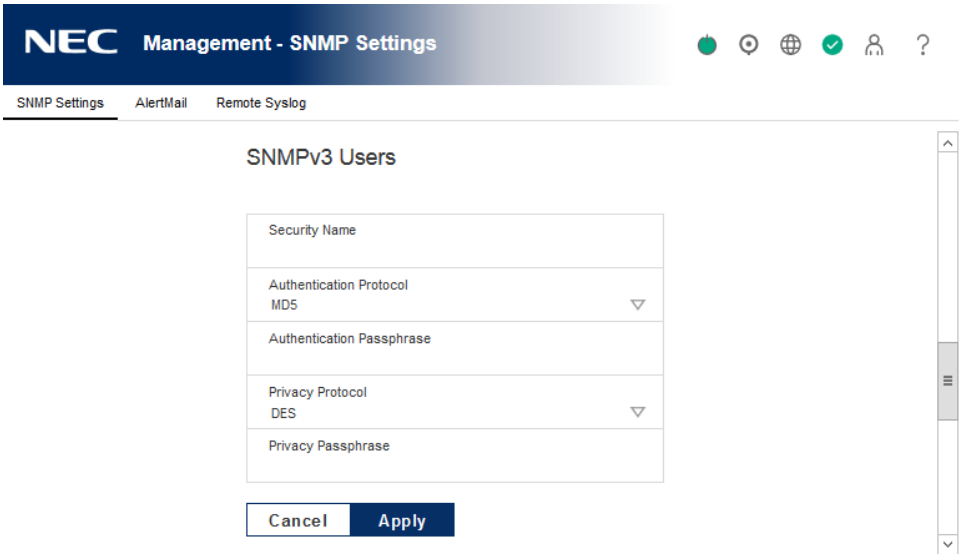
Configure iLO Settings privilege

Procedure

1. Click **Management** in the navigation tree. The **SNMP Settings** page is displayed.
2. Select a user profile in the **SNMPv3 Users** section, and then click **Edit**.

   If user profiles are not configured, the **Security Name** column displays each profile with the value **unset**.

   The iLO web interface updates to show the SNMPv3 user options.



3. Enter the following values:
   - **Security Name**
   - **Authentication Protocol**
   - **Authentication Passphrase**
   - **Privacy Protocol**
   - **Privacy Passphrase**
4. To save the user profile, click **Apply**.

SNMPv3 user options

- **Security Name**—The user profile name. Enter an alphanumeric string of 1 to 32 characters.
- **Authentication Protocol**—Sets the message digest algorithm to use for encoding the authorization passphrase. The message digest is calculated over an appropriate portion of an SNMP message, and is included as part of the message sent to the recipient. Select **MD5** or **SHA**.
- **Authentication Passphrase**—Sets the passphrase to use for sign operations. Enter a value of 8 to 49 characters.
- **Privacy Protocol**—Sets the encryption algorithm to use for encoding the privacy passphrase. A portion of an SNMP message is encrypted before transmission. Select **AES** or

DES.

- **Privacy Passphrase**—Sets the passphrase used for encrypt operations. Enter a value of 8 to 49 characters.

Deleting an SNMPv3 user profile

Prerequisites

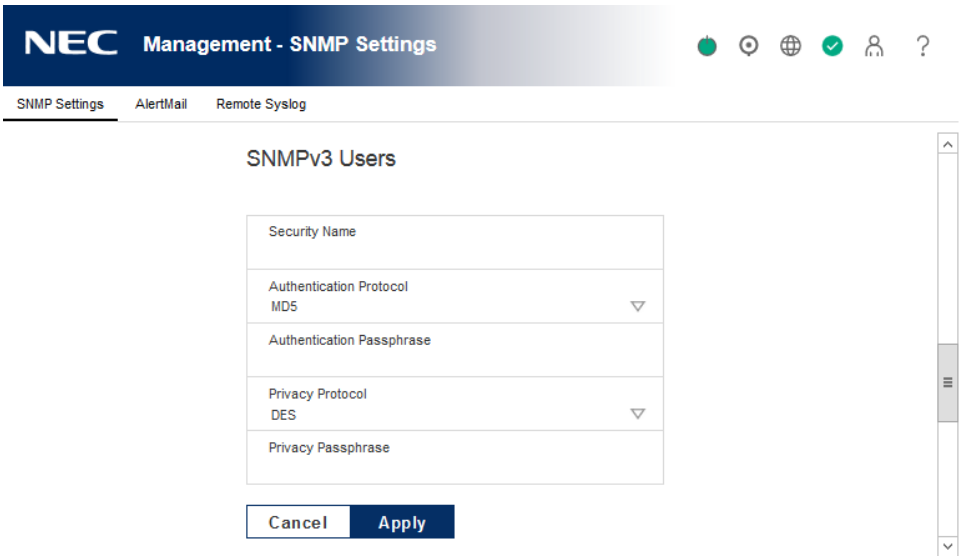
Configure iLO Settings privilege

Procedure

1. Click **Management** in the navigation tree.

   The **SNMP Settings** page is displayed.

2. Scroll to the **SNMPv3 Users** section.



3. Select a user profile in the **SNMPv3 Users** section, and then click **Delete**.
4. When prompted to confirm the request, click **OK**.

Configuring the SNMPv3 Engine ID

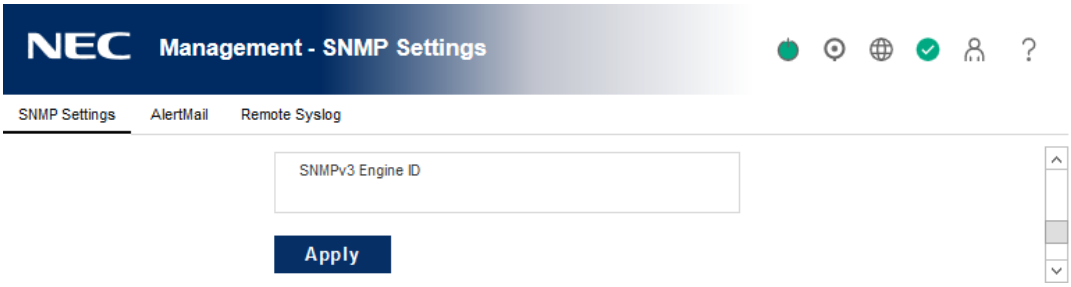
The **SNMPv3 Engine ID** sets the unique identifier of an SNMP engine belonging to an SNMP agent entity.

Prerequisites

Configure iLO Settings privilege

Procedure

1. Click **Management** in the navigation tree. The **SNMP Settings** page is displayed.



2. Enter a value in the **SNMPv3 Engine ID** box.
3. This value must be a hexadecimal string of 6 to 32 characters, not counting the preceding 0x, and must be an even number of characters (for example, 0x01020304abcdef).
4. Click **Apply**.

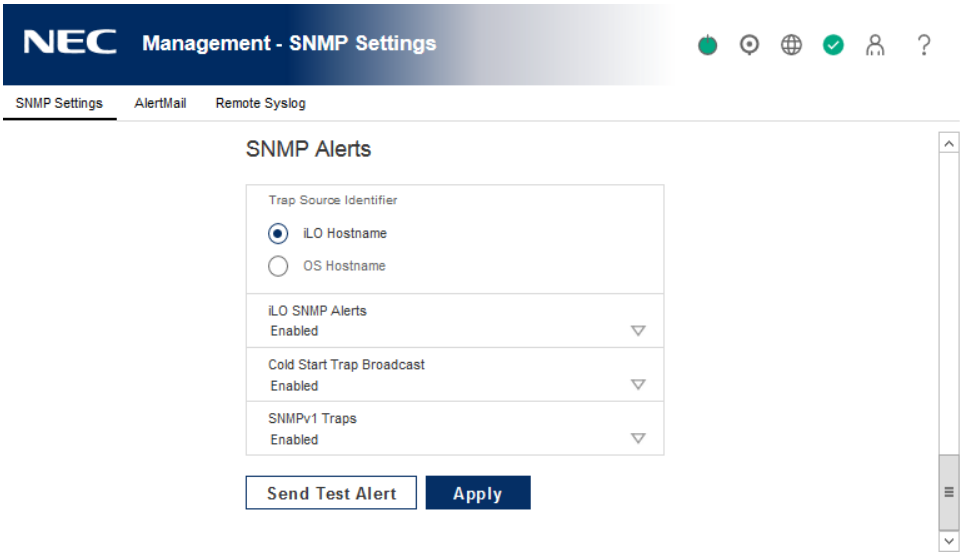
Configuring SNMP alerts

Prerequisites

Configure iLO Settings privilege

Procedure

1. Click **Management** in the navigation tree. The **SNMP Settings** page is displayed.



2. Scroll to the **SNMP Alerts** section.
3. Configure the **Trap Source Identifier** by selecting **iLO Hostname** or **OS Hostname**.
4. Enable or disable the following alert types:
   - **iLO SNMP Alerts**
   - **Cold Start Trap Broadcast**
   - **SNMPv1 Traps**
5. Optional: To generate a test alert and send it to the UDP addresses in the **SNMP Alert Destination(s)**
6. boxes, click **Send Test Alert**.

   Test alerts are used to verify the network connectivity of iLO with the **SNMP Alert Destination(s)** addresses. After the alert is generated, check the alert destination for receipt of the alert.
7. To save the configuration, click **Apply**.

SNMP alert settings

Trap Source Identifier

Determines the host name that is used in the SNMP-defined sysName variable when iLO generates SNMP traps. The default setting is iLO Hostname

The host name is an OS construct and does not remain persistent with the server when the

hard drives are moved to a new server platform. The iLO sysName, however, remains persistent with the system board.

iLO SNMP Alerts

Alert conditions that iLO detects independently of the host operating system can be sent to specified SNMP alert destinations. If this option is disabled, no traps will be sent to the configured SNMP alert destinations.

Cold Start Trap Broadcast

When this option is enabled and no valid trap destinations are configured, Cold Start Trap is broadcast to a subnet broadcast address.

The Cold Start Trap is broadcast when any of the following conditions is met:

SNMP Alert Destinations are not configured.

iLO failed to resolve all the SNMP Alert Destinations to IP addresses.

The subnet broadcast address for an IPv4 host is obtained by performing a bitwise logical `OR` operation between the bit complement of the subnet mask and the host IP address. For example, the host `192.168.1.1`, which has the subnet mask `255.255.252.0`, has the broadcast address `192.168.1.1 | 0.0.3.255 = 192.168.3.255.`

SNMPv1 Traps

When enabled, SNMPv1 traps are sent to the remote management systems configured in the SNMP Alert Destination(s) boxes.

Using the AMS Control Panel to configure SNMP and SNMP alerts (Windows only)

Procedure

1. Open the Agentless Management Service Control Panel.
2. Click the **SNMP** tab.
3. Update the SNMP settings.
4. Optional: To generate a test alert and send it to the TCP/IP addresses in the **Trap Destination(s)** boxes, click **Send Test Trap**.

   Test alerts are used to verify the network connectivity of iLO with the **Trap Destination(s)** addresses. After the alert is generated, check the alert destination for receipt of the alert.
5. To save the configuration, click **Apply**.

SNMP traps

SNMP traps lists the SNMP traps that you can generate with iLO 5.

Table 3: SNMP traps

Trap number	Trap name	Description
0	Cold Start Trap	SNMP has been initialized, the system has completed POST, or AMS has started.
4	Authentication Failure Trap	SNMP has detected an authentication failure.
1006	cpqSeCpuStatusChange	An uncorrectable machine check exception has been detected in a processor.
1010	cpqSeUSBStorageDeviceReadErrorOccurred	A read error occurred on an attached USB storage device.
1011	cpqSeUSBStorageDeviceWriteErrorOccurred	A write error occurred on an attached USB storage device.
1012	cpqSeUSBStorageDeviceRedundancyLost	USB storage device redundancy was lost.
1013	cpqSeUSBStorageDeviceRedundancyRestored	USB storage device redundancy was restored.
1014	cpqSeUSBStorageDeviceSyncFailed	The sync operation to restore USB storage device redundancy failed.
1015	cpqSePCIeDiskTemperatureFailed	The temperature of the PCIe disk crossed the upper critical threshold.
1016	cpqSePCIeDiskTemperatureOk	The temperature of the PCIe disk is normal.
1017	cpqSePCIeDiskConditionChange	The status of the PCIe disk changed.
1018	cpqSePCIeDiskWearStatusChange	The PCIe disk wear status changed.
1019	cpqSePciDeviceAddedOrPoweredOn	A PCI disk was added or powered on.
1020	cpqSePciDeviceRemovedOrPoweredOff	A PCI device was removed or powered off.
2014	cpqSiIntrusionInstalled	System intrusion hardware installed.
2015	cpqSiIntrusionRemoved	System intrusion hardware removed.
2016	cpqSiHoodReplaced	System hood replaced.

Table Continued

Trap number	Trap name	Description
2017	cpqSiHoodRemovedOnPowerOff	System hood removed when server power was off.
3033	cpqDa6CntlrStatusChange	A change has been detected in the status of the Smart Array controller.
3034	cpqDa6LogDrvStatusChange	A change has been detected in the status of a Smart Array logical drive.
3038	cpqDa6AccelStatusChange	A change has been detected in the status of a Smart Array cache module.
3039	cpqDa6AccelBadDataTrap	The Smart Array cache module has lost backup power.
3040	cpqDa6AccelBatteryFailed	The Smart Array cache module backup power has failed.
3046	cpqDa7PhyDrvStatusChange	A change has been detected in the status of a Smart Array physical drive.
3047	cpqDa7SpareStatusChange	A change has been detected in the status of a Smart Array spare drive.
3049	cpqDaPhyDrvSSDWearStatusChange	A change has been detected in the SSD wear status of a Smart Array physical drive.
6026	cpqHe3ThermalConfirmation	The server was shut down due to a thermal anomaly and is now operational.
6027	cpqHe3PostError	One or more POST errors have occurred.
6032	cpqHe3FltTolPowerRedundancyLost	The fault-tolerant power supplies have lost redundancy for the specified chassis.
6033	cpqHe3FltTolPowerSupplyInserted	A fault-tolerant power supply has been inserted.
6034	cpqHe3FltTolPowerSupplyRemoved	A fault-tolerant power supply has been removed.
6035	cpqHe3FltTolFanDegraded	The fault-tolerant fan condition has been set to **Degraded**.
6036	cpqHe3FltTolFanFailed	The fault-tolerant fan condition has been set to **Failed**.

Table Continued

Trap number	Trap name	Description
6037	cpqHe3FltTolFanRedundancyLost	The fault-tolerant fans have lost redundancy.
6038	cpqHe3FltTolFanInserted	A fault-tolerant fan has been inserted.
6039	cpqHe3FltTolFanRemoved	A fault-tolerant fan has been removed.
6040	cpqHe3TemperatureFailed	Temperature exceeded on the server.
6041	cpqHe3TemperatureDegraded	The temperature status has been set to **Degraded**, and the temperature is outside the normal operating range. Depending on the system configuration, this system might be shut down.
6042	cpqHe3TemperatureOk	The temperature status has been set to **OK**.
6048	cpqHe4FltTolPowerSupplyOk	The fault-tolerant power supply condition has been reset to **OK**.
6049	cpqHe4FltTolPowerSupplyDegraded	The fault-tolerant power supply condition has been set to **Degraded**.
6050	cpqHe4FltTolPowerSupplyFailed	The fault-tolerant power supply condition has been set to **Failed**.
6051	cpqHeResilientMemMirroredMemoryEngaged	The Advanced Memory Protection subsystem has detected a memory fault. Mirrored Memory has been activated.
6054	cpqHe3FltTolPowerRedundancyRestore	The fault-tolerant power supplies have returned to a redundant state.
6055	cpqHe3FltTolFanRedundancyRestored	The fault-tolerant fans have returned to a redundant state.
6061	cpqHeManagementProcInReset	The management processor is resetting.
6062	cpqHeManagementProcReady	The management processor is ready.
6064	cpqHe5CorrMemReplaceMemModule	Memory errors have been corrected. Replace the memory module.
6069	cpqHe4FltTolPowerSupplyACpowerloss	The fault-tolerant power supply in the specified chassis and bay reported AC power loss.

Table Continued

Trap number	Trap name	Description
6070	cpqHeSysBatteryFailed	The Smart Storage Battery has failed.
6071	cpqHeSysBatteryRemoved	The Smart Storage Battery has been removed.
6072	cpqHeSysPwrAllocationNotOptimized	iLO could not determine the power requirements. The server power allocation is not optimized.
6073	cpqHeSysPwrOnDenied	The server could not power on because the hardware cannot be identified.
6074	cpqHePowerFailureError	A device power failure has been detected.
6075	cpqHeInterlockFailureError	A device is missing or improperly seated on the system board.
8029	cpqSs6FanStatusChange	The storage enclosure fan status changed.
8030	cpqSs6TempStatusChange	The storage enclosure temperature status changed.
8031	cpqSs6PwrSupplyStatusChange	The storage enclosure power status changed.
8032	cpqSsConnectionStatusChange	The storage enclosure status changed.
9001	cpqSm2ServerReset	The server power has been reset.
9003	cpqSm2UnauthorizedLoginAttempts	The maximum unauthorized login attempt threshold has been exceeded.
9005	cpqSm2SelfTestError	iLO 5 detected a self test error.
9012	cpqSm2SecurityOverrideEngaged	iLO 5 detected that the security override jumper has been toggled to the engaged position.
9013	cpqSm2SecurityOverrideDisengaged	iLO 5 detected that the security override jumper has been toggled to the disengaged position.
9017	cpqSm2ServerPowerOn	The server has been powered on.
9018	cpqSm2ServerPowerOff	The server has been powered off.

Table Continued

Trap number	Trap name	Description
9019	cpqSm2ServerPowerOnFailure	A request was made to power on the server, but the server could not be powered on because of a failure condition.
9021	cpqSm2FirmwareValidationScanFailed	Firmware validation failure happened on iLO/ IE/ SPS firmware
9022	cpqSm2FirmwareValidationScanErrorRepaired	Firmware integrity scan issue reported has been repaired.
9023	cpqSm2FirmwareValidationAutoRepairFailed	Firmware recovery failure
11003	cpqHo2GenericTrap	Generic trap. Verifies that the SNMP configuration, client SNMP console, and network are operating correctly. You can use the iLO web interface to generate this alert to verify receipt of the alert on the SNMP console.
11018	cpqHo2PowerThresholdTrap	A power threshold has been exceeded.
11020	cpqHoMibHealthStatusArrayChangeTrap	A change in the health status of the server has occurred.
5022	cpqSasPhyDrvStatusChange	AMS detected a change in the status of an SAS or SATA physical drive.
14004	cpqIdeAtaDiskStatusChange	AMS detected a change in the status of an ATA disk drive.
16028	cpqFca3HostCntlrStatusChange	AMS detected a change in the status of a Fibre Channel host controller.
18011	cpqNic3ConnectivityRestored	Connectivity was restored to a logical network adapter.
18012	cpqNic3ConnectivityLost	The status of a logical network adapter changed to **Failed**.
18013	cpqNic3RedundancyIncreased	AMS detected that a previously failed physical adapter in a connected logical adapter group returned to the OK status.
18014	cpqNic3RedundancyReduced	AMS detected that a physical adapter in a logical adapter group changed to **Failed** status, but at least one physical adapter remains in **OK** status.
169001	cpqiScsiLinkUp	AMS detected that an iSCSI session is up.
169002	cpqiScsiLinkDown	AMS detected that an iSCSI session is down.

For more information about these SNMP traps, see the following MIB files in the MIB update kit:

cpqida.mib	Drive array
cpqhost.mib	Server host system details
cpqhlth.mib	Server health system
cpqsm2.mib	Integrated Lights-Out
cpqide.mib	IDE subsystem
cpqscsi.mib	SCSI system
cpqiscsi.mib	iSCSI system
cpqnic.mib	System NIC
cpqstsys.mib	Storage systems
cpqstdeq.mib	Server standard equipment
cpqfca.mib	Fibre Channel array
cpqsinfo.mib	System Information
cpqstsys.mib	Smart Array storage

IMPORTANT:

When SNMP setting is used on OS environment and AMS(Agentless Management Service) is working, AMS sends some same traps as iLO.

In this case, same trap number is sent by both AMS and iLO. However, the sender's IP address is different between AMS and iLO. Please refer to either AMS or iLO traps.

iLO AlertMail

iLO AlertMail enables you to configure iLO to send alert conditions detected independently of the host operating system to a specified email address. iLO mail alerts include major host system events.

Some email service providers establish filters and rules to block problem emails such as spam, commercial content, and unwanted volume. These tools might block the receipt of messages generated by iLO. These email services are not suitable for receiving iLO AlertMail messages.

Sample of AlertMail

```
Subject: NEC iLO AlertMail-280: (CAUTION) System Fan Removed (Fan 4, Location System)
From: =iLO hostname < hostname.example.com@example.com>
To: mailreceiver@example.com
----------------------------------------------------------------------------------------------------------------------------------
---
EVENT (15-Aug-2017 00:46): System Fan Removed (Fan 4, Location System)

Integrated Management Log Severity:CAUTION



iLO URL: https://hstname.example.com
iLO IP: https://172.16.0.1
iLO Name:      hstname
iLO firmware:  1.10 Jun 07 2017

Server Model:  Express5800/R120h-2M
System ROM:    U30 06/14/2017 Server UUID:   01234567-89AB-CDEF-0123-4367890ABCDE




PLEASE DO NOT REPLY TO THIS EMAIL. For more details about NEC iLO technology, visit: jpn.nec.com/express/
```

Enabling AlertMail

Prerequisites

- An iLO license that supports this feature is installed.
- Configure iLO Settings privilege

Procedure

1. Click **Management** in the navigation tree, and then click the **AlertMail** tab.
2. Set the **Enable iLO AlertMail** option to enabled.
3. Enter the following information:
   - **Email Address**
   - **Sender Domain**
   - **SMTP Port**
   - **SMTP Server**
4. Optional: To send a test message to the configured email address, click **Send Test AlertMail**.

   This button is available only when AlertMail is enabled.
5. To save the changes, click **Apply**.

AlertMail options

- **Email Address**—The destination email address for iLO email alerts. This string can be up to 63 characters and must be in standard email address format. You can enter only one email address.
- **Sender Domain**—The domain name specified in the sender (From) email address. The sender email address is formed by using the iLO name as the host name, and the sender domain as the domain name. This string can be up to 63 characters.
- **SMTP Port**—The port that the SMTP server will use for unauthenticated SMTP connections. The default value is 25.
- **SMTP Server**—The IP address or DNS name of the SMTP server or the MSA. This server cooperates with the MTA to deliver the email. This string can be up to 63 characters.

IMPORTANT:

For iLO 5 Firmware Version 1.10 Jun 07 2017：It is not able to perform name resolution on the IPv6 DNS server. When using in IPv6 environment, you set the **SMTP Server** with the IP address.

Disabling AlertMail

Prerequisites

- An iLO license that supports this feature is installed.
- Configure iLO Settings privilege

Procedure

1. Click **Management** in the navigation tree, and then click the **AlertMail** tab.
2. Set the **Enable iLO AlertMail** option to disabled.
3. To save the changes, click **Apply**.

Remote Syslog

The Remote Syslog feature allows iLO to send event notification messages to Syslog servers. The iLO firmware Remote Syslog includes the IML and iLO Event Log.

Enabling iLO Remote Syslog

Prerequisites

- An iLO license that supports this feature is installed.
- Configure iLO Settings privilege

Procedure

1. Click **Management** in the navigation tree, and then click the **Remote Syslog** tab.
2. Set the **Enable iLO Remote Syslog** option to enabled.
3. Enter the following information:
   - Remote Syslog Server
   - Remote Syslog Port
4. Optional: To send a test message to the configured syslog server, click **Send Test Syslog**.

   This button is available only when iLO Remote Syslog is enabled.
5. To save the changes, click **Apply**.

Remote syslog options

- **Remote Syslog Server**—The IP address, FQDN, IPv6 name, or short name of the server running the Syslog service. To enter multiple servers, separate the server IP address, FQDN, IPv6 name, or short name with a semicolon. You can enter up to 63 characters per server, and a total of 127 characters.

  On Linux systems, a tool called syslog logs system events. You can set a syslog server on a remote system that will act as a central logging system for iLO systems. If the iLO Remote Syslog feature is enabled in iLO, it can send its logs to the syslog server.

  IMPORTANT:

  For iLO 5 Firmware Version Aug 17 2017 or earlier：It is not able to perform name resolution on the IPv6 DNS server. When using in IPv6 environment, you set the **Remote Syslog Server** with the IP address.

- **Remote Syslog Port**—The port number through which the Syslog server is listening. Only one port number can be entered in this box. When you enter multiple Remote Syslog servers, they must use the same port. The default value is 514.

Disabling iLO Remote Syslog

Prerequisites

- An iLO license that supports this feature is installed.
- Configure iLO Settings privilege

Procedure

1. Click **Management** in the navigation tree, and then click the **Remote Syslog** tab.
2. Set the **Enable iLO Remote Syslog** option to disabled.
3. To save the changes, click **Apply**.

16. IPMI server management

Server management through IPMI is a standard method for controlling and monitoring the server. The iLO firmware provides server management based on the IPMI version 2.0 specification, which defines the following:

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

IPMI communications depend on the BMC and the SMS. The BMC manages the interface between the SMS and the platform management hardware. The iLO firmware emulates the BMC functionality, and various industry-standard tools can provide the SMS functionality. For more information, see the IPMI specification on the Intel website at **http://www.intel.com**.

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

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

- **IPMI version 2.0 Command Test Tool**—A low-level MS-DOS command-line tool that enables hex-formatted IPMI commands to be sent to an IPMI BMC that implements the KCS interface. You can download this tool from the Intel website at **http://www.intel.com**.
- **IPMItool**—A utility for managing and configuring devices that support the IPMI version 1.5 and version specifications. IPMItool can be used in a Linux environment. You can download this tool from the IPMItool website at **http://ipmitool.sourceforge.net/index.html**.
- **FreeIPMI**—A utility for managing and configuring devices that support the IPMI version 1.5 and version 2.0 specifications. You can download FreeIPMI from the following website: **http:// www.gnu.org/software/freeipmi/**.
- **IPMIUTIL**—A utility for managing and configuring devices that support the IPMI version 1.0, 1.5, and version 2.0 specifications. You can download IPMIUTIL from the following website: **http://ipmiutil.sourceforge.net/**

When emulating a BMC for the IPMI interface, iLO supports all mandatory commands listed in the IPMI version 2.0 specification. The SMS should use the methods described in the specification for determining which IPMI features are enabled or disabled in the BMC (for example, using the `Get Device ID` command).

If the server OS is running, and the iLO driver is enabled, any IPMI traffic through the KCS interface can affect iLO driver performance and system health. Do not issue any IPMI commands through the KCS interface that might have a negative effect on iLO driver monitoring. This restriction includes any command that sets or changes IPMI parameters, such as `Set Watchdog Timer` and `Set BMC Global Enabled`. Any IPMI command that simply returns data is safe to use, such as `Get Device ID` and `Get Sensor Reading`.

Advanced IPMI tool usage on Linux

The Linux IPMI tool can communicate securely with the iLO firmware by using the IPMI 2.0 RMCP+ protocol. This feature is the `ipmitool lanplus` protocol feature.

For example: To retrieve the iLO Event Log, enter:

```
ipmitool -I lanplus -H <iLO ip address> -U <username> -P <password> sel list
```

Output example:

```
1  | 03/18/2000 | 00:25:37 | Power Supply #0x03 | Presence detected | Deasserted
2  | 03/18/2000 | 02:58:55 | Power Supply #0x03 | Presence detected | Deasserted
3  | 03/18/2000 | 03:03:37 | Power Supply #0x04 | Failure detected | Asserted
4  | 03/18/2000 | 03:07:35 | Power Supply #0x04 | Failure detected | Asserted
```

17. Managing iLO reboots, factory reset, and NMI

Rebooting (resetting) iLO

In some cases, it might be necessary to reset iLO; for example, if iLO is not responding to the browser.

Using the **Reset** option does not make any configuration changes, but ends all active connections to the iLO firmware. If a firmware file upload is in progress, it is terminated. If a firmware flash is in progress, you cannot reset iLO until the process is finished.

iLO reset methods

- Click **Reset** on the **Diagnostics** page in the iLO web interface.
- Use the CLI.
- Use the BMC Configuration Utility.
- Use the server UID button on supported servers.
- Use the iLO RESTful API.
- Use IPMI.

If none of these methods are available or working as expected, you must power down the server and disconnect the power supplies.

Rebooting (resetting) the iLO processor with the web interface

Prerequisites

Configure iLO Settings privilege

Procedure

1. Click **Information** in the navigation tree, and then click the **Diagnostics** tab.
2. Click **Reset**.
3. When prompted to confirm the request, click **OK**.

   iLO resets and closes your browser connection.

Rebooting (resetting) iLO with the BMC Configuration Utility

Prerequisites

Configure iLO Settings privilege

Procedure

1. Optional: If you access the server remotely, start an iLO remote console session.
2. Restart or power on the server.
3. Press **F9** in the server POST screen.

The UEFI System Utilities start.

4. From the **System Utilities** screen, click **System Configuration**, and then click **BMC Configuration Utility**.
5. Select **Yes** in the **Reset iLO** menu.

   The BMC Configuration Utility prompts you to confirm the reset.
6. Click **OK**.
7. iLO resets and all active connections are ended. If you are managing iLO remotely, the remote console session is automatically ended.

   When you reset iLO, the BMC Configuration Utility is not available again until the next server reboot.
8. Resume the boot process:
   a. Optional: If you are managing iLO remotely, wait for the iLO reset to finish, and then start the iLO remote console.
   b. The UEFI System Utilities are open from the previous session.
   c. Press **Esc** until the main menu is displayed.
   d. Click **Exit and resume system boot**.
   e. When prompted to confirm the request, click **OK** to exit the utility and resume the normal boot process.

Rebooting (resetting) iLO with the server UID button

The UID button on supported servers can be used to initiate a manual reboot of iLO. For more information about the UID button, see the server user guide.

Performing a graceful iLO reboot with the server UID button

When you initiate a graceful iLO reboot, the iLO firmware initiates the iLO reboot.

Initiating a graceful iLO reboot does not make any configuration changes, but ends all active connections to iLO. If a firmware file upload is in progress, it is terminated. If a firmware flash is in progress, you cannot reboot iLO until the process is finished.

Procedure

1. To initiate a graceful iLO reboot, press and hold the UID button for 5 to 9 seconds.

   The UID button/LED flashes blue 4 Hz/cycle per second to indicate that a graceful iLO reboot is in progress.

Performing a hardware iLO reboot with the server UID button

When you initiate a hardware iLO reboot, the server hardware initiates the iLO reboot.

Procedure

1. To initiate a hardware iLO reboot, press and hold the UID button for 10 seconds or longer.

> **CAUTION:**
>
> Initiating a hardware iLO reboot does not make any configuration changes, but ends all active connections to iLO. If a firmware flash is in progress, it is interrupted, which might cause data corruption on the flash device. If data corruption occurs on the flash device, use the secure recovery or iLO network failed flash recovery features. Data loss or NVRAM corruption might occur during a hardware iLO reboot.
>
> Do not initiate a hardware reboot if other troubleshooting options are available.

The UID button/LED flashes blue 8 Hz/cycle per second to indicate that an iLO hardware reboot is in progress.

More Information

iLO network Failed Flash Recovery

Server power-on

Reset iLO to the factory default settings

In some cases, you might need to reset iLO to the factory default settings. For example, you must reset iLO to the default settings when you disable FIPS mode. You can use the BMC Configuration Utility, the iLO RESTful API to perform this task.

- To use the BMC Configuration Utility, see **Resetting iLO to the factory default settings (BMC Configuration Utility)** .
- To use the iLO RESTful API.

Resetting iLO to the factory default settings (BMC Configuration Utility)

CAUTION:

When you reset iLO to the factory default settings, all iLO settings are erased, including user data, license data, configuration settings, and logs. If the server has a factory installed license key, the license key is retained.

Events related to the reset are not logged to the iLO Event Log and Integrated Management Log because this step clears all the data in the logs.

Procedure

1. Optional: If you access the server remotely, start an iLO remote console session.
2. Restart or power on the server.
3. Press **F9** in the server POST screen.

   The UEFI System Utilities start.
4. From the **System Utilities** screen, click **System Configuration**, and then click **BMC Configuration Utility**.
5. Select **Yes** in the **Set to factory defaults** menu.
6. The BMC Configuration Utility prompts you to confirm the request.
7. Click **OK**.
8. iLO resets to the factory default settings. If you are managing iLO remotely, the remote console session is automatically ended. You cannot access the BMC Configuration Utility again until after the next system reboot.
9. Resume the boot process:
   a. Optional: If you are managing iLO remotely, wait for the iLO reset to finish, and then start the iLO remote console.

      The BMC Configuration Utility screen is still open from the previous session.
   b. Press **Esc** until the main menu is displayed.
   c. Click **Exit and resume system boot**.

d. When prompted to confirm the request, click **OK** to exit the screen and resume the boot process.

10. Optional: Use the default iLO account information to log in to iLO after the reset.

Generating an NMI

The Generate NMI to System feature enables you to stop the operating system for debugging.

CAUTION:

Generating an NMI as a diagnostic and debugging tool is used primarily when the operating system is no longer available. NMI is not used during normal operation of the server. Generating an NMI does not gracefully shut down the operating system, but causes the operating system to crash, resulting in lost service and data. Use the Generate NMI to System button only in extreme cases in which the OS is not functioning correctly and an experienced support organization has recommended an NMI.

Prerequisites

Virtual Power and Reset privilege

Procedure

1. Click **Information** in the navigation tree, and then click the **Diagnostics** tab.
2. Click **Generate NMI to System**.
3. When iLO warns you that generating an NMI to the system might cause data loss, click **OK** to confirm, or click **Cancel**.

   If you clicked **OK**, iLO confirms that the NMI was sent.

18. Troubleshooting

Using the iLO Virtual Serial Port with Windbg

If you want to debug a server, you can use the iLO Virtual Serial Port feature with the Windows `Windbg` kernel debugger running on a local test system.

Prerequisites

PuTTY is installed on the local test system. You can download PuTTY from the following website: **http://www.putty.org/**.

Procedure

1. Using the iLO web interface of the server with kernel issues, navigate to the **Security - Access Settings** page, and configure the **Serial Command Line Interface Speed**.

   The default value is 9600.

2. Configure the debug options in Windows (the `boot.ini` parameters for the serial connection).

   Use `debugport=com2`, and set the baud rate to match the configured **Serial Command Line Interface Speed**.

3. Start or restart the server.

4. Press **F9** in the server POST screen.

   The ROM-based configuration utility starts.

5. Configure the following settings:
   - Disable EMS and BIOS Serial Console.
   - Set the Virtual Serial Port to `COM 2`.

6. To access the selection menu for the Windows debug boot option, reboot the server.

7. From the local test system, use PuTTY to connect to iLO and log in.

8. Enter the IP address for the session host name. Use the default settings for an SSH session.

   When the PuTTY iLO CLI session opens, a user login window opens, unless the PuTTY session is configured to use private keys.

   It might take a minute for the prompt to appear.

9. At the `</>iLO->` prompt, enter the following command: `windbg_enable`.

   This command opens a socket to the Virtual Serial Port on port 3002.

10. To start the Windows debugger, enter the following command: `windbg -k com:port=<IP-address>,ipport=3002`.

    `<IP-address>` is the iLO IP address, and `3002` is the socket to connect to (the raw serial

data socket for iLO).

The `ipport` parameter is optional. The default port is 3002.

You can add other `windbg` command-line parameters if necessary. NEC Corporation recommends using the `-b` parameter for the initial breakpoint.

11. Go to the server console (or access the iLO Remote Console), and press **Enter** to boot the debug selection on the OS load menu.

    This step might take several minutes.

12. When you are finished debugging the host server, use PuTTY to connect to the CLI and turn off the debug socket to the Virtual Serial Port. Then, enter the following command: `windbg_disable`.

    You can disconnect and reconnect the Windows debugger as long as you keep the iLO debug socket enabled.

Using the Server Health Summary

You can use iLO to display the Server Health Summary on an external monitor when the server is powered on or off. This feature is useful for troubleshooting when the server will not start up, and can also be used to view the server IP address and other health information.

Prerequisites

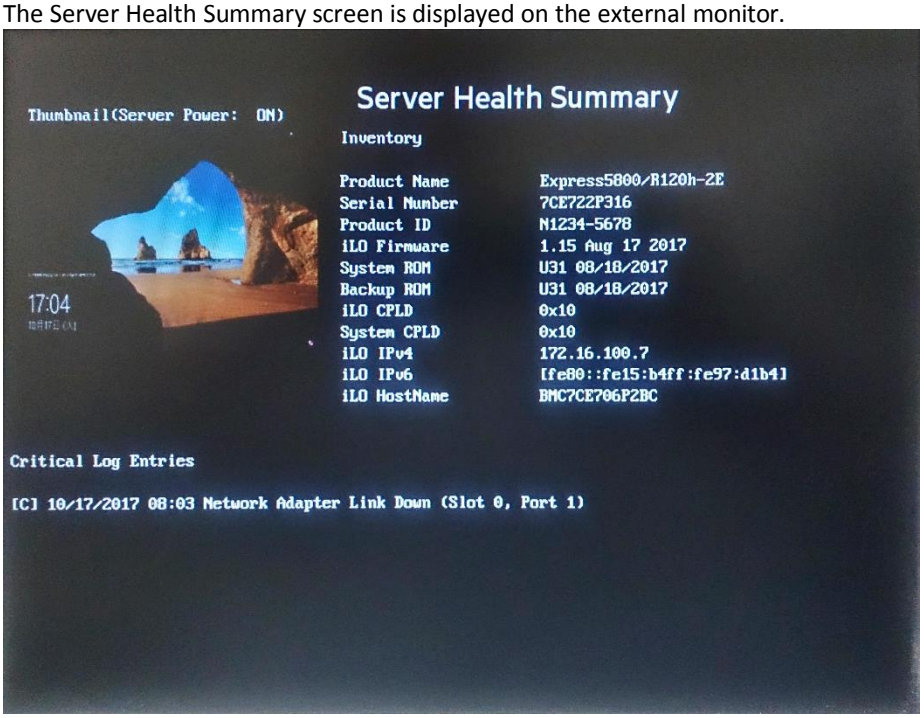
- The server has a UID button.
- An external monitor is connected.

Procedure

1. Press the UID button on the server.

> **CAUTION:**
>
> Press and release the UID button. Holding it down at any time for more than 5 seconds initiates a graceful iLO reboot or a hardware iLO reboot. Data loss or NVRAM corruption might occur during a hardware iLO reboot.

The Server Health Summary screen is displayed on the external monitor.



2. Press the UID button again to close the Server Health Summary screen.

Server Health Summary details

Server screen thumbnail

A thumbnail image of the server screen.

Server Power

The server power status.

Product Name

The server model.

Serial Number

The server serial number.

Product ID

The product with which this iLO processor is integrated.

iLO Firmware

The installed iLO Firmware version.

System ROM

The installed system ROM version.

Backup ROM

The backup system ROM version.

iLO CPLD

The installed iLO CPLD version.

System CPLD

The installed system CPLD version.

Embedded Smart Array

The installed Smart Array firmware version. This value is displayed only if server POST has successfully completed since the last auxiliary power cycle.

iLO IPv4

The iLO IPv4 address. This value is displayed only if **Show iLO IP during POST** is enabled on the **Access Settings** page.

iLO IPv6

The iLO IPv6 address. This value is displayed only if **Show iLO IP during POST** is enabled on the **Access Settings** page.

iLO Hostname

The iLO hostname.

Critical Log Entries

The most recent **Critical** events from the IML are displayed, with the most recent event displayed first.

Incorrect time stamp on iLO Event Log entries

Symptom

iLO Event Log entries have an incorrect date or time.

Cause

The NTP server addresses or the time zone is configured incorrectly.

Action

1. Verify that the SNTP settings are configured correctly.

Login and iLO access issues

iLO firmware login name and password not accepted

Symptom

An iLO firmware login attempt fails.

Cause

The user account information was entered incorrectly.

Action

Enter the correct user account information.

Passwords are case-sensitive.

User names are not case-sensitive. Uppercase and lowercase characters are treated the same (for example, Administrator is treated as the same user as administrator).

iLO management port not accessible by name

Symptom

The iLO management port is not accessible by name.

Cause

The iLO management port can register with a WINS server or DDNS server to provide the name-to-IP- address resolution required to access the iLO management port by name. The environment is not configured to support accessing the iLO management port by name.

Action

Verify that your environment meets the following requirements:

The WINS or DDNS server must be up and running before the iLO management port is powered on.

The iLO management port is configured with the IP address of the WINS or DDNS server. You can use DHCP to configure the required IP addresses.

The iLO management port has a valid route to the WINS or DDNS server.

The clients used to access the iLO management port are configured to use the same DDNS server where the IP address of the management port is registered.

If you use a WINS server and a nondynamic DNS server, iLO management port access might be faster if you configure the DNS server to use the WINS server for name resolution. For more information, see the Microsoft documentation.

Unable to access the iLO login page

Symptom

The iLO web interface login page will not load.

Solution 1

Cause

The SSL encryption level in the browser is not set to 128-bit or higher.

The SSL encryption level in iLO is set to 128-bit or higher and cannot be changed. The browser and iLO encryption levels must be the same.

Action

1. Set the SSL encryption level of your browser to 128-bit or higher.

Solution 2

Cause

iLO is configured to use the Shared Network Port, and NIC teaming is enabled for the NIC the Shared Network Port uses. In this configuration, network communications might be blocked in the following cases:

The selected NIC teaming mode causes the switch that iLO is connected with to ignore traffic from the server NIC/port that iLO is configured to share.

The selected NIC teaming mode sends all traffic destined for iLO to a NIC/port other than the one that iLO is configured to share.

Action

1. Ensure that your Shared Network Port configuration follows the iLO NIC teaming guidelines.

Unable to connect to iLO after changing network settings

Symptom

iLO is inaccessible after an update to the network settings.

Cause

The NIC and the switch settings are not the same.

Action

1. Verify that both sides of the connection (the NIC and the switch) have the same settings for transceiver speed autoselect, speed, and duplex.

For example, if one side is autoselecting the connection, the other side must use the same

setting.

Unable to return to iLO login page after iLO reset

Symptom

The iLO login page will not open after an iLO reset.

Action

1. Clear the browser cache and restart the browser.

An iLO connection error occurs after an iLO firmware update

Symptom

You cannot connect to iLO after updating the firmware by using the web interface.

Action

1. Clear the browser cache and try again.

Unable to connect to iLO processor through NIC

Symptom

The iLO processor is inaccessible through the NIC.

Action

- Ping the IP address of the NIC from a separate network workstation.
- Attempt to connect with a browser by entering the IP address of the NIC as the URL. You can see the iLO login page from this address.
- Reset iLO. If a network connection is established, you might have to wait up to 90 seconds for the DHCP server request.

Unable to log in to iLO after installing iLO certificate

Symptom

iLO is inaccessible after the iLO self-signed certificate is installed in the browser certificate store.

Cause

When you reset iLO to the factory default settings or change the iLO hostname, a new self-signed certificate is generated. In some browsers, if the self-signed certificate is installed permanently, you might not be able to log in to iLO after a new self-signed certificate is generated.

Action

1. Remove the self-signed certificate from the browser certificate store.

The self-signed certificate has iLO in the certificate name, and the **Issued By** value includes the text

Default Issuer**.**

Do not install the iLO self-signed certificate in the browser certificate store. If you want to install a certificate, request a permanent certificate from a CA and import it into iLO.

See the browser documentation for more information about working with certificates.

Unable to connect to iLO IP address

Symptom

Cannot connect to iLO through the iLO IP address.

Cause

The web browser is configured to use a proxy server.

Action

1. To connect to iLO without using the proxy server, add iLO to the list of proxy server exceptions. See the browser documentation for instructions.

iLO TCP/IP communication fails

Symptom

iLO communications fail.

Cause

A firewall is preventing iLO communications through one or more TCP/IP ports.

Action

1. Configure the firewall to allow communications on the ports iLO uses.

Secure Connection Failed error when using Firefox to connect to iLO

Symptom

The following error occurs when you try to use Firefox to connect to iLO:

`sec_error_reused_issuer_and_serial`.

Solution 1

Cause

The installed certificate contains the same serial number as another certificate issued by the certificate authority.

Action

1. Click the menu button, and then select **Options**.
2. Click **Advanced**.
3. Click **Certificates**.
4. Click **View Certificates**.
5. Click the **Servers** tab, and then delete any certificates related to iLO.

6. Click the **Others** tab, and then delete any certificates related to iLO.
7. Click **OK**.
8. Start Firefox and connect to iLO.

Solution 2

Cause

The installed certificate contains the same serial number as another certificate issued by the certificate authority.

Action

Close Firefox.

Navigate to the Firefox `AppData` folder, and then delete all of the `*.db` files in all of the Firefox directories.

The `AppData` folder is typically in the following location: `C:\\Users\<user name>\AppData\Local\Mozilla\Firefox\`

Certificate error when navigating to iLO web interface with Internet Explorer

Symptom

When you navigate to the iLO web interface with Internet Explorer, a certificate error appears.

Solution 1

Action

Click the **Continue to this website (not recommended)** link.

Log in to iLO.

Solution 2

Action

Navigate to the **Administration** > **Security** > **SSL Certificate** page.

Obtain and import an SSL certificate.

Reset iLO.

Certificate error when navigating to iLO web interface with Chrome

Symptom

When you navigate to the iLO web interface with Chrome, a certificate error appears.

Solution 1

Action

1. Click **Advanced**.
2. **Click** Proceed to <iLO hostname or IP address> (unsafe)**.**
3. Log in to iLO.

Solution 2

Action

1. Navigate to the **Administration** > **Security** > **SSL Certificate** page.
2. Obtain and import an SSL certificate.
3. Reset iLO.

Certificate error when navigating to iLO web interface with Firefox

Symptom

When you navigate to the iLO web interface with Firefox, a certificate error appears.

Solution 1

Action

1. Click I Understand the Risks, and then click Add Exception.
2. In the Add Security Exception dialog box, enter https://<iLO hostname or IP address> in the Location box.
3. Click Confirm Security Exception.
4. The security exception is saved and the iLO login screen appears.
5. Log in to iLO.

Solution 2

Action

1. Navigate to the Administration > Security > SSL Certificate page.
2. Obtain and import an SSL certificate.
3. Reset iLO.

iLO login page displays a Website Certified by an Unknown Authority message

Cause

The message `Website Certified by an Unknown Authority` is displayed when you navigate to the iLO login page.

Action

1. To ensure that you are browsing to the correct management server (not an imposter), view the certificate.
   a. Verify that the Issued To name is your management server. Perform any other steps you feel necessary to verify the identity of the management server.
   b. If you are not sure that you navigated to the correct management server, do not proceed. You might be browsing to an imposter and giving your login credentials to that imposter when you log in.

Contact the administrator. To cancel the connection, exit the certificate window, and then click **No** or **Cancel**.

2. After verifying the items in the previous step, choose from the following options:
   - Accept the certificate temporarily for this session.
   - Accept the certificate permanently.
   - Stop now and import a certificate into your browser from a file provided by an administrator.

iLO responds to pings intermittently or does not respond

Symptom

iLO responds to pings intermittently or does not respond.

Cause

- iLO is configured to use the Shared Network Port, and NIC teaming is enabled for the NIC the Shared Network Port uses. In this configuration, network communications might be blocked in the following cases:
- The selected NIC teaming mode causes the switch that iLO is connected with to ignore traffic from the server NIC/port that iLO is configured to share.
- The selected NIC teaming mode sends all traffic destined for iLO to a NIC/port other than the one that iLO is configured to share.

Action

1. Ensure that your Shared Network Port configuration follows the NIC teaming guidelines.

Directory issues

Logging in to iLO with Kerberos authentication fails

Symptom

A Kerberos login attempt fails.

Solution 1

Cause

The client does not have a ticket or has an invalid ticket.

Action

1. To lock the client PC and get a new ticket, press Ctrl+Alt+Del.

Solution 2

Cause

Kerberos login is configured incorrectly. Possible reasons follow:

- The Kerberos realm that the client PC is logged in to does not match the Kerberos realm for which iLO is configured.
- The key in the Kerberos keytab file stored in iLO does not match the Active Directory key.
- iLO is configured for an incorrect KDC server address.
- The date and time do not match between the client PC, the KDC server, and iLO. Set the date and time on these systems to the same value. The date and time on these systems must not differ by more than 5 minutes.

Action

1. Verify that your environment meets the requirements for Kerberos support.

Solution 3

Cause

There is a problem with the directory user account. Possible problems follow:

- The iLO computer account does not exist in Active Directory, or the account is disabled.
- The user logged in to the client PC is not a member of a universal or global directory group authorized to access iLO.

Action

1. Repair the DNS server.

iLO credential prompt appears during Kerberos login attempt

Symptom

When a user clicks the **Zero Sign In** button, a credential prompt appears.

Cause

The browser is not configured correctly for Kerberos login.

Action

1. Configure the browser to support Kerberos login.

iLO credential prompt appears during Kerberos login by name attempt

Symptom

A credential prompt appears when a user tries to log in to iLO with a user name in Kerberos SPN format and the associated domain password.

Cause

The computer account for iLO is part of a child domain and the Kerberos configuration parameters reference the parent domain.

Action

1. Verify that the following Kerberos parameters are configured correctly: **Kerberos Realm**, **Kerberos KDC Server Address**, and **Kerberos KDC Server Port**.

A directory connection to iLO ends prematurely

Symptom

An Active Directory session ends prematurely.

Cause

Network errors can cause iLO to conclude that a directory connection is no longer valid. If iLO cannot detect the directory, it ends the directory connection. Any attempt to continue using the terminated connection redirects the browser to the login page.

This issue might occur in the following situations:

- The network connection is terminated.
- The directory server is shut down.

Action

1. Log back in and continue using iLO.

If the directory server is unavailable, log in with a local user account.

Configured directory user contexts do not work with iLO login

Symptom

Directory user contexts are configured, but the login options they provide do not work.

Cause

The user object in the directory or the user context is not configured correctly.

Action

Verify that the full DN of the user object exists in the directory. This information appears after the first `CN=` in the DN.

Verify that the remainder of the DN was added as a user context.

User contexts are not case-sensitive, and any other characters, including spaces, are part of the user context.

iLO directory user account does not log out after directory timeout expires

Symptom

A directory user is not logged out after being idle for the amount of time configured for the directory login timeout.

Cause

The iLO **Idle Connection Timeout** value is set to **Infinite**. With this configuration, the Remote Console periodically pings the iLO firmware to verify that the connection exists. When the Remote Console pings iLO, the iLO firmware queries the directory for user permissions. This periodic query keeps the directory connection active, and prevents a user from being logged out based on the directory timeout settings.

Action

1. Change the **Idle Connection Timeout** setting.

Failure generating Kerberos keytab file for iLO Zero Sign In configuration

Symptom

When you try to generate a keytab file with `ktpass`, the process fails.

Cause

The `ktpass` command was formatted incorrectly.

Action

1. Try again, and ensure that the principal name in the `ktpass` command is formatted correctly.

Error when running `Setspn` for iLO Kerberos configuration

Symptom

An error occurred when running the `Setspn` command.

Action

1. Use MMC with the `ADSIEdit` snap-in, and find the computer object for iLO.
2. Set the `DNSHostName` property to the iLO DNS name.

For example: `cn=iloname,ou=us,ou=clients,dc=example,dc=net`

OpenLDAP authentication fails when configured with nested groups or posixgroups

Symptom

OpenLDAP authentication fails when the directory is configured with nested groups or posixgroups.

Cause

iLO does not support nested groups or posixgroups with OpenLDAP.

Action

1. Configure iLO with a group in which the LDAP user has a direct membership. Make sure the OpenLDAP directory group has an objectClass of the type groupOfNames.

iLO Zero Sign In fails after domain controller OS reinstall

Symptom

The iLO web interface **Zero Sign In** option does not work after the domain controller OS is reinstalled.

Cause

The key version number sequence is reset when the domain controller OS is reinstalled.

Action

1. Generate and install a new Kerberos keytab file.

Failed iLO login with Active Directory credentials

Symptom

User authentication fails when iLO is configured to use Active Directory.

Cause

There is a certificate problem:

- An SSL certificate is not installed on the Active Directory server.
- An old SSL certificate on the Active Directory server points to a previously trusted CA with the same name as the CA in the current certificate. This situation might happen if a certificate service is added and removed, and then added again.

You can verify this cause by checking the SSL Connection test results on the Directory Tests page.

Action

1. Open the MMC.
2. Add the certificates snap-in.
3. When prompted, select Computer Account for the type of certificates you want to view.
4. To return to the certificates snap-in, click OK.
5. Select the Personal > Certificates folder.
6. Right-click the folder and select Request New Certificate.
7. Verify that the Type is domain controller, and click Next until a certificate is issued.

Directory Server DNS Name test reports a failure

Symptom

The Directory Server DNS Name test reports the status Failed.

Cause

iLO cannot obtain an IP address for the directory server.

Action

- Verify that the DNS server configured in iLO is correct.
- Verify that the directory server FQDN is correct.
- As a troubleshooting tool, use an IP address instead of the FQDN.
- If the problem persists, check the DNS server records and network routing.

Ping Directory Server test reports a failure

Symptom

The Ping Directory Server test reports the status **Failed**.

Cause

iLO pinged the directory server and did not receive a response.

Action

- Check to see if a firewall is active on the directory server.
- Check for network routing issues.

Connect to Directory Server test reports a failure

Symptom

The Connect to Directory Server test reports the status Failed.

Cause

iLO failed to initiate an LDAP connection with the specified directory server.

Action

- Verify that the configured directory server is the correct host.
- Verify that iLO has a clear communication path to the directory server through port 636 (consider any routers or firewalls between iLO and the directory server).
- Verify that any local firewall on the directory server is enabled to allow communications through port 636.

Connect using SSL test reports a failure

Symptom

The Connect using SSL test reports the status **Failed**.

Cause

The SSL handshake and negotiation between iLO and the directory server were unsuccessful.

Action

- Enable the directory server for SSL negotiations.
- If you are using Microsoft Active Directory, verify that Active Directory Certificate Services is installed.

Bind to Directory Server test reports a failure

Symptom

The Bind to Directory Server test reports the status **Failed**.

Cause

iLO failed to bind the connection with the specified user name or an anonymous bind.

Action

- Verify that the directory server allows anonymous binding.
- If you entered a user name in the test boxes, verify that the credentials are correct.

- If you verified that the user name is correct, try using other user name formats; for example, `user@domain.com`, `DOMAIN\username`, `username` (called Display Name in Active Directory), or `userlogin`.
- Verify that the specified user is allowed to log in and is enabled.

Directory Administrator Login test reports a failure

Symptom

The Directory Administrator Login test reports the status **Failed**.

Cause

You entered values in the optional **Directory Administrator Distinguished Name** and **Directory Administrator Password** boxes, and login to the directory server failed.

Action

1. Verify that the directory administrator credentials were entered correctly.

User Authentication test reports a failure

Symptom

The User Authentication test reports the status **Failed**.

Cause

Authentication failed with the provided user name and password.

Action

- Verify that the user credentials were entered correctly.
- Try using other user name formats; for example, `user@domain.com`, `DOMAIN\username`, `username` (called Display Name in Active Directory), or `userlogin`.
- Verify that the specified user is allowed to log in and is enabled.
- Check to see if access restrictions are configured for the specified user account.

User Authorization test reports a failure

Symptom

The User Authorization test reports the status Failed.

Cause

Authorization failed with the provided user name and password.

Action

- Verify that the specified user name is part of the specified directory group.

- Check to see if access restrictions are configured for the specified user account.

Directory User Contexts test reports a failure

Symptom

The Directory User Contexts test reports the status Failed.

Cause

When iLO used the provided Directory Administrator Distinguished Name to search for a specified user context, the container was not found in the directory.

Action

1. Verify that the search contexts were entered correctly.

LOM Object Exists test reports a failure

Symptom

The LOM Object Exists test reports the status **Failed**.

Cause

iLO failed to locate the directory object specified by the **iLO Object Distinguished Name** configured on the **Security - Directory** page.

Action

- Verify that the LDAP FQDN of the iLO object is correct.

Remote Console issues

The following sections discuss troubleshooting Remote Console issues.

IMPORTANT:

Pop-up blocking applications, which prevent the automatic opening of new windows, prevent the Remote Console from running. Disable any pop-up blocking programs before you start the Remote Console.

iLO Java IRC displays red X when Firefox is used to run Java IRC on Linux client

Symptom

The Java IRC displays a red X icon when you run the Java IRC on a Linux system.

Cause

Firefox is not configured to accept cookies.

Action

1. Configure Firefox to accept cookies.

iLO Java IRC does not start

Symptom

The Java IRC fails to start when you do not accept the security warning and confirm that you want to run the application.

Cause

You cannot run the Java IRC without accepting the security warning and confirming that you want to run the application.

Action

1. Click the Clear button in the Java Console window.
2. To close the Java Console window, click the Close button.
3. Reset iLO.
4. Clear the browser cache.
5. Close the browser and open a new browser window.
6. Log in to iLO, start the Java IRC, and then accept the certificate.

Cursor cannot reach iLO Remote Console window corners

Symptom

The mouse cursor cannot be moved to the corners of the Remote Console window.

Action

1. Right-click and drag the mouse cursor outside the Remote Console window, and then drag it back inside.

iLO Remote Console text window not updated correctly

Symptom

When you use the Remote Console to display text windows that scroll at a high rate of speed, the text window might not be updated correctly.

Cause

This issue might occur when video updates happen faster than the iLO firmware can detect and display them. Typically, only the upper left corner of the text window is updated while the rest of the text window remains static.

Action

1. After the text window stops scrolling, click Refresh to update the Remote Console window.

Mouse or keyboard not working in iLO .NET IRC or Java IRC (Java Web Start)

Symptom

The mouse or keyboard does not work in the .NET IRC or Java IRC (Java Web Start option).

Solution 1

Action

1. Close the .NET IRC or Java IRC.
2. Navigate to the **Power Settings** page.
3. Clear the **Enable persistent mouse and keyboard** check box, and then click **Apply**.
4. Start the .NET IRC or Java IRC again.

Solution 2

Action

1. Right-click and drag the mouse cursor outside the Remote Console window, and then drag

it back inside.

Mouse or keyboard not working in iLO Java IRC (Java Applet)

Symptom

The mouse or keyboard does not work in the Java IRC (Java Applet option).

Solution 1

Action

1. Close the Java IRC.
2. Navigate to the Power Settings page.
3. Clear the Enable persistent mouse and keyboard check box, and then click Apply.
4. Start the Java IRC again.

Solution 2

Action

1. Right-click and drag the mouse cursor outside the Remote Console window, and then drag it back inside.

Solution 3

Action

1. Close the browser window and exit the browser.
2. Open the Java Control Panel.
3. Navigate to the Java Runtime Environment Settings dialog box.
4. Add the following runtime parameter: `-Dsun.java2d.d3d=false`.
5. Click OK and close the Java Runtime Environment Settings window.
6. Click Apply, and then click OK to close the Java Control Panel.
7. Viewing your changes before you click Apply might reset the Runtime Parameters dialog box, causing your edits to be lost.
8. Start the browser and log in to iLO.
9. Start the Java IRC again.

iLO .NET IRC sends characters continuously after switching windows

Symptom

When you switch to a different window, the .NET IRC sends characters continuously.

Cause

If you press a key during a .NET IRC session, and you switch windows, the key might remain pressed in the session. This situation causes the character to repeat continuously.

Action

1. Bring the Remote Console window to the front of your desktop by clicking the .NET IRC window.

iLO Java IRC displays incorrect floppy and USB key device information

Symptom

When the Firefox browser is used, the Java IRC might display incorrect floppy drive and USB key device information.

Cause

The client OS or Java software might be out of date.

Action

1. Make sure that Red Hat Enterprise Linux 6 or later is installed on the local client system.
2. Install the latest version of Java and configure it to connect through the Firefox browser.
3. Log in to the iLO web interface.
4. Insert a USB key or floppy disk on the local client system.
5. Verify that you can access the USB key or floppy disk.
6. Open a Java IRC session.
7. **Select** Virtual Drives **>** Image File Removable Media**.**
8. The **Choose Disk Image File** dialog box opens.
9. Type or select the path of the USB key or floppy disk (`/dev/disk`) inserted in the client.
10. You can also mount the USB key or floppy disk by label.
11. Click **OK**.

Caps Lock out of sync between iLO and Java IRC

Symptom

When you log in to the Java IRC, the Caps Lock setting might be out of sync between iLO and

the Java IRC.

Action

1. To synchronize the Caps Lock settings, select Keyboard > Caps Lock in the Java IRC.

Num Lock out of sync between iLO and Shared Remote Console

Symptom

When you log in to a Shared Remote Console session, the **Num Lock** setting might be out of sync between iLO and some of the Remote Console sessions.

Action

1. To synchronize the **Num Lock** settings, select **Keyboard** > **Num Lock** in the Remote Console.

Keystrokes repeat unintentionally during iLO Remote Console session

Symptom

A keystroke repeats unintentionally during a Remote Console session.

Solution 1

Cause

A network issue might be causing network latency.

Action

1. Identify and fix problems that might cause network latency.

Solution 2

Cause

The remote system settings are causing a delay.

Action

Adjust the following settings on the remote machine:

- Increase the typematic delay—This setting controls the delay before a character repeats when you press and hold a key on the keyboard.
- Decrease the typematic rate—This setting controls the rate at which a character repeats when you press and hold a key on the keyboard.
- The exact name of these settings varies depending on the OS you are using. For more information about changing the typematic delay and rate, see your OS documentation.

Session leader does not receive connection request when iLO .NET IRC is in

replay mode

Symptom

When a Remote Console session leader plays captured video data, a prompt is not displayed when another user requests to access or share the .NET IRC.

Cause

The request to access or share the .NET IRC timed out.

Action

1. Contact the other user or use the Remote Console acquire feature to take control of the .NET IRC.

iLO Remote Console keyboard LED does not work correctly

Symptom

The client keyboard LED does not reflect the state of the Remote Console keyboard.

Cause

The client keyboard LED does not reflect the true state of the Remote Console keyboard lock keys. The **Caps Lock**, **Num Lock**, and **Scroll Lock** keys are fully functional when you use the keyboard options in the Remote Console.

Action

1. No action needed.

iLO .NET IRC becomes inactive or disconnects

Symptom

The iLO .NET IRC becomes inactive or disconnects during periods of high activity. .NET IRC activity slows before becoming inactive. Symptoms of an inactive .NET IRC include the following:

- The .NET IRC display is not updated.
- Keyboard and mouse activity is not recorded.
- Shared Remote Console requests do not register.
- You can replay a captured video file, but the other .NET IRC features remain inactive.

Solution 1

Cause

Multiple users are logged in to iLO.

Action

- Reduce the number of simultaneous iLO user sessions.

- Reset iLO.

Solution 2

Cause

A connected Virtual Media session is being used to perform a continuous copy operation. The continuous copy operation takes priority and, consequently, the .NET IRC loses synchronization. Eventually, the Virtual Media connection resets multiple times and causes the USB media drive for the OS to lose synchronization with the Virtual Media client.

Action

- Reconnect to the .NET IRC and the Virtual Media.
- Reset iLO.

iLO .NET IRC failed to connect to server

Symptom

iLO displays the message `Failed to connect to server` when it attempts to establish a .NET IRC session.

Solution 1

Cause

The network response is delayed. The iLO .NET IRC client waits a specified amount of time for a connection to be established with iLO. If the client server does not receive a response in this amount of time, it displays an error message.

Action

2. Correct the network delay and retry the .NET IRC connection.

Solution 2

Cause

A Shared Remote Console session is requested, but the session leader delayed sending an acceptance or denial message. The iLO .NET IRC client waits a specified amount of time for a connection to be established with iLO. If the client server does not receive a response in this amount of time, it displays an error message.

Action

3. Contact the .NET IRC session leader and retry the request, or use the Remote Console acquire feature.

File not present after copy from server to iLO Virtual Media USB key

Symptom

If you copy files from a target server to an iLO virtual drive, the files are not visible in Windows

Explorer on the client computer.

Cause

File changes on an iLO Virtual Media USB key cannot be viewed in Windows Explorer by the user on the client computer.

Windows Explorer keeps a cached copy of the files on the USB key. The iLO Remote Console does not notify the Windows Shell when the USB key is updated with file changes. If you refresh the Explorer window, the cached information is sent back to the USB key, so the changed information cannot be viewed.

Action

1. Connect a USB key to a Windows client computer.
2. Start the .NET IRC, and connect the USB key by selecting it in the **Virtual Drives** menu.
3. Make file changes to the connected device (copy, delete, and so on).
4. To ensure that all data is updated on the device, unmount the device from the target server.
5. Disconnect the device by using the **Virtual Devices** menu in the .NET IRC.
6. Do not use Windows Explorer to refresh the contents of the USB key.
7. Use the **Safely Remove Hardware** feature to eject the device from the client computer.
8. Remove the device from the client computer.
9. When you connect the USB key to any computer, the file changes will be visible in Windows Explorer.

iLO .NET IRC takes a long time to verify application requirements

Symptom

When you start the .NET IRC from the iLO web interface, the **Launching Application** dialog box appears and remains on the screen for a long time.

Action

1. Open Internet Explorer.
2. Select **Tools** > **Internet Options**.
3. The **Internet Options** window opens.
4. Click the **Connections** tab, and then click the **LAN settings** button.
5. The **Local Area Network (LAN) Settings** window opens.
6. Clear the **Automatically detect settings** check box.
7. Optional: If needed, configure the proxy server settings.
8. Close all of the browser windows.

9. Restart the browser and start the .NET IRC.

iLO .NET IRC will not start

Symptom

When you start the .NET IRC, the **Cannot Start Application** dialog box appears with the message

`Application cannot be started. Contact the application vendor.`

Action

1. Clear the ClickOnce application cache by entering the following command from the Windows Command Prompt: **`rundll32 %windir%\system32\dfshim.dll CleanOnlineAppCache`**

iLO .NET IRC cannot be shared

Symptom

When you try to join a shared .NET IRC session, the **Unable to connect** dialog box appears with the message `Unable to connect to shared IRC. This might be due to a firewall blocking port 17990.`

Action

- Make sure that there is a communication path between the session leader .NET IRC client and each shared .NET IRC client.
- Make sure that the firewall settings on all clients allow an inbound connection to the Remote Console port (the default port is 17990).

iLO .NET IRC will not start in Firefox

Symptom

When you launch the .NET IRC in Mozilla Firefox, the application might fail to start.

Cause

If the iLO system uses the default iLO SSL certificate (not a signed trusted certificate) the iLO web interface uses HTTP instead of HTTPS to start the .NET IRC. Since the iLO web interface uses HTTPS, and the web interface starts the Remote Console by using HTTP, the browser displays a warning.

Action

- Import an SSL certificate into iLO and enable the IRC Requires a Trusted Certificate in iLO setting on the iLO Integrated Remote Console page. This configuration is the most secure solution.
- Click the shield icon in the address bar, and then select Options > Disable protection for

now.

- Use a different browser.

iLO .NET IRC will not start in Google Chrome

Symptom

When you launch the .NET IRC in Google Chrome, the application fails to start.

Cause

Previous versions of Google Chrome could run the .NET IRC with an NPAPI plug-in that supported ClickOnce. Google Chrome 42 and later does not support NPAPI-based plug-ins.

Action

- Use a different browser.
- Use the Java IRC.

Unable to boot to DOS using a USB key mounted with the iLO Remote Console

Symptom

An error occurs when you try to boot to a DOS-bootable USB key that is mounted by using the iLO Remote Console.

If the USB key is 2 GB or less, the following message is displayed:

```
Attempting Boot from CD-ROM
Attempting Boot from USB DriveKey (C:) Cannot load DOS! Any key to retry
```

If the USB key is larger than 2 GB, the server does not progress beyond following message:

```
Attempting Boot from USB DriveKey (C:)Boot from Drive Operating system load
error
```

Cause

The Remote Console does not have sufficient privileges to access the boot sector of the USB key.

Action

- Right-click Internet Explorer, and then select **Run as administrator**. Start the iLO web interface, launch the Remote Console, and then boot to the USB key.
- Plug the USB key directly into the server.

SSH issues

Initial PuTTY input slow with iLO

Symptom

During the initial connection to iLO through a PuTTY client, input is accepted slowly for approximately 5 seconds.

Action

Verify that the client configuration options are correct.

Clear the **Disable Nagle's algorithm** check box in the low-level TCP connection options.

PuTTY client unresponsive with iLO Shared Network Port

Symptom

When you use a PuTTY client with the Shared Network Port, the PuTTY session becomes unresponsive.

Cause

A large amount of data is being transferred or you are using a Virtual Serial Port and Remote Console.

Action

1. Close the PuTTY client and restart the session.

An SSH session fails to start or terminates unexpectedly

Symptom

An SSH session fails to start or terminates unexpectedly.

Cause

iLO is configured to use the Shared Network Port, and NIC teaming is enabled for the NIC the Shared Network Port uses. In this configuration, network communications might be blocked in the following cases:

- The selected NIC teaming mode causes the switch that iLO is connected with to ignore traffic from the server NIC/port that iLO is configured to share.
- The selected NIC teaming mode sends all traffic destined for iLO to a NIC/port other than the one that iLO is configured to share.

Action

1. Ensure that your Shared Network Port configuration follows the NIC teaming guidelines.

iLO Federation issues

Query errors occur on iLO Federation pages

Symptom

When you open an iLO Federation page, iLO peers and associated data might be missing from the page, and the following error is displayed:

```
Errors occurred during query, returned data may be incomplete or
inconsistent.
```

Cause

This error might occur when a network communication error, configuration problem, or failed iLO system prevents the retrieval of data from all systems in an iLO Federation group.

Action

- Wait for twice the configured **Multicast Announcement Interval**, and then refresh the iLO Federation page.

If an iLO system was reconfigured and can no longer communicate with the local iLO system, it will be dropped from its peer relationships after they expire.

- Check the **Multi-System Map** page for errors.

This page can help you identify communication problems between iLO peers.

- Verify that the switches in the network are configured to allow communication between iLO peers.
- If you changed the network routes, subnet mask, IP address, or HTTP port for an iLO peer, verify that the peer has a communication path to the local iLO system.
- Ensure that a communication path exists between the local iLO system and the peer with the error.

An intermediate firewall or a change to the iLO network configuration and HTTP port setting might block communication between the local iLO system and the peer.

A timeout error is displayed on the iLO Multi-System Map page

Symptom

The Multi-System Map page displays a `Timed Out` error for a peer of the local iLO system.

Cause

This error might occur in the following situations:

- A peer of the local iLO system has a peer that has failed.
- An intermediate firewall is preventing communication between the local iLO system and a peer.

- Network configuration changes are preventing communication between the local iLO system and a peer.
- The enclosure that contains the peer is not configured for iLO Federation support.

Action

- Remove or repair the failed peer.
- Verify that the network is configured to allow communication between the iLO peers.

iLO Multi-System Map page displays a 502 error

Symptom

The Multi-System Map page shows a 502 error.

Cause

The listed peer rejected a request from the local iLO system.

Action

1. Ensure that a communication path exists between the local iLO system and the peer with the error.

An intermediate firewall or a change to the iLO network configuration and HTTP port setting might block communication between the local iLO system and the peer.

iLO Multi-System Map page displays a 403 error

Symptom

The **Multi-System Map** page shows a 403 Forbidden/Authorization error.

Cause

The group key on the local iLO system does not match the group key on a peer iLO system.

Action

1. Ensure that the group key matches for all iLO systems that are members of the selected group.

iLO peers are not displayed on iLO Federation pages

Symptom

iLO peers (systems in the same group as the local iLO system) are not displayed on iLO Federation pages.

Action

- Ensure that the group key matches for all iLO systems that are members of the selected group.

- Wait for twice the configured multicast interval, and then refresh the iLO Federation page.

If an iLO system was reconfigured and can no longer communicate with the local iLO system, it will be dropped from its peer relationships after they expire.

- Verify that the switches in the network are configured to allow communication between iLO peers.
- Ensure that a communication path exists between the local iLO system and the peer with the error.

An intermediate firewall or a change to the iLO network configuration and HTTP port setting might block communication between the local iLO system and the peer.

iLO peers are displayed with IPv6 addresses on IPv4 networks

Symptom

iLO peers on an IPv4 network are displayed with IPv6 addresses on iLO Federation pages.

Action

Verify that the iLO Client Applications use IPv6 first check box is not selected on the iLO Dedicated Network Port - IPv6 page.

Firmware update issues

Unsuccessful iLO firmware update

Symptom

The following issues occur when you try to update the iLO firmware:

- iLO firmware is not responding.
- iLO did not accept the firmware update request.
- An iLO firmware update stopped before the update was complete.

Solution 1

Cause

A communication or network issue occurred.

Action

1. Attempt to connect to iLO through the web browser. If you cannot connect, there is a communication issue.
2. Attempt to ping iLO. If you are successful, the network is working.
3. Try the firmware update again.

Solution 2

Action

1. Try a different firmware update method.

iLO firmware update error

Symptom

The following error is displayed during a firmware update:

```
The last firmware update attempt was not successful. Ready for the next
update.
```

Cause

An incorrect file was used to update the iLO firmware.

Action

1. To reset the flash process, click **Clear Error**, and then try the firmware update again with the correct firmware file.

If you do not clear the error, the same error might occur even when you use the correct firmware file.

iLO network Failed Flash Recovery

Most firmware upgrades finish successfully. In the unlikely event of server power loss during an iLO firmware upgrade, iLO might be recoverable when power is restored.

When the iLO starts, the startup code performs image validation on the main image. If the image is corrupted or incomplete and it cannot be recovered automatically with the Secure Recovery feature, iLO enters Failed Flash Recovery mode. Failed Flash Recovery activates an FTP server within iLO. The FTP server enables you to send an image to iLO for programming. The FTP server does not provide any other services.

This feature is available only if iLO is configured to use the Production security state.

A network client can connect to the FTP server. The user name for the connection is **test**, and the password is **flash**. To send a firmware image to iLO, use the FTP client `PUT` command. After receiving the image, iLO validates the image. If the image is a complete, signed, and valid firmware image, the kernel begins programming the FLASH partition.

After the image is programmed into the FLASH partition, reset iLO by issuing the `RESET` command to the iLO FTP server.

Example:

```
F:\ilo>ftp 192.168.1.2
Connected to 192.168.1.2.
220 FTP Recovery server ready. User (192.168.1.2:(none)): ftp
331 Password required. Password:
231 Logged in. ftp> put iLO.bin
200 Ok.
150 ready for file 226-Checking file 226-File acceptable
226-Flashing     3% complete
226-Flashing     4% complete
226-Flashing     6% complete
.
.
.
226-Flashing     97% complete
226-Flashing     99% complete
226-Flashing 100% complete 226-Flashing completed
226 Closing file
ftp: 8388608 bytes sent in 1.38Seconds 6100.81 Kbytes/sec. ftp> quote reset
221 Goodbye (reset).
Connection closed by remote host. ftp> quit
```

More Information

Server power-on

Licensing issues

License key installation errors

Symptom

You see a License Key Erroror a License Installation Failedmessage.

Solution 1

Cause

The key is not an iLO license key.

Action

1. Obtain an iLO license key, and then try again.

Solution 2

Cause

An evaluation key was submitted when a regular license was previously installed.

Action

1. None. iLO does not support installing an evaluation key when a regular key was previously installed.

Solution 3

Cause

The iLO date and time settings are incorrect.

Action

1. Check the iLO date and time settings, and then try again.

Solution 4

Cause

The license key entered is incorrect.

Action

1. Check for errors in the license key, and then try again.

Unable to access Virtual Media or graphical Remote Console

Symptom

The Virtual Media and graphical Remote Console features are unavailable.

Cause

You enable the iLO Virtual Media and graphical Remote Console features by installing an optional iLO license. If a license is not installed, a message informs you that these features are not available without a license.

Action

1. Install an iLO license that supports these features.

Agentless Management, AMS, and SNMP issues

AMS is installed but unavailable in iLO

Symptom

AMS is installed on a server, but it is listed as Not available in the iLO web interface.

Action

1. Verify that AMS is installed.
2. Restart AMS.
3. Reset iLO.

A. iLO license options

Table 4 lists the features that are included with each iLO license.

Table 4 iLO standard and licensed features

Feature	Onboard features (Standard)	License for Remote Management (Advanced) N8115-33	License for Remote Management (Scale-Out) N8115-34	License for Remote Management (Essentials) N8115-36
Directory Service Authentication (Active Directory, LDAP)	×	○	×	×
Kerberos Authentication	×	○	×	×
Virtual Media via Integrated Remote Console	×	○	×	○
Scripted Virtual Media	×	○	×	×
Integrated Remote Console(IRC)	Pre-OS only	○	Pre-OS only	○
Global Team Collaboration via Integrated Remote Console	×	○	×	×
Integrated Remote Console Record and Playback	×	○	×	×
Virtual Serial Port Record and Playback	×	○	○	×
Text-based Remote Console via SSH	×	○	○	×
Email-Based Alerting	×	○	○	○
Remote Syslog	×	○	○	×
Advanced Power Management(Power History Graphs, Dynamic Power Capping)	×	○	○	×
iLO Federation Management	×	○	○	×
iLO Federation Discovery	○	○	○	○
Virtual Serial Port	○	○	○	○
Server Health Summary	○	○	○	○
Rebooting iLO	○	○	○	○
Redfish® API	○	○	○	○
Agentless Management	○	○	○	○
Embedded Health System	○	○	○	○
Web-Based GUI	○	○	○	○
Virtual Power Buttons	○	○	○	○
SSH Command Line Interface /SMASH (Including serial console redirection)	○	○	○	○
IPMI/DCMI (Including serial console redirection)	○	○	○	○

B. Ports used in iLO

iLO uses the TCP/IP and UDP/IP ports listed below.

Table 5 iLO uses the TCP/IP and UDP/IP ports

Module name	iLO Port #	Direction	Protocol	Port #
Secure Shell (SSH)	22[*1]	⇔	TCP	Dynamic[*6]
Web Non-SSL	80[*1]	⇔	TCP	Dynamic[*6]
NetBIOS-NS	137	⇔	UDP	Dynamic[*6]
SNMP	161[*1]	⇔	UDP	Dynamic[*6]
Web SSL	443[*1]	⇔	TCP	Dynamic[*6]
IPMI/DCMI over LAN	623[*1]	⇔	UDP	Dynamic[*6]
Universal Plug and Play	1900	⇔	UDP	Dynamic[*6]
Link-Local Multicast Name Resolution(LLMNR)	5355	⇔	UDP	5355
Virtual Media	17988[*1]	⇔	TCP	Dynamic[*6]
Remote Console	17990[*1]	⇔	TCP	Dynamic[*6]
SMTP	Dynamic[*6]	⇔	TCP	25[*2]
DNS	Dynamic[*6]	⇔	UDP	53
Web Non-SSL	Dynamic[*6]	⇔	TCP	80[*5]
Kerberos KDC	Dynamic[*6]	⇔	TCP	88[*3]
NTP	Dynamic[*6]	⇔	UDP	123
SNMP Trap	Dynamic[*6]	⇔	UDP	162[*1]
Web SSL	Dynamic[*6]	⇔	TCP	443[*5]
Remote Syslog	Dynamic[*6]	⇔	UDP	514[*4]
LDAP	Dynamic[*6]	⇔	TCP	636[*3]

[1] Change the port number on Security - Access Settings page.

[2] Change the port number on Management - AlertMail page.

[3] Change the port number on Security - Directory page.

[4] Change the port number on Management - Remote Syslog page.

[5] Depending on the URL.

[6] The Dynamic ports are dynamically allocated ports and usually ranged from 1024 to 65535.

Glossary

3DES	Triple DES, the Data Encryption Standard cipher algorithm.
ABEND	Abnormal end.
ACPI	Advanced Configuration and Power Interface.
AES	Advanced Encryption Standard.
AHS	Active Health System (AHS) monitors the status/configuration of the server, and records it to a log file if any changes occur. AHS log is used for maintenance to investigate the failure.
AMP	Advanced Memory Protection (AMP) is a technology for realizing a fault tolerance of the server by memory redundancy (such as mirroring).
AMS	Agentless Management Service (AMS) is an OS service for sending information (such as OS events) that iLO cannot collect directly. iLO records the information recieved by AMS, and send it to Agentless Management.
API	Application Programming Interface.
ARP	Address Resolution Protocol.
ASR	Automatic Server Recovery.
BIOS	Basic Input/Output System.
BMC	Baseboard management controller.
CA	Certificate authority.
CLP	Command Line Protocol.
CN	Common Name.
COM port	Communication port.
cookie	A small, unscriptable text file placed on your hard drive by a website to preserve specific settings. When you return to the site, your system opens the cookie with the previously saved settings so they can be passed along to the site. Cookies are also used to store session data temporarily.
CR	Certificate request.
CSR	Certificate Signing Request.
CSV	Comma-separated value.
DCMI	Data Center Manageability Interface.
DD	A Unix program used to convert and copy a file.
DDNS	Dynamic Domain Name System.
DDR	Double data rate.
DER	Distinguished Encoding Rules.
DHCP	Dynamic Host Configuration Protocol.
DHE	Diffie–Hellman key exchange.
DIMM	Dual in-line memory module. A small circuit board holding memory chips.
DLL	Dynamic-link library.
DMTF	Distributed Management Task Force.
DN	Distinguished Name.
DNS	Domain Name System.
DSA	Digital Signature Algorithm.
DVO	Digital Video Out.
ECC	Error-correcting code.

EMS	Emergency Management Services.
Express Report Service	Software that can report the server failure to the contact center by E-mail or modem. This software is installed with NEC ESMPRO ServerAgentService to the server.
Express Report Service (HTTPS)	Software that can report the server failure to the contact center by HTTPS. This software is installed with NEC ESMPRO ServerAgentService to the server.
EXPRESSBUILDER	Software for setting up the server. EXPRESSBUILDER can be started by pressing <F10> key during POST.
FAT	File Allocation Table.
FIPS	Federal Information Processing Standard.
FQDN	Fully Qualified Domain Name.
FSMO	Flexible Single Master Operations.
GMT	Greenwich Mean Time.
GRUB	Grand Unified Bootloader.
HEM	High Efficiency Mode.
Hexalobular	A type of screw head characterized by a 6-point star-shaped pattern. This is often called as "Torx" (the Torx is another company's trademark). Head sizes are described from T1 to T100. This is sometimes abbreviated as 6lobe.
ICMP	Internet Control Message Protocol.
IDE	Integrated Drive Electronics.
IETF	Internet Engineering Task Force.
IIS	Internet Information Services.
iLO	A built-in controller that supports the IPMI version 2.0 protocol. The controller is called as iLO5 because this server adopts a generation 5 version controller.
IML	Integrated Management Log.
IPMI	Intelligent Platform Management Interface.
IRC	Integrated Remote Console.
ISO	International Organization for Standardization.
Java IRC	Java version of the Integrated Remote Console.
JRE	Java Runtime Environment.
JSON	JavaScript Object Notation.
KCS	Keyboard Controller Style.
KDC	Key Distribution Center.
KDE	K Desktop Environment (for Linux).
KVM	Keyboard, video, and mouse.
LDAP	Lightweight Directory Access Protocol.
LDIFDE	A utility that allows you to import and export information to and from Active Directory.
LILO	Linux Loader.
LOM	Lights-Out Management.
MAC	Media Access Control.
MD5	Message-Digest algorithm 5.
MIB	Management Information Base. A database of managed objects accessed by network management protocols. An SNMP MIB is a set of parameters that an SNMP management station can query or set in the SNMP agent of a network device (for example, a router).
MIME	Multipurpose Internet Mail Extensions.

MLD	Multicast Listener Discovery.
MMC	Microsoft Management Console.
MSA	Mail Submission Agent.
MTA	Mail Transfer Agent.
NAND	A partition of non-volatile flash memory that is embedded on the system board. The NAND flash is used for files such as Active Health System data and the EXPRESSBUILDER software.
NEC ESMPRO Manager	Software for managing a number of servers on network.
NEC ESMPRO ServerAgentService	Software for monitoring the server. This works with NEC ESMPRO Manager. You can choose Service Mode or Non-Service Mode when installing this software. Service Mode resides as the OS service and Non-Service Mode does not use the OS service to reduce memory, CPU power, and other OS resources.
NIC	Network interface card. A device that handles communication between a device and other devices on a network.
NMI	Non-maskable interrupt.
NTLM	NT LAN Manager.
NTP	Network Time Protocol.
NVMe	Non-Volatile Memory Express.
OU	Active Directory Organizational Units.
PAL	Programmable Array Logic.
PC for Management	A computer for managing the server on network. A general Windows/Linux computer can be used as "PC for Management".
PIM	Protocol-Independent Multicast.
PKCS	Public-key cryptography standards.
POST	Power-on self test.
Product Info Collection Utility	Software for collecting several hardware/software statuses and event logs. You can easily collect the data for the server maintenance by using this software.
PuTTY	A terminal emulator that can act as a client for the SSH, Telnet, rlogin, and raw TCP protocols and as a serial console client.
RAID Report Service	A service that monitors the RAID system of the server and sends information to NEC ESMPRO if the RAID system has a failure.
RBSU	ROM-Based Setup Utility (RBSU) is a built-in utility that can configure connected devices and BIOS settings. RBSU is called from System Utilities.
REST	Representational State Transfer.
RESTful Interface Tool	A tool that supports API based on Representational State Transfer (REST) architecture. You can send maintenance commands in JSON format to iLO by HTTP protocol after installing this tool.
RPM	RPM Package Manager.
RSA	An algorithm for public-key cryptography.
SAID	Service Agreement Identifier.
SAS	Serial Attached SCSI.
SATA disk	Serial ATA (SATA) disk. The evolution of the ATA (IDE) interface that changes the physical architecture from parallel to serial and from primary-secondary (master-slave) to point-to-point. Unlike parallel ATA interfaces that connect two drives; one

	configured as primary (master), the other as secondary (slave), each SATA drive is connected to its own interface.
SD	Secure Digital.
SHA	Secure Hash Algorithm.
SID	System Insight Display (SID) is an optional product that can indicate the statuses of each device on motherboard.
SLAAC	Stateless address autoconfiguration.
SMASH	Systems Management Architecture for Server Hardware.
SMS	System Management Software.
SNMP	Simple Network Management Protocol.
SNTP	Simple Network Time Protocol.
SPN	Service principal name.
SPP	Standard Program Package (SPP) is a software package that includes BIOS, FW, driver, and other basic software. SPP is included in Starter Pack.
SSA	Smart Storage Administrator (SSA) is a utility that can configure RAID arrays. SSA is provided for Windows/Linux and can also start from F10 key function.
SSD	Solid-state drive.
SSH	Secure Shell.
SSL	Secure Sockets Layer.
SSO	Single Sign-On.
Starter Pack	A software package that includes SPP, instruction manual, application, and other software for the server. This must be installed before using OS on the server. Starter Pack is provided as an optional product and ISO data on our website.
SUM	Software Update Manager.
System Maintenance Switch	A DIP switch on motherboard. This switch can enable/disable initialization, password, iLO settings, and other functions of maintenance.
System Utilities	System Utilities is a built-in utility that provides system information, calling RBSU, collecting system log, and other system utilities. You can start System Utilities by F9 key during POST.
TLS	Transport layer security.
TM	Trusted Module.
TPM	Trusted Platform Module.
TPM Kit	An optional product of Trusted Platform Module for the server.
UDP	User Datagram Protocol.
UEFI	Unified Extensible Firmware Interface.
UHCI	Universal Host Controller Interface.
UID	Unit identification.
UPN	User principal name.
UPnP	Universal Plug and Play.
UPS	Uninterruptible Power Supply.
USB	Universal serial bus. A serial bus standard used to interface devices.
USM	User-based Security Model.
UTC	Coordinated Universal Time.
UTP	Unshielded twisted pair.
UUID	Universally unique identifier.

VSP	Virtual Serial Port.
WBEM	Web-Based Enterprise Management.
WINS	Windows Internet Name Service.

NEC Express Server

iLO 5 User's Guide

October 2017
NEC Corporation
7-1 Shiba 5-Chome, Minato-Ku
Tokyo 108-8001, Japan