Supplement of iLO FW Updating

Thank you for purchasing our product. This document provides the precautions on the updating of iLO firmware. If you do not follow this document, a trouble, such as a start failure of the server, may occur. Read this instruction carefully, in order to prevent any error in the update operations. Furthermore, if the server malfunctions or the power is disconnected, due to blackout, thunder, disconnection, noise and other unexpected accidents during rewriting the data, in the worst case, damage occurs in the server and it does not work properly. In these cases, you might be responsible for paying for the repairs.

- Do not refresh the web browser screen by using the browser's reload button or pressing F5 key during updating the iLO FW. If you refresh the screen and the updating is unable to finish, reset the iLO.
- A TPM or TM is installed in this server. Before updating a system ROM or iLO firmware, suspend or back up any software that stores data on the TPM or TM. For example, if you use drive encryption software, suspend it before updating a firmware. Failure to follow these instructions might result in losing access to your data. Suspend software that uses TPM or TM before you update System ROM (BIOS) or iLO firmware.
- Reconfigure the SNMPv3 alert settings by using iLO web interface when updating from iLO firmware 1.10/1.15 to 1.30. Reconfigure the settings after updating when the server enables the SNMPv3 alert function.
- The SMTP Secure Connection (SSL/TLS) of AlertMail settings in iLO web interface is set to enable when you update to iLO firmware 1.30 by this procedure. If you have enabled iLO AlertMail in previous iLO version, reconfigure AlertMail settings in accordance with your environment.
- On iLO FW 1.30, you can restore the iLO settings backed up by iLO FW 1.20 but you cannot restore the other version's backed up data. After operating this step, you need

to configure the alert mail settings again because SMTP Secure and SMTP auth settings are newly added in iLO 1.30.

- To recover from losing iLO license key and iLO settings due to a hardware failure, we recommend that you back up the iLO settings by using the backup and restore function after updating iLO firmware.

- In addition to updating this iLO firmware, update the following firmware and software.
  a) System ROM (BIOS): Applying from Standard Program Package on Starter Pack.
  b) Agentless Management Service: Applying from Standard Program Package on Starter Pack.
  c) NEC ESMPRO ServerAgentService: Applying from Applications on Starter Pack.
  d) Product Info Collection Utility: Applying from Applications on Starter Pack.
  e) RESTful Interface Tool: Applying from Applications on Starter Pack.
  f) NEC ESMPRO Manager: See "*Supplement of ESMPRO updating*".
  g) Express Report Service (MG) Receiving Information: See "*Supplement of ESMPRO updating*".
- When viewing the System Information tree in iLO 5 web interface, the Smart Array firmware displays a different version than the version in the Storage Information tab.

- When iLO 5 web interface session is timed out, HTML5 IRC remote console session is also disconnected. If you want to install OS by using virtual media, use another IRC remote console.

- About IPMI 2.0 RCMP+ Authentication Remote Password Hash Vulnerability (RAKP).

  Perform any of the following:

  - When you do not need to use IPMI, disable it. You can disable IPMI on iLO by using the Disable IPMI over LAN command. IPMI over LAN is disabled by default on iLO 5.

  - Maintain the latest iLO firmware that contains the most recent security patches.

  - Employ best practices in the management of the protocols and passwords on your systems and networks. Use strong passwords wherever possible.

  - If you have to use IPMI, use a separate management LAN or VLAN, Access Control Lists (ACLs), or VPN to limit and restrict access to your iLO management interfaces.

- iLO 5 .NET Integrated Remote Console (IRC) does not launch from the Microsoft Edge 42 web browser. Perform any of the following:

- Install a trusted certificate, and then enable the Integrated Remote Console Trust Setting located on the Remote Console & Media -> Security tab. This will prevent the redirection to HTTP and allow the .NET application to be trusted.
- Click the "See all content" button from the blocked content menu to authorize untrusted content for the current session. Microsoft Edge will then reload the window and allow the .NET integrated remote console to launch as in prior versions of the web browser.
- Use Internet Explorer 11 to launch the .NET integrated remote console.
- Use the standalone .NET console application.

- When the untrusted certificate warning pop-up window is displayed on iLO 5 web interface with the Microsoft Edge 42 web browser, perform either of the following:
  - Click the "Details" link on the popup window, and then click "Go on to the webpage" link to proceed. This will be required each time a help topic is opened in a pop-up window.
  - Use a different web browser that does not prompt to trust the sites untrusted certificate each time.
- Update to .NET Framework version 4.5.1 or later when you use iLO 5 .NET Integrated Remote Console (IRC) after installing this firmware.
- The remote console thumbnail in the iLO5 web interface may not be displayed on some systems with Microsoft Edge 42 web browser. To view the remote console thumbnail, use Internet Explorer 11 or another web browser (Firefox, Chrome mobile/Desktop) besides the Microsoft Edge 42 web browser.
- On any server running VMware VMware ESXi 6.0,VMware ESXi 6.5 or VMware ESXi 6.7 with iLO 5 version 1.30, warnings on some of the sensors viewed in the hardware status tab in the vSphere Web Client will be displayed. The warnings described in this advisory do not have any impact on production and can be safely ignored.
- Power supply status changes (such as loss of AC power to a supply, an unplugged power cable, or the supply experiencing a general failure) in iLO5 web interface may be delayed.
- Peak server power in iLO5 web interface may exceed power supply capacity for short periods of time.

- Device inventory page in iLO5 web interface may display a parse error on Internet Explorer 11 when certain PCI cards (unsupported Ethernet 10Gb 2-port 560SFP+ Adapter) are installed.

Revision History

Sep 11, 2018 iLO Firmware 1.38

- Fix the issue that the OS panic or OS stall may be happen in Linux or VMware.

Aug 14, 2018 iLO Firmware 1.35

- Fix for improper Smart Array error reported: Cache module board backup power failed.
- Fixed where iLO5 may become unresponsive after ejecting virtual media.
- Changed the design of the icons that indicate privilege level of user or group in web interface.

This version adds support for the following features and enhancements:

- VGA Port Detect Override--Controls how devices connected to the system video port are detected. Dynamic detection protects the system from abnormal port voltages. This setting is enabled by default, and can be used for troubleshooting cases when there is no video output to displays, KVM concentrators, or active dongles.
- DHCP Client ID override via iLO5 RESTful API.
- Modified the following security vulnerability.
  - Remote execution of arbitrary code, Local Disclosure of Sensitive Information(CVE-2018-7105)

May 31, 2018 iLO Firmware 1.30

- When you use iLO Virtual Media to install an operating system, installation might fail when iLO is configured to use the Shared Network Port.
- In rare cases, a server runs out of available SSH sessions because the sessions are not reclaimed when a client disconnects.
- iLO 5 unexpectedly restored itself to the factory default settings when a user did not initiate the process.
- When Auto Power-On is set to Always Power On or Restore Last Power State, the server might not power on after a cold reset.
- NVMe drive model numbers are incorrect or inconsistent.
- Added support for RSA-PSS certificate signatures.
- If ” Web Server Non-SSL Port” is set to value except for the default port number, EXPRESSBUILDER is not launched.

- If ”Web Server Non-SSL Port” is set to value except for the default port number, JAVA IRC is not launched.
- When the same time zone is set between BIOS and iLO, the system time will be incorrect time.
- iLO cannot display Express5800/R120h-1M and R120h-2M standard network adapter(Ethernet 1Gb 4-port 331i) MAC address.
- The significant improvements to the write algorithm for the embedded 4 GB non-volatile flash memory (also known as the NAND). These improvements increase the NAND lifespan.
- Improved HTML5 IRC performance, including:
  - Added virtual keys to improve the ability to send keyboard actions to the server.
  - Added the ability to configure the keyboard layout in the HTML5 IRC
  - Added Virtual Media support for local ISO and IMG files.
- Firmware and software update enhancements:
  - iLO users can now view, create, and delete maintenance windows.
  - A new check box allows users to clear the installation queue when initiating an install set.
  - Updated the iLO RESTful API and iLO web interface to report when a reboot is required after an installation task completes.
- Each time iLO starts, it backs up the iLO configuration to the nonvolatile flash memory (NAND). If the SRAM is erased, the configuration is automatically restored.
- AlertMail now supports SSL (TLS) for secure email.
- AlertMail now supports external SMTP mail servers.
- Added an SNMP trap for when all host NICs are down.
- Updated to OpenSSL-1.0.2u-fips-2.0.16.
- Added the list of open source licenses to the login page.
- Added Intelligent System Tuning features to the iLO web interface. From the iLO web interface, you can view the configured settings, configure Jitter Smoothing, and launch Intelligent Provisioning to configure Workload Matching and Core Boosting.
- Improved Active Health System logging efficiency to prolong the NAND lifespan.
- Added iLO health status to the Overview page. If the status is Degraded, this value is also displayed on the Login page.
- Re-signed the Java IRC to extend the certificate expiration date.
- Re-signed the .NET IRC to extend the certificate expiration date.
  With this enhancement, the .NET IRC requires version 4.5.1 or later of the .NET Framework.
- Added the ability to remove an SSL certificate and regenerate the iLO self-signed certificate.

- Modified the following security vulnerability.
  - Alert Regarding Vulnerability in Drupal(CVE-2018-7600)
  - Remote or Local Code Execution(CVE-2018-7078)
  - Remote Code Execution and Denial of Service Vulnerability(CVE-2018-0101)

Feb 2, 2018 iLO Firmware 1.20

- Support for HTML5 Integrated Remote Console (IRC) in English keyboard environment.
- Support for a mouse wheel in Integrated Remote Console (IRC).
- Support for IPv6 on Shared Network Port.
- Support for iLO Federation on Shared Network Port.
- Support for importing SSL certificates of the RSA-PSS algorithm.
- Support for SNMPv3 Inform notification.
- Enhanced SNMP alert function, which enables to select any of SNMPv1 Trap, SNMPv3 Trap, and SNMPv3 Inform, for each alert destination.
- Enhanced SNMP alert function, which enables to configure the engine ID for each SNMPv3 user.
- The maximum number of the registerable alert destinations increased to 8.
- The maximum number of the registerable SNMPv3 users increased to 8.
- Support for periodic HAS Trap function.
- Support for new “Add to Queue” pane on enhanced firmware and software update page.
- Support for “Remove All” option on enhanced firmware and software update page.
- Support for “Update Recovery Set” option on enhanced firmware and software update page.
- Support for the function to display the names of software installed in OS and/or running software in Japanese on Web interface. (Agentless Management Service needs to be updated.)
- Support for properties of NVMe drive on RESTful API.
- Support for device inventory on RESTful API.
- Support for Service Account option to distinguish iLO user accounts used in management software and the like.
- Change the IML event recorded when the status of system LAN is changed.
- Improved the problem that the System ROM (BIOS) version is missing in AlertMail messages.
- Improved the problem that Virtual Media devices are inaccessible when two virtual devices are mounted simultaneously.
- Improved the problem that a floppy image connected through a script virtual media is always mounted read-only.

- Improved the problem that the alert is not always issued in case FQDN is specified in the address of the remote Syslog server.
- Improved the problem that the alert is not always issued in case FQDN is specified in the SMTP server and the IPv6 address is returned when the name is resolved.

Aug 17, 2017 iLO Firmware 1.15

- Support for the functions to backup and restore the iLO configuration.
- Support for diffie-hellman-group-exchange-sha256 as SSH Key Exchange authentication method.
- Support for multiple destination AlertMail email addresses. Enter the addresses separated by a semicolon.
- Support for Power Cycle on RESTful API.
- Support for properties of High Efficiency Mode on RESTful API.
- Support for properties of Cache Module Serial Number on RESTful API.
- Support for properties of Login Security Banner on RESTful API.
- Support for properties of Current Power On Time on RESTful API. (Provides the time since the system was last powered on.)
- Support for properties of Persistent Mouse/Keyboard Enabled on RESTful API.
- Support for properties of current Cipher Suite on RESTful API.
- Support for propagate NTP Time to Host function to transfer the time which iLO obtained from SNTP server to the host, at the first POST after turning AC to ON.
- Improved the problem that the iLO web interface intermittently displays incorrect memory status after a system reset.
- Improved the problem that the server power page stalls when loading the server power information.
- Improved the problem that Virtual Media status is not displayed in the Java IRC.
- Improved the problem that the local client keyboard might get disabled when the Java IRC is in use.
- Improved the problem that the maximum available power is displayed incorrectly.
- Improved the problem that the first attempt to clear IML fails if the IML contains a maintenance note.
- Improved the problem that secure boot cannot be configured through the RESTful API, even if the pending configuration is in UEFI mode.
- Improved the problem that Onetimeboot and Continuousboot do not take effect in RESTful API.
- Improved the problem that an iLO web interface error occurs after an installed SSL certificate was deleted by using the RESTful API.

- Improved the problem that an iLO Federation authentication error might occur when group names with unsupported characters are used in URLs without correct encoding.
- Improved the problem that a false positive “Insecure Cache Management Policy” issue is reported by some security scanners.
- Improved the problem that iLO federation group cannot be created by the one or two-byte group key.

Jun 7, 2017 iLO Firmware 1.10

- Initial release.