NEC

Maintenance Guide

NEC Express Server
Express5800 Series

Express5800/R120h-1M, R120h-2M
EXP804, EXP805

10.201.01-104.02
November 2017

Manuals

Booklets	
Safety Precautions and Regulatory Notices	Describes points of caution to ensure the safe use of this server. **Read these cautions before using this server.**
Getting Started	Describes how to use this server, from unpacking to operations. See this guide first and read the outline of this product.
The electronic edition has been published on a website (http://www.nec.com/express/).	
User's Guide	
Chapter 1: General Description	Overviews, names, and functions of the server's parts
Chapter 2: Preparations	Installation of additional options, connection of peripheral devices, and suitable location for this server。
Chapter 3: Setup	System Utility configurations and summary of EXPRESSBUILDER
Chapter 4: Appendix	Specifications and other information
Installation Guide (Windows)	
Chapter 1: Installing Windows	Installation of Windows and drivers, and precautions for installation
Chapter 2: Installing the Bundled Software	Installation of NEC ESMPRO, and other bundled software
Maintenance Guide	
Chapter 1: Maintenance	Server maintenance and troubleshooting
Chapter 2: Useful Features	The details of System Utility, RAID Configuration Utility, Starter Pack, and EXPRESSBUILDER
Chapter 3: Appendix	Error messages and Windows Event Logs
Other manuals	
The details of NEC ESMPRO, and other features	

Contents

Conventions Used in This Document

Signs and symbols for safety

WARNING and CAUTION are used in this guide as the following meaning.

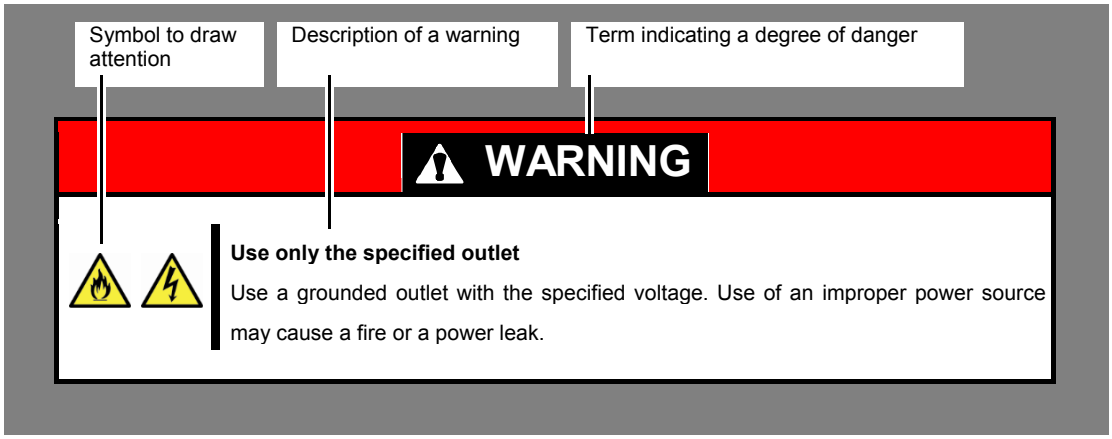
⚠ WARNING Indicates there is a risk of death or serious personal injury

⚠ CAUTION Indicates there is a risk of burns, other personal injury, or property damage

Precautions and notices against hazards are presented with one of the following three symbols. The individual symbols are defined as follows:

	**Attention**	This symbol indicates the presence of a hazard if the instruction is ignored. An image in the symbol illustrates the hazard type.	(Example) 
	**Prohibited Action**	This symbol indicates prohibited actions. An image in the symbol illustrates a particular prohibited action.	(Example) 
	**Mandatory Action**	This symbol indicates mandatory actions. An image in the symbol illustrates a mandatory action to avoid a particular hazard.	(Example)  (Disconnect a plug)

(Example)



Notations used in the text

In addition to safety-related symbols urging caution, three other types of notations are used in this document. These notations have the following meanings.

Important	Indicates critical items that must be followed when handling hardware or operating software. If the procedures described are not followed, **hardware failure, data loss, and other serious malfunctions could occur**.
Note	Indicates items that must be confirmed when handling hardware or operating software.
Tips	Indicates information that is helpful to keep in mind when using this server.

Optical disk drive

This server is equipped with one of the following drives. These drives are referred to as *optical disk drive* in this document.

- **DVD-ROM drive**
- **DVD Super MULTI drive**

Hard disk drive

Unless otherwise stated, *hard disk drive* described in this document refer to both of the following.

- **Hard disk drive (HDD)**
- **Solid state drive (SSD)**

Abbreviations of Operating Systems (Windows)

Windows Operating Systems are referred to as follows.

See *Chapter 1* (*1.2 Supported Windows OS)* in *Installation Guide (Windows)* for detailed information.

Notations in this document	Official names of Windows
Windows Server 2016	Windows Server 2016 Standard
	Windows Server 2016 Datacenter
Windows Server 2012 R2	Windows Server 2012 R2 Standard
	Windows Server 2012 R2 Datacenter

POST

POST described in this manual refers to the following.

- **Power On Self-Test**

BMC

BMC described in this manual refers to the following.

- **Baseboard Management Controller**

The device employs iLO5 as a BMC.

Trademarks

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

Intel, Pentium, and Xeon are registered trademarks of Intel Corporation of the United States.

Linux is a trademark or registered trademark of Linus Torvalds in Japan and other countries.

Red Hat and Red Hat Enterprise Linux are trademarks or registered trademarks of Red Hat, Inc. in the United States and other countries.

Broadcom, NetXtreme, LiveLink, Smart Load Balancing are registered trademarks or trademarks of the Broadcom Corporation in the U.S. and other countries.

SD and microSD are trademarks or the registered trademarks of SD-3C in the United states and other countries.

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

All other product, brand, or trade names used in this publication are the trademarks or registered trademarks of their respective trademark owners.

License Notification

Open source software of following license is included in the part of this product (system utility).

- UEFI EDK2 License
- The MIT License Agreement
- PNG Graphics File Format Software End User License Agreement
- zlib End User License Agreement

UEFI EDK2 License

UEFI EDK2 Open Source License

Copyright (c) 2012, Intel Corporation. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

==========

UEFI FAT File System Driver Open Source License

Copyright (c) 2006, Intel Corporation. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

. Neither the name of Intel nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Additional terms: In addition to the forgoing, redistribution and use of the code is conditioned upon the FAT 32 File System Driver and all derivative works thereof being used for and designed only to read and/or write to a file system that is directly managed by Intel's Extensible Firmware Initiative (EFI) Specification v. 1.0 and later and/or the Unified Extensible Firmware Interface (UEFI) Forum's UEFI Specifications v.2.0 and later (together the "UEFI Specifications"); only as necessary to emulate an implementation of the UEFI Specifications; and to create firmware, applications, utilities and/or drivers.

==========

The MIT License Agreement

The MIT License

Copyright (c) <year> <copyright holders>

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

PNG Graphics File Format Software End User License Agreement

Copyright (c) 1998-2001 Greg Roelofs. All rights reserved.

This software is provided "as is," without warranty of any kind, express or implied. In no event shall the author or contributors be held liable for any damages arising in any way from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. Redistributions of source code must retain the above copyright notice, disclaimer, and this list of conditions.
2. Redistributions in binary form must reproduce the above copyright notice, disclaimer, and this list of conditions in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

   This product includes software developed by Greg Roelofs and contributors for the book, "PNG: The Definitive Guide," published by O'Reilly and Associates.

---

zlib End User License Agreement

zlib License

zlib.h -- interface of the 'zlib' general purpose compression library
version 1.2.2, October 3rd, 2004

Copyright (C) 1995-2004 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly jloup@gzip.org
Mark Adler madler@alumni.caltech.edu

Warnings and Additions to This Document

1. Unauthorized reproduction of the contents of this document, in part or in its entirety, is prohibited.
2. This document is subject to change at any time without notice.
3. Do not make copies or alter the document content without permission from NEC Corporation.
4. If you have any concerns, or discover errors or omissions in this document, contact your sales representative.
5. Regardless of article 4, NEC Corporation assumes no responsibility for effects resulting from your operations.
6. The sample values used in this document are not actual values.

Keep this document for future use

Latest editions

This document was created based on the information available at the time of its creation. The screen images, messages and procedures are subject to change without notice. Substitute as appropriate when content has been modified.

The most recent version of this guide, as well as other related documents, is also available for download from the following website.

http://www.nec.com/express/

NEC Express5800 Series
Express5800/R120h-1M, R120h-2M

1 Maintenance

This chapter explains maintenance of server, and what actions are to be taken in case of trouble when operating this server.

1. **Relocation and Storage**
   Describes how to relocate and store this server.

2. **Daily Maintenance**
   Describes what you confirm for daily use, how to manage files, and how to clean the server.

3. **User Support**
   Describes various services on this product.

4. **Collecting Failure Information**
   Describes how to collect information about the location where a failure occurred and its cause if the server malfunctions. See this section in case of a failure.

5. **Troubleshooting**
   Describes how to identify the causes of problems and what actions are to be taken to address them. See this section if you suspect a failure.

6. **Windows System Recovery**
   Describes Windows recovery setup. See this section if Windows is corrupt.

7. **Resetting and Clearing the Server**
   Describes how to reset or clear the server. See this section if the server is not working or if you want to restore BIOS settings to the factory settings.

I. Relocation and Storage

Follow the steps below if you want to relocate or store this server.

⚠ WARNING

Be sure to observe the following precautions to use the server safety. Failure to observe the precautions may cause death or serious injury. For details, see *Safety Precautions and Regulatory Notices*.

- **Do not disassemble, repair, or alter the server.**
- **Do not remove the lithium battery, NiMH, or Li-ion battery.**
- **Disconnect the power plug before installing or removing the server.**

⚠ CAUTION

Be sure to observe the following precautions to use the server safely. Failure to observe the precautions may cause burns, injury, and property damage. For details, see *Safety Precautions and Regulatory Notices*.

- **Make sure to complete installation.**
- **Do not get your fingers caught.**
- **Be careful of handling internal components that may be at high temperatures.**

Note

- If the server has hard disk drives, move the server while being careful not to damage the drive.
- When storing the server, monitor the environmental conditions of the storage area.
  Temperature: −10°C to 55°C, Humidity: 20% to 80%
  (No dew condensation is permitted)

Tips

Make backup copies of important data stored in the hard disk drive.

1. Remove the disc from the optical disk drive.
2. Power off the server (POWER LED goes off).
3. Unplug the power cord of the server from the power outlet.
4. Disconnect all the cables from the server.
5. Pack the server securely to protect from damage, shock, and vibration.

Important

If this server and internal optional devices are suddenly moved from a cold place to a warm place, condensation will occur. Wait for a sufficient period of time before using the server and other components.

Note

Check and adjust the system clock before operating after relocating or storing the server.

2. Daily Maintenance

To use this server under good conditions at all times, periodically check and maintain as follows. If failures are found, ask your sales representative, avoiding impossible operation.

2.1 Checking and Applying Updates

Express5800 Series posts update information for BIOS, firmware (FW), driver, and others of the server and peripheral devices on our website. We recommend you to apply the latest update always.

NEC corporate site: **http://www.nec.com/**

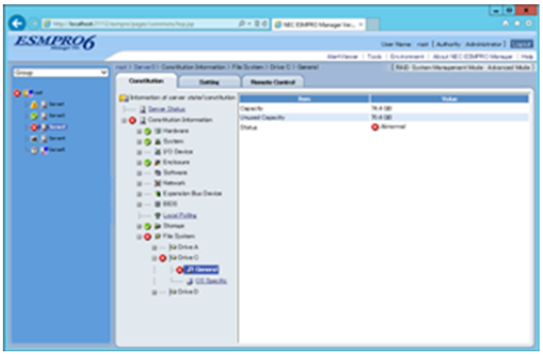
[Support & Downloads]

Tips NEC recommends that you back up data before applying the latest update.

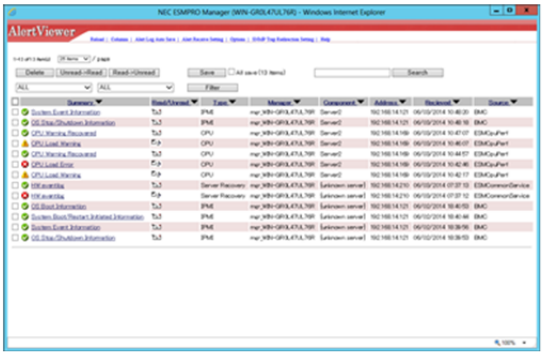
2.2 Checking Alerts

Use NEC ESMPRO Manager (for Windows) to constantly verify that no abnormalities are discovered on the monitored server and that no alerts have been issued.
You can download and install NEC ESMPRO Manager (for Windows) from our Website.

Example image of NEC ESMPRO Manager



NEC ESMPRO Manager



AlertViewer

2.3 Checking STATUS LED

After powering on the server or before shutting down the system and powering off the server, check STATUS LED on the front of the server. For the functions and descriptions of the LED, see *Chapter 1 (5. Names and Functions of Parts)* in *User's Guide.* If the indicator shows the server abnormality, contact your sales representative.

2.4 Backup

We recommend that you periodically back up the data on HDD.

If a RAID array has been configured on your system, back up the RAID configuration data. We also recommend that you back up it after a rebuilding process required due to HDD failure.

2.5 Cleaning

Regularly clean the server to keep it in good condition.

WARNING

Be sure to observe the following precautions to use the server safety. Failure to observe the precautions may cause death or serious injury. For details, see *Safety Precautions and Regulatory Notices*.

- **Do not disassemble, repair, or alter the server.**
- **Disconnect the power plug before cleaning the server.**

2.5.1 Cleaning the server

Wipe the external surfaces of the server with a dry soft cloth. Follow the steps below if stains remain on the surfaces.

Important

- **Do not use thinner and benzene, and other volatile solvents to clean the server.**
- **The power outlet, cables, connectors on the rear panel of the server, and the inside of the server must be kept dry.**

1. Confirm that the power is OFF (POWER LED is OFF).
2. Unplug the power cord of the server from a power outlet.
3. Wipe off dust from the power cord plug with a dry cloth.
4. Soak a soft cloth in neutral detergent that is diluted with cold or lukewarm water, and squeeze it firmly.
5. Rub off stains on the server with the cloth prepared in step 4.
6. Soak a soft cloth in water, squeeze it firmly, and wipe the server with it once again.
7. Wipe the server with a dry cloth.

2.5.2 Cleaning the tape drive

A dirty tape drive head causes unsuccessful file backup and damages the tape cartridge. Periodically clean the tape drive with the designated cleaning tape.

For the cleaning interval and method, the estimated usable period and lifetime of the tape cartridge, refer to the instructions attached to the tape drive.

2.5.3 Cleaning the keyboard and mouse

Wipe the surface of the keyboard with a dry cloth after confirming that the whole system, including the server and the peripherals, are shut down and POWER LED is off.

An optical mouse does not work properly if the lens area is not clean. Wipe the sensor with a dry cloth to remove any dirt or dust.

3. User Support

Before getting after-sales service, check the contents of the warranty and service.

3.1 Maintenance Services

Service representatives from NEC subsidiary companies or companies authorized by NEC provide maintenance services. For the services, contact your sales representative.

3.2 Before Asking for Repair

If you think that a failure occurred, follow the steps below:

1. Check if the power cord and cables to other products are properly connected.
2. See *Chapter 1 (5. Troubleshooting)*. If you find a symptom similar to your problem, take the action as instructed.
3. Confirm that the required software has been properly installed.
4. Scan for viruses using a commercial Antivirus Software.

If the problem persists after taking the measures above, contact your sales representative. Take notes on LED indications and the display on the screen at the failure, which will be useful information for the repair.

For repair within the warranty period, be sure to apply with your warranty.

4. Collecting Failure Information

If the server does not work normally, you can collect failure information by using the following way.
The failure information to be described is to be collected only at the request of your sales representative.

Important **When the system restarts after a failure has occurred, a message may appear indicating virtual memory shortage. Ignore this message and proceed with starting the system. Restarting the system may result in an inability to properly dump the data.**

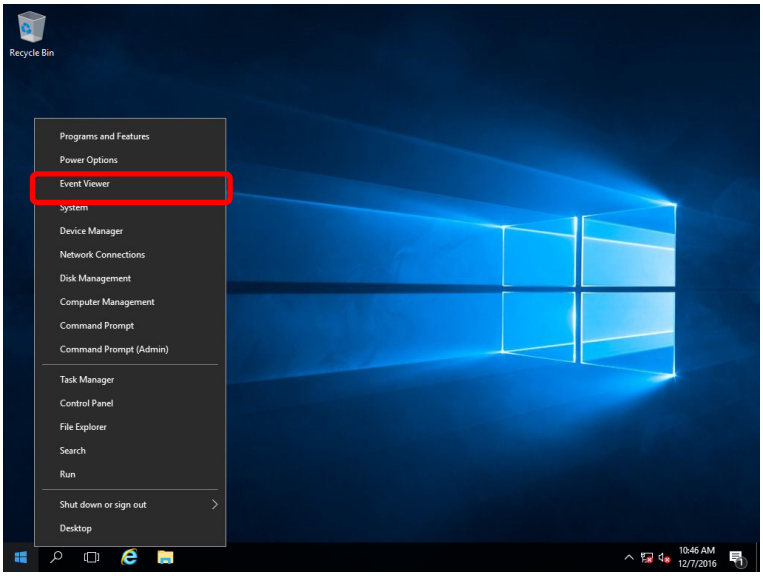
4.1 Collecting Event Logs

To collect various event logs follow the steps below.

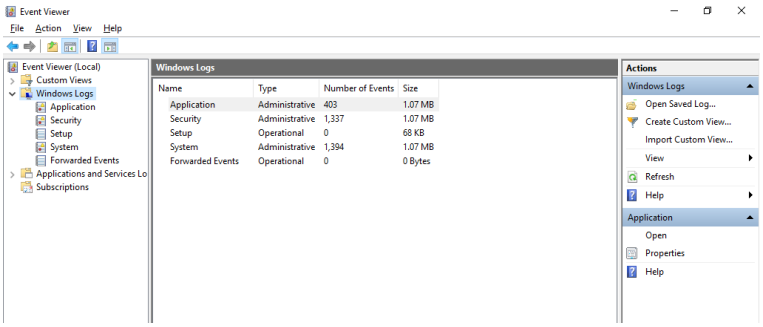
Tips If a STOP error, system error, or system stall occurs, restart Windows and follow the steps below.

4.1.1 Windows Server 2016

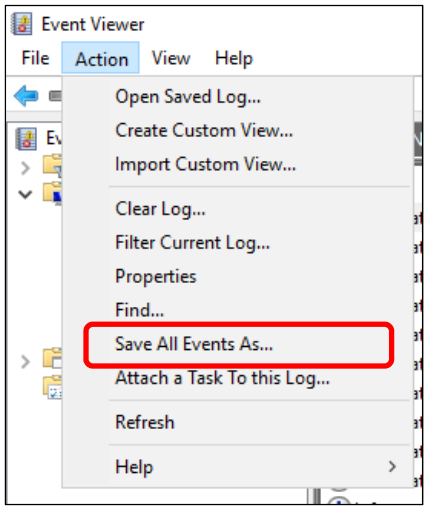
1. Right-click the left bottom of screen, and click **Event Viewer** from the menu displayed.



2. Select the type of log in **Windows Logs**.
   Application records events related to running applications.
   Security records events related to security.
   System records events that occur in Windows system components.



3. Click **Save All Events As** from **Action** menu.



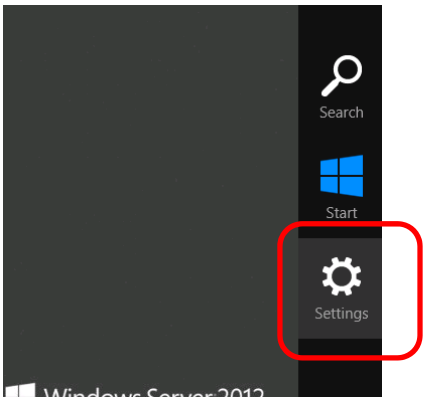
4. Type the file name of the archived log in **File name**.
5. Select the type of the log file you want to save in **Save as type**, and then click **Save**.

4.1.2 Windows Server 2012 R2

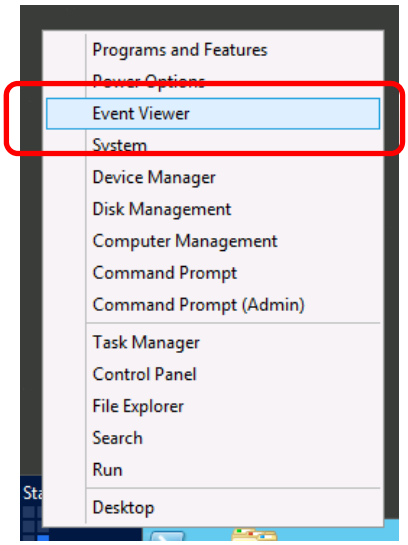
1. Click **Settings** on Charms Bar.

   To go to the step 4, you can directly choose **Event Viewer** by right-clicking on the lower left corner of the screen.

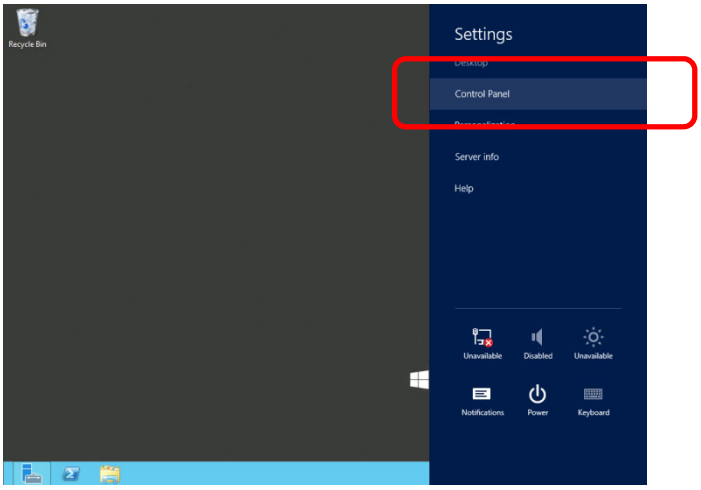
Charms Bar



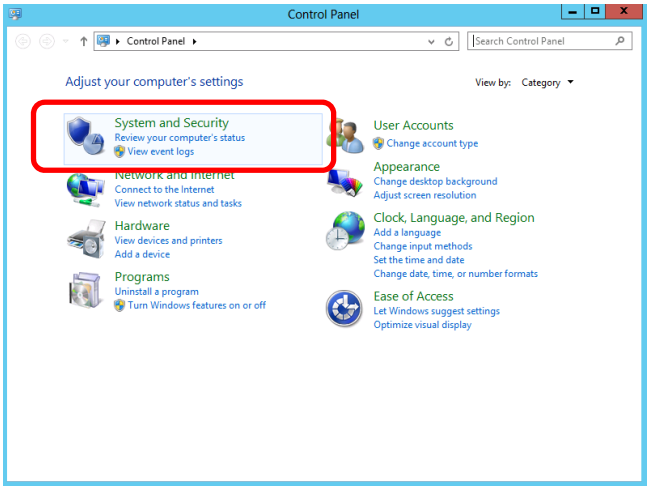
Right-click menu



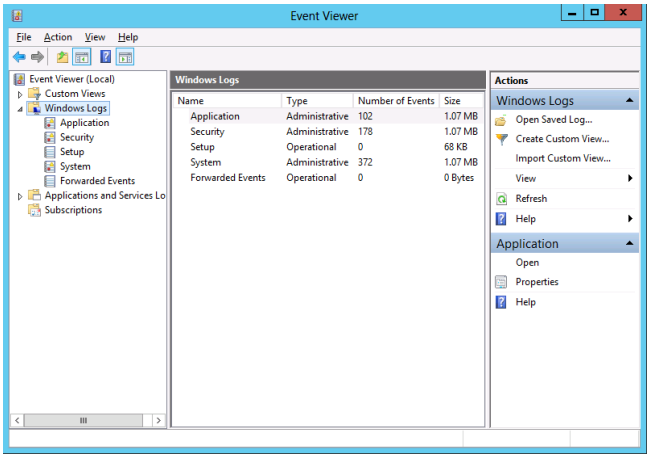
2. Click **Control Panel** from **Settings**.



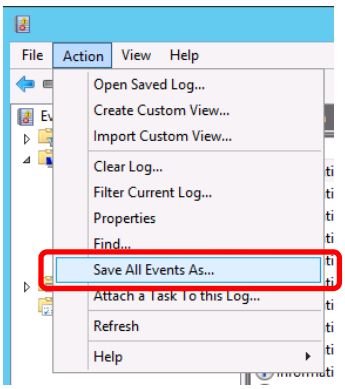
3. Click **View event logs** of **System and Security** on **Control Panel**.



4. Select the type of log in **Windows Logs**.
   Application records events related to running applications.
   Security records events related to security.
   System records events that occur in Windows system components.



5. Click **Save All Events As** from **Action** menu.



6. Type the file name of the log file in **File name**.
7. Select the type of the log file you want to save in **Save as type**, and then click **Save**.

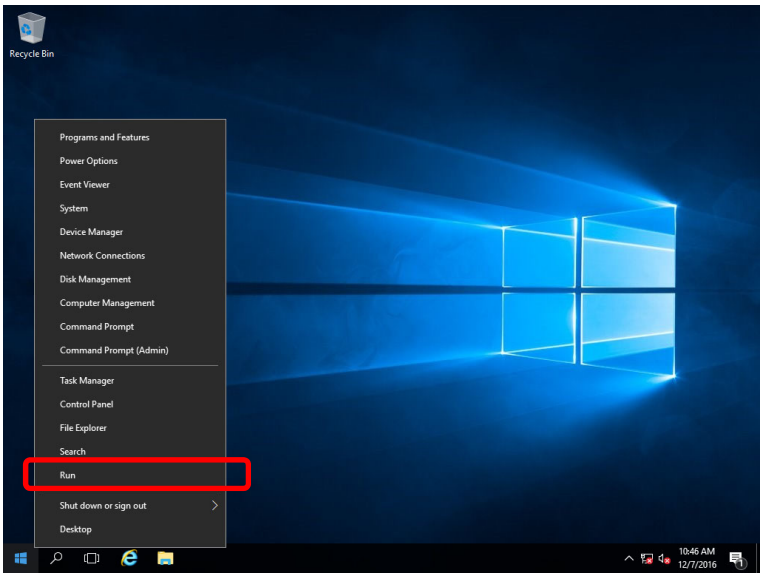
4.2 Collecting Configuration Information

This section describes how to collect hardware information or configuration.

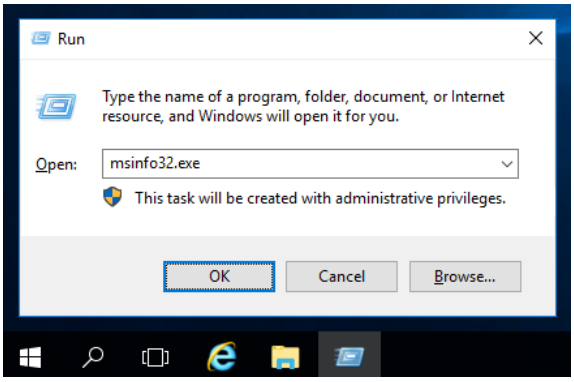
Tips If a STOP error, system error, or system stall occurs, restart Windows and then follow the procedure below.

4.2.1 Windows Server 2016

1. Right-click the left bottom of screen, and click **Run** from the menu displayed.



2. **Type `msinfo32.exe`,** and then press <Enter> key.



System Information starts.

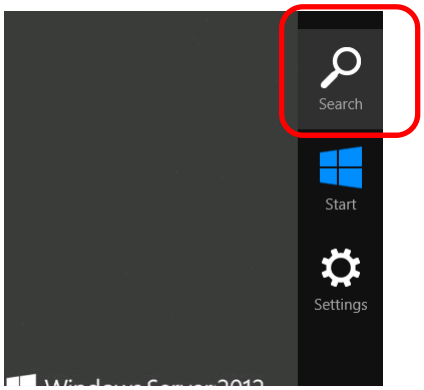
3. Click **Export** from **File** menu.
4. Type a file name to save in **File Name**, and then Click **Save**.

4.2.2 Windows Server 2012 R2

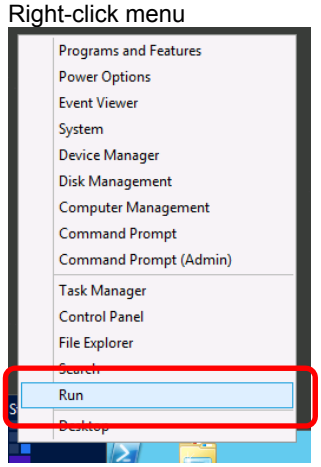
1. Click **Search** on Charms Bar.

   You can also use **Run** feature by right-clicking on the lower left corner of the screen.

Charms Bar

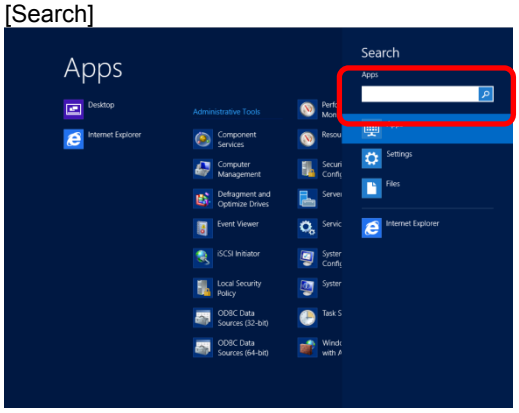


Right-click menu

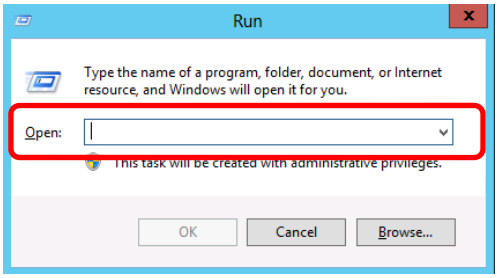


2. Type `msinfo32.exe` in the text box, and then press <Enter> key.

[Search]



[Run]



3. **System Information** starts.
4. Click **Export** from **File** menu.
5. Type a file name to save in **File Name**, and then Click **Save**.

4.3 Collecting User-Mode Process Dump

The user-mode process dump is the failure information related to application errors.

For details, see *Chapter 1 (5.2 How to Create a User-Mode Process Dump File)* in "*Installation Guide (Windows)*".

4.4 Collecting Memory Dump

If an error occurs, the dump file will be saved to acquire necessary information. You can specify any location for saving the diagnostic information. For details, see *Chapter 1 (5.1 Specifying Memory Dump Settings (Debug Information))* in "*Installation Guide (Windows)*".

Consult with your sales representative before dumping the memory. Dumping the memory while the server is in operating normally will affect the system operation.

Important **A message indicating insufficient virtual memory may appear when restarting the system due to an error. Ignore this message and proceed. Restarting the system may result in an inability to properly dump the data.**

5. Troubleshooting

If this system does not operate as intended, check it according to the contents of the following checklist before sending it for repair. If an item in the checklist corresponds with a problem you are experiencing, follow the subsequent check and processing instructions.

If the system still does not operate normally, write down the messages displayed on the screen and then contact your sales representative.

5.1 Problem of Powering On

[?] **Fail to power on the server**

- ☐ Is the server properly supplied with power?
  - → Check if the power cord connects to the power outlet (or UPS) that meets the power specifications for the server.
  - → Use the power cord that comes with the server. Additionally, check the power cord for broken shield or bent plugs.
  - → Make sure the power breaker for the connected power outlet is on.
  - → If the power cord is plugged to a UPS, make sure the UPS is powered and it outputs power. Refer to the manual that comes with the UPS for details.
    Power supply to the server may be linked with UPS using the Setup Utility.
- ☐ Have you pressed the POWER switch?
- ☐ Is the STATUS LED indicator lit in green?
  - → If the STATUS LED indicator is lit in red or amber, check the system status using the iLO, and also check the connection of cables and optional items. If the problem persists, contact your maintenance service company.
- ☐ Is the window shown on the display?
  - → Check the cable connection to the display and the power supply of the display.

[?] **POST does not complete**

- ☐ Is memory installed correctly?
  - → Check if memory is installed correctly.
- ☐ Is the memory size large?
  - → Wait for a while. The memory check takes longer than usual when the installed memory size is large.
- ☐ Did you perform any keyboard or mouse operation immediately after you started the server?
  - → Restart the server and do not perform any keyboard or mouse operation until the POST start-up message appears.
- ☐ Are memory and PCI devices supported for use with this server?
  - → Operation of the server with unauthorized devices is not supported.

[?] Fail to power on the server

- ☐ Did you press POWER Switch?
  - → Press the power switch and verify that the power lamp has turned green.
- ☐ Does the POWER LED light amber?
  - → Press the power switch and wait for 45 seconds.
- ☐ Does the STATUS LED light red or amber?
  - → Use iLO to verify the contents of the Integrated Management Log (IML), and reattach the component indicated in the log. If nothing changes, replace the component.
- ☐ Is the power supply plugged in correctly?
  - → Reinstall the power supply.
  - → Verify that there are no faults in the power cable wiring.
  - → Plug another device into the grounded outlet to verify that the outlet is working.
  - → Verify that the power cord is not damaged by replacing it with one that is known to be working correctly.
- ☐ Is the power working correctly?
  - → If the power is not working correctly, replace the power unit.
  - → Verify that the corresponding circuit breaker is switched on.
  - → Ask a certified technician to check the voltage and verify that the required specifications are satisfied.
  - → If a kinetic enclosure power consumption cap or enclosure power restriction is enabled on a supported server, verify that enough power is being supplied to support the server.
- ☐ Does the server power unit meet the power requirements for the server's configuration?
  - → If the server power unit does not meet the power requirements for the server's configuration, replace it.
- ☐ Is the device connected to a UPS?
  - → When connected to a UPS, verify that the UPS power is on, and that power is being outputted from the UPS. Refer to the UPS's manual for details. Linked power supply settings for the UPS can be configured using the Setup Utility.
- ☐ Are you experiencing a problem not mentioned above?
  - → Use iLO and check the Server Health Summary on the external monitor.

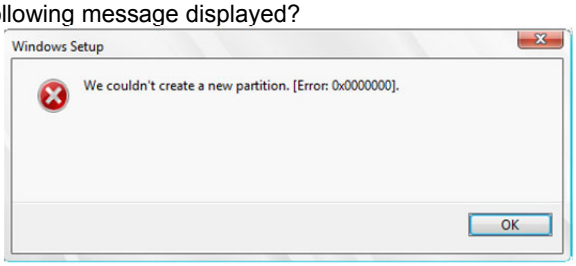
[?] The server does not complete POST, or the server completes POST with errors.

- ☐ Is the memory installed correctly?
  - → Verify that the memory is installed correctly.
- ☐ Are the installed memory and PCI device supported by the device?
  - → The functionality of devices other than those specified by our firm cannot be guaranteed.
- ☐ Does the STATUS LED light red or amber?
  - → Use iLO to verify the contents of the Integrated Management Log (IML), and reattach the component indicated in the log. If nothing changes, replace the component.
- ☐ Is there a problem with the display?
  - → Correct the display's wiring.

5.2 Problem of Installing OS

[?] **Unable to create a partition when installing Windows Server 2012 R2**

☐ Is the following message displayed?



→ The message above means that you failed to create a partition. In this case, delete the partition you attempted to create, and then create a new partition.
If you have connected a data disk to a partition, be careful not to delete that partition.

For details, refer to the Microsoft website below:

Windows Server 2012 R2

https://technet.microsoft.com/en-us/library/dn387077.aspx

[?] **Unable to install OS**

☐ Is the hard disk drive properly installed?

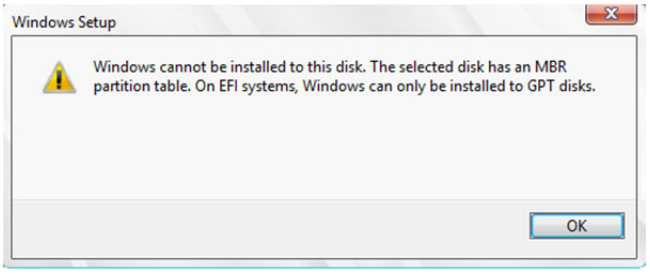
→ Make sure that the hard disk drive is installed securely and that cables are properly connected.

☐ Is the disk format correct?

→ Follow the table below to create a partition depending on the boot mode.

Boot mode	Disk format
UEFI Mode	GPT (GUID partition table)
Legacy Mode	MBR (master boot record)

For example, the following message appears if an MBR disk is specified as the system drive of Windows on UEFI boot mode.



To change the disk format, clear the partition configuration and create a new partition. All of the data on the hard disk drive will delete. Back up necessary data before clearing the partition configuration.

☐ Did you configure the RAID controller?

→ For a RAID system, use EXPRESSBUILDER or RAID Configuration Utility (Off-line Utility or LSI Software RAID Configuration Utility) to properly configure the RAID controller before installing OS.

☐ Did you create a logical drive?

→ For a RAID system, create a logical drive using EXPRESSBUILDER or RAID Configuration Utility (Off-line Utility or LSI Software RAID Configuration Utility) to install OS.

[?] Unable to install Windows

☐ Did you check the precautions for installation?

→ For installing OS, see "*Installation Guide (Windows)*".

[?] A product key is not requested

☐ Did you use the backup DVD-ROM?

→ You do not need to type the product key when installing Windows with the backup DVD-ROM.

[?] The Telnet Service is not installed

→ Adjust the computer name to 14 characters or less (*), and then install the Telnet Service according to the following procedure:

(1) Click **Run** on Start menu.

(2) Enter `tlntsvr/service` in **Open**, and then click **OK**.

(3) Click Start menu, point to **Control Panel,** click **Administrative Tools**, and then click **Services** to confirm whether the Telnet Service is registered.

* You can specify the computer name at 15 characters or more after installing the telnet service.

[?] An error message appears after the graphics accelerator is installed

☐ Is the Server Core installation of Windows Server 2012 R2?

→ An application error is recorded in event log after restarting. Ignore this event log because it does not affect system operation.

5.3 Problem of Starting OS

[?] **Unable to start OS**

- ☐ Have the settings of the RAID controller changed?
  - → Specify the correct settings with RAID Configuration Utility (Off-line Utility or LSI Software RAID Configuration Utility).
- ☐ Is the RAID controller found by POST?
  - → Be sure to connect the RAID controller correctly and retry.
- ☐ Is the RAID controller installed firmly straight into the PCI slot?
  - → Install the RAID controller properly.
- ☐ Is the RAID controller mounted on the PCI slot for which the mounting is restricted?
  - → Check the mounting restrictions of the server and then mount the RAID controller on the correct slot.
- ☐ Are the hard disk drives properly installed?
  - → Install the hard disk drives properly.
- ☐ Is the cable connected to the hard disk drive or disk array unit correctly?
  - → Connect the SAS cable properly.
- ☐ Is OS Boot Manager registered in “UEFI Boot Order”?
  - → In UEFI boot, in case OS Boot Manager (Windows Boot Manager, Red Hat Enterprise Linux, etc.) is not registered in “UEFI Boot Order”, use “One-Time Boot” menu for now to boot OS from your boot device. By the OS you started, OS Boot Manager is registered at the top of “UEFI Boot Order”. After that, you will be able to start from OS Boot Manager you registered. In case you cannot boot OS from the boot device even after you have executed the above step, add manually the file and pass of OS Boot Manager to “UEFI Boot Order” from “Add Boot Options” menu.
- ☐ Is Boot Order in the order you expected?
  - → Set up the suitable Boot Order from “UEFI Boot Order” menu or “Legacy BIOS Boot Order” menu.
- ☐ Does the boot mode setting of System Utility march the “Boot Mode” of the installed OS?
  - → Select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Boot Options** from System Utility, and then set “Boot Mode” appropriately.
- ☐ When enabling Secure Boot, does the optional card used for booting support Secure Boot?
  - → When "Secure Boot" is enabled, the optional card UEFI driver must be signed with Microsoft key in order to make the optional card recognized as a bootable device. Set to the UEFI driver of.

[?] **Unable to start OS**

- ☐ Does the configured boot media match the OS installed on the boot media?
  - → Configure bood mode property.
- ☐ In an OS installed on the intended boot device?
  - → Install an OS on the intended boot device.
- ☐ Is VMware ESX starting up in UEFI boot mode?
  - → When booting VMware ESX in UEFI Boot Mode, enable UEFI Optimized boot.
- ☐ Is secure boot enabled?

→ To make the option card recognizable as a bootable device when Secure Boot has been enabled, you need to have an option card UEFI driver that has been signed with the Microsoft key. Set all option cards to signed UEFI driver.

5.4 Problem of RAID System

[?] **Unable to rebuild the RAID array**

☐ Is the capacity of the hard disk drive to be rebuilt correct?

→ Use a hard disk drive with the same capacity as that of the faulty hard disk drive.

☐ Is the logical drive RAID0?

→ RAID0 cannot be rebuilt because it has no redundancy. Replace the failed hard disk drive, reconfigure the RAID array, and recover the drive using backup data.

[?] **Unable to automatically rebuild the RAID array**

☐ Did you wait for sufficient time until the hard disk drive was replaced?

→ Follow the steps below to use the auto-rebuilding feature.

(1) Remove a failure HDD.

(2) Wait for at least 90 seconds.

(3) Install a new HDD.

[?] **The hard disk drive failed**

→ Contact your sales representative.

[?] **Additional battery is not found**

☐ Are the cable between the battery pack and battery board and the control cable between the battery board and battery connector connected correctly?

→ Connect the cables correctly.

☐ Is this message displayed after the battery is connected?

→ If the battery charging status is low, the battery is not found. If the battery is not found although 24 hours has passed, restart the system once.

If the battery is not found although the above action has been taken, the additional battery may be faulty. Contact your sales representative.

[?] **DISK LED flashes**

☐ Does DISK LED flashes frequently even while the hard disk drive is not accessed?

→ Ignore the flashing. When Patrol Read is running, the DISK LED flashes even if the hard disk drive is not being accessed. If a SATA hard disk drive is used, the DISK LED stays on.

[?] **During the POST process, the controller is not visible or shows errors**

→ Make sure that the controller is supported for the server.

→ Make sure that the controller is installed and seated properly.

→ Make sure that the cables are properly connected.

→ If the controller is physically damaged, replace it.

→ If the controller is recognized by the system ROM, then reseat the controller.

→ Run controller diagnostics and follow the steps displayed.

→ Update the firmware.

→ Download the Active Health System log.

[?] **Controllers are no longer redundant (the controller shows errors during the POST process, or the cache is disabled)**

→ Make sure that the controllers are supported for the server.

→ Make sure the controllers are installed and seated properly.

→ Make sure that the cables are properly connected.

→ If the controller is physically damaged, replace it.

→ Run controller diagnostics and follow the steps displayed.

→ Make sure that the controllers are compatible controller models.

→ Verify that the controller cache sizes are compatible.

→ Verify that the FBU (flash backup unit) is installed and connected correctly.

→ Update the firmware.

→ Download the Active Health System log.

[?] **Smart Array S100i SR Gen10 SW RAID drives are not found when RAID mode is disabled**

→ When Smart Array S100i SR Gen10 SW RAID controller is enabled on a server and RAID mode is disabled in the System Utility, then the drives are listed as AHCI drives or H220i drives and the RAID controller is not found in POST or device manager. When RAID mode is enabled, the drives appear as Smart Array S100i SR Gen10 SW RAID controller drives.

Below is the procedure to correct the problem.

1. Press the <F9> key during the startup process to access System Utility.
2. In the System Configuration menu, select **BIOS/Platform Configuration (RBSU)** → **Storage Options** → **SATA Controller Options** → **Embedded SATA Configuration** → **Smart Array SW RAID Support**.
3. Press <F10> key to save the configuration.
4. Reboot the server.

[?] **Data located on drives accessed in RAID mode is not compatible with data accessed from non-RAID mode**

→ Recommends that you access drive data only when the same RAID or non-RAID mode is enabled. Back up and restore the data on the drives.

[?] **The Smart Array controller does not show logical drives after moving drives to a new server or JBOD**

→ Be sure to follow all drive roaming rules when migrating drives.

Note

Drive roaming lets you move disk drives and arrays while maintaining data availability. You can move one or more disk drives in a configured logical drive to a different bay position as long as the new bay position is accessible by the same controller. In addition, you can move a complete array from one controller to another, even if controllers are in different servers. The logical drive status must be good before you move physical drives to a new bay position.

Drive roaming is an offline feature. There is no method for removing an array while the server is online and then moving it to a new physical location.

5.5 Problem of Internal Devices and Other Hardware

[?] **Unable to access the internal or external devices**

- ☐ Are cables properly connected?
  - → Make sure that the interface cables and power cord are properly connected. Also make sure that the cables are connected in the correct order.
- ☐ Is the power-on order correct?
  - → When the server has any external devices connected, power on the external devices first, then the server.
- ☐ Did you install drivers for connected optional devices?
  - → Some optional devices require specific device drivers. Refer to the manual that comes with the device to install its driver.
- ☐ Is option board setting correct?
  - → Refer to the manual that comes with the board for details to specify I/O port address, and other settings.

[?] **The keyboard or mouse does not work**

- ☐ Is the cable properly connected?
  - → Make sure that the cable is connected to the connector on the front or rear of the server.
- ☐ Is BIOS configuration correct?
  - → In System Utility, you can change the configuration of USB. In System Utility, from **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **System Options** > **USB Options**, check the configuration of USB port to which the keyboard is connected.
- ☐ Are the server drivers installed?
  - → Refer to the manual that comes with your OS to check that the keyboard and mouse drivers are installed.

[?] **Unable to access the hard disk drive**

- ☐ Is the hard disk drive supported by the server?
  - → Operation of any device that is not authorized by NEC is not supported.
- ☐ Is the hard disk drive properly installed?
  - → Check the hard disk drive installation status and the cable connections.

[?] **The hard disk drive is failed**

→ Be sure no loose connections exist.

→ Update the components, if an update is available for any of the following components:

- Smart Array Controller firmware
- Dynamic Smart Array driver
- Host bus adapter firmware
- Expander backplane SEP firmware
- System ROM

→ Be sure the drive or backplane is cabled properly.

→ If the drive's data cable is faulty, replace it.

→ If a dummy tray is attached, verify that it is attached correctly.

→ Run SSA and check the status of the failed drive.

→ Be sure the replacement drives within an array are the same size or larger.

→ Be sure the replacement drives within an array are the same drive type, such as SAS, SATA, or SSD.

→ Power cycle the server. If the drive shows up, check to see if the drive firmware needs to be updated.

[?] **Drives are not recognized**

→ Be sure no power issues exist.

→ Be sure no loose connections exist.

→ Update the components, if an update is available for any of the following components:

- Smart Array Controller firmware
- Dynamic Smart Array driver
- Host bus adapter firmware
- Expander backplane SEP firmware
- System ROM

→ Be sure the drive or backplane is cabled properly.

→ Check the drive LEDs to be sure they indicate normal function.

→ Be sure the drive is supported.

→ Power cycle the server. If the drive appears, check to see if the drive firmware needs to be updated.

→ Be sure the drive bay is not defective by installing the hard drive in another bay.

→ Be sure the replacement drives within an array are the same size or larger.

→ Be sure the replacement drives within an array are the same drive type, such as SAS, SATA, or SSD.

→ When using a disk array controller, be sure the drive is configured in a disk array by running SSA.

→ Be sure that the correct controller drivers are installed.

→ Be sure that the controller supports the hard drives being installed.

→ If SAS expanders are used, be sure the Smart Array controller contains a cache module.

→ If a storage enclosure is used, be sure the storage enclosure is powered on.

→ If a SAS switch is used, be sure disks are zoned to the server using the Virtual SAS Manager.

→ Be sure that RAID mode is enabled in System Utility.

[?] **Data is inaccessible**

☐ Are the files corrupt?

→ Run the repair utility for the operating system.

☐ Do viruses exist on the server?

→ Run a current version of a virus scan utility.

☐ If a TPM is installed, is it correctly enabled on the server?

→ Be sure that the TPM is enabled in System Utility. If the TPM is not enabled, follow the TPM replacement recovery procedure in the operating system document.

☐ Does an encrypted file exist?

→ When migrating encrypted data to a new server, follow the recovery procedures in the operating system document.

[?] **Server response time is slower than usual**

→ Review information about the operating system encryption technology, which can cause a decrease in server performance.

☐ Is the drive full?

→ Be sure the drive is not full. If needed, increase the amount of free space on the drive. Recommends that drives have a minimum of 15 percent free space.

☐ Is a recovery operation pending on the logical drive?

→ Make sure that a recovery operation is not pending on the logical drive by using SSA.

[?] **SmartDrive icons or LEDs illuminate errors for the wrong drive or an error message is displayed in POST, SSA, or SSADUCLI**

→ Make sure that the cabling from the drive backplane to the mother board is correct.

[?] **POST message or IML message is registered**

→ Replace the device, because the device is approaching the maximum usage limit for writes to the device.

[?] **Additional internal or external devices do not operate correctly.**

→ Be sure the internal or external devices being installed are a supported option on the server.

→ Be sure the issue is not caused by a change to the hardware release. For details, see the NEC web site.

→ Be sure the new internal or external devices are installed properly.

→ Be sure no memory, I/O, or interrupt conflicts exist.

→ Be sure all cables are connected to the correct locations and are the correct lengths.

→ Be sure other components were not accidentally unseated during the installation of the new internal or external devices.

→ Be sure all necessary software updates, such as device drivers, ROM updates, and patches, are installed and current, and the correct version for the hardware is installed.

→ After installing or replacing boards or other options, verify that the system recognizes all changes to the hardware in the options setup in System Utiliti. If the new hardware is not properly configured, a POST Error message indicating the configuration error may be registered.

→ Be sure all switch settings are set correctly.

→ Be sure all boards are properly installed in the server.

[?] **An unknown problem occurs with an internal or external device.**

→ Check the server LEDs to see if any statuses indicate the source of the issue.

→ Be sure no loose connections exist.

→ Turn the server's power off, and follow the procedure below.

1. Power down and disconnect power to the server. Remove all power sources to the server.
2. Reduce the server to the minimum hardware configuration by removing all cards or devices that are not necessary to power on the server. Keep the monitor connected to view the server power-on process.
3. Reconnect power, and then power on the system. If the system fails in this minimum configuration, one of the primary components has failed. If you have already verified that the processor, power supply, and memory are working before getting to this point, replace the motherboard. If not, be sure each of those components is working.
4. If the system boots and video is working, add each component back to the server one at a time, restarting the server after each component is added to determine if that component is the cause of the issue. When adding each component back to the server, be sure to disconnect power to the server and follow the description in the server document.

[?] **A problem is occurs when using an internal or external device made by another company.**

→ Be sure that the server and OS support the device.

→ Verify that the latest version of the driver, or the version of the driver appropriate for the device is installed.

→ Be sure the device is properly installed.

[?] **The cooling fan does not operate correctly.**

→ Verify that the fan is attached correctly. If the fan is not attached correctly, remove the top cover and fix the fan in place according to the user's guide for the server.

→ Make sure that the cooling fan configuration meets the functional requirements of the server.

→ Replace any required non-functioning cooling fans and restart the server.

→ Be sure all fan slots have the cooling fans or blanks installed.

→ Check the cooling fan airflow path is not blocked by cables or other material.

→ Verify that the top cover is attached correctly. If the server is operated for an extended period of time with the top cover removed, airflow might be impeded, causing thermal damage to components.

→ Be sure no POST error messages are displayed while booting the server that indicate temperature violation or fan failure information. For the temperature requirements for the server, see the User's Guide of the server.

→ Use iLO or an optional IML viewer to access the IML to see if any event list error messages relating to the cooling fans are listed

→ In the iLO web interface, navigate to the **Information** > **System Information** page and check the following information:

1. Click the **Fans** tab and verify the fan status and fan speed.
2. Click the **Temperatures** tab and verify the temperature readings for each location on the Temperatures tab. If a hot spot is located, then check the airflow path for blockage by cables and other material. A hot spot is not an absolute temperature but is relative to a component specification. Hot spot is defined as temperature on a sensor within 3°C of a Caution threshold listed on the Temperature tab.

→ For BladeSystem c-Class enclosure fan issues, review the fan section of OA SHOW ALL and the FAN FRU low-level firmware.

[?] **The cooling fan operates at a higher speed than normal.**

→ In the iLO web interface, navigate to the **Information** > **System Information** page and check the following information:

- Click the **Fans** tab. Fan speeds can be high if a sensor temperature is within approximately 10°C of the Caution threshold.
- Click the **Temperatures** tab, and check the fan status and fan speed. Fan speeds greater than 60% are expected to be loud.

→ Update the server to the latest firmware versions, such as iLO firmware, system ROM, option firmware, etc.

→ Verify that all air ducts and required blanks, such as drive blanks, processor heatsink blanks, dummy trays, etc., are installed.

→ Make sure that the correct processor heatsink is installed.

→ Make sure that the correct fan is installed, if the system supports both standard fans and performance fans.

[?] **The cooling fan makes excessive noise while operating at low speed.**

→ Replace the cooling fan.

[?] **A cooling fan with hot-plug support does not operate correctly.**

→ Check the server LEDs to see if any statuses indicate the source of the issue.

→ Be sure no POST error messages are displayed.

→ Be sure hot-plug fan requirements are being met. For details, see User's Guide of the server.

[?] **The TPM is no longer detected from System Utility.**

→ Contact your maintenance service company, and replace it with the new motherboard and TPM kit.

[?] **The memory does not function correctly.**

→ Check any server LEDs that correspond to memory slots.
→ Be sure the memory meets the server requirements. For details, see User's Guide of the server.
→ Be sure the memory installs properly.
→ Update the system ROM to the latest version.
→ Verify that the DIMM is installed correctly according to the procedure.
→ Reseat the DIMM.
→ Replace the DIMM.
→ If the third-party memory is installed on the server, remove it.

[?] **Server is out of memory**

→ Be sure the memory meets the server requirements. For details, see User's Guide of the server.
→ Be sure no operating system errors are indicated.
→ Update the system ROM to the latest version.

[?] **POST error message or IML message of DIMM is displayed.**

→ Make sure that the Advanced Memory Protection settings and DIMMs are installed properly.
→ Make sure that the DIMMs are supported on the server.
→ Be sure that the associated processor is installed for all DIMMs on the server.
→ Update the system ROM to the latest version.

[?] **Server fails to recognize existing memory.**

→ Be sure the server supports processor installed in the server.
→ For all DIMMs installed in the server, be sure the associated processor is installed.
→ Be sure the memory is configured properly.
→ Reseat the DIMM.
→ Update the system ROM to the latest version.
→ Replace the DIMM.

[?] **The server does not recognize new memory installed on the server**

→ Be sure the memory is the correct type for the server.
→ Be sure the memory is installed according to the server requirements. For details, see User's Guide of the server.
→ Be sure you have not exceeded the memory limits of the server or operating system. For details, see User's Guide of the server.
→ Be sure the server supports the number of processor cores. For details, see User's Guide of the server.
→ Be sure no Event List error messages are displayed in the IML.
→ Be sure the memory is installed properly.
→ Be sure no conflicts are occurring with existing memory. Run the server setup utility.
→ If the memory is faulty, replace it.

→ Update the system ROM to the latest version.

[?] **A STOP error, a blue screen (Windows), or a purple diagnostic screen (VMware) is displayed.**

→ Reseat the DIMM.
→ Update the system ROM to the latest version.
→ Replace the DIMM.

[?] **A Linux kernel panic occurs.**

→ Reseat the DIMM.
→ Update the system ROM to the latest version.
→ Replace the DIMM.

[?] **Server restarts or powers down unexpectedly**

→ Reseat the DIMM.
→ Update the system ROM to the latest version.
→ Replace the DIMM.

[?] **Parity errors occur**

→ Reseat the DIMM.
→ Update the system ROM to the latest version.
→ Replace the DIMM.

[?] **Performance of memory is degraded**

→ Reseat the DIMM.
→ Update the system ROM to the latest version.
→ Replace the DIMM.

[?] **The memory LED is amber**

→ Reseat the DIMM.
→ Update the system ROM to the latest version.
→ Replace the DIMM.

[?] **ECC errors occur with no other symptoms**

→ Reseat the DIMM.
→ Update the system ROM to the latest version.
→ Replace the DIMM.

[?] **POST error message or IML message is displayed indicating an NVDIMM restore error**

→ Remove and replace the failed NVDIMM.

[?] **POST error message or IML message is displayed indicating an NVDIMM backup error**

→ Sanitize the NVDIMM

→ If the error persists, replace the NVDIMM.

[?] **POST error message or IML message is displayed indicating an NVDIMM uncorrectable memory error**

→ Sanitize the NVDIMM

→ If the error persists, replace the NVDIMM.

[?] **If NVDIMM-N Memory Interleaving is enabled, all NVDIMMs on a processor are disabled**

→ Sanitize the NVDIMM

→ If the error persists, replace the NVDIMM.

[?] **If NVDIMM-N Memory Interleaving is disabled, only the NVDIMM indicated is disabled**

→ Sanitize the NVDIMM

→ If the error persists, replace the NVDIMM.

[?] **POST error message or IML message is displayed indicating an NVDIMM backup power error**

→ Check that the Flash Backup Unit (FBU) is installed and functioning properly.

→ Reseat the NVDIMM and DIMM.

→ If the error persists, replace the NVDIMM.

[?] **A POST Error message or an IML message indicating the error of the NVDIMM controller will be registered**

→ Update the NVDIMM firmware.

→ If the error persists, replace the NVDIMM.

[?] **A POST Error message or an IML message indicating the erasure error of the NVDIMM will be registered**

→ Copy the data to the new NVDIMM by following the procedure below.

1. Save the contents of the NVDIMM to other media to preserve the data.
2. Replace the NVDIMM.
3. Sanitize the new NVDIMM.
4. Copy the preserved data to the new NVDIMM.

[?] **A POST Error message or an IML message indicating the equipment error of NVDIMM will be registered**

→ Copy the data to the new NVDIMM by following the procedure below.

1. Save the contents of the NVDIMM to other media to preserve the data.

2. Replace the NVDIMM.
3. Sanitize the new NVDIMM.
4. Copy the preserved data to the new NVDIMM.

[?] **A POST Error message indicating the sanitization error of the NVDIMM will be registered**

→ Retry sanitizing the NVDIMM

→ If the error persists, replace the NVDIMM.

[?] **If one or more new NVDIMMs are installed in the server where the NVDIMM has been already installed, an Error message indicating that all the NVDIMMs are disabled will be registered**

→ Do one of the following:

- Remove the newly installed NVDIMMs to continue using the existing NVDIMMs in the server.
- Sanitize the NVDIMMs indicated to begin using all NVDIMMs in the server.

[?] **If NVDIMM interleaving is disabled, only the NVDIMMs with corrupted metadata are disabled**

→ Sanitize all NVDIMMs disabled due to corrupt metadata.

[?] **If NVDIMM Interleaving is enabled, all NVDIMMs on a processor are disabled**

→ Sanitize all NVDIMMs disabled due to corrupt metadata.

[?] **All NVDIMMs on processor X are disabled**

→ One or more NVDIMMs were removed from this server and the server has NVDIMM-N Memory Interleaving enabled. Do one of the following:

- Reinstall the missing NVDIMMs.
- Sanitize all NVDIMMs on processor X to begin using the smaller interleaved set.

[?] **A POST Error message or an IML message indicating the memory initialization error or the uncorrectable error will be registered. If NVDIMM Interleaving is enabled, all NVDIMMs on processor X are disabled. If NVDIMM Interleaving is disabled, then only the affected NVDIMMs are disabled.**

→ Perform the procedure below.

1. Reseat the NVDIMMs and all DIMMs in the server.
2. Sanitize all NVDIMMs disabled due to this error.
3. If the error persists, replace the NVDIMM.

[?] **A POST Error message or an IML message will be registered. If NVDIMM Interleaving is enabled, all NVDIMMs on processor X are disabled. If NVDIMM Interleaving is disabled, then only the affected NVDIMMs are disabled.**

☐ Does the server not match the original server in which the NVDIMM was used, and is NVDIMM-N Memory Interleaving enabled?

→ Perform the procedure below.

1. Remove the processor and replace it with the previously installed processor type.
2. Reboot the server.
3. Save the contents of the NVDIMM to other media to preserve the data.
4. Remove the processor and replace it with the new processor.
5. Sanitize all NVDIMMs in the system.
6. Restore data to the NVDIMM.
7. Remove the processor and replace it with the previously installed processor type.

☐ Was the NVDIMM moved?

→ Perform one of the procedures below.

- To preserve data, install the NVDIMM in the location indicated by the message.
- Sanitize all NVDIMMs indicated by the message. The data on the NVDIMM is not available after sanitization.

[?] **QPI Snoop Configuration error message for NVDIMMs is received and all NVDIMMs on a processor are disabled**

→ Perform one of the procedures below.

- Change the QPI Snoop Configuration setting to match the previous system.
- Sanitize all NVDIMMs indicated by the error. The data on the NVDIMM is not available after sanitization.

[?] **POST error message or IML message is displayed, and NVDIMMs are disabled in the system (the NVDIMM-N Memory Interleaving is enabled, then all NVDIMMs on processor X are disabled)**

☐ The NVDIMM was previously being used in a server with NVDIMM-N Memory Interleaving enabled, but is this server configured for NVDIMM-N Memory Interleaving disabled?

→ Perform one of the procedures below.

- Change the NVDIMM-N Memory Interleaving setting for the NVDIMM to the same setting for the server and then, reboot the server. Below is the procedure to change the settings.
  -- If the NVDIMM was previously installed in a server that had NVDIMM-N Memory Interleaving enabled, enable NVDIMM-N Memory Interleaving in System Utility.
- Sanitize all NVDIMMs indicated. All data on the NVDIMM will not be available after sanitization.

[?] **POST error message or IML message is displayed, and NVDIMMs are disabled in the system (the NVDIMM-N Memory Interleaving is disabled, then only affected NVDIMMs are disabled)**

☐ The NVDIMM was previously being used in a server with NVDIMM-N Memory Interleaving disabled, but is this server configured for NVDIMM-N Memory Interleaving enabled?

→ Perform one of the procedures below.

- Change the NVDIMM-N Memory Interleaving setting for the NVDIMM to the same setting for the server and then, reboot the server. Below is the procedure to change the settings.
  -- If the NVDIMM was previously installed in a server that had NVDIMM-N Memory Interleaving disabled, disable NVDIMM-N Memory Interleaving in System Utility.

- Sanitize all NVDIMMs indicated. All data on the NVDIMM will not be available after sanitization.

[?] **POST error message or IML message is displayed, and all NVDIMMs on processor X are disabled.**

☐ Was the NVDIMM previously inserted in a server on which Channel Interleaving was enabled, while Channel Interleaving is disabled on the current server?

→ Perform one of the procedures below.

- Change the Channel Interleaving setting in System Utility. Below is the procedure to change the settings.
  -- If the NVDIMM was previously installed in a server that had Channel Interleaving enabled, enable Channel Interleaving in System Utility.
- Sanitize all NVDIMMs on processor X.

[?] **POST error message or IML message is displayed, and all NVDIMMs in the system are disabled**

☐ Are NVDIMMs installed on a server?

→ Disable Node Interleaving in System Utility.

☐ Is Advanced Memory Protection set to an option other than Advanced ECC.

→ Change the setting for Advanced Memory Protection to Advanced ECC.

[?] **A POST Error message or an IML message indicating that the Flash Backup Unit (FBU) is not fully charged will be registered**

→ To continue using the NVDIMMs, do one of the following:

- Change NVDIMM-N Backup Power Policy to **Wait for Backup Power on Boot**.
- If NVDIMM-N Backup Power Policy is already configured to **Wait for Backup Power on Boot**, then reboot the server.
- Wait for the flash backup unit (FBU) to charge sufficiently.

[?] **POST error message or IML message is received indicating an unsupported NVDIMM on the system**

→ Replace the NVDIMM with a supported HPE SmartMemory NVDIMM

[?] **POST error message or IML message is displayed, and the system halts**

→ Remove the unsupported capacitor pack from the system, and then install a flash backup unit (FBU).

[?] **POST error message or IML message is displayed indicating that the System Programmable Logic Device revision in this system does not meet minimum requirements for operation with NVDIMMs**

→ Remove all NVDIMMs from the server.

[?] **POST error message or IML message of the processor is received**

→ Be sure each processor is supported by the server and is installed as directed in the server documentation. The processor socket requires very specific installation steps and only supported processors should be installed.

→ Be sure the server ROM is current.

→ Be sure you are not mixing processor stepping, core speeds, or cache sizes if this is not supported on the server.

→ If the server has only one processor installed, reseat the processor.

→ If the server has only one processor installed, replace it with a known functional processor.

→ If the server has multiple processors installed, test each processor:

1. Remove all but one processor from the server. Replace each with a processor terminator board or blank, if applicable to the server.
2. Replace the remaining processor with a known functional processor. If the issue is resolved after you restart the server, a fault exists with one or more of the original processors. Install each processor one by one, restarting each time, to find the faulty processor or processors. At each step, be sure the server supports the processor configurations.

[?] **POST error message or IML message is received indicating an uncorrectable machine check exception**

→ Replace the processor.

[?] **Error message is received indicating low power or loss of power**

→ Replace the battery.

[?] **POST message or IML message is received indicating an issue with either the motherboard or the power backplane**

→ Check all error messages for possible issues with other components and troubleshoot components identified.

→ Make sure that no loose connections exist on the motherboard or power backplane. It is not necessary to reseat processors.

→ Remove any components recently added.

→ Using System Utility <F9>, set the system configuration back to the default value. To set the system configuration back to the default value in case the system does not start, use Jumper Switch SW6.

→ Gather necessary information and contact your sales representative.

[?] **System does not boot from the SD or microSD card**

→ Be sure the drive boot order in the System Utility is set so that the server boots from the SD or microSD card.

→ Use the iLO web interface to verify that the SD card is detected by LO.

→ Remove all power from the server. Reseat the SD or microSD card, and then power on the server.

[?] **System does not boot from the USB drive key**

→ Be sure that USB is enabled in the System Utility.

→ Make sure that the server is configured to boot from the USB drive in "UEFI Boot Order" or "Legacy BIOS Boot Order" of System Utility.

→ Reseat the USB drive key.

→ Move the USB drive key to a different USB port, if available.

[?] **The tape drive is stuck and will not eject**

→ Manually press the eject button. Wait for up to 10 minutes for the tape to rewind and eject.

→ Perform a forced eject:

1. Press and hold the Eject button for at least 10 seconds.
2. Wait for up to 10 minutes for the tape to rewind and eject. The green Ready LED should flash.

→ Power cycle the drive. Wait for up to 10 minutes for the drive to become ready again.

→ Check for conflicts in backup software services.

→ Check the SAS/HBA/Driver configuration of the drive.

→ Inspect media and cables, and discard any that are faulty or damaged.

[?] **A trouble of data import or export has occurred on the tape drive.**

→ Execute Drive Assessment Test with StorageWorks Library and Tape Tools.

Important **If you execute Drive Assessment Test, the tape is overwritten. If you do not want the tape to be overwritten, execute log-based Device Analysis Test instead.**

→ Execute Media Assessment Test with StorageWorks Library and Tape Tools (This is a read-only test).

[?] **The back-up of tape drive cannot be completed without problem.**

→ Execute Drive Assessment Test with StorageWorks Library and Tape Tools.

Important **If you execute Drive Assessment Test, the tape is overwritten. If you do not want the tape to be overwritten, execute log-based Device Analysis Test instead.**

→ Check the back-up log.

→ Check whether the constitution used is supported.

→ Check the followings and confirm whether the media is not damaged.

- Whether the position of label is right
- Whether the reader pin is damaged, left out or becomes loose
- Whether there is damage on the joint of cartridge
- Whether the device is used under wrong circumstances

→ Check the problems of software.

・Check your back-up software.

・Check whether the execution of virus scan software is scheduled when back-up is executed.

→ Check whether a tape can be formatted.

→ Check whether the media used has a proper product number.

→ Using StorageWorks Library and Tape Tools, extract Support Ticket.

・Look for problems in Cartridge STATUS Section.

・Look for problems in Drive STATUS Section.

→ Check whether Tape Error LED is on.

1. Reload the tape that might be the cause of trouble. If the blink of Tape Error LED stops, there is no trouble.

2. Load a new tape or a tape with which no trouble is confirmed. If the blink of Tape Error LED stops, there is no trouble.

3. Reload the tape that might be the cause of trouble. In case Tape Error LED blinks, you should judge the tape is damaged and dispose it.

→ Dispose the media used under the circumstance whose temperature is over 45℃ or below 5℃.

[?] Nothing is displayed for 60 seconds or longer after the server is switched on.

→ Check whether the power cord of monitor is connected to a properly functioning electrical outlet with an earth.

→ Turn on the monitor and check that the power light is on and electricity is supplied to the monitor.

→ Check whether the monitor is connected to a targeted server or a console switch via cable.

→ Check the following connections to confirm there are not any poor connections.

・In case you use a rack-mount type server, check the cable connected to the console switch. In addition, check whether the switch is properly configured for the server. There may be a case that you need to connect the monitor directly to the server to check that the console switch is not damaged.

・In case you use a tower type server, check the connections of cables from the monitor to the sever and from the server to the outlet.

・In case you use a blade, check that SUV cable of c-Class blade is connected to VGA cable of the monitor and to the connector at the front of blade

→ Press any key or enter your password and wait a while until the screen becomes active. Then check that the power saver feature is not enabled.

→ Check that additional power is not needed for the action of PCIe device or the graphic controller.

→ Check that any video expansion board is not added instead of an on-board video. In case a video expansion board is added, there is a case that the video looks not to be functioning. Remove the video cable from the on-board video and connect the cable to the video jack on the expansion board.

Note In all servers, in case any video expansion board is installed, an on-board video becomes disabled automatically.

→ Press any key or enter your password, and wait a while until the screen becomes active. Then check that the power-on password feature is not enabled. In addition, you can check whether the power-on

password is valid according to whether the key-shaped icon is displayed on the screen when POST is completed. In case you do not know your password, you should make the power-on password invalid using the password disabling switch on the motherboard.

→ In case a video expansion board is installed to the slot compatible with PCI hot plug, check the power lamp of slot to confirm electricity is supplied to the slot.

→ Check that the video expansion board is supported on the server and OS.

→ Check that the driver of video is up to date.

[?] The monitor does not function properly when the power saver feature is used.

→ Check that the power saver feature is supported by the monitor. If it is not supported, make the feature disabled.

[?] The colors of video are not displayed properly on the monitor.

→ Check that 15 pin VGA cable is firmly connected to the proper VGA port of the server and the monitor.

→ Check that the monitor and the console switch are compatible with the VGA output of the server.

→ Check that the VGA cable is not damaged. Use the cable which confirmed to be functioning.

[?] Slow moving horizontal lines are displayed on the monitor.

→ Check that electromagnetic interference has not occurred. Move the monitor away from other monitors or transformers.

[?] The mouse and keyboard does not operate properly.

→ Check the followings to confirm there are not any poor connections.

・In case you use a console switching device, you should check that the server is properly connected to the switch.

・In case you use a rack-type server, check the cable to the switch box. In addition, check that the switch is properly configured for the server.

・In case you use a tower-type server, check the connection of cable connecting the input device and the server.

→ In case you use a console switching device, check that all the cables and connectors have proper length and are supported by the switches. Refer to the document of switch.

→ Check whether the latest driver for operating system is installed.

→ Change the device driver and confirm the device driver is not broken.

→ Restart the system and after the server is rebooted, check whether the input devices functions properly.

→ Change the device to an equivalent device (another mouse or keyboard of same type) whose action is confirmed.

・In case any problems occur even with a new mouse or a keyboard, the connector board of system I/O board is damaged. Replace the board.

・If you do not find any troubles, the previous input device is damaged. Change the device.

→ Check that the keyboard and mouse are connected to the proper ports. Check that the LED on the keyboard blinks or NumLock LED lights during POST. In case you cannot observe that, change the connection port.

→ Check that the keyboard and mouse are not dirty.

[?] Recovery method is required from the system while you change an expansion board on a server encrypted by BitLocker.

→ In case you change an expansion board on a server encrypted by BitLocker, disable BitLocker before changing the expansion board. If you do not make BitLocker disabled, System requires the recovery method that was selected when BitLocker was configured. If you cannot enter one or more proper recovery passwords, you will become unable to access all the encrypted data. Enable BitLocker after the installment is finished.

[?] Network Controller or LOM Card does not operate.

→ Check the LED on Network Controller or that of LOM Card to confirm whether there is a status showing the cause of trouble.

→ Check that there are no poor connections.

→ Check that a proper kind of cable suitable for the network speed or that a proper SFP or DAC cable is used. In case you use 10GB network device of dual port, the type of media (DAC cable, equivalent SPF+ module, etc.) should be same on both sides of SFP ports. Mixed use of different SFPs (SR/LR) on one device is not supported.

→ Change the network cable to another cable which is proved to run properly to confirm the network cable functions properly.

→ Check that the problem of software is not the cause of malfunction.

→ Check that the server and the operating system support the controller.

→ In System Utility, check that Controller is enabled.

→ Check that the server's ROM is the latest version.

→ Check that the controller's driver is the latest version.

→ Check that a valid IP address is given to the controller and the configuration is proper.

[?] Network controller or LOM card has become unable to operate.

→ Check the LED on Network controller or that of LOM Card to confirm whether there is a status showing the cause of trouble.

→ Check that a proper network driver for the controller is installed and the driver file is not broken. Re-install the driver.

→ Check that there are no poor connections.

→ Change the network cable to another cable which is proved to run properly to confirm the network cable functions properly.

→ Check that the network controller or LOM card is not damaged.

[?] **Network controller or LOM Card has stopped operating after the addition of expansion board to the server.**

→ Check that there are no poor connections.

→ Check that the server and the operating system support the controller.

→ In case you install a new expansion board, you should re-install network driver not to change the configuration of the server.

1. From the operating system, uninstall the network controller driver of a controller which does not function.
2. Reboot the server and execute the suitable option of System Utility. Check that the server can recognize the controller and the controller can use the resource.
3. Reboot the server and re-install the network driver again.

→ Check that a suitable driver is installed.

→ Check that the parameters of the driver match with the configuration of the network controller.

[?] **A problem has occurred on the network inter connect blade.**

→ Check that the network inter connect blade is properly attached and connected.

[?] **During POST process, the controller is not displayed or an error is displayed.**

→ Check that the controller is supported by the server.

→ Check that the controller is properly connected and fixed.

→ Check that the cable is properly connected.

→ In case that the controller is physically damaged, replace it.

→ In case the controller is recognized by system BIOS, re-install the controller.

→ Execute the diagnosis of controller and follow the procedure displayed.

→ Update the firmware to the latest version.

→ Download Active Health System log.

[?] **The duplication of controller has been lost (an error is not displayed during POST process or cache has been disabled).**

→ Check that the controller is supported by the server.

→ Check that the controllers are properly connected and fixed.

→ Check that the cable is properly connected.

→ In case that the controller is physically damaged, replace it.

→ Execute the diagnosis of controller and follow the procedure displayed.

→ Check that the controllers are compatible models.

→ Check that the cache sizes of controllers are compatible.

→ Check that Flash Backup Unit (FBU) is properly installed and connected.

→ Update the firmware to the latest version.

→ Download Active Health System log.

[?] A POST Error message or an IML message will be registered on an arbitrary server where the Flash Backup Unit (FBU) is configured for the Smart Array Controller

→ Check that Flash Backup Unit (FBU) is properly installed.

→ Confirm whether Flash Backup Unit (FBU) is fully charged.

→ Update the system ROM.

[?] An error, retry, time-out, or a drive error not included in the guarantee occurs when an old Mini-SAS cable is used.

→ The product life cycle of Mini-SAS connector is 250 times of connection/disconnection (outer, inner and cable Mini-SAS connector).

→ If you use an old Mini-SAS cable whose product life cycle is ending, replace it.

[?] In a connection using SUV cable, a USB device is not recognized, an error message is displayed, or a device cannot be turned on.

→ Remove the USB device and execute any of the followings.

・Connect a USB device which needs less than 500mA of electricity.

・Connect the USB hub of external power source to the SUV cable and connect the USB device to the hub.

[?] On the flow control of LAN Controller

→ In case Flow Control is set to “Auto Negotiation”, “Rx & Tx Enabled”, “Tx Enabled” or “transmission enabled”, or “transmission/reception enabled”, when the packet processing of OS stops in the state of heavy reception load due to system hang etc., PauseFrame might be transmitted continuously. In such cases, due to massive pile-up of packets at the switch side, the buffer within the switch becomes scarce and all communication devices connected to the switch may be affected. In order to avoid such cases, set Flow Control to “Disabled” or “Invalid”.

5.6 Problem of OS Operation

[?] Windows operation is unstable

☐ Have you installed Starter Pack?

→ See "*Installation Guide (Windows)*" to install Starter Pack.

If you restore the Windows from a backup tool, Starter Pack is needed to install again.

[?] Cannot turn the power OFF at the blue screen (STOP error screen)

→ Perform the forced shutdown (continue to press the power switch at least four seconds) to turn off the server.

[?] Unable to connect to a network

☐ Is the cable connected properly?

→ Securely connect the proper cable to the network port on the rear of the server. Additionally, make sure that the cable conforms to the network interface standards.

☐ Are BIOS settings correct?

→ With System Utility, you can set the internal network controller to disabled. Check the BIOS settings with Setup Utility.

☐ Have you completed protocol and services settings?

→ Confirm that the network driver for the server has been installed and various settings, such as TCP/IP protocol, have been properly specified.

☐ Are transfer rate settings correct?

→ Confirm that the transfer rate and duplex mode are the same as those of the connecting hubs.

[?] OS stops

→ Using a latest virus scan utility, scan viruses.

→ Check the event log.

→ Check IML.

→ In order that you can check when needs emerge, collect the information on NMI crash dump.

→ Acquire Active Health System Log and inform the content to your sales representative.

[?] An error message is displayed in the error log

→ Follow the information displayed in the error log.

[?] After starting Windows, the time advances or delays by several hours

☐ Is Time Zone of the RBSU correctly set?

→ Check whether Time Format is set to "Local Time" in Date and Time of the RBSU. In addition, check whether Time Zone is set to "Unspecified Time Zone" in this case.

If it is set to "Local Time" while not set to "Unspecified Time Zone," change the settings in the following procedure.

1. Select Date and Time from System Utility (<F9> Launch).
2. Change Time Format to "UTC."
3. Change Time Zone to "Unspecified Time Zone."
4. Set Time Format back to "Local Time" while keeping the status set in step 3.
5. Press the <F10> key to save the setting. If it is saved using the <F12> key at this time, the setting can not be reflected correctly since the OS will be started without rebooting.
6. Select "Reboot the System" from System Utility, then restart it.

[?] On Windows OS, there is a Virtual Install Disk (a Drive called VID).

→ By following the steps below, you can disable the Virtual Install Disk.

Tips

In the Virtual Install Disk, the drivers used during the installation of Windows OS are stored.
When Virtual Install Disk is installed by the manual option, it is automatically enabled and automatically install the necessary drivers.

1. Press the F10 key during POST to start the EXPRESSBUILDER.
2. After restarting from EXPRESSBUILDER, click [Perform Maintenance].
3. Click [BIOS/Platform Configuration].
4. Go to [BIOS/Platform Configuration (RBSU)] - [System Options] - [USB Options] - [Virtual Install Disk] and set to Disabled.
5. Click the [BIOS/Platform Configuration (RBSU)] on the left pane and click [Update].
6. After restarting, VID will be disabled.

With this, the procedure is completed.

5.7 Problem of Starter Pack DVD

[?] Unable to read the manuals

☐ Have you installed Adobe Reader to your computer?
→ To read the manuals, install Adobe Reader in your computer.

☐ Is an error message "Internet Explorer has stopped" displayed?
→ Close the dialog box and continue the operation. When the same error message appears again, double-click "version.xml" under the root directory of the DVD, and choose Yes in the dialog box.

[?] The menu item of Integrated Installation is gray

☐ Is your system environment suitable?
→ To run Integrated Installation, log on to the Windows on the server with an administrative account.

[[?] The menu is displayed with a wrong language

☐ Is your system environment suitable?
→ Confirm the settings of **Regional and Language Options**. Specify the language settings of each tab to **English (US)**.

5.8 Problem of Bundled Software

[?] The installer is displayed by a wrong language or resulted in an error

☐ Is your system environment correct?

→ Confirm the settings of **Regional and Language Options**. Set the language settings of each tab to **English (US)**.

[?] The problem of NEC ESMPRO ServerAgentService (for Windows)

→ For details of NEC ESMPRO ServerAgentService (for Windows), see *NEC ESMPRO ServerAgentService Installation Guide (Windows)* in Starter Pack.

[?] The problem of NEC ESMPRO Manager

→ For details of NEC ESMPRO Manager, see *NEC ESMPRO Manager Installation Guide* or online help.

5.9 Problem of Optical Disk Drive

[?] Unable to access or play CD, DVD and other optical disks

☐ Is the disk properly set in the optical disk drive tray?

→ There is a holder in the tray to secure the disk. Make sure that the disk is securely placed in the holder.

[?] Unable to access or play DVD/CD-ROMs

☐ Is the DVD/CD-ROM supported by the server?

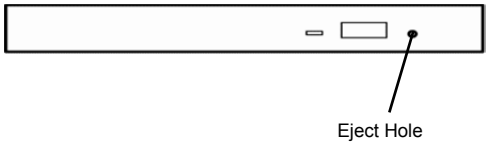
→ For a CD with copy guard which does not conform to the CD standard, the playback of such a disk with the optical disk drive is not supported.

→ The DVD/CD-ROM for Macintosh is not supported.

[?] Unable to eject a disk using the eject button

→ Eject the disk in the following steps.

1. Press the power switch to turn off the server (POWER/SLEEP LED is off).
2. Use a 100 mm long metal pin that is 1.2 mm in diameter (or uncoil a thick paper clip) and insert it into Eject Hole at the front of the tray. Keep pressing slowly until the tray comes out.



Important
- **Do not use toothpicks, plastic and other fragile pins.**
- **If you still cannot eject the disk, contact your sales representative.**

3. Pull the tray out with your hands.
4. Remove the disk.
5. Push the tray back to its original position.

[?] Unable to start the system from the CD-ROM or the DVD drive.

→ Regarding the drive boot process of System Utility, check that the server is configured to start first from the CD-ROM or the DVD drive.
→ Check whether there is a poor connection.
→ Check whether the disc is not damaged.
→ Check whether the drive is not damaged.
→ In case that the OS and the server support boot from USB CD-ROM or DVD drive and boot is possible, check whether legacy support of USB CD-ROM or DVD drive.

[?] Data read out from a CD-ROM or a DVD drive is broken or data cannot be read out.

→ If contamination or residue is left on the surface of CD or DVD, clean the drive and the disc. In case a label is attached to the surface of disc, remove the label and the residue of adhesive.
→ Check whether the device supports the specification of disc.

[?] Unable to detect a CD-ROM or a DVD drive.

→ Check whether there is a poor connection.
→ Check whether the drive or the cable is not damaged.
→ Update the driver to the latest version.

6. Windows System Recovery

Recover the Windows system by using the following instructions if the system does not work normally.

Note

- After recovering the system, be sure to install each driver and Standard Program Package.
  See "*Installation Guide (Windows)*" to install Standard Program Package and device drivers.
- If the Windows system cannot find hard disk drives, you cannot recover the Windows system.

6.1 Recovery of Windows Server 2016 / Windows Server 2012 R2

If the Windows does not start normally, you can recover it using the feature of the Windows installation disc.
To run this feature, start the installation disc, and then choose **Repair your computer** in **Windows Setup** wizard.
We recommend that this option is performed by the system administrator.

If the RAID controller driver is required, take the following steps:

Note

In case you use an on-board RAID controller and an internal optical disc drive, load the driver from a removable media.
Copy the following folder from Starter Pack DVD to a removable media beforehand.
<DVD>:**\software\001\drivers\sw_raid1_driver**

1. Turn on the power to the display and this server in that order or restart.
   Set the OS install media.
2. Press <F11> key during POST to start Boot Menu.
   In **One-Time Boot Menu**, select the optical disc drive to which OS install media is set.
3. Start the OS from the OS installation media.
   The message "Press any key to boot from CD or DVD..." appears on the upper part of the screen.
   To boot from the media, press the <Enter> key.
   While boot-up proceeds, the message "Loading files..." appears.
4. Choose **Repair your computer** in **Windows Setup wizard**.
5. Click **Troubleshoot**.
6. Click **Command Prompt**.
7. After setting Starter Pack DVD to the drive, execute the following command to load the driver:

For on-board RAID controller:

```
drvload <DVD>:\software\001\drivers\sw_raid1_driver\SmartDQ.inf
```

Tips

In case you use an on-board RAID controller or an internal optical disc drive, load the driver from a removable media.

drvload <Removable Media>:\sw_raid1_driver\SmartDQ.inf

For RAID controller (N8103-189/190/191/192/193/194/195/201)

```
drvload <DVD>:\software\001\drivers\dac1_driver\SmartPqi.inf
```

Tips

The volume label for each drive can be checked from the display result of the dir command.

Example: **dir C:**

8. Exit the command prompt.

The driver installation is completed.

7. Resetting and Clearing the Server

See this section if the server does not work or if you want to set the system settings back to the default settings.

7.1 Software Reset

In case POST processing stops and does not operate, or the server stops during the start-up of System Utility, press <Delete> key while pressing <Ctrl> key and <Alt> key. Clear all the data in progress that are stored in the memory and restart.

7.2 Forced Shutdown

In case you cannot turn off the power in the following situations, press the power switch of device for 4 seconds or longer. You can forcefully turn off the power.

- Unable to turn off the power although you have executed the shutdown from OS.
- Unable to turn off the power although you have pressed the POWER switch.

Regarding the position of POWER switch, see *Chapter 1 (4.2 Front View (Without Front Bezel))* in *User's Guide*.

Note If you want to turn on the power again, do so after you wait for 30 seconds or longer.

7.3 Initialization of System Configuration Information

7.3.1 Description on the Features of System Maintenance Switch

Here we describe the features of system maintenance switch of the server.

Table: Detailed Features of System Maintenance Switch

Position	Default	Configuration	Features
SW1 *1, *5	OFF	OFF	Set to OFF usually.
		ON	Set the security of iLO5 to disabled.
SW2	OFF	Reserved	—
SW3	OFF	Reserved	—
SW4	OFF	Reserved	—
SW5 *2, 5	OFF	OFF	Set to OFF usually.
		ON	Clears power-on password and administrator password.
SW6 *3, *5	OFF	OFF	Set to OFF usually.
		ON	Set the system configuration back to the default values. *4
SW7	OFF	Reserved	—
SW8	OFF	Reserved	—
SW9	OFF	Reserved	—
SW10	OFF	Reserved	—
SW11	OFF	Reserved	—
SW12	OFF	Reserved	—

Important **Do not change the system maintenance switch that says “Reserved” unless it is instructed by the document. It may cause the trouble or malfunction of device.**

*1 Set SW1 to ON in the following cases.
- When the passwords of all the users which administrator authority is given of iLO5 have become unknown
- When you change the feature of iLO5 from disabled to enabled

*2 Regarding the operation procedure of SW5, see *Chapter 2 (7.3.4 Clearing a Password)* of this document.
*3 Regarding the operation procedure of SW6, see *Chapter 2 (7.3.3 Set the System Configuration Back to Default Values).*
*4 Default values may be different from the factory preset.
*5 When you set SW1, SW5, and SW6 to ON at the same time, boot with the backup ROM.

7.3.2 Operation Procedure of System Maintenance Switch

When you operate the system maintenance switch, follow the procedure below.

1. Check the position of the system maintenance switch: SWx (x stands for the number of the switch).

2. Regarding the positions of system maintenance switch, refer to the following diagram of R120h-2M or R120h-1M.

3. Referring to *Chapter 2 (1.2 Overview of Installation and Removal)* in *User's Guide* attached to the device, remove the top cover.

4. In case you cannot operate the system maintenance switch because of an option board installed, remove the raiser cage referring to *Chapter 2 (1.11 Riser Card)* in *User's Guide*.

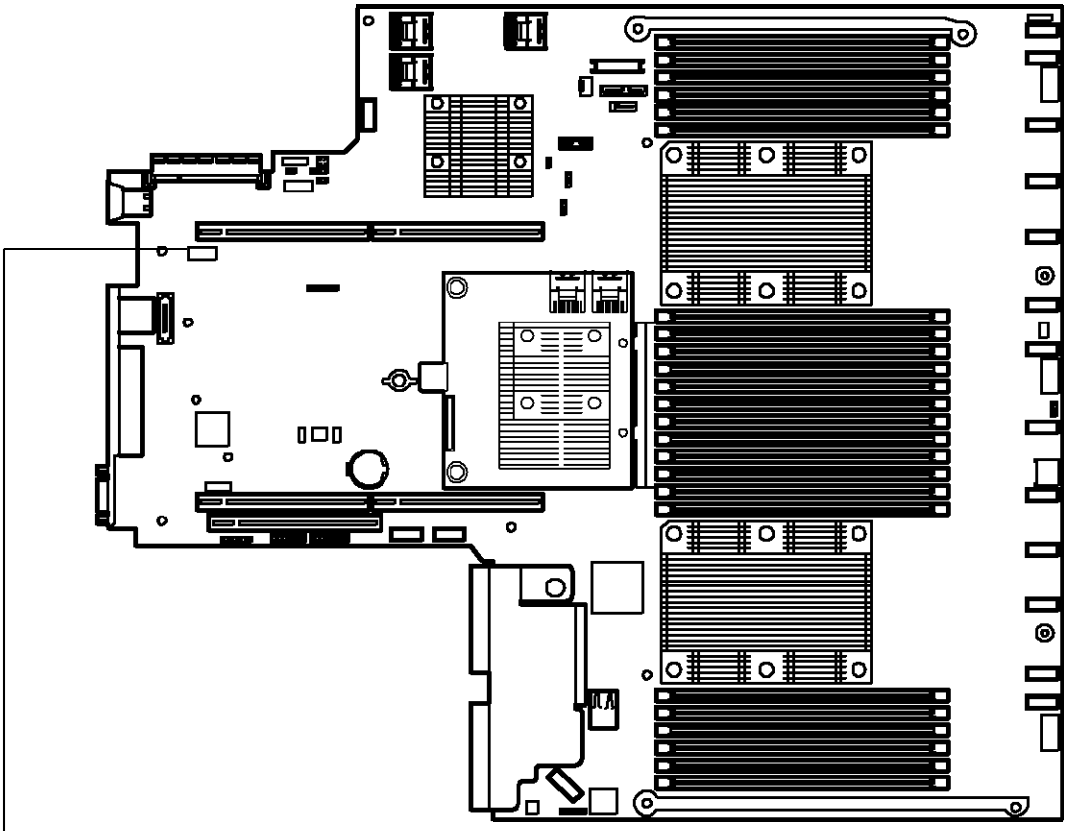
5. Change the system maintenance switch you want to operate to ON or OFF.

Important **Referring to *Chapter 1 (1.8 Measures against Electrostatic Discharge)* in "For the Safe Use", work caring for electrostatic discharge.**

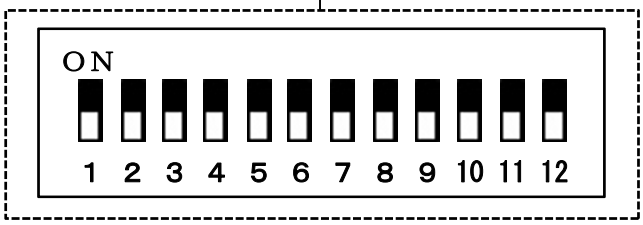
Important **When you handle the system maintenance switch, use a sharp tool such as a pointed toothpick or tweezers (however, avoid ones with sharp edges) and slide it horizontally to the direction of your handling. Do not operate with a mechanical pencil.**

6. Assemble the parts you removed to the original state, and then connect the power cord.

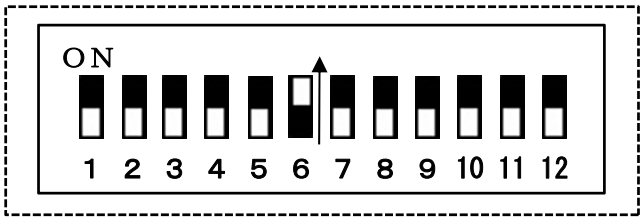
R120h-2M



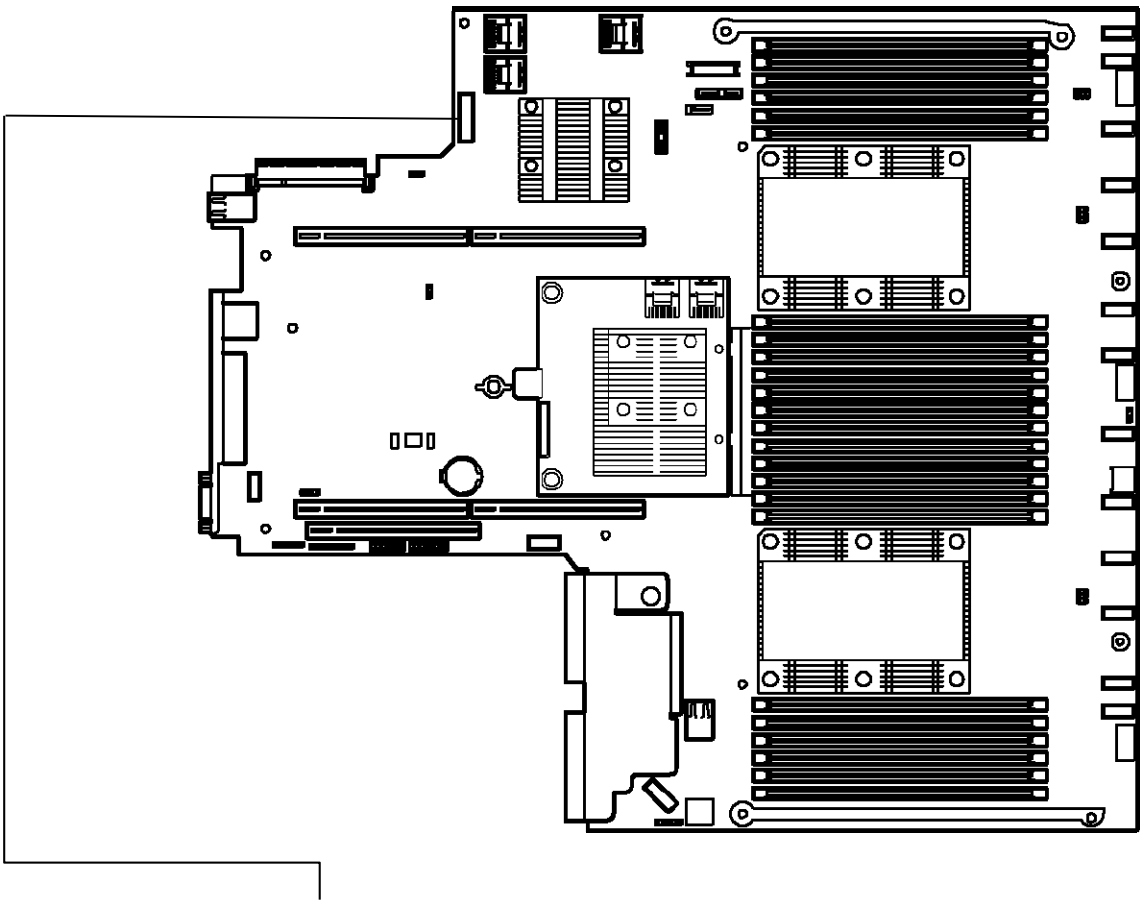
In case all the switches are OFF (default)

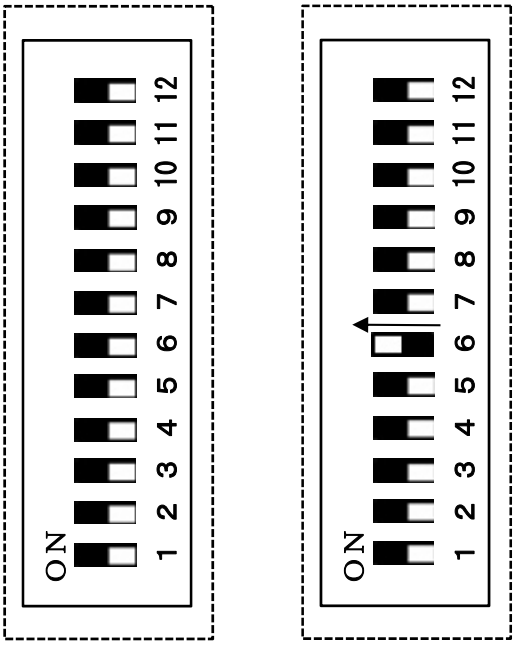


(Ex.) In case you changed only SW6 to ON



R120h-1M





In case all the switches are OFF (default)

(Ex.) In case you changed only SW6 to ON

7.3.3 Set the System Configuration Back to Default Values

In case the device cannot be started due to the change of system configuration etc., you can initialize the system configuration by operating the system maintenance switch SW6 on the motherboard. It has the same function as the Restore Default Manufacturing Settings in the System Default Options menu. For more details, please refer to *Chapter 2 (1. System Utilities)* of this book.

The operation procedure of system maintenance switch SW6 is as follows.

1. Follow *Chapter 2 (7.4.2 Operation Procedure of System Maintenance Switch)* of this document to change the system maintenance switch: SW6 to ON.

2. Press POWER Switch to turn on the power.

3. After about 10 seconds, the following message is displayed.
   Maintenance switch detected in the On position.
   The System is being default configured. This may take a few minutes…

4. Then after about 20 seconds, the following message is displayed.
   Power off the server and toggle the maintenance switch to the Off position.

5. Keep pressing POWER Switch for longer than 4 seconds to turn off the power forcibly.

6. Follow *Chapter 2 (7.3.2 Operation Procedure of System Maintenance Switch)* of this document to set the system maintenance switch: SW6 back to ON.

7. Press POWER Switch to turn on the power.

8. The following error message is displayed during POST.
   267 – IMPORTANT: Default configuration settings have been restored at the request of the user.
   Action: Restore any desired configuration settings which differ from defaults.

9. Press <F9> key to start System Utility.

10. In **System Default Options** menu, select **Restore Default Manufacturing Settings** and set it to **Yes, restore the default settings**.

11. A dialog that says **[Question] Do you want to reboot the system?** appears.

12. If you select **OK**, the device restarts.

Tips When you start the device after initializing the system configuration, the device may restart during POST.

Tips You can set the system configuration back to the default values when SW6 is ON, but Power On Password and Administrator Password are not included.

7.3.4 Clearing a Password

In case you forget a password to log in System Utility or Power On Password, you can clear passwords by operating the system maintenance switch SW5.

To operate the system maintenance switch SW5, follow the procedure below.

1. Turn the system maintenance switch: SW5 into ON in accordance with *Chapter 2 (7.3.2 Operating Procedure of System Maintenance Switch)* in this manual

2. Press POWER Switch to turn on the power.

3. Press the <F9> key during POST execution.

4. The following message is displayed on the screen and then POST will be stopped.

   Password override switch detected in the 'ON'
   position.
   Power off the server and turn switch to the

5. When POST stops, press the POWER switch to turn the power OFF.

6. Turn the system maintenance switch: SW5 into OFF again in accordance with *Chapter 2 (7.3.2 Operating Procedure of System Maintenance Switch)* in this manual.

Tips If the <F9> key is not pressed, POST will proceed normally without displaying the message. However, the password will be cleared. In that case, turn off the power after waiting until POST is completed.

7. Press POWER Switch to turn on the power.

NEC Express5800 Series
Express5800/R120h-1M, R120h-2M

2 Useful Features

This chapter explains useful features of this product. Refer to it when necessary.

1. **System Utilities**
   This section explains how to configure the system and details the parameters.

2. **RAID System Configuration**
   This section explains the RAID configuration utility built in this machine.

3. **Details of EXPRESSBUILDER**
   This section explains EXPRESSBUILDER, which comes with this machine.

4. **Details of Starter Pack**
   This section details Starter Pack.

5. **iLO 5**
   This section explains iLO 5.

6. **NEC ESMPRO**
   This section explains NEC ESMPRO, an application for management and monitoring.

7. **NEC Product Info Collection Utility**
   This section explains the NEC Product Info Collection Utility.

8. **Smart Storage Administrator**
   This section explains Smart Storage Administrator.

9. **Express Report Service / Express Report Service (HTTPS)**
   This section explains Express Report Service and Express Report Service (HTTPS), which automatically report failure information about this machine.

10. **Express Report Service (MG)**
    This section explains Express Report Service and Express Report Service (MG), which automatically report failure information about this machine.

1. System Utilities

The System Utilities, built in the system ROM, provide the configuration instructions for the launching order, the diagnostic function for detecting system abnormality, and the log collection function for enabling quick analysis after occurrence of a system failure, as well as system information checking and the function of configuring the devices.

1.1 Launch the System Utilities

To launch the System Utilities, power on this machine or restart it to advance POST.
After a while, the following message appears at the bottom of the screen.
Press the <F9> key. POST ends at this time. The System Utilities is launched.

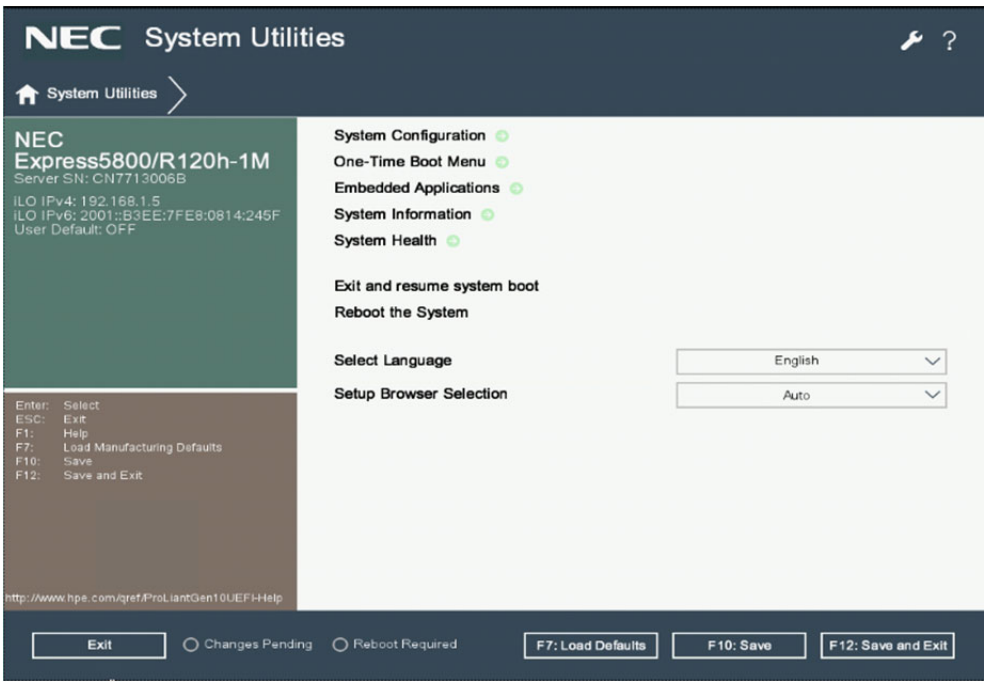
Tips The messages displayed vary, depending on the environment.

1.2 Parameter Descriptions

When the System Utilities are launched, the following menu appears.

- **System Configuration**
- **One-Time Boot**
- **Embedded Application**
- **System Information**
- **System Health**
- **Exit and resume system Boot**
- **Reboot the System**
- **Select Language**
- **Setup Browser Selection**

These menus have submenus for relevant items. Selecting submenus allows you to configure further detailed parameters.



For details about the options, see the table below.

Option	Parameter	Description
System Configuration	–	Displays the **System Configuration** menu. You can use this option to set up the System Utilities, the other system devices, and the option card devices.
One-Time Boot	–	Displays the **One-Time Boot** menu. Use this option to boot the system only one time from a device not dependent on the predefined boot order. Selecting a device through **One-Time Boot** menu does not change the predefined boot order.
Embedded Application	–	Displays the [Embedded Application] menu. By using this option, you can update **Embedded UEFI Shell**, [EXPRESSBUILDER], and firmware or display [Embedded Diagnostics], [Integrated Management Log], and [Active Health System Log].
System Information	–	Displays the **System Information** menu. Use this menu to view system information including the system name, system ROM version, date, processor information, and memory information.
System Health	–	Displays the **System Health** menu. Use this option to display the health status of all the devices within this machine. When an error is detected during POST, <F2> View Information/Errors appears. This starts up by pressing the <F2> key.
Exit and resume system boot	–	Exits the System Utilities and continues with the usual boot process.
Reboot the System	–	Exits the System Utilities and restart the BIOS.
Select Language	[English] Simplified Chinese Japanese	Changes the current language of the system.
Seup Browser Selection	GUI Text [Auto]	Selects the setup browser to use. In the [Auto] mode, use [Text] when the user enters the System Utilities via the serial console or [GUI] when the user enters it via the IRC or physical terminal.

[ ]: Default setting

1.2.1 System Configuration

When you select **System Configuration** from the System Utilities, the following menu appears.

- **BIOS/Platform Configuration (RBSU)**
- **BMC Configuration Utility**
- **Embedded device information**

For details about the options, see the table below.

Option	Parameter	Description
BIOS/Platform Configuration (RBSU)	–	Accesses **BIOS/Platform Configuration (RBSU)** to set up the System Utilities and other platforms.
BMC Configuration Utility	–	Launches **BMC Configuration Utility** in order to set up BMC.
(Embedded device name)	–	Sets the embedded device parameter. The number of options displayed increases or decreases, depending on whether or not a PCIe device is installed. Example: Embedded LOM

1.2.2 BIOS/Platform Configuration (RBSU)

When you select **System Configuration** > **BIOS/Platform Configuration (RBSU)** from the System Utilities, the **BIOS/Platform Configuration (RBSU)** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
Workload Profile	General Power Efficient Compute General Peak Frequency Compute General Throughput Compute Virtualization - Power Efficient Virtualization - Max Performance Low Latency Mission Critical Transactional Application Processing High Performance Compute(HPC) Decision Support Graphic Processing I/O Throughput Custom	Select this option to choose a workload profile for power and performance.
System Options	–	Select this option to display the available System Options. System Options include various configuration options.
Processor Options	–	Select this option to display Processor options, such as configuring Intel Hyper-Threading, Processor Core Enablement, and x2APIC Support.
Memory Options	–	Use this option to configure additional memory options, such as Advanced Memory Protection.
Virtualization Options	–	Select this option to display virtualization options, such as Virtualization Technology, Intel VT-d, and SR-IOV.
Boot Options	–	Select this option to display the Boot Options menu. Use this menu to configure Boot Options, such as Boot Mode, UEFI Optimized Boot, Boot Order Policy, UEFI Boot Order, and Legacy BIOS Boot Order.
Network Options	–	Select to enter the Network Options.
Storage Options	–	Use this option to configure storage options, such as PCIe Slot Storage Boot Policy options.
Power and Performance Options	–	Select this option to display Power Management and Performance options. Use this menu to set the Power Regulator, Advanced Power Options, Intel Turbo Boost, ACPI SLIT, and other Power and Performance options.
Embedded UEFI Shell	–	Select this option to display the Embedded UEFI Shell options menu. Use this menu to enable the Embedded UEFI Shell, add the Embedded UEFI Shell in the boot order, and enable automatic execution of the default UEFI Shell startup script.
Server Security	–	Select this option to display the Server Security menu. Use this menu to set the power-on and administrator password, and to set access to EXPRESSBUILDER and the Trusted Platform Module (TPM).

Option	Parameter	Description
PCIe Devices Configuration	–	Select this option to display the PCI Express (PCIe) Device options menu. Use this menu to configure options, such as PCIe Device Disable, and other PCIe related power and performance options.
Advanced Options	–	Select this option to display all the available Advanced Options. Advanced Options do not generally require modification from their default values, but might need to be modified in some situations.
Date and Time	–	Use this option to enter the Date and Time options.
System Default Options	–	Select this option to display the System Default Options.

[ ]: Default setting

(1) System Options Menu

When you select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **System Options** from the System Utilities, the **System Options** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
Boot Time Optimizations	–	Select this option to display Boot Time Optimizations options, such as Dynamic Power Capping, and Extended Memory Test.
Serial Port Options	–	Select this option to display the Serial Port Options menu. Use this menu to configure the Embedded and Virtual Serial Port settings.
USB Options	–	Select this option to display USB options, such as setting USB control, USB boot support, and removable flash media boot sequence.
Server Availability	–	Select this option to display the Server Availability menu. Use this menu to enable the Automatic Server Recovery Status and Timeout, configure Power-on-Self-Test, set the Power Button Mode, and set the Power-On Delay.
Server Asset Information	–	Select this option to display the Server Asset Information options. Use this menu to modify server information, administrator contact information, service contact information, and the system startup message.
Diagnostics Options	–	This device does not support it.

(a) Boot Time Optimizations Menu

When you select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **System Options**> **Boot Time Optimizations** from the System Utilities, the **Boot Time Optimizations** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
Dynamic Power Capping Functionality (*1)	Auto Enabled [Disabled]	This setting is to correct the power value during POST. If this is set to [Auto], the power value is corrected at the first startup of this device. After this, correction of this value is performed when this device is configured or the settings are changed. If this is set to [Disabled], the power value is not corrected, and Dynamic Power Capping is not supported. If this is set to [Enabled], the power value is corrected every time the device starts up.
Extended Memory Test	Enabled [Disabled]	When enabled, the system validates memory during the memory initialization process. If uncorrectable memory errors are detected, the memory is mapped out, and the failed DIMMs are logged to the Integrated Management Log (IML). Enabling this option can result in a significant increase in the server boot time.
Memory Fast Training	[Enabled] Disabled	This option enables a boot time reduction by controlling when the BIOS bypasses the full memory training. When enabled, the server bypasses the full memory training during boot, and uses memory parameters determined on a previous boot to decrease boot time. Note that even when enabled, the BIOS performs a full memory training if the DIMM configuration or processor configuration changes, or if there is a change in any BIOS setting related to memory or processor configuration. When disabled, the server performs a full memory training on every server boot.
UEFI POST Discovery Mode	[Auto] Force Full Discovery Force Fast Discovery	Use this option to configure the UEFI POST Discovery Mode. When Auto is selected, the system selectively starts devices which are required for booting the devices in the UEFI Boot Order list. Note: For some situations with auto mode like system configuration change, the system will change to start all devices for discovering all boot devices. When Force Full Discovery is selected, the system starts all devices in the system providing full boot device availability. Note: When Force Full Discovery is selected, boot time might significantly increase. When Force Fast Discovery is selected, the system starts devices as less as possible for getting the shortest boot time. Note: When Force Fast Discovery is selected, some unsupported device might not work properly. You might need to replace the unsupported device with the supported one.
Memory Clear on Warm Reset	Enabled [Disabled]	Use this option to configure when memory is cleared on warm resets. When disabled, the contents of memory are only cleared on a warm reset if requested by the operating system. When enabled, memory is cleared on all reboots. Disabling this option can save boot time by skipping the clearing of memory on warm resets.

[ ]: Default setting

*1: an option usable with System ROM Version 1.20 or later.

(b) Serial Port Options Menu

When you select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **System Options** > **Serial Port Options** from the System Utilities, the **Serial Port Options** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
BIOS Serial Console and EMS	-	Select this option to display the BIOS Serial Console and EMS menu. Use the menu to view POST error messages and run the System Utilities remotely through a serial connection to the server COM port or Virtual Serial port. The remote server does not require a keyboard or mouse.
Embedded Serial Port	COM 1; IRQ4; I/O: 3F8h-3FFh [COM 2; IRQ3; I/O: 2F8h-2FFh] Disabled	Select this option to assign the logical COM port address and associated default resources to the selected physical serial port. The operating system can overwrite this setting.
Virtual Serial Port	[COM 1; IRQ4; I/O: 3F8h-3FFh] COM 2; IRQ3; I/O: 2F8h-2FFh Disabled	Use this option to assign the logical COM port address and associated default resources used by the Virtual Serial Port (VSP). In order to support BIOS Serial Console and serial console of operating system, VSP enables emulated serial port that provides management processor.

[ ]: Default setting

①. BIOS Serial Console and EMS Menu

When you select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **System Options** > **Serial Port Options** > **BIOS Serial Console and EMS** from the System Utilities, the **BIOS Serial Console and EMS** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
BIOS Serial Console Port	[Auto] Disabled Physical Serial Port Virtual Serial Port	Use this option to re-direct video and keystrokes through the serial port to OS boot. This option can interfere with non-terminal devices attached to the serial port. In such cases, set this option to disabled. This option is only supported in English language mode when running in the UEFI pre-boot System Utilities.
BIOS Serial Console Emulation Mode	VT100 ANSI [VT100+] VT-UTF8	Use this option to select the emulation mode type. The option you select depends on the emulation you want to use in your serial terminal program (such as HyperTerminal or PuTTy). The BIOS Serial Console Emulation Mode must match the mode you select in your terminal program.
BIOS Serial Console Baud Rate	9600 19200 38400 57600 [115200]	This is the transfer rate at which data is transmitted through the serial port.

Option	Parameter	Description
EMS Console	[Disabled] Physical Serial Port Virtual Serial port	Use this option to configure the ACPI serial port settings, which include the ability to redirect the Windows Server Emergency Management console (EMS) through either the physical or virtual serial port.

[ ]: Default setting

(c) USB Options Menu

When you select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **System Options** > **USB Options** from the System Utilities, the **USB Options** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
USB Control	[All USB Ports Enabled] All USB Ports Disabled External USB Ports Disabled Internal USB Ports Disabled	All USB Ports Enabled: Enables all USB ports and embedded devices. All USB Ports Disabled: Disables all USB ports and embedded devices. External USB Ports Disabled: Disables only external USB ports. Internal USB Ports Disabled: Disables only internal USB ports.
USB Boot Support	[Enabled] Disabled	Set this option to disabled to prevent the system from booting to any USB devices connected to the server. This includes preventing boot to virtual media devices, and the embedded SD or uSD card slot (if supported).
Removable Flash Media Boot Sequence	Internal SD Card First Internal DriverKeys First [External DriveKeys First]	Use this option to select which USB or SD Card devices you want to search for first when enumerating boot devices. You can select whether the system boots to external USB drive keys, internal USB drive keys, or the internal SD card slot. This option does not override the device boot order in the Standard Boot Order (IPL) option. You can only configure this option when Boot Mode is set to Legacy BIOS.
Virtual Install Disk	Enabled [Disabled]	Use this option to control the Virtual Install Disk. The Virtual Install Disk contains drivers specific to this server that an OS can use during installation. If enabled, the Virtual Install Disk appears as a drive in the operating system.
Internal SD Card Slot	[Enabled] Disabled	Use this option to enable or disable the Internal SD Card Slot. When set to disabled, the SD card slot is disabled, regardless of whether an SD Card is installed or not. The SD Card will not be visible in the pre-boot environment or under the operating system.

[ ]: Default setting

(d) Server Availability Menu

When you select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **System Options** > **Server Availability** from the System Utilities, the **Server Availability** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
ASR Status	[Enabled] Disabled	Use this option to configure the Automatic Server Recovery option, which enables the system to automatically reboot if the server locks up.
ASR Timeout	[10 Minutes] 15 Minutes 20 Minutes 30 Minutes 5 Minutes	When Automatic Server Recovery is enabled, you can use this option to set the time to wait before rebooting the server in the event of an operating system crash or server lockup.
Wake-On LAN	[Enabled] Disabled	You can configure the server to be powered on remotely when it receives a special packet. This option requires a NIC, NIC driver, and operating system that are WOL-capable.
POST F1 Prompt	[Delayed 20 Seconds] Delayed 2 Seconds Disabled	Use this option to configure the system to display the F1 key on the server POST screen. If an error is encountered, you can press the F1 key to continue with the server power-up sequence. Select one of the following options: Delayed 20 Seconds - If an error occurs, the system pauses for 20 seconds at the F1 prompt and continues to boot the OS. Delayed 2 Seconds - If an error occurs, the system pauses for 2 seconds at the F1 prompt and continues to boot the OS. Disabled - If an error occurs, the system bypasses the F1 prompt and continues to boot the OS. Note: For critical errors, the system pauses for 20 seconds at the F1 prompt, regardless of how this option is configured.
Power Button Mode	[Enabled] Disabled	Disabling this option disables the momentary power button functionality. This option does not affect the four-second power button override or the remote power control functionality.
Automatic Power-On	Always Power On Always Power Off [Restore Last Power Stats]	Use this option to configure the server power state when AC power is applied to the system. By default, the system returns to its previous power state when AC power is restored after an AC power loss. Always Power On and Always Power Off cause the system to always return to the "on" and "off" state, respectively, whenever power is applied, even if the system is in the "off" state when power is lost.
Power-On Delay	[No Delay] random Delay 15 Second Delay 30 Second Delay 45 Second Delay 60 Second Delay	Use this option to delay the server from turning on for a specified time. Pressing the power button (using the Virtual Power Button), or Wake-ON LAN events, and RTC Wake-up events override the delay and power on the server without any additional delay. This enables staggering when servers power-up after a power loss to prevent power usage spikes. Note that the actual delay before the server is powered on will be longer than the specified time because the server must always wait for iLO FW to initialize before the server attempts to power on.

[ ]: Default setting

(e) Server Asset Information Menu

When you select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **System Options** > **Server Asset Information**, the **Server Availability** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
Server Information	−	Select this option to modify the server information.
Administrator Information	−	Enter the administrator's contact information.
Service Contact Information	−	Enter the service contact information.
Cutom POST Messages	String of up to 62 alphanumeric and/or special characters	Enter a message to be displayed on POST screen during system startup. This feature limits POST screen messaging to 62 characters, special characters are also accepted.

[ ]: Default setting

①. Server Information Menu

When you select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **System Options** > **Server Asset Information**, the **Server Information** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
Server Name	String of up to 28 characters	Select this option to modify the server name text line.
Server Assert Tag	String of up to 33 characters	Select this option to modify the Server Asset Tag text line.
Assert Tag Protection	Locked [Unlocked]	Use this option to lock Asset Tag information. When set to lock, the Asset Tag is not erased if the default system settings are restored.
Server Primary OS	String of up to 43 characters	Use this option to modify the Server Primary OS text line.
Server Other Information	String of up to 28 characters	Use this option to modify the Other Server text line.
Power-On Logo	[Enabled] Disabled	Use this option to disable the display of the logo during system boot. This option does not affect the server boot time.

[ ]: Default setting

②. Administrator Information Menu

When you select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **System Options** > **Server Asset Information** > **Administrator Information**, the **Administrator Information** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
Administrator Name	String of up to 28 characters	Enter the server administrator's name text.
Administrator Phone Number	Phone number String of up to 28 characters	Enter the server administrator's phone number text.
Administrator E-mail Address	E-Mail Address String of up to 28 characters	Enter the server administrator's e-mail address.
Administrator Other Information	String of up to 28 characters	Enter the server administrator's information text.

[ ]: Default setting

③. Service Contact Information Menu

When you select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **System Options** > **Server Assert Information** > **Service Contact Information**, **Service Contact Information** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
Service Contact Name	String of up to 28 characters	Enter the server service contact name text.
Service Contact Phone Number	Phone number String of up to 28 characters	Enter the server service contact phone number text.
Service Contact E-mail Address	E-Mail Address String of up to 28 characters	Enter the server service contact e-mail address.
Service Contact Other Information	String of up to 28 characters	Enter the other server service contact information text.

(f) Diagnostics Options Menu

When you select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **System Options** > **Diagnostics Options** from the System Utilities, the **Diagnostics Options** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
Embedded Diagnostics	[Enabled] Disabled	This device does not support it.
Embedded Diagnotics Mode	[Auto] Text Console	This device does not support it.

[ ]: Default setting

(2) Processor Options Menu

When you select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Processor Options** from the System Utilities, the **Processor Options** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
Intel(R) Hyper-Threading	Disabled [Enabled]	Use this option to enable or disable Intel Hyper-Threading. When enabled, each physical processor core operates as two logical processor cores. When disabled, each physical processor core operates as one logical processor core. Enabling this option can improve overall performance for applications that benefit from a higher processor core count. This appears only when the processor that supports this function is mounted. This option is displayed only when the installed processor supports this feature.
Enabled Cores per Processor	[0]-X	This option enables limiting the number of enabled processor cores per physical processor. You can set the number of enabled cores to a value supported by the physical processor. Setting the value to 0 or a value larger than the number of supported cores of the installed processor will result in all processor cores in the socket being enabled.
Processor x2APIC Support	[Enabled] Force Enabled Disabled	x2APIC support enables operating systems to run more efficiently on high core count configurations. It also optimizes interrupt distribution in virtualized environments. In most cases, set this option to enabled. This configures the operating system to optionally enable x2APIC support when it loads. Some older hypervisors and operating systems might have issues with optional x2APIC support, in which case disabling x2APIC might be necessary to address those issues. Additionally, some hypervisors and operating systems will not use X2APIC unless this option is set to Force Enabled prior to booting. The Force Enabled option also causes the Intel(R) VT-d setting to be set to enabled.

[ ]: Default setting

(3) Memory Options Menu

When you select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **System Options** > **Memory Options** from the System Utilities, the **Memory Options** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
Advanced Memory Protection	Fast Fault Tolerant (ADDDC) [Advanced ECC Support] Online Spare with Advnced ECC Support Mirrored Memory with Advanced ECC Support	Use this option to configure additional memory protection with ECC (Error Checking and Correcting). Options and support vary per system. Advanced ECC keeps all installed memory available for use while still protecting the system against all single-bit failures and certain multi-bit failures. Online Spare Memory enables a system to automatically map out a group of memory that is detected to be at an increased risk of receiving uncorrected memory errors based on an advanced analysis of corrected memory errors. The mapped out memory is automatically replaced by a spare group of memory without interrupting the system. Mirrored Memory provides the maximum protection against uncorrected memory errors that might otherwise result in a system failure. Fault Tolerant Advanced Double Device Data Correction (ADDDC) enables the system to correct memory errors and continue to operate in cases of multiple DRAM device failures on a DIMM. This provides protection against uncorrectable memory errors beyond what is available with Advanced ECC.
Memory Refresh Rate	[1x Refresh] 2x Refresh	This option controls the refresh rate of the memory controller and might affect the performance and resiliency of the server memory. It is recommended that you leave this setting in the default state unless indicated in other documentation for this server.
Channel Interleaving	[Enabled] Disabled	You can only configure this option if the Workload Profile is set to Custom. Use this option to modify the level of interleaving for which the memory system is configured. Typically, higher levels of memory interleaving result in maximum performance. However, reducing the level of interleaving can result in power savings.
Maximum Memory Bus Frequency	[Auto] 2667 MHz 2400MHz 2133 MHz 1867 MHz	You can only configure this option if the Workload Profile is set to Custom. Use this option to configure the memory system to run memory at a lower maximum speed than that supported by the installed processor and DIMM configuration. Setting this option to Auto configures the system to run memory at the maximum speed supported.
Memory Patrol Scrubbing	[Enabled] Disabled	This option corrects memory soft errors so that, over the length of the system runtime, the risk of producing multi-bit and uncorrectable errors is reduced.

Option	Parameter	Description
Node Interleaving	Enabled [Disabled]	Use this option to disable the NUMA architecture properties for the system. All operating system platforms support NUMA architectures. In most cases, optimum performance is obtained by disabling the Node Interleaving option. When this option is enabled, memory addresses are interleaved across the memory installed for each processor. Some workloads might experience improved performance when this option is enabled. Node Interleaving cannot be enabled when NVDIMMs are present in the system.
Memory Mirroring Mode	[Full Mirroring] Partial Mirror(Os Cinfigured) Partial Mirror(Memory below 4GB) Partial Mirror(10% above 4GB) Partial Mirror(20% above 4GB)	Use this option to select from the available Memory Mirroring modes. Full Mirror - reserves 50% of the total available memory for mirroring. Partial Mirror (20% above 4GB) - reserves 20% of the total available Memory above 4GB for Mirroring. Partial Mirror (10% above 4GB) - reserves 10% of the total available Memory above 4GB for Mirroring. Partial Mirror (Memory below 4GB) - depending on the memory configuration, sets up 2GB or 3GB of lower memory below 4GB for Mirroring. Partial Mirror (OS Configured) - sets up the system to configure Partial Mirroring at OS level.
Memory Remap	[No Action] All Memory	Use this option to remap memory that may have been previously disabled from the system due to a failure event, such as an uncorrectable memory error. The Remap All Memory Option causes the system to make all memory in the system available again on the next boot. The No Action option leaves any affected memory unavailable to the system.
Persistent Memory Options	_	Use this option to configure persistent memory when it is present in the system.

[ ]: Default setting

(a) Persistent Memory Options Menu

When you select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **System Options** > **Memory Operations** > **Persistent Memory Options** from the System Utilities, the **Persistent Memory Options** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
Persistent Memory Backup Power Policy	[Wait for Backup Power on Boot] Continue Boot without Backup Power	This option controls whether the system waits during system boot for batteries to charge if sufficient battery backup power for the installed persistent memory is not available. If this option is configured for 'Continue Boot without Backup Power', the server boots even if sufficient battery backup power is not installed. In this case, if sufficient battery backup power is not enabled, the configured memory will NOT be used by the operating system as persistent storage or as system memory.
Persistent Memory Integrity Check	[Enabled] Disabled	When this option is enabled, persistent memory will be checked during system boot to determine data integrity. Depending on the Persistent Memory Address Range Scrub setting, discovered errors during the data integrity check will either be presented to the operating system for recovery or cause the persistent memory to be mapped out and unavailable to the operating system. If this option is disabled, any persistent memory which has issues with the ability to read data or which has bad data may result in uncorrectable errors that result in a system crash.
Persistent Memory Address Range Scrub	[Enabled] Disabled	Use this option to configure the NVDIMM memory Address Range Scrub support. When enabled, this option allows a supported OS to attempt recovery from an uncorrectable memory error detected in the NVDIMM memory. When disabled, the NVDIMM memory will be disabled on the following boot after detecting an uncorrectable memory error in the NVDIMM. If the NVDIMM memory Memory Interleaving option is enabled, a disabled NVDIMM will include all the modules or regions within the set.
Scalable Persistent Memory Options	_	Use this option to configure persistent memory region allocation.

[ ]: Default setting

(4) Virtualization Options Menu

When you select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Virtualization Options** from the System Utilities, the **Virtualization Options** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
Intel(R) Virtualization Technology (Intel VT)	[Enabled] Disabled	When enabled, a hypervisor or operating system supporting this option can use hardware capabilities provided by Intel VT. Some hypervisors require that you enable Intel VT. You can leave this set to enabled even if you are not using a hypervisor or an operating system that uses this option.
Intel(R) VT-d	[Enabled] Disabled	If enabled, a hypervisor or operating system supporting this option can use hardware capabilities provided by Intel VT for Directed I/O. You can leave this set to enabled even if you are not using a hypervisor or an operating system that uses this option.
SR-IOV	[Enabled] Disabled	If enabled, SR-IOV support enables a hypervisor to create virtual instances of a PCI-express device, potentially increasing performance. If enabled, the BIOS allocates additional resources to PCI-express devices. You can leave this option set to enabled even if you are not using a hypervisor.

[ ]: Default setting

(5) Boot Options Menu

When you select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Boot Options** from the System Utilities, the **Boot Options** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
Boot Mode	[UEFI Mode] Legacy BIOS Mode	Use this option to select the boot mode of the system. Selecting UEFI Mode configures the system to boot Unified Extensible Firmware Interface (UEFI) compatible operating systems. Selecting Legacy BIOS Mode configures the system to boot traditional operating systems in Legacy BIOS compatibility mode. The operating system can only boot in the mode in which it is installed. The following options require booting in UEFI Mode: Secure Boot, IPv6 PXE Boot, boot > 2.2 TB Disks in AHCI SATA Mode, and Smart Array SW RAID.
UEFI Optimized Boot	[Enabled] Disabled	When enabled, the system BIOS boots using native UEFI graphics drivers. When disabled, the system BIOS boots using INT10 legacy video support. You cannot disable this option if Secure Boot is enabled. You can only configure this option if Boot Mode is configured to UEFI Mode. Set this option to enabled for compatibility with VMWare ESXi operating systems on a system configured for UEFI Mode.
Boot Order Policy	[Retry Boot Order Indefinitely] Attempt Boot Order Once Reset After Failed Boot Attempt	Use this option to configure how the system attempts to boot devices per the Boot Order list when no bootable device is found. If configured to 'Retry Boot Order Indefinitely,' the system continuously attempts to process the Boot Order list until a bootable device is found. If configured to 'Attempt Boot Order Once,' the system attempts to process all items in the Boot Order list once, and if unsuccessful, waits for user input to proceed. If configured for 'Reset After Failed Boot Attempt,' the system attempts to process all items in the Boot Order list once, and then reboots the system.
UEFI Boot Settings	–	Changes the UEFI boot option order. Enables or disables an individual UEFI boot option. Adds or deletes UEFI boot options.
Legacy BIOS Boot Order	–	Use this option to configure the Legacy BIOS Boot Order list. You can only configure this option if the Boot Mode is configured to Legacy BIOS Mode.

[ ]: Default setting

(a) UEFI Boot Settings Menu

When you select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Boot Options** > **UEFI Boot Settings** from the System Utilities, the **UEFI Boot Settings** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
UEFI Boot Order	-	Use this option to change the order of the UEFI Boot list. You can only configure this option if the Boot Mode is configured to UEFI Mode.
UEFI Boot Order Control	-	Enables or disables individual UEFI boot options. Enabled items are selected (checked). Disabled items remain in their location in the UEFI Boot Order, but are not attempted during the boot process.
Add Boot Option	-	Use this option to browse FAT16/FAT32 file systems that are available in the system, and to select X64 UEFI (.EFI) applications to add as a new UEFI Boot Option, such as an OS boot loader or other UEFI applications. The new boot option is added to the end of the UEFI Boot Order list.
Delete Boot Option	-	Use this setting to delete a UEFI Boot Option from the UEFI Boot Order list. If the option points to a standard boot location, such as a network PXE boot or a removable media device, the system BIOS adds the option on the next reboot.

How to change the boot order of bootable devices

1. Select the **UEFI Boot Order** menu. Then, move the cursor to the position of each device by using the < ↑ > and < ↓ > keys, and change the boot order using the <+> and <−> keys.

About the boot order of bootable devices

1. If two or more bootable devices are connected to this machine

   Boot the devices, beginning with the earliest boot order preset in **UEFI Boot Order**. If booting a device fails to boot, the device of the next order and the subsequent are booted in order.

   ・ Adding a bootable device

   When a new bootable device is connected to this machine, the added one is registered as the one with the largest boot order.

2. Removing a bootable device

   When a bootable device is removed from this machine, it is deleted from **UEFI Boot Order**.

Tips

- In the UEFI boot mode, the hard disk model number may be assigned to **UEFI Boot Order**.
- To make a change to the bootable devices, use the System Utilities rather than Windows bcdedit or Linux efibootmgr.

(b) Legacy BIOS Boot Order Menu

When you select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Boot Options** > **Legacy BIOS Boot Order** from the System Utilities, the **Legacy BIOS Boot Order** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
Standard Boot Order(IPL)	–	Use this option to configure the Legacy BIOS Boot Order list. You can only configure this option if the Boot Mode is configured to Legacy BIOS Mode.
Boot Controller Order	–	Use this option to configure the Legacy BIOS Boot Order list. You can only configure this option if the Boot Mode is configured to Legacy BIOS Mode.

(6) Network Options Menu

When you select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Network Options** from the System Utilities, the **Network Options** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
Network Boot Options	–	Use this option to configure network boot settings, such as enabling or disabling network boot for embedded NICs, setting the network boot retry support, or setting the PXE boot policy.
Pre-Boot Network Settings	–	Use this option to configure the preboot network settings such as the IPv4 address, the subnet mask, the gateway, and the primary and secondary DNS servers.
iSCSI Configuration	–	Select this option to display the iSCSI Configuration menu. Use this menu to configure the iSCSI Software Initiator settings to access remote targets. In UEFI boot mode, these targets will appear as bootable devices in the UEFI Boot Order. This option is available only if Network Boot Options > iSCSI Policy is set to Software Initiator.
VLAN Configuration	–	Use this option to set the Global VLAN UEFI configuration for all enabled network interfaces as defined in the IEEE 802.1Q standard. This setting applies to UEFI PXE boot, iSCSI Software Initiator Boot, and UEFI HTTP Boot. It also applies to all pre-boot network access from the UEFI Shell.

(a) Network Boot Option Menu

When you select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Network Options** > **Network Boot Options** from the System Utilities, the **Network Boot Options** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
Pre-Boot Network Environment	[Auto] IPv4 IPv6	Use this option to set the preference for Pre-Boot Network. If configured for Auto, all the network operations initiated in the pre boot environment occur over IPv4 or IPv6. The order of the existing network boot devices is not modified in the UEFI Boot Order list. New network boot devices are added to the end of the list using the default policy of the System BIOS. If configured for IPv4, all the network operations initiated in the pre boot environment only occur over IPv4. All existing IPv6 network boot devices are removed in the UEFI Boot Order. No new IPv6 network boot devices are added to the list. If configured for IPv6, all the network operations initiated in the pre boot environment only occur over IPv6. All existing IPv4 network boot devices in the UEFI Boot Order are removed. No new IPv4 network boot devices are added to the list.
IPv6 DHCP Unique Identifier	[Auto] DUID-LLT	Use this option to control the IPv6 DHCP Unique Identifier (DUID). If configured for Auto, the DUID is set using the Universal Unique Identifier (UUID) of the server, or using the DUID-LLT method if the server UUID is not available. If configured for DUID-LLT, the DUID is set based on the Link-layer Address Plus Time [DUID-LLT] method.
Network Boot Retry Support	[Enable] Disabled	Use this option to configure the Network Boot Retry Support. When enabled, the system BIOS attempts to boot the network device up to the number of times configured in the Network Boot Retry Count option before attempting to boot the next network device. This setting only takes effect when attempting to boot a network device from the F12 function key and one-time boot options.
Network Boot Retry Count	0-X [20]	Use this option to control the number of times the system BIOS attempts to boot a network device.

Option	Parameter	Description
HTTP Support	[Auto] HTTPS only HTTP only Disabled	Use this option to control the UEFI HTTP(s) boot support when in UEFI Mode, and the 'Discover Shell Auto-Start Script using DHCP' option under 'Embedded UEFI Shell' settings. When 'Auto' is selected, the system automatically adds HTTP(S) boot options to the UEFI Boot Order list for every network port that is enabled for Network Boot. Selecting this option enables the system to boot to the HTTP or HTTPS URLs provided by the DHCP server. Any other URLs provided by the DHCP server are ignored. When 'HTTP only' is selected, the system automatically adds HTTP boot options to the UEFI Boot Order list for every network port that is enabled for Network Boot. Selecting this option enables the system to boot to the HTTP URLs provided by the DHCP server, and to ignore any HTTPS or other URLs that are provided. When 'HTTPS only' is selected, the system automatically adds HTTPS boot options to the UEFI Boot Order list for every network port that is enabled for Network Boot. Selecting this option enables the system to boot to the HTTPS URLs provided by the DHCP server, and to ignore any HTTP or other URLs that are provided. To enable HTTPS boot either by selecting 'Auto' or 'HTTPS only', you must enroll the respective TLS certificate of the HTTPS server under Server Security > TLS (HTTPS) Options. Note: This setting only affects the HTTP boot options added for the network ports, and the Discover Shell Auto-Start Script provided by the DHCP server. Other settings, such as Boot from URL, are not affected by this setting.
iSCSI Policy	[Software Initiator] Adapter Initiator	Use this option to set the iSCSI Policy. If configured to Software Initiator, the iSCSI software initiator will be used to access iSCSI targets on any configured NIC ports. If configured to Adapter Initiator, the adapter specific iSCSI initiator will be used instead. The adapter firmware must be configured to access iSCSI targets from the adapter initiator.
Network Interface Cards (NICs) Example: Embedded LOM 1 Port 1	[Network Boot] Disabled	Use this option to enable or disable network boot (PXE, iSCSI, FCoE or UEFI HTTP) for the selected NIC. You might need to configure the NIC firmware for the boot option to be active.
Embedded LOM X Port X	Network Boot [Disabled]	Use this option to enable or disable network boot (PXE, iSCSI, FCoE or UEFI HTTP) for the selected NIC. You might need to configure the NIC firmware for the boot option to be active.
PCIe Slot Network Boot	-	Use this option to enable or disable network boot for NIC cards in PCIe Slots.

[ ]: Default setting

①. PCIe Slot Network Boot

When you select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Network Options** > **Network Boot Options** > **PCIe Slot Network Boot** from the System Utilities, the **PCIe Slot Network Boot** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
Slot 1 NIC Port 1 Boot	[Network Boot] Disabled	Use this option to enable or disable UEFI PXE Boot, UEFI HTTP Boot and iSCSI Software Initiator for the selected NIC. You might need to configure the NIC firmware for the boot option to be active.
Slot X NIC Port Y Boot	Network Boot [Disabled]	Use this option to enable or disable UEFI PXE Boot, UEFI HTTP Boot and iSCSI Software Initiator for the selected NIC. You might need to configure the NIC firmware for the boot option to be active.

[ ]: Default setting

(b) Pre-Boot Network Setting Menu

When you select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Network Options** > **Pre-Boot Network Setting** from the System Utilities, the **Pre-Boot Network Setting** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
Pre-Boot Network Interface	[Auto] SlotX PortY : Intel(R) Ethernet Controller	Use this option to select the network interface used for pre-boot network connections. When the selection is Auto, the system uses the first available port with a network connection.
Pre-boot Network Proxy	HTTP URL	Use this option to configure a pre-boot network proxy. When set, network operations for 'Pre-Boot Network Interface' are attempted through the configured proxy. The proxy must be in a HTTP URL format, and can be specified as http://IPv4_address:port, http://IPv6 address:port or http://FQDN:port.
DHCPv4	[Enabled] Disabled	When enabled, this option enables obtaining the pre-boot network IPv4 configuration from a DHCP server. Individual settings are not available. When disabled, you must configure static IP address settings individually.
IPv4 Address	IP Address	Use this option to specify the pre-boot network IPv4 address. Enter a static IP address using dotted-decimal notation (for example, 127.0.0.1). If DHCP is used (the DHCPv4 option is enabled), this setting is unavailable because the value is supplied automatically.
IPv4 Subnet Mask	IP Address	Use this option to specify the pre-boot network subnet mask. Enter a static IP address using dotted-decimal notation (for example, 255.255.255.0). If DHCP is used (the DHCPv4 option is enabled), this setting is unavailable because the value is supplied automatically.
IPv4 Gateway	IP Address	Use this option to specify the pre-boot network gateway IPv4 address. Enter a static IP address using dotted-decimal notation (for example, 127.0.0.1). If DHCP is used (the DHCPv4 option is enabled), this setting is unavailable because the value is supplied automatically.

Option	Parameter	Description
IPv4 Primary DNS	IP Address	Use this option to specify the pre-boot network Primary DNS Server IPv4 address. Enter a static IP address using dotted-decimal notation (for example, 127.0.0.1). If DHCP is used (the DHCPv4 option is enabled), this setting is unavailable because the value is supplied automatically.
IPv4 Secondary DNS	IP Address	Use this option to specify the pre-boot network Secondary DNS Server IPv4 address. Enter a static IP address using dotted-decimal notation (for example, 127.0.0.1). If DHCP is used (the DHCPv4 option is enabled), this setting is unavailable because the value is supplied automatically.
IPv6 Config Policy	[Automatic] Manual	When set to Automatic, this option enables obtaining the pre-boot network IPv6 configuration automatically. Individual settings are not available. When set to Manual, you must configure static IP address settings individually.
IPv6 Address	IP Address	Use this option to specify the pre-boot network IPv6 address. Enter a static IP address in the standard colon separated format (for example, 1234::1000). If IPv6 Config Policy is set to Automatic, this setting is unavailable because the value is supplied automatically.
IPv6 Gateway	IP Address	Use this option to specify the pre-boot network gateway IPv6 address. Enter a static IP address in the standard colon separated format (for example, 1234::1000). If IPv6 Config Policy is set to Automatic, this setting is unavailable because the value is supplied automatically.
IPv6 Primary DNS	IP Address	Use this option to specify the pre-boot network Primary DNS Server IPv6 address. Enter a static IP address in the standard colon separated format (for example, 1234::1000). If IPv6 Config Policy is set to Automatic, this setting is unavailable because the value is supplied automatically.
IPv6 Secondary DNS	IP Address	Use this option to specify the pre-boot network Secondary DNS Server IPv6 address. Enter a static IP address in the standard colon separated format (for example, 1234::1000). If IPv6 Config Policy is set to Automatic, this setting is unavailable because the value is supplied automatically.

Option	Parameter	Description
Boot from URL X	HTTP/HTTPS URL	Use this option to configure a network URL to a bootable ISO or EFI file. URLs in HTTP/HTTPS are accepted using either an IPv4 or IPv6 server address, or using a host name. For example, the URLs can be in any of the following formats: http://192.168.0.1/file/image.iso, http://example.com/file/image.efi, https://example.com/file/image.efi, http://[1234::1000]/image.iso. When configured, this URL is listed as a boot option in the UEFI boot menu. Selecting this boot option downloads the file to the system memory, and configures the system to attempt to boot from it. There is no specific ordering on this option. It can be independently ordered in the boot menu. This setting requires configuring the 'Pre-Boot Network Interface' option if you want to access the URL location through a specific network interface. When a HTTPS URL is configured, this setting requires enrolling the respective TLS certificate of the HTTPS server under Server Security > TLS (HTTPS) Options. This is only applicable in UEFI Mode. Note: Booting from an ISO file can involve only booting a preliminary OS environment image, such as WinPE or a mini Linux, or a complete OS install image if the OS supports the HTTP Boot feature (Old OS versions may not support this). Please check your OS documentation for the HTTP Boot feature support.

[ ]: Default setting

(c) iSCSI Configuration Menu

When you select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Network Options** > **iSCSI Boot Configuration** from the System Utilities, the **iSCSI Boot Configuration** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
iSCSI Initiator Name	String of 4 to 223 alphanumeric characters	The worldwide unique iSCSI Qualified Name (IQN) of the iSCSI initiator. Only IQN format is accepted. EUI format is not supported. For example: iqn.2001-04.com.example:uefi-13021088
Add an iSCSI Attempt	-	Add an iSCSI Attempt
Delete iSCSI Attempts	-	Deletes one or more iSCSI attempts.
iSCSI Attempts	-	-
AttemptX	-	-

[ ]: Default setting

①. Add an iSCSI Attempt Menu

When you select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Network Options** > **iSCSI Boot Configuration** > **Add an iSCSI Attempt** from the System Utilities, the **Add an iSCSI Attempt** menu appears.

This menu increases or decreases, depending on the installed status of the network interface card.

For details about the options, see the table below.

Option	Parameter	Description
(UEFI LAN Driver name) Example: SlotX PortY : Intel(R) Ethernet Controller	-	-

i. (UEFI LAN Driver) Menu

When you select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Network Options** > **iSCSI Boot Configuration** > **Add an iSCSI Attempt** > **(UEFI LAN Driver)** from the System Utilities, the **(UEFI LAN Driver)** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
iSCSI Attempt Name	[1]	A descriptive name for this iSCSI attempt configuration.
iSCSI Boot Control	[Disabled] Enabled Enabled for MPIO	Use this option to set the iSCSI mode for this attempt, or to enable the Multi-Path I/O (MPIO) capability.
IP Addrss Type	[IPv4] IPv6 Auto	Use this option to configure the iSCSI initiator IP address type (IPv4 or IPv6). In Auto mode, the iSCSI connection uses the IPv4 stack, and if the connection fails, is re-attempted using the IPv6 stack.
Connection Retry Count	0-16 [3]	The number of times to retry the iSCSI connection. Valid values are between 0 and 16. A value of 0 means no retries.
Connection Timeout	100-[20000]	The iSCSI connection timeout value in milliseconds. Valid values are between 100 milliseconds and 20 seconds (20000 milliseconds).(def:1000)
Initiator DHCP Config	(Check Box)	Enables or disables configuring the iSCSI initiator IP address from DHCP.(def:0)

Option	Parameter	Description
Initiator IP Address	IP Address	The IP address of the iSCSI initiator if not configured via DHCP. The Initiator IP Address is always auto-assigned if IP address type is IPv6. The address can be IPv4 or IPv6, depending on the IP address type.
Inisator Subnet Mask	IP Address	The subnet mask of the iSCSI initiator if not configured via DHCP. The address needs to be an IPv4 or IPv6 address, depending on the IP address type.
Initiator Gateway	IP Address	The gateway address of the iSCSI initiator if not configured via DHCP. The address needs to be an IPv4 or IPv6 address, depending on the IP address type.
Target DHCP Config	(Check Box)	Enables or disables configuring the iSCSI target settings from DHCP.(def:0)
Traget Name	String of 4 to 223 alphanumeric characters	The unique iSCSI Qualified Name (IQN) of the iSCSI target, if not configured via DHCP. Only IQN format is accepted. EUI format is not supported. For example: iqn.2015-02.com.hpe:iscsitarget-iscsidisk-target.
Target IP Address	IP Address	The IP Address of the iSCSI target, if not configured via DHCP. The address must be an IPv4 or IPv6 address, depending on the IP address type.
Target Port	1-65535 [3260]	The iSCSI target TCP port number, if not configured via DHCP. Valid port numbers range from 1-65535. Typical iSCSI port numbers include 860 or 3260. If no port number or any other number deemed invalid is specified, the value 3260 will be used.
Target Boot LUN	[0]	The iSCSI target Logical Unit Number (LUN), if not obtained from DHCP. This value must follow the SAM-2 spec. E.g. 0001-1234-5678-9ABC. If the number is less than 5 characters, a dash character is not required. E.g. 0001. If the lun number is 12345, input 1234-5.
Authentication Type	CHAP [None]	The iSCSI connection authentication method. This can be None for no security or CHAP for Challenge Handshake Authentication Protocol (CHAP).
CHAP Type	[One way] Mutual	The CHAP authentication type. When configured to One way, the target authenticates the initiator. When configured to Mutual, both the initiator and target authenticate each other. This is applicable only when the Authentication Method is set to CHAP.
CHAP Use Name	String of up to 126 characters	The user name for CHAP authentication from the initiator to the target. This is applicable only when the Authentication Method is set to CHAP.
CHAP Secret	String of 12 to 16 alphanumeric characters	The password needed for CHAP authentication. Must be between 12 and 16 characters long. This is applicable only when the Authentication Method is set to CHAP.
Mutual CHAP User Name	String of up to 126 characters	The user name for Mutual (reverse) CHAP authentication (from the target to the initiator). This is applicable only when the Authentication Method is set to CHAP and the CHAP Type is set to Mutual.

Option	Parameter	Description
Mutual CHAP Secret	String of 12 to 16 alphanumeric characters	The password needed for Mutual (reverse) CHAP authentication (from the target to the initiator).The password must be between 12 and 16 characters long. This is applicable only when the authentication type is set to CHAP and the CHAP Type is set to Mutual.

[ ]: Default setting

(d) VLAN Configuration Menu

When you select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Network Options** > **VLAN Configuration** from the System Utilities, the **VLAN Configuration** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
VLAN Control	Enabled [Disabled]	Use this option to enable or disable VLAN tagging on all enabled network interfaces.
VLAN ID	[0]-4094	Use this option to set the global VLAN ID for all enabled network interfaces. Valid values are 0 to 4094.A value of 0 sets the device to send untagged frames.
VLAN Priority	[0]-7	Use this option to set the priority for the VLAN tagged frames. Valid values are 0 to 7.

[ ]: Default setting

(7) Storage Options Menu

When you select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Storage Options** from the System Utilities, the **Storage Options** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
SATA Controller Options	–	Select this option to display SATA Controller options, such as selecting the Embedded SATA configuration.
Embedded Storage Boot Policy	–	Use this option to select the UEFI BIOS boot devices for embedded storage controllers. This option is only supported in UEFI Mode.
PCIe Slot Storage Boot Policy	–	Use this option to select the UEFI BIOS boot devices for storage controllers in PCIe slots. This option overrides the Fibre Channel/FCoE Scan Policy for Fibre channel controllers in PCIe slots. This option is only supported in UEFI Mode.
Fibre Channel/FCoE Scan Policy	Scan All Targets [Scan Configured Targets Only]	Use this option to change the default Fibre Channel or FCoE policy for scanning for boot devices. When configured for Scan All Targets, each installed FC/FCoE adapter scans all available targets. When configured for Scan Configured Targets Only, the FC/FCoE adapters only scan targets that are preconfigured in the devices settings. This option overrides any individual device settings configured in the device-specific setup.
NVM Express Options	–	Select this option to display Logical NVDIMM-N NVM Express Configuration Options.

[ ]: Default setting

(a) SATA Controller Options Menu

When you select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Storage Options** > **SATA Controller Options** from the System Utilities, the **SATA Controller Options** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
Embedded SATA Configuration	[Enable SATA AHCI Support] Smart Array SW RAID Support	Important: Smart Array SW RAID is not supported when Boot Mode is set to Legacy BIOS Mode. Use this option to configure the embedded chipset SATA controller. When selecting the Advanced Host Controller Interface (AHCI) or RAID (if supported), make sure the proper operating system drivers are used for proper operation.
SATA Secure Erase	Enabled [Disabled]	Use this option to control whether Secure Erase functionality is supported. When enabled, the Security Freeze Lock command is not sent to supported SATA hard drives, enabling Secure erase to function (the Secure Erase command is supported). This option is only supported when the SATA controller is in AHCI mode. Secure Erase only operates with hard drives that support the Secure Erase command.

[ ]: Default setting

(b) Embedded Storage Boot Policy Menu

When you select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Storage Options** > **Embedded Storage Boot Policy** from the System Utilities, the **Embedded Storage Boot Policy** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
(UEFI Driver Name)	Boot All Targets [Boot Limit to 24 Targets] Boot No Targets	If you select [Boot All Targets], all the enabled boot targets connected to the storage controller are available in the UEFI boot order list. If you select [Boot No Targets], the boot targets from the storage controller are not available in the UEFI boot order list. If you select [Boot Limit to 24 Targets], the 24 boot targets connected to the storage controller are available in the UEFI boot order list.

[ ]: Default setting

(c) PCIe Slot Storage Boot Policy Menu

When you select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Storage Options** > **PCIe Slot Storage Boot Policy** from the System Utilities, the **PCIe Slot Storage Boot Policy** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
PCI Slot X	Boot All Targets [Boot Limit to 24 Targets] Boot No Targets	If you select [Boot All Targets], all the enabled boot targets connected to the storage controller are available in the UEFI boot order list. If you select [Boot No Targets], the boot targets from the storage controller are not available in the UEFI boot order list. If you select [Boot Limit to 24 Targets], the 24 boot targets connected to the storage controller are available in the UEFI boot order list.

[ ]: Default setting

(d) NVM Express Options Menu

When you select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Storage Options** > **NVM Express Options** from the System Utilities, the **NVM Express Options** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
Embedded NVM Express Options ROM	[Enabled] Disabled	Use this option to enable or disable embedded NVM Express Option ROM. When enabled, the system loads the NVM Express Option ROM provided by the system BIOS. When disabled, the system loads the NVM Express Option ROM provided by the adapter.

[ ]: Default setting

(8) Power and Performance Options Menu

When you select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Power and Performance Options** from the System Utilities, the **Power and Performance Options** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
Power Regulator	[Dynamic Power Savings Mode] Static Low Power Mode Static High Performance Mode OS Control Mode	You can only configure this option if the Workload Profile is set to Custom. Use this option to configure the following Power Regulator support: - Dynamic Power Savings Mode: Automatically varies processor speed and power usage based on processor utilization. Enables the reduction of overall power consumption with little or no impact on performance. Does not require OS support. - Static Low Power Mode: Reduces processor speed and power usage. Guarantees a lower maximum power usage for the system. Performance impacts are greater for environments with higher processor utilization. - Static High Performance Mode: Processors run in their maximum power/performance state at all times, regardless of the OS power management policy. - OS Control Mode: Processors run in their maximum power/performance state at all times unless the OS enables a power management policy.
Minimum Processor Idle Power Core C-State	[C6 State] C1E State No C-states	You can only configure this option if Workload Profile is set to Custom. Use this option to select the lowest idle power state (C-state) of the processor that the operating system uses. The higher the C-state, the lower the power usage of that idle state. (C6 is the lowest power idle state supported by the processor).
Minimum Processor Idle Power Package C-State	[Package C6(retention) State] Package C6(non-retention) State No Package State	You can configure this option only if the Workload Profile is set to Custom. Use this option to select the lowest idle package power state (C-state) of the processor. The processor automatically transitions into package C-states based on the Core C-states in which cores on the processor have transitioned. The higher the package C-state, the lower the power usage of that idle package state. (Package C6 (retention) is the lowest power idle package state supported by the processor).
Intel(R) Turbo Boost Technology	Disabled [Enabled]	Turbo Boost Technology enables the processor to transition to a higher frequency than the processor's rated speed if the processor has available power and is within temperature specifications. Disabling this option reduces power usage, and also reduces the system's maximum achievable performance under some workloads. This appears only when the processor that supports this function is mounted. This option is displayed only when the installed processor supports this feature.

Option	Parameter	Description
Energy/Performance Bias	Maximum Performance [Balanced Performance] Balanced Power Power SavingMode	You can only configure this option if the Workload Profile is set to Custom. Use this option to configure several processor subsystems to optimize the performance and power usage of the processor. Balanced Performance provides optimum power efficiency, and is recommended for most environments. Maximum Performance Mode is recommended for environments that require the highest performance and lowest latency but are not sensitive to power consumption. Only use Power Savings Mode in environments that are power sensitive and can accept reduced performance.
Collaborative Power Control	[Enabled] Disabled	For operating systems that support the Processor Clocking Control (PCC) Interface, enabling this option enables the Operating System to request processor frequency changes even if the Power Regulator option on the server are configured for Dynamic Power Savings Mode. For Operating Systems that do not support the PCC Interface, or when the Power Regulator Mode is not configured for Dynamic Power Savings Mode, this option has no effect on system operation.
Intel DMI Link Frequency	[Auto] Gen 1 Speed Gen 2 Speed	Use this option to force the link speed between the processor and the southbridge to run at slower speeds to save power.
NUMA Group Size Optimization	[Flat] Clustered	Use this option to configure how the System BIOS reports the size of a NUMA node (number of logical processors), which assists the Operating System in grouping processors for application use (referred to as Kgroups). The default setting of Clustered provides better performance due to optimizing the resulting groups along NUMA boundaries. However, some applications might not be optimized to take advantage of processors spanning multiple groups. In such cases, selecting the Flat option might be necessary in order for those applications to utilize more logical processors.
Intel Performance Monitoring Support	[Disabled] Enabled	This option does not impact performance. When enabled, this option exposes certain chipset devices that can be used with the Intel Performance Monitoring Toolkit.
Uncore Frequency Scaling	[Auto] Maximum Minimum	This option controls the frequency scaling of the processor's internal busses (the uncore.) Setting this option to Auto enables the processor to dynamically change frequencies based on workload. Forcing to the maximum or minimum frequency enables tuning for latency or power consumption.
Sub- NUMA Clustering	Enabled [Disabled]	When enabled, Sub-NUMA Clustering divides the processor's cores, cache, and memory into multiple NUMA domains. Enabling this feature can increase performance for workloads that are NUMA aware and optimized. Note: When this option is enabled, up to 1GB of system memory may become unavailable.

Option	Parameter	Description
Energy Efficient Turbo	[Enabled] Disabled	This option controls whether the processor uses an energy efficiency based policy when engaging turbo range frequencies. This option is only applicable when Turbo Mode is enabled.
Local/Remote Threshold	[Auto] Low Medium High Disabled	Local/Remote Threshold setting.
LLC Dead Line Allocation (*1)	[Enabled] Disabled	When it is made effective, it may meet the dead line of LLC depending on the situation. When it is made disable, it will not meet the dead line of LLC.
Stale A to S (*1)	Enabled [Disabled]	It optimizes the directories from A to S which have become old.
Processor Prefetcher Options	-	Use this menu to set options such as HW Prefetcher, Adjacent Sector Prefetcher, DCU Stream Prefetcher, and DCU IP Prefetcher.
I/O Options	-	Use this menu to adjust ACPI SLIT Preferences, INTEL NIC DMA Channels, ACPI PXM Enablement, and I/O Non-Posted Prefetching.
Intel UPI Options	-	Select this option to display the Intel UPI Options menu. Use this menu to change settings for ACPI SLIT, Intel NIC DMA, Memory Proximity Reporting for I/O, and I/O Non-posted Prefetching.
Advanced Performance Tuning Options	-	Select this option to display the Advanced Performance Tuning Options menu.
Advanced Power Options	-	Select this option to display the Advanced Power Options menu. Use this menu to enable advanced power features, such as Channel Interleaving and Collaborative Power Control. You can also set the UPI Link Frequency to a lower speed and set the Processor Idle Power State.

[ ]: Default setting

*1: an option usable with System ROM Version 1.20 or later.

(a) Processor Prefetcher Options Menu

When you select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Power and Performance Options** > **Processor Prefetcher Options** from the System Utilities, the **Processor Prefetcher Options** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
HW Prefetcher	[Enabled] Disabled	Use this option to disable the processor HW prefetch feature. In some cases, setting this option to disabled can improve performance. Typically, setting this option to enabled provides better performance. Only disable this option after performing application benchmarking to verify improved performance in the environment.
Adjacent Sector Prefetch	[Enabled] Disabled	Use this option to disable the processor Adjacent Sector Prefetch feature. In some cases, setting this option to disabled can improve performance. Typically, setting this option to enabled provides better performance. Only disable this option after performing application benchmarking to verify improved performance in the environment.
DCU Stream Prefetcher	[Enabled] Disabled	Use this option to disable the processor DCU Stream Prefetcher feature. In some cases, setting this option to disabled can improve performance. Typically, setting this option to enabled provides better performance. Only disable this option after performing application benchmarking to verify improved performance in your environment.
DCU IP Prefetcher	[Enabled] Disabled	Use this option to disable the processor DCU IP Prefetcher feature. In some cases, setting this option to disabled can improve performance. In most cases, the default value of enabled provides optimal performance. Only disable this option after performing application benchmarking to verify improved performance in the environment.
LLC Prefetch	Enabled [Disabled]	Use this option to configure the processor Last Level Cache (LLC) prefetch feature. In some cases, setting this option to disabled can improve performance. Typically, setting this option to enabled provides better performance. Only disable this option after performing application benchmarking to verify improved performance in the environment.
XPT Prefetcher (*3)	[Auto] (*2) Enabled Disabled	"Enabled" setting of this option is not supported. Use this option with "Auto" or "Disabled" setting.

[ ]: Default setting

*2: this parameter has been added after System ROM Version 1.20.

*3: the factory out setting of this option was changed after System ROM Version 1.20.

(b) I/O Options Menu

When you select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Power and Performance Options** > **I/O Options** from the System Utilities, the **I/O Options** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
ACPI SLIT	[Enabled] Disabled	The ACPI SLIT (System Locality Information Table) defines the relative access times between processors, memory subsystems, and I/O subsystems. Operating systems that support the SLIT can use this information to improve performance by allocating resources and workloads more efficiently.
Intel NIC DMA Channels (IOAT)	[Enabled] Disabled	Use this option to select the Intel NIC DMA Channels support. This is a NIC acceleration option that only runs on Intel-based NICs.
Memory Proximity Reporting for I/O	[Enabled] Disabled	When enabled, the System BIOS reports the proximity relationship between I/O devices and system memory to the operating system. Most operating systems can use this information to efficiently assign memory resources for devices, such as network controllers and storage devices. Additionally, certain I/O devices might not be able to take advantage of I/O handling benefits if their OS drivers are not properly optimized to support this feature. See your operating system and I/O device documentation for more details.

[ ]: Default setting

(c) Intel UPI Options Menu

When you select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Power and Performance Options** > **Intel UPI Options** from the System Utilities, the **Intel UPI Options** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
Intel UPI Link Enablement	[Auto] Single Link Operation	Use this option to configure the UPI topology to use fewer links between processors, when available. Changing from the default can reduce UPI bandwidth performance in exchange for less power consumption.
Intel UPI Link Power Management	[Enable] Disable	Use this option to place the Quick Path Interconnect (UPI) links into a low power state when the links are not being used. This lowers power usage with minimal effect on performance. You can only configure this option if two or more CPUs are present and the Workload Profile is set to custom.
Intel UPI Link Frequency	[Auto] Min UPI Speed	Use this option to set the UPI Link frequency to a lower speed. Running at a lower frequency can reduce power consumption, but can also affect system performance. You can only configure this option if two or more CPUs are present and the Workload Profile is set to custom.
UPI Prefetcher	[Enable] Disable	Use this option to disable the processor UPI Prefetch feature. In some cases, setting this option to disabled can improve performance. Typically, setting this option to enabled provides better performance. Only disable this option after performing application benchmarking to verify improved performance in the environment. This option must be enabled when Sub-NUMA Clustering (SNC) is enabled.

[ ]: Default setting

(d) Advanced Performance Tuning Options Menu

When you select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Power and Performance Options** > **Advanced Performance Tuning Options** from the System Utilities, the **Advanced Performance Tuning Options** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
Processor Jitter Control	[Disabled] Auto-tuned Manual-tuned	Processor Jitter Control allows the customer to manage processor frequency variance to do technologies such as Turbo which vary the frequency based on power, thermals, and active cores. When configured for Auto-tuned, the platform will monitor frequency variance and automatically make adjustments to minimize variance over time. When configured for Manual-tuned, the customer can choose to attempt to operate the processor at a fixed frequency and can select lower or higher frequencies statically.
Processor Jitter Control Frequency	[0]-X	Processor Jitter Control Frequency allows the customer to stipulate the starting frequency in the Auto-tuned mode, or the desired frequency in the Manual-tuned mode. The input frequency is in units of Megahertz. System firmware will adjust the frequency to the nearest higher intermediate frequency supported by the processor if the input frequency is not supported.
Core Boosting*1	Enabled [Disabled]	This enables or disables the core boost technology that enhances the processor performance. This appears only when the processor that supports this function is mounted.

[ ]: Default setting

*1: this parameter has been added after System ROM Version 1.20.

(e) Advanced Power Options Menu

When you select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Power and Performance Options** > **Advanced Power Options** from the System Utilities, the **Advanced Power Options** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
Redundant Power Supply Mode	[Balanced Mode] High Efficiency Mode (Auto) High Efficiency Mode (Odd Supply Standard) High Efficiency Mode (Even Supply Standard)	Use this option to configure how the system handles redundant power supply configurations. Balanced Mode shares the power delivery equally between all installed power supplies. All High Efficiency Mode options provide the most power efficient operation with redundant power supplies by keeping half of the power supplies in standby mode at lower power usage levels. The High Efficiency Mode options enable the system to select which power supply to place in standby. Auto enables the system to select between the odd or even power supply based on a semi-random distribution within a group of systems.

[ ]: Default setting

(9) Embedded UEFI Shell Menu

When you select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Embedded UEFI Shell** from the System Utilities, the **Embedded UEFI Shell** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
Embedded UEFI Shell	[Enabled] Disabled	Use this option to enable or disable the Embedded UEFI Shell. When enabled, you can launch the Embedded UEFI Shell from the pre-boot environment. When enabled and the Boot Mode is configured for UEFI Mode, you can add the Embedded UEFI Shell to the UEFI Boot Order list by selecting the option entitled 'Add Embedded UEFI Shell to Boot Order'. When disabled, the Embedded UEFI Shell is not available in the pre-boot environment, and you cannot add it to the UEFI Boot Order list. The Embedded UEFI Shell is a pre-boot command line environment that you can use for scripting and running UEFI applications. It provides CLI-based commands to configure the server, update the System BIOS and other firmware, and obtain system information and error logs.
Add Embedded UEFI Shell to Boot Order	Enabled [Disabled]	When enabled, this option adds the Embedded UEFI Shell as an entry in the UEFI Boot Order list. This option is only available when the Boot Mode is configured to UEFI Mode and the Embedded UEFI Shell is enabled.
UEFI Shell Script Auto-Start	Enabled [Disabled]	Use this option to enable or disable automatic execution of the Embedded UEFI Shell startup script. You can store the script file on local media or access it from a network location. You must name the script file "startup.nsh" and place it on local media or a network location accessible to the server.
Shell Script Verification	Enabled [Disabled]	Enable this option to allow verification of UEFI shell script files when Secure Boot is enabled. For successful execution of script, make sure that UEFI shell scripts are enrolled in the Secure Boot database (db).
Shell Auto-Start Script Location	[Auto] File System on Attached Media Network Location	Use this option to select the location of the Embedded UEFI Shell startup script. For the 'File Systems on Attached Media' option, you must name the script file "startup.nsh" and place it on a UEFI accessible local file system, such as a FAT32 partition on a USB disk or HDD. For the 'Network Location' option, the file must end with a .nsh extension, and must be placed at an HTTP/HTTPS or FTP location accessible to the system. When you select the 'Auto' option, the system attempts to retrieve the startup script from the network location first, followed by locally attached media.

Option	Parameter	Description
Discover Shell Auto-Start Script using DHCP	Enabled [Disabled]	Use this option to let the Shell discover its startup script URL using DHCP. This option is available only if the 'HTTP Support' policy is not set to 'Disabled' and Auto-Start Script Location is set to 'Network Location', or 'Auto'. When set to 'Enabled', the Shell sends DHCP requests with the DHCP User Class option set to the string 'UEFIShell'. The DHCP server must be configured to provide HTTP/HTTPS or FTP URLs when this DHCP User Class string is present in the DHCP request. The User Class option is Option 77 when using DHCP over IPv4, and Option 15 when using DHCP over IPv6. URLs in HTTP/HTTPS must use either an IPv4 or IPv6 server address, or a host name. FTP formats are accepted using either an IPv4 server address or a host name. The URL provided by the DHCP server should match the 'HTTP Support' policy. When 'HTTP Support' policy is set to 'Auto', any HTTP/HTTPS or FTP URL provided by the DHCP server is used. When policy is set to 'HTTPS only', only HTTPS URLs are used, and other URLs are ignored. When policy is set to 'HTTP only', only HTTP or FTP URLs are used, and other URLs are ignored. When policy is set to 'Disabled', the Shell does not send any DHCP request.
Network Location for Shell Auto-Start Script	URL of HTTP or FTP server	Use this option to configure a network URL to a UEFI Shell startup script. This option is available and used only when the Auto-Start Script Location is set to 'Network Location', or 'Auto', and the Shell Auto-Start Script discovery using DHCP is set to 'Disabled'. URLs in HTTP/HTTPS are accepted using either an IPv4 or IPv6 server address, or using a host name. FTP formats are accepted using either an IPv4 server address or a host name. For example, the URLs can be in any of the following formats: http://192.168.0.1/file/file.nsh, http://example.com/file/file.nsh, https://example.com/file/file.nsh, http://[1234::1000]/file.nsh. The file must end with an .nsh extension. When configured, the Embedded UEFI Shell attempts to load and execute the startup script from the network location pointed to by this URL. When a HTTPS URL is configured, you must enroll the respective HTTPS server's TLS certificate under Server Security > TLS(HTTPS) Options.

[ ]: Default setting

(10) Server Security Menu

When you select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Server Security** from the System Utilities, the **Server Security** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
Set Power On Password	String of up to 31 alphanumeric characters	When the server powers on, a prompt is displayed to enter a password before continuing the boot process. In the event of an ASR reboot, the Power-On Password is bypassed, and the server boots normally.
Set Admin Password	String of up to 31 alphanumeric characters	Use this option to enter the administrator password to protect the server configuration. When this option is enabled, you are prompted for this password before being allowed to modify the configuration.
Secure Boot Settings	–	Select this option to display the Secure Boot Configuration menu. Use this menu to enable or disable Secure Boot Mode, and to add or remove certificates in the Secure Boot databases. Before configuring Secure Boot, ensure that you selected the UEFI Mode, and that the UEFI Optimized Boot option is enabled (under the Boot Mode menu).
TLS (HTTPS) Options	–	Select this option to display the TLS Certificate management and other options menu.
Trusted Platform Module Options	–	Select this option to enter the Trusted Platform Module Setup options.
Intel (R) TXT Support	Enabled [Disabled]	Use this option to modify Intel TXT support.
One-Time Boot Menu (F11 Prompt)	[Enabled] Disabled	Use this option to disable the POST One-Time Boot F11 Prompt.
EXPRESSBUILDER (F10 Prompt)	[Enabled] Disabled	Use this option to enable or disable the EXPRESSBUILDER functionality. When disabled, you are prevented from entering the EXPRESSBUILDER environment by pressing F10 during server boot. You must set this option to enabled to use EXPRESSBUILDER functionality.
Processor AES-NI Support	[Enabled] Disabled	Use this option to enable or disable the Advanced Encryption Standard Instruction Set (AES-NI) in the processor.
Backup ROM Image Authentication	Enabled [Disabled]	Use this option to enable cryptographic authentication of the backup ROM image on startup. When this option is disabled, only the primary image is authenticated on each startup. Enable this option to also perform cryptographic authentication of the backup ROM image.

[ ]: Default setting

Tips

- Do not set the password before OS installation.
- If you forget your password, perform the password initialization and set the password again according to the procedure in "Chapter 1 (7. Reset and Clear)".

(a) Secure Boot Settings Menu

When you select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Server Security** > **Secure Boot Settings** from the System Utilities, the **Secure Boot Settings** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
Current Secure Boot State	(Display only)	This option shows whether Secure Boot is currently enabled or disabled.
Attempt Secure Boot	Enabled [Disabled]	Enable/Disable the Secure Boot feature after platform reset.
Advance Secure Boot Options	–	Use this option to configure Advanced Secure Boot options, such as Platform Key (PK) Options, Key Exchange (KEK) Options, Allowed Signatures Database (DB), and Forbidden Signatures Database (DBX) Options.

[ ]: Default setting

Tips

- To enable **Secure Boot**, it is recommended that you set **Admin Password**.
- To make the option card recognizable as a bootable device when **Secure Boot** has been enabled, you need to have an option card UEFI driver that has been signed with the Microsoft key.

①. Advance Secure Boot Options Menu

When you select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Server Security** > **Secure Boot Settings** > **Advance Secure Boot Options** from the System Utilities, the **Secure Boot Settings** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
PK - Platform Key	–	Select this option to display the Platform Key (PK) Options menu. Use this menu to enroll or delete the PK certificate. The file must be in DER-encoded certificate format.
KEK - Key Exchange Key	–	Select this option to display the Key Exchange Key (KEK) Options menu. Use this menu to enroll, delete, view or export the KEK certificates. The file must be in DER-encoded certificate format.
DB - Allowed Signatures Database	–	Select this option to display the Allowed Signatures (DB) Options menu. Use this menu to enroll, delete, view or export the DB signatures.
DBX - Forbidden Signatures Database	–	Select this option to display the Forbidden Signatures (DBX) Options menu. Use this menu to enroll, delete, view or export the DBX signatures.
DBT - Timestamp Signatures Database	–	Select this option to display the Secure Boot Timestamps Signatures Database (DBT) Options menu. Use this menu to enroll, delete, view or export the DBT signatures.
Delete all keys	–	Deletes all the keys, i.e. PK, KEK, DB, and DBX.
Export all keys	–	Use this option to export all keys to files.
Reset all keys to platform defaults	–	Reinitializes all the keys to the platform defaults.

i. PK - Platform Key Menu

When you select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Server Security** > **Secure Boot Settings** > **Advance Secure Boot Options** > **PK - Platform Key** from the System Utilities, the **SPK - Platform Key** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
View PK Entry	-	Use this option to list and view Platform Key (PK) entry. The expiration date of the certificate is shown in Coordinated Universal Time (UTC).
Enroll PK	-	Use this option to enroll a new Platform Key (PK). Only one PK can exist in the system. If a PK already exists, you must delete it before you can enroll a new PK. A valid PK must be present for Secure Boot to be enabled.
Delete PK	-	Use this option to delete the Platform Key (PK). Doing so requires an immediate system reboot and disables Secure Boot until you enroll a new PK. Changing the default security certificate may cause this machine to fail to boot from some devices or cause it to fail to launch some software such as EXPRESSBUILDER. Use this option to download Active Health Log.
Export PK Entry	-	Use this option to export the PK certificate to a file on an attached media device. Supported formats include .der, .cer, and .crt.
Reset to platform defaults	-	Resets the PK key to the platform default.

ii. KEK - Key Exchange Key Menu

When you select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Server Security** > **Secure Boot Settings** > **Advance Secure Boot Options** > **KEK - Key Exchange Key** from the System Utilities, the **KEK - Key Exchange Key** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
View KEK Entry	-	Use this option to list and view Key Exchange Key (KEK) entries. The expiration date of the certificate is shown in Coordinated Universal Time (UTC).
Enroll KEK Entry	-	Use this option to enroll a new entry in the Key Exchange Key (KEK) security database.
Delete KEK Entry	-	Use this option to delete a new entry in the Key Exchange Key (KEK) security database.
Export KEK Entry	-	Use this option to export the KEK certificate to a file on an attached media device. Supported formats include .der, .cer, and .crt.
Reset to platform defaults	-	Restores the KEK settings to the default parameters.

Important **Changing the default security certificate from the Delete Key Entry option may cause the system to fail to boot from some devices or cause it to fail to launch some software such as EXPRESSBUILDER.**

ii-1. Enroll KEK Entry Menu

When you select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Server Security** > **Secure Boot Settings** > **Advance Secure Boot Options** > **KEK - Key Exchange Key** > **Enroll KEK Entry** from the System Utilities, the **Enroll KEK Entry** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
Enroll KEK using File	-	Use this option to read the KEK certificate from a file on an attached media device. Supported formats include .der, .cer, and .crt.
Signature Owner GUID (optional)	[Other] Hewlett Packard Enterprise Company Hewlett-Packard Company Microsoft Corporation SUSE Linux Products HmbH	Select the Signature Owner to use their Signature GUID in the Certificate.
Signature GUID (optional)	String of 32 digits (“0” to “9”) and alphabetic characters “A” to “F”	Enter the optional security certificate Signature GUID. You must enter the data in the following GUID format: 11111111-2222-3333-4444-1234567890ab. For Hewlett Packard Enterprise certificates, enter 1E910BE1-4BEB-6337-19F1-8A8AC107D512. For Hewlett-Packard certificates, enter F5A96B31-DBA0-4faa-A42A-7A0C9832768E. For Microsoft certificates, enter 77fa9abd-0359-4d32-bd60-28f4e78f784b. For SUSE certificates, enter 2879c886-57ee-45cc-b126-f92f24f906b9.
Commit changes and exit	-	Commit changes and exit.
Discard changes and exit	-	Discard changes and exit.

[ ]: Default setting

iii. DB - Allowed Signatures Database

When you select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Server Security** > **Secure Boot Settings** > **Advance Secure Boot Options** > **DB - Allowed Signatures Database** from the System Utilities, the **DB - Allowed Signatures Database** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
View Signatures	-	Shows the signature. The expiration date of the certificate is shown in Coordinated Universal Time (UTC).
Enroll Signatures	-	Enrolls the signature.
Delete Signature	-	Deletes the enrolled signature.
Export Signature	-	Use this option to export the signature to a file on an attached media device. Supported formats include .der, .cer, and .crt.
Reset to platform defaults	-	Restores the DB setting to the default.

iii-1. Enroll Signatures

When you select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Server Security** > **Secure Boot Settings** > **Advance Secure Boot Options** > DB - Allowed Signatures Database > **Enroll Signature** from the System Utilities, the **Enroll Signature** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
Enroll Signature using File	-	Enrolls the signature using a file.
Signature Owner GUID (optional)	[Other] Hewlett Packard Enterprise Company Hewlett-Packard Company Microsoft Corporation SUSE Linux Products HmbH	Select the Signature Owner to use their Signature GUID in the Certificate.
Signature GUID (optional)	String of 32 digits (“0” to “9”) and alphabetic characters “A” to “F”	Enter the optional security certificate Signature GUID. You must enter the data in the following GUID format: 11111111-2222-3333-4444-1234567890ab. For Hewlett Packard Enterprise certificates, enter 1E910BE1-4BEB-6337-19F1-8A8AC107D512. For Hewlett-Packard certificates, enter F5A96B31-DBA0-4faa-A42A-7A0C9832768E. For Microsoft certificates, enter 77fa9abd-0359-4d32-bd60-28f4e78f784b. For SUSE certificates, enter 2879c886-57ee-45cc-b126-f92f24f906b9.
Commit changes and exit	-	Commit changes and exit.
Discard changes and exit	-	Discard changes and exit.

[ ]: Default setting

iv. DBX - Forbidden Signatures Database

When you select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Server Security** > **Secure Boot Settings** > **Advance Secure Boot Options** > **DBX - Forbidden Signatures Database** from the System Utilities, the **DBX - Forbidden Signatures Database** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
View Signatures	-	Shows the hash value of the currently registered DBX.
Enroll Signatures	-	Adds a DBX.
Delete Signature	-	Deletes the enrolled signatures.
Export Signature	-	Use this option to export the signature to a file on an attached media device. Supported formats include .der, .cer, and .crt.
Reset to platform defaults	-	Resets the DBX key to the platform default.

iv-1.Enroll Signatures

When you select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Server Security** > **Secure Boot Settings** > **Advance Secure Boot Options** > **DBX - Forbidden Signature Database** > **Enroll Signature** from the System Utilities, the **Enroll Signature** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
Enroll Signature using File	-	Enrolls the signature using a file.
Signature Owner GUID (optional)	[Other] Hewlett Packard Enterprise Company Hewlett-Packard Company Microsoft Corporation SUSE Linux Products HmbH	Select the Signature Owner to use their Signature GUID in the Certificate.
Signature GUID (optional)	String of 32 digits (“0” to “9”) and alphabetic characters “A” to “F”	Enter the optional security certificate Signature GUID. You must enter the data in the following GUID format: 11111111-2222-3333-4444-1234567890ab. For Hewlett Packard Enterprise certificates, enter 1E910BE1-4BEB-6337-19F1-8A8AC107D512. For Hewlett-Packard certificates, enter F5A96B31-DBA0-4faa-A42A-7A0C9832768E. For Microsoft certificates, enter 77fa9abd-0359-4d32-bd60-28f4e78f784b. For SUSE certificates, enter 2879c886-57ee-45cc-b126-f92f24f906b9.
Signature Format	SHA256 SHA384 SHA512 [RAW]	Select the certicate format used to enroll certificate into database. Ensure correct signature format SHA256/SHA384/SHA512 is selected for the certificate with EFI_CERT_X509_SHA*_GUID signature type. For all other certificate types please select RAW signature format.
Commit changes and exit	-	Commit changes and exit.
Discard changes and exit	-	Discard changes and exit

[ ]: Default setting

v. DBT - Timestamp Signatures Database

When you select System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > Secure Boot Settings > Advance Secure Boot Options > DBT - Timestamp Signatures Database from the System Utilities, the DBT - Timestamp Signatures Database menu appears.

For details about the options, see the table below.

Option	Parameter	Description
Enroll Signatures	-	Enrolls the signature.
Delete Signature	-	Deletes the enrolled signature.

v-1. Enroll Signatures

When you select System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > Secure Boot Settings > Advance Secure Boot Options > DBT - Timestamp Signatures Database > Enroll Signature from the System Utilities, the Enroll Signature menu appears.

For details about the options, see the table below.

Option	Parameter	Description
Enrpll Signature using File	–	Enrolls the signature using a file.
Signature Owner GUID (optional)	[Other] Hewlett Packard Enterprise Company Hewlett-Packard Company Microsoft Corporation SUSE Linux Products HmbH	Select the Signature Owner to use their Signature GUID in the Certificate.
Signature GUID (optional)	String of 32 digits ("0" to "9") and alphabetic characters "A" to "F"	Enter the optional security certificate Signature GUID. You must enter the data in the following GUID format: 11111111-2222-3333-4444-1234567890ab. For Hewlett Packard Enterprise certificates, enter 1E910BE1-4BEB-6337-19F1-8A8AC107D512. For Hewlett-Packard certificates, enter F5A96B31-DBA0-4faa-A42A-7A0C9832768E. For Microsoft certificates, enter 77fa9abd-0359-4d32-bd60-28f4e78f784b. For SUSE certificates, enter 2879c886-57ee-45cc-b126-f92f24f906b9.
Commit changes and exit	–	Commit changes and exit.
Discard changes and exit	–	Discard changes and exit

[ ]: Default setting

(b) TLS (HTTPS) Options Menu

When you select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Server Security** > **TLS (HTTPS) Options** from the System Utilities, the **TLS (HTTPS) Options** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
View Certificates	–	Use this option to list and view enrolled TLS certificates.
Enroll Certificate	–	Use this option to enroll a new TLS certificate.
Delete Certificate	–	Use this option to delete one or more TLS certificates.
Export Certificate	–	Use this option to export TLS certificate to a file on an attached media device. Supported formats are .der, .pem.
Advanced Secure Settings	–	Use this option to configure Advanced TLS Security Settings, such as Cipher suites allowed for TLS connections, Certificate validation settings.
Delete all Certificates	–	Deletes all the TLS certificates from the platform.
Export all Certificates	–	Saves the certificates enrolled in DER or PEM format to the external media.
Reset all settings to platform defaults	–	Removes all the certificates from the platform and restores all the Advanced TLS Security settings to the platform defaults.

①. Advanced Secure Settings Menu

When you select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Server Security** > **TLS (HTTPS) Options** > **Advanced Security Settings** from the System Utilities, the **TLS (HTTPS) Options** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
Cipher suites allowed for TLS connections	-	Use this option to select the Cipher suites that are allowed for TLS connections.
Certificate validation for every TLS connection	[PEER] NONE	Use this option to select the validation process of the certificate. It is recommended to validate the certificate presented by the Peer for secure communication. Select option 'PEER' for verification or 'NONE' to skip this process.
Strict Hostname chacking	[Disabled] Enabled	Use this option to enable or disable verification of the connected server's hostname with the hostname in the certificate supplied by the server.
TLS Protocol Version Support	[AUTO] 1.0 1.1 1.2	Use this option to specify which TLS protocol version to use for TLS connections. AUTO will negotiate the highest version supported by both TLS server and the client.

[ ]: Default setting

(c) Trusted Platform Module options Menu

When you select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Server Security** > **Trusted Platform Module Options** from the System Utilities, the **Trusted Platform Module Options** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
Current TPM Type	(Display only)	Current TPM device type.
Current TPM State	(Display only)	Current TPM device state: Not Present; Present and Disabled; Present and Enabled.
Current TPM 2.0 Active PCRs	(Display only)	Current TPM 2.0 Active PCRs: SHA1, SHA256 or SHA1_SHA256 Appears only when TPM is installed.
Current TPM 2.0 Software Interface Status	(Display only)	Current TPM 2.0 Software Interface Status: FIFO or CRB. Appears only when TPM is installed.
TPM 2.0 Operation	[No Action] Clear	Use this option to perform a clear operation on the TPM. Clearing the TPM can prevent the server from booting to a TPM-aware operating system if the operating system uses TPM's measurements. TPM 2.0 is only supported in UEFI Mode. Selectable only when TPM is installed.
TPM Mode Switch Operation	[No Action] TPM 1.2 TPM 2.0	Use this option to switch the TPM chip to TPM 1.2/2.0, FIPS mode or non-FIPS mode. Selectable only when TPM is installed.
TPM 2.0 Software Interface Operation	[No Action] FIFO interface CRB interface	TPM 2.0 Software Interface Operation: FIFO or CRB. Selectable only when TPM is installed.
TPM Visibility	Hidden [Visible]	Use this option to hide the TPM from the operating system. When the TPM is hidden, BIOS secure startup is disabled, and the TPM does not respond to any commands. Intended use is for removing the TPM option from the system without removing the actual hardware. Selectable only when TPM is installed.
TPM UEFI Option ROM Measuurement	[Enabled] Disabled	Use this option to enable measuring the UEFI PCI option ROMs. Disabling this option skips measuring the UEFI PCI option ROMs. Selectable only when TPM is installed.

[ ]: Default setting

(11) PCIe Device Configuration Menu

When you select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **PCI Device Configuration** from the System Utilities, the **PCI Device Configuration** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
Advanced PCIe Configuration	–	Select this option to display the Advanced PCIe options menu.
(DriverName)	–	Select this option to enable or disable PCI devices.

[ ]: Default setting

(a) Advanced PCIe Configuration Menu

When you select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **PCIe Device Configuration** > **Advanced PCIe Configuration** from the System Utilities, the **Advanced PCIe Configuration** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
NVMe PCIe Resource Padding	[Normal] Medium High	Use this option to configure PCIe resources to support PCIe hot-add for NVMe drives. When Normal is selected, PCIe resources are only allocated to devices installed at boot time, and PCIe hot-add is not supported. When Medium is selected, additional PCIe resources are allocated for each PCIe Root Port, which might enable a PCIe hot-add event to work without requiring a system reboot to enumerate the device. When High is selected, a maximum amount of PCIe resources are set aside to allow for the best chance of supporting a PCIe hot-add event.
Maximum PCI Express Speed	[Per Port Control] PCIe Generation 1.0	You can only configure this option if the Workload Profile is set to Custom. If a PCI Express device does not run properly at its optimal speed, lowering the speed at which the device is running can address this issue. This option enables you to lower the maximum PCI Express speed at which the server allows PCI Express devices to operate. You can also use it to address issues with problematic PCI Express devices. Setting this value to Maximum Supported configures the platform to run at the maximum speed supported by the platform or the PCIe device, whichever is lower.

[ ]: Default setting

(b) （Driver Name) Menu

The number of options displayed in this menu increases or decreases, depending on whether or not a PCIe device is installed.

①. Embedded LOM Driver

When you select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **PCIe Device Configuration** > **Embedded LOM Driver** from the System Utilities, the **Embedded LOM Driver** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
PCIe Device Disable	[Auto] Disabled	Select this option to enable or disable PCI devices.
PCIe Link Speed	[Auto] PCIe Generation 1.0	Use this option to configure the PCIe Link Speed for the selected device. When configured for Auto, the selected device trains at the maximum supported speed of the PCIe link. When configured for PCIe Generation, the selected device trains at a maximum of PCIe Generation 1 linkspeed.
PCIe Option ROM	[Enabled] Disabled	Use this option to enable or disable Device Option ROM.

[ ]: Default setting

②. Embedded SATA Controller

When you select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **PCIe Device Configuration** > **Embedded SATA Controller** from the System Utilities, the **Embedded SATA Controller** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
SATA Device Disable	[Auto] Disabled	Select this option to enable or disable SATA devices.
SATA Power Management(SALP)	[Enabled] Disabled	Use this option to enable or disable Aggressive Link Power Management (SALP).
PCIe Option ROM	[Enabled] Disabled	Use this option to enable or disable Device Option ROM.

[ ]: Default setting

(12) Advanced Options Menu

When you select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Advanced Options** from the System Utilities, the **Advanced Options** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
ROM Selection	[Use Current ROM] Switch to Backup ROM	Use this option to revert the server to a previous BIOS ROM image. The backup image is the BIOS ROM image that was used prior to the last flash event.
Embedded Video Connection	[Auto] Always Disabled Always Enabled	When configured for Auto mode, the external video connection to the embedded video controller is automatically disabled to save power when a monitor is not attached. It is automatically enabled when a monitor is attached, including when the server is operating. When configured for Always Disabled, the external video connection to the embedded video controller is disabled, and a monitor connected to this port does not display except during system boot. This can be used for security reasons. When configured for Always Enabled, the external video connection to the embedded video controller is always enabled. This option is only required if a monitor is attached with a monitor detection that does not function properly (making AUTO mode not work properly). Note: This option does not affect Integrated Remote Console video. Also, if you press F9 or F11 during system boot, the configured video connector behavior is overridden, and the video console remains enabled. This lets you reconfigure the Embedded Video Connection option even if the video is disabled.
Consistent Device Naming	[CDN Support for LOMs and Slots] CDN Suppot LOMs Only Disabled	Use this option to select the level of Consistent Device Naming. On supported operating systems, NIC ports are named based on their location in the system. CDN Support for LOMs Only names Embedded NICs and FlexibleLOMs. Existing NIC connections retain their names until reinstalled under the OS environment.
Mixed Power Suppy Reporting	[Enabled] Disabled	When enabled, the server logs a message that a mixed power supply configuration is present. When disabled, the server no longer logs messages that a mixed power supply configuration is present.
High Precision Event Timer (HPET) ACPI Support	[Enabled] Disabled	Use this option to disable the High Precision Event Timer (HPET) table and device object in ACPI. When disabled, the HPET is not available to an operating system that supports the HPET through the industry standard ACPI name space.
Fan and Thermal Options	–	Use this option to display the Fan and Thermal Options menu. Use this menu to configure advanced fan and thermal options, such as Thermal Configuration, Thermal Shutdown, and Thermal and Fan Policies.
Advanced Service Options	–	Select this option to display the Advanced Service Options menu. Use this menu to enter a chassis serial number and Part Number Leave all the options under this one unchanged unless otherwise specified. If you want to change them, contact the dealer or maintenance service company.
Advanced Debug Options	–	Select this option to display the Debug Options menu. Use this menu to enable or disable the advanced debug options UEFI serial debug level and POST Verbose Boot Progress. Leave all the options under this one unchanged unless otherwise specified. If you want to change them, contact the dealer or maintenance service company.
Advanced Security Options	–	Select this option to display the Advanced Security Options menu.

[ ]: Default setting

(a) Fan and Thermal Options Menu

When you select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Advanced Options** > **Fan and Thermal Options** from the System Utilities, the **Fan and Thermal Options** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
Thermal Configuration	[Optimal Cooling] Increased Cooling Maximum Cooling	Use this option to select the fan cooling solution for the system. Optimal Cooling provides the most efficient solution by configuring fan speeds to the minimum required speed to provide adequate cooling. Increased Cooling runs fans at higher speeds to provide additional cooling. Select Increased Cooling when third-party storage controllers are cabled to the embedded hard drive cage, or if the system is experiencing thermal issues that cannot be resolved. Maximum cooling provides the maximum cooling available on this platform.
Thermal Shutdown	[Enabled] Disabled	Use this option to control the reaction of the system to caution level thermal events. When disabled, the System Management Firmware ignores thermal events, and the system immediately powers off in data-destructive situations.
Fan Installation Requirements	[Enable Messaging] Disable Messaging	With this function, you can set the correspondence method of the system when the fan required for the system configuration is removed. When configured for Enable Messaging, the server displays messages and log events to the Integrated Management Log (IML) when required fans are not installed. The server can still boot and operate. When configured for Disable Messaging, the server does not display messages and log events when required fans are not installed. Not all information will be notified. It is recommended that you leave Fan Installation Requirements in the default state of Enable Messaging. Operating without the required fans can result in damage to hardware components.
Fan Failuer Policy	[Shutdown/Halt on Critical Fan Failures] Allow Operation with Critical Fan Failures	With this function, the correspondence method of the system can be set when a fan failure occurs. If "Shutdown/Halt on Critical Fan Failures" is set, the system will be shut down when the fan configuration required for the system is no longer available. If "Allow Operation with Critical Fan Failures" is set, the system can continue operation without the fan configuration required for the system.
Extended Ambient Temperature Support	[Disabled] Enabled for 40c Ambient(ASHRAE 3) Enabled for 45c Ambient(ASHRAE 4)	Use this option to enable the server to operate at higher ambient temperatures than normally supported. These options are only supported with specific hardware configurations. See your server documentation before configuring the server to enable extended ambient temperature support. Improper system operation or damage to hardware components can result from enabling these options in unsupported configurations. Selecting Enabled for 40c Ambient (ASHRAE 3) enables the server to operate in environments with ambient temperatures up to 40 degrees Celsius. Selecting Enabled for 45c Ambient (ASHRAE 4) enables the server to operate in environments with ambient temperatures up to 45 degrees Celsius. Not all servers support both 40c Ambient (ASHRAE 3) and 45c Ambient (ASHRAE 4).

[ ]: Default setting

Tips

- "Fan Failure Policy" is factory set to "Allow Operation with Critical Fan Failures."
- If NEC ESMPRO ServerAgentService is installed, set "Thermal Shutdown" to "Disabled" because shutdown at high temperature is executed by NEC ESMPRO ServerAgentService.

(b) Advanced Service Options Menu

When you select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Advanced Options** > **Advanced Service Options** from the System Utilities, the **Advanced Service Options** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
Serial Number	String of up to 16 alphanumeric characters	Use this option to set the system serial number. This value must always match the serial number sticker located on the chassis. Leave all the options unchanged unless otherwise specified.
Product ID	String of up to 16 alphanumeric characters	Use this option to set the system Part Number. This value must always match the Part Number sticker located on the chassis. Leave all the options unchanged unless otherwise specified.

[ ]: Default setting

(c) Advanced Debug Options Menu

When you select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Advanced Options** > **Advanced Debug Options** from the System Utilities, the **Advanced Debug Options** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
UEFI Serial Debug Message Level	[Disabled] Errors Only Medium Network Verbose Custom	Use this option to enable the UEFI Serial Debug output and verbosity level. Selecting Verbose can impact server boot time significantly. This option is only applicable in UEFI Mode.
POST Verbose Boot Progress	[Disabled] Serial Only All	Use this option to enable verbose boot progress messaging. Because this option displays additional debug information to the screen and serial console, it might be helpful for determining why a server became unresponsive during the boot process.

[ ]: Default setting

(d) Advanced Security Options Menu

When you select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Advanced Options** > **Advanced Security Options** from the System Utilities, the **Advanced Security Options** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
TPM FIPS Mode Switch	[No Action] Regular mode FIPS mode	Use this option to switch the TPM chip to FIPS mode, regular mode.

[ ]: Default setting

(13) Date and Time Menu

When you select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Date and Time** from the System Utilities, the **Date and Time** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
Date (mm-dd-yyyy)	[mm/dd/yyyy]	Enter the date in the month/day/year (mm/dd/yyyy) format. Use 1-12 for entering months, 1-31 for entering days, and 1900-9999 for entering years.
Time (hh:mm:ss)	[hh:mm:ss]	Enter the time in hh:mm:ss format. Use the 24-hour format for entering hours: 15:00 for 3 PM. Use 0-59 for entering minutes and seconds.
Time Zone	UTC-12:00, International Date Line West … UTC+09:00, Osaka Sapporo, Tokyo, Seoul, Yakutsk … UTC+14:00, Line Islands Unspecified Time Zone	This option displays the current time zone setting for the system.
Daylight Savings Time	Enabled [Disabled]	This option controls the Daylight Savings Time (DST) adjustment to the displayed local time. If this option is disabled, the displayed local time will not be adjusted for DST. If this option is enabled, the displayed local time will be advanced by one hour.
Time Format	[Coordinated Universal Time (UTC)] Local Time	This option controls how the system time is stored in the hardware Real Time Clock (RTC). When configured to 'Coordinated Universal Time (UTC)' (default) the local time is calculated from the associated time zone value. When configured to 'Local Time' the time is stored directly as local time and the time zone option does not have meaning. Setting this option to 'Local Time' works around an issue when using Microsoft Windows operating systems in Legacy Boot Mode where the time is set incorrectly.

[ ]: Default setting

Tips

Check that the time, date, and time zone are correct.

Check the system clock about once every month. If you want to operate it with high accuracy, it is recommended that you use a time server (NTP server) or the like.
If the system clock significantly delays or advances over time even after you adjust it, contact your dealer or maintenance service company.
If you are using Windows, set **Time Format** to **Local Time**.

(14) System Default Options Menu

When you select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **System Default Options** from the System Utilities, the **System Default Options** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
Restore Default System Settings	[No, cancel the restore procedure.] Yes, restore the defult settings.	When "Yes, restore the default settings" is selected, the setting in the "BIOS / Platform Configuration (RBSU)" menu is reset to the default value. However, if the user default is enabled with "User Default Options", it will be reset to the user default value. Rebooting the system is required to reset the setting. In addition, the following settings are not reset to default values. ・ Settings under "Secure Boot Settings" menu ・ Settings under "Data and Time" menu except "Time Format" ・ Settings of "ROM Selection" option
Restore Default Manufacturing Settings	[No, cancel restore procedure.] Yes, restore the default settings.	If you select "Yes, restore the default settings.", the settings in the "BIOS / Platform Configuration (RBSU)" menu will be reset to their default values. However, if the user default is enabled with "User Default Options", it will be reset to the user default value. Rebooting the system is required to reset the setting. In addition, the following settings are not reset to default values. ・ Settings under "Data and Time" menu except "Time Format" ・ Settings of "ROM Selection" option If this option is selected, security settings such as the key database for secure boot will also be erased. If you do not want to reset to the user default value, delete the user default in "User Default Options > Erase User Defaults", then select "Yes, restore the default settings." for this option.
Default UEFI Device Priority	–	Use this option to change the UEFI device priority when system or manufacturing defaults are restored. The initial UEFI Boot Order list is created based on the priority defined in this setting. This setting only applies when user custom defaults are set.
User Default Options	–	Use this option to define default configuration settings. When the default configuration settings are loaded, the saved default settings are used instead of the factory defaults. Configure the system as necessary, and then enable this option to save the configuration as the default configuration.

[ ]: Default setting

Note

User default values are set at shipment for each model. Please reset the user default according to the environment to use refering the *Chapter 3 (2.4 setting required case)* in the *User's Guide* and the setting list of each additional optional parts.

(15) User Default Options Menu

When you select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **User Default Options** from the System Utilities, the **User Default Options** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
Save User Defaults	[No, Cancel] Yes, Save	If you select "Yes, Save", you can save the settings in the current "BIOS / Platform Configuration (RBSU)" menu as user defaults. User defaults are saved when you exit System Utility by pressing the <F12> key. However, settings under the "Secure Boot Settings" menu are not saved.
Erase User Defaults	[No, Cancel] Yes, erase the current settings.	When "Yes, erase the current settings." is selected, the saved user default is erased. Rebooting of the system is required for erasing.
User Defaults	(Display only)	Displays whether user default settings are enabled or disabled.

[ ]: Default setting

1.2.3 BMC Configuration Utility

When you select **System Configuration** > **BMC Configuration Utility** from the System Utilities, the **BMC Configuration Utility** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
Network Options	−	Select to enter the Network Options.
Advanced Network Options	−	Select to enter the Advanced Network Options.
User Management	−	Manage BMC user account.
Setting Options	−	Manage BMC Option Setting.
Set to factory defaults	[No] Yes	BMC configuration will be set to the factory default. BMC will be reset and this configuration utility will not be available until next system reboot.
Reset BMC	[No] Yes	BMC will be reset and this configuration utility will not be available until next system reboot. BMC remote console will be disconnected and BMC IP address may be changed after reset.
About	−	Display BMC information.

[ ]: Default setting

(1) Network Options Menu

When you select **System Configuration** > **BMC Configuration Utility** > **Network Options** from the System Utilities, the **Network Options** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
MAC Address	(Display only)	Shows the MAC address of the selected BMC network interface.
Network Interface Adapter	[ON] OFF Shared Network Port - LOM Shared Network Port - FlexibleLOM	Selects the BMC network interface.
Transciver Speed Autoselect	[ON] OFF	Enables or disables automatic selection of the transmission speed.
DHCP Enable	[ON] OFF	Enables or disables the DHCP server.
DNS Name	String of up to 50 alphanumeric characters	Sets the BMC DNS name.
IP Address	IP Address	Sets the BMC IP address.
Subnet Mask	IP Address	Sets the BMC subnetwork mask.
Gateway IP Address	IP Address	Sets the BMC gateway IP address.

[ ]: Default setting

(2) Advanced Network Options Menu

When you select **System Configuration** > **BMC Configuration Utility** > **Advanced Network Options** from the System Utilities, the **Advanced Network Options** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
Gateway from DHCP	[Enabled] Disabled	Enables or disables the BMC to use the gateway from DHCP.
Gateway #1	IP Address	Sets the Gateway #1 IP address.
Gateway #2	IP Address	Sets the Gateway #2 IP address.
Gateway #3	IP Address	Sets the Gateway #3 IP address.
DHCP Routes	[Enabled] Disabled	Enables or disables use of the route provided by DHCP.
Route 1	IP Address	Sets the Route 1 IP address.
Route 2	IP Address	Sets the Route 2 IP address.
Route 3	IP Address	Sets the Route 3 IP address.
DNS from DHCP	[Enabled] Disabled	Enables or disables use of WINS from DHCP.
DNS Server 1	IP Address	Sets the DNS Server 1 IP address.
DNS Server 2	IP Address	Sets the DNS Server 2 IP address.
DNS Server 3	IP Address	Sets the DNS Server 3 IP address.
WINS from DHCP	[Enabled] Disabled	Enables or disables use of WINS from DHCP.
Register with WINS Server	[Enabled] Disabled	Enables or disables registration in the WINS server.
WINS Server #1	IP Address	Sets the WINS Server #1 IP address.
WINS Server #2	IP Address	Sets the WINS Server #2 IP address.
Domain Name	Character string	Sets the BMC domain name.

[ ]: Default setting

(3) User Management Menu

When you select **System Configuration** > **BMC Configuration Utility** > **User Management** from the System Utilities, the **User Management** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
Add User	−	Adds a user.
Edit/Remove User	−	Edits or deletes a user.

(a) Add User Menu

When you select **System Configuration** > **BMC Configuration Utility** > **User Management** > **Add User** from the System Utilities, the **Add User** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
New User BMC Privileges	-	-
Administer User Accounts	[YES] NO	Enables or disables user account administration.
Remote Console Access	[YES] NO	Enables or disables use of remote console access.
Virtual Power and Reset	[YES] NO	Enables or disables the virtual power and reset.
Virtual Media	[YES] NO	Enables or disables the virtual media.
Configure Settings	[YES] NO	Enables or disables configuration of the settings.
Host BIOS	[YES] NO	The host BIOS settings can be configured using System Utility.
Host NIC	[YES] NO	The host NIC settings can be configured.
Host Storage	[YES] NO	The host storage settings can be configured.
New User Information	-	-
New User Name	String of up to 39 characters	Sets a new user name.
Login Name	String of up to 39 characters	Sets the login name.
Password	String of up to 39 characters	Sets the password.

[ ]: Default setting

(b) Edit/Remove User Menu

When you select **System Configuration** > **BMC Configuration Utility** > **Edit/Remove User** from the System Utilities, the **Edit/Remove User** menu appears.

For details about the options, see the table below.

When you select "Edit" from "Action", the items after "Loginname" are displayed.

Option	Parameter	Description
1. User Name	String of up to 39 characters	Sets a user name.
Action	[No Change] Delete Edit	Selects whether the user information is modified or deleted.
Loginname	String of up to 39 characters	Sets the login name.
Password	String of up to 39 characters	Sets the password.
Administrater User Accounts	[YES] NO	Enables or disables user account administration.
Remote Console Access	[YES] NO	Enables or disables remote console access.
Virtual Power and Reset	[YES] NO	Enables or disables the virtual power and reset.
Virtual Media	[YES] NO	Enables or disables the virtual media.
Configure Setting	[YES] NO	Enables or disables configuration of the settings.
Host BIOS	[YES] NO	The host BIOS settings can be configured using System Utility.
Host NIC	[YES] NO	The host NIC settings can be configured.
Host Storage	[YES] NO	The host storage settings can be configured.

[ ]: Default setting

(4) Setting Options Menu

When you select **System Configuration** > **BMC Configuration Utility** > **Setting Options** from the System Utilities, the **Setting Options** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
BMC Functionality	[Enabled] Disabled	You can enable or disable BMC functionality.
BMC Configuration Utility	[Enabled] Disabled	When BMC Configuration Utility is disabled, BMC Configuration Utility will not be part of the System Configuration Utility.
Require user login and configuration privilege for BMC Configuration	[Disabled] Enabled	This setting determines whether a user-credential prompt is displayed when a user accesses BMC configuration utility.
Show BMC IP Address during POST	[Enabled] Disabled	Show BMC IP Address during POST.
Local Users	[Enabled] Disabled	Enables or disables local users.
Serial CLI Status	[Enabled-Authenticarion Required] Enabled-No Authentication required Disabled	Sets the serial CLI status.
Serial CLI Speed(bits/second)	[9600] 19200 57600 115200	Sets the serial CLI speed (bits/s).
BMC Web Interface	[Enabled] Disabled	

[ ]: Default setting

(5) About Menu

When you select **System Configuration** > **BMC Configuration Utility** > **About** from the System Utilities, the **About** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
Firmware Date	(Display only)	Shows the date of firmware revision.
Firmware Version	(Display only)	Shows the firmware version.
Hardware Version	(Display only)	Shows the software version.
BMC CPLD Version	(Display only)	Shows the CPLD version.
Host CPLD Version	(Display only)	Shows the host CPLD version.
PCI BUS	(Display only)	Shows the PCI BUS to which the processor is connected.
Device	(Display only)	Shows the device number assigned to the BMC within the PCI bus.

1.2.4 Embedded Device Information

(1) (Embedded RAID) Menu

When you select **System Configuration** > **(Embedded RAID)** from the SystemManager, the **(Embedded RAID)** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
Controller Information	–	Provides the information of the controller like PCI Bus :Device:Function, Firmware Revision, UEFI Driver Version, Controller Temperature etc.
Enable/Disable Smart array Debug Messages	(Check Box)	Select or deselect the check box to enable or disable the Smart array debug message.
Configure Controller Settings	–	Configures the supported controller settings, advanced controller settings(if applicable) and clear the controller's current configuration.
Array Configuration	–	Creates new array(s) from the list of drives available and manages the existing arrays.
Disk Utilities	–	Displays the list of drives that are connected to the controller and allows the user to perform certain operations on the disks available.
Exit and launch Smart Storage Administrator(SSA)	–	Launch the Smart Storage Administrator (SSA) to configure RAID levels.

(2) (Embedded LOM) Menu

When you select **System Configuration** > **(Embedded LOM)** from the SystemManager, the **(Embedded LOM)** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
Firmware Image Menu	–	Firmware image information.
Disable HP Shared Memory features	Disabled [Enabled]	Disable usage of reserved memory regions to allow direct assignment of device to guest virtual machines.
Blink LEDs	[0]-X	Blink LEDs for a duration up to 15 seconds.(def:0)
Pre-boot Wake On LAN	Disabled [Enabled]	Configure Pre-boot Wake on LAN (WOL).
Chip Type	(Display only)	Shows the type and revision number of the chip.
PCI Device ID	(Display only)	Shows the PCI device ID.
Bus:Device:Function	(Display only)	Shows the "PCI_bus_number:device_ number:function_number" of this device.
Link Status	(Display only)	Shows the link status.
Permanent MAC Address	(Display only)	Shows the fixed MAC address.
Vitual MAC Address	(Display only)	Shows the virtual MAC address.

[ ]: Default setting

1.2.5 One-Time Boot

When you select **One-Time Boot** from the System Utilities or press the <F11> key on the POST screen, the **One-Time Boot** menu appears.

You can select the UEFI boot device using the **One-Time Boot** menu.

Selecting this option does not change any predefined Boot Order settings.

The options are as below.

Option	Parameter	Description
OS boot manager such as Windows Boot Manager	–	Boots the installed OS.
Generic USB Boot	–	Boots from the installed USB boot device. Provides the placeholder of the USB device bootable with UEFI. By setting the boot order of this option, you can retain the boot order when using the USB device that may be installed in the future.
Embedded LOM	–	Boots from the boot device connected to Embedded LOM.
Embedded UEFI Shell	–	Boots from Embedded UEFI Shell.
Embedded SATA Port	–	Boots from the boot device connected to Embedded SATA Port.
Run the UEFI application from the file system	–	Selects the UEFI applications that run from the file system. Shows all the FAT file systems available in the system.
Legacy BIOS One-Time Boot Menu	–	Launches **Legacy BIOS One-Time Boot Menu**.

1.2.6 Embedded Applications

When you select **Embedded Applications** from the System Utilities, the **Embedded Applications** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
Embedded UEFI Shell	–	Exits the System Utilities and launches the built-in UEFI shell. which is used to script and run UEFI applications, such the UEFI boot loader, in the preboot command line environment.
Intergrated Management Log (IML)	–	Displays [Integrated Management Log (IML)]. IML shows the log of the events that occurred on this machine. IML entries help diagnose problems or identify potential problems.
Active Health System Log	–	The Active Health System monitors and records changes in the server hardware and system configuration. The Active Health System assists in diagnosing problems and delivering rapid resolution when system failures occur.
Firmware Update	–	Select this option to update firmware components on your system.
Embedded Diagnostics	–	This device does not support it.
EXPRESSBUILDER	–	Use this option to enable or disable the EXPRESSBUILDER functionality. When disabled, you are prevented from entering the EXPRESSBUILDER environment by pressing F10 during server boot. You must set this option to enabled to use EXPRESSBUILDER functionality.

1.2.7 System Information

When you select **System Information** from the System Utilities, the **System Information** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
Summary	–	Displays a summary of System Information.
Processor Information	–	Displays detailed information about the CPU(s) on the system.
Memory Information	–	Displays detailed information about the memory on the system.
PCI Device Information	–	Displays detailed information about the PCI Devices found in the system.
Firmware Information	–	Displays detailed information about the firmware images reported by the devices in the system.
Export System Information to file	–	Exports the System Information to a file.

(1) Summary Menu

When you select **System Information** > **Summary** from the System Utilities, the **Summary** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
System Name	(Display only)	Displays the system name and generation.
Serial Number	(Display only)	Displays the system serial number.
Product ID	(Display only)	Displays the Part Number.
System ROM	(Display only)	Displays the System ROM version and date.
Redundant System ROM	(Display only)	Displays the Redundant System ROM version and date.
Power Management Controller FW Virsion	(Display only)	Shows the firmware version of the power management controller.
User Defaults	(Display only)	Displays whether user default settings are enabled.
Boot Mode	(Display only)	Displays the Boot Mode setting.
Total Installed System Memory	(Display only)	Displays the total memory installed in the system.
Total Available System Memory	(Display only)	Displays the amount of configured system memory available for use in the system.
Processor 1	(Display only)	Displays processor information.
Processor 2	(Display only)	Displays processor information.
iLO Firmware Version	(Display only)	Shows the iLO firmware version.
iLO IPv4 address	(Display only)	Shows the iLO IPv4 address.
iLO IPv6 address	(Display only)	Shows the iLO IPv6 address.
Network Devices	(Display only)	–
Embedded LOM x Port x	(Display only)	Shows the MAC address of the selected network device.

(2) Processor Information Menu

When you select **System Information** > **Processor Information** from the System Utilities, the **Processor Information** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
CPU	(Display only)	The CPU number as enumerated by BIOS.
Socket	(Display only)	The CPU socket as enumerated by BIOS.
Socket Locator	(Display only)	The CPU socket as labeled on the system board.
Populated	(Display only)	Whether the CPU socket is populated with a CPU package.
Manufacturer Description	(Display only)	A brief description of the CPU written by the CPU manufacturer. This string is retrieved from the CPU itself.
Characteristics	(Display only)	Functions that the processor supports.
Core Count	(Display only)	The number of physical cores found in the CPU package.
Enabled Core Count	(Display only)	The number of physical cores that are enabled in the CPU package.
Thread Count	(Display only)	The number of logical cores found in the CPU package.
Rated Speed	(Display only)	The nominal speed rating of the processor as defined by the manufacturer.
External Clock	(Display only)	The external clock speed of the processor as defined by the manufacturer.
Voltage	(Display only)	The nominal supply voltage of the processor as defined by the manufacturer.
Microcode Patches	–	A list of microcode patches that have been released from the processor manufacturer and are being installed by BIOS.
ID	(Display only)	Shows the processor microcode ID.
Date	(Display only)	Shows the release date of this microcode patch.
CPUID	(Display only)	Shows the CPUID associated to this microcode patch.
L1 Cahce	–	Detailed information about the L1 cache for this processor.
Maximum Size	(Display only)	The total amount of cache found in the socket for this cache level.
Installed Size	(Display only)	The actual amount of cache installed for this cache level.
Speed	(Display only)	The rated speed of this cache device as defined by the manufacturer.
Associativity	(Display only)	The technique used to map this cache device to main memory.
ECC Type	(Display only)	The error correction technique used by this cache device.
Policy	(Display only)	The technique used to maintain data coherency for this cache device.
Supported SRAM Type	(Display only)	The type of SRAM technology that this cache device supports.
Current SRAM Type	(Display only)	The type of SRAM technology that this cache device is configured to use.
Type	(Display only)	The type of data that is being cached by this cache device.
L2 Cahce	–	Detailed information about the L2 cache for this processor.
Maximum Size	(Display only)	The total amount of cache found in the socket for this cache level.
Installed Size	(Display only)	The actual amount of cache installed for this cache level.
Speed	(Display only)	The rated speed of this cache device as defined by the manufacturer.
Associativity	(Display only)	The technique used to map this cache device to main memory.
ECC Type	(Display only)	The error correction technique used by this cache device.
Policy	(Display only)	The technique used to maintain data coherency for this cache device.
Supported SRAM Type	(Display only)	The type of SRAM technology that this cache device supports.

Option	Parameter	Description
Current SRAM Type	(Display only)	The type of SRAM technology that this cache device is configured to use.
Type	(Display only)	The type of data that is being cached by this cache device.
L3 Cahce	–	Detailed information about the L3 cache for this processor.
Maximum Size	(Display only)	The total amount of cache found in the socket for this cache level.
Installed Size	(Display only)	The actual amount of cache installed for this cache level.
Speed	(Display only)	The rated speed of this cache device as defined by the manufacturer.
Associativity	(Display only)	The technique used to map this cache device to main memory.
ECC Type	(Display only)	The error correction technique used by this cache device.
Policy	(Display only)	The technique used to maintain data coherency for this cache device.
Supported SRAM Type	(Display only)	The type of SRAM technology that this cache device supports.
Current SRAM Type	(Display only)	The type of SRAM technology that this cache device is configured to use.
Type	(Display only)	The type of data that is being cached by this cache device.

(3) Memory Information Menu

When you select **System Information** > **Memory Information** from the System Utilities, the **Memory Information** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
Total System Memory	(Display only)	Shows the total amount of the detected system memory.
Total Memory Slots	(Display only)	Shows the total number of physical memory slots within this system.
Operating Frequency	(Display only)	The effective frequency of all the memory modules within the system in operation is determined from the bus rate, module rate, and others.
Operating Voltage	(Display only)	Shows the supply voltage of all the memory modules within the system.
Location	(Display only)	Shows the physical CPU package to which all the following memory modules are directly connected.
Total Memory	(Display only)	Shows the total amount of the system memory that is directly connected to this CPU package.
Number of Slot	(Display only)	Shows the total number of physical memory slots that are directly connected to this CPU package.
Installed Modules	(Display only)	Shows the number of memory modules that are directly connected to this CPU package.
Socket Locator	(Display only)	Shows the memory module socket labeled on the system board.
Status	(Display only)	Shows the currently known status of this memory module or socket.
Size	(Display only)	Shows the total amount of memory within this memory module.
Manufacturer	(Display only)	Shows the vendor of this memory module.
Memory Type	(Display only)	Shows the memory type used by the memory module.
Part Number	(Display only)	Shows the serial number of the memory module.
Type	(Display only)	Shows the type of this memory module. Example: DIMM, DDR
Technology	(Display only)	Shows the industry standard technology used by this memory module.
Maximum Supported Frequency	(Display only)	Shows the maximum effective frequency of this memory module.
Minimum Supported Voltage	(Display only)	Shows the minimum supply voltage supported by this memory module.
Maximum Supported Voltage	(Display only)	Shows the maximum supply voltage supported by this memory module.
Configured Voltage	(Display only)	Shows the supply voltage of this memory module although it is currently set.
Ranks	(Display only)	Shows the number of ranks on this memory module.
Data Width	(Display only)	Shows the data width (bits) supported by this memory module.
Total Width	(Display only)	Shows the total width (bits) supported by this memory module. This value can include other overhead such as error correction.
Error Correction	(Display only)	Shows the error correction technique used in this memory module.

(4) PCI Device Information Menu

When you select **System Information** > **System Information** > **PCI Device Information** from the System Utilities, the **PCI Device Information** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
Location	(Display only)	Shows the physical position (of this PCI device) within the system.
Slot Description	(Display only)	Shows details of this PCI slot.
UEFI Device Path	(Display only)	Shows that logical path to the device that was determined by the UEFI BIOS firmware.
UEFI Structured Name	(Display only)	Shows that logical name of the device that was determined by the UEFI BIOS firmware.
Popufated	(Display only)	Specifies but shows whether a device is installed to this PCI slot.
Enabled	(Display only)	Specifies whether this PCI slot is enabled.
Device Name	(Display only)	Shows the device name.
Device Type	(Display only)	Shows the device type.
PCI Address	(Display only)	Shows the logical address of the PCI device within the PCI topology of the system.
PCI Vendor ID	(Display only)	Shows the hexadecimal number that signifies the 16-bit device vendor ID.
PCI Device ID	(Display only)	Shows the 16-bit device ID assigned with a hexadecimal number.
PCI Sub Vendor ID	(Display only)	Shows the 16-bit ID (hexadecimal number) with which the original design of the device may have been changed.
PCI Sub Device ID	(Display only)	Shows the PCI sub device ID (hexadecimal number).
PCI Class Code	(Display only)	Shows the general type of this PCI device. For details, see "Use of PCI".
PCI Sub Class Code	(Display only)	Shows a specific type of this PCI device. For details, see "Use of PCI".
Firmware	(Display only)	Shows the version of the firmware reported by the device. Note that it reports that the device has multiple firmware revisions.

(5) Firmware Information Menu

When you select **System Information** > **System Information** > **Firmware Information** from the System Utilities, the **Firmware Information** menu appears.

The number of options displayed increases or decreases, depending on whether or not a PCIe device is installed.

OptionFor details about the options, see the table below.

Option	Parameter	Description
System ROM	(Display only)	Shows the device name and firmware version reported by the device.
Redundant System ROM	(Display only)	Shows the device name and firmware version reported by the device.
Power Management Controller Firmware	(Display only)	Shows the device name and firmware version reported by the device.
Power Management Controller Firmware Bootloader	(Display only)	Shows the device name and firmware version reported by the device.
System Programmable Logic Device	(Display only)	Shows the device name and firmware version reported by the device.
Server PItform Services (SPS) Firmware	(Display only)	Shows the device name and firmware version reported by the device.
Intelligent Patform Abstraction Data	(Display only)	Shows the device name and firmware version reported by the device.
EXPRESSBUILDER	(Display only)	Shows the device name and firmware version reported by the device.
ME SPI Descriptor	(Display only)	Shows the device name and firmware version reported by the device.
Innovation Engine(IE) Firmware	(Display only)	Shows the device name and firmware version reported by the device.
(DeviceName)	(Display only)	Shows the device name and firmware version reported by the device.
BMC Firmware Version	(Display only)	Shows the BMC firmware version.

1.2.8 System Health

When you select **System Health** from the System Utilities, the **System Health** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
View System Health	–	Displays the **View System Health** menu. Use this option to display the health status of all the devices within the system.
Download Active Health System Log	–	Active Health System monitors and records changes in server hardware and system configuration. It assists in diagnosing the problem and solving it quickly when a system failure occurs.

(1) View System Health Menu

When you select **System Health** > **View System Health** from the System Utilities, the **View System Health** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
[Healthy] System BIOS	–	Shows the system status detected by the system BIOS.
[Healthy] BMC embedded health Device	–	Shows the BMC status.
[Healhy] (Device name) Example: SlotX PortY : Intel(R) Ethernet Controller	–	Shows the status of the selected device. The number of options displayed increases or decreases, depending on whether or not a PCIe device is installed.

(2) Download Active Health System Log Menu

When you select **System Health** > **Download Active Health System Log** from the System Utilities, the **Download Active Health System Log** menu appears.

For details about the options, see the table below.

Option	Parameter	Description
Available Download Period	(Display only)	Shows the download period of the Active Health System Log available on the system.
Download Entire Log	–	Downloads all available Active Health System log entries.
Range Start Date	–	Select a start range for the Active Health System log in days.
Range End Date	–	Select an end range for the Active Health System log in days.
Select File Location	–	Create an Active Health System Log file. This requires a writable file system of FAT16 or FAT32 partitions on local or virtual media.
Add Customer Infrmation (Optional)	(Check Box)	Please help us provide better service by providing the following contact details (Optional). Note: Contact information is not saved, but only appended to the downloaded log file.
Support Case Number	–	Adds support case number in AHS log file.
Contact Name	–	Adds contact name in AHS log file.
Phone Number	–	Adds customer phone number in AHS log file.
Email	–	Adds customer email in AHS log file.
Company Name	–	Adds customer company name in AHS log file.
Start Download	–	Starts the AHS Log download process.

2. RAID System Configuration

Use HPE Smart Array S100i Software RAID Configuration Utility to configure RAID, such as creating virtual drives and make a hot spare. Refer to following sections for detail of its operation. You can also configure RAID by Smart Storage Administrator. Refer to a document for detail that *Smart Storage Administrator User's Guide* which is uploaded on the following ftp site.

http://www.nec.com/express/

2.1 Start HPE Smart Array S100i Utility

Use the System Utilities to start the HPE Smart Array S100i Utility.

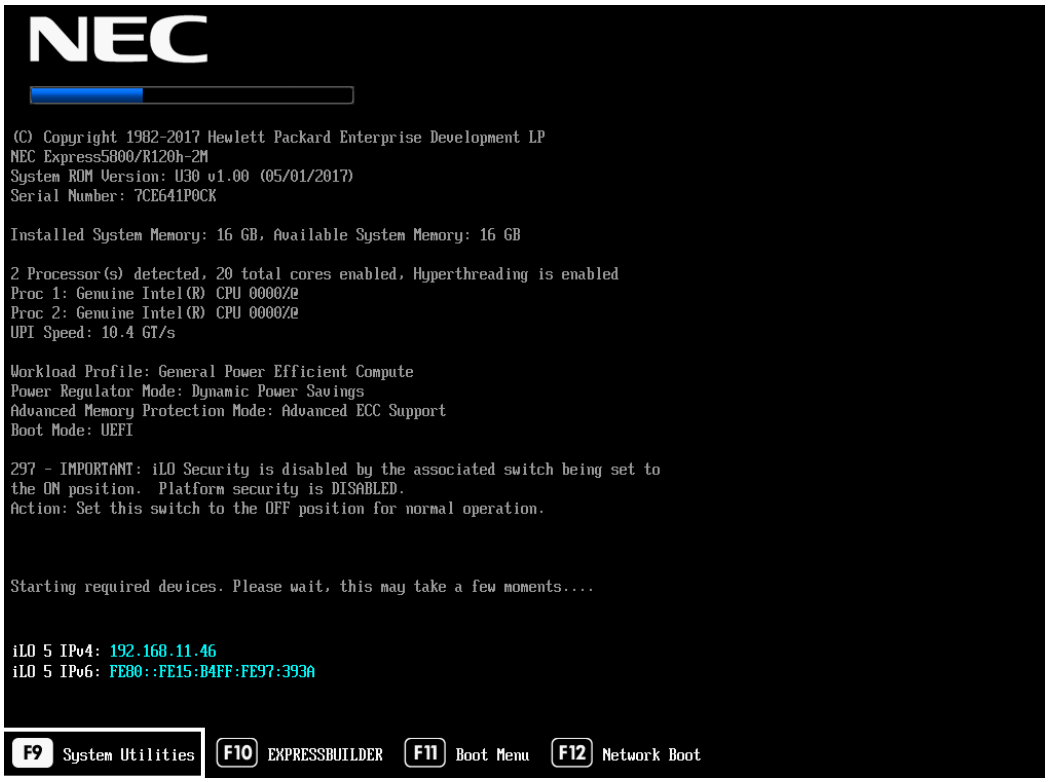
Step1

Turn on the server and wait for POST to proceed.

After a while, the following message appears at the bottom left of the screen.

F9 System Utilities

If you press the < F9> key, SETUP starts upon completion of POST and the System Utilities menu is displayed.

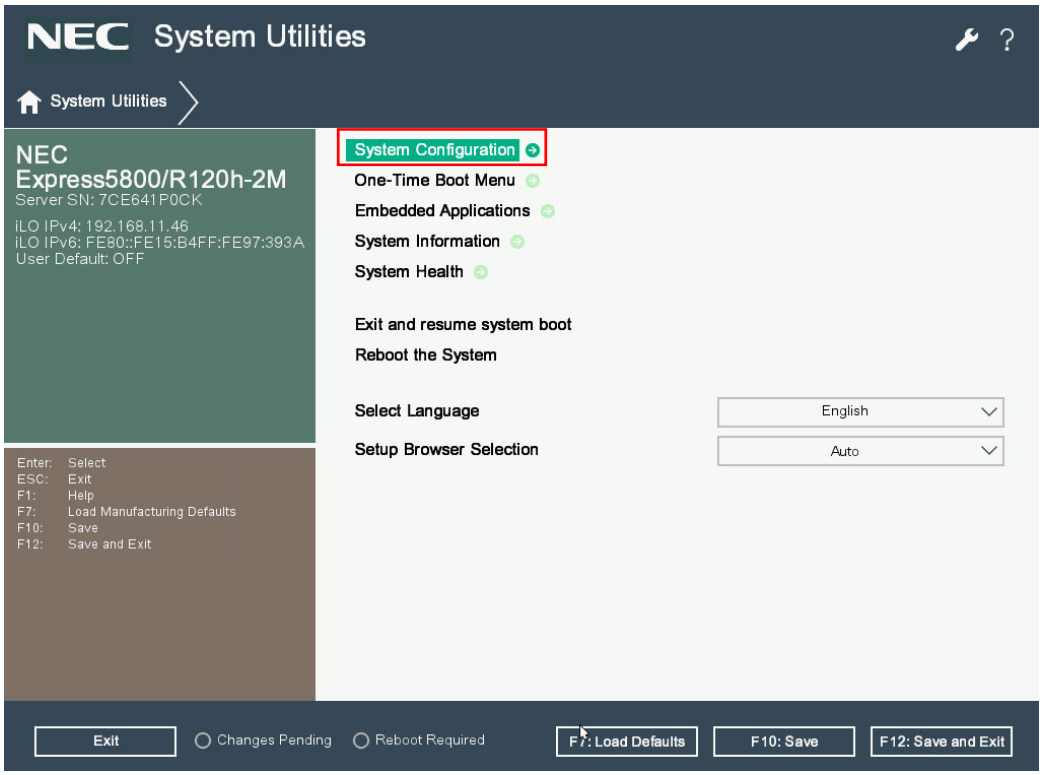


Tips

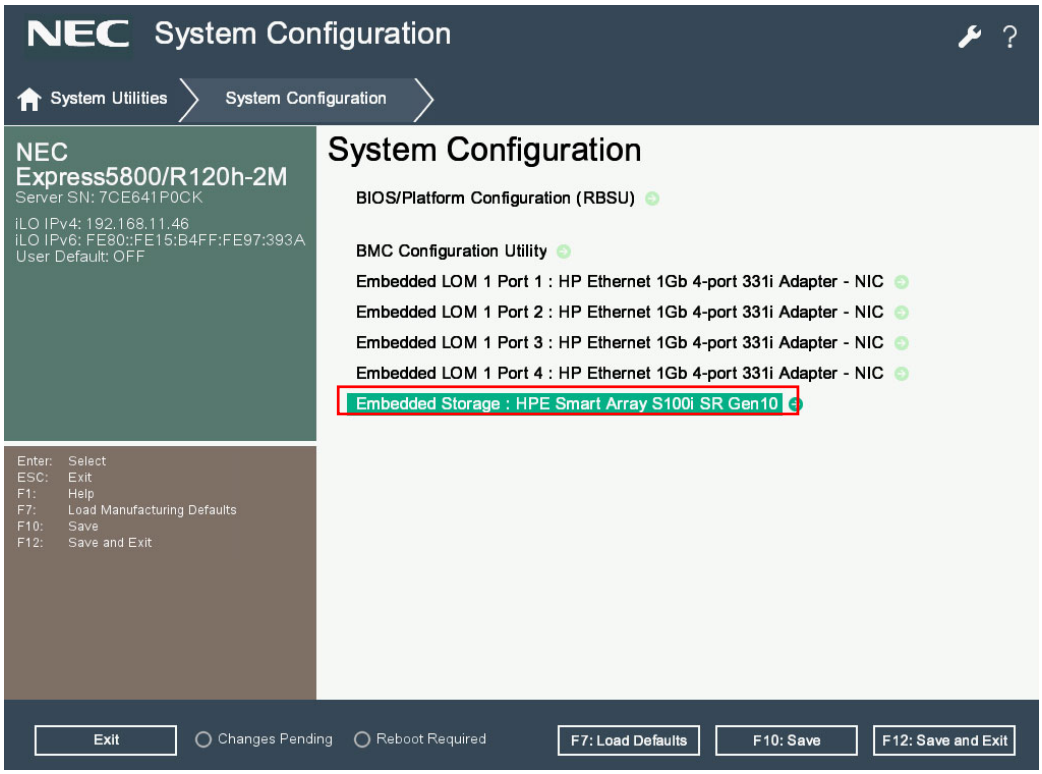
Please note that the white color background of F9 means the function is selected, if it's not turn to white color after you pressed the button, wait for a moment of system initialization.

Step2

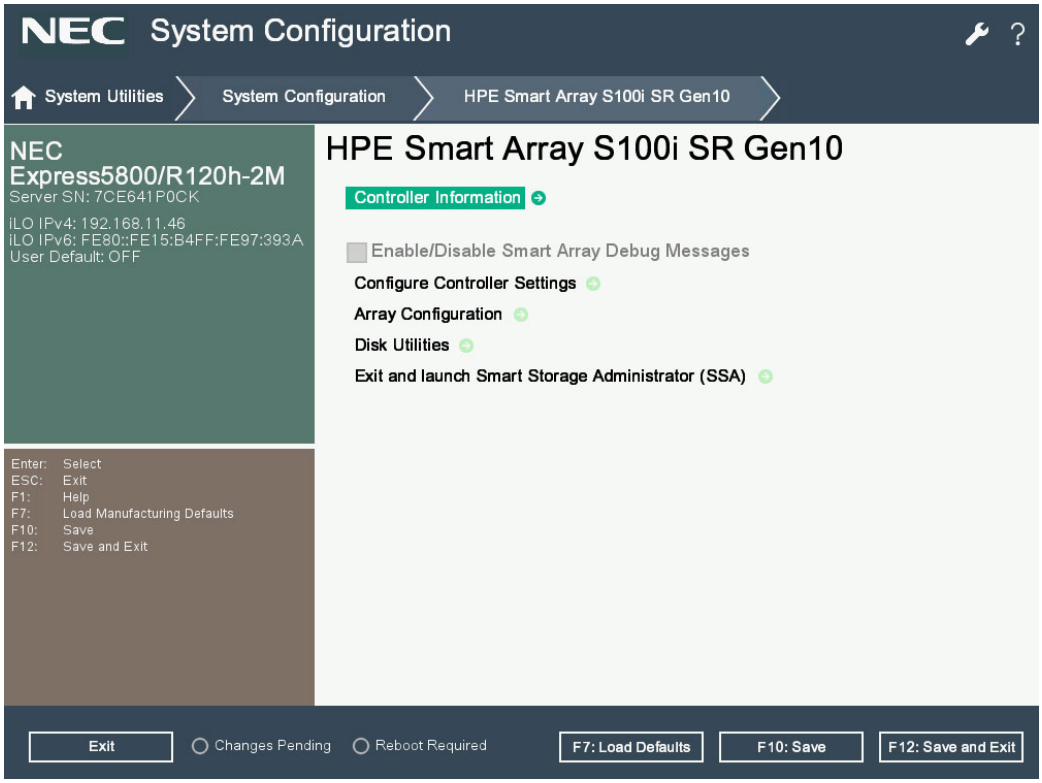
The **System Utilities** menu appears
If you select **System Configuration**, the following submenu appears.



Select **Embedded Storage: HPE Smart Array S100i SR Gen10** and press the <Enter> key.

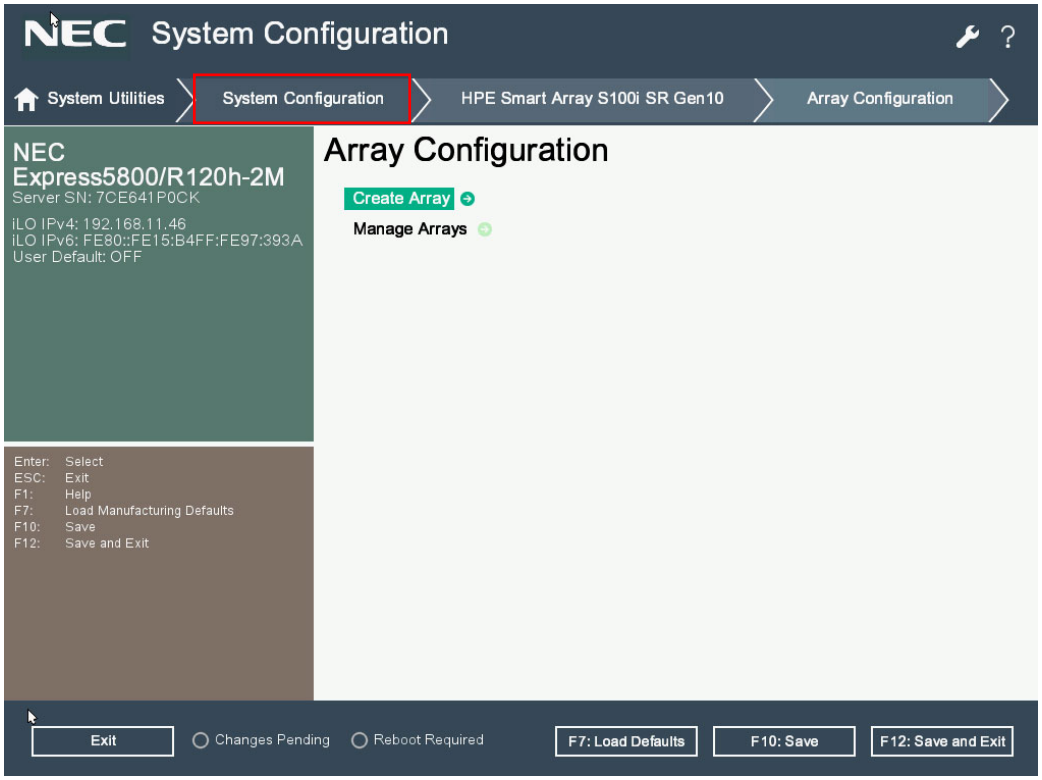


The following HPE Smart Array S100i SR Gen10 submenu appears.

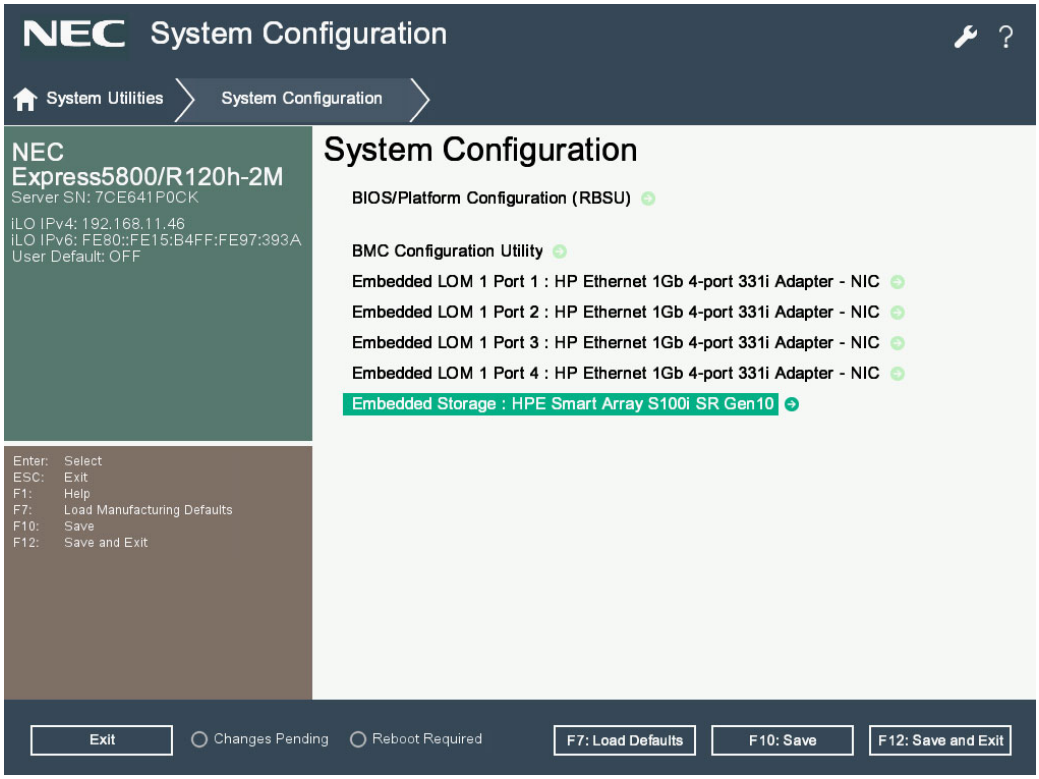


2.2 Exit HPE Smart Array S100i Utility

To quit the utility, press the <Esc> key a few times or click the top of selection as below figure red square indicated



When the following screen appears, the HPE Smart Array S100i Utilities is exited.



2.3 Menu Tree of HPE Smart Array S100i Utility

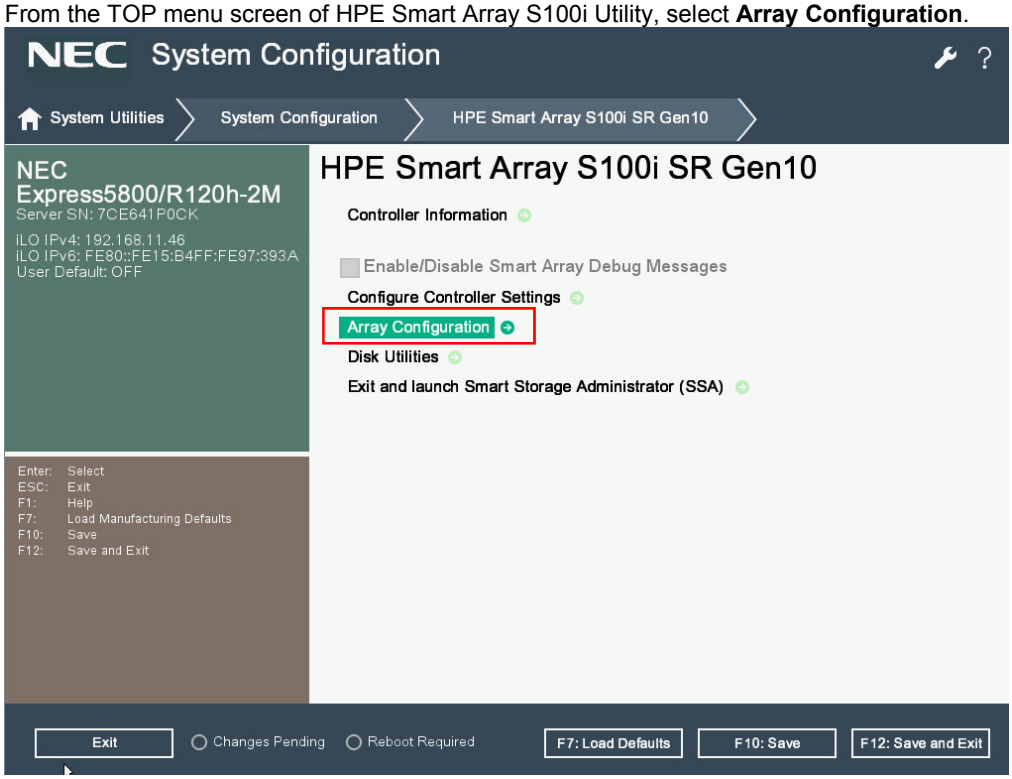
Menu	Default Value	Descriptions
Controller Information		
UEFI Driver version		UEFI Driver version
UEFI Driver release date		UEFI Driver release date
Firmware version		Firmware version
Firmware release date		Firmware release date
PCI device ID		PCI device ID
PCI Slot number		PCI Slot number
Configure Controller Settings		
> Modify Controller Settings		
Rebuild Priority	Low	Priority at which the logical drives are rebuilt from the failed state. It can be low, medium, medium high or high.
Surface Scan Analysis Priority	3	0:Disable. 31:High. 1-31:Idle(with delay).Modifies the amount of delay/idle time of the controller before the surface scan analysis is resumed again.
Current Parallel Surface Scan Count	1	Set the maximum number of surface scans that can run at the same time. Setting 1 disables the feature.
Physical Drive Write Cache State	Disabled	Option for enabling the write cache on the physical drives.
Spare Activation Mode	Failure Spare Activation	Option to change between the failure or predictive spare activation modes.
Port1I Mode	RAID	Connector Mode: For multiple domain connections.
Port 2I Mode	RAID	Connector Mode: For multiple domain connections.
Port 3I Mode	RAID	Connector Mode: For multiple domain connections.
Port 4I Mode	RAID	Connector Mode: For multiple domain connections.
Port 5I Mode	RAID	Connector Mode: For multiple domain connections.
Port 6I Mode	RAID	Connector Mode: For multiple domain connections.
> Advanced Controller Settings		
Degraded Mode Performance Optimization	Disabled	Parity RAID Degraded Mode performance optimization.
Physical Drive Request Elevator Sort	Enabled	It enables or disables the physical drive cache write elevator sort algorithm.
Maximum Drive Request Queue Depth	Automatic	The maximum number of physical drive requests the firmware will submit to a drive at a given time.
Monitor and Performance Analysis Delay	60	0-1440: input range. 60: Default. Set the monitor and performance analysis delay.
HDD Flexible Latency Optimization	Disabled	Enables or Disables the flexible Latency scheduler to limit the high latency request from the HDDs.
> Clear Configuration		Removes the controller meta-data, array information and partition information.

Delete all array configurations		Deletes the all the array present in the controller and the data present in the arrays will be lost.
Delete RIS on all physical drives		Deletes RAID metadata on the drives which are not part of array.
> Backup power source		
Backup power status		
Array Configuration		
> Create Array		
RAID Level		Select the RAID level based on the drives were be chosen.
Logical Drive Label		Alphabets and Numbers enter
Stripe Size /Full Stripe Size		The stripe size is the amount of data that is stored on each physical drive in the array.
Sector per track		The number of sectors per track presented to the operating system as part of legacy disk geometry (C/H/S) information.
Size		The value of logical volume.
Unit Size		Logical Drive Unit Size (MiB/GiB/TiB)
> Manage Array		
List Logical Drives		
-Logical Drive Details		Shows the detail of logical unit.
-Delete Logical Drive		Delete logical unit
Create Logical Drive		Create another logical unit
Manage Spare Drives		
-Assign Dedicated Spare		Drives assigned as dedicated spares can only be used as spare drives.
-Assign Auto Replace Spare		When drives assigned as auto replace, it will automatically become part of the array.
Delete Array		Delete all array information and meta data
Disk Utilities		
> Device Information		Provide the information related to the particular device
> Identify Device		Turn On/Off the device identification LED
Identification Duration (Seconds)	86400	Device LED identification Duration in seconds: 1-86400: input range. 86400:Default
Start		Start to turn on the device identification LED
Stop		Stop to turn on the device identification LED
Exit and launch Smart Storage Administrator (SSA)		SSA doesn't support SWRAID under offline mode. Use SSA under OS.

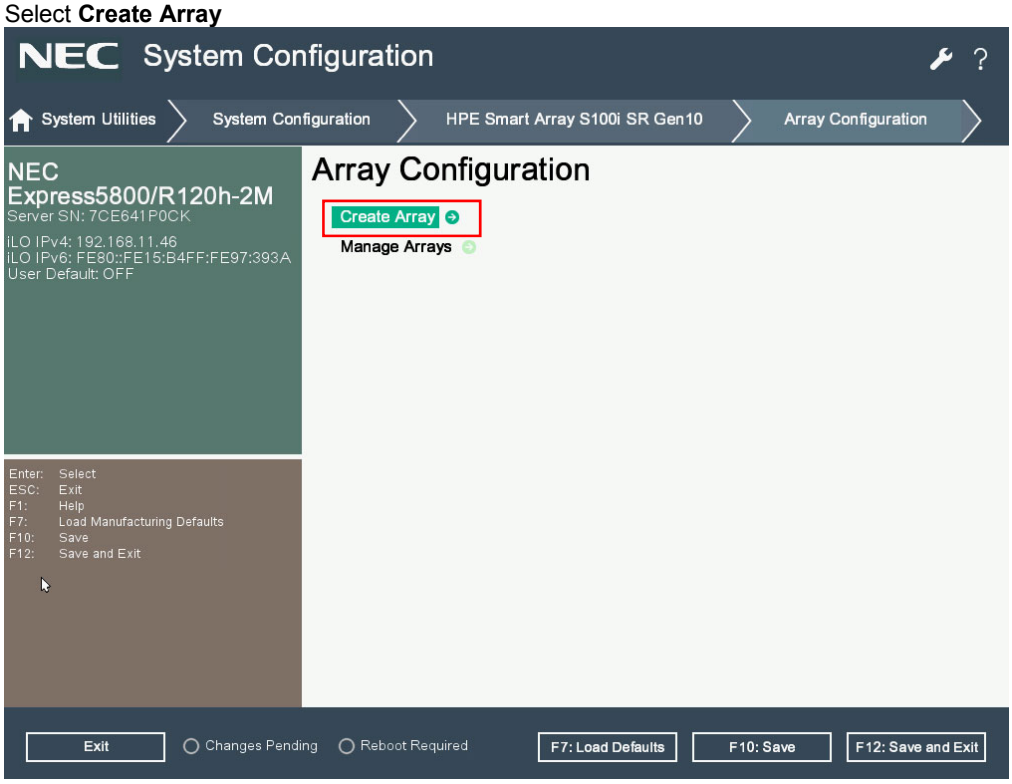
2.4 Procedures for Using Configuration Utility

2.4.1 Create configuration

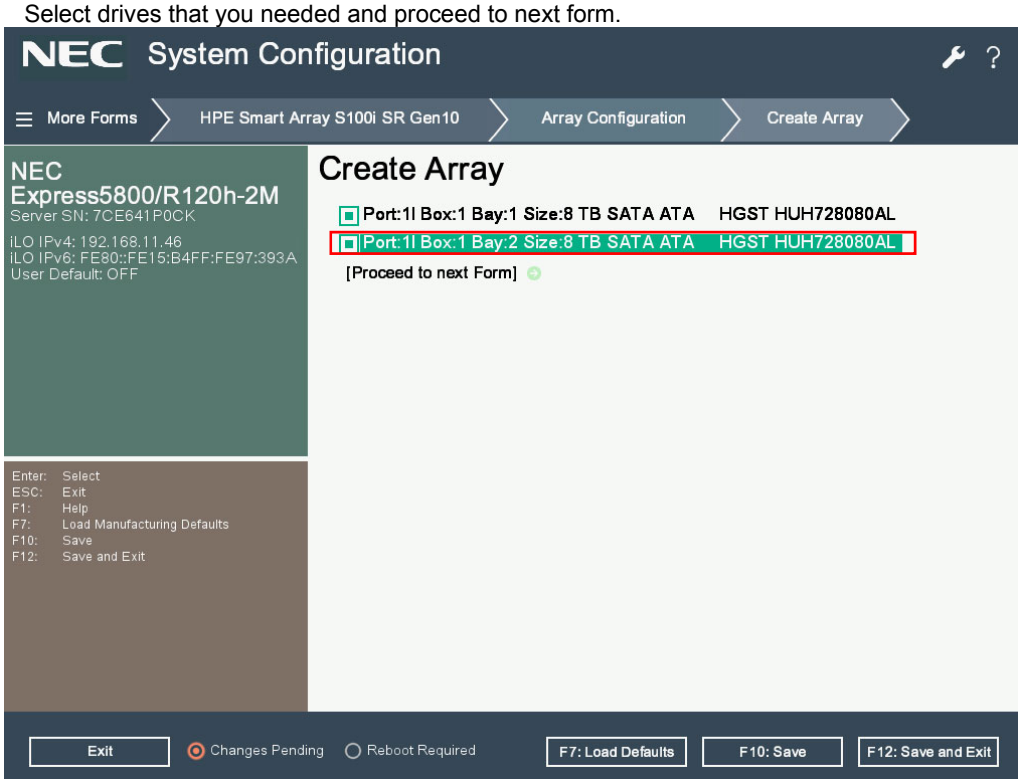
1. Run HPE Smart Array S100i Utility.
2. From the TOP menu screen of HPE Smart Array S100i Utility, select **Array Configuration**.



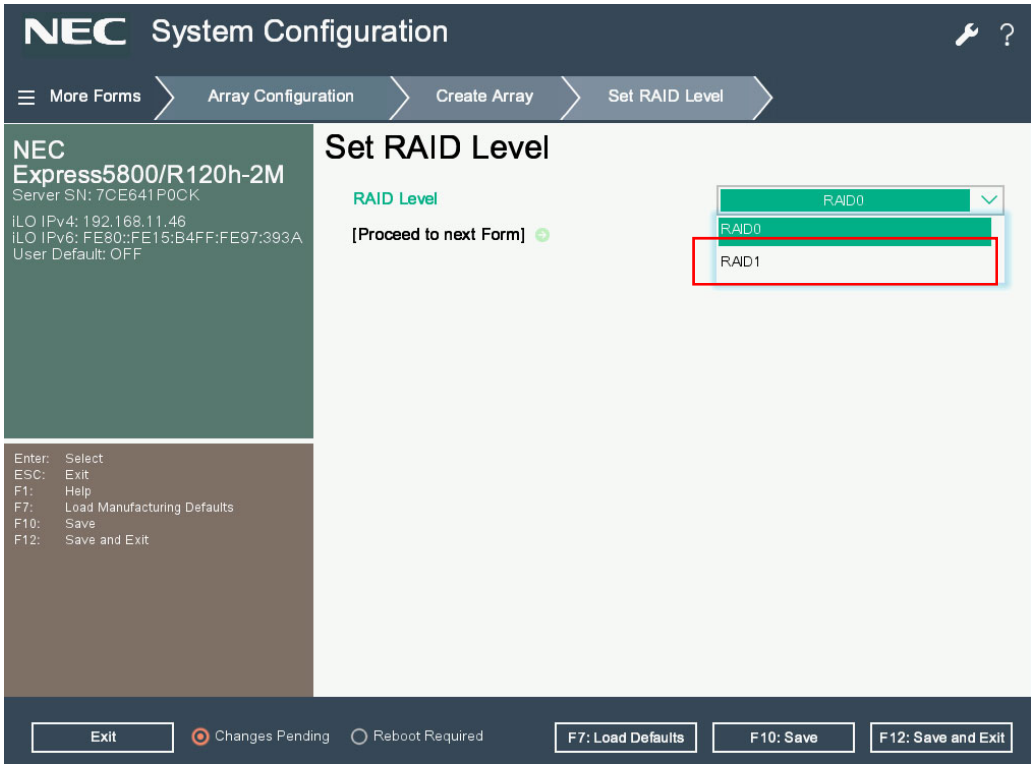
3. Select **Create Array**



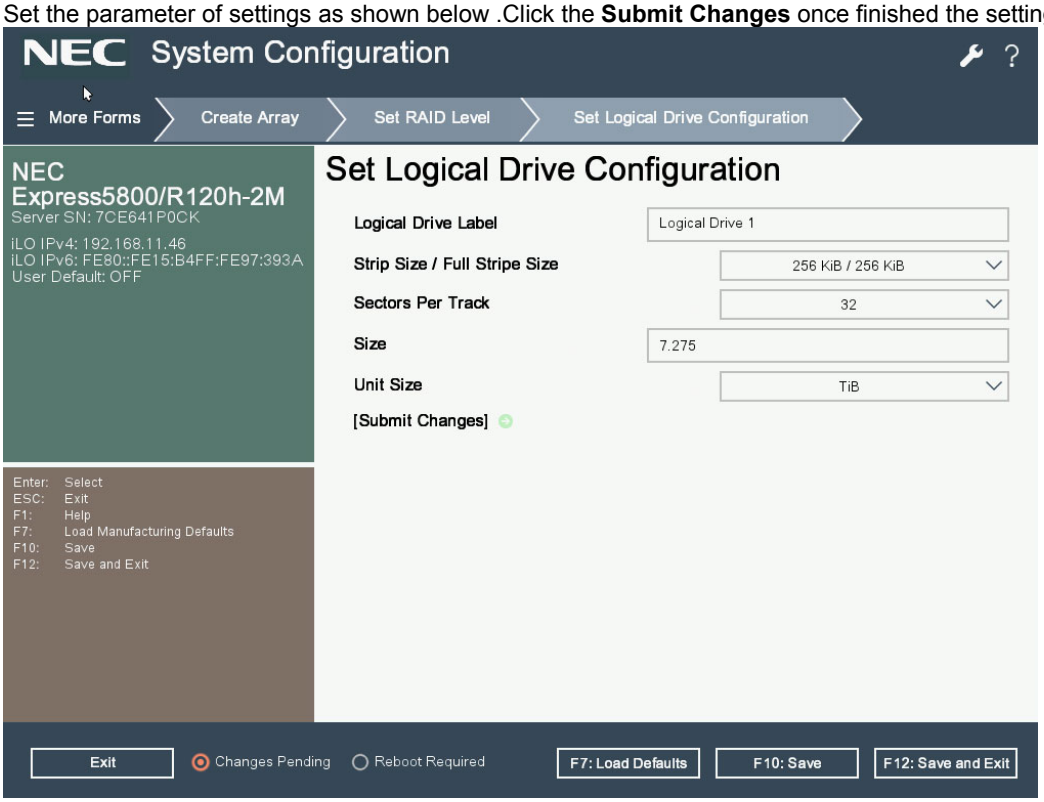
4. Select drives that you needed and proceed to next form.



5. **Set RAID Level** on the following screen, select the RAID level (RAID0 or RAID1) then proceed to next form.

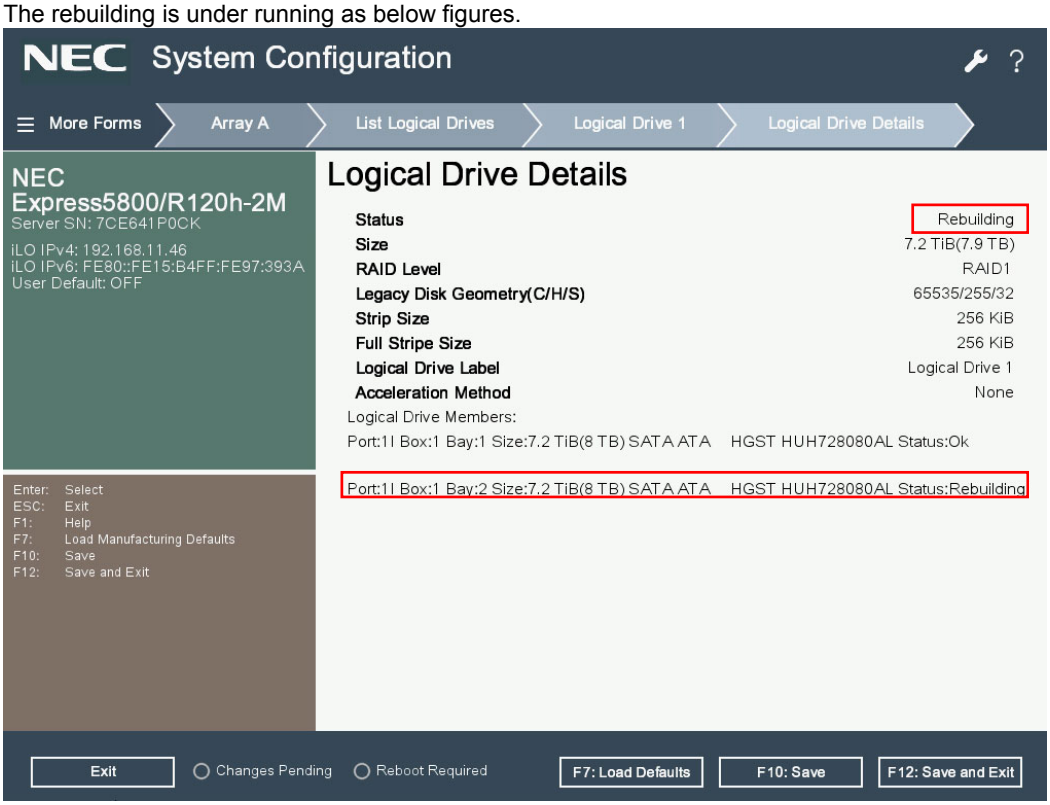


6. Set the parameter of settings as shown below .Click the **Submit Changes** once finished the settings.



2.4.2 Rebuild

1. Replace a physical device, and then rebuild operation will automatically start.
2. The rebuilding is under running as below figures.



Tips The progress of rebuilding should be checked in SSA (Smart Storage Administrator) under OS.

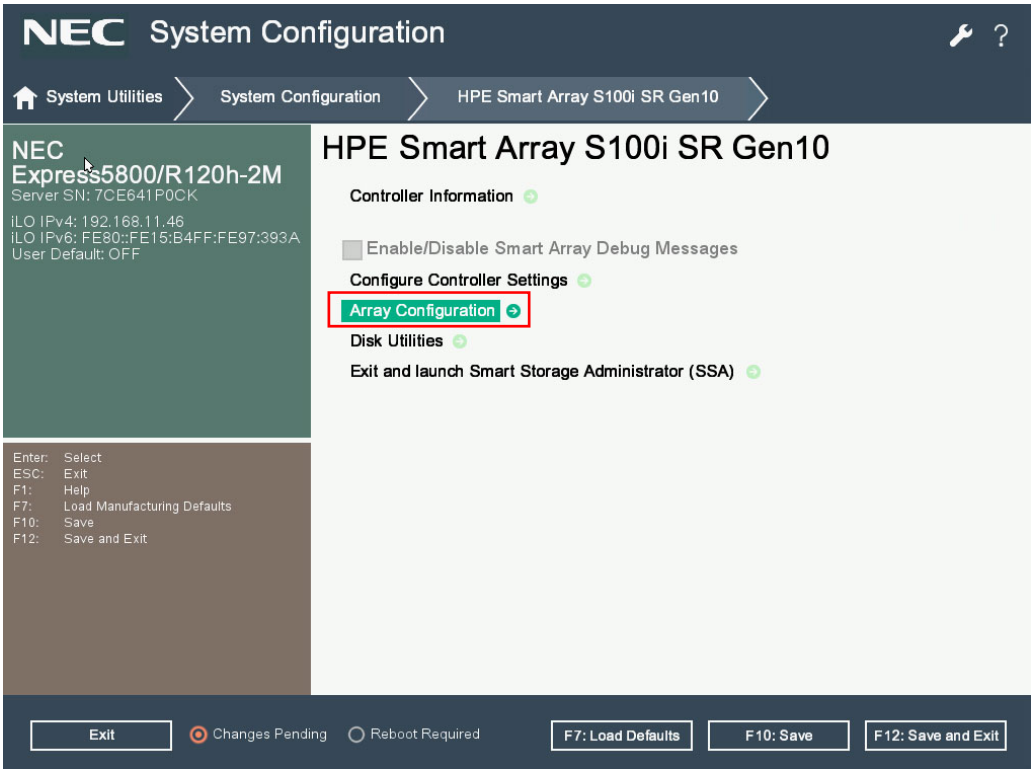
2.4.3 Configure HotSpare

(1) Assign Dedicated Spare

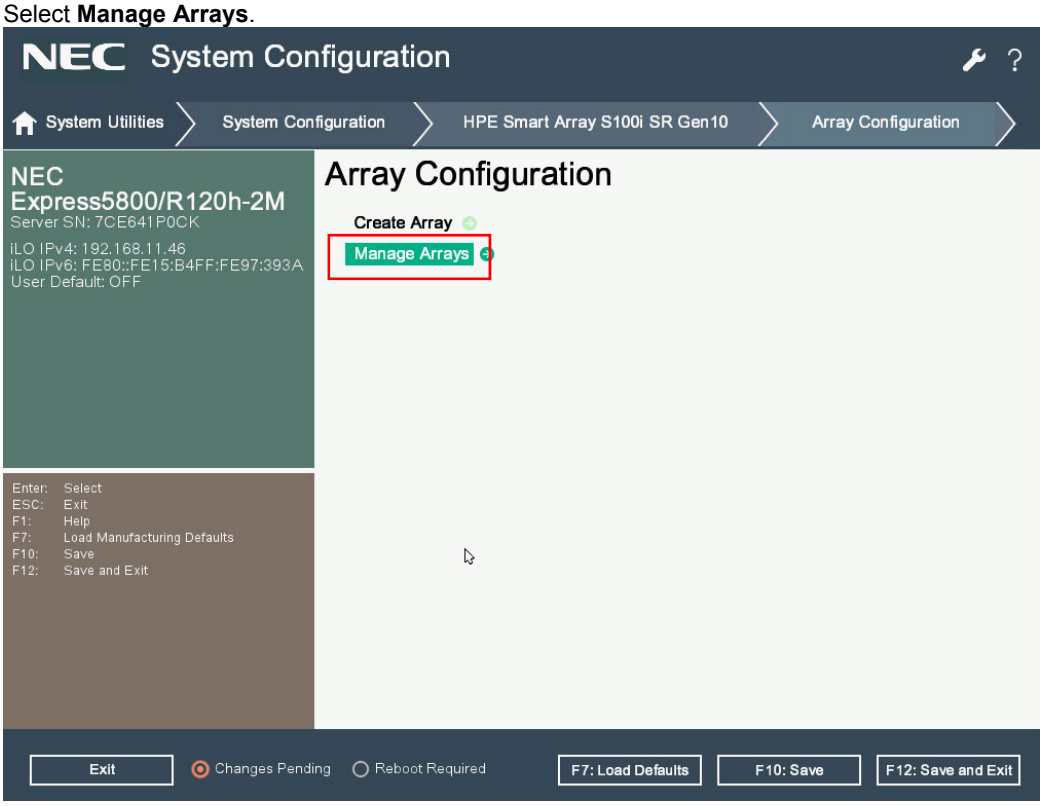
1. Connect a physical device for hot sparing, and then turn on the server.
2. Run HPE Smart Array S100i Utility.

On the TOP menu screen of HPE Smart Array S100i utility, select **Array Configuration**

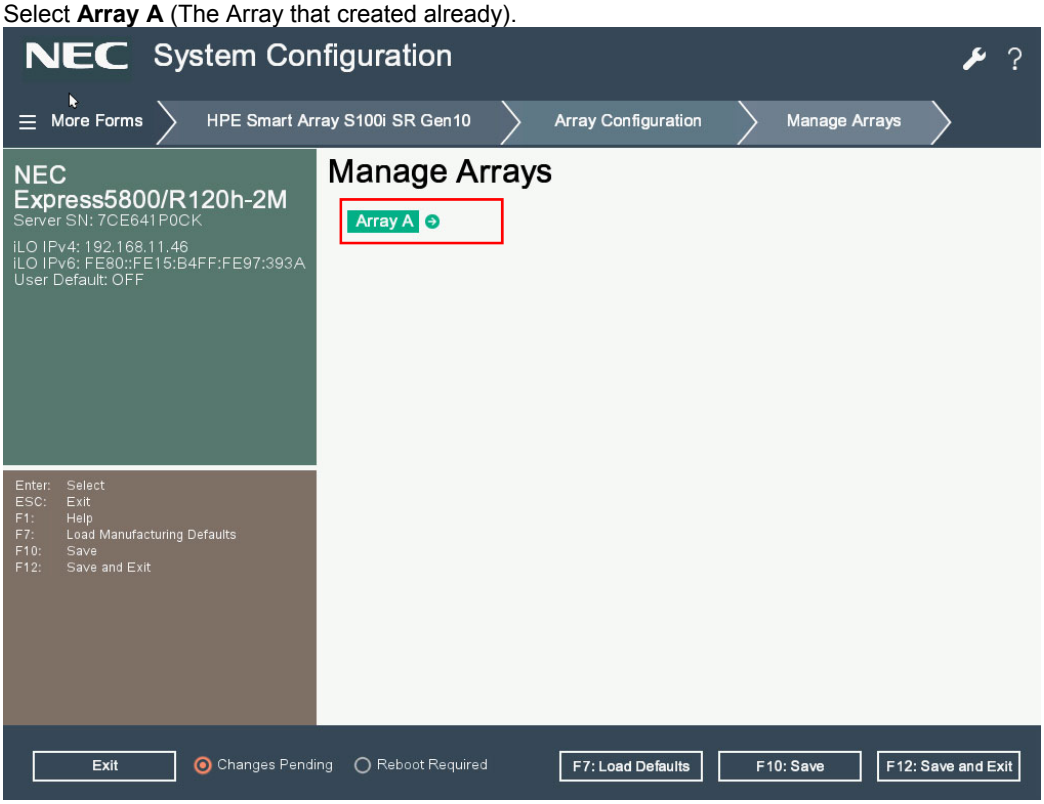
The following screen appears.



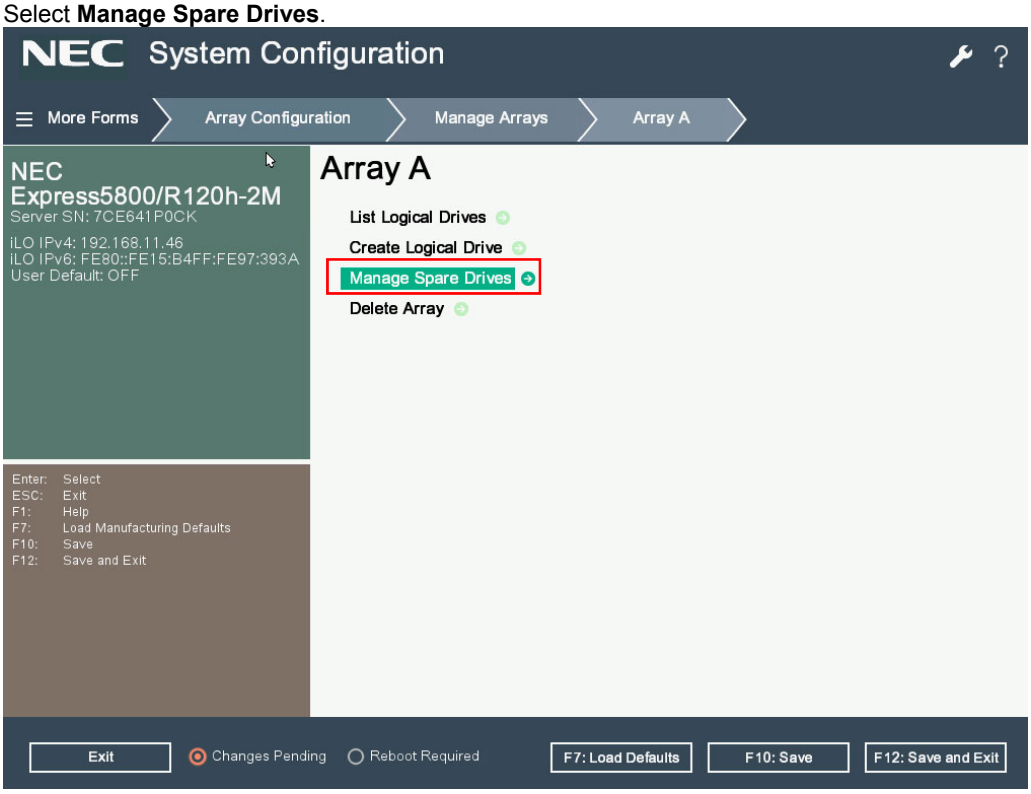
3. Select **Manage Arrays**.



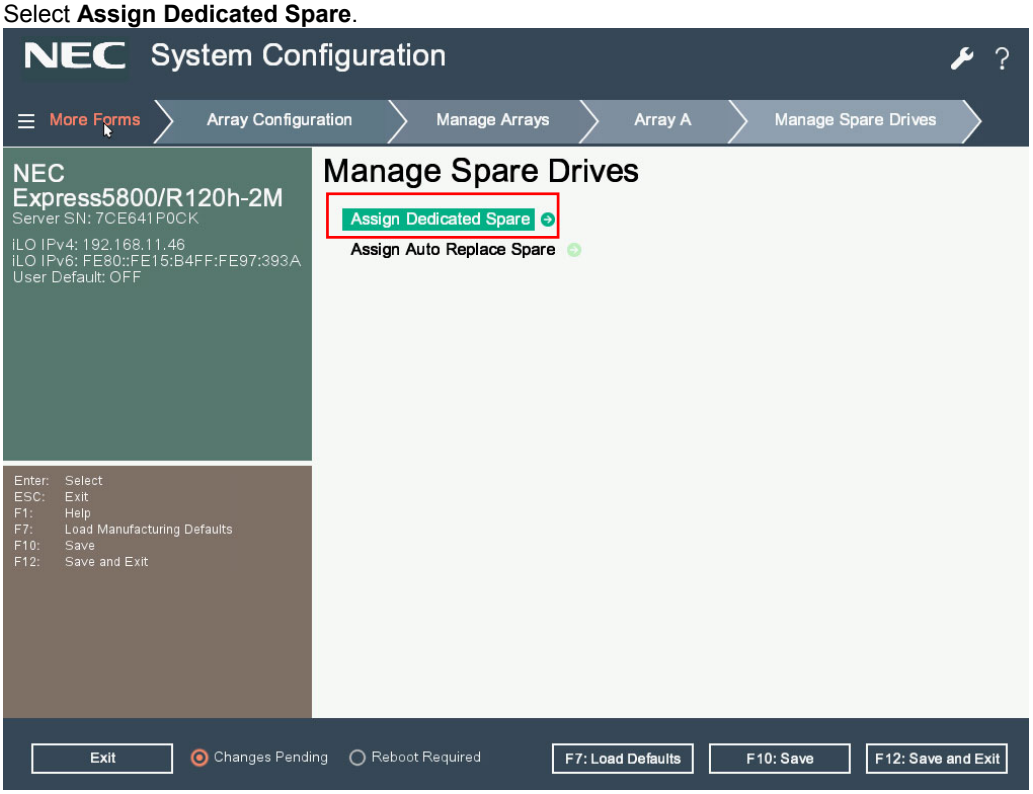
4. Select **Array A** (The Array that created already).



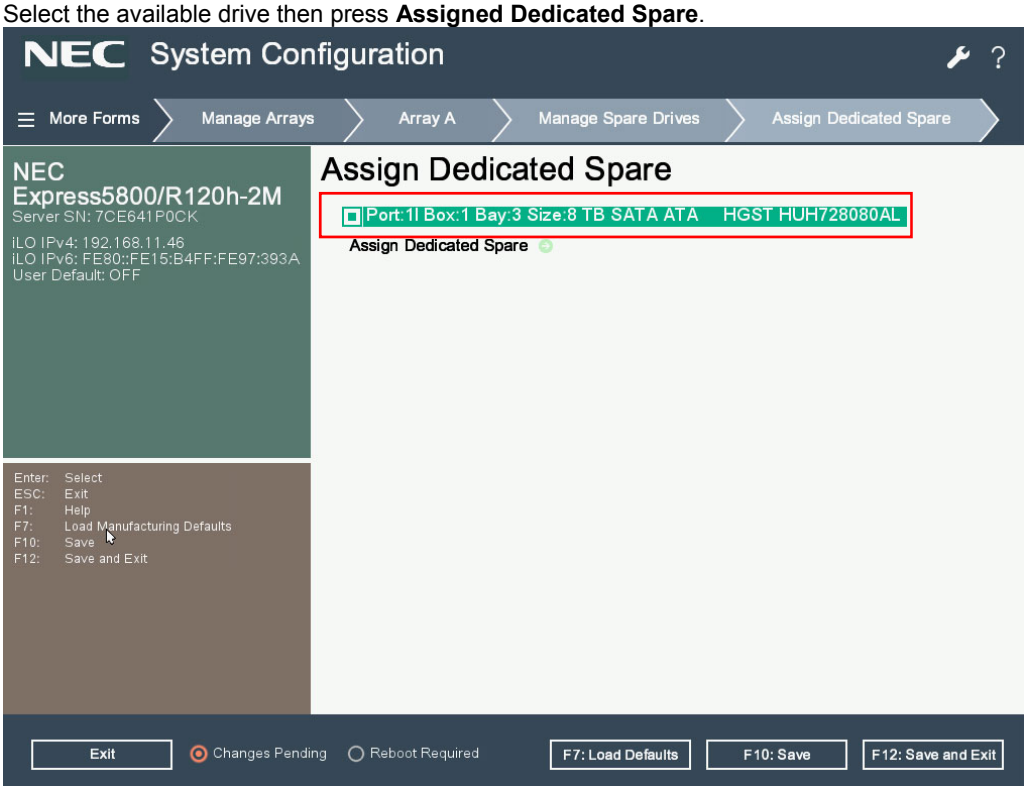
5. Select **Manage Spare Drives**.



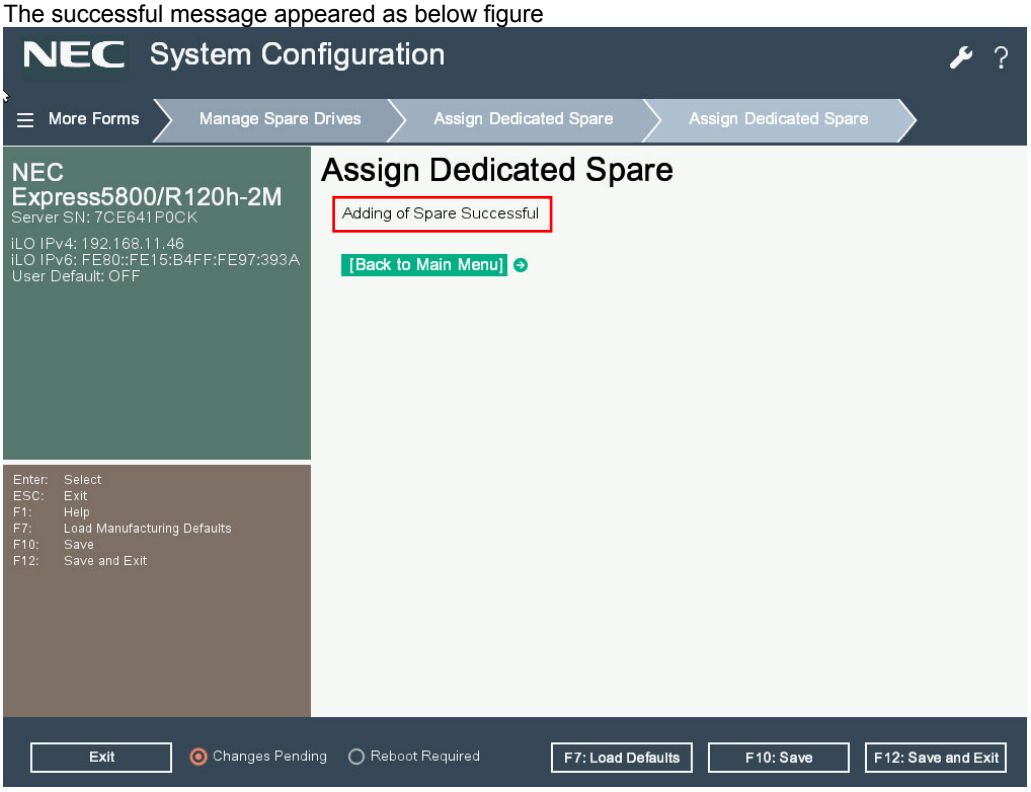
6. Select **Assign Dedicated Spare**.



7. Select the available drive then press **Assigned Dedicated Spare**.

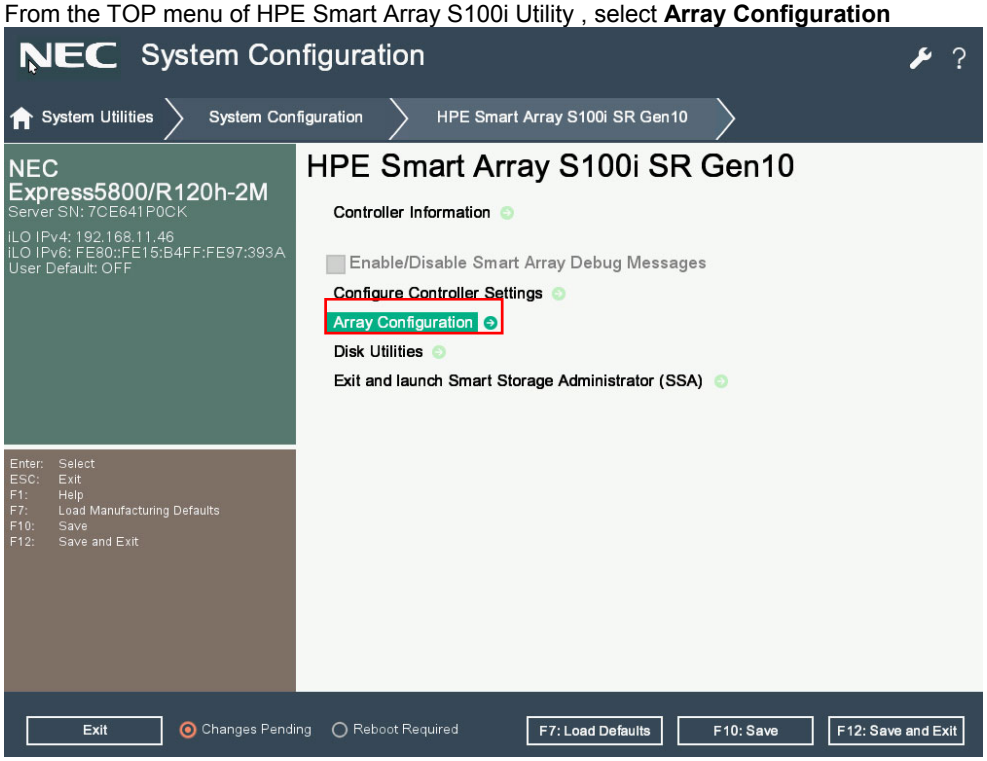


8. The successful message appeared as below figure

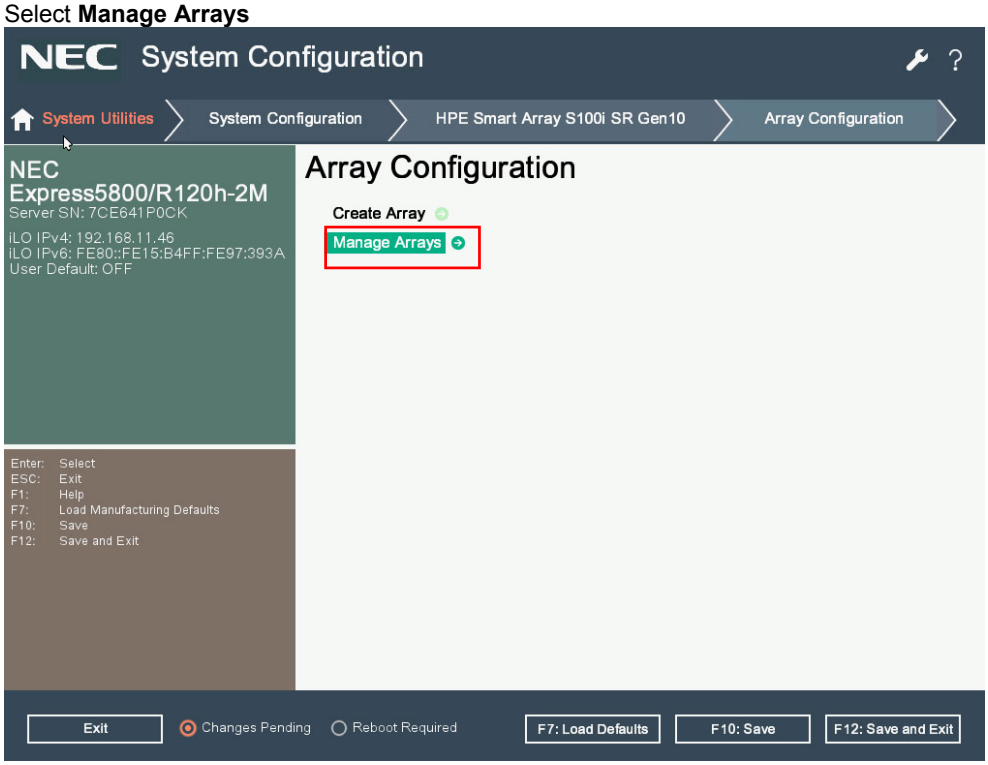


9. Check the logical drive has a spare member that added before

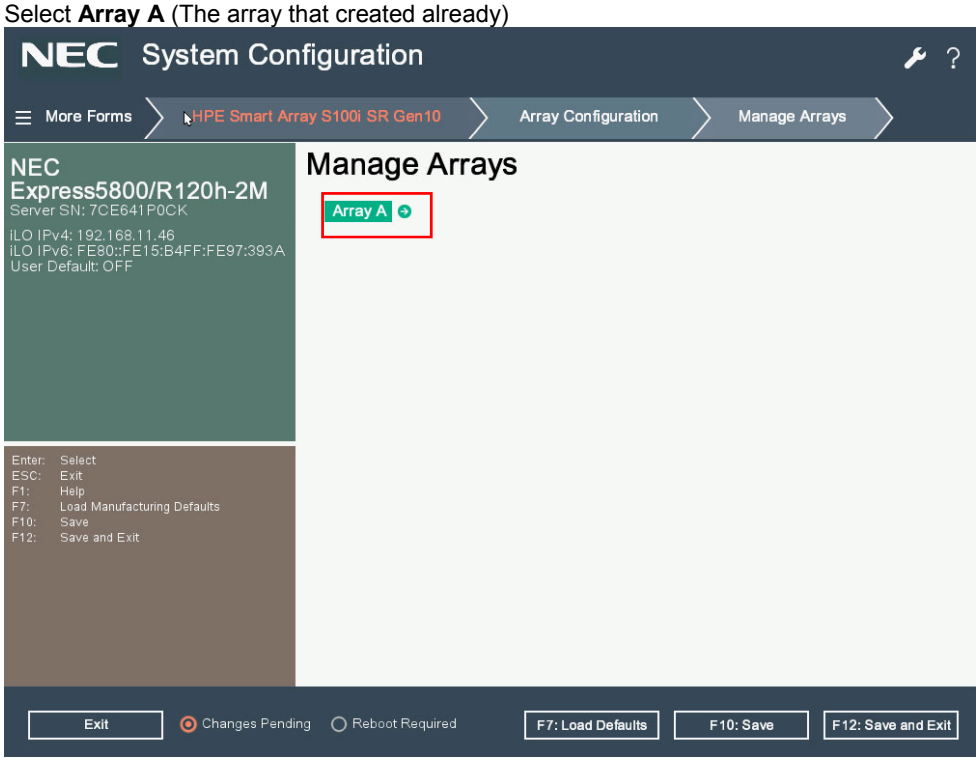
① From the TOP menu of HPE Smart Array S100i Utility , select **Array Configuration**



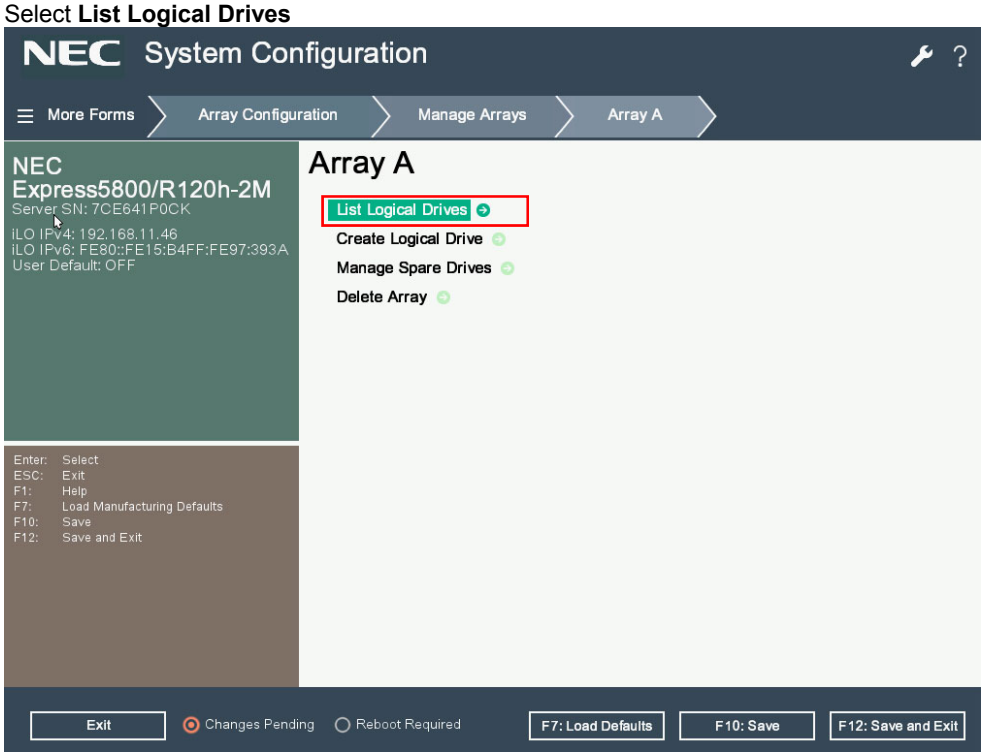
② Select **Manage Arrays**



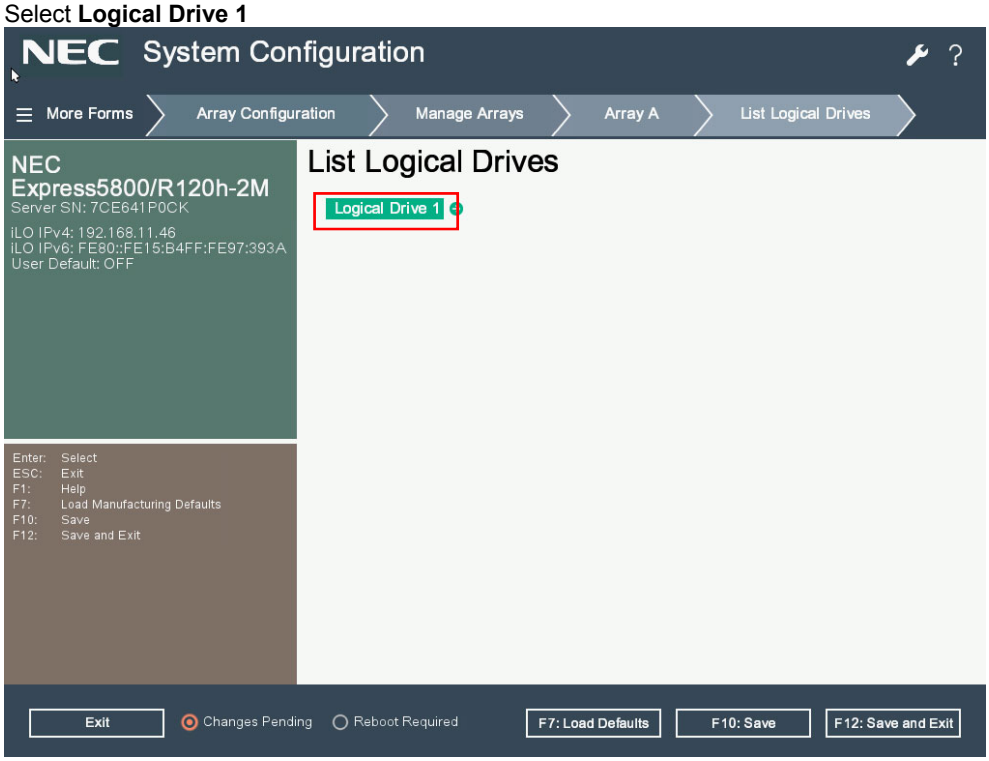
③ Select **Array A** (The array that created already)



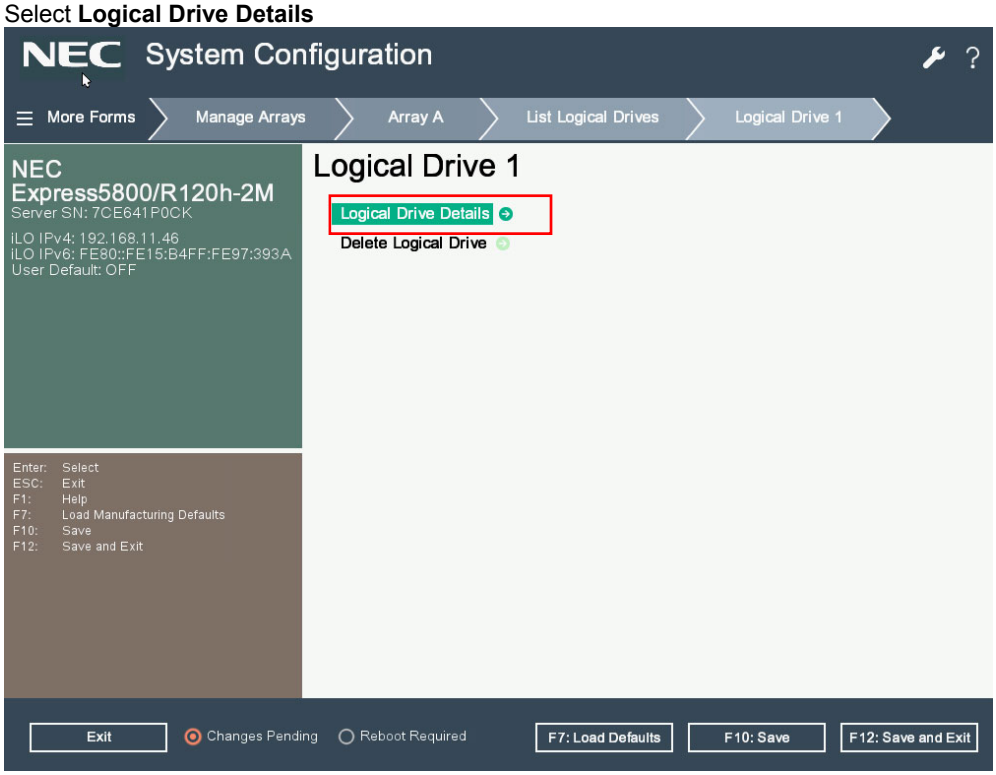
④ Select **List Logical Drives**



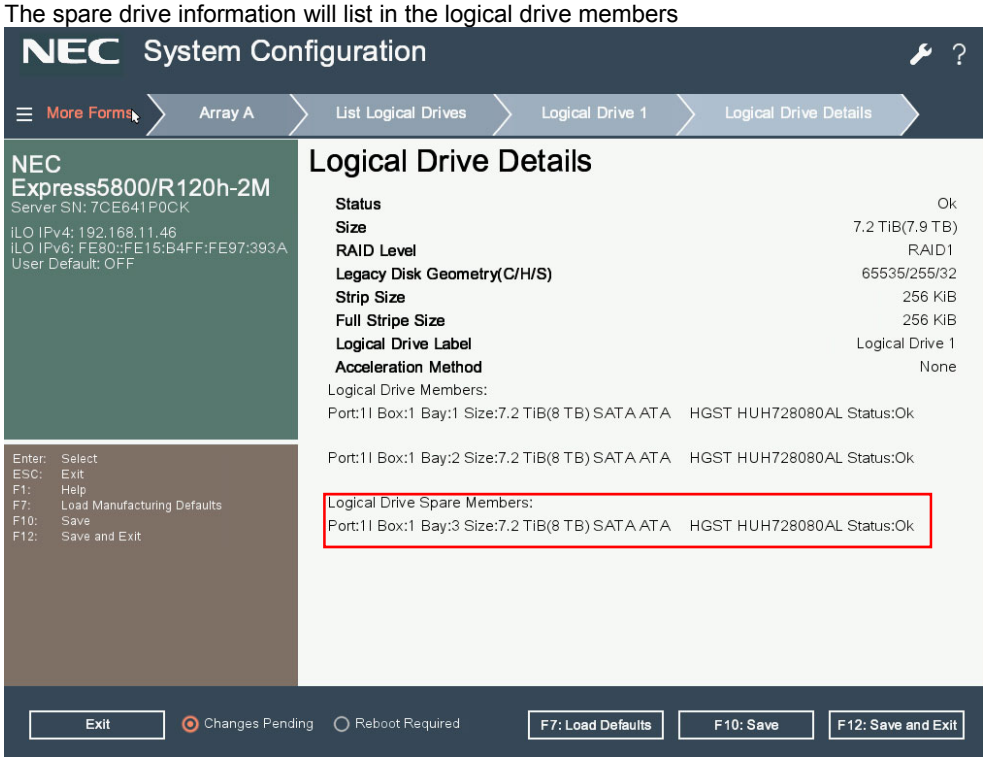
⑤ Select **Logical Drive 1**



⑥ Select **Logical Drive Details**



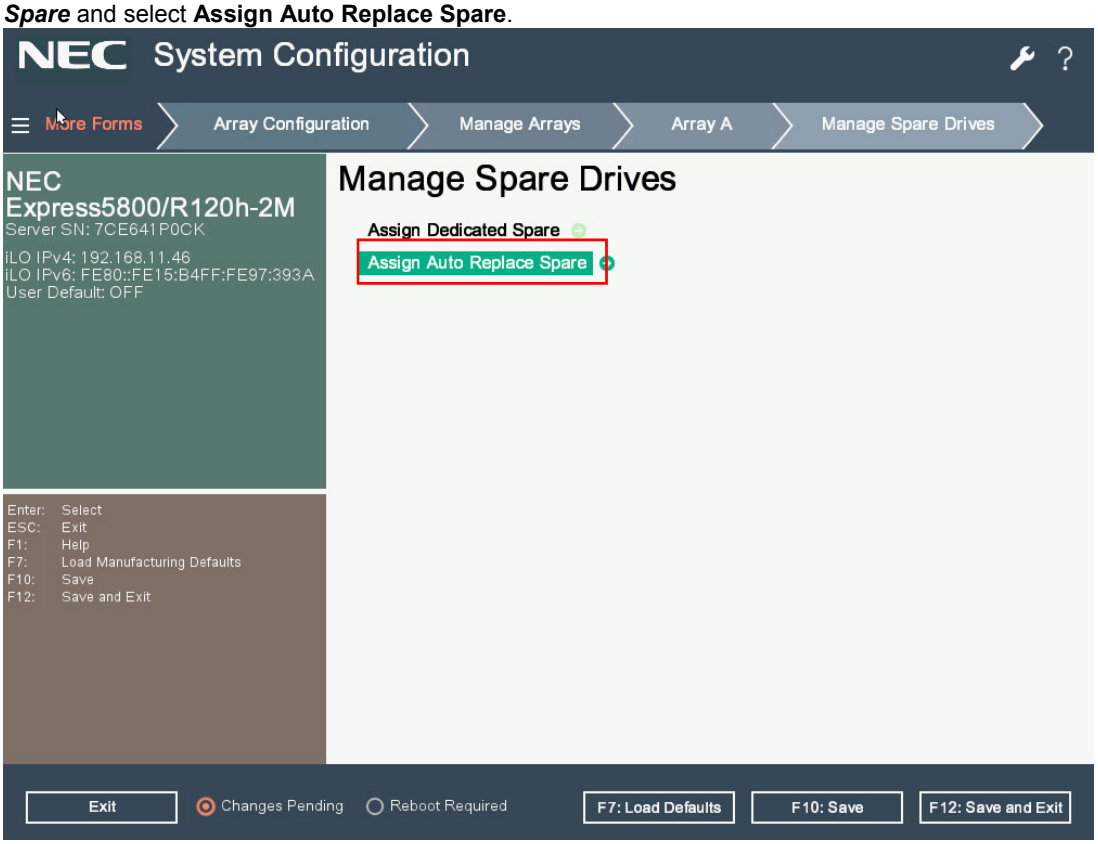
⑦ The spare drive information will list in the logical drive members



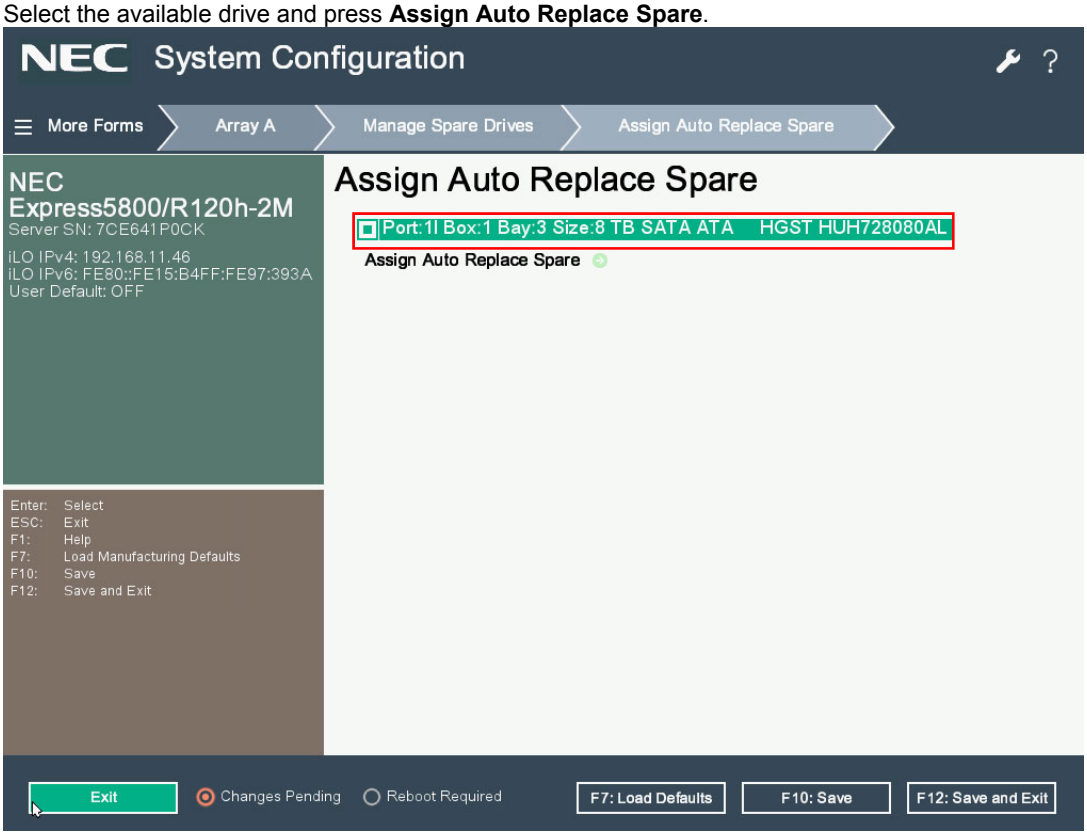
10. Exit **HPE Smart Array S100i Utility**.

(2) Assign Auto Replace Spare

1. Refer to steps from 1 to 5 procedure in the section in *3.4.3 Configure HotSpare* ***(1) Assigned Dedicated Spare*** and select **Assign Auto Replace Spare**.



2. Select the available drive and press **Assign Auto Replace Spare**.



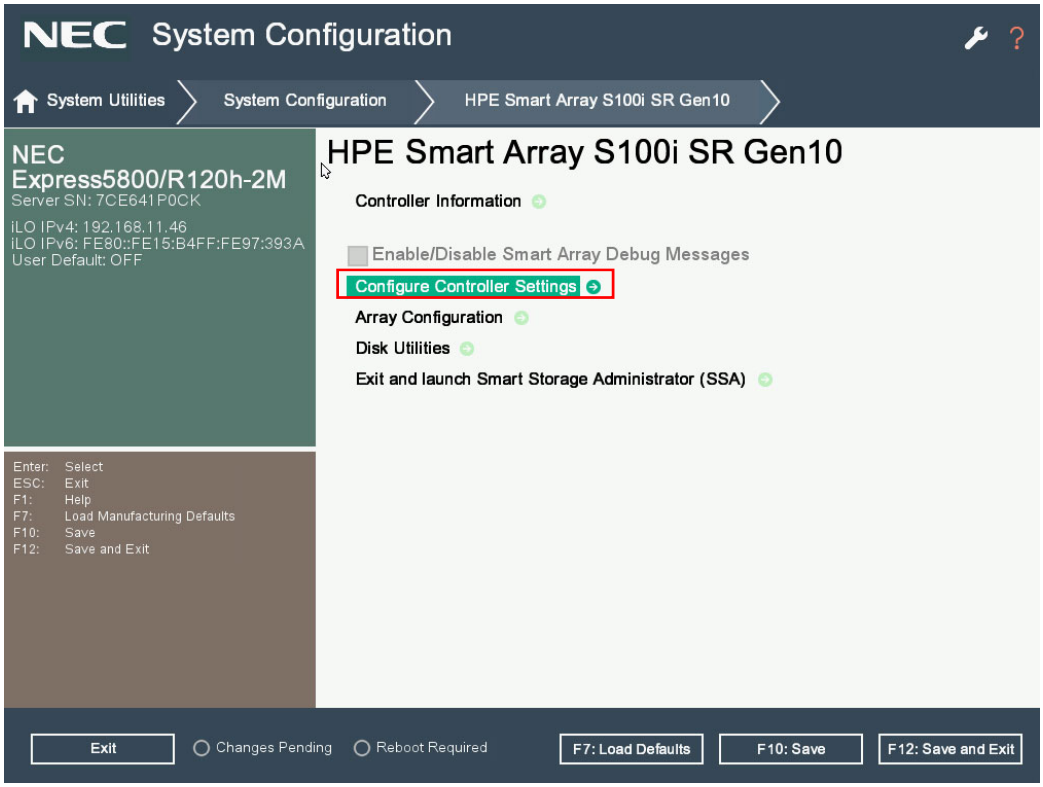
3. Then check the spare drive is one of the logical drive members , refer to Step 9 ①~⑦procedure in the section *3.4.3 Configure HotSpare* ***(1) Assigned Dedicated Spare*** section.
4. Exit **HPE Smart Array S100i Utility**.

2.4.4 Others

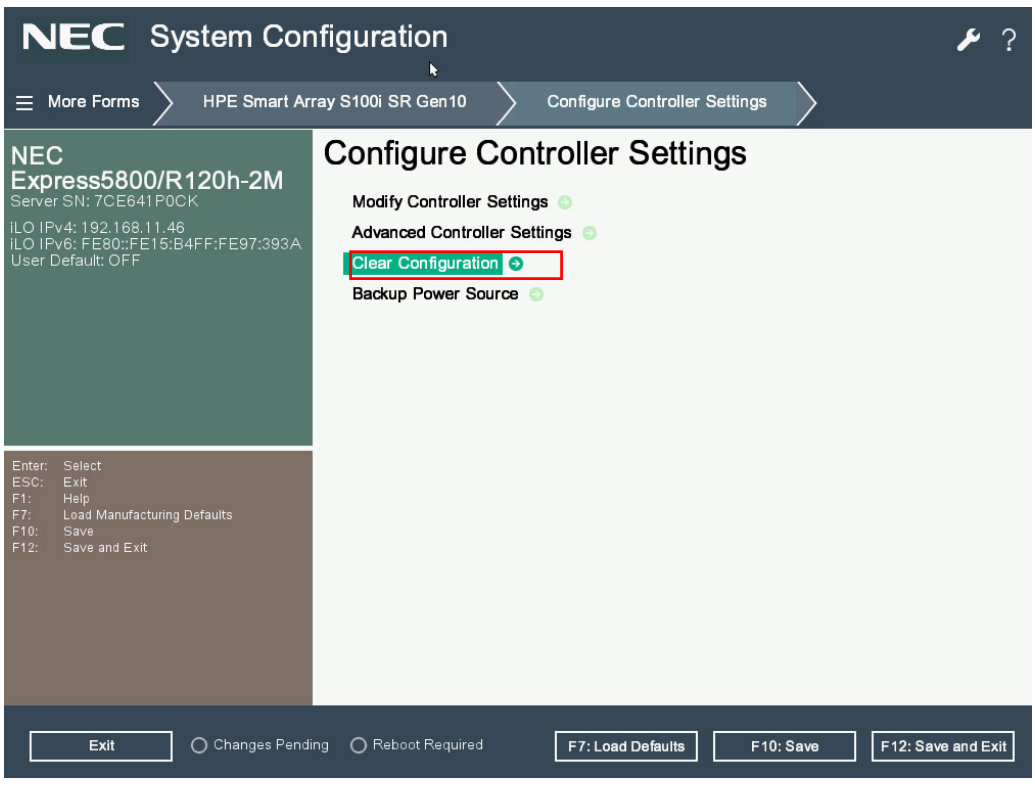
(1) Clear Configuration

Use this feature to clear configuration information. **Please make sure all the data that already backup before do it.**

1. From the TOP menu of HPE Smart Array S100i Utility. Select **Configure Controller Settings**.

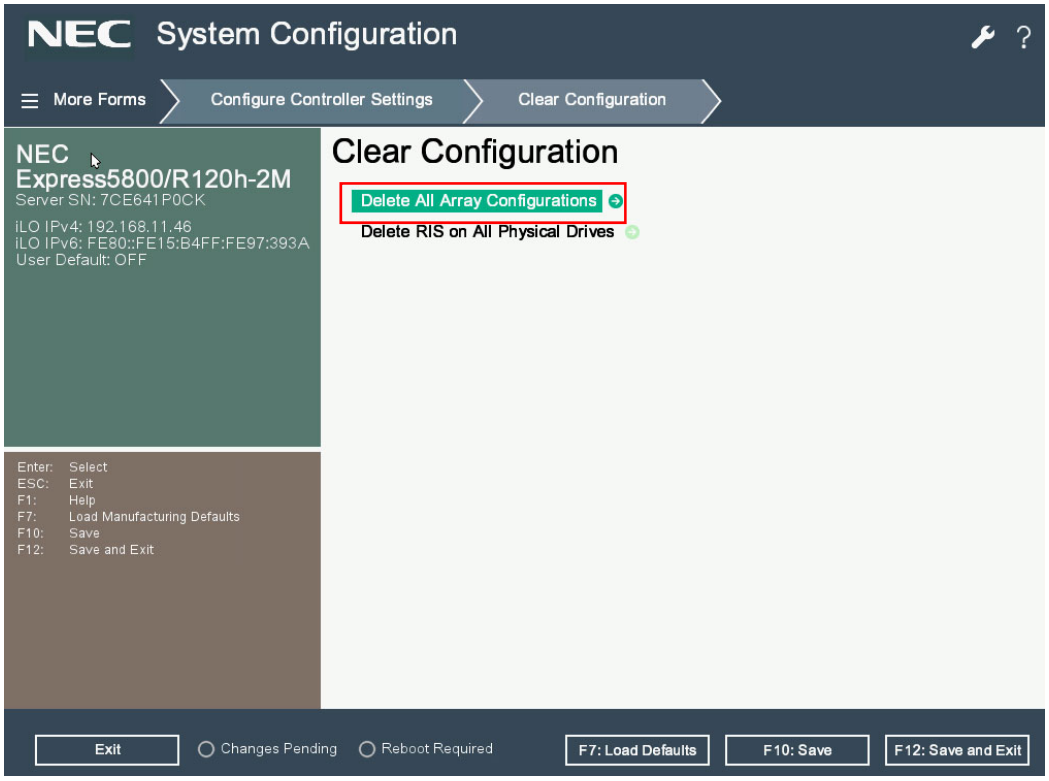


2. Select **Clear Configuration**.



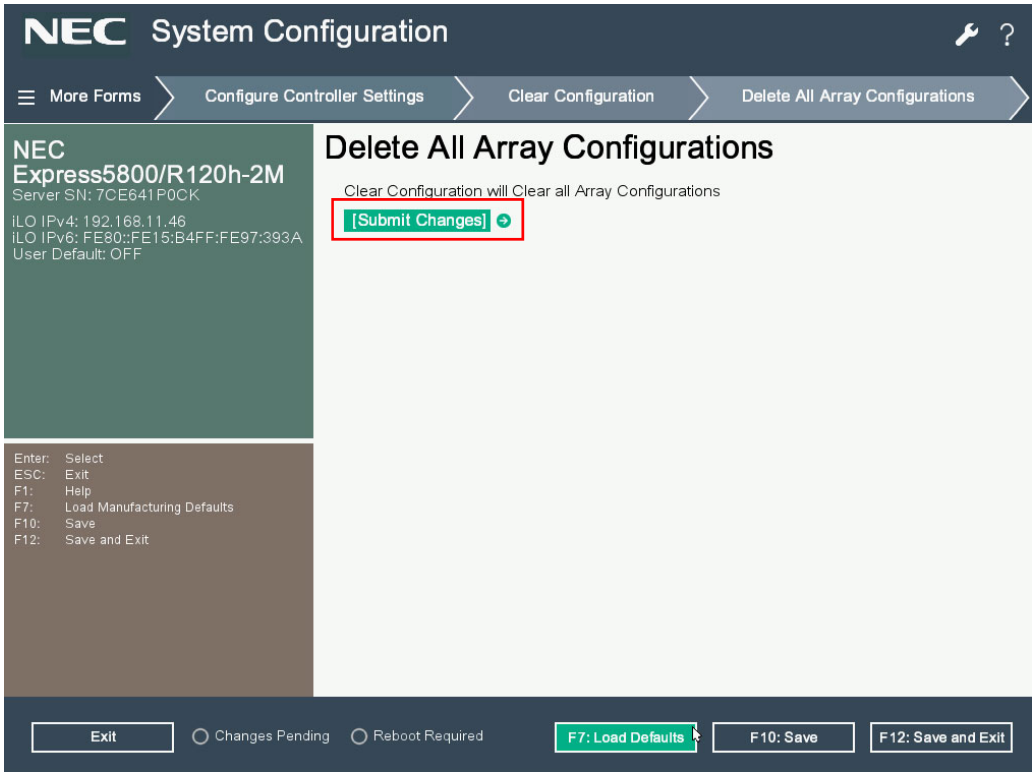
3. Select **Delete All Array Configurations**.

Important **The operation clears whole array information from controller and all data in the array will be lost.**

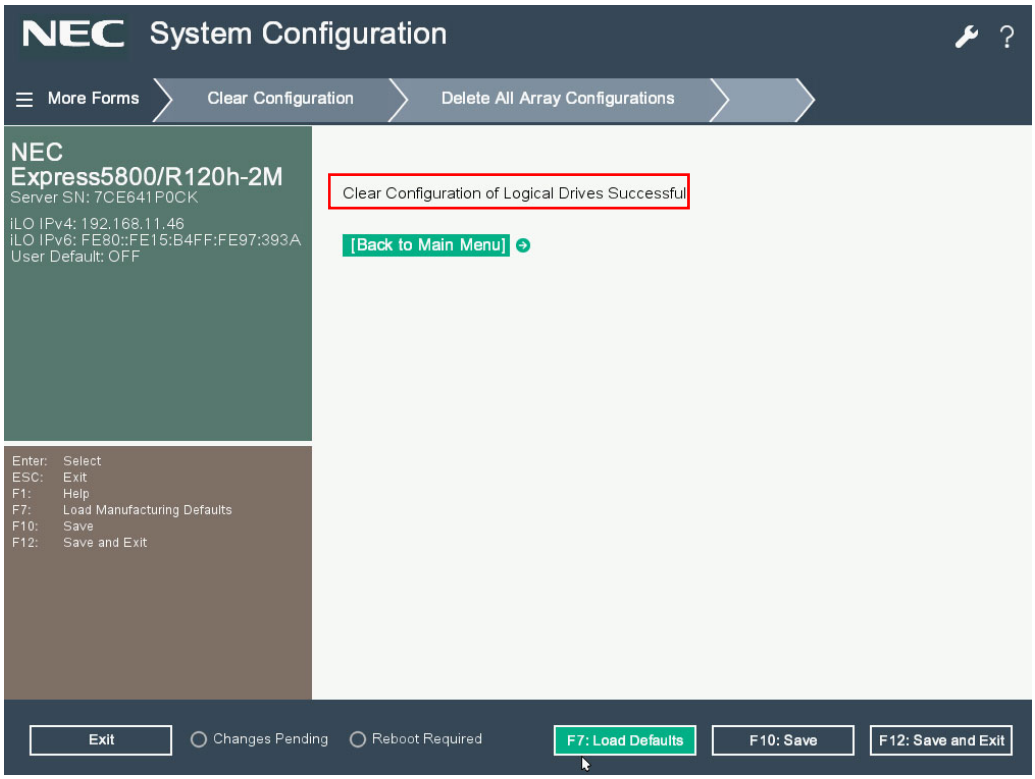


Note To delete the array data in physical drives, please select Delete RIS on All physical Drives.

4. All array data will be cleared and lost once click the **Submit Changes**.

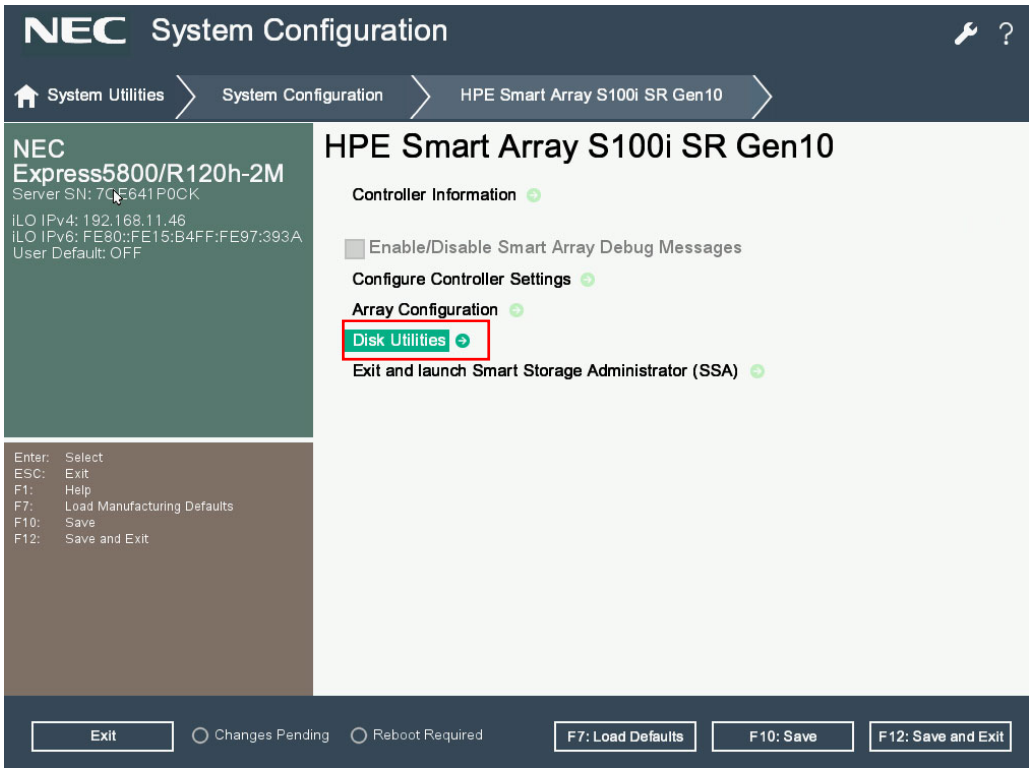


5. Successful message appeared after clear configuration then click **Back to Main Menu**

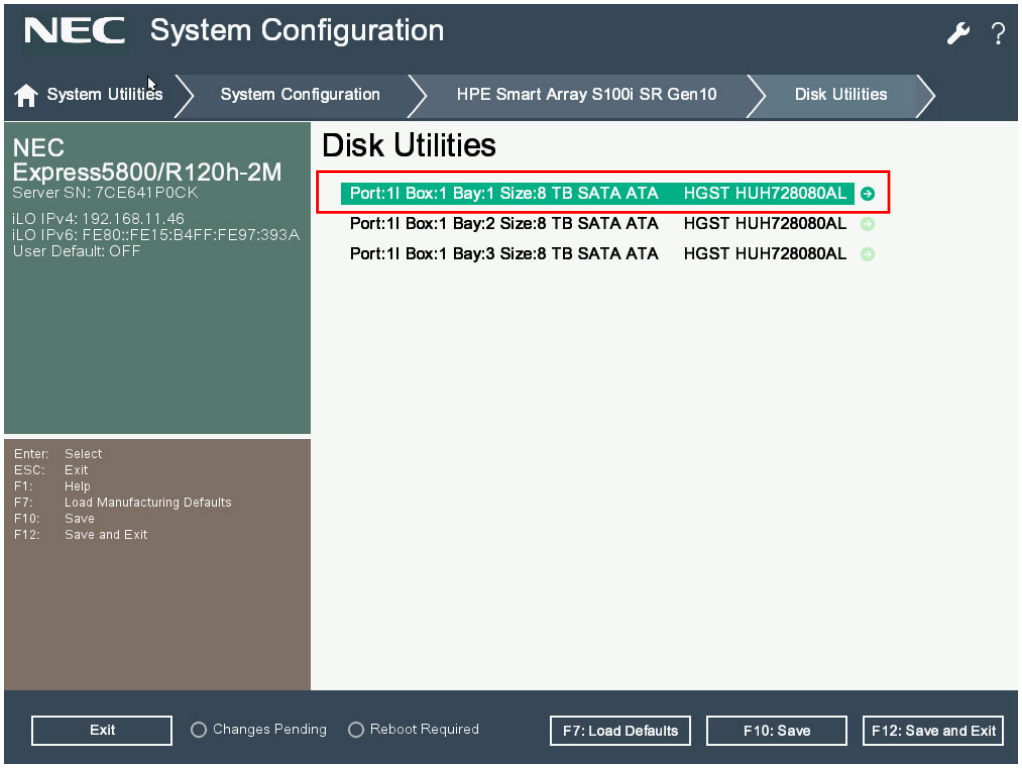


(2) Physical device information

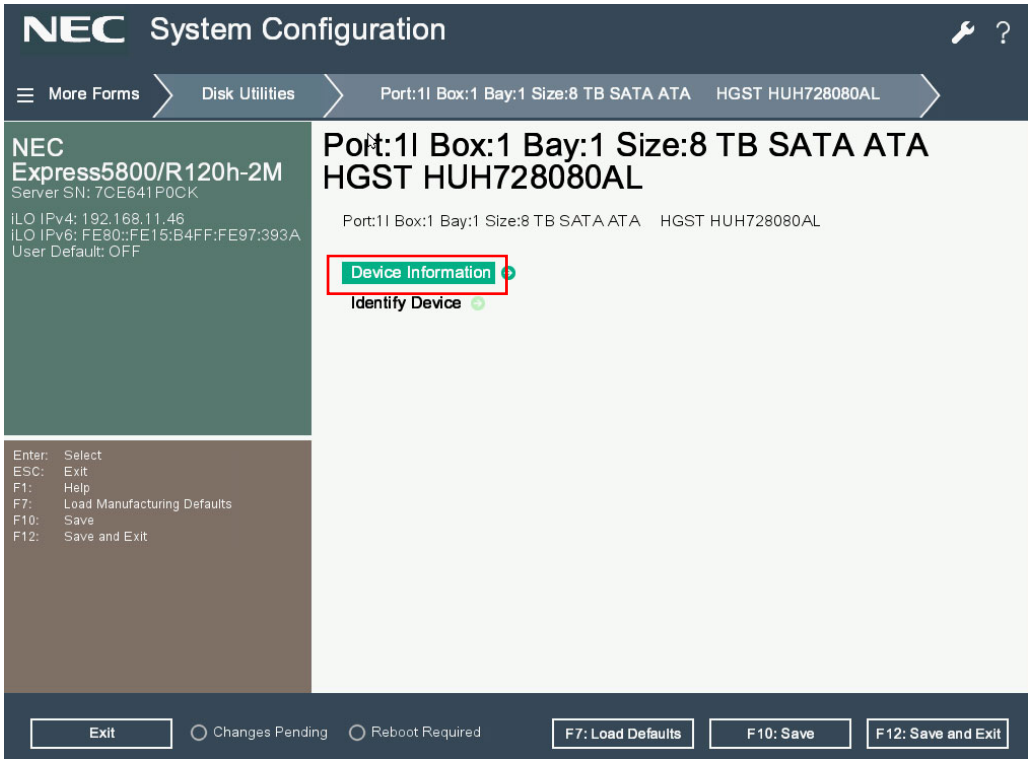
1. Use this feature to display physical device information.
From the TOP menu of HPE Smart Array S100i Utility, select **Disk Utilities**



2. Select a drive to see more details



3. Select **Device Information**



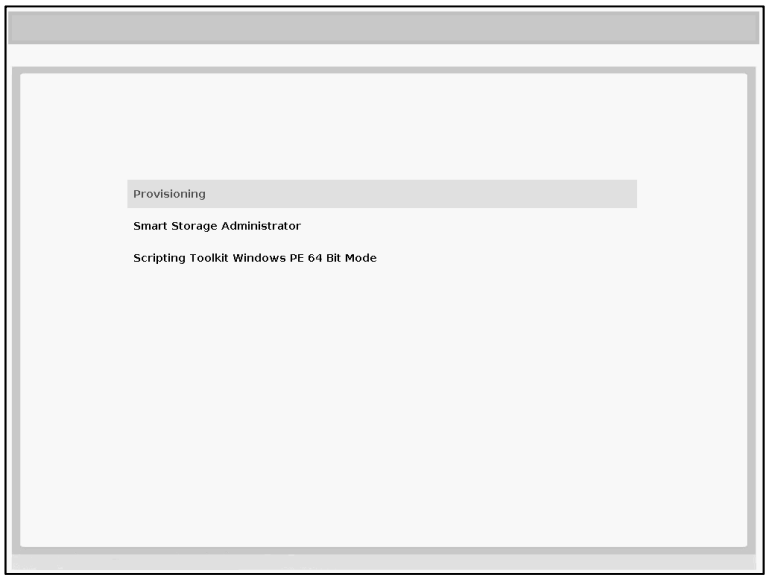
4. Then the drive information shows as below figure

3. Details of EXPRESSBUILDER

3.1 Starting EXPRESSBUILDER

1. Turn on the server, or press <Ctrl> + <Alt> + <Delete> keys to restart it.
2. Press the <F10> key on the POST screen.

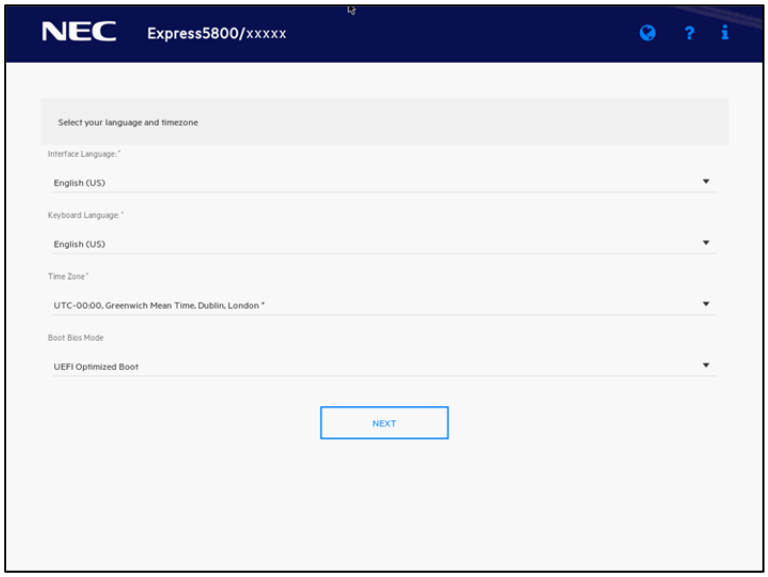
   The following menu will be displayed.



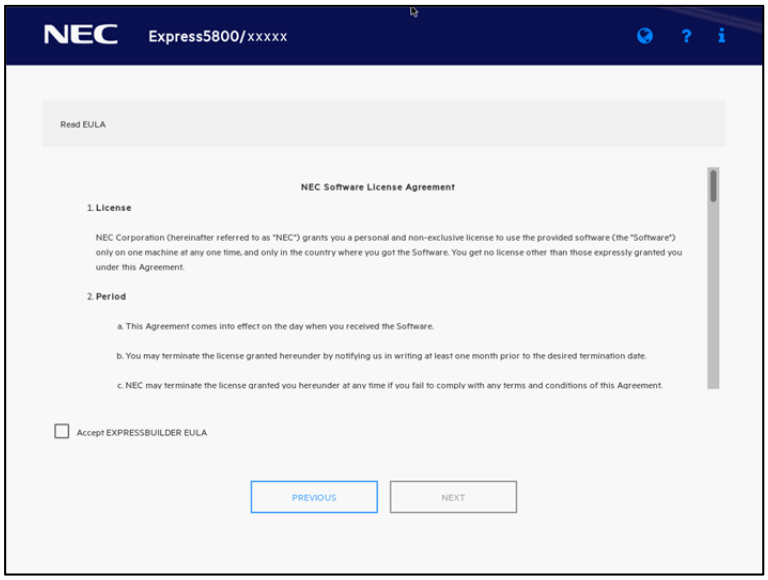
3. Select **Provisioning** on screen.

4. Only on the initial startup, click **First Time Set Up Wizard** to set the operating environment of EXPRESSBUILDER.

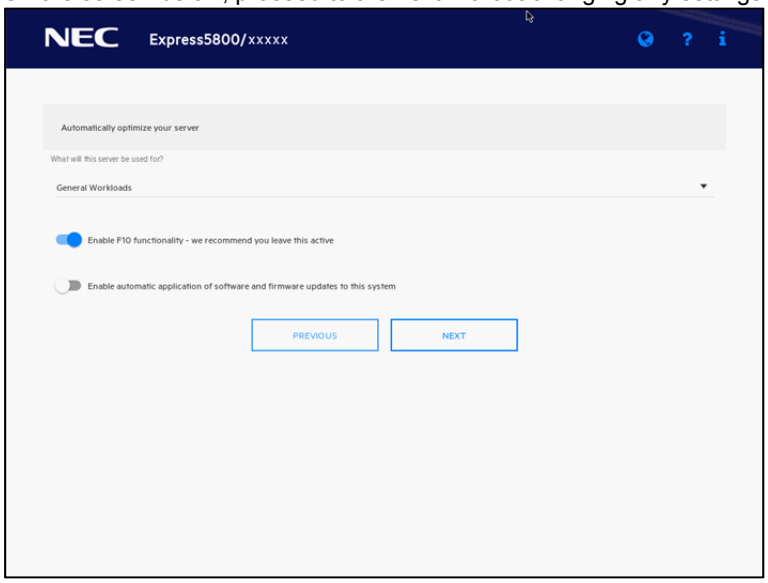
   (1) On the screen below, change **Interface Language** and **Keyboard Language** to your language and **Time Zone** to **UTC-00:00**, **Greenwich**, and then proceed to the next. Do not change any other settings.



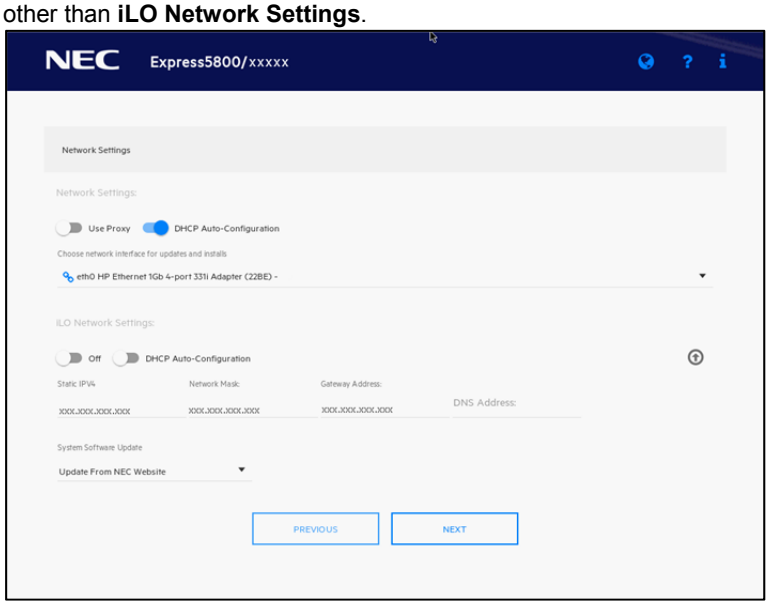
   (2) On the screen below, read the End User License (EULA), fill in the check box, and then proceed to the next.



(3) On the screen below, proceed to the next without changing any settings.



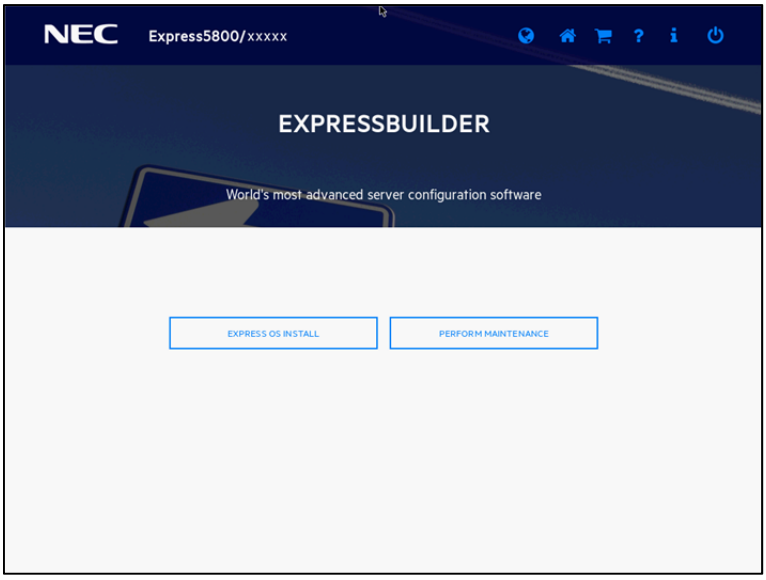
(4) On the screen below, change **iLO Network Settings** to your iLO network environment and then proceed to the next. The default of this setting is the current iLO network setting. Do not change other than **iLO Network Settings**.



(5) A confirmation window will be displayed. Select **YES** and exit.

3.2 Menus of EXPRESSBUILDER

You can operate EXPRESSBUILDER using on screen menus.



a) EXPRESS OS INSTALL

Installs the OS. For details, see *Installation Guide (Windows)*.

b) PERFORM MAINTENANCE

Starts the following maintenance tools individually.

(1) EXPRESSBUILDER Preferences

Configures the preferences explained at step 4 in *Chapter 2 (5.1 Startup the EXPRESSBUILDER)*.

(2) Active Health System Log

Saves the AHS log for analysis of failure to external media.

(3) Deployment Settings

Deploys the server installation settings to one or more servers.

(4) BIOS/Platform Configuration

BIOS settings are available.

(5) iLO Configuration

Configures the iLO settings instead of web console.

(6) System Erase and Reset

Erases the preferences or the hard disk drive.

Choosing **All Hard Drives** erases the contents in all the HDDs connected to the server. Also, if **Wipe Hard Drives** is chosen, user data will be completely erased by overwriting random patterns several times for all HDDs.

Important **If you erase the HDD using this function, the data recorded in the HDD can not be recovered. In addition, for running Wipe Hard Drive, it may take several days to be completed depending on the capacity of the HDD connected.**

(7) RAID Configuration

Starts Smart Storage Administrator (SSA) that can configure RAID arrays with GUI.

4. Details of Starter Pack

4.1 Starting the Menu

1. Prepare Starter Pack (optional product) or download it from the following web site.
   http://www.nec.com/express/

2. Start Windows on the server or any other computer.

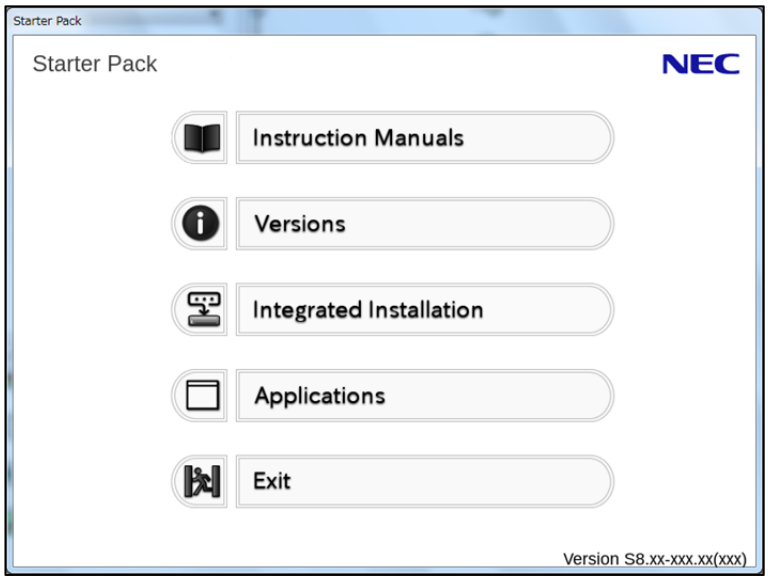
3. Insert the medium prepared in Step 1 into the computer on which Windows operates in Step 2.

4. Run the Explorer, and double-click "version.xml" in the root folder of the DVD. When the web browser opens, confirm that the window appears as shown below, and then close this window.

```
<?xml version="1.0" encoding="UTF-8"?>
- <XB_V5>
    <version type="S" medium="1" comp="01" revision="001" series="10" major="8"/>
</XB_V5>
```

(The figure is a sample and the displayed message is subject to change)

5. On the Explorer, start "start_up.bat" in the root folder of the DVD.
   The menu opens as shown below.



4.2 Functions of Starter Pack

In the menu, you can select the following items listed in this order.

a) Instruction Manuals

Shows instruction manuals.

b) Versions

Shows the versions of the included software, and drivers.

c) Integrated Installation

Installs Standard Program Package (SPP) and the application for server management easily. If the menu is not run on the server or the logon user does not have the administrator privilege, this item is not available.

d) Applications

Installs or runs applications individually.

e) Exit

Closes the menu.

5. iLO 5

Using iLO 5, which is an LSI for system management, enables various functions.

For more information about the functions of iLO 5, see *iLO 5 User's Guide*.

5.1 Various functions of the iLO5

iLO 5 has the control functions listed below.

Main functions of iLO	Description
Server status monitoring	iLO monitors the temperature inside the server and controls the cooling fan to cool the server appropriately. It also monitors the statuses of the network and many of the components such as the cooling fan, memory, processor, power supply unit, storage, and other devices that are installed in the server. In addition to these, the versions of the installed firmware and software are also monitored.
Agentless management	Agentless Management settings enable services to operate in the iLO firmware instead of the host OS. It also enables management without using any resources from the memory and processor on the host OS. In addition to monitoring the important internal subsystems, iLO can send an SNMP report directly to the management software, such as NEC ESMPRO Manager even when the host OS is not installed.
Integrated management log (IML)	IML can display events occurred on the server and set the notifications, such as SNMP report, Email alert, and Remote syslog .
Active health system log (AHS Log)	Downloads the Active Health System log. If necessary, the AHS log file may need to be sent to NEC, or the maintenance staff may collect it from you.
iLO linkage management	The iLO linkage function enables detection and management of multiple servers simultaneously without using management software.
Integrated remote control (IRC)	You can access the server safely at high speed from a remote console located anywhere in the world as long as the network is connected to the server.
Virtual media	You can remotely mount a high-performance virtual media device on the server.
Virtual power control	This function controls the power supply state of the management target server safely.

Main functions of iLO	Description
Deployment and provisioning	By using a GUI or CLI of the multiple tasks including automation of deployment or provisioning, you can use the power supply control and the virtual media.
Power consumption and settings	This function monitors the power consumption, sets the upper limit of the power consumption of the supported server.
User account	You can log in to iLO via a local or directory service user account.
Kerberos supported	You can set the Kerberos authentication here. The **Zero sign-in** button will be added to the login screen.

If you purchase the separately sold license, the following functions become available.

Item	On-board function	Extended license of remote management (Advanced) N8115-33	Extended license of remote management (Scale-out) N8115-34
Directory service authentication （Active Directory, LDAP）	×	○	×
Two-Factor authentication (Kerberos supported)	×	○	×
Use of virtual media through the integrated remote console	×	○	×
Scripted virtual media	×	○	×
Integrated remote console (IRC)	Pre-OS only	○	Pre-OS only
Global team collaboration through an IRC with up to six server administrators	×	○	×
Recording and playing back a video through an IRC	×	○	×
Recording and playing back a virtual serial port	×	○	○
Text-base remote console through SSH	×	○	○
E-mail alert	×	○	○
Remote Syslog	×	○	○
Advanced power management (graphic chart of electric power and upper limit setting of dynamic power consumption) *	×	○	○
iLO linkage management	×	○	○

Item	On-board function	Extended license of remote management (Advanced) N8115-33	Extended license of remote management (Scale-out) N8115-34
iLO linkage detection	○	○	○
Remote serial console (virtual serial port)	○	○	○
Server Health Summary	○	○	○
iLO restart	○	○	○
Redfish® API	○	○	○
Agentless Management	○	○	○
Server status monitoring	○	○	○
Web-base GUI	○	○	○
Virtual power control	○	○	○
SSH/SMASH CLI (including serial console redirection)	○	○	○
IPMI/DCMI (including serial console redirection)	○	○	○

* Some units may not be supported.

5.2 NMI Function

When the system hangs, the administrator may execute a memory dump by NMI.

Memory dump analysis is important for eliminating reliability issues such as hangs or crashes in OS, device drivers and applications.

If crashes occur frequently, the system may hang. In this case, the recovery action for administrators will be turning OFF/ON the system power (hard reset).

Although the information that supports root cause analysis will be erased when the system is reset, performing a memory dump by NMI before hard reset can protect these information.

The administrators can use the iLO Virtual NMI function to force the OS a memory dump by NMI.

If the OS crashes, a STOP error will occur on the system running Microsoft Windows. In this case, Microsoft recommends the system administrators to perform the NMI events. The hung system will respond once more by performing the NMI event.

Describes how to use the iLO Virtual NMI function.

1. Open under **Information** -> **Diagnostics** in the left side menu of the iLO5.

2. Click the **Generate NMI to System** button on **Non-Maskable Interrupt (NMI) Button**.

6. NEC ESMPRO

6.1 NEC ESMPRO ServerAgentService (for Windows)

For details of NEC ESMPRO ServerAgentService (for Windows), see "*NEC ESMPRO ServerAgentService Installation Guide (Windows)*" in Starter Pack.

6.2 NEC ESMPRO Manager

NEC ESMPRO Manager can remotely control and monitor the hardware and the RAID system of the server. To use these features, install the bundle software for the server such as NEC ESMPRO ServerAgentService.

For details, see "*NEC ESMPRO Manager Installation Guide*" or online help.

7. NEC Product Info Collection Utility

NEC Product Info Collection Utility can collect various data and logs related to the server all at once.

You can collect the server information (Product Info) for maintenance by using this utility.

7.1 Usage(for Windows)

Run the `\stdclct\collect.exe` contained in the installation folder of this utility.

This utility is usually installed to the `C:\ezclct` folder.

The `log` folder is created in the `stdclct` folder and “Product Info” is stored in a compressed (zip) file.

Tips

- Log on to Windows with an account that has an administrator privilege.
- The installation drive requires a free space of at least 2.5 GB.

8. Smart Storage Administrator

Smart Storage Administrator is an application to manage or monitor the following RAID controllers.

- Onboard RAID Controller
- N8103-189 RAID Controller (0GB, RAID 0/1)
- N8103-190 RAID Controller (2GB, RAID 0/1/5/6)
- N8103-191 RAID Controller (4GB, RAID 0/1/5/6)
- N8103-192 RAID Controller (0GB, RAID 0/1)
- N8103-193 RAID Controller (2GB, RAID 0/1/5/6)
- N8103-194 RAID Controller (4GB, RAID 0/1/5/6)
- N8103-195 RAID Controller (0GB, RAID 0/1)
- N8103-201 RAID Controller (2GB, RAID 0/1/5/6)
- N8103-196 RAID Controller (4GB, RAID 0/1/5/6)

See "*Installation Guide (Windows)*" for the installation of Smart Storage Administrator.

For more details on Smart Storage Administrator's operation method and function, see "*Smart Storage Administrator User's Guide*" on the following website.

NEC corporate site: http://www.nec.com/
[Products & Solutions]-[Servers]-[NEC Express5800 Server Series]-[Download]

9. Express Report Service / Express Report Service (HTTPS)

For details about Express Report Service / Express Report Service (HTTPS), see "*Express Report Service / Express Report Service (HTTPS) Installation Guide* (Windows)" in Starter Pack.

10. Express Report Service (MG)

Express Report Service (MG) installer and manual can be downloaded from the website below.

http://www.58support.nec.co.jp/global/download/index.html

For details about Express Report Service (MG), see “Express Report Service (MG) Installation Guide (Windows)”.

NEC Express5800 Series
Express5800/R120h-1M, R120h-2M

3

Appendix

1. **IML Error Message**
   A list on all error messages and error codes recorded in the Integrated Management Log (IML).

2. **List of Windows Event Logs**
   Shows a list of Windows event logs

3. **Accessing Data for Electrical Power, Temperature, and Processor Utilization**
   Describes how to check power consumption in watts, intake temperature, and logical processor utilizations.

4. **Glossary**

5. **Revision Record**

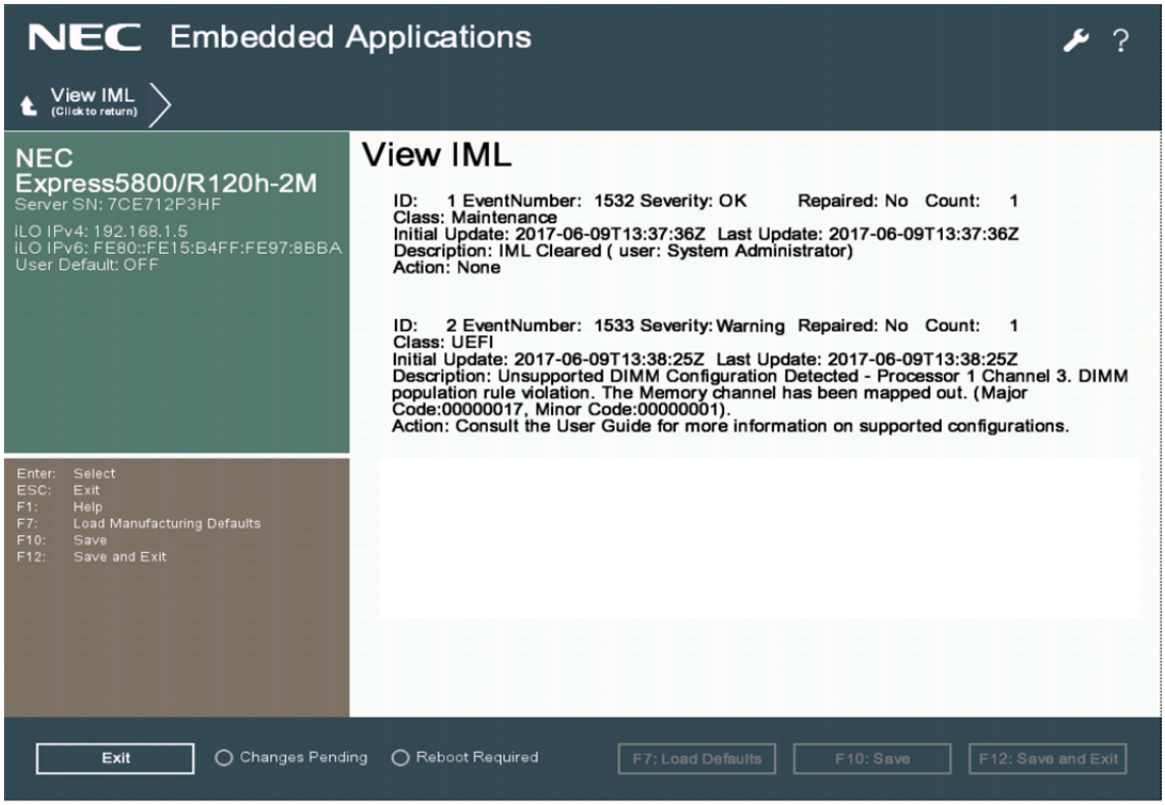
I. IML Error Message

A list on all error messages recorded in the Integrated Management Log (IML) and the error handling procedure. Depending on the system configuration and options, the recorded message varies. Therefore, error messages that are not displayed on the unit are also included in the list. In addition, messages which not showing errors, but only displaying information are included in the list.

Note

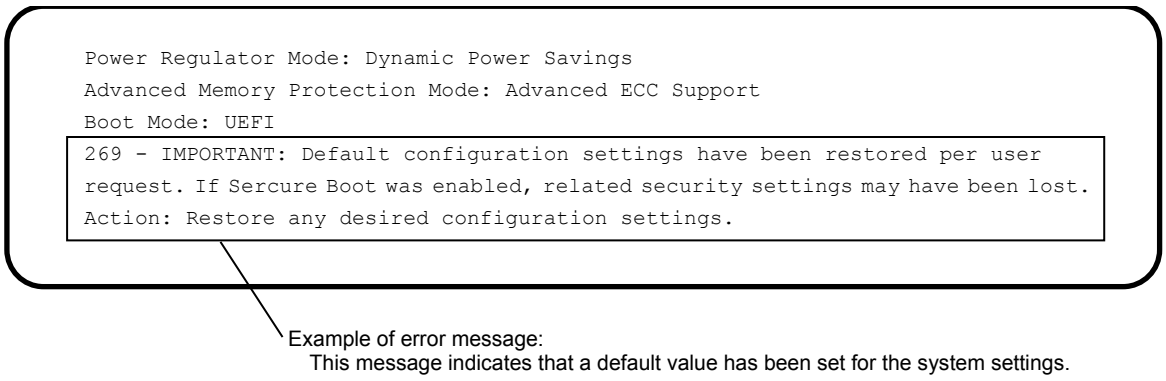
- For installing/ dismantling of options, refer to the user's guide of the device or the manuals of options.
- The contents of the list are subject to change without notice.
- In some cases, parts replacement is required to cope with a problem. Regarding the preparation of spare parts, ask the maintenance service company. In addition, in case trouble cannot be solved, ask the maintenance service company.

The message of the Integrated Management Log (IML) can be confirmed, such as via **Embedded Applications> Integrated Management Log (IML)** in the system utility.



The example of the IML error message display

Important messages for the errors detected by Integrated Management Log (IML) will be shown as you can see in the following example.



Example of error message:
This message indicates that a default value has been set for the system settings.

Tips

- When you call the maintenance service company, inform an error message. It can be useful information for maintenance.
- In the list below, messages outputted by the option are not included. For the messages which the options output, refer to the manuals of options.
- The list below includes entries composed of % and [number], such as %1, %2, %3, %4, etc., in error messages. When they are displayed, these entries are replaced by numbers or letters indicating details of situation.

(1) List on Error messages related to the operating environment of the server

Class	Error code	Error message	Action
Environment	13	System Overheating (Temperature Sensor %1, Location %2, Temperature %3)	Check the ambient temperature where the unit is being operated. If the problem persists, contact your sales representative.
Environment	14	External Chassis Overheating (Chassis %1, Temperature Sensor %2, Location %3, Temperature %4)	Check the ambient temperature where the expansion chassis connected to the unit is being operated. If the problem persists, contact your sales representative.
Environment	15	%1 Storage System Overheating (%2Slot %3, Temperature Sensor %4, Location %5, Temperature %6)	Check the ambient temperature where the %1 connected to the unit is being operated. If the problem persists, contact your sales representative.
Environment	16	%1 Overheating (Temperature Sensor %2, Location %3, Temperature %4, %5)	Check the ambient temperature where the %1 connected to the unit is being operated. If the problem persists, contact your sales representative.
Environment	17	Fan Failure (Fan %1, Location %2)	Contact your sales representative.
Environment	18	External Chassis Fan Failure (Chassis %1, Fan %2, Location %3)	Contact your sales representative.
Environment	19	%1 Storage System Fan Failure (%2 Slot %3, Fan %4, Location %5)	Contact your sales representative.
Environment	1A	%1 Fan Failure (Fan %2, Location %3, %4)	Contact your sales representative.
Environment	1B	System Fan Removed (Fan %1, Location %2)	Action is not necessary.
Environment	1C	External Chassis Fan Removed (Chassis %1, Fan %2, Location %3)	Action is not necessary.
Environment	1D	%1 Storage System Fan Removed (%2Slot %3, Fan %4, Location %5)	Action is not necessary.
Environment	1E	%1 Fan Removed (Fan %2, Location %3, %4)	Action is not necessary.
Environment	1F	System Fan Inserted (Fan %1, Location %2)	Action is not necessary.
Environment	20	External Chassis Fan Inserted (Chassis %1, Fan %2, Location %3)	Action is not necessary.
Environment	21	%1 Storage System Fan Inserted (%2Slot %3, Fan %4, Location %5)	Action is not necessary.

Class	Error code	Error message	Action
Environment	22	%1 Fan Inserted (Fan %2, Location %3, %4)	Disposal is not necessary.
Environment	23	System Fans Not Redundant (Location %1)	Contact your sales representative.
Environment	24	External Chassis Fans Not Redundant (Chassis %1, Location %2)	Contact your sales representative.
Environment	25	%1 Storage System Fans Not Redundant (%2Slot %3, Location %4)	Contact your sales representative.
Environment	26	%1 Fans Not Redundant (Location %2, %3)	Contact your sales representative.
Environment	27	Critical Temperature Threshold Exceeded	Check the ambient temperature where the unit is being operated. If the problem persists, contact your sales representative.
Environment	28	Critical Temperature Threshold Exceeded (Temperature Sensor %1, Location %2, Temperature %3C %4)	Check the ambient temperature where the unit is being operated. If the problem persists, contact your sales representative.
Environment	29	External Chassis Overheating (Chassis %1, Temperature Sensor %2, Location %3, Temperature %4)	Check the ambient temperature where the expansion chassis connected to the unit is being operated. If the problem persists, contact your sales representative.
Environment	2A	%1 Storage System Overheating (%2Slot %3, Temperature Sensor %4, Location %5, Temperature %6)	Check the ambient temperature where the %1 connected to the unit is being operated. If the problem persists, contact your sales representative.
Environment	2B	%1 Overheating (Temperature Sensor %2, Location %3, Temperature %4, %5)	Check the ambient temperature where the %1 connected to the unit is being operated. If the problem persists, contact your sales representative.
Environment	2C	Temperature exceeded on PCIe disk %1.	Contact your sales representative.
Environment	2D	Intrusion Alert Hardware installed.	No additional action is required, if the applicable HW has been added. If the problem persists, contact your sales representative.
Environment	2E	#ILO had detected the removal of the Intrusion Alert hardware.	No additional action is required, if the applicable HW has been removed. If the problem persists, contact your sales representative.

Class	Error code	Error message	Action
Environment	2F	Intrusion Alert Detection - The server chassis hood is currently not installed.	The cover of the unit has been removed. Please attach the cover. If it is not a record of the intended operation, the security of the unit may have been compromised. Please take an appropriate measure. If the problem persists, contact your sales representative.
Environment	30	The chassis hood has been replaced.	It detected that the cover of the unit has been removed. If it is not a record of the intended operation, the security of the unit may have been compromised. Please take an appropriate measure. If the problem persists, contact your sales representative.
Environment	31	%1 Storage Enclosure Fan Failure (Fan %2, Location %3, Box %4, %5)	Contact your sales representative.
Environment	32	%1 Storage Enclosure Overheating (Temperature Sensor %2, Location %3, Box %4, %5)	Contact your sales representative.
Environment	33	Fan Degraded (Fan %1, Location %2)	Contact your sales representative.
Environment	34	Insufficient Fan Solution	Check the FAN connected to the server. If the problem persists, contact your sales representative.
Environment	35	Insufficient power supply configuration.	From the LED indicator of PSU or the connection of AC cord, confirm whether electricity is supplied to the PSU of device. If it occurs directly after the change of configuration, confirm whether it is beyond the supply capacity of PSU due to addition or change of components. In case a problem is not resolved, call the maintenance service company.

(2) The list on the messages related to processor, UPI bus, and PCIe bus

Class	Error code	Error message	Action
CPU	3	Uncorrectable Machine Check Exception (Processor %2, APIC ID 0x%3, Bank 0x%4, Status 0x%5'%6, Address 0x%7'%8, Misc 0x%9'%10).	Contact your sales representative.
Host Bus	3	Uncorrectable UPI Error was detected on Processor %1	Contact your sales representative.
PCI Bus	2	Uncorrectable PCI Express Error Detected. Slot %1 (Segment %2, Bus %3, Device %4, Function %5). Uncorrectable Error Status: %6	Contact your sales representative.
PCI Bus	3	Uncorrectable PCI Express Error Detected. Embedded %1 (Segment %2, Bus %3, Device %4, Function %5). Uncorrectable Error Status: %6	Contact your sales representative.
PCI Bus	4	Uncorrectable PCI Express Error Detected. Slot %1 (Segment %2, Bus %3, Device %4, Function %5).	Contact your sales representative.

(3) The list on the messages related to POST

Class	Error code	Error message	Action
UEFI	101	Option ROM Error. An option ROM for a PCIe device is invalid.	Contact your sales representative.
UEFI	104	ASR Timer Failure	Contact your sales representative.
UEFI	121	A Critical Error occurred prior to this power-up.	Contact your sales representative.
UEFI	218	DIMM Initialization Error - All DIMMs are mapped out due to memory errors except for one to allow the system to boot. Additional errors may be present on the remaining DIMM. System is booting in a degraded state.	Contact your sales representative.
UEFI	224	Power Fault Detected - FlexLOM %1	Turn off the power on the unit, disconnect the power cord, and check the installation of FlexLOM %1. Wait 30 seconds, and then restart it. If the problem persists, contact your sales representative.
UEFI	225	Power Fault Detected-Mezzanine %1.	Turn off the power on the unit, disconnect the power cord, and check the installation of mezzanine %1. Wait 30 seconds, and then restart it. If the problem persists, contact your sales representative.

Class	Error code	Error message	Action
UEFI	226	Power Fault Detected - Embedded Storage Controller %1.	Turn off the power on the unit, disconnect the power cord, and check the installation of internal storage controller %1. Wait 30 seconds, and then restart it. If the problem persists, contact your sales representative.
UEFI	227	Power Fault Detected - M.2 riser	Turn off the power on the unit, disconnect the power cord, and check the installation of M.2 riser. Wait 30 seconds, and then restart it. If the problem persists, contact your sales representative.
UEFI	244	IMPORTANT: The device in PCIe Slot %1 is SRIOV capable but is installed in a slot that does NOT support SRIOV.	When using the SRIOV, install an optional card in the slot where the SRIOV is supported. If the problem persists, contact your sales representative.
UEFI	251	IMPORTANT: Switches SW1 and SW3 are ON. This is only used to recover %1 functionality.	Set the maintenance switch to OFF unless the setting is specified in the operating procedure etc. When operating the maintenance switch, follow the procedure in *Chapter 1 (7. Resetting and Clearing the Server)* in this manual. If the problem persists, contact your sales representative.
UEFI	253	IMPORTANT: One or more embedded PCIe Device(s) are attached to a non-installed processor and will not function.	Some built-in devices are not available unless the processor is added. Add a processor if necessary. If the problem persists, contact your sales representative.
UEFI	254	IMPORTANT: The PCIe Device installed in Slot %1 has no corresponding processor installed and will not function.	The optional card is connected to a PCIe slot that is not available unless a processor is added. Change the slot which the PCIe expansion card is connected to, otherwise add a processor. If the problem persists, contact your sales representative.
UEFI	261	Server Platform Services Firmware requires update.	Update the server platform service firmware. If the problem persists, contact your sales representative.
UEFI	264	Server Platform Services Firmware in Recovery Mode. SPS Firmware Update Switch 12 of the Maintenance Switch is in the ON position.	Set the maintenance switch SW12 to OFF unless the setting is specified in the operating procedure etc. When operating the maintenance switch, follow the procedure in *Chapter 1 (7. Resetting and Clearing the Server)* in this manual. If the problem persists, contact your sales representative.
UEFI	266	Non-Volatile Memory Corruption Detected. Configuration settings restored to defaults. If enabled, Secure Boot security settings may be lost.	The system configuration has been initialized to default. Make the necessary settings in the system utility. If the problem persists, contact your sales representative.
UEFI	267	IMPORTANT: Default configuration settings have been restored at the request of the user.	The system configuration has been initialized to default. Make the necessary settings in the system utility. If the problem persists, contact your sales representative.

Class	Error code	Error message	Action
UEFI	268	UEFI Non-Volatile Variable Store Corruption Detected. If enabled, Secure Boot security settings may be lost.	The system configuration has been initialized to default. Make the necessary settings in the system utility. If the problem persists, contact your sales representative.
UEFI	269	IMPORTANT: Default configuration settings have been restored per user request. If Secure Boot was enabled, related security settings may have been lost.	The system configuration has been initialized to default. Make the necessary settings in the system utility. If the problem persists, contact your sales representative.
UEFI	270	%1 FW Communication Issue - Unable to communicate with %2 FW. Certain management functionality is not available.	Turn off the unit, disconnect the power cord, wait 30 seconds, and then restart it. If the problem persists, contact your sales representative.
UEFI	271	Processor %1, DIMM %2 could not be authenticated as genuine %3. Enhanced and extended %4 features will not be active.	The DIMM failed to be authenticated as an authorized part. Check the DIMM connected to the unit. If the problem persists, contact your sales representative.
UEFI	272	IMPORTANT: Processor %1, DIMM %2 may not be a Genuine %3 DIMM.	The DIMM failed to be authenticated as an authorized part. Check the DIMM connected to the unit. If the problem persists, contact your sales representative.
UEFI	276	Option Card Configuration Error. An option card is requesting more memory mapped I/O than is available.	The memory space for the optional card failed to be allocated. Remove the added optional card so that the system can be booted. If the problem persists, contact your sales representative.
UEFI	277	Secure Boot Authentication Failure - The image on %1 failed authentication and was not executed.	If the error occurs due to adding of the optional card, check whether the added card supports the secure boot. If the problem persists, contact your sales representative.
UEFI	278	Secure Boot Authentication Failure - The image on %1 was not authorized due to revoked certificate(s) and was not executed.	If the error occurs due to adding an optional card, make sure whether the added card meets the conditions required for secure boot. If the problem persists, contact your sales representative.
UEFI	281	IMPORTANT: SW12 is ON indicating physical presence. This switch should only be ON to override certain security protections.	Set the maintenance switch SW12 to OFF unless the setting is specified in the operating procedure etc. When operating the maintenance switch, follow the procedure in *Chapter 1 (7. Resetting and Clearing the Server)* in this manual. If the problem persists, contact your sales representative.
UEFI	282	Invalid Server Serial Number and Product ID - The Serial Number and/or Product ID have been corrupted or lost.	The serial number and product ID for identifying the unit are not correctly set. Contact your maintenance service company.
UEFI	284	DIMM Failure - Uncorrectable Memory Error - Processor %1 Dimm %2	Contact your sales representative.

Class	Error code	Error message	Action
UEFI	286	IMPORTANT: The removal of a storage device has been detected. The device has been removed from the Boot Controller Order.	Action is not necessary.
UEFI	287	IMPORTANT: The removal of a network device has been detected. The device has been removed from the Standard Boot Order (IPL)	Action is not necessary.
UEFI	288	IMPORTANT: A new storage device has been detected and has been added to the end of the Boot Controller Order.	Action is not necessary.
UEFI	289	A new network or storage device has been detected. This device will not be shown in the Legacy BIOS Boot Order options in RBSU until the system has booted once.	Action is not necessary.
UEFI	291	IMPORTANT: The Standard Boot Order (IPL) has been detected as corrupted and has been restored to default values.	Action is not necessary.
UEFI	292	Invalid %1 Software RAID Configuration. %2 SW RAID Mode is NOT supported when the Boot Mode is configured for legacy BIOS Mode.	When using the corresponding Software RAID, the boot mode must be changed to the UEFI mode. If the problem persists, contact your sales representative.
UEFI	297	IMPORTANT: iLO Security is disabled by the associated switch being set to the ON position. Platform security is DISABLED.	The maintenance switch SW1 should be set to OFF unless the setting is specified in the operating procedure etc. When operating the maintenance switch, follow the procedure in *Chapter 1 (7. Resetting and Clearing the Server)* in this manual. If the problem persists, contact your sales representative.
UEFI	311	%1 Configuration Error - The system has exceeded the installed battery capacity.	Add more batteries for the capacity increase, or reduce the number of devices that need battery backup. If the problem persists, contact your sales representative.
UEFI	312	%1 %2 Failure - Communication with the battery failed. Its output may not be enabled.	Make sure that the battery is correctly installed. If the problem persists, contact your sales representative.
UEFI	313	%1 %2 Failure - Battery Shutdown Event Code: 0x%3.	Restart the server. If the problem persists, contact your sales representative.
UEFI	315	An uncorrectable memory error was detected prior to this system boot.	Contact your sales representative.
UEFI	319	An Unexpected Shutdown was detected prior to this boot.	Action is not necessary.
UEFI	320	Enclosure Power Event detected. Boot delayed until condition is resolved.	Action is not necessary.

Class	Error code	Error message	Action
UEFI	321	%1 Dual microSD Device Unsupported Configuration - A microSD card is not installed in Slot %2	Make sure whether the corresponding microSD card is correctly mounted. If the problem persists, contact your sales representative.
UEFI	322	%1 Dual microSD Device Unsupported Configuration - No microSD cards are installed.	Make sure whether the corresponding microSD card is correctly mounted. If the problem persists, contact your sales representative.
UEFI	323	%1 Dual microSD Device Error - The microSD card in Slot %2 has failed.	Contact your sales representative.
UEFI	324	%1 Dual microSD Device Error - Both microSD cards have failed.	Contact your sales representative.
UEFI	325	%1 Dual microSD Device Error - microSD cards have conflicting metadata. Configuration required.	Use the system utility to set up the primary microSD card. If the problem persists, contact your sales representative.
UEFI	326	%1 Dual microSD Device Error - The microSD card in Slot %2 has failed. A microSD card is not installed in Slot %3.	Contact your sales representative.
UEFI	327	AMP Configuration Error - An installed processor does NOT support the configured AMP Mode. System will operate in Advanced ECC Mode.	Contact your sales representative.
UEFI	328	Power Management Controller Firmware Error - The firmware is in Recovery Mode.	Update the firmware of the power management controller. If the problem persists, contact your sales representative.
UEFI	329	Power Management Controller FW Error - Unable to communicate with the FW.	Please take actions in the following order. 1. Turn off the unit, disconnect the power cord, wait 30 seconds, and then restart it. 2. If the problem persists, contact your sales representative.
UEFI	333	%1 RESTful API Error - Unable to communicate with iLO FW. BIOS configuration resources may not be up-to-date.	Please take actions in the following order. 1. Reset the iLO following the procedure of *Chapter 1 (7. Resetting and Clearing the Server)* in this manual. Also, restart the unit. 2. If the problem persists, turn off the power of the unit, disconnect the power cord, wait 30 seconds, and then restart it. 3. If the problem persists, contact your sales representative.

Class	Error code	Error message	Action
UEFI	334	%1 RESTful API Error - RESTful API GET request failed (HTTP Status Code = %2). BIOS configuration resources were not consumed.	Please take actions in the following order. 1. Turn off the unit, disconnect the power cord, wait 30 seconds, and then restart it. 2. If the problem persists, reset the iLO following the procedure in *Chapter 1 (7. Resetting and Clearing the Server)* in this manual. 3. If the problem persists, updating the iLO firmware/system ROM may solve the problem. Update the iLO firmware/system ROM. 4. If the problem persists, contact your sales representative.
UEFI	335	%1 RESTful API Error - RESTful API PUT request failed (HTTP Status Code = %2). BIOS configuration resources may not be up-to-date.	Please take actions in the following order. 1. Turn off the unit, disconnect the power cord, wait 30 seconds, and then restart it. 2. If the problem persists, reset the iLO following the procedure in *Chapter 1 (7. Resetting and Clearing the Server)* in this manual. 3. If the problem persists, updating the iLO firmware/system ROM may solve the problem. Update the iLO firmware/system ROM. 4. If the problem persists, contact your sales representative.
UEFI	336	%1 RESTful API Error - One or more configuration settings could not be applied.	Refer to the SettingsResult property of RESTful API to check the setting contents. If the problem persists, contact your sales representative.
UEFI	337	%1 RESTful API Error - Unable to communicate with %2 FW due to Datacenter Configuration Lock being enabled. BIOS configuration resources may not be up-to-date.	Disable data center configuration lock. If the problem persists, contact your sales representative.
UEFI	338	%1 RESTful API Error - Unable to communicate with iLO FW. BIOS configuration resources may not be up-to-date.	Restore the factory default settings using the **Restore Default Manufacturing Settings** option via **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **System Default Options** in the system utility. If the problem persists, contact your sales representative.
UEFI	340	NVDIMM Error - Backup Error - Processor %1, DIMM %2 (SN:%3-%4-%5-%6). Persistent data backup failed and data is irrecoverably lost.	Contact your sales representative.
UEFI	341	NVDIMM Error - Restore Error - Processor %1, DIMM %2 (SN:%3-%4-%5-%6). Persistent data restore failed and data is not available. Data is not lost unless the issue persists.	Contact your sales representative.

Class	Error code	Error message	Action
UEFI	342	NVDIMM Error - Uncorrectable Memory Error - Processor %1, DIMM %2 (SN:%3-%4-%5-%6). This NVDIMM will not be available to the operating system and data may have been lost.	Contact your sales representative.
UEFI	343	IMPORTANT: NVDIMM backup power has been lost and a future backup is not possible. Data from the last successful backup is intact, but data modified after the last successful backup will be lost if power cannot be restored.	Check the backup power supply of the NVDIMM. Back up the contents recorded in the NVDIMM to other media to protect the data. If the problem persists, contact your sales representative.
UEFI	344	NVDIMM Error - NVDIMM Controller Error - Processor %1, DIMM %2 (SN:%3-%4-%5-%6). An error was found with the NVDIMM controller. The OS will not use the NVDIMM. Data from last successful backup is still available, but will be lost if controller error persists.	Please take actions in the following order. 1. Back up the contents recorded in the NVDIMM to other media to protect the data. 2. Contact your sales representative.
UEFI	345	NVDIMM Error - Erase Error - Processor %1, DIMM %2 (SN:%3-%4-%5-%6). NVDIMM could not be erased by the NVDIMM controller FW and future backups are not possible.	Please take actions in the following order. 1. Back up the contents recorded in the NVDIMM to other media to protect the data. 2. Contact your sales representative.
UEFI	346	NVDIMM Error - Arming Error - Processor %1, DIMM %2 (SN:%3-%4-%5-%6). NVDIMM could not be armed and future backups are not possible.	Please take actions in the following order. 1. Back up the contents recorded in the NVDIMM to other media to protect the data. 2. Contact your sales representative.
UEFI	351	IMPORTANT: %1 is not charged sufficiently to support the energy-backed persistent memory installed in the system. The system will wait for the battery to charge sufficiently before continuing boot.	Perform one of the following actions. 1. Wait until the battery is fully charged so that the unit can continue to be operated. 2. Press the <ESC> key to continue operating without waiting for the battery fully charged.
UEFI	352	IMPORTANT: %1 is not charged sufficiently to support the energy-backed persistent memory installed in the system. System configured to not wait for battery to charge. Persistent memory regions may not be available in the OS.	Perform one of the following actions. 1. Wait until the battery is fully charged so that the unit can continue to be operated. 2. Change to the setting where the unit operation is suspended until the battery is fully charged.
UEFI	353	IMPORTANT: Possible Password Corruption. The PW authentication algorithm detected an issue which has been corrected.	Reset your password. To clear the currently set password, follow the procedure in *Chapter 1 (7. Resetting and Clearing the Server)* in this manual. If the problem persists, contact your sales representative.

Class	Error code	Error message	Action
UEFI	354	Unsupported NVDIMM-N Configuration Detected - Processor %1 DIMM %2. The installed NVDIMM-N is not supported.	A connection of unavailable NVDIMM-N has been detected. Check the installation of the NVDIMM - N. If the problem persists, contact your sales representative.
UEFI	355	IMPORTANT: Processor %1, DIMM %2 - This NVDIMM-N was selected for Sanitizing/Erasing. All data saved in the NVDIMM has been erased.	Action is not necessary.
UEFI	356	NVDIMM Error - Sanitization Error - Processor %1, DIMM %2 (SN:%3-%4-%5-%6) - This NVDIMM-N was selected for Sanitizing/Erasing, but this process was not successful.	Please take actions in the following order. 1. Restart sanitization of the NVDIMM. 2. Contact your sales representative.
UEFI	357	IMPORTANT: Processor %1, DIMM %2 - This NVDIMM is NOT a %3 NVDIMM. Only %4 NVDIMMs are supported. NVDIMM will be used as a standard DIMM.	Contact your sales representative.
UEFI	360	IMPORTANT: The System Programmable Logic Device revision in this system does not meet minimum requirements for operation with NVDIMMs. All NVDIMM functionality has been disabled.	Update the system programmable logic device. If the problem persists, contact your sales representative.
UEFI	361	IMPORTANT: The Processor RAPL wattage value is configured to an invalid value. User provided value was %1, but %2 has been assigned since it is closest to %3.	Please take actions in the following order. 1. Set an appropriate value for **Processor RAPL wattage value**. 2. If the problem persists, contact your sales representative.
UEFI	362	IMPORTANT: The DRAM RAPL wattage value is configured to an invalid value. User provided value was %1, but %2 has been assigned since it is closest to %3.	Please take actions in following order. 1. Set an appropriate value for **DRAM RAPL wattage value**. 2. If the problem persists, contact your sales representative.
UEFI	363	IMPORTANT: New NVDIMM(s) detected on Processor %1. All NVDIMMs on Processor %2 have been disabled.	Sanitize the NVDIMM connected to the corresponding processor. If the problem persists, contact your sales representative.
UEFI	364	NVDIMM Error - NVDIMM Controller Error - Processor %1, DIMM %2. The controller firmware has been corrupted. The OS will not use the NVDIMM.	Please take actions in following order. 1. Update the NVDIMM firmware. 2. Contact your sales representative.

Class	Error code	Error message	Action
UEFI	371	IMPORTANT: Processor %1, DIMM %2. New NVDIMM detected and has been disabled.	Sanitize the NVDIMM connected to the corresponding processor. If the problem persists, contact your sales representative.
UEFI	372	IMPORTANT: Processor %1, DIMM %2. New NVDIMM detected and has been disabled.	Sanitize the NVDIMM connected to the corresponding processor. If the problem persists, contact your sales representative.
UEFI	373	IMPORTANT: NVDIMM(s) have been removed from Processor %1. All NVDIMMs on Processor %2 have been disabled.	Please take actions in following order. 1. Sanitize the NVDIMM connected to the corresponding processor. 2. If the problem persists, contact your sales representative.
UEFI	374	NVDIMM Error - Processor %1, DIMM %2 (SN:%3-%4-%5-%6) received a memory initialization or uncorrectable error. All NVDIMMs on Proc %7 are disabled. Data on NVDIMM may have been lost	Please take actions in following order. 1. Sanitize the NVDIMM. 2. Contact your sales representative.
UEFI	375	NVDIMM Error - Processor %1, DIMM %2 (SN:%3-%4-%5-%6) received a memory initialization or uncorrectable error. All NVDIMMs on Proc %7 are disabled. Data on NVDIMM may have been lost.	Please take actions in following order. 1. Sanitize the NVDIMM. 2. Contact your sales representative.
UEFI	376	NVDIMM Error - Processor %1, DIMM %2. NVDIMM set for interleaving disabled but system configured for interleaving enabled. All NVDIMMs on Processor %3 are disabled.	Set **NVDIMM Interleaving** to **Disabled**, or sanitize the NVDIMM. If the problem persists, contact your sales representative.
UEFI	377	NVDIMM Error - Processor %1, DIMM %2. NVDIMM set for interleaving enabled but system configured for interleaving disabled. NVDIMM has been disabled.	Set **NVDIMM Interleaving** to **Enabled**, or sanitize the NVDIMM. If the problem persists, contact your sales representative.
UEFI	378	NVDIMM Error - Processor %1, DIMM %2. NVDIMM is configured for a different processor type. All NVDIMMs on Processor %3 are disabled.	Sanitize the NVDIMM. If the problem persists, contact your sales representative.
UEFI	379	NVDIMM Error - Processor %1, DIMM %2. NVDIMM is configured for a different processor type. NVDIMM has been disabled.	Sanitize the NVDIMM. If the problem persists, contact your sales representative.
UEFI	380	NVDIMM Error - Processor %1, DIMM %2. NVDIMM location changed. All NVDIMMs on Processor %3 are disabled.	Install the NVDIMM in the corresponding DIMM slot, or sanitize the NVDIMM. If the problem persists, contact your sales representative.
UEFI	381	NVDIMM Error - Processor %1, DIMM %2. NVDIMM location changed. NVDIMM has been disabled.	Install the NVDIMM in the corresponding DIMM slot, or sanitize the NVDIMM. If the problem persists, contact your sales representative.

Class	Error code	Error message	Action
UEFI	382	NVDIMM Error - Proc %1, DIMM %2 is NOT configured for Sub-NUMA Clustering but system is configured for Sub-NUMA Clustering. All NVDIMMs on Proc %3 are disabled.	Set **Sub-Numa Clustering** to **Disabled**, or sanitize the NVDIMM. If the problem persists, contact your sales representative.
UEFI	383	NVDIMM Error - Proc %1, DIMM %2 is configured for Sub-NUMA Clustering but system is NOT configured for Sub-NUMA Clustering. All NVDIMMs on Proc %3 are disabled.	Set **Sub-Numa Clustering** to **Enabled**, or sanitize the NVDIMM. .If the problem persists, contact your sales representative.
UEFI	384	NVDIMM Error - Processor %1, DIMM %2. NVDIMM set for Channel Interleaving disabled but system configured for enabled. All NVDIMMs on Processor %3 are disabled.	Set **Channel Interleaving** to **Disabled**, or sanitize the NVDIMM. If the problem persists, contact your sales representative.
UEFI	385	NVDIMM Error - Processor %1, DIMM %2. NVDIMM set for Channel Interleaving enabled but system configured for disabled. All NVDIMMs on Processor %3 are disabled.	Set **Channel Interleaving** to **Enabled**, or sanitize the NVDIMM. If the problem persists, contact your sales representative.
UEFI	386	NVDIMM Error - Processor %1, DIMM %2. NVDIMM Metadata is corrupted. All NVDIMMs on Processor %3 are disabled.	Sanitize the NVDIMM. If the problem persists, contact your sales representative.
UEFI	387	NVDIMM Error - Processor %1, DIMM %2. NVDIMM Metadata is corrupted. NVDIMM is disabled.	Sanitize the NVDIMM. If the problem persists, contact your sales representative.
UEFI	388	Uncorrectable Memory Error - The failed memory module could not be determined.	Contact your sales representative.
UEFI	391	NVDIMM Configuration Error - Node Interleaving is Enabled. This is NOT supported with NVDIMMs installed. All NVDIMMs are disabled.	Set **Node Interleaving** to **Disabled**. If the problem persists, contact your sales representative.
UEFI	392	NVDIMM Configuration Error - The Advanced Memory Protection mode is not Advanced ECC. Only Advanced ECC is supported with NVDIMMs. All NVDIMMs are disabled.	Set **Advanced Memory Protection** to **Advanced ECC Support**. If the problem persists, contact your sales representative.
UEFI	393	IMPORTANT: New NVDIMM(s) detected and all NVDIMMs have been disabled.	Sanitize the NVDIMM. If the problem persists, contact your sales representative.

Class	Error code	Error message	Action
UEFI	394	NVDIMM Error - Processor %1, DIMM %2 (SN:%3-%4-%5-%6). Unable to set event notification for this NVDIMM to generate alerts for health changes, including a loss of data persistency.	Updating the system ROM and the innovation engine firmware may solve the error. Please update the system ROM and the innovation engine firmware. If the problem persists, contact your sales representative.
UEFI	395	NVDIMM Error - Processor %1, DIMM %2 (SN:%3-%4-%5-%6). NVDIMM Persistency is lost and future data backup is not available.	Please take actions in following order. 1. Back up the contents recorded in the NVDIMM to other media to protect the data. 2. Contact your sales representative.
UEFI	396	IMPORTANT: Processor %1, DIMM %2 - NVDIMM Persistency is restored and future data backup is available.	Action is not necessary.
UEFI	397	WARNING: Processor %1, DIMM %2 (SN:%3-%4-%5-%6). NVDIMM lifetime has reached.	Please take actions in following order. 1. Back up the contents recorded in the NVDIMM to other media to protect the data. 2. Contact your sales representative.
UEFI	398	NVDIMM Configuration Error - Processor %1, DIMM %2 (SN:%3-%4-%5-%6). Backup power is not available to this DIMM slot. NVDIMM is disabled.	Install the NVDIMM in the slot where the NVDIMM is available. If the problem persists, contact your sales representative.
UEFI	399	INFORMATION: Processor %1, DIMM %2 (SN:%3-%4-%5-%6). Extended Diagnostic Information (Data1 = 0x%7, Data2 = 0x%8, Data3 = 0x%9, Data4 = 0x%10).	Action is not necessary. However, if the error is recorded repeatedly, please contact your sales representative.
UEFI	400	Intrusion Alert Detection - The server chassis hood is currently not installed.	An intrusion warning has been detected. The cover of the server has not been installed. Check the installation of the cover. If the problem persists, contact your sales representative.
UEFI	401	Intrusion Alert Detection - The server chassis hood was removed prior to this power on.	An intrusion warning has been detected. It detected that the server cover has been once removed. Check the status of the server. If the problem persists, contact your sales representative.
UEFI	402	Intrusion Alert Detection - The required intrusion detection cable is missing.	An intrusion warning has been detected. The intrusion detection cable is not connected. Check the status of the server. If the problem persists, contact your sales representative.
UEFI	403	Intrusion Alert Configuration Error - Intrusion Alert Detection cable is installed but the feature is not enabled.	An intrusion warning has been detected. While the intrusion detection cable has been connected, its function is not enabled. Check the settings of the server. If the problem persists, contact your sales representative.

Class	Error code	Error message	Action
UEFI	410	Innovation Engine Error - The Innovation Engine is not operating properly. (Error Code %1).	Updating the system ROM and the innovation engine firmware may solve the error. Please update the system ROM and the innovation engine firmware. If the problem persists, contact your sales representative.
UEFI	411	Innovation Engine Error - The Innovation Engine is operating in recovery mode.	Set the maintenance switch SW12 to OFF unless the setting is specified in the operating procedure etc. When operating the maintenance switch, follow the procedure in *Chapter 1 (7. Resetting and Clearing the Server)* in this manual. If the problem persists, contact your sales representative.
UEFI	414	Server Platform Services Firmware Error - The SPS Firmware is not operating properly. (Error Code %1).	Updating the latest server platform service firmware may solve the error. Please update the server platform service firmware. If the problem persists, contact your sales representative.
UEFI	420	TLS certificate verification error 0x%1 while downloading from %2:%3.	Register the certificate required for authentication, and check the TLS setting.
UEFI	421	TLS certificate verification failed due to hostname mismatch.	Check whether the certificate required for authentication has been registered, or check the TLS setting.
UEFI	422	TLS certificate verification failed. The passed certificate is self-signed and the same certificate cannot be found in the list of trusted certificates.	Check whether the certificate required for authentication has been registered, or check the TLS setting.
UEFI	423	TLS certificate verification failed. The issuer certificate of a looked up certificate could not be found. This normally means the list of trusted certificates is not complete.	Check whether the certificate required for authentication has been registered, or check the TLS setting.
UEFI	424	No TLS certificate enrolled. At least one certificate authority must be enrolled when TLS verification mode is set to PEER.	Register the certificate required for authentication, and check the TLS setting.
UEFI	430	Scalable Persistent Memory uncorrectable memory error on %1 Logical NVDIMM %2. The memory region will not be available to the OS and data may have been lost.	Contact your sales representative.
UEFI	431	Scalable Persistent Memory backup failed on %1 Logical NVDIMM %2. Persistent data has been lost.	Contact your sales representative.
UEFI	432	Scalable Persistent Memory restore failed for %1 Logical NVDIMM %2. Persistent data may have been lost.	Contact your sales representative.

Class	Error code	Error message	Action
UEFI	433	Scalable Persistent Memory backup device failure on Box %1 Bay %2. Persistent data may have been lost.	Please take actions in following order. 1. Back up the contents recorded in the persistent memory to other media to protect the data. 2. Contact your sales representative.
UEFI	434	Scalable Persistent Memory configuration data on backup device Box %1 Bay %2 is invalid. Persistent data may be lost.	Reinitialize the backup device of Box %1, Bay %2. If the problem persists, contact your sales representative.
UEFI	435	Scalable Persistent Memory backup device on Box %1 Bay %2 is missing.	Contact your sales representative.
UEFI	437	Scalable Persistent Memory backup media write error on %1 Logical NVDIMM %2. Persistent data may have been lost.	Contact your sales representative.
UEFI	438	Scalable Persistent Memory backup media read error on %1 Logical NVDIMM %2. Persistent data may have been lost.	Contact your sales representative.
UEFI	439	New Scalable Persistent Memory configuration rejected. System has reverted to the previous configuration.	Review the setting of the persistent memory. If the problem persists, contact your sales representative.
UEFI	440	Persistent Memory Address Range Scrub has detected an error at 0x%1'%2.	Contact your sales representative.
UEFI	441	NVDIMM Configuration Error - Scalable Persistent Memory functionality is not supported when NVDIMM-N is present in the system. Scalable Persistent Memory functionality has been disabled.	When using the persistent memory, remove the NVDIMM-N from the server. If the problem persists, contact your sales representative.
UEFI	442	Scalable Persistent Memory backup media write error on Box %1 Bay %2. Persistent data may have been lost.	Contact your sales representative.
UEFI	443	Scalable Persistent Memory backup media read error on Box %1 Bay %2. Persistent data may have been lost.	Contact your sales representative.
UEFI	444	Scalable Persistent Memory arming error on %1, Logical NVDIMM %2. The Logical NVDIMM could not be armed and future backups are not possible.	Back up the contents recorded in the non-volatile memory of the NVDIMM to other media. Contact your sales representative.
UEFI	445	Scalable Persistent Memory backup device error on Box %1 Bay %2.	Contact your sales representative.

Class	Error code	Error message	Action
UEFI	446	IMPORTANT: The Scalable Persistent Memory backup power requirements have exceeded the available backup battery power. Logical NVDIMM persistency has been lost.	Contact your sales representative.
UEFI	447	IMPORTANT: %1 is not charged sufficiently to support the energy-backed persistent memory installed in the system. The charging process was skipped by the user. Persistent memory regions may not be available in the OS.	Depending on the situation, reboot the device. If a continuous recording is a problem, contact your sales representative.
UEFI	448	IMPORTANT: %1 is not charged sufficiently to support the energy-backed persistent memory installed in the system. The charging process timed out and did not complete. Persistent memory regions may not be available in the OS.	Reboot the device. If a continuous recording is a problem, contact your sales representative.
UEFI	449	Scalable Persistent Memory Address Range Scrub error threshold exceeded on %1, Logical NVDIMM %2. Logical NVDIMM Persistency is lost and future data backups are not possible.	Contact your sales representative.
UEFI	451	Unsupported NVDIMM-N Configuration Detected - Processor %1 DIMM %2. The installed NVDIMM-N is not supported.	A connection of unavailable NVDIMM-N has been detected. Updating the system ROM may solve the error. Please update the system ROM. If the problem persists, contact your sales representative.
UEFI	452	%1 FW Communication Issue - Unable to communicate with %2 FW. One or more configuration settings may be used from the last system boot. One or more configuration changes since the last boot may not have taken affect.	Please take actions in following order. 1. Turn off the unit, disconnect the power cord, wait 30 seconds, and then restart it. 2. If the problem persists, updating the corresponding firmware may solve the error. Please update the corresponding firmware. 3. If the problem persists, contact your sales representative.
UEFI	454	NVDIMM Error - Persistent Memory Address Range Scrub error threshold exceeded on Processor %1, DIMM %2 (SN:%3-%4-%5-%6). NVDIMM Persistency is lost and future data backups are not possible.	Contact your sales representative.
UEFI	455	IMPORTANT: The %1 in Bay %2 will soon be incapable of supporting the Scalable Persistent Memory backup.	Contact your sales representative.
UEFI	456	IMPORTANT: The %1 in Bay %2 cannot support the Scalable Persistent Memory backup. Logical NVDIMM persistency has been lost.	Contact your sales representative.
UEFI	460	Correctable Memory Error Threshold Exceeded (%1 %2, DIMM %3).	Contact your sales representative.
UEFI	461	High rate of corrected memory errors, performance may be degraded (%1 %2, DIMM %3).	Contact your sales representative.
UEFI	463	Mirrored Memory Engaged due to an Uncorrectable Memory Error (%1 %2, DIMM %3).	Contact your sales representative.
UEFI	464	Online Spare Memory Copy Process	Contact your sales representative.

Class	Error code	Error message	Action
		Started for Faulty Module (%1 %2, DIMM %3).	
UEFI	465	Online Spare Memory Switchover Complete.	Action is not necessary.
UEFI	466	Correctable Memory Error Threshold Exceeded (%1 %2, Channel %3).	Contact your sales representative.
UEFI	467	Uncorrectable Error was detected on Processor %1.	Contact your sales representative.
UEFI	470	SATA device on Controller %1 Port %2 is unresponsive.	Contact your sales representative.
UEFI	480	IMPORTANT: Processor %1, DIMM %2 - NVDIMM-N firmware updated. Current version is %3.	Action is not necessary.
UEFI	481	NVDIMM Error - Firmware Update Error - Processor %1, DIMM %2 (SN:%3-%4-%5-%6). NVDIMM-N firmware was not updated. Current version is %7.	Contact your sales representative.
UEFI	482	NVDIMM Error - Invalid Firmware Image Detected - Processor %1, DIMM %2 (SN:%3-%4-%5-%6). NVDIMM-N switching to backup image. Current version is %7.	Contact your sales representative.
UEFI	483	NVDIMM Error - NVDIMM(s) cannot be initialized due to internal error (Code = %1). NVDIMM functionality might be impacted	Updating the system ROM and the innovation engine firmware may solve the error. Please update the system ROM and the innovation engine firmware. If the problem persists, contact your sales representative.
UEFI	490	System Health Error. A critical system health error requires the system to be shutdown.	Contact your sales representative.
UEFI	491	System Health Error. A critical system health error has kept the system from booting. -System Halted!	Contact your sales representative.
UEFI	500	ASR NMI Detected - The Automatic Server Recovery (ASR) NMI has been signaled (per the system configuration policy).	Contact your sales representative.
UEFI	501	IPMI Watchdog NMI Detected - The IPMI Watchdog NMI has been signaled (per the system configuration policy).	Contact your sales representative.
UEFI	502	Application Watchdog NMI Detected - The Application Watchdog NMI has been signaled (per the system configuration policy).	Contact your sales representative.

Class	Error code	Error message	Action
UEFI	510	The installed number of DIMMs on one or more processors results in an unbalanced memory configuration across memory controllers. This may result in non-optimal memory performance.	Referring to the user's guide, change the mounting positions or number of DIMM. In case a problem is not resolved, contact your sales representative.
UEFI	511	One or more DIMMs have been mapped out due to a memory error, resulting in an unbalanced memory configuration across memory controllers. This may result in non-optimal memory performance.	Contact your sales representative.
UEFI	530	Core Boost Technology Disabled.	System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Option -> From [Advanced Performance Tuning Options], set the [Core Boosting] option to [Enabled]. If the problem persists, contact your sales representative.
UEFI	1626	Unsupported Power Supply Configuration - Unsupported Power Supply detected.	Contact your sales representative.
UEFI	1636	%1 Trusted Platform Module Error.	Contact your sales representative. The motherboard and the TPM module must be replaced as a set.
UEFI	1809	Slot %1 Encryption Failure - Communication issue prevents drive keys from being retrieved. Encrypted logical drives are offline. System may not boot.	Refer to the page of the iLO key manager to check the corrective action.
UEFI	1810	Slot %1 Encryption Failure - Master Key is incorrect on or not retrieved from Remote Key Manager. Encrypted logical drives may be offline. System may not boot.	Correct the problem with the Key Manager.
UEFI	1811	Slot %1 Encryption Failure - Drive Keys not retrieved from the Remote Key Manager. Dependent encrypted logical drives are offline. System may not boot.	Correct the problem with the Key Manager.
UEFI	1812	Slot %1 Encryption Failure - Invalid Drive Keys on Remote Key Manager. Encrypted logical drives may be offline. System may not boot.	Restore the correct version of the drive key with the Key Manager.
UEFI	1814	Slot %1 Encryption Failure - Communication issue prevents keys from being retrieved. Dependent encrypted logical drives are offline. System may not boot.	After turning off the server power and disconnecting the power cord, check the installation of the Slot% 1 controller (card). Wait 30 seconds, and then restart it. If the problem persists, contact your sales representative.
UEFI	1822	Slot %1 Encryption Failure - Imported encrypted logical drives are offline. Matching Local Master Key required. System may not boot.	Enter the local master key using the Smart Storage Administrator.

Class	Error code	Error message	Action
UEFI	1900	Slot %1 Smart Array - Controller Failure. %2	Please take actions in following order. 1. After turning off the unit power and disconnecting the power cord, check the installation of the Slot% 1 controller (card). Wait 30 seconds, and then restart it. 2. If the problem persists, contact your sales representative.
UEFI	1901	Slot %1 Smart Array - Controller failed on previous power-up due to lock up code 0x%2	Contact your sales representative.
UEFI	1902	Slot %1 Smart Array - Controller not configured.	Check the connection between the Slot% 1 controller (card) and back plane and hard disk drive. Configure the drive using the Smart Storage Administrator.
UEFI	1903	Slot %1 Smart Array - Memory error occurred during self-test.	Contact your sales representative.
UEFI	1904	Slot %1 Smart Array - Redundant ROM programming failure.	Updating the firmware of the Slot% 1 controller (card) to the latest version may solve the error. Please update the corresponding firmware. If the problem persists, contact your sales representative.
UEFI	1905	Slot %1 Smart Array - Redundant ROM image checksum error. Backup ROM activated.	Updating the firmware of the Slot% 1 controller (card) to the latest version may solve the error. Please update the corresponding firmware. If the problem persists, contact your sales representative.
UEFI	1906	Slot %1 Smart Array - Last configuration not committed. %2	Set the configuration of the Slot% 1 controller again.
UEFI	1910	Slot %1 Smart Array - One or more drives could not be authenticated as genuine drives. Smart Array will not control the LEDs to these drives.	The hard disk drive connected to the Slot% 1 controller (card) could not be verified as an authorized part. To confirm the corresponding hard disk drive, check it via the Smart Storage Administrator.
UEFI	1911	Slot %1 Smart Array - Drive(s) are failed: %2	Contact your sales representative.
UEFI	1912	Slot %1 Smart Array - Drive(s) are overheated: %2	Contact your sales representative.
UEFI	1913	Slot %1 Smart Array - Drive Erase Operation In Progress (or Queued). The following drive(s) will be erased upon completion: %2	Action is not necessary.
UEFI	1914	Slot %1 Smart Array - Predictive drive failure: %2	Contact your sales representative.
UEFI	1920	Slot %1 Smart Array - Storage enclosure problem detected: %2. %3	Contact your sales representative.
UEFI	1921	Slot %1 Smart Array - Storage enclosure firmware upgrade problem detected: %2. %3	Contact your sales representative.

Class	Error code	Error message	Action
UEFI	1922	Slot %1 Smart Array - More devices attached than this controller supports. Some devices are ignored.	Please take actions in the following order. 1. Updating the firmware of the Slot% 1 controller to the latest version may solve the error. Refer to the release notes to check if there are related improvements. If there are related improvements, update the firmware of the Slot% 1 controller. 2. Reduce the number of hard disk drives connected to the Slot% 1 controller.
UEFI	1930	Slot %1 Smart Array - Valid data found in write-back Cache. Data will automatically be written to the logical drive(s).	Although the power has been turned off with the data still in the write-back cache, the data was automatically written to the logical drive. If the data is not recorded repeatedly, no action is required. To prevent data from remaining in the write-back cache, perform a normal shutdown of the system. If the problem persists, contact your sales representative.
UEFI	1931	Slot %1 Smart Array - Data in write-back cache has been lost.	Perform the following measures 1. Check the integrity of the data stored in the drive. 2. To prevent data from remaining in the write-back cache, perform a normal shutdown of the system. 3. If the data is missing, restore the previous backup data.
UEFI	1932	Slot %1 Smart Array - Write-back cache configuration error. %2	Take either of the following steps. 1. Change the drive array configuration back to what matches the cache. 2. Clear the data in the cache by executing the storage software.
UEFI	1933	Slot %1 Smart Array - Consecutive power loss during I/O transactions on non-optimal write-back volumes. This might have resulted in data integrity issues.	Please take actions in following order. 1. Make sure the controller (card) in slot %1 to be installed. 2. Make sure the power supply and the batteries have no problem.
UEFI	1934	Slot %1 Smart Array - Battery is not present. Caching is disabled.	Install the cache module battery.
UEFI	1935	Slot %1 Smart Array - Battery is charging. Caching will be enabled once the battery has been charged.	Action is not necessary.
UEFI	1936	Slot %1 Smart Array - Cache Module Self-Test Error Occurred. %2	Contact your sales representative.
UEFI	1937	Slot %1 Smart Array - Battery is present but the controller battery cable is not attached.	Make sure the battery cable for the controller is properly connected. Make sure the cable is properly connected to the connector. If the problem persists, contact your sales representative.
UEFI	1940	Slot %1 Smart Array - The following logical drives are failed: %2.	Contact your sales representative.

Class	Error code	Error message	Action
UEFI	1941	Slot %1 Smart Array - The following logical drives are missing: %2	Make sure all cables are properly connected. Make sure all hard disk drives are connected. Make sure the power is supplied to the back plane when the hard disk drive is connected through the back plane. If the problem persists, contact your sales representative.
UEFI	1942	Slot %1 Smart Array - Configured drive(s) are missing %2	Please take actions in following order. 1. Turn the unit's power OFF. 2. Turn the power OFF if the hard disk drive external enclosure is connected. 3. Make sure all cables are properly connected. 4. Make sure all hard disk drives are properly connected. 5. Turn ON the power of the unit and the hard disk drive external enclosure to determine whether the problem still exists. 6. If the problem persists, contact your sales representative.
UEFI	1943	Slot %1 Smart Array - Not able to import logical drive(s).	Reconnect the hard disk drives to the controllers to which they was originally connected. If the problem persists, contact your sales representative.
UEFI	1944	Slot %1 Smart Array - Foreign configuration(s) found on adapter.	Import the configuration settings of the inserted storage, or remove the appropriate RAID volume. If the problem persists, contact your sales representative.
UEFI	2150	Corrected Memory Error (%1 %2, DIMM %3, Address 0x%4'%5, Count %6)	The action is not necessary unless the failure of recording occurs repeatedly. If the problem persists, contact your sales representative.
UEFI	2200	Secure Boot - Secure Boot has been enabled.	Action is not necessary unless an unintended consequence occurs.
UEFI	2201	Secure Boot - Secure Boot has been disabled.	Action is not necessary unless an unintended consequence occurs.
UEFI	2202	Secure Boot - A new Platform Key (PK) has been enrolled	Action is not necessary unless an unintended consequence occurs.
UEFI	2203	Secure Boot - A new entry in the Key Exchange Key (KEK) security database has been enrolled.	Action is not necessary unless an unintended consequence occurs.
UEFI	2204	Secure Boot - A new entry in the db security database has been enrolled.	Action is not necessary unless an unintended consequence occurs.
UEFI	2205	Secure Boot - A new entry in the dbx security database has been enrolled.	Action is not necessary unless an unintended consequence occurs.
UEFI	2206	Secure Boot - A new entry in the dbt security database has been enrolled.	Action is not necessary unless an unintended consequence occurs.
UEFI	2207	Secure Boot - All of the keys have been reset to defaults.	Action is not necessary unless an unintended consequence occurs.

Class	Error code	Error message	Action
UEFI	2208	Secure Boot - Key Exchange Keys (KEK) have been reset to the platform defaults.	Action is not necessary unless an unintended consequence occurs.
UEFI	2209	Secure Boot - Platform Keys (PK) have been reset to the platform defaults.	Action is not necessary unless an unintended consequence occurs.
UEFI	2210	Secure Boot - db keys have been reset to the platform defaults.	Action is not necessary unless an unintended consequence occurs.
UEFI	2211	Secure Boot - dbx keys have been reset to the platform defaults.	Action is not necessary unless an unintended consequence occurs.
UEFI	2212	Secure Boot - dbt keys have been reset to the platform defaults.	Action is not necessary unless an unintended consequence occurs.
UEFI	2213	Secure Boot - All of the keys in the platform have been deleted.	Action is not necessary unless an unintended consequence occurs.
UEFI	2214	Secure Boot - The Platform Key (PK) Secure Boot variable has been deleted.	Action is not necessary unless an unintended consequence occurs.
UEFI	2215	Secure Boot - The Key Exchange Key (KEK) Secure Boot variable has been deleted.	Action is not necessary unless an unintended consequence occurs.
UEFI	2216	Secure Boot - The db Secure Boot variable has been deleted.	Action is not necessary unless an unintended consequence occurs.
UEFI	2217	Secure Boot - The dbx Secure Boot variable has been deleted.	Action is not necessary unless an unintended consequence occurs.
UEFI	2218	Secure Boot - The dbt Secure Boot variable has been deleted.	Action is not necessary unless an unintended consequence occurs.
UEFI	2219	Secure Boot - A Key Exchange Key (KEK) entry has been deleted from KEK database.	Action is not necessary unless an unintended consequence occurs.
UEFI	2220	Secure Boot - A db entry has been deleted from db database.	Action is not necessary unless an unintended consequence occurs.
UEFI	2221	Secure Boot - A dbx entry has been deleted from dbx database.	Action is not necessary unless an unintended consequence occurs.
UEFI	2222	Secure Boot - A dbt entry has been deleted from dbt database.	Action is not necessary unless an unintended consequence occurs.
UEFI	2223	Secure Boot - Unable to enable/disable secure boot. Only a physically present user can enable/disable Secure Boot.	Change the settings from the local console.
UEFI	2224	Secure Boot - Unable to enroll a new entry.	Set the required settings again using the System Utility after restoring factory default settings by selecting **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **System Defult Options** - **Restore Default Manufacturing Settings** options from the menu of the System Utility. If the problem persists, contact your sales representative.

Class	Error code	Error message	Action
UEFI	2225	Secure Boot - Unable to reset one or more keys.	Set the required settings again using the System Utility after restoring factory default settings by selecting **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **System Defult Options** - **Restore Default Manufacturing Settings** options from the menu of the System Utility. If the problem persists, contact your sales representative.
UEFI	2226	Secure Boot - Unable to delete one or more variables.	Set the required settings again using the System Utility after restoring factory default settings by selecting **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **System Defult Options** - **Restore Default Manufacturing Settings** options from the menu of the System Utility. If the problem persists, contact your sales representative.
UEFI	2227	Secure Boot - Unable to delete one or more entries.	Set the required settings again using the System Utility after restoring factory default settings by selecting **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **System Defult Options** - **Restore Default Manufacturing Settings** options from the menu of the System Utility. If the problem persists, contact your sales representative.
UEFI	2319	Test event. This is only a test.	Action is not necessary.
UEFI	2400	Slot %1 SAN Error - SAN link is down. SAN connection not possible.	Confirm the SAN switches and the configuration. Then reconnect SAN ports or restart the server.
UEFI	2401	Slot %1 SAN Error - Fabric Login (FLOGI) failed. SAN connection not possible.	Confirm the SAN switches and the configuration. Then reconnect SAN ports or restart the server.
UEFI	2402	Slot %1 SAN Error - Name Server login failed. Boot from SAN not possible.	Confirm the SAN switches and the configuration. Then reconnect SAN ports or restart the server.
UEFI	2403	Slot %1 SAN Error - No targets found. Boot from SAN not possible.	Confirm the SAN switches and the configuration. Then reconnect SAN ports or restart the unit.
UEFI	2404	Slot %1 SAN Error - Adapter restart failed. Firmware not ready. Boot from SAN not possible.	Reconnect SAN ports or restart the server. If the problem persists, contact your sales representative.
UEFI	2405	Slot %1 Error - Vital Product Data (VPD) is not available.	Update the firmware of the card in slot %1. If the problem persists, contact your sales representative.
UEFI	2406	Slot %1 NIC Error - NIC personality (Ethernet, iSCSI, or FCoE) could not be changed. FW may require update.	Update the firmware of the NIC card in slot %1 before restarting the server.
UEFI	2407	Slot %1 Error - The firmware update did not complete successfully.	Update the firmware of the card again after confirming the firmware image of the card in slot %1 is correct.
UEFI	2408	Slot %1 Error - Firmware image recovery not successful.	Restart the unit. If the problem persists, contact your sales representative.

Class	Error code	Error message	Action
UEFI	2409	Slot %1 Error - Failure to apply Virtual Connect (VC) settings.	Confirm the VC configuration. Apply the VC configuration again after restarting the server.
UEFI	2410	Slot %1 Error - Controller I/O timeout failure.	Restart the unit. If the problem persists, contact your sales representative.
UEFI	2411	%1: iSCSI Error - Failed to acquire DHCP client network address.	Check the network cables and the DHCP server configuration. Restart the server.
UEFI	2412	%1: iSCSI Error - Failed to acquire DHCP target network address.	Check the network cables and the DHCP server configuration. Restart the server.
UEFI	2413	%1: iSCSI Error - Failed to acquire DHCP iSNS Server IP address.	Check the network cables, the DHCP server configuration and the iSNS server configuration. Restart the server.
UEFI	2414	%1: iSCSI Error - iSCSI login failed.	Confirm and set the cable connection, the controller configuration, and the configurations of iSCSI initiator and the target properly. Then restart the server.
UEFI	2415	%1: iSCSI Error - Boot LUN not available.	Confirm and set the controller configuration and the iSCSI server configuration properly. Then restart the server.
UEFI	2416	%1: Error - Controller firmware not ready.	Restart the unit. If the problem continues, update FW. If the problem persists, contact your sales representative.
UEFI	2419	%1 %2 Error - Rx/Tx is disabled on this device because an unsupported SFP+ or QSFP module type was detected.	Contact your sales representative.
UEFI	2420	%1 %2 Error - The UEFI driver for the device detected an older version of the NVM image than expected.	Update the NVM image. If the problem persists, contact your sales representative.
UEFI	2421	%1 %2 Error - The UEFI driver for the device detected a newer version of the NVM image than expected.	Update the NVM UEFI driver to the latest version. If the problem persists, contact your sales representative.
UEFI	2422	%1 %2 Error - The UEFI driver for the device stopped because the NVM image is newer than expected.	Update the NVM UEFI driver to the latest version. If the problem persists, contact your sales representative.
UEFI	3100	Trusted Platform Module (TPM) was successfully bound to system.	Action is not necessary. The unit restarts automatically.
UEFI	3101	Unbound Trusted Platform Module (TPM) detected.	Action is not necessary. The TPM is integrated into the unit after being cleared.
UEFI	120	A Critical Error Event that has kept the system from booting. -System Halted!	Contact your sales representative.
UEFI	163	Time & Date Not Set.	Set the date and time of the server.
UEFI	209	Unsupported DIMM Configuration Detected - Installed DIMM configuration does NOT support configured AMP Mode. System will operate in Advanced ECC Mode. (Major Code:%1 Minor Code:%2).	For the details of the DIMM configuration required to use the AMP mode, refer to the *User's Guide*. If the problem persists, contact your sales representative.

Class	Error code	Error message	Action
UEFI	210	Unsupported DIMM Configuration Detected - Installed DIMMs could not support the currently configured interleave mode. (Major Code:%1, Minor Code:%2).	For the details of the DIMM configuration required to use the interleaved mode, refer to the *User's Guide*. If the problem persists, contact your sales representative.
UEFI	211	Unsupported DIMM Configuration Detected - Processor %1 DIMM %2. The DIMM does not support ECC. (Major Code:%3, Minor Code:%4).	Remove the DIMM which was pointed out. For the details of the DIMM configuration, refer to the *User's Guide*. If the problem persists, contact your sales representative.
UEFI	212	Processor UPI Initialization Error. A processor UPI initialization error was detected. %1 (Major Code:%2, Minor Code:%3).	Contact your sales representative.
UEFI	213	Unsupported DIMM Configuration Detected - Processor %1 DIMM %2. The DIMM has more ranks than is supported by this system. (Major Code:%3, Minor Code:%4).	Contact your sales representative.
UEFI	214	Unsupported DIMM Configuration Detected - Processor %1 DIMM %2. The DIMM requires a frequency not supported by the system. (Major Code:%3, Minor Code:%4).	Contact your sales representative.
UEFI	215	DIMM Initialization Error - Processor %1 DIMM %2. The identified processor and memory failed to initialize properly. %3 (Major Code:%4, Minor Code:%5).	Contact your sales representative.
UEFI	216	DIMM Initialization Error. A fatal error was detected while initializing memory. %1 (Major Code:%2, Minor Code:%3).	Contact your sales representative.
UEFI	217	DIMM Initialization Error - Processor %1 DIMM %2. The identified processor and memory are operating at an incorrect voltage. %3 (Major Code:%4, Minor Code:%5).	Contact your sales representative.
UEFI	219	Memory Configuration Error - One or more of the installed processors has a total amount of memory installed which exceeds the amount supported by that processor. %1 (Major Code:%2, Minor Code:%3).	Contact your sales representative.
UEFI	220	KTI Initialization Error - A fatal KTI initialization error has been detected. %1 (Major Code: %2, Minor Code: %3).	Contact your sales representative.

Class	Error code	Error message	Action
UEFI	221	Unknown Initialization Error. The system has experienced a fatal initialization error. %1 (Major Code: %2, Minor Code: %3).	Contact your sales representative.
UEFI	228	Unsupported DIMM Configuration Detected - Processor %1 Channel %2. DIMM population rule violation. The Memory channel has been mapped out. (Major Code:%3, Minor Code:%4).	Check and change the DIMM configuration for the rules of the installation. For the details of the DIMM configuration, refer to the *User's Guide*. If the problem persists, contact your sales representative.
UEFI	229	Unsupported DIMM Configuration Detected - Processor %1 DIMM %2. The identified DIMM is not supported in the system. (Major Code:%3, Minor Code:%4).	Remove the DIMM which was pointed out. For the details of the DIMM configuration, refer to the *User's Guide*. If the problem persists, contact your sales representative.
UEFI	230	Unsupported DIMM Configuration Detected - Processor %1 Channel %2. The number of installed DIMM ranks exceeds the number supported by the channel. (Major Code:%3, Minor Code:%4).	Remove the DIMM of the memory channel which was pointed out. For the details of the DIMM configuration, refer to the *User's Guide*. If the problem persists, contact your sales representative.
UEFI	231	Memory Configuration Error - No memory is available. If DIMMs are installed, verify that the corresponding processor is installed. %1 (Major Code:%2, Minor Code:%3).	Contact your sales representative.
UEFI	232	DIMM Initialization Error - A memory initialization error was detected. %1 (Major Code:%2, Minor Code:%3).	Contact your sales representative.
UEFI	233	DIMM Initialization Error - Processor %1 Channel %2. The identified memory channel could not be properly trained and has been mapped out. (Major Code:%3, Minor Code:%4).	Contact your sales representative.
UEFI	234	DIMM Initialization Error - Processor %1 DIMM %2. The identified DIMM could not be properly trained and has been mapped out. (Major Code:%3, Minor Code:%4).	Contact your sales representative.
UEFI	235	Unsupported DIMM Configuration Detected - Mixed DIMM configurations are not support on this system. %1 (Major Code:%2, Minor Code:%3).	Remove the DIMM which was pointed out. For the details of the DIMM configuration, refer to the *User's Guide*. If the problem persists, contact your sales representative.

Class	Error code	Error message	Action
UEFI	236	Unsupported DIMM Configuration Detected - Processor %1 DIMM %2. The DIMM does not support the required voltage. (Major Code:%3, Minor Code:%4).	Remove the DIMM which was pointed out. For the details of the DIMM configuration, refer to the *User's Guide*. If the problem persists, contact your sales representative.
UEFI	237	Unsupported DIMM Configuration Detected - Octal and Quad Rank DIMMs are not supported on the same memory channel . (Major Code:%1, Minor Code:%2).	Check and change the DIMM configuration for the rules of the installation. For the details of the DIMM configuration, refer to the User's Guide. If the problem persists, contact your sales representative.
UEFI	238	Unsupported DIMM Configuration Detected - Mixing octal rank LRDIMMs with non-octal rank LRDIMMs is not supported. %1 (Major Code:%2, Minor Code:%3).	Check and change the DIMM configuration for the rules of the installation. For the details of the DIMM configuration, refer to the User's Guide. If the problem persists, contact your sales representative.
UEFI	242	Unsupported Processor Configuration Detected - System does not support booting with three processors installed.	Make sure the processor is properly installed. If the problem persists, contact your sales representative.
UEFI	243	Unsupported Processor Configuration Detected - The installed processors are not 4-socket capable and this server only supports 4-socket capable processors.	Make sure the processor is properly installed. If the problem persists, contact your sales representative.
UEFI	259	Unsupported Processor Configuration Detected. All installed processors do not have the same model number.	Make sure the processor is properly installed. If the problem persists, contact your sales representative.
UEFI	265	System Configuration Error. The system configuration has exceeded the non-volatile storage capacity of the server and certain settings may be lost.	Set the required settings again using the System Utility after restoring factory default settings by selecting **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **System Default Options** - **Restore Default Manufacturing Settings** options from the menu of the System Utility. If the problem persists, contact your sales representative.
UEFI	270	%1 FW Communication Issue - Unable to communicate with %2 FW. Certain management functionality is not available.	Turn off the power of this device, pull off the power code and after 30 minutes, reboot the device. In case a problem is not resolved, contact your sales representative.
UEFI	275	Unsupported Processor Detected - Processor stepping not supported.	Contact your sales representative.
UEFI	298	IMPORTANT: The Boot Mode has been changed to Legacy Boot Mode for this boot only. On the next reboot, the Boot Mode will return to UEFI Boot Mode.	Action is not necessary.

Class	Error code	Error message	Action
UEFI	299	The Boot Mode has been changed to UEFI Boot Mode for this boot only. On the next reboot, the Boot Mode will return to Legacy Boot Mode.	Action is not necessary.
UEFI	305	Redundant ROM Error: Both the Primary and Backup System ROMs are invalid.	Update the system ROM and the redundant ROM. If the problem persists, contact your sales representative.
UEFI	318	Trusted Platform Module (TPM) Self-Test Error.	Turn off the unit, disconnect the power cord, wait 30 seconds, and then restart it. If the problem persists, contact your sales representative.
UEFI	330	Unsupported Processor Configuration Detected - Processors are installed in the incorrect order.	Make sure the processor is properly installed. If the problem persists, contact your sales representative.
UEFI	347	NVDIMM Population Error - %1 NVDIMMs are present in the system. Only %2 NVDIMMs are supported.	Confirm the installation of NVDIMM. In case a problem is not resolved, contact your sales representative.
UEFI	347	NVDIMM Population Error - %1 NVDIMMs are present in the system. Only %2 NVDIMMs are supported.	Make sure the NVDIMM is properly installed. If the problem persists, contact your sales representative.
UEFI	348	Unsupported DIMM Configuration Detected - Processor %1 DIMM %2. Registered DIMMs are only supported when an NVMDIMM is present in the system. (Major Code:%3, Minor Code:%4).	Remove the DIMM which was pointed out. For the details of the DIMM configuration, refer to the *User's Guide*. If the problem persists, contact your sales representative.
UEFI	349	NVDIMM Population Error - NVDIMMs and LRDIMMs are installed in this system. NVDIMMs are only supported with RDIMMs on this system.	Remove the LRDIMM. For the details of the DIMM configuration, refer to the *User's Guide*. If the problem persists, contact your sales representative.
UEFI	350	NVDIMM Population Error - Processor %1, DIMM %2. NVDIMMs and RDIMMs are in the incorrect order on Channel %3. NVDIMMs on the channel should be closest to the CPU.	Check and change the DIMM configuration for the rules of the installation. For the details of the DIMM configuration, refer to the *User's Guide*. If the problem persists, contact your sales representative.
UEFI	358	IMPORTANT: Processor %1, DIMM %2 - The installed NVDIMM has a Supercap attached. This is not supported.	Remove the Supercap which was pointed out. For the details of the DIMM configuration, refer to the *User's Guide*. If the problem persists, contact your sales representative.
UEFI	359	NVDIMM Population Error - Processor 1 must have at least one RDIMM installed when NVDIMMs are present in the system.	Check and change the DIMM configuration for the rules of the installation. For the details of the DIMM configuration, refer to the User's Guide. If the problem persists, contact your sales representative.

Class	Error code	Error message	Action
UEFI	365	Unsupported NVDIMM-N Configuration Detected - The installed NVDIMM-Ns are not compatible with each other. (Major Code:%1, Minor Code:%2).	Check and change the DIMM configuration for the rules of the installation. For the details of the DIMM configuration, refer to the *User's Guide*. If the problem persists, contact your sales representative.
UEFI	367	System ROM Authentication Error - The System ROM image could not be authenticated or recovered.	Update the system ROM and the redundant ROM. If the problem persists, contact your sales representative.
UEFI	368	System ROM Authentication Error - The BIOS image could not be authenticated.	An attempt will be made to recover automatically. If the problem persists, contact your sales representative.
UEFI	369	System ROM Authentication Error - The system is operating on a recovered or redundant image. Redundant ROM functionality is NOT available.	Confirm the revision of the system ROM. Update the ROM to restore the redundancy of the system ROM. If the problem persists, contact your sales representative.
UEFI	370	Redundant ROM Image Authentication Error - The Redundant ROM image could not be authenticated. Redundant ROM functionality is NOT available.	Update the system ROM and the redundant ROM. If the problem persists, contact your sales representative.
UEFI	389	Unexpected Shutdown and Restart - An undetermined error type resulted in a reboot of the server.	If the problem persists, contact your sales representative.
UEFI	412	Server Platform Services Firmware Error - The Server Platform Services firmware is operating in factory mode.	Update the system ROM and Server Platform Services Firmware. If the problem persists, contact your sales representative.
UEFI	413	Innovation Engine Image Authentication Error. The Innovation Engine image could not be authenticated.	Update Innovation Engine Firmware. If the problem persists, contact your sales representative.
UEFI	436	Scalable Persistent Memory on %1 Logical NVDIMM %2 does not have enough memory to initialize.	Confirm an additional DIMM is unnecessary. Instead, confirm an additional record about a memory error in Integrated Management Log (IML). If there is an additional record, follow on how to deal with the additional record. If the problem persists, contact your sales representative.
UEFI	450	%1 is in High Security Mode and there is no System ROM Admin Password set.	Restart the unit after setting the Admin password for the system ROM.
UEFI	453	Unsupported DIMM Configuration Detected - Processor %1 DIMM %2. Unsupported persistent memory module is present in the system. This module is not supported by the installed processor(s). -System Halted!	Remove the persistent memory which was pointed out. For the details of the DIMM configuration, refer to the *User's Guide*. If the problem persists, contact your sales representative.

Class	Error code	Error message	Action
UEFI	462	Uncorrectable Memory Error Threshold Exceeded (%1 %2, DIMM %3). The DIMM is mapped out and is currently not available.	Contact your sales representative.
UEFI	471	IMPORTANT: The UEFI Variable space is close to exceeding the non-volatile storage capacity. This may impact OS installations and may limit the ability to configure certain options.	Restore the factory default settings using the "Restore Default Manufacturing Settings" option via **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **System Defult Options** in the system utility. If the problem persists, contact your sales representative.
UEFI	3010	MemBIST RMT: %1 margin out of range at CPU %2 DIMM %3 - Count %4	Contact your sales representative.
UEFI	3011	MemBIST MEMTEST: UnCorrectable Memory Error found at CPU %1 DIMM %2 Rank %3 - UC Count %4	Contact your sales representative.
UEFI	3012	MemBIST MEMTEST: Correctable Memory Error found at CPU %1 DIMM %2 Rank %3 Strobe %4 - CE Count %5	Contact your sales representative.
UEFI	3013	Processor Built-In Self-Test (BIST) Failure. Processor %1, Error Code = 0x%2.	Contact your sales representative.

(4) The list of messages about the power supply

Class	Error code	Error message	Action
Power	15	Mismatched Power Supply Installed	Confirm the PSU mounted on the unit. If the problem persists, contact your sales representative.
Power	1B	System Board Power Protection Fault	Contact your sales representative.
Power	1C	Power Supply or Power Backplane Detection Error	Contact your sales representative.
Power	1E	Smart Storage Battery Removed (Battery %1)	Contact your sales representative.
Power	24	Power On Denied (Service Information: %1)	Contact your sales representative.
Power	28	System Power Supply: %1 (Power Supply %2)	Contact your sales representative.
Power	29	External Chassis Power Supply: %1 (Chassis %2, Power Supply %3)	Contact your sales representative.
Power	2A	%1 Storage System Power Supply: %2 (%3Slot %4, Power Supply %5)	Contact your sales representative.
Power	2B	%1 Power Supply: %2 (Power Supply %3, %4)	Contact your sales representative.
Power	2C	System Power Supply Removed (Power Supply %1)	Action is not necessary.

Class	Error code	Error message	Action
Power	2D	External Chassis Power Supply Removed (Chassis %1, Power Supply %2)	Action is not necessary.
Power	2E	%1 Storage System Power Supply Removed (Chassis %2 Slot %3, Power Supply %4)	Action is not necessary.
Power	2F	%1 Power Supply Removed (Power Supply %2, Enclosure Address %3)	Action is not necessary.
Power	30	%1 Power Supply Removed (Power Supply %2, Enclosure Serial Number %3)	Action is not necessary.
Power	31	System Power Supply Inserted (Power Supply %1)	Action is not necessary.
Power	32	External Chassis Power Supply Inserted (Chassis %1, Power Supply %2)	Action is not necessary.
Power	33	%1 Storage System Power Supply Inserted (Chassis %2 Slot %3, Power Supply %4)	Action is not necessary.
Power	34	%1 Power Supply Inserted (Power Supply %2, Enclosure Address %3)	Action is not necessary.
Power	35	%1 Power Supply Inserted (Power Supply %2, Enclosure Serial Number %3)	Action is not necessary.
Power	36	System Power Supplies Not Redundant	Contact your sales representative.
Power	37	External Chassis Power Supplies Not Redundant (Chassis %1)	Contact your sales representative.
Power	38	%1 Storage System Power Supplies Not Redundant (Chassis %2 Slot %3)	Contact your sales representative.
Power	3A	%1 Power Supplies Not Redundant (Enclosure Serial Number %2)	Contact your sales representative.
Power	3B	%1 Power Supplies Not Redundant (Enclosure Address %2)	Action is not necessary.
Power	3C	System Power Fault Detected (XR: %1 %2 MID: %3)	Action is not necessary.
Power	3D	System Power Fault Detected (XR: %1 %2 MID: %3)	Contact your sales representative.
Power	3E	Smart Storage Battery failure (Battery %1, service information: %2).	Contact your sales representative.

Class	Error code	Error message	Action
Power	3F	Smart Storage Battery did not charge at the expected rate, indicating a faulty battery (Battery %1, service information: 0x03)	Contact your sales representative.
Power	40	Smart Storage Battery disabled due to high ambient temperature, will be re-enabled when temp is lowered (Battery %1, service information: 0x04)	Contact your sales representative.
Power	41	Smart Storage Battery discharged to below minimum voltage, resulting in the inability of the battery to recharge properly (Battery %1, service information: 0x05)	Contact your sales representative.
Power	42	Smart Storage Battery has exceeded the maximum amount of devices supported (Battery %1, service information: 0x07)	Contact your sales representative.
Power	43	Smart Storage Battery failure (Battery %1)	Contact your sales representative.
Power	44	%1 Storage Enclosure Power Supply Failure (Power Supply %2, Box %3, %4)	Contact your sales representative.
Power	52	System Power Supply: %1 (Power Supply %2)	Contact your sales representative.
Power	53	Power redundancy loss warning: server power: %1W exceeded the redundant power threshold: %2W	Contact your sales representative.
Power	54	System Power Supply: %1 (Power Supply %2)	Contact your sales representative.
Power	55	Battery Backup Unit: %1 (Power Supply %2)	Contact your sales representative.

(5) The list of messages about the rack infrastructure

Class	Error code	Error message	Action
Rack Infrastructure	1B	%1 Inadequate Power To Power On: %2 (Enclosure Serial Number %3, Slot %4)	Contact your sales representative.
Rack Infrastructure	1C	%1 Inadequate Power To Power On: %2 (Enclosure Address %3, Slot %4)	Action is not necessary.
Rack Infrastructure	1D	%1 Rack Name Changed (Enclosure Serial Number %2)	Action is not necessary.
Rack Infrastructure	1E	%1 Rack Name Changed (Enclosure Address %2)	Action is not necessary.
Rack Infrastructure	1F	%1 Name Changed (Enclosure Serial Number %2)	Action is not necessary.
Rack Infrastructure	20	%1 Name Changed (Enclosure Address %2)	Action is not necessary.

Class	Error code	Error message	Action
Rack Infrastructure	21	%1 Service Change (Enclosure Serial Number %2)	Action is not necessary.
Rack Infrastructure	22	%1 Service Change (Enclosure Address %2)	Action is not necessary.
Rack Infrastructure	23	%1 Rack Name Conflict (Enclosure Serial Number %2)	Action is not necessary.
Rack Infrastructure	24	%1 Rack Name Conflict (Enclosure Address %2)	Action is not necessary.
Rack Infrastructure	25	%1 Rack Unique ID Changed (Enclosure Serial Number %2)	Action is not necessary.
Rack Infrastructure	26	%1 Rack Unique ID Changed (Enclosure Address %2)	Action is not necessary.
Rack Infrastructure	27	%1 LAN Settings Changed (Enclosure Serial Number %2)	Action is not necessary.
Rack Infrastructure	28	%1 LAN Settings Changed (Enclosure Address %2)	Action is not necessary.
Rack Infrastructure	29	%1 UID LED State Changed (Enclosure Serial Number %2)	Action is not necessary.
Rack Infrastructure	2A	%1 UID LED State Changed (Enclosure Address %2)	Action is not necessary.
Rack Infrastructure	2B	%1 Rack Infrastructure Changed (Enclosure Serial Number %2, Type %3)	Action is not necessary.
Rack Infrastructure	2C	%1 Rack Infrastructure Changed (Enclosure Address %2, Type %3)	Action is not necessary.
Rack Infrastructure	2D	Chassis Enclosure Serial Number %1 requires minimum firmware revision 0x%2.0x%3. It is currently 0x%4.0x%5.	Updating the firmware to the latest version can resolve the problems. Update the firmware of the enclosure whose serial number is %1. If the problem persists, contact your sales representative.
Rack Infrastructure	2E	Chassis Enclosure Address %1 requires minimum firmware revision 0x%2.0x%3. It is currently 0x%4.0x%5.	Updating the firmware to the latest version can resolve the problems. Update the firmware of the enclosure whose address is %1. If the problem persists, contact your sales representative.
Rack Infrastructure	2F	%1 Power Request Denied: %2 %3 (Enclosure Serial Number %4, Slot %5)	Contact your sales representative.
Rack Infrastructure	30	%1 Power Request Denied: %2 (Enclosure Address %3, Slot %4)	Action is not necessary.

(6) The list of the other messages

Class	Error code	Error message	Action
ASR	1	ASR Detected by System ROM	Contact your sales representative.
ASR	3	ASR Reset Limit Detected by System ROM	Contact your sales representative.
OS	2	Automatic Operating System Shutdown %1	Contact your sales representative.

Class	Error code	Error message	Action
OS	4	A User initiated NMI Switch event detected	If the record results from the NMI switch operation, an additional action is not required.
OS	6	A User initiated remote NMI Switch event detected	If the record results from the NMI switch operation, an additional action is not required.
Network	8	Network Adapter Link Down (Slot %1, Port %2)	Contact your sales representative.
Network	9	Network Adapter Link Down (Chassis %1, Slot %2, Port %3)	Contact your sales representative.
Drive Array	12	%1 Smart Array - Controller Failure (Status: %2)	Contact your sales representative.
Drive Array	13	Drive Array Controller Failure (Chassis %1, Slot %2)	Contact your sales representative.
Drive Array	14	%1 Smart Array â€“ Drive is failed: Port %2 Box %3 Bay %4	Contact your sales representative.
Drive Array	15	%1 Smart Array - SSD Wear Status Level %2: Port %3 Box %4 Bay %5	Contact your sales representative.
Drive Array	16	%1 Smart Array - Predictive drive failure: Port %2 Box %3 Bay %4	Contact your sales representative.
Drive Array	17	%1 Smart Array - Cache Status: %2 (Error Code: %3)	Contact your sales representative.
Drive Array	18	%1 Smart Array - Drive could not be authenticated as genuine drive. Smart Array will not control the LEDs: Port %2 Box %3 Bay %4	Contact your sales representative.
System Error	5	Unrecoverable I/O Error has occurred. System Firmware will log additional details in a separate IML message entry if possible.	Contact your sales representative.
System Error	7	Server Critical Fault (Service Information: %1)	Contact your sales representative.
System Error	8	Enclosure Induced Event (Service Information: Enclosure Power Loss, %1)	Action is not necessary.
System Revision	2	Firmware flashed (%1)	Action is not necessary.
System Revision	3	#ILO detected invalid %1 firmware.	If the record continues, contact your maintenance service company.
System Revision	4	#ILO was unable to automatically repair the %1 firmware.	Update the server platform service firmware. If the problem persists, contact your sales representative.

Class	Error code	Error message	Action
Maintenance	1	IML Cleared (%1 user: %2)	Action is not necessary.
Maintenance	2	Maintenance note: %1	Action is not necessary.
Power Cap	1	Processor(s) Operating at Reduced Performance Level Due to a Low Power Cap	Contact your sales representative.
Power Cap	3	Power Cap Cannot Be Reached With Current System Configuration (Power Cap %1W)	Contact your sales representative.
Power Cap	4	Power allocation not optimized. Increased power allocation requested. Server performance is not degraded	Contact your sales representative.
Flash Media	1	Boot From Flash Error (%1)	Connect the USB memory device again.
Interlock	1	Improperly seated or missing device (%1, %2)	Contact your sales representative.

2. List of Windows Event Logs

OS

Event Log

ID	Source	Type	Message (Description)
	Timing when an event is logged		Action

All Windows OS

System Event Log

51	Cdrom	Warning	Error detected on the device \Device\CdRom0 during the paging operation.
	When installing an OS		This event may be registered in the event viewer, but this does not affect system operation.
56	Application Popup	Error	The SCSI device driver returned an invalid ID for a child device (XXXXXX). * This event can be displayed as follows, but this does not affect the system operation. The ID can be different depending on your environment. " The description of event ID 56 from the source "Application Popup" cannot be found. The component which causes this event is not installed on the local computer or the installation is damaged. Install the component on the local computer or repair it. If the event occurs on another computer, you must save the displayed information with it. The event contains the following information: SCSI XXXXXX The message resource is present, but the messages can not be found in string table or message table.
	When starting system		This event can be registered in the system, which multiple RAID controllers and SAS controllers are connected to, but this does not affect the system operation.
129	SmartDQa	Warning	Reset was issued to the device \Device\RaidPort(x). (x is any number)
	While the system is running		If this message has been registered as a log during heavy I/O, there is no problem since the OS has succeeded in retry. Continue using.
129	SmartPqi	Warning	Reset was issued to the device \Device\RaidPort(x). (x is any number)
	When running the system		Even if the message is registered in the log, there is no problem because the OS has successfully completed the retry. you don't need any changes.

157	Disk	Warning	Disk x is suddenly removed.
	When creating a RAID		If you create new RAID on Windows, this event can be registered, but this does not affect the system operation.

Windows Server 2016

System Log

4	l2nd	Warning	HPE Ethernet 10Gb 2-port 530SFP+ Adapter #xx: The network link is down. Check to make sure the network cable is properly connected.
	When installing an OS, starting system, or applying Standard Program Package		This event does not affect system operation.
4	l2nd	Warning	HPE Ethernet 10Gb 2-port 530T Adapter #xx: The network link is down. Check to make sure the network cable is properly connected.
	When installing an OS, starting system, or applying Standard Program Package		This event does not affect system operation.
4	l2nd	Warning	HPE FlexFabric 10Gb 2-port 533FLR-T Adapter #xx: The network link is down. Check to make sure the network cable is properly connected.
	When installing an OS, starting system, or applying Standard Program Package		This event does not affect system operation.
4	l2nd	Warning	QLogic BCM57810 10 Gigabit Ethernet (NDIS VBD Client) #xx: The network link is down. Check to make sure the network cable is properly connected.
	When installing an OS		This event does not affect system operation.
4	l2nd2	Warning	HPE Ethernet #xx: The network link is down. Check to make sure the network cable is properly connected. Besides, the device name in this event is not shown correctly but it does not affect the operation of the device.
	When installing an OS, starting system, or applying Standard Program Package		This event does not affect system operation. Although the device name is incorrectly displayed in this event, there is no problem with the operation.
4	q57nd60a	Warning	HPE Ethernet 1Gb 4-port 331i Adapter #xx: The network link is down. Check to make sure the network cable is properly connected.
	When installing an OS, starting system, or applying Standard Program Package		This event does not affect system operation.
4	q57nd60a	Warning	HPE Ethernet 1Gb 4-port 331T Adapter #xx: The network link is down. Check to make sure the network cable is properly connected.
	When installing an OS, starting system, or applying Standard Program Package		This event does not affect system operation.
4	q57nd60a	Warning	HPE Ethernet 1Gb 4-port 331FLR Adapter #xx: The network link is down. Check to make sure the network cable is properly connected.
	When installing an OS, starting system, or applying Standard Program Package		This event does not affect system operation.
4	q57nd60a	Warning	HPE Ethernet 1Gb 2-port 332T Adapter #xx: The network link is down. Check to make sure the network cable is properly connected.
	When installing an OS, starting system, or applying Standard Program Package		This event does not affect system operation.

4	b57nd60a	Warning	Broadcom NetXtreme Gigabit Ethernet #xx: The network link is down. Check to make sure the network cable is properly connected.
	When installing an OS		This event does not affect system operation.
27	e1rexpress	Warning	HP Ethernet 1Gb 2-port 361T Adapter #xx Network link is disconnected.
	When installing an OS, starting system, or applying Standard Program Package		This event does not affect system operation.
27	e1rexpress	Warning	HP Ethernet 1Gb 4-port 366T Adapter #xx Network link is disconnected.
	When installing an OS, starting system, or applying Standard Program Package		This event does not affect system operation.
27	e1rexpress	Warning	HP Ethernet 1Gb 4-port 366FLR Adapter #xx Network link is disconnected.
	When installing an OS, starting system, or applying Standard Program Package		This event does not affect system operation.
27	e1iexpress	Warning	Intel(R) I350 Gigabit Network Connection #xx Network link is disconnected.
	When installing an OS		This event does not affect system operation.
27	ixgbs	Warning	HPE Ethernet 10Gb 2-port 562FLR-T Adapter #xx Network link is disconnected.
	When installing an OS, starting system, or applying Standard Program Package		This event does not affect system operation.
27	ixgbs	Warning	HPE Ethernet 10Gb 2-port 562T Adapter #xx Network link is disconnected.
	When installing an OS, starting system, or applying Standard Program Package		This event does not affect system operation.
27	ixgbi	Warning	HPE Ethernet 10Gb 2-port 562FLR-T Adapter #xx Network link is disconnected.
	When installing OS		This event does not affect system operation.
27	ixgbi	Warning	HPE Ethernet 10Gb 2-port 562T Adapter #xx Network link is disconnected.
	When installing OS		This event does not affect system operation.
27	i40ea	Warning	HPE Ethernet 10Gb 2-port 562SFP+ Adapter #xx Network link is disconnected.
	When installing an OS, starting system, or applying Standard Program Package		This event does not affect system operation.
27	i40ea	Warning	HPE Ethernet 10Gb 562SFP+ Adapter #xx Network link is disconnected.
	When installing an OS, starting system, or applying Standard Program Package		This event does not affect system operation.
27	i40ea	Warning	HP Ethernet 10Gb 2-port 562FLR-SFP+ Adapter Network link is disconnected.
	When installing an OS, starting system, or applying Standard Program Package		This event does not affect system operation.

27	i40ei	Warning	The description for Event ID 27 from source "i40ei" cannot be found. Either the component that raises this event is not installed on your local computer or the installation is corrupted. You can install or repair the component on the local computer.
	When installing an OS		This event does not affect system operation.
219	Microsoft-Windows-Kernel-PnP	Warning	The driver \Driver\WudfRd failed to load for the device xxxxxxxxxxxxxxxxx.
	When starting system or connecting a disk		This may be recorded when starting the system or connecting a disk depending on timing, but does not affect system operation.
225	Kernel-PnP	Warning	The application YYY with process id XXX stopped the removal or ejection for the device ZZZ. * ZZZ : Instance name of the device YYY : Name of the process that was using the device XXX : ID of the process that was using the device
	When applying Starter Pack		This event does not affect system operation if it is logged when applying Starter Pack.
7023	Service Control Manager	Error	"xxxxxxxx service terminated with the following error: A device attached to the system is not functioning."
	When running an OS for the first time		This event does not affect system operation if it is recorded only on the first startup and not recorded repeatedly.
7023	Service Control Manager	Error	The Data Sharing Service service terminated with the following error: %%3239247874 * The description for Event ID 7023 from source Service Control Manager cannot be found. Either the component that raises this event is not installed on your local computer or the installation is corrupted. You can install or repair the component on the local computer. If the event originated on another computer, the display information had to be saved with the event. The following information was included with the event: Data Sharing Service %%3239247874 The locale specific resource for the desired message is not present.
	When running an OS for the first time or rebooting it, or while the system is in use		This event does not affect system operation.
7030	Service Control Manager	Error	The Printer Extensions and Notifications service is marked as an interactive service. However, the system is configured to not allow interactive services. This service may not function properly.
	When running an OS for the first time		This event does not affect system operation if it is recorded only on the first startup and not recorded repeatedly.
10010	Microsoft-Windows-DistributedCOM	Error	The server {XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX} did not register with DCOM within the required timeout.
	When running an OS for the first time or rebooting it		Refer to the following website. http://support.microsoft.com/kb/956479/
10317	Microsoft-Windows-NDIS	Error	Miniport Microsoft Network Adapter Multiplexor Driver, {xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx}, had event Network Interface deleted while PNP Device still exists. Note that this event is provided for informational purpose and might not be an error always (Eg: In case of vSwitch which was recently un-installed or a LBFO team was removed)
	When removing a team		This event does not affect system operation.

Application Event Log

1014	Microsoft-Windows-Security-SPP	Warning	Acquisition of End User License failed. hr=0x80072EE7
	When running an OS for the first time		This event does not affect system operation if it is not recorded repeatedly after activating the Windows.
1015	Microsoft-Windows-Security-SPP	Warning	Detailed HRESULT. Returned hr=0xC004F022, Original hr=0x80049E00
	When running an OS for the first time		This event does not affect system operation if it is not recorded repeatedly after activating the Windows.
1534	Microsoft-Windows-User Profiles Service	Warning	Profile notification of event Create for component {2c86c843-77ae-4284-9722-27d65366543c} failed, error code is Not implemented.
	When running an OS for the first time		This event does not affect system operation if it is recorded only on the first startup and not recorded repeatedly.
8198	Microsoft-Windows-Security-SPP	Error	License Activation (slui.exe) failed with the following error code: hr=0x******** Command-line arguments: RuleId=******************************
	When running an OS for the first time or rebooting it		This event does not affect system operation if it is not recorded repeatedly after activating the Windows.
8200	Microsoft-Windows-Security-SPP	Error	License acquisition failure details. hr=0x80072EE7
	When running an OS for the first time or rebooting it		This event does not affect system operation if it is not recorded repeatedly after activating the Windows.

Applications and Services Logs

69	Microsoft-Windows-AppModel-Runtime	Error	Failed with 0x490 modifying AppModel Runtime status for package ********** for user ********* (current status = 0x0, desired status = 0x20).
	When running an OS for the first time		This event does not affect system operation if it is recorded only on the first startup and not recorded repeatedly.
134	Microsoft-Windows-Time-Service	Warning	NtpClient was unable to set a manual peer to use as a time source because of DNS resolution error on 'time.windows.com,0x8'. NtpClient will try again in 15 minutes and double the reattempt interval thereafter.
	When running an OS for the first time or rebooting it		This event does not affect system operation if it is not recorded after connecting to the internet.
200	Microsoft-Windows-DeviceSetupManager	Warning	A connection to the Windows Update service could not be established.
	When running an OS for the first time or rebooting it		This event does not affect system operation if it is not recorded after connecting to the internet.

201	Microsoft-Windows-DeviceSetupManager	Warning	A connection to the Windows Metadata and Internet Services (WMIS) could not be established.
	When running an OS for the first time or rebooting it		This event does not affect system operation if it is not recorded after connecting to the internet.
202	Microsoft-Windows-DeviceSetupManager	Warning	The Network List Manager reports no connectivity to the internet.
	When running an OS for the first time or rebooting it		This event does not affect system operation if it is not recorded after connecting to the internet.
506	Microsoft-Windows-DeviceManagement-Pushrouter	Error	DmWapPushService: Failed to register WNF with EventAggregator for WAP messages received by SMS Router. Result: (0xC002000B).
	When running an OS for the first time		This event does not affect system operation if it is recorded only on the first startup and not recorded repeatedly.

Windows Server 2012 R2

System Log

4	l2nd	Warning	HPE Ethernet 10Gb 2-port 530SFP+ Adapter #xx: The network link is down. Check to make sure the network cable is properly connected.
	When installing an OS, starting system, or applying Standard Program Package		This event does not affect system operation.
4	l2nd	Warning	HPE Ethernet 10Gb 2-port 530T Adapter #xx: The network link is down. Check to make sure the network cable is properly connected.
	When installing an OS, starting system, or applying Standard Program Package		This event does not affect system operation.
4	l2nd	Warning	HPE FlexFabric 10Gb 2-port 533FLR-T Adapter #xx: The network link is down. Check to make sure the network cable is properly connected.
	When installing an OS, starting system, or applying Standard Program Package		This event does not affect system operation.
4	l2nd	Warning	Broadcom BCM57810 #xx: The network link is down. Check to make sure the network cable is properly connected.
	When installing an OS		This event does not affect system operation.
4	l2nd2	Warning	HPE Ethernet #xx: The network link is down. Check to make sure the network cable is properly connected.
	When installing an OS, starting system, or applying Standard Program Package		This event does not affect system operation. Besides, the device name in this event is not shown correctly but it does not affect the operation of the device.
4	q57nd60a	Warning	HPE Ethernet 1Gb 4-port 331i Adapter #xx: The network link is down. Check to make sure the network cable is properly connected.
	When installing an OS, starting system, or applying Standard Program Package		This event does not affect system operation.
4	q57nd60a	Warning	HPE Ethernet 1Gb 4-port 331T Adapter #xx: The network link is down. Check to make sure the network cable is properly connected.
	When installing an OS, starting system, or applying Standard Program Package		This event does not affect system operation.

4	q57nd60a	Warning	HPE Ethernet 1Gb 4-port 331FLR Adapter #xx: The network link is down. Check to make sure the network cable is properly connected.
	When installing an OS, starting system, or applying Standard Program Package		This event does not affect system operation.
4	q57nd60a	Warning	HPE Ethernet 1Gb 2-port 332T Adapter #xx: The network link is down. Check to make sure the network cable is properly connected.
	When installing an OS, starting system, or applying Standard Program Package		This event does not affect system operation.
4	b57nd60a	Warning	Broadcom NetXtreme Gigabit Ethernet #xx: The network link is down. Check to make sure the network cable is properly connected.
	When installing an OS		This event does not affect system operation.
27	ixgbs	Warning	HPE Ethernet 10Gb 2-port 562FLR-T Adapter #xx The network link has been cut off.
	When installing an OS, starting system, or applying Standard Program Package		This event does not affect system operation.
27	ixgbs	Warning	HPE Ethernet 10Gb 2-port 562T Adapter #xx Network link is disconnected.
	When installing an OS, starting system, or applying Standard Program Package		This event does not affect system operation.
27	i40ea	Warning	HPE Ethernet 10Gb 2-port 562SFP+ Adapter #xx Network link is disconnected.
	When installing an OS, starting system, or applying Standard Program Package		This event does not affect system operation.
27	i40ea	Warning	HPE Ethernet 10Gb 562SFP+ Adapter #xx Network link is disconnected.
	When installing an OS, starting system, or applying Standard Program Package		This event does not affect system operation.
27	i40ea	Warning	HP Ethernet 10Gb 2-port 562FLR-SFP+ Adapter Network link is disconnected.
	When installing an OS, starting system, or applying Standard Program Package		This event does not affect system operation.
46	volmgr	Error	Crash dump initialization failed!
	When installing an OS		Go to the following Microsoft website for details. http://support.microsoft.com/kb/2756313
134	Microsoft-Windows-Time-Service	Warning	NtpClient was unable to set a manual peer to use as a time source because of a DNS resolution error on 'time.windows.com,0x9'. NtpClient will try again in 15 minutes and double the reattempt interval thereafter.
	When installing an OS, starting system, or applying Starter Pack		If it is not registered after connecting to the Internet, there is no problem with system operation.

1500	SNMP	Error	The SNMP Service encountered an error while accessing the registry key SYSTEM\CurrentControlSet\Services\SNMP\Parameters\TrapConfiguration.
	When installing an OS		If this event is logged only when SNMP is enabled and does not occur repeatedly, there is no problem with system operation. Go to the following Microsoft website for details. http://support.microsoft.com/kb/2002303/
7023	Service Control Manager	Error	The Network List Service terminated with the following error: The device is not ready.
	When installing an OS		If this event is logged only when installing an OS and does not occur repeatedly, there is no problem in system operation.
7023	Service Control Manager	Error	The IP Helper service terminated with the following error: The service cannot be started, either because it is disabled or because there are no enabled devices associated with it.
	When starting an OS		If this event is logged only when installing an OS and does not occur repeatedly, there is no problem in system operation.
7023	Service Control Manager	Error	The WMI Performance Adapter service terminated with the following error: The error cannot be identified.
	When starting an OS or shutting down an OS		Ignore this error because there is no impact on the system.
7030	Service Control Manager	Error	Printer Extensions and Notifications service is marked as interactive service. However, the system is not allowed to use interactive service. Thus, this service might not work correctly.
	When installing an OS		If this event is logged only when installing an OS and does not occur repeatedly, there is no problem in system operation.
10010	Microsoft-Windows-DistributedCOM	Error	The server {xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx} did not register in DCOM within the necessary timeout period.
	When installing an OS		For details, refer to the following website: http://support.microsoft.com/kb/956479/ja (Japanese only)
10016	Microsoft-Windows-DistributedCOM	Error	In the settings of application-specific access authorization, access authorization of local activation for COM server applications with CLSID {D63B10C5-BB46-4990-A94F-E40B9D520160} and APPID {9CA88EE3-ACB7-47C8-AFC4-AB702511C276} cannot be granted to the user NT AUTHORITY SYSTEM SID (S-1-5-18) whose address is LocalHost (LRPC used) running with an SID unable to use application containers (utilization disabled). This security access authorization can be changed using the component service management tool.
	When running an OS for the first time		If this is logged at the first boot of OS and the same event log is not continuously logged, there is no problem.
10149	Microsoft-Windows-WinRM	Warning	The WinRM service is not listening for WS-Management requests.
	When installing an OS		If this event is logged together with ID 7036 "Service Control Manager (Windows Remote Management (WS-Management) service has stopped.), there is no problem in system operation. Also, if WinRM event 10148 (WinRM service is listening WS-Management requests.) is output immediately after this event, there is no problem in system operation.

Application Event Log

24	Microsoft-Windows-WMI	Error	Event provider MLNXProvider attempted to register query "select * from MLNX_NetAdapterStatusEvent" whose target class "MLNX_NetAdapterStatusEvent" in //./root/standardcimv2/mlnx namespace does not exist. The query will be ignored. * There may be cases that the above message is somewhat different.
	At the time of applying Starter Pack		This event is logged in the system when InfiniBand Adapter is connected. This event does not affect system operation.
1014	Microsoft-Windows-Security-SPP	Error	Failed to obtain end-user license. hr=0x80072EE7
	When installing an OS		If this event is logged only when installing an OS and does not occur repeatedly, there is no problem in system operation.
1015	Microsoft-Windows-Security-SPP	Warning	Detailed information of HRESULT Returned hr=0xC004F022, original hr=0x80049E00
	When installing an OS		If this event is logged only when installing an OS and does not occur repeatedly, there is no problem in system operation.
1058	Microsoft-Windows-Security-SPP	Error	Failed to obtain certificate of purchase from ACPI table. Error code: 0xC004F057
	When installing an OS		This event does not affect system operation.
1534	Microsoft-Windows-User Profiles Service	Warning	Profile notification of event Create for component {2c86c843-77ae-4284-9722-27d65366543c} failed.
	When installing an OS		If this event is logged only when installing an OS and does not occur repeatedly, there is no problem in system operation. Error code is not implemented.
8198	Microsoft-Windows-Security-SPP	Error	License Activation (slui.exe) failed with the following error code: Error code: hr=0xC004F063
	When installing an OS		Unless this event is not logged after license authentication, there is no problem in system operation.
8200	Microsoft-Windows-Security-SPP	Error	Detailed information about failure of license authentication hr=0x80072EE7
	When installing an OS		Unless this event is not logged repeatedly after license authentication, there is no problem in system operation.

Applications and Services Logs

2	Microsoft-Windows-Kernel-EventTracing	Error	The session "" cannot be started due to the following error: 0xC000000D
	When running the system		If it is logged at the time of displaying the management screen of the computer, there is no problem.
104	Microsoft-Windows-DeviceSetupManager	Error	The DSM service cannot be started. Result=0x800706B5
	When installing an OS		If this is logged when the OS is installed and the same event log is not continuously logged, there is no problem.

200	Microsoft-Windows-DeviceSetupManager	Warning	A connection to the Windows Update Services could not be established.
	When running the system		If this event is not registered after the Internet connection is established, there is no problem in system operation.
201	Microsoft-Windows-DeviceSetupManager	Warning	A connection to the Windows Metadata and Internet Services (WMIS) could not be established.
	When running the system		If this event is not registered after the Internet connection is established, there is no problem in system operation.
202	Microsoft-Windows-DeviceSetupManager	Warning	The Network List Manager reports no connectivity to the internet.
	When running the system		If this event is not registered after the Internet connection is established, there is no problem in system operation.
215	Microsoft-Windows-AppReadiness	Error	'ART:ResolveStoreCategories' of Administrator failed. Error: 'Class not registered' (0.0469065 sec.)
	When installing an OS		If this event is logged only at the first sign-in after OS installation and does not occur repeatedly, there is no problem in system operation.
1001	Microsoft-Windows-Dhcp-Client	Error	The address of the network card with the network address of <MAC address> could not be assigned to this computer from the network (DHCP server). The following error occurred: 0x79 Address acquisition is tried again from the network address (DHCP) server.
	When installing an OS or Starter Pack		If this does not occur continuously, there is no problem of system operation.

3. Accessing Data for Electric Power, Temperature, and Processor Utilization

This section describes how to access data related to input power consumption in watts, intake temperature, and all logical processor utilizations in the Express Server during usual operation in accordance with ENERGY STAR® Program Requirements.

3.1 Windows

The sample program below is verified to be run normally on Windows Server 2016.

3.1.1 Power consumption

Execute the following commands to access power consumption readings on Baseboard Management Controller (BMC) by using Intelligent Platform Management Interface (IPMI).

`Network Function Code:` 2Ch (Group Extension)

`Command Code:` 02h (Get Power Reading)

Request Data : 000001DCh

Below is the sample file created by using Visual Basic Script (named as Power.vbs).

```
' Start Script
Option Explicit

' Prepare for IPMI Driver
Dim osvc, oclass
Dim oinstance, oipmi
set osvc = getobject("winmgmts:root¥wmi")
set oclass = osvc.get("microsoft_ipmi")
for each oinstance in osvc.instancesof("microsoft_ipmi")
        set oipmi = oinstance
next

'Format the IPMI command request
Dim oinparams
set oinparams = oclass.methods_("requestresponse").inparameters
oinparams.networkfunction = &h2c
oinparams.lun = 0
oinparams.responderaddress = &h20
oinparams.command = &h02
oinparams.requestdata = array (&hdc, &h01, &h00, &h00)
oinparams.requestdatasize = 4


'call the driver
Dim outparams
set outparams = oipmi.execmethod_("requestresponse",oinparams)

WScript.Echo " Completion Code = 0x" & hex(outparams.Completioncode)
If outparams.Completioncode <> 0 Then
   Wscript.Echo " Not supported"
Else
   'WScript.Echo " Data LS Byte    = 0x" & hex(outparams.ResponseData(2))
   'WScript.Echo " Data MS Byte    = 0x" & hex(outparams.ResponseData(3))
   WScript.Echo " Power Consumption = " & outparams.ResponseData(3)*256 + _
                                       outparams.ResponseData(2) & " watts"
End If
' End Script
    ' Start Script
```

- Execution example

```
C:¥VBS> cscript //nologo Power.vbs
```

- Execution result

```
Completion Code = 0x0
Power Consumption = 306 watts
```

The power consumption is 306 watts.

Tips Power consumption readings may not be acquired depending on the power supply configuration of the server.
The completion code in such cases is `0xC1` or `0xCB`.

3.1.2 Intake air temperature

Execute the following standard commands that conform to IPMI to search Sensor Data Record (SDR) for the temperature sensor and obtain intake air temperature data.

- `Get SDR Repository Info`
- `Reserve SDR Repository`
- `Get SDR`
- `Get Sensor Reading`

Below is the sample file created by using Visual Basic Script (named as Sensor.vbs),

```
'Start Script
Option Explicit

' Prepare for MS IPMI Driver
Dim osvc, oclass
Dim oinstance, oipmi
set osvc = getobject("winmgmts:root¥wmi")
set oclass = osvc.get("microsoft_ipmi")
for each oinstance in osvc.instancesof("microsoft_ipmi")
         set oipmi = oinstance
next

' (Get SDR Repository Info)
Dim oinparams
set oinparams = oclass.methods_("requestresponse").inparameters
' (Get SDR Repository Info)
oinparams.networkfunction = &ha
oinparams.lun = 0
oinparams.responderaddress = &h20
oinparams.command = &h20
oinparams.requestdatasize = 0
' Fire IPMI Command
Dim outparams
Dim i, RecordCount
set outparams = oipmi.execmethod_("requestresponse",oinparams)
RecordCount = outparams.ResponseData(3)*256 + outparams.ResponseData(2)

' (Reserve SDR Repository)
oinparams.networkfunction = &ha
oinparams.lun = 0
oinparams.responderaddress = &h20
oinparams.command = &h22
oinparams.requestdatasize = 0
Dim Reserve_LS, Reserve_MS
set outparams = oipmi.execmethod_("requestresponse",oinparams)
Reserve_LS = outparams.ResponseData(1)
Reserve_MS = outparams.ResponseData(2)

' (Get SDR) for each record
Dim Record_LS,Record_MS, Offset, Length
Dim cnt, sensorNum, sensorType
' First Record
Record_LS = 0
Record_MS = 0
For cnt = 0 to RecordCount-1
   Offset = 0
   Length = 9
   oinparams.networkfunction = &ha
   oinparams.lun = 0
   oinparams.responderaddress = &h20
   oinparams.command = &h23
   oinparams.requestdata = array(Reserve_LS, Reserve_MS, Record_LS, Record_MS, Offset, Length)
   oinparams.requestdatasize = 6
   set outparams = oipmi.execmethod_("requestresponse",oinparams)
```

```
    If outparams.Completioncode = 0 Then
       If outparams.ResponseData(6) = 1 Then          ' Full Sensor Record
          call GetSensorType(Reserve_LS, Reserve_MS, Record_LS, Record_MS, sensorType)
          If sensorType = 1 Then                    ' Temperature
             WScript.Echo "========================================="
             call GetIDString(Reserve_LS, Reserve_MS, Record_LS, Record_MS)
             WScript.Echo " Sensor Type = Temperature"
             sensorNum = outparams.ResponseData(10)
             call GetSensor(Reserve_LS, Reserve_MS, Record_LS, Record_MS,sensorNum)
          End If
       End If
       Record_LS = outparams.ResponseData(1)
       Record_MS = outparams.ResponseData(2)
       If Record_LS = &hff And Record_MS = &hff Then
           exit For
       End If
    End If
Next

Sub GetSensorType(rv_ls, rv_ms, rc_ls, rc_ms, sensorType)
    Dim outtmp
    oinparams.networkfunction = &ha
    oinparams.lun = 0
    oinparams.responderaddress = &h20
    oinparams.command = &h23
    oinparams.requestdata = array(rv_ls, rv_ms, rc_ls, rc_ms, 12, 2)
    oinparams.requestdatasize = 6
    set outtmp = oipmi.execmethod_("requestresponse",oinparams)
    sensorType = outtmp.ResponseData(3)
End Sub

Sub GetSensor(rv_ls, rv_ms, rc_ls, rc_ms, sensorNum)
    Dim outtmp, units1, units2, sensortype
    oinparams.networkfunction = &ha
    oinparams.lun = 0
    oinparams.responderaddress = &h20
    oinparams.command = &h23
    oinparams.requestdata = array(rv_ls, rv_ms, rc_ls, rc_ms, 20, 14)
    oinparams.requestdatasize = 6
    set outtmp = oipmi.execmethod_("requestresponse",oinparams)

    units1 = outtmp.ResponseData(3)
    Select Case outtmp.ResponseData(4)
       case 0: units2 = "unspecified"
       case 1: units2 = "degrees C"
       case 6: units2 = "Watts"
       case else: units2 = "Refer to IPMI Specification: Type=0x" _
                           & hex(outtmp.ResponseData(4))
    End Select

    ' (Get Sendor Reading)
    Dim sensorData, rawData, currentValue
    oinparams.networkfunction = &h4
    oinparams.lun = 0
    oinparams.responderaddress = &h20
    oinparams.command = &h2d
    oinparams.requestdata = array(sensorNum)
    oinparams.requestdatasize = 1
    set sensorData = oipmi.execmethod_("requestresponse",oinparams)
    If sensorData.Completioncode <> 0 Then
       'WScript.Echo " Sensor Not Available"
       exit Sub
    End If
    rawData = sensorData.ResponseData(1)
    If units1 and &h40 Then
       If rawData And &h80 Then
          rawData = rawData Xor &hff
       End If
    Elseif units1 and &h80 Then
       call get2complement(rawData, rawData, 8)
    End If
    If (sensorData.ResponseData(2) And &h80) = 0 Or _
      (sensorData.ResponseData(2) And &h40) = 0 Or _
      (sensorData.ResponseData(2) And &h20) Then
       WScript.Echo " Event Status: Unavailable"
    Else
       'WScript.Echo " Event Status: ok"
       Dim M,B,k1,k2
       Dim ret
       M = (outtmp.ResponseData(8) And &hc0) * 4 + outtmp.ResponseData(7)
       B = (outtmp.ResponseData(10) And &hc0) * 4 + outtmp.ResponseData(9)
       call get2complement(M, M, 10)
       call get2complement(B, B, 10)
       call get2complement(outtmp.ResponseData(12) And &h0f, k1, 4)
       call get2complement((outtmp.ResponseData(12) And &hf0)/16, k2, 4)
       currentValue = CDbl (((M * rawData) + (B * (10 ^ k1))) * (10 ^ k2))
       WScript.Echo " Current Value = " & currentValue & " " & units2
    End If
End Sub
```

```
Sub get2complement(raw, rv, bit)
   Select Case bit
      case 4:
         If raw And &h8 Then
            rv = 0 - ((&h10 - raw) and &h0f)
         Else
            rv = raw
         End If
      case 8:
         If raw And &h80 Then
            rv = 0 - ((&h100 - raw) and &h0ff)
         Else
            rv = raw
         End If
      case 10:
         If raw And &h200 Then
            rv = 0 - ((&h400 - raw) and &h3ff)
         Else
            rv = raw
         End If
   End Select
End Sub

Sub GetIDString(rv_ls, rv_ms, rc_ls, rc_ms)
   Dim tmpMessage
   Dim outsdridstringtype
   oinparams.networkfunction = &ha
   oinparams.lun = 0
   oinparams.responderaddress = &h20
   oinparams.command = &h23
   oinparams.requestdata = array(rv_ls, rv_ms, rc_ls, rc_ms, 47, 1)
   oinparams.requestdatasize = 6
   set outsdridstringtype = oipmi.execmethod_("requestresponse",oinparams)

   Dim outsdridstring
   Dim idlength, j
   idlength = outsdridstringtype.ResponseData(3) and 31
   oinparams.networkfunction = &ha
   oinparams.lun = 0
   oinparams.responderaddress = &h20
   oinparams.command = &h23
   oinparams.requestdata = array(rv_ls, rv_ms, rc_ls, rc_ms, 48, idlength)
   oinparams.requestdatasize = 6
   set outsdridstring = oipmi.execmethod_("requestresponse",oinparams)
   tmpMessage = " ID String = "
   For j = 3 to idlength + 2
      tmpMessage = tmpMessage & Chr(outsdridstring.ResponseData(j))
   Next
   WScript.Echo tmpMessage
End Sub
'End Script
```

- Execution example

```
C:¥VBS> cscript //nologo Sensor.vbs
```

- Execution result

```
==========================================
 ID String = Baseboard Temp4
 Sensor Type = Temperature
 Current Value = 45 degrees C
==========================================
 ID String = FntPnl Amb Temp
 Sensor Type = Temperature
 Current Value = 27 degrees C
==========================================
 ID String = CPU1_DIMM1 Temp
 Sensor Type = Temperature
 Current Value = 35 degrees C
==========================================
 ID String = CPU1_DIMM2 Temp
 Sensor Type = Temperature
 Event Status: Unavailable
==========================================
```

Intake air temperature data is obtained from the sensor with an ID string that contains any of the following: `Amb`, `Ambient`, or `Front Panel`.

In the case of the sample above, the data is obtained from a sensor that contains `FntPnl Amb Temp` in its ID, with a resulting intake air temperature of 27°C.

3.1.3 Processor utilization

The utilization rate of all logical processors is given by executing the Win32_PerfFormattedData_PerfOS_Processor class that Windows OS provides. Below is the sample file created by using Visual Basic Script (named as Proc.vbs). This script outputs the processor utilization rate every 30 seconds.

```
' Start Script
strComputer = "."
Set objWMIService = GetObject("winmgmts:" _
   & "{impersonationLevel=impersonate}!¥¥" & strComputer & "¥root¥cimv2")
set objRefresher = CreateObject("WbemScripting.Swbemrefresher")
Set objProcessor = objRefresher.AddEnum _
   (objWMIService, "Win32_PerfFormattedData_PerfOS_Processor").objectSet
objRefresher.Refresh
Dim first
first = true
Do
  For each intProcessorUse in objProcessor
    If first Then
      If intProcessorUse.Name = "_Total" Then
        first = false
      End If
    else
      Wscript.Echo "Proc" & intProcessorUse.Name & " : " & _
                 "PercentProcessorTime=" & _
                 intProcessorUse.PercentProcessorTime
    End If
  Next
  Wscript.Sleep 30*1000   'sleep 30 * 1000ms
  objRefresher.Refresh
Loop
' End Script
```

- Execution example

```
C:¥VBS> cscript //nologo Proc.vbs
```

- Execution result

```
Proc0 : PercentProcessorTime=0
Proc1 : PercentProcessorTime=0
Proc2 : PercentProcessorTime=0
Proc3 : PercentProcessorTime=0
Proc4 : PercentProcessorTime=76
Proc5 : PercentProcessorTime=0
Proc6 : PercentProcessorTime=0
Proc7 : PercentProcessorTime=0
Proc_Total : PercentProcessorTime=9
```

`Proc 0` to `Proc 7` show the utilization rate of each processor while `Proc_Total` shows the total processor utilization rate.

4. Glossary

Terms	Description
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.
EXPRESSBUILDER	Software for setting up the server. EXPRESSBUILDER can be started by pressing <F10> key during POST.
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.
Hexalobular	A type of screw head characterized by a 6-point star-shaped pattern. This is often called as "Torx" (the Torx is a third party's trademark). Head sizes are described from T1 to T100. This is sometimes abbreviated as 6lobe.
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.
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.
NEC ESMPRO Manager	Software for managing a number of servers on network.
PC for Management	A computer for managing the server on network. A general Windows/Linux computer can be used as "PC for Management".
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.
RAID Report Service	This service monitors the RAID status and notifies failures.
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.
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.
SID	System Insight Display (SID) is an optional product that can indicate the statuses of each device on motherboard.
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.
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.
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.
TPM Kit	An optional product of Trusted Platform Module for the server.

5. Revision Record

Revision (Document Number)	Date Issued	Description
10.201.01-104.01	August 2017	Newly created
10.201.01-104.02	November 2017	PCIe SSD (NVMe) has been supported. Event logs have been added.

NEC Express Server

Express5800/R120h-1M, R120h-2M
Maintenance Guide

November 2017

NEC Corporation
7-1 Shiba 5-Chome, Minato-Ku
Tokyo 108-8001, Japan