ThinkSystem HR330A User Guide and Hardware Maintenance Manual

Please read this manual before using the product.

Contents

Disclaimer

Thank you for purchasing a Lenovo product.

This manual is intended as a guide to the use of Lenovo server products (hereinafter referred to as "Product"). Before installing and using the Product for the first time, be sure to carefully read all information provided with the product, especially the precautions stated in this manual. This will help you use the Product more effectively and safely. Please keep this manual for future reference.

The descriptions in this manual are not intended as specifications for the Product or of its hardware or software settings. For actual product specifications and settings, please refer to relevant agreements, packing lists, or any documents describing product specifications and settings. Alternatively, you may contact the seller for more information.

Lenovo shall not be liable for any damage that may result from the improper installation, use or storage of this Product in proper manner or as instructed in this manual, or of any damage that may result from the repair or modification of this Product by anyone other than authorized technical personnel.

The photographs, pictures, diagrams and illustrations provided in this manual are for illustrative and descriptive purposes only, and may differ from the actual product. Due to continued product improvements, product specifications may change from time to time, and may differ from the contents of this manual.

References to third party websites are provided for the convenience of our users. The information contained in these websites does not constitute part of Lenovo's product information and are not part of the services provided by Lenovo. Lenovo shall not be responsible for the accuracy and reliability of these websites and of the information contained therein. Such websites should only be accessed at the user's own risks.

The contents of this manual shall not be construed to constitute any expressed or implied warranty or guarantee by Lenovo for its products or services, including (but not limited to) the applicability, safety, salability, or suitability of the products to the stated purposes. The guarantee and warranty for this Product and its related services shall be executed according to applicable agreements, or standard product warranty terms and conditions. Lenovo shall not be liable for any damage arising from the use or inability to use the Product, including, but not limited to, direct or indirect personal damages, loss of business profits, business interruption, loss of business information, or any other pecuniary loss, to the greatest legal extent possible.

Lenovo accepts no responsibility for the use of the software supplied with this Product on any other devices, or for using software other than that provided with the Product or which has been verified and recommended by Lenovo on this Product.

Although due care has been taken in compiling and checking the information provided in this manual, we cannot guarantee that the Information is free from error and omission. As an effort towards improving our service, the contents of this manual, as well as the software and hardware described herein, are subject to changes without notice. Should you find any inconsistency between the actual Product and the contents of this manual, or should you wish to find out the latest information or to send us your questions or comments, please call our service hotline or visit the Lenovo service website.

Trademarks

Safety Information

IMPORTANT: Each caution and danger statement in this document is labeled with a number. This number is used to cross reference an English-language caution or danger statement with translated versions of the caution or danger statement in the Safety Information document.

Be sure to read all caution and danger statements in this document before you perform the procedures. Be sure to read all additional safety information that comes with the server and the optional device before you install, remove or replace any device.

Statement 1

DANGER

Electrical current from power, telephone, and communication cables is hazardous. To avoid a shock hazard:

•Do not connect or disconnect any cables or perform installation, maintenance, or reconfiguration of this Product during an electrical storm.

•Connect all power cords to properly wired and grounded electrical outlets.

•Connect all equipment that will be attached to this Product to properly wired outlets.

•When possible, use one hand only to connect or disconnect signal cables.

•Never turn on any equipment when there is evidence of fire, water, or structural damage.

•Disconnect the attached power cords, telecommunications systems, networks, and modems before you open the device covers, unless otherwise instructed in the installation and configuration procedures.

•Connect and disconnect cables as described in the following table when installing, moving, or opening covers on this Product or the attached devices.

The power button on the front panel does not disconnect the internal system from the AC power supply completely. To prevent electrical shock and equipment damage, be sure to unplug the power cord from the power outlet before performing any operation described in this manual.

To connect:	To disconnect:
1. Turn everything OFF. 2. First, attach all cables to devices. 3. Attach signal cables to connectors. 4. Attach power cords to outlet. 5. Turn device ON.	1. Turn everything OFF. 2. First, remove power cords from outlet. 3. Remove signal cables from connectors. 4. Remove all cables from devices.

Do not plug or unplug any connector from the chassis backplane without first disconnecting the power supply.

Statement 2

DANGER

Danger of explosion if battery is incorrectly replaced. When replacing the lithium coin cell battery, use only the same or an equivalent type that is recommended by the manufacturer. The battery contains lithium and can explode if not properly used, handled, or disposed of.
Do not:
1. Throw or immerse into water
2. Heat to more than 100℃ (212°F)
3. Repair or disassemble
Dispose of the battery as required by local ordinances or regulations.

Statement 3

CAUTION:

When laser products (such as CD-ROMs, DVD drives, fiber optic devices, or transmitters) are installed, note the following:

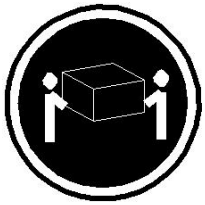
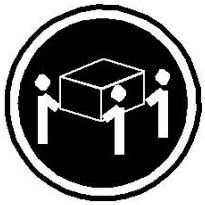
•Do not remove the covers. Removing the covers of laser products may result in exposure to hazardous laser radiation. There are no serviceable parts inside these devices.

•Controls or adjustments, or performance of procedures other than those specified herein, may result in hazardous radiation exposure.

DANGER

Some laser products contain embedded Class 3A or Class 3B laser diodes. Note the following: Laser radiation when open. Do not stare into the beam, do not view directly with optical instruments, and avoid direct exposure to the beam.

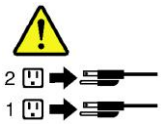
Statement 4

		
≥ 18 kg (39.7 lb)	≥ 32 kg (70.5 lb)	≥ 55 kg (121.2 lb)
< 32 kg (70.5 lb)	< 55 kg (121.2 lb)	< 100 kg (220.5 lb)

CAUTION: Use safe practices when lifting.

Statement 5

CAUTION: The power control button on the device and the power switch on the power supply do not turn off the electrical current supplied to the device. The device may have more than one power cord. To remove all electrical current from the device, ensure that all power cords are disconnected from the power source.



Statement 6

CAUTION: If you install a strain-relief bracket option over the end of the power cord that is connected to the device, you must connect the other end of the power cord to a power source that is easily accessible, in case it needs to be disconnected.

Statement 7

CAUTION: If the device has doors, ensure that you remove or secure the doors before moving or lifting the device to protect against personal injury. The doors will not support the weight of the device.

Statement 8

CAUTION: Never remove the cover on a power supply or any part that has the following label attached.

Hazardous voltage, current, and energy levels are present inside any component that has this label attached. There are no serviceable parts inside these components. If you suspect a problem with one of these parts, contact a service technician.

Statement 9

CAUTION: Disconnect the hot-swap fan cables before removing the fan from the device to protect against personal injury.

Statement 10

CAUTION: The following label indicates a sharp-edge hazard.

Statement 11

CAUTION: The following label indicates a potential heat hazard.

Statement 12

DANGER

Overloading a branch circuit is a potential fire hazard and shock hazard under certain conditions. To avoid these hazards, ensure that your system electrical requirements do not exceed branch current ratings at the installation site.

Statement 13

CAUTION: Ensure that the rack is secured properly to avoid tipping when the server unit is extended on the rails.

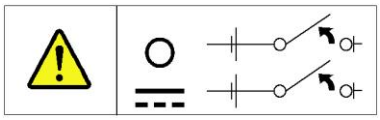
Statement 14

CAUTION: Some accessory or option board outputs exceed Class 2 or limited power source limits. You must install the appropriate interconnecting cabling in accordance with your local electrical code requirements.

Statement 15

CAUTION: The power-control button on the device may put the device in standby mode instead of turning off the device. In addition, the device may have multiple connections to DC power. To remove all electrical current from the device, ensure that all connections to DC power are disconnected at the DC power input terminals.

Statement 16



CAUTION: To reduce the risk of electric shock or energy hazards:

•This equipment must be installed by trained service personnel in a restricted-access location, as defined by your local electrical code and the latest edition of IEC 60950.

•Connect the equipment to a reliably grounded safety extra low voltage (SELV) source. An SELV source is a secondary circuit that is designed so that normal and single fault conditions do not cause the voltages to exceed a safe level (60 V direct current).

•The branch circuit overcurrent protection must be rated in accordance with local electrical code requirements.

•Use only 1.3 mm^2 or 16 American Wire Gauge (AWG) copper conductors, not exceeding 3 meters in length.
•Torque the wiring-terminal screws to 1.4 newton-meters (12 inch-pounds).

•Provide a readily available approved and rated disconnect device in the field wiring.

Statement 17

CAUTION:

This Product contains a Class 1M laser. Do not view directly with optical instruments.

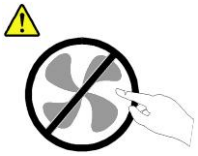
Statement 18

CAUTION:

Do not place any object on top of rack-mounted products.

Statement 19

CAUTION:
Hazardous moving parts are nearby. Keep fingers and other body parts away.



Statement 20

The device is equipped with a replaceable battery. Using an incorrect battery may present a risk of explosion.

Caution: Risk of explosion if battery is replaced with an incorrect type. Dispose of used batteries as instructed.

Statement 21

This device is not intended for use in the direct field of view at visual display workplaces. To avoid incommoding reflex ions at visual display workplaces this device must not be placed in the direct field of view.

Chapter 1 Introduction

This chapter provides an overview of the server and details its features and specifications. Depending on the model, some features might not be available, or some specifications might not apply.

1.1 Product overview

The ThinkSystem™ HR330A is a 1U rack server that combines performance, flexibility, and manageability into a package. It uses the latest Ampere ARM eMAG 8180 server processor and supports up to 16 DDR4 dual-inline memory modules (DIMMs). The front panel of the server supports up to four 3.5-inch SATA/NVMe hard disk drives (HDDs). The server supports a maximum of two 550-watt hot-swap power supplies for redundancy power support. These combined features makes this server ideal for various server applications, include storage server, file server, and QA server.

1.2 Features

1.2.1 High reliability

1. Supports DDR4 2667/2400 ECC memory.
2. Supports hot-swap SATA SSD HDD.
3. Uses highly-reliable, server-dedicated power supply.

1.2.2 High availability

1. Supports one Ampere eMAG 8180 CPU (up to 32 cores).
2. Supports DDR4 2667/2400 RDIMM.

1.2.3 High expandability

1. Supports three PCIe slots (Riser Card 1 supporting one slot + Riser Card 2 supporting two slots).
2. Supports 16 DIMM memory slots (up to 512 GB memory).
3. Supports four 3.5-inch SATA /NVME HDDs.

1.2.4 High manageability

1. Equipped with two front USB connectors.
2. Equipped with automatic power saving and noise reduction technologies that adjust the fan speed according to the actual operating environment.

1.3 Specifications

The following information is a summary of the features and specifications of the server.

Specifications	Descriptions
Processor	One Ampere ARM eMAG 8180, supports up to 32 cores
Memory module	DDR4 2667/ 2400, RDIMM Number of slots: 16 DIMMs
System hard disk support	Up to four 3.5-inch hot-swap SATA/NVME HDDs (NVMe does not support hot-swap.)
Display	Integrated graphics chip
Network	One dedicated management chip
Expansion slots	Supports up to three PCIe slots
Device connectors	One serial connector Two VGA connectors (one on the front panel, one on the rear panel) Four USB 2.0 connectors (two on the front panel, two on the rear panel) One RJ45 connector
System fan	Support hot-plug Features automatic energy saving and noise reduction technologies
Operating system	CentOS 7.5, Oracle Linux 7.5 Note: The supported operating system varies with system configurations. If you have any question, contact Lenovo.
Altitude	Supported altitude* (unpressurized): 0-10 000 ft (0-3048 m) A2: Operating temperature value decreases by 1°C (1.8°F) with every 300 m (984 ft) of altitude increase.
Ambient temperature (operating)	System supports ASHRAE A2-with limitations. Design by project, but if system follows ASHRAE standard, it should follow the below requirements: Maximum rate of change (°C/hr) should be ≤ 20 Humidity transition rate should ≤10%/hr. A2: 10°C (50°F) to 35°C (95°F). Humidity: 8%-80% RH, Non-condensing. Supported Altitude* (unpressurized): 0-10000 ft (0-3050 m) A2 - Derate maximum allowable dry-bulb temperature 1°C/300 m above 900 m. Please refer to ASHRAE standard.
Ambient temperature (transport/storage)	Temperature: -40°C (-40°F) to 70°C (158°F) Humidity: 8%-90% RH, non-condensing
Relative humidity (operating)	8%-90%, non-condensing
Relative humidity (transport/storage)	8%-90%, non-condensing (in original shipping packaging) 8%-90%, non-condensing (without original shipping packaging)
Power supply voltage	Input voltage low range: Minimum: 100 V ac Maximum: 127 V ac Input voltage high range:

	Minimum: 200 V ac Maximum: 240 V ac
Power	Two 550-watt hot-swap power supplies for redundancy support
Dimensions	Height: 43.0 mm (1.7 inches) Width: With rack latches: 481.7 mm (19.0 inches) Without rack latches: 434.4 mm (17.1 inches) Depth: With rack latches: 748.6 mm (29.5 inches) Without rack latches: 734.0 mm (28. inches)

Chapter 2 Server components and hardware replacement procedures

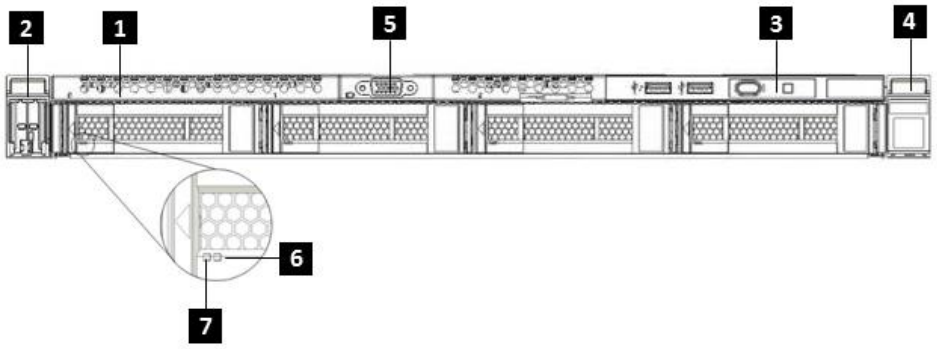
This chapter provides detailed information about the components of the server, and specifies the replacement procedures of related parts.

Note: The following procedures should only be performed by qualified operators or service personnel trained in server maintenance. Do not perform any removal procedure until you have read and understood all warnings and cautions stated in the "Lenovo Server User Guide - Read Me First" (hereinafter referred to as "Read Me First"). All removals should be performed strictly as instructed.

Note: All pictures in this chapter are for reference only, and may differ from actual product appearance.

2.1 Server components

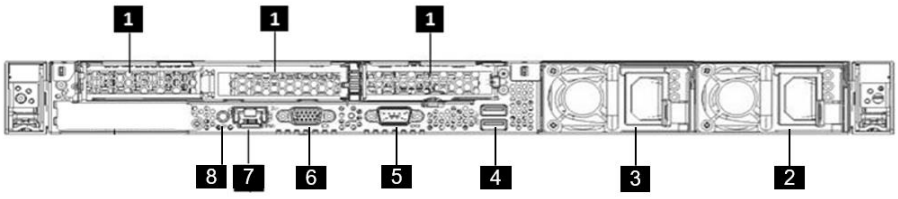
2.1.1 Front view



Front view of the server (four 3.5-inch HDDs configuration)

1. 3.5-inch hot-swap drive (4)	5. Front VGA connector
2. Rack handle (left)	6. Drive status LED (yellow)
3. Front controller module	7. Drive activity LED (green)
4. Rack handle (right)	

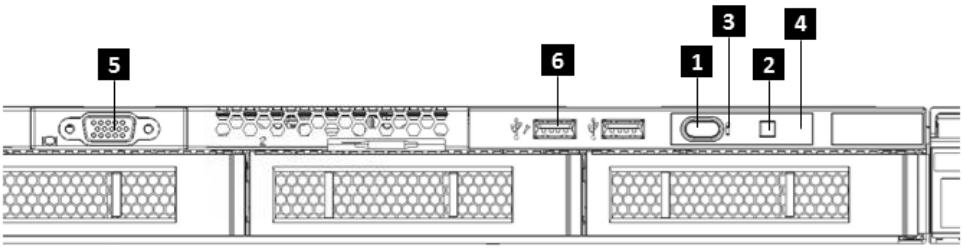
2.1.2 Rear view



Rear views of the server

1. Half-height, half-length PCIe card slot	5. Serial connector
2. Hot-swap power supply 2	6. VGA connector
3. Hot-swap power supply 1	7. Network connection (management)
4. USB 2.0 connector (2)	8. System ID button with LED

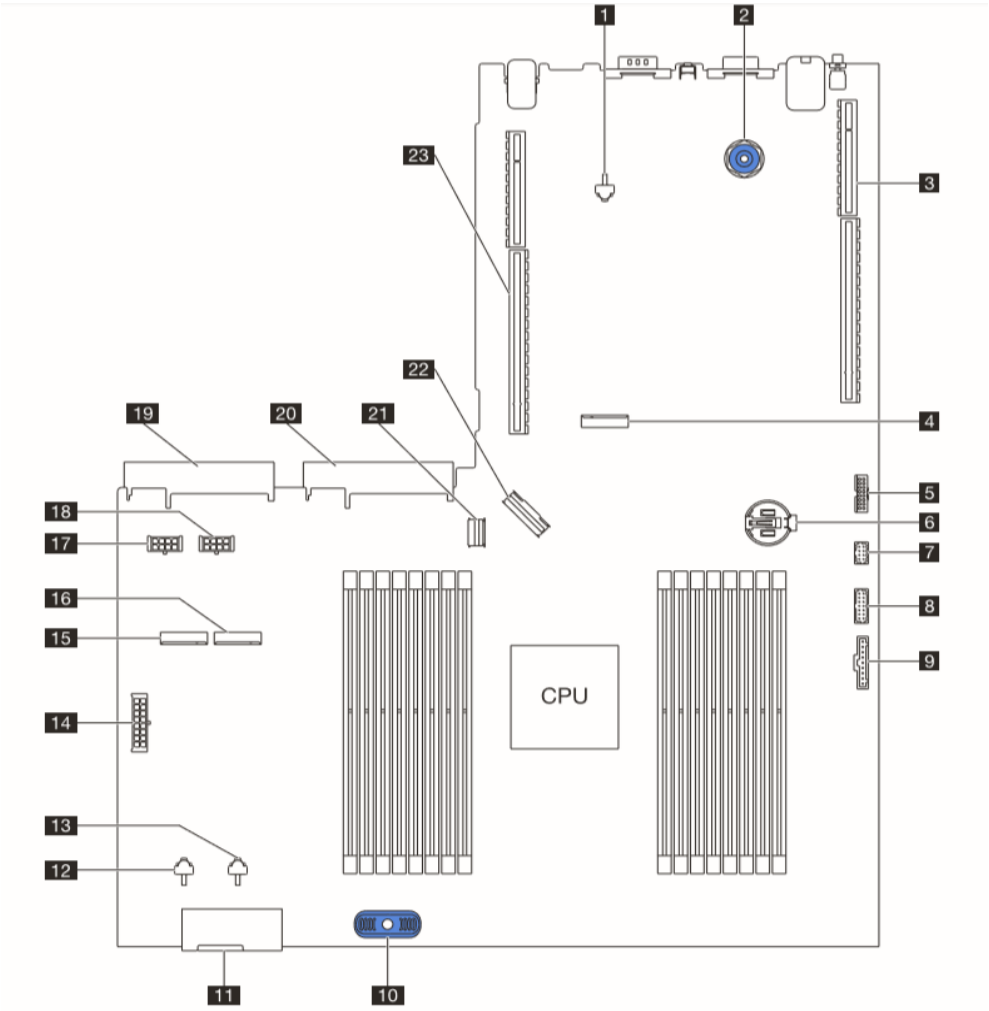
2.1.3 Front control panel



Front control panel

1. Power button with power status LED	1. Steady green light: the server is on. 2. Off: the server is off. 3. Blinking green: the server is DC off.
2. System ID button with ID LED	1. Steady blue light: the server is identified. 2. Off: the server is not identified. 3. Press 5 secs, initiate BMC reset.
3. Network status LED	1. Steady green light: the network is connected. 2. Blinking green light: the network is connected and active. 3. Off: the server is disconnected from the network or the server is off.
4. System health LED	1. Steady yellow light: key component failure. 2. Off: the server is off, or the server is on and is working correctly.
5. VGA connector	
6. USB2.0 connector (2)	

2.1.4 System board components



1. M.2 Clip	13. M.2 Clip
2. System Board Plunger	14. BP Power Connector
3. Riser slot 1	15. M.2 connector (SATA)
4. M.2 connector (PCIe)	16. M.2 connector (SATA)
5. TPM connector	17. GPU power connector 2
6. RTC battery	18. GPU power connector 1
7. Front USB connector	19. PSU 2 connector
8. Front VGA connector	20. PSU 1 connector
9. Front panel connector	21. SATA slimline connector
10. System board handle	22. NVMe slimline connector
11. System fan board connector	23. Riser slot 2
12. M.2 clip	

2.2 Hardware replacement procedures

Safety Precautions

Read and follow all safety precautions specified in "Read Me First". If the instructions provided with the server differs from the instructions contained in this manual, contact a service technician from the supplier to confirm the correct procedures.

Note: The power button does not completely turn off the AC current supplied to the device. To remove all AC current from the device, unplug all power cords connected to the server from the AC power sockets.

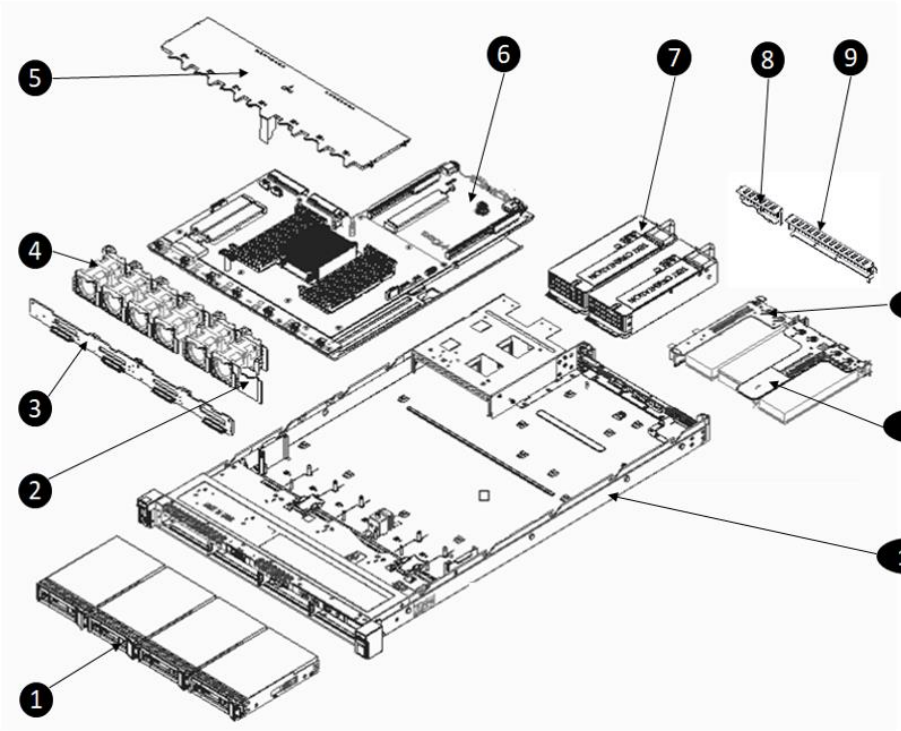
To ensure proper cooling and ventilation, be sure to replace the cover before using the server normally.

As the components of server as extremely sensitive to electrostatic discharge (ESD), the following operations should be performed on ESD workbenches. Where ESD workbenches are not available, minimize ESD damage by doing the following:

1. Wear an ESD wrist strap, and connect it to a metal part of the server.
2. Touch the metal casing of the server chassis before handling other server components.
3. Ensure that part of your body is in contact with the metal chassis when removing or installing a component; this helps to release static electricity.
4. Avoid unnecessary movement.
5. Always handle a component (especially boards) by its edges or frame.
6. Place the server on a grounded, static-free work surface. Use a conductive foam pad if available. Do not use the package that the component came in.
7. Avoid sliding the unit across the work surface.

Tools required
1. Phillips (cross) screwdriver.
2. Anti-static wrist strap and conductive foam pad (recommended).
3. Pen and paper to record changes in server configuration, and information specific to installed components.

2.2.1 Parts list



1. HDD Module	5. System Air duct	9. LP + LP Riser Dummy
2. 4056 Fan Dummy	6. System Board	10. Riser 1 Bracket (LP)
3. 4 x 3.5-inch HDD Backplane	7. Power Supply	11. Riser 2 Bracket (LP + LP)
4. 4056 Fan Module	8. LP Riser Dummy	12. Chassis Base

2.2.2 Rack handles replacement

Do not proceed before reading and understanding the "Safety Precautions" section of this chapter and "Read Me First".

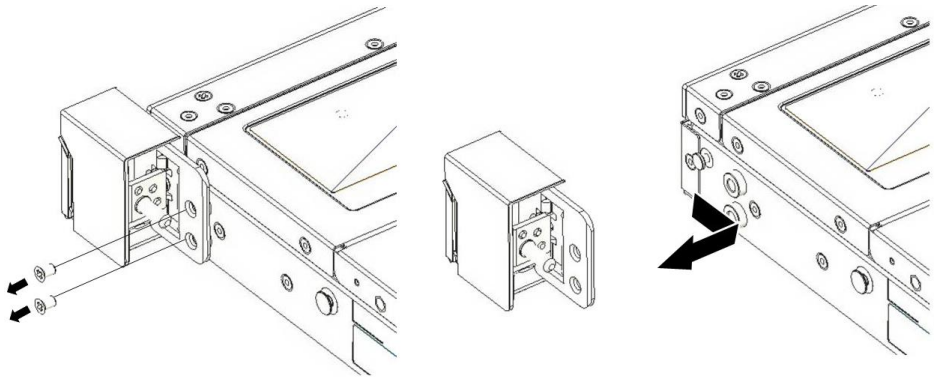
CAUTION:

Do not place any object on top of rack-mounted products.

The power-control button on the device may put the device in standby mode instead of turning off the device. In addition, the device may have multiple connections to DC power. To remove all electrical current from the device, ensure that all connections to DC power are disconnected at the DC power input terminals.

To remove the rack handles, do the following:

1. Turn off all attached devices and the server.
2. Disconnect the ac power cord from the electrical outlet.
3. Remove the screws of the rack handles.
4. Slide and pull-out the rack handles.



To reinstall, reverse the steps above.

2.2.3 Top cover replacement

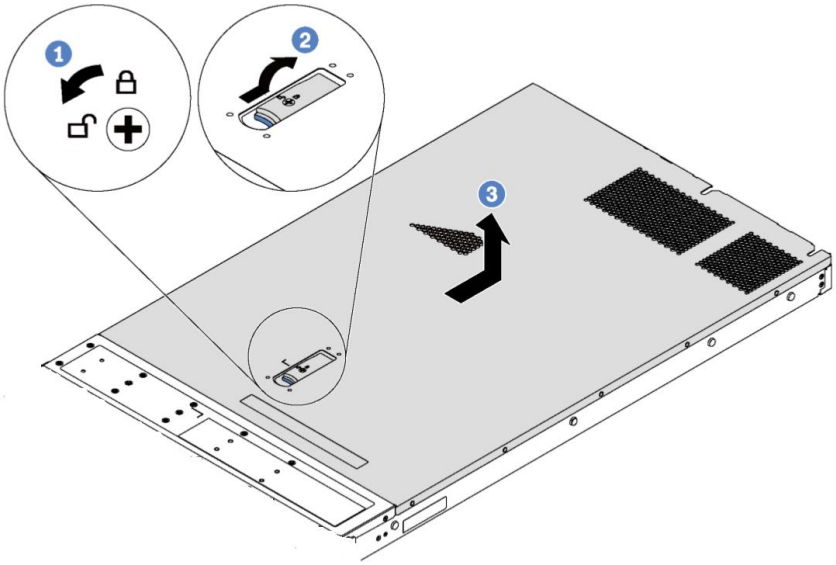
Do not proceed before reading and understanding the "Safety Precautions" section of this chapter and "Read Me First".

CAUTION:

If the device has doors, ensure that you remove or secure the doors before moving or lifting the device to protect against personal injury. The doors will not support the weight of the device.

To remove the top cover, do the following:

1. Turn off all attached devices and the server.
2. Disconnect the ac power cord from the electrical outlet.
3. Unlock the latch with screwdriver (Step 1).
4. Push button and lift the latch (step 2).
5. Pull the cover backwards, then lift to remove (Step 3).



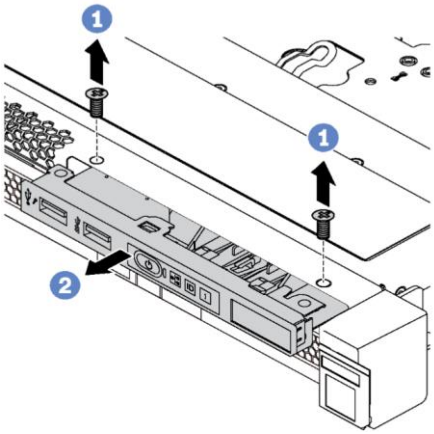
To reinstall, reverse the steps above.

2.2.4 Front I/O module replacement

Do not proceed before reading and understanding the "Safety Precautions" section of this chapter and "Read Me First".

CAUTION:
The power control button on the device and the power switch on the power supply do not turn off the electrical current supplied to the device. The device may have more than one power cord. To remove all electrical current from the device, ensure that all power cords are disconnected from the power source.

To remove the front I/O module, do the following:
1.Turn off all attached devices and the server.
2.Disconnect the ac power cord from the electrical outlet.
3.Remove the top cover. See "2.2.3 Top cover replacement".
4.Disconnect the Front I/O cable from the system board.
5.Remove screws for front I/O module (Step 1).
6.Pull-out the front I/O module (Step 2).



To reinstall, reverse the steps above.

2.2.5 Backplane replacement

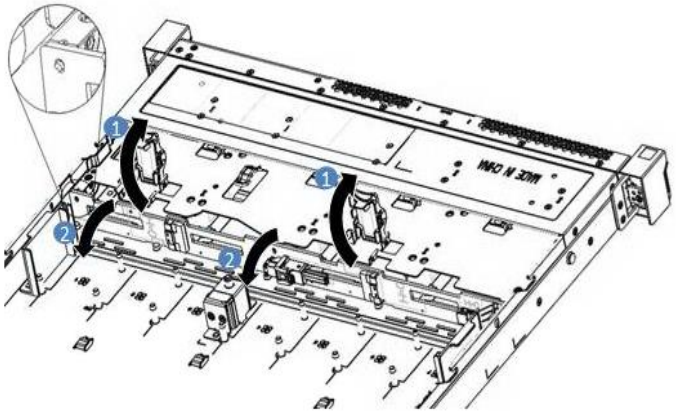
Do not proceed before reading and understanding the "Safety Precautions" section of this chapter and "Read Me First".

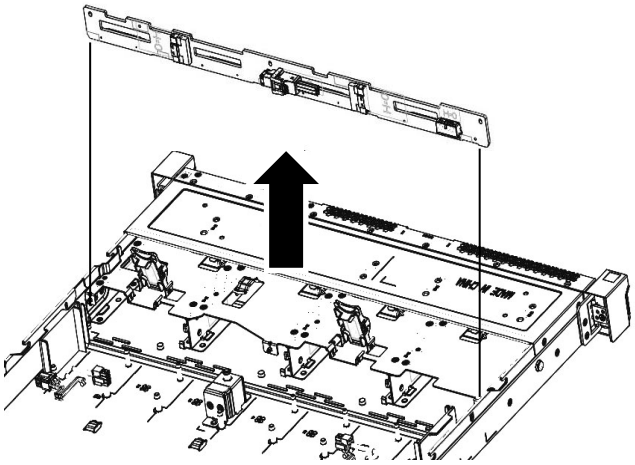
CAUTION:

The power-control button on the device may put the device in standby mode instead of turning off the device. In addition, the device may have multiple connections to DC power. To remove all electrical current from the device, ensure that all connections to DC power are disconnected at the DC power input terminals.

To remove the backplane, do the following:

1. Turn off all attached devices and the server.
2. Disconnect the ac power cord from the electrical outlet.
3. Remove the top cover. See "2.2.3 Top cover replacement".
4. Disconnect the power and SATA/NVMe cables on the back plane.
5. Remove all the front hard drive from the chassis.
6. Open the latch on back plane (Step 1).
7. Grab the back plane and turn it away from the location pin (Step 2).
8. Lift up and remove the backplane.





To reinstall, reverse the steps above.

2.2.6 Air baffle replacement

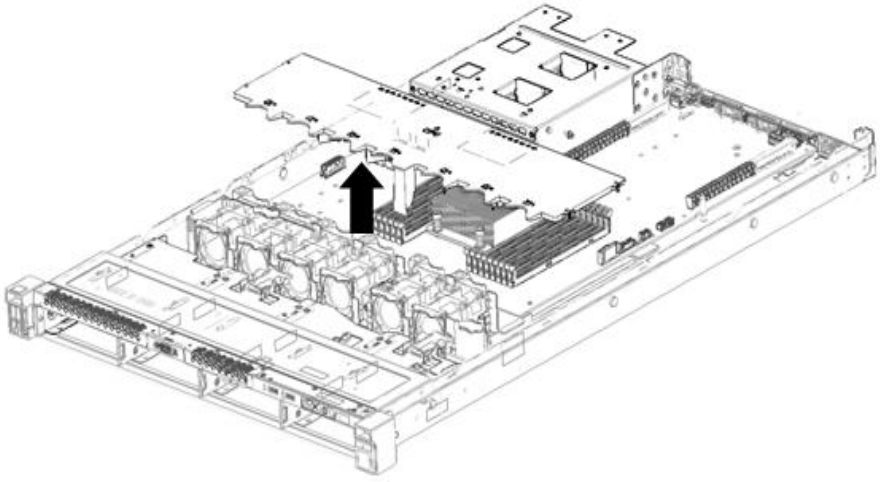
Do not proceed before reading and understanding the "Safety Precautions" section of this chapter and "Read Me First".

CAUTION:

If your server has air ducts or air baffles, do not remove them while the server is running. Operating the server without the air ducts or air baffles might cause the microprocessor(s) to overheat.

To remove the air baffle, do the following:

1.Turn off all attached devices and the server.
2.Disconnect the ac power cord from the electrical outlet.
3.Remove the top cover. See "2.2.3 Top cover replacement".
4.Lift the system air baffle straight up and out of the chassis.



To reinstall, reverse the steps above.

2.2.7 Memory module replacement

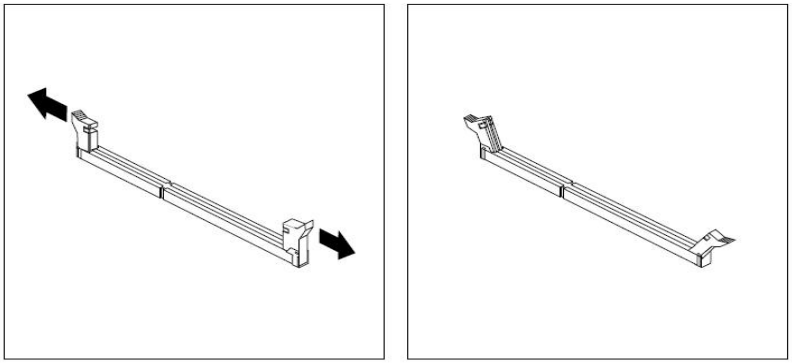
Do not proceed before reading and understanding the "Safety Precautions" section of this chapter and "Read Me First".

CAUTION: The following label indicates a sharp-edge hazard.

To install a memory module, do the following:

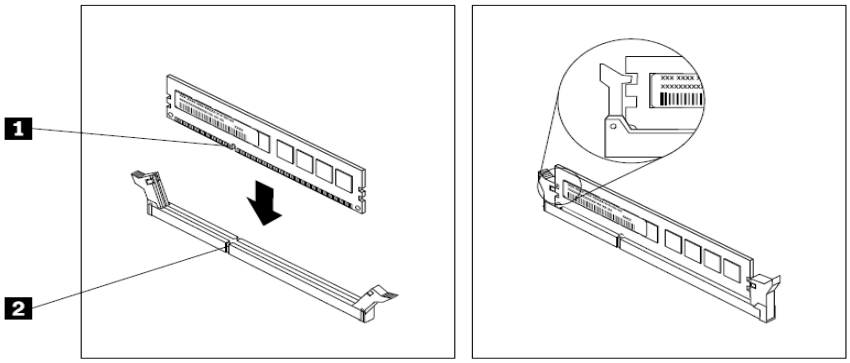
1. Turn off all attached devices and the server.

2. Disconnect the ac power cord from the electrical outlet.
3. Remove the top cover. See "2.2.3 Top cover replacement".
4. Remove the system air baffle. See "2.2.6 Air baffle replacement".
5. Open the retaining clips of the appropriate memory slot.



Open the retaining clips of the memory slot

6. Ensure that notch 1 on the new memory module is aligned with key 2 in the memory slot, then insert the memory module.
7. Press the top of the new memory module straight down until the retaining clips close and the new memory module snaps into position.



Installing a memory module.

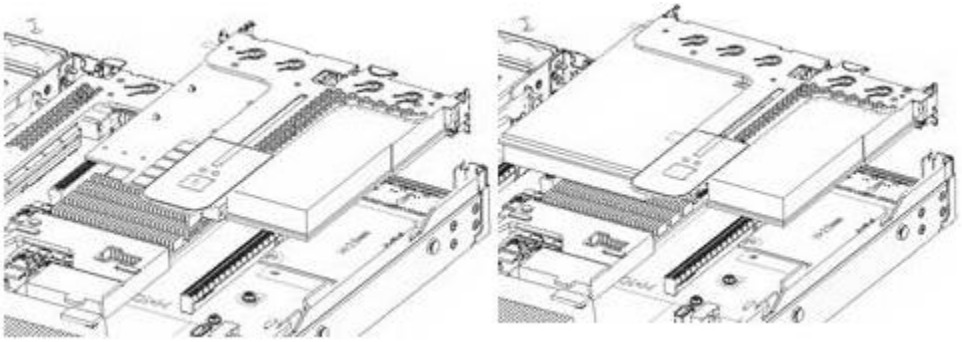
To remove, reverse the steps above.

2.2.8 Riser assembly replacement

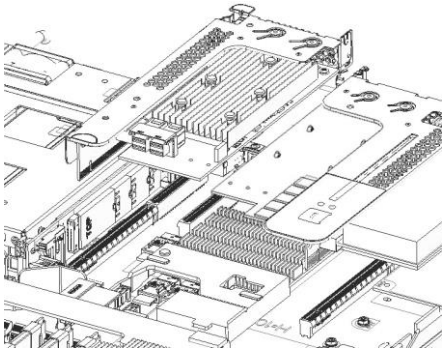
Do not proceed before reading and understanding the "Safety Precautions" section of this chapter and "Read Me First".

To remove the Riser 1, 2, do the following:

1. Turn off all attached devices and the server.
2. Disconnect the ac power cord from the electrical outlet.
3. Remove the top cover. See "2.2.3 Top cover replacement".
4. Disconnect all cables connected to the PCIe cards.
5. Grasp the riser card assembly by its edges (near the blue point on the module) and carefully lift it out of the chassis.



Removing the riser 1 module



Removing the riser 2 module

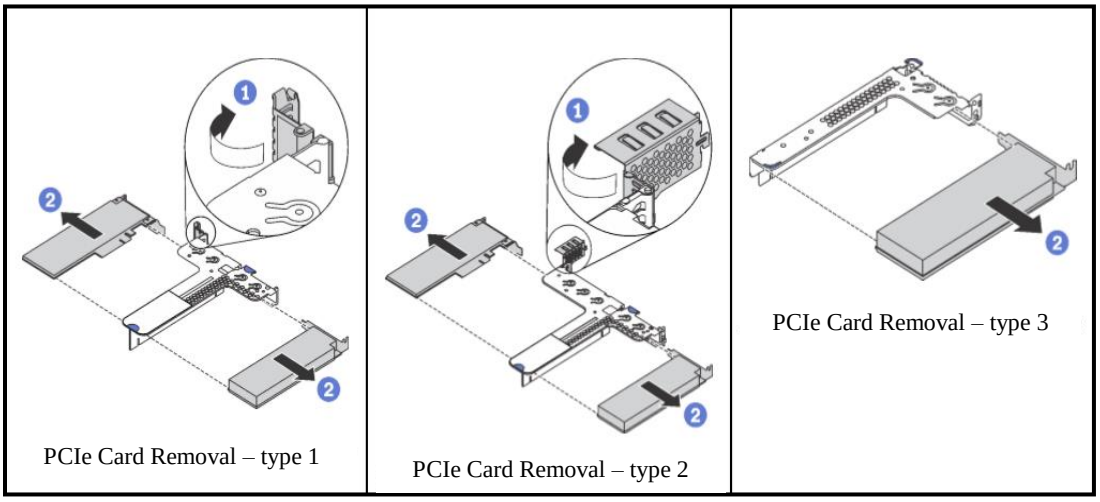
To reinstall, reverse the steps above.

2.2.9 PCIe card and riser card replacement

Do not proceed before reading and understanding the "Safety Precautions" section of this chapter and "Read Me First".

To remove a PCIe card on riser module, do the following:

1. Turn off all attached devices and the server.
2. Disconnect the ac power cord from the electrical outlet.
3. Remove the top cover. See "2.2.3 Top cover replacement".
4. Remove the riser assembly. See "2.2.8 Riser assembly replacement".
5. Rotate the latch (Step 1).
6. Pull the PCIe card outwards carefully to remove it (Step 2).

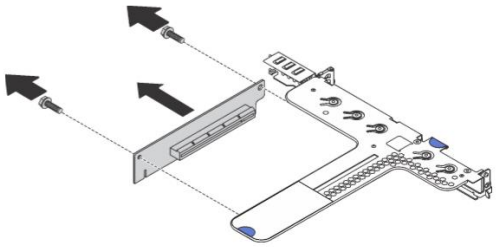


PCIe Card Removal – type 1

PCIe Card Removal – type 2

PCIe Card Removal – type 3

7. Unscrew the screws of riser card and remove the riser card from the PCIe riser cage.



Riser card Removal

To reinstall, reverse the steps above.

Special Note: Refer to the table below for the specifications and the assigned slots for PCIe cards supported by HR330A.

Slot no.	Supported size	Slot specifications
1	Half-height, half-length	×8
2	Half-height, half-length	×16
3	Half-height, half-length	×8

2.2.10 Heat sink replacement

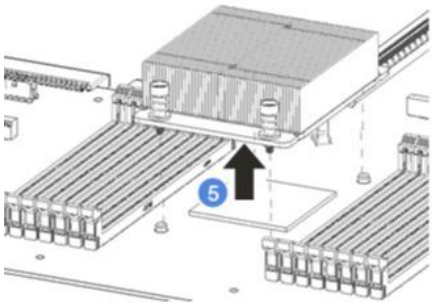
Do not proceed before reading and understanding the "Safety Precautions" section of this chapter and "Read Me First".

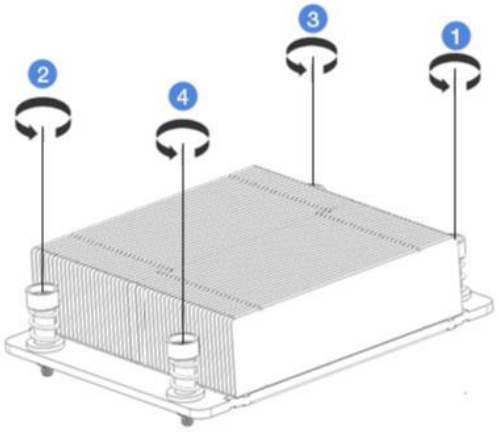
CAUTION:

The heat sink might be very hot. Turn off the server and wait several minutes to let the server cool before removing the server cover.

To remove a heat sink, do the following:

1. Turn off all attached devices and the server.
2. Disconnect the ac power cord from the electrical outlet.
3. Remove the top cover. See "2.2.3 Top cover replacement".
4. Remove the air baffle. See "2.2.6 Air baffle replacement".
5. Unscrew the heat sink with torque screwdriver and follow the sequence 1-2-3-4 in figure.



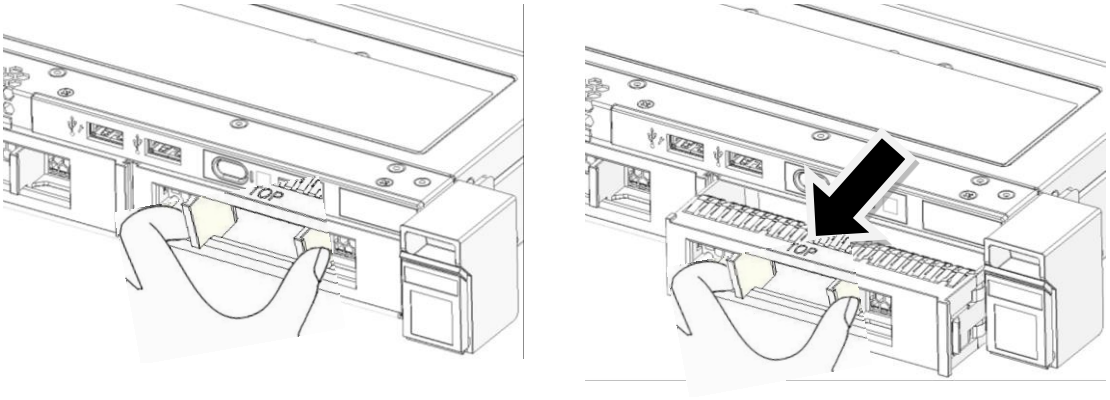


To remove, reverse the steps above.

2.2.11 Hot-swap-drive dummy tray replacement

Do not proceed before reading and understanding the "Safety Precautions" section of this chapter and "Read Me First".

To remove the dummy tray for a 3.5-inch hot-swap drive, do the following:
1.Grab the handle of the dummy tray.
2.Pull the 3.5-inch dummy tray out of the chassis.



Grab the handle of the 3.5-inch dummy tray

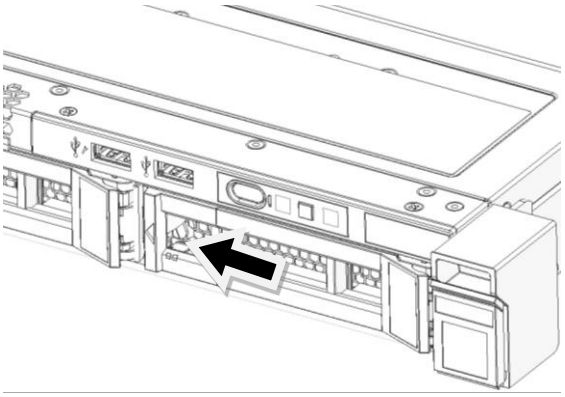
To reinstall, reverse the steps above.

2.2.12 Hot-swap drive replacement

Do not proceed before reading and understanding the "Safety Precautions" section of this chapter and "Read Me First".

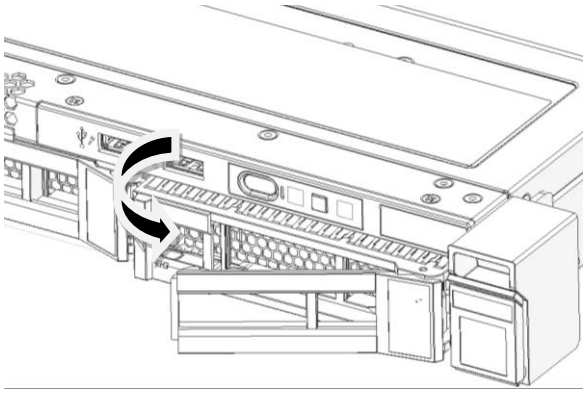
To remove a 3.5-inch hot-swap drive, do the following:

1. Gently push the release latch of the hot-swap drive to open the handle of the drive.



Pushing the release latch of a 3.5-inch hot-swap drive

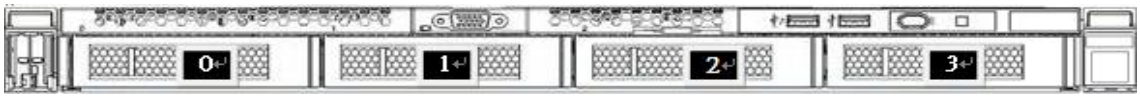
2. Pull the handle to slide the drive out of the chassis.



Removing a 3.5-inch hot-swap drive

To reinstall, reverse the steps above.

Special Note: Install the hot-swap drives into the available bays in the order numbered in the diagrams below. Install dummy trays in all vacant hot-swap drive bays.



Order of installation for 3.5-inch hot-swap drives

2.2.13 Hot-swap power supply replacement

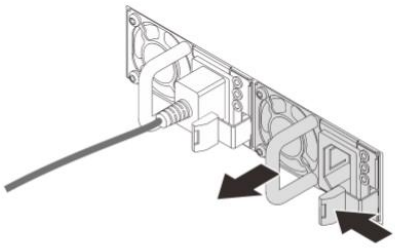
Do not proceed before reading and understanding the "Safety Precautions" section of this chapter and "Read Me First".

CAUTION: Hazardous moving parts. Keep fingers and other body parts away.

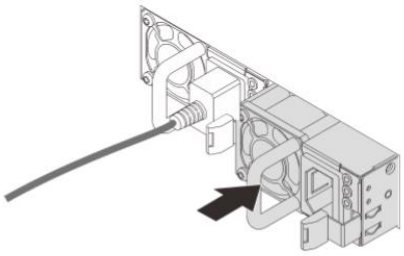
CAUTION: Disconnect the hot-swap fan cables before removing the fan from the device to protect against personal injury.

CAUTION: Never remove the cover on a power supply or any part that has the following label attached.

1.Disconnect the power cord.
2. Push the latch and pull hot-swap power supply out.



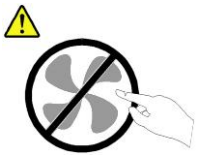
To install, do the following steps:
1. Slide the hot-swap power supply into the chassis until it snaps into position.
2. Connect the power cord.



2.2.14 System fan replacement

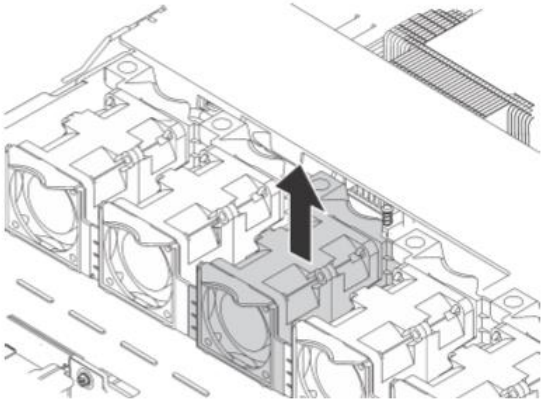
Do not proceed before reading and understanding the "Safety Precautions" section of this chapter and "Read Me First".

Caution: Hazardous moving parts. Keep fingers and other body parts away.



To remove a system fan, do the following:

1. Remove the top cover. See "Top cover replacement".
2. Lift the system fan module out of the server.

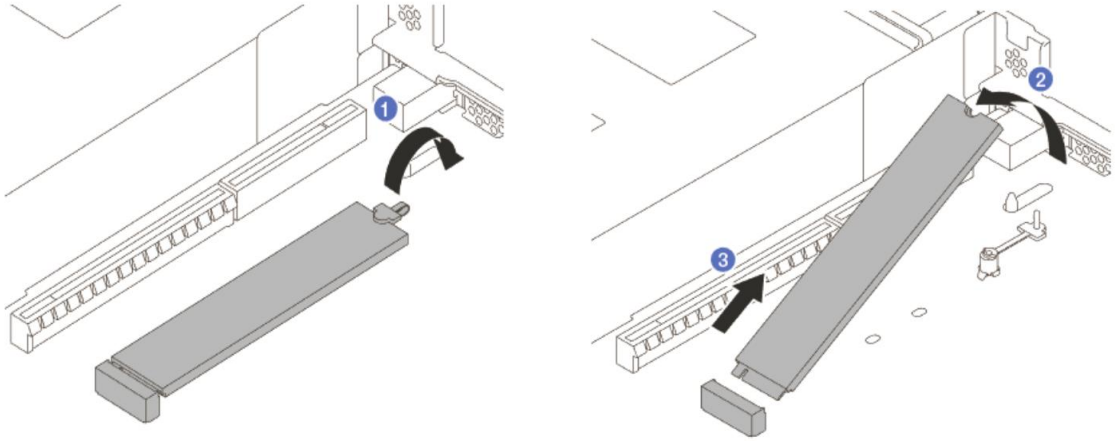


To reinstall, reverse the steps above.

2.2.15 M.2 drive replacement

Do not proceed before reading and understanding the "Safety Precautions" section of this chapter and "Read Me First".

1. Turn off all attached devices and the server
2. Disconnect the ac power cord from the electrical outlet
3. Remove the top cover. See "2.2.3 Top cover replacement".
4. Remove the riser assembly. See "2.2.8 Riser assembly replacement".
5. Remove the air baffle. See "2.2.6 Air baffle replacement".
6. Open the M.2 holder to release the M.2 drive.
7. Pull the M.2 drive up to an angle of approximately 30 degrees.
8. Remove the M.2 drive from the connector.



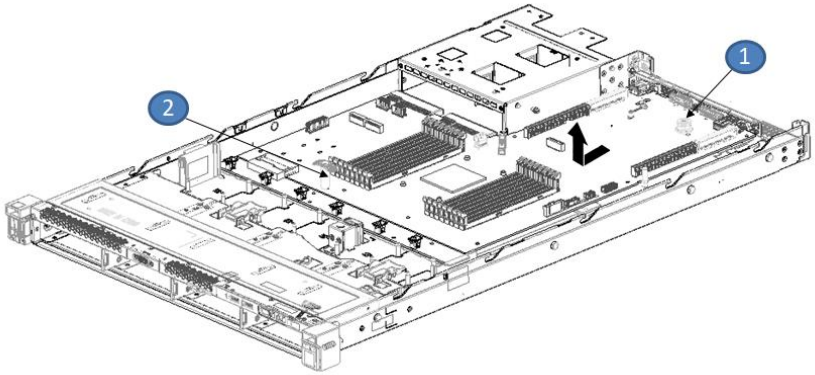
To reinstall, reverse the steps above.

2.2.16 System board replacement

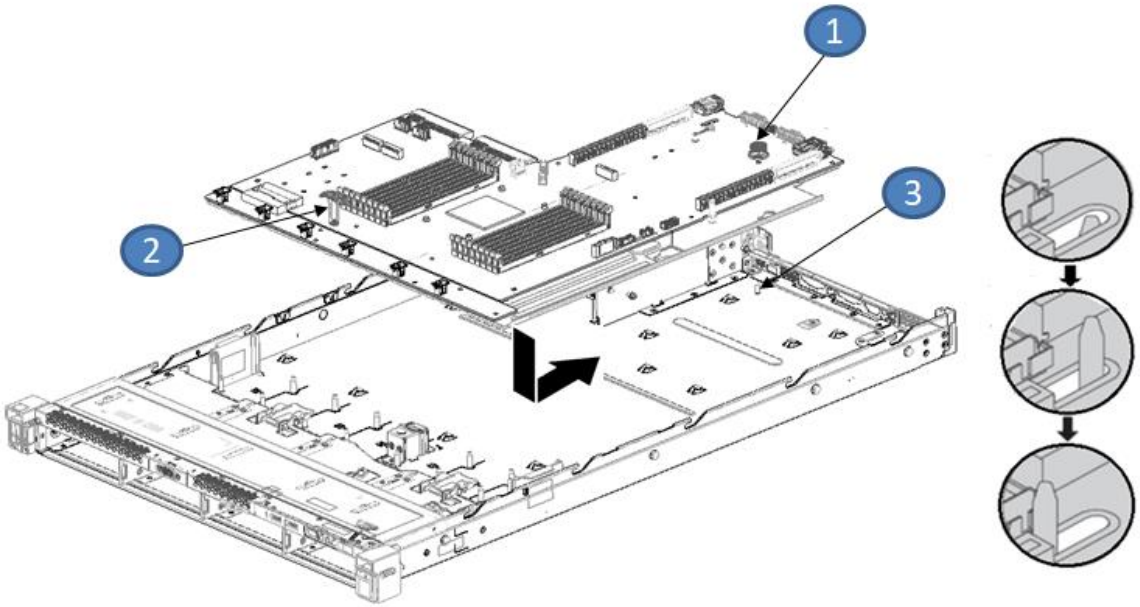
Do not proceed before reading and understanding the "Safety Precautions" section of this chapter and "Read Me First".

1. Turn off all attached devices and the server.

2. Disconnect the ac power cord from the electrical outlet.
3. Remove the hot-swap power supply. See “2.2.13 Hot-swap power supply replacement".
4. Remove the top cover. See "2.2.3 Top cover replacement".
5. Remove the riser assembly. See "2.2.8 Riser assembly replacement".
6. Remove the air baffle. See "2.2.6 Air baffle replacement".
7. Remove the system fan module. See “2.2.14 System fan replacement".
8. Grab the plunger & handle (position 1, 2).
9. Slide to front side and lift up the system board.



To install
1. Handle the system board by grabbing the plunger & handle (position 1, 2).
2. Align to location pin (Position 3) on chassis and put down the system board.
3. Slide to back side.



Chapter 3. BIOS Setup

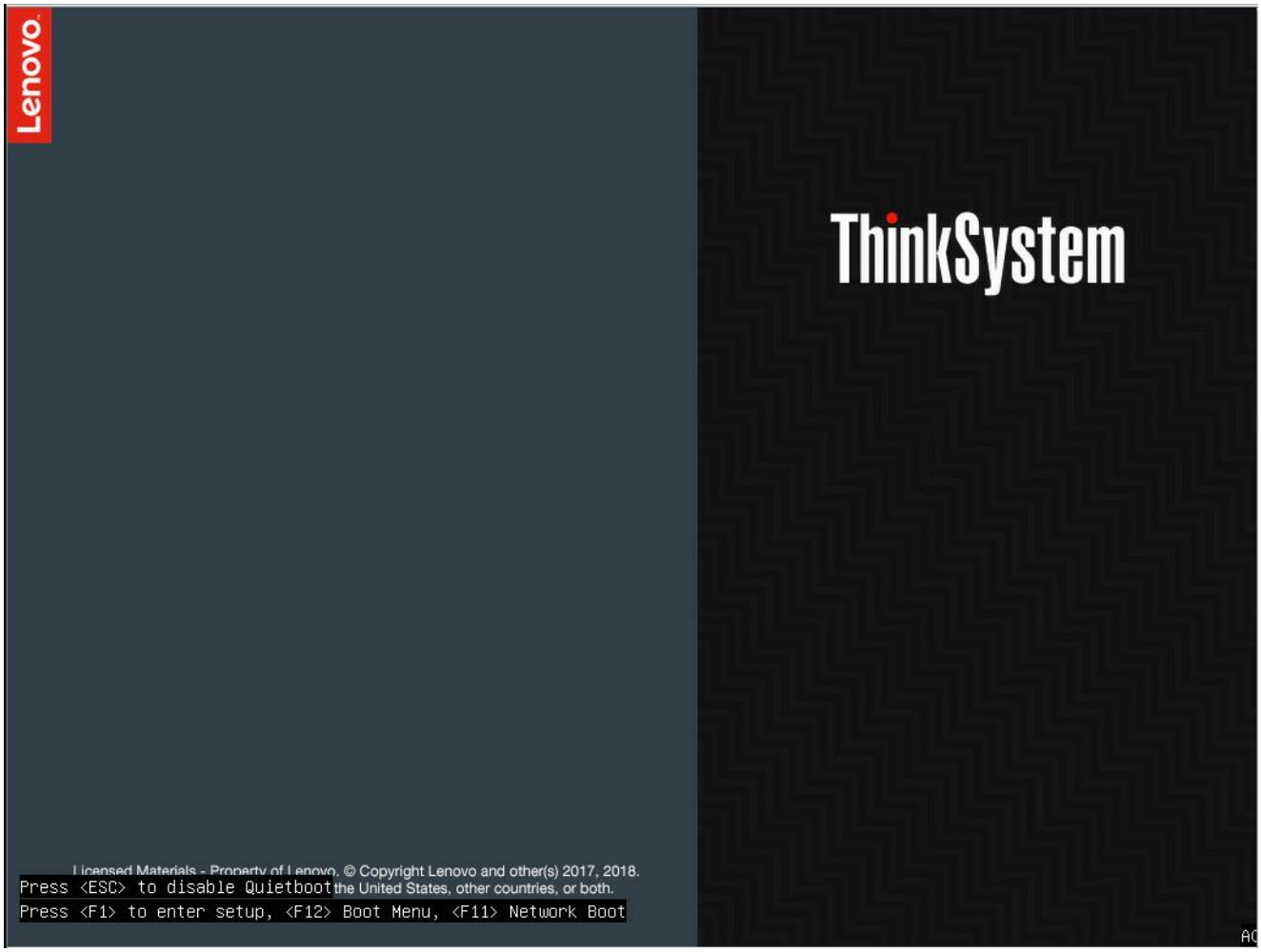
3.1 Introduction

This chapter describes the functions and features provided by eMAG™ UEFI for the HR330A.

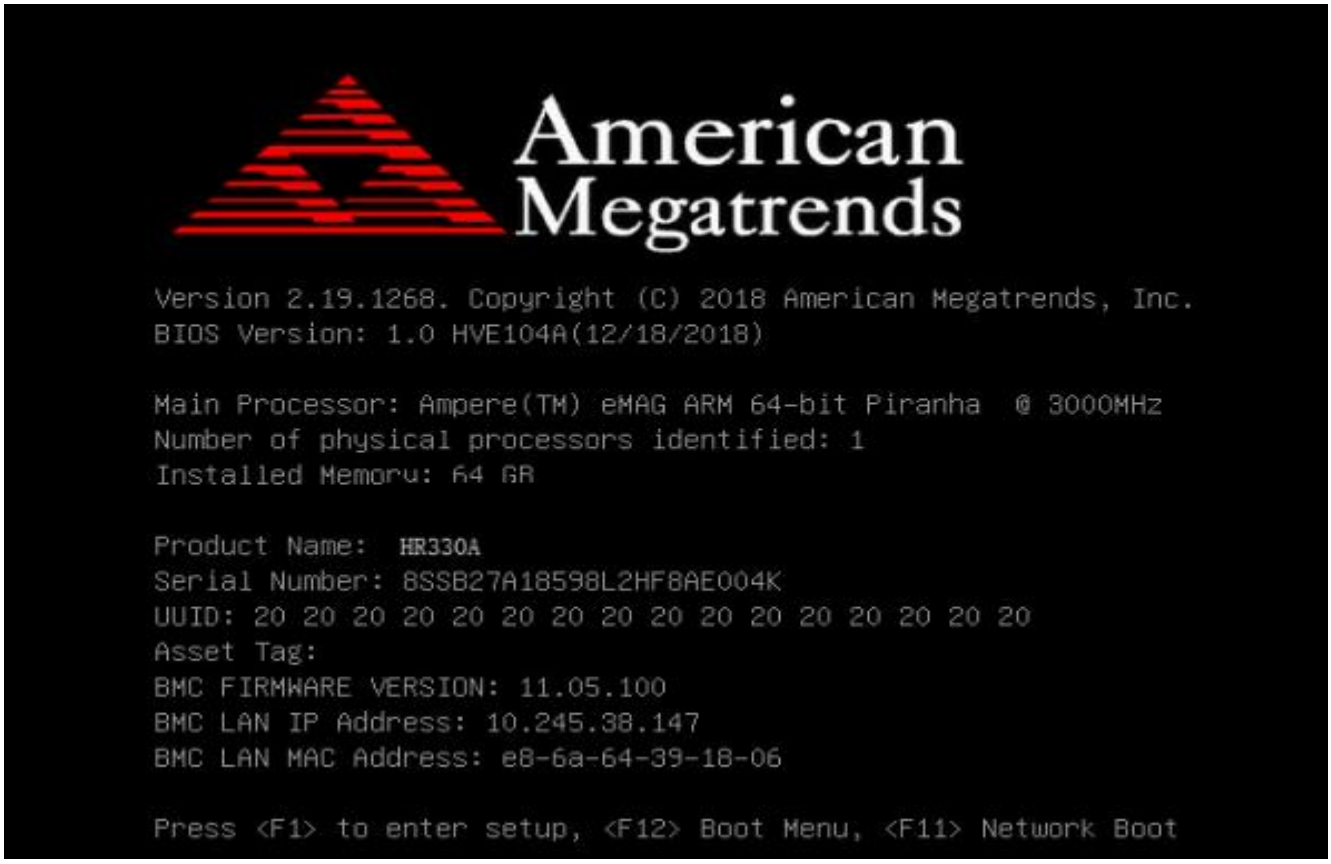
3.2 POST Screen

The POST screen is the first page displayed when the system starts up.
There are two kinds of POST screens:

- Normal POST screen: the screen which contains the logo and copyright messages.



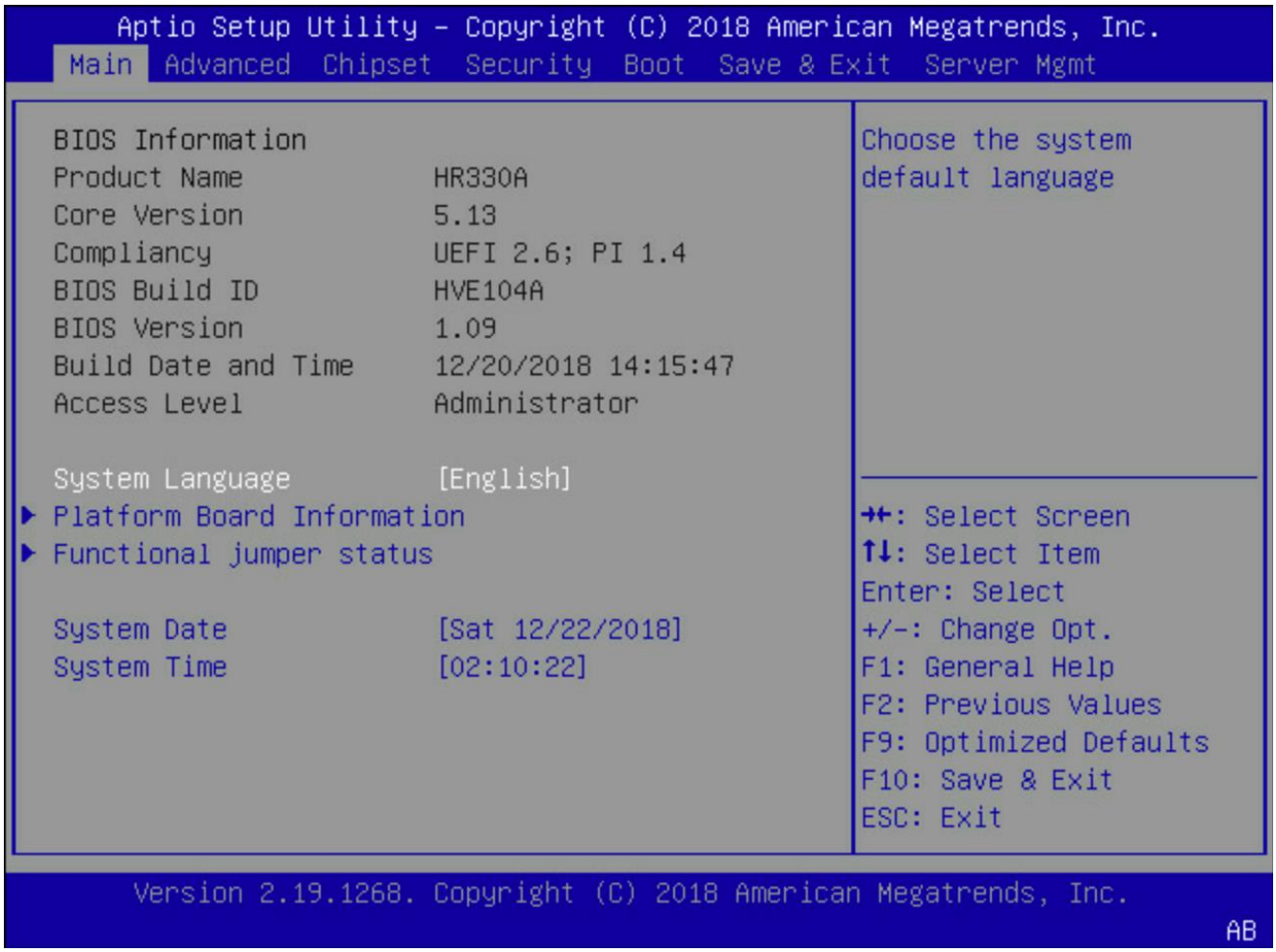
- Quiet POST screen: the screen which contains only the Lenovo logo. By default, quiet POST screen is enabled. Users can switch to normal POST screen by pressing ESC.



Below information should be shown in POST screen:

- BIOS and firmware version
- BMC version, product name, serial number, asset tag, and UUID (if "BMC Support" option is enabled.)
- BMC IP and MAC address (if "BMC Support" option is enabled.)
- Memory information
- CPU, HDD, and NVMe information

3.3 Main



3.3.1 BIOS Information

Below BIOS Information is shown in the Main setup screen:
1. Product Name
2. Core Version
3. Compliancy
4. BIOS Build ID
5. BIOS Version
6. Build Date and Time
7. Access Level

3.3.2 System Language

Allows user to change the language displayed. Currently, only English is supported.

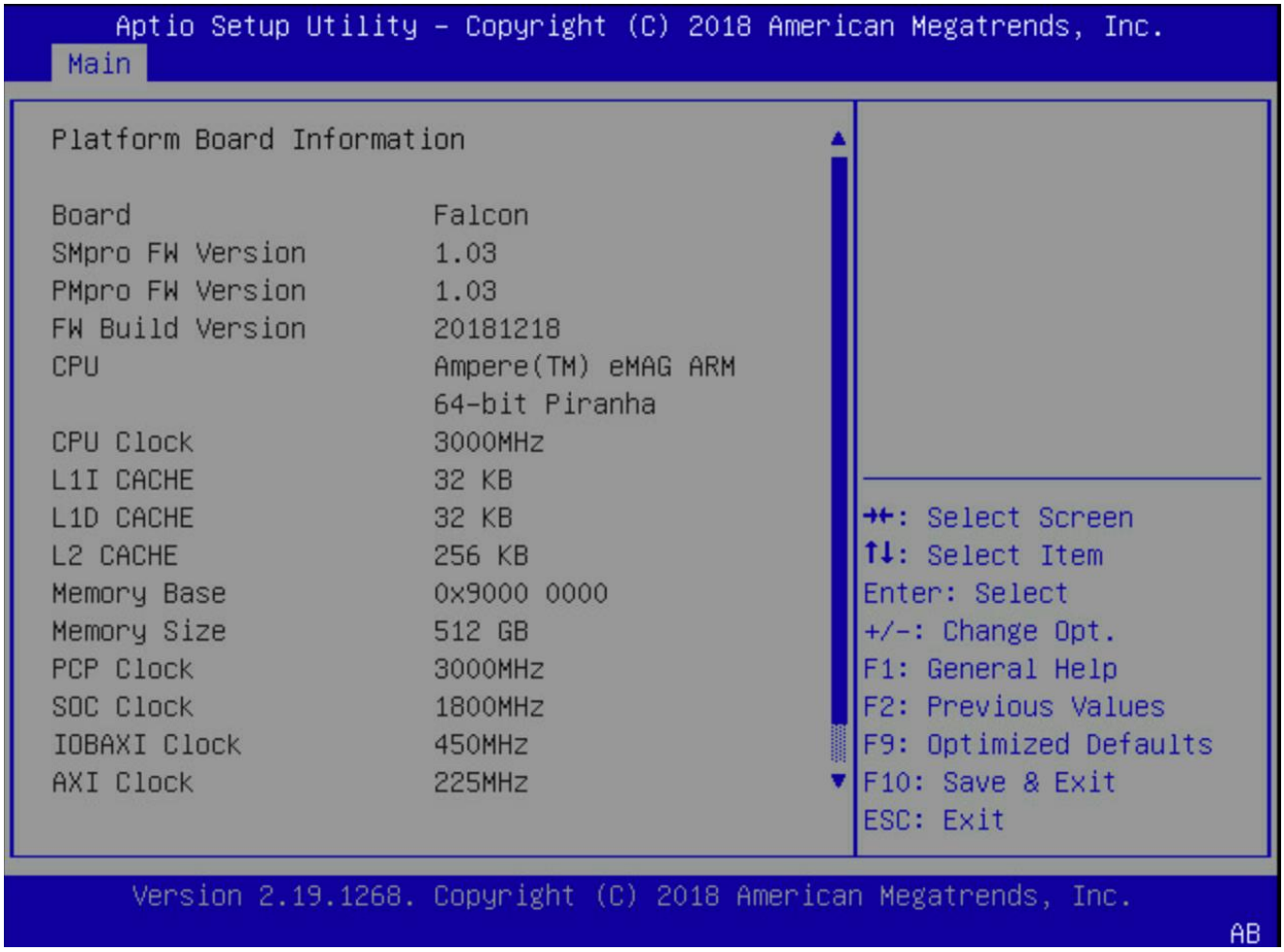
3.3.3 System Date/Time

Use this option to change the system time and date:
1. Highlight System Time or System Date using the arrow keys.
2. Enter new values using the keyboard.

3. Press the arrow keys to move between fields.
4. The date must be entered in Date MM/DD/YYYY format.
5. The Time is entered in HH:MM:SS format.

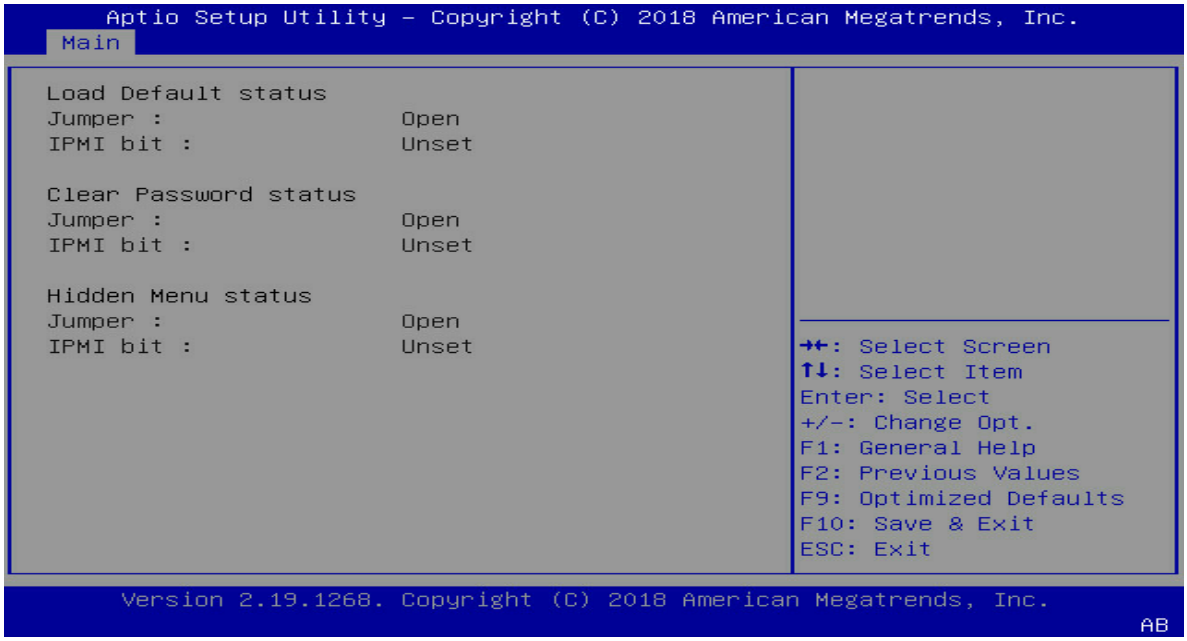
3.3.4 Platform Board Information

Display general information about the board, including board name, SCP firmware version, clock, and so on.



3.3.5 Functional Jumper Status

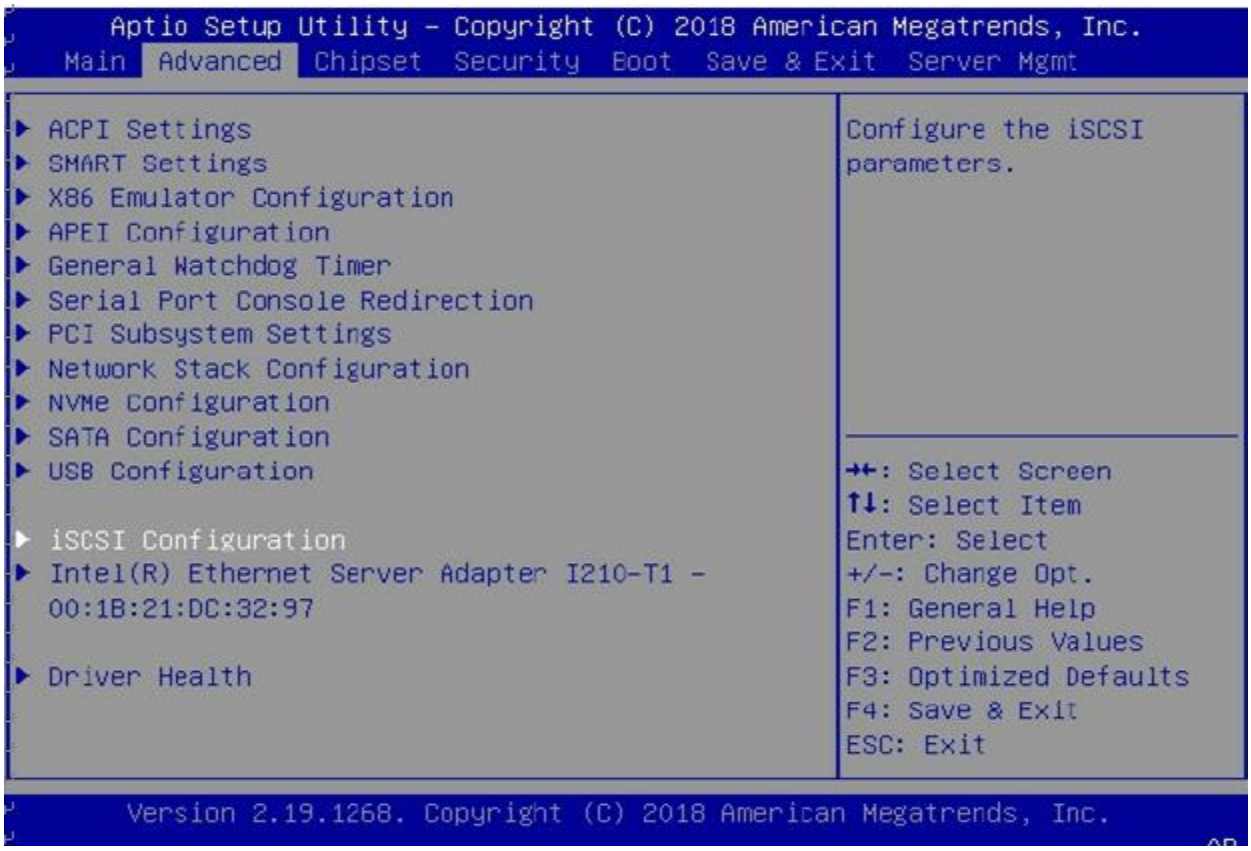
This screen shows status of the functional jumpers and the corresponding IPMI commands.



- Jumper: ‘Open’ if the jumper is not set. Otherwise ‘Close’.
- IPMI bit: ‘Unset’ if users have not executed the IPMI command to set the corresponding function. Otherwise, ‘Set’.

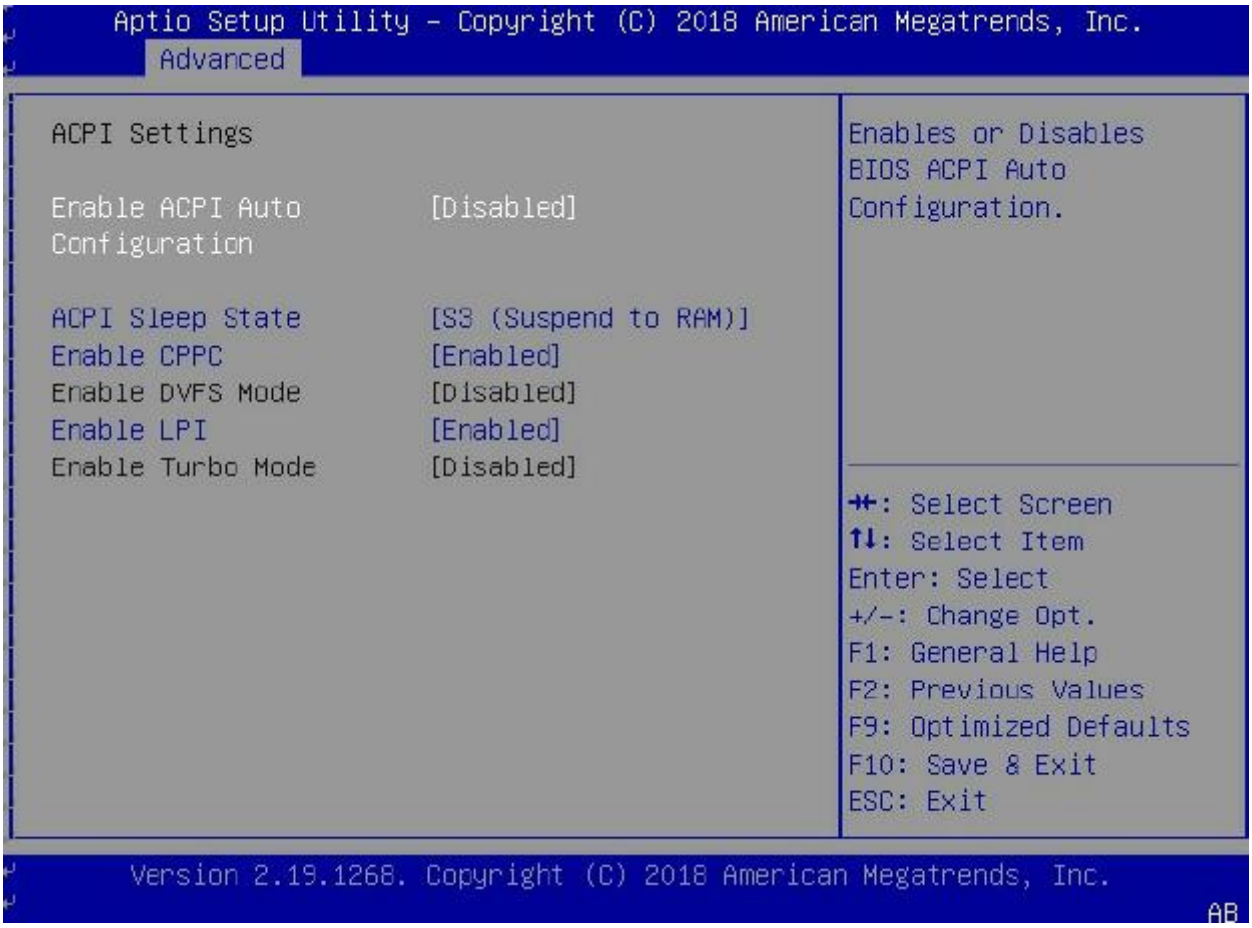
3.4 Advanced

Use the arrow keys to select Advanced on top of the screen. The Advanced Configuration screen looks like below.



If the system is unstable after changing any settings in advanced configuration, revert to the default settings in the “Save & Exit” screen. Use the arrow keys to select each screen and press Enter to access the submenu items.

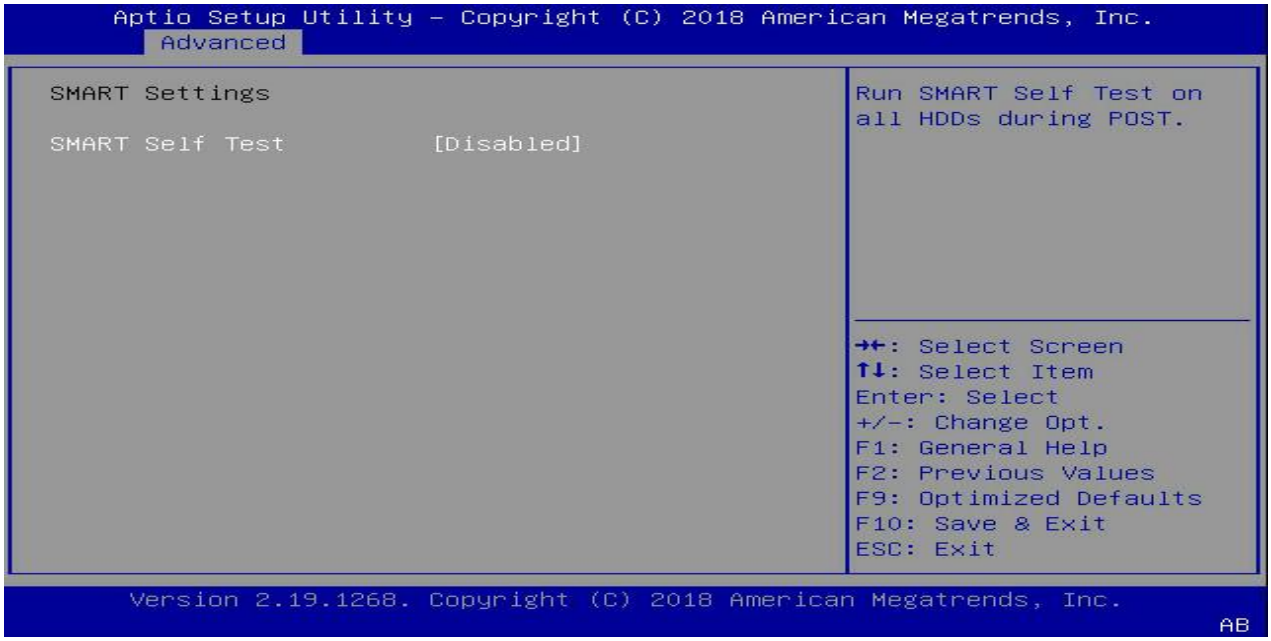
3.4.1 ACPI Settings



ACPI Settings	**Description**
Enable ACPI Auto Configuration	Select Enabled to let the BIOS select the best ACPI options for the system. Select **Disabled** to manual change ACPI following settings.
ACPI Sleep State	Supports only Sleep State S3. The options are **S3** and Disabled.
Enable CPPC	Allow Firmware to communicate with OS using CPPC (Collaborative Processor Performance Control). The options are **Enabled** and Disabled.
Enable DVFS	Enable DVFS (Dynamic Voltage and Frequency Scaling) mode. This mode can be changed only when CPPC enabled and the chip supports it. The options are Enabled and **Disabled**.
Enable LPI	Allow the system to go to LPI (Lower Power Idle) mode. The options are **Enabled** and Disabled.

Enable Turbo mode	Allow the system to go to Turbo mode in which the system may run at highest speed 3.3 GHz. This mode can be changed only when the Chip supports it. If the Chip does not support Turbo mode, this configuration will be hidden. The options are **Enabled** and Disabled.

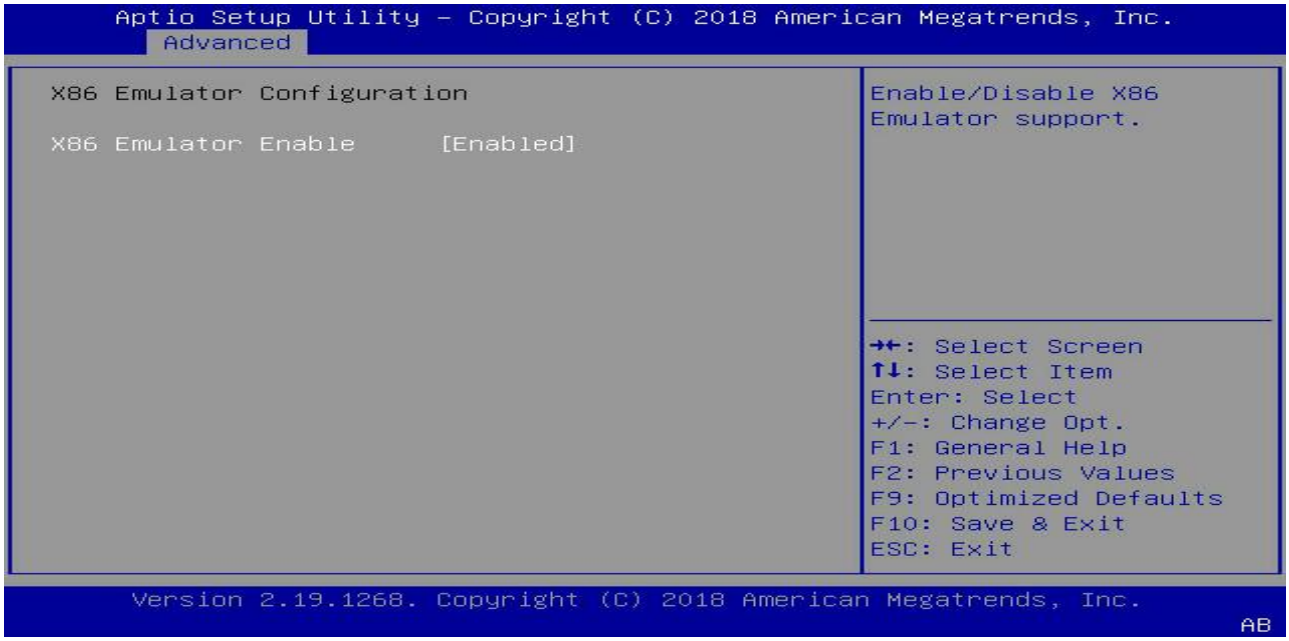
3.4.2 SMART Settings



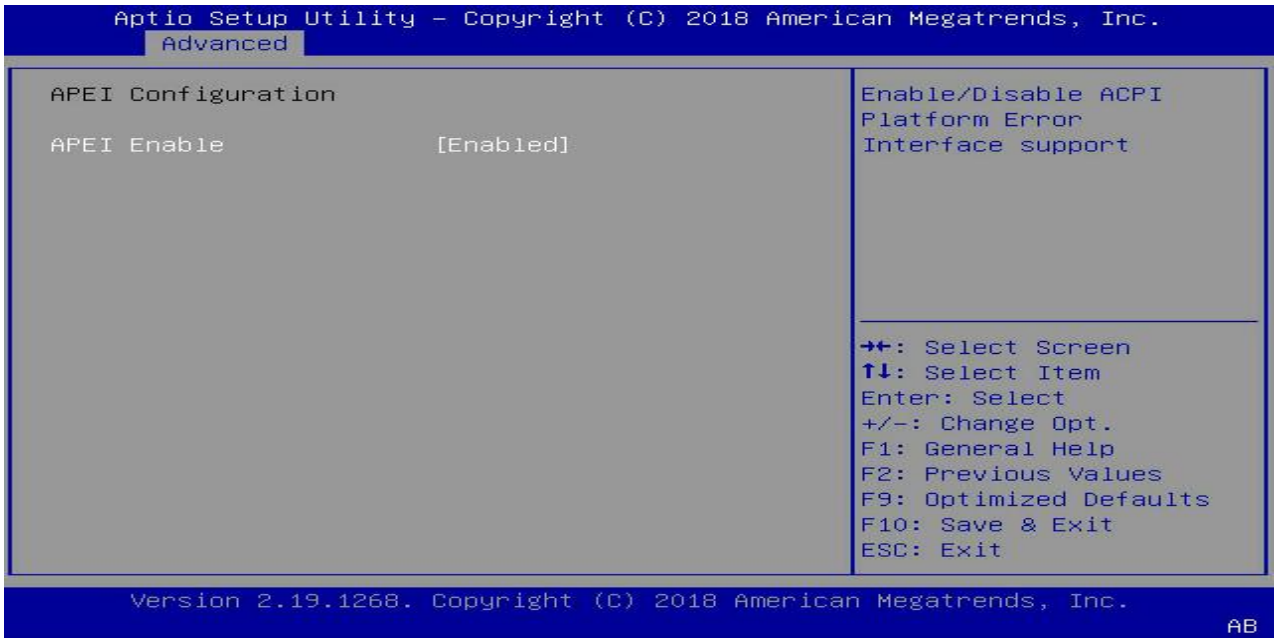
SMART Self-Test: Allow users to enable/disable running SMART self-test on all HDDs during POST. The options are Enabled and **Disabled**.

3.4.3 X86 Emulator Configuration

This screen allows users to enable X86 Emulator support. The options are **Enabled** and Disabled.

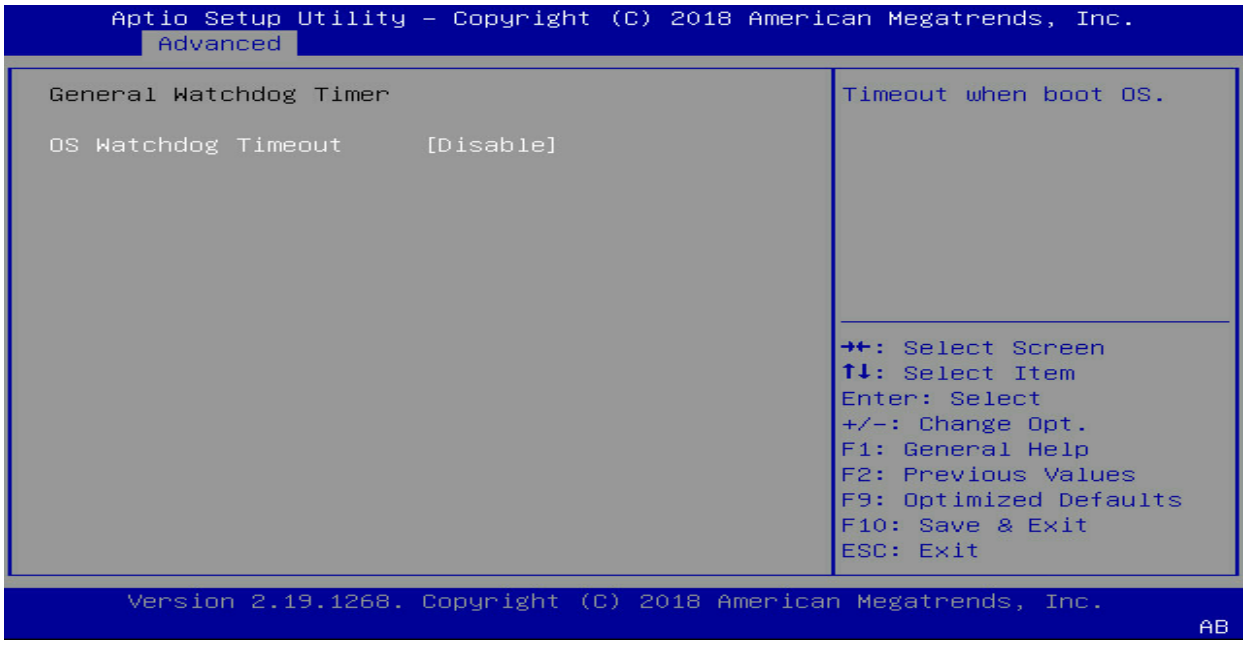


3.4.4 APEI Configuration



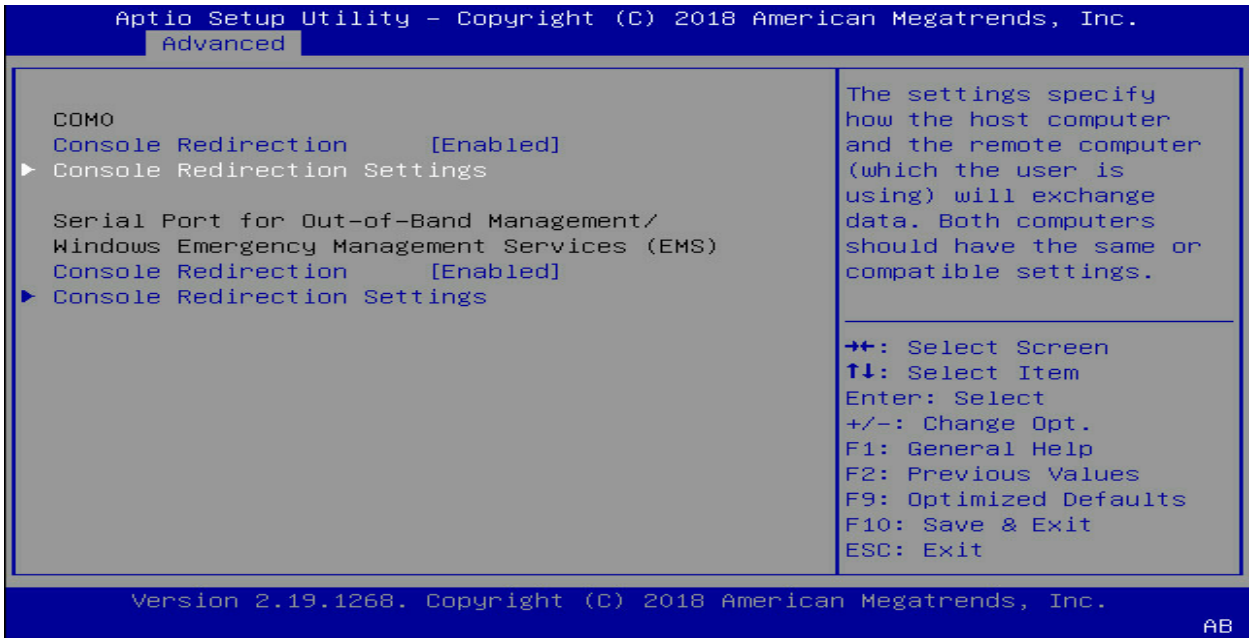
APEI Enable: Allow the system to support APEI (ACPI Platform Error Interface). Enable this feature to make the system report any HW errors to OS. The options are **Enabled** and Disabled.

3.4.5 General Watchdog Timer



OS Watchdog Timeout: This feature allows the system reboot when OS fail to boot. Use this feature if your OS fully support ARM general Watchdog Timer. Select Disabled if not sure. The options are Enabled and **Disabled**.

3.4.6 Serial Port Console Redirection

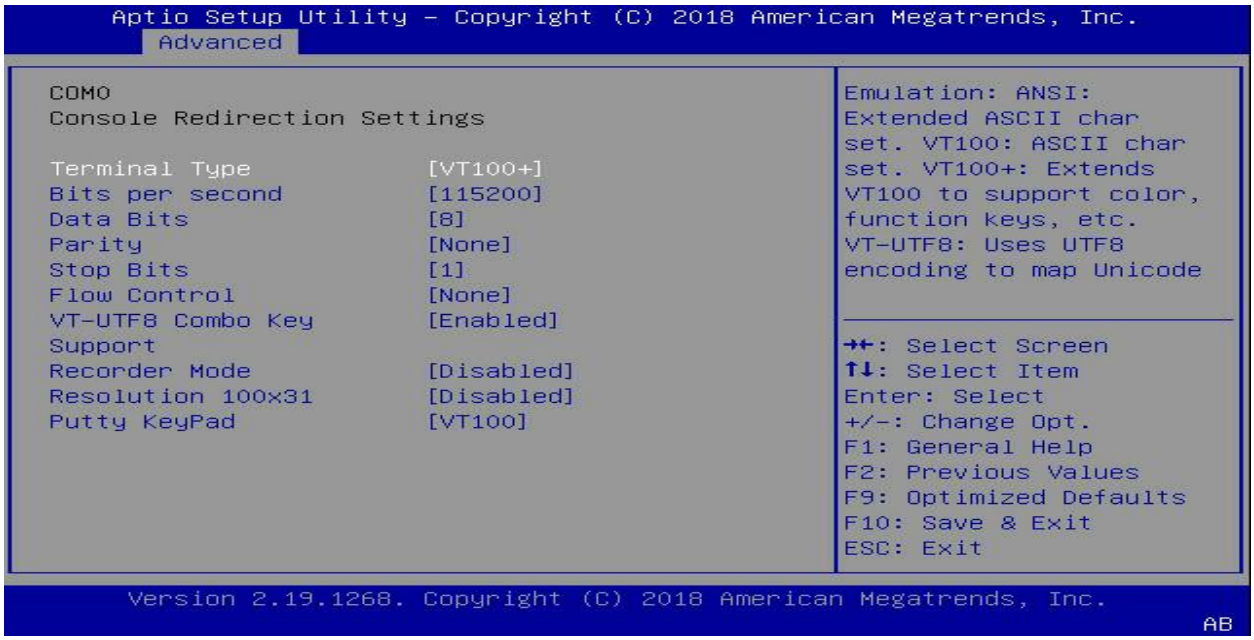


This setup screen allows users to configure serial ports for COM0 and Out-of-Band Management port. More detailed information is in below sections.

3.4.6.1 COM0

Console Redirection: Select Enabled to enable console redirection support for a serial port specified by the user. The options are Enabled and Disabled.

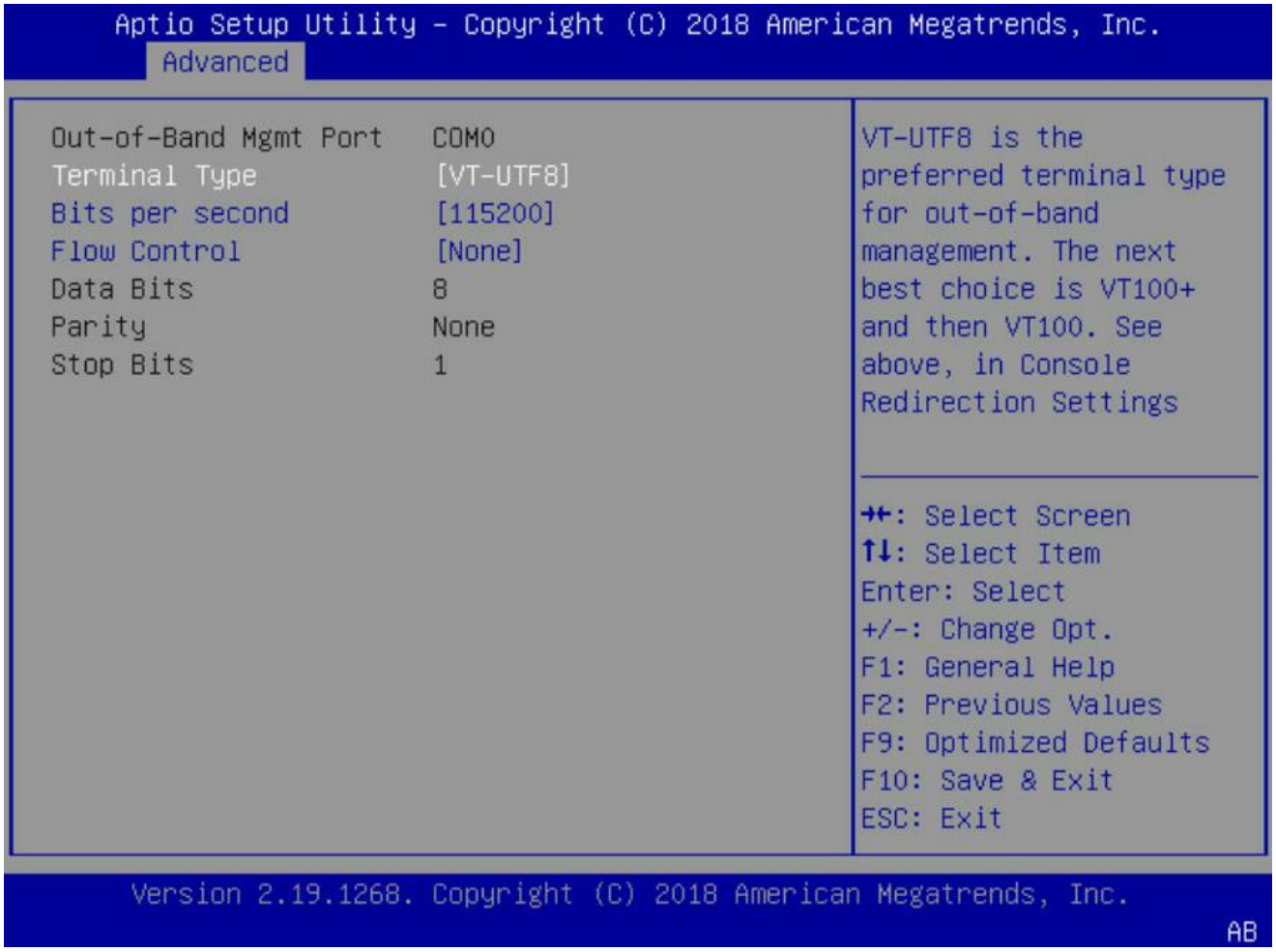
If the item above set to Enabled, the following items will become available for user's configuration:



Console ReDirection Settings	Description
Terminal Type	This feature allows the user to select the target terminal emulation type for Console Redirection: - Select VT100 to use the ASCII Character set. - Select VT100+ to add color and function key support. - Select ANSI to use the Extended ASCII Character Set. - Select VT-UTF8 to use UTF8 encoding to map Unicode characters into one or more bytes. The options are VT100, VT100+, VT-UTF8, and ANSI.
Bits per second	Use this option to set the transmission speed for a serial port used in Console Redirection. Make sure that the same speed is used in the host computer and the client computer. A lower transmission speed may be required for long and busy lines. The options are 9600, 19200, 38400, 57600 and 115200 (bits per second).
Date Bits	Use this feature to set the data transmission size for Console Redirection. The options are 7 and 8.
Parity	A parity bit can be sent along with regular data bits to detect data transmission errors. - Select Even if the parity Bit is set to 0, and the numBer of 1's in data Bits is even. - Select Odd if the parity Bit is set to 0, and the numBer of 1's in data Bits is odd. - Select None if you do not want to send a parity Bit with your data Bits in transmission. - Select Mark to add a mark as a parity Bit to be sent along with the data Bits.

	- Select Space to add a Space as a parity Bit to Be sent with your data Bits. The options are None, Even, Odd, Mark, and Space.
Stop Bits	A stop bit indicates the end of a serial data packet. Select 1 Stop Bit for standard serial data communication. Select 2 Stop Bits if slower devices are used. The options are **1** and 2.
Flow Control	Use this feature to set the flow control for Console Redirection to prevent data loss caused by buffer overflow. Send a "Stop" signal to stop sending data when the receiving buffer is full. Send a "Start" signal to start sending data when the receiving buffer is empty. The options are None and Hardware RTS/CTS.
VT-UTF8 Combo Key	Select Enabled to enable VT-UTF8 Combination Key support for ANSI/VT100 terminals. The options are Disabled and Enabled.
Recorder Mode	Select Enabled to capture the data displayed on a terminal and send it as text messages to a remote server. The options are Disabled and Enabled.
Resolution 100x31	Enable or disables extended terminal resolution. The options are Disabled and Enabled.
Putty KeyPad	This feature selects the settings for Function Keys and KeyPad used for Putty, which is a terminal emulator designed for the Windows OS. The options are VT100, LINUX, XTERMR6, SC0, ESCN, and VT400.

3.4.6.2 Serial Port for Out-of-Band Management/Windows Emergency Management Services (EMS)



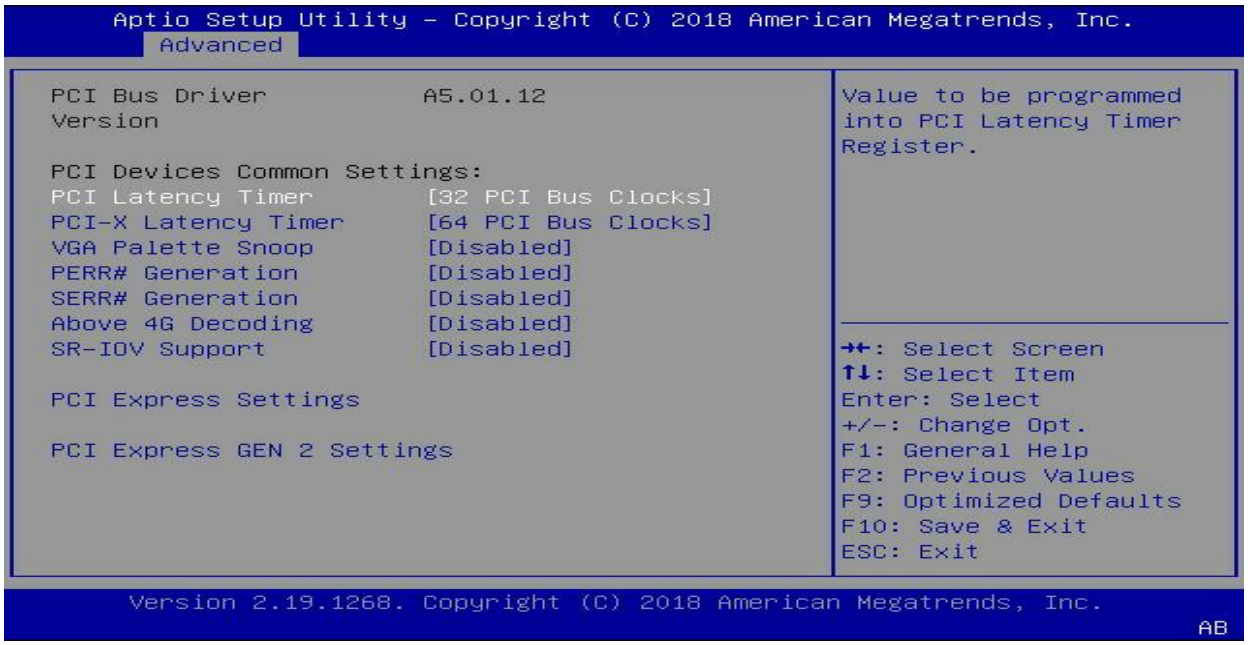
Console Redirection: Select Enabled to enable SOL console redirection support for a serial port specified by the user. The options are **Enabled** and Disabled.

If the item above set to Enabled, the following items will become available for user's configuration:

Console Redirection Settings	Description
Terminal Type	This feature allows the user to select the target terminal emulation type for Console Redirection. Select VT100 to use the ASCII Character set. Select VT100+ to add color and function key support. Select ANSI to use the Extended ASCII Character Set. Select VT-UTF8 to use UTF8 encoding to map Unicode characters into one or more bytes.The options are VT100, VT100+, **VT-UTF8**, and ANSI.
Bits per second	Use this feature to set the transmission speed for a serial port used in Console Redirection. Make sure that the same speed is used in the host computer and the client computer. A lower transmission speed may be required for long and busy lines. The options are 9600, 19200,38400, 57600, and 115200 (bits per second).
Flow Control	Use this feature to set the flow control for Console Redirection to prevent data loss caused by buffer overflow. Send a "Stop" signal to stop sending data when the receiving buffer is full. Send a "Start" signal to start sending data when the receiving buffer is empty.The options are **None**, Hardware RTS/CTS, and Software Xon/Xoff.
Data Bits	8
Parity	None
Stop Bits	1

3.4.7 PCI Subsystem Settings

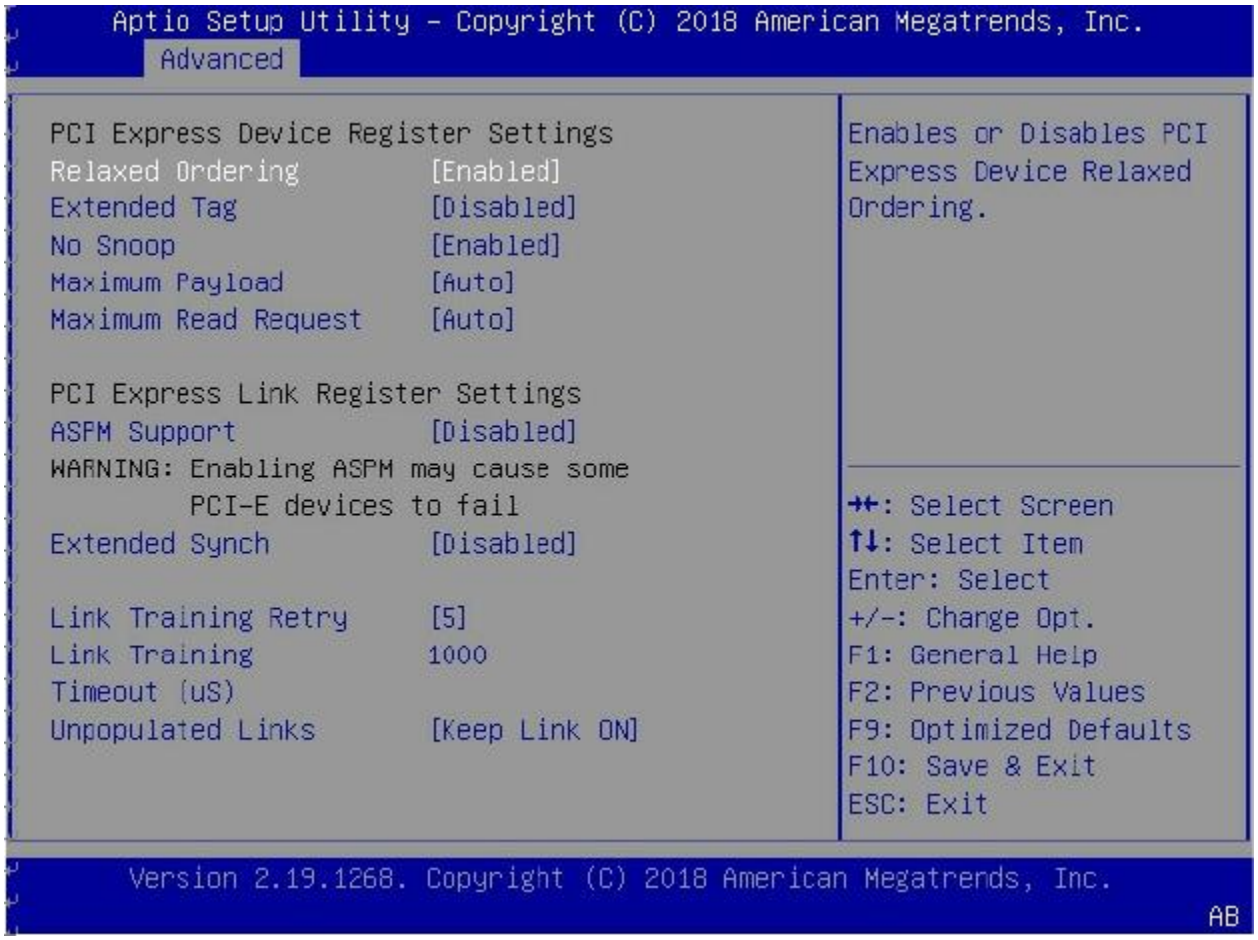
This menu provides standard PCIe configuration settings and information.



Below table explains about PCIE Device Common setting, applied for all devices:

PCIE Device Common Settings	Description
Above 4G DecoDing	This setting **Enables** or Disables 64-bit capable devices ability to be decoded in above 4G address space.
SR-IOV Support	If the system has SR-IOV capable PCI-E devices, the setting will Enable or **Disable** the Single Root IO Virtualization Support for the system.
PCI Latency Timer	Value to be programmed into PCI Latency Timer Register
PCI-X Latency Timer	Value to be programmed into PCI Latency Timer Register
VGA Palette Snoop	Enables or **Disables** VGA Palette Registers Snooping
PERR# Generation	Enables or **Disables** PCI Device to Generate PERR#
SERR# Generation	Enables or **Disables** PCI Device to Generate SERR#
PERR# Generation	Enables or **Disables** PCI Device to Generate PERR#
SERR# Generation	Enables or **Disables** PCI Device to Generate SERR#

3.4.7.1 PCI Express Settings

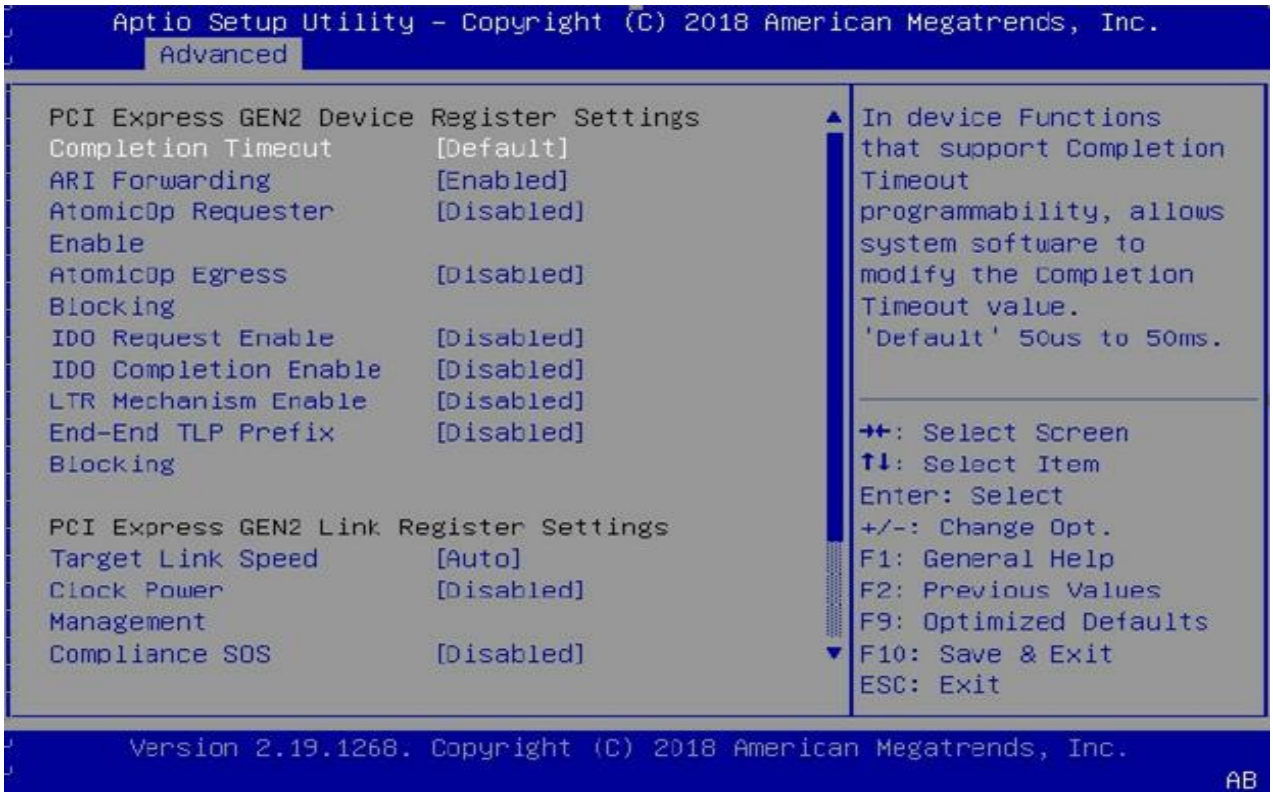


PCI Express Link Register Settings	
ASPM Support	Set the ASPM Level: - Force L0s - Force all links to L0s State - AUTO - BIOS auto configure - **DISABLE** - DisaBles ASPM
Extended Synch	If Enabled, allows generation of Extended Synchronization patterns.
Link Training Retry	Defines number of Retry Attempts software will take to retrain the link if previous training attempt was unsuccessful.
Link Training Timeout	Defines number of Microseconds software will wait before polling 'Link Training' bit in Link Status register. Value ranges from 10 to 10000 uS.
Unpopulated Links	In order to save power, software will disable unpopulated PCI Express links, if this option set to Disable. The options are **Keep Link ON** and Disalbel Link.

Setting	Description
PCI Express Device Register Settings	
Relaxed Ordering	**Enables** or Disables PCI Express Device Relaxed Ordering
Extended Tag	If **Enabled**, allows Device to use 8-bit Tag field as a requester
No Snoop	**Enables** or Disables PCI Express Device No Snoop option
Maximum Payload	Set Maximum Payload of PCI Express Device or allow System BIOS to select the value. The available options are **Auto**, 128 Bytes, 256 Bytes, 512Bytes, 1024 Bytes, 2048 Bytes, and 4096 Bytes.
Maximum Read Request	Set Maximum Read Request Size of PCI Express Device or allow System BIOS to select the value. The available options are **Auto**, 128 Bytes, 256 Bytes, 512 Bytes, 1024 Bytes, 2048 Bytes, and 4096 Bytes.
PCI Express Link Register Settings	
ASPM Support	Set the ASPM Level: - Force L0s - Force all links to L0s State - AUTO - BIOS auto configure - **DISABLE** - Disables ASPM
Extended Synch Link Training Retry	If Enabled, allows generation of Extended Synchronization patterns.
Link Training Retry	Defines number of Retry Attempts software will take to retrain the link if previous training attempt was unsuccessful.
Link Training Timeout	Defines number of Microseconds software will wait before polling 'Link Training' bit in Link Status register. Value range from 10 to 10000 uS.
Unpopulated Links	In order to save power, software will disable unpopulated PCI Express links, if this option set to **Disable**.

WARNING: Enabling ASPM might cause some PCI-E devices to fail!

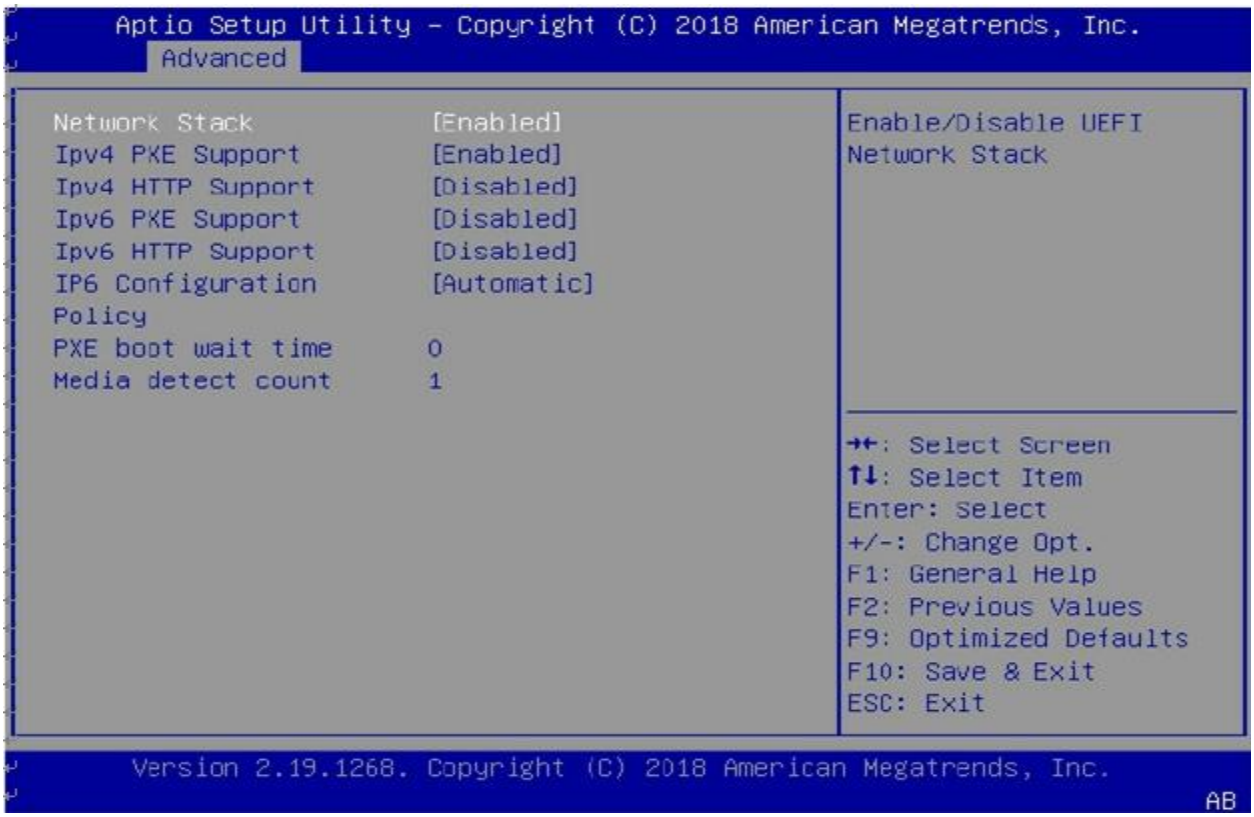
3.4.7.2. PCI Express GEN 2 Settings



Setting	Description
PCI Express GEN2 Device Register Settings	
Completion Timeout	In device Functions that support Completion Timeout programmability, allows system software to modify the Completion Timeout value. 'Default' 50us to. 50ms. If 'Shorter' is selected, software will use shorter timeout ranges supported by hardware. If 'Longer' is selected, software will use longer timeout ranges.
ARI Forwarding	If supported by hardware and set to 'Enabled', the Downstream Port disables its traditional Device Number filed being 0 enforcement when turning a Type1 Configuration. Request into a Type0 Configuration Request, permitting access to Extended Functions in an ARI Device immediately below the Port. Default value: '**Enabled**'.
Atomicop Requester Eanble	If supported by hardware and set to 'Enabled', this function initiates AtomicOp Requests only if Bus Master Enable bit is in theCommand Register Set. Default value: '**Disabled**'.
Atomicop Egress Blocking	If supported by hardware and set to 'Enable', outbound AtomicOp Requests via Egress Ports will be blocked. Default value: '**Disabled**'.
IDO Request Enable	If supported by hardware and set to 'Enable', this permits setting the number of ID-Based Ordering (IDO) bit (Attribute[2]) requests to be initiated. Default value: '**Disabled**'.
IDO Completion Enable	If supported by hardware and set to 'Enable', this permits setting the number of ID-Based Ordering (IDO) bit (Attribute[2]) requests to be initiated. Default value: '**Disabled**'.
LTR Mechanism Enable	If supported by hardware and set to 'Enable', this enables the Latency Tolerance Reporting (LTR) Mechanism. Default value: '**Disabled**'.
End-End TLP Prefix Blocking	If supported by hardware and set to 'Enable', this function will block forwarding of TLPs containing End-End TLP Prefixes. Default value: 'Disabled'.
PCI Express GEN2 Link Register Settings	
Target Link Speed	If supported by hardware and set to 'Force to X.X GT/s' for Downstream Ports, this sets an upper limit on Link operational speed by restricting the values advertised by the Upstream component in itstraining sequences. When '**Auto**' is selected HW initialized data will be used. The options are: **Auto**, 'Force to 2.5 GT/s', 'Force to 5.0 GT/s', 'Force to 8.0 GT/s', and 'Force to 16.0 GT's'.
Clock Power Management	If supported by hardware and set to 'Enable', the device is permitted to use CLKREQ# signal for power management of Link clock in accordance to protocol. Default value: '**Disabled**'.
Compliance SOS	If supported by hardware and set to 'Enable', this will force LTSSM to send SKP Ordered Sets between sequences when sending Compliance Pattern or Modified Compliance Pattern. Default value: '**Disabled**'.
Hardware Autonomous Width	If supported by hardware and set to 'Disabled', this will disable the hardware's ability to change link width except width size reduction for the purpose of correcting unstable link operation. The default setting is '**Enabled**'.

Hardware Autonomous Speed	If supported by hardware and set to 'Disabled', this will disable the hardware's ability to change link speed except speed rate reduction for the purpose of correcting unstable link operation. The default setting is '**Enabled**'.

3.4.8 Network Stack Configuration



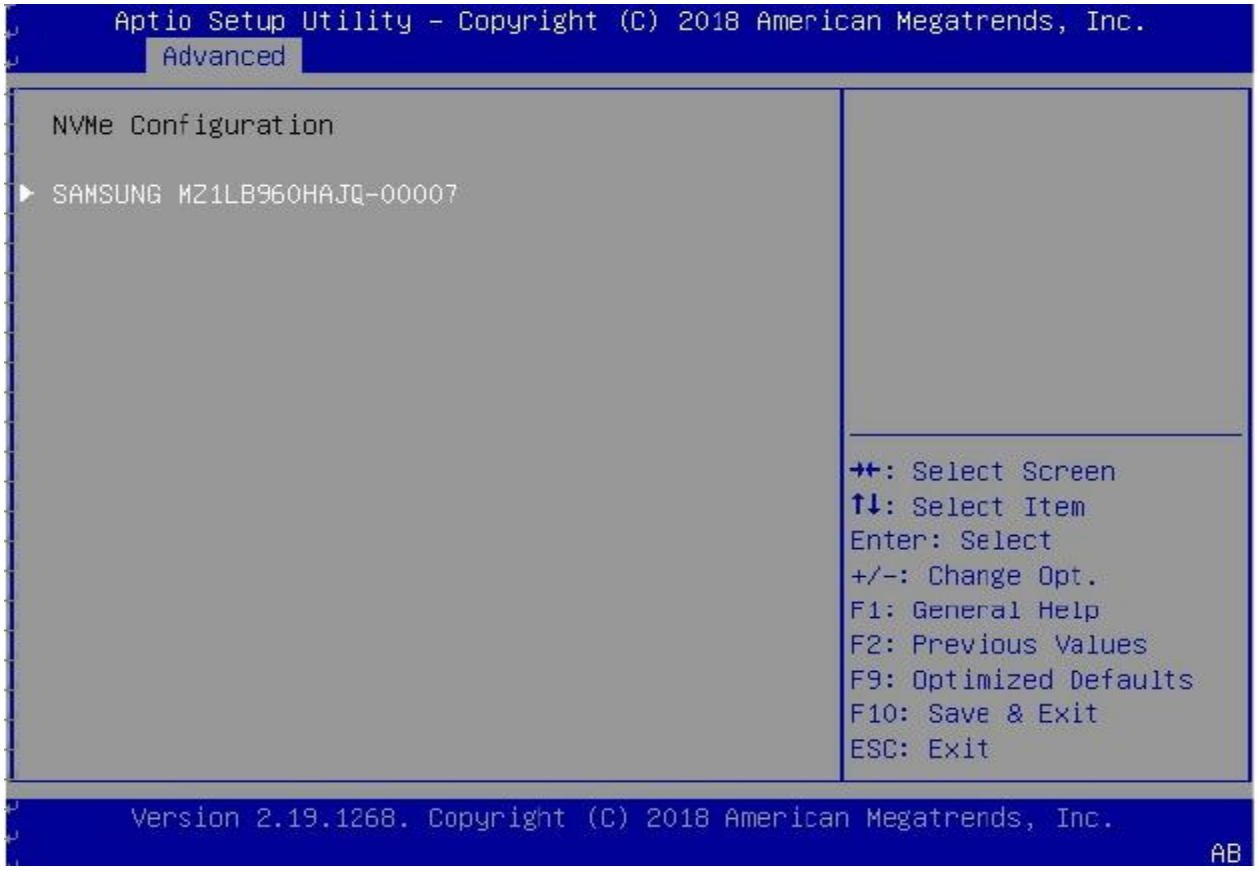
Setting	Description
Network Stack	**Enable**/Disable UEFI Network Stack
Ipv4 PXE Support	**Enable**/Disable IPv4 PXE boot support. If disabled, IPv4 PXE boot support will not be available.
Ipv4 HTTP Support	Enable/**Disable** IPv4 HTTP boot support. If disabled, IPv4 HTTP boot support will not be available.
Ipv6 PXE Support	Enable/**Disable** IPv6 PXE boot support. If disabled, IPv6 PXE boot support will not be available.
Ipv6 HTTP Support	Enable/**Disable** IPv6 HTTP boot support. If disabled, IPv6 HTTP boot support will not be available
IP6 Configuration Policy	Support to **Enable**/Disable IPSEC certificate for kev.
PXE boot wait time	Wait time in seconds to press ESC key to abort the PXE boot. Use either +/- or numeric keys to set the value. The default value: **0**

Medhand-ia Detect count	Number of times the presence of media will be checked. Use either +/- or numeric keys to set the value. The default value: **1**

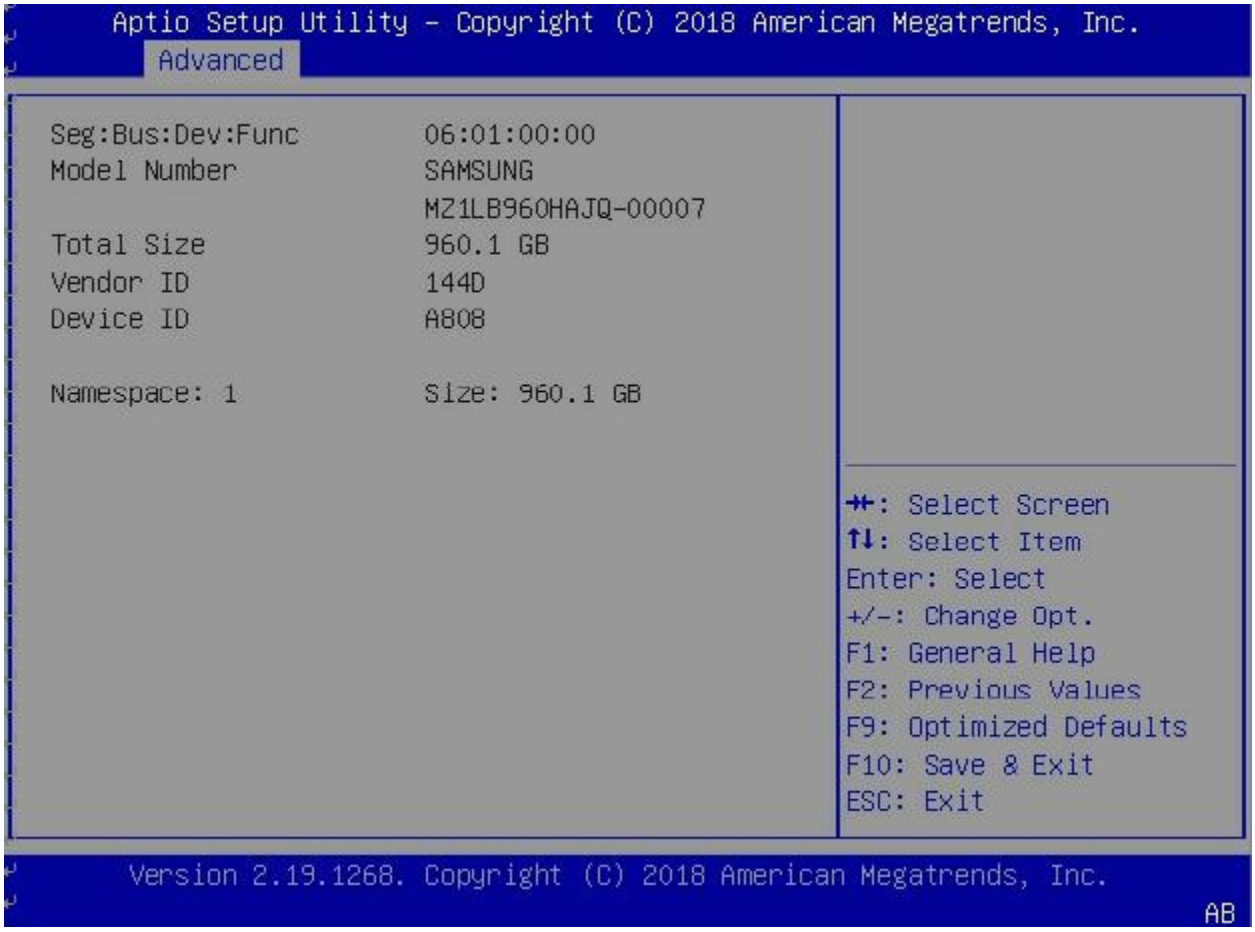
3.4.9 NVMe Configuration

This screen displays information about the NVMe devices detected in the system.

When user selects a device name, more detail information will be displayed as below figure:

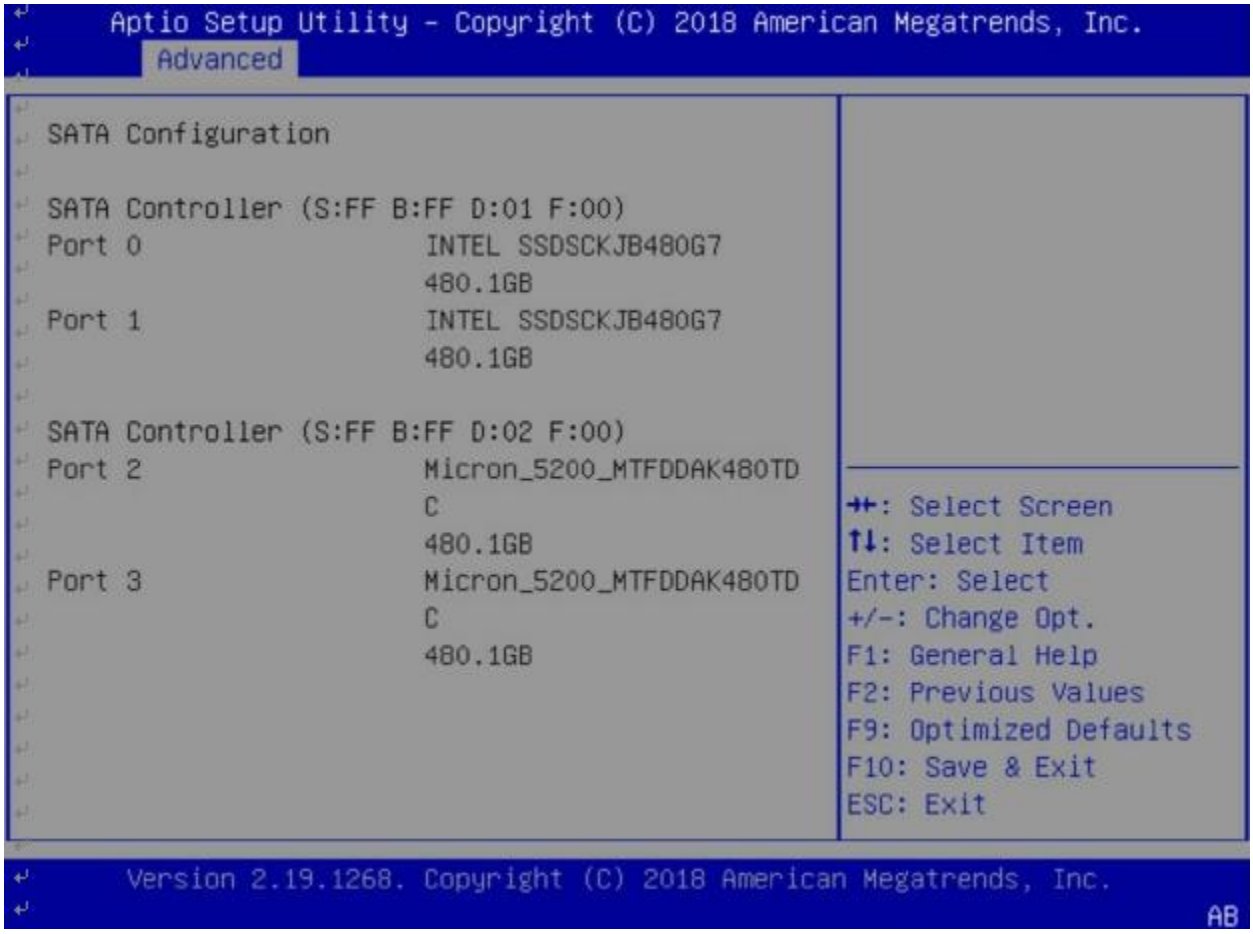


When user selects a device name, more detailed information will be displayed as seen below:


Aptio Setup Utility – Copyright (C) 2018 American Megatrends, Inc.
Advanced
Seg:Bus:Dev:Func 06:01:00:00
Model Number SAMSUNG
MZ1LB960HAJQ-00007
Total Size 960.1 GB
Vendor ID 144D
Device ID A808
Namespace: 1 Size: 960.1 GB
→←: Select Screen
↑↓: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F2: Previous Values
F9: Optimized Defaults
F10: Save & Exit
ESC: Exit
Version 2.19.1268. Copyright (C) 2018 American Megatrends, Inc.
AB

3.4.10 SATA Configuration

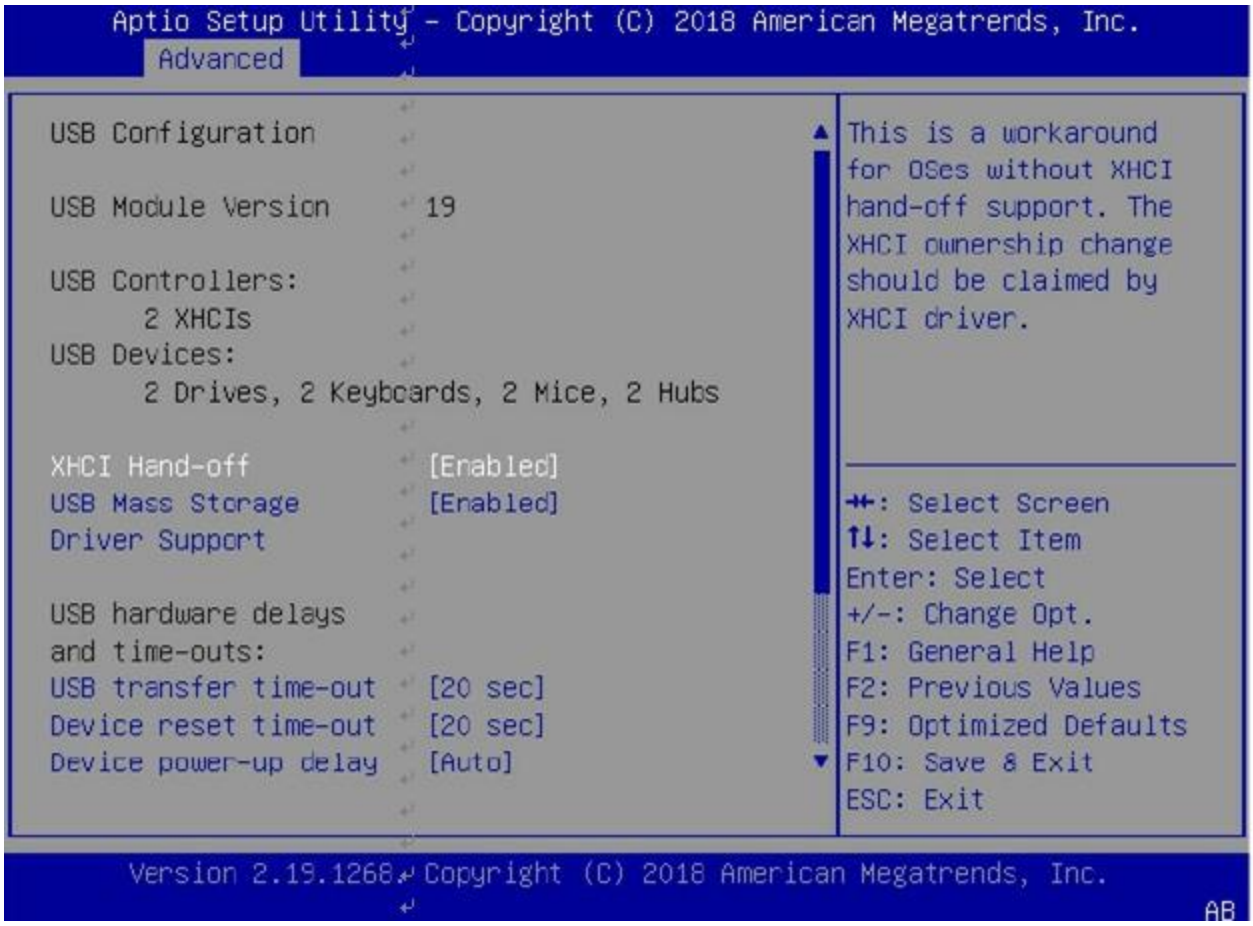
This screen displays information about SATA devices detected in the system.



SATA Controller (S:X B: X D:X F:X): Displays the SATA info of the SATA controller on a PCIe downstream device.

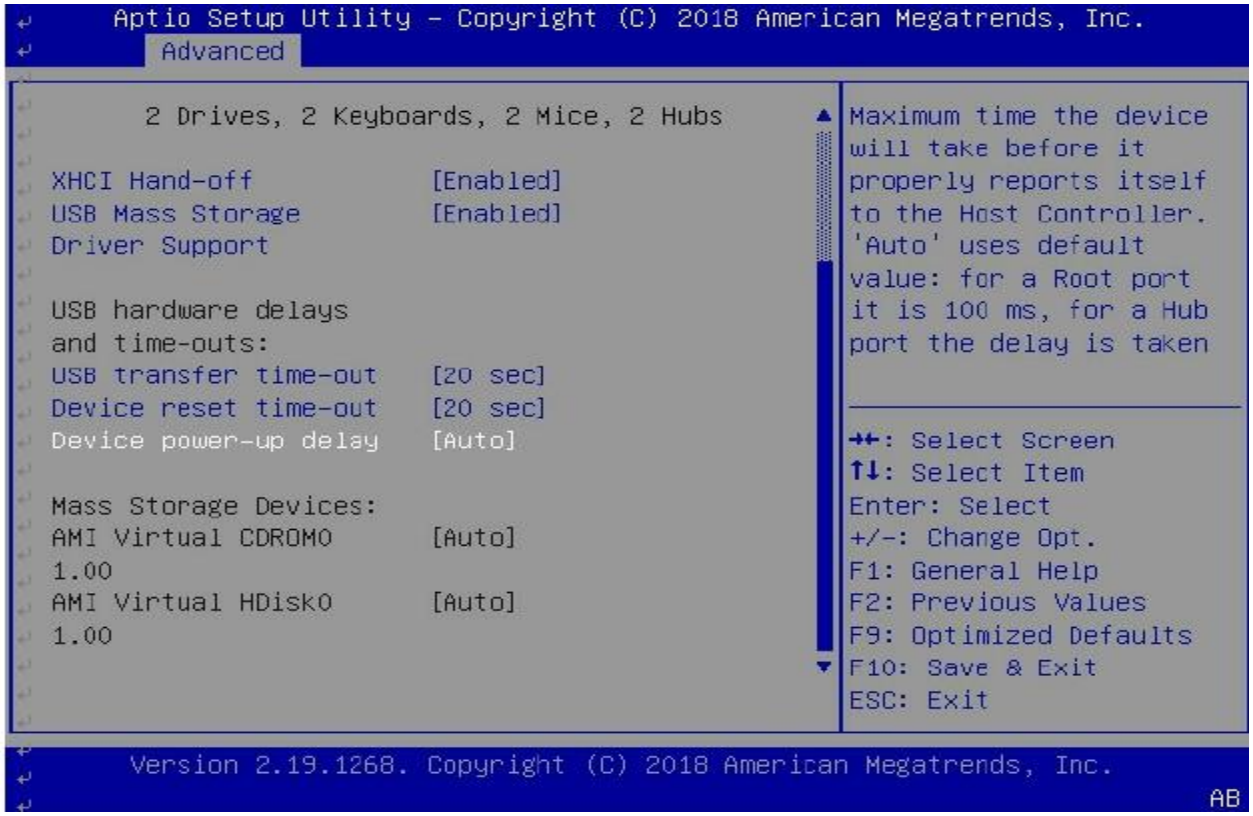
3.4.11 USB Configuration

This screen displays the detected USB devices installed on the system.



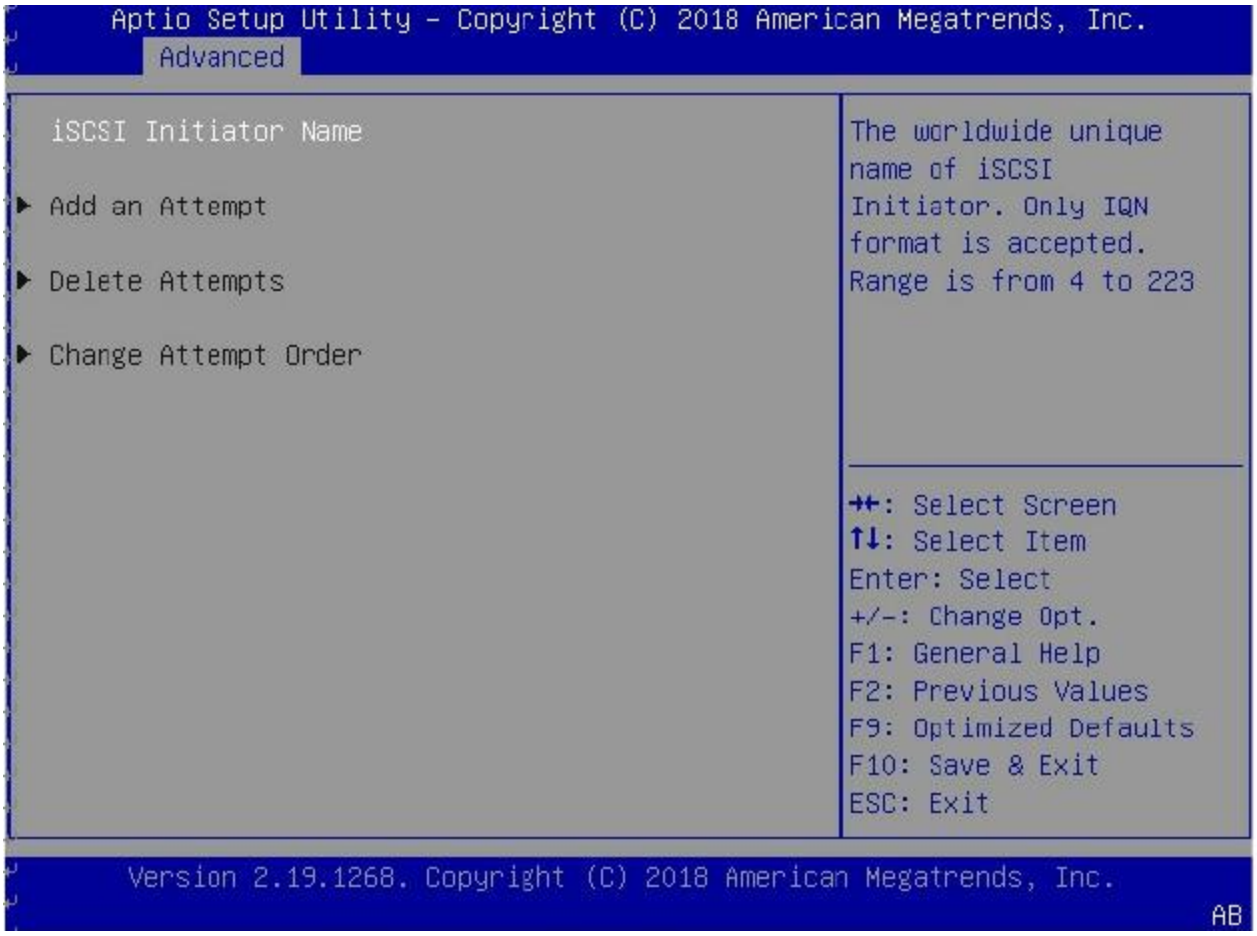
Below table explains fields from this USB configuration setting:

Setting	Description
USB Controllers	Number of USB controllers installed in the system.
USB Devices	Displays list of category USB devices detected in the system.
XHCI HanD-off	This is a workaround for OSes without XHCI hand-off support. The XHCI ownership change should be claimed by XHCI driver. Default value: 'Enabled'.
USB Mass Storage Driver Support	Enable/Disable USB Mass Storage Driver Support.
USB transfer time-out	The time-out value for Control, Bulk, and Interrupt transfers.
Device reset time-out	USB mass storage device Start Unit Command time-out.
Device power-up Delay	Maximum time the device will take before it properly reports itself to the Host Controller. 'Auto' uses default value: for a Root port it is 100 ms, for a Hub port the delay is taken form Hub description.
Mass Storage Devices	Displays list of mass storage devices detected in the system.


Aptio Setup Utility – Copyright (C) 2018 American Megatrends, Inc.
Advanced
2 Drives, 2 Keyboards, 2 Mice, 2 Hubs
XHCI Hand-off [Enabled]
USB Mass Storage Driver Support [Enabled]
USB hardware delays and time-outs:
USB transfer time-out [20 sec]
Device reset time-out [20 sec]
Device power-up delay [Auto]
Mass Storage Devices:
AMI Virtual CDROM0 1.00 [Auto]
AMI Virtual HDisk0 1.00 [Auto]
Maximum time the device will take before it properly reports itself to the Host Controller. 'Auto' uses default value: for a Root port it is 100 ms, for a Hub port the delay is taken
→←: Select Screen
↑↓: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F2: Previous Values
F9: Optimized Defaults
F10: Save & Exit
ESC: Exit
Version 2.19.1268. Copyright (C) 2018 American Megatrends, Inc.
AB

3.4.12 iSCSI Configuration

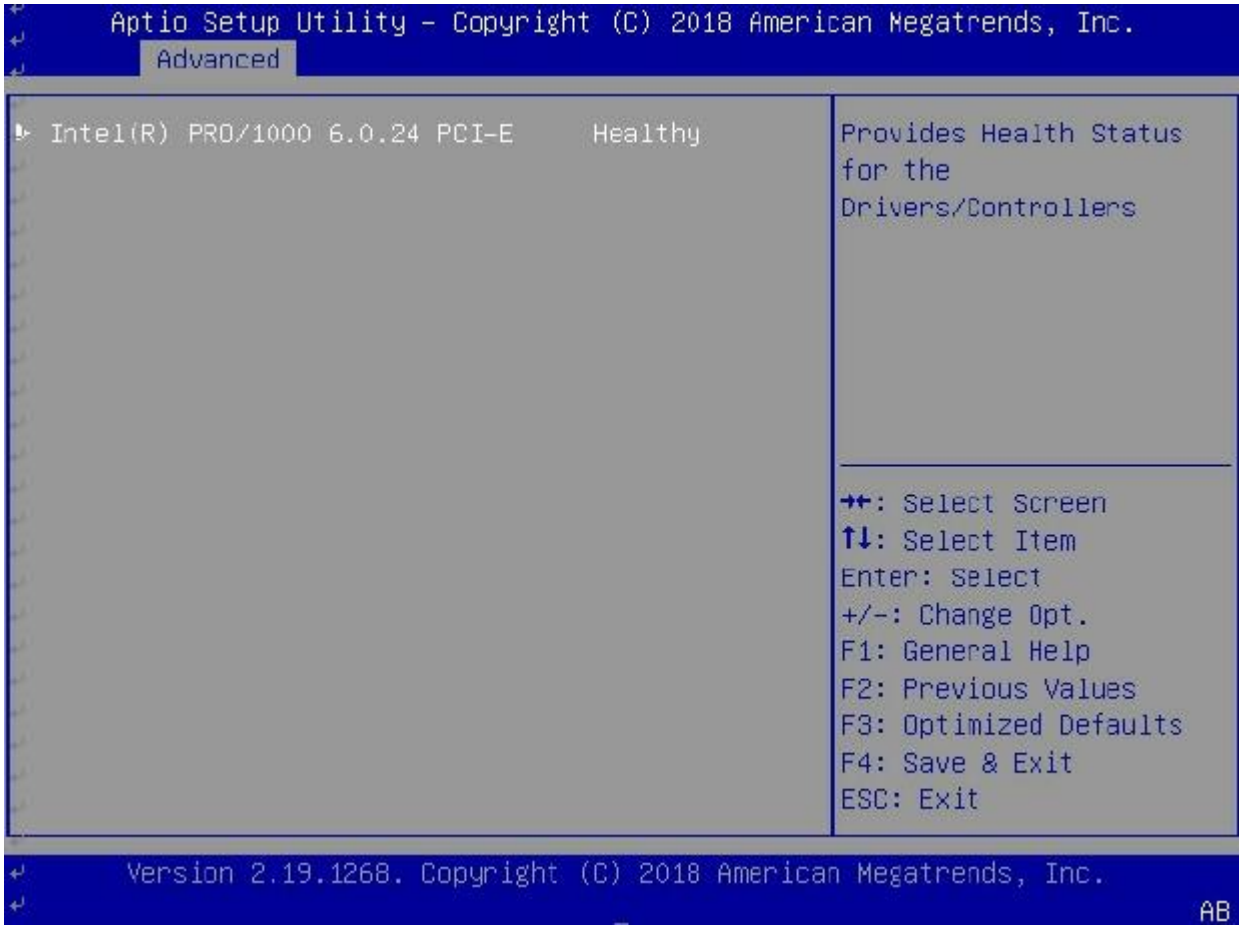
This feature allows the user to enter the unique name of the iSCSI Initiator in IQN format.



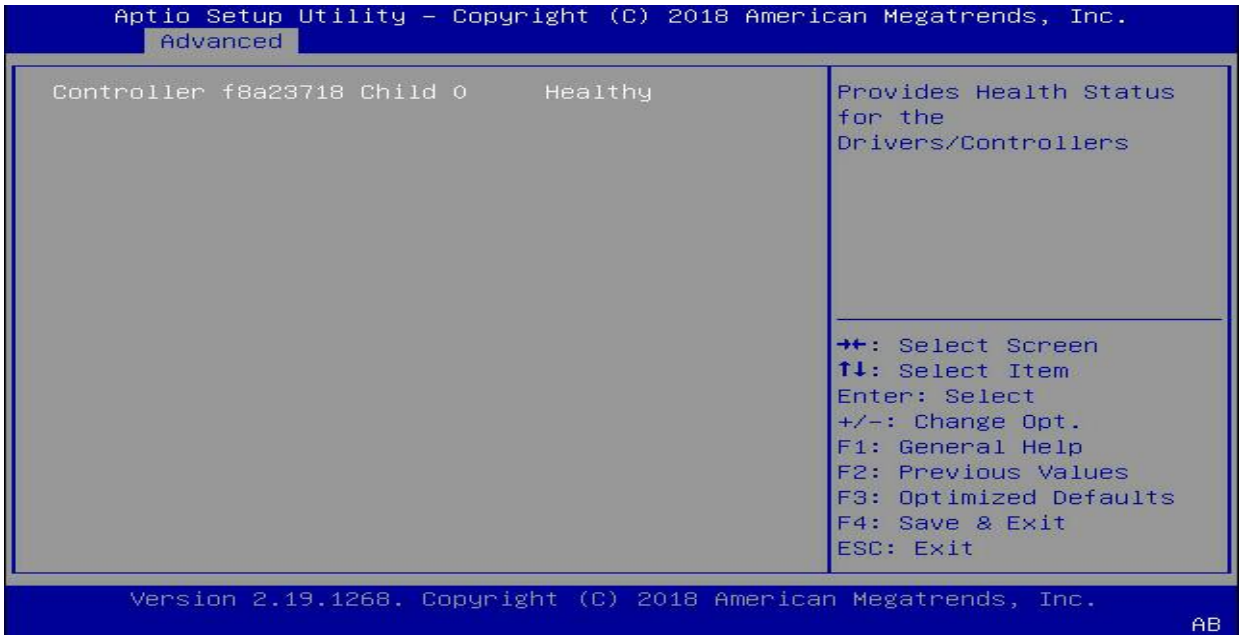
3.4.13 Driver Health

From the Advance tab, press Enter at the “Driver Health” to enter this setup screen.

This screen shows all the PCI devices that their driver installs the driver health protocol.

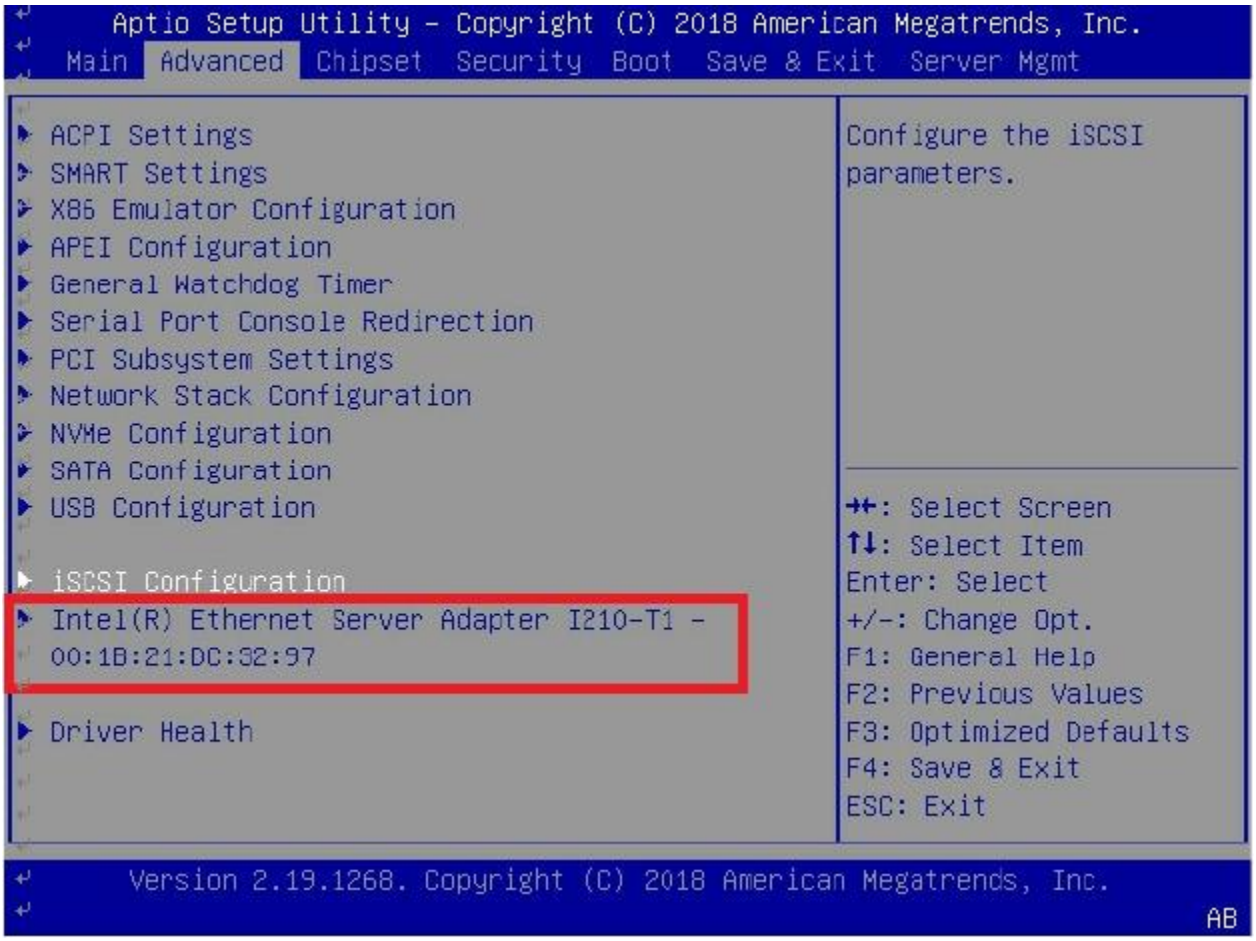


Enter the selected item to know the status of the driver like healthy, failed, configuration (Depends on the information that the driver provides).

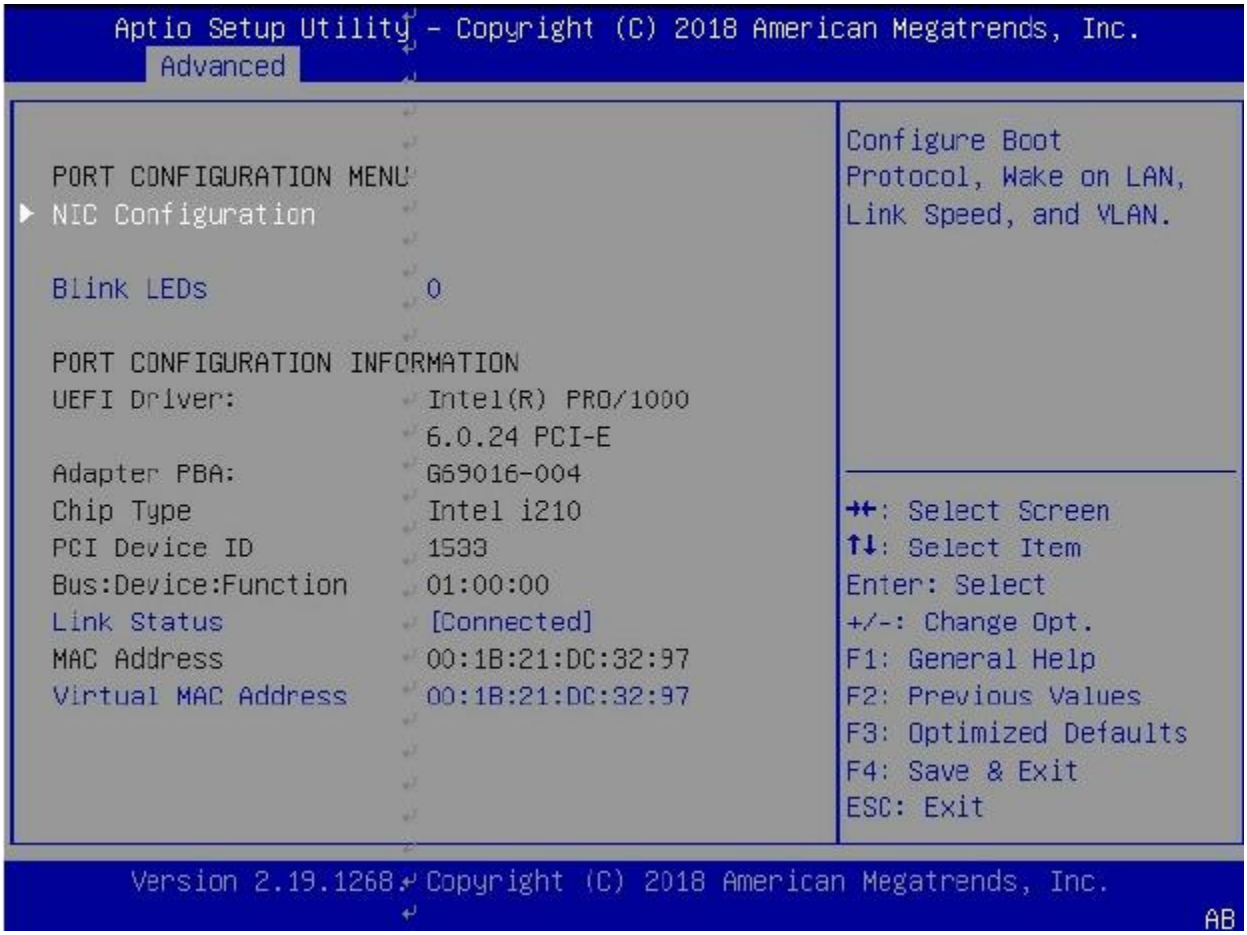


3.4.14 Other Configuration Items

Depend on the device drivers for the PCIE devices plugged, additional menu items might display on the Advance setup page.

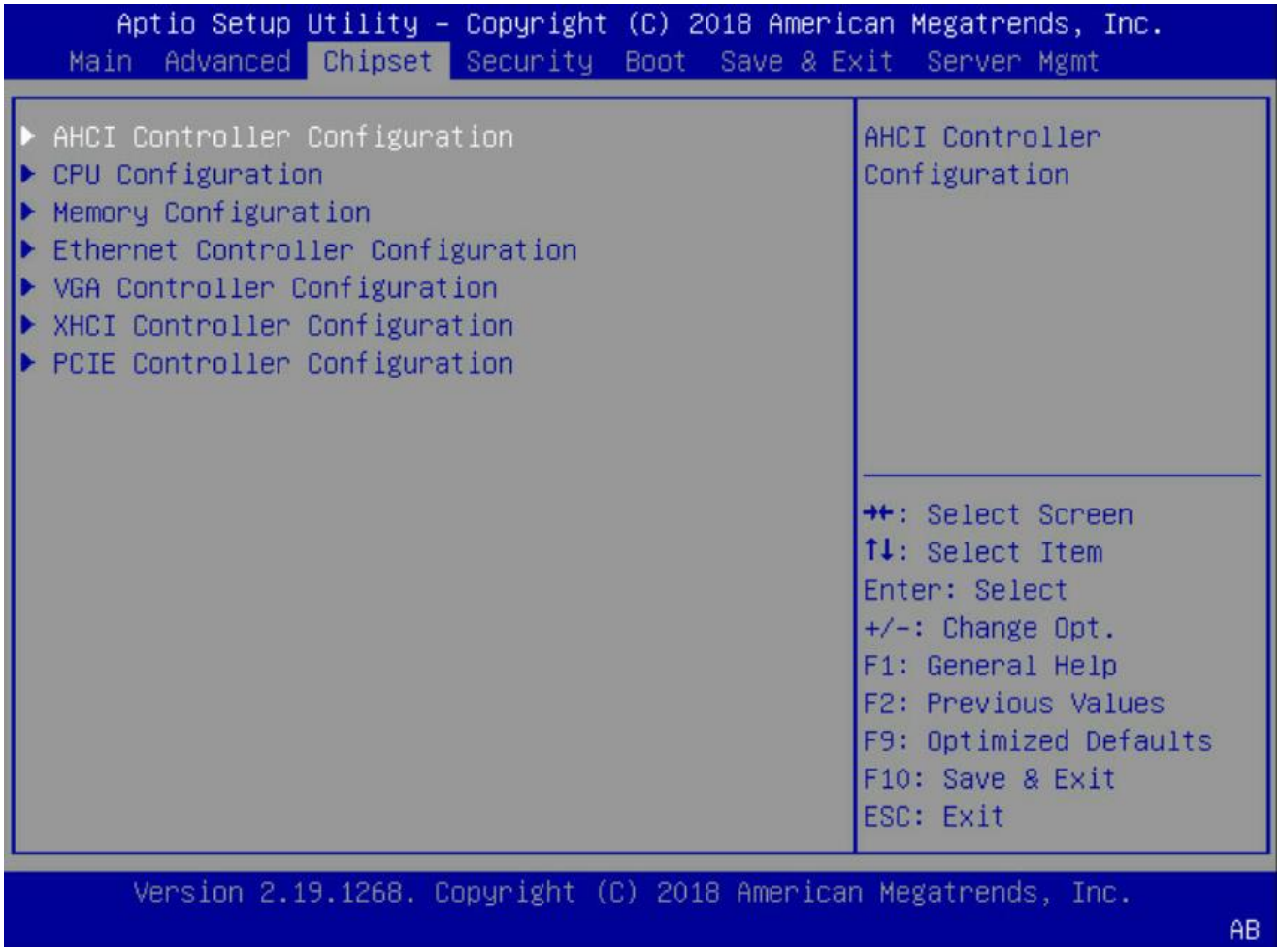


Entering this menu item will allow users to configure the device parameters:



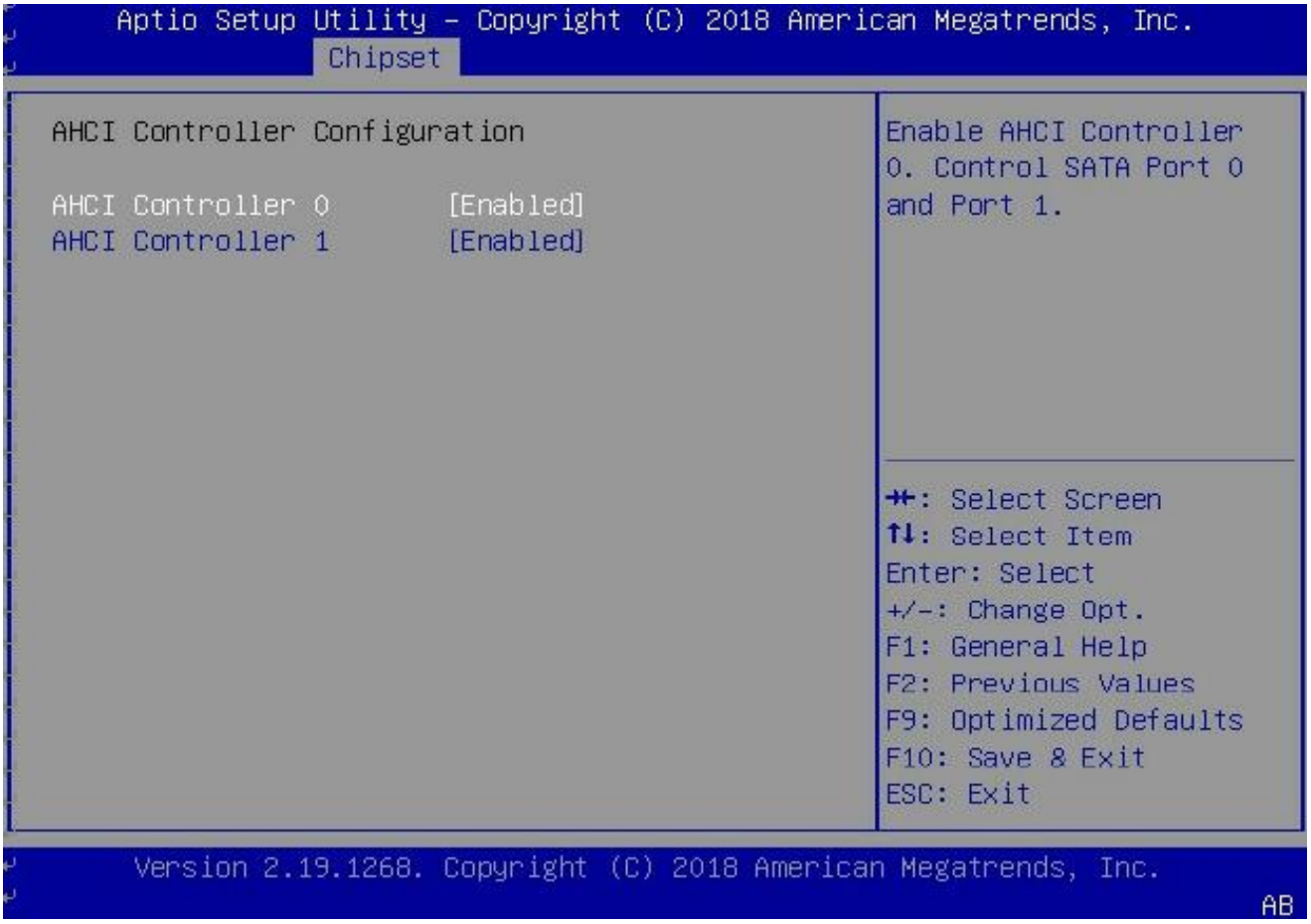
3.5 Chipset

Use the arrow keys to select Chipset on top of the screen. The Chipset Configuration screen looks like below. This screen allows to change settings such as turn on/off some Chip's IPs,



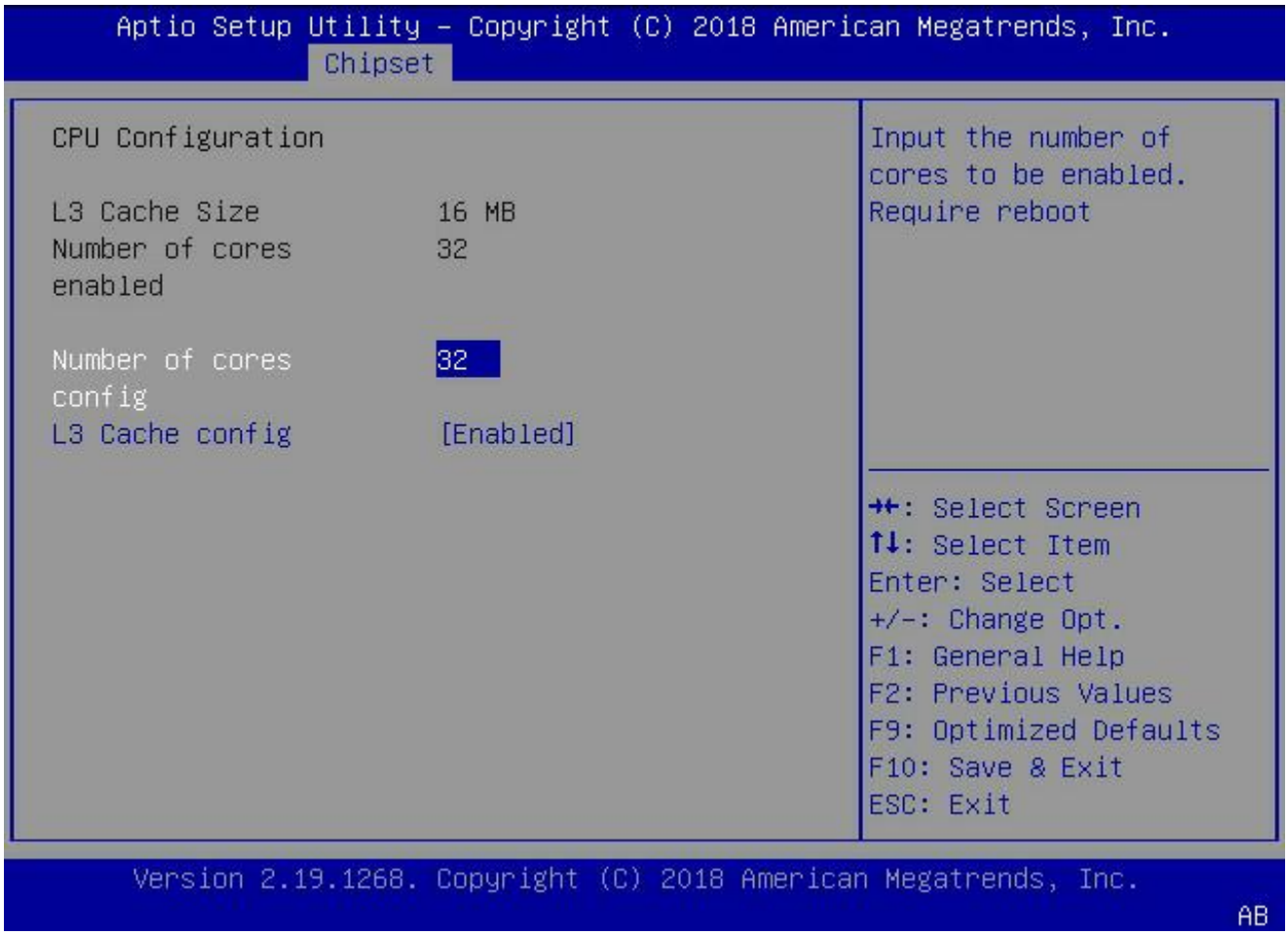
If the system is unstable after changing any settings in advanced configuration, revert to the default settings in the "Save & Exit" screen.

3.5.1 AHCI Controller Configuration



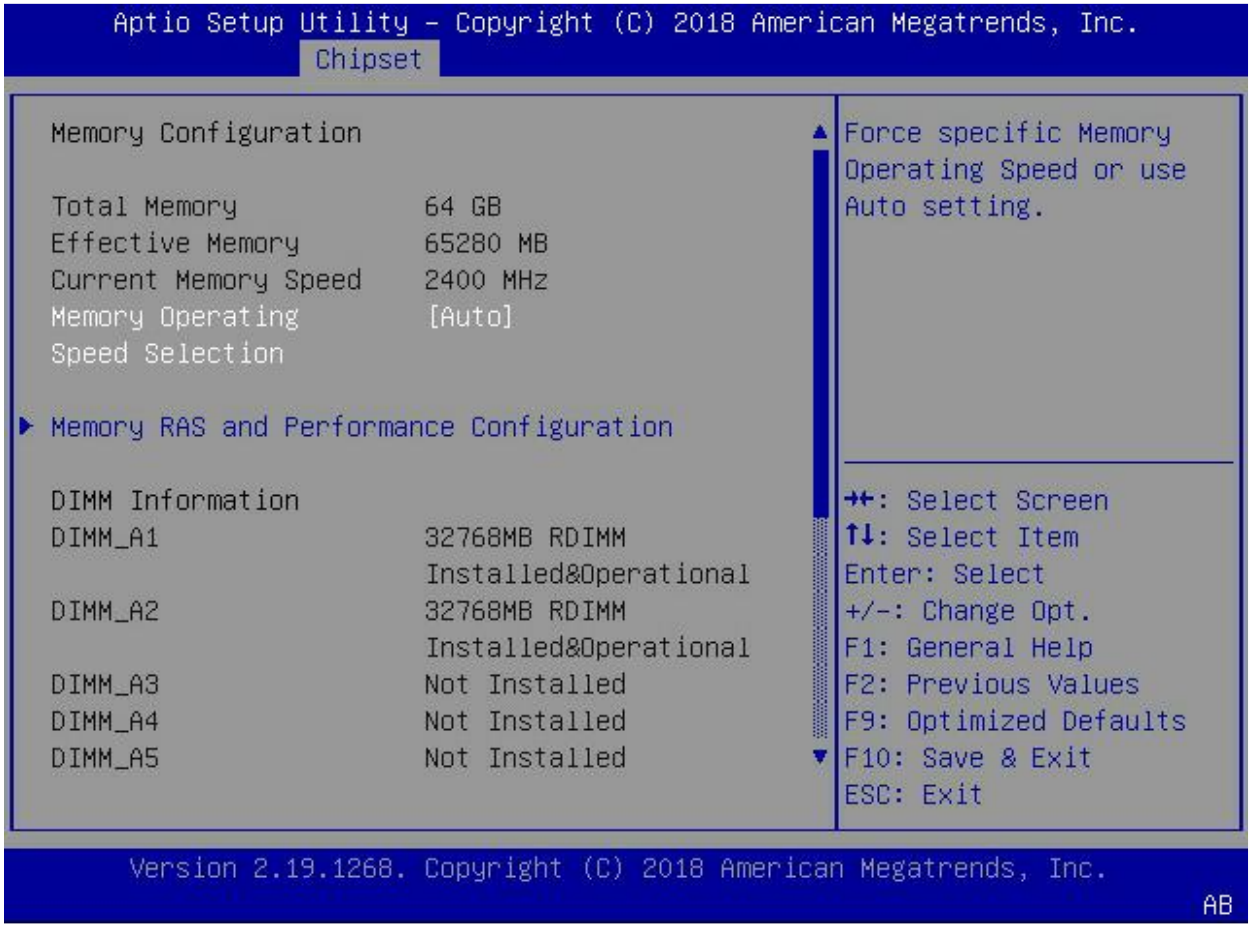
- **AHCI Controller 0:** This option allows to enable/disable AHCI controller 0 which controls SATA port 0/1.
- **AHCI Controller 1:** This option allows to enable/disable AHCI controller 1 which controls SATA port 2/3.

3.5.2 CPU Configuration



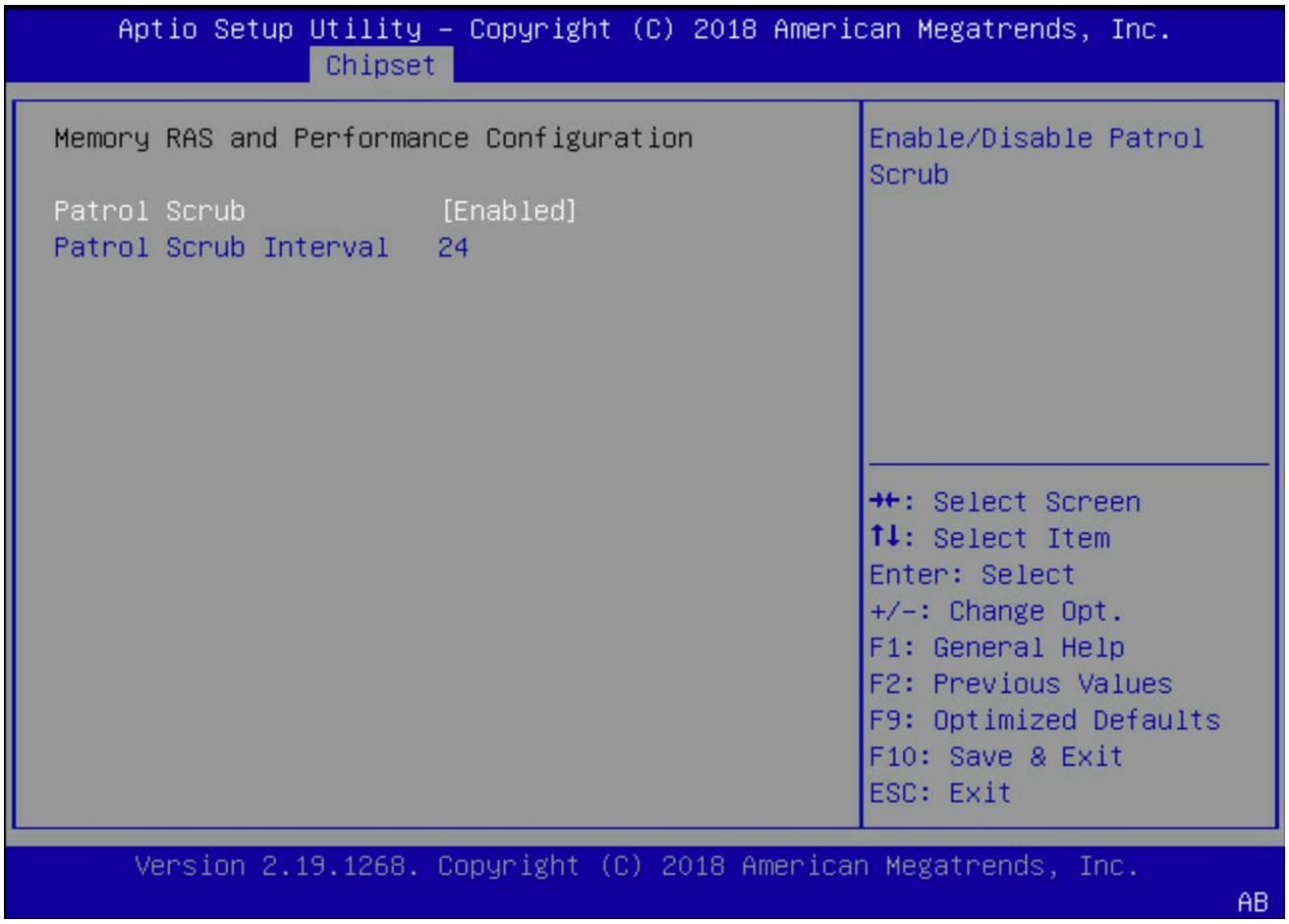
- **L3 Cache Size:** Display the size of CPU L3 Cache in MB.
- **Number of cores enabled:** Display the number of cores enabled in this system.
- **Number of cores configuration:** Input the number of cores to be enabled in the system. This option requires a system reboot to take effect. The number needs to be even. The default value is **32**.
- **L3 Cache configuration:** This option allows to **enable**/disable L3 Cache. Disabling L3 cache will make the system run slower so it is not recommended to disable it.

3.5.3 Memory Configuration



Memory Configuration parameters are explained in the following table:

Setting	Description
Total memory	The total memory installed in the system.
Effective Memory	The memory that can be used for BIOS and OSes. Some memory is preserved for Firmware which is not available to use.
Current Memory Speed	The current speed in MHz that the DDR controller is running.
Memory Operating Speed Selection	Allows to set the desired speed of DDR controller. The options are: **Auto**, 1600, 1866, 2133, 2400, and 2667. Changing this option may make the system unstable and the system will recover to previous value in case of booting failure.
Memory RAS and Performance Configuration	Displays and provides options to change the memory RAS and performance settings.
DIMM Information	Display DDR information of all slots in the system.

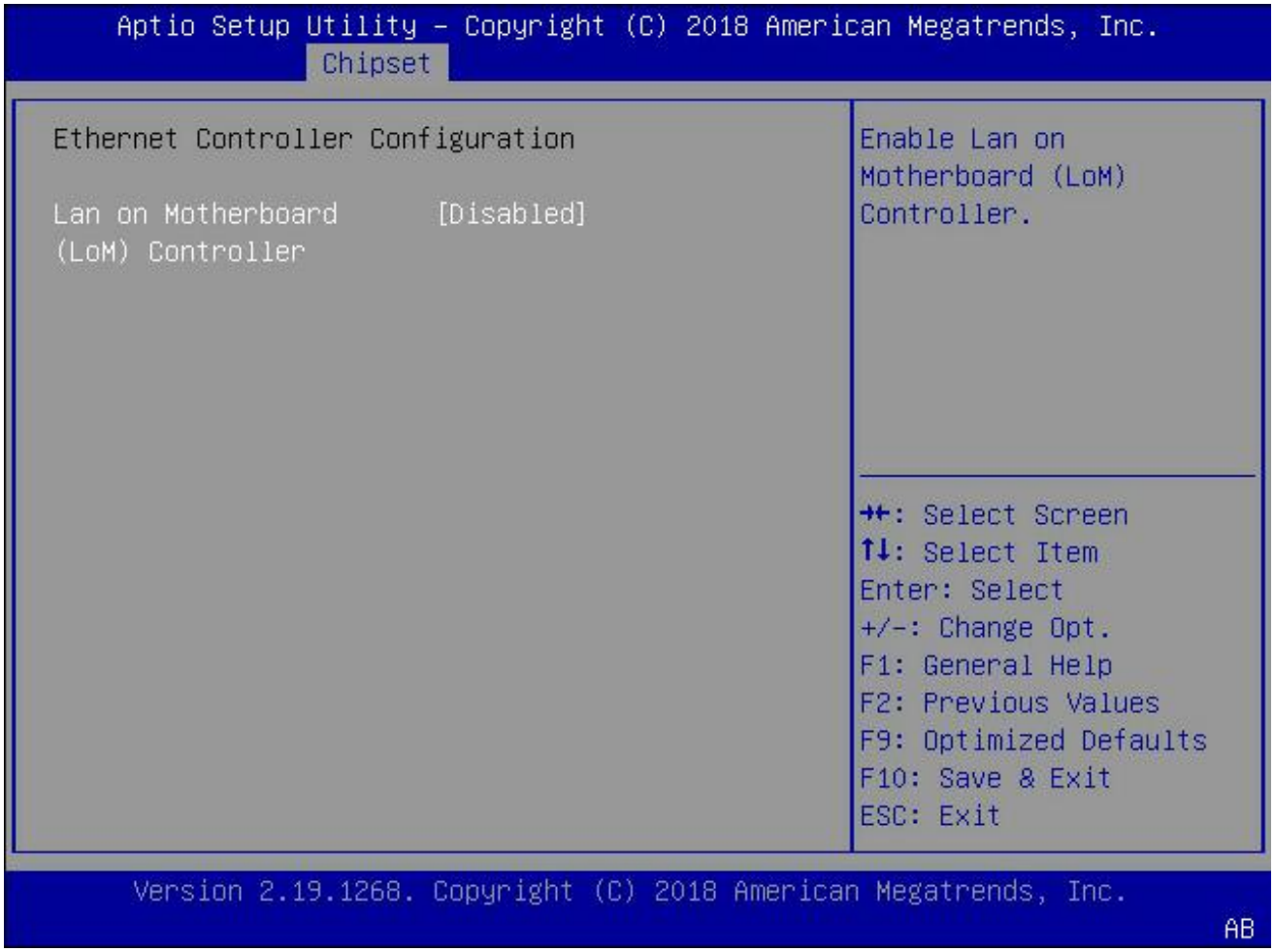


Patrol Scrub: Enable/disable Patrol Scrub for DDR controller.

3.5.4 Ethernet Controller Configuration

This setting allows users to enable/disable the LOM Controller.

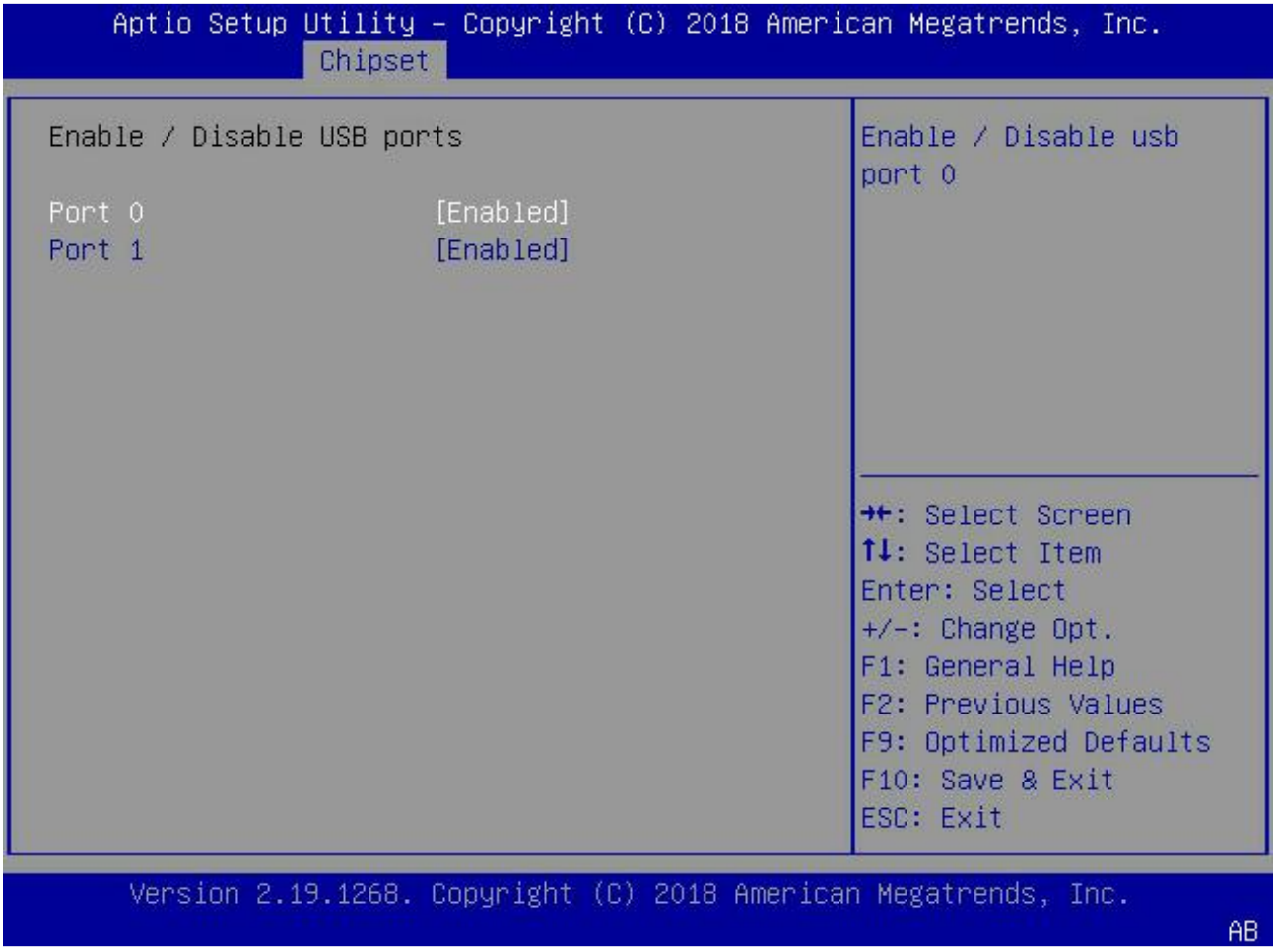
Note that there is no LOM controller available in the M/B board so users should never enable this option.



3.5.5 VGA Controller Configuration

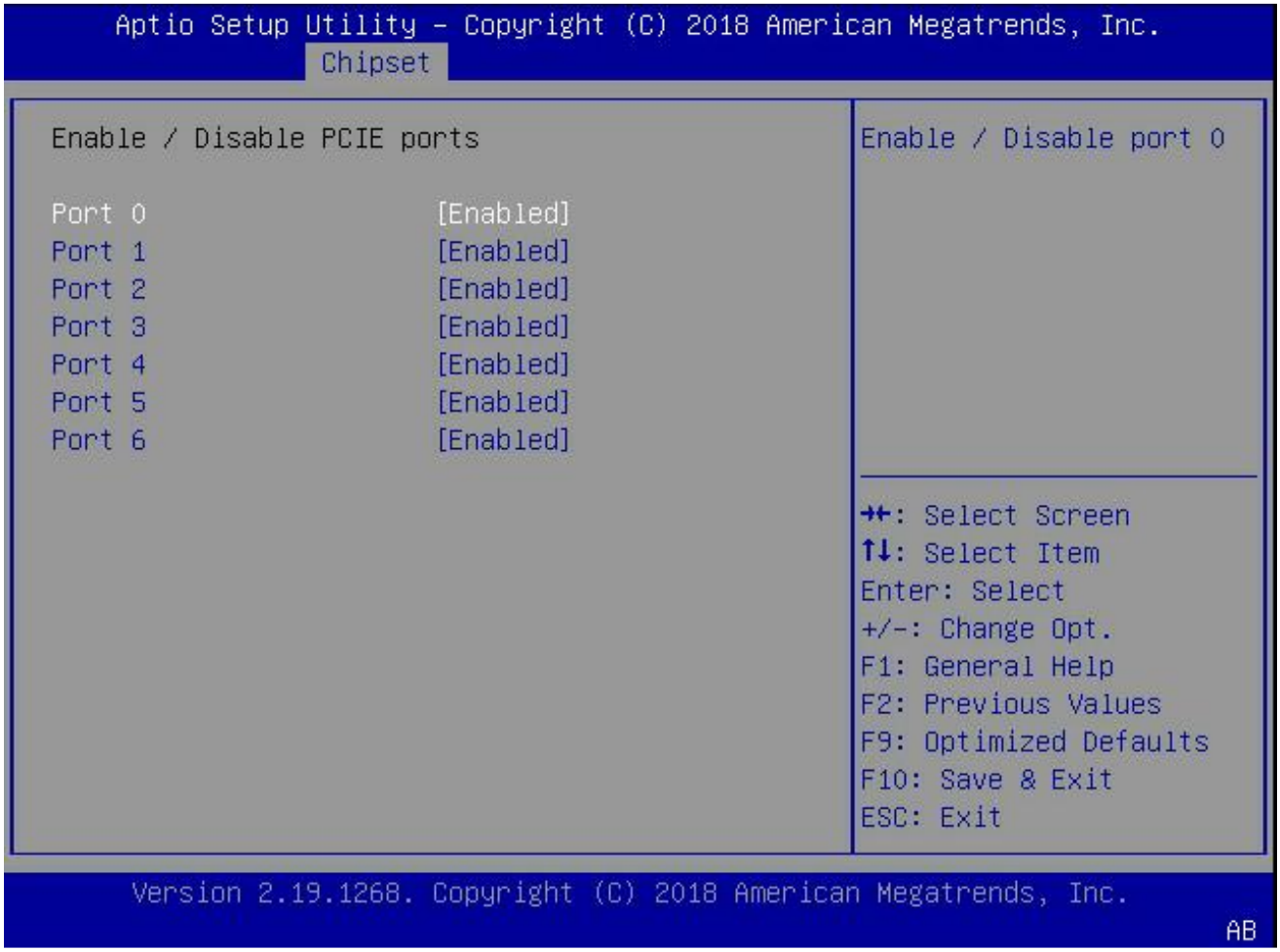
Allow users to **enable**/disable the Aspeed VGA controller. When disabled is selected, the on-board VGA controller will not be available to use.

3.5.6 XHCI Controller Configuration



- Port 0: allows to **enable**/disable the USB port 0.
- Port 1: allows to **enable**/disable the USB port 1.

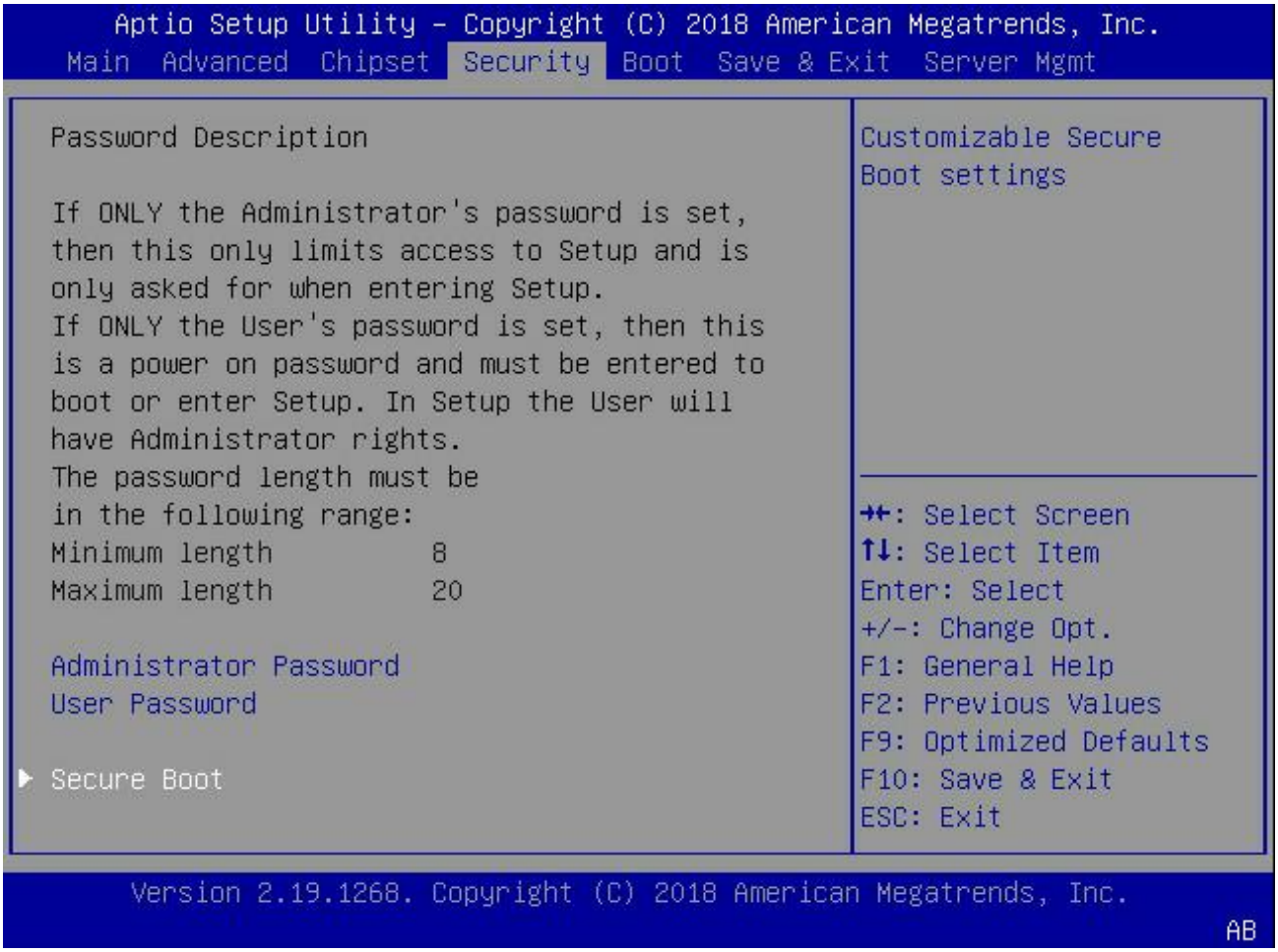
3.5.7 PCIE Controller Configuration



NOTE: PCIe configuration is auto-configured by the BIOS based on the detected riser cards. Users should never change anything in this menu.

3.6 Security Configuration

Use the arrow keys to select Security on top of the screen. The Security Configuration screen looks like below:

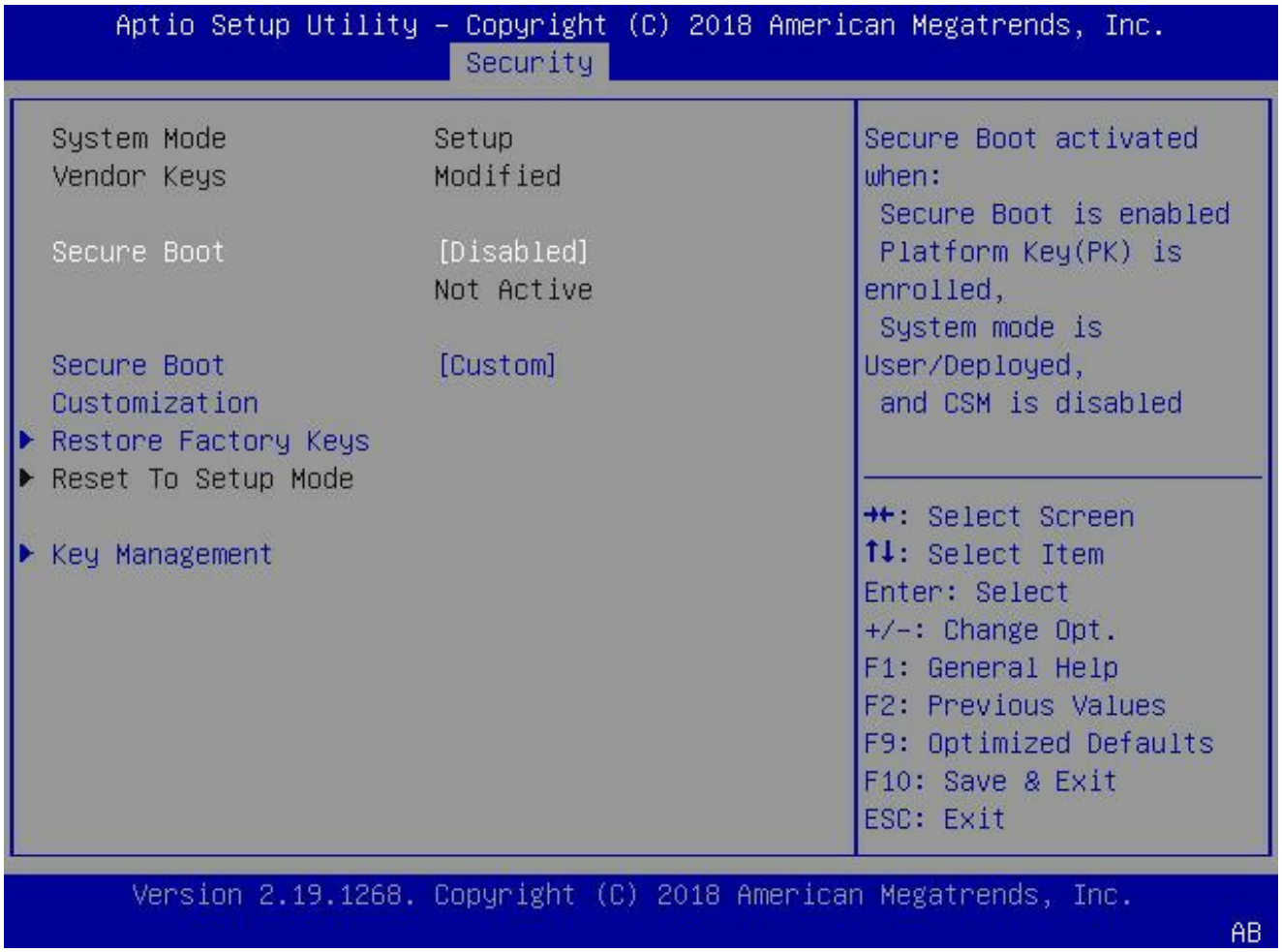


Administrator Password: allows users to set Administrator password.
User Password: allows users to set User password.

The Administrator and User Password MUST follow below policy:
- String length 8~20 characters;
- Include non-alpha numeric characters (~`!@#$%^&*()-+={}[]|:;"'<>,?/._), uppercase characters, lowercase characters, and numbers.
- The number characters are needed. Must contains 2 type characters of non-alpha numeric characters, uppercase characters, lowercase characters.
- No more than 2 consecutive occurrences of the same character
- Can’t use a password that you have used in your past 3 password changes.

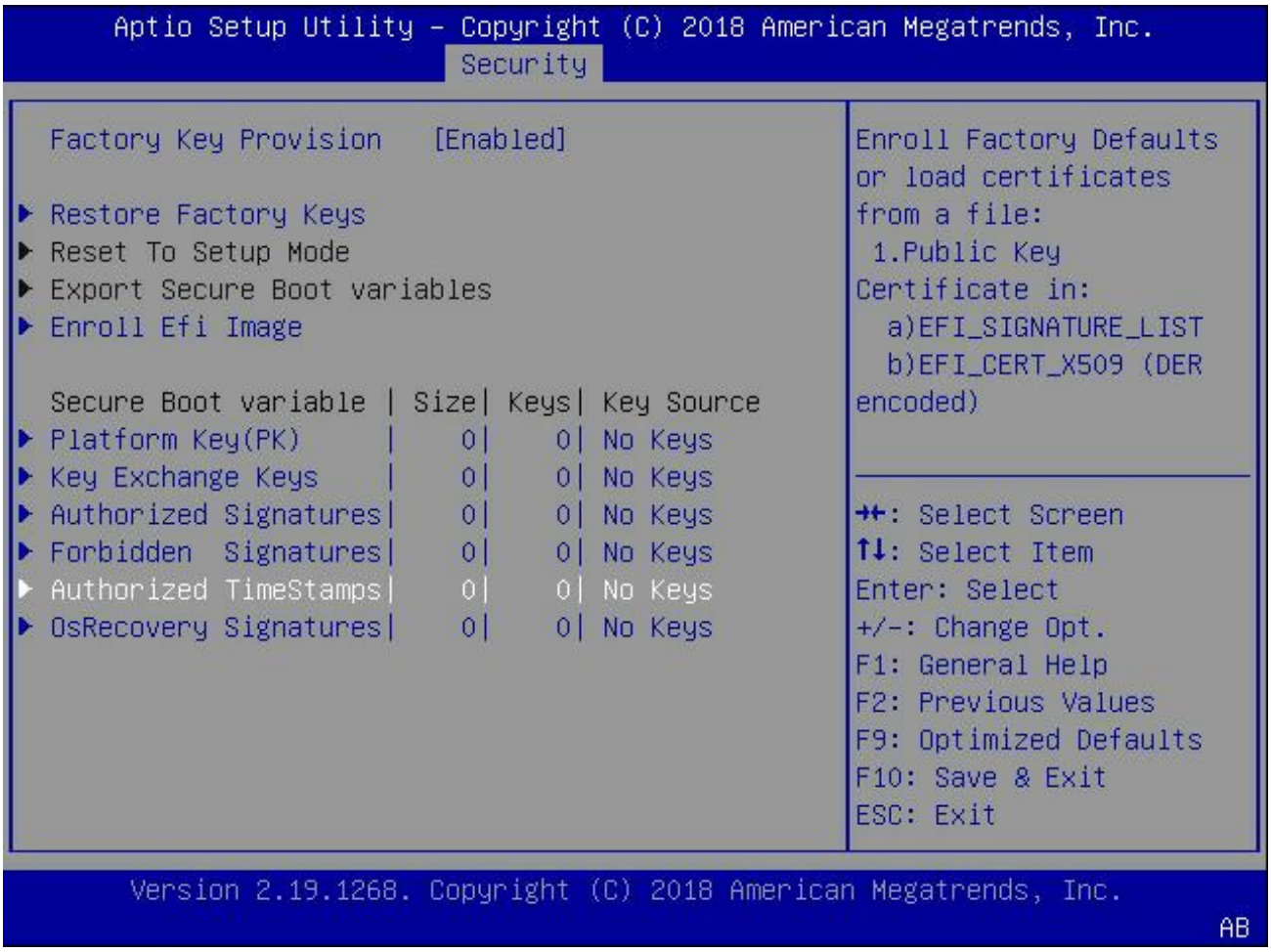
3.6.1 Secure Boot

Allow users to configure boot mode and key management.



- **Secure Boot:** Allow users to enable/disable secure boot feature. The default value is '**Disabled**'. Secure Boot feature is active if Secure Boot is Enabled, Platform Key (PK) is enrolled and the system is in User Mode. The mode change requires a platform reset.
- **Secure Boot Customization:** Secure Boot mode options: '**Standard'** or 'Custom'. In Custom mode, Secure Boot Policy variables can be configured by a physically present user without full authentication.
- **Restore Factory Keys:** Force system to User Mode and install factory default Secure Boot key databases.
- **Reset to Setup Mode:** Delete NVRAM content of all UEFI Secure Boot key database.
- **Key Management:** Allows the user to configure the following key Management settings:

3.6.1.1 Key Management



Key management access the following format:

- P**ublic Key Certificate:** EFI Signature List, EFI CERT X509 (DER Encoded), EFI CERT RSA2048 (Bin), EFI SERT SHAXXX
  Authenticated UEFI Variable
- **Key Source:** Factory, External, Mixed.

Setting for key management:

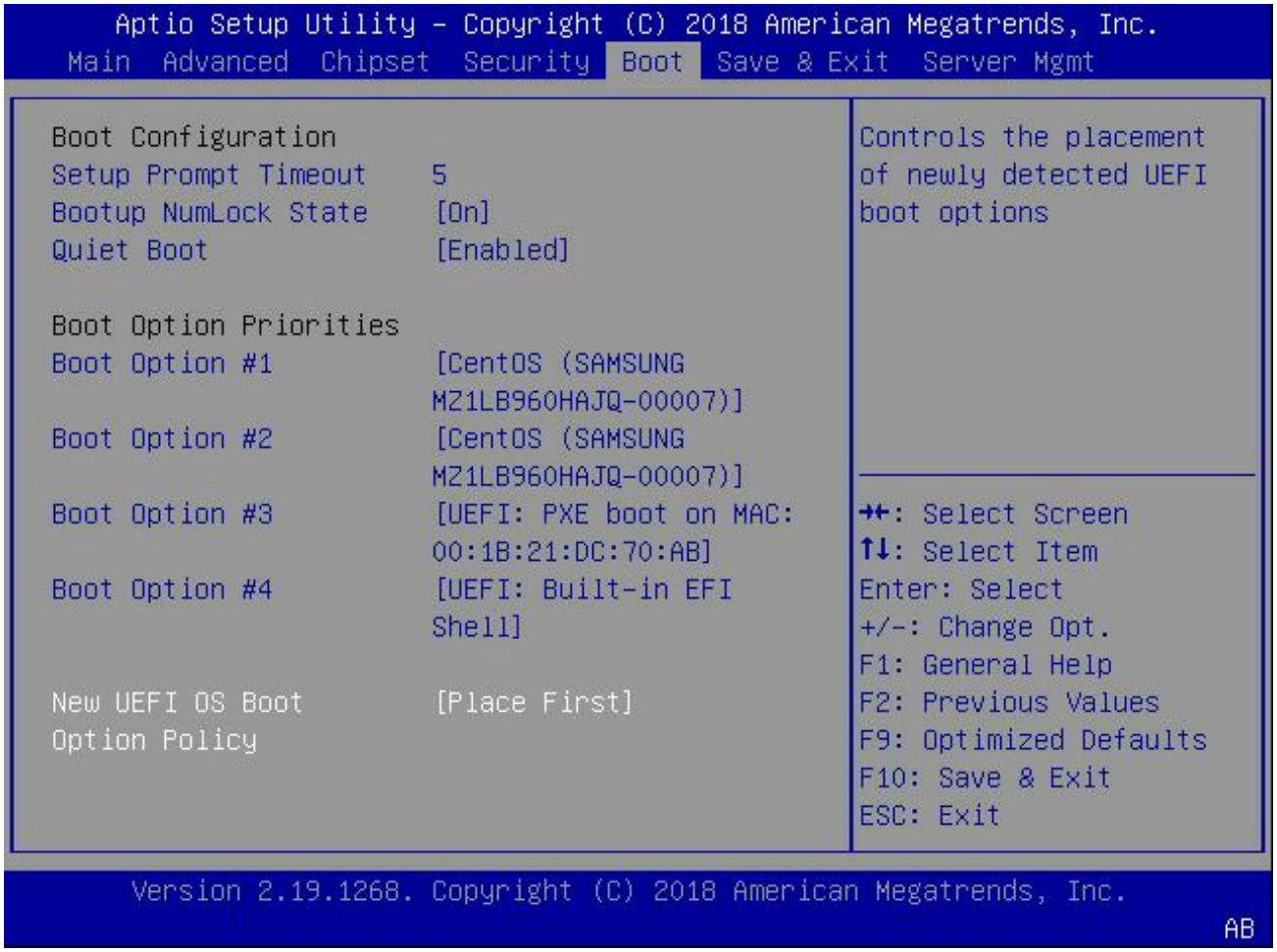
- **Factory Key Provision:** If enabled, install factory default Secure Boot keys after the platform resets. It is applicable only when the system is in Setup Mode.
- **Restore Factory Keys:** Force system to User Mode by configuring NVRAM to contain OEM-defined factory default Secure Boot keys.
- **Reset to Setup Mode:** Delete all Secure Boot key databases from NVRAM.
- **Secure Boot variables:** Copy NVRAM content of Secure Boot variables to files in a root folder on a file system device.
- **Enroll EFI Image:** Allow the image to run in Secure Boot mode. Enroll SHA256 hash certificate of a PE image into Authorized Signature Database (db).

Secure Boot variable:
1. **Platform Key (PK):** This feature allows the user to configure the settings of the Platform Keys. User can update it using value from Factory Defaults or from a file in the file system.
2. **Key Exchange Keys:** This feature allows the user to configure the settings of the Key Exchange Keys. User can update/append it using value from Factory Defaults or from a file in the file system.
3. **Authorized Signatures:** This feature allows the user to configure the settings of the Authorized Signatures. User can update/append it

using the value from Factory Defaults or from a file in the file system.
4. **Forbidden Signatures:** This feature allows the user to configure the settings of the Forbidden Signatures. User can update/append it using value from Factory Defaults or from a file in the file system.
5. **Authorized TimeStamps:** This feature allows the user to configure the settings of the Authorized TimeStamps. User can update/append it using value from Factory Defaults or from a file in the file system.
6. **OsRecovery Signatures:** This feature allows the user to configure the settings of the OsRecovery Signatures. User can update/append it using value from Factory Defaults or from a file in the file system.

3.7 Boot

Use the arrow keys to select Boot on top of the screen. The Boot Settings screen looks like below.

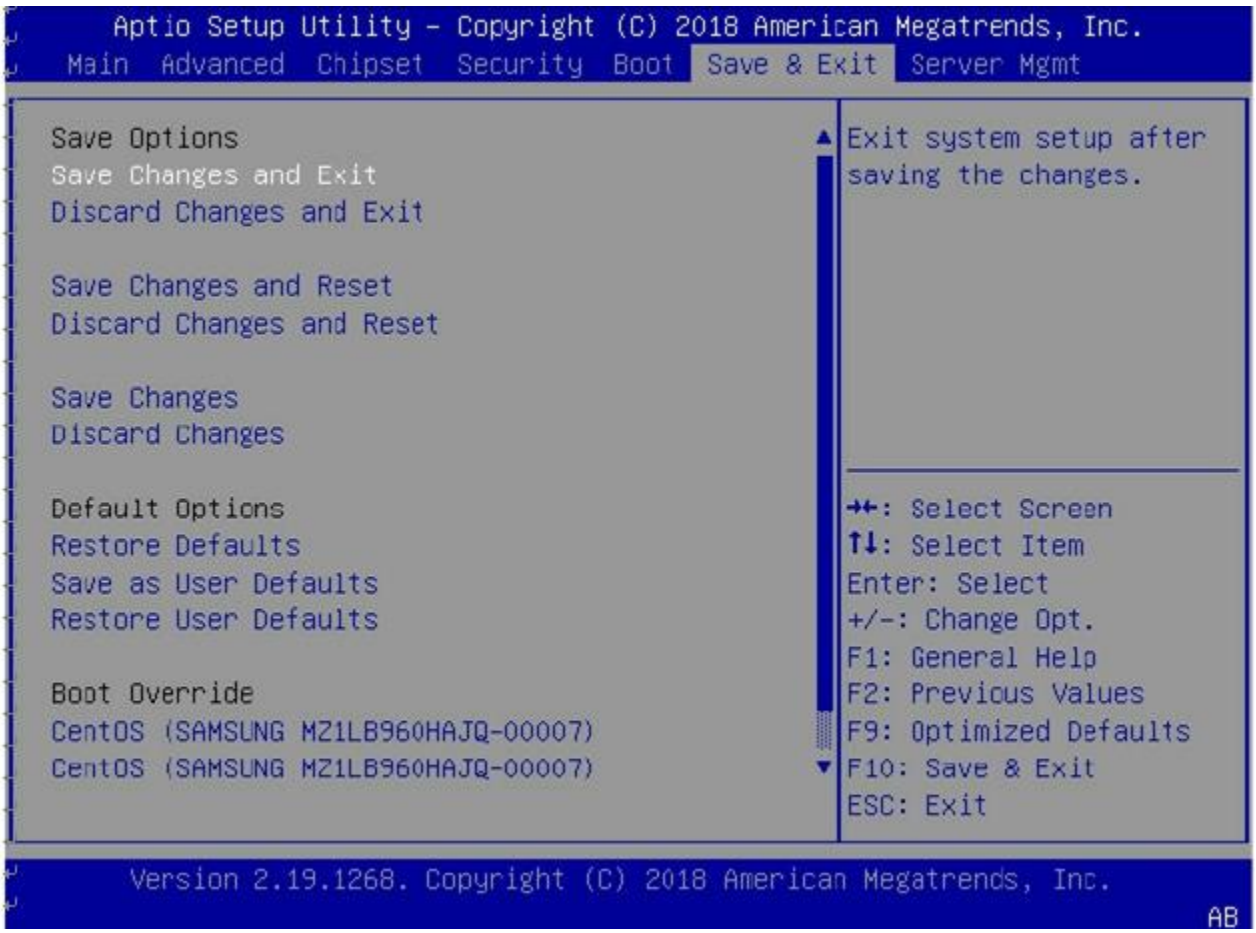


Boot Configuration:

- **Setup Prompt Timeout:** Set the number of seconds to wait for setup activation key. 65535 (0xFFFF) means indefinite waiting. The default value is 5 seconds
- **Bootup NumLock State:** Select the keyboard NumLock state when boot. The options are: On and Off
- **Quiet Boot:** Enables or disables Quiet Boot option. The default value is 'Enabled'
- **Boot Option Priorities:** Prioritizes the order of bootable devices that the system boots from. Press <Enter> on each entry from top to bottom to select devices.
- **New UEFI OS Boot Option Policy:** Controls the placement of newly detected UEFI boot options. The default value is '**Place First**' so any new OS installed will have highest priority. The options are: 'Default', 'Place First', 'Place Last'.

3.8 Save & Exit

Use the arrow keys to select Save & Exit on top of the screen. The Save and Exit screen looks like below.



3.8.1 Save Options

- **Save Changes and Exit:** Set this option to exit system setup after saving the changes.
- **Discard Changes and Exit:** Select this option to quit the BIOS Setup without making any permanent changes to the system configuration.
- **Save Changes and Reset:** Select this option to reset the system after saving the changes
- **Save Changes:** Select this option to save the changes from users and allow users to continue to make changes.
- **Discard Changes:** Select this option to revert the changes from users.
- **Discard Changes and Reset:** Select this option to reset the system without making any permanent changes to the system configuration.

NOTE: The BIOS is reset when you select “Save Changes and Exit” option when users changes below BIOS setting:

- L3 Cache Enable
- Memory Operating Speed Selection.

3.8.2 Default Options

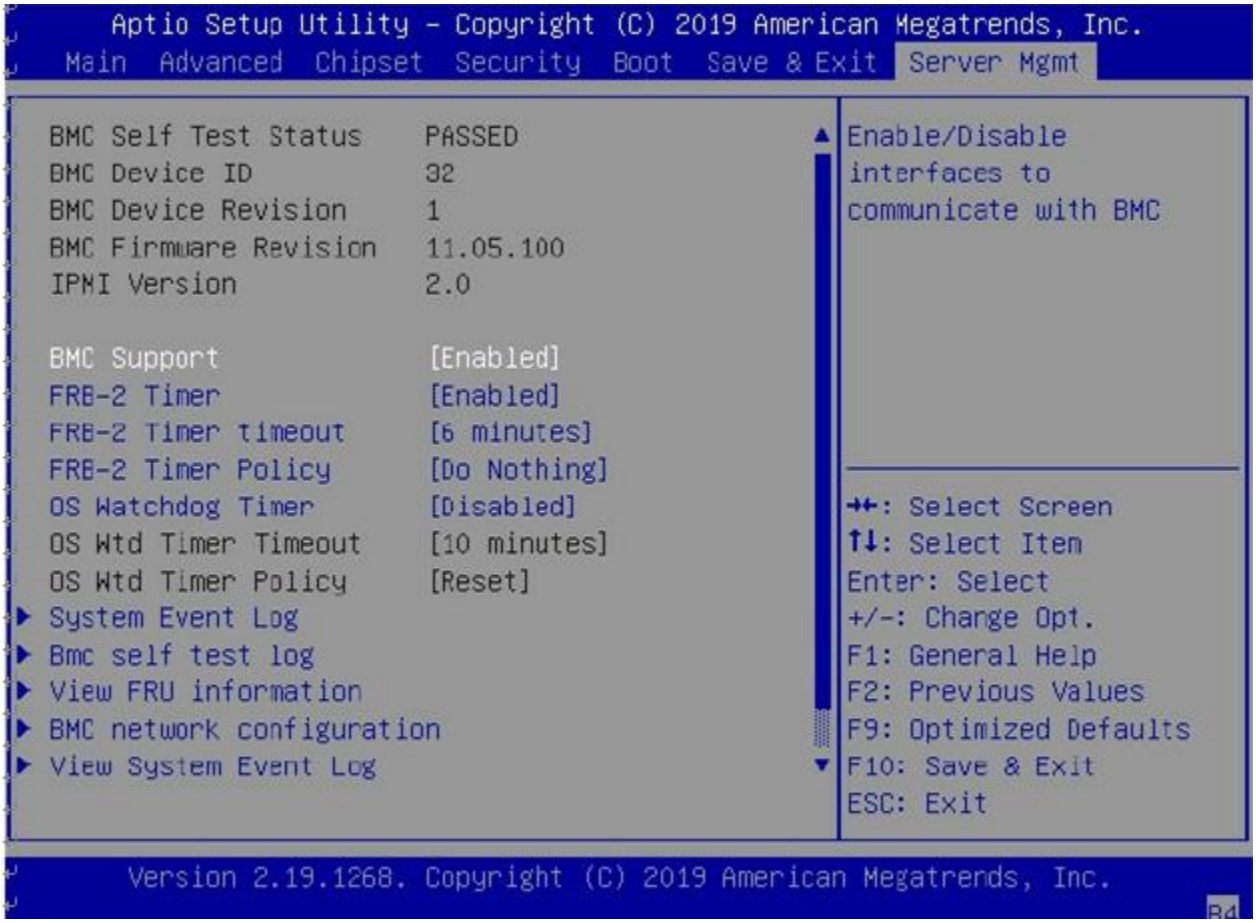
- **Restore Defaults:** Select this option to restore the factory settings which is designed for maximum system stability, but not for maximum performance.
- **Save as User Defaults:** Select this option to enable the user to save any changes to the BIOS setup for future use.
- **Restore User Defaults:** Select this option to retrieve user-defined settings that were saved previously.

3.8.3 Boot Override

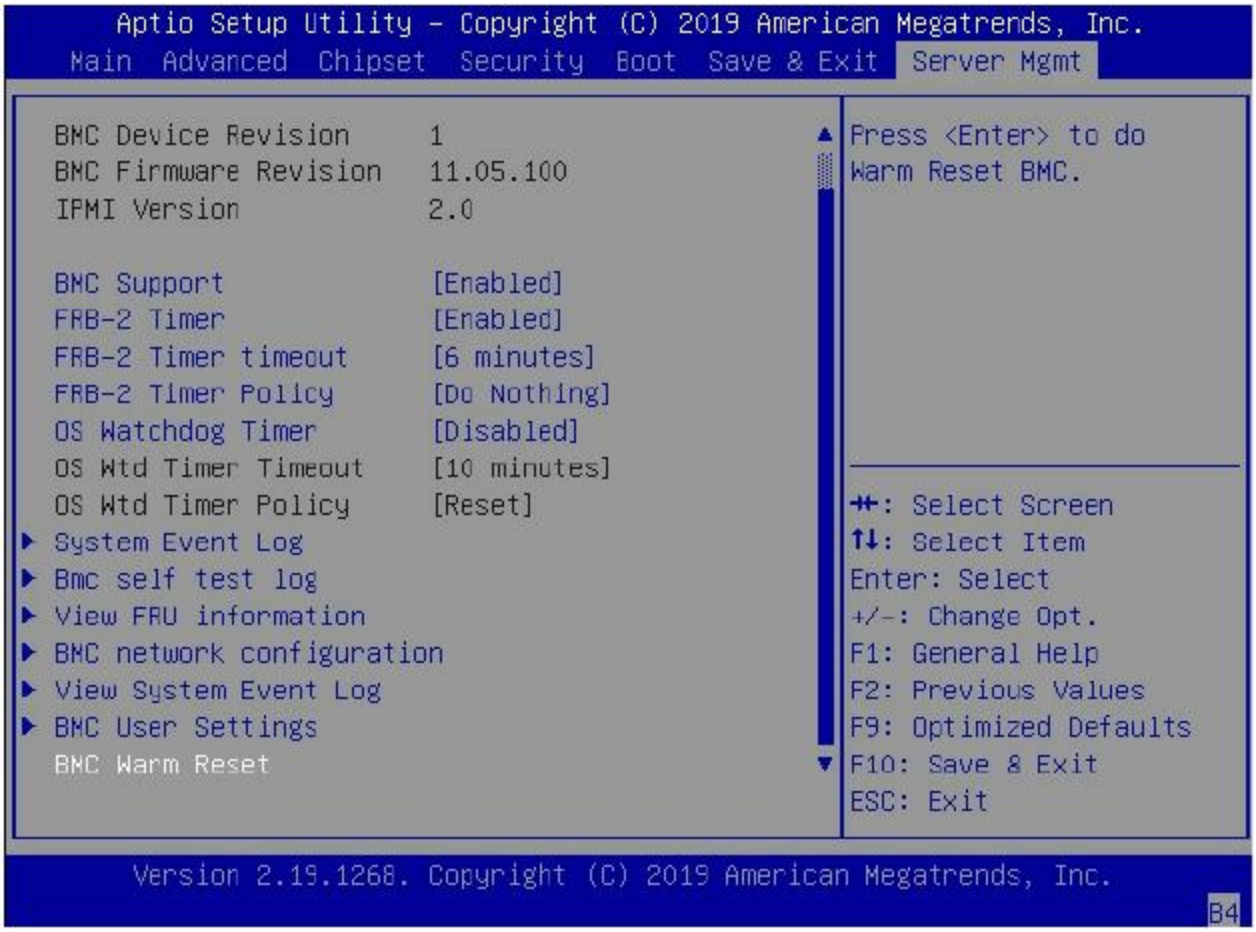
Listed in this section are all the boot options for the system. Select an option and press Enter. The system will boot to the selected boot option.

3.9 Server Management

Use the arrow keys to select Server mgmt on top of the screen. The Server mgmt screen looks like below.



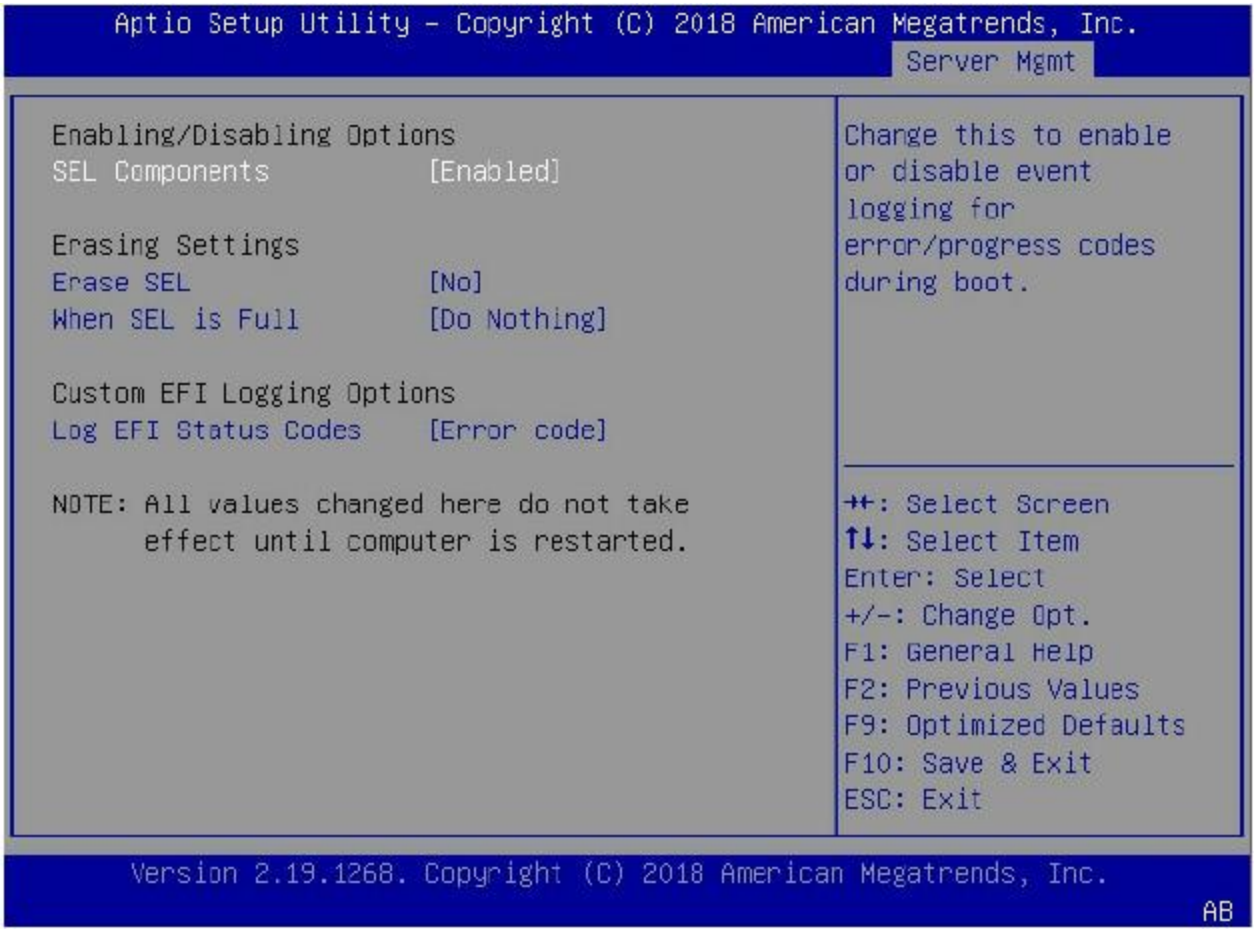
- **BMC Support:** Enable/Disable interface to communicate with BMC.
- **FRB-2 Timer:** Enable/Disable Fault Resilient Booting (FRB-2) timer (POST Timer). When Enabled, BMC ensures that the system completes BIOS POST operation.
- **FRB-2 Timer timeout:** Enter value between 3 to 6 minutes for FRB-2 Timer Expiration value. The default value is 6 minutes.
- **FRB-2 Timer Policy:** Select what to do in case the FRB-2 Timer expires. The options are: 'Do nothing', 'Reset', 'Power Down', and 'Power Cycle'.
- **System Event Log:** Press Enter to go to the System Event Log setup screen. More information is in section 3.9.1.
- **BMC self-test log:** Press Enter to go to the BMC self-test log setup screen. More information is in section 3.9.2.
- **View FRU information:** Press Enter to go to the View FRU information setup screen. More information is in section 3.9.3.
- **BMC network configuration:** Press Enter to go to the BMC network configuration setup screen. More information is in section 3.9.4.
- **OS Watchdog Timer:** If enabled, starts a BIOS timer which can only be shut off by the BMC after the OS loads. This helps to determine that the OS successfully loaded.
- **OS Wtd Timer Timeout:** Configure the length of the OS Boot Watchdog Timer. Not available if OS Boot Watchdog Timer is disabled.
- **OS Wtd Timer Policy:** Configure how the system should respond if the OS Boot Watchdog Timer expires. Not available if OS Boot Watchdog Timer is disabled. Available options: Do nothing, Reset, Power Down, and Power cycle.



- **View System Event Log:** This feature allows you to view all the System Event Log entries. It may take time to retrieve all logs.
- **BMC User Settings:** Press Enter to go to the BMC User Setting setup page. More information is in section 3, 9, and 6.
- **BMC Warm Reset:** Press Enter to perform a Warm Reset of the BMC.

NOTE: BMC Warm Reset will not make the BMC Heartbeat LED perform quick flashing.

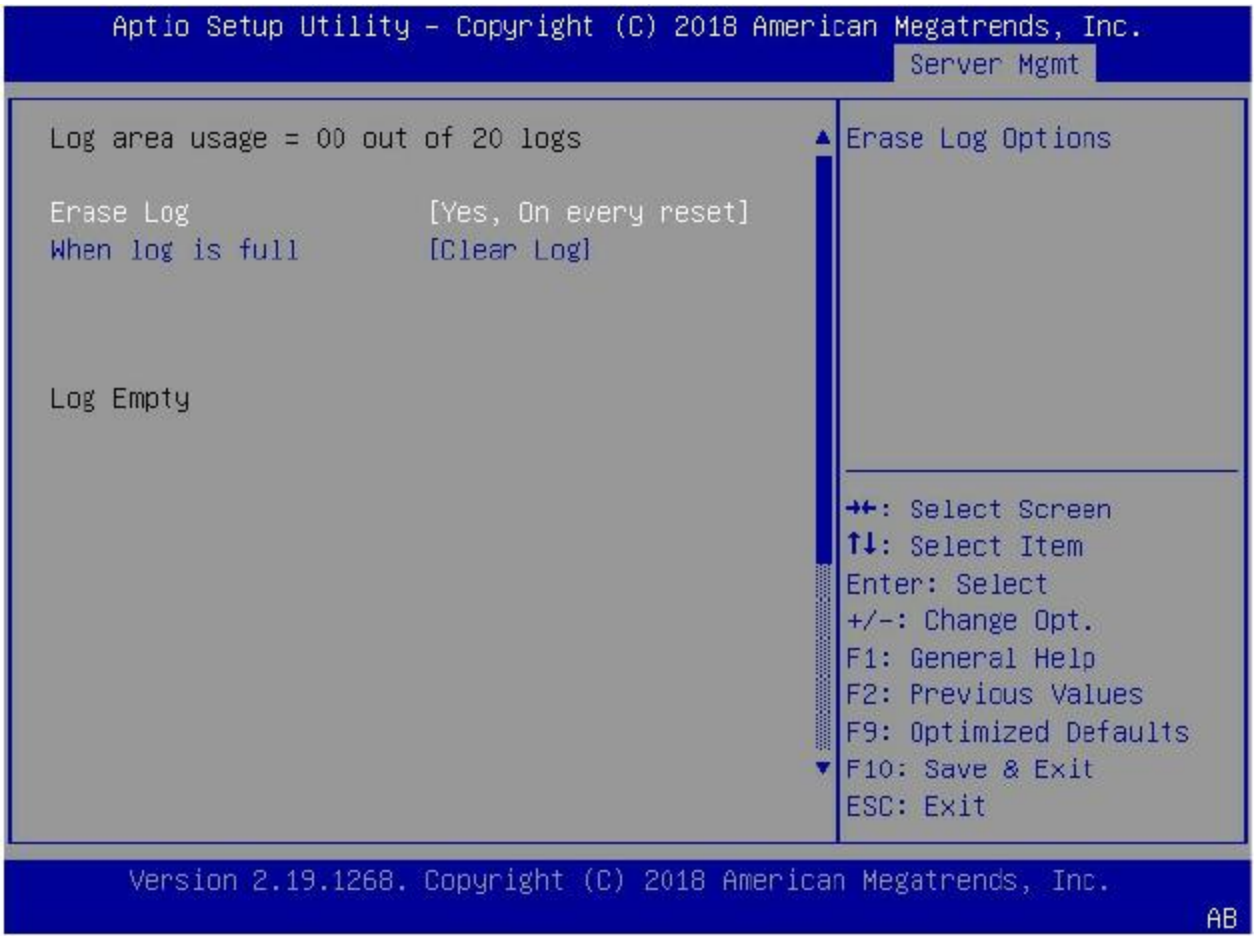
3.9.1 System Event Logs



- **SEL Components:** Change this to enable or disable event logging for error/progress codes during boot. The default value is **Eanbled**.
- **Erase SEL:** Select Yes, on next reset to erase all system event logs upon next system reboot. Select No to keep all system event logs after each system reboot. The default value is 'NO'
- **When SEL is Full:** This feature allows the user to decide what the BIOS should do when the system event log is full. Select Erase Immediately toerase all events in the log when the system event log is full. The options are 'Do Nothing' and Erase Immediately.
- **Log EFI Status Codes:** Disable the logging of EFI Status Codes or log only error code or only progress code or both. The default value is 'Error Code' only.

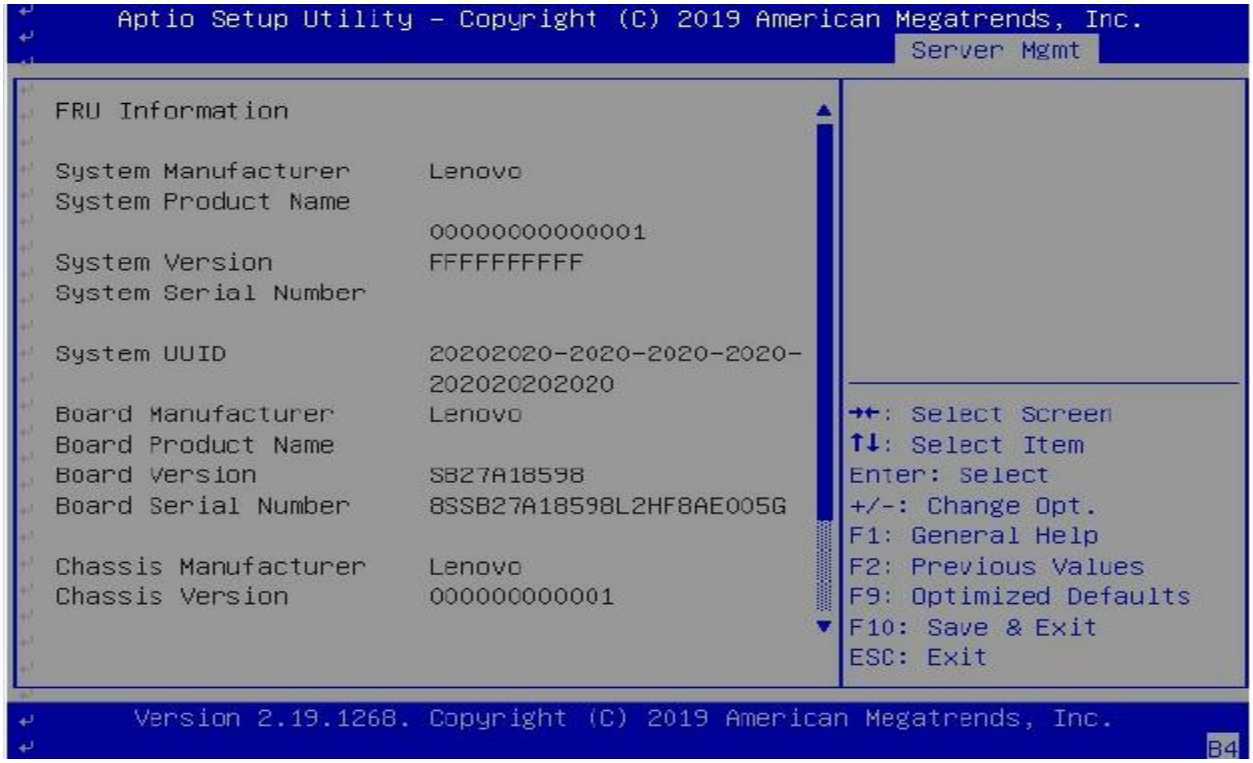
NOTE: all values changed for these options do not take effect until the server is restarted.

3.9.2 BMC self-test log



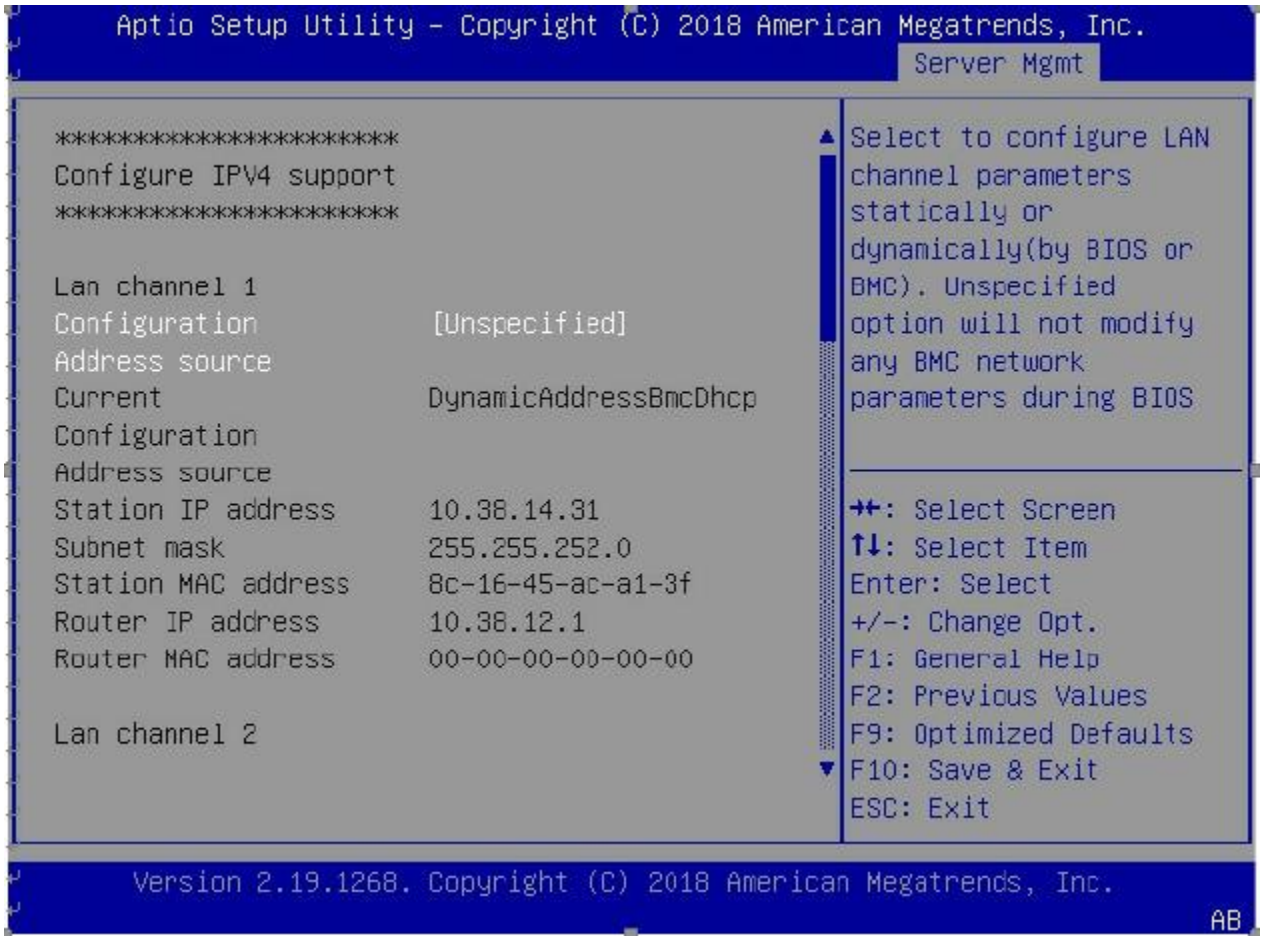
- Erase Log: The option to erase log on every reset or keep it. The default value is ‘Yes, on every reset’.
- When log is full: Select the action to be taken when log is full. The options are: ‘Clear log’, ‘Do not log any more’.

3.9.3 View FRU Information



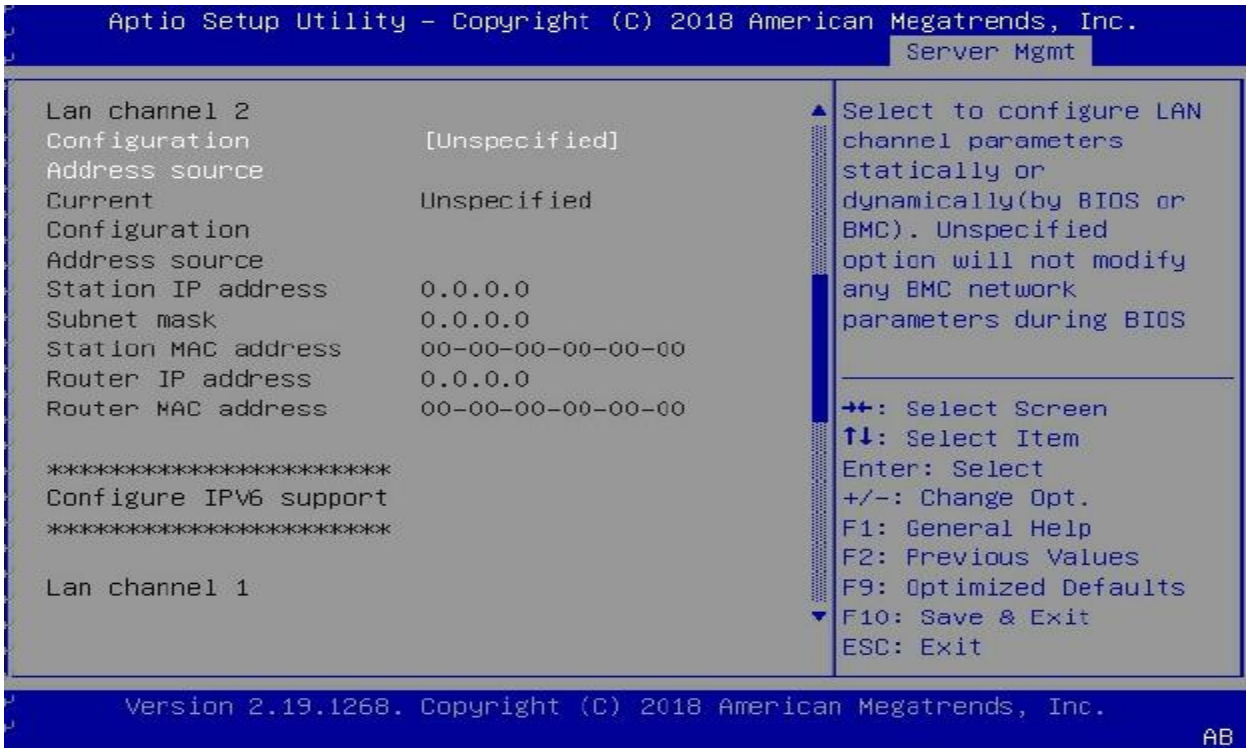
3.9.4 BMC Network Configuration

3.9.4.1 Configure IPv4 support



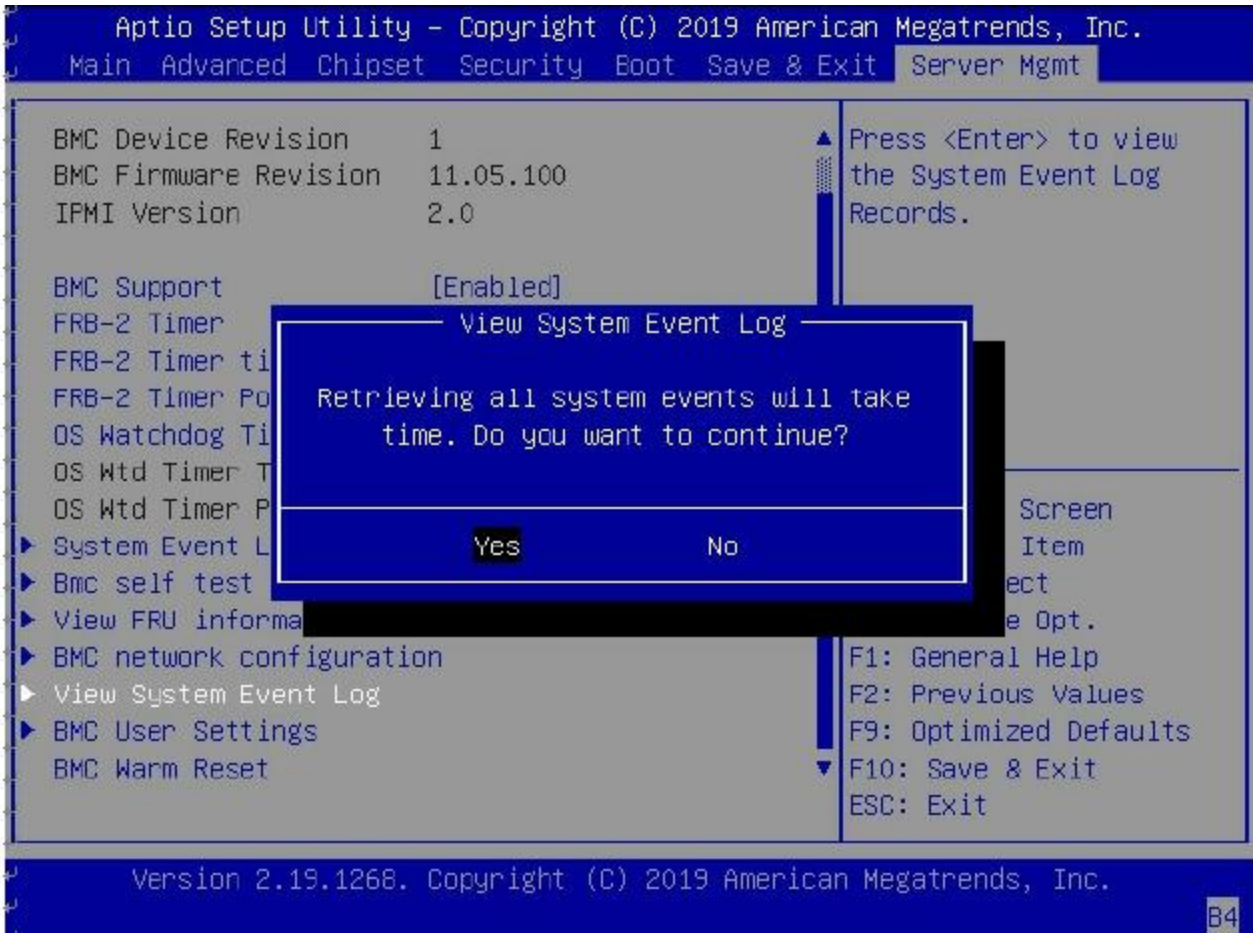
Configuration Address source: This feature allows the user to select the source of the IP address for the BMC network. If Static is selected, you will need to know the BMC IP and enter it into the system manually. If DynamicBmcDhcp is selected, the BMC IP will be requested using DHCP from the management controller. If DynamicBmcNonDhcp is selected, the BMC IP will be requested using the BMC address protocol. If unspecified, option will not modify the BMC network during BIOS booting.

3.4.9.2 Configure IPv6 support

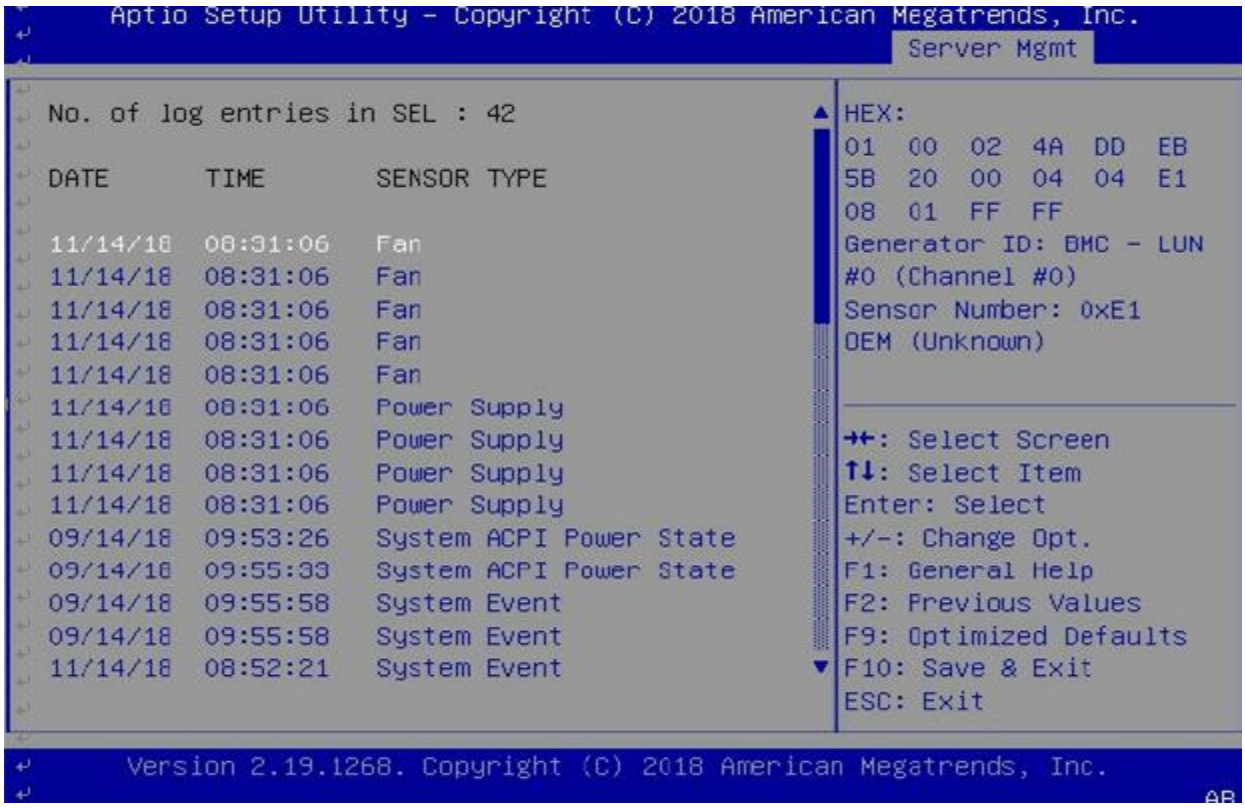


Configuration Address source: This feature allows the user to select the source of the IP address for the BMC network. If Static is selected, you will need to know the BMC IP and enter it into the system manually. If DynamicBmcDhcp is selected the BMC IP will be requested using DHCP from the management controller. If unspecified, option will not modify the BMC network during BIOS booting.

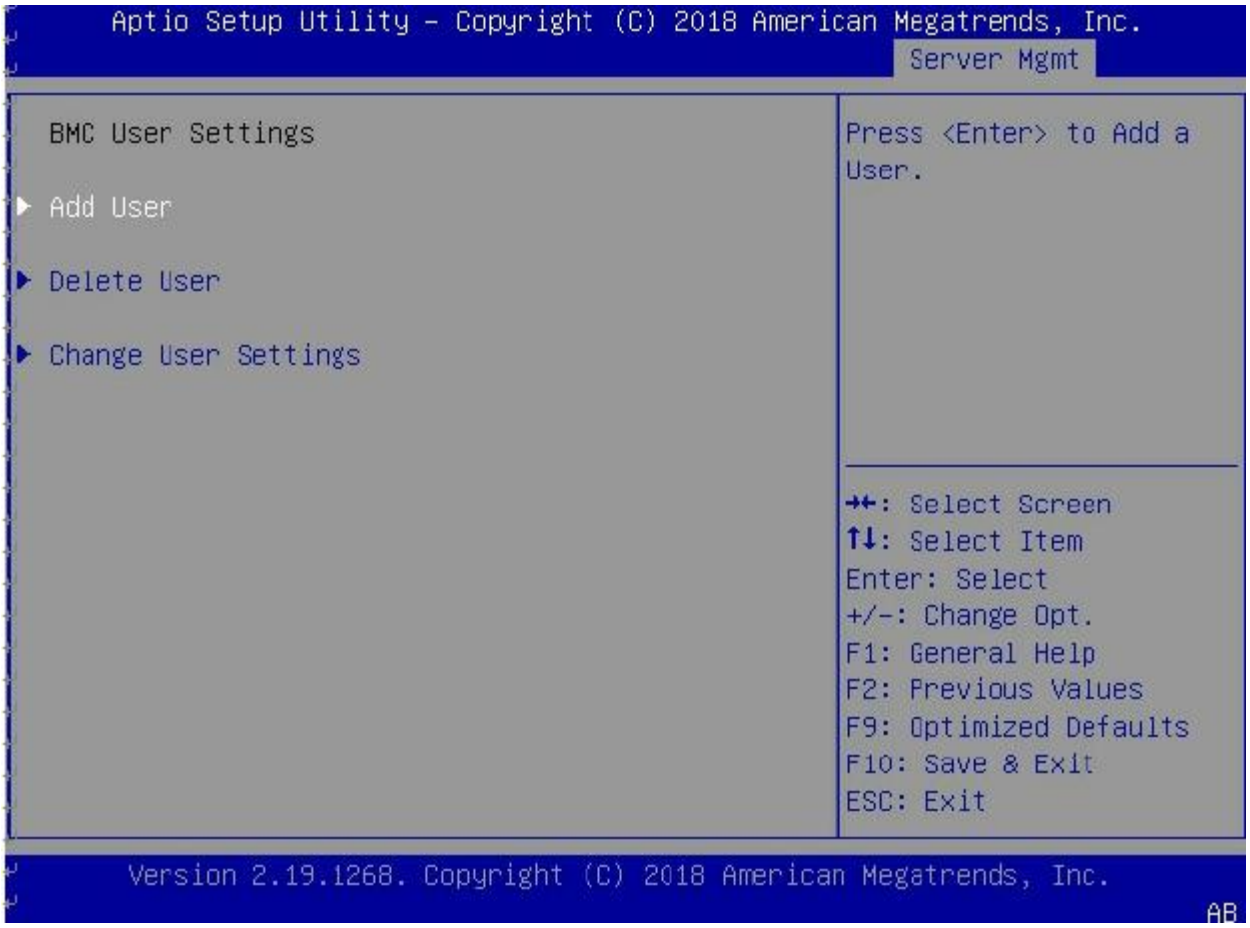
3.9.5 View System Event Log



This feature allows to view all the System Event Log. It may take time to retrieve all logs.

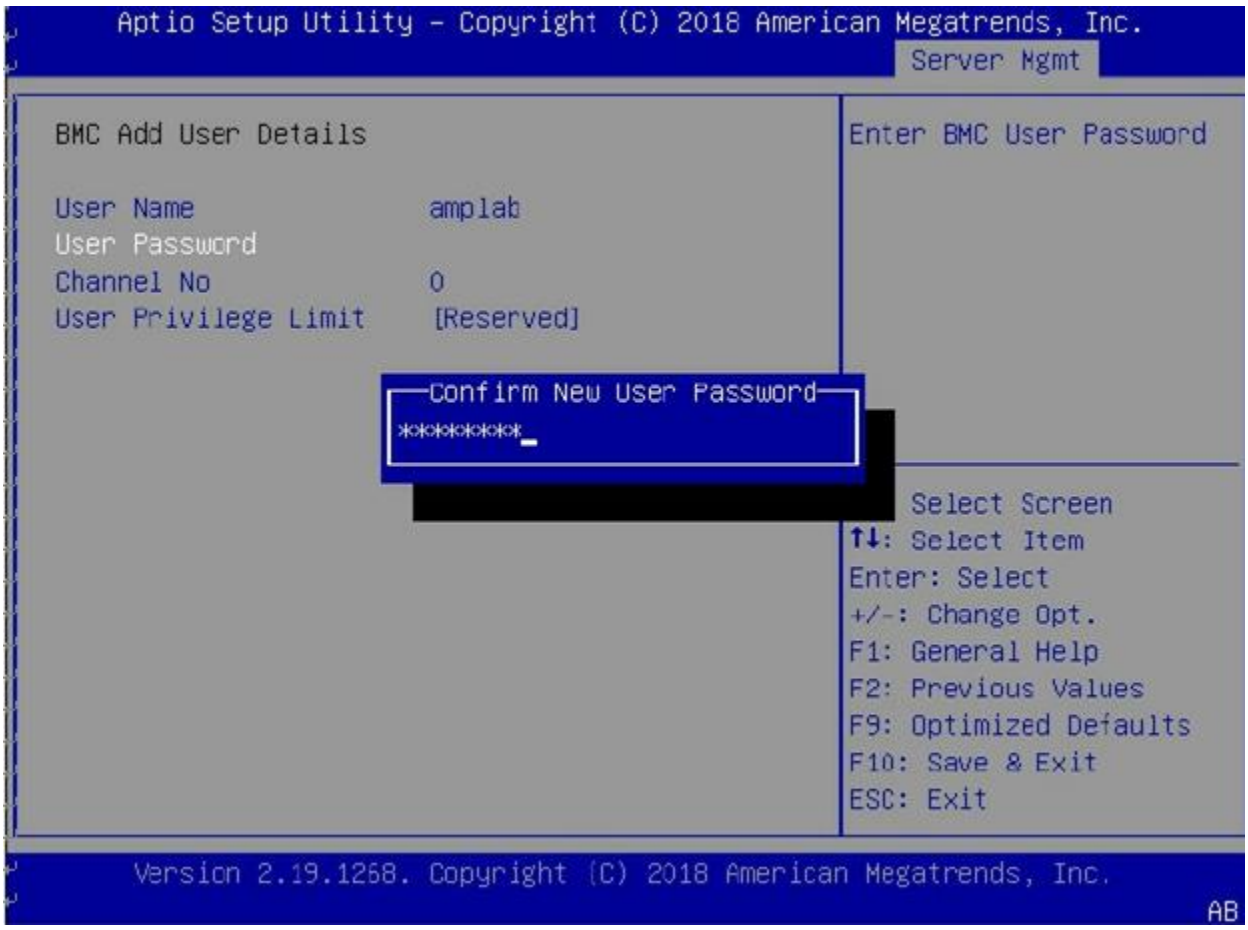

Aptio Setup Utility – Copyright (C) 2018 American Megatrends, Inc.
Server Mgmt
No. of log entries in SEL : 42
DATE TIME SENSOR TYPE
11/14/18 08:31:06 Fan
11/14/18 08:31:06 Fan
11/14/18 08:31:06 Fan
11/14/18 08:31:06 Fan
11/14/18 08:31:06 Fan
11/14/18 08:31:06 Power Supply
11/14/18 08:31:06 Power Supply
11/14/18 08:31:06 Power Supply
11/14/18 08:31:06 Power Supply
09/14/18 09:53:26 System ACPI Power State
09/14/18 09:55:33 System ACPI Power State
09/14/18 09:55:58 System Event
09/14/18 09:55:58 System Event
11/14/18 08:52:21 System Event
HEX:
01 00 02 4A DD EB
5B 20 00 04 04 E1
08 01 FF FF
Generator ID: BMC – LUN #0 (Channel #0)
Sensor Number: 0xE1
OEM (Unknown)
→←: Select Screen
↑↓: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F2: Previous Values
F9: Optimized Defaults
F10: Save & Exit
ESC: Exit
Version 2.19.1268. Copyright (C) 2018 American Megatrends, Inc.
AB

3.9.6 BMC User Settings



This section allows users to Add/Delete and Set Privilege levels for BMC users.

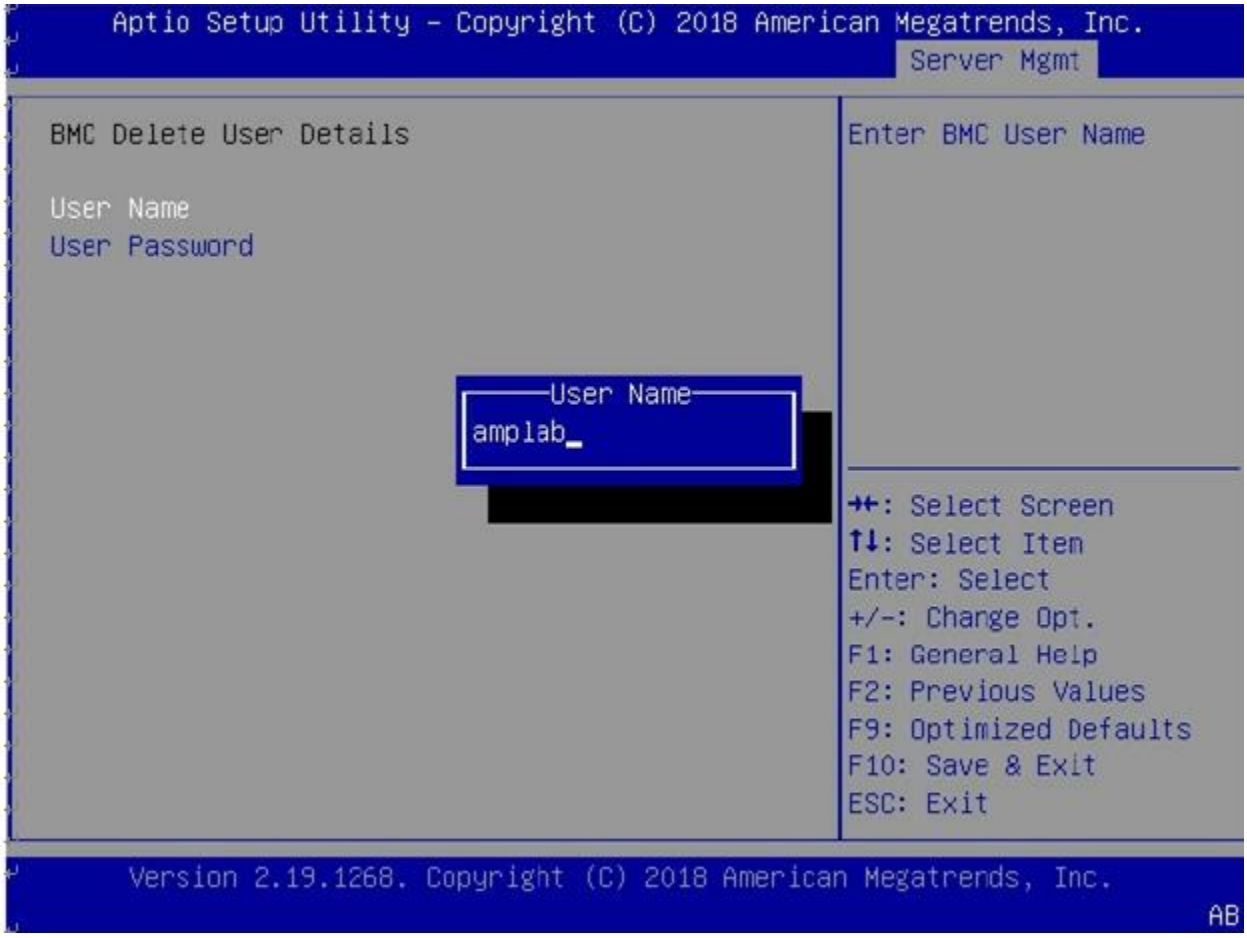
Add User



Add a user to the BMC user list. To add a user, you need to fill out the following information:

- User Name: press Enter to fill in the user name you would like to create.
- User Password: press Enter to fill in the user password (and confirm the password).
- Channel No: Set the LAN channel that the user can access the BMC on if the system has more than 1 LAN port. Otherwise, set to 0.
- User Privilege Limit: Choose the privilege level of this user for the selected channel. The options are: ‘Reserved’, ‘Callback’, ‘User’, ‘Operator’, ‘Administrator’, ‘OEM Proprietary’, and ‘No Access’.

Del User

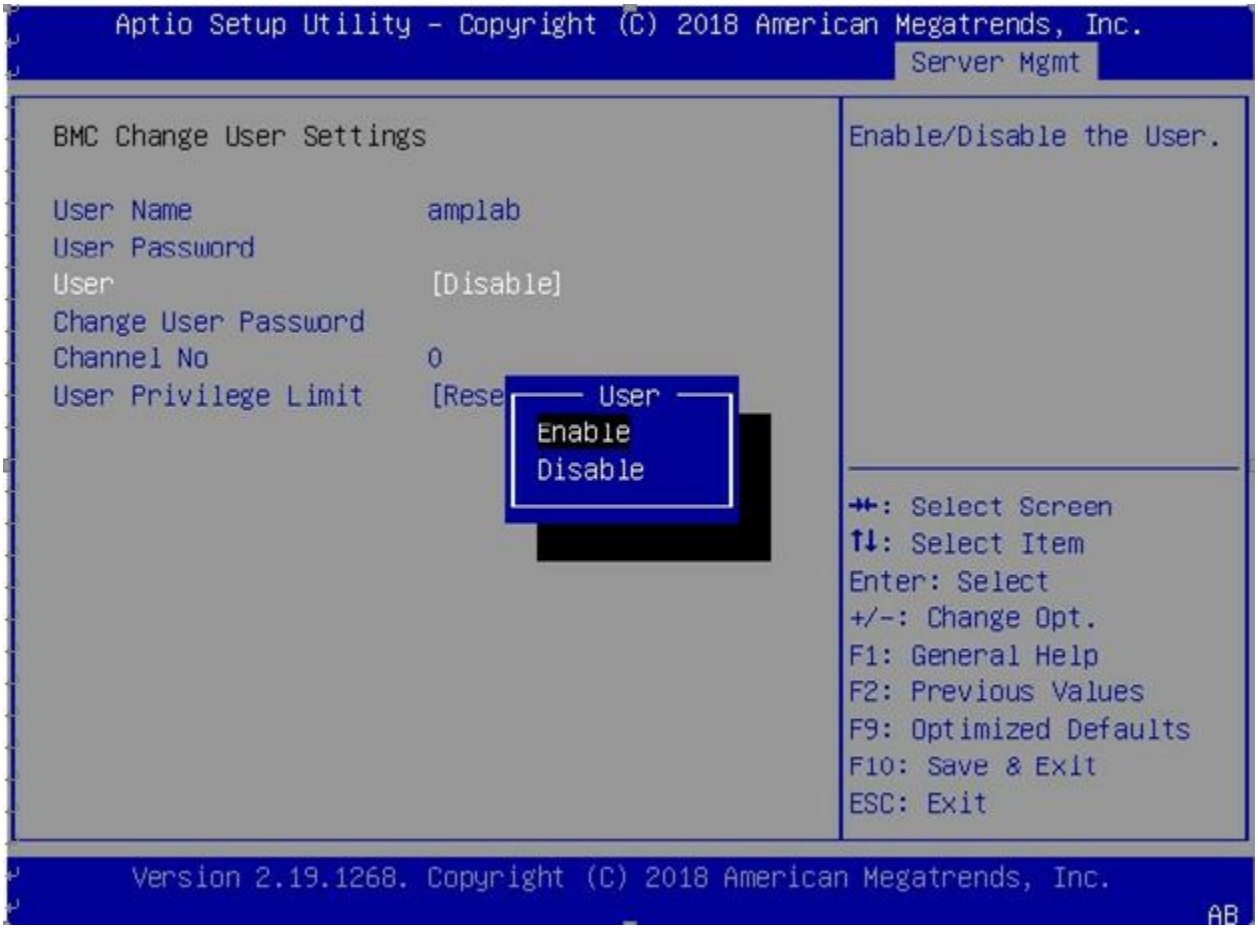


Delete a user from BMC's user list. To delete a user, you need to fill out the following information. If the information matches, the user will be deleted.

The information includes:

- User Name: press Enter to fill the user name.
- User Password: press Enter to fill the password.

Change User Settings



Change user settings. To change the settings of a user, you need to fill out the user name and password before other settings can be changed.

The settings that can be changed are:

User: Enable/disable the access for this user. If Disabled is selected, then this user doesn't have access to BMC.

- Change User Password: press Enter to set new user password.
- Channel No: type the Channel Number to change.
- User Privilege Limit: Choose the Privilege of this user for selected Channel. Note that, this option is not available for 'Channel No. 0'.The options are: 'Reserved', 'Callback', 'User', 'Operator', 'Administrator', 'OEM Proprietary', and 'No Access'.

Chapter 4. BMC Setup

4.1 Overview of the Lenovo Think System Management Module

This section describes the features of the Remote Management Module.

The Remote Management Module runs on the server system as an integrated solution and integrates the embedded operating system. Independent of the server operating system, the embedded operating system can provide a whole set of complete, stable and effective solution for the server. As a system administrator, you can respond anytime and anywhere to emergency failure and take remote control on the server through the network.

Features of the ThinkSystem Remote Management Module

The ThinkSystem Remote Management Module is easily accessible by remote KVM and controllable via LAN or Internet. It will digitize and compress the collected video signal, keyboard, mouse signals and then send to the remote console. Embedded with remote access and related control software, the module also allows integrated remote power management via IPMI. Key features of the Remote Management Module are as follows:

- Embedded Web UI - Remote power on / off, system health, system information, alert notification and event log.
- USB 2.0 media redirection - boot from remote media
- Security - open source SSL
- Compatible with IPMI V2.0
- KVM - allow remote viewing and configuring in the POST and BIOS setup utility

4.2 Configuration of the ThinkSystem Remote Management Module

When first installed, the Remote Management Module by default will search DHCP server on the network to automatically assign IP address, subnet mask and gateway. It is recommended that users manually set a fixed IP address in the BIOS.

To set an IP address, do the following:
1. Press F1 as soon as you see the logo screen.
2. From the BIOS setup menu, select Server Management → BMC Network Configuration → Configuration Address Source.
3. From the Configuration option, you can choose STATIC or DHCP to set IP address source, Subnet mask, and so on.
4. When you finish the configuration, press F10 to save the settings.

Table 1. IPMI 2.0 Configuration submenu

Configuration Address Source	STATIC	Static IP configuration. IP and the subnet mask can be set manually.
	DHCP	Dynamic IP configuration. The system can obtain IP automatically.

4.3 ThinkSystem Remote Management Module Quick Start

This topic describes how to quickly acquaint with related operations of the Remote Management Module. In addition, it also describes the advanced features of how to log on the module and options available while browsing, and how to log out.

4.3.1 Prestart

The Remote Management Module has an embedded Web server and an application with multiple standard interfaces. This topic describes these interfaces and their usages. You can use the TCP/IP protocol to access these interfaces.

Note: As the supported functions of the product vary with configurations, refer to the actual product description.

For more information about the initial settings, see Chapter 3 “Configuration of the ThinkSystem Remote Management Module” on page XXX. The user name in this topic is “lenovo”. Besides “lenovo”, other user names and passwords are also accepted. The default user name and password are as follows:

• Username =ADMIN
• Password = ADMIN

The Remote Management Module is accessible through the standard HTML5 Web browser with HTTP and HTTPS.

HTTP / HTTPS: The embedded Web server provides full access permission. You can access the Remote Management Module via encrypted HTTPS protocol or HTTP protocol. When accessing through the HTTP protocol, note the following:
1. With access to ThinkSystem Remote Management Module via the HTTPS protocol, the browser may prompt you to trust and install the security digital certification, and you just follow the prompts to import and confirm the certification.
2. In IE11 on the Microsoft® Windows Server® 2008 operating system, if using HTTPS protocol to access the Remote Management Module, you need to do the following amendments to the Configure IE ESC item of the security information of the server manager, as shown in the following figures

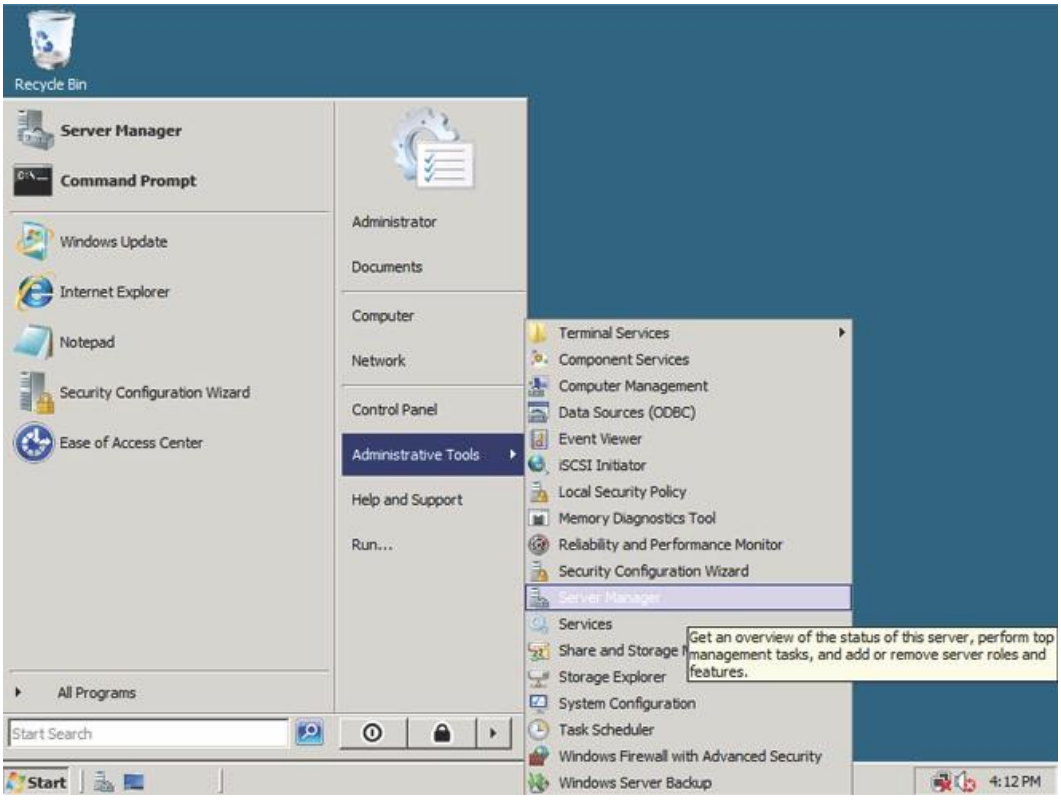


Figure 1. Configuring IE ESC - step

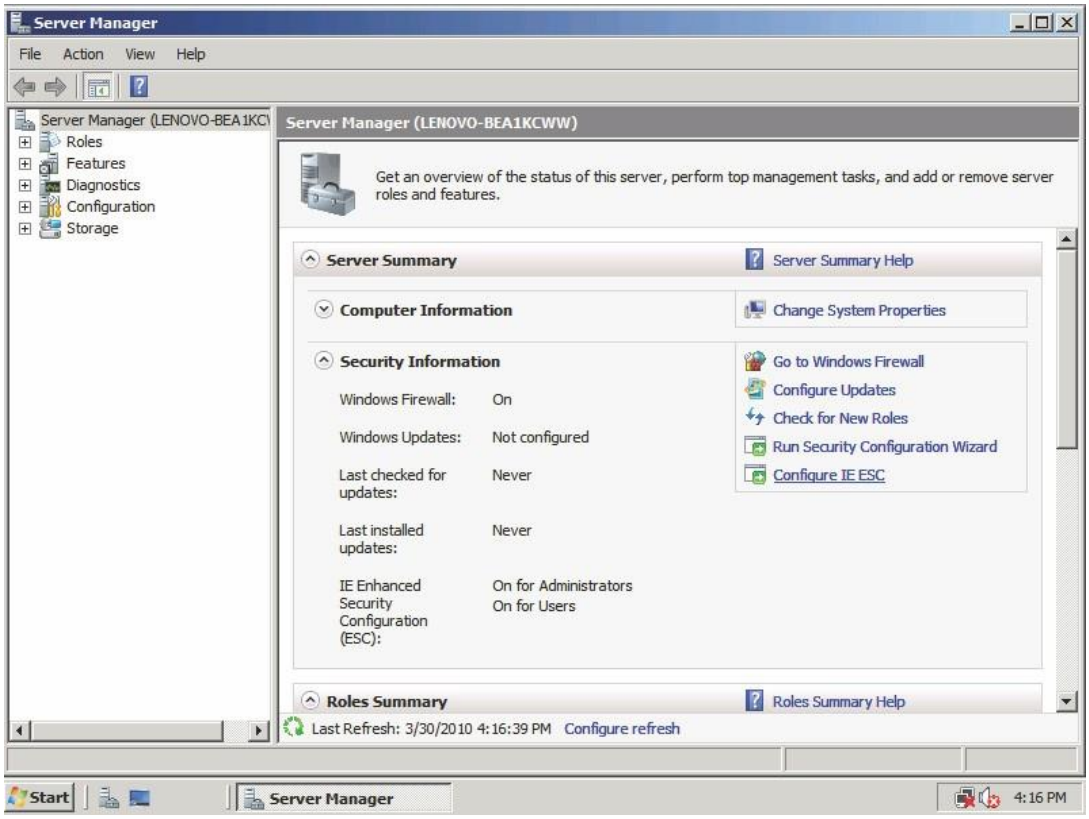


Figure 2. Configuring IE ESC - step 2

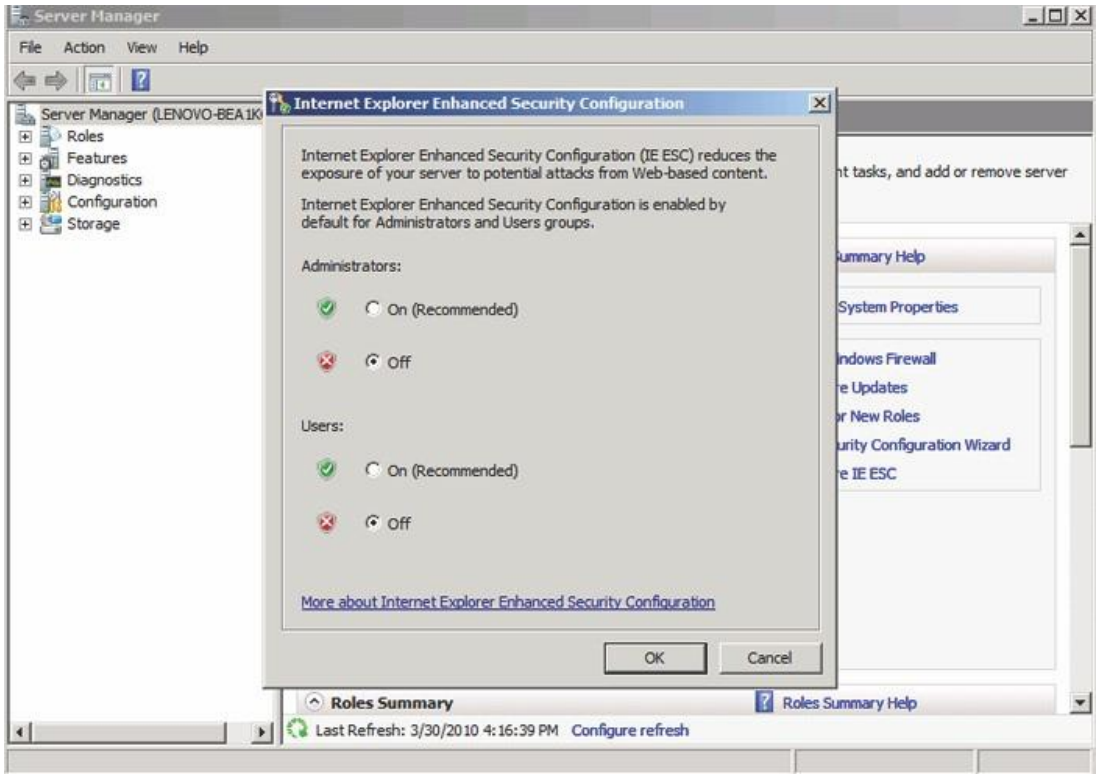
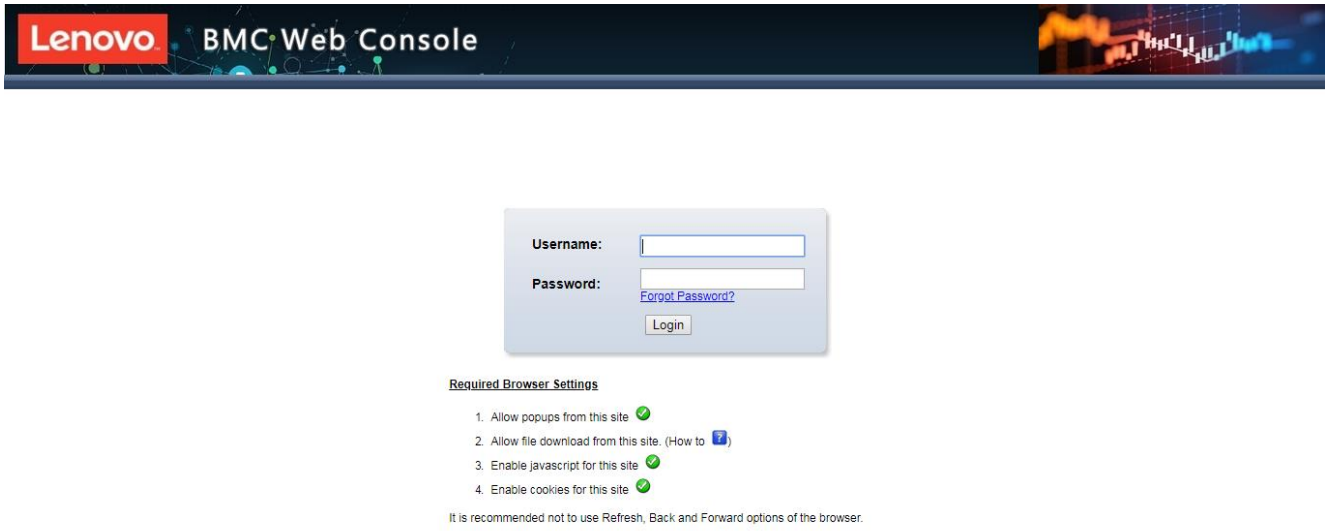


Figure 3. Configuring IE ESC - step 3

For making the remote console (KVM) window of the managed server works, you must install Java runtime environment (JRE) V6.0 Update 24 or later.

4.3.2 Log-on

To log on to the ThinkSystem Remote Management Module, do the following:
1. Enter the IP address assigned by the ThinkSystem Remote Management Module into the Web browser.
For example:
http://10.223.131.36/
For secure connection, refer to the following example:
https://10.223.131.36/
The Web browser will then be directed to the logon page of the Remote Management Module.



2. On the logon page of the Remote Management Module, enter the user name and password. For example:

• Username = ADMIN
• Password = ADMIN
3. Click OK to view the home page of the Remote Management Module.

After a successful initial logon, the system administrator can create new users and has full permission of Remote Management Module.

4.3.3 Navigation

When the ThinkSystem Remote Management Module is successfully logged on, the ThinkSystem Remote Management Module home page is displayed.

There are several tabs on the vertical toolbar which is on the left pane of the ThinkSystem Remote Management Module home page. By clicking these tabs, you can get the specific system information and take the relevant tasks listed in the following table:

Table 2. Tabs on the ThinkSystem Remote Management Module home page

Tab	**Comments**
Dashboard	Displays the overall information about the device status.
System Inventory	This tab contains the following submenus: • CPU • DIMM
FRU Information	Display FRU information include MB FRU, front BP FRU and rear BP FRU.
Server Health	This tab contains the following submenus: • Sensor Readings • IPMI Event Log • System Log • Audit Log • BSOD Screen
Configuration	This tab contains the following submenus: • Active Directory • DNS • Mouse Mode • Event Log • LDAP/E-Directory • Images Redirection • Network • Network Link • NTP • PAM Order • Platform Event Filter • RADIUS • Services • Remote Session • SMTP Settings • SSL • System and Audit Log • System Firewall • User • Virtual Media • IPMI Configuration
Remote Control	This tab contains the following submenus: • Console Redirection • Server Power Control • JAVASOL
Auto Video Recording	The Auto Video Recording consists of the following. • Video Recording Configuration • Recorded Video

Firmware Update	This group of pages allows you to do the following. The menu contains the following items: • Firmware Update • Protocol Configuration • Dual Image Configuration
Maintenance	Maintenance BMC configuration and firmware. • Preserve Configuration • Restore Configuration • System Administrator • Backup and Restore Configuration
Sign out	Terminate the current Web Console session. Note: If the remote console (KVM) window is active, it will close automatically when you are logging out. After logout, the Web console will back to logon screen.

There also are tabs on the top of the home page:

Table 3. Tabs on the top of the ThinkSystem Remote Management Module home page

Tab	**Comments**
Message	Display the messages received
Notification	Display the notification received
Sync	On/Off to Sync with latest sensor and eventlog updates
Refresh	Reloads the current page
Username	Display the current log-in user name

4.3.4 Log-out

To log out the ThinkSystem Remote Management Module and turn back to the log on page, click “Sign out” on the left down of the toolbar.

Note: Automatic Timeout: If the Web console detects no user activity within five minutes, the current session will be automatically terminated. If the user has opened the KVM remote console window, then the Web session will not automatically timeout. When the automatic timeout happens, the system will inform the user to log on again if the user wants to access the Web console to take operations.

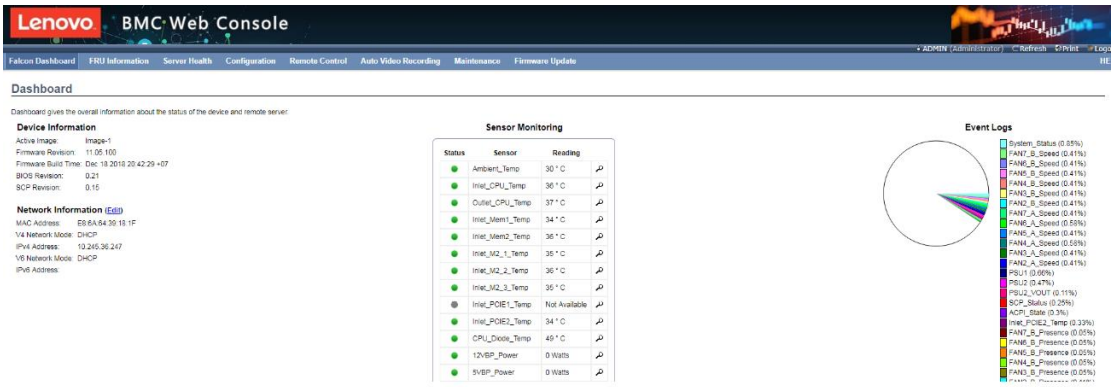
4.4 ThinkSystem Remote Management Module Web Console Options

This topic describes every page of the Web console and each page is divided into several parts corresponding separately to the several tabs at the left side of the panel. In each part, there are detailed illustrations and introductions for each menu option.

4.4.1 Dashboard

By default, the home page of the ThinkSystem Remote Management Module shows the Dashboard page, including general information about the server. Dashboard displays the overall information about the device status. Launch the remote console redirection window from this page. To launch it, you must have Administrator privilege or KVM privilege.

Figure dashboard information



4.4.2 Dashboard Information

The dashboard Information page shows the summary of the general information as table 4.

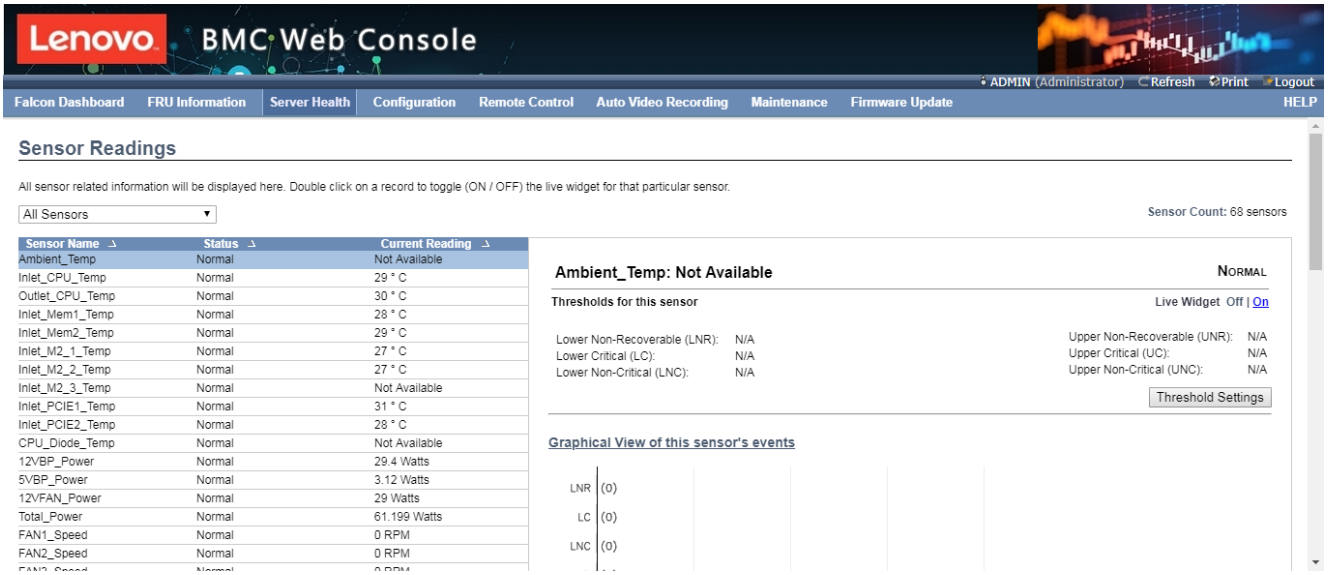
Table 4. Dashboard information page

Dashboard	
Category	Description
Product Information List	Display product information.
Remote Console Control	To redirect the host remotely, click the Launch button.
Sensor Monitor Auto Refresh	To set refresh frequency
System Status List	Display system status
System Inventory List	Display system inventory

4.5 Sensor

4.5.1 Sensor Reading

A list of sensor readings will be displayed here.



Click on a record to show more information about that particular sensor, including thresholds and a graphical representation of all associated events.

4.6 System Inventory

4.6.1 CPU

This page gives detailed information for the CPU present in this system.

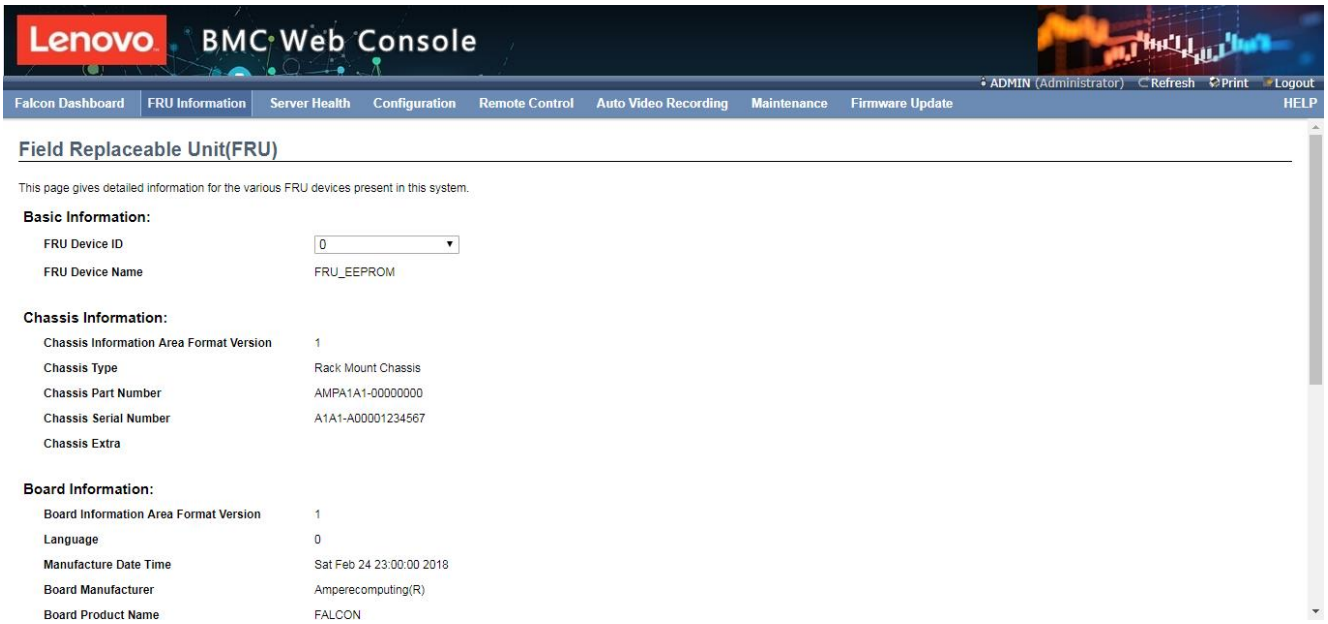
4.6.2 DIMM

This page gives detailed information for the DIMM present in this system.

4.7 FRU Information

4.7.1 Field Replaceable Unit (FRU) Information

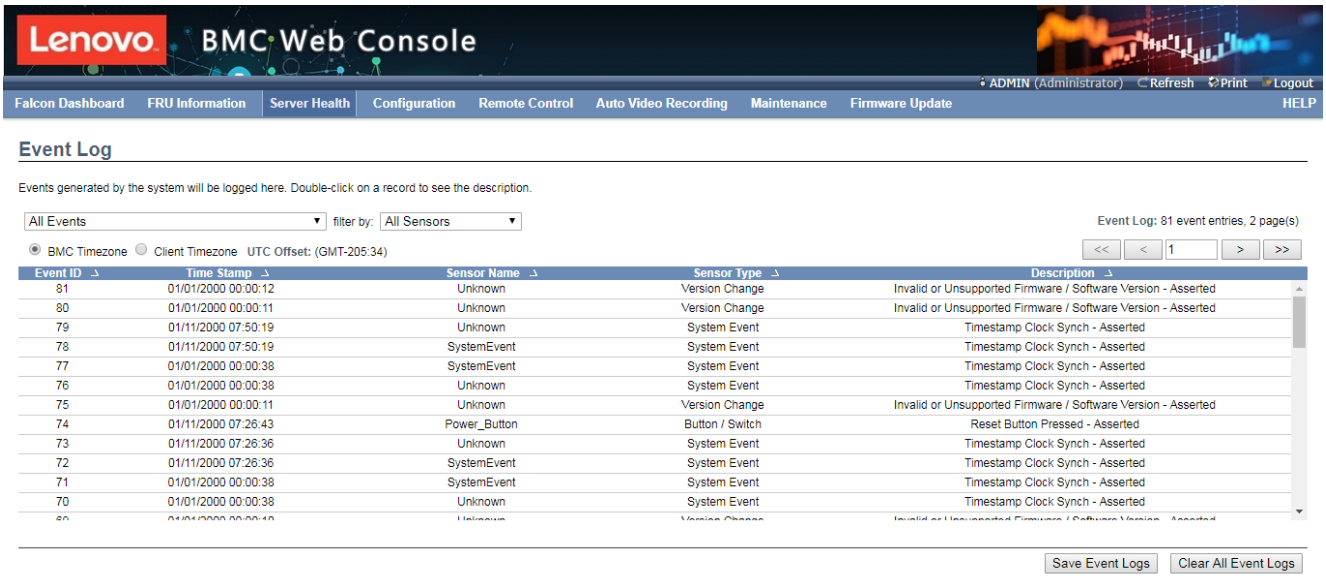
This page displays the BMC FRU file information. On selecting any particular FRU Device ID its corresponding FRU information will be displayed.
It displays the FRU device name for the selected FRU device ID. This page displays the Chassis, Board, and Product details (if available) for the items shown in each field.



4.8 Logs & Reports

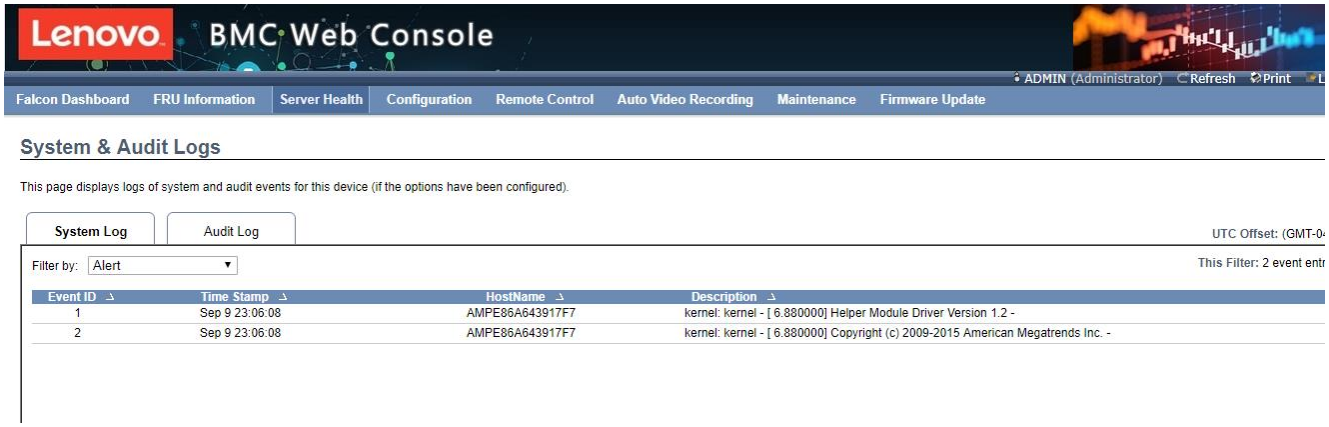
4.8.1 IPMI Event Log

This page displays the list of events incurred by different sensors on this device. Click on a record to see the details of that entry. Also use the sensor type or sensor name filter options to view those specific events logged in the device.



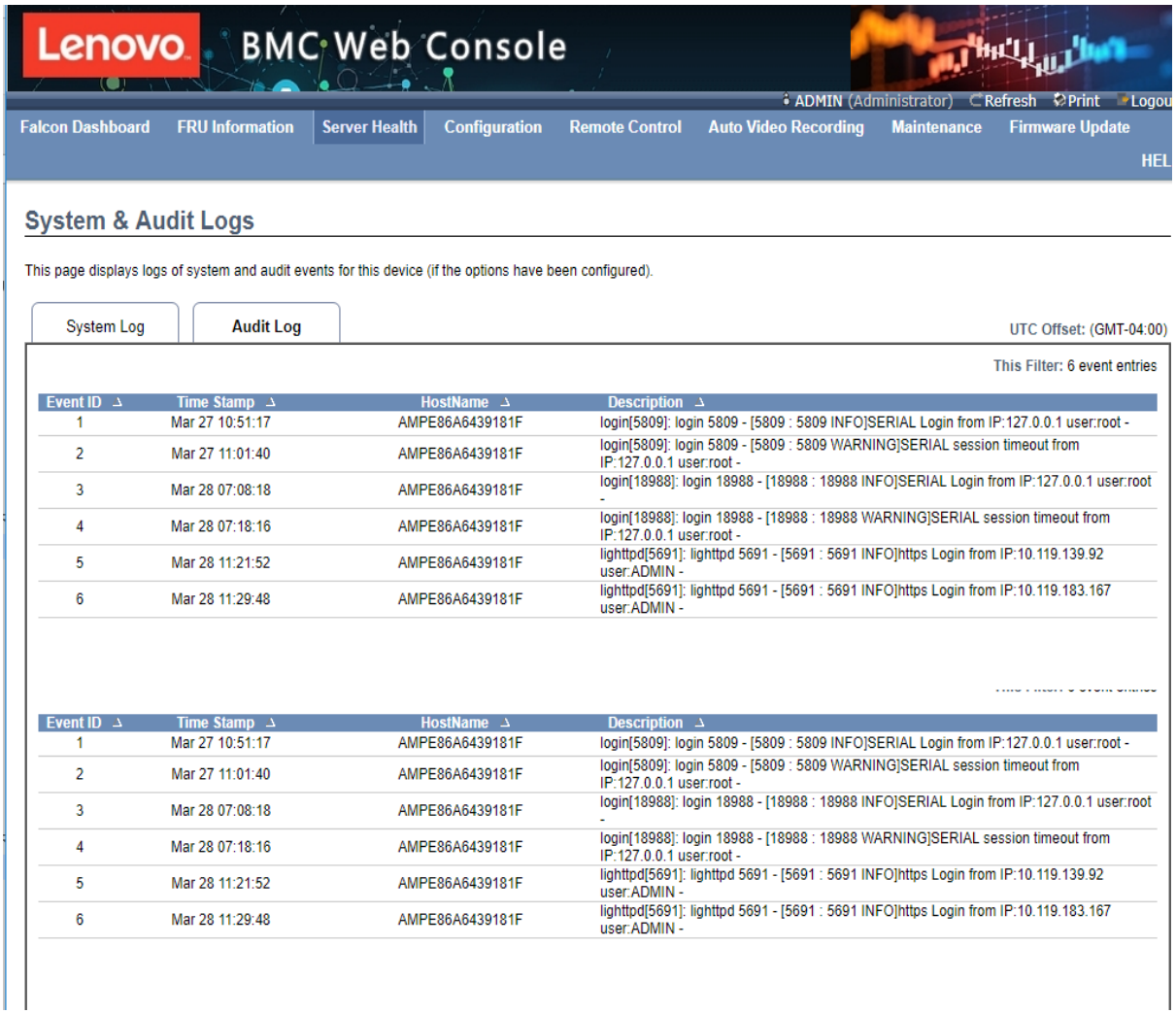
4.8.2 System Log

This page displays logs of system events for this device.



4.8.3 Audit Log

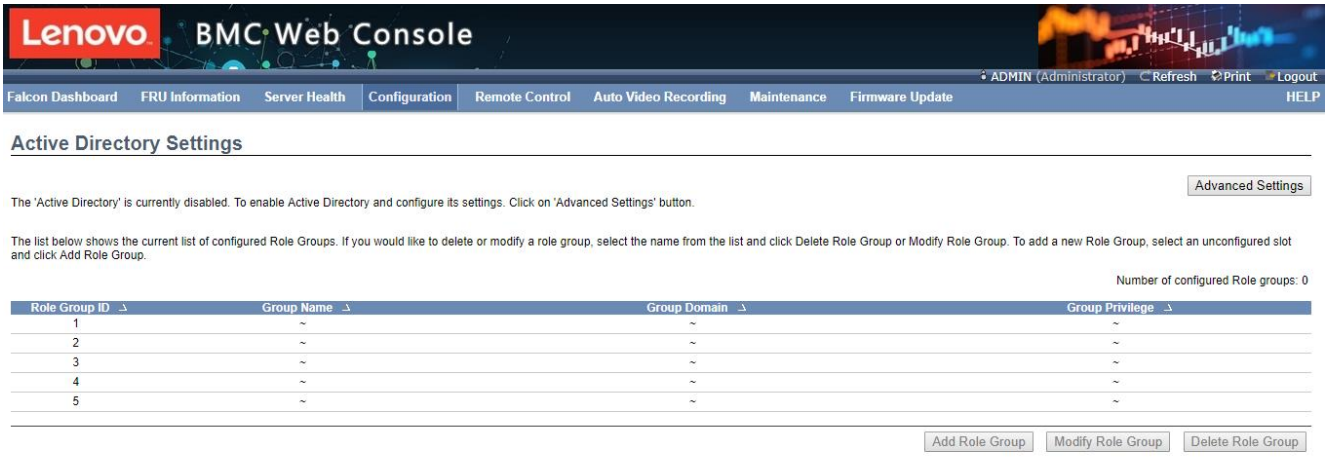
This page displays logs of audit events for this device.



4.9 Configuration

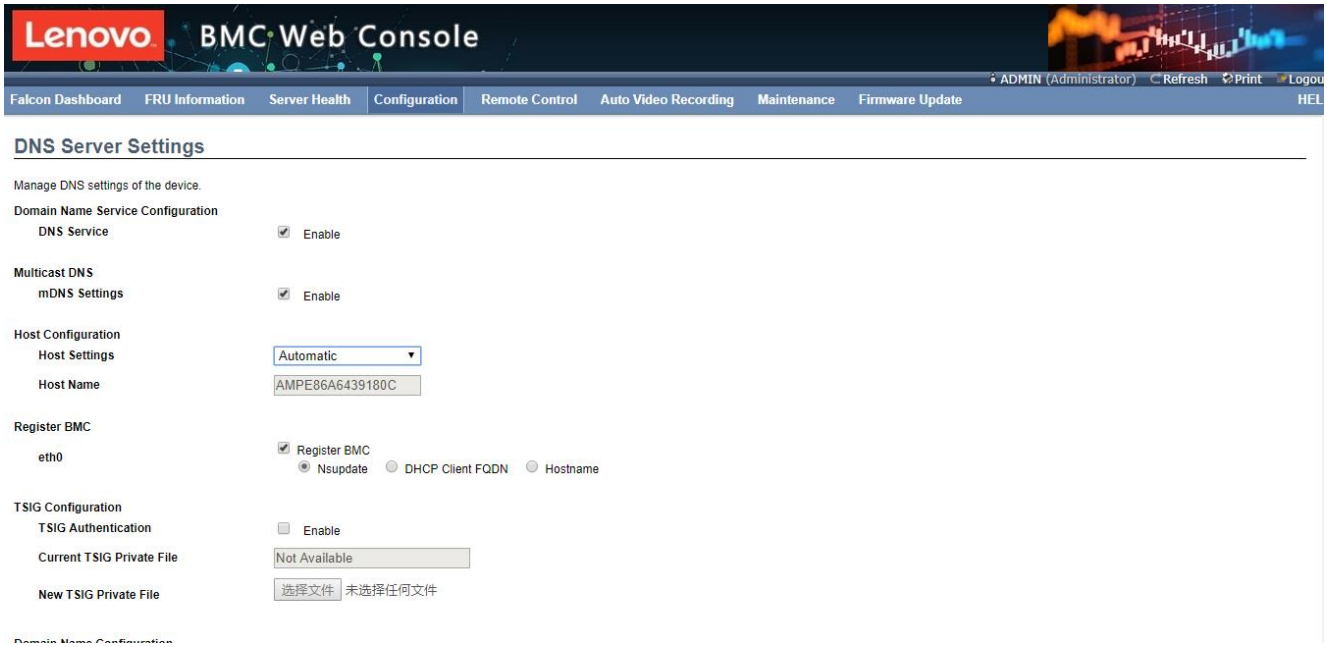
4.9.1 Active Directory

An active directory is a directory structure used on Microsoft Windows based computers and servers to store information and data about networks and domains.



4.9.2 DNS

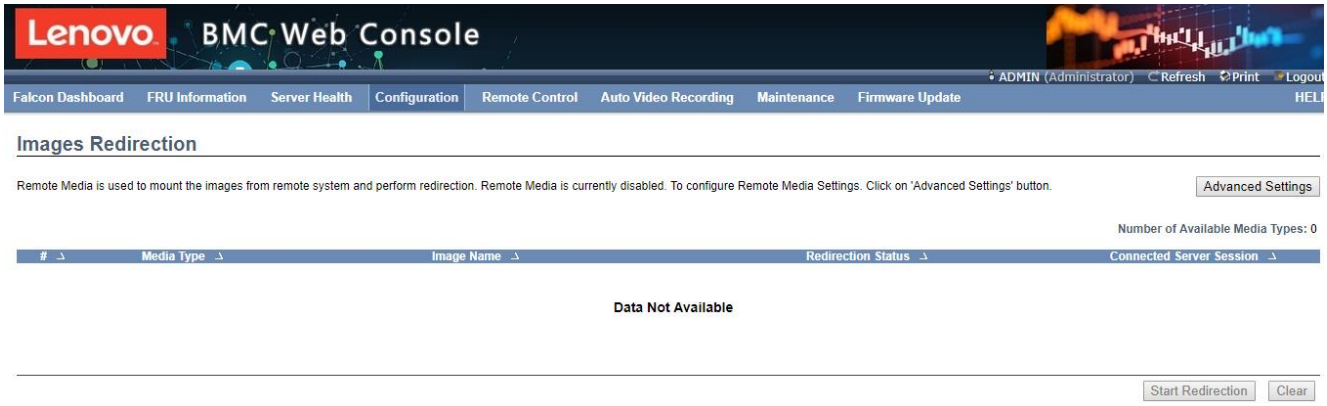
The Domain Name System (DNS) is a distributed hierarchical naming system for computers, services, or any resource connected to the Internet or a private network.



4.9.3 Event Log

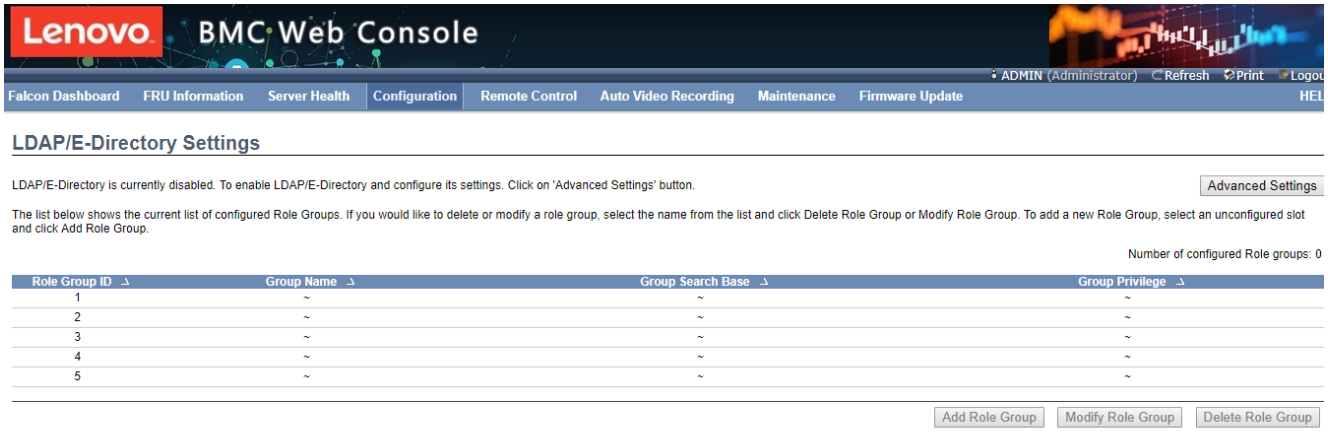
4.9.4 Images Redirection

This page is used to configure the images into BMC for redirection.



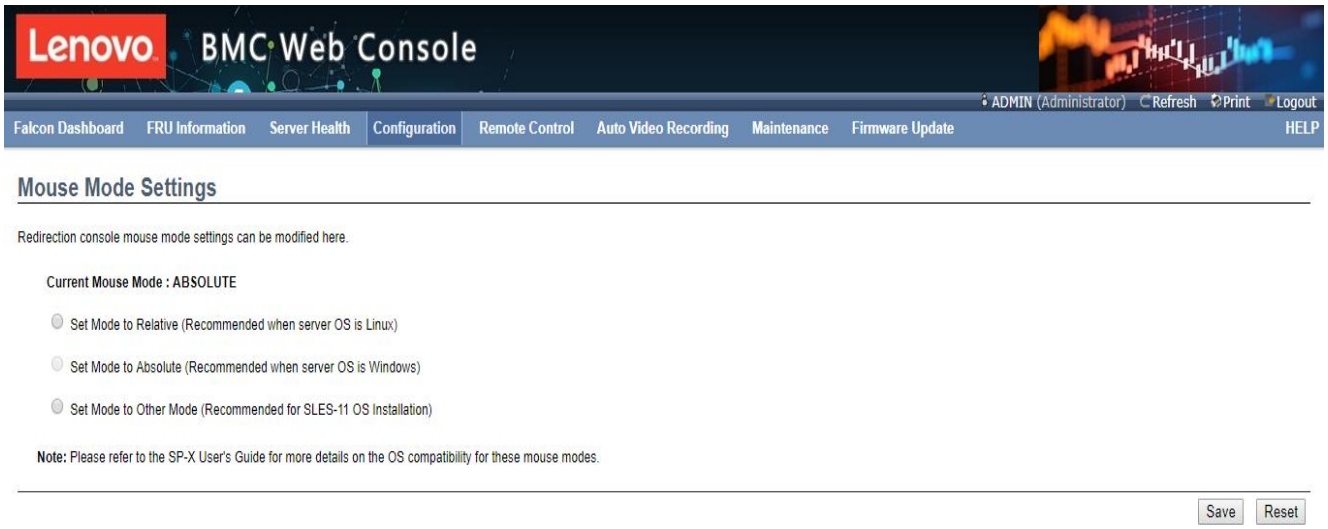
4.9.5 LDAP/E-Directory Settings

The Lightweight Directory Access Protocol (LDAP)/E-Directory Settings is an application protocol for querying and modifying data of directory services implemented in Internet Protocol (IP) networks.



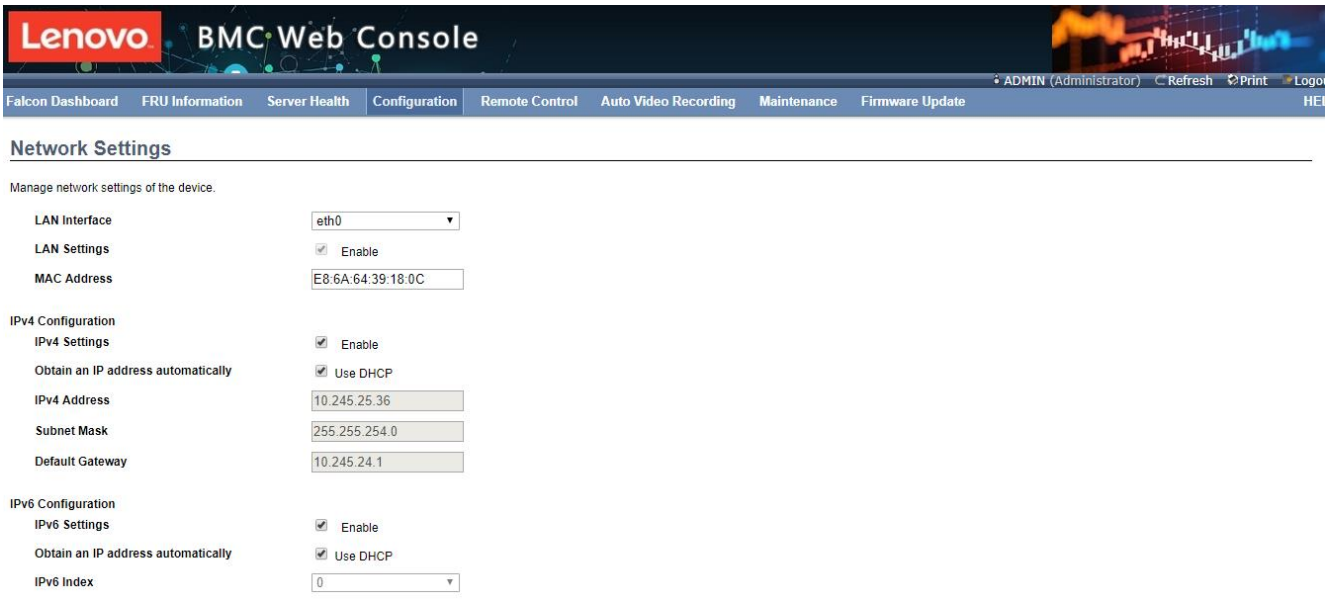
4.9.6 Mouse Mode

This page is used to configure the media into BMC for redirection.



4.9.7 Network

This page is used to configure the network settings for the available LAN channels.

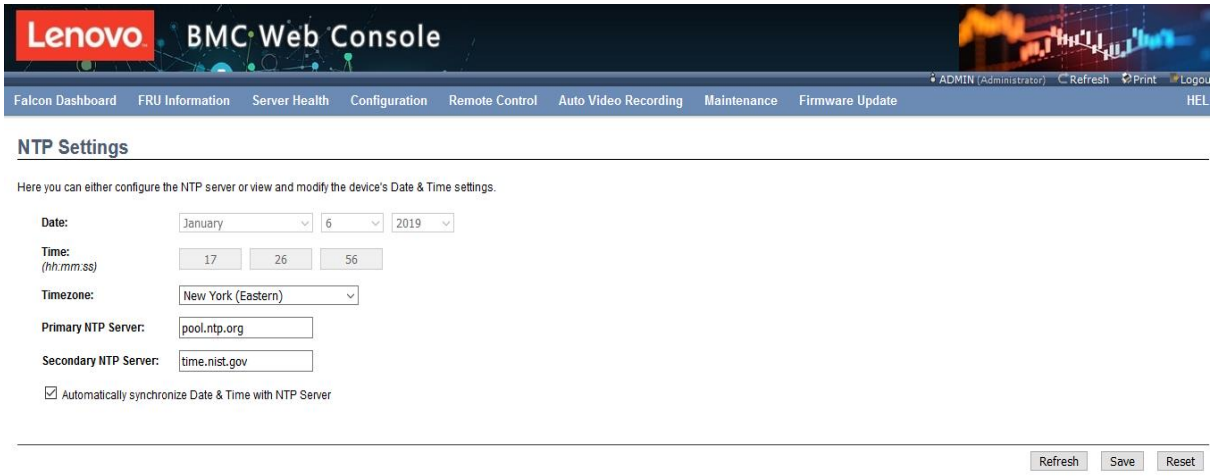


4.9.8 Network Link

This field is used to configure the video recording function of the KVM server and SOL setting.

4.9.9 NTP

The Network Time Protocol (NTP) is a protocol for synchronizing the clocks of computer systems over packet-switched, variable-latency data networks. It is designed particularly to resist the effects of variable latency by using a jitter buffer.

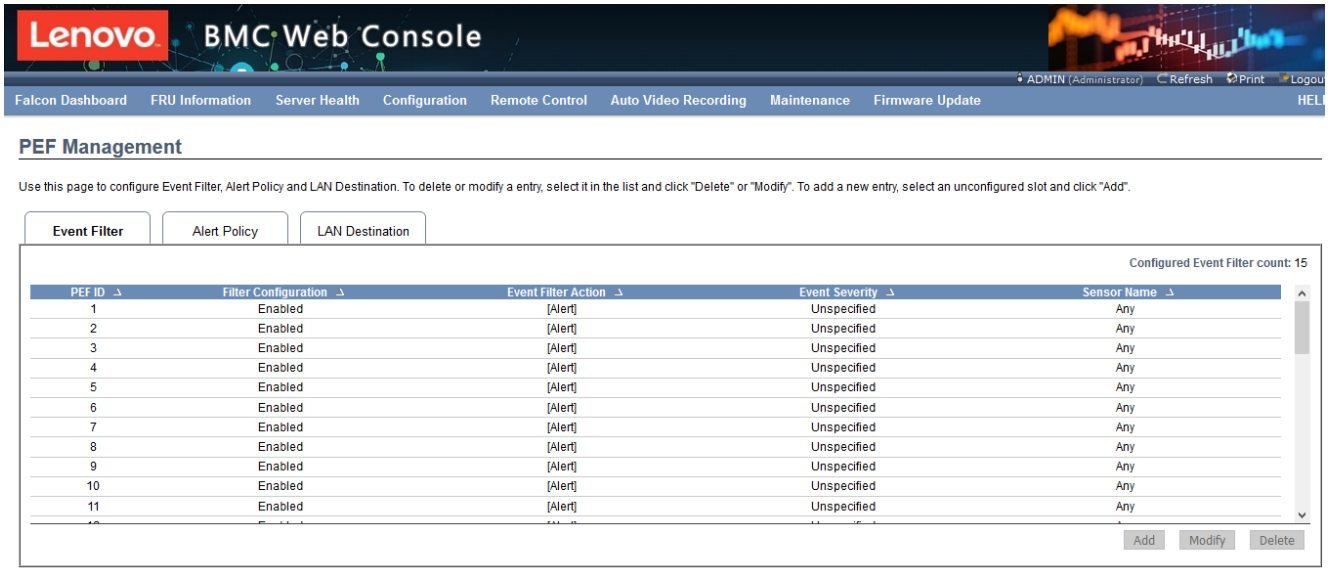


4.9.10 PAM Order Settings

This page is used to configure the PAM order for user authentication into the BMC.

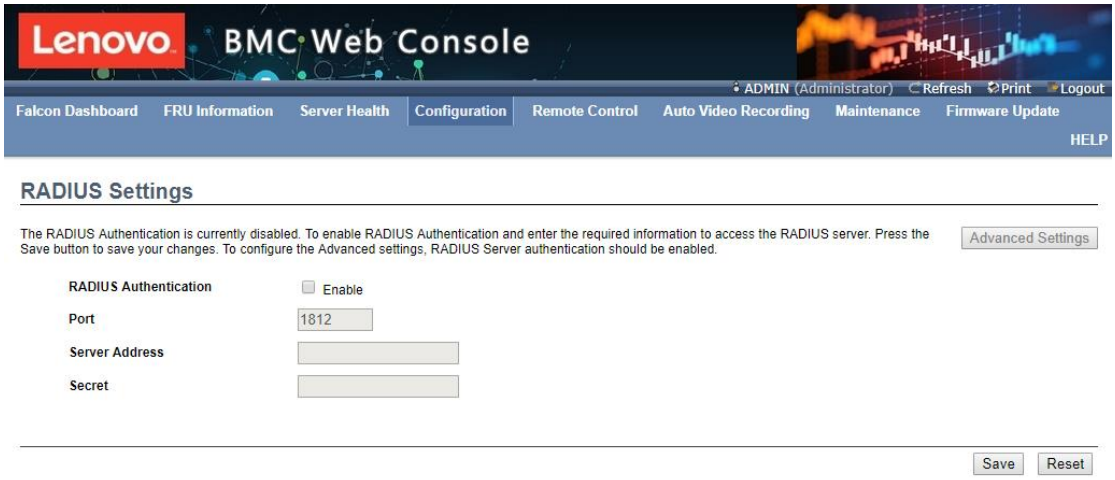
4.9.11 Platform Event Filter

This platform event filter provides a mechanism for configuring the BMC to take selected actions on event messages that it receives or has internally generated.



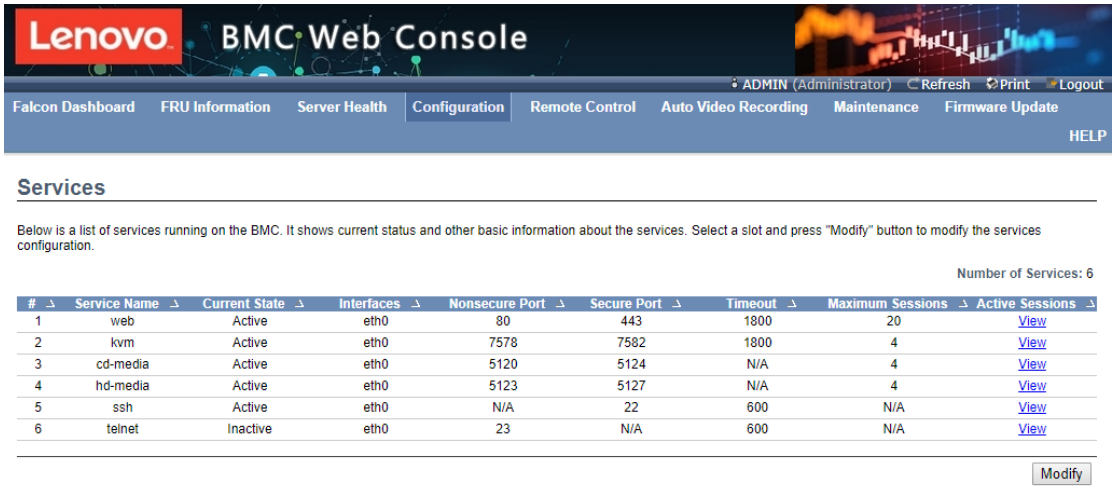
4.9.12 RADIUS

Radius is a modular, high performance and feature-rich RADIUS suite including server, clients, development libraries and numerous additional Radius related utilities.



4.9.13 Services

This page list all services running on the BMC, click icon on the right side of service to view and modify the service configuration.

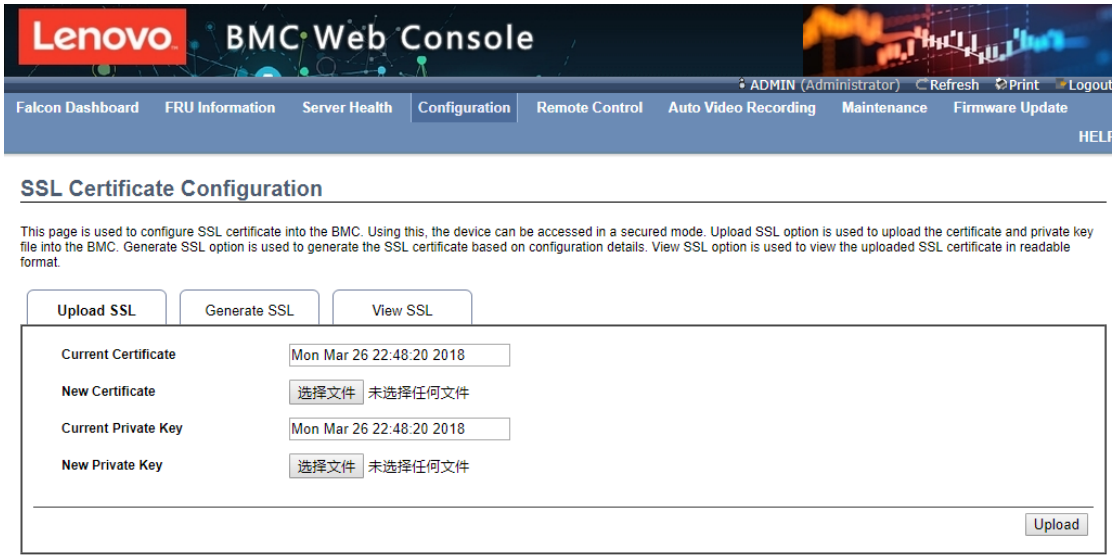


4.9.14 SMTP Settings

This page is used to configure the SMTP settings.

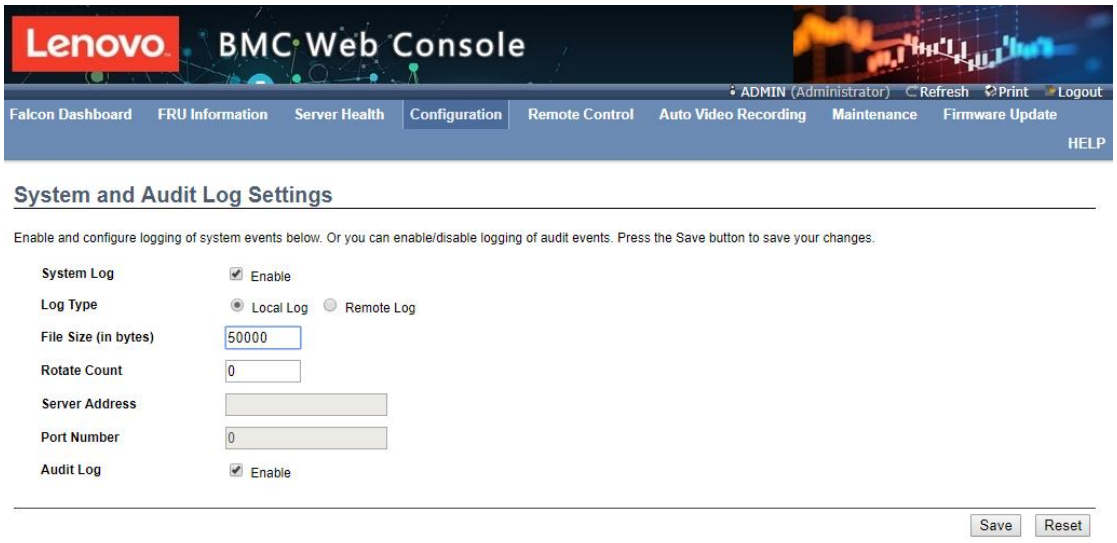
4.9.15 SSL Settings

This field is used to configure SSL certificate into the BMC.



4.9.16 System and Audit Log

In MegaRAC GUI, System and Audit log page displays a list of system logs and audit logs occurred in this device.



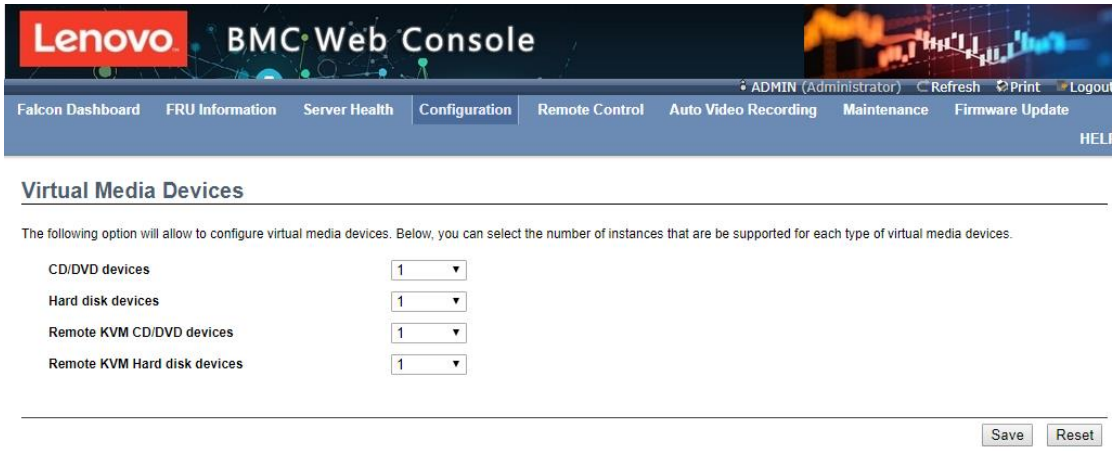
4.9.17 System Firewall

This field is used to configure firewall setting.

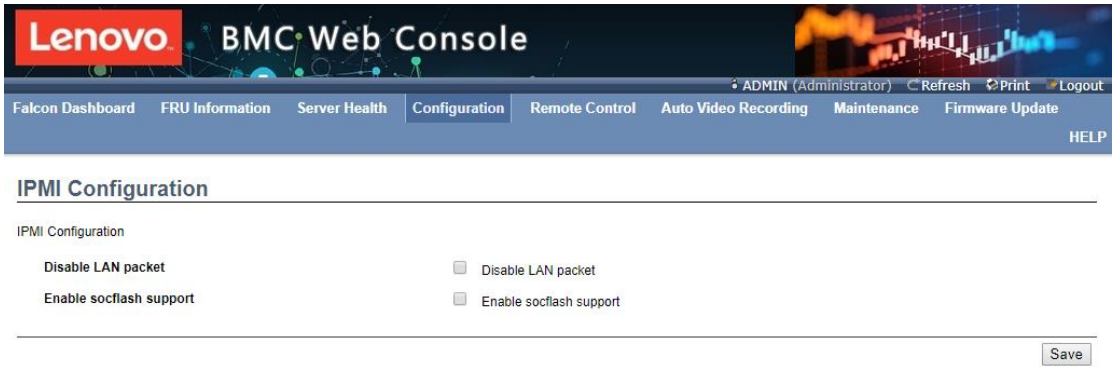
4.9.18 User Management

This page is used to manage users. By clicking user icon, administrator can add a new user and modify or delete the existing users.

4.9.19 Virtual Media

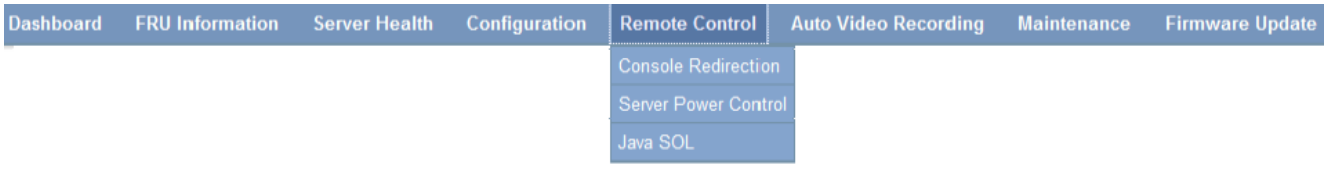


4.9.20 IPMI Configuration



4.10 Remote Control

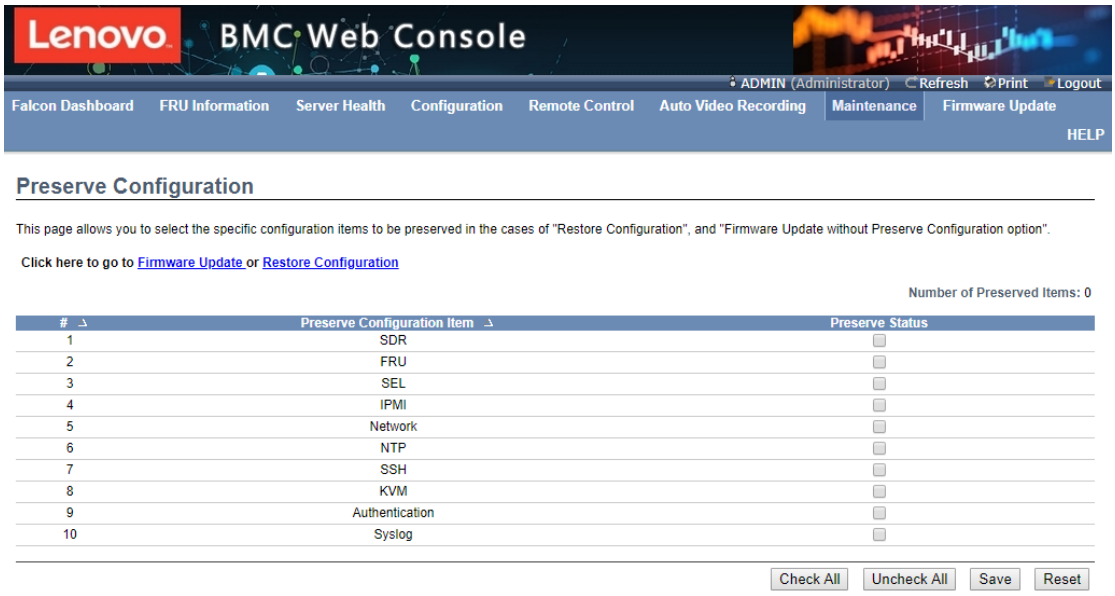
This page is used to launch KVM.



4.11 Maintenance

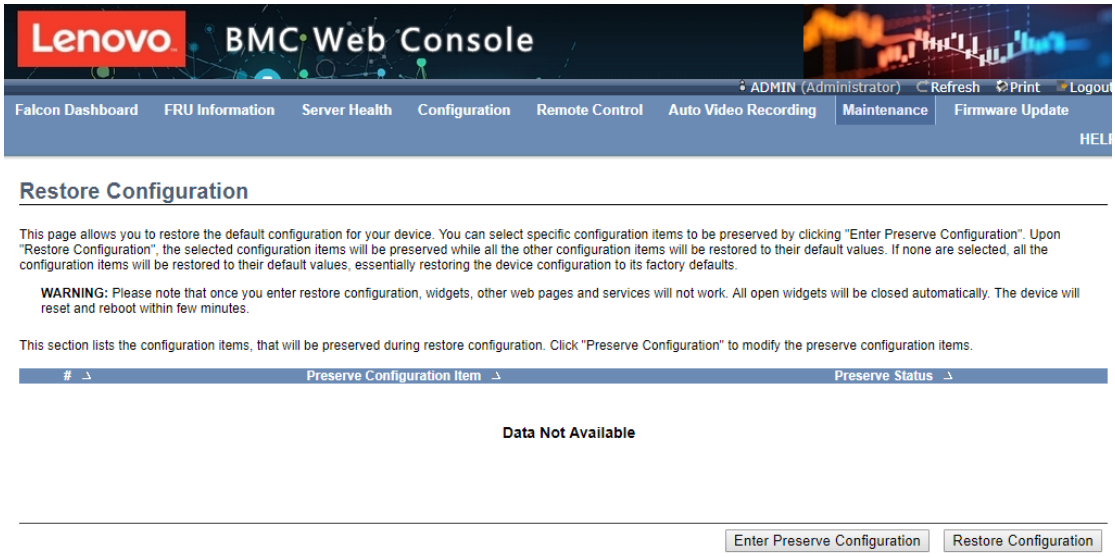
4.11.1 Preserve Configuration

This page allows you to select the specific configuration items to be backup.



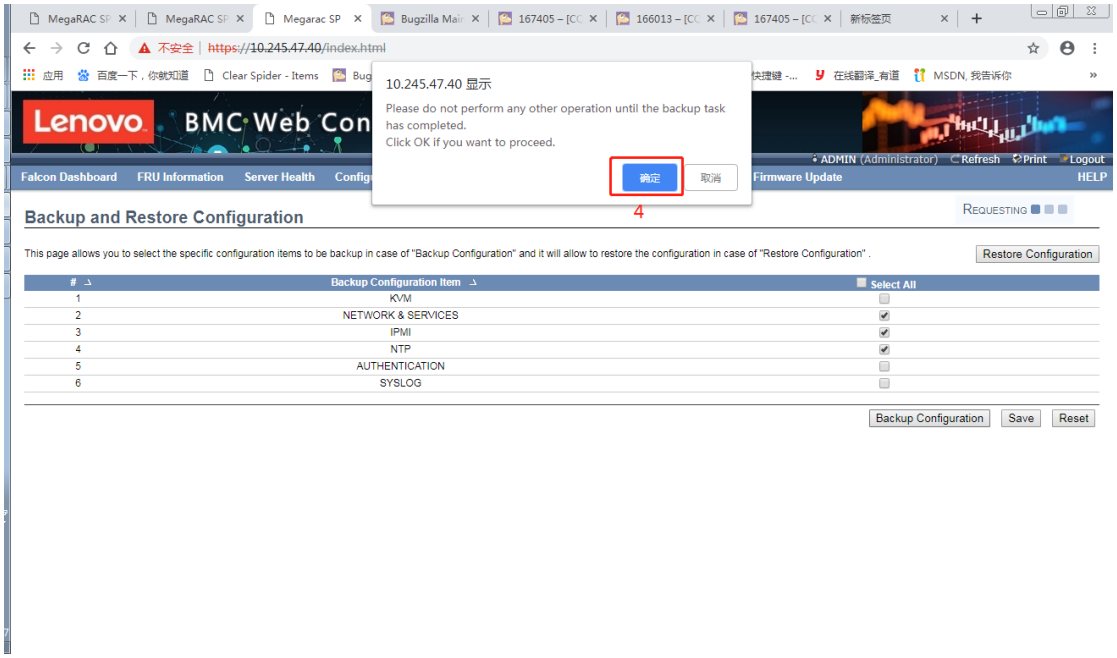
4.11.2 Restore Configuration

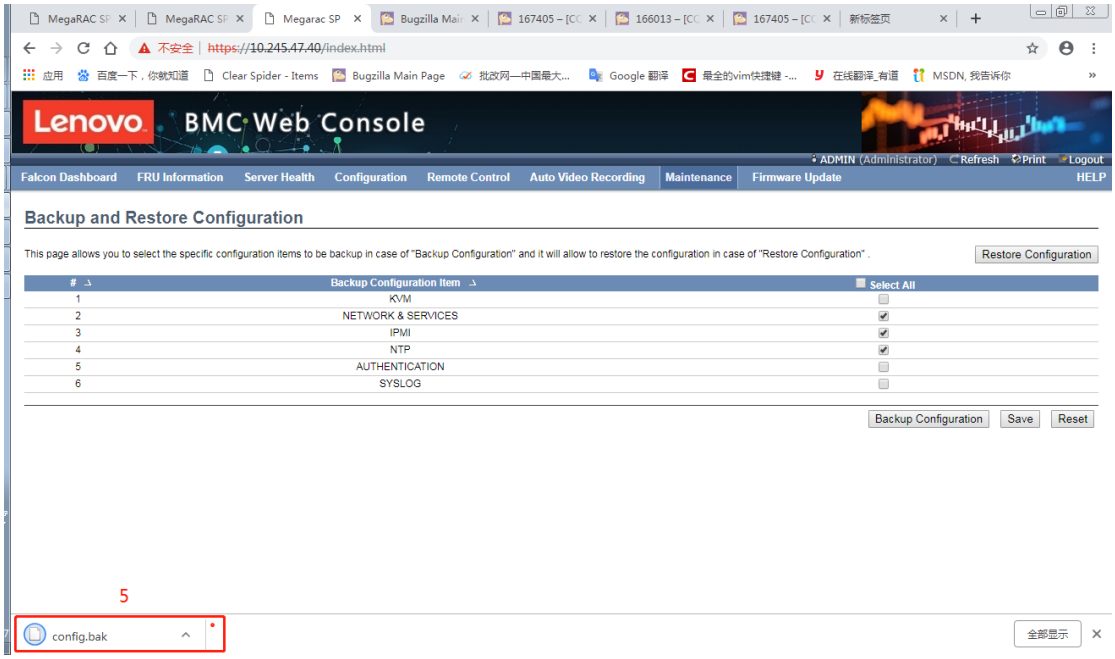
This page allows user to restore the configuration files from the client system to the BMC.



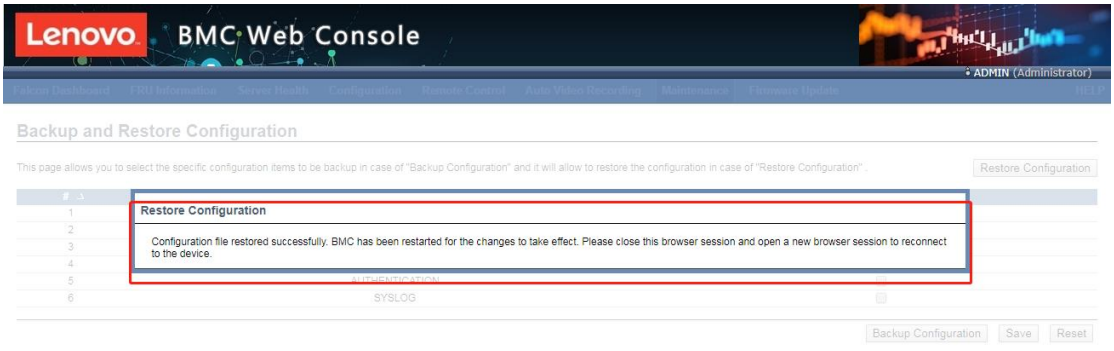
1. Select the option you want to save, or Select "Select All" to save All configurations, and click "save".

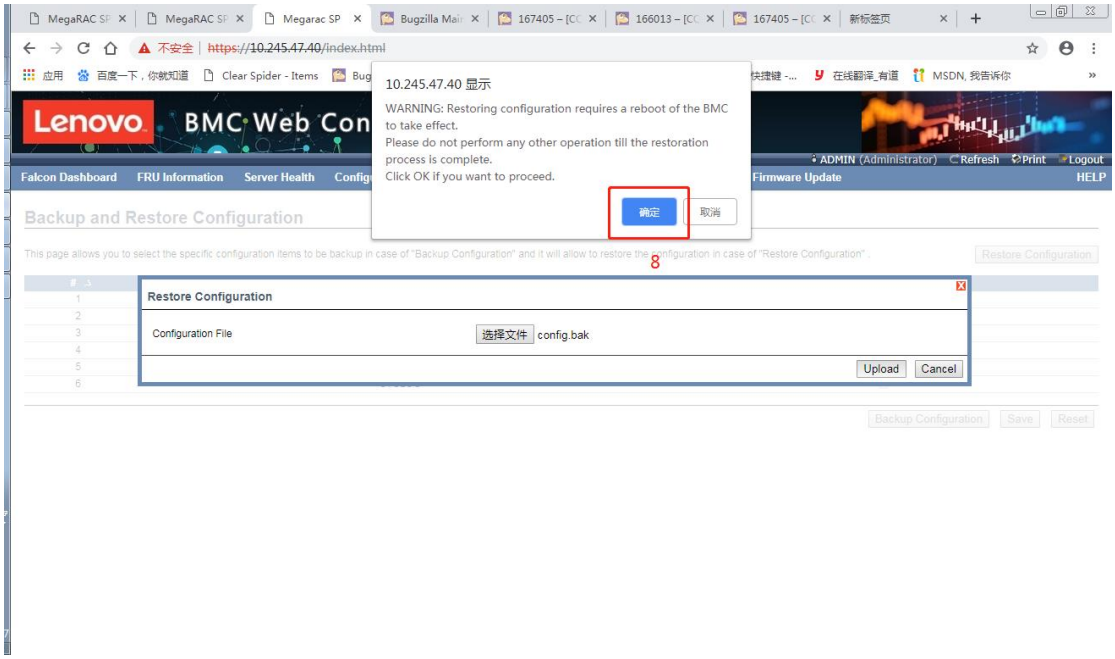
2. Click "Backup Configration" to download the Backup configuration file





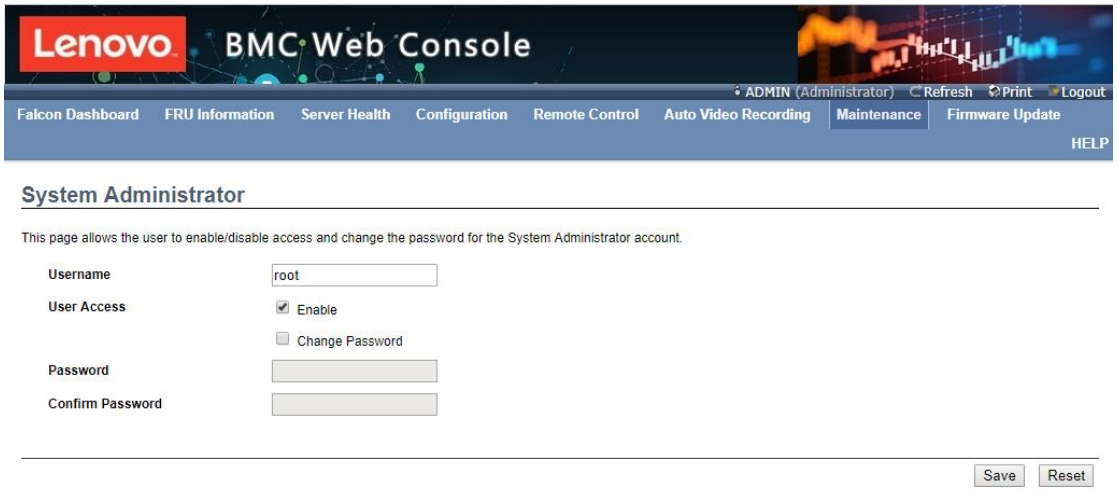
3. Select "Restore Configuration" and upload the downloaded backup files.




MegaRAC SP
MegaRAC SP
Megarac SP
不安全 https://10.245.47.40/index.html
Lenovo
BMC Web Con
ADMIN (Administrator)
Refresh
Print
Logout
Falcon Dashboard
FRU Information
Server Health
Firmware Update
HELP
10.245.47.40 显示
WARNING: Restoring configuration requires a reboot of the BMC to take effect.
Please do not perform any other operation till the restoration process is complete.
Click OK if you want to proceed.
确定
取消
Backup and Restore Configuration
Restore Configuration
Restore Configuration
Configuration File
选择文件
config.bak
Upload
Cancel
Backup Configuration
Save
Reset

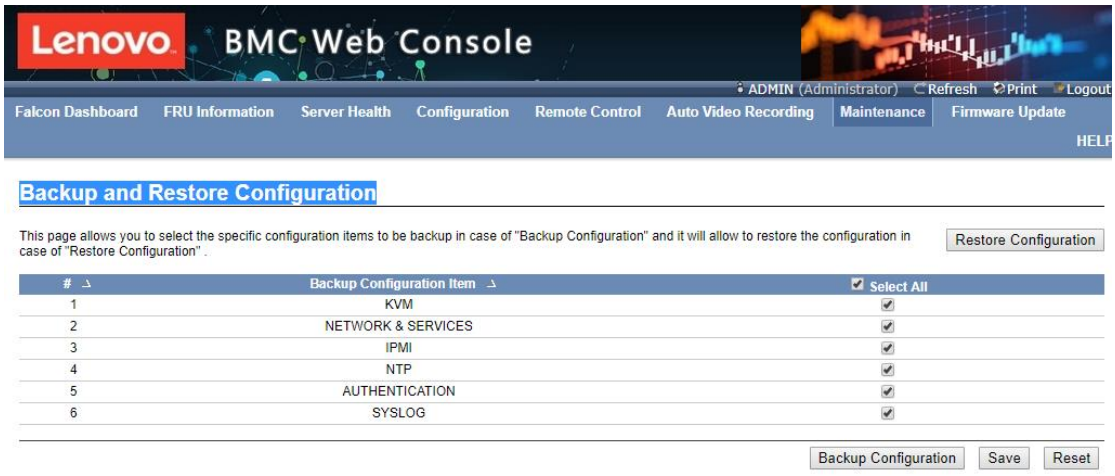
4.11.3 System Administrator

This page is used to configure the System Administrator settings.



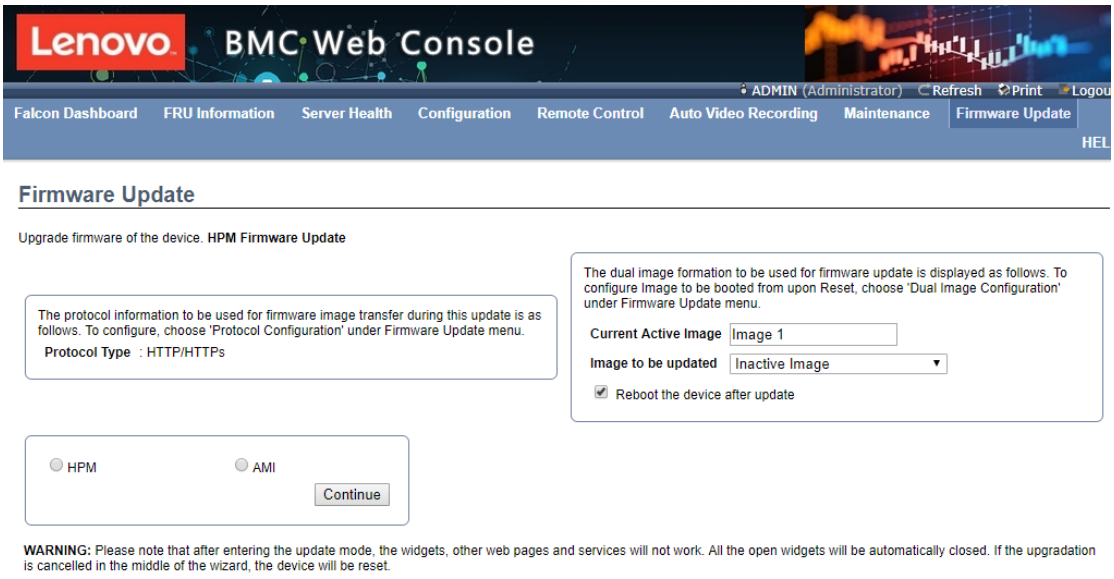
4.11.4 Backup and Restore Configuration

This page allows you to configure BMC Recovery settings.

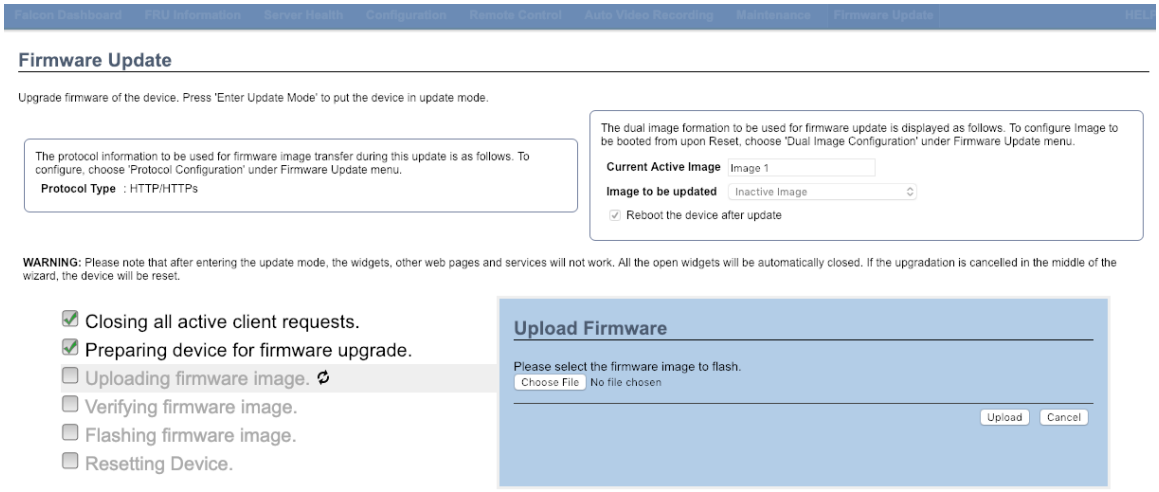


4.11.5 Firmware Update

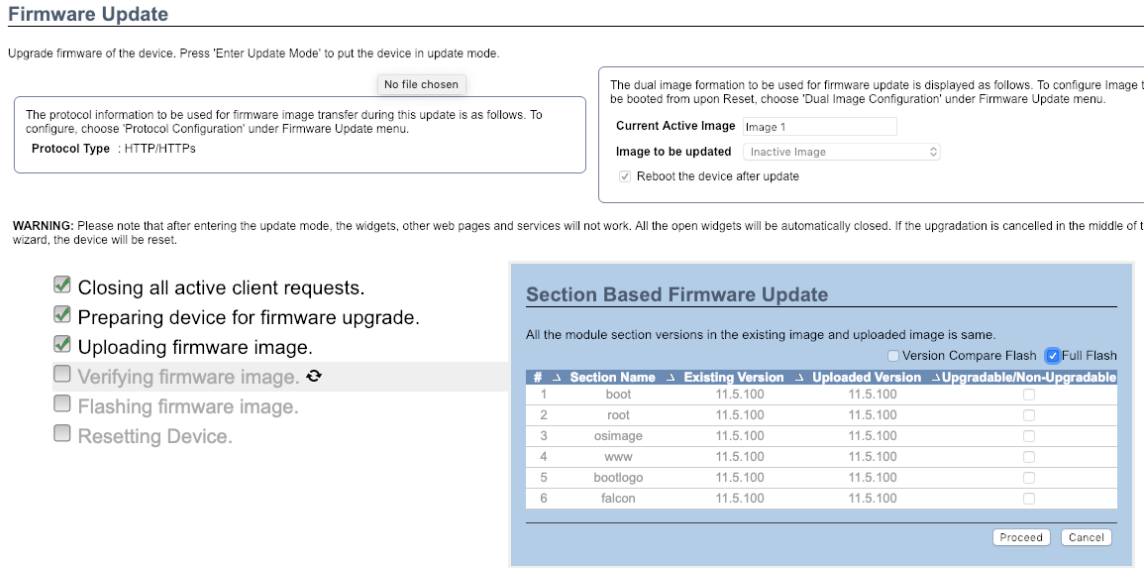
This wizard takes you through the process of firmware upgradation.



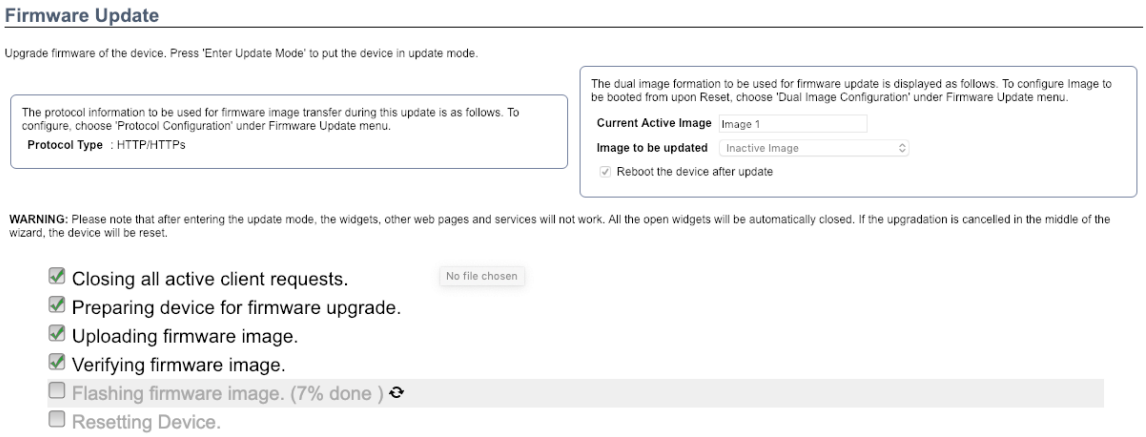
Click “Enter Update Mode” - Select the BMC firmware to update - select Upload.



- Check on Full Flash checkbox to flash all then click on Proceed to start firmware update.



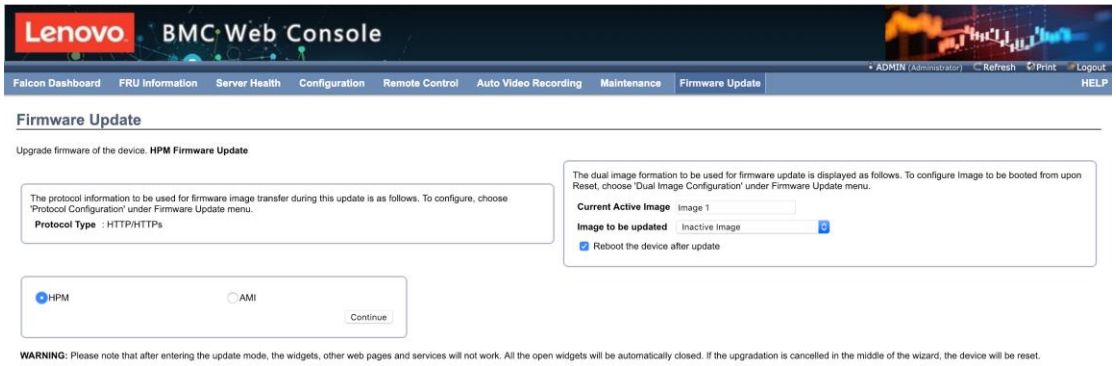
The upgrade process will start.



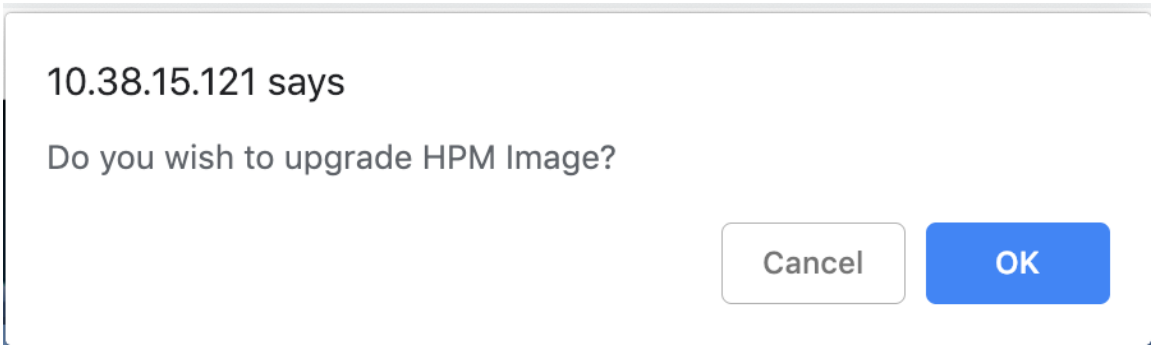
After upgrade complete, BMC will automatically restart.

Out-of-bound WebUI update

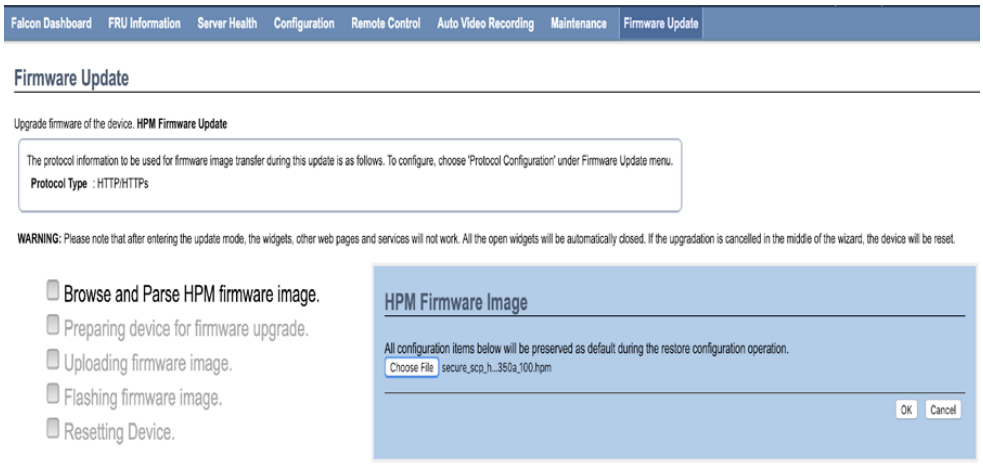
Below steps can be done to upgrade SCP and BIOS firmware using WebUI:
- Login to WebUI
- Select Firmware Update à Firmware Update
- Select HPM option then click Continue.



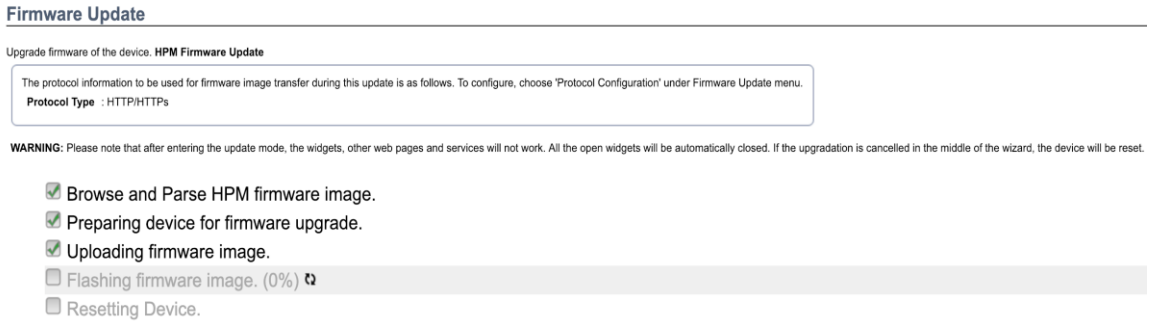
Select OK to continue.



Click on the “Choose File” button, browser and choose the SCP image to upgrade - Click OK to continue



Select “Update All” checkbox and click on “Process” button to continue. Click OK to confirm the action.



After the upgrade complete, reload the page to continue to use WebUI.

Chapter 5. Troubleshooting and diagnostics

5.1 Problems with initial start up

Should you encounter any problem starting up the system for the first time, follow the suggested actions below, in the listed order, until the problem is resolved:

1. Verify that the server's hardware configuration is as stated on the packing list.
2. Verify that all power cords and cables are connected correctly and securely.
3. Verify that the CPU heat sink has full contact with CPU and torqued to the proper tightness.
4. Verify that all PCI cards are fully and securely inserted into their respective slots on the raiser card.
5. Verify that there are no resource conflicts between any newly-added card and the standard cards (e.g. two cards sharing the same interrupt).
6. Verify that all external devices are working properly.
7. Verify that all SATA/NVMe drives have been properly formatted or configured.
8. Verify that all device drivers are installed properly.
9. Check if the user has made any changes to the BIOS settings.
10. Verify that the operating system is installed correctly (Refer to the sections relating to the operating system).
11. Verify both Power Supply Units are installed.
12. Verify that the server power button is turned on.

If the problem is not resolved, follow the suggested actions below, or contact your sales agent.

5.2 Resolving Other Problems

5.2.1 Monitor display problems

If your monitor does not display properly, perform the following checks:

1. Verify that the monitor's power switch is turned on. Solution: Turn on the monitor's power switch.

2. Verify that the power cords of the server and monitor are securely and correctly connected to the power outlets. Solution: Plug the one end of the power cord securely into the connector at the back of the server/monitor and the other end into a power outlet. Make sure that the power outlet used is working properly.

3. Verify that the monitor signal cable is properly connected, and there are no bent or broken pins. Solution: Connect the monitor signal cable securely to the corresponding signal outlet on the server.

4. Verify that the system fan is running. If the system fan does not run, shut down the server immediately and disconnect it from all power sources. Open the side panel of the server as instructed in this manual and verify that all connections are securely fastened.

5.2.2 Wavy lines on the screen

If you see wavy lines running across your display screen, do the following:

1. Verify that the monitor signal cable is correctly connected to the server: plug the ends of the signal cable securely into the adapter at the front of the server and into the corresponding connector at the rear of the monitor. Make sure that the power outlet used is working properly.

2. Some monitors have relatively noisy displays; these monitors should be replaced.

3. If the wavy lines persist, unplug the KVM signal line from the rear.

5.2.3 Clearing system configuration

In event of any of the following, clear the current system configuration (refer to Chapter 3 for clearing CMOS using jumpers) and restore the system to its default settings.

1. The system malfunctions after the default hardware configuration was changed, e.g. after adding/removing a network card or memory module.

2. "CPU Fail" or other error messages are displayed on the screen during the startup self-test.

3. The system malfunctions after the BIOS settings were changed (unable to start up the server).

4. Error in system configuration due to sudden power outage.

Contact your local Lenovo service center to have the above procedures performed at your site.

Note: All maintenance work performed by the user shall be at his/her own risk. Lenovo shall not be responsible for any hardware damage that may arise as a consequence.

5.2.4 Replacing the system board battery

The server battery should be replaced if missing server configuration error occurs frequently, system startup is unstable, or the error message: "CMOS Battery Fails" is displayed on the screen during the startup self-test. Contact your local Lenovo service center to have the server battery replaced at your site.

Note: All maintenance work performed by the user shall be at his/her own risk. Lenovo shall not be responsible for any hardware damage that may arise as a consequence.

After replacing the battery, restart the system. To reset system configuration, enter the system BIOS, then select Load Default Settings.

5.2.5 Common problems encountered while operating and using the system

1. The operating systems in following list do not support partitions larger than 2.2 TB in size. When installing these systems, make sure that the size of each partition is less than 2.2 TB.

The list is as follows:
CentOS 7.5
Oracle Linux 7.5

2. When installing a Linux OS, turn off UTC time synchronization. Under a Linux OS, enabling UTC time synchronization can result in an 8-hour time difference between BMC and Linux.

3. The BIOS setup menu is not displayed on full-screen. This is due to changes in terminal resolution when console redirection is enabled. To display the BIOS setup menu on full screen, go to the Console Redirection Settings submenu and enable the Resolution 100x31 option for serial port.

4. If the mouse mode is changed due to problems with the remote screen ratio, refresh the remote desktop or adjust the size of the iKVM window to counter this problem.

5. When accessing the BMC with Firefox to edit system configuration, if a window with the option to "Prevent this page from creating additional dialogs" pops up, do not check this option. The new configuration cannot be saved when this option is selected.

6. Before using the remote desktop tool (JViewer) to install an OS, do not enable KVM encryption and media encryption. Enabling KVM and media encryption might compromise the performance of the operating system installed.

Appendix A CentOS 7.5 Installation Guide

1. Introduction

This document provides the instructions for installing and working with CentOS on eMAG server platforms. At the time of this writing, CentOS 7.5 with Linux kernel 4.14 is supported.

1.1 System Requirements

- HR330A system board or derivative hardware designs with support for AMI BIOS.
- Latest CentOS ARM64 ISO image downloadable from CentOS repository.
- Latest Ampere Computing CentOS kernel updates downloadable from Ampere Customer Connect portal: https://connect.amperecomputing.com (requires registration).
- CentOS should work with all scenarios hereafter with 16GB system RAM.

2. Installing CentOS

2.1 Installing CentOS via Installation Media

2.1.1 Preparing CentOS Installation Media

1. Prepare one USB storage device (8GB) and one SATA drive.
2. On a Linux machine, download the latest CentOS ISO file and ddto a USB storage device (>= 8GB)

```
$ wget http://mirror.centos.org/altarch/7/isos/aarch64/CentOS-7-aarch64-Everything-1804.iso
$ dd if= CentOS-7-aarch64-Everything-1804.iso of=/dev/sdX
$ sync
```

2.1.2 Installing CentOS

1. Plug the USB device and SATA disk into the board.
2. Boot the system to the bootloader menu (Aptio Setup Utility) by pressing “Esc” during system boot-up.

2.1.2.1 Instructions for Aptio Setup Utility

3. In the Aptio Setup Utility screen, select the Save & Exit tab then select UEFI: Built-in EFI Shell entry, as highlighted below.

```
        Aptio Setup Utility - Copyright (C) 2017 American Megatrends, Inc.
     Main  Advanced  Security  Boot  Save & Exit  Server Mgmt
  /-------------------------------------------------+------------------------\
|   Discard Changes and Exit Save                    ^|                        |
|   Changes and Reset Discard Changes                *|                        |
|   and Reset                                        *|                        |
|                                                    *|                        |
|   Save Options                                     *|                        |
|   Save Changes                                     *|                        |
|   Discard Changes                                  *|                        |
|                                                    *|                        |
|   Restore Defaults                                 *|                        |
|  Save as User Defaults                             *|------------------------|
|  Restore User Defaults                             *|><: Select Screen       |
|                                                    *|^v: Select Item         |

|   Boot Override                                    *|Enter: Select           |
|   CentOS (P1: HGST HUS726020ALE610)                *|+/-: Change Opt.        |
|   UEFI: PXE boot on MAC: xx:xx:xx:xx:xx:xx         *|F1: General Help        |
|   UEFI: PXE boot on MAC: xx:xx:xx:xx:xx:xx         +|F2: Previous Values     |
|   UEFI: PXE boot on MAC: xx:xx:xx:xx:xx:xx         +|F3: Optimized Defaults  |
|    UEFI:  UFD 3.0 Silicon-Power8G PMAP             +|F4: Save & Exit         |
|   UEFI:  Built-in EFI Shell                         |ESC: Exit               |
```

4. In the UEFI Shell, after typing FS0:\EFI\BOOT\BOOTAA64.EFI, the following menu will be displayed:

```
Install CentOS Linux AltArch 7
Test this media & install CentOS Linux AltArch 7
Troubleshooting -->
Use the ↑ and ↓ keys to change the selection.
Press 'e' to edit the selected item, or 'c' for a command prompt.
```

5. Move the cursor to Install CentOS Linux AltArch 7.

   If your hardware uses a different console UART other than the default UART0, from grub menu, hit “e” to enter grub config and add appropriate console parameters to re-direct terminal output to a proper serial line:

   “console=ttyS1,115200” for the board which uses UART1

   “console=ttyS2,115200” for the board which uses UART2

   “console=ttyS3,115200” for the board which uses UART3

6. Hit “Return” to start the installer.
7. Wait for the installation menu.
8. Select Timezone settings to set your time zone.
9. Select Software Selection then choose GNOME Desktop to install the GUI package if the board supports VGA. Otherwise, Minimal Install installation is preferred.
10. Select Install Destination, then select the SATA disk which will be used to install CentOS.
11. Set password for root via Root password.
12. Create user via User creation options (optional).
13. Set the network configuration via Network configuration option (optional).

```
Installation

 1) [x] Language settings                 2) [x] Time settings
        (English (United States))                (US/Central timezone)
 3) [x] Installation source               4) [x] Software selection
        (Local media)                            (Minimal Install)
 5) [x] Installation Destination          6) [x] Kdump
        (Automatic partitioning                  (Kdump is enabled)
        selected)                         8) [x] Root password
 7) [ ] Network configuration                    (Password is set.)
        (Not connected)
 9) [ ] User creation
        (No user will be created)
Please make your choice from above ['q' to quit | 'b' to begin installation | 'r' to refresh]
```

14. Press “b” to start installation.
15. Wait for the installation to complete, and then hit “Return” to reboot.

```
Performing post-installation setup tasks
.
Configuring installed system
.
Writing network configuration
.
Creating users
.
Configuring addons
.
Generating initramfs
.
Running post-installation scripts
Installation complete.  Press return to quit
```

16. After system reboot, BIOS will select CentOS as the first boot entry. The following screen will be displayed.

```
CentOS Linux (4.14.0-49.e17.aarch64) 7 (AltArch)
CentOS Linux (0-rescue-3f6e9491e8ab4eb6b00f6ccb5f5616f9) 7 (AltArch)


Use the ↑ and ↓ keys to change the selection.
Press 'e' to edit the selected item, or 'c' for a command prompt.
```

17. Select the first grub entry and then hit “Return” to boot CentOS, or the system will boot the default entry.

2.1.3 Updating CentOS Kernel

Install the necessary packages:

```
# yum install net-tools wget
```

2.1.3.1 Updating Vanilla CentOS Kernel

1. Check for CentOS kernel updates as shown below:

```
# uname –r
4.14.0-49.el7.aarch64
# yum check-update | grep kernel
kernel.aarch64                  4.5.0-23.el7                  updates
kernel-tools.aarch64            4.5.0-23.el7                  updates
kernel-tools-libs.aarch64       4.5.0-23.el7                  updates
```

2. Apply the update as shown below:

```
# yum –y update
# reboot
```

2.1.3.2 Updating Ampere Computing Generic CentOS Kernel

Obtain the Ampere Computing CentOS tarball. It should have a name similar to amp_sw_centos_7.5-yymmdd.tar.xz.

```
# tar xvf amp_sw_centos_7.5-yymmdd.tar.xz
# cd aarch64/
# ls
kernel-headers-4.14.0-49.el7.yymmdd+amp.aarch64.rpm
kernel-4.14.0-49.el7.yymmdd+amp.aarch64.rpm
kernel-devel-4.14.0-49.el7.yymmdd+amp.aarch64.rpm
kernel-debug-4.14.0-49.el7.yymmdd+amp.aarch64.rpm
kernel-debug-devel-4.14.0-49.el7.yymmdd+amp.aarch64.rpm

# yum –y install *.rpm
# reboot
```

WARNING: If the vanilla kernel is newer than the Ampere Computing CentOS kernel mentioned in the README, the update may fail. In that case please contact Ampere Computing Support for assistance.

2.1.3.3 Updating Ampere Computing Optimized CentOS Kernel with ILP32 Support

If ILP32 kernel is to be used, obtain the Ampere Computing CentOS tarball with ILP32 support. It should have a name similar to amp_sw_centos_7.5-yymmdd.ilp32-src.tar.xz.

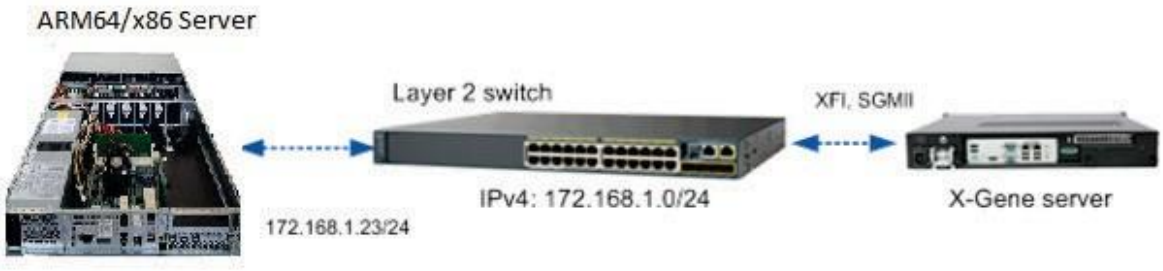
```
# tar xvf amp_sw_centos_7.5-yymmdd.ilp32.tar.xz
# cd aarch64/
# ls
kernel-headers-4.14.0-49.el7.yymmdd+amp.ilp32.aarch64.rpm
kernel-4.14.0-49.el7.yymmdd+amp.ilp32.aarch64.rpm
kernel-devel-4.14.0-49.el7.yymmdd+amp.ilp32.aarch64.rpm
kernel-debug-4.14.0-49.el7.yymmdd+amp.ilp32.aarch64.rpm
kernel-debug-devel-4.14.0-49.el7.yymmdd+amp.ilp32.aarch64.rpm

# yum –y install *.rpm
# reboot
```

2.2 Installing CentOS via PXE

2.2.1 Preparing PXE Installation System

System Configuration

Figure 1: A Server running Ubuntu (15.04 or later) or CentOS 7.x



Configuring PXE Server

1. Installing necessary packages:
   - Ubuntu 15.x:

```
# apt-get install -y isc-dhcp-server xinetd tftpd-hpa wget apache2
```

   - CentOS 7.x:

```
# yum install -y xinetd tftp tftp-server dhcp httpd wget createrepo
```

2. Adding (or modifying) the /etc/dhcp/dhcpd.conf file
   - Ubuntu 15.x and CentOS 7.x:

```
# vi /etc/dhcp/dhcpd.conf
default-lease-time 600;
max-lease-time 600;
log-facility local7;
authoritative;
option arch code 93 = unsigned integer 16; # RFC4578
option domain-name-servers 8.8.4.4, 8.8.8.8;
subnet 172.168.1.0 netmask 255.255.255.0 {
range dynamic-bootp 172.168.1.30 172.168.1.254;
option broadcast-address 172.168.1.255;
option routers 172.168.1.23;
next-server 172.168.1.23;
class "pxeclients" {
        match if substring (option vendor-class-identifier, 0, 9) = "AMPClient";
        if option arch = 00:0b {
            # Installing Centos
                    filename "/AMP/centos-repo/EFI/BOOT/grubaa64.efi";
        }
```

```
}
class "pxeclients" {
        match if substring (option vendor-class-identifier, 0, 9) = "PXEClient";
        if option arch = 00:0b {
            # Installing Centos
                    filename "/AMP/centos-repo/EFI/BOOT/grubaa64.efi";
        }
}
}
# systemctl enable dhcpd
# systemctl restart dhcpd
```

3. Downloading the CentOS 7 ISO file and creating PXE repository.

```
# wget http://mirror.centos.org/altarch/7/isos/aarch64/CentOS-7-aarch64-Everything.iso
# mkdir -p /media/centos-arm64-iso/
# mount -o loop CentOS-7-aarch64-Everything.iso /media/centos-arm64-iso
# mkdir -p /var/lib/tftpboot/AMP/centos-repo/
# cp -rf /media/centos-arm64-iso/EFI /media/centos-arm64-iso/images
/var/lib/tftpboot/AMP/centos-repo/
# mkdir -p /var/www/html/AMP/centos-repo
# cp -rf /media/centos-arm64-iso/* /var/www/html/AMP/centos-repo/
# umount /media/centos-arm64-iso
```

4. Changing “menuentry” in the /var/lib/tftpboot/AMP/centos-repo/EFI/BOOT/grub.cfg file.
   - Ubuntu 15.x and CentOS 7.x:

```
# sudo vi /var/lib/tftpboot/AMP/centos-repo/EFI/BOOT/grub.cfg
set default="0"
function load_video {
  if [ x$feature_all_video_module = xy ]; then
    insmod all_video
  else
    insmod efi_gop
    insmod efi_uga
    insmod ieee1275_fb
    insmod vbe
    insmod vga
    insmod video_bochs
    insmod video_cirrus
  fi
}

load_video
set gfxpayload=keep
```

```
insmod gzio insmod
part_gpt insmod ext2

set timeout=60
### END /etc/grub.d/00_header ###

search --no-floppy --set=root -l 'CentOS-7-AArch64'

### BEGIN /etc/grub.d/10_linux ###
menuentry 'Install CentOS Linux 7' --class red --class gnu-linux --class gnu --class os { linux /AMP/centos-repo/images/pxeboot/vmlinuz inst.stage2=http://172.168.1.23/AMP/centos-repo ro
        initrd /AMP/centos-repo/images/pxeboot/initrd.img
}
menuentry 'Test this media & install CentOS Linux 7' --class red --class gnu-linux --class gnu --class os {
        linux /images/pxeboot/vmlinuz inst.stage2=hd:LABEL=CentOS-7-AArch64 rd.live.check initrd /images/pxeboot/initrd.img
}
submenu 'Troubleshooting -->' {
        menuentry 'Install CentOS Linux 7 in basic graphics mode' --class red --class gnu- linux --class gnu --class os {
                linux /images/pxeboot/vmlinuz inst.stage2=hd:LABEL=CentOS-7-AArch64 nomodeset initrd
                /images/pxeboot/initrd.img
        }
        menuentry 'Rescue a CentOS Linux system' --class red --class gnu-linux --class gnu -- class os {
                linux /images/pxeboot/vmlinuz inst.stage2=hd:LABEL=CentOS-7-AArch64 rescue initrd
                /images/pxeboot/initrd.img
        }
```

5. Editing the TFTP server's configuration.
   - Ubuntu 15.x:

```
$ sudo vi /etc/default/tftpd-hpa
TFTP_USERNAME="tftp"
TFTP_DIRECTORY="/var/lib/tftpboot"
TFTP_ADDRESS="0.0.0.0:69"
TFTP_OPTIONS="--secure --create"
$ sudo chmod 777 -R /var/lib/tftpboot/
$ sudo chown tftp:nogroup -R /var/lib/tftpboot/
$ sudo systemctl enable xinetd
$ sudo systemctl restart xinetd
```

```
$ sudo systemctl stop firewalld
$ sudo systemctl disable firewalld
```

- CentOS 7.x:

```
# vi /etc/xinetd.d/tftp
service tftp
{
        socket_type             = dgram
        protocol                = udp
        wait                    = yes
        user                    = root
        server                  = /usr/sbin/in.tftpd
        server_args             = -c -s /var/lib/tftpboot
        disable                 = no
        per_source              = 11
        cps                     = 100 2
        flags                   = IPv4
}
# chmod 777 -R /var/lib/tftpboot/
# setsebool -P tftp_anon_write 1
# setsebool -P tftp_home_dir 1
# systemctl enable xinetd
# systemctl restart xinetd
# systemctl stop firewalld
# systemctl disable firewalld
```

6. Verifying TFTP server.
   - Ubuntu 15.x and CentOS 7.x:

```
# tftp 172.168.1.23
tftp> get /AMP/centos-repo/EFI/BOOT/grubaa64.efi
Received 883074 bytes in 0.1 seconds
tftp>
```

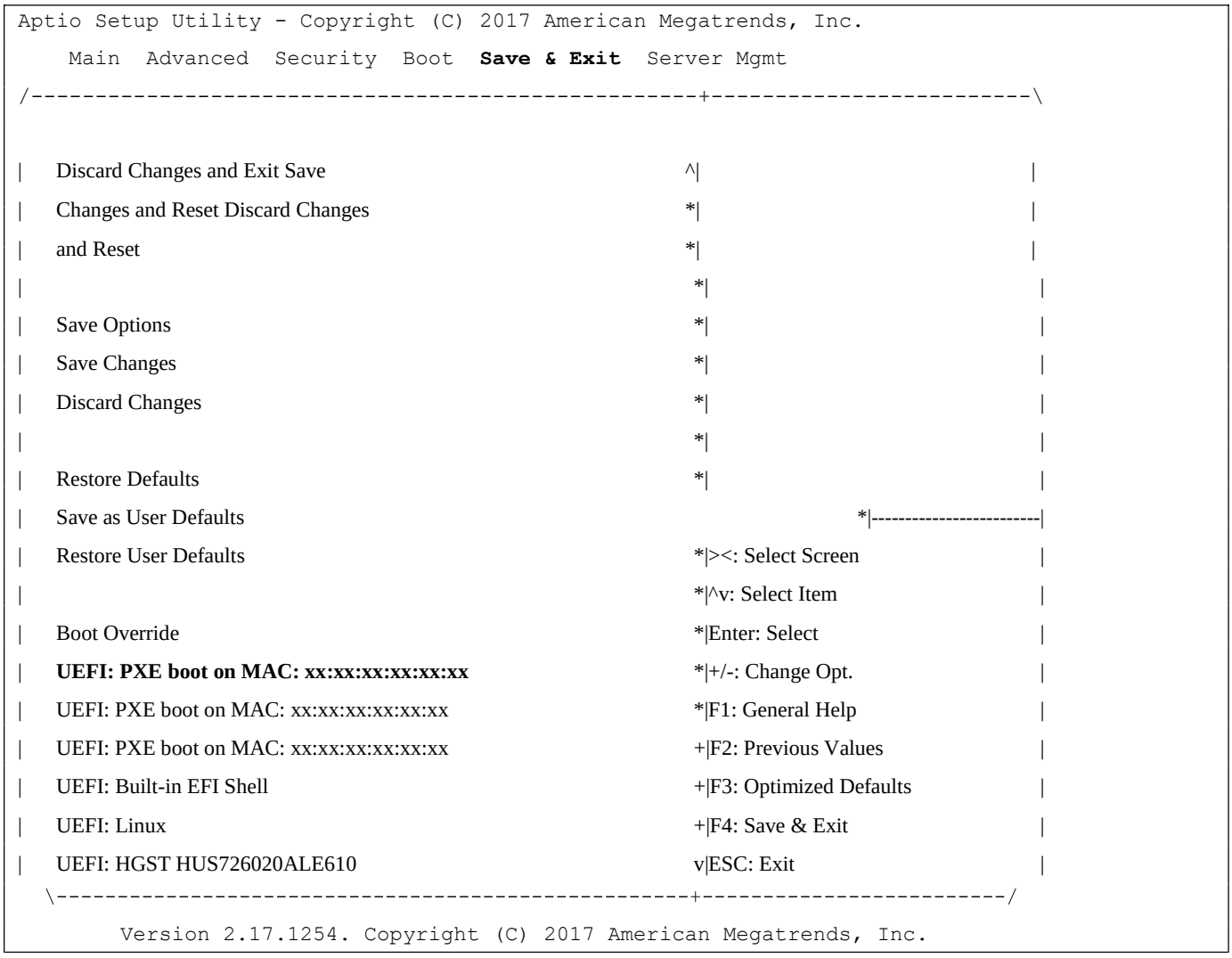
7. Starting Apache web server.
   - Ubuntu 15.x:

```
$ sudo systemctl enable apache2
$ sudo systemctl restart apache2
Centos 7.x:
# systemctl enable httpd
# systemctl restart httpd
Verifying web server access
# wget http://172.168.1.23/AMP/centos-repo/EFI/BOOT/grubaa64.efi
```

2.2.2 Installing CentOS

2.2.2.1 Instructions for Aptio Setup Utility

1. Boot the system to Aptio Setup Utility by pressing “Esc” duringsystem boot-up.
2. Select the “Save & Exit” tab and then select Ethernet PXE boot entry, as shownbelow.



3. Activating Management Ethernet

If the network configuration is skipped during the installation, try the following to activate eth0 as the Management Ethernet. Make sure the board's Ethernet is connected to the network.

1. Edit the CentOS network script as in the example below.

```
# vi /etc/sysconfig/network-scripts/ifcfg-eth0
TYPE=Ethernet
BOOTPROTO=dhcp
DEFROUTE=yes
PEERDNS=yes
PEERROUTES=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=yes
IPV6_AUTOCONF=yes
IPV6_DEFROUTE=yes
IPV6_PEERDNS=yes
IPV6_PEERROUTES=yes
IPV6_FAILURE_FATAL=no
NAME=eth0
UUID=885235a6-f66e-4dc6-aa31-87149d95f4ad
DEVICE=eth0
ONBOOT=yes
```

2. Restart the network service, then try ping to make sure that the Ethernet is working:

```
# systemctl restart network
# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=58 time=2.19 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=58 time=20.9 ms


--- 8.8.8.8 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 2.195/11.591/20.988/9.397 ms
```

4. GNOME Desktop Support (Optional)

If GUI is not selected during installation, follow the steps below for support:

1. Install additional xorg-x11-server packages.

```
# yum groups install "GNOME Desktop"
# yum install xorg-x11-server-devel
# yum install libXrandr-devel
```

2. Start X server with GNOME.

```
# startx
```

Enable GUI as default system target.

```
# systemctl set-default graphical.target
# systemctl enable gdm.service
# reboot
```

3. Disable the GUI and revert to use VGA console.

```
# systemctl disable graphical.target
# systemctl disable gdm.service
# reboot
```

5. Building CentOS Kernel

5.1 Setting up Native CentOS Development Environment

First, install the necessary development packages (if not done already).

```
# yum groupinstall "Development Tools"
# yum install ncurses-devel
# yum install hmaccalc zlib-devel binutils-devel elfutils-devel libelf-devel newt-devel
python-devel
# yum install audit-libs-devel numactl-devel pciutils-devel openssl-devel
# yum install bc bison perl-ExtUtils-Embed.noarch xmlto asciidoc
```

5.2 Building Ampere Computing CentOS Kernel

Ampere Computing provides the Ampere Computing CentOS kernel source in SRPM package and patch forms. The SRPM package allows the user to install and build the kernel immediately. The Ampere Computing CentOS patch is for users who wish to apply Ampere Computing changes on top of CentOS vanilla kernel source and build instead.

Both SRPM and patch forms allow the user to build a generic Linux kernel based on default CentOS configuration, and an ILP32-enabled Linux kernel with Ampere Computing's optimized configuration. While either CentOS native toolchain or Ampere Computing toolchain can be used to build the generic kernel, the Ampere Computing toolchain is specifically required to compile the ILP32-enabled kernel. Applications compilation, on the other hand, must use the default CentOS provided native toolchain.

Installing Ampere Computing Toolchain

If there is a need to recompile Ampere Computing CentOS kernel, follow the instructions below:

1. Refer to the appropriate Ampere Computing Release Notes for information about the latest Ampere Computing toolchain and download it.
   - Login to http://connect.amperecomputing.com
   - Go to http://connect.amperecomputing.com/products/pd/system-software
   - Click on Ampere eMAG Toolchain 9.0.7 to see the actual file
   - Click on amp-9.0.7-le-20170222-nativetools.tar.bz2 to start downloading it
2. Install the toolchain on the board.

```
# mkdir -p /opt/amp/9.0.7-le
# tar --strip-components=1 -xf amp-9.0.7-le-20170222-nativetools.tar.bz2 -C /opt/amp/9.0.7-le
```

3. Set PATH to point to the Ampere Computing toolchain.

```
$ export PATH=/opt/amp/9.0.7-le/usr/bin:$PATH;
$ which gcc
/opt/amp/9.0.7-le/usr/bin/gcc
```

Building Ampere Computing CentOS Kernel from SRPM

1. Execute "uname –r"

   It should show something similar to "**4.14.0-49.el7.yymmdd+amp.aarch64**" such as **4.14.0-49.e17.170125+amp.aarch64**

2. Obtain the matching SRPM kernel source package from the release. The name of the package should be similar to:
   a) amp_sw_centos_7.5-yymmdd.src.tar.xz or – this is the SRPM for the generic kernel
   b) amp_sw_centos_7.5-yymmdd.ilp32-src.tar.xz – this is the SRPM for the ILP32 kernel

3. Extract kernel source package:

```
$ tar xf amp_sw_centos_7.5-yymmdd.src.tar.xz
```

4. Install the SRPM.

```
$ cd SRPMS/
$ rpm –ivh kernel-aarch64-4.14.0-49.el7.yymmdd+amp.src.rpm
```

5. Build the kernel source.

```
$ cd ~/rpmbuild
$ ls
SOURCES/   SPECS/
$ rpmbuild --define "%_topdir `pwd`" -bb --without debuginfo --without perf --without tools
SPECS/kernel-xgene.spec
# To build ILP32 kernel, use the ilp32-src package and kernel-xgene-optimized.spec
$ rpmbuild --define "%_topdir `pwd`" -bb --without debuginfo --without perf --without tools
SPECS/kernel-xgene-optimized.spec
```

6. Refer to the generic CentOS documentation and RPMBUILD manual on how rpmbuild should work.

Building Ampere Computing CentOS Kernel using Ampere Computing CentOS Patches

1. Clone ampere-centos-kernel

```
$ mkdir ampere-centos
$ cd ampere-centos
$ git clone https://github.com/AmpereComputing/ampere-centos-kernel
$ git clone https://github.com/AmpereComputing/ampere-centos-build
```

2. Checkout Ampere CentOS 7.5

```
$ cd ampere-centos-kernel
$ git checkout amp-centos-7.5-kernel
$ cd ../ampere-centos-build
$ git checkout amp-centos-7.5-build
```

3. Build Ampere CentOS RPM files

```
$ ./ampere-centos-build.sh
```

When the above steps are completed, the Ampere CentOS RPM files would be located at:

./amp_sw_centos_7.5-yymmdd.tar.xz ./amp_sw_centos_7.5-yymmdd.ilp32.tar.xz

Where yy is the last two digits of the year, mm is the digit of the month, and dd is the digit of the day. The amp_sw_centos_7.5-yymmdd.tar.xz is the non-optimized version of the Ampere CentOS kernel. The amp_sw_centos_7.5-yymmdd.ilp32.tar.xz is the optimized version of the Ampere CentOS kernel.

Building Applications SRPMs

Application builds need to use the CentOS native compiler instead of Ampere Computing native compiler.

Remove the Ampere Computing toolchain's path from PATH and execute rpmbuild for the applications RPM package in the normal manner.

6. Ampere Computing CentOS RAS/APEI Support

The Ampere Computing CentOS kernel is compiled with ACPI Platform Error Interface (APEI) support and Generic Hardware Error Source (GHES) support.

GHES is a non-x86 specific error type in APEI for describing error sources via the Hardware Error Source (HEST) table. It is a defined mechanism for reporting errors to the kernel from firmware

```
CONFIG_ACPI_APEI=y
CONFIG_ACPI_APEI_GHES=y
```

For eMAG 8180, there are currently 9 Generic Hardware Error Sources (GHES) that are used to report errors to the kernel. The *Osprey RAS/APEI User Guide* describes the type of APEI error messages that can be reported to the APEI/GHES interface and UEFI Common Platform Error Record (CPER) interface in the kernel.

7. CentOS AHCI Platform Boot Failure Recovery

In BIOS version 4.05 series, the SATA driver was switched from Ampere Computing eMAG driver to standard AHCI platform driver. This creates a disk detection issue at boot time if you originally installed CentOS with Ampere Computing eMAG SATA driver. To recover from this boot failure, follow the steps below:

1. Boot up CentOS using rescue kernel.
2. Run the following command to see all the currently installed kernel version images.

```
# rpm -qa kernel | sed -e 's/kernel-//g'
```

3. Run the following command to recover the desired kernel.

```
# dracut -f --kver <desired kernel version>
```

4. Reboot to that kernel version.

8. KVM Support

Mismatching of the Linux kernel, QEMU and libVirt could cause errors when using virtual machines. The user must take care to update all packages to the latest within a target release. Mixing packages from different releases could result in unpredictable behavior. Therefore, to set up VM, it is recommended to use one of the following options:

- Option A: Configure yum repository to use the CentOS 7.5 website depot only and not the latest CentOS 7.5 depot.
- Option B: Upgrade your system completely to the latest CentOS 7.5.

In addition, please be aware that Ampere Computing CentOS optimized version – with the file named text "ilp32" – does not sup

Appendix B HR330A OEM Command Specification

1. Introduction

This document describes detail OEM commands that are specific for the HR330A board.

2. HR330A OEM Commands

2.1 Load UEFI default setting

The command is used to erase the UEFI NVRAM, command will be affected on next boot.

Linux command:

$ ipmitool raw 0x3c 0x1

Description:

NetFn	**0x3c**
Command	0x1

Request data:

Response data:

Byte	Data field
1	Completion Code

2.2 Clear or un-clear the UEFI password

The command is used to clear the UEFI password, command with be affected on next boot.

Linux command:

$ ipmitool raw 0x3c 0x2 0x2 0xff

Description:

NetFn	**0x3c**
Command	0x2

Request data:

Mask	**0x2 – Use bit 1 to control the feature, the effect depends on the value.**
Value **[7:0]**	0x0 - Trigger to disable the feature that clear UEFI password 0xff - Trigger to enable the feature that clear the UEFI password

Response data:

Byte	Data field
1	Completion Code

2.3 Set or un-set the UEFI manufacturing mode (Deprecated)

The command is used to set the UEFI to run on manufacturing mode on next boot.

Linux command:

$ ipmitool raw 0x3c 0x2 0x4 0xff

Description:

NetFn	**0x3c**
Command	0x2

Request data:

Mask	**0x4 – Use bit 2 to control the feature, the effect depends on the value.**
Value **[7:0]**	0x0 - Trigger to disable the feature that running at manufacturing mode 0xff - Trigger to enable the feature that running at manufacturing mode

Response data:

Byte	**Data field**
1	Completion Code

2.4 Hide or un-hide the UEFI menu

The command is used for UEFI to Hide / Un-hide the UEFI menu setting.

Linux command:
$ ipmitool raw 0x3c 0x2 0x8 0xff

Description:

NetFn	**0x3c**
Command	0x2

Request data:

Mask **[7:0]**	**0x8 – Use bit 3 to control the feature, the effect depends on the value.**
Value **[7:0]**	0x0 - Trigger to disable the feature that running at manufacturing mode 0xff - Trigger to enable the feature that running at manufacturing mode

Response data:

Byte	Data field
1	Completion Code

2.5 Get the UEFI control FLAG

The command is to get the UEFI setting flag which contains the setting bits for functions in section 2.2, 2.3 and 2.4 above. Please be noted that the control flag should be set before by command 0x2. If not, the 'Unspecified Error' will be returned.

Linux command:
$ ipmitool raw 0x3c 0x3

Description:

NetFn	**0x3c**
Command	0x3

Request data:

Response data:

Completion	Completion Code
UEFI Flag	[7:4] - Reserve [3] 1b = Hide/Un-hide UEFI setting [2] 1b = Set/Un-set UEFI manufacturing mode (Deprecated) [1] 1b = Clear/Un-clear UEFI password [0] 1b = Reserved

2.6 MUX Switching command

The command is used to switch the MUX lines to SOL and SYS.

Linux command:

$ ipmitool raw 0x3c 0xee <Port Index> <Direction>

Description:

NetFn	**0x3c**
Command	0xee

Request data:

Byte	Data filed
1	Port Index: 0x0 – UART 0 0x1 – UART 1 0x2 – UART 4
2	Direction: 00 – MUX to SYS 01 – MUX to BMC 02 – MUX to SOL

Response data:

Byte	Data field
1	Completion Code
2	Direction: 00 – MUX to SYS 01 – MUX to BMC 02 – MUX to SOL

2.7 Get MUX Configuration

The command is used to get the MUX configuration for the specify port.

Linux command:

$ ipmitool raw 0x3c 0xe0 <Port Index>

Description:

NetFn	**0x3c**
Command	0xe0

Request data:

Byte	Data filed
1	Port Index: 0x0 – UART 0 0x1 – UART 1 0x2 – UART 4

Response data:

Byte	Data field
1	Completion Code
2	Direction: 00 – MUX to SYS 01 – MUX to BMC 02 – MUX to SOL

2.8 Restore default Configuration

This is the AMI command that support to restore the default configurations values.

Linux command:

$ ipmitool raw 0x32 0x66

Description:

NetFn	**0x32 – The AMI NetFn**
Command	0x66

Request Data:

Response Data:

Byte	Data field
1	Completion Code

2.9 Write BMC MAC Address to FRU

This is the AMI command that support to write BMC MAC address to FRU.

Linux command:

```
$ ipmitool raw 0x3c 0x4 0x0 0xB0 0xB1 0xB2 0xB3 0xB4 0xB5
$ ipmitool raw 0x3c 0x4 0x1 0xB0 0xB1 0xB2 0xB3 0xB4 0xB6
```

Description:

NetFn	**0x3c**
Command	0x4

Request Data:

Byte	**Data field**
1	MAC1, MAC2 select: 0x0 – BMC MAC1 0x1 – BMC MAC2
2 – 7	MAC address

Response Data:

Byte	**Data field**
1	Completion Code
2	Written bytes count

2.10 Notify BMC backup component (Deprecated)

This is the command to notify BMC uses the recent component as backup component.

Linux command:

$ ipmitool raw 0x3c 0x09 0x04 (Backup BIOS Component)

$ ipmitool raw 0x3c 0x09 0x20 (Backup BOOTFW Component)

$ ipmitool raw 0x3c 0x09 0x24 (Backup BOTH Component)

Description:

NetFn	**0x3c**
Command	0x09

Request Data:

Byte	**Data field**
1	Component ID (BIOS: 04h, BOOTW: 20h, BOTH: 24h) [7:6] – Reserved [5] – BOOTFW Component (SCP) [4:3] – Reserved [2] – BIOS Component [1:0] – Reserved

Response Data:

Byte	**Data field**
1	Completion Code
2	Requested Component ID
3	Result: 00h: Success 20h: Failed to backup BOOTFW – No BOOTFW Image Found 40h: Failed to backup BOOTFW – No BOOTFW Version Info 04h: Failed to backup BIOS – No

2.11 Select rollback component

As ipmitool hpm rollback feature does not support option to select component to be rollbacked. This command aims to help to select the component to be rollbacked. However, current BMC implementation did not support to rollback both component at the same time. This is a limitation.

Linux command:

$ ipmitool raw 0x3c 0x08 0x04 (Select BIOS Component)

$ ipmitool raw 0x3c 0x08 0x20 (Select BOOTFW Component)

Description:

NetFn	**0x3c**
Command	0x08

Request Data:

Byte	**Data field**
1	Component ID (BIOS: 04h, BOOTW: 20h, BOTH: 24h) [7:6] – Reserved [5] – BOOTFW Component (SCP) [4:3] – Reserved [2] – BIOS Component [1:0] – Reserved

Response Data:

Byte	**Data field**
1	Completion Code
2	Requested Component ID
3	Result: 00h: Success 20h: Failed to select BOOTFW – No BOOTFW Image Found 04h: Failed to select BIOS – No BIOS Image Found

2.12 Clean backup component

This is the command to notify BMC cleans up backup component.

Linux command:

$ ipmitool raw 0x3c 0x0a 0x04 (Clean BIOS backup component)

$ ipmitool raw 0x3c 0x0a 0x20 (Clean BOOTFW backup component)

$ ipmitool raw 0x3c 0x0a 0x24 (Clean both backup component)

Description:

NetFn	**0x3c**
Command	0x0a

Request Data:

Byte	**Data field**

1	Component ID (BIOS: 04h, BOOTW: 20h, BOTH: 24h) [7:6] – Reserved [5] – BOOTFW Component (SCP) [4:3] – Reserved [2] – BIOS Component [1:0] – Reserved

Response Data:

Byte	**Data field**
1	Completion Code
2	Requested Component ID
3	Result: 00h: Success 20h: Failed to clean BOOTFW – No BOOTFW Image Found 04h: Failed to clean BIOS – No BIOS Image Found 24h: Failed to clean BOTH Component

2.13 Disable cooling manager support

This is the command to disable cooling manager support. If this command executes successful, cooling manager will be disabled and fan will start at 100% duty cycle, then user can use pwmtachtool to control fan to expected duty cycle.

Linux command:

$ ipmitool raw 0x3c 0x0b 0x01 (Disable)

$ ipmitool raw 0x3c 0x0b 0x00 (Enable)

Description:

NetFn	**0x3c**
Command	0x0b

Request Data:

Byte	**Data field**
1	01h: Disable 00h: Enable

Response Data:

Byte	**Data field**
1	Completion Code

2	Result: 01h: Disabled 00h: Enabled

2.14 Get cooling manager status

This is the command to get cooling manager support status.

Linux command:

$ ipmitool raw 0x3c 0x0c

Description:

NetFn	**0x3c**
Command	0x0c

Request Data:

Byte	**Data field**
NONE	NONE

Response Data:

Byte	**Data field**
1	Completion Code
2	Result: 01h: Disabled 00h: Enabled

2.15 Set Fault LED Status

This is the command to turn on/off fault led.

Linux command:

$ ipmitool raw 0x3c 0x10

Description:

NetFn	**0x3c**
Command	0x10

Request Data:

Byte	**Data field**

1	Status 01h – Turn on fault led 00h – Turn off fault led (Fault led mask will be automatically set to 0x00 to mask all of errors, user needs to use command 0x12 to set mask to 0xff again so that fault led will works as normal, see detail in command “Set Fault Led Mask”)

Response Data:

Byte	**Data field**
1	Completion Code
2	Status 01h: Fault led is turned on 00h: Fault led is turned off

2.16 Get Fault LED Status

This is the command to get fault led status.

Linux command:

$ ipmitool raw 0x3c 0x11

Description:

NetFn	**0x3c**
Command	0x11

Request Data:

Byte	**Data field**
NONE	NONE

Response Data:

Byte	**Data field**
1	Completion Code
2	Status

2.17 Set Fault LED Mask

This is the command to set fault led mask to enable/disable the error affects fault led.

Linux command:

$ ipmitool raw 0x3c 0x12

Description:

NetFn	**0x3c**
Command	0x12

Request Data:

Byte	Data field
1	Mask Byte 0xFF: Any of below errors will turn on fault led 0x00: Mask all of errors The bit description is below: [7] – PSU Error Mask [6] – Undetermined Error Mask [5] – CPU Fault Mask [4] – Overtemp Mask [3] – Hightemp Mask [2] – DIMM Error Mask [1] – FAN Error Mask [0] – Sensor Error Mask

Response Data:

Byte	Data field
1	Completion Code
2	Mask – The mask is set

2.18 Get Fault LED Mask

This is the command to get fault led mask.

Linux command:

```
$ ipmitool raw 0x3c 0x13
```

Description:

NetFn	**0x3c**
Command	0x13

Request Data:

Byte	Data field
NONE	NONE

Response Data:

Byte	Data field
1	Completion Code
2	Mask [7] – PSU Error Mask [6] – Undetermined Error Mask [5] – CPU Fault Mask [4] – Overtemp Mask [3] – Hightemp Mask [2] – DIMM Error Mask [1] – FAN Error Mask [0] – Sensor Error Mask

2.19 Set Fan Speed

This is the command to set fan pwm duty cycle. User needs to use command 0x0b to disable cooling manager support first so that the fan will not be controlled by thermal algorithm anymore.

Linux command:

```
$ ipmitool raw 0x3c 0x14
```

Description:

NetFn	**0x3c**
Command	0x14

Request Data:

Byte	Data field
1	Fan number 2 - 6: 2U Chassis 2 - 7: 1U Chassis
2	Pwm Duty (0-100)

Response Data:

Byte	Data field
1	Completion Code
2	Result 00h: Success 01h: Invalid fan number

2.20 Get System Error Status

This is the command to get system error status.

Linux command:

$ ipmitool raw 0x3c 0x15

Description:

NetFn	**0x3c**
Command	0x15

Request Data:

Byte	**Data field**
NONE	NONE

Response Data:

Byte	**Data field**
1	Completion Code
2	System Error Status [7] – PSU Error [6] – Undetermined Error [5] – CPU Fault [4] – Overtemp [3] – Hightemp [2] – DIMM Error [1] – FAN Error [0] – Sensor Error

2.21 Get ID LED Status

This is the command to get ID LED status.

Linux command:

$ ipmitool raw 0x3c 0x16

Description:

NetFn	**0x3c**
Command	0x16

Request Data:

Byte	**Data field**

NONE	NONE

Response Data:

Byte	Data field
1	Completion Code
2	Status 01h: LED is currently on 00h: LED is currently off

2.22 Get Riser Mode

This is the command to get riser mode.

Linux command:

```
$ ipmitool raw 0x3c 0x17
```

Description:

NetFn	**0x3c**
Command	0x17

Request Data:

Byte	Data field
1	Riser Num 0x01: Riser 1 0x02: Riser 2

Response Data:

Byte	Data field
1	Completion Code
2	Riser Mode 0Fh: Riser 1 is not available 07h: Riser 2 is not available Others: Riser ID Example: 02h: Riser ID = 0x02

2.23 Get SEP Status Register

This is the command to get psoc status register.

Linux command:

$ ipmitool raw 0x3c 0x18

Description:

NetFn	**0x3c**
Command	0x18

Request Data:

Byte	Data field
1	PSOC NUM 0x00: PSOC 0 (SEP4S/2U or SEP4M/1U) 0x01: PSOC 1 (SEP4M/2U)

Response Data:

Byte	Data field
1	Completion Code
2:12	SEP Status Register (See detail in Item #8.2: SEP Status Register, BP Spec Rev 1.08)

2.24 Get Chassis Type

This command is to get system chassis type (1U/2U).

Linux command:

$ ipmitool raw 0x3c 0x19

Description:

NetFn	**0x3c**
Command	0x19

Request Data:

Byte	Data field
NONE	NONE

Response Data:

Byte	Data field
1	Completion Code

2	Chassis Type 0: 1U chassis 1: 2U chassis

2.25 Enable/Disable SOCFlash Support

This command is to enable/disable socflash support. This command only works with LAN channel and privilege access permission.

Linux command:

$ ipmitool-I lanplus-H <BMCIP>-U <USERNAME>-P <PASSWORD> raw 0x3c 0x20

Description:

NetFn	**0x3c**
Command	0x20

Request Data:

Byte	**Data field**
1	1: Enable 0: Disable

Response Data:

Byte	**Data field**
1	Completion Code
2	Enable/Disable Status: 1: Enabled 0: Disabled

2.26 Get SOCFlash Support Status

This command is to get the socflash support status.

Linux command:

$ ipmitool raw 0x3c 0x21

Description:

NetFn	**0x3c**
Command	0x21

Request Data:

Byte	**Data field**
NONE	NONE

Response Data:

Byte	Data field
1	Completion Code
2	Enable/Disable Status: 1: Enabled 0: Disabled

2.27 Trigger SOL Archive

This command is to trigger SOL archive log so that user can download it via ipmitool/webui.

Linux command:

```
$ ipmitool raw 0x3c 0x22
```

Description:

NetFn	**0x3c**
Command	0x22

Request Data:

Byte	Data field
NONE	NONE

Response Data:

Byte	Data field
1	Completion Code
2	0: Success

2.28 Read PSU Registers

This command is to read PSU registers.

Linux command:

```
$ ipmitool raw 0x3c 0x23
```

Description:

NetFn	**0x3c**
Command	0x23

Request Data:

Byte	Data field
1	PSU Number 1: PSU1 2: PSU2
2	PSU Command Code (See PSU Spec for detail)

Response Data:

Byte	Data field
1	Completion Code
2:N	PSU Register Value (See PSU Spec for detail)

2.29 Write PSU Registers

This command is to write PSU registers.

Linux command:

$ ipmitool raw 0x3c 0x24

Description:

NetFn	0x3c
Command	0x24

Request Data:

Byte	Data field
1	PSU Number 1: PSU1 2: PSU2
2	PSU Command Code (See PSU Spec for detail)
3:N	Data to write

Response Data:

Byte	Data field
1	Completion Code
2	Writing result 0: Success Others: Failure

2.30 Enable/Disable Auto-recovery Support

This command is to enable/disable auto-recovery support.

Linux command:

$ ipmitool raw 0x3c 0x26

Description:

NetFn	**0x3c**
Command	0x26

Request Data:

Byte	Data field
1	1: Enable 0: Disable
2	Component ID 2: BIOS Component 5: SCP Component

Response Data:

Byte	Data field
1	Completion Code
2	Current Enable/Disable Status 1: Enabled 0: Disabled

2.31 Get Auto-recovery Support Status

This command is to get auto-recovery support status.

Linux command:

$ ipmitool raw 0x3c 0x27

Description:

NetFn	**0x3c**
Command	0x27

Request Data:

Byte	Data field

1	Component ID 2: BIOS Component 5: SCP Component

Response Data:

Byte	**Data field**
1	Completion Code
2	Current Enable/Disable Status 1: Enabled 0: Disabled

2.32 Get Component Firmware Version

This command is to get component firmware version.

Linux command:

```
$ ipmitool raw 0x3c 0x28
```

Description:

NetFn	**0x3c**
Command	0x28

Request Data:

Byte	**Data field**
1	Component ID 2: BIOS Component 5: SCP Component

Response Data:

Byte	**Data field**
1	Completion Code
2	Major Version
3	Minor Version

2.33 Write BMC Time (UTC) to RTC

This command is to write bmc time (utc) to rtc.

Linux command:

```
$ ipmitool raw 0x3c 0x29
```

Description:

NetFn	**0x3c**
Command	0x29

Request Data:

Byte	**Data field**
NONE	NONE

Response Data:

Byte	**Data field**
1	Completion Code

2.34 Sync RTC Time (UTC) to BMC

This command is to sync rtc time (utc) to bmc.

Linux command:

```
$ ipmitool raw 0x3c 0x30
```

Description:

NetFn	**0x3c**
Command	0x30

Request Data:

Byte	**Data field**
NONE	NONE

Response Data:

Byte	**Data field**
1	Completion Code

2.35 Get SEP Control Register

This is the command to get psoc control register.

Linux command:

```
$ ipmitool raw 0x3c 0x33
```

Description:

NetFn	**0x3c**
Command	0x33

Request Data:

Byte	**Data field**
1	PSOC NUM 0x00: PSOC 0 (SEP4S/2U or SEP4M/1U) 0x01: PSOC 1 (SEP4M/2U)

Response Data:

Byte	**Data field**
1	Completion Code
2:N	SEP Control Register (See BP Spec for detail)

3. Standard IPMI command

1.1 Lock / Unlock the power button

This is standard IPMI command which used to control to lock or unlock the power button.

Linux command:
$ ipmitool raw 0x0 0xa 0x1

Description:

NetFn	**0x0 – The standard chassis NetFn**
Command	0xa – Set the front panel enable

Request data:

Byte	**Data field**
1	Front Panel Button Enables [7:4] – reserved [3] – 1b = disable Standby (sleep) button for entering standby (sleep) [2] – 1b = disable Diagnosis Interrupt button [1] – 1b = disable reset button [0] – 1b = disable Power off button for power off only (in the case there is a single combined power/standby (sleep) button, then is also disables sleep request via that button)

Response Data:

Byte	**Data field**
1	Completion Code

Appendix C- Terms and Abbreviations

BIOS

Basic Input/Output System

BPS

Bits per second.

CMOS

Complementary Metal Oxide Semiconductor

COM serial port

MS-DOS supports up to four serial ports. The default interrupt for COM1 and COM3 is IRQ4; the default interrupt for COM2 and COM 4 is IRQ3.

CPU

Central Processing Unit

DIMM

Dual In-line Memory Module

DMA

Direct Memory Access; The DMA channel allows certain types of data to be communicated directly between the RAM and device, while bypassing the microprocessor.

DRAM

Dynamic Random Access Memory; RAMs for computers are usually in the form of DRAM chips.

ECC

Error Checking and Correction

EMC

Electromagnetic Compatibility

EMI

Electromagnetic Interference

ESD

Electrostatic Discharge

FAT

File Allocation Table

FTP

File Transfer Protocol

GB

Gigabyte; 1 GB is equivalent to 1024 MB or 1,073,741,824 bytes

HZ

Hertz

I/O

Input/Output

I2O

Intelligent Input/Output

IP

Internet Protocol

IRQ

Interrupt Request; A signal sent to the microprocessor via an IRQ line to inform the later of impending data sending or receipt by peripheral devices.

KB

Kilobytes, equivalent to 1024 bytes.

LAN

Local Area Network

LCD

Liquid Crystal Display

LED

Light Emitting Diode; An electronic device that emits light when a current passes through it.

LUN

Logical Unit Number

MB

Megabytes; Equivalent to 1,048,576 bytes.

MBR

Master Boot Record

MHZ

Megahertz

MTBF

Mean Time Before Failures

NIC

Network Interface Controller

NTFS

NT File System

PCI

Peripheral Component Interconnect

POST

Power-On Self-Test; After booting up and before loading the operating system, POST is performed to examine the various components of the system.

RAM

Random Access Memory Commonly referred to as memory.

ROM

Read-Only Memory

RTC

Real-Time Clock

SDRAM

Synchronous Dynamic Random Access Memory

SMART

Self-Monitoring Analysis and Reporting Technology

SNMP

Simple Network Management Protocol

TCP/IP

Transmission Control Protocol/Internet Protocol

UPS

Uninterrupted Power Supply

USB

Universal Serial Bus