

QuantaGrid Series

S31A-1U

**Compact 1U Server with full feature
User's Guide**

Version: 1.0

Copyright

Copyright © 2015 Quanta Computer Inc. This publication, including all photographs, illustrations and software, is protected under international copyright laws, with all rights reserved. Neither this guide, nor any of the material contained herein, may be reproduced without the express written consent of the manufacturer. All trademarks and logos are copyrights of their respective owners.

Version 1.0 / September 22, 2015

Disclaimer

The information in this document is subject to change without notice. The manufacturer makes no representations or warranties with respect to the contents hereof and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, the manufacturer reserves the right to revise this publication and to make changes from time to time in the content hereof without obligation of the manufacturer to notify any person of such revision or changes.

For the latest information and updates please see www.QCT.io

All the illustrations in this technical guide are for reference only and are subject to change without prior notice.

TABLE OF CONTENT

About the System

Introduction	1-1
Package Contents	1-3
A Tour of the System	1-4
System Overview	1-4
System Front View	1-6
Front Control Panel (FCP)	1-6
System Rear View	1-7
System Rear I/O	1-8
Power Sub-System (Redundant PSU SKU)	1-8
Power Sub-System (Fixed PSU SKU)	1-9
LED Status Definitions	1-9
Front Control Panel LED	1-9
LAN LED	1-10
BMC Management Port LED	1-11
HDD LED	1-11

BIOS

BIOS Setup Utility	2-1
Operation	2-1
Setup Page Layout	2-1
Entering BIOS Setup	2-1
Keyboard Commands	2-2
Menu Selection Bar	2-4
Server Platform Setup Utility Screens	2-4
Main Screen	2-5
Advanced Screen	2-6

Chipset Screen	2-7
Server Management Screen.....	2-8
Boot Options Screen.....	2-9
Security Screen.....	2-11
Exit Screen	2-12
Loading BIOS Defaults	2-14
BIOS Update Utility	2-15
BIOS Update Utility	2-15
AFULNX:.....	2-15
ME Region Update	2-15
BIOS Setting Utility.....	2-16
BIOS Revision	2-16
Clear CMOS	2-19
Clear Password	2-19
Server Management.....	2-20
Console Redirection	2-20
Serial Configuration Settings	2-20
Keystroke Mapping	2-20
Reset	2-21
Limitations	2-21
Interface to Server Management (Optional)	2-22
Network BIOS Support.....	2-22
PXE Boot.....	2-22
Checkpoints.....	2-22
Standard Checkpoint.....	2-22
ACPI/ASL Checkpoints	2-28
OEM-Reserved Checkpoint Ranges	2-28

BMC

Server Management Software	3-1
Server System Overview	3-1

BMC Key Features and Functions.....	3-1
Power System	3-1
Front Panel User Interface	3-2
Power Button	3-2
ID Button	3-2
LEDs.....	3-2
LAN Interface.....	3-2
Session and User.....	3-3
Serial Over LAN.....	3-3
Time Sync.....	3-3
SEL	3-3
Platform Event	3-3
Platform Event Filter	3-3
BMC Firmware Update.....	3-4
DOS Recovery Utility	3-4
WebUI Update	3-4
BMC Recovery.....	3-5
Recovery Process in DOS System.....	3-5
Recovery Process in Linux System.....	3-5
Recovery Process in Windows System	3-5
SMASH.....	3-6
System Level Commands.....	3-7
BMC Information.....	3-10
Web Graphical User Interface (GUI) for ESMS	3-12
Using the Web GUI	3-12
Login	3-12
Dashboard	3-13
Device Information	3-14
Network Information.....	3-15
Sensor Monitoring	3-15
Event Logs.....	3-16

Server Information	3-16
FRU Information.....	3-16
Server Component.....	3-18
Server identify	3-19
BIOS POST Code	3-20
Server Health Group	3-20
Sensor Readings	3-21
Event Log.....	3-23
Configuration Group	3-26
Active Directory.....	3-26
DNS	3-30
LDAP/E-Directory	3-34
Mouse Mode.....	3-37
Network	3-39
PEF	3-42
RADIUS	3-50
Remote Session.....	3-52
SMTP	3-53
SOL.....	3-56
SSL	3-57
User Management	3-62
Virtual Media	3-66
Services	3-67
LAN Port Settings	3-70
Remote Control	3-70
Console Redirection.....	3-71
Server Power Control	3-82
Java SOL.....	3-83
Maintenance Group	3-85
Preserve Configuration.....	3-86
Restore Factory Defaults	3-88
Firmware Update.....	3-89
BMC Firmware Update	3-89

BIOS Update	3-96
Log Out	3-96
User Privilege	3-96

Regulatory and Compliance Information

Electromagnetic Compatibility Notices.....	4-1
FCC Verification Statement (USA)	4-1
Europe (CE Declaration of Conformity)	4-1
VCCI (Japan).....	4-1
BSMI (Taiwan)	4-1
Regulated Specified Components.....	4-2
Restriction of Hazardous Substances (RoHS) Compliance	4-2
End of Life / Product Recycling.....	4-2
Product Regulatory Compliance Markings.....	4-3

Conventions

Several different typographic conventions are used throughout this manual. Refer to the following examples for common usage.

Bold type face denotes menu items, buttons and application names.

Italic type face denotes references to other sections, and the names of the folders, menus, programs, and files.

<Enter> type face denotes keyboard keys.

.Warning information appears before the text it references and should not be ignored as the content may prevent damage to the device.



WARNING!

Warning information appears before the text it references and should not be ignored as the content may prevent damage to the device.



CAUTION!

CAUTIONS APPEAR BEFORE THE TEXT IT REFERENCES, SIMILAR TO NOTES AND WARNINGS. CAUTIONS, HOWEVER, APPEAR IN CAPITAL LETTERS AND CONTAIN VITAL HEALTH AND SAFETY INFORMATION.

Note:

Highlights general or useful information and tips.

Precautionary Measures

Read all caution and safety statements in this document before performing any of the instructions. To reduce the risk of bodily injury, electrical shock, fire, and equipment damage, read and observe all warnings and precautions in this chapter before installing or maintaining your system. To avoid personal injury or property damage, before you begin installing the product, read, observe, and adhere to all of the following instructions and information. The following symbols may be used throughout this guide and may be marked on the product and / or the product packaging.

Safety Instructions about your system

In the event of a conflict between the information in this guide and information provided with the product or on the website for a particular product, the product documentation takes precedence.

Your system should be integrated and serviced only by technically qualified persons.

You must adhere to the guidelines in this guide and the assembly instructions in related chapters to ensure and maintain compliance with existing product certifications and approvals. Use only the described, regulated components specified in this guide. Use of other products / components will void the UL Listing and other regulatory approvals of the product, and may result in noncompliance with product regulations in the region(s) in which the product is sold.

Table 1: Warning and Cautions







CAUTION	Indicates the presence of a hazard that may cause minor personal injury or property damage if the CAUTION is ignored.
WARNING	Indicates the presence of a hazard that may result in serious personal injury if the WARNING is ignored.
	Indicates potential hazard if indicated information is ignored.
	Indicates shock hazards that result in serious injury or death if safety instructions are not followed.
	Indicates hot components or surfaces.
	Indicates do not touch fan blades, may result in injury.
	Remove the system from the rack to disconnect power system.

Table 1: Warning and Cautions (Continued)

	The enclosure is designed to carry only the weight of the system sled. Do not use this equipment as a workspace. Do not place additional load onto any equipment in this system.
	Indicates two people are required to safely handle the system.
	<p>Restricted Access Location: The system is intended for installation only in a Server Room or Computer Room where both these conditions apply:</p> <ul style="list-style-type: none"> • access can only be gained by SERVICE PERSONS or by USERS who have been instructed about the reasons for the restrictions applied to the location and about any precautions that shall be taken; and • access is through the use of a TOOL or lock and key, or other means of security, and is controlled by the authority responsible for the location.

Intended Application Uses

This product was evaluated as Information Technology Equipment (ITE), which may be installed in offices, schools, computer rooms, and similar commercial type locations. The suitability of this product for other product categories and environments (such as medical, industrial, residential, alarm systems, and test equipment), other than an ITE application, may require further evaluation.

Site Selection

The system is designed to operate in a typical office environment. Choose a site that is:

- Clean, dry, and free of airborne particles (other than normal room dust).
- Well-ventilated and away from sources of heat including direct sunlight and radiators.
- Away from sources of vibration or physical shock.
- Isolated from strong electromagnetic fields produced by electrical devices.
- In regions that are susceptible to electrical storms, we recommend you plug your system into a surge suppressor and disconnect telecommunication lines to your modem during an electrical storm.
- Provided with a properly grounded wall outlet.
- Provided with sufficient space to access the power system, because they serve as the product's main power disconnect.
- Provided with either two independent DC power system or two independent phases from a single power system.

Equipment Handling Practices

Reduce the risk of personal injury or equipment damage:

- Conform to local occupational health and safety requirements when moving and lifting equipment.
- Use mechanical assistance or other suitable assistance when moving and lifting equipment.
- To reduce the weight for easier handling, remove any easily detachable components.
- Never lift or move your system solely by the handle on the component.

Power and Electrical Warnings



CAUTION!

MAKE SURE THE SYSTEM IS REMOVED FROM THE RACK BEFORE SERVICING ANY NON-HOT PLUG COMPONENTS. THE BUS BAR CLIPS MUST BE DISCONNECTED FROM THE POWER SYSTEM IN ORDER TO FULLY SEPARATE THE SYSTEM FROM THE POWER SOURCE.



CAUTION!

TO AVOID RISK OF ELECTRIC SHOCK, DISCONNECT ALL CABLING FROM THE SYSTEM AND REMOVE THE SYSTEM FROM THE RACK.

System Access Warnings



CAUTION!

TO AVOID PERSONAL INJURY OR PROPERTY DAMAGE, THE FOLLOWING SAFETY INSTRUCTIONS APPLY WHENEVER ACCESSING THE INSIDE OF THE PRODUCT:

- Disconnect from the power source by removing the system from the rack.
- Disconnect all cabling running into the system.
- Retain all screws or other fasteners when servicing. Upon completion servicing, secure with original screws or fasteners.



CAUTION!

IF THE SERVER HAS BEEN RUNNING, ANY INSTALLED HDD MODULES MAY BE HOT.



CAUTION!

UNLESS YOU ARE ADDING OR REMOVING A HOT-PLUG COMPONENT, ALLOW THE SYSTEM TO COOL BEFORE SERVICING.



CAUTION!

TO AVOID INJURY DO NOT CONTACT MOVING FAN BLADES. IF YOUR SYSTEM IS SUPPLIED WITH A GUARD OVER THE FAN, DO NOT OPERATE THE SYSTEM WITHOUT THE FAN GUARD IN PLACE.

Rack Mount Warnings

The following installation guidelines are required by UL for maintaining safety compliance when installing your system into a rack.

The equipment rack must be anchored to an unmovable support to prevent it from tipping when your system or piece of equipment is extended from it. The equipment rack must be installed according to the rack manufacturer's instructions.

Install equipment in the rack from the bottom up, with the heaviest equipment at the bottom of the rack.

Extend only one piece of equipment from the rack at a time.

You are responsible for installing a main power disconnect for the entire rack unit. This main disconnect must be readily accessible, and it must be labeled as controlling power to the entire unit, not just to the system(s).

To avoid risk of potential electric shock, a proper safety ground must be implemented for the rack and each piece of equipment installed in it.

Elevated Operating Ambient - If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum ambient temperature (T_{ma}) specified by the manufacturer.

Reduced Air Flow - Installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised.

Mechanical Loading - Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.

Circuit Overloading - Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of the circuits might have on over-current protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.

Reliable Earthing - Reliable earthing of rack-mounted equipment should be maintained.

Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g. use of power strips).

Electrostatic Discharge (ESD)



CAUTION!

ESD CAN DAMAGE DRIVES, BOARDS, AND OTHER PARTS. WE RECOMMEND THAT YOU PERFORM ALL PROCEDURES AT AN ESD WORKSTATION. IF ONE IS NOT AVAILABLE, PROVIDE SOME ESD PROTECTION BY WEARING AN ANTI-STATIC WRIST STRAP ATTACHED TO CHASSIS GROUND -- ANY UNPAINTED METAL SURFACE -- ON YOUR SERVER WHEN HANDLING PARTS.

Always handle boards carefully. They can be extremely sensitive to ESD. Hold boards only by their edges without any component and pin touching. After removing a board from its protective wrapper or from the system, place the board component side up on a grounded, static free surface. Use a conductive foam pad if available but not the board wrapper. Do not slide board over any surface.

Cooling and Airflow



CAUTION!

CAREFULLY ROUTE CABLES AS DIRECTED TO MINIMIZE AIRFLOW BLOCKAGE AND COOLING PROBLEMS. FOR PROPER COOLING AND AIRFLOW, OPERATE THE SYSTEM ONLY WITH THE CHASSIS COVERS* / AIR DUCT INSTALLED. OPERATING THE SYSTEM WITHOUT THE COVERS / AIR DUCT IN PLACE CAN DAMAGE SYSTEM PARTS . TO INSTALL THE COVERS* / AIR DUCT:

- Check first to make sure you have not left loose tools or parts inside the system.
- Check that cables, add-in cards, and other components are properly installed.

Attach the covers* / air duct to the chassis according to the product instructions.

* May not apply to all systems.

Please be aware that slots and openings on the front and rear side of the chassis are designed for ventilation; to make sure reliable operation of your system and to protect it from overheating, these openings must not be covered or blocked. The openings should never be covered or blocked by placing the product on a bed, sofa, rug, or other similar surface. This product should never be placed near or over a radiator or heat register, or in a built-in installation unless proper ventilation is provided.

Laser Peripherals or Devices



CAUTION!

TO AVOID RISK OF RADIATION EXPOSURE AND / OR PERSONAL INJURY:

- Do not open the enclosure of any laser peripheral or device.
- Laser peripherals or devices are not serviceable.
- Return to manufacturer for servicing.

Use certified and rated Laser Class I for Optical Transceiver product.

Heed safety instructions: Before working with the system, whether using this manual or any other resource as a reference, pay close attention to the safety instructions. Adhere to the assembly instructions in this manual to ensure and maintain compliance with existing product certifications and approvals. Use only the described, regulated components spec-

ified in this manual. Use of other products / components will void the UL listing and other regulatory approvals of the product and will most likely result in non-compliance with product regulations in the region(s) in which the product is sold.

System power on/off: To remove power from system, you must remove the system from rack. Make sure the system is removed from the rack before opening the chassis, adding, or removing any non hot-plug components.

Hazardous conditions, devices and cables: Hazardous electrical conditions may be present on power, telephone, and communication cables. Turn off the system and disconnect the cables attached to the system before opening it. Otherwise, personal injury or equipment damage can result.

Electrostatic discharge (ESD) and ESD protection: ESD can damage drives, boards, and other parts. We recommend that you perform all procedures in this chapter only at an ESD workstation. If one is not available, provide some ESD protection by wearing an antistatic wrist strap attached to chassis ground any unpainted metal surface on the server when handling parts.

ESD and handling boards: Always handle boards carefully. They can be extremely sensitive to electrostatic discharge (ESD). Hold boards only by their edges. After removing a board from its protective wrapper or from the server, place the board component side up on a grounded, static free surface. Use a conductive foam pad if available but not the board wrapper. Do not slide board over any surface.

Installing or removing jumpers: A jumper is a small plastic encased conductor that slips over two jumper pins. Some jumpers have a small tab on top that can be gripped with fingertips or with a pair of fine needle nosed pliers. If the jumpers do not have such a tab, take care when using needle nosed pliers to remove or install a jumper; grip the narrow sides of the jumper with the pliers, never the wide sides. Gripping the wide sides can damage the contacts inside the jumper, causing intermittent problems with the function controlled by that jumper. Take care to grip with, but not squeeze, the pliers or other tool used to remove a jumper, or the pins on the board may bend or break.

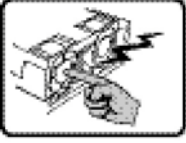
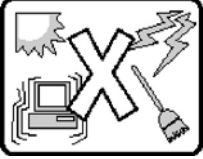


General Information

The information about rack and the wording “rack” in this guide supports the organization of Open Compute definition.

The term *Rack* as found in this guide refers to the term *Rack* or *Open Rack* as described and used in the Open Compute Project definition.

Before servicing this system, it is recommended to read this technical guide completely to be aware of any safety issues or requirements involved in the servicing of this system.

Assembly Safety Guidelines

	<p>The power system in this product contains no user-serviceable parts. Refer servicing only to qualified personnel.</p>
	<p>The system is designed to operate in a typical office environment. Choose a site that is:</p> <ul style="list-style-type: none"> • Clean and free of airborne particles (other than normal room dust). • Well ventilated and away from sources of heat including direct sunlight. • Away from sources of vibration or physical shock. • Isolated from strong electromagnetic fields produced by electrical devices. • In regions that are susceptible to electrical storms, we recommend you plug your system into a surge suppressor and disconnect telecommunication lines to your modem during an electrical storm. • Provided with a properly grounded wall outlet. • Provided with sufficient space to access the power system, because they serve as the product's main power disconnect.
	<p>WARNING!</p> <p>The system is safety certified as rack-mounted equipment for use in a server room or computer room, using an approved customer rack. The enclosure is designed to carry only the weight of the system sled. Do not place additional load onto any equipment.</p>
	<p>Heavy object. Indicates two people are required to safely handle the system.</p>

Structure of this guide

- Chapter 1: About the System

“This section introduces the system, its different configuration(s) and the main features.”

- Chapter 2: BIOS

“This section provides information regarding the BIOS architecture, BIOS update utility, server management, checkpoints, and error handling found in the system.”

- Chapter 3: BMC

“This section provides information and key features of BMC (Baseboard Management Controller).”

- Chapter 4: Regulatory and Compliance Information

“This section provides regulatory and compliance information applicable to this system.”

About the System

Chapter 1

This section introduces the system, its different configuration(s) and the main features.

1.1 Introduction

System Features

The QuantaGrid S31A-1U with four 3.5" HDD is available in two models, a fixed PSU model and a redundant PSU model. The compact 1U server is built on the Intel® C236 chipset, featuring the Intel® Xeon® processor E3-1200 v5.

The system is optimized for the dedicated hosting, front-end web, content delivery networks (CDN), and cloud computing applications..

- Greener and More Powerful

Powered by the Intel® Xeon® processor E3-1200 v5 product family and DDR4 memory technology, the QuantaGrid S31A-1U allows owners to upgrade computing performance without overextending power consumption. With Quanta's enhanced thermal design, the server can operate under ambient temperatures as high as 40°C. This allows owners to save unnecessary costs associated with datacenter cooling needs and achieve higher data center infrastructure efficiency (DCIE) value.

- Flexible and Scalable I/O options

QuantaGrid S31A-1U provides flexible I/O scalability for today's diverse data center application requirements. It features OCP LAN mezzanine card solutions in addition to dual GbE or 10GbE LAN on motherboards (LoM). The onboard SAS controller offers multiple QCT SAS mezzanine card options with different RAID levels and data transfer bandwidth so customers can tailor the SAS controller for specific application needs.

Specifications

Table 1.1: System Specifications

SPECIFICATIONS	DESCRIPTION
Form factor	1U rack mount
Chassis dimensions (W x H x D)	17.24 x 1.7 x 24 inches 438 x 43.2 x 609.6 mm
Processor	Processor type: Intel® Xeon® processor E3-1200 v5 product family Max. TDP support: 80W Number of processor: 1 Last Level Cache (LLC): Up to 8 MB
Chipset	Intel® C236
Memory	Total slots: 4 Capacity: Up to 64GB ECC UDIMM Memory type: 2133 MHz DDR4 ECC UDIMM Memory size: 16 GB, 8 GB, 4GB ECC UDIMM

Table 1.1: System Specifications (Continued)

SPECIFICATIONS	DESCRIPTION
Storage controller	Onboard (Intel® C236): <ul style="list-style-type: none"> 2 mini-SAS HD connectors supporting 8x SATA 6Gb/s ports 2x M.2 connector supporting SATA or PCIe SSD Optional controller: <ul style="list-style-type: none"> Please refer to our Compatible Component List for more information
Networking	LOM: <ul style="list-style-type: none"> 2x Intel® I210 GbE port Dedicated GbE management port Optional NIC: <ul style="list-style-type: none"> Please refer to our Compatible Component List for more information
Expansion slot	Riser <ul style="list-style-type: none"> PCIe Expansion Card Riser: One x 8 PCIe 3.0, Low profile MD-2 QCT mezzanine Riser: One x8 PCIe 3.0, SAS mezzanine slot OCP mezzanine slot <ul style="list-style-type: none"> One x8 PCIe 3.0 slot
Storage	<ul style="list-style-type: none"> 4x 3.5" hot-plug SAS/SATA HDD/SSD 2x 2.5" internal SATA SSD
Onboard storage	2x M.2 SSD (SATA or PCIe)
Video	Integrated Aspeed AST2400 with 8MB DDR3 video memory
Front I/O	<ul style="list-style-type: none"> Power/ID/Reset Buttons LAN/HDD/Status/ID LEDs 2x USB 2.0 ports
Rear I/O	<ul style="list-style-type: none"> 2x USB 3.0 ports 1x VGA port 1x RS232 serial port 2x GbE RJ45 port 1x GbE RJ45 management port 1x ID button with LED
TPM	Yes (optional)
Power supply	SKU1: 1+1 redundant hot-plug PSU, 80 Plus Platinum <ul style="list-style-type: none"> 3Y 700W 100-240Vac, 50-60Hz, 10-5A 3Y 400W 100-240Vac, 50-60Hz, 6-3A Acbel 700W 100-127/200-240Vac, 50/60Hz, 9.5/5A Acbel 400W 100-127/200-240Vac, 50/60Hz, 6/3A SKU2: 1x fixed PSU, 80 Plus Platinum
Rating (per PSU inlet)	100-127/200-240Vac, 50/60Hz, 4/2A
Fan	3x dual rotor fans (5+1 redundant)
System management	IPMI v2.0 Compliant, on board "KVM over IP" support
Operating environment	<ul style="list-style-type: none"> Operating temperature: 5°C to 40°C (41°F to 104°F) Non-operating temperature: -40°C to 70°C (-40°F to 158°F) Operating relative humidity: 50% to 85%RH. Non-operating relative humidity: 20% to 90%RH

1.2 Package Contents

- (1) S31A-1U system
- (1) processor heat sink
- (1) power supply unit
- (1) power cord (optional)
- (1) utility CD (This Guide included)
- (1) rail kit

Note:

Note: For exact shipping contents, contact your sales representative.

1.3 A Tour of the System

System Overview

The server is available as a redundant PSU (SKU1) and fixed PSU (SKU2) configuration.

The redundant PSU SKU configuration system overview is displayed in the following image:

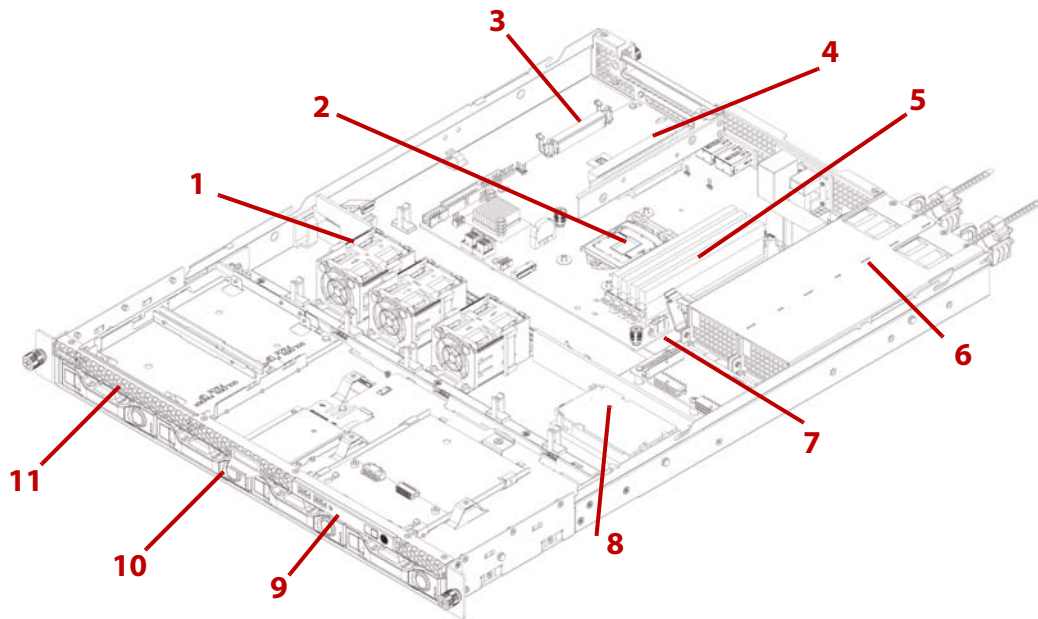


Figure 1-1. Redundant PSU System (SKU1) Component Overview

The fixed PSU configuration system overview is displayed in the following image:

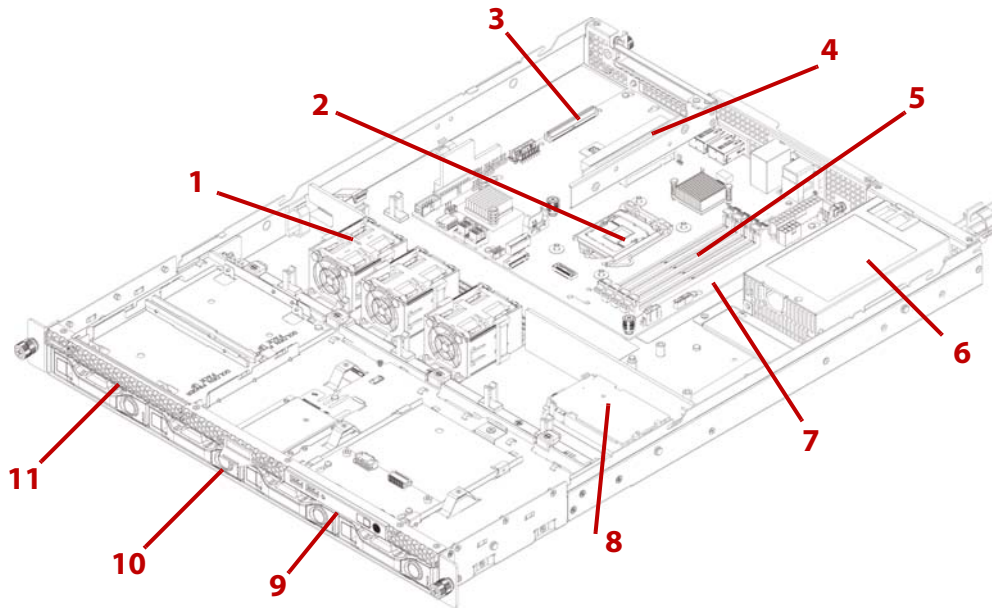


Figure 1-2. Fixed PSU System (SKU2) Component Overview

Table 2: Component Overview

No.	ITEM	DESCRIPTION
1	Fan module	(3) System fan modules
2	CPU socket	LGA 1151 socket
3	OCP mezz slot	Support OCP mezzanine card, PCIe x8, Gen 3.0
4	Riser assembly	<ul style="list-style-type: none"> Support PCIe expansion card, PCIe x 8, Gen 3.0 Support QCT SAS mezzanine card, PCIe x 8, Gen 3.0
5	DIMM slots	(4) DDR4 DIMM slots
6	PSU assembly	<ul style="list-style-type: none"> SKU1: Redundant power supply unit assembly SKU2: Fixed power supply unit assembly
7	Mainboard	System mainboard
8	Backup battery	Backup battery for SAS mezzanine card
9	Front control panel	See <i>Front Control Panel (FCP)</i> on page 1-6
10	HDD assembly	4 x 3.5" SAS/SATA hard disk drive assemblies
11	SSD assembly	2 x solid state disk drive assemblies.

System Front View

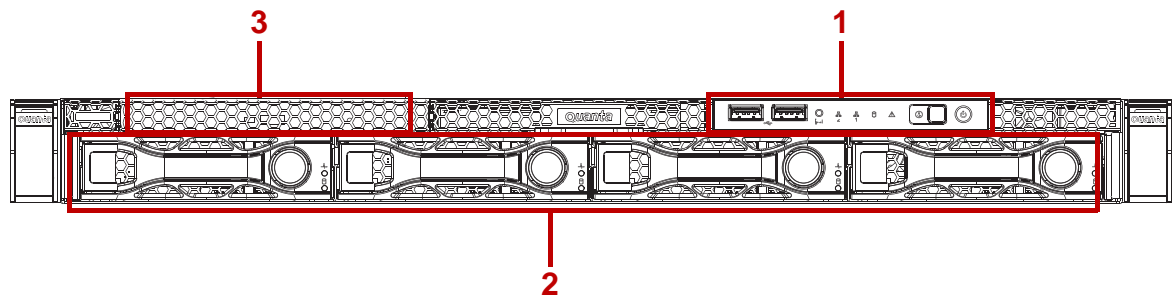


Figure 1-3. System Front View

Table 3: Front Panel View

No.	NAME	DESCRIPTION
1	Front control panel	See <i>Front Control Panel LED</i> on page 1-9 for further information.
2	HDD bays	4 x 3.5" SAS/SATA HDD
3	SSD tray	2 x SSD

Front Control Panel (FCP)

For purposes of this procedure, the FCP is used for the numbering indicators.

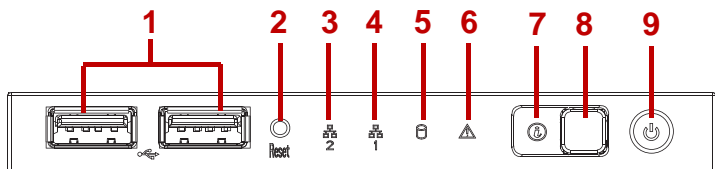




Figure 1-4. Front Control Panel

Table 4: Front Control Panel Definition

No.	ICON	NAME	DESCRIPTION
1		USB ports	USB ports 1 & 2
2		Reset button	Soft reset system function
3		LAN2 LED	LAN access
4		LAN1 LED	LAN access
5		HDD activity LED	Hard disk drive access
6		Fault LED	Provides critical and non-critical failure notification

Table 4: Front Control Panel Definition (Continued)

No.	ICON	NAME	DESCRIPTION
7		Identification LED	Activate ID LED to identify system
8		ID button	Toggles ID LED
9		Power button	Power on / off

System Rear View

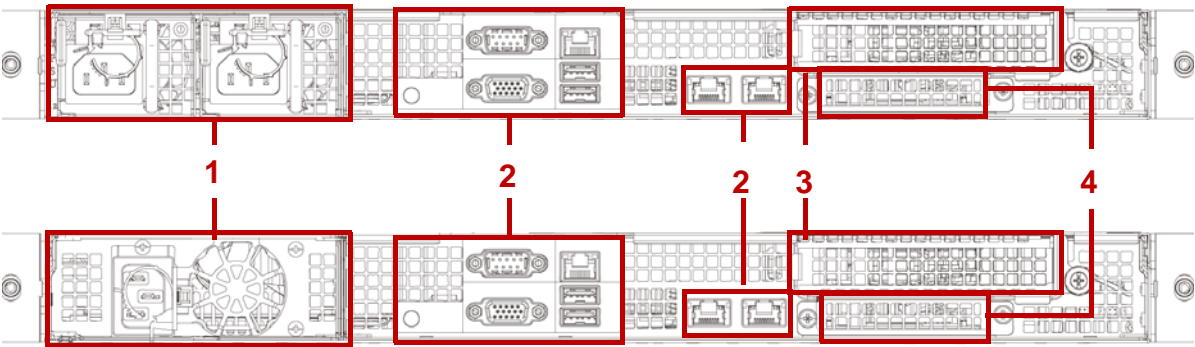


Figure 1-5. System Rear View

Table 5: System Rear View

No.	FEATURE	DESCRIPTION
1	Power sub-system	Upper: Redundant power supply unit. Bottom: Fixed power supply unit. See <i>Power Sub-System (Redundant PSU SKU)</i> on page 1-8.
2	System I/O ports	See <i>System Rear I/O</i> on page 1-8
3	Expansion slot	PCIe expansion slot with PCIe x8 signal
4	OCP mezzanine slot	Support OCP mezzanine card with PCIe x 8 signal

System Rear I/O

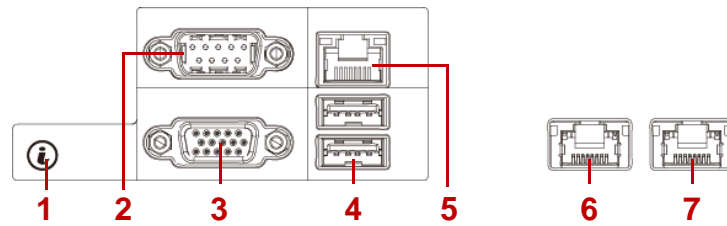


Figure 1-6. System Rear I/O

Table 6: System Rear I/O Definition

No.	ICON	NAME	DESCRIPTION
1		ID button with LED	Toggle the identification when pressing
2		COM port	DB9 port for debug or terminal concentrator
3		VGA connector	Maximum display resolution: 1920x1200 32bpp@60Hz (reduced blanking)
4		USB ports	USB 3.0 ports
5		Dedicated NIC	Dedicated RJ45 connector
6		LAN2	RJ45 connector featuring share NIC
7		LAN1	RJ45 connector

Power Sub-System (Redundant PSU SKU)

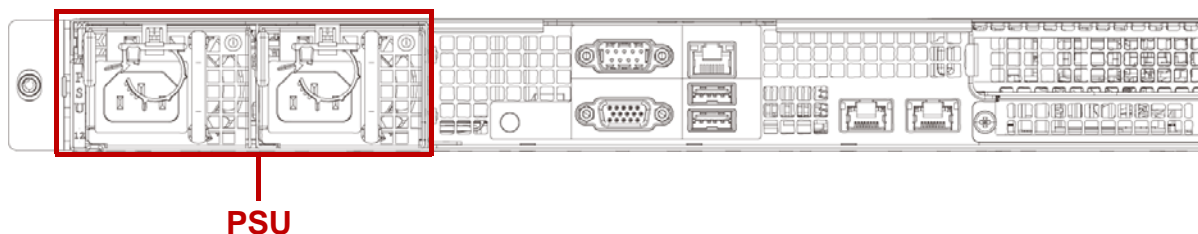


Figure 1-7. Redundant PSU to Mainboard Module Description

A single power supply unit (default) and power distribution board (PDB) are supplied in the system. A secondary PSU is available for redundancy functionality.

Table 7: Power Supply Units by Model

PSU	AC INPUT
2 x 400W high efficiency redundant PSU	100-240V AC 50/60Hz

Power Sub-System (Fixed PSU SKU)

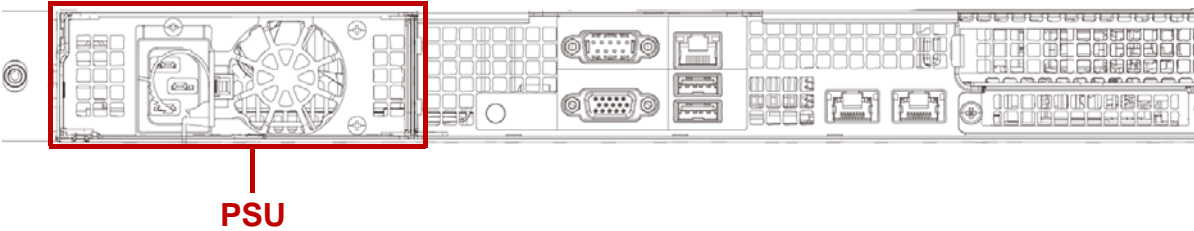


Figure 1-8. Fixed PSU to Mainboard Module Description

A fixed power supply unit is supplied in the system.

Table 8: Power Supply Units by Model

PSU	AC INPUT
1 x 400W high efficiency PSU	100-240V AC 50/60Hz

LED Status Definitions

Front Control Panel LED

For further information and location of the FCP LEDs, see *Front Control Panel LED* on page 1-9.

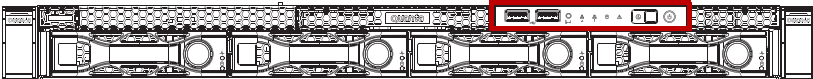


Figure 1-9. System Front Control Panel LEDs

Table 9: Front Control Panel LED Behavior

NAME	COLOR	CONDITION	DESCRIPTION
Power LED	Blue	On	System power on
		Off	System power off
Identification	Blue	Blinking	Unit selected for identification
		Off	No identification request

Table 9: Front Control Panel LED Behavior (Continued)

NAME	COLOR	CONDITION	DESCRIPTION
Fault LED	Amber	Blinking	Critical Failure: critical fan, voltage, temperature state.
			Non-Critical Failure: non-critical fan, voltage, temperature state, CPU thermal trip, DC off.
		Off	SEL cleared
			Last pending warning or error has been de-asserted.
HDD activity	Blue	Blinking	Hard disk drive access (only on board SATA port)
		Off	No access (non-SAS)
LAN1 LED	Blue	On	Link
		Blinking	LAN access (off when there is traffic)
LAN2 LED	Blue	On	Link
		Blinking	LAN access (off when there is traffic)

LAN LED

The system mainboard includes dual GbE network with GbE dedicated management port. Each RJ45 connector has two built-in LEDs. See the following illustration and table for details.

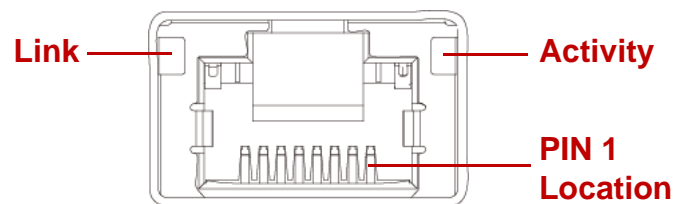


Figure 1-10. RJ45 LAN Connector

Table 10: RJ45 LED Description

CONDITION	LINK	ACTIVITY
Unplugged	Off	Off
1G active link	On amber	Blinking green
100M active link	On green	Blinking green
10M active link	Off	Blinking green

BMC Management Port LED

The system mainboard includes GbE dedicated management port. The RJ45 connector has two built-in LEDs. See the following illustration and table for details.

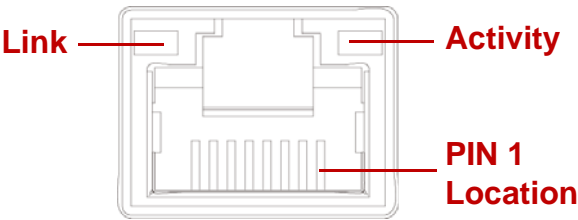


Figure 1-11. RJ45 LAN Connector

Table 11: RJ45 LED Description

CONDITION	LINK	ACTIVITY
Unplugged	Off	Off
1G active link	On amber	Blinking green
100M active link	On green	Blinking green
10M active link	Off	Blinking green

HDD LED

The following LED behavior table represents LED conditions when a driver is online and the slot is not empty.

Table 12: HDD LED Status Behavior

ICON	NAME	COLOR	CONDITION	DESCRIPTION
	HDD Present	Blue	On	Drive is online
	HDD Fault	Amber	On	HDD failure
	HDD Access	Blue	Blinking	HDD access is active
			Off	No access

* Only support SATA/SAS HDD/SSD.

BIOS

Chapter 2

This section provides information regarding the BIOS architecture, BIOS update utility, server management, checkpoints, and error handling found in the system.

2.1 BIOS Setup Utility

The BIOS Setup utility is provided to perform system configuration changes and to display current settings and environment information.

The BIOS Setup utility stores configuration settings in system non-volatile storage. Changes affected by BIOS Setup will not take effect until the system is rebooted. The BIOS Setup Utility can be accessed during POST by using the <**DEL**> or <**F2**> key.

The following sections describe the look and behavior for platform Setup.

Operation

BIOS Setup has the following features:

- The server board BIOS will only be available in English.
- BIOS Setup is functional via console redirection over various terminal emulation standards. This may limit some functionality for compatibility, e.g., usage of colors, some keys or key sequences, or support of pointing devices.

Setup Page Layout

The setup page layout is sectioned into functional areas. Each occupies a specific area of the screen and has dedicated functionality. The following table lists and describes each functional area.

Table 1: BIOS Setup Page Layout

FUNCTIONAL AREA	DESCRIPTION
Title Bar	The title bar is located at the top of the screen and displays the title of the form (page) the user is currently viewing. It may also display navigational information.
Setup Item List	The Setup Item List is a set of controllable and informational items. Each item in the list occupies the left column of the screen. A Setup Item may also open a new window with more options for that functionality on the board.
Item Specific Help Area	The Item Specific Help area is located on the right side of the screen and contains help text for the highlighted Setup Item. Help information may include the meaning and usage of the item, allowable values, effects of the options, etc.
Keyboard Command Bar	The Keyboard Command Bar is located at the bottom right of the screen and continuously displays help for keyboard special keys and navigation keys.

Entering BIOS Setup

BIOS Setup is started by pressing <**DEL**> or <**F2**> during boot time when the OEM (Quanta) logo is displayed.

When Quiet Boot is disabled, the message “press or <F2> to enter setup” will be displayed on the diagnostics screen.

Keyboard Commands

The bottom right portion of the Setup screen provides a list of commands that are used to navigate through the Setup utility. These commands are displayed at all times.

Each Setup menu page contains a number of features. Except those used for informative purposes, each feature is associated with a value field. This field contains user-selectable parameters. Depending on the security option chosen and in effect by the password, a menu feature's value may or may not be changeable. If a value is non-changeable, the feature's value field is inaccessible and displays as "grayed out."

Table 2: Keyboard Commands

KEY	OPTION	DESCRIPTION
<Enter>	Execute Command	The <Enter> key is used to activate sub-menus when the selected feature is a sub-menu, or to display a pick list if a selected option has a value field, or to select a sub-field for multi-valued features like time and date. If a pick list is displayed, the <Enter> key will select the currently highlighted item, undo the pick list, and return the focus to the parent menu.
<Esc>	Exit	The <Esc> key provides a mechanism for backing out of any field. When the <Esc> key is pressed while editing any field or selecting features of a menu, the parent menu is re-entered. When the <Esc> key is pressed in any sub-menu, the parent menu is re-entered. When the <Esc> key is pressed in any major menu, the exit confirmation window is displayed and the user is asked whether changes can be discarded. If “No” is selected and the <Enter> key is pressed, or if the <Esc> key is pressed, the screen is returned to the one before pressing the <Esc> key, without affecting any existing any settings. If “Yes” is selected and the <Enter> key is pressed, setup is exited and the BIOS returns to the main System Options Menu screen.
↑	Select Item	The up arrow is used to select the previous value in a pick list, or the previous option in a menu item's option list. The selected item must then be activated by pressing the <Enter> key.
↓	Select Item	The down arrow is used to select the next value in a menu item's option list, or a value field's pick list. The selected item must then be activated by pressing the <Enter> key.
←→	Select Menu	The left and right arrow keys are used to move between the major menu pages. The keys have no affect if a sub-menu or pick list is displayed.
<Tab>	Select Field	The <Tab> key is used to move between fields. For example, <Tab> can be used to move from hours to minutes in the time item in the main menu.

Table 2: Keyboard Commands (Continued)

KEY	OPTION	DESCRIPTION
-	Change Value	The minus key on the keypad is used to change the value of the current item to the previous value. This key scrolls through the values in the associated pick list without displaying the full list.
+	Change Value	The plus key on the keypad is used to change the value of the current menu item to the next value. This key scrolls through the values in the associated pick list without displaying the full list. On 106-key Japanese keyboards, the plus key has a different scan code than the plus key on the other keyboard, but will have the same effect.
k	Scroll Bar	The k key is used to scroll up in the item specific help area. The scroll bar keys have no affect if help string was not longer than the maximum allocated space in item specific help area.
m	Scroll Bar	The m key is used to scroll down in the item specific help area. The scroll bar keys have no affect if help string was not longer than the maximum allocated space in item specific help area.
<F8>	Previous Values	<p>Pressing <F8> causes the following to appear:</p> <div data-bbox="715 913 1265 1057" data-label="Form"> <p>Load Optimized Defaults?</p> <p>Yes No</p> </div> <p>If Yes is highlighted and <Enter> is pressed, all Setup fields are set to their previous values. If No is highlighted and <Enter> is pressed, or if the <Esc> key is pressed, the screen is returned to the one before <F8> was pressed without affecting any existing field values</p>
<F9>	Setup Defaults	<p>Pressing <F9> causes the following to appear:</p> <div data-bbox="715 1301 1265 1444" data-label="Form"> <p>Load Optimized Defaults?</p> <p>Yes No</p> </div> <p>If Yes is highlighted and <Enter> is pressed, all Setup fields are set to their default values. If No is highlighted and <Enter> is pressed, or if the <Esc> key is pressed, the screen is returned to the one before <F9> was pressed without affecting any existing field values</p>
<F10>	Save and Exit	<p>Pressing <F10> causes the following message to appear:</p> <div data-bbox="715 1688 1265 1832" data-label="Form"> <p>Save configuration and exit?</p> <p>Yes No</p> </div> <p>If Yes is highlighted and <Enter> is pressed, all changes are saved and Setup is exited. If No is highlighted and <Enter> is pressed, or the <Esc> key is pressed, the screen is returned to the one before <F10> was pressed without affecting any existing values.</p>

Menu Selection Bar

The Menu Selection Bar is located at the top of the BIOS Setup Utility screen. It displays the major menu selections available to the user. By using the left and right arrow keys, the user can select the menus listed here.

Server Platform Setup Utility Screens

The sections below describe the screens available for the configuration of a server platform. In these sections, tables are used to describe the contents of each screen. These tables follow the following guidelines:

- The text and values in the Setup Item, Options, and Help columns in the tables are displayed on the BIOS Setup screens.
- **Bold text** in the Options column of the tables indicates default values. These values are not displayed in bold on the setup screen. The bold text in this document is to serve as a reference point.
- The Comments column provides additional information where it may be helpful. This information does not appear in the BIOS Setup screens.
- Information in the screen shots that is enclosed in brackets (< >) indicates text that varies, depending on the option(s) installed. For example <Current Date> is replaced by the actual current date.
- Information that is enclosed in square brackets ([]) in the tables indicates areas where the user needs to type in text instead of selecting from a provided option.
- Whenever information is changed (except Date and Time) the systems requires a save and reboot to take place. Pressing <ESC> will discard the changes and boot the system according to the boot order set from the last boot.

Main Screen

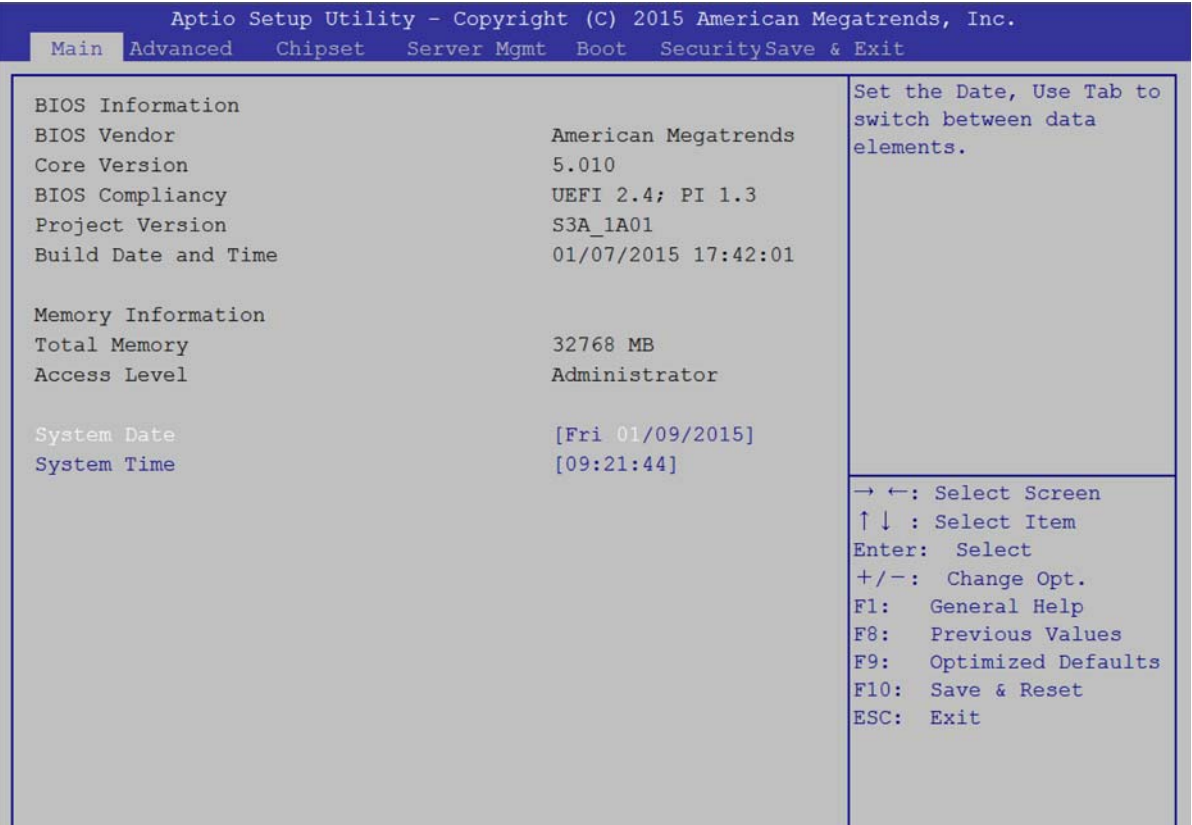


Figure 2-1. Main Screen

Table 3: Main Screen Description

SETUP ITEM	OPTIONS	HELP TEXT	COMMENTS
BIOS Vendor			Information only. Displays the BIOS Vendor.
Core Version			Information only. Displays the AMI BIOS Core version.
Compliance			Information only. Displays the BIOS compliance.
Project Version			Information only. Displays the Project version.
Build Date and Time			Information only. Displays the BIOS build date.
Total Memory			Information only. Displays the Total System Memory Size.
Access Level			Information only. Displays the Total System Memory Size.
System Date	[Day of week MM/DD/YYYY]	Set the Date. Use Tab to switch between Date elements.	Valid range of year : 1998~2099.
System Time	[HH:MM:SS]	Set the Time. Use Tab to switch between Time elements.	

Advanced Screen

The Advanced screen provides an access point to configure several options. On this screen, the user selects the option that is to be configured. Configurations are performed on the selected screen, not directly on the Advanced screen.

To access this screen from the Main screen, press the right arrow until the Advanced screen is chosen.

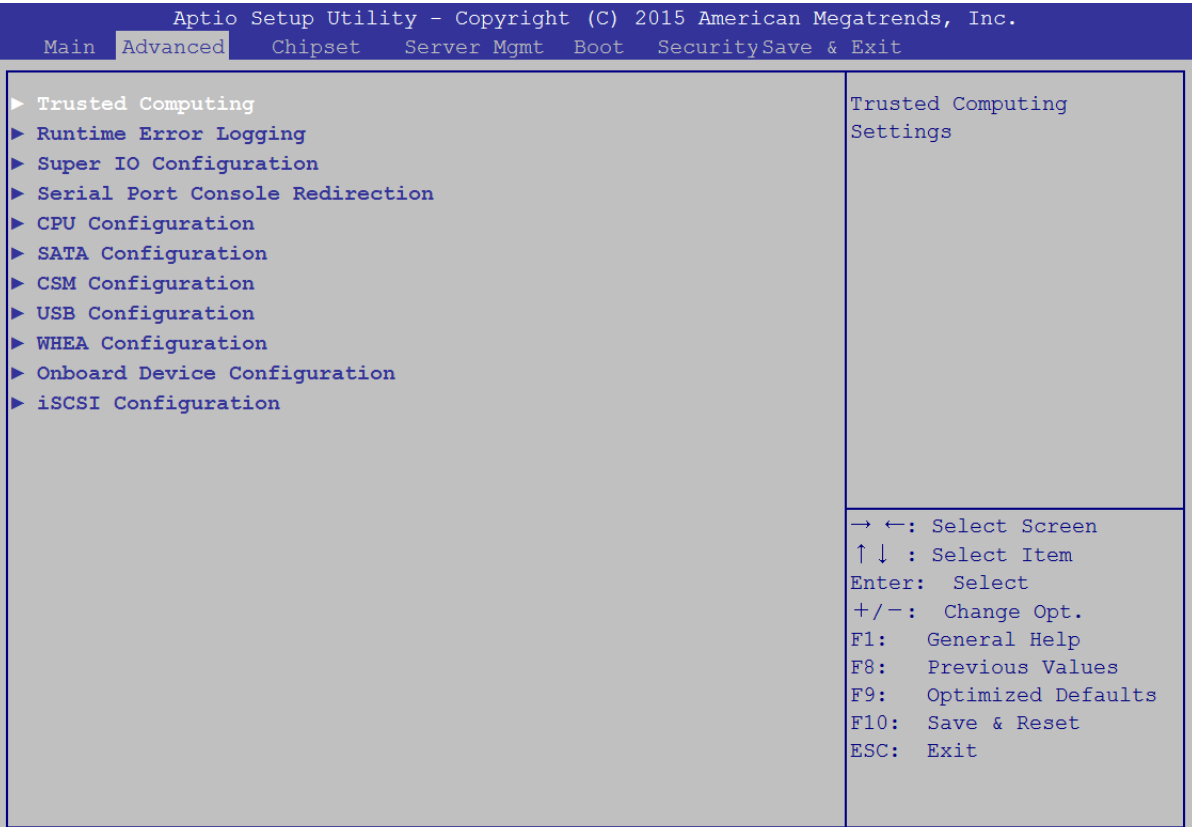


Figure 2-2. Advanced Screen

Table 4: Advanced Screen Description

SETUP ITEM	OPTIONS	HELP TEXT	COMMENTS
Trusted Computing		Trusted Computing Settings	
Runtime Error Logging		Runtime Erro Logging Support Setup Options	
Super IO Configuration		System Super IO Chip Parameters.	
Serial Port Console Redirection		Serial Port Console Redirection	
CPU Configuration		CPU Configuration Parameters	
SATA Configuration		SATA Device Opton Settings	
CSM Configuration		CSM configuration: Enable/Disable, Option ROM execution settings, etc.	
USB Configuration		USB Configuration Parameters	
WHEA Configuration		General WHEA Configuration Settings	

Table 4: Advanced Screen Description (Continued)

SETUP ITEM	OPTIONS	HELP TEXT	COMMENTS
Onboard Device Configuration		Onboard Device Parameters	
iSCSI Configuration		Configure the iSCSI Parameters	Dynamic

Chipset Screen

The Chiptset screen provides an access point to configure several options. On this screen, the user selects the option that is to be configured. Configurations are performed on the selected screen, not directly on the Chipset screen.

To access this screen from the Main screen, press the right arrow until the Chipset screen is chosen.

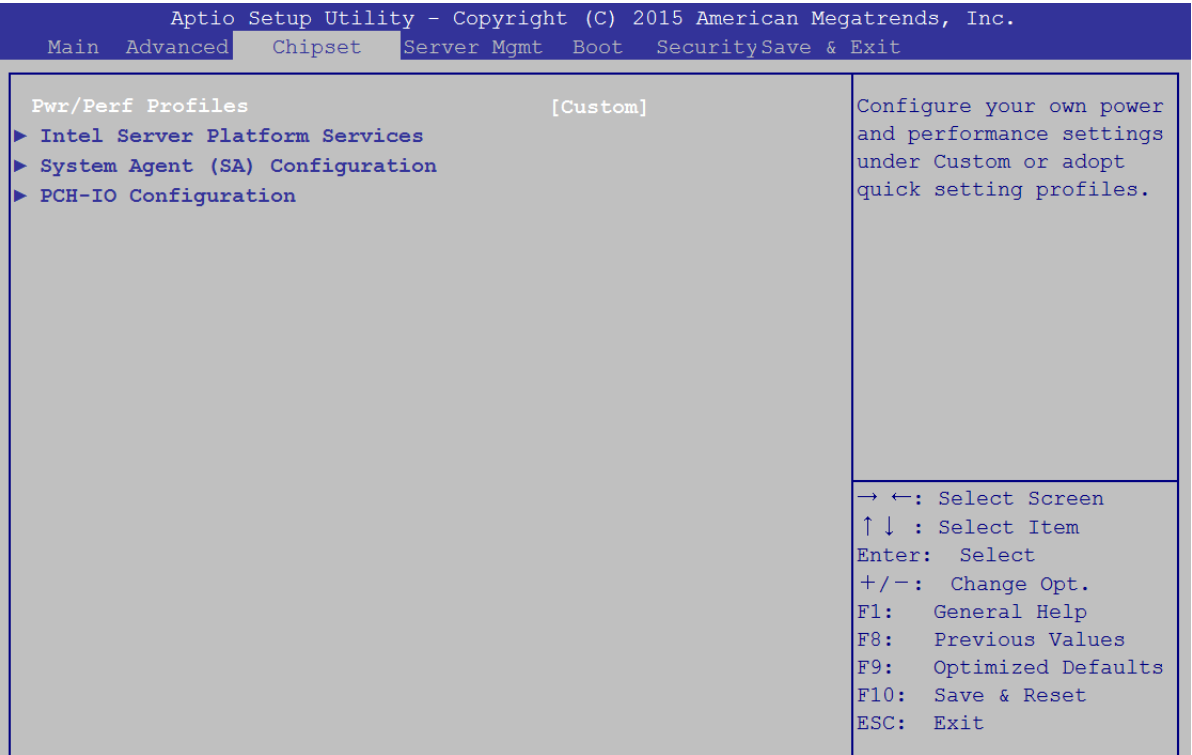


Figure 2-3. Chipset Screen

Table 5: Chipset Screen Description

SETUP ITEM	OPTIONS	HELP TEXT	COMMENTS
Pwr/Perf Profiles	[Custom] [Energy-Saving Mode] [Balanced Mode] [Virtualization Mode] [HPC Mode]	Configure your own power and performance settings under Custom or adopt quick setting profiles.	
Intel Server Platform Services		Intel Server Platform Services Parameters	

Table 5: Chipset Screen Description (Continued)

SETUP ITEM	OPTIONS	HELP TEXT	COMMENTS
System Agent (SA) Configuration		System Agent (SA) Parameters	
PCH-IO Configuration		PCH Parameters	

Server Management Screen

The Server Management screen displays information of the BMC, and allows the user to configure desired settings.

To access this screen from the Main screen, select Server Mgmt Options.

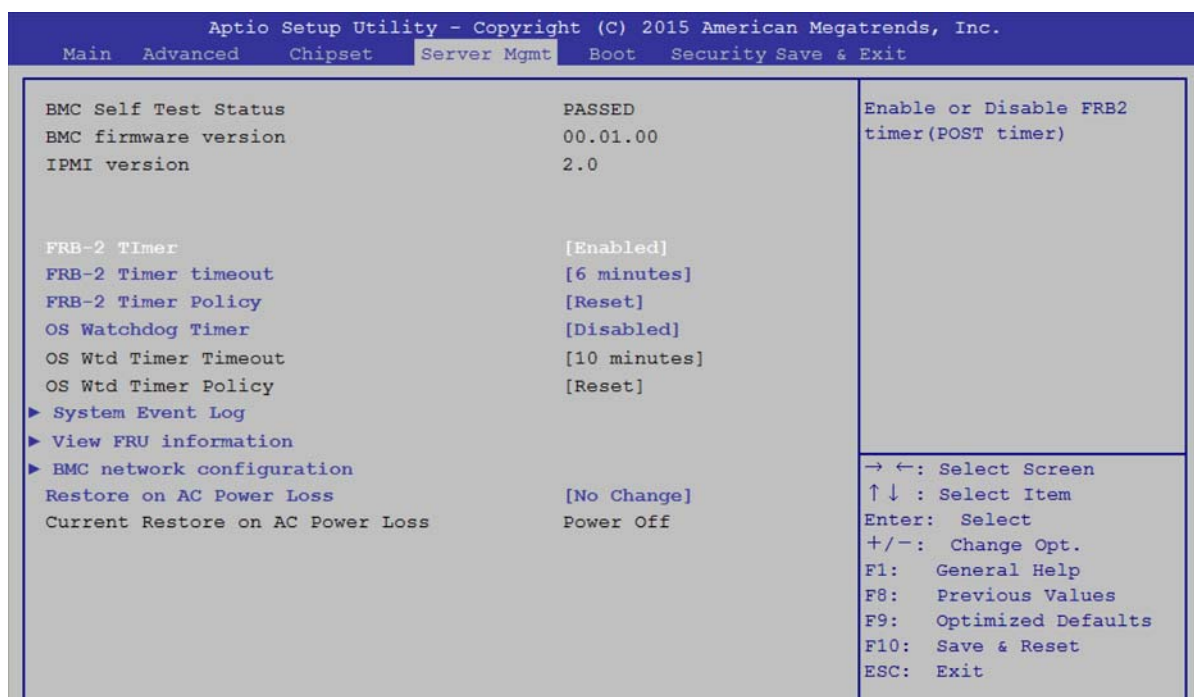


Figure 2-4. Server Management Screen

Table 6: Server Management Screen Description

SETUP ITEM	OPTIONS	HELP TEXT	COMMENTS
BMC Self Test Status			Information only. Displays the BMC Self Test Status.
BMC firmware version			Information only. Displays the BMC firmware version.
IPMI version			Information only. Displays the IPMI version.
FRB-2 Timer	[Enabled] [Disabled]	Enable or Disable FRB2 timer (POST timer)	

Table 6: Server Management Screen Description (Continued)

SETUP ITEM	OPTIONS	HELP TEXT	COMMENTS
FRB-2 Timer timeout	[3 minutes] [4 minutes] [5 minutes] [6 minutes]	Enter value Between 3 to 6 min for FRB-2 Timer Expiration value	Not available if FRB2 Timer is disabled.
FRB-2 Timer Policy	[Do Nothing] [Reset] [Power Down]	Configure how the system should respond if the FRB2 Timer expires. Not available if FRB2 Timer is disabled.	Not available if FRB2 Timer is disabled.
OS Watchdog Timer	[Enabled] [Disabled]	If enabled, starts a BIOS timer which can only be shut off by Intel Management Software after the OS loads. Helps determine that the OS successfully loaded or follows the O/S Boot Watchdog Timer policy.	
OS Wtd Timer Timeout	[5 minutes] [10 minutes] [15 minutes] [20 minutes]	Configure the length of the OS Boot Watchdog Timer. Not available if OS Boot Watchdog Timer is disabled.	
OS Wtd Timer Policy	[Do Nothing] [Reset] [Power Down]	Configure how the system should respond if the O/S Boot Watchdog Timer expires. Not available if O/S Boot Watchdog Timer is disabled.	
System Event Log		Press < Enter > to change the SEL event log configuration.	
View FRU information		Press < Enter > to view FRU information.	
BMC network configuration		Configure BMC network parameters	
Restore on AC Power Loss	[Power Off] [Power On] [Last State] [No Change]	System action to take on AC power loss	
Current Restore on AC Power Loss			Current system action to take on AC power loss.

Boot Options Screen

The Boot Options screen displays any bootable media encountered during POST, and allows the user to configure desired boot device.

If no boot devices are available – for example, both onboard LAN are disabled and no bootable device connected when Boot Mode is set to Legacy – the system will auto boot into BIOS setup menu.

To access this screen from the Main screen, select Boot Options.

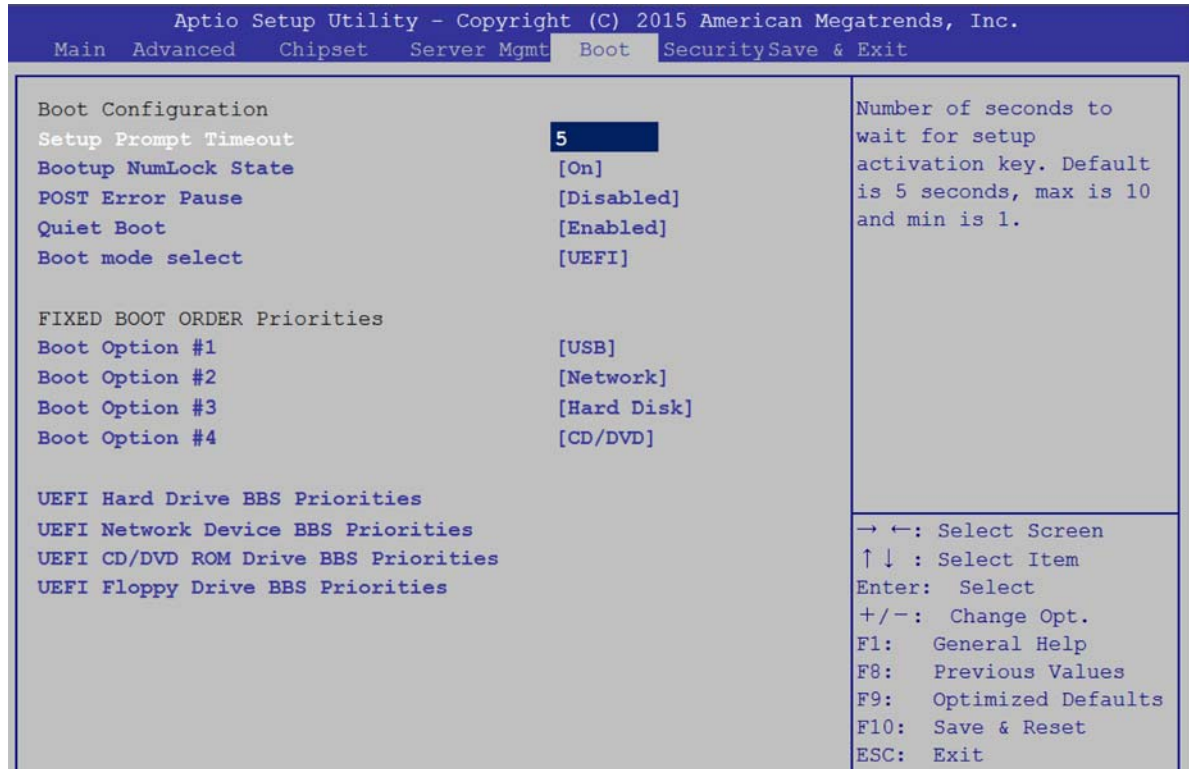


Figure 2-5. Boot Options Screen

Table 7: Boot Options Screen Description

SETUP ITEM	OPTIONS	HELP TEXT	COMMENTS
Setup Prompt Timeout	[<number>]	Number of seconds to wait for setup activation key. Default is 5 seconds, max is 10 and min is 1.	
Bootup Num-Lock State	[On] [Off]	Select the keyboard NumLock state	
POST Error Pause	[Disabled] [Enabled]	Enables or disables POST Error Pause	
Quiet Boot	[Disabled] [Enabled]	Enables or disables Quiet Boot option	
Boot mode select	[LEGACY] [UEFI]	Select boot mode LEGACY/UEFI	This item decides what devices (Legacy or UEFI) BIOS should try to boot when let the system auto boot up without manually select boot device.

Table 7: Boot Options Screen Description (Continued)

SETUP ITEM	OPTIONS	HELP TEXT	COMMENTS
Boot Option #1	[<Device String 1> [<Device String 2> ... [Disabled]	Sets the system boot order	
Boot Option #2	[<Device String 1> [<Device String 2> ... [Disabled]	Sets the system boot order	
Boot Option #3	[<Device String 1> [<Device String 2> ... [Disabled]	Sets the system boot order	
Boot Option #4	[<Device String 1> [<Device String 2> ... [Disabled]	Sets the system boot order	
Hard Drive BBS Priorities		Set the order of the legacy devices in this group	Only appears when at least one Hard Disk is detected.
Network Device BBS Priorities		Set the order of the legacy devices in this group	
CD/DVD ROM Drive BBS Priorities		Set the order of the legacy devices in this group	Only appears when at least one CD/DVD Drive is detected.
Floppy Drive BBS Priorities		Set the order of the legacy devices in this group	

Security Screen

The Security screen provides fields to enable and set the user and administrative password and to lockout the front panel buttons so they cannot be used.

To access this screen from the Main screen, select the Security option.

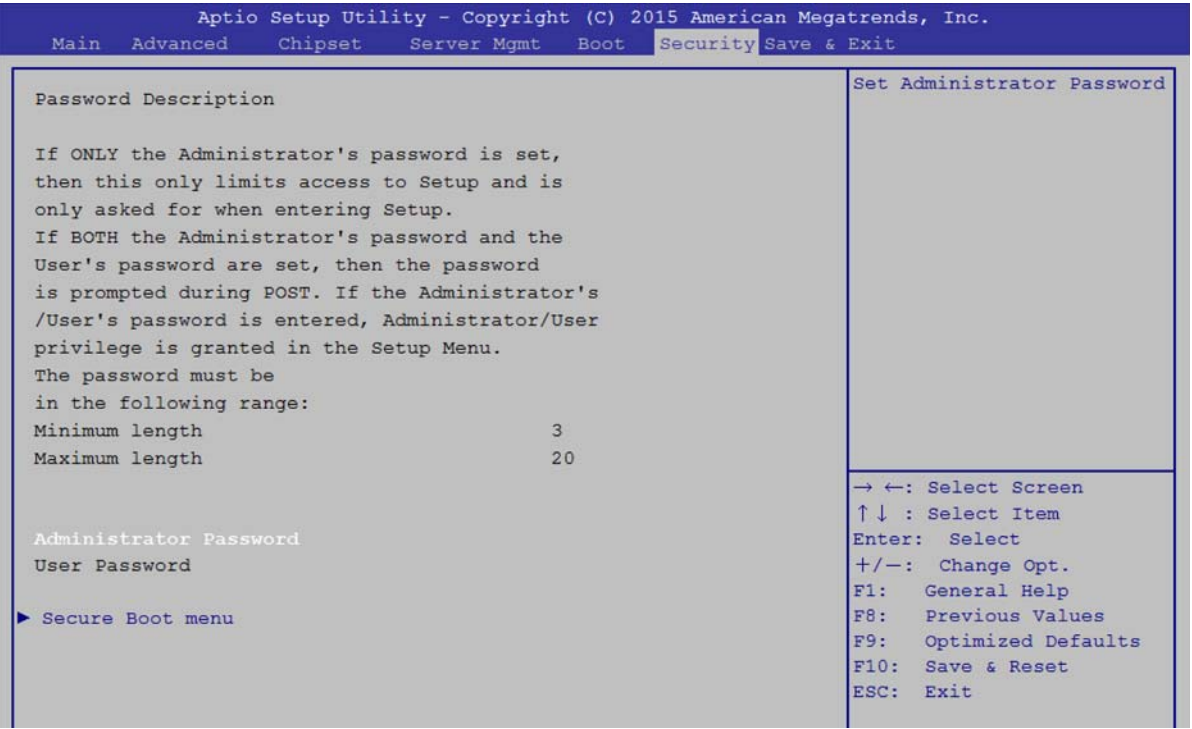


Figure 2-6. Security Screen

Table 8: BIOS Screen Description

SETUP ITEM	OPTIONS	HELP TEXT	COMMENTS
Administrator Password		Set Administrator Password	
User Password		Set User Password	
Secure Boot menu		Customizable Secure Boot settings	

Exit Screen

The Exit screen allows the user to choose to save or discard the configuration changes made on the other screens. It also provides a method to restore the server to the factory defaults or to save or restore a set of user defined default values. If Restore Defaults is selected, the default settings, noted in bold in the tables in this chapter, will be applied. If

Restore User Default Values is selected, the system is restored to the default values that the user saved earlier, instead of being restored to the factory defaults.

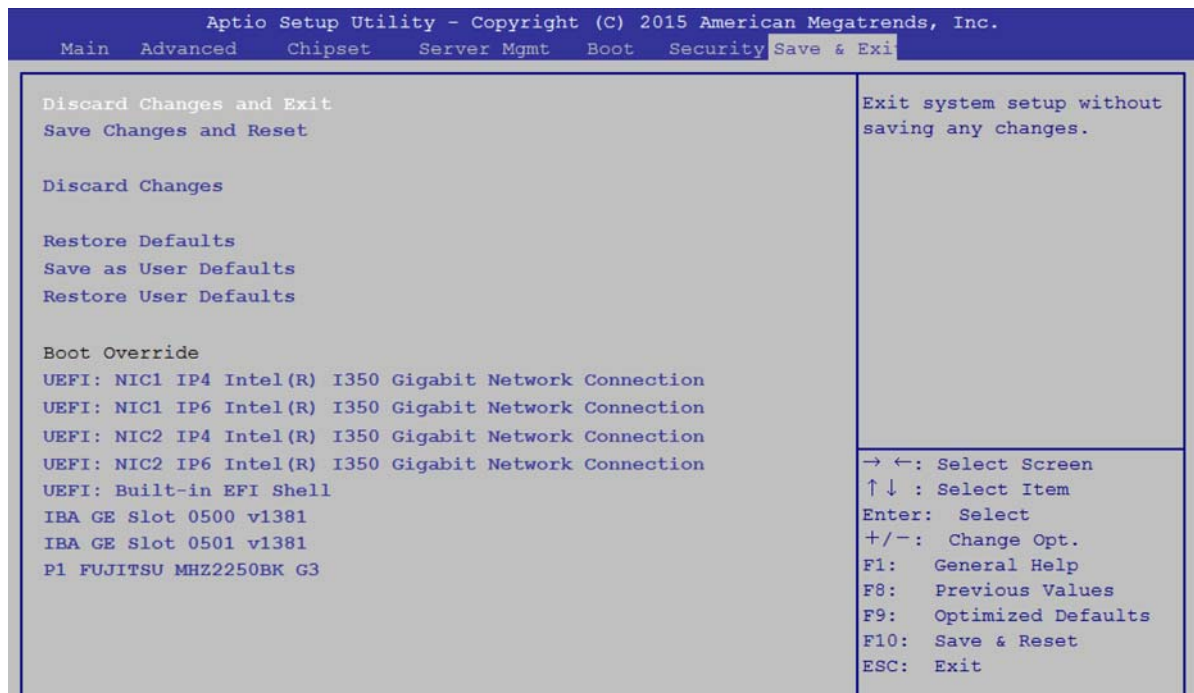


Figure 2-7. Exit Screen

Table 9: Exit Screen Description

SETUP ITEM	OPTIONS	HELP TEXT	COMMENTS
Discard Changes and Exit		Exit system setup without saving any changes.	
Save Changes and Reset		Reset the system after saving the changes.	
Discard Changes		Discards changes done so far to any of the setup options.	
Restore Defaults		Restore/Load Default values for all the setup options.	
Save as User Defaults		Save the changes done so far as User Defaults.	
Restore User Defaults		Restore the User Defaults to all the setup options.	
[<Device String 1>]			Boot with Device <Device String 1>
[<Device String 2>]			Boot with Device <Device String 2>
[<Device String 3>]			Boot with Device <Device String 3>
[<Device String 4>]			Boot with Device <Device String 4>
[<Device String 5>]			Boot with Device <Device String 5>

Table 9: Exit Screen Description (Continued)

SETUP ITEM	OPTIONS	HELP TEXT	COMMENTS
[<Device String 6>]			Boot with Device <Device String 6>

Loading BIOS Defaults

Different mechanisms exist for resetting the system configuration to the default values. When a request to reset the system configuration is detected, the BIOS loads the default system configuration values during the next POST. The request to reset the system to the defaults can be sent in the following ways:

- Pressing <**F9**> from within the BIOS Setup utility
- Load BIOS defaults by jumper as follows:
 1. Power down the system.
 2. Move CMOS clear jumper from pins 2-3 to pins 1-2 for a few seconds.
 3. Move CMOS clear jumper back to pins 2-3.
 4. System automatically powers on.
 5. Check BIOS defaults are loaded.

2.2 BIOS Update Utility

The flash ROM contains system initialization routines, the BIOS Setup Utility, and runtime support routines. The exact layout is subject to change, as determined by BIOS. The flash ROM also contains initialization code in compressed form for onboard peripherals, like SCSI, NIC and video controllers. The complete ROM is visible, starting at physical address 4 GB minus the size of the flash ROM device.

A 16-KB parameter block in the flash ROM is dedicated to storing configuration data that controls the system configuration (ESCD). Application software must use standard APIs to access these areas; application software cannot access the data directly.

BIOS Update Utility

Server platforms support DOS-based, Windows-based, and Linux-based firmware update utilities. It is very important to follow the rule, and use official provided package to update BIOS under DOS/Linux/ EFI shell environment. Using incorrect flash option to flash BIOS may cause damage to your system. This utility loads a fresh copy of the BIOS into the flash ROM.

The BIOS update may affect the following items:

- The system BIOS, including the setup utility and strings.
- Onboard video BIOS, RAID BIOS, and other option ROMS for the devices embedded on the server board.
- Memory reference code.
- Microcode updates.

AFULNX:

1. Please refer to the README.txt that each official release BIOS attached.
2. Reboot system then new BIOS runs.

ME Region Update

Update utility also provide ME region update function, please refer to the README.txt that each official release BIOS attached.

The BIOS update may affect the following items:

- The system BIOS, including the setup utility and strings.
- Onboard video BIOS, RAID BIOS, and other option ROMS for the devices embedded on the server board.
- Memory reference code.

- Microcode updates.
- ME Firmware.

BIOS Setting Utility

Use AMISCE to import/export BIOS setting in Linux:

1. Export BIOS setting and generate script file:
/o /s NVRAM.txt
2. Import BIOS setting with script file:
/i /s NVRAM.txt

BIOS Revision

The BIOS revision is used to identify the BIOS image and BIOS phase.

Table 10: Terminology

Term	Description
ACPI	Advanced Configuration and Power Interface. ACPI is an open industry specification proposed by Intel, Microsoft and Toshiba. ACPI enables and supports reliable power management through improved hardware and OS coordination.
AHCI	Advanced Host Controller Interface, a SATA controller standard.
ANSI	American National Standards Institute.
API	Application Programming Interface. A software abstraction provided by the BIOS to applications and/or the OS.
ASCII	American Standard Code for Information Interchange. An 8-level code (7 bits plus parity check) widely used in data processing and data communications systems.
ATA	Advanced Technology Attachment, a disk interface standard.
BAR	Base Address Register. Device configuration registers that define the start address, length and type of memory space required by a device.
BIOS	Basic Input/Output System – Firmware interface to the system hardware.
BIST	Built-in Self Test.
BMC	Baseboard Management Controller.
BSP	Boot strap processor. The processor selected at boot time to be the primary processor in a multi-processor system.
CATERR	Catastrophic Error Signal.
CE	Correctable Error (memory ECC error).
CMOS	Complementary Metal-oxide-semiconductor.
COM1	Communication Port 1, serial port 1.
DCA	Direct Cache Access.
DDR4	Double Data Rate 4 is a high bandwidth memory technology.
DIMM	Dual In-line Memory Module, a plug-in memory module with signal and power pins on both sides of the internal printed circuit board (front and back).

Table 10: Terminology (Continued)

Term	Description
DMA	Direct Memory Access.
DMI	Direct Media Interface – connection from the processor to the PCH.
DRAM	Dynamic Random Access Memory, memory chips from which DIMMs are constructed.
DXE	Driver Execution Environment. Component of Intel® Platform Innovation Framework for EFI architecture.
ECC	Error Correction Code. Refers to a memory system that has extra bit(s) to support limited detection/correction of memory errors.
EEPROM	Electrically Erasable Programmable Read Only Memory – called “Flash memory”.
EFI	Extensible Firmware Interface (see also UEFI).
EHCI	Enhanced Host Controller Interface, a USB controller standard.
Flash	Short for “Flash Memory”, solid-state memory based on EEPROMs.
FRU	Field Replaceable Unit.
FV	Firmware Volume.
GbE	Gigabit Ethernet, an Ethernet connection operating at gigabit/second speed.
GUID	Globally Unique Identifier.
HotKey	A “HotKey” is a key combination recognized as an unprompted command input. For example, pressing <F2> during POST will take the operator to the Setup Utility.
HT	Intel® Hyper-Threading Technology.
IBMC	Integrated Baseboard Management Controller.
ICH	I/O Control Hub, a chipset component.
IDE	Integrated Drive Electronics, a disk interface standard.
IIO	Integrated I/O – I/O controller integrated into the processor chip.
IMC	Integrated Memory Controller – memory controller integrated into the processor chip.
INTR	Interrupt Request.
I/O	Input/Output.
IPMI	Intelligent Platform Management Interface – an industry standard that defines standardized, abstracted interfaces to platform management hardware.
IRQ	Interrupt Request.
KVM	Keyboard, Video, and Mouse – an attachment that mimics those devices, and connects them to a remote I/O user.
LAN	Local Area Network.
LED	Light Emitting Diode.
LRDIMM	Load Reduced DIMM memory modules have buffer registers for both address and data between the SDRAM modules and the system's memory controller.
MCA	Machine Check Architecture.
MCE	Machine Check Exception.
MMIO	Memory Mapped I/O.
MRC	Memory Reference Code.

Table 10: Terminology (Continued)

Term	Description
MSR	Model Specific Register.
NIC	Network Interface Card.
NM	Node Manager – now “Intel® Intelligent Power Node Manager”.
NMI	Non-Maskable Interrupt.
OEM	Original Equipment Manufacturer.
OS	Operating System.
PCH	Platform Controller Hub.
PCI	Peripheral Component Interconnect, or PCI Local Bus Standard – also called “Conventional PCI”.
PCIe	PCI Express* -- an updated form of PCI offering better throughput and better error management.
PCR	Platform Configuration Register.
PECI	Platform Environmental Control Interface.
PEI	Pre EFI Initialization. Component of Intel® Platform Innovation Framework for EFI architecture.
PERR	Parity Error.
PIC	Programmable Interrupt Controller.
PMI	Platform Management Interrupt.
PnP	Plug and Play. Used as “PnP BIOS” and “PnP ISA”.
POST	Power On Self Test – BIOS activity from the time on Power On until Operating System boot begins.
PXE	Pre-execution Environment.
QPI	Intel® QuickPath Interconnect.
RAID	Redundant Array of Inexpensive Disks – provides data security by spreading data over multiple disk drives. RAID 0, RAID 1, RAID 10, and RAID 5 are different patterns of data on varying numbers of disks to provide varying degrees of security and performance.
RAS	Reliability, Availability, and Serviceability.
RDIMM	Registered DIMM (also called buffered) memory modules have an address buffer register between the SDRAM modules and the system's memory controller.
ROM	Read-Only Memory.
RTC	Real Time Clock.
SAS	Serial Attached SCSI, a high speed serial data version of SCSI.
SATA	Serial ATA, a high speed serial data version of the disk ATA interface.
SCI	System Control Interrupt.
SCSI	Small Computer System Interface, a connection usually used for disks of various types.
SDR	Sensor Data Record.
SEL	System Event Log.
SERR	System Error.

Table 10: Terminology (Continued)

Term	Description
SKU	Stock Keeping Unit – indicates a specific marketing package, in this sense based around a server board configuration.
SMBIOS	System Management BIOS.
SMI	System Management Interrupt.
SMM	System Management Mode.
SOL	Serial Over LAN.
SPI	Serial Peripheral Interface, a serial data interface used for Flash memory.
UDIMM	Unbuffered DIMM (also called Unregistered) memory modules do not have a register between the SDRAM modules and the system's memory controller.
UE or UCE	Uncorrectable Error (memory ECC error).
UEFI	Unified Extensible Firmware Interface – replacement for Legacy BIOS and the Legacy DOS interface.
USB	Universal Serial Bus, a standard serial expansion bus meant for connecting peripherals.
UUID	Universally Unique Identifier. See also GUID.
WHEA	Windows Hardware Error Architecture.

Clear CMOS

The following steps will load the BIOS defaults by jumper:

1. Power down the system.
2. Move CMOS clear jumper from pins 2-3 to pins 1-2 for a few seconds.
3. Move CMOS clear jumper back to pins 2-3.
4. System automatically powers on.
5. Check BIOS defaults are loaded.

Clear Password

1. Power down the system.
2. Move password clear jumper from pins 2-3 to pins 1-2.
3. Power on the system.
4. Make sure password is cleared.
5. Power down the system.
6. Move password clear jumper from pins 1-2 back to pins 2-3.
7. Power on the system.
8. Set new password.

2.3 Server Management

The BIOS supports many standard-based server management features and several proprietary features. The Intelligent Platform Management Interface (IPMI) is an industry standard and defines standardized, abstracted interfaces to platform management hardware. The BIOS implements many proprietary features that are allowed by the IPMI specification, but these features are outside the scope of the IPMI specification. This section describes the implementation of the standard and proprietary features.

Console Redirection

The BIOS supports redirection of both video and keyboard via a serial link (serial port). When console redirection is enabled, the local, or host server, keyboard input and video output are passed both to the local keyboard and video connections, and to the remote console through the serial link. Keyboard inputs from both sources are considered valid and video is displayed to both outputs.

As an option, the system can be operated without a host keyboard or monitor attached to the system and run entirely via the remote console. Utilities that can be executed remotely include BIOS Setup.

Serial Configuration Settings

The BIOS does not require that the splash logo be turned off for console redirection to function. The BIOS supports multiple consoles, some of which are in graphics mode and some in text mode. The graphics consoles can display the logo and the text consoles receive the redirected text.

Keystroke Mapping

During console redirection, the remote terminal sends keystrokes to the local server. The remote terminal can be a dumb terminal with a direct connection and running a communication program. The keystroke mapping follows VT-UTF8 format with the following extensions.

Table 11: Keystroke Mappings

KEY	ANSI ESCAPE SEQUENCE	WINDOWS PLATFORM DESIGN NOTE
F1	<ESC><Shift>op	<ESC>1
F2	<ESC><Shift>oq	<ESC>2
F3	<ESC><Shift>or	<ESC>3
F4	<ESC><Shift>os	<ESC>4
F5		<ESC>5
F6		<ESC>6
F7		<ESC>7

Table 11: Keystroke Mappings (Continued)

KEY	ANSI ESCAPE SEQUENCE	WINDOWS PLATFORM DESIGN NOTE
F8		<ESC>8
F9		<ESC>9
F10		<ESC>0
F11		<ESC>!
F12		<ESC>@
Home	<ESC>[<Shift>h	<ESC>h
End	<ESC>[<Shift>k	<ESC>k
Ins		<ESC>+
Del		<ESC>-
Page Up		<ESC>?
Page Down		<ESC>/
Reset		<ESC>R<ESC>r<ESC>R

Standalone <Esc> Key for Headless Operation

The Microsoft Headless Design Guidelines describes a specific implementation for the <Esc> key as a single standalone keystroke:

To complete an escape sequence, the timeout must be two seconds for entering additional characters following an escape.

- <Esc> followed by a two-second pause must be interpreted as a single escape.
- <Esc> followed within two seconds by one or more characters that do not form a sequence described in this specification must be interpreted as <Esc> plus the character or characters, not as an escape sequence.

The escape sequence in the following table is an input sequence. This means it is sent to the BIOS from the remote terminal.

Reset

BIOS provides another friendly method to reset system from console. User could use <Ctrl> + <Shift> + '-' to reboot system from remote console.

Limitations

- BIOS Console redirection terminates after an operating system has being loaded. The operating system is responsible for continuing console redirection after that.
- BIOS console redirection is a text console. Graphical data, such as a logo, are not redirected.

Interface to Server Management (Optional)

If the BIOS determines that console redirection is enabled, it will read the current baud rate and pass this value to the appropriate management controller via the Intelligent Platform Management Bus (IPMB).

Network BIOS Support

PXE Boot

The BIOS supports the EFI PXE implementation. To utilize this, the user must load EFI Simple Network Protocol driver and the UNDI driver specific for the network interface card being used. The UNDI driver should be included with the network interface card. The Simple Network Protocol driver can be obtained from <http://developer.intel.com/technology/framework>.

The BIOS supports legacy PXE option ROMs in legacy mode and includes the necessary PXE ROMs in the BIOS image for the onboard controllers. The legacy PXE ROM is required to boot a non-EFI operating system over the network.

Checkpoints

A checkpoint is either a byte or word value output to Debug port. The BIOS outputs checkpoints throughout bootblock and Power-On Self Test (POST) to indicate the task the system is currently executing. Checkpoints are very useful in aiding software developers or technicians in debugging problems that occur during the pre-boot process.

Checkpoints can be defined as follow:

- Standard Checkpoint
- ACPI/ASL Checkpoint
- OEM-Reserved Checkpoint
- MRC POST Code Checkpoints

Standard Checkpoint

A checkpoint is either a byte or word value output to Debug port. The BIOS outputs checkpoints throughout bootblock and Power-On Self Test (POST) to indicate the task the system is currently executing. Checkpoints are very useful in aiding software developers or technicians in debugging problems that occur during the pre-boot process.

Table 12: Checkpoint Range Description

STATUS CODE RANGE	DESCRIPTION
0x01 – 0x0B	SEC execution
0x0C – 0x0F	SEC errors
0x10 – 0x2F	PEI execution up to and including memory detection
0x30 – 0x4F	PEI execution after memory detection
0x50 – 0x5F	PEI errors
0x60 – 0x8F	DXE execution up to BDS
0x90 – 0xCF	BDS execution
0xD0 – 0xDF	DXE errors
0xD0 – 0xDF	S3 Resume (PEI)
0xE9 – 0xEF	S3 Resume errors (PEI)

SEC Phase

Table 13: SEC Phase

STATUS CODE	DESCRIPTION
0x00	Not used
Progress Codes	
0x01	Power on. Reset type detection (soft/hard).
0x02	AP initialization before microcode loading
0x03	North Bridge initialization before microcode loading
0x04	South Bridge initialization before microcode loading
0x05	OEM initialization before microcode loading
0x06	Microcode loading
0x07	AP initialization after microcode loading
0x08	North Bridge initialization after microcode loading
0x09	South Bridge initialization after microcode loading
0x0A	OEM initialization after microcode loading
0x0B	Cache initialization
SEC Error Codes	
0x0C – 0x0D	Reserved for future AMI SEC error codes
0x0E	Microcode not found
0x0F	Microcode not loaded

PEI Phase

Table 14: PEI Phase

STATUS CODE	DESCRIPTION
Progress Codes	
0x10	PEI Core is started
0x11	Pre-memory CPU initialization is started
0x12	Pre-memory CPU initialization (CPU module specific)
0x13	Pre-memory CPU initialization (CPU module specific)
0x14	Pre-memory CPU initialization (CPU module specific)
0x15	Pre-memory North Bridge initialization is started
0x16	Pre-Memory North Bridge initialization (North Bridge module specific)
0x17	Pre-Memory North Bridge initialization (North Bridge module specific)
0x18	Pre-Memory North Bridge initialization (North Bridge module specific)
0x19	Pre-memory South Bridge initialization is started
0x1A	Pre-memory South Bridge initialization (South Bridge module specific)
0x1B	Pre-memory South Bridge initialization (South Bridge module specific)
0x1C	Pre-memory South Bridge initialization (South Bridge module specific)
0x1D	Waiting BMC initialization
0x1E – 0x2A	OEM pre-memory initialization codes
0x2B	Memory initialization. Serial Presence Detect (SPD) data reading
0x2C	Memory initialization. Memory presence detection
0x2D	Memory initialization. Programming memory timing information
0x2E	Memory initialization. Configuring memory
0x2F	Memory initialization (other).
0x30	Reserved for ASL (see ASL Status Codes section below)
0x31	Memory Installed
0x32	CPU post-memory initialization is started
0x33	CPU post-memory initialization. Cache initialization
0x34	CPU post-memory initialization. Application Processor(s) (AP) initialization
0x35	CPU post-memory initialization. Boot Strap Processor (BSP) selection
0x36	CPU post-memory initialization. System Management Mode (SMM) initialization
0x37	Post-Memory North Bridge initialization is started
0x38	Post-Memory North Bridge initialization (North Bridge module specific)
0x39	Post-Memory North Bridge initialization (North Bridge module specific)
0x3A	Post-Memory North Bridge initialization (North Bridge module specific)
0x3B	Post-Memory South Bridge initialization is started
0x3C	Post-Memory South Bridge initialization (South Bridge module specific)
0x3D	Post-Memory South Bridge initialization (South Bridge module specific)

Table 14: PEI Phase (Continued)

STATUS CODE	DESCRIPTION
0x3E	Post-Memory South Bridge initialization (South Bridge module specific)
0x3F – 0x4E	OEM post memory initialization codes
0x4F	DXE IPL is started
PEI Error Codes	
0x50	Memory initialization error. Invalid memory type or incompatible memory speed
0x51	Memory initialization error. SPD reading has failed
0x52	Memory initialization error. Invalid memory size or memory modules do not match.
0x53	Memory initialization error. No usable memory detected
0x54	Unspecified memory initialization error.
0x55	Memory not installed
0x56	Invalid CPU type or Speed
0x57	CPU mismatch
0x58	CPU self test failed or possible CPU cache error
0x59	CPU micro-code is not found or micro-code update is failed
0x5A	Internal CPU error
0x5B	reset PPI is not available
0x5C-0x5F	Reserved for future AML error codes
S3 Resume Progress Codes	
0xE0	S3 Resume is started (S3 Resume PPI is called by the DXE IPL)
0xE1	S3 Boot Script execution
0xE2	Video repost
0xE3	OS S3 wake vector call
0xE4 – 0xE7	Reserved for future AML progress codes
S3 Resume Error Codes	
0xE8	S3 Resume Failed
0xE9	S3 Resume PPI not Found
0xEA	S3 Resume Boot Script Error
0xEB	S3 OS Wake Error
0xEC – 0xEF	Reserved for future AML error codes

DXE Phase

Table 15: DXE Phase

STATUS CODE	DESCRIPTION
0x60	DXE Core is started
0x61	NVRAM initialization

Table 15: DXE Phase (Continued)

STATUS CODE	DESCRIPTION
0x62	Installation of the South Bridge Runtime Services
0x63	CPU DXE initialization is started
0x64	CPU DXE initialization (CPU module specific)
0x65	CPU DXE initialization (CPU module specific)
0x66	CPU DXE initialization (CPU module specific)
0x67	CPU DXE initialization (CPU module specific)
0x68	PCI host bridge initialization
0x69	North Bridge DXE initialization is started
0x6A	North Bridge DXE SMM initialization is started
0x6B	North Bridge DXE initialization (North Bridge module specific)
0x6C	North Bridge DXE initialization (North Bridge module specific)
0x6D	North Bridge DXE initialization (North Bridge module specific)
0x6E	North Bridge DXE initialization (North Bridge module specific)
0x6F	North Bridge DXE initialization (North Bridge module specific)
0x70	South Bridge DXE initialization is started
0x71	South Bridge DXE SMM initialization is started
0x72	South Bridge devices initialization
0x73	South Bridge DXE Initialization (South Bridge module specific)
0x74	South Bridge DXE Initialization (South Bridge module specific)
0x75	South Bridge DXE Initialization (South Bridge module specific)
0x76	South Bridge DXE Initialization (South Bridge module specific)
0x77	South Bridge DXE Initialization (South Bridge module specific)
0x78	ACPI module initialization
0x79	CSM initialization
0x7A – 0x7F	Reserved for future AMI DXE codes
0x80 – 0x8F	OEM DXE initialization codes
0x90	Boot Device Selection (BDS) phase is started
0x91	Driver connecting is started
0x92	PCI Bus initialization is started
0x93	PCI Bus Hot Plug Controller Initialization
0x94	PCI Bus Enumeration
0x95	PCI Bus Request Resources
0x96	PCI Bus Assign Resources
0x97	Console Output devices connect
0x98	Console input devices connect
0x99	Super IO Initialization

Table 15: DXE Phase (Continued)

STATUS CODE	DESCRIPTION
0x9A	USB initialization is started
0x9B	USB Reset
0x9C	USB Detect
0x9D	USB Enable
0x9E – 0x9F	Reserved for future AML codes
0xA0	IDE initialization is started
0xA1	IDE Reset
0xA2	IDE Detect
0xA3	IDE Enable
0xA4	SCSI initialization is started
0xA5	SCSI Reset
0xA6	SCSI Detect
0xA7	SCSI Enable
0xA8	Setup Verifying Password
0xA9	Start of Setup
0xAA	Reserved for ASL (see ASL Status Codes section below)
0xAB	Setup Input Wait
0xAC	Reserved for ASL (see ASL Status Codes section below)
0xAD	Ready To Boot event
0xAE	Legacy Boot event
0xAF	Exit Boot Services event
0xB0	Runtime Set Virtual Address MAP Begin
0xB1	Runtime Set Virtual Address MAP End
0xB2	Legacy Option ROM Initialization
0xB3	System Reset
0xB4	USB hot plug
0xB5	PCI bus hot plug
0xB6	Clean-up of NVRAM
0xB7	Clean-up of NVRAM
0xB8 – 0xBF	Reserved for future AML codes
0xC0 – 0xCF	OEM BDS initialization codes
DXE Error Codes	
0xD0	CPU initialization error
0xD1	North Bridge initialization error
0xD2	South Bridge initialization error
0xD3	Some of the Architectural Protocols are not available

Table 15: DXE Phase (Continued)

STATUS CODE	DESCRIPTION
0xD4	PCI resource allocation error. Out of Resources
0xD5	No Space for Legacy Option ROM
0xD6	No Console Output Devices are found
0xD7	No Console Input Devices are found
0xD8	Invalid password
0xD9	Error loading Boot Option (LoadImage returned error)
0xDA	Boot Option is failed (StartImage returned error)
0xDB	Flash update is failed
0xDC	Reset protocol is not available

ACPI/ASL Checkpoints

Table 16: ACPI/ASL Checkpoints

STATUS CODE	DESCRIPTION
0x01	System is entering S1 sleep state
0x02	System is entering S2 sleep state
0x03	System is entering S3 sleep state
0x04	System is entering S4 sleep state
0x05	System is entering S5 sleep state
0x10	System is waking up from the S1 sleep state
0x20	System is waking up from the S2 sleep state
0x30	System is waking up from the S3 sleep state
0x40	System is waking up from the S4 sleep state
0xAC	System has transitioned into ACPI mode. Interrupt controller is in PIC mode.
0xAA	System has transitioned into ACPI mode. Interrupt controller is in APIC mode.

OEM-Reserved Checkpoint Ranges

Table 17: OEM Reserved Checkpoint Ranges

STATUS CODE	DESCRIPTION
0x05	OEM SEC initialization before microcode loading
0x0A	OEM SEC initialization after microcode loading
0x1D – 0x2A	OEM pre-memory initialization codes
0x3F – 0x4E	OEM PEI post memory initialization codes
0x80 – 0x8F	OEM DXE initialization codes
0xC0 – 0xCF	OEM BDS initialization codes

BMC

Chapter 3

This section provides information and key features of BMC (Baseboard Management Controller).

3.1 Server Management Software

Server System Overview

In a server system, BMC is an independent system of the host server system. This independent system has its own processor and memory; the host system can be managed by the BMC system even if the host hardware or OS hangs or is unable to function.

BMC Key Features and Functions

- Supports IPMI v1.5 and v2.0.
- Support SNMP v1,v2c and v3.
- Support SMASH.
- Support delivers alerts such as SNMP traps in the Platform Event Trap (PET) format.
- Out-of-band monitoring and control for sever management over LAN.
- Share NIC for remote management via network.
- The FRU information report includes main board part number, product name, manufacturer, etc.).
- Health status/Hardware monitoring report.
- Events log, view, and clear.
- Event notification via lighting chassis LED indicator and Platform Event Trap (by SNMP trap) or Mail (by Simple Mail Transfer Protocol).
- Platform Event Filtering (PEF) to take selected actions for selected events, including NMI.
- Chassis management includes power control and a status report, front panel buttons and LED control.
- Watchdog and auto server restart and recovery.
- Supports multi-session users, and alert destination for LAN channel.
- Support IPMB connector that advanced server management card can communicate with BMC.

Power System

BMC controls system power through GPIO pins and IPMI chassis commands.

Front Panel User Interface

The BMC provides control panel interface functionality including indicators (Fault/status and Identify LEDs) and buttons (Power/ID).

Power Button

The Power buttons allow to control the system status.

ID Button

The control panel Chassis Identify button toggles the state of the Chassis ID LED. If the ID LED is off, then a button press will turn the LED on (blinking). If the LED is on, a button press or IPMI Chassis Identify command will turn the LED off.

LEDs

The following table contains information on Status, ID and Heartbeat LED's.

Table 3.1: Status LED, ID LED, and Heartbeat LED

LEDs	COLOR	STATUS	DESCRIPTION
Status LED	Amber (Status LED)	Blinking	System Event
		Off	Normal status
	Blue	On	Power on
		Off	Power off
ID LED	Blue	Off	Normal status
		Blinking	Identify the system with interval
		Solid ON	Identify the system
Heartbeat LED	Green	On/Off	BMC is not Ready
		Blinking	BMC is Ready

LAN Interface

BMC LAN interface in AST2400 is assigned to its Shared NIC LAN and a dedicated NIC (Default) in the system. IPMI Specification v2.0 defines how IPMI messages, encapsulated in RMCP/RMCP+ packet format, can be sent to and from the BMC. This capability allows a remote console application to access the BMC and perform the following operations:

- Chassis control: obtain chassis status, reset and power-up the chassis
- Obtain system sensor status
- Obtain and Set system boot options
- Obtain Field Replaceable Unit (FRU) information

- Obtain System Event Log (SEL) entries
- Obtain Sensor Data Records (SDR)
- Set Platform Event Filtering (PEF)
- Set LAN configurations

In addition, the BMC supports LAN alerting in the form of SNMP traps that conform to the IPMI Platform Event Trap (PET) format.

Session and User

This BMC supports ten (10) user accounts. Each can have a different user name, password and privilege level. Four accounts can login simultaneously. The available user privilege levels are User, Operator, and Administrator.

Serial Over LAN

BMC supports 1 IPMI (Spec v2.0) specific SOL session. BMC supports redirect data from UART interface.

Time Sync

In BMC design, BMC does not have a local RTC to know what time it is. Each time BMC will get the current time from system PCH after BMC boot. The current time is updated periodically from the PCH. The remote console program interpret this time as pre-initial.

SEL

BMC supports IPMI 1.5/2.0 standard SEL operation. It can keep SEL log. Event happened in BIOS side will be logged by using Add SEL Entry command. BMC will store them in FLASH, the time stamp field will be filled by BMC. When SEL is full, the new SEL won't be logged but will go through PEF as usual. If AC powers off, all SELs will remain in NV.

Platform Event

Platform Event Filter

The BMC implements selectable action on an event or LAN alerting base on event. By default, no any PEF entries or actions exist, applications need to configure it to enable.

- Dedicated and Shared NIC
- The policy to match an event to Platform Event Filter Table entry is IPMI 1.5 standard.
- The action support Power off, Power Reset, Power Cycle and NMI.

- All Platform Event Filter Table is default disabled.
- PEF Startup Delay and Last Processed Event tracking is not supported.
- PEF table lookup isn't correlated to log SEL to SEL Repository.
- Serial Alerting is no support.

BMC Firmware Update

The BMC will allow users to upgrade firmware image on following entities:

- BMC
- All other upgradable entities

The update capability is provided by local and remote interfaces.

DOS Recovery Utility

SOCFLASH Utility.

WebUI Update

Remote update can be performed through the remote Web console.

3.2 BMC Recovery

This section provides guidelines on BMC recovery process in DOS and Linux systems.

Recovery Process in DOS System

To recover BMC on a DOS system, do as follows:

1. Copy BMC firmware package to your USB key.
2. Boot into DOS.
3. Run *dos.bat*.

The BMC recovery is complete.

Recovery Process in Linux System

To recover BMC on a Linux system, do as follows:

1. Copy BMC firmware package to your USB drive.
2. Boot into Linux.
3. Run *linux.sh*.

The BMC recovery is complete.

Recovery Process in Windows System

To recover BMC on a Windows system, do as follows:

1. Copy BMC firmware package to your USB key.
2. Boot into Windows.
3. Run *win.bat*.

The BMC recovery is complete.

3.3 SMASH

Quanta SMASH is a tool that allows you to use Secure Shell (SSH) to login in the embedded Linux of BMC from remote terminal and gather information as well as give you control over things like power resets, power off. The basic structure is shown as below:

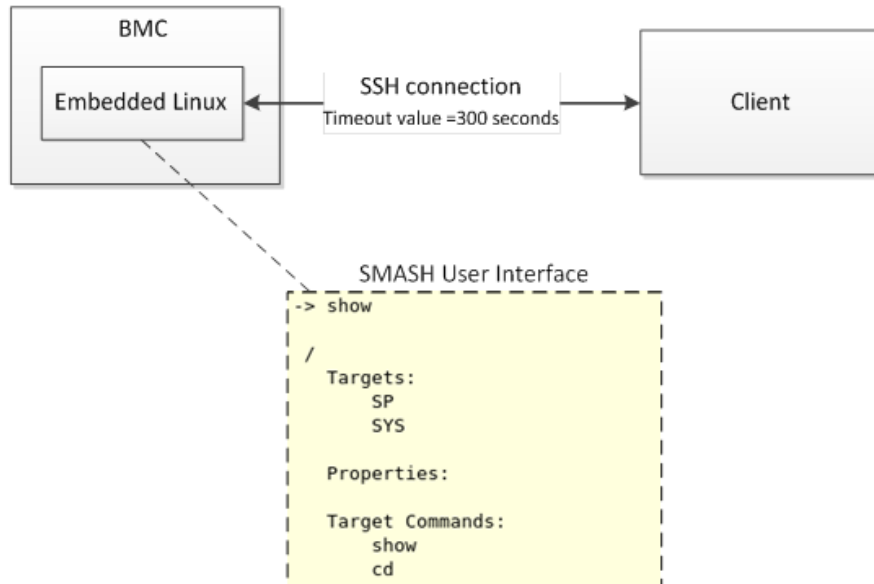


Figure 3-1. Using SSH to login in

Here presents an activity diagram, user could use SSH to login in embedded Linux of BMC from remote terminal. After login in successfully, SMASH would be executed automatically. In this time, SMASH is running and allowing user to input commands. The connection will be terminated if the terminal console is idle more than five minutes.

Default SSH UserName / Password (User Account in Linux): **sysadmin / superuser**

Input command in Linux: **ssh sysadmin@<Server IP>**

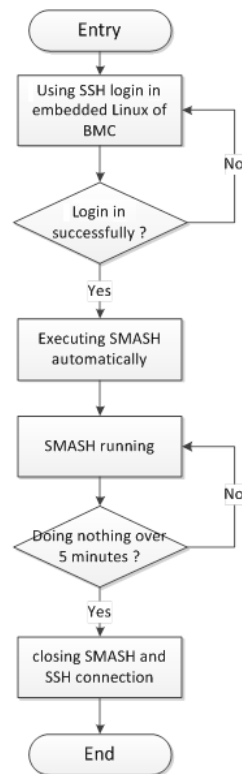


Figure 3-2. SMASH Activity Diagram

Here provides you the commands about system level and BMC level.

System Level Commands

The system level commands provide you the information and power state control.

Table 3.2: Targets and Verbs

RELATED TARGETS	SUPPORTED VERBS										
	CD	EXIT	HELP	CREATE	DELETE	SET	SHOW	RESET	START	STOP	VERSION
/	v	v	v				v				v
/SYS	v	v	v				v	v	v	v	v
/SYS/voltage	v	v	v				v				v
/SYS/fan	v	v	v				v				v
/SYS/temperature	v	v	v				v				v
/SYS/powerSupply	v	v	v				v				v

- Displays information for the board
show /SYS
- Power-on system
start /SYS

- Power-off system
stop /SYS
- Power-reset system
reset /SYS
- Display all system voltage
show /SYS/voltage
- Display all system fan
show /SYS/fan
- Display all system temperature
show /SYS/temperature
- Display all system power supply
show /SYS/powerSupply

/SYS

This command provides you the high-level status of the system chassis and main power subsystem.

Table 3.3: /SYS

PROPERTY NAME	VALID VALUE	ACCESS	DESCRIPTION
LOM/OCP Mezz/QCT Mezz	System MAC Address	R	<p>Dynamically to show System MAC address by LOM/OCP/QCT</p> <pre> /SYS Targets: voltage fan temperature powerSupply Properties: OCP Mezz = 08:9E:01:93:CD:88 OCP Mezz = 04:7D:7B:D9:4A:1D Quanta Mezz = 04:7D:7B:AC:D1:70 Quanta Mezz = 04:7D:7B:AC:D1:71 ChassisStatus = powerIsOFF Target Commands: show cd start stop reset </pre>
ChassisStatus	powerIsOFF powerIsON	R	<p>ChassisStatus provides the high-level status of the system chassis and main power subsystem.</p> <p>PowerIsOFF: indicates the system power is off</p> <p>PowerIsON: indicates the system power is on.</p>

Q&A

Q: I tried to turn system power off by IPMI command “**power soft**” when there is no response from operating system and system could not be shutdown. What is the Chassis Status?

A: The status of ChassisStatus is “**powerIsON.**”

/SYS/voltage

This command returns a high level version of the system voltages health status.

Table 3.4: /SYS/voltage

PROPERTY NAME	VALID VALUE	ACCESS	DESCRIPTION
Sensor name list of voltage	na ok nonCritical critical	R	na indicates the status not available /unknown (typically because system power is off) ok indicates the monitored parameters within normal operating ranges nonCritical indicates the hardware outside normal operating range critical indicates the hardware exceeding specified ratings

*The sensor name list depends on the Server Hardware.

/SYS/fan

This command returns a high level version of the system fan health status.

Table 3.5: /SYS/fan

PROPERTY NAME	VALID VALUE	ACCESS	DESCRIPTION
Sensor name list of fan	na ok nonCritical critical	R	na indicates the status not available /unknown (typically because system power is off) ok indicates the monitored parameters within normal operating ranges nonCritical indicates the hardware outside normal operating range critical indicates the hardware exceeding specified ratings

*The sensor name list depends on the Server Hardware.

/SYS/temperature

This command returns a high level version of the system temperature health status.

Table 3.6: /SYS/temperature

PROPERTY NAME	VALID VALUE	ACCESS	DESCRIPTION
Sensor name list of temperature	na ok nonCritical critical	R	na indicates the status not available /unknown (typically because system power is off) ok indicates the monitored parameters within normal operating ranges nonCritical indicates the hardware outside normal operating range critical indicates the hardware exceeding specified ratings

*The sensor name list depends on the Server Hardware.

/SYS/powerSupply

This command provides the specification of the Sensor Type sensor-specific event.

Table 3.7: /SYS/powerSupply

PROPERTY NAME	VALID VALUE	ACCESS	DESCRIPTION
Sensor name list of power supply	Presence* Power Supply Failure Detected* Predictive Fail* Power Supply Input Lost (AC/DC)* All Deasserted (*Note: Only for certain models.)	R	Presence Detected indicates the Power Supply Presence detected Power Supply Failure Detected indicates the Power Supply Failure detected Predictive Fail indicates the Power Supply Predictive Failure Power Supply Input Lost (AC/DC) indicates the Power Supply input lost, such as power cord not inserted All Deasserted indicates the power supply is not inserted
Redundancy	Fully Redundant Redundancy Lost	R	Fully Redundant Indicates the power redundancy is OK. Redundancy Lost Indicates the power redundancy is fail. One PSU is removed or AC lost. na When system powered off, the state is not available.

*The sensor name list depends on the Server Hardware.

Q&A:

Q1: My system supports two power supply slots and only one power supply unit connected. What is the other power supply status?

A1: The other power supply status is " AllDeasserted ".

Q2: My system supports two power supply slots and two power supply units connected. But only one power cord plugged. What is the other power supply status?

A2: The other power supply status shows "**Presence Detected, Predictive Fail, Power Supply Input Lost (AC/DC)**".

BMC Information

The BMC level commands provide several options to configure and display parameters of the management agent.

Table 3.8: Targets and Verbs

RELATED TARGETS	SUPPORTED VERBS										
	CD	EXIT	HELP	CREATE	DELETE	SET	SHOW	RESET	START	STOP	VERSION
/	v	v	v				v				v
/SP	v	v	v			v	v	v			v

- Displays information for the board

show /SP

- Reset BMC

reset /SP

- Set server identify LED to be off

set /SP ServerIdentify=off

- Set server identify LED to be on

set /SP ServerIdentify=on

- Set server identify LED to be blinking

set /SP ServerIdentify=blinking

/SP

Table 3.9: /SYS/fan

PROPERTY NAME	VALID VALUE	ACCESS	DESCRIPTION
BMCVersion		R	Display BMC firmware revision
BMCGUID		R	Display BMC GUID
ServerIdentify	off on blinking	R/W	Configuring server identify LED
BMCMAC		R	Display the NIC physical address used by server management agent

3.4 Web Graphical User Interface (GUI) for ESMS

Using the Web GUI

The BMC firmware features an embedded web server enabling users to connect to the BMC using a Web browser (e.g. Microsoft Internet Explorer). The Web GUI shows system information, system events, system status of managed servers, and other system-related information.

The Web-based GUI is supported on the following browsers:

- Internet Explorer 7 and above
- Firefox 8.0 and above
- Google Chrome 2.0 and above

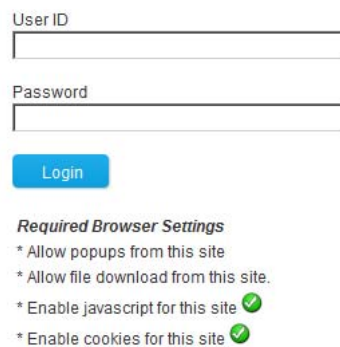
Login

Enter the IP address or URL (default DHCP\static IP address) into the address bar of the web browser.

When connecting to the BMC the Login screen prompts for the username and password. This authentication with SSL protection prevents unauthorized intruders from gaining access to the BMC web server.

When a user is authenticated they can manage the server according to the privilege of their role.

The OEM Proprietary, Administrator and Operator privilege levels are authorized to login to the web interface. The User and No Access privilege levels do not allow access through the BMC web GUI.



The screenshot shows the BMC login web page. It features two input fields: 'User ID' and 'Password'. Below these fields is a blue 'Login' button. Under the button, there is a section titled 'Required Browser Settings' with four bullet points: '* Allow popups from this site', '* Allow file download from this site', '* Enable javascript for this site' (marked with a green checkmark), and '* Enable cookies for this site' (marked with a green checkmark).

Figure 3-3. Login Web Page

Table 4: Default Username and Password

FIELD	DEFAULT
Username	qct.admin
Password	qct.admin

After passing authentication, the following web page appears.

Note:

The default username and password are in lowercase characters. It is advised to change the admin password once you have logged in.

Click the **Help** button on the right corner of the page for assistance, the **Refresh** button to refresh the page, or the **Logout** button to exit.

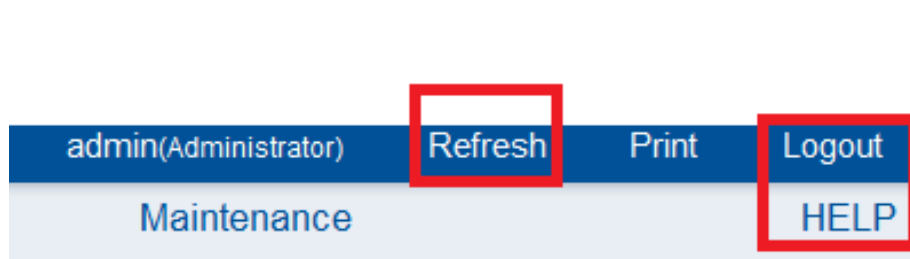


Figure 3-4. Main Web Page

Table 5: Main Web Page

MENU ITEM	DESCRIPTION
Dashboard	Displays the device, network, sensor monitoring and event logs information.
Server information	Shows system information.
Server Health	Monitoring status of the server.
Configuration	Configuration of the IPMI settings.
Remote Control	Launch KVM console and perform power control.
Maintenance	Allows the user to configure the preserve configuration items.
Firmware Update	Allows the user to do firmware update

Dashboard

In MegaRAC GUI, the Dashboard page displays the overall information on status of the device.

To open the **Dashboard** page, click Dashboard from the main menu. A sample screenshot of the Dashboard page is as follows:

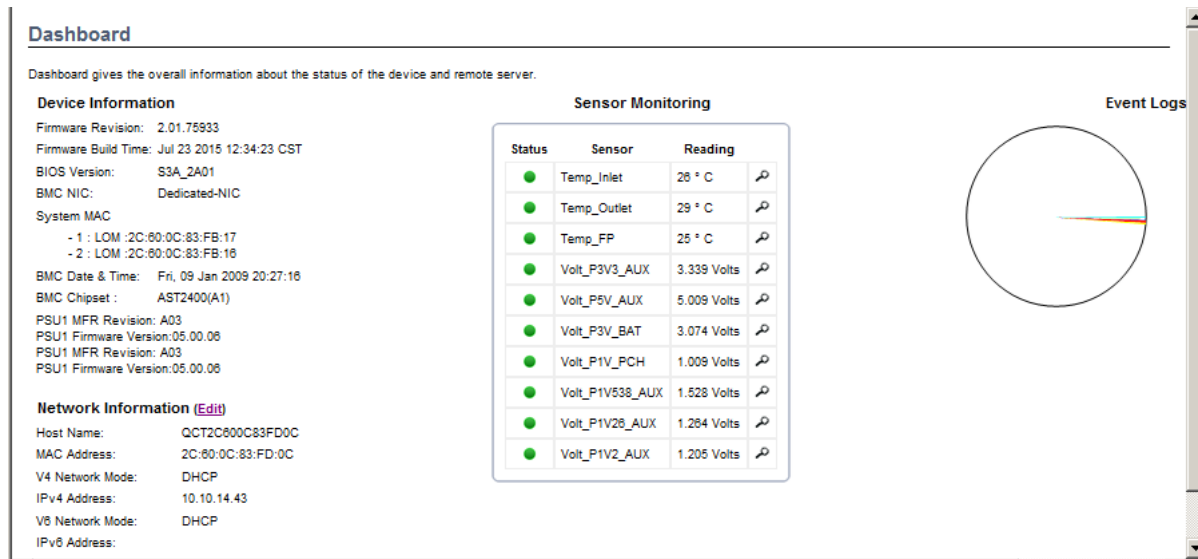


Figure 3-5. Dashboard

A brief description of the Dashboard page is given in the next section.

Device Information

The Device Information displays the following information:

Table 6: Device Information Page

ITEM	DESCRIPTION
Firmware Revision	The revision number of the firmware.
Firmware Build Time	Firmware date and time.
BIOS Version	The current BIOS firmware version.
PSU1 MFR Revision	Display PSU1 manufacture revision.
PSU1 Firmware version	Display PSU1 Firmware version.
PSU2 MFR Revision	Display PSU2 manufacture revision.
PSU2 Firmware version	Display PSU2 firmware version.
PDB Firmware Version	The current PDB (Power Distribution Board) firmware version.
FCB Version	The current FCB (Fan Control Board) firmware version.
PSU Max output Power	Display power supply max output power (Watts).
MB Position	Display the current position of the mainboard within the chassis.
Blackplane F/W version	Display current backplane firmware version.
BMC NIC	Display current used NIC.
System MAC	The maximum MAC address of system LAN port is 8. From Grantley platform, BMC supports to show LAN Card Type (LOM/OCF Mezzanine/Quanta Mezzanine) for System MAC.

Table 6: Device Information Page (Continued)

ITEM	DESCRIPTION
BMC Date & Time	The current time of BMC system.
BMC Chipset	This field shows BMC chipset type.

Note:

BMC Chipset type support list:

- (1) AST2300/AST2400: support virtual KVM function and related setting item.
- (2) AST2300/AST2400 without RKVM: not support virtual KVM function and related setting item.
- (3) AST2050/AST2150: support virtual KVM function and related setting item.
- If BMC Chipset type is "AST2300/AST2400 without RKVM", Console Redirection, Mouse Mode, Remote Session, and Virtual Media menu item will be removed.

Network Information

The Network Information of the device with the following fields is shown in the following table. To edit the network Information, click **Edit**.

Table 7: Network Information

ITEM	DESCRIPTION
Host Name	Read only field showing the DNS Hostname of the device.
MAC Address	Read only field showing the BMC MAC address of the device.
V4 Network Mode	The v4 network mode options are static or DHCP.
IPv4 Address	The IPv4 address of the device (could be static or DHCP).
V6 Network Mode	The v6 network mode options are static or DHCP.
IPv6 Address:	The IPv6 address of the device.
IPv6 Link Local Address	The IPv6 link local address of the device.

Sensor Monitoring

Lists all the available sensors on the device.

The status column displays the state of the device as follows:

Table 3-1:





STATUS (ICON)	DESCRIPTION
	Normal state

Table 3-1:

STATUS (ICON)	DESCRIPTION
	Warning state
	Critical state

If you click on , the sensor page for that particular sensor will be displayed.

Event Logs

A graphical representation of all events incurred by various sensors as well as occupied/available space in logs. Clicking on the color-coded rectangle in the Legend for the chart, allows to view a list of specific events only.

Server Information

The Server Information Group consists of the following items:

- FRU Information
- Server Component
- Server Identify
- BIOS POST Code

The following screenshot displays the Server Information menu items:

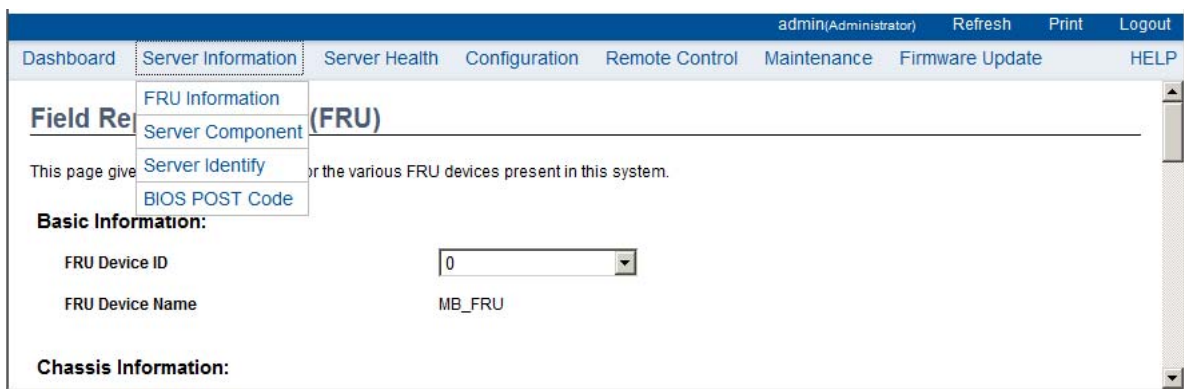


Figure 3-6. Server Information – Menu

FRU Information

In the MegaRAC GUI, the FRU Information Page displays the BMC FRU file information. The information displayed in this page is Basic Information, Common Header Information, Chassis Information, Board Information and Product Information of the FRU device.

To open the FRU Information Page, click on **FRU Information** on top menu. Select a FRU Device ID from the Basic Information section to view the details of the selected device. A screenshot of FRU Information page is shown as follows:

Field Replaceable Unit(FRU)

This page gives detailed information for the various FRU devices present in this system.

Basic Information:

FRU Device ID: 0

FRU Device Name: MB_FRU

Chassis Information:

Chassis Information Area Format Version: 1

Chassis Type: Rack Mount Chassis

Chassis Part Number: N/A

Chassis Serial Number: N/A

Chassis Extra: N/A N/A

Board Information:

Board Information Area Format Version: 1

Language: English

Manufacture Date Time: Thu Jan 1 12:12:00 2009

Board Manufacturer: Quanta Computer Inc.

Board Product Name: S3A

Board Serial Number: dfgfhdfg

Figure 3-7. FRU Information Page

A brief description of the fields is given in the following sections.

Basic Information

Table 4: Basic Information

ITEM	DESCRIPTION
FRU device ID	The ID of the device.
FRU Device Name	The device name of the selected FRU device.

Chassis Information

- Chassis Information Area Format Version
- Chassis Type
- Chassis Part Number
- Chassis Serial Number
- Chassis Extra

Board Information

- Board Information Area Format Version
- Language

- Manufacture Date Time
- Board Manufacturer
- Board Product Name
- Board Serial Number
- Board Part Number
- FRU File ID
- Board Extra

Product Information

- Product Information Area Format Version
- Language
- Manufacturer Name
- Product Name
- Product Part Number
- Product Version
- Product Serial Number
- Asset Tag

Server Component

The Component Information page displays the CPU and memory information. The Number of CPU Socket field and the Number of Memory Slot field display the total number of the motherboard supported.

admin(Administrator)RefreshPrintLogout

DashboardServer InformationServer HealthConfigurationRemote ControlMaintenanceFirmware UpdateHELP

Component Information

This page displays component information. You can choose a category from the pull-down box to filter the components, and also sort them by clicking on a column header. Select a component type category:

CPU Information

Number of CPU Socket: 1 sockets

ID	Status	Socket	Manufacturer	Model	Frequency
1	Enable	CPU	Intel	Skylake S	2600MHz

Refresh

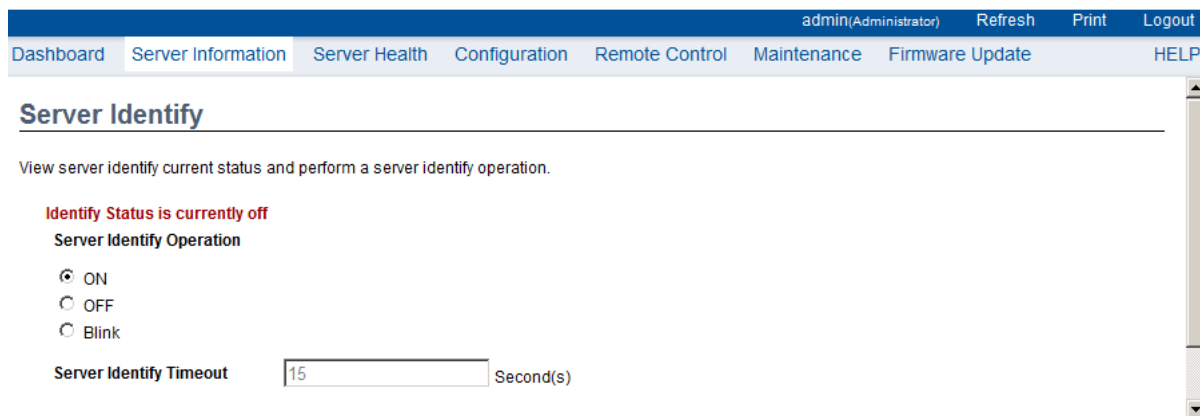
Figure 3-8. Component Information Page

Table 5: Component Information Page

ITEM	DESCRIPTION
CPU Information	Displays the following information: <ul style="list-style-type: none"> • CPU ID, • Status, • Socket, • Manufacturer, • Model, • Frequency
Memory Information	Displays the following information: <ul style="list-style-type: none"> • Memory ID, • Status, • Socket, • Module Size, • Model, • Frequency

Server identify

The Server Identify page displays the indicator LED status. You can select a Server Identify Operation to control the indicator LED.



The screenshot shows the BMC web interface with the 'Server Information' tab selected. The 'Server Identify' section displays the current status as 'off' and provides options to set the LED operation to ON, OFF, or Blink. A timeout value of 15 seconds is entered for the Blink operation.

Figure 3-9. Server Identify Page

Table 6: Server Identify Page

ITEM	DESCRIPTION
Current Server Identify Status	The server status: On or Off.
Server Identify Operation	Server identify LED operation with the following options: <ul style="list-style-type: none"> • ON • OFF • Blink
Server Identify Timeout	Setup server timeout value when a Blink Identify Operation is selected. For Blink Operation the time period must be from 1 to 255 seconds. When 255 seconds is selected, the blinking is continuous.

Table 6: Server Identify Page (Continued)

ITEM	DESCRIPTION
Perform Action	Executes the selected Server Identify Operation.

BIOS POST Code

The page displays recent BIOS Port 80h POST code.

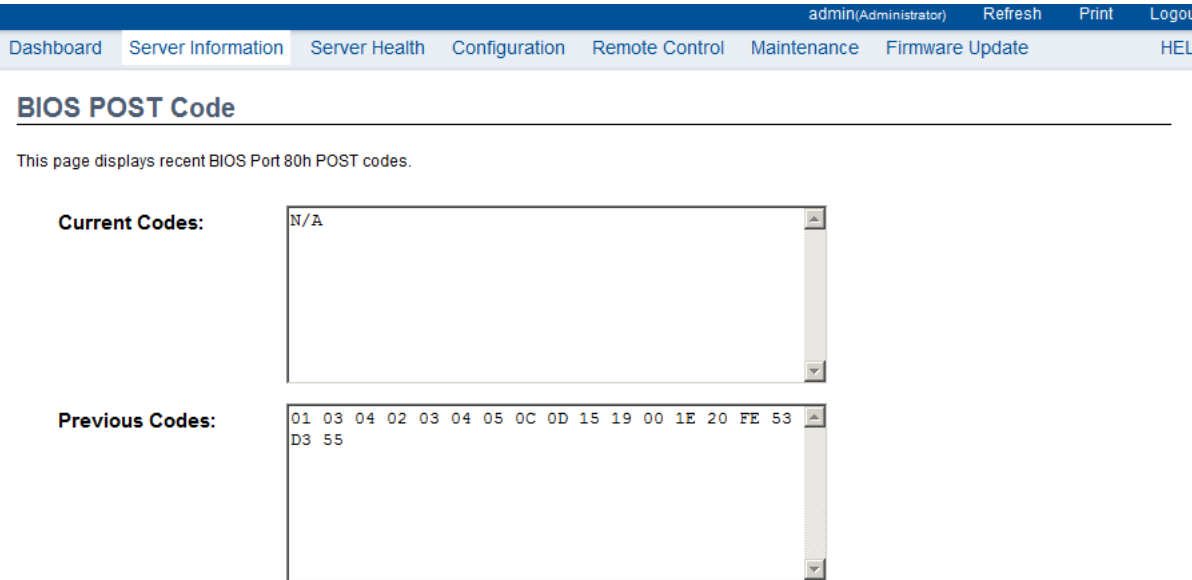


Figure 3-10. BIOS POST Code

Table 7: BIOS POST Code Page

ITEM	DESCRIPTION
Current Codes	Current BIOS Port 80h POST code
Previous Codes	Previous BIOS Port 80h POST code

Server Health Group

The Server Health Group consists of the following items:

- Sensor Readings
- Event Log

The Server Health screenshot allows to select Sensor Readings or Event Log as shown in the following image:

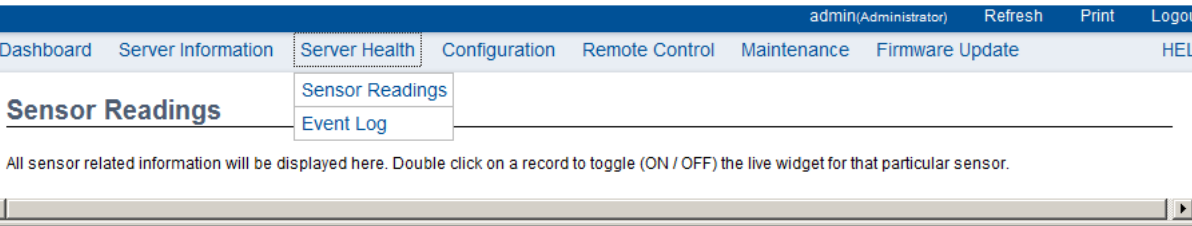


Figure 3-11. Server Health – Menu

Sensor Readings

In MegaRAC GUI, the Sensor Readings page displays all the sensor related information.

To open the Sensor readings page, click **Server Health > Sensor Readings** from the top menu. Click on a record to display more information on a particular sensor, including thresholds and a graphical representation of all associated events. A screenshot of Sensor Readings page is shown in the following image:

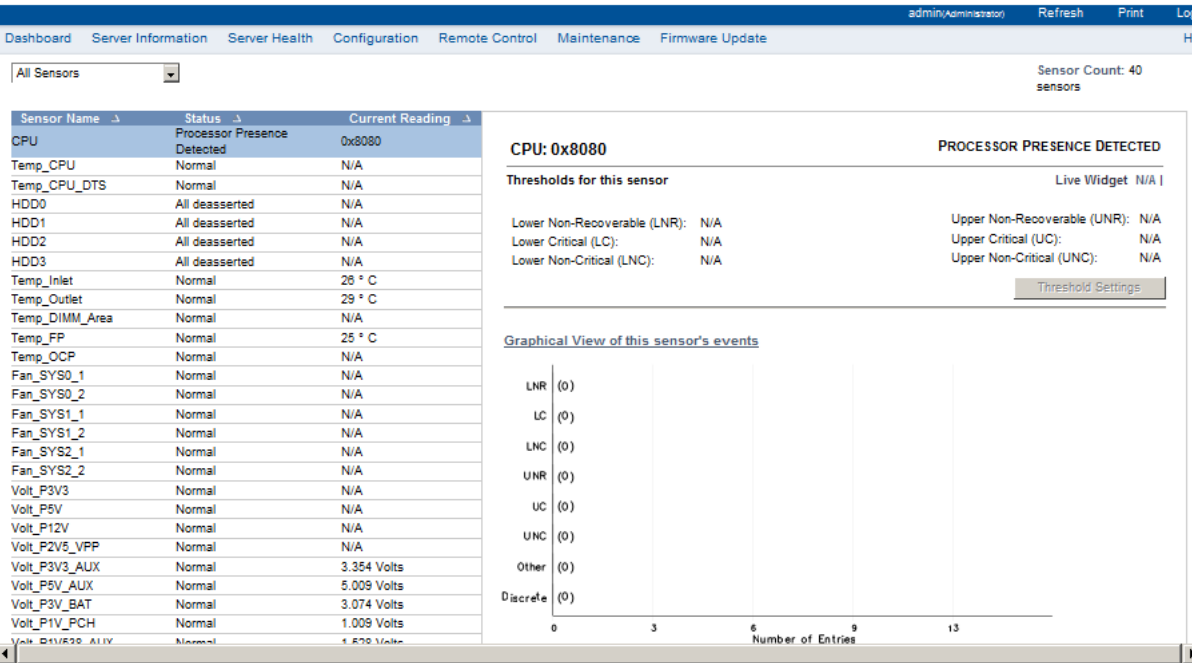


Figure 3-12. Sensor Readings Page

A brief description of the Sensor Readings page fields is given in the following sections.

Sensor Type

This drop down menu allows you to select the type of sensor. The List of sensors with the Sensor Name, Status and Current Reading will be displayed in the list. If you select All Sensors, all the available sensor details will appear else you can choose the sensor type that

you want to display in the list. Some examples of other sensors include Temperature Sensors, Fan Sensors, and Voltage Sensors etc.

Select a particular sensor from the list. You can view the Thresholds for this sensor on the right hand side of the screen.

Thresholds are of six types:

- Lower Non-Recoverable (LNR)
- Lower Critical (LC)
- Lower Non-Critical (LNC)
- Upper Non-Recoverable (UNR)
- Upper Critical (UC)
- Upper Non-Critical (UNC)

The threshold states could be:

Lower Non-critical - going low,
Lower Non-critical - going high,
Lower Critical - going low,
Lower Critical - going high,
Lower Non-recoverable - going low,
Lower Non-recoverable - going high,
Upper Non-critical - going low,
Upper Non-critical - going high,
Upper Critical - going low,
Upper Critical - going high,
Upper Non-recoverable - going low,
Upper Non-recoverable - going high.

A graphical view of these events (Number of event logs vs. Thresholds) can be viewed as shown in the Sensor Readings Page screenshot.

Live Widget

The widget window can be turned On and Off for a selected sensor. Widget provides a dynamic representation of the readings for the sensor. The following image shows an example widget:

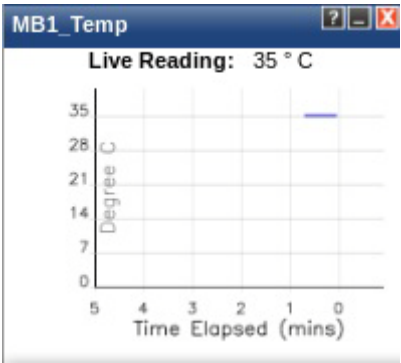


Figure 3-13. Widget Window

Note:

Widgets are little gadgets, which provide real time information about a particular sensor. User can track a sensor's behavior over a specific amount of time at specific intervals. The result will be displayed as a line graph in the widget. The session will not expire, until the widgets gets a live data of the last widget that is kept opened.

View this Event Log

View the Event Log page for the selected sensor.

Sensor Reading status

You can read currently sensor status in this page, each sensor name has its SDR setting data, the status according SDR setting will display as following matrix:

Table 8: Sensor Readings status

STATUS	CURRENT READING
N/A	N/A
All deasserted	0x80xx(*2)
Normal	Value with unit
Event string(*1)	
(*1) Please refer IPMI2.0 standard specification chapter 42.	
(*2) Please refer IPMI2.0 standard specification chapter 42 and SDR setting in BMC function specification.	

Event Log

In MegaRAC GUI, this page displays the list of event logs occurred by the different sensors on this device. Double click on a record to see the details of that entry. You can use the

sensor type or sensor name filter options to view those specific events or you can also sort the list of entries by clicking on any of the column headers.

To open the Event Log page, click **Server Health > Event Log** from the top menu. A sample screenshot of the Event Log page is shown as follows.

admin(Administrator) Refresh Print Log

Dashboard Server Information Server Health Configuration Remote Control Maintenance Firmware Update HE

Event Log

Events generated by the system will be logged here. Double-click on a record to see the description.

All Events filter by: All Sensors Event Log: 13 event entries, 1 page(s)

☒ BMC Timezone ☐ Client Timezone UTC Offset: (GMT+05:00)

Event ID	Time Stamp	Severity	Sensor Name	Sensor Type	Description
13	01/09/2009 20:15:34	i	Power Unit	Power Unit	Power Off / Power Down - Asserted
12	01/09/2009 20:15:29	i	Button	Button / Switch	Power Button Pressed - Asserted
11	01/09/2009 20:12:31	x	CATERR	Processor	IERR - Asserted
10	01/09/2009 20:12:31	w	POSTF	POST POSTF	System Firmware Error No system memory is physically

Save Event Logs Clear All Event Logs

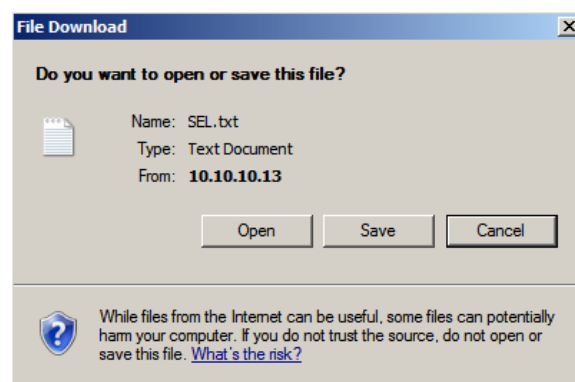
Figure 3-14. Event Log Page

Save Event Logs

Note:

The size of event log is 909 records for maximum and $909 \times 75\% = 681$ records for almost full. The status LED blinks with color amber when the event logs reach almost full. It stops recording new events when full.

You could click on **Save Event Logs** button to save your system's event logs.



The Event Log page consists of the following fields.

Table 9: Event Log Page




ITEM	DESCRIPTION
Event Log Category	<p>The category options:</p> <ul style="list-style-type: none"> • All Events, • System Event Records, • BIOS Generated Events, • SMI Handler Events, • System Management Software Events, • System Software - OEM Events, • Remote Console Software Events, • Terminal Mode Remote Console Software Events.
Filter Type	<p>Filtering can be done with the sensors mentioned in the list. Once the Event Log category and Filter type are selected, the list of events will be displayed with:</p> <ul style="list-style-type: none"> • Event ID • Time Stamp • Sensor Type • Sensor Name • Description
BMC Timezone	BMC UTC offset timestamp value of the events.
Client Timezone	Events of client UTC offset timestamp.
UTC Offse	Displays the current UTC Offset value based on which event Time Stamps will be updated. Navigational arrows can be used to selectively access different pages of the Event Log.
Clear All Event Logs	Deletes all the existing records for all the sensors.
Save Event Logs	To save all the existing Event Log records.

Procedure:

1. Select the event categories from the **Event Log Category** drop-down menu.
2. Select the sensor name filter to view the event for the selected filter from the **Filter Type** drop-down list.
3. Select either **BMC Timezone** or **Client Timezone**. The list of events is listed.
4. Click the **Clear All Event Logs** button to clear all events from the list.
5. To save all the existing event logs, click on **Save Event Logs** button.

SEL Severity

The Event Log page specifies the severity of the SEL to identify the event severity code as follows:

- : Severity Information
- : Severity Warning
- : Severity Critical

-  : Severity Unspecified

Configuration Group

Configuration Group page allows to access various configuration settings. A screenshot of the Configuration Group menu is shown in the following figure:

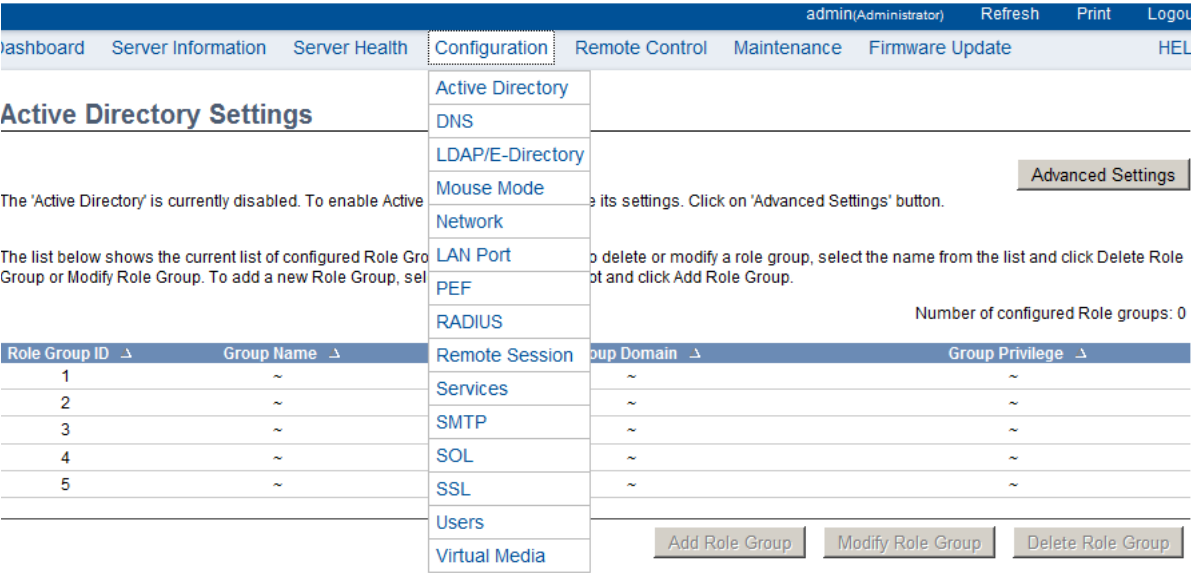


Figure 3-15. Configuration Group Menu

A detailed description of the Configuration menu is given in the following sections.

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. An active directory (sometimes referred to as an AD) does a variety of functions including the ability to provide information on objects, helps organize these objects for easy retrieval and access, allows access by end users and administrators and allows the administrator to set up security for the directory.

This page in MegaRAC SP-X, allows you to configure Active Directory Server Settings.

To open Active Directory Settings page, click on **Configuration > Active Directory** from the main menu. A sample screenshot of Active Directory Settings Page is shown in the screenshot below.

admin(Administrator) Refresh Print Logout

Dashboard Server Information Server Health Configuration Remote Control Maintenance Firmware Update HELP

Active Directory Settings

The 'Active Directory' is currently disabled. To enable Active Directory and configure its settings. Click on 'Advanced Settings' button.

Advanced Settings

The list below shows the current list of configured Role Groups. If you would like to delete or modify a role group, select the name from the list and click Delete Role Group or Modify Role Group. To add a new Role Group, select an unconfigured slot and click Add Role Group.

Number of configured Role groups: 0

Role Group ID ↴	Group Name ↴	Group Domain ↴	Group Privilege ↴
1	~	~	~
2	~	~	~
3	~	~	~
4	~	~	~
5	~	~	~

Add Role Group Modify Role Group Delete Role Group

Figure 3-16. Active Directory Settings Page

Table 10: Active Directory Settings Page

ITEM	DESCRIPTION
Advanced Settings	This option is used to configure Active Directory Advanced Settings. Options are: Enable Active Directory Authentication, User Domain name, Time Out and up to three Domain Controller Server Addresses.
Role Group ID	The ID that identifies the role group in the Active Directory.
Group Name	This name identifies the role group in Active Directory. Note: <ul style="list-style-type: none"> Role Group Name is a string of 64 alpha-numeric characters. Special symbols (hyphen and underscore) are allowed.
Group Domain	The domain where the role group is located. Note: <ul style="list-style-type: none"> Domain Name is a string of 255 alpha-numeric characters. Special symbols (hyphen and underscore) and dot are allowed.
Group Privilege	The level of privilege to assign this role group.
Add Role Group	To add a new role group to the device.
Modify Role Group	To modify that role group. Alternatively, double click on the configured slot.
Delete Role Group	To delete an existing Role Group.

Procedure:

Entering the details in Advanced Active Directory Settings Page

1. Click on **Advanced Settings** to open the Advanced Active Directory Settings Page.

Figure 3-17. Advanced Active Directory Settings Page

2. In the Active Directory Settings page, select or unselect the Enable check box to enable or disable Active Directory Authentication respectively..

Note:

If you have enabled Active Directory Authentication, enter the required information to access the Active Directory server.

3. Specify the Secret user name and password in the Secret User Name and Secret Password fields respectively.

Note:

Enter the required information to access the Active Directory server if Active Directory Authentication enabled.

- Secret username/password for AD is not mandatory. if the AD's secret username/password is not provided, AD should be kept in the last location in PAM order.
- User Name is a string of 1 to 64 alpha-numeric characters.
- It must start with an alphabetical character.
- It is case-sensitive.
- Special characters like comma, period, colon, semicolon, slash, backslash, square brackets, angle brackets, pipe, equal, plus, asterisk, question mark, ampersand, double quotes, space are not allowed.
- Password must be at least 6 character long and will not allow more than 127 characters.
- White space is not allowed.

4. Specify the Domain Name for the user in the **User Domain Name** field. e.g. MyDomain.com.
5. Specify the time (in seconds) to wait for Active Directory queries to complete in the **Time Out** field.

Note:

- Default Time out value: 120 seconds.
- Range from 15 to 300 allowed.

6. Configure IP addresses in **Domain Controller Server Address1**, **Domain Controller Server Address2** & **Domain Controller Server Address3**.

Note:

IP address of Active Directory server: At least one Domain Controller Server Address must be configured.

- IP Address made of 4 numbers separated by dots as in "xxx.xxx.xxx.xxx".
- Each number ranges from 0 to 255.
- First number must not be 0.

Domain Controller Server Addresses will support IPv4 Address format and IPv6 Address format.

7. Click **Save** to save the settings and return to Active Directory Settings Page.
8. Click **Cancel** to cancel the entry and return to Active Directory Settings Page.

To add a new Role Group

1. Select a blank row and click **Add Role Group** in the Active Directory Settings Page to open the Add Role Group Page as shown in the screenshot below.

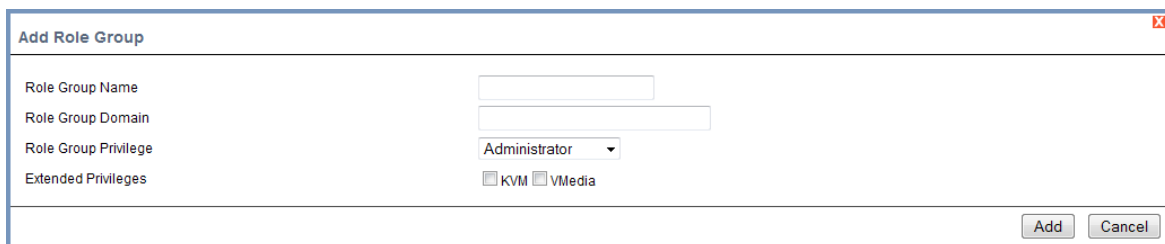


Figure 3-18. Add Role Group Page

2. Enter the name that identifies the role group in the Active Directory from the **Role Group Name** field.

Note:

- Role Group Name is a string of 255 alpha-numeric characters.
- Special symbols hyphen and underscore are allowed.

3. Enter the domain where the role group is located in the **Role Group Domain** field.

Note:

- Domain Name is a string of 255 alpha-numeric characters.
- Special symbols hyphen, underscore and dot are allowed.

4. Enter the level of privilege to assign this role group in the **Role Group Privilege** field.

5. Select the required options (KVM or VMedia) in the Extended Privilege.
6. Click **Add** to save the new role group and return to the Role Group List.
7. Click **Cancel** to cancel the settings and return to the Role Group List.

To modify a Role Group

1. Select the row or double click the row that you would like to modify and click **Modify Role Group** in the Advanced Directory Settings Page.
2. Make the necessary changes and click **Save**.

To delete a Role Group

Select the row to delete and click **Delete Role Group**, in the Advanced Directory Settings Page.

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. It associates the information with domain names assigned to each of the participants. Most importantly, it translates domain names meaningful to humans into the numerical (binary) identifiers associated with networking equipment for the purpose of locating and addressing these devices worldwide.

In Mega-RAC GUI, the DNS Server settings page is used to manage the DNS settings of a device.

In DNS Server Settings page, you can click **Configuration > DNS** from the main menu. A DNS Server Settings Page is shown in the screenshot below.

The screenshot shows the 'DNS Server Settings' page. At the top, there's a navigation bar with 'admin/Administrator', 'Refresh', 'Print', and 'Logout'. Below it, a menu bar includes 'Dashboard', 'Server Information', 'Server Health', 'Configuration', 'Remote Control', 'Maintenance', 'Firmware Update', and 'HELP'. The main heading is 'DNS Server Settings'. Underneath, it says 'Manage DNS settings of the device.' The settings are organized into several sections: 'Domain Name Service Configuration' with a 'DNS Service' checkbox checked and labeled 'Enable'; 'Multicast DNS' with 'mDNS Settings' checkbox unchecked and labeled 'Enable'; 'Host Configuration' with 'Host Settings' dropdown set to 'Automatic' and 'Host Name' text field containing 'QCT2C800C83FD0C'; 'Register BMC' with 'bond0' interface, 'Register BMC' checkbox checked, and radio buttons for 'Nsupdate' (selected), 'DHCP Client FQDN', and 'Hostname'; 'Domain Name Configuration' with 'Domain Settings' dropdown set to 'bond0_v4' and 'Domain Name' text field containing 'gate204.local'; and 'Domain Name Server Configuration' with 'DNS Server Settings' dropdown set to 'bond0', 'IP Priority' radio buttons for 'IPv4' (selected) and 'IPv6', 'DNS Server1' text field containing '168.95.1.1', and 'DNS Server2' text field containing '10.10.10.204'.

Figure 3-19. DNS Server Settings Page

The fields of DNS Server Settings page are explained below.

Table 11: DNS Server Settings Page

ITEM		DESCRIPTION
DOMAIN NAME SERVICE CONFIGURATION	DNS Service	To enable/disable all the DNS Service Configurations.
MULTICAST DNS SUPPORT	mDNS Settings	To enable/disable the mDNS Support Configurations.
HOST CONFIGURATION	Host Settings	Choose either Automatic or Manual settings.
	Host Name	<p>It displays hostname of the device. If the Host setting is chosen as Manual, then specify the hostname of the device.</p> <p>Note:</p> <ul style="list-style-type: none"> - Value ranges from 1 to 64 alpha-numeric characters. - Special characters '-'(hyphen) and '_'(underscore) are allowed. - It must not start or end with a '-'(hyphen). IE browsers won't work correctly if any part of the host name contain underscore () character.

Table 11: DNS Server Settings Page (Continued)

ITEM		DESCRIPTION
REGISTER BMC		To enable/disable Register BMC.
TSIG CONFIGURATION	TSIG Authentication	To enable/disable TSIG authentication while registering in DNS via Direct Dynamic DNS.
	Current TSIG Private File	The information of Current TSIG private file along with its up-loaded date/time will be displayed (read only).
	New TSIG Private File	Browse and navigate to the TSIG private file. Note: TSIG file should be of private type.
DOMAIN NAME CONFIGURATION	Domain Settings	It lists the option for domain interface as Manual, v4 or v6 for multiLAN channels. Note: If you choose DHCP, then select v4 or v6 for DHCP servers.
	Domain Name	It displays the domain name of the device. If the Domain setting is chosen as Manual, then specify the domain name of the device. If you chose Automatic, the Domain Name cannot be configured as it will be done automatically. The field will be disabled.
DOMAIN NAME SERVER CONFIGURATION	DNS Server Settings	It lists the option for DNS settings for the device, Manual and available LAN interfaces. If you choose Manual setting, you have to configure the DNS Server IP addresses. If you have chosen DHCP, then you have to select the interface from which the IP address is to be received.
	IP Priority	If IP Priority is IPv4, it will have 2 IPv4 DNS servers and 1 IPv6 DNS server. If IP Priority is IPv6, it will have 2 IPv6 DNS servers and 1 IPv4 DNS server. Note: It is not applicable for Manual configuration.
	DNS Server1, DNS Server2, and DNS Server3	Specify the DNS (Domain Name System) server address to be configured for the BMC. <ul style="list-style-type: none"> IPv4 Address made of 4 numbers separated by dots as in "xxx.xxx.xxx.xxx". Each number ranges from 0 to 255. First number must not be 0. DNS Server Address will support the following: <ul style="list-style-type: none"> IPv4 Address format. IPv6 Address format. Note: <ul style="list-style-type: none"> If IP Priority is IPv4 then DNS Server1, DNS Server2 will be IPv4 and DNS Server3 will be IPv6. If IP Priority is IPv6 then DNS Server1, DNS Server2 will be IPv6 and DNS Server3 will be IPv4. If no IP, DNS Server field will be empty.
SAVE		To save the entered changes.
RESET		To reset the entered changes.

Procedure:

1. In **Domain Name Service Configuration**, Enable **DNS Service**.
 - Check the option **Enable** to enable all the DNS Service Configurations.
2. Choose the **Host Configuration** either Automatic or Manual.

Note:

If you choose Automatic, you need not enter the Host Name and if you choose Manual, you need to enter the Host Name.

3. Enter the **Host Name** in the given field if you have chosen Manual Configuration.
4. Under **Register BMC**, choose the BMC's network port to register with DNS settings.
 - Check the option **Register BMC** to register with this DNS settings.
 - **Nsupdate** - Choose **Nsupdate** option to register with DNS server using nsupdate application.
 - **DHCP Client FQDN** - Choose **DHCP Client FQDN** option to register with DNS Server using DHCP option 81.
 - **Hostname** - Choose **Hostname** option to register with DNS server using DHCP option 12.

Note:

Hostname option should be selected if the DHCP client FQDN option is not supported by DHCP server.

5. Enable **TSIG Authentication** in **TSIG Configuration**.
 - The current file name will be displayed in Current TSIG private file.
 - To view a new one, browse and navigate to the TSIG private file.
6. In the **Domain Name Configuration**,
 - Select the **Domain Settings** from the drop-down list.
 - Enter the **Domain Name** in the given field if the option "**Manual**" is being selected in domain settings field.
7. In the **Domain Name Server Configuration**,
 - Select the **DNS Server Settings** from the drop-down list.
 - In the **IP Priority**, set IPV4 or IPV6 as a top priority.
 - In the **DNS Server1/DNS Server2/DNS Server3** field,
If the DNS Server Settings is setting to Manual mode, user needs to fill those fields with DNS IP address manually according to IPv4 or IPv6 format. Otherwise, if it is in non-Manual mode, DNS server IP address is assigned by DHCP server.
8. Click **Save** to save the entries.
9. Click **Reset** to reset the entries.

LDAP/E-Directory

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

In MegaRAC GUI, LDAP is an Internet protocol that MegaRAC® card can use to authenticate users. If you have an LDAP server configured on your network, you can use it as an easy way to add, manage and authenticate MegaRAC® card users. This is done by passing login requests to your LDAP Server. This means that there is no need to define an additional authentication mechanism, when using the MegaRAC card. Since your existing LDAP Server keeps an authentication centralized, you will always know who is accessing the network resources and can easily define the user or group-based policies to control access.

To open LDAP Settings page, click **Configuration > LDAP** from the main menu. A sample screenshot of LDAP Settings Page is shown in the screenshot below.

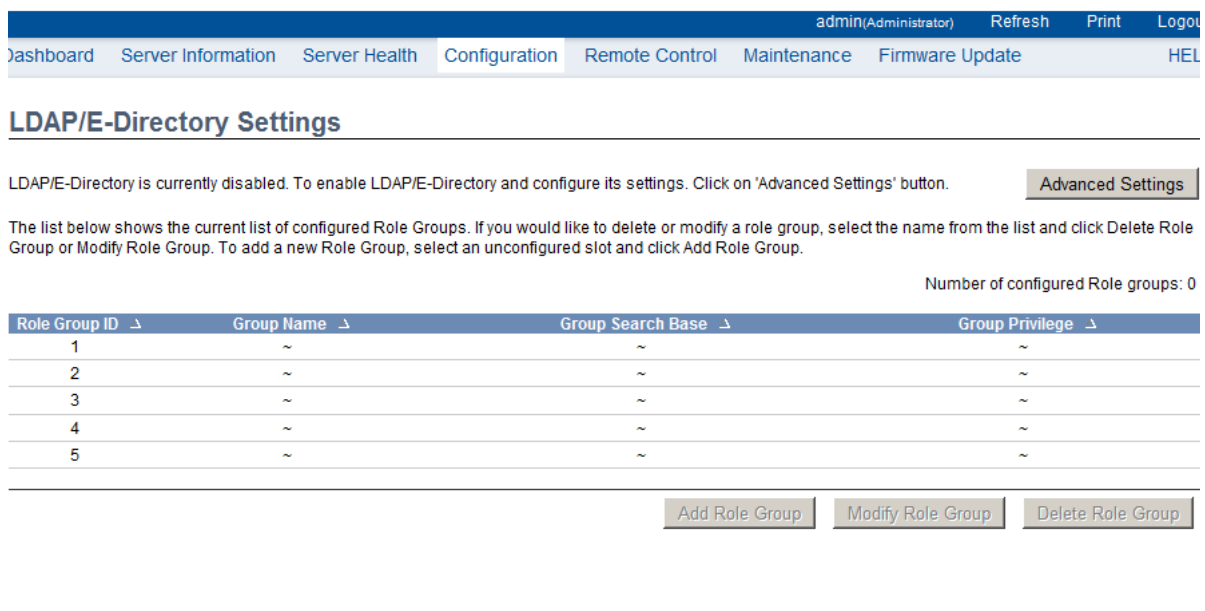


Figure 3-20. LDAP Settings Page

The fields of LDAP Settings Page are explained below.

Table 12: LDAP Settings Page

ITEM	DESCRIPTION
Advanced Settings	To configure LDAP Advanced Settings. Options are Enable LDAP Authentication, IP Address, Port and Search base.
Add Role Group	To add a new role group to the device. Alternatively, double click on a free slot to add a role group.
Modify Role Group	To modify the particular role group.
Delete Role Group	To delete a role group from the list.

Procedure:

Entering the details in Advanced LDAP/E-Directory Settings Page

1. In the LDAP Settings Page, click Advanced Settings. A sample screenshot of LDAP/E-Directory Settings page is given below.

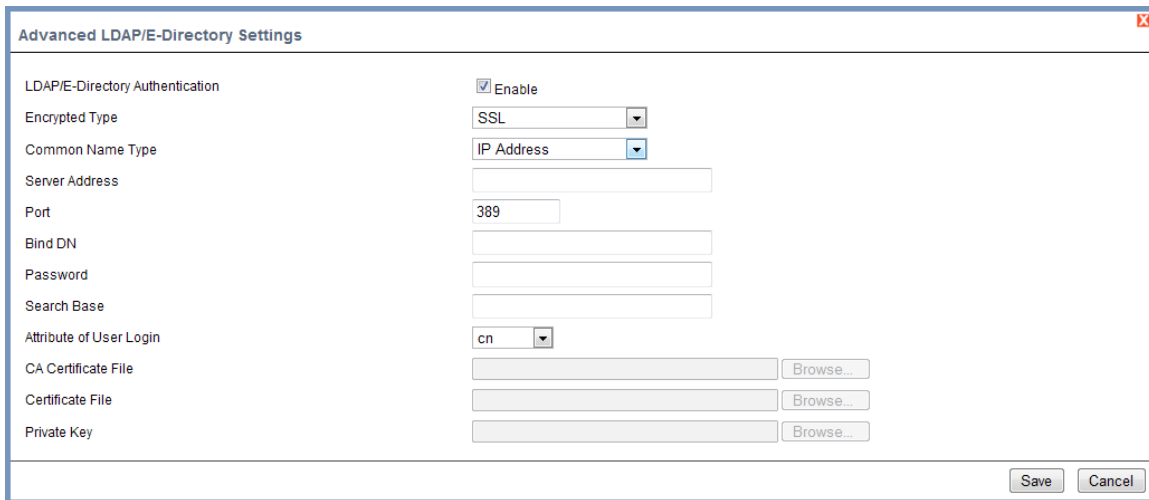


Figure 3-21. Advanced LDAP/E-Directory Settings

2. To enable/disable LDAP/E-Directory Authentication, check or uncheck the **Enable** checkbox respectively.

Note:

During login prompt, use username to login as an LDAP Group member.

3. Select the encryption type for LDAP/E-Directory from the Encrypted Type drop-down list.

Note:

Configure proper port number, when SSL is enabled.

4. Select the **Common Name Type** as **IP Address**.
5. Enter the IP address of LDAP server in the **Server Address** field.

Note:

- IP Address made of 4 numbers separated by dots as in 'xxx.xxx.xxx.xxx'.
- Each Number ranges from 0 to 255.
- First Number must not be 0.
- Supports IPv4 Address format and IPv6 Address format.

6. Specify the LDAP Port in the **Port** field.

Note:

Default Port is 389. For Secure SSL connection, default port is 636. The Port value ranges from 1 to 65535.

7. Specify the **Bind DN** that is used during bind operation, which authenticates the client to the server.

Note:

- Bind DN is a string of 4 to 64 alpha-numeric characters.
- It must start with an alphabetical character.
- Special Symbols like dot(.), comma(,), hyphen(-), underscore(_), equal-to(=) are allowed.
- Example: cn=manager, ou=login, dc=domain, dc=com .

8. Enter the password in the **Password** field.

Note:

- Password must be at least one character long.
- White space is not allowed.
- This field will not allow more than 48 characters.

9. Enter the **Search Base**. The Search base tells the LDAP server which part of the external directory tree to search. The search base may be something equivalent to the organization, group of external directory.

Note:

- Search base is a string of 4 to 63 alpha-numeric characters.
- It must start with an alphabetical character.
- Special Symbols like dot (.), comma (,), hyphen(-), underscore (_), equal-to (=) are allowed.
- Example: ou=login, dc=domain, dc=com

10. Select **Attribute of User Login** to find the LDAP/E-Directory server which attribute should be used to identify the user.

Note:

It only supports cn or uid.

11. Select **CA Certificate File** from the Browse field to identify the certificate of the trusted CA certs.

12. Select the **Certificate File** to find the client certificate filename.

13. Select **Private Key** to find the client private key filename.

Note:

All the 3 files are required, when StartTLS is enabled.

14. Click **Save** to save the settings.

15. Click **Cancel** to cancel the modified changes.

To add a Role Group

1. Select a blank row and click **Add Role Group** to open the Add Role Group Page as shown in the screenshot below from the LDAP/E-Directory Settings Page.

Figure 3-22. Add Role Group Page

2. Enter the name that identifies the role group in the **Role Group Name** field.

Note:

- Role Group Name is a string of 255 alpha-numeric characters.
- Special symbols hyphen and underscore are allowed.

3. Enter the path from where the role group is located to Base DN in the **Role Group Search Base** field.

Note:

- Search Base is a string of 255 alpha-numeric characters.
- Special symbols hyphen, underscore and dot are allowed.

4. Enter the level of privilege to assign to this role group in the **Role Group Privilege** field.
5. Select the required options (KVM or VMedia) in the Extended Privileges option.
6. Click **Add** to save the new role group and return to the Role Group List.
7. Click **Cancel** to cancel the settings and return to the Role Group List.

To Modify Role Group

1. Select the row or double click that you would like to modify and click **Modify Role Group** in the LDAP/E-Directory Settings Page.
2. Make the necessary changes and click **Save**.

To Delete a Role Group

Select the row that you wish to delete and click on **Delete Role Group** in the LDAP/E-Directory Settings Page.

Mouse Mode

In MegaRAC GUI, Redirection Console handles mouse emulation from local window to remote screen in either of two methods. User has to be an Administrator to configure this option. To open Mouse Mode page, click **Configuration > Mouse Mode** from the main

menu. A sample screenshot of Mouse Mode Settings Page is shown in the screenshot below.

Figure 3-23. Mouse Mode Settings Page

The fields of Mouse Mode Settings page are explained below.

Table 13: Mouse Mode Settings Page

ITEM	DESCRIPTION
Absolute Mode	The absolute position of the local mouse is sent to the server.
Relative Mode	Relative mode sends the calculated relative mouse position displacement to the server.
Other Mode	For the Host OS which is neither Absolute Mode nor Relative Mode.
Save	To save any changes made.
Reset	To Reset the modified changes.

Procedure:

1. Choose either of the following as your requirement:

- Set mode to Absolute

Note:

Applicable for all Windows versions; RHEL Linux versions not below than RHEL6; Fedora Linux versions not below than FC14.

- Set mode to Relative

Note:

Applicable for RHEL Linux versions below than RHEL6; Fedora Linux versions below than FC14; SLES Linux versions below than SLES11.

- Set mode to Other

Note:

Applicable for SLES Linux version SLES11.

2. Click **Save** button to save the changes made.
3. Click **Reset** to reset the modified changes.

Network

In MegaRAC GUI, the Network Settings Page is used to configure the network settings for the available LAN channels.

To open Network Settings page, click **Configuration > Network** from the main menu. A sample screenshot of Network Settings Page is shown in the screenshot below.

The screenshot displays the 'Network Settings' page within the MegaRAC GUI. The top navigation bar includes 'Dashboard', 'Server Information', 'Server Health', 'Configuration', 'Remote Control', 'Maintenance', 'Firmware Update', and 'HELP'. The 'Configuration' menu is active, and the user is logged in as 'admin(Administrator)'. The page title is 'Network Settings'. Below the title, there is a section 'Manage network settings of the device.' with the following fields:

- LAN Interface:** A dropdown menu showing 'bond0'.
- LAN Settings:** A checkbox labeled 'Enable' which is checked.
- MAC Address:** A text input field containing '2C:60:0C:83:FD:0C'.
- IPv4 Configuration:**
 - IPv4 Settings:** A checkbox labeled 'Enable' which is checked.
 - Obtain an IP address automatically:** A checkbox labeled 'Use DHCP' which is checked.
 - IPv4 Address:** A text input field containing '10.10.14.43'.
 - Subnet Mask:** A text input field containing '255.255.0.0'.
 - Default Gateway:** A text input field containing '10.10.10.204'.
- IPv6 Configuration:**
 - IPv6 Settings:** A checkbox labeled 'Enable' which is checked.
 - Obtain an IP address automatically:** A checkbox labeled 'Use DHCP' which is checked.
 - IPv6 Address:** An empty text input field.

Figure 3-24. Network Settings Page

The fields of Network Settings page are explained below.

Table 14: Network Settings Page

ITEM	DESCRIPTION
LAN Interface	Lists the LAN interfaces.
LAN Settings	To enable or disable the LAN Settings.
MAC Address	This field displays the MAC Address of the device. This is a read only field.
IPv4 Settings	<p>This option lists the IPv4 configuration settings.</p> <ul style="list-style-type: none"> Obtain IP Address automatically: This option is to dynamically configure IPv4 address using DHCP (Dynamic Host Configuration Protocol). IPv4 Address, Subnet Mask, and Default Gateway: These fields are for specifying the static IPv4 address, Subnet Mask and Default Gateway to be configured to the device. <p>Note:</p> <ul style="list-style-type: none"> IP Address made of 4 numbers separated by dots as in "xxx.xxx.xxx.xxx". Each Number ranges from 0 to 255.
IPv6 Configuration	<p>This option lists the following IPv6 configuration settings.</p> <ul style="list-style-type: none"> IPv6 Settings: This option is to enable the IPv6 settings in the device. Obtain an IPv6 address automatically: This option is to dynamically configure IPv6 address using DHCP (Dynamic Host Configuration Protocol). IPv6 Address: To specify a static IPv6 address to be configured to the device. Eg: 2004:2010 Subnet prefix length: To specify the subnet prefix length for the IPv6 settings. <p>Note:</p> <ul style="list-style-type: none"> Value ranges from 0 to 128. Default Gateway: Specify v6 default gateway for the IPv6 settings. Reserved IPv6 Address: Some IPv6 addresses are reserved by IETF. List is showed as below, so when users set these Blocking IPv6 addresses, WebUI will pop-up warning message.
VLAN Configuration	<p>It lists the VLAN configuration settings.</p> <ul style="list-style-type: none"> VLAN Settings: To enable/disable the VLAN support for selected interface. VLAN ID: The Identification for VLAN configuration. <ul style="list-style-type: none"> Value ranges from 2 to 4094. VLAN Priority: The priority for VLAN configuration. <ul style="list-style-type: none"> Value ranges from 0 to 7. 7 is the highest priority for VLAN.
Save	To save the entries.
Reset	To Reset the modified changes.

Table 15: Reserved IPv6 Address

IPv6 PREFIX	ALLOCATION	REFERENCE
0000::/8	Reserved by IETF	[RFC4291]
0100::/8	Reserved by IETF	[RFC4291]
0200::/7	Reserved by IETF	[RFC4048]
0400::/6	Reserved by IETF	[RFC4291]
0800::/5	Reserved by IETF	[RFC4291]
1000::/4	Reserved by IETF	[RFC4291]
4000::/3	Reserved by IETF	[RFC4291]
6000::/3	Reserved by IETF	[RFC4291]
8000::/3	Reserved by IETF	[RFC4291]
a000::/3	Reserved by IETF	[RFC4291]
c000::/3	Reserved by IETF	[RFC4291]
e000::/4	Reserved by IETF	[RFC4291]
f000::/5	Reserved by IETF	[RFC4291]
f800::/6	Reserved by IETF	[RFC4291]
fe00::/9	Reserved by IETF	[RFC4291]
fe80::/10	Link-Scoped Unicast	[RFC4291]
fec0::/10	Reserved by IETF	[RFC3879]
ff00::/8	Multicast	[RFC4291]
2001::/32	Reserved by IETF	[RFC4380]

Procedure

1. Select the **LAN Interface** from the drop down list.
2. Check **Enable** to enable the LAN Settings.
3. In IPv4 Configuration, enable **Use DHCP to Obtain an IP address automatically** to dynamically configure IPv4 address using DHCP.
4. If the field is disabled, enter the **IPv4 Address, Subnet Mask** and **Default Gateway** in the respective fields.
5. In IPv6 Configuration, if you wish to enable the IPv6 settings, check **Enable**.
6. If the IPv6 setting is enabled, enable or disable the option **Use DHCP for obtaining the IP address automatically**.
7. If the field is disabled, enter the **IPv6 Address, Subnet Prefix length** and **Default Gateway** in the given field.
8. In VLAN Configuration, if you wish to enable the VLAN settings, check **Enable**.
9. Enter the **VLAN ID** in the specified field.
10. Enter the **VLAN Priority** in the specified field.
11. Click **Save** to save the entries.

12. Click **Reset** if you want to reset the modified changes.

PEF

Platform Event Filtering (PEF) provides a mechanism for configuring the BMC to take selected actions on event messages that it receives or has internally generated. These actions include operations such as system power-off, system reset, as well as triggering the generation of an alert.

In MegaRAC GUI, the PEF Management is used to configure the following:

- Event Filter
- Alert Policy
- LAN Destination

To open PEF Management Settings page, click **Configurations > PEF** from the main menu. A sample screenshot of PEF Management Settings Page is shown in the screen shot below. Each tab is explained below.

Event Filter Tab

A PEF implementation is recommended to provide at least 16 entries in the event filter table. A subset of these entries should be pre-configured for common system failure events, such as over-temperature, power system failure, fan failure events, etc. Remaining entries can be made available for 'OEM' or System Management Software configured events. Note that individual entries can be tagged as being reserved for system use - so this ratio of pre-configured entries to run-time configurable entries can be reallocated if necessary.

The screenshot displays the 'PEF Management' page with the 'Event Filter' tab selected. The page includes a navigation bar at the top with links like 'Dashboard', 'Server Information', 'Server Health', 'Configuration', 'Remote Control', 'Maintenance', 'Firmware Update', and 'HELP'. Below the navigation bar, there's a section for 'PEF Management' with a brief instruction: 'Use this page to configure Event Filter, Alert Policy and LAN Destination. To delete or modify a entry, select it in the list and click "Delete" or "Modify". To add a new entry, select an unconfigured slot and click "Add".' Below this instruction are three tabs: 'Event Filter', 'Alert Policy', and 'LAN Destination'. The 'Event Filter' tab is active, showing a table with 9 entries. The table has columns for 'PEF ID', 'Filter Configuration', 'Event Filter Action', 'Event Severity', and 'Sensor Name'. The entries are numbered 1 through 9, all with 'Enabled' filter configuration, '[Alert]' action, 'Unspecified' severity, and 'Any' sensor name. At the bottom right of the table, there are three buttons: 'Add', 'Modify', and 'Delete'.

PEF ID	Filter Configuration	Event Filter Action	Event Severity	Sensor Name
1	Enabled	[Alert]	Unspecified	Any
2	Enabled	[Alert]	Unspecified	Any
3	Enabled	[Alert]	Unspecified	Any
4	Enabled	[Alert]	Unspecified	Any
5	Enabled	[Alert]	Unspecified	Any
6	Enabled	[Alert]	Unspecified	Any
7	Enabled	[Alert]	Unspecified	Any
8	Enabled	[Alert]	Unspecified	Any
9	Enabled	[Alert]	Unspecified	Any

Figure 3-25. PEF Management – Event Filter

The fields of PEF Management – Event Filter Tab are explained below.

This page contains the list of configured PEF's.

Table 16: PET Management - Event Filter

ITEM	DESCRIPTION
PEF ID	This field displays the ID for the newly configured PEF entry (read-only).
Filter configuration	Check box to enable the PEF settings.
Event Filter Action	Check box to enable PEF Alert action. This is a mandatory field.
Event Severity	To choose any one of the Event severity from the list.
Sensor Name	To choose the particular sensor from the sensor list.
Add	To add the new event filter entry and return to Event filter list.
Modify	To modify the existing entries.
Delete	To delete Event filter list.

Procedure:

1. Click the **Event Filter** Tab to configure the event filters in the available slots.
2. To Add an Event Filter entry, select a free slot and click **Add** or alternatively double click the empty slot to open the Add event Filter entry Page. A sample screenshot of Add Event Filter Page is shown below.

Figure 3-26. Add Event Filter Entry Page

3. In the Event Filter Configuration section,
 - **PEF ID** displays the ID for configured PEF entry (read-only).
 - In **Filter Configuration**, check the box to enable the PEF settings.
 - In **Event Severity**, select any one of the Event severity from the list.
4. In the Filter Action configuration section,
 - Event Filter Action is a mandatory field and checked by default, which enable PEF Alert action (read-only).

- Select any one of the Power action either Power down, Power reset or Power cycle from the drop down list
- Choose any one of the configured alert policy number from the drop down list.

Note:

Alert Policy has to be configured - under **Configuration** -> **PEF** -> **Alert Policy**.

5. In the **Generator ID** configuration section,

- Check **Generator ID Data** option to fill the Generator ID with raw data.
- **Generator ID 1** field is used to give raw generator ID1 data value.
- **Generator ID 2** field is used to give raw generator ID2 data value.

Note:

*In **RAW** data field, specify hexadecimal value prefix with '0x.'*

- In the **Event Generator** section, choose the event generator as Slave Address - if event was generated from IPMB. Otherwise as System Software ID - if event was generated from sys-tem software.
- In the **Slave Address/Software ID** field, specify corresponding I2C Slave Address or System Software ID.
- Choose the particular **Channel Number** that event message was received over. Or choose '0' if the event message was received via the system interface, primary IPMB, or internally generated by the BMC.
- Choose the corresponding **IPMB Device LUN** if event generated by IPMB.

6. In the **Sensor configuration** section,

- Select the sensor type of sensor that will trigger the event filter action.
- In the sensor name field, choose the particular sensor from the sensor list.
- Choose event option to be either All Events or Sensor Specific Events.

7. In the **Event Data configuration** section,

- Event Trigger field is used to give Event/Reading type value.

Note:

Value ranges from 1 to 255.

- Event Data 1 AND Mask field is used to indicate wildcarded or compared bits.

Note:

Value ranges from 0 to 255.

- Event Data 1 Compare 1 & Event Data 1 Compare 2 field is used to indicate whether each bit position's comparison is an exact comparison or not.

Note:

Value ranges from 0 to 255.

8. In the Event Data 2 Configuration section,
 - Event Data 2 AND Mask field is similar to Event Data 1 AND Mask.
 - Event Data 2 Compare 1 & Event Data 2 Compare 2 fields are similar to Event Data 1 Compare 1 and Event Data 1 Compare 2 respectively.
9. In the Event Data 3 Configuration section,
 - Event Data 3 AND Mask field is similar to Event Data 1 AND Mask.
 - Event Data 3 Compare 1 & Event Data 3 Compare 2 fields are similar to Event Data 1 Compare 1 and Event Data 1 Compare 2 respectively.
10. Click on **Add** to save the modification and return to Event filter list.
11. Click on **Cancel** to cancel the modification and return to Event filter list.
12. In the **Event filter list**, select the configured slot and click **Modify** or alternatively double click the configured slot to modify the existing event filter entry.
13. In the **Event filter list**, click **Delete** to delete the existing filter.

Alert Policy Tab

This page is used to configure the Alert Policy and LAN destination. You can add, delete or modify an entry in this page.

The screenshot displays the 'PEF Management' section with the 'Alert Policy' tab selected. It shows a table of configured alert policies. The table has 6 columns: Policy Entry #, Policy Number, Policy Configuration, Policy Set, Channel Number, and Destination Selector. There are 9 rows of data, all with 'Disabled' configuration and 'Always send alert to this destination' policy set. The 'Configured Alert Policy count' is 15. At the bottom right, there are 'Add', 'Modify', and 'Delete' buttons.

Policy Entry #	Policy Number	Policy Configuration	Policy Set	Channel Number	Destination Selector
1	1	Disabled	Always send alert to this destination	1	0
2	2	Disabled	Always send alert to this destination	1	0
3	3	Disabled	Always send alert to this destination	1	0
4	4	Disabled	Always send alert to this destination	1	0
5	5	Disabled	Always send alert to this destination	1	0
6	6	Disabled	Always send alert to this destination	1	0
7	7	Disabled	Always send alert to this destination	1	0
8	8	Disabled	Always send alert to this destination	1	0
9	9	Disabled	Always send alert to this destination	1	0

Figure 3-27. PEF Management – Alert Policy

The fields of the PEF Management – Alert Policy Tabs are explained below.

Table 17: PEF Management - Alert Policy

ITEM	DESCRIPTION
Policy Entry #	Displays Policy entry number for the newly configured entry (read-only).
Policy Number	Displays the Policy number of the configuration.
Policy Configuration	To enable or disable the policy settings.
Policy Set	<p>To choose any one of the Policy set values from the list.</p> <ul style="list-style-type: none"> 0: Always send alert to this destination. 1: If alert to previous destination was successful, do not send alert to this destination. Proceed to next entry in this policy set. 2: If alert to previous destination was successful, do not send alert to this destination. Do not process any more entries in this policy set. 3: If alert to previous destination was successful, do not send alert to this destination. Proceed to next entry in this policy set that is to a different channel. 4: If alert to previous destination was successful, do not send alert to this destination. Proceed to next entry in this policy set that is to a different destination type.
Channel Number	To choose a particular channel from the available channel list.
Destination Selector	<p>To choose a particular destination from the configured destination list.</p> <p>Note: LAN Destination has to be configured - under Configuration -> PEF -> LAN Destination.</p>
Modify	To modify the existing entries.
Delete	To delete Alert Policy list.

Procedure:

1. In the Alert Policy Tab, select the slot for which you have to configure the Alert policy. That is, In the **Event Filter Entry Page**, if you have chosen Alert Policy number as 4, you have to configure the 4th slot (the slot with Policy Number 4) in the Alert Policy Tab.
2. Double click the slot and click **Add** to open the **Add Alert Policy Entry Page** as shown in the screenshot below.

The screenshot shows a window titled "Add Alert Policy entry". It contains the following fields and controls:

- Policy Entry #: Text box with value 3
- Policy Number: Dropdown menu with value 1
- Policy Configuration: Check box labeled "Enable" (unchecked)
- Policy Set: Dropdown menu with value 0
- Channel Number: Dropdown menu with value 1
- Destination Selector: Dropdown menu with value 1
- Alert String: Check box labeled "Event Specific" (unchecked)
- Alert String Key: Dropdown menu with value 0
- Buttons: "Add" and "Cancel" at the bottom right.

Figure 3-28. Add Alert Policy Entry Page

3. **Policy Entry #** is a read-only field.
4. Select the **Policy Number** from the list.
5. In the **Policy Configuration** field, check **Enable** if you wish to enable the policy settings.
6. In the **Policy Set** field, choose any of the Policy set from the list.
7. In the **Channel Number field**, choose particular channel from the available channel list.
8. In the **Destination Selector field**, choose particular destination from the configured destination list.

Note:

LAN Destination has to be configured under **Configuration -> PEF -> LAN Destination**. That is if you select the number 4 for destination selector in Alert Policy Entry page, then you have to configure the 4th slot (LAN Destination Number 4) in the LAN Destination tab.

9. In the **Alert String field**, enable the check box if the Alert policy entry is Event Specific.
10. In the **Alert String Key** field, choose any one value that is used to look up the Alert String to send for this Alert Policy entry.
11. Click **Add** to save the new alert policy and return to Alert Policy list.
12. Click **Cancel** to cancel the modification and return to Alert Policy list.
13. In the **Alert Policy Page**, to modify a configuration, select the slot to be modified and click **Modify**.
14. In the **Alert Policy Page**, to delete a configuration, select the slot and click **Delete**.

PEF Management LAN Destination Page

This page is used to configure the Event filter, Alert Policy and LAN destination. A sample screenshot of PEF Management LAN Destination Page is given below.

Figure 3-29. PEF Management - LAN Destination

The fields of PEF Management – LAN Destination Tab are explained below.

Table 18: PEF Management - LAN Destination

ITEM	DESCRIPTION
LAN Channel Number	Displays LAN Channel Number for the selected slot (read-only).
LAN Destination	Displays Destination number for the newly configured entry (read-only).
Destination Type	Destination type can be either an SNMP Trap or an Email alert. For Email alerts, the 3 fields – Username, Subject and body of the message needs to be filled. The SMTP server information also has to be added - under Configuration -> SMTP . For SNMP Trap, only the destination IP address has to be filled.
Destination Address	If Destination type is SNMP Trap, then enter the IP address of the system that will receive the alert. Destination address will support the following: <ul style="list-style-type: none"> IPv4 address format. IPv6 address format.

Table 18: PEF Management - LAN Destination (Continued)

ITEM	DESCRIPTION
Subject & Message	These fields must be configured if e-mail alert is chosen as destination type with the user configured in FixedSubject-Format. If the selected user for mail alert is configured with AMI-Format then the Subject and message fields will be greyed out. An e-mail will be sent to the configured e-mail address in case of any severity events with a subject specified in subject field and will contain the message field's content as the e-mail body. Note: User should be configured under Configuration-->Users
Send Test Alert	These fields must be configured if email alert or SNMP Trap is chosen as destination type. This field will send a test message in the message field's content to specified destination.
Add	To add a new entry to the device. Alternatively, double click on a free slot.
Modify	To modify that entry. Alternatively, double click on the configured slot.
Delete	To delete the selected configured LAN destination.

Procedure:

1. In the **LAN Destination Tab**, choose the slot to be configured. This should be the same slot that you have selected in the Alert Policy Entry- Destination Selector field. That is if you have chosen the Destination Selector as 4 in the Alert Policy Entry page of Alert Policy Tab, then you have to configure the 4th slot of LAN Destination Page.
2. Double click on the slot and click **Add**. This opens the **Add LAN Destination entry**.

Add LAN Destination entry

LAN Channel Number: 1

LAN Destination: 1

Destination Type: Snmp Trap

Destination Address:

Username:

Subject:

Message:

Add Cancel

Figure 3-30. Add LAN Destination entry Page

3. In the **LAN Channel Number** field, the LAN Channel Number for the selected slot is displayed and this is a read-only field.

4. In the **LAN Destination** field, the destination for the newly configured entry is displayed and this is a read-only field.
5. In the **Destination Type** field, select the one of the types.
6. In the **Destination Address** field, enter the destination address.

Note:

If Destination type is Email Alert, then give the email address that will receive the email.

7. Select the **User Name** from the list of users.
8. In the **Subject** field, enter the subject.
9. In the **Message** field, enter the message.
10. Click **Add** to save the new LAN destination and return to LAN destination list.
11. Click **Cancel** to cancel the modification and return to LAN destination list.
12. In the **LAN Destination Tab**, to modify a configuration, select the row to be modified and click **Modify**.
13. In the **LAN Destination Tab**, to delete a configuration, select the slot and click **Delete**.

RADIUS

RADIUS is a modular, high performance and feature-rich RADIUS suite including server, clients, development libraries and numerous additional RADIUS related utilities. In MegaRAC GUI, this page is used to set the RADIUS Authentication.

To open RADIUS Settings page, click **Configuration > RADIUS** from the main menu. A sample screenshot of RADIUS Settings Page is shown in the screenshot below.

Figure 3-31. RADIUS Settings Page

The fields of RADIUS Settings Page are explained below.

Table 19: RADIUS Settings Page

ITEM	DESCRIPTION
RADIUS Authentication	Option to enable RADIUS authentication.
Port	The RADIUS Port number. Note: Default Port is 1812. Port value ranges from 1 to 65535.
Server Address	The IP address of RADIUS server. Note: <ul style="list-style-type: none"> IP Address made of 4 numbers separated by dots as in "xxx.xxx.xxx.xxx". Each Number ranges from 0 to 255. First Number must not be 0.
Secret	The Authentication Secret for RADIUS server. Note: <ul style="list-style-type: none"> This field will not allow more than 31 characters. Secret phrase must be at least 4 characters long. White space is not allowed.
Extended Privileges	This field is used to assign KVM and VMedia privilege for the user.
Advanced Settings	For setting the advanced features.
Save	To save the settings.
Reset	To reset the modified changes.

Procedure:

1. Enable the **RADIUS Authentication** checkbox to authenticate the RADIUS.
2. Click on **Advanced Settings** button. This opens the Radius Authorization window as shown below.
 - For Authorization Purpose, configure the Radius user with Vendor Specific Attribute in Server side.

Example:1

testadmin Auth-Type :=PAP,Cleartext-Password:="admin"

Auth-Type :=PAP, Vendor-Specific="H=4"

Example:2

testoperator Auth-Type := PAP,Cleartext-Password := "operator"

Auth-Type :=PAP, Vendor-Specific="H=3"

If you change the Vendor-Specific value in server then you should change the same values in this page.

3. Click **Save** to save the changes made else click **Cancel** to go back to the previous screen.

Remote Session

In MegaRAC SP, use this page to configure virtual media configuration settings for the next redirection session. Encryption is disabled by default.

To open Remote Session page, click **Configuration > Remote Session** from the main menu. A sample screenshot of Remote Session Page is shown in the screenshot below.

Figure 3-32. Remote Session

The fields of Remote Session Settings Page are explained below.

Table 20: Remote Session Settings Page

ITEM	DESCRIPTION
Single Port Application	Enable/Disable single port support by runtime. On changing this configuration, KVM and VMedia Sessions will be restarted. If this support is enabled, KVM session will not use its dedicated port whereas both Web and KVM sessions will be established only via Web Port. If this support is disabled, KVM and Web sessions will use their own dedicated ports respectively.
KVM Encryption	Enable/Disable Encryption of KVM data for the next redirection session. If KVM Encryption is enabled, the KVM session will use the Secure port which has been configured in Configuration > Services page. If KVM Encryption is disabled, the KVM session will use the Non-Secure port which has been configured in Configuration > Services page. Note: This option is disabled if Single Port is enabled.
Keyboard Languages	This option is used to select the keyboard supported languages.
Retry Count	This option is used to retry the redirection session for certain number of attempts.
Retry Interval	This option is used to give time interval for each attempt.

Table 20: Remote Session Settings Page (Continued)

ITEM	DESCRIPTION
Automatically OFF Local Monitor, When JViewer Launches	Enable/disable Automatically OFF Local Monitor, When JViewer Launches.
Save	To save the current changes. Note: It will automatically close the existing remote redirection either KVM or Virtual media sessions, if any.
Reset	To reset the modified changes.

Procedure:

1. In **KVM encryption**, check or uncheck the option **Enable**.
2. Choose the **Keyboard Language** from the list of supported keyboard languages.
3. Enter a value in the **Retry Count** field to set the number of attempts for retrying the redirection session.
4. Enter a value in the **Retry Interval** field to assign time interval for each attempt.
5. Select the **Local Monitor OFF** check box to enable Local Monitor ON/OFF command during runtime.
6. Select the **Automatically OFF Local Monitor, When JViewer Launches** check box to automatically lock the local monitor during JViewer launch.
7. In **Virtual media Attach mode**, select **Auto Attach** or **Attach** from the drop-down list as required.
8. Click **Save** to save the current changes.
9. Click **Reset** to reset the modified changes.

SMTP

Simple Mail Transfer Protocol (SMTP) is an Internet standard for electronic mail (e-mail) transmission across Internet Protocol (IP) networks.

Using MegaRAC GUI, you can configure the SMTP settings of the device.

To open SMTP Settings page, click **Configuration > SMTP** from the main menu. A sample screenshot of SMTP Settings Page is shown in the screenshot below.

Figure 3-33. SMTP Settings Page

The fields of SMTP Settings Page are explained below.

Table 21: SMTP Settings Page

ITEM	DESCRIPTION
LAN Channel Number	Displays the list of LAN channels available.
Sender Address	The 'Sender Address' valid on the SMTP Server.
Machine Name	The 'Machine Name' of the SMTP Server. <ul style="list-style-type: none"> Machine Name is a string of maximum 31 alpha-numeric characters. Space, special characters are not allowed.
Primary SMTP Server	Lists the Primary SMTP Server configuration.
SMTP Support	Enable/Disable SMTP support for the BMC.
Port	Specify the SMTP Port. <p>Note: Default Port is 25. Port value ranges from 1 to 65535.</p>
Server Address	The 'IP address' of the SMTP Server. It is a mandatory field. <p>Note:</p> <ul style="list-style-type: none"> IP Address made of 4 numbers separated by dots as in "xxx.xxx.xxx.xxx". Each Number ranges from 0 to 255. First Number must not be 0. Supports IPv4 Address format and IPv6 Address format.

Table 21: SMTP Settings Page (Continued)

ITEM	DESCRIPTION
SMTP Server requires Authentication	<p>Enable/disable SMTP Authentication.</p> <p>Note: SMTP Server Authentication Types supported are:</p> <ul style="list-style-type: none"> • CRAM-MD5 • LOGIN • PLAIN <p>If the SMTP server does not support any one of the above authentication types, the user will get an error message stating, "<i>Authentication type is not supported by SMTP Server</i>"</p>
Username	<p>The username to access SMTP Accounts.</p> <p>Note:</p> <ul style="list-style-type: none"> • User Name can be of length 4 to 64 alpha-numeric characters. • It must start with an alphabet. • Special characters ','(comma), ':'(colon), ';' (semicolon), ' '(space) and '\'(backslash) are not allowed.
Password	<p>The password for the SMTP User Account.</p> <p>Note:</p> <ul style="list-style-type: none"> • Password must be at least 4 characters long. • White space is not allowed. • This field will not allow more than 64 characters.
Enable STARTTLS Support	<p>Check this option to enable STARTTLS support for the SMTP Client.</p> <ul style="list-style-type: none"> • SMTP CA Certificate File: File that contains the certificate of the trusted CA certs. • SMTP Certificate File: Client certificate filename. • SMTP Private Key: Client private key filename. <p>Note: To enable STARTTLS support, the respective SMTP support option should be enabled.</p>
Secondary SMTP Server	<p>It lists the Secondary SMTP Server configuration. It is an optional field. If the Primary SMTP server is not working fine, then it tries with Secondary SMTP Server configuration.</p>
Save	To save the new SMTP server configuration.
Reset	To reset the modified changes.

Procedure:

1. Select the **LAN Channel Number** from the drop-down list.
2. Enter the **Sender Address** in the specified field.
3. Enter the **Machine Name** in the specified field.
4. In Primary SMTP Server, check **Enable** to enable the **SMTP Support** option.

Note:

The Server Address can be edited only when the SMTP Support option is enabled.

5. Enter the **Port** value in the specified field.
6. Enter the **Server Address** in the specified field.
7. Enable the check box **SMTP Server requires Authentication** if you want to authenticate SMTP Server.
8. Enter your **User name and Password** in the respective fields.
9. 9. In Secondary SMTP Server, check **Enable** to enable the **SMTP Support** option.

Note:

The Server Address can be edited only when the SMTP Support option is enabled.

10. Enter the **Port** value in the specified field.
11. Enter the **Server Address** in the specific field.
12. Enable the check box **SMTP Server requires Authentication** if you want to authenticate SMTP Server.
13. Enter your **User name and Password** in the respective fields.
14. Click **Save** to save the entered details else click **Reset** to update the entered details.

SOL

Here, you can configure the Serial over LAN settings, select or change values for each attribute and click the Save button to save any changes.

admin/Administrator Refresh Print Logout

Dashboard Server Information Server Health Configuration Remote Control Maintenance Firmware Update HELP

Serial Over LAN Settings

You can configure Serial Over LAN Settings on this page.

Enable Serial Over LAN ☒

Baud Rate

Channel Privilege Level Limit

Figure 3-34. SOL Settings Page

The fields of SOL Settings Page are explained below.

Table 22: SOL Settings Page

ITEM	DESCRIPTION
Enable Serial over LAN	Checked=Enabled; Unchecked=Disabled.
Channel Privilege Level Limit	Select the IPMI Serial over LAN minimum user privilege: <ul style="list-style-type: none">• Administrator• Operator• User
Save	Use this button to save your settings.
Advanced SOL Settings	Use this button to go to advanced SOL page.

Use this page to configure the advanced SOL settings.

admin/Administrator

Refresh

Print

Logout

[Dashboard](#) [Server Information](#) [Server Health](#) [Configuration](#) [Remote Control](#) [Maintenance](#) [Firmware Update](#) [HELP](#)

Serial Over LAN Advanced Settings

You can configure Advanced Serial Over LAN Settings on this page.

Character Accumulate Interval

12

Character Send Threshold

96

Save

Cancel

Figure 3-35. SOL Advanced Settings Page

Table 23: SOL Advanced Settings Page

ITEM	DESCRIPTION
Character Accumulate Interval	The amount of the time that the BMC will wait before transmitting a partial SOL character data package. 1-based 5ms increments. This value must be from 1 to 255
Character Send Threshold	The BMC will send an SOL character data package containing the characters as soon as this number of characters (or greater) has been accepted. 1-based units. This value must be from 1 to 255.
Save	Use this button to save your settings.
Cancel	Use this button to cancel your settings.

SSL

The **Secure Socket Layer** protocol was created by Netscape to ensure secure transactions between web servers and browsers. The protocol uses a third party, a **Certificate Authority (CA)**, to identify one end or both end of the transactions.

Using MegaRAC GUI, configure SSL certificate into the BMC. Using this, the device can be accessed in a secured mode.

To open SSL Certificate Configuration page, click **Configuration > SSL** from the main menu. There are three tabs on this page.

- **Upload SSL** option is used to upload the certificate and private key file into the BMC.
- **Generate SSL** option is used to generate the SSL certificate based on configuration details.
- **View SSL** option is used to view the uploaded SSL certificate in readable format.

A sample screenshot of SSL Management Page is shown in the screenshot below.

Figure 3-36. SSL Certificate Configuration – Upload SSL

The fields of SSL Certificate Configuration – Upload SSL tab are explained below.

Table 24: SSL Certificate Configuration - Upload SSL

ITEM	DESCRIPTION
Current Certificate	Current certificate information will be displayed (read-only).
New Certificate	Certificate file should be of pem type
Current Privacy Key	Current privacy key information will be displayed (read-only).
New Privacy Key	Privacy key file should be of pem type.
Upload	To upload the SSL certificate and privacy key into the BMC.

Note:

Upon successful upload, HTTPs service will get restarted to use the newly uploaded SSL certificate.

admin/Administrator Refresh Print Logout

Dashboard Server Information Server Health Configuration Remote Control Maintenance Firmware Update HEL

SSL Certificate Configuration

This page is used to configure SSL certificate into the BMC. Using this, the device can be accessed in a secured mode. Upload SSL option is used to upload the certificate and private key file into the BMC. Generate SSL option is used to generate the SSL certificate based on configuration details. View SSL option is used to view the uploaded SSL certificate in readable format.

Upload SSL **Generate SSL** View SSL

Common Name(CN)

Organization(O)

Organization Unit(OU)

City or Locality(L)

State or Province(ST)

Country(C)

Email Address

Valid for days

Key Length bits

Generate

Figure 3-37. SSL Certificate Configuration – Generate SSL

The fields of SSL Certificate Configuration – Generate SSL tab are explained below.

Table 25: SSL Certificate Configuration - Generate SSL

ITEM	DESCRIPTION
Common Name (CN)	Common name for which certificate is to be generated. <ul style="list-style-type: none"> Maximum length of 64 characters. Special characters '#' and '\$' are not allowed.
Organization (O)	Organization name for which the certificate is to be generated. <ul style="list-style-type: none"> Maximum length of 64 characters. Special characters '#' and '\$' are not allowed.
Organization Unit (OU)	Over all organization section unit name for which certificate is to be generated. <ul style="list-style-type: none"> Maximum length of 64 characters. Special characters '#' and '\$' are not allowed.
City or Locality (L)	City or Locality of the organization (mandatory). <ul style="list-style-type: none"> Maximum length of 64 characters. Special characters '#' and '\$' are not allowed.
State or Province (ST)	State or Province of the organization (mandatory). <ul style="list-style-type: none"> Maximum length of 64 characters. Special characters '#' and '\$' are not allowed.
Country (C)	Country code of the organization (mandatory). <ul style="list-style-type: none"> Only two characters are allowed. Special characters are not allowed.
Email Address	Email Address of the organization (mandatory).

Table 25: SSL Certificate Configuration - Generate SSL (Continued)

ITEM	DESCRIPTION
Vaild for	Validity of the certificate. <ul style="list-style-type: none"> Value ranges from 1 to 3650 days.
Key Length	The key length bit value of the certificate.
Generate	To generate the new SSL certificate.

Note:

HTTPs service will get restarted, to use the newly generated SSL certificate.

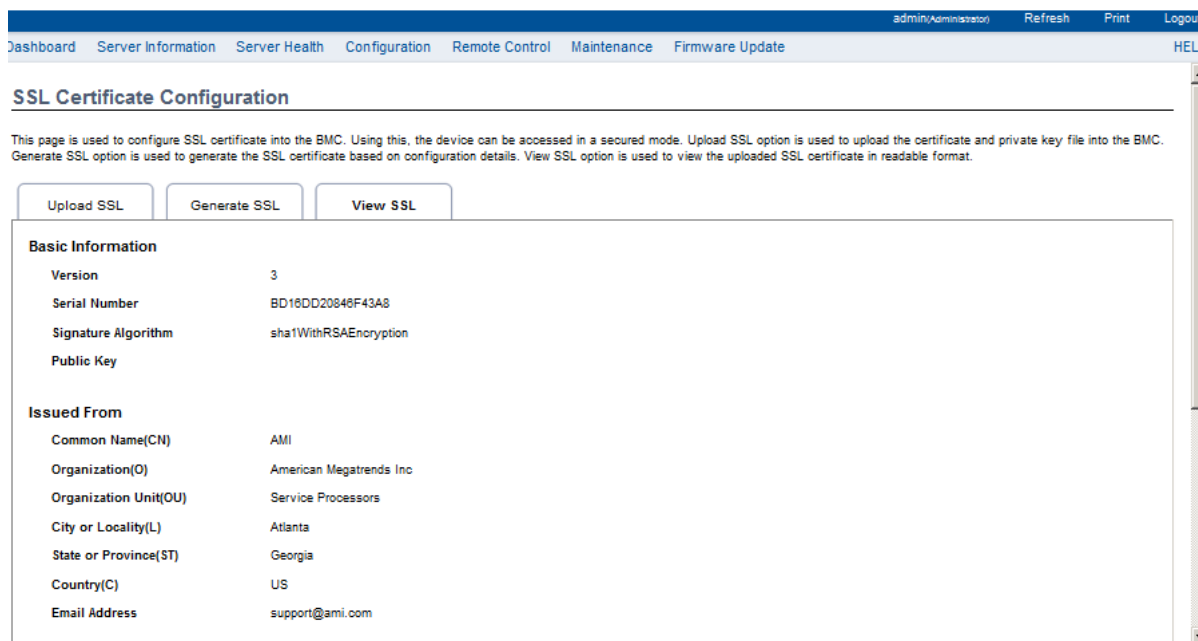


Figure 3-38. SSL Certificate Configuration – View SSL

The fields of SSL Certificate Configuration – View SSL tab are explained below.

Table 26: SSL Certificate Configuration – View SSL

ITEM	DESCRIPTION
Basic Information	This section displays the basic information about the uploaded SSL certificate. It displays the following fields. <ul style="list-style-type: none"> Version Serial Number Signature Algorithm Public Key

Table 26: SSL Certificate Configuration – View SSL (Continued)

ITEM	DESCRIPTION
Issued From	<p>This section describes the following Certificate Issuer information.</p> <ul style="list-style-type: none"> • Common Name (CN) • Organization (O) • Organization Unit (OU) • City or Locality (L) • State or Province (ST) • Country (C) • Email Address
Validity Information	<p>This section displays the validity period of the uploaded certificate.</p> <ul style="list-style-type: none"> • Valid From • Valid To
Issued To	<p>This section display the information about the certificate issuer.</p> <ul style="list-style-type: none"> • Common Name (CN) • Organization (O) • Organization Unit (OU) • City or Locality (L) • State or Province (ST) • Country (C) • Email Address

Procedure:

1. Click the Upload SSL Tab, **Browse** the **New Certificate** and **New Privacy** key.
2. Click **Upload** to upload the new certificate and privacy key.
3. In **Generate SSL** tab, enter the following details in the respective fields
 - The **Common Name** for which the certificate is to be generated.
 - The **Name of the Organization** for which the certificate is to be generated.
 - The **Overall Organization Section Unit** name for which certificate to be generated.
 - The **City or Locality** of the organization.
 - The **State or Province** of the organization.
 - The **Country** of the organization.
 - The **email address** of the organization.
 - The number of days the certificate will be valid in the **Valid For** field.
4. Choose the **Key Length** bit value of the certificate.
5. Click **Generate** to generate the certificate.
6. Click **View SSL** tab to view the uploaded SSL certificate in user readable format.

Note:

- Once you Upload/Generate the certificates, only HTTPs service will get restarted.
- You can now access your Generic MegaRAC® SP securely using the following format in your IP Address field from your Internet browser: https://<your MegaRAC® SP's IP address here>
- For example, if your MegaRAC® SP's IP address is 192.168.0.30, enter the following: https://192.168.0.30
- Please note the <s> after <http>. You must accept the certificate before you are able to access your Generic MegaRAC® SP.

User Management

In MegaRAC GUI, the User Management page allows you to view the current list of user slots for the server. You can add a new user and modify or delete the existing users.

To open User Management page, click **Configuration > Users** from the main menu. A sample screenshot of User Management Page is shown in the screenshot below.

The list below shows the current list of available users. To delete or modify a user, select the user name from the list and click "Delete User" or "Modify User". To add a new user, select an unconfigured slot and click "Add User"

Number of configured users: 2

UserID ↕	Username ↕	User Access ↕	Network Privilege ↕	Email ID ↕
1	anonymous	Disabled	Administrator	~
2	admin	Enabled	Administrator	~
3	~	~	~	~
4	~	~	~	~
5	~	~	~	~
6	~	~	~	~
7	~	~	~	~
8	~	~	~	~
9	~	~	~	~
10	~	~	~	~

[Add User](#)
[Modify User](#)
[Delete User](#)

Figure 3-39. User Management

The fields of User Management Page are explained below.

Table 27: User Management Page

ITEM	DESCRIPTION
User ID	Displays the ID number of the user. Note: The list contains a maximum of ten users only.
User Name	Displays the name of the user.

Table 27: User Management Page (Continued)

ITEM	DESCRIPTION
User Access	To enable or disable the access privilege of the user.
Network Privilege	Displays the network access privilege of the user.
SNMP Status	Displays if the SNMP status for the user is Enabled or Disabled.
E-mail ID	Displays e-mail address of the user.
Add User	To add a new user.
Modify User	To modify an existing user.
Delete User	To delete an existing user.

Procedure:**Note:**

The Free slots are denoted by "~" in all columns for the slot.

Add a new user:

1. To add a new user, select a free slot and click **Add User**. This opens the Add User screen as shown in the screenshot below.

Figure 3-40. Add User Page

2. Enter the name of the user in the **User Name** field.

Note:

- User Name is a string of 4 to 16 alpha-numeric characters.
- It must start with an alphabetical character.
- It is case-sensitive.
- Special characters like '-' (hyphen), '_' (underscore) and '.' (dot) are allowed, but not in the prefix and suffix.

3. In the **Password** and **Confirm Password** fields, enter and confirm your new password.

Note:

- Password must be at least 4 characters long.
- White space is not allowed.
- This field will not allow more than 20 characters if "20 Bytes" option is chosen.

4. Enable or Disable the **User Access** Privilege.
5. In the **Network Privilege** field, enter the network privilege assigned to the user which could be Administrator, Operator, User, Callback or OEM proprietary.
6. In the Extended Privileges, check the required options,
 - KVM
 - VMedia

Note:

It is recommended that the Extended privileges support to KVM and VMedia should be provided only to the ADMIN user and shouldn't be provided to USER and OPERATOR privilege level users. The Admin user can provide the Extended privilege support to USER and OPERATOR privilege level users at their own risk.

7. Check the **SNMP Status** check box to enable SNMP access for the user.

Note:

Password field is mandatory, if SNMP Status is enabled.

8. Choose the SNMP Access level option for user from the **SNMP Access** drop-down list. Either it can be Read Only or Read Write.
9. Choose the **Authentication Protocol** to use for SNMP settings from the drop-down list.

Note:

Password field is mandatory, if Authentication protocol is changed.

10. Choose the Encryption algorithm to use for SNMP settings from the **Privacy protocol** drop-down list.
11. In the **Email ID** field, enter the email ID of the user. If the user forgets the password, the new password will be mailed to the configured email address.

Note:

SMTP Server must be configured to send emails.

- Email Format: Two types of formats are available:
 - AMI-Format: The subject of this mail format is 'Alert from (your Hostname)'. The mail content shows sensor information, ex: Sensor type and Description.

- **Fixed-Subject Format:** This format displays the message according to user's setting. You must set the subject and message for email alert.

12. In the **New SSK Key** field, click Browse and select the SSH key file.

Note:

SSH key file should be of pub type.

13. Click **Add** to save the new user and return to the users list.

14. Click **Cancel** to cancel the modification and return to the users list.

Modify an existing user:

1. Select an existing user from the list and click **Modify User**. This opens the Add User screen as shown in the screenshot below.

Figure 3-41. Modify User Page

2. Edit the required fields.
3. To change the password, enable the **Change Password** option.
4. After editing the changes, click **Modify** to return to the users list page.

Note:

SNMP related fields will not show at setting page while BMC did not support this function

Delete an existing User

To delete an existing user, select the user from the list and click **Delete User**.

Note:

There is a list of reserved users which cannot be added / modified as BMC users. Please Refer "MEGARAC SP-X Platform Porting Guide" section "Changing the Configurations in PMC File-> User Configurations in PMC File" for the list of reserved users.

Virtual Media

In MegaRAC GUI, this page is to configure Virtual Media device settings. If you change the configuration of the virtual media in this page, it shows the appropriate device in the JViewer Vmedia dialog. For example, if you select two floppy devices in Configure Virtual Media page, then in **JViewer > Vmedia**, you can view two floppy device panel, these virtual media devices will only setup when Launching the KVM.

To open Virtual Media page, click **Configuration > Virtual Media** from the main menu. A sample screenshot of User Management Page is shown in the screenshot below.

The following option will allow to configure virtual media devices. Below, you can select the number of instances that are be supported for each type of virtual media devices.

Floppy devices	4
CD/DVD devices	4
Hard disk devices	4
Remote KVM Floppy devices	2
Remote KVM CD/DVD devices	2
Remote KVM Hard disk devices	2

Save Reset

Figure 3-42. Configure Virtual Media Devices

The following fields are displayed in this page.

Table 28: Configure Virtual Media Devices

ITEM	DESCRIPTION
Floppy devices	The number of floppy devices that support for Virtual Media redirection.
CD/DVD devices	The number of CD/DVD devices that support for Virtual Media redirection.
Hard disk devices	The number of hard disk devices that support for Virtual Media redirection.
Remote KVM Floppy Devices	The number of floppy devices that support for KVM Virtual Media redirection.
Remote KVM CD/DVD Devices	The number of CD/DVD devices that support for KVM Virtual Media redirection.
Remote KVM Hard disk Devices	The number of Hard disk devices that support for KVM Virtual Media redirection.
Save	To save the configured settings.
Reset	To reset the previously-saved values.

Procedure:

1. Select the number of Floppy devices, CD/DVD devices and Hard disk devices from the dropdown list.

Note:

Maximum of two devices can be added in Floppy, CD/DVD and Hard disk drives.

2. Enable the **Local Media Support** if needed.
3. Click **Save** to save the changes made else click Reset to reset the previously saved values.

Note:

If there are two device panels for each device, and when you click the Connect button, then the redirected device panel will be disabled.

Services

This page used for port setting and displays the basic information about services running in the BMC. Only Administrator can modify the service.

To open Services page, click **Configuration > Services** from the menu bar. A sample screenshot of Services Page is shown below.

admin(Administrator) Refresh Print Logou									
Dashboard	Server Information	Server Health	Configuration	Remote Control	Maintenance	Firmware Update	HEL		

Services									
Below is a list of services running on the BMC. It shows current status and other basic information about the services. Select a slot and press "Modify" button to modify the services configuration.									
Number of Services: 8									
#	Service Name	Current State	Interfaces	Nonsecure Port	Secure Port	Timeout	Maximum Sessions	Active Sessions	
1	web	Active	bond0	80	443	1800	20		View
2	kvm	Active	bond0	7578	7582	1800	2		View
3	cd-media	Active	bond0	5120	5124	N/A	4		View
4	fd-media	Active	bond0	5122	5126	N/A	4		View
5	hd-media	Active	bond0	5123	5127	N/A	4		View
6	ssh	Active	N/A	N/A	22	600	N/A		View
7	telnet	Inactive	N/A	23	N/A	600	N/A		View
8	solssh	Inactive	bond0	52123	N/A	60	N/A		View
Modify									

Figure 3-43. Services page

The fields of Services Page are explained below.

Table 29: Services

ITEM	DESCRIPTION
Service Name	Displays service name of the selected slot (read-only).
Current State	Displays the current status of the service, either active or inactive state.

Table 29: Services (Continued)

ITEM	DESCRIPTION
Interfaces	It shows the interface in which service is running.
Nonsecure Port	<p>This port is used to configure non secure port number for the service.</p> <ul style="list-style-type: none"> - Web default port is 80 - KVM default port is 7578 - CD Media default port is 5120 - FD Media default port is 5122 - HD Media default port is 5123 - Telnet default port is 23 <p>Note: SSH service will not support non secure port. If single port feature is enabled, KVM, CD Media, FD Media and HD Media ports cannot be edited.</p>
Secure Port	<p>Used to configure secure port number for the service.</p> <ul style="list-style-type: none"> - Web default port is 443 - KVM default port is 7582 - CD Media default port is 5124 - FD Media default port is 5126 - HD Media default port is 5127 - SSH default port is 22 <p>Note: Telnet service will not support secure port. If single port feature is enabled, KVM, CD Media, FD Media and HD Media ports cannot be edited.</p>
Timeout	<p>Displays the session timeout value of the service. For Web, user can configure the session timeout value.</p> <p>Note:</p> <ul style="list-style-type: none"> - Web timeout value ranges from 300 to 1800 seconds. - KVM timeout value ranges from 300 to 1800 seconds. - SSH and Telnet timeout value ranges from 60 to 1800 seconds. - SSH and telnet timeout value should be in multiples of 60 seconds. - SSH and telnet service will be using the shared timeout value. - If you configure SSH timeout value, it will be applied to telnet service also and vice versa. - If KVM is launched then the web session timeout will not take effect.
Maximum Sessions	Displays the maximum number of allowed sessions for the service.
Active Sessions	To view the current active sessions for the service.

Procedure

1. Click **View** to view the details about the active sessions for the service.

2. This opens the **Active Session** screen (for example - Web Service screen) as shown in the screenshot below.

Active Session - Web						
#						Number of Sessions: 1
#	Session ID	Session Type	IP Address	User ID	User Name	User Privilege
1	6	HTTP	10.0.3.41	2	admin	Administrator
						<input type="button" value="Terminate"/> <input type="button" value="Cancel"/>

Session ID: Displays the ID number of the active sessions.

Session Type: Displays the type of the active sessions.

IP Address: Displays the IP addresses that are already configured for the active sessions.

User ID: Displays the ID number of the user.

User Name: Displays the name of the user.

User Privilege: Displays the access privilege of the user.

3. Select a slot and click **Terminate** to terminate the particular session of the service else click **Cancel** to cancel the modification and return to Services list.

Modify: To modify the existing services.

Procedure

1. Select a slot and click **Modify** to modify the configuration of the service. Alternatively, double click on the slot.

Note:

Whenever the configuration is modified, the service will be restarted automatically. User has to close the existing opened session for the service if needed.

2. This opens the Modify Service screen as shown in the screenshot below.

Modify Service	
Service Name	<input type="text" value="kvm"/>
Current State	<input checked="" type="checkbox"/> Active
Interfaces	<input type="text" value="both"/>
Nonsecure Port	<input type="text" value="7578"/>
Secure Port	<input type="text" value="7582"/>
Timeout	<input type="text" value="1800"/> seconds
Maximum Sessions	<input type="text" value="2"/>
<input type="button" value="Modify"/>	

Figure 3-44. Service modify

3. **Service Name** is a read only field
4. Activate the **Current State** by enabling the Activate check box.

Note:

Interfaces, Nonsecure port, Secure port, Time out and Maximum Sessions will not be active unless the current state is active.

5. Choose any one of the available interfaces from the **Interface** drop-down list.
6. Enter the Nonsecure port number in the **Nonsecure Port** field.
7. Enter the Secure Port Number in the **Secure Port** field.
8. Enter the timeout value in the **Timeout** field.

Note:

The values in the **Maximum Sessions** field cannot be modified.

9. Click **Modify** to save the entered changes and return to the Services Page else Click **Cancel** to exit.

LAN Port Settings

Here you can configure LAN Port setting of the BMC NIC.

admin(Administrator) Refresh Print Logout

Dashboard Server Information Server Health Configuration Remote Control Maintenance Firmware Update HELP

LAN Port Settings

You can configure LAN Port Settings on this page.

WARNING: Please make sure the selected device has been properly configured with IP and it's connected to switch. Changing to an un-configured device will result in BMC connection lost, and require manually re-install the HW connection.

Select LAN port

Dedicated-NIC
Dedicated-NIC
Shared-NIC (LOM)

Save Reset

Figure 3-45. LAN Port Settings

Procedure:

1. Select **LAN Port** from the dropdown list
2. Click **Save** to save the change or click **Reset** to reset the previously saved values.

Remote Control

The Remote Control consists of the following menu items.

- Console Redirection
- Server Power Control
- Java SOL

A sample screenshot of the Remote Control menu is given below.

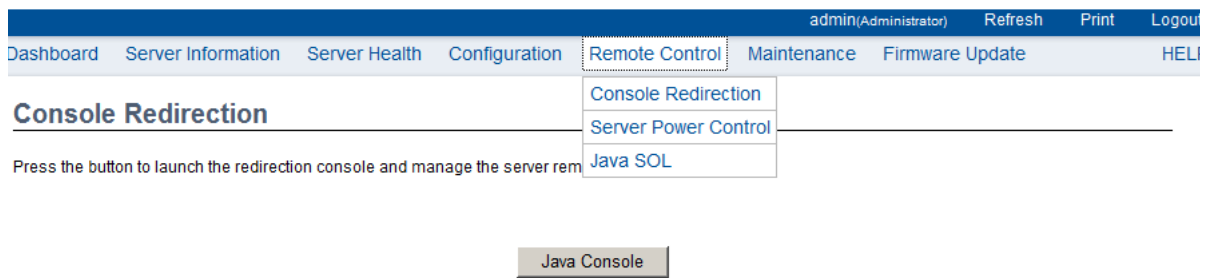


Figure 3-46. Remote Control Menu

A detailed description of the menu items are given ahead

Console Redirection

The remote console application, which is started using the WebGUI, allows you to control your server's operating system remotely, using the screen, mouse, and keyboard, and to redirect local CD/DVD, Floppy diskette and Hard disk/USB thumb drives as if they were connected directly to the server.

List of Supported Client Operating Systems

- WinXP
- W2K3 - 32 bit
- W2K3 - 64 bit
- RHEL 4 - 32 bit
- RHEL 4 - 64 bit
- RHEL 5.4 - 32 bit
- RHEL 5.4 - 64 bit
- RHEL 6.0 - 64 bit
- RHEL 6.0 - 32 bit
- Ubuntu 9.10 LTS - 32 bit
- Ubuntu 9.10 LTS - 64 bit
- Ubuntu 8.10 -32 bit
- Ubuntu 8.10 -64 bit
- OpenSuse 11.2 -32 bit
- OpenSuse 11.2 -64 bit

- FC 9 - 32 bit
- FC 9 - 64 bit
- FC 10 - 32 bit
- FC 10 - 64 bit
- FC 12 - 32 bit
- FC 12 - 64 bit
- FC 13 - 32 bit
- FC 13 - 64 bit
- FC 14 - 32 bit
- FC 14 - 64 bit
- MAC - 32 bit
- MAC - 64 bit

List of Supported Host OS

- RHEL 5
- RHEL 6
- W2K3
- W2K8
- RHEL 4
- OpenSuse 11.2
- OpenSuse 10.x
- Ubuntu 8.10
- Ubuntu 9.10
- Ubuntu 11.04

Supported JRE Version

Java™ SE Runtime Environment 1.6.0 +

Note:

If OS use 32 bit then use JRE 32 bit version

If OS use 64 bit then use JRE 64 bit version

To get JRE version command in Linux/Windows: java -version

Windows example:

```
C:\Users>java -version
java version "1.7.0_45"
Java(TM) SE Runtime Environment (build 1.7.0_45-b18)
Java HotSpot(TM) Client VM (build 24.45-b08, mixed mode, sharing)
```

Browser Settings

For Launching the KVM, pop-up block should be disabled. For Internet explorer, enable the download file options from the settings.

Java Console

This is an OS independent plug-in which can be used in Windows as well as Linux with the help of JRE. JRE should be installed in the client's system. You can install JRE from the following link.

<http://www.java.com/en/download/manual.jsp>

Procedure:

In MegaRAC GUI, the Java Console can be launched in two ways:

1. Open the Dashboard Page and click Launch for Java Console in Remote control section.
2. Open **Remote Control** > **Console Redirection** Page and click **Java Console**.

This will download the **.jnlp** file from BMC.

To open the **.jnlp** file, use the appropriate JRE version (Javaws).

When the downloading is done, it opens the Console Redirection window.

Note:

Web page will be timeout after open 30 minutes, but it will be connected continually when open RKVM.

The Console Redirection main menu consists of the following menu items.

- Video
- Keyboard
- Mouse
- Options
- Media
- Keyboard Layout
- Video Record
- Active Users
- Help

A detailed explanation of these menu items are given below.

Video

This menu contains the following sub menu items.

Table 30: Video

ITEM	DESCRIPTION
Pause redirection	This option is used for pausing Console Redirection.
Resume Redirection	This option is used to resume the Console Redirection when the session is paused.
Refresh Video	This option can be used to update the display shown in the Console Redirection window.
Compression mode	This option is used to select the video compression mode which includes YUV 420, YUV 444, YUV 444 + 2 colors VQ and YUV 444 + 4 colors VQ in Java console.
DCT Quantization table	There are eight levels to select the Video quality. If using low bandwidth, user can use lower level to get better video fluency but may not more clear. If using high bandwidth, user can use higher level to get clearer page.
Host video output	If you enable this option, the server display will be blank but you can view the screen in Console Redirection. If you disable this option, the display will be back in the server screen.
Full Screen	This option is used to view the Console Redirection in full screen mode (Maximize). This menu is enabled only when both the client and host resolution are the same.
Exit	This option is used to exit the console redirection screen.

Keyboard

This menu contains the following sub menu items.

Table 31: Keyboard

ITEM	DESCRIPTION
Hold Right Ctrl Key	This menu item can be used to act as the right-side <CTRL> key when in Console Redirection.
Hold Right Alt Key	This menu item can be used to act as the right-side <ALT> key when in Console Redirection.
Hold Left Ctrl Key	This menu item can be used to act as the left-side <CTRL> key when in Console Redirection.
Hold Left Alt Key	This menu item can be used to act as the left-side <ALT> key when in Console Redirection.
Left Windows Key	This menu item can be used to act as the left-side <WIN> key when in Console Redirection. You can also decide how the key should be pressed: Hold Down or Press and Release.

Table 31: Keyboard (Continued)

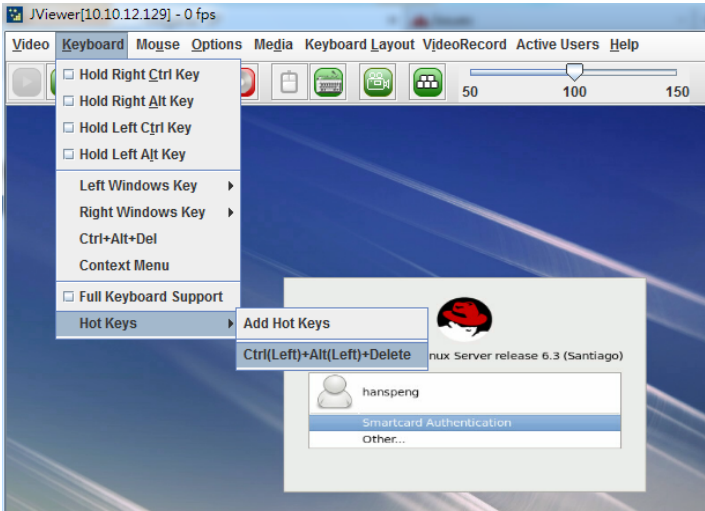
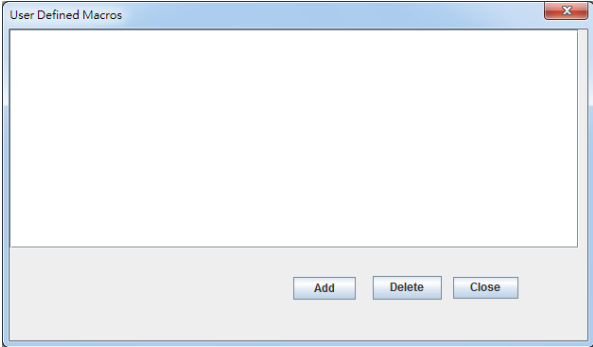
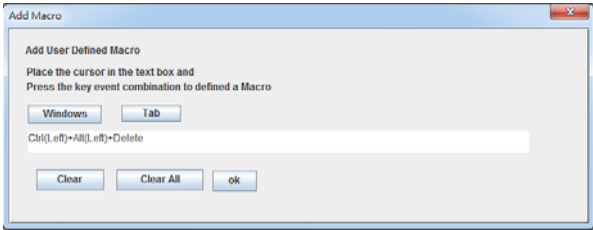

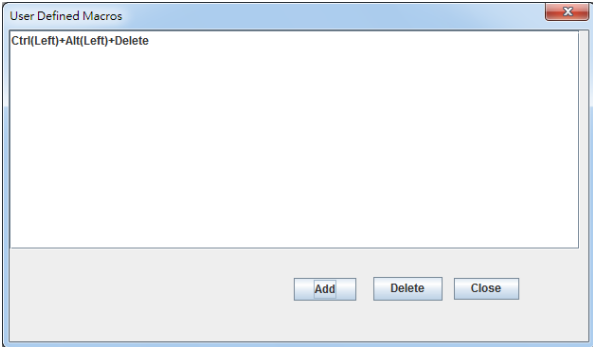
ITEM	DESCRIPTION
Right Windows Key	This menu item can be used to act as the right-side <WIN> key when in Console Redirection. You can also decide how the key should be pressed: Hold Down or Press and Release.
Alt+Ctrl+Del	This menu item can be used to act as if you depressed the <CTRL>, <ALT> and keys down simultaneously on the server that you are redirecting.
Full keyboard support	This menu item can be used to act as totally host OS keyboard in Console Redirection. It will disable the hot-key of RKVM when enable "Full Keyboard Support". If the hot-key is used in client OS, It can't be used in RKVM host OS. Because the hot-key is used by client OS first.
Context menu	This menu item can be used to act as <Context Menu> key in Console Redirection.
Hot Keys	<p>This menu item is used to add Hot Keys as below screenshot.</p> 


Table 31: Keyboard (Continued)

ITEM	DESCRIPTION
Add Hot Keys	<p>Procedure:</p> <ol style="list-style-type: none">Click Keyboard > Hot Keys > Add Hot Keys to show below snap-shot <div></div> <ul style="list-style-type: none">Add: used to add User Defined MacrosDelete: used to delete User Defined MacrosClose: used to close User Defined Macros window <ol style="list-style-type: none">Click Add to define macro <div></div> <ul style="list-style-type: none">Windows: used to define Windows keyTab: used to define Tab keyClear: used to delete the latest defined keyClear All: used to delete all defined keyok: used to confirm and add defined macro <p>Note:</p> <p>Please press key one by one to define the macro. If click  to close this window and then click Add to open again, defined macro kept is normal. Support maximum 6 combo keys in 1 macros</p> <ol style="list-style-type: none">Click ok to add this macro as below <div></div>

Mouse

This menu contains the following sub menu items.

Table 32: Mouse

ITEM	DESCRIPTION
Show cursor	This option is used to display or hide the client mouse cursor in Java Console.
Mouse Calibration	It is used to adjust the mouse calibration.
Mouse mode	<ul style="list-style-type: none"> ● Absolute mouse mode: To select mouse mode to "Absolute", depending upon the Host Operating System (All Windows versions; RHEL Linux versions not below than RHEL5.8; Fedora Linux versions not below than FC14). In this mode, the default value will enable "Show Cursor" feature and you will see two mice in remote KVM. The first mouse is in remote PC end; the second mouse is in local server end. On the different RHEL system, the mouse of acceleration setting is not different. So user will see two mice (remote/local mice) not synchronized sometimes ● Relative mouse mode: To select mouse mode to "Relative", depending upon the Host Operating System (RHEL Linux versions below than RHEL5.8; Fedora Linux versions below than FC14; SLES Linux versions below than SLES11). ● Other mouse mode: For the Host Operating System which is neither "Absolute" nor "Relative" mouse mode (SLES Linux version SLES11). "Other Mouse Mode" does not support Zoom In/Zoom Out and Maximize Window button is removed like this . When this mode is selected, scroll bar will disappear and video screen scaling function will resize the original video screen of remote to fit the current frame size of video display panel. <p>Note: When both Keyboard > Full Keyboard Support and Mouse > Other mouse mode are enabled at the same time, the mouse cursor will NOT be moved to outside the window unless to press "Alt+Tab" to switch window. And move mouse cursor to other window by pressing "Alt+C."</p>

Options

This menu contains the following sub menu items.

Table 33: Options

ITEM	DESCRIPTION
Bandwidth	This option is used to select the bandwidth manually or automatically.
Keyboard/Mouse Encryption	This option is used to enable or disable encryption for the data payload of Keyboard/Mouse transferring.
Zoom	This option is used to adjust the video screen for zoom in or zoom out.

Media

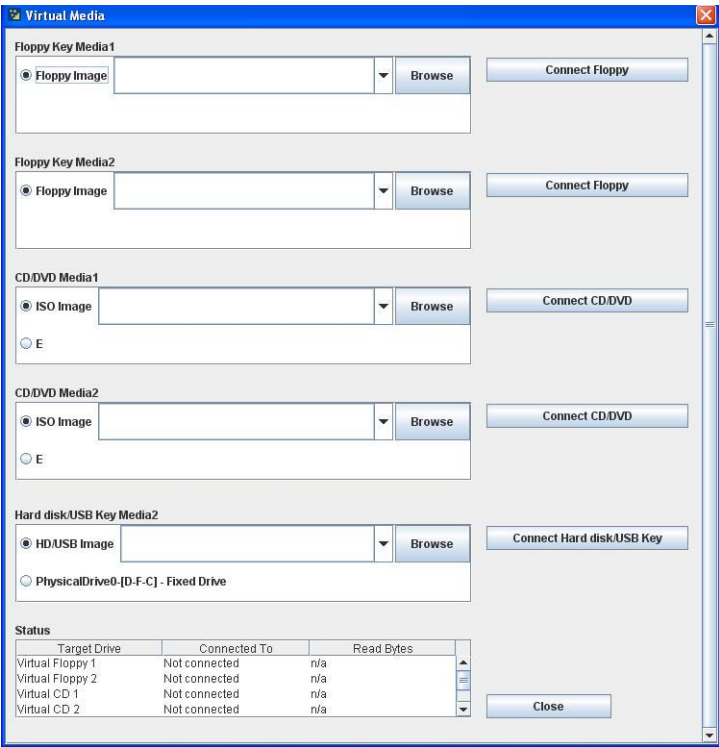


Figure 3-47. Virtual Media

Table 34: Virtual Media

ITEM	DESCRIPTION
Floppy Key Media	<p>This menu item can be used to start or stop the redirection of a physical floppy drive and floppy image types such as *.img.</p> <p>Note:</p> <p>Floppy Redirection is not an available feature on all versions of the MegaRAC® SPs.</p>
CD/DVD Media	<p>This menu item can be used to start or stop the redirection of a physical DVD/CD-ROM drive and cd image types such as *.iso.</p>
Hard disk/USB Key Media	<p>This menu item can be used to start or stop the redirection of a Hard Disk/USB key image and USB key image such as *.img.</p> <p>Note:</p> <p>For windows client, if the logical drive of the physical drive is dismount then the logical device is redirected with Read/Write Permission else it is redirected with Read permission only.</p> <p>For MAC client, External USB Hard disk redirection is only supported.</p> <p>For Linux client, fixed hard drive is redirected only as Read Mode. It is not Write mode supported.</p> <p>For USB key image redirection, support FAT 16, FAT 32 and NTFS.</p>

Keyboard Layout

Table 35: Keyboard Layout

ITEM	DESCRIPTION
Auto Detect	This option is used to detect keyboard layout automatically. The languages supported automatically are English – US, French – France, Spanish – Spain, German- Germany, Japanese- Japan. If the client and host languages are the same, then for all the languages other than English mentioned above, you must select this option to avoid typo errors.
Soft Keyboard	<p>This option allows you to select the keyboard layout. It will show the dialog as similar to onscreen keyboard. If the client and host languages are different, then for all the languages other than English mentioned above, you must select the appropriate language in the list shown in JViewer and use the soft keyboard to avoid typo errors.</p> <p>Note: Soft keyboard is applicable only for JViewer Application not for other application in the client system.</p>

Video Record

Note:

This option is available only when you launch the Java Console.

Table 36: Video Record

ITEM	DESCRIPTION
Important	To view this menu option you must download the Java Media Framework (JMF). It can be downloaded from the link http://www.oracle.com/technetwork/java/javase/download-142937.html
Start Record	This option is to start recording the screen.
Stop Record	This option is used to stop the recording.
Settings	To set the settings for video recording.

Procedure:

Note:

Before you start recording, you have to enter the settings.

1. Click **Video Record > Settings** to open the settings page as shown in the screenshot below.

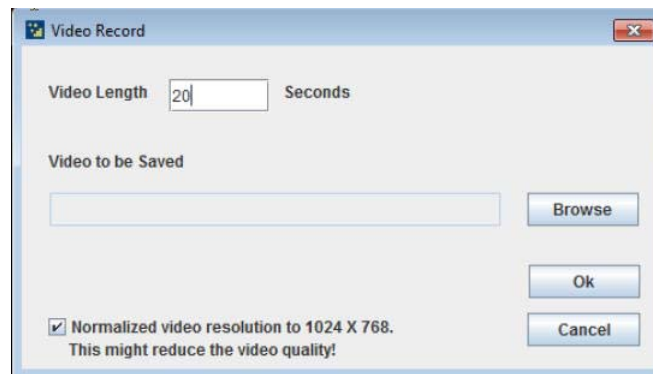


Figure 3-48. Video Record Settings Page

2. Enter the **Video Length** in seconds.
3. **Browse** and enter the location where you want the video to be saved.
4. Enable the option **Normalized video resolution to 1024X768**.
5. Click **OK** to save the entries and return to the Console Redirection screen.
6. Click **Cancel** if you don't wish to save the entries.
7. In the Console Redirection window, click **Video Record > Start Record**.
8. Record the process.
9. To stop the recording, click **Video Record > Stop Record**.

Active Users

Click this option to displays the active users and their system IP address.

Help

About Jviewer: Displays the copyright and version information

Quick Buttons

The lower right of Console Redirection windows displays all the quick buttons. These quick buttons helps you to perform these functions by just clicking them.

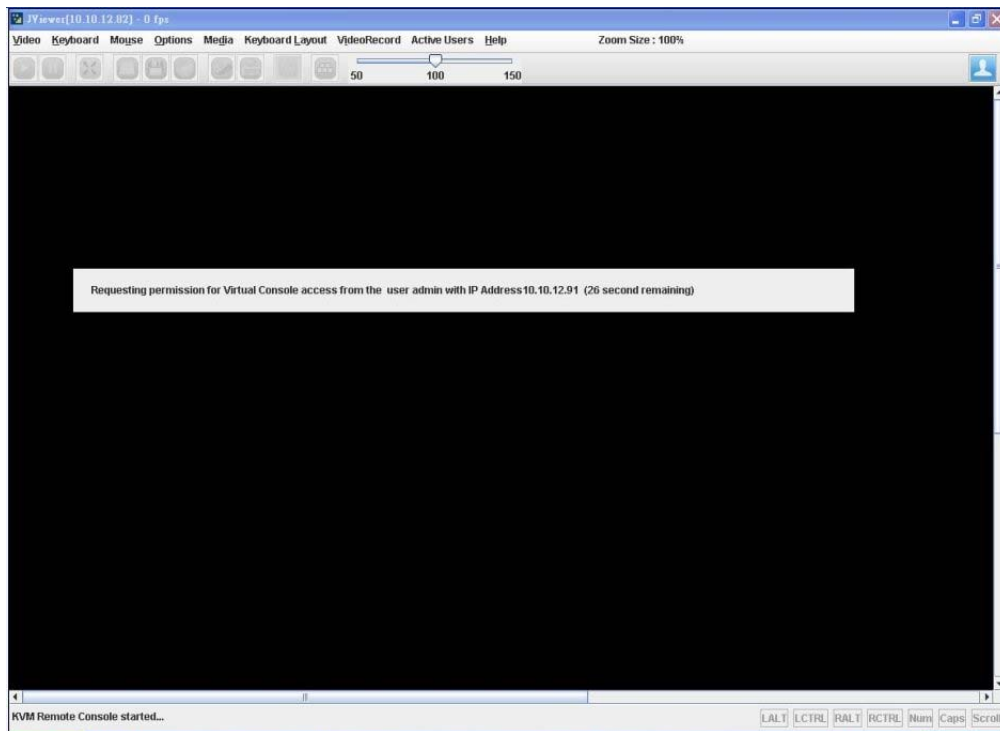
Note:

This option is available only when you launch the Java Console. The keyboard mapping is abnormal for number key(0-9) in remote KVM when console side is using laptop without dedicated number key. User need to press the "Num Lock" key to change its lock mode.

Multi-users in Remote KVM console

The Remote KVM console is only able to allow two users to login simultaneously. Regarding to KVM privilege, the first user has the greatest power to decide the second user access right.

The second user wants to launch remote KVM if first user already login remote KVM, and second user needs to wait for first user permit in 30 seconds, then second user will get the waiting information as shown below.

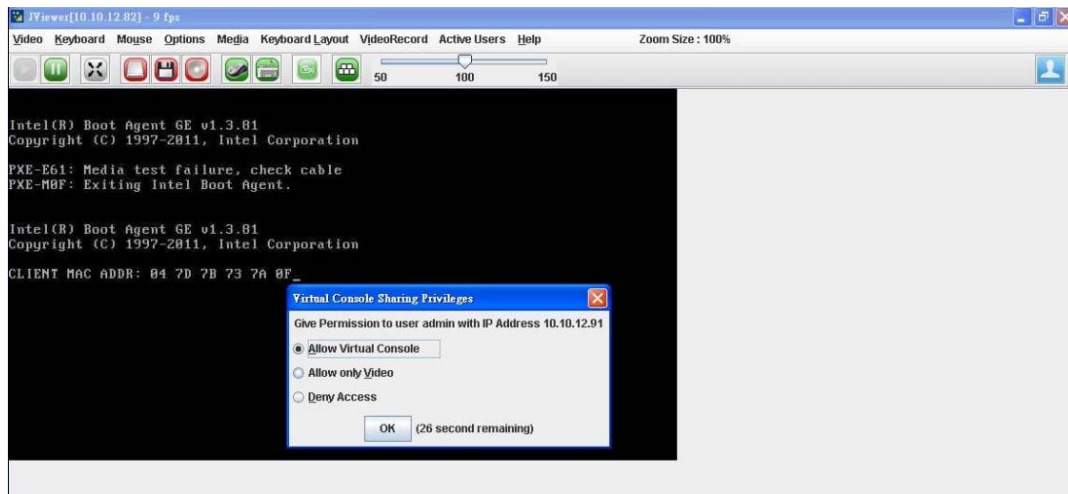


At the moment, first user needs to give permission to second user. And there are three options to decide the second user access right for the first user as below.

Allow Virtual Console: Second user is the same as first user access right, and second user can access the Keyboard, mouse, and Video function.

Allow only Video: Second user has only Video function.

Deny Access: Second user can not have any access right to access Keyboard, mouse, and Video function.



Server Power Control

This page allows you to view and control the power of your server.

In Power Control and Status page, you can click **Remote Control > Server Power Control** from the main menu, and then there are more options to control server system. Such as: reset system, power off (immediate), power off (orderly), power on and power cycle. A sample screenshot of Power Control and Status page is shown in the screenshot below.

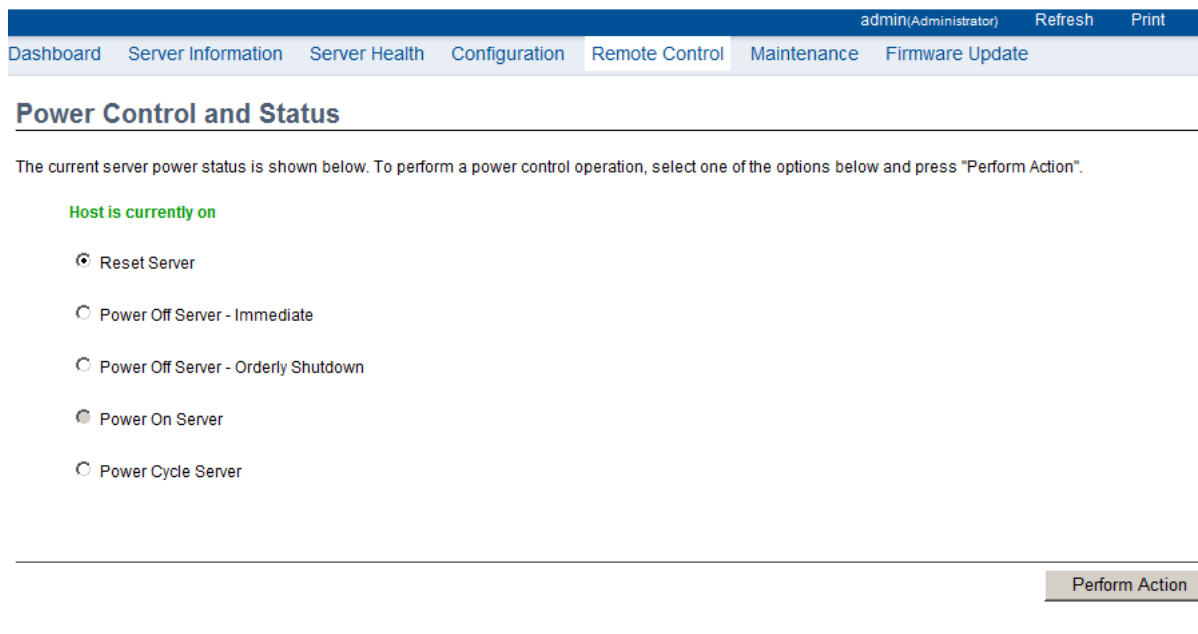


Figure 3-49. Power Control and Status Page

The various options of Power Control are given below.

Table 37: Server Power Control

ITEM	DESCRIPTION
Reset Server	This option will reboot the system without powering off (warm boot).
Power off Server – Immediate	This option will immediately power off the server.
Power off Server – Orderly Shut-down	This option will initiate operating system shutdown prior to the shut-down.
Power On Server	This option will power on the server.
Power Cycle Server	This option will first power off, and then reboot the system (cold boot).
Perform Action	Click this option to perform the selected operation.

Procedure:

Select an action and click **Perform Action** to proceed with the selected action.

Note:

You will be asked to confirm your choice. Upon confirmation, the command will be executed and you will be informed of the status.

Java SOL

This page allows you to launch the Java SOL. The Java SOL is used to view the host screen using the SOL Redirection.

To open Java SOL page, click **Remote Control > Java SOL** from the menu bar. A sample screenshot of Java SOL page is shown below.

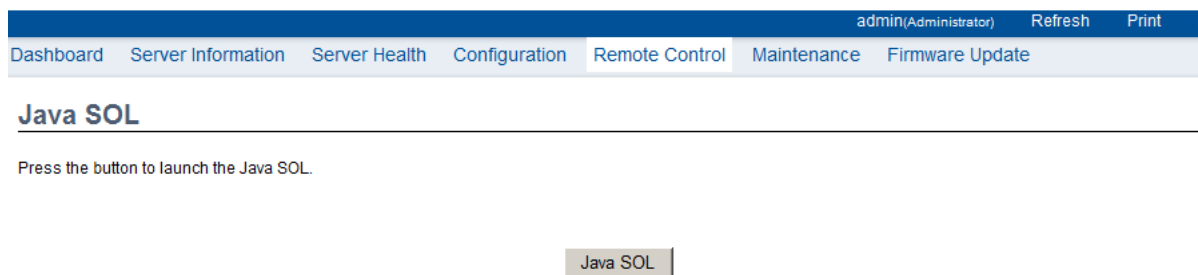


Figure 3-50. Java SOL Page

The various options of Power Control are given below.

Table 38: Server Power Control

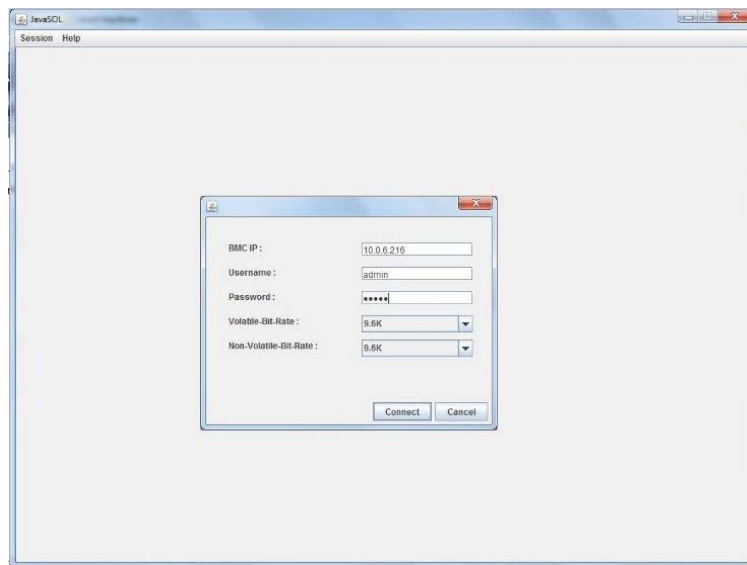
ITEM	DESCRIPTION
Reset Server	This option will reboot the system without powering off (warm boot).
Power off Server – Immediate	This option will immediately power off the server.

Table 38: Server Power Control (Continued)

ITEM	DESCRIPTION
Power off Server – Orderly Shut-down	This option will initiate operating system shutdown prior to the shut-down.
Power On Server	This option will power on the server.
Power Cycle Server	This option will first power off, and then reboot the system (cold boot).
Perform Action	Click this option to perform the selected operation.

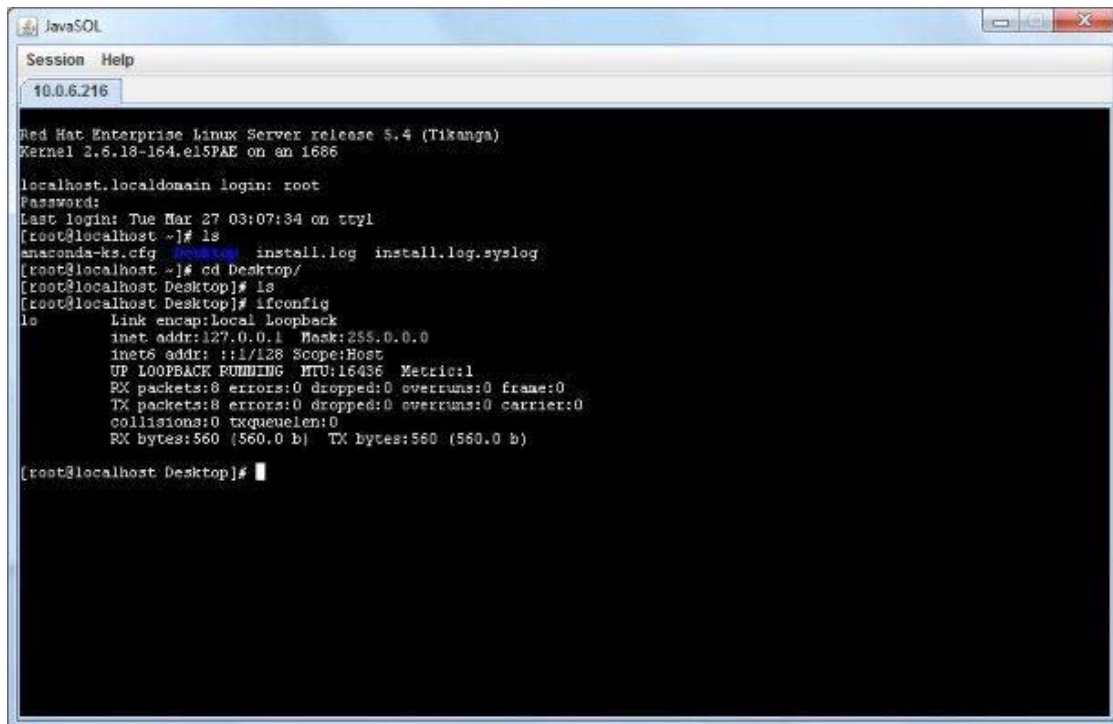
Procedure:

1. Click the Java SOL button to open the Java SOL window.



2. Enter the BMC IP address, User Name and Password in the respective fields.
3. Select the Volatile-Bit-Rate and Non-Volatile-Bit-Rate from the drop down lists.

- Click **Connect** to open the SOL redirection window as shown in the screenshot below.



```

JavaSOL
Session Help
10.0.6.216

Red Hat Enterprise Linux Server release 5.4 (Tikanga)
Kernel 2.6.18-164.el5PAE on an i686

localhost.localdomain login: root
Password:
Last login: Tue Mar 27 03:07:34 on tty1
[root@localhost ~]# ls
anaconda-ks.cfg  anaconda.log  install.log  install.log.syslog
[root@localhost ~]# cd Desktop/
[root@localhost Desktop]# ls
[root@localhost Desktop]# ifconfig
lo          Link encap:Local Loopback
            inet addr:127.0.0.1  Mask:255.0.0.0
            inet6 addr: ::1/128 Scope:Host
            UP LOOPBACK RUNNING  MTU:16386  Metric:1
            RX packets:8 errors:0 dropped:0 overruns:0 frame:0
            TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:560 (560.0 b)  TX bytes:560 (560.0 b)

[root@localhost Desktop]#

```

Maintenance Group

This group of pages allows you to do maintenance tasks on the device. The menu contains the following items:

- Preserve Configuration
- Restore Factory Defaults



Figure 3-51. Restore Factory Defaults

Preserve Configuration

This page allows the user to configure the preserve configuration items, which will be used by the Restore factory defaults to preserve the existing configuration without over-writing with default configuration.

admin/Administrator Refresh Print Logout

[Dashboard](#) [Server Information](#) [Server Health](#) [Configuration](#) [Remote Control](#) [Maintenance](#) [Firmware Update](#) [Help](#)

Preserve Configuration

This page allows you to select the specific configuration items to be preserved in the cases of "Restore Configuration", and "Firmware Update without Preserve Configuration option".

Click here to go to [Firmware Update](#) or [Restore Configuration](#)

Number of Preserved Items: 0

#	Preserve Configuration Item	Preserve Status
1	SDR	<input type="checkbox"/>
2	FRU	<input type="checkbox"/>
3	SEL	<input type="checkbox"/>
4	IPMI	<input type="checkbox"/>
5	Network	<input type="checkbox"/>
6	NTP	<input type="checkbox"/>
7	SSH	<input type="checkbox"/>
8	KVM	<input type="checkbox"/>
9	Authentication	<input type="checkbox"/>
10	Syslog	<input type="checkbox"/>

Figure 3-52. Preserve Configuration Page

Item Verification Procedure

1. SDR

Step 1: add OEM record (Please refer to IPMI 2.0 Spec. page 468/644)

Command: **ipmitool raw 0x0a 0x24 0x0 0x0 0x51 0xc0 4 0x57 0x01 0x0 0xf5**

Response: 55 00 „» 55 is the last record ID

Step 2: get OEM record, to use the last record ID to check if added successfully (Please refer to IPMI 2.0 Spec. page 466/644)

Command: **ipmitool raw 0x0a 0x23 0x0 0x0 0x55 0x0 0x0 0xff**

Response: ff ff 55 00 51 c0 04 57 01 0 f5 „» ff ff means record ID 55 is the last record ID

Step 3: go to Web-UI to check "SDR" to be preserved

Step 4: upgrade firmware

Step 5: after Step 4, go to Step 2 and check if the OEM record is still preserved (if preserved then PASS, else FAIL)

2. SEL

Step 1: Please use IPMI command to add an event. Ex: ipmitool event 1

Step 2: go to Event Log to check if the event added

Step 3: go to Web-UI to check "SEL" to be preserved

Step 4: upgrade firmware

Step 5: after Step 4, go to Step 2 and check if the event is still preserved
(if preserved then PASS, else FAIL)

3. IPMI

Step 1: Please add a new user by Web.

Step 2: check if the user added

Step 3: go to Web-UI to check "IPMI" to be preserved

Step 4: upgrade firmware

Step 5: after Step 4, go to Step 2 and check if the user is still exist
(if preserved then PASS, else FAIL)

4. Network

Step 1: Please change BMC IPv4 address source to be STATIC or DHCP mode by Web.

Step 2: check if the mode changed

Step 3: go to Web-UI to check "Network" to be preserved

Step 4: upgrade firmware

Step 5: after Step 4, go to Step 2 and check if the mode is still preserved
(if preserved then PASS, else FAIL)

5. SNMP (supported from Grantley platform)

Step 1: Please go to add a new user and enable SNMP function.

Step 2: check if the user added and SNMP function enabled

Step 3: go to Web-UI to check "SNMP" to be preserved

Step 4: upgrade firmware

Step 5: after Step 4, go to Step 2 and check if the setting is still preserved
(if preserved then PASS, else FAIL)

6. SSH

Step 1: Please go to add a new user and update the NEW SSH key.

Step 2: check if the user added SSH key updated

Step 3: go to Web-UI to check "SSH" to be preserved

Step 4: upgrade firmware

Step 5: after Step 4, go to Step 2 and check if the mode is still preserved
(if preserved then PASS, else FAIL)

7. KVM

Step 1: Please modify the "Remote Session", "Mouse Mode", and "Virtual Media Devices" setting by Web.

Step 2: check if the setting changed

Step 3: go to Web-UI to check "KVM" to be preserved

Step 4: upgrade firmware

Step 5: after Step 4, go to Step 2 and check if the setting is still preserved (if preserved then PASS, else FAIL)

8. Services (supported from Grantley and Microserver platform)

Step 1: Please change the default value of each item by Web.

Step 2: check if the setting changed

Step 3: go to Web-UI to check "Services" to be preserved

Step 4: upgrade firmware

Step 5: after Step 4, go to Step 2 and check if the setting is still preserved (if preserved then PASS, else FAIL)

Restore Factory Defaults

In MegaRAC GUI, this option is used to restore the factory defaults of the device firmware.

Note:

SSL cert doesn't support restore default



WARNING!

Please note that after entering restore factory widgets, other web pages and services will not work. All open widgets will be closed automatically. The device will reset and reboot within a few minutes.

To open Restore Factory Defaults page, click **Maintenance > Restore Factory Defaults** from the main menu. A sample screenshot of Restore Factory Defaults Page is shown in the screenshot below.

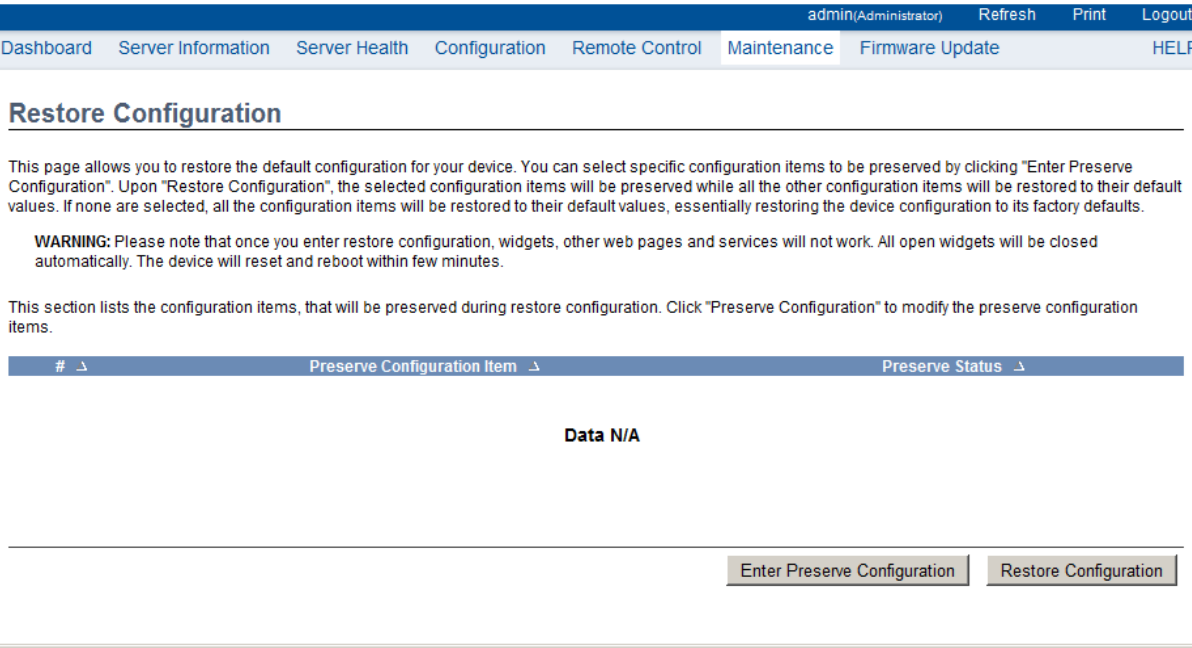


Figure 3-53. Restore Factory Defaults Page

Procedure:

Click **Restore Factory** to restore the factory defaults of the device firmware.

Firmware Update

This group of pages allows you to do Firmware Update on the device. The menu contains the following items:

- BMC Firmware Update
- BIOS Update

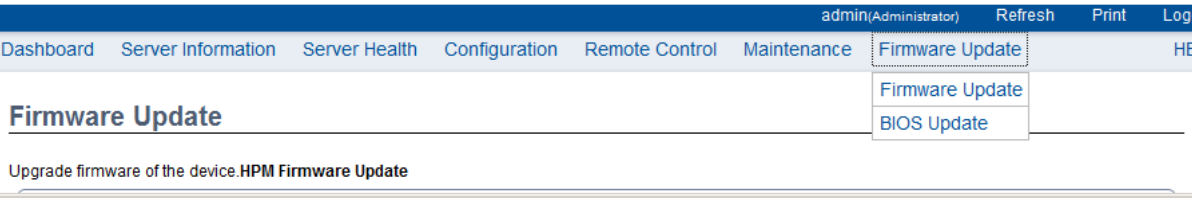


Figure 3-54. Firmware Update Menu

BMC Firmware Update

In MegaRAC GUI, this wizard takes you through the process of firmware up gradation. A reset of the box will automatically follow if the upgrade is completed or cancelled. An

option to preserve configuration will be presented. Enable it, if you wish to preserve configured settings through the upgrade.



WARNING!

Please note that after entering update mode widgets, other web pages and services will not work. All open widgets will be closed automatically. If upgrade process is cancelled in the middle of the wizard, the device will be reset.

Note:

The firmware upgrade process is a crucial operation. Make sure that the chances of a power or connectivity loss are minimal when performing this operation.

Once you enter into *Update Mode* and choose to cancel the firmware flash operation, the MegaRAC® card must be reset. This means that you must close the Internet browser and log back onto the MegaRAC® card before you can perform any other types of operations.

To open Firmware Update page, click **Firmware Update** > **Firmware Update** from the main menu. A sample screenshot of Firmware Update Page is shown in the screenshot below.

admin(Administrator) Refresh Print Logout

Dashboard Server Information Server Health Configuration Remote Control Maintenance Firmware Update HELP

Firmware Update

Upgrade firmware of the device.HPM Firmware Update

The protocol information to be used for firmware image transfer during this update is as follows. To configure, choose 'Protocol Configuration' under Firmware Update menu.

Protocol Type : HTTP/HTTPS

☒ HPM ☐ AMI

Continue

WARNING: Please note that after entering the update mode, the widgets, other web pages and services will not work. All the open widgets will be automatically closed. If the upgradation is cancelled in the middle of the wizard, the device will be reset.

Figure 3-55. Firmware Update Page

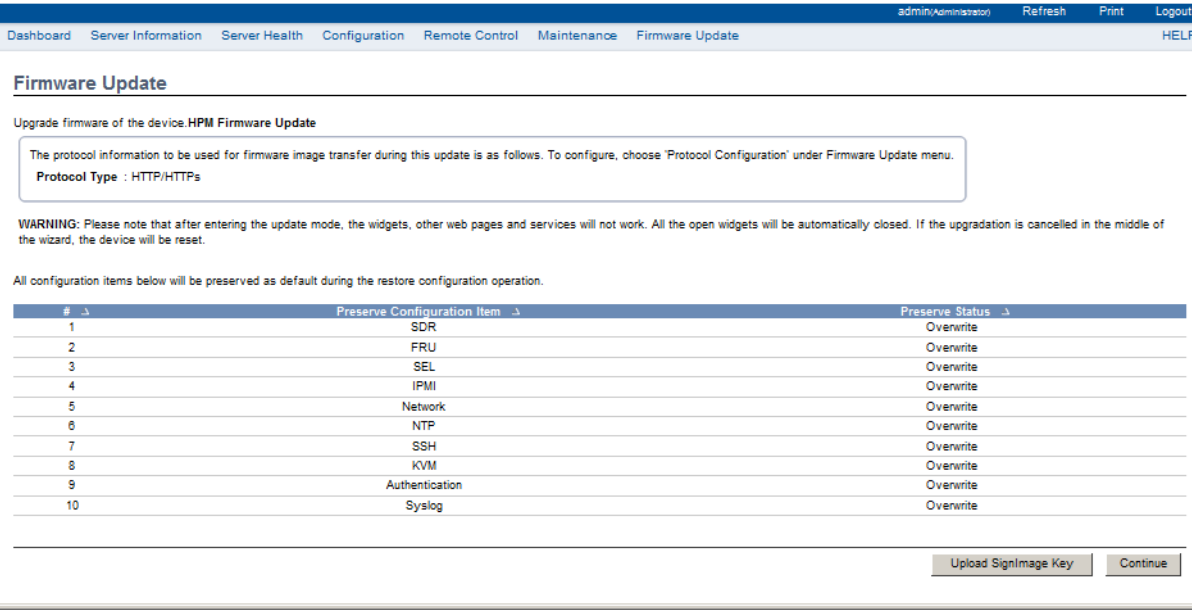
The types of Firmware Update are as follows.

- HPM
- AMI

HPM

This wizard takes you through the process of HPM based firmware upgrade.

To process **HPM** Firmware Upgradation, select **HPM** option and click **Continue** to upgrade the current device firmware. The screenshot of HPM Firmware Update is as shown below.



Note:

All configuration items below will be preserved as default during the restore configuration operation.

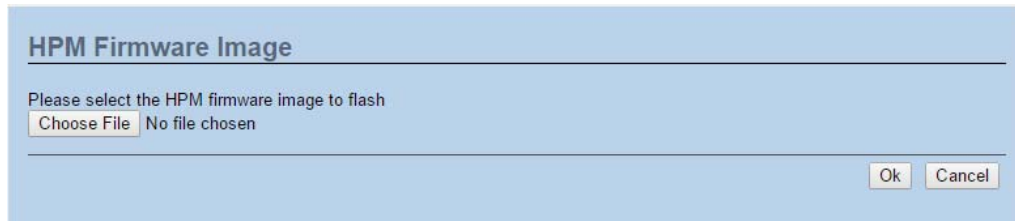
The various are listed below.

Preserve Configuration Item: The Preserve Configuration items will be listed.

Preserve Status: The status of the Preserve Configuration items.

Procedure

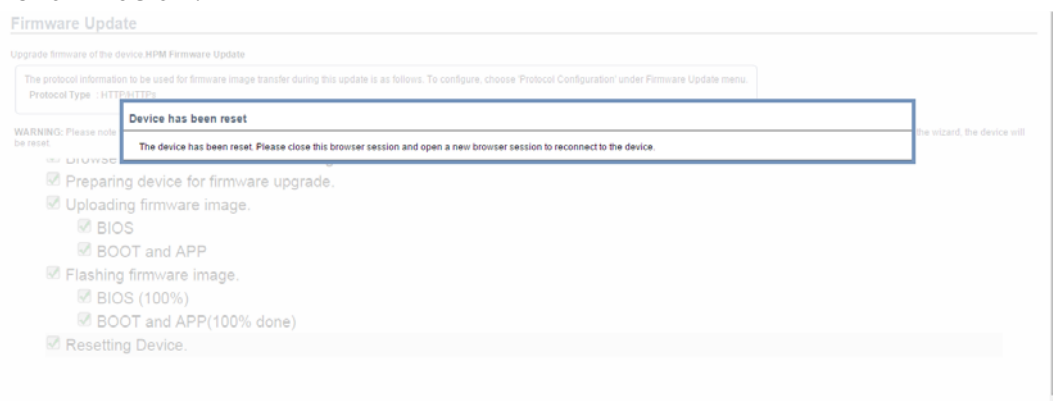
1. To proceed HPM Firmware Update, click **Continue**. The Firmware update undergoes the following steps:
 - a. Click Choose **File** to browse and select the Firmware image to flash and click **Ok**.



Note:

While creating HPM image with multiple components, Boot and App components should be placed at the end of the conf file.

- b. Preparing Device for Firmware Upgrade.
- c. Uploading Firmware Image.
- d. If flashing is required for all Components, select the option **Update All** to update all the Components or select any specific **Component Name** and click **Proceed** to update the Firmware. The list of components used to allow you to configure the Firmware image will be displayed as shown in the below screenshot.
- e. Flashing the image.
- f. Resetting the image. The sample screenshot of HPM Firmware update is as shown below.



Note:

You will not be able to perform any other tasks until firmware upgrade is completed and the device is rebooted. You can now follow the instructions presented in the subsequent pages to successfully update the card's firmware. The device will reset if update is canceled. The device will also reset upon successful completion of firmware update.

AMI

This wizard takes you through the process of AMI based firmware upgrade.

To process **AMI** Firmware Upgrade, select **AMI** option and click **Continue** to upgrade the current device firmware. The screenshot of AMI Firware Update is as shown below.

admin/Administrator Refresh Print

Dashboard Server Information Server Health Configuration Remote Control Maintenance **Firmware Update**

Firmware Update

Upgrade firmware of the device. Press 'Enter Update Mode' to put the device in update mode.

The protocol information to be used for firmware image transfer during this update is as follows. To configure, choose 'Protocol Configuration' under Firmware Update menu.

Protocol Type : HTTP/HTTPS

WARNING: Please note that after entering the update mode, the widgets, other web pages and services will not work. All the open widgets will be automatically closed. If the upgradation is cancelled in the middle of the wizard, the device will be reset.

☐ Preserve all Configuration. This will preserve all the configuration settings during the firmware update - irrespective of the individual items marked as preserve/overwrite in the table below. All configuration items below will be preserved as default during the restore configuration operation. Click "Enter Preserve Configuration" to modify the Preserve status settings.

#	Preserve Configuration Item	Preserve Status
1	SDR	Overwrite
2	FRU	Overwrite
3	SEL	Overwrite
4	IPMI	Overwrite
5	Network	Overwrite
6	NTP	Overwrite
7	SSH	Overwrite
8	KVM	Overwrite
9	Authentication	Overwrite
10	Syslog	Overwrite

Upload SignImage Key Enter Preserve Configuration Enter Update Mode

Note:

All configuration items below will be preserved as default during the restore configuration operation.

The various are listed below.

Preserve All Configurations: To preserve all the listed configurations.

Preserve Configuration Item: The Preserve Configuration items will be listed.

Preserve Status: The status of the Preserve Configuration items.

Enter Preserve Configuration: To redirect to the Preserve Configuration page.

Enter Update Mode: To upgrade the current device firmware.

WARNING:

Please note that after entering the update mode, the widgets, other web pages and services will not work. All the open widgets will be automatically closed. If the upgradation is cancelled in the middle of the wizard, the device will be reset.

Procedure

Note:

To configure Protocol information, choose **Protocol Configuration** under Firmware Update menu. To configure Image to be booted from upon Reset, choose **Dual Image Configuration** under **Firmware Update** menu.

1. Check the option **Preserve All Configuration** to preserve all the listed configurations.
2. Click **Enter Preserve Configuration** to redirect to **Preserve Configuration** page, which is used to preserve the particular configuration not to be overwritten by the default configuration. The sample screenshot is shown below.

admin(Administrator) Refresh Print Log

Dashboard Server Information Server Health Configuration Remote Control Maintenance Firmware Update HE

Preserve Configuration

This page allows you to select the specific configuration items to be preserved in the cases of "Restore Configuration", and "Firmware Update without Preserve Configuration option".

Click here to go to [Firmware Update](#) or [Restore Configuration](#)

Number of Preserved Items: 0

#	Preserve Configuration Item	Preserve Status
1	SDR	<input type="checkbox"/>
2	FRU	<input type="checkbox"/>
3	SEL	<input type="checkbox"/>
4	IPMI	<input type="checkbox"/>
5	Network	<input type="checkbox"/>
6	NTP	<input type="checkbox"/>
7	SSH	<input type="checkbox"/>
8	KVM	<input type="checkbox"/>
9	Authentication	<input type="checkbox"/>
10	Syslog	<input type="checkbox"/>

Check All Uncheck All Save Reset

3. Select **Check All** to select the configuration items to be preserved in the cases of "Restore Configuration", and "Firmware Update without Preserve Configuration option".
4. Click **Save** to preserve the Configuration Items.
5. Click **Enter Update Mode** to upgrade the current device firmware. The Firmware update undergoes the following steps:
 - a. Closing all active client requests
 - b. Preparing Device for Firmware Upgrade
 - c. Uploading Firmware Image

Note:

A file upload pop-up will be displayed for http/https but in the case of tftp files, the file is automatically uploaded displaying the status of upload.

- d. Browse and select the Firmware image to flash and click **Upload**.

- e. Verifying Firmware Image

In Section Based Firmware Update, you can configure the firmware image for section based flashing. Check the required sections and click **Proceed** to update the firmware.

- If flashing is required for all images, select the option **Full Flash**.
- If you select **Version Compare Flash** option from web, the current and uploaded module versions, FMHlocation, size will be compared.
- If the modules differ in size and location, proceed with force firmware upgrade.
- If all the module versions are same, restart BMC by saying all the module versions are similar.
- If only few module versions are differ, those module will be flashed.

Note:

Only selected sections of the firmware will be updated. Other sections are skipped. Before starting flash operation, you are advised to verify the compatibility between image sections.

#	Section Name	Existing Version	Uploaded Version	Upgradable/Non-Upgradable
1	boot	1.4	1.4	<input type="checkbox"/>
2	conf	1.4	1.4	<input type="checkbox"/>
3	bkupcon	1.4	1.4	<input type="checkbox"/>
4	root	1.4	1.4	<input type="checkbox"/>
5	osimage	1.4	1.4	<input type="checkbox"/>
6	www	1.4	1.4	<input type="checkbox"/>
7	lmedia	1.4	1.4	<input type="checkbox"/>
8	hornet	1.4	1.4	<input type="checkbox"/>

- f. Flashing Firmware Image
- g. Resetting Device

Note:

You will not be able to perform any other tasks until firmware upgrade is complete and the device is rebooted. You can now follow the instructions presented in the subsequent pages to successfully update the card's firmware.

The device will reset if update is canceled. The device will also reset upon successful completion of firmware update.

BIOS Update

This page allow user to update BIOS image, but only works when DC is off. Please note the filename extension of BIOS image shall be **.bin*. For example: BIOS3A22.bin. After BIOS update complete, system must perform AC cycle to take effect.

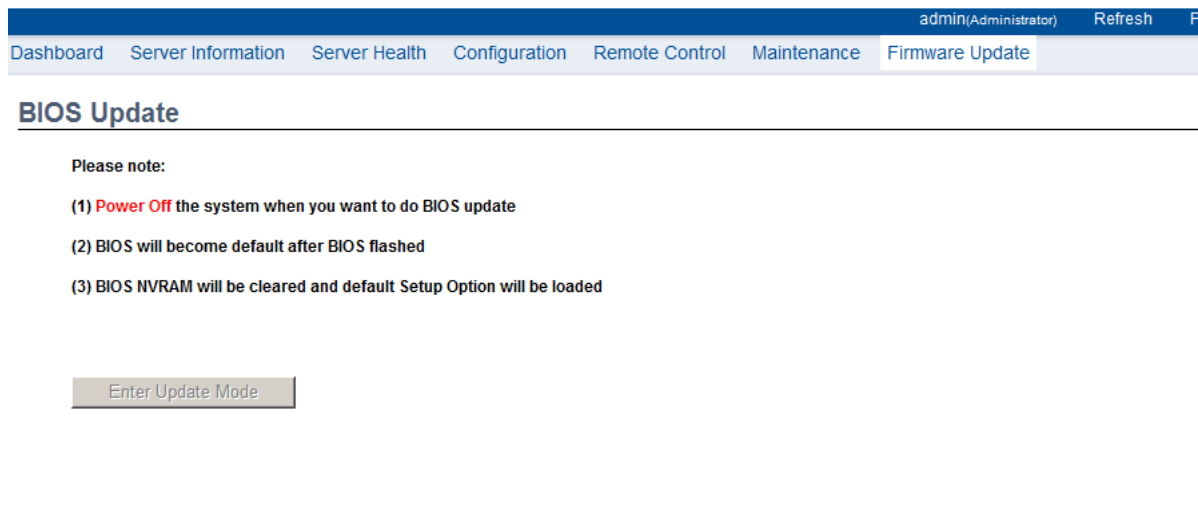


Figure 3-56. BIOS Update Page

Log Out

To log out of the MegaRAC GUI, click the logout link on the top right corner of the screen.

User Privilege

Below table describes user privilege definition and the main different features.

Table 39: User Privilege Definition

USER PRIVILEGE	DEFINITION
Administrator	All Web-UI functions are allowed.
Operator	Only allow to view all Web-UI functions.
OEM	Only allow to view all Web-UI functions. But Users, DNS, Network and PEF are not allowed to be viewed.
User/Callback	Support for ipmitool, not for Web-UI.

Note:

Command privilege level table defined in IPMI 2.0 Specification Appendix G – Command Assignments. According to IPMI 2.0 Specification, **Chassis Identify** command is allowed for Operator privilege. Because this command didn't

change BMC configuration, just to trigger Identify LED used to display where Server is. So it is expected behavior. After checked other Operator privilege command by IPMI 2.0 Specification, **Chassis Control command** (Power On/Off) is also allowed. But in our code base, we raise **Chassis Control** command to be Administrator to protect system. So, in **Server Power Control** page, only Administrator can control server power.

Table 40: User Privilege

WEB GUI PRIVILEGE LIST	PRIVILEGE ASSOCIATION BETWEEN IPMI AND WEB GUI			
	ADMINISTRATOR	OPERATOR	USER/ CALLBACK	OEM
login BMC from Web GUI	O	O	X	O
configure BMC from Web GUI	O	X	X	X
configure users from Web GUI	O	X	X	X
clear logs from Web GUI	O	X	X	X
execute server power control from Web GUI	O	X	X	X
virtual KVM redirection	O	X	X	X
virtual media	O	X	X	X
View Users	O	O	X	X
View DNS	O	O	X	X
View Network	O	O	X	X
View PEF	O	O	X	X

Login BMC through SSH

- ID: **sysadmin**, Password: **superuser**
- Web Account can't login SSH
- SMASH

If supported SMASH then to login SSH will go to SMASH.

If NOT Support SMASH then to login SSH will go to BMC console.

Regulatory and Compliance Information

Chapter 4

This section provides regulatory and compliance information applicable to this system.

4.1 Electromagnetic Compatibility Notices

FCC Verification Statement (USA)

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Europe (CE Declaration of Conformity)

This product has been tested in accordance too, and complies with the Low voltage Directive (2006/95/EC) and EMC Directive (2004/108/EC). The product has been marked with the CE Mark to illustrate its compliance.

VCCI (Japan)

この装置は、クラス A 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。
VCCI-A

English translation of the notice above:

This is a Class A product based on the standard of the Voluntary Control Council for Interference (VCCI) from Information Technology Equipment. If this is used near a radio or television receiver in a domestic environment, it may cause radio interference. Install and use the equipment according to the instruction guide.

BSMI (Taiwan)

The BSMI Certification Marking and EMC warning is located on the outside rear area of the product

警告使用者：

此為甲類資訊技術設備，於居住環境中使用時，可能會造成射頻擾動，在此種情況下，使用者會被要求採取某些適當的對策。

Regulated Specified Components

To maintain the UL listing and compliance to other regulatory certifications and/or declarations, the following regulated components must be used and conditions adhered to. Interchanging or use of other component will void the UL listing and other product certifications and approvals.

Updated product information for configurations can be found on the site at the following URL: <http://www.QCT.io>

If you do not have access to the Web address, please contact your local representative.

- Add-in cards: must have a printed wiring board flammability rating of minimum UL94V-1. Add-in cards containing external power connectors and/or lithium batteries must be UL recognized or UL listed. Any add-in card containing modem telecommunication circuitry must be UL listed. In addition, the modem must have the appropriate telecommunications, safety, and EMC approvals for the region in which it is sold.
- Peripheral Storage Devices: must be UL recognized or UL listed accessory and TUV or VDE licensed. Maximum power rating of any one device is 19 watts. Total server configuration is not to exceed the maximum loading conditions of the power supply.

Restriction of Hazardous Substances (RoHS) Compliance

Quanta Computer Inc. has a system in place to restrict the use of banned substances in accordance with the European Directive 2011/65/EU. Compliance is based on declaration that materials banned in the RoHS Directive are either (1) below all applicable threshold limits or (2) an approved / pending RoHS exemption applies.

RoHS implementation details are not fully defined and may change.

Threshold limits and banned substances are noted below:

- Quantity limit of 0.1% by mass (1000 PPM) for:
 - Lead
 - Mercury
 - Hexavalent Chromium
 - Polybrominated Biphenyls Diphenyl Ethers (PBDE)
- Quantity limit of 0.01% by mass (100 PPM) for:
 - Cadmium

End of Life / Product Recycling

Product recycling and end-of-life take-back systems and requirements vary by country. Contact the retailer or distributor of this product for information about product recycling and / or take-back.

4.2 Product Regulatory Compliance Markings

This product is marked with the following product certification markings:

Table 1: Product Regulatory Compliance Markings

REGULATORY COMPLIANCE	REGION	MARKING
cULus Listing Mark	USA / Canada	
CE Mark	Europe	
FCC Marking (Class A)	USA	This device complies with Part 15 of the FCC Rules. Operation of this device is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) This device must accept any interference received, including interference that may cause undesired operation.
VCCI Marking (Class A)	Japan	この装置は、クラス A 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。 VCCI-A
BSMI Certification & Class A Warning	Taiwan	 警告使用者： 此為甲類資訊技術設備，於居住環境中使用時，可能會造成射頻擾動，在此種情況下，使用者會被要求採取某些適當的對策。
ICES	Canada	CAN ICES-3(A)/NMB-3(A)
Recycling Package Mark	Other than China	
EAC Marking	Russia	