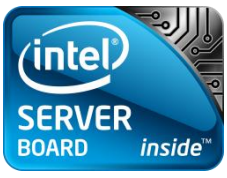
Intel® Server Board S1600JP

Technical Product Specification

Intel order number G68018-002



Revision 1.1

October 2012

Enterprise Platforms and Services Division – Marketing

Revision History

Date	Revision Number	Modifications
May 2012	0.5	Initial release.
June 2012	0.6	▪ Updated Memory Support Guidelines. ▪ Updated Processor Information.
July 2012	1.0	▪ Updated All Block Diagrams. ▪ Updated Risers Information. ▪ Updated BIOS Setup Interface. ▪ Updated Connector and Header Location and Pin-out. ▪ Updated Power Supply Specific Guidelines.
October 2012	1.1	▪ Updated BIOS Setup Interface. ▪ Update the Memory Support Guidelines.

Disclaimers

Information in this document is provided in connection with Intel® products. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted by this document. Except as provided in Intel®'s Terms and Conditions of Sale for such products, Intel® assumes no liability whatsoever, and Intel® disclaims any express or implied warranty, relating to sale and/or use of Intel® products including liability or warranties relating to fitness for a particular purpose, merchantability, or infringement of any patent, copyright or other intellectual property right. Intel® products are not intended for use in medical, life-saving, or life sustaining applications. Intel® may make changes to specifications and product descriptions at any time, without notice.

Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined." Intel® reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them.

This document contains information on products in the design phase of development. Do not finalize a design with this information. Revised information will be published when the product is available. Verify with your local sales office that you have the latest datasheet before finalizing a design.

This document may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

This document and the software described in it are furnished under license and may only be used or copied in accordance with the terms of the license. The information in this manual is furnished for informational use only, is subject to change without notice, and should not be construed as a commitment by Intel Corporation. Intel Corporation assumes no responsibility or liability for any errors or inaccuracies that may appear in this document or any software that may be provided in association with this document.

Except as permitted by such license, no part of this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means without the express written consent of Intel Corporation.

Intel and Xeon are trademarks or registered trademarks of Intel Corporation.

*Other brands and names may be claimed as the property of others.

Table of Contents

List of Figures

List of Tables

<This page is intentionally left blank.>

1. Introduction

The Intel® Server Board S1600JP is a half width, single socket server board using the Intel® Xeon® Processor E5-2600 series or Intel® Xeon® Processor E5-1600 series processor, in combination with Intel® C600 chipset to provide a balance feature set between technology leadership and cost.

This Technical Product Specification (TPS) provides board-specific information detailing the features, functionality, and high-level architecture of the Intel® Server Boards S1600JP.

For design-level information of specific components or subsystems relevant to the server boards described in this document, additional documents can be obtained through Intel®. The reference documents lists documents used as reference to compile much of the data provided here. Some of the listed documents are not publically available and must be ordered through your local Intel® representative.

1.1 Section Outline

This document is divided into the following chapters:

- Chapter 1 – Introduction
- Chapter 2 – Server Board Overview
- Chapter 3 – Product Architecture Overview
- Chapter 4 – Platform Management Functional Overview
- Chapter 5 – BIOS Setup Interface
- Chapter 6 – Configuration Jumpers
- Chapter 7 – Connector and Header Location and Pin-out
- Chapter 8 – Intel® Light-Guided Diagnostics
- Chapter 9 – Environmental Limits Specifications
- Chapter 10 – Power Supply Specification Guidelines
- Appendix A – Integration and Usage Tips
- Appendix B – Integrated BMC Sensor Tables
- Appendix C – BIOS Sensors and SEL Data
- Appendix D – POST Code LED Decoder
- Appendix E – Video POST Code Errors
- Glossary
- Reference Documents

1.2 Server Board Use Disclaimer

Intel Corporation server boards contain a number of high-density VLSI and power delivery components that need adequate airflow to cool. Intel® ensures through its own chassis development and testing, that when Intel® server building blocks are used together, the fully integrated system will meet the intended thermal requirements of these components. It is the responsibility of the system integrator who chooses not to use Intel® developed server building blocks to consult vendor datasheets and operating parameters to determine the amount of air flow required for their specific application and environmental conditions. Intel Corporation cannot be held responsible if components fail or the server board does not operate correctly when used outside any of their published operating or non-operating limits.

2. Server Board Overview

The Intel® Server Board S1600JP is a monolithic Printed Circuit Board (PCB) with features designed to support the high performance and high density computing markets. This server board is designed to support the Intel® Xeon® processor E5-2600 or Intel® Xeon® processor E5-1600 product family. Previous generation Intel® Xeon® processors are not supported. Many of the features and functions of the server board family are common. A board will be identified by name when a described feature or function is unique to it.

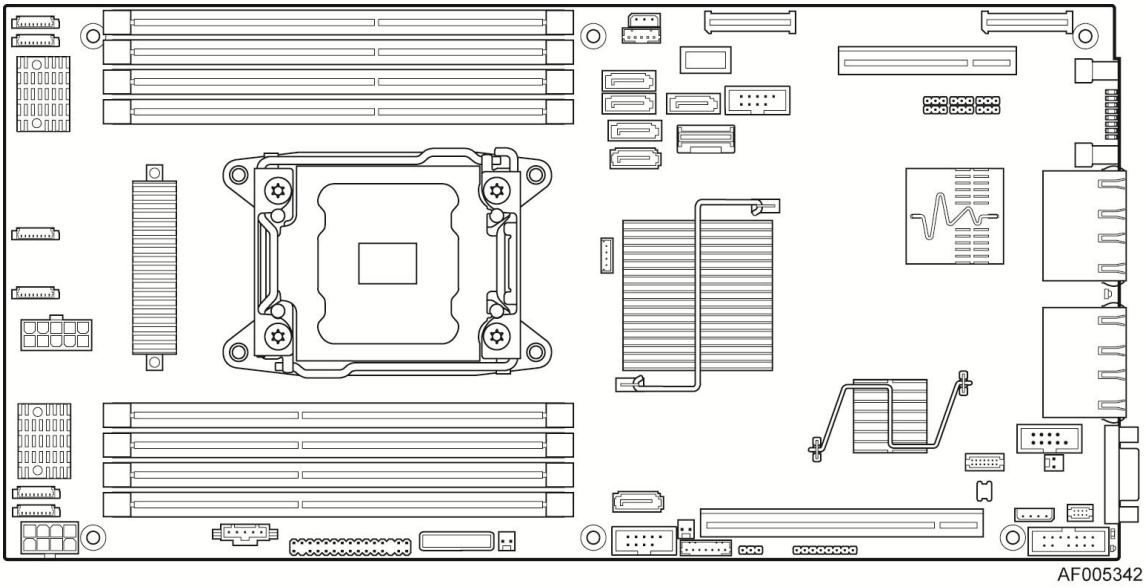


Figure 1. Intel® Server Board S1600JP (4NIC SKU)

There are two board SKUs based on different hardware configurations:

- **S1600JP4**: Base SKU with Quad NIC
- **S1600JP2:** Base SKU with Dual NIC

The following table provides a high-level product feature list:

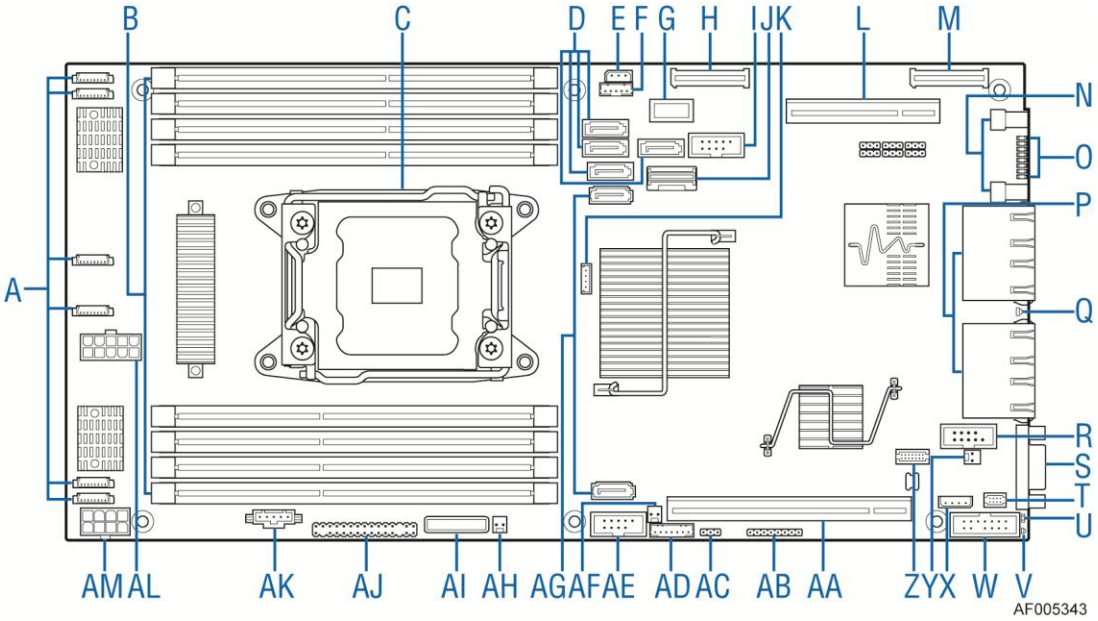
Table 1. Intel® Server Board S1600JP Feature Set

Feature	Description
Processors	Support for one Intel® Xeon® Processor E5-2600 series or one Intel® Xeon® Processor E5-1600 series ▪ LGA 2011 Socket R ▪ Thermal Design Power (TDP) up to 135 Watts for Intel® Xeon® Process E5-2600 series or up to 130 Watts for Intel® Xeon® Processor E5-1600 series

Feature	Description
Memory	▪ Eight DIMM slots, four memory channels, two DIMM slots per channel ▪ Unbuffered DDRIII (UDIMM), Registered DDRIII (RDIMM) and Load Reduced DDRIII (LRDIMM) ▪ Memory DDRIII data transfer rate of 800/1066/1333/1600MT/s ▪ DDRIII standard I/O voltage of 1.5V (all speed) and DDRIII Low Voltage of 1.35V (1333MT/s or below)
Chipset	Intel® C600-A Platform Controller Hub (PCH) with support for optional Storage Upgrade Key.
External I/O Connections	▪ DB-15 Video connectors ▪ Four RJ-45 Network Interface for 10/100/1000 LAN (SKU: S1600JP4) ▪ Two RJ-45 Network Interface for 10/100/1000LAN (SKU: S1600JP2) ▪ Two USB 2.0 connectors
Internal I/O connectors/headers	▪ One Type A USB connector ▪ Two 2 x 5 USB connectors ▪ One 2 x 5 serial port connector ▪ One internal video connector for the front video ▪ Six SATA connectors ▪ One mini SAS connector
Power Connections	▪ One 2 x 4 connector for board main power ▪ One 2 x 5 connector for board main power
System Fan Support	Six system fan connectors
Add-in Riser Support	Three PCIe Gen III riser slots ▪ Riser slot 1 and 3 support PCIe Gen III x16 Riser ▪ Riser slot 2 supports PCIe Gen III x8 Riser (Intel® rIOM)
Video	▪ Integrated 2D Video Graphics controller ▪ 128 MB DDRIII Memory
Hard Drive Support	Two SATA ports at 6Gbps, four SATA ports at 3Gbps and one mini-SAS port
RAID Support	▪ Intel® RSTe SW RAID 0/1/10/5 for SATA mode ▪ ESRTII SW RAID 0/1/10/5
Server Management	▪ Onboard Emulex* LLC Pilot III* Controller ▪ Support for Intel® Remote Management Module 4 Lite solutions ▪ Intel® Light-Guided Diagnostics on field replaceable units ▪ Support for Intel® System Management Software ▪ Support for Intel® Intelligent Power Node Manager (Need PMBus*-compliant power supply)

2.1 Server Board Connector and Component Layout

The following illustration provides a general overview of the server board, identifying key feature and component locations. The majority of the items identified are common in the Intel® Server Board S1600JP family. The accompanying table will identify variations when present.

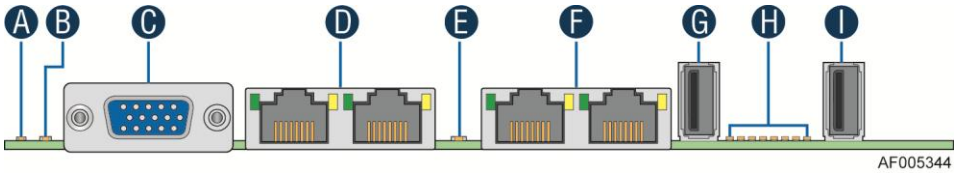


A	6 system fans	K	Storage upgrade key	U	5V standby LED	AE	Internal USB
B	8 DIMM sockets	L	Riser slot 2	V	ID LED	AF	HDD LED Header
C	CPU socket	M	Riser Slot 3A	W	Internal Video connector	AG	Two 6Gbps SATA ports
D	Four 3Gbps SATA ports	N	Two external rear USBs	X	IPMB	AH	HDD LED
E	HSBP I^2C	O	Diagnostic LED	Y	Chassis intrusion	AI	Battery
F	SGPIO	P	4 NIC 1Gbe ports	Z	TPM connector	AJ	Front panel connector
G	TypeA USB	Q	System status LED	AA	Riser slot 1	AK	PMBus*
H	Riser Slot 3B	R	Internal Serial port	AB	JPLD TAG	AL	5x2 Main power 1
I	Internal USB	S	Video port	AC	PECI	AM	4x2 Main power 2
J	Mini SAS port	T	RMM4 lite	AD	LCP		

Figure 2. Intel® Server Board S1600JP Components

2.1.1 Board Rear Connector Placement

The Intel® Server Board S1600JP has the following board rear connector placement:



	Description		Description
A	ID LED	F	Two NIC ports (RJ45)
B	5V standby LED	G	USB connector
C	DB15 Video out	H	Diagnostic LED
D	Two NIC ports (RJ45)	I	USB connector
E	System status LED		

Figure 3. Rear Panel Connector Placement

2.1.2 Server Board Mechanical Drawings

The following figures are mechanical drawings for the Intel® Server Board S1600JP:

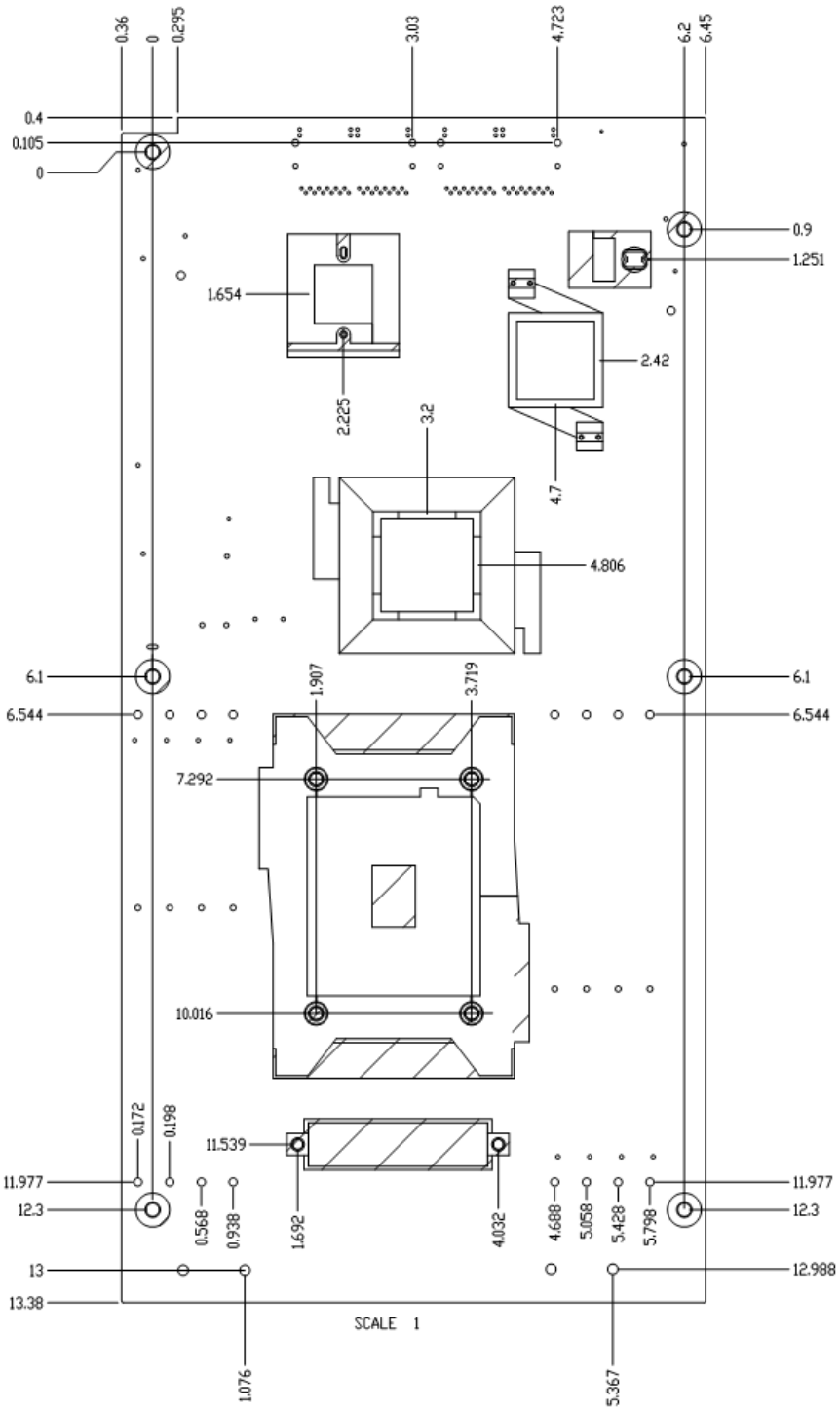


Figure 4. Baseboard and Mounting Holes

3. Product Architecture Overview

The Intel® Server Board S1600JP is a purpose build, rack-optimized server board used in a high-density rack system. It is designed around the integrated features and functions of the Intel® Xeon® processor E5-2600 or Intel® Xeon® processor E5-1600 product family, the Intel® C600-A chipset, and other supporting components including the Emulex* PILOT III Integrated BMC, the Intel® I350-AM4 Quad 1GbE network controller.

3.1 High Level Product Features

Table 2. Intel® Server Board S1600JP Features

Board	S1600JP
Form Factor	Half Width form-factor (13.8" x 6.8")
CPU Socket	Socket R, LGA2011
Chipset	Intel® C600 Chipset PCH – A SKU
Memory	▪ Support for 8 DDR-III LRDIMMs ▪ Support for 8 DDR-III RDIMMs ▪ Support for 8 DDR-III UDIMMs
Slots	▪ 2 PCIe GenIII x16 connector ▪ 1 PCIe GenIII x8 connector for rIOM
Ethernet	▪ Dual Intel® I350-AM4 GbE (S1600JP2) ▪ Quad Intel® I350-AM4 GbE(S1600JP4)
SATA	▪ 6 SATA ports from AHCI including 2x SATA 6Gb/s and 4x SATA 3Gb/s
SAS	One Mini SAS port
SW RAID	Intel® ESRT2 SAS/SATA RAID 0,1,5,10 or Intel® RSTe SATA RAID 0,1,5, and 10
Processor Support	▪ 135W maximum for Intel® Xeon® Processor E5-2600 product family ▪ 130W maximum for Intel® Xeon® Processor E5-1600 product family
Video	Integrated on Emulex* PILOT III BMC: ▪ Matrox G200 Core ▪ 16MByte of video memory assigned
SMS	Emulex* PILOT III BMC w/IPMI 2.0 support
Chassis	1U Rack Chassis
Power Supply	12V and 5VS/B PMBus*

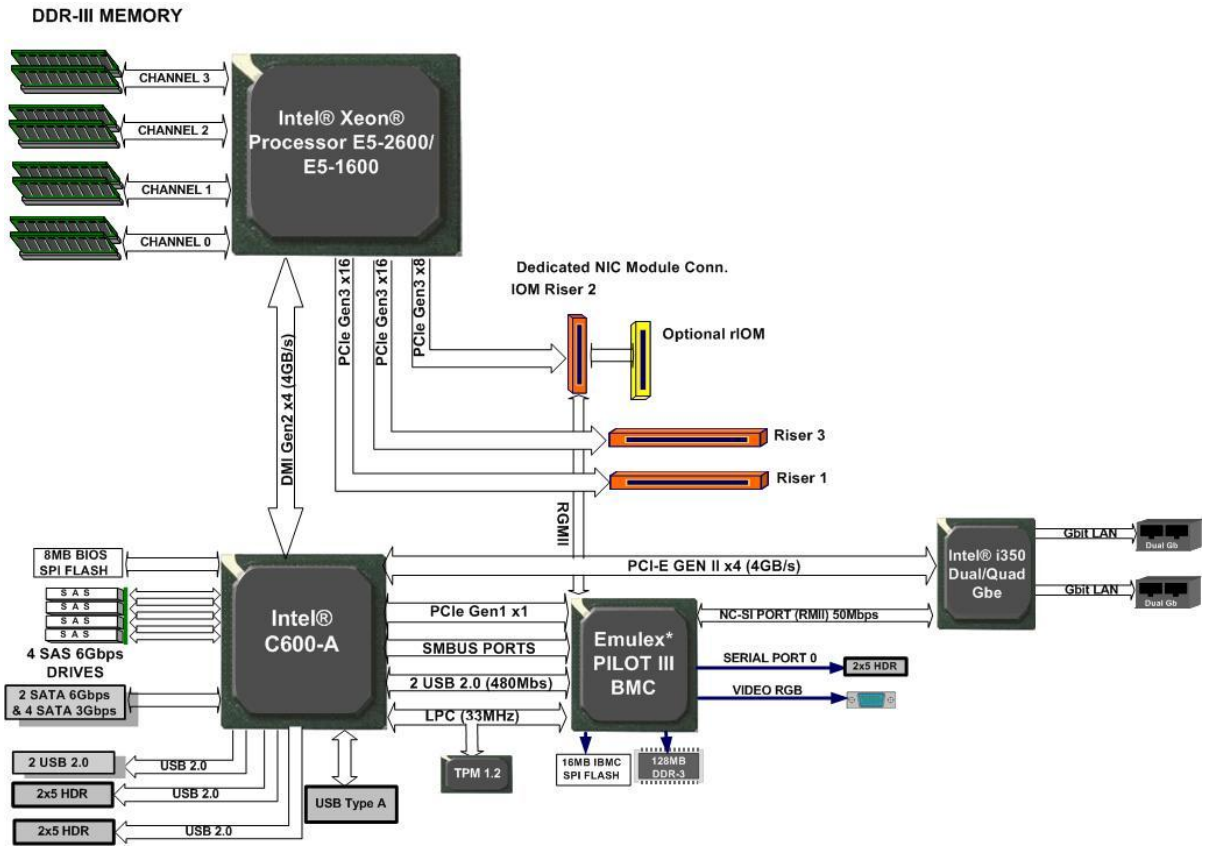


Figure 5. Intel® Server Board S1600JP Functional Block Diagram

3.2 Processor Support

The server board includes one Socket-R (LGA2011) processor socket and can support the Intel® Xeon® processor E5-2600 or Intel® Xeon® processor E5-1600 product family, with a Thermal Design Power (TDP) of up to 135W for Intel® Xeon® processor E5-2600 product family or up to 130W for Intel® Xeon® processor E5-1600 product family.

The Intel® Xeon™ E5-2600 processor family is composed of 6/8 cores respectively, and the Intel® Xeon™ E5-1600 processor family is composed of 4/6 cores respectively. The microprocessors include an integrated DDRIII memory controller (IMC) with four memory channels which can support up to three ECC Registered DIMMs or three Un-buffered ECC DIMMs per memory channel, an integrated I/O controller with 40 PCI Express* GenIII lanes controlled by ten PCI Express* Master Controllers.

Previous generation Intel® Xeon® processors are **NOT** supported on the Intel® server boards described in this document.

Visit the Intel® website for a complete list of supported processors.

3.2.1 Processor Socket Assembly

The processor socket of the server board is pre-assembled with an Independent Latching Mechanism (ILM) and Back Plate that allow for secure placement of the processor and processor heat to the server board.

The following illustration identifies each sub-assembly component:

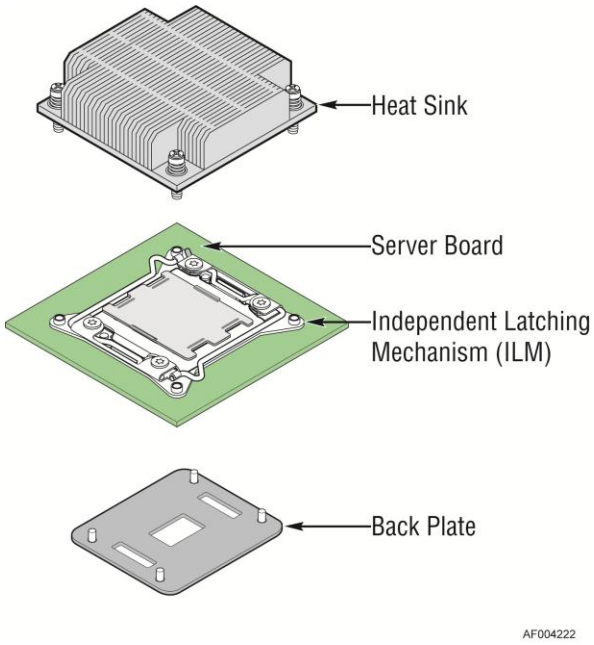


Figure 6. Processor Socket Assembly

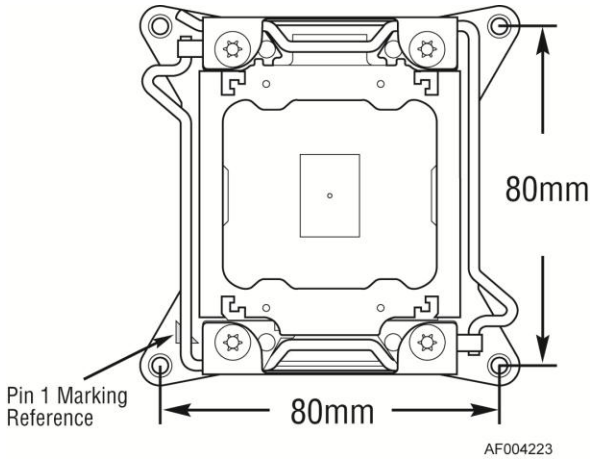


Figure 7. Processor Socket ILM Variations

The square ILM has an 80x80mm heatsink mounting hole pattern and is used on the Intel® Server Board S1600JP.

3.3 Processor Function Overview

With the release of Intel® Xeon® processor E5-2600 and Intel® Xeon® processor E5-1600 product family, several key system components, including the CPU, Integrated Memory Controller (IMC), and Integrated IO Module (IIO), have been combined into a single processor package and feature per socket; two Intel® QuickPath Interconnect point-to-point links capable of up to 8.0 GT/s, up to 40 lanes of GenIII PCI Express* links capable of 8.0 GT/s, and 4 lanes of DMI2/PCI Express* Gen 2 interface with a peak transfer rate of 5.0 GT/s. The processor supports up to 46 bits of physical address space and 48-bit of virtual address space.

The following sections will provide an overview of the key processor features and functions that help to define the performance and architecture of the server board. For more comprehensive processor specific information, refer to the Intel® Xeon® processor E5-2600 or Intel® Xeon® processor E5-1600 product family documents listed in the *Reference Document list* in the chapter Reference Documents.

Processor Feature Details:

- Up to eight execution cores for Intel® Xeon® processor E5-2600 product family or up to six execution cores for Intel® Xeon® processor E5-1600 product family
- Each core supports two threads (Intel® Hyper-Threading Technology), up to 16 threads per socket for Intel® Xeon® processor E5-2600 product family or up to 12 threads per socket for Intel® Xeon® processor E5-1600 product family
- 46-bit physical addressing and 48-bit virtual addressing
- 1 GB large page support for server applications
- A 32-KB instruction and 32-KB data first-level cache (L1) for each core
- A 256-KB shared instruction/data mid-level (L2) cache for each core
- Up to 20 MB last level cache (LLC): up to 2.5 MB per core instruction/data last level cache (LLC), shared among all cores

Supported Technologies:

- Intel® Virtualization Technology (Intel® VT)
- Intel® Virtualization Technology for Directed I/O (Intel® VT-d)
- Intel® Virtualization Technology Intel® Xeon® E5-2600 and Intel® Xeon® E5-1600 Processor Extensions
- Intel® Trusted Execution Technology (Intel® TXT)
- Intel® 64 Architecture
- Intel® Streaming SIMD Extensions 4.1 (Intel® SSE4.1)
- Intel® Streaming SIMD Extensions 4.2 (Intel® SSE4.2)
- Intel® Advanced Vector Extensions (Intel® AVX)
- Intel® Hyper-Threading Technology
- Execute Disable Bit
- Intel® Turbo Boost Technology
- Intel® Intelligent Power Technology
- Enhanced Intel® SpeedStep Technology

3.3.1 Integrated Memory Controller (IMC) and Memory Subsystem

- Unbuffered DDRIII and registered DDRIII DIMMs
- LR DIMM (Load Reduced DIMM) for buffered memory solutions demanding higher capacity memory subsystems
- Independent channel mode or lockstep mode
- Data burst length of eight cycles for all memory organization modes
- Memory DDRIII data transfer rates of 800, 1066, 1333, and 1600 MT/s
- 64-bit wide channels plus 8-bits of ECC support for each channel
- DDRIII standard I/O Voltage of 1.5V for all speed
- DDRIII Low Voltage of 1.35V for 1333MT/s or below
- 1-Gb, 2-Gb, and 4-Gb DDRIII DRAM technologies supported for these devices:
    - UDIMM DDRIII – SR x8 and x16 data widths, DR – x8 data width
    - RDIMM DDRIII – SR, DR, and QR – x4 and x8 data widths
    - LRDIMM DDRIII – QR – x4 and x8 data widths with direct map or with rank multiplication
- Up to 8 ranks supported per memory channel, 1, 2, or 4 ranks per DIMM
- Open with adaptive idle page close timer or closed page policy
- Per channel memory test and initialization engine can initialize DRAM to all logical zeros with valid ECC (with or without data scrambler) or a predefined test pattern
- Isochronous access support for Quality of Service (QoS)
- Minimum memory configuration: Independent channel support with one DIMM populated
- Integrated dual SMBus* master controllers
- Command launch modes of 1n/2n
- RAS Support:
    - Rank Level Sparing and Device Tagging
    - Demand and Patrol Scrubbing

- DRAM Single Device Data Correction (SDDC) for any single x4 or x8 DRAM device. Independent channel mode supports x4 SDDC. x8 SDDC requires lockstep mode
- Lockstep mode where channels 0 and 1 and channels 2 and 3 are operated in lockstep mode
- Data scrambling with address to ease detection of write errors to an incorrect address
- Error reporting through Machine Check Architecture
- Read Retry during CRC error handling checks by iMC
- Channel mirroring within a socket
- Error Containment Recovery
- Improved Thermal Throttling with dynamic Closed Loop Thermal Throttling (CLTT)

▪ Memory thermal monitoring support for DIMM temperature

3.3.1.1 Supported Memory

Table 3. Intel® Xeon® processor E5-2600 product family UDIMM Support Guidelines

Ranks Per DIMM and Data Width	Memory Capacity Per DIMM[1]			Speed (MT/s) and Voltage Validated by Slot Per Channel (SPC) and DIMM Per Channel (DPC)[2]			
				2 Slots Per Channel			
				1DPC		2DPC	
				1.35V	1.5V	1.35V	1.5V
SRx8 Non-ECC	1GB	2GB	4GB	n/a	1066, 1333	n/a	1066, 1333
DRx8 Non-ECC	2GB	4GB	8GB	n/a	1066, 1333	n/a	1066, 1333
SRx16 Non-ECC	512MB	1GB	2GB	n/a	1066, 1333	n/a	1066, 1333
SRx8 ECC	1GB	2GB	4GB	1066, 1333, 1600[3]	1066, 1333	1066	1066, 1333
DRx8 ECC	2GB	4GB	8GB	1066, 1333, 1600[3]	1066, 1333	1066	1066, 1333

Notes:

1. Supported DRAM Densities are 1Gb, 2Gb, and 4Gb. Only 2Gb and 4Gb are validated by Intel®.
2. Command Address Timing is 1N for 1DPC and 2N for 2DPC.
3. These speed options are only available when “Memory SPD Override” option in BIOS is enabled.

Table 4. Intel® Xeon® processor E5-2600 product family RDIMM Support Guidelines

Ranks Per DIMM and Data Width	Memory Capacity Per DIMM[1]			Speed (MT/s) and Voltage Validated by Slot Per Channel (SPC) and DIMM Per Channel (DPC)[2,3]			
				2 Slots Per Channel			
				1DPC		2DPC	
				1.35V	1.5V	1.35V	1.5V
SRx8	1GB	2GB	4GB	1066, 1333, 1600[4]	1066, 1333, 1600	1066, 1333, 1600[4]	1066, 1333, 1600
DRx8	2GB	4GB	8GB	1066, 1333 1600[4]	1066, 1333, 1600	1066, 1333, 1600[4]	1066, 1333, 1600
SRx4	2GB	4GB	8GB	1066, 1333 1600[4]	1066, 1333, 1600	1066, 1333, 1600[4]	1066, 1333, 1600
DRx4	4GB	8GB	16GB	1066, 1333 1600[4]	1066, 1333, 1600	1066, 1333, 1600[4]	1066, 1333, 1600
QRx4	8GB	16GB	32GB	800	1066	800	800
QRx8	4GB	8GB	16GB	800	1066	800	800

Notes:

1. Supported DRAM Densities are 1Gb, 2Gb, and 4Gb. Only 2Gb and 4Gb are validated by Intel®.
2. Command Address Timing is 1N.
3. QR RDIMM are supported but only validated by Intel® in a homogenous environment. The coverage will have limited system level testing, no signal integrity testing, and no interoperability testing. The passing QR RDIMMs will be web posted.
4. These speed options are only available when “Memory SPD Override” option in BIOS is enabled.

Table 5. Intel® Xeon® processor E5-2600 product family LRDIMM Support Guidelines

Ranks Per DIMM and Data Width[1]	Memory Capacity Per DIMM[2]		Speed (MT/s) and Voltage Validated by Slot Per Channel (SPC) and DIMM Per Channel (DPC)[3,4]	
			2 Slots Per Channel	
			1DPC and 2DPC	
			1.35V	1.5V
QRx4 (DDP)[5]	16GB	32GB	1066	1066, 1333

QRx8 (DDP)[5]	8GB	16GB	1066	1066, 1333

Notes:

1. Physical Rank is used to calculate DIMM Capacity.
2. Supported and validated DRAM densities are 2Gb and 4Gb.
3. Command Address Timing is 1N.
4. The speeds are estimated targets and will be verified through simulation.
5. DDP - Dual Die Package DRAM stacking. P – Planer monolithic DRAM Die.

Table 6 Intel® Xeon® processor E5-1600 product family UDIMM Support Guidelines

Ranks Per DIMM and Data Width	Memory Capacity Per DIMM[1]			Speed (MT/s) and Voltage Validated by Slot Per Channel (SPC) and DIMM Per Channel (DPC)[2]	
				2 Slots Per Channel (1.5V)	
				1DPC	2DPC
SRx8 Non-ECC	1GB	2GB	4GB	1066, 1333	1066, 1333
DRx8 Non-ECC	2GB	4GB	8GB	1066,1333	1066,1333
SRx16 Non-ECC	512MB	1GB	2GB	1066,1333	1066,1333
SRx8 ECC	1GB	2GB	4GB	1066, 1333	1066, 1333
DRx8 ECC	2GB	4GB	8GB	1066, 1333	1066, 1333

Notes:

1. Supported DRAM Densities are 1Gb, 2Gb, and 4Gb. Only 2Gb and 4Gb are validated by Intel®.
2. Command Address Timing is 1N for 1DPC and 2N for 2DPC.

Table 7. Intel® Xeon® processor E5-1600 product family RDIMM Support Guidelines

Ranks Per DIMM and Data Width	Memory Capacity Per DIMM[1]	Speed (MT/s) and Voltage Validated by Slot Per Channel (SPC) and DIMM Per Channel (DPC)[2, 3]	
		2 Slots Per Channel (1.5V)	
		1DPC	2DPC

Ranks Per DIMM and Data Width	Memory Capacity Per DIMM[1]			Speed (MT/s) and Voltage Validated by Slot Per Channel (SPC) and DIMM Per Channel (DPC)[2, 3]	
				2 Slots Per Channel (1.5V)	
				1DPC	2DPC
SRx8	1GB	2GB	4GB	1066, 1333, 1600	1066, 1333, 1600
DRx8	2GB	4GB	8GB	1066, 1333, 1600	1066, 1333, 1600
SRx4	2GB	4GB	8GB	1066, 1333, 1600	1066, 1333, 1600
DRx4	4GB	8GB	16GB	1066, 1333, 1600	1066, 1333, 1600
QRx4	8GB	16GB	32GB	1066	800
QRx8	4GB	8GB	16GB	1066	800

Notes:

1. Supported DRAM densities are 1Gb, 2Gb, and 4Gb. Only 2Gb and 4Gb are validated by Intel®.
2. Command Address Timing is 1N.
3. QR RDIMM are supported but only validated by Intel® in a homogenous environment. The coverage will have limited system level testing, no signal integrity testing, and no interoperability testing. The passing QR RDIMMs will be web posted.

3.3.1.2 Memory population rules

Note: All memory on Intel® Server Board S1600JP is expected to match in all respects, including the memory vendor. S1600JP does not support any mix of memory parts, whether or not a mixed configuration may be able to operate successfully in a particular instance.

The processor provides four banks of memory, each capable of supporting up to 4 DIMMs.

- DIMMs are organized into physical slots on DDRIII memory channels that belong to processor sockets.
- The memory channels from the processor socket are identified as Channel A, B, C, and D. The silk screened DIMM slot identifiers on the board provide information about the channel. For example, DIMM_A1 is the first slot on Channel A; DIMM_A2 is the second DIMM socket on Channel A.

On the Intel® Server Board S1600JP, a total of eight DIMM slots is provided. The nomenclature for DIMM sockets is detailed in the following table:

Table 8. Intel® Server Board S1600JP DIMM Nomenclature

Processor Socket			
(0) Channel A	(1) Channel B	(2) Channel C	(3) Channel D
A1	B1	C1	D1
A2	B2	C2	D2

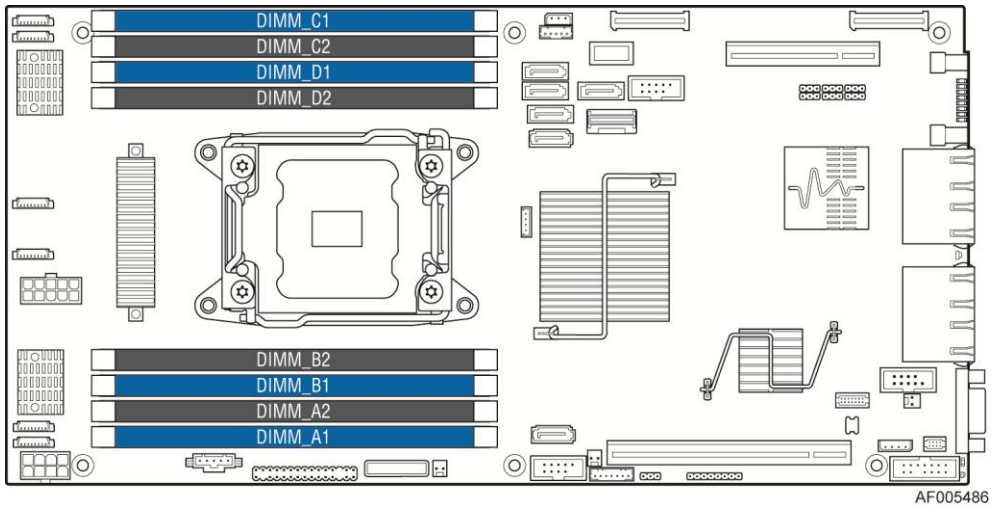


Figure 8. Intel® Server Board S1600JP DIMM Slot Layout

The following are generic DIMM population requirements that generally apply to the Intel® Server Board S1600JP:

- All DIMMs must be DDRIII DIMMs.
- Unbuffered DIMMs can be ECC.
- Mixing of Registered and Unbuffered DIMMs is not allowed per platform.
- Mixing of LRDIMM with any other DIMM type is not allowed per platform.
- Mixing of DDRIII voltages is not validated within a socket or across sockets by Intel®. If 1.35V (DDRIIIL) and 1.50V (DDRIII) DIMMs are mixed, the DIMMs will run at 1.50V.
- Mixing of DDRIII operating frequencies is not validated within a socket or across sockets by Intel®. If DIMMs with different frequencies are mixed, all DIMMs will run at the common lowest frequency.
- Quad rank RDIMMs are supported but not validated by Intel®.
- A maximum of 8 logical ranks (ranks seen by the host) per channel is allowed.
- Mixing of ECC and non-ECC DIMMs is not allowed per platform.

3.3.1.3 Publishing System Memory

- The BIOS displays the “Total Memory” of the system during POST if Display Logo is disabled in the BIOS setup. This is the total size of memory discovered by the BIOS during POST, and is the sum of the individual sizes of installed DDRIII DIMMs in the system.

- The BIOS displays the “Effective Memory” of the system in the BIOS setup. The term *Effective Memory* refers to the total size of all DDRIII DIMMs that are active (not disabled) and not used as redundant units.
- The BIOS provides the total memory of the system in the main page of the BIOS setup. This total is the same as the amount described by the first bullet above.
- If Display Logo is disabled, the BIOS displays the total system memory on the diagnostic screen at the end of POST. This total is the same as the amount described by the first bullet above.

3.3.1.4 RAS Features

The server board supports the following memory RAS modes:

- Independent Channel Mode
- Rank Sparing Mode
- Mirrored Channel Mode
- Lockstep Channel Mode

Note that support of RAS modes that require matching DIMM population between channels (Mirrored and Lockstep) require that ECC DIMMs be populated.

For RAS modes that require matching populations, the same slot positions across channels must hold the same DIMM type with regards to size and organization. DIMM timings do not have to match but timings will be set to support all the DIMMs populated (that is, DIMMs with slower timings will force faster DIMMs to the slower common timing modes).

3.3.1.4.1 Independent Channel Mode

Channels can be populated in any order in Independent Channel Mode. All four channels may be populated in any order and have no matching requirements. All channels must run at the same interface frequency but individual channels may run at different DIMM timings (RAS latency, CAS latency, and so forth).

3.3.1.4.2 Rank Sparing Mode

In Rank Sparing Mode, one rank is a spare of the other ranks on the same channel. The spare rank is held in reserve and is not available as system memory. The spare rank must have identical or larger memory capacity than all the other ranks (sparing source ranks) on the same channel. After sparing, the sparing source rank will be lost.

3.3.1.4.3 Mirrored Channel Mode

In Mirrored Channel Mode, the memory contents are mirrored between Channel 0 and Channel 2 and also between Channel 1 and Channel 3. As a result of the mirroring, the total physical memory available to the system is half of what is populated. Mirrored Channel Mode requires that Channel 0 and Channel 2, and Channel 1 and Channel 3 must be populated identically with regards to size and organization. DIMM slot populations within a channel do not have to be identical, but the same DIMM slot location across Channel 0 and Channel 2 and across Channel 1 and Channel 3 must be populated the same.

3.3.1.4.4 Lockstep Channel Mode

In Lockstep Channel Mode, each memory access is a 128-bit data access that spans Channel 0 and Channel 1, and Channel 2 and Channel 3. Lockstep Channel mode is the only RAS mode

that allows SDDC for x8 devices. Lockstep Channel Mode requires that Channel 0 and Channel 1, and Channel 2 and Channel 3 must be populated identically with regards to size and organization. DIMM slot populations within a channel do not have to be identical, but the same DIMM slot location across Channel 0 and Channel 1 and across Channel 2 and Channel 3 must be populated the same.

3.3.2 Processor Intergrated I/O Module (I/O)

The processor's integrated I/O module provides features traditionally supported through chipset components. The integrated I/O module provides the following features:

- **PCI Express* Interfaces:** The integrated I/O module incorporates the PCI Express* interface and supports up to 40 lanes of PCI Express*. Following are key attributes of the PCI Express* interface:
  - GenIII speeds at 8 GT/s (no 8b/10b encoding)
  - X16 interface bifurcated down to two x8 or four x4 (or combinations)
  - X8 interface bifurcated down to two x4
- **DMI2 Interface to the PCH:** The platform requires an interface to the legacy Southbridge (PCH) which provides basic, legacy functions required for the server platform and operating systems. Since only one PCH is required and allowed for the system, any sockets which do not connect to PCH would use this port as a standard x4 PCI Express* 2.0 interface.
- **Integrated IOAPIC:** Provides support for PCI Express* devices implementing legacy interrupt messages without interrupt sharing.
- **Non Transparent Bridge:** PCI Express* Non-Transparent Bridge (NTB**) acts as a gateway** that enables high performance, low overhead communication between two intelligent subsystems; the local and the remote subsystems. The NTB allows a local processor to independently configure and control the local subsystem, provides isolation of the local host memory domain from the remote host memory domain while enabling status and data exchange between the two domains.

3.3.2.1 Riser Types

There are 3 PCIe riser slots on the server board, and they are customized on pin definition.

The riser slot 1 is a standard 164-pin x 16 connector but it is not compatible with standard PCIe pinout. It has a x16 PCIe GenIII electrical interface. It can be configured as a single x16, dual x8, or dual x4 plus single x8 (with different risers) if required.

The riser slot 2 is a standard 98-pin x8 connector but it is also not compatible with standard PCIe pinout. The riser slot 2 supports rIOM mounted on a riser carrier.

The riser slot 3 include two 60-pin connectors that can host a riser with a single PCIe GenIII x16 (electrical/mechanical) slot for a double width PCI Express* card or dual PCIe GenIII x8 (electrical/mechanical) slots for general purpose boards.

Each riser slot support will have the power budget as shown in the following table:

Table 9. Power budget for riser slot

Riser Slot#	12V Capability	3.3V Capability

Riser Slot 1	2A	6A
Riser Slot 2	1A	3A
Riser Slot 3	5.5A	6A

Supported 1U riser cards include:

- 1U low profile Riser slot 1 with one PCIe slot – It provides electrical connectivity for a PCIe x16 GenIII low profile adapter card. It supports a PCIe GenIII X16 card edge connection and a x16/x16 mech PCIe connector. The X16 PCIe card edge connection are not compatible with the standard PCIe pinout but the x16 PCIe connector is compatible. Product Code: F1UJP1X16RISER.

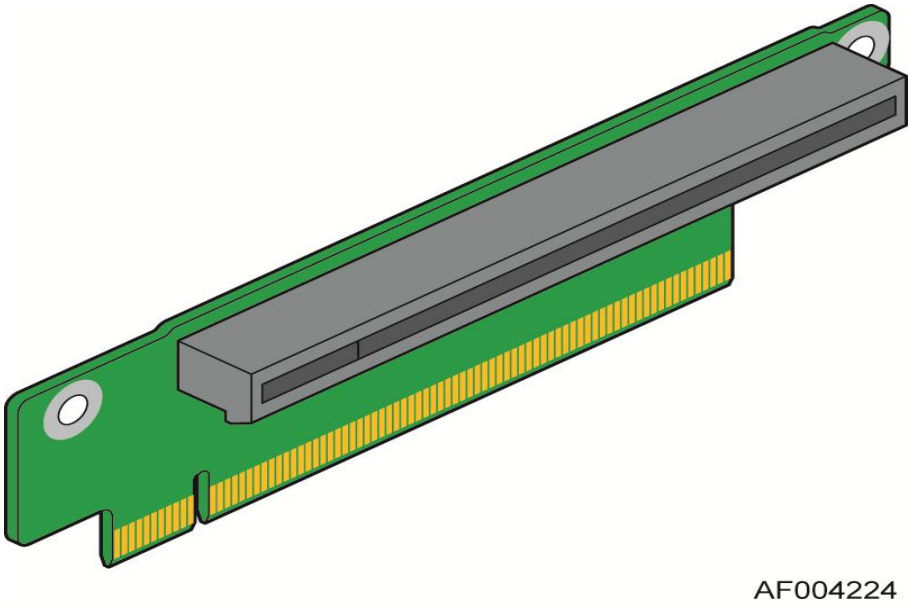


Figure 9. PCIe Riser for Slot 1

- 1U Riser for Slot 2 with one PCIe slot – It supports PCIe GenIII x8 connection to the IOM module and a RGMII interface across to the IOM Carrier Board. The x8 PCIe card edge connection and x8 PCIe connector do not follow the standard PCIe pinout. Product Code: A1UJPRMM4IOM.

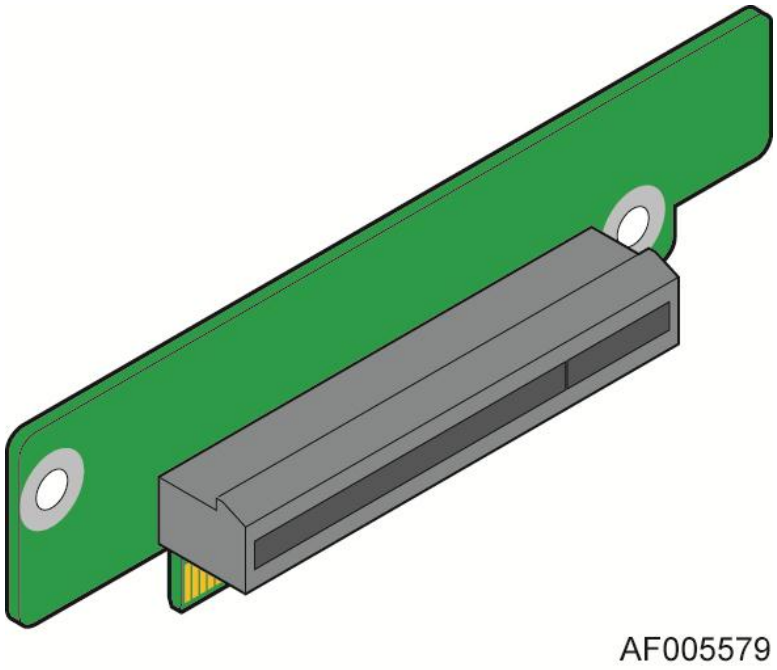


Figure 10. PCIe Riser for Slot 2

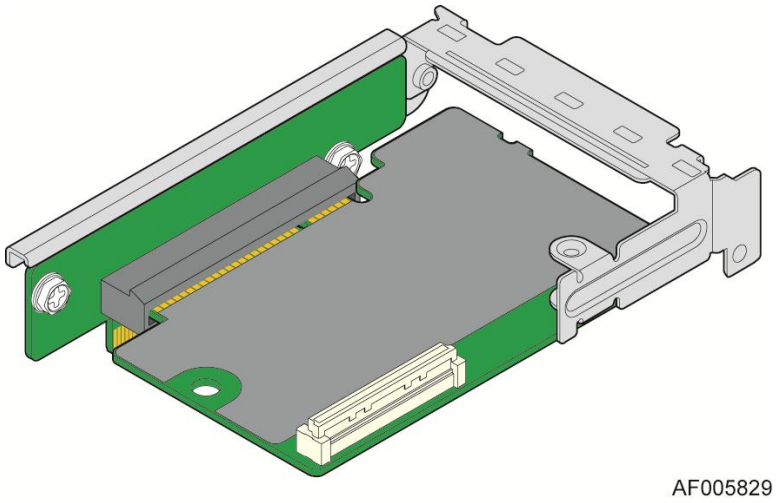


Figure 11. Riser Carrier Board

- 1U PCIe double width PCI Express* card Riser for slot 3 with one PCIe slot - It provides electrical connectivity for a PCIe x16 GenIII double width PCI Express* card. It supports a PCIe GenIII 2X60pin card edge connection and a x16/x16 mech PCIe connector. The 2X60 pin PCIe card edge connection are not compatible with the standard PCIe pinout but the x16 PCIe connector is compatible. Product Code: F1UJPMICRISER.

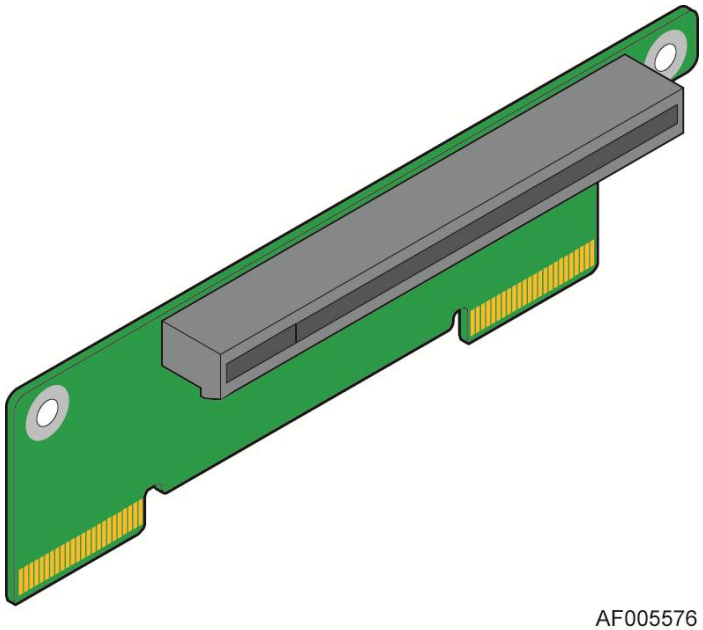


Figure 12. 1U PCIe Double Width PCI Express* Card Riser for Slot3

- 1U PCIe FHFL Riser for slot 3 with two PCIe slots - It provides electrical connectivity for two standard PCIe x8 GenIII FHFL PCIE card. It supports x2 60 pin PCIE card edge and one GenIII x8/x16 mech PCIE connector and one GenIII x8/x8 mech PCIE connector. The 2x60 pin PCIe card connection are not compatible with the standard PCIe pinout, but the two PCIe connectors are compatible. Product Code: F1UJP2X8RISER.

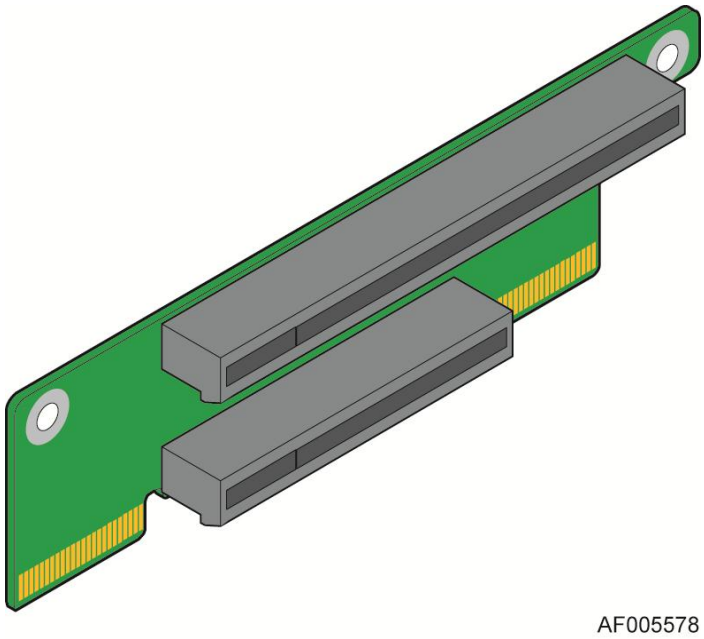


Figure 13. 1U PCIe FHFL Riser for Slot3

3.3.2.2 Network Interface

The on-board Intel® i350 Ethernet controller provides four/two 10/100/1000Gbps Ethernet ports in four/two RJ45 ports in S1600JP4/S1600JP2.

3.3.2.3 I/O Module Support

To broaden the standard on-board feature set, the server board supports the option of adding a single I/O module providing external ports for a variety of networking interfaces. The I/O module attaches to a high density 80-pin connector of I/O module carrier on the Riser 2.

3.4 Intel® C600-A PCH Functional Overview

The following sub-sections will provide an overview of the key features and functions of the Intel® C600-A chipset used on the server board. For more comprehensive chipset specific information, refer to the *Intel® C600-A Series chipset documents* through: http://www.intel.com/content/www/us/en/chipsets/server-chipsets/server-workstation-chipsets.html.

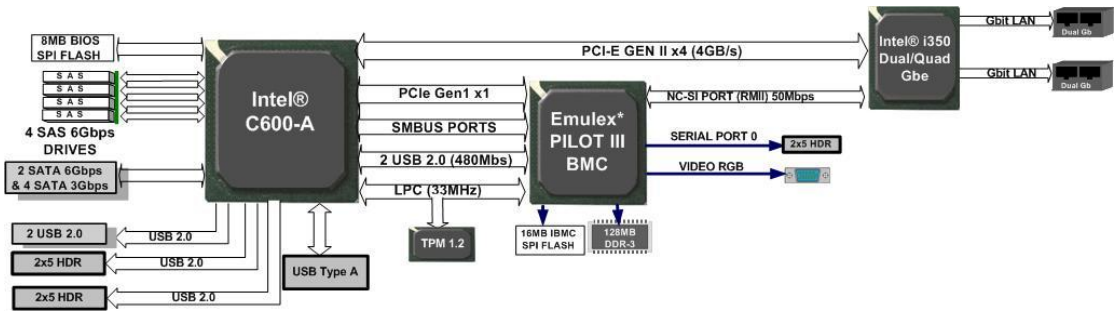


Figure 14. Intel® C600-A PCH connection

The Intel® C600-A PCH component provides extensive I/O support. Functions and capabilities include:

- *PCI Express* Base Specification, Revision 2.0* support for up to eight ports with transfers up to 5 GT/s.
- *PCI Local Bus Specification, Revision 2.3* support for 33 MHz PCI operations (supports up to four Req/Gnt pairs).
- *ACPI Power Management Logic Support, Revision 4.0a*
- Enhanced DMA controller, interrupt controller, and timer functions
- Integrated Serial Attached SCSI host controllers at transfer rate up to 6Gb/s on up to eight ports.
- Integrated Serial ATA host controllers with independent DMA operation on up to six ports.
- USB host interface with two EHCI high-speed USB 2.0 Host controllers and 2 rate matching hubs provide support for support for up to fourteen USB 2.0 ports
- Integrated 10/100/1000 Gigabit Ethernet MAC with System Defense
- *System Management Bus (SMBus*) Specification, Version 2.0* with additional support for I^2C* devices
- Supports Intel® High Definition Audio
- Supports Intel® Rapid Storage Technology (Intel® RST)

- Supports Intel® Virtualization Technology for Directed I/O (Intel® VT-d)
- Supports Intel® Trusted Execution Technology (Intel® TXT)
- Low Pin Count (LPC) interface
- Firmware Hub (FWH) interface support
- Serial Peripheral Interface (SPI) support
- Intel® Anti-Theft Technology (Intel® AT)
- JTAG Boundary Scan support

3.4.1 PCI Express*

The Intel® C600 PCH provides up to 8 PCI Express* Root Ports, supporting the *PCI Express* Base Specification, Revision 2.0*. Each Root Port x1 lane supports up to 5 Gb/s bandwidth in each direction (10 Gb/s concurrent). PCI Express* Root Ports 1-4 or Ports 5-8 can independently be configured to support four x1s, two x2s, one x2 and two x1s, or one x4 port widths.

From PCH on Intel® Server Board S1600JP, PCIe Port8 x1 GenII is connected to BMC Gen1 Uplink. Ports 1-4 are connected to Intel® I350 GbE NIC. The remaining PCIe GenII interconnect (Port 5-7, 1 based numbering) are unused.

3.4.2 Universal Serial Bus (USB)

There are fourteen USB 2.0 ports available from Intel® C600 PCH. All ports are high-speed, full-speed, and low-speed capable. A total of 7 USB 2.0 dedicated ports are used by Intel® Server Board S1600JP. The USB port distribution is as follows:

- Emulex* BMC PILOT III consumes two USB 2.0 ports (one USB1.1 and one USB2.0)
- Two rear USB 2.0 ports
- Two internal USB port for extension of front-panel USB port.
- One Type-A USB port

Note: Intel® Server Board S1600JP supports 3 high power USB ports (1 at rear port, 1 at internal USB port1 and 1 at internal USB port2) + 4 low power USB ports at the same time.

3.4.3 Serial Attached SCSI (SAS) and Serial ATA (SATA) Controller

The Intel® C600-A chipset provides storage support through two integrated controllers: AHCI and SCU. By default, the server board supports up to six SATA ports: Two single 6Gb/sec SATA ports and four 3Gb/s SATA ports. The board supports up to four 3Gb/s SATA/SAS ports from the mini-SAS port.

It supports the *Serial ATA Specification, Revision 3.0*, and several optional sections of the *Serial ATA II: Extensions to Serial ATA 1.0 Specification, Revision 1.0* (AHCI support is required for some elements).

Intel® Server Board S1600JP implements six SATA/SAS ports. The implementation is as follows:

Table 10. Intel® Server Board S1600JP SATA/SAS port

Port#		Speed	Connector
0		6Gb/s SATA	On Server board
1		6Gb/s SATA	On Server board
2		3Gb/s SATA	On Server board
3		3Gb/s SATA	On Server board
4		3Gb/s SATA	On Server board
5		3Gb/s SATA	On Server board
SCU0	0	3Gb/s SATA/SAS	On board mini SAS
	1		
	2		
	3		

There are two embedded software RAID options using the storage ports configured from the SCU only:

- Intel® Embedded Server RAID Technology 2 (ESRT2) based on LSI* MegaRAID SW RAID technology supporting SATA RAID levels 0,1,10, 5.
- Intel® Rapid Storage Technology (RSTe) supporting SATA RAID levels 0,1,5,10.

The server board is capable of supporting additional chipset embedded SAS and RAID options from the SCU controller when configured with one of the several available Intel® RAID C600 Storage Upgrade Keys. Upgrade keys install onto a 4-pin connector on the server board labeled "SAS/SATA Key".

The following table identifies available upgrade key options and their supported features:

Table 11. Intel® RAID C600 Storage Upgrade Key Options for S1600JP

Intel® RAID C600 Upgrade Key Options (Intel® Product Codes)	Key Color	Description
Default – No option key installed	**N/A**	4 Port SATA with Intel® ESRT RAID 0,1,10 and Intel® RSTe RAID 0,1,5,10
RKSATA4R5	**Black**	4 Port SATA with Intel® ESRT2 RAID 0,1, 5, 10, and Intel® RSTe RAID 0,1,5,10
RKSAS4	**Green**	4 Port SAS with Intel® ESRT2 RAID 0,1,10 and Intel® RSTe RAID 0,1,10
RKSAS4R5	**Yellow**	4 Port SAS with Intel® ESRT2 RAID 0,1, 5, 10 and Intel® RSTe RAID 0,1,10

3.4.4 PCI Interface

The Intel® C600 PCH PCI Interface provides a 33 MHz, Revision 2.3 implementation. It integrates a PCI arbiter that supports up to four external PCI bus masters in addition to the PCH internal requests. This allows for combinations of up to four PCI down devices and PCI slots.

3.4.5 Low Pin Count (LPC) Interface

The Intel® C600 PCH implements an LPC Interface as described in the *LPC 1.1 Specification*. The Low Pin Count (LPC) bridge function of the PCH resides in PCI Device 31: Function 0. In addition to the LPC bridge interface function, D31:F0 contains other functional units including DMA, interrupt controllers, timers, power management, system management, GPIO, and RTC.

3.4.6 Digital Media Interface (DMI)

Digital Media Interface (DMI) is the chip-to-chip connection between the processor and Intel® C600 PCH. This high-speed interface integrates advanced priority-based servicing allowing for concurrent traffic and true isochronous transfer capabilities. Base functionality is completely software-transparent, permitting current and legacy software to operate normally.

3.4.7 Serials Peripheral Interface (SPI)

The Intel® C600 PCH implements an SPI Interface as an alternative interface for the BIOS flash device. An SPI flash device can be used as a replacement for the FWH, and is required to support Gigabit Ethernet and Intel® Active Management Technology. The PCH supports up to two SPI flash devices with speeds up to 50 MHz, utilizing two chip select pins.

3.4.8 Compatibility Modules (DMA Controller, Timer/Counters, Interrupt Controller)

The DMA controller incorporates the logic of two 8237 DMA controllers, with seven independently programmable channels. Channels 0–3 are hardwired to 8-bit, count-by-byte transfers, and channels 5–7 are hardwired to 16-bit, count-by-word transfers. Any two of the seven DMA channels can be programmed to support fast Type-F transfers. Channel 4 is reserved as a generic bus master request.

The Intel® C600 PCH supports LPC DMA, which is similar to ISA DMA, through the PCH's DMA controller. LPC DMA is handled through the use of the LDRQ# lines from peripherals and special encoding on LAD[3:0] from the host. Single, Demand, Verify, and Increment modes are supported on the LPC interface.

The timer/counter block contains three counters that are equivalent in function to those found in one 8254 programmable interval timer. These three counters are combined to provide the system timer function, and speaker tone. The 14.31818 MHz oscillator input provides the clock source for these three counters.

The Intel® C600 PCH provides an ISA-Compatible Programmable Interrupt Controller (PIC) that incorporates the functionality of two, 8259 interrupt controllers. The two interrupt controllers are cascaded so that 14 external and two internal interrupts are possible. In addition, the PCH supports a serial interrupt scheme. All of the registers in these modules can be read and restored. This is required to save and restore system state after power has been removed and restored to the platform.

3.4.9 Advanced Programmable Interrupt Controller (APIC)

In addition to the standard ISA compatible Programmable Interrupt Controller (PIC) described in the previous section, the Intel® C600 PCH incorporates the Advanced Programmable Interrupt Controller (APIC).

3.4.10 Real Time Clock (RTC)

The Intel® C600 PCH contains a Motorola MC146818B-compatible real-time clock with 256 bytes of battery-backed RAM. The real-time clock performs two key functions: keeping track of the time of day and storing system data, even when the system is powered down. The RTC operates on a 32.768 KHz crystal and a 3V battery. The RTC also supports two lockable memory ranges. By setting bits in the configuration space, two 8-byte ranges can be locked to read and write accesses. This prevents unauthorized reading of passwords or other system security information. The RTC also supports a date alarm that allows for scheduling a wake up event up to 30 days in advance, rather than just 24 hours in advance.

3.4.11 GPIO

Various general purpose inputs and outputs are provided for custom system design. The number of inputs and outputs varies depending on the Intel® C600 PCH configuration.

3.4.12 Enhanced Power Management

The Intel® C600 PCH power management functions include enhanced clock control and various low-power (suspend) states. A hardware-based thermal management circuit permits software-independent entrance to low-power states. The PCH contains full support for the *Advanced Configuration and Power Interface (ACPI) Specification, Revision 4.0a*.

3.4.13 Fan Speed Control

The Intel® C600 PCH integrates four fan speed sensors (four TACH signals) and four fan speed controllers (three Pulse Width Modulator signals), which enables monitoring and controlling up to four fans on the system. With the new implementation of the single-wire Simple Serial Transport (SST) 1.0 bus and Platform Environmental Control Interface (PECI), the PCH provides an easy way to connect to SST-based thermal sensors and access the processor thermal data.

3.4.14 Intel® Virtualization Technology for Direct I/O (Intel® VT-d)

The Intel® Virtualization Technology is designed to support multiple software environments sharing same hardware resources. Each software environment may consist of an OS and applications. The Intel® Virtualization Technology can be enabled or disabled in the BIOS setup. The default behavior is disabled.

Note: If the setup options are changed to enable or disable the Virtualization Technology setting in the processor, the user must perform an AC power cycle for the changes to take effect.

The chipset supports DMA remapping from inbound PCI Express* memory Guest Physical Address (GPA) to Host Physical Address (HPA). PCI devices are directly assigned to a virtual machine leading to a robust and efficient virtualization.

3.4.15 KVM/Serial Over LAN (SOL) Function

These functions support redirection of keyboard, mouse, and text screen to a terminal window on a remote console. The keyboard, mouse, and text redirection enables the control of the client machine through the network without the need to be physically near that machine. Text, mouse, and keyboard redirection allows the remote machine to control and configure the client by entering BIOS setup. The KVM/SOL function emulates a standard PCI serial port and redirects the data from the serial port to the management console using LAN. KVM has additional requirements of internal graphics and SOL may be used when KVM is not supported.

3.4.16 IDE-R Function

The IDE-R function is an IDE Redirection interface that provides client connection to management console ATA/ATAPI devices. When booting from IDE-R, the IDE-R interface will send the client's ATA/ATAPI command to the management console. The management console will then provide a response command back to the client. A remote machine can setup a diagnostic SW or OS installation image and direct the client to boot from IDE-R. The IDE-R interface is the same as the IDE interface and is compliant with ATA/ATAPI-6 specifications. IDE-R does not conflict with the usage of PXE boot. The system can support both interfaces and continue to boot from the PXE as with any other boot devices. However, during management boot session the Intel® AMT solution will use IDE-R when remote boot is required. The devices attached to the IDER channel are only visible to software during management boot session. During normal boot session the IDE-R channel does not appear as a present device.

3.4.17 Manageability

Intel® C600 PCH integrates several functions designed to manage the system and lower the Total Cost of Ownership (TCO) of the system. These system management functions are designed to report errors, diagnose the system, and recover from system lockups without the aid of an external microcontroller. The functionality provided by the SPS firmware is different from Intel® Active Management Technology (Intel® AMT or AT) provided by the ME on client platforms.

- **TCO Timer:** The Intel® C600 PCH's integrated programmable TCO timer is used to detect system locks. The first expiration of the timer generates an SMI# that the system can use to recover from a software lock. The second expiration of the timer causes a system reset to recover from a hardware lock.
- **Processor Present Indicator:** The Intel® C600 PCH looks for the processor to fetch the first instruction after reset. If the processor does not fetch the first instruction, the PCH will reboot the system.
- **ECC Error Reporting:** When detecting an ECC error, the host controller has the ability to send one of several messages to the Intel® C600 PCH. The host controller can instruct the PCH to generate any of SMI#, NMI, SERR#, or TCO interrupt.
- **Function Disable**: The Intel® C600 PCH provides the ability to disable the following integrated functions: LAN, USB, LPC, Intel® HD Audio, SATA, PCI Express*, or SMBus*. Once disabled, these functions no longer decode I/O, memory, or PCI configuration space. Also, no interrupts or power management events are generated from the disabled functions.
- **Intruder Detect:** The Intel® C600 PCH provides an input signal (INTRUDER#) that can be attached to a switch that is activated by the system case being opened. The Intel®

C600 PCH can be programmed to generate either SMI# or TCO interrupt due to an active INTRUDER# signal.

3.4.18 System Management Bus (SMBus* 2.0)

The Intel® C600 PCH contains a SMBus* Host interface that allows the processor to communicate with SMBus* slaves. This interface is compatible with most I^2C devices. Special I^2C commands are implemented.

The Intel® C600 PCH's SMBus* host controller provides a mechanism for the processor to initiate communications with SMBus* peripherals (slaves). Also, the PCH supports slave functionality, including the Host Notify protocol. Hence, the host controller supports eight command protocols of the SMBus* interface (see *System Management Bus (SMBus*) Specification, Version 2.0*): Quick Command, Send Byte, Receive Byte, Write Byte/Word, Read Byte/Word, Process Call, Block Read/Write, and Host Notify.

The Intel® C600 PCH's SMBus* also implements hardware-based Packet Error Checking for data robustness and the Address Resolution Protocol (ARP) to dynamically provide address to all SMBus* devices.

3.4.19 Network Interface Controller (NIC)

Network interface support is provided from the onboard Intel® I350 NIC, which is a dual-port, compact component with two fully integrated GbE Media Access Control (MAC) and Physical Layer (PHY) ports. The Intel® I350 NIC provides the server board with support for dual LAN ports designed for 10/100/1000 Mbps operation. Refer to the *Intel® I350 Gigabit Ethernet Controller Datasheet* for full details of the NIC feature set.

The NIC device provides a standard IEEE 802.3 Ethernet interface for 1000BASE-T, 100BASE-TX, and 10BASE-T applications (802.3, 802.3u, and 802.3ab) and is capable of transmitting and receiving data at rates of 1000 Mbps, 100 Mbps, or 10 Mbps.

The Intel® I350 controller also requires the use of Intel® C600 PCH SMBus* interface during Sleep states S4 and S5 as well as for ME Firmware. The Intel® I350 LAN controller will be on standby power so that Wake on LAN and manageability functions can be supported.

Intel® I350 will be used in conjunction with the Emulex* PILOT III BMC for in band Management traffic. The BMC will communicate with Intel® I350 over a NC-SI interface (RMII physical). The NIC will be on standby power so that the BMC can send management traffic over the NC-SI interface to the network during sleep states S4 and S5.

The NIC supports the normal RJ-45 LINK/Activity speed LEDs as well as the Proset ID function. These LEDs are powered from a Standby voltage rail.

S1600JP4 has Quad NIC ports. S1600JP2 has Dual NIC ports.

The link/activity LED (at the right of the connector) indicates network connection when on, and transmit/receive activity when blinking. The speed LED (at the left of the connector) indicates 1000-Mbps operation when green, 100-Mbps operation when amber, and 10-Mbps when off. The following table provides an overview of the LEDs.

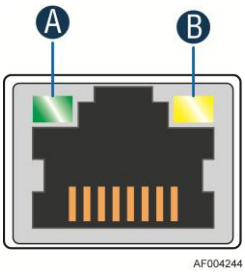


Figure 15. 1GbE NIC port LED

Table 12. NIC Status LED

LED Color	LED State	NIC State
Green/Amber (B)	Off	10 Mbps
	Amber	100 Mbps
	Green	1000 Mbps
Green (A)	On	Active Connection
	Blinking	Transmit/Receive activity

3.4.19.1 MAC Address Definition

The Intel® Server Board S1600JP2 has the following four MAC addresses assigned to it at the Intel® factory.

- NIC 1 MAC address
- NIC 2 MAC address = NIC 1 MAC address + 1
- Integrated BMC LAN channel 1 MAC address = NIC1 MAC address + 2
- Integrated BMC LAN channel 2 MAC address = NIC1 MAC address + 3
- Integrated BMC LAN channel 3 (RMM) MAC address = NIC1 MAC address + 4

The Intel® Server Board S1600JP4 has the following four MAC addresses assigned to it at the Intel® factory.

- NIC 1 MAC address
- NIC 2 MAC address = NIC 1 MAC address + 1
- NIC 3 MAC address = NIC 1 MAC address + 2
- NIC 4 MAC address = NIC 1 MAC address + 3
- Integrated BMC LAN channel 1 MAC address = NIC1 MAC address + 4
- Integrated BMC LAN channel 2 MAC address = NIC1 MAC address + 5
- Integrated BMC LAN channel 3 (RMM) MAC address = NIC1 MAC address + 6

The Intel® Server Board S1600JP has a white MAC address sticker included with the board. The sticker displays the NIC 1 MAC address in both barcode and alphanumeric formats.

3.4.19.2 LAN Manageability

Port2 of the Intel® I350 NIC will be used by the BMC firmware to send management traffic. In standby in order to save power, Port2 will be the only port to support Wake on LAN. The

EEPROM is programmed to turn off this feature from the other ports in order to maximize power savings during sleep states.

3.4.19.3 Wake-On-LAN

WOL is supported on the Intel® I350 LAN controller for all supported Sleep states.

3.4.19.4 Intel® i350 Thermal Sensor

Intel® i350 NIC will have an integrated digital thermal sensor accessible through CSR and manageability registers. The thermal sensor can be programmed to trigger digital pins and thermal throttling with hysteresis.

3.5 Integrated Baseboard Management Controller Overview

The server board utilizes the Baseboard Management features of the Emulex* Pilot III Server Management Controller. The following is an overview of the features as implemented on the server board from each embedded controller.

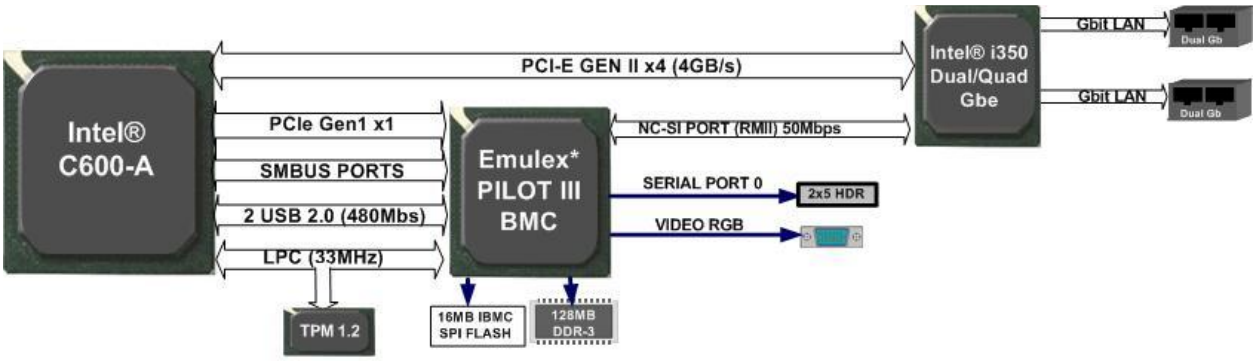


Figure 16. Integrated BMC implementation overview (S1600JP2)

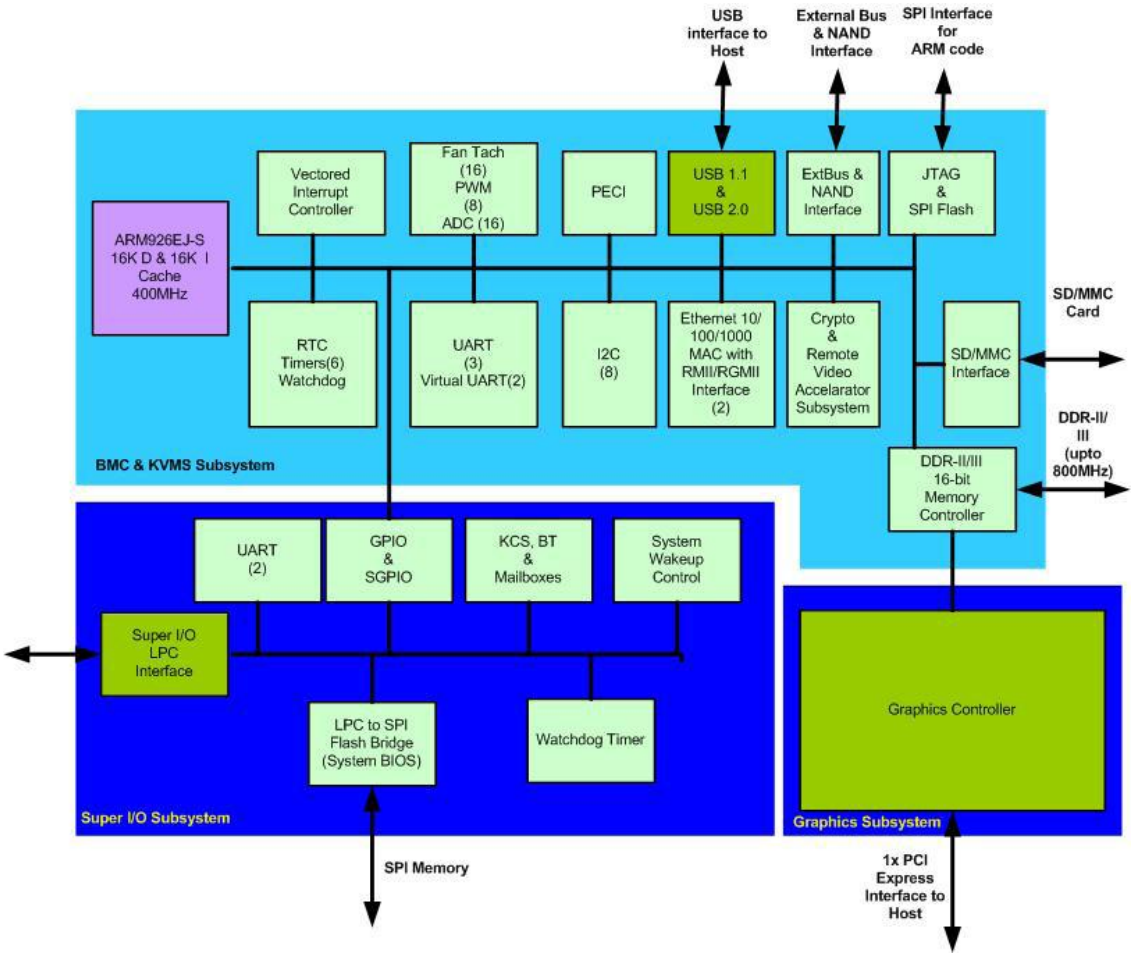


Figure 17. Integrated BMC Functional Block Diagram

The Integrated BMC is provided by an embedded ARM9 controller and associated peripheral functionality that is required for IPMI-based server management. Firmware usage of these hardware features is platform dependent.

The following is a summary of the Integrated BMC management hardware features that comprise the BMC:

- 400MHz 32-bit ARM9 processor with memory management unit (MMU)
- Two independent 10/100/1000 Ethernet Controllers with RMII/RGMII support
- DDRII/III 16-bit interface with up to 800 MHz operation
- 12 10-bit ADCs
- 16 fan tachometers
- Eight Pulse Width Modulators (PWM)
- Chassis intrusion logic
- JTAG Master
- Eight I^2C interfaces with master-slave and SMBus* timeout support. All interfaces are SMBus* 2.0 compliant
- Parallel general-purpose I/O Ports (16 direct, 32 shared)

- Serial general-purpose I/O Ports (80 in and 80 out)
- Three UARTs
- Platform Environmental Control Interface (PECI)
- Six general-purpose timers
- Interrupt controller
- Multiple SPI flash interfaces
- NAND/Memory interface
- Sixteen mailbox registers for communication between the BMC and host
- LPC ROM interface
- BMC watchdog timer capability
- SD/MMC card controller with DMA support
- LED support with programmable blink rate controls on GPIOs
- Port 80h snooping capability
- Secondary Service Processor (SSP), which provides the HW capability of offloading time critical processing tasks from the main ARM core

Emulex* Pilot III contains an integrated SIO, KVMS subsystem, and graphics controller with the following features:

3.5.1 Super I/O Controller

The integrated super I/O controller provides support for the following features as implemented on the server board:

- Keyboard Style/BT interface for BMC support
- Two Fully Functional Serial Ports, compatible with the 16C550
- Serial IRQ Support
- Up to 16 Shared GPIO available for host processor
- Programmable Wake-up Event Support
- Plug and Play Register Set
- Power Supply Control

3.5.1.1 Keyboard and Mouse Support

The server board does not support PS/2 interface keyboards and mice. However, the system BIOS recognizes USB specification-compliant keyboards and mice.

3.5.1.2 Wake-up Control

The super I/O contains functionality that allows various events to power on and power off the system.

3.5.2 Graphics Controller and Video Support

The integrated graphics controller provides support for the following features as implemented on the server board:

- Integrated Graphics Core with 2D Hardware accelerator

- DDR-II/III memory interface supports up to 256MB of memory
- Supports all display resolutions up to 1600 x 1200 16bpp @ 60Hz
- High speed Integrated 24-bit RAMDAC

The integrated video controller supports all standard IBM VGA modes. The following table shows the 2D modes supported for both CRT and LCD:

Table 13. Video Modes

2D Mode	Refresh Rate (Hz)	2D Video Mode Support		
		8 bpp	16 bpp	32 bpp
640x480	60, 72, 75, 85, 90, 100, 120, 160, 200	Supported	Supported	Supported
800x600	60, 70, 72, 75, 85, 90, 100, 120,160	Supported	Supported	Supported
1024x768	60, 70, 72, 75,85,90,100	Supported	Supported	Supported
1152x864	43,47,60,70,75,80,85	Supported	Supported	Supported
1280x1024	60,70,74,75	Supported	Supported	Supported
1600x1200**	60	Supported	Supported	Supported

** Video resolutions at 1600x1200 are only supported through the external video connector located on the rear I/O section of the server board. Utilizing the optional front panel video connector may result in lower video resolutions.

The server board provides two video interfaces. The primary video interface is accessed using a standard 15-pin VGA connector found on the back edge of the server board. In addition, video signals are routed to a 14-pin header labeled “FP_Video” on the leading edge of the server board, allowing for the option of cabling to a front panel video connector. Attaching a monitor to the front panel video connector will disable the primary external video connector on the back edge of the board.

The BIOS supports dual-video mode when an add-in video card is installed.

- In the single mode (dual monitor video = disabled), the on-board video controller is disabled when an add-in video card is detected.

In the dual mode (on-board video = enabled, dual monitor video = enabled), the on-board video controller is enabled and is the primary video device. The add-in video card is allocated resources and is considered the secondary video device. The BIOS Setup utility provides options to configure the feature as follows:

Table 14. Video mode

On-board Video	**Enabled** Disabled	
Dual Monitor Video	**Enabled** Disabled	Shaded if on-board video is set to "Disabled"

3.5.3 Remote KVM

The Integrated BMC contains a remote KVMS subsystem with the following features:

- USB 2.0 interface for Keyboard, Mouse, and Remote storage such as CD/DVD ROM and floppy
- USB 1.1/USB 2.0 interface for PS2 to USB bridging, remote Keyboard and Mouse
- Hardware Based Video Compression and Redirection Logic
- Supports both text and Graphics redirection
- Hardware assisted Video redirection using the Frame Processing Engine
- Direct interface to the Integrated Graphics Controller registers and Frame buffer
- Hardware-based encryption engine

4. Platform Management Functional Overview

Platform management functionality is supported by several hardware and software components integrated on the server board that work together to control system functions, monitor and report system health, and control various thermal and performance features in order to maintain (when possible) server functionality in the event of component failure and/or environmentally stressed conditions.

This chapter provides a high level overview of the platform management features and functionality implemented on the server board. For more in depth and design level Platform Management information, refer the *BMC Core Firmware External Product Specification (EPS)* (Intel® Order Number: G31813) and *BIOS Core External Product Specification (EPS*) for Intel® Server products based on the Intel® Xeon® processor E5-4600, 2600, and 1600 product families.

4.1 Baseboard Management Controller (BMC) Firmware Feature Support

The following sections outline general features that the integrated BMC firmware can support. Support and utilization for some features is dependent on the server platform in which the server board is integrated and any additional system level components and options that may be installed.

4.1.1 IPMI 2.0 Features

- Baseboard Management Controller (BMC)
- IPMI Watchdog timer
- Messaging support, including command bridging and user/session support
- Chassis device functionality, including power/reset control and BIOS boot flags support
- Event receiver device: The BMC receives and processes events from other platform subsystems
- Field Replaceable Unit (FRU) inventory device functionality: The BMC supports access to system FRU devices using IPMI FRU commands
- System Event Log (SEL) device functionality: The BMC supports and provides access to a SEL
- Sensor Data Record (SDR) repository device functionality: The BMC supports storage and access of system SDRs
- Sensor device and sensor scanning/monitoring: The BMC provides IPMI management of sensors. It polls sensors to monitor and report system health
- IPMI interfaces
    - Host interfaces include system management software (SMS) with receive message queue support, and server management mode (SMM)
    - IPMB interfaces
    - LAN interface that supports the IPMI-over-LAN protocol (RMCP, RMCP+)
- Serial-over-LAN (SOL)
- ACPI state synchronization: The BMC tracks ACPI state changes that are provided by the BIOS

- BMC self-test: The BMC performs initialization and run-time self-tests and makes results available to external entities

See also the *Intelligent Platform Management Interface Specification Second Generation v2.0.*

4.1.2 Non IPMI Features

The BMC supports the following non-IPMI features. This list does not preclude support for future enhancements or additions.

- In-circuit BMC firmware update
- BMC FW reliability enhancements:
  - Redundant BMC boot blocks to avoid possibility of a corrupted boot block resulting in a scenario that prevents a user from updating the BMC
  - BMC System Management Health Monitoring
  - Signed firmware images for increased security
- Fault resilient booting (FRB): FRB2 is supported by the watchdog timer functionality
- Enable/Disable of System Reset Due CPU Errors
- Chassis intrusion detection
- Fan speed control
- Fan redundancy monitoring and support
- Hot-swap fan support
- Power Supply Fan Sensors
- System Airflow Monitoring
- Exit Air Temperature Monitoring
- Acoustic management: Support for multiple fan profiles
- Ethernet Controller Thermal Monitoring
- Global Aggregate Temperature Margin Sensor
- Platform environment control interface (PECI) thermal management support
- Memory Thermal Management
- DIMM temperature monitoring: New sensors and improved acoustic management using closed-loop fan control algorithm taking into account DIMM temperature readings
- Power supply redundancy monitoring and support
- Power unit management: Support for power unit sensor. The BMC handles power-good dropout conditions
- Intel® Intelligent Power Node Manager support
- Signal testing support: The BMC provides test commands for setting and getting platform signal states
- The BMC generates diagnostic beep codes for fault conditions
- System GUID storage and retrieval
- Front panel management: The BMC controls the system status LED and chassis ID LED. It supports secure lockout of certain front panel functionality and monitors button presses. The chassis ID LED is turned on using a front panel button or a command
- Power state retention

- Power fault analysis
- Intel® Light-Guided Diagnostics
- Address Resolution Protocol (ARP): The BMC sends and responds to ARPs (supported on embedded NICs)
- Dynamic Host Configuration Protocol (DHCP): The BMC performs DHCP (supported on embedded NICs)
- E-mail alerting
- Embedded web server
  - Support for embedded web server UI in Basic Manageability feature set
  - Human-readable SEL
  - Additional system configurability
  - Additional system monitoring capability
  - Enhanced on-line help
- Integrated KVM
- Integrated Remote Media Redirection
- Local Directory Access Protocol (LDAP) support
- Sensor and SEL logging additions/enhancements (for example, additional thermal monitoring capability)
- SEL Severity Tracking and the Extended SEL
- BMC Data Repository (Managed Data Region Feature)
- Embedded platform debug feature which allows capture of detailed data for later analysis
- Provisioning and inventory enhancements:
  - Signed Firmware (improved security)
  - Inventory data/system information export (partial SMBIOS table)
- DCMI 1.1 compliance
- Management support for PMBus* rev1.2 compliant power supplies
- Energy Star Server Support
- SmaRT/CLST
- Power Supply Cold Redundancy
- Power Supply FW Update for supported Intel® supplies
- Power Supply Compatibility Check

4.1.3 New Manageability Features

The new generation EPSD server products offer a number of changes and additions to the manageability features that are supported on the previous generation of servers. The following is a list of the more significant changes that are common to all EPSD servers of this new generation:

- Sensor and SEL logging additions/enhancements (for example, additional thermal monitoring capability)
- SEL Severity Tracking and the Extended SEL
- Embedded platform debug feature which allows capture of detailed data for later analysis

- Provisioning and inventory enhancements:
  - Signed Firmware (improved security)
  - Inventory data/system information export (partial SMBIOS table)
- Enhancements to fan speed control
- DCMI 1.1 compliance
- Support for embedded web server UI in *Basic Manageability* feature set
- Enhancements to embedded web server
  - Human-readable SEL
  - Additional system configurability
  - Additional system monitoring capability
  - Enhanced on-line help
- Enhancements to KVM redirection
  - Support resolution up to 1600x1200
- Management support for PMBus* rev1.2 compliant power supplies
- BMC Data Repository (Managed Data Region Feature)
- System Airflow Monitoring
- Exit Air Temperature Monitoring
- Ethernet Controller Thermal Monitoring
- Global Aggregate Temperature Margin Sensor
- Memory Thermal Management
- Power Supply Fan Sensors
- Enable/Disable of System Reset Due CPU Errors
- Energy Star Server Support
- SmaRT/CLST
- Power Supply Cold Redundancy
- Power Supply FW Update
- Power Supply Compatibility Check
- BMC FW reliability enhancements:
  - Redundant BMC boot blocks to avoid possibility of a corrupted boot block resulting in a scenario that prevents a user from updating the BMC
  - BMC System Management Health Monitoring

4.2 Advanced Configuration and Power Interface (ACPI)

The server board has support for the following ACPI states:

Table 15. ACPI Power States

State	Supported	Description
S0	Yes	Working. ▪ The front panel power LED is on (not controlled by the BMC). ▪ The fans spin at the normal speed, as determined by sensor inputs. ▪ Front panel buttons work normally.

State	Supported	Description
S1	Yes	**Sleeping.** Hardware context is maintained; equates to processor and chipset clocks being stopped. ▪ The front panel power LED blinks at a rate of 1 Hz with a 50% duty cycle (not controlled by the BMC). ▪ The watchdog timer is stopped. ▪ The power, reset, front panel NMI, and ID buttons are unprotected. ▪ Fan speed control is determined by available SDRs. Fans may be set to a fixed state, or basic fan management can be applied. The BMC detects that the system has exited the ACPI S1 sleep state when the BIOS SMI handler notifies it.
S2	No	Not supported.
S3	No	Supported only on Workstation platforms. See appropriate platform specific information for more information.
S4	No	Not supported.
S5	Yes	Soft off. ▪ The front panel buttons are not locked. ▪ The fans are stopped. ▪ The power-up process goes through the normal boot process. ▪ The power, reset, front panel NMI, and ID buttons are unlocked.

4.3 Platform Management SMBus* and I²C Implementation

SMBus*/ I²C interconnections are a fundamental interface for various manageability components. There are three buses that are used in a multi-master fashion.

- **Primary IPMB**. An IPMB header is provided on the baseboard to support connectivity with third-party management PCIe cards. This bus operates as 100 kHz bus.
- **Secondary IPMB**. This is the SMLink0 bus that connects the BMC with the ME in the SSB. This bus is considered a secondary IPMB. The ME and BMC communicate over this bus using IPMB protocol messages. Any devices on the bus must be 400 kHz bus tolerant.
- **PMBus***. This is the SMLink1 bus that both the ME and BMC use to communicate with the power supplies. This bus operates as 100 kHz bus.

For all multi-master buses, the master that initiates a transaction is responsible for any bus recovery sequence if the bus hangs.

The BMC acts as master for the other buses connected to it.

4.4 BMC Internal Timestamp Clock

The BMC maintains an internal timestamp clock that is used by various BMC subsystems, for example, for time stamping SEL entries. As part of BMC initialization after AC power is applied or the BMC is reset, the BMC initializes this internal clock to the value retrieved from the SSB component's RTC through a SMBus* slave read operation. This is the system RTC and is on the battery power well so it maintains the current time even when there is no AC supplied to the system.

The BMC reads the RTC using the same SMBus* (the "host SMBus*") that is used by BIOS during POST, so the BMC FW must not attempt to access the RTC between the time the

system is reset or powered-on and POST completes, as indicated by the assertion of the POST-complete signal. Additionally, the BMC should cancel any pending reads of the RTC if the POST-complete signal deasserts (for example, due to a reset). Normally the BMC reads the RTC when AC power is first applied and before the system is powered-on, so this is not a concern. However, if AC power is applied and the power button is immediately pressed, it is possible that POST would be in progress by the time the BMC is ready to read the RTC. Another potential conflict can occur if the BMC gets reset and POST is in progress when the BMC has re-initialized. For either of these cases, the BMC FW initializes its internal time clock to 0 and begins counting up from there. When POST completes, BIOS will then update the BMC's time clock to the current system time.

The BMC's internal timestamp clock is read and set using the *Get SEL Time* and *Set SEL Time* commands, respectively. The *Get SDR Time* command can also be used to read the timestamp clock. These commands and the IPMI time format are specified in the *IPMI 2.0 specification*. Whenever the BMC receives the *Set SEL Time* command, it updates only its internal time clock. Note that an update of this internal time clock does not result in a change to the system RTC.

4.5 Sensor Monitoring

The BMC monitors system hardware and reports system health. The information gathered from physical sensors is translated into IPMI sensors as part of the "IPMI Sensor Model". The BMC also reports various system state changes by maintaining virtual sensors that are not specifically tied to physical hardware.

4.6 Messaging Interfaces

The supported BMC communication interfaces include:

- Host SMS interface by means of low pin count (LPC)/keyboard controller style (KCS) interface
- Host SMM interface by means of low pin count (LPC)/keyboard controller style (KCS) interface
- Intelligent Platform Management Bus (IPMB) I^2C interface
- LAN interface using the IPMI-over-LAN protocols

4.6.1 Channel Management

Every messaging interface is assigned an IPMI channel ID by IPMI 2.0. Commands are provided to configure each channel for privilege levels and access modes. The following table shows the standard channel assignments:

Table 16. Standard Channel Assignments

Channel ID	Interface	Supports Sessions
0	Primary IPMB	No
1	LAN 1	Yes
2	LAN 2	Yes
3	LAN3 [1] (Provided by the Intel® Dedicated Server Management NIC)	Yes

Channel ID	Interface	Supports Sessions
4	Reserved	Yes
5	USB	No
6	Secondary IPMB	No
7	SMM	No
8 – 0Dh	Reserved	–
0Eh	Self [2]	–
0Fh	SMS/Receive Message Queue	No

Notes:
1. Optional hardware supported by the server system.
2. Refers to the actual channel used to send the request.

4.6.2 User Model

The BMC supports the IPMI 2.0 user model including *User ID 1* support. 15 user IDs are supported. These 15 users can be assigned to any channel. The following restrictions are placed on user-related operations:

1. User names for User IDs 1 and 2 cannot be changed. These are always " " (Null/blank) and "root" respectively.
    a) A "*CCh*" error completion code is returned if a user attempts to modify these names.
2. User 2 ("root") always has the administrator privilege level.
    b) A "*CCh*" error completion code is returned if a user attempts to modify this value.
    c) Trying to set any parameter for User ID 2 (root user) with the Set User Access command fails with a CCh completion code.
3. All user passwords (including passwords for 1 and 2) may be modified.
4. User IDs 3-15 may be used freely, with the condition that user names are unique. Therefore, no other users can be named "" (Null), "root," or any other existing user name.

Resetting a user name to a value equivalent to its current value, results in a 0xCC error code. A list of default user values is given in the following table.

Table 17. Default User Values

Users	User name	Password	Status	Default Privilege	Characteristics
User 1	[Null]	[Null]	Disabled	Admin	Password can be changed. This user may not be used to access the embedded web server.

Users	User name	Password	Status	Default Privilege	Characteristics
User 2	root	superuser	Disabled	Admin	Password can be changed.
User 3	test1	superuser	Disabled	Admin	User name and password can be changed.
User 4	test2	superuser	Disabled	Admin	User name and password can be changed.
User 5	test3	superuser	Disabled	Admin	User name and password can be changed.
User 6-15	undefined	undefined	Disabled	Admin	User name and password can be changed.

4.6.3 Sessions

The maximum number of IPMI-based sessions that can be supported by the BMC is returned as the byte 3 (number of possible active sessions) of the IPMI Command *Get Session Info* (App, 3Dh). Embedded Web Server and Media Redirection are not IPMI-based sessions. KVM is a type of payload in a RMCP+ Session.

Table 18. Channel/Media-specific minimum number of sessions

Channels/Media type	Session Type	Minimum Number of Sessions
LAN Channel1, Intel® Dedicated Server Management NIC [4]	IPMI Over LAN [1]	4 [6, 7]
HTTP [5]	Embedded Web Server [3]	2 [8, 9]
--- [5]	Media Redirection [6]	2 [8]
--- [1]	KVM [2]	2 [10]

Notes:

1. Session type defined by the IPMI Spec and includes RMCP and RMCP+ sessions (including all the payloads supported).
2. KVM is a RMCP+ **Payload Type**. Not an IPMI session.
3. These sessions are not defined by *IPMI Specification* and are not based on IPMI protocol. Counting them as IPMI Session violates the Specification.
4. If Intel® Dedicated Server Management NIC is not present, the minimum number of sessions still holds but only over LAN Channel 1.
5. It is not an IPMI Channel.
6. Maximum of 15 IPMI sessions are allowed per channel that is defined.
7. IPMI-based session and counted as an IPMI Session in all calculations.
8. These sessions are not counted as IPMI sessions. (For example, *Get Session Info* only returns values based on IPMI Sessions).
9. This type of Non-IPMI session can open IPMI sessions as part of a normal operation and those IPMI sessions are counted as IPMI sessions. For example, within a Web Session, one or more IPMI Over LAN

Session are opened to GetandSet IPMI parameters. But since these IPMI sessions are not over LAN1 or Intel® Dedicated Server Management NIC, they are not counted as LAN1 or Intel® Dedicated Server Management NIC IPMI channel sessions but are counted as IPMI sessions in limit calculations.

10. It is an IPMI Over LAN RMCP+ session and is included in counts as part of the larger IPMI Over LAN group.

Note: The number of possible active session values returned by *Get Session Info* is the total number of allocated memory session slots in BMC firmware for IPMI Sessions. The actual number of IPMI sessions that can be established at any time is dependent on Channel and User IPMI configuration parameters and in compliance with the IPMI Specification, which is always less than the total available slots.

4.6.4 BMC LAN Channels

The BMC supports three RMII/RGMII ports that can be used for communicating with Ethernet devices. Two ports are used for communication with the on-board NICs and one is used for communication with an Ethernet PHY located on an optional add-in card (or equivalent on-board circuitry).

4.6.4.1 Baseboard NICs

The specific Ethernet controller (NIC) used on a server is platform-specific but all baseboard device options provide support for an NC-SI manageability interface. This provides a sideband high-speed connection for manageability traffic to the BMC while still allowing for a simultaneous host access to the OS if desired.

The Network Controller Sideband Interface (NC-SI) is a DMTF industry standard protocol for the side band management LAN interface. This protocol provides a fast multi-drop interface for management traffic.

The baseboard NIC(s) are connected to a single BMC RMII/RGMII port that is configured for RMII operation. The NC-SI protocol is used for this connection and provides a 100 Mb/s full-duplex multi-drop interface which allows multiple NICs to be connected to the BMC. The physical layer is based upon RMII, however RMII is a point-to-point bus whereas NC-SI allows one master and up to four slaves. The logical layer (configuration commands) is incompatible with RMII.

Multi-port baseboard NICs on some products will provide support for a dedicated management channel that can be configured to be hidden from the host and only used by the BMC. This mode of operation is configured through a BIOS setup option.

4.6.4.2 Dedicated Management Channel

An additional LAN channel dedicated to BMC usage and not available to host SW is supported through an optional add-in card. There is only a PHY device present on the add-in card. The BMC has a built-in MAC module that uses the RGMII interface to link with the card's PHY. Therefore, for this dedicated management interface, the PHY and MAC are located in different devices.

The PHY on the card connects to the BMC's other RMII/RGMII interface (that is, the one that is not connected to the baseboard NICs). This BMC port is configured for RGMII usage.

In addition to the use of an add-in card for a dedicated management channel, on systems that support multiple Ethernet ports on the baseboard, the system BIOS provides a setup option to

allow one of these baseboard ports to be dedicated to the BMC for manageability purposes. When this is enabled, that port is hidden from the OS.

4.6.4.3 Concurrent Server Management Use of Multiple Ethernet Controllers

Provided the HW supports a management link between the BMC and a NIC port, the BMC FW supports concurrent OOB LAN management sessions for the following combination:

- Two on-board NIC ports
- One on-board NIC and the optional dedicated add-in management NIC
- Two on-board NICs and optional dedicated add-in management NIC

All NIC ports must be on different subnets for the above concurrent usage models.

MAC addresses are assigned for management NICs from a pool of up to 3 MAC addresses allocated specifically for manageability. The total number of MAC addresses in the pool is dependent on the product HW constraints (for example, a board with 2 NIC ports available for manageability would have a MAC allocation pool of 2 addresses).

For these channels, support can be enabled for IPMI-over-LAN and DHCP.

For security reasons, embedded LAN channels have the following default settings:

- IP Address: Static
- All users disabled

Network failover mode must be used for IPMI capable interfaces that are on the same subnet.

Host-BMC communication over the same physical LAN connection – also known as “loopback” – is not supported. This includes “ping” operations.

On baseboards with more than two onboard NIC ports, only the first two ports can be used as BMC LAN channels. The remaining ports have no BMC connectivity.

Maximum bandwidth supported by BMC LAN channels are as follows:

BMC LAN 1 (Baseboard NIC port)	100M (10M in DC off state)
BMC LAN 2 (Baseboard NIC port)	100M (10M in DC off state)
BMC LAN 3 (Dedicated NIC)	1000M

4.6.5 IPv6 Support

In addition to IPv4, the Intel® Server Board S1600JP supports IPv6 for manageability channels. Configuration of IPv6 is provided by extensions to the *IPMI Set and Get LAN Configuration Parameters* commands as well as through a Web Console IPv6 configuration web page.

The BMC supports IPv4 and IPv6 simultaneously so they are both configured separately and completely independently. For example, IPv4 can be DHCP configured while IPv6 is statically configured or vice versa. The parameters for IPv6 are similar to the parameters for IPv4 with the following differences:

- An IPv6 address is 16 bytes versus 4 bytes for IPv4.

- An IPv6 prefix is 0 to 128 bits whereas IPv4 has a 4 byte subnet mask.
- The IPv6 Enable parameter must be set before any IPv6 packets will be sent or received on that channel.
- There are two variants of automatic IP Address Source configuration versus just DHCP for IPv4.

The three possible IPv6 IP Address Sources for configuring the BMC are:

- **Static (Manual)**: The IP, Prefix, and Gateway parameters are manually configured by the user. The BMC ignores any Router Advertisement messages received over the network.

- **DHCPv6**: The IP comes from running a DHCPv6 client on the BMC and receiving the IP from a DHCPv6 server somewhere on the network. The Prefix and Gateway are configured by Router Advertisements from the local router. The IP, Prefix, and Gateway are read-only parameters to the BMC user in this mode.

- **Stateless auto-config**: The Prefix and Gateway are configured by the router through Router Advertisements. The BMC derives its IP in two parts: the upper network portion comes from the router and the lower unique portion comes from the BMC's channel MAC address. The 6-byte MAC address is converted into an 8-byte value per the EUI-64* standard. For example, a MAC value of 00:15:17:FE:2F:62 converts into a EUI-64 value of 215:17ff:fefe:2f62. If the BMC receives a Router Advertisement from a router at IP 1:2:3:4::1 with a prefix of 64, it would then generate for itself an IP of 1:2:3:4:215:17ff:fefe:2f62. The IP, Prefix, and Gateway are read-only parameters to the BMC user in this mode.

- IPv6 can be used with the BMC's Web Console, JViewer (remote KVM and Media), and Systems Management Architecture for Server Hardware – Command Line Protocol (SMASH-CLP) interface (ssh). There is no standard yet on how IPMI RMCP or RMCP+ should operate over IPv6 so that is not currently supported.

4.6.5.1 LAN Failover

The BMC FW provides a LAN failover capability such that the failure of the system HW associated with one LAN link will result in traffic being rerouted to an alternate link. This functionality is configurable through IPMI methods as well as through the BMC's Embedded UI, allowing for user to specify the physical LAN links constitute the redundant network paths or physical LAN links constitute different network paths. BMC will support "only-all-or-nothing" approach – that is, all interfaces bonded together, or none are bonded together.

The LAN Failover feature applies only to BMC LAN traffic. It bonds all available Ethernet devices but only one is active at a time. When enabled, if the active connection's leash is lost, one of the secondary connections is automatically configured so that it has the same IP address. Traffic immediately resumes on the new active connection.

The LAN Failover enable/disable command may be sent at any time. After it has been enabled, standard IPMI commands for setting channel configuration that specify a LAN channel other than the first will return an error code.

4.7 System Event Log (SEL)

The BMC implements the system event log as specified in the *Intelligent Platform Management Interface Specification, Version 2.0.* The SEL is accessible regardless of the system power state through the BMC's in-band and out-of-band interfaces.

The BMC allocates 65,502 bytes (approx. 64 KB) of non-volatile storage space to store system events. The SEL timestamps may not be in order. Up to 3,639 SEL records can be stored at a time. Any command that results in an overflow of the SEL beyond the allocated space is rejected with an “Out of Space” IPMI completion code (C4h).

4.7.1 Servicing Events

Events can be received while the SEL is being cleared. The BMC implements an event message queue to avoid the loss of messages. Up to three messages can be queued before messages are overwritten.

The BMC recognizes duplicate event messages by comparing sequence numbers and the message source. For details, see the *Intelligent Platform Management Interface Specification Second Generation v2.0*. Duplicate event messages are discarded (filtered) by the BMC after they are read from the event message queue. The queue can contain duplicate messages.

4.7.2 SEL Entry Deletion

The BMC does not support individual SEL entry deletion. The SEL may only be cleared as a whole.

4.7.3 SEL Erasure

SEL erasure is a background process. After initiating erasure with the *Clear SEL* command, additional *Clear SEL* commands must be executed to get the erasure status and determine when the SEL erasure is completed. This may take several seconds. SEL events that arrive during the erasure process are queued until the erasure is complete and then committed to the SEL.

SEL erasure generates an *Event Logging Disabled* (*Log Area Reset/Cleared* offset) sensor event.

4.7.4 SEL Extension Capabilities

The BMC provides an OEM extension to all SEL entries. Each entry includes an additional 8 bytes for storing extra event data that will not fit into the original 3 data bytes provided by standard IPMI SEL entries. The first extension byte is always valid for all SEL entries and specifies the severity of the SEL event as well as the number of valid extension bytes following the first one. That leaves up to 7 SEL extension data bytes that can be defined for each SEL event entry.

All standard IPMI SEL commands work the same as if there were no SEL extensions.

In order to store and access the extended SEL information, 5 OEM commands are implemented that closely follow the standard IPMI SEL commands but provide support for the SEL Extension data. These OEM commands are specified in the *Intel® General Application Commands table*.

4.8 Sensor Data Record (SDR) Repository

The BMC implements the sensor data record (SDR) repository as specified in the *Intelligent Platform Management Interface Specification, Version 2.0.* The SDR is accessible through the BMC's in-band and out-of-band interfaces regardless of the system power state. The BMC allocates 65,519 bytes of non-volatile storage space for the SDR.

4.9 Field Replaceable Unit (FRU) Inventory Device

The BMC implements the interface for logical FRU inventory devices as specified in the *Intelligent Platform Management Interface Specification, Version 2.0.* This functionality provides commands used for accessing and managing the FRU inventory information. These commands can be delivered through all interfaces.

The BMC provides FRU device command access to its own FRU device and to the FRU devices throughout the server. The FRU device ID mapping is defined in the *Platform Specific Information*. The BMC controls the mapping of the FRU device ID to the physical device.

4.10 Diagnostics and Beep Code Generation

The BMC may generate beep codes upon detection of failure conditions. Beep codes are sounded each time the problem is discovered (for example, on each power-up attempt), but are not sounded continuously. Common supported codes are listed in **Table 17**.

Additional platform-specific beep codes can be found in the appropriate Platform specific information. Each digit in the code is represented by a sequence of beeps whose count is equal to the digit.

Table 19. BMC Beep Codes

Code	Reason for Beep	Associated Sensors	Supported
1-5-2-1	No CPUs installed	CPU Missing Sensor	Yes
1-5-2-4	MSID Mismatch	MSID Mismatch Sensor	Yes
1-5-4-2	Power fault: DC power is unexpectedly lost (power good dropout)	Power unit – power unit failure offset	Yes
1-5-4-4	Power control fault (power good assertion timeout)	Power unit – soft power control failure offset	Yes
1-5-1-2	VR Watchdog Timer sensor assertion	VR Watchdog Timer	
1-5-1-4	The system does not power on or unexpectedly powers off and a power supply unit (PSU) is present that is an incompatible model with one or more other PSUs in the system	PSU status	

4.11 Diagnostics Interrupt (NMI)

The BMC generates an NMI pulse under certain conditions. The BMC-generated NMI pulse duration is at least 30ms. Once an NMI has been generated by the BMC, the BMC does not generate another NMI until the system has been reset or powered down.

The following actions cause the BMC to generate an NMI pulse:

a. Receiving a *Chassis Control* command to pulse the diagnostic interrupt. This command does not cause an event to be logged in the SEL.
b. Detecting that the front panel diagnostic interrupt button has been pressed.
c. Watchdog timer pre-timeout expiration with NMI/diagnostic interrupt pre-timeout action enabled.

The following table shows behavior regarding NMI signal generation and event logging by the BMC.

Table 20. NMI Signal Generation and Event Logging

Causal Event	NMI (IA-32 Only)	
	Signal Generation	Front Panel Diagnostic Interrupt Sensor Event Logging Support
Chassis Control command (pulse diagnostic interrupt)	X	–
Front panel diagnostic interrupt button pressed	X	X
Watchdog Timer pre-timeout expiration with NMI/diagnostic interrupt action	X	–

4.12 BMC Basic and Advanced Management Features

The Intel® Server Board S1600JP product includes support for an upgrade module to support the advanced server management functionality.

Table 21. Basic and Advanced Management Features

Feature	Basic*	Advanced**
IPMI 2.0 Feature Support	X	X
In-circuit BMC Firmware Update	X	X
FRB 2	X	X
Chassis Intrusion Detection	X	X
Fan Redundancy Monitoring	X	X
Hot-Swap Fan Support	X	X
Acoustic Management	X	X
Diagnostic Beep Code Support	X	X
Power State Retention	X	X
ARP/DHCP Support	X	X

Feature	Basic*	Advanced**
PECI Thermal Management Support	X	X
E-mail Alerting	X	X
Embedded Web Server	X	X
SSH Support	X	X
Integrated KVM		X
Integrated Remote Media Redirection		X
Local Directory Access Protocol (LDAP)	X	X
Intel® Intelligent Power Node Manager Support***	X	X
SMASH CLP	X	X

* Basic management features provided by Integrated BMC.
**Advanced management features available with optional Intel® Remote Management Module 4 Lite.
***Intel® Intelligent Power Node Manager Support requires PMBus*-compliant power supply.

4.12.1 Enabling Advanced Manageability Features

The Advanced management features are to be delivered as part of the BMC FW image. The BMC's baseboard SPI flash contains code/data for both the Basic and Advanced features. An optional module Intel® RMM4 Lite is used as the activation mechanism. When the BMC FW initializes, it attempts to access the Intel® RMM4 lite. If the attempt to access Intel® RMM4 Lite is successful, then the BMC activates the advanced features.

Advanced manageability features are supported over all NIC ports enabled for server manageability. This includes baseboard NICs as well as the LAN channel provided by the optional Dedicated NIC add-in card.

Table 22. Management features and Benefits

Manageability Hardware	Benefits
Intel® Integrated BMC	Comprehensive IPMI based base manageability features
Intel® Remote Management Module4 – Lite Package contains one module – ▪ Key for advance Manageability features	No dedicated NIC for management Enables KVM and media redirection through onboard NIC
Intel® Remote Management4 Module Package includes 2 modules – ▪ Key for advance features ▪ Dedicated NIC (1Gbe) for management	Dedicated NIC for management traffic. Higher bandwidth connectivity for KVM and media Redirection with 1Gbe NIC

4.12.1.1 Keyboard, Video, and Mouse (KVM) Redirection

The BMC firmware supports keyboard, video, and mouse redirection (KVM) over LAN. This feature is available remotely from the embedded web server as a Java applet. This feature is enabled when the Intel® RMM4 Lite is present. The client system must have a Java Runtime Environment (JRE) version 5.0 or later to run the KVM or media redirection applets.

The Integrated BMC supports an embedded KVM application (Remote Console) that can be launched from the embedded web server from a remote console. USB1.1 or USB 2.0 based mouse and keyboard redirection are supported. It is also possible to use the KVM-redirection (KVM-r) session concurrently with media-redirection (media-r). This feature allows a user to interactively use the keyboard, video, and mouse (KVM) functions of the remote server as if the user were physically at the managed server.

The KVM-redirection feature automatically senses video resolution for best possible screen capture and provides high-performance mouse tracking and synchronization. It allows remote viewing and configuration in pre-boot POST and BIOS setup, once BIOS has initialized video.

Other attributes of this feature include:

- Encryption of the redirected screen, keyboard, and mouse
- Compression of the redirected screen

4.12.1.2 Remote Console

The Remote Console is the redirected screen, keyboard and mouse of the remote host system. To use the Remote Console window of your managed host system, the browser must include a Java* Runtime Environment plug-in. If the browser has no Java support, such as with a small handheld device, the user can maintain the remote host system using the administration forms displayed by the browser.

The Remote Console window is a Java Applet that establishes TCP connections to the Integrated BMC. The protocol that is run over these connections is a unique KVM protocol and not HTTP or HTTPS. This protocol uses ports #7578 for KVM, #5120 for CDROM media redirection, and #5123 for Floppy/USB media redirection (both supporting encryption).

4.12.1.3 Performance

The remote display accurately represents the local display. The feature adapts to changes to the video resolution of the local display and continues to work smoothly when the system transitions from graphics to text or vice-versa. The responsiveness may be slightly delayed depending on the bandwidth and latency of the network.

Enabling KVM and/or media encryption will degrade performance. Enabling video compression provides the fastest response while disabling compression provides better video quality.

For the best possible KVM performance, a 2Mb/sec link or higher is recommended.

The redirection of KVM over IP is performed in parallel with the local KVM without affecting the local KVM operation.

4.12.1.4 Security

The KVM redirection feature supports multiple encryption algorithms, including RC4 and AES. The actual algorithm that is used is negotiated with the client based on the client's capabilities.

4.12.1.5 Availability

The remote KVM session is available even when the server is powered-off (in stand-by mode). No re-start of the remote KVM session shall be required during a server reset or power on/off.

An Integrated BMC reset (for example, due to an Integrated BMC Watchdog initiated reset or Integrated BMC reset after Integrated BMC firmware update) will require the session to be re-established.

KVM sessions persist across system reset, but not across an AC power loss.

4.12.1.6 Timeout

The remote KVM session will automatically timeout after a configurable amount of time (30 minutes is the default).

The default inactivity timeout is 30 minutes, but may be changed through the embedded web server. Remote KVM activation does not disable the local system keyboard, video, or mouse. Remote KVM is not deactivated by local system input, unless the feature is disabled locally.

4.12.1.7 Usage

As the server is powered up, the remote KVM session displays the complete BIOS boot process. The user is able to interact with BIOS setup, change and save settings as well as enter and interact with option ROM configuration screens.

At least two concurrent remote KVM sessions are supported. It is possible for at least two different users to connect to the same server and start remote KVM sessions.

4.12.2 Media Redirection

The embedded web server provides a Java applet to enable remote media redirection. This may be used in conjunction with the remote KVM feature, or as a standalone applet.

The media redirection feature is intended to allow system administrators or users to mount a remote USB HDD or USB CD-ROM, floppy drive, or a USB flash disk as a remote device to the server. Once mounted, the remote device appears just like a local device to the server, allowing system administrators or users to install software (including operating systems), copy files, update BIOS, and so on, or boot the server from this device.

The following capabilities are supported:

- The operation of remotely mounted devices is independent of the local devices on the server. Both remote and local devices are useable in parallel.
- It is possible to boot all supported operating systems from the remotely mounted device and to boot from disk IMAGE (*.IMG) and CD-ROM or DVD-ROM ISO files. See the tested/supported *Operating System List* for more information.
- Media redirection shall support redirection for a minimum of two virtual devices concurrently with any combination of devices. As an example, a user could redirect two CD or two USB devices.
- The media redirection feature supports multiple encryption algorithms, including RC4 and AES. The actual algorithm that is used is negotiated with the client based on the client's capabilities.
- A remote media session is maintained even when the server is powered-off (in standby mode). No restart of the remote media session is required during a server reset or power

on/off. An Integrated BMC reset (for example, due to an Integrated BMC reset after Integrated BMC firmware update) will require the session to be re-established.

- The mounted device is visible to (and useable by) the managed system's OS and BIOS in both pre-boot and post-boot states.
- The mounted device shows up in the BIOS boot order and it is possible to change the BIOS boot order to boot from this remote device.
- It is possible to install an operating system on a bare metal server (no OS present) using the remotely mounted device. This may also require the use of KVM-r to configure the OS during install.
- USB storage devices will appear as floppy disks over media redirection. This allows for the installation of device drivers during OS installation.
- If either a virtual floppy device is remotely attached during system boot, the virtual floppy is presented as a bootable device. It is not possible to present only a single-mounted device type to the system BIOS.

4.12.2.1 Availability

The default inactivity timeout is 30 minutes and is not user-configurable.

Media redirection sessions persist across system reset but not across an AC power loss or BMC reset.

4.12.2.2 Network Port Usage

The KVM and media redirection features use the following ports:

- 5120 – CD Redirection
- 5123 – FD Redirection
- 5124 – CD Redirection (Secure)
- 5127 – FD Redirection (Secure)
- 7578 – Video Redirection
- 7582 – Video Redirection (Secure)

4.12.3 Embedded Web server

Integrated BMC Base manageability provides an embedded web server and an OEM-customizable web GUI which exposes the manageability features of the Integrated BMC base feature set. It is supported over all on-board NICs that have management connectivity to the Integrated BMC as well as an optional dedicated add-in management NIC. At least two concurrent web sessions from up to two different users is supported. The embedded web user interface shall support the following client web browsers:

- Microsoft Internet Explorer 7.0*
- Microsoft Internet Explorer 8.0*
- Microsoft Internet Explorer 9.0*
- Mozilla Firefox 3.0*
- Mozilla Firefox 3.5*

- Mozilla Firefox 3.6*

The embedded web user interface supports strong security (authentication, encryption, and firewall support) since it enables remote server configuration and control. The user interface presented by the embedded web user interface shall authenticate the user before allowing a web session to be initiated. Encryption using 128-bit SSL is supported. User authentication is based on user id and password.

The GUI presented by the embedded web server authenticates the user before allowing a web session to be initiated. It presents all functions to all users but grays-out those functions that the user does not have privilege to execute. (For example, if a user does not have privilege to power control, then the item shall be displayed in gray-out font in that user's UI display). The web GUI also provides a launch point for some of the advanced features, such as KVM and media redirection. These features are grayed out in the GUI unless the system has been updated to support these advanced features.

A partial list of additional features supported by the web GUI includes:

- Present all the Basic features to the users.
- Power on/off/reset the server and view current power state.
- Virtual front panel display and overall system health.
- Provide embedded firmware version information.
- Configuration of various IPMI parameters (LAN parameters, users, passwords, and so on.)
- Configuration of alerting (SNMP and SMTP).
- Display system asset information for the product, board, and chassis.
- Display of BMC-owned sensors (name, status, current reading, enabled thresholds), including color-code status of sensors.
- Automatic refresh of sensor data with a configurable refresh rate.
- On-line help.
- Display/clear SEL (display is in easily understandable human readable format).
- Supports major industry-standard browsers (Internet Explorer and Mozilla Firefox).
- Automatically logs out after user-configurable inactivity period.
- The GUI session automatically times-out after a user-configurable inactivity period. By default, this inactivity period is 30 minutes.
- Embedded Platform Debug feature - Allow the user to initiate a "diagnostic dump" to a file that can be sent to Intel® for debug purposes.
- Display of power statistics (current, average, minimum, and maximum) consumed by the server.

4.12.4 Data Center Management Interface (DCMI)

The DCMI Specification is an emerging standard that is targeted to provide a simplified management interface for Internet Portal Data Center (IPDC) customers. It is expected to become a requirement for server platforms which are targeted for IPDCs. DCMI is an IPMI-

based standard that builds upon a set of required IPMI standard commands by adding a set of DCMI-specific IPMI OEM commands.

4.12.5 Lightweight Directory Authentication Protocol (LDAP)

The Lightweight Directory Access Protocol (LDAP) is an application protocol supported by the Integrated BMC for the purpose of authentication and authorization. The Integrated BMC user connects with an LDAP server for login authentication. This is only supported for non-IPMI logins including the embedded web UI and SM-CLP. IPMI users/passwords and sessions are not supported over LDAP.

LDAP can be configured (IP address of LDAP server, port, and so on.) through the Integrated BMC's Embedded Web UI. LDAP authentication and authorization is supported over the any NIC configured for system management. The BMC uses a standard Open LDAP implementation for Linux*.

4.12.6 Platform/Chassis Management

Within an IPMI 2.0 framework, the BMC Firmware provides functionality to support management and control of several aspects of the platform operation. This includes:

- **Front Panel Support** (for example, secure lock out of power and reset buttons and System Status LED control)
- **Hardware/Sensor Monitoring** (for example, system voltages, thermal sensors, fans, power supplies, and so on)
- **Power/Reset Control and Monitoring** (for example, local and remote power/reset control and power restore policy)
- **Hardware and Manufacturing Test Features**
- **Asset Inventory and System Identification** (for example, system GUID and FRU management)
- **Thermal and Acoustics Management** – The BMC firmware provides a comprehensive set of fan control capabilities utilizing various system thermal sensors (for example, CPU, DIMMs, front panel thermal sensor). Additionally, the BMC participates in the memory CLTT by pushing dim thermal data to the iMC in the CPU.
- **Power Management (Node Manager) Support** – BMC firmware provides an external (LAN) interface for a remote management console to communicate with the ME's Node Manager Functionality.

4.12.7 Thermal Control

The system shall support thermal management through open loop throttling (OLTT) or static closed loop throttling (CLTT) of system memory based on availability of valid temperature sensors on the installed memory DIMMs. The Integrated Memory Controller (IMC) dynamically changes throttling levels to cap throttling based on memory and system thermal conditions as determined by the system and DIMM power and thermal parameters. CLTT on mixed-mode DIMM populations is not supported (that is, some installed DIMMs have valid temp sensors and some do not). The Integrated BMC fan speed control functionality is related to the memory throttling mechanism used.

The following terminology is used for the various memory throttling options:

- **Static Open Loop Thermal Throttling (Static-OLTT):** OLTT control registers are configured by BIOS MRC remain fixed after post. The system does not change any of the throttling control registers in the embedded memory controller during runtime.
- **Static Closed Loop Thermal Throttling (Static-CLTT):** CLTT control registers are configured by BIOS MRC during POST. The memory throttling is run as a closed-loop system with the DIMM temperature sensors as the control input. Otherwise, the system does not change any of the throttling control registers in the embedded memory controller during runtime.
- **Dynamic Open Loop Thermal Throttling (Dynamic-OLTT):** OLTT control registers are configured by BIOS MRC during POST. Adjustments are made to the throttling during runtime based on changes in system cooling (fan speed).
- **Dynamic Closed Loop Thermal Throttling (Dynamic-CLTT):** CLTT control registers are configured by BIOS MRC during POST. The memory throttling is run as a closed-loop system with the DIMM temperature sensors as the control input. Adjustments are made to the throttling during runtime based on changes in system cooling (fan speed).

4.12.7.1 Fan Speed Control Profiles

BIOS and BMC software work cooperatively to implement system thermal management support. During normal system operation, the BMC will retrieve information from the BIOS and monitor several platform thermal sensors to determine the required fan speeds.

In order to provide the proper fan speed control for a given system configuration, the BMC must have the appropriate platform data programmed. Platform configuration data is programmed using the FRUSDR utility during the system integration process and by System BIOS during run time.

Table 23. Fab Profile Mapping

Type	Profile	Details
OLTT	0	Acoustic, 300M altitude
OLTT	1	Performance, 300M altitude
OLTT	2	Acoustic, 900M altitude
OLTT	3	Performance, 900M altitude
OLTT	4	Acoustic, 1500M altitude
OLTT	5	Performance, 1500M altitude
OLTT	6	Acoustic, 3000M altitude
OLTT	7	Performance, 3000M altitude
CLTT	0	300M altitude
CLTT	2	900M altitude
CLTT	4	1500M altitude
CLTT	6	3000M altitude

4.12.7.2 System Configuration using FRUSDR Utility

The Field Replaceable Unit and Sensor Data Record Update Utility (FRUSDR utility) is a program used to write platform-specific configuration data to NVRAM on the server board. It allows the user to select which supported chassis (Intel® or Non-Intel®) and platform chassis

configuration is used. Based on the input provided, the FRUSDR writes sensor data specific to the configuration to NVRAM for the BMC controller to read each time the system is powered on.

4.13 Intel® Intelligent Power Node Manager

4.13.1 Overview

Power management deals with requirements to manage processor power consumption and manage power at the platform level to meet critical business needs. Node Manager (NM) is a platform resident technology that enforces power capping and thermal-triggered power capping policies for the platform. These policies are applied by exploiting subsystem knobs (such as processor P and T states) that can be used to control power consumption. NM enables data center power management by exposing an external interface to management software through which platform policies can be specified. It also implements specific data center power management usage models such as power limiting and thermal monitoring.

Note: Support for NM is product-specific. This section details how NM would be supported on products that provide this capability.

The NM feature is implemented by a complementary architecture utilizing the ME, BMC, BIOS, and an ACPI-compliant OS. The ME provides the NM policy engine and power control/limiting functions (referred to as Node Manager or NM) while the BMC provides the external LAN link by which external management software can interact with the feature. The BIOS provides system power information utilized by the NM algorithms and also exports ASL code used by OSPM for negotiating processor P and T state changes for power limiting. PMBus*-compliant power supplies provide the capability to monitoring input power consumption, which is necessary to support NM.

The NM architecture applicable to this generation of servers is defined by the *NPTM Architecture Specification v2.0*. NPTM is an evolving technology that is expected to continue to add new capabilities that will be defined in subsequent versions of the specification. The ME NM implements the NPTM policy engine and control/monitoring algorithms defined in the NPTM specification.

4.13.2 Features

NM provides feature support for policy management, monitoring and querying, alerts and notifications, and an external interface protocol. The policy management features implement specific IT goals that can be specified as policy directives for NM. Monitoring and querying features enable tracking of power consumption. Alerts and notifications provide the foundation for automation of power management in the data center management stack. The external interface specifies the protocols that must be supported in this version of NM.

The role of BMC in Node Manager will include:

- External communication links
- Command passing through BMC
- Alerting
- BIOS-BMC-ME communication

4.14 Management Engine (ME)

4.14.1 Overview

The Intel® Server Platform Services (SPS) is a set of manageability services provided by the firmware executing on an embedded ARC controller within the IOH. This management controller is also commonly referred to as the Management Engine (ME). The functionality provided by the SPS firmware is different from Intel® Active Management Technology (Intel® AMT or AT) provided by the ME on client platforms.

Server Platform Services (SPS) are value-added platform management options that enhance the value of Intel® platforms and their component ingredients (CPUs, chipsets, and I/O components). Each service is designed to function independently wherever possible, or grouped together with one or more features in flexible combinations to allow OEMs to differentiate platforms.

4.14.2 BMC – Management Engine (ME) Distributed Model

The Intel® Server Board S1600JP covered in this specification will require Node Manager 2.0 (NM2.0) support. The following management architecture would need to be supported on the baseboard to meet product and validation requirements. The NM 2.0 functionality is provided by the Intel® C600 PCH Management Engine (ME).

The server management architecture is a partitioned model which places the Management Engine, which is an embedded controller in the Intel® C600 PCH, in between the BMC and the processors. In this architecture, the PCH Management Engine is the owner of the PECI 3.0 bus and the Emulex* Pilot III BMC communicates with the ME through a SMBus* connection (SMLINK 0.) The ME provides PECI proxy support that allows the ServerEngines* Pilot III BMC firmware to access processor functions available on the PECI bus.

The primary function of ME is to implement the NM 2.0 feature set. In this architectural model, the Emulex* Pilot III BMC provides the external (LAN) interface to ME in the form of IPMI bridging. A remote Node Manager application would establish a management session with the Emulex* Pilot III BMC which in turn would bridge IPMI commands through the secondary IPMB to the ME. In this scenario, the Emulex* Pilot III BMC simply acts as a proxy for this communication pipe. The ME may also generate alerts to the Emulex* Pilot III BMC, which may log these into the system SEL and/or output them to the remote application in the form of IPMI LAN alerts.

The Emulex* Pilot III BMC needs access to various system registers in the processor core silicon and integrated memory controller subsystem. Examples include Processor core and Memory DIMMs temperature information. The Emulex* Pilot III BMC requires this information as input into its fan speed control algorithms. The Emulex* Pilot III BMC accesses these registers through the secondary IPMB bus connection to ME. Depending on the particular data or register access needed, this is done using either the ME's PECI proxy functionality or through an abstracted data construct provided by the ME.

Also in this architecture, both the Emulex* Pilot III BMC and the ME are connected to the system power supplies through a common PMBus* (SMBUS* physical) connection (SMLINK 1.) The ME accesses the system power supplies in support of various NM 2.0 features. The Emulex* Pilot III BMC monitors the power supplies in support of various power-related telemetry and status information that is exposed as IPMI sensors.

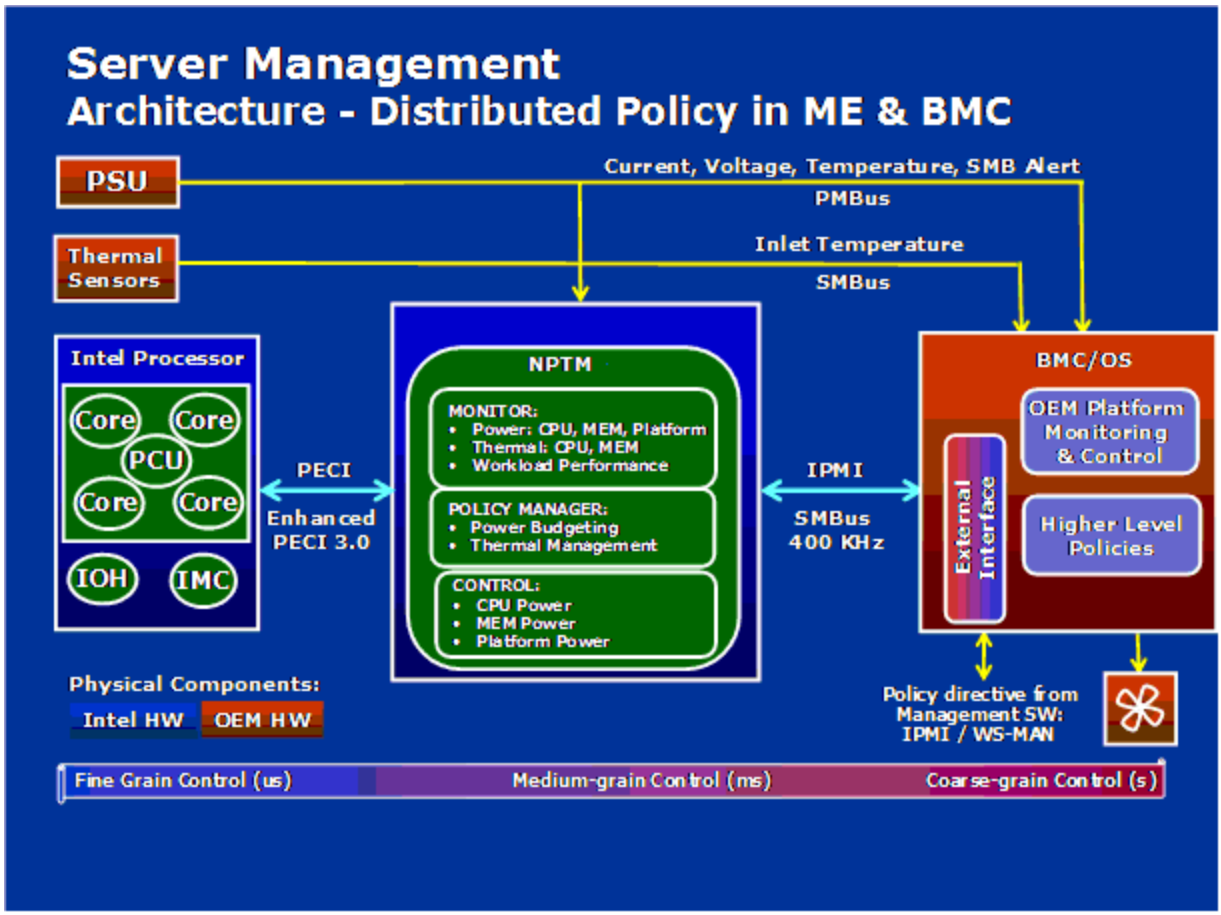


Figure 18. Management Engine Distribution Model

4.14.3 ME System Management Bus (SMBus*) Interface

- The ME uses the SMLink0 on the SSB in multi-master mode as a dedicated bus for communication with the BMC using the IPMB protocol. The EPSD BMC FW considers this a secondary IPMB bus and runs at 400 kHz.
- The ME uses the SMLink1 on the SSB in multi-master mode bus for communication with PMBus* devices in the power supplies for support of various NM-related features. This bus is shared with the BMC, which polls these PMBus* power supplies for sensor monitoring purposes (for example, power supply status, input power, and so on.). This bus runs at 100 KHz.
- The Management Engine has access to the “Host SMBus*”.

4.14.4 BMC - Management Engine Interaction

Management Engine-Integrated BMC interactions include the following:

- Integrated BMC stores sensor data records for ME-owned sensors.
- Integrated BMC participates in ME firmware update.
- Integrated BMC initializes ME-owned sensors based on SDRs.
- Integrated BMC receives platform event messages sent by the ME.
- Integrated BMC notifies ME of POST completion.

- BMC may be queried by the ME for inlet temperature readings.

4.14.5 ME Power and Firmware Startup

On Intel® Server Board S1600JP, the ME is on standby power. The ME FW will begin its startup sequence at the same time that the BMC FW is booting. As the BMC FW is booting to a Linux* kernel and the ME FW uses an RTOS, the ME FW should always complete its basic initialization before the BMC. The ME FW can be configured to send a notification message to the BMC. After this point, the ME FW is ready to process any command requests from the BMC.

In S0/S1 power states, all ME FW functionality is supported. Some features, such as power limiting, are not supported in S3/S4/S5 power states. Refer to *ME FW documentation* for details on what is not supported while in the S3/S4/S5 states.

The ME FW uses a single operational image with a limited-functionality recovery image. In order to upgrade an operational image, a boot to recovery image must be performed. The ME FW does not support an IPMI update mechanism except for the case that the system is configured with a dual-ME (redundant) image. In order to conserve flash space, which the ME FW shares with BIOS, EPSD systems only support a single ME image. For this case, ME update is only supported by means of BIOS performing a direct update of the flash component. The recovery image only provides the basic functionality that is required to perform the update; therefore other ME FW features are not functional therefore when the update is in progress.

4.14.6 SmaRT/CLST

The power supply optimization provided by SmaRT/CLST relies on a platform HW capability as well as ME FW support. When a PMBus*-compliant power supply detects insufficient input voltage, an over current condition, or an over-temperature condition, it will assert the SMBAlert# signal on the power supply SMBus* (also known as the PMBus*). Through the use of external gates, this results in a momentary assertion of the PROCHOT# and MEMHOT# signals to the processors, thereby throttling the processors and memory. The ME FW also sees the SMBAlert# assertion, queries the power supplies to determine the condition causing the assertion, and applies an algorithm to either release or prolong the throttling, based on the situation.

System power control modes include:

- **SmaRT:** Low AC input voltage event; results in a onetime momentary throttle for each event to the maximum throttle state
- **Electrical Protection CLST:** High output energy event; results in a throttling hiccup mode with fixed maximum throttle time and a fix throttle release ramp time
- **Thermal Protection CLST:** High power supply thermal event; results in a throttling hiccup mode with fixed maximum throttle time and a fix throttle release ramp time

When the SMBAlert# signal is asserted, the fans will be gated by HW for a short period (~100ms) to reduce overall power consumption. It is expected that the interruption to the fans will be of short enough duration to avoid false lower threshold crossings for the fan tach sensors; however, this may need to be comprehended by the fan monitoring FW if it does have this side-effect.

4.15 Other Platform Management

The platform supports the following sleep states, S1 and S5. Within S0, the platform supports additional lower power states, such as C1e and C6, for the CPU.

4.15.1 Wake On LAN (WOL)

- Wake On LAN (WOL) is supported on both LAN ports and IOM LAN modules for all supported Sleep states.
- Wake on Ring is supported on the external Serial port only for all supported Sleep states.
- Wake on USB is supported on the rear and front panel USB ports for S1 only.
- Wake on RTC is supported for all supported Sleep states.
- Wake IPMI command is supported (BMC function no additional hardware requirement) for all supported Sleep states.

4.15.2 PCI Express* Power management

L0 and L3 power management states are supported on all PCI Express* slots and embedded end points.

4.15.3 PMBus*

Power supplies that have PMBus* 1.1 are supported and required to support Intel® Dynamic Power Node Manager. Intel® Server Board S1600JP supports the features of Intel® Dynamic Power Node Manager version 1.5 except the inlet temperature sensor.

5. BIOS Setup Interface

5.1 HotKeys Supported During POST

Certain “HotKeys” are recognized during POST. A HotKey is a key or a key combination that is recognized as an unprompted command input, that is, the operator is not prompted to press the HotKey and typically the HotKey will be recognized even while other processing is in progress.

The Intel® Server Board S1600JP Family BIOS recognizes a number of HotKeys during POST. After the OS is booted, HotKeys are the responsibility of the OS and the OS defines its own set of recognized HotKeys.

Following are the POST HotKeys, with their functions:

Table 24. POST HotKeys Recognized

HotKey Combination	Function
<F2>	Enter Setup
<F6>	Pop up BIOS Boot Menu
<F12>	Network boot

5.2 POST Logo/Diagnostic Screen

The logo/Diagnostic Screen displays in one of two forms:

- If Quiet Boot is enabled in the BIOS setup, a logo splash screen displays. By default, Quiet Boot is enabled in the BIOS setup. If the logo displays during POST, press <Esc> to hide the logo and display the diagnostic screen.
- If a logo is not present in the flash ROM or if Quiet Boot is disabled in the system configuration, the POST Diagnostic Screen is displayed with a summary of system configuration information.

The diagnostic screen displays the following information:

- “Copyright <year> Intel Corporation”
- AMI Copyright statement
- BIOS version (ID)
- BMC firmware version
- SDR version
- ME firmware version
- Platform ID
- System memory detected (total size of all installed DDRIII DIMMs)
- Current memory speed (currently configured memory operating frequency)
- Processor information (Intel® Brand String identifying type of processor and nominal operating frequency, and number of physical processors identified).
- Keyboards detected, if any attached

- Mouse devices detected, if any attached
- Instructions showing HotKeys for going to Setup, going to popup Boot Menu, starting Network Boot

5.3 BIOS Boot Pop-up Menu

The BIOS Boot Specification (BBS) provides a Boot Pop-up menu that can be invoked by pressing the **<F6>** key during POST. The BBS Pop-up menu displays all available boot devices. The boot order in the pop-up menu is not the same as the boot order in the BIOS setup. The pop-up menu simply lists all of the available devices from which the system can be booted, and allows a manual selection of the desired boot device.

When an Administrator password is installed in Setup, the Administrator password will be required in order to access the Boot Pop-up menu using the **<F6>** key. If a User password is entered, the Boot Pop-up menu will not even appear – the user will be taken directly to the Boot Manager in the Setup, where the User password allows only booting in the order previously defined by the Administrator.

5.4 BIOS Setup Utility

The BIOS Setup utility is a text-based utility that allows the user to configure the system and view current settings and environment information for the platform devices. The Setup utility controls the platform's built-in devices, the boot manager, and error manager.

The BIOS Setup interface consists of a number of pages or screens. Each page contains information or links to other pages. The advanced tab in Setup displays a list of general categories as links. These links lead to pages containing a specific category's configuration.

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

5.4.1 BIOS Setup Operation

The BIOS Setup Utility has the following features:

- Localization – The Intel® Server Board BIOS is only available in English. However, BIOS Setup uses the Unicode standard and is capable of displaying data and input in Setup fields in all languages currently included in the Unicode standard.
- Console Redirection – BIOS Setup is functional through Console Redirection over various terminal emulation standards. This may limit some functionality for compatibility, for example, usage of colors or some keys or key sequences or support of pointing devices.
- Setup screens are designed to be displayable in an 80-character x 24-line format in order to work with Console Redirection, although that screen layout should display correctly on any format with longer lines or more lines on the screen.
- Password protection – BIOS Setup may be protected from unauthorized changes by setting an Administrative Password in the Security screen. When an Administrative Password has been set, all selection and data entry fields in Setup (except System Time and Date) are grayed out and cannot be changed unless the Administrative Password has been entered.

Note: if an Administrative Password has **not** been set, anyone who boots the system to Setup has access to all selection and data entry fields in Setup and can change any of them.

5.4.1.1 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.

The Setup page is designed to a format of 80 x 24 (24 lines of 80 characters each). The typical display screen in a Legacy mode or in a terminal emulator mode is actually 80 characters by 25 lines, but with "line wrap" enabled (which it usually is) the 25th line cannot be used with the Setup page.

Table 25. BIOS Setup Page Layout

Functional Area	Description
Title (Tab) Bar	The Title Bar is located at the top of the screen and displays "Tabs" with the titles of the top-level pages, or screens that can be selected. Using the left and right arrow keys moves from page to page through the Tabs. When there are more Tabs than can be displayed on the Title (Tab) Bar, they will scroll off to the left or right of the screen and temporarily disappear from the visible Title Bar. Using the arrow keys will scroll them back onto the visible Title Bar. When the arrow keys reach either end of the Title Bar, they will "wrap around" to the other end of the Title Bar. For multi-level hierarchies, this shows only the top-level page above the page which the user is currently viewing. The Page Title gives further information.
Page Title	In a multi-level hierarchy of pages beneath one of the top-level Tabs, the Page Title identifying the specific page which the user is viewing is located in the upper left corner of the page. Using the <ESC> (Escape) key will return the user to the higher level in the hierarchy, until the top-level Tab page is reached.
Setup Item List	The Setup Item List is a set of control entries and informational items. The list is displayed in two columns. For each item in the list: ▪ The left column of the list contains Prompt String (or Label String), a character string which identifies the item. The Prompt String may be up to **34 characters** long in the 80 x 24 page format. ▪ The right column contains a data field which may be an informational data display, a data input field, or a multiple choice field. Data input or multiple-choice fields are demarcated by square brackets ("[....]". This field may be up to **90 characters** long, but only the first **22 characters** can be displayed on the 80 x 24 page (**24 characters** for an informational display-only field). The operator navigates up and down the right hand column through the available input or choice fields. A Setup Item may also represent a selection to open a new screen with a further group of options for specific functionality. In this case, the operator navigates to the desired selection and presses <Enter> to go to the new screen.
Item-Specific Help Area	The Item-specific Help Area is located on the right side of the screen and contains Help Text specific to the highlighted Setup Item. Help information may include the meaning and usage of the item, allowable values, effects of the options, and so on. The Help Area is a **29 character by 11 line** section of the 80 x 24 page. The Help Text may have explicit line-breaks within it. When the text is longer than 29 characters, it is also broken to a new line, dividing the text at the last space (blank) character before the 29th character. An unbroken string of more than 29 character will be arbitrarily wrapped to a new line after the 29th character. Text that extends beyond the end of the 11th line will not be displayed.

Functional Area	Description
Keyboard Command Area	The Keyboard Command Area is located at the bottom right of the screen and continuously displays help for keyboard special keys and navigation keys.

5.4.1.2 Entering BIOS Setup

To enter the BIOS Setup using a keyboard (or emulated keyboard), press the <F2> function key during boot time when the OEM or Intel logo is displayed. The following message is displayed on the diagnostics screen and under the Quiet Boot logo screen:

Press <F2> to enter setup

When the Setup Utility is entered, the Main screen is displayed. However, serious errors cause the system to display the Error Manager screen instead of the Main screen.

It is also possible to cause a boot to Setup using an IPMI 2.0 command “Get/Set System Boot Options”. For details on that capability, see the explanation in the IPMI description.

5.4.1.3 Setup Navigation 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. Each feature is associated with a value field, except those used for informative purposes. Each value field contains configurable parameters. Depending on the security option chosen and in effect by the password, a menu feature’s value may or may not be changed. If a value cannot be changed, its field is made inaccessible and appears grayed out.

Table 26. BIOS Setup: Keyboard Command Bar

Key	Option	Description
<Enter>	Execute Command	The **<Enter>** key is used to activate submenus when the selected feature is a submenu, or to display a pick list if a selected option has a value field, or to select a subfield for multi-valued features like time and date. If a pick list is displayed, the **<Enter>** key selects the currently highlighted item, undoes the pick list, and returns 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 submenu, 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 user is returned to where they were before **<Esc>** was pressed, without affecting any existing settings. If “Yes” is selected and the <Enter> key is pressed, the 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 effect if a sub-menu or pick list is displayed.

Key	Option	Description
<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.
-	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 keyboards, but will have the same effect.
<F9>	Setup Defaults	Pressing the **<F9>** key causes the following to display: Load Optimized Defaults? Yes No 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 user is returned to where they were before **<F9>** was pressed without affecting any existing field values.
<F10>	Save and Exit	Pressing the **<F10>** key causes the following message to display: Save configuration and reset? Yes No If "Yes" is highlighted and **<Enter>** is pressed, all changes are saved and the Setup is exited. If "No" is highlighted and **<Enter>** is pressed, or the **<Esc>** key is pressed, the user is returned to where they were before **<F10>** was pressed without affecting any existing values.

5.4.1.4 Setup Screen Menu Selection Bar

The Setup Screen Menu selection bar is located at the top of the BIOS Setup Utility screen. It displays tabs showing the major screen selections available to the user. By using the left and right arrow keys, the user can select the listed screens. Some screen selections are out of the visible menu space, and become available by scrolling to the left or right of the current selections displayed.

5.4.2 BIOS Setup Utility Screens

The following sections describe the screens available in the BIOS Setup utility for the configuration of the server platform.

For each of these screens, there is an image of the screen with a list of Field Descriptions which describe the contents of each item on the screen. Each item on the screen is hyperlinked to the relevant Field Description. Each Field Description is hyperlinked back to the screen image.

These lists follow the following guidelines:

- The text heading for each Field Description is the actual text as displayed on the BIOS Setup screen. This screen text is a hyperlink to its corresponding Field Description.

- The text shown in the Option Values and Help Text entries in each Field Description are the actual text and values are displayed on the BIOS Setup screens.
- In the Option Values entries, the text for default values is shown with an underline. These values do not appear underline on the BIOS Setup screen. The underlined text in this document is to serve as a reference to which value is the default value.
- The Help Text entry is the actual text which appears on the screen to accompany the item when the item is the one in focus (active on the screen).
- The Comments entry provides additional information where it may be helpful. This information does not appear on the BIOS Setup screens.
- Information enclosed in angular brackets (< >) in the screen shots identifies text that can vary, depending on the option(s) installed. For example, *<Amount of memory installed>* is replaced by the actual value for "Total Memory".
- Information enclosed in square brackets ([ ]) in the tables identifies areas where the user must 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 in order for the changes to take effect. Alternatively, pressing <ESC> discards the changes and resumes POST to continue to boot the system according to the boot order set from the last boot.

5.4.2.1 Map of Screens and Functionality

There are a number of screens in the entire Setup collection. They are organized into major categories. Each category has a hierarchy beginning with a top-level screen from which lower-level screens may be selected. Each top-level screen appears as a tab, arranged across the top of the Setup screen image of all top-level screens.

There are more categories than will fit across the top of the screen, so at any given time there will be some categories which will not appear until the user has scrolled across the tabs which are present.

The categories and the screens included in each category are listed as follows, with links to each of the screens named:

Table 27. Screen Map

Categories (Top Tabs)	2nd Level Screens	3rd Level Screens
Main Screen (Tab)		

Categories (Top Tabs)	2nd Level Screens	3rd Level Screens
Advanced Screen (Tab)		
↳	Processor Configuration	
↳	Power & Performance	
↳	Memory Configuration	
	↳	Memory RAS and Performance Configuration
↳	Mass Storage Controller Configuration	
↳	PCI Configuration	
	↳	NIC Configuration
↳	PCIe Port Oprom Control	
↳	USB Configuration	
↳	System Acoustic and Performance Configuration	
Security Screen (Tab)		
Server Management Screen (Tab)		
↳	Console Redirection	
↳	System Information	
↳	BMC LAN Configuration	
Boot Options Screen (Tab)		
↳	CDROM Order	
↳	Hard Disk Order	
↳	Floppy Order	
↳	Network Device Order	
↳	BEV Device Order	
↳	Add EFI Boot Option	
↳	Delete EFI Boot Option	

Categories (Top Tabs)	2nd Level Screens	3rd Level Screens
Boot Manager Screen (Tab)		
Error Manager Screen (Tab)		
Save and Exit Screen (Tab)		

5.4.2.2 Main Screen (Tab)

The Main Screen is the first screen that appears when the BIOS Setup configuration utility is entered, unless an error has occurred. If an error has occurred, the Error Manager Screen appears instead.

Figure 19. Main Screen

Table 28. Setup Utility – Main Screen Fields

Setup Item	Options	Help Text	Comments
Logged in as	Administrator / User	None	Information only. Displays password level that setup is running in: Administrator or User. With no passwords set, Administrator is the default mode.
Platform ID	Platform ID	None	Information only. Displays the Platform ID: S1600JP

Setup Item	Options	Help Text	Comments
System BIOS			
BIOS Version	BIOS version ID	None	Information only. The BIOS version displayed uniquely identifies the BIOS that is currently installed and operational on the board. The version information displayed is taken from the BIOS ID String, with the timestamp segment dropped off. The segments displayed are: Platform: Identifies that this is the correct platform BIOS 86B: Identifies this BIOS as being an EPSD Server BIOS xx: Major Revision level of the BIOS yy: Minor Revision level for this BIOS zzzz: Release Number for this BIOS
Build Date	Date and time when the currently installed BIOS was built	None	Information only. The time and date displayed are taken from the timestamp segment of the BIOS ID String.
Memory			
Total Memory	Amount of memory installed in the system	None	Information only. Displays the total physical memory installed in the system, in MB or GB. The term physical memory indicates the total memory discovered in the form of installed DDRIII DIMMs.
Quiet Boot	**Enabled** Disabled	[Enabled] – Display the logo screen during POST. [Disabled] – Display the diagnostic screen during POST.	This field controls whether the full diagnostic information is displayed on the screen during POST. When Console Redirection is enabled, the Quiet Boot setting is disregarded and the text mode Diagnostic Screen is displayed unconditionally.
POST Error Pause	Enabled **Disabled**	[Enabled] – Go to the Error Manager for critical POST errors. [Disabled] – Attempt to boot and do not go to the Error Manager for critical POST errors.	If enabled, the POST Error Pause option takes the system to the error manager to review the errors when major errors occur. Minor and fatal error displays are not affected by this setting.

Setup Item	Options	Help Text	Comments
System Date	System Date initially displays the current system calendar date, including the day of the week	System Date has configurable fields for Month, Day, and Year. The year must be between 2005 and 2099. Use [Enter] or [Tab] key to select the next field. Use [+] or [-] key to modify the selected field.	This field will initially display the current system day of week and date. It may be edited to change the system date. When the System Date is reset by the "BIOS Defaults" jumper, BIOS Recovery Flash Update, or other method, the date will be the earliest date in the allowed range – Saturday 01/01/2005.
System Time	System Time initially displays the current system time of day, in 24-hour format	System Time has configurable fields for Hours, Minutes, and Seconds. Hours are in 24-hour format. Use [Enter] or [Tab] key to select the next field. Use [+] or [-] key to modify the selected field.	This field will initially display the current system time (24 hour time). It may be edited to change the system time. When the System Time is reset by the "BIOS Defaults" jumper, BIOS Recovery Flash Update, or other method, the time will be the earliest time of day in the allowed range – 00:00:00

5.4.2.3 Advanced Screen (Tab)

The Advanced screen provides an access point to configure several groups of options. On this screen, the user can select the option group to be configured. Configuration actions are performed on the selected screen, and not directly on the Advanced screen.

To access this screen from the **Main** screen or other top-level "Tab" screen, press the right or left arrow keys to traverse the tabs at the top of the Setup screen until the **Advanced** screen is selected.

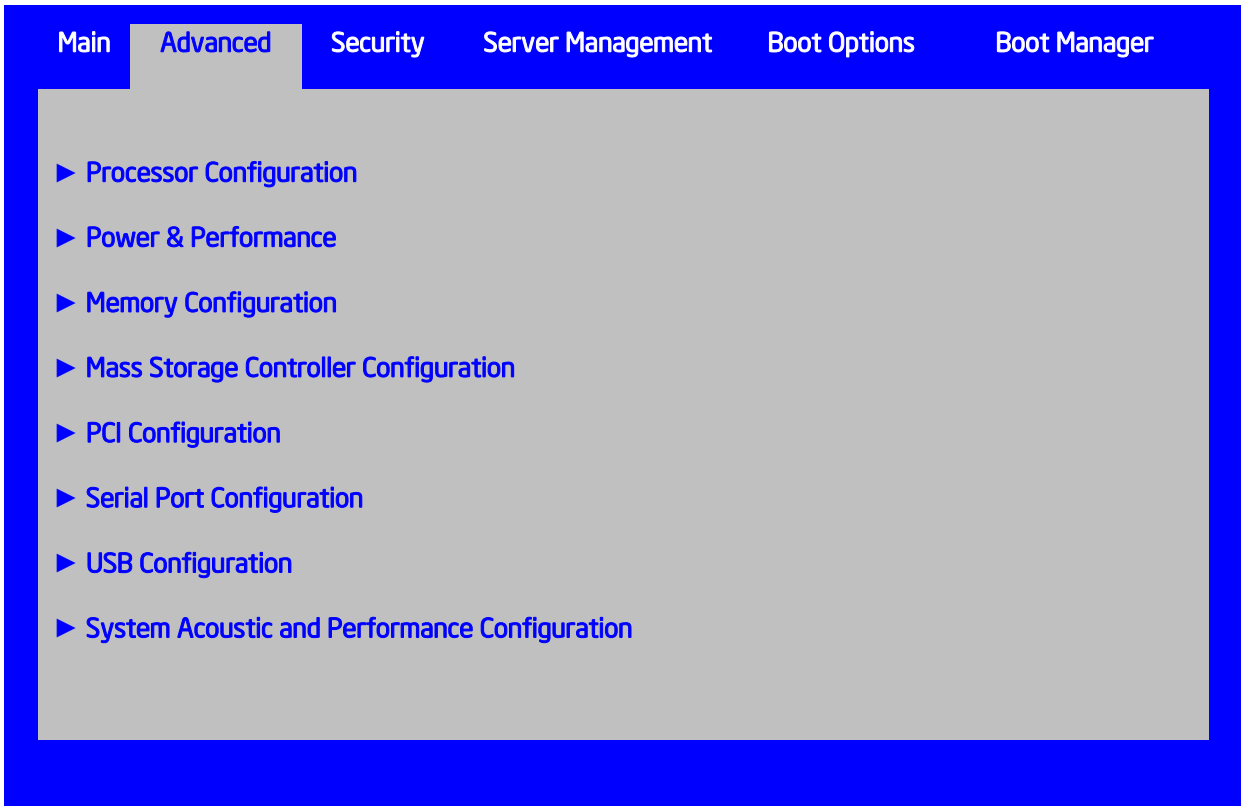


Figure 20. Advanced Screen

Table 29. Setup Utility – Advanced Screen Display Fields

Setup Item	Options	Help Text	Comments
Processor Configuration	None	View/Configure processor information and settings.	Selection only. Select this line and press the <Enter> key to go to the Processor Configuration group of configuration settings.
Power & Performance	None	View/Configure power and performance policy	Selection only. Select this line and press the <Enter> key to go to the Power and Performance group of configuration settings.
Memory Configuration	None	View/Configure memory information and settings.	Selection only. Select this line and press the <Enter> key to go to the Memory Configuration group of configuration settings.
Mass Storage Controller Configuration	None	View/Configure mass storage controller information and settings.	Selection only. Select this line and press the <Enter> key to go to the Mass Storage Controller Configuration group of configuration settings.

Setup Item	Options	Help Text	Comments
PCI Configuration	None	View/Configure PCI information and settings.	Selection only. Select this line and press the <Enter> key to go to the PCI Configuration group of configuration settings.
Serial Port Configuration	None	View/Configure serial port information and settings.	Selection only. Select this line and press the <Enter> key to go to the Serial Port Configuration group of configuration settings.
USB Configuration	None	View/Configure USB information and settings.	Selection only. Select this line and press the <Enter> key to go to the USB Configuration group of configuration settings.
System Acoustic and Performance Configuration	None	View/Configure system acoustic and performance information and settings.	Selection only. Select this line and press the <Enter> key to go to the System Acoustic and Performance Configuration group of configuration settings.

5.4.2.4 Processor Configuration

The Processor Configuration screen displays the processor identification and microcode level, core frequency, cache sizes for all processors currently installed. It also allows the user to enable or disable a number of processor options.

To access this screen from the **Main** screen, select **Advanced** > **Processor Configuration**. To move to another screen, press the **<Esc>** key to return to the **Advanced screen**, then select the desired screen.

Figure 21. Processor Configuration Screen

Table 30. Setup Utility – Processor Configuration Screen Fields

etup Item	Options	Help Text	Comments
Processor ID	CPUID	None	Information only. Processor CPUID
Processor Frequency	Current Processor Operating Frequency	None	Information only. Current frequency of the processor.
Microcode Revision	Microcode Revision Number	None	Information only. Revision of the loaded microcode.

etup Item	Options	Help Text	Comments
L1 Cache RAM	L1 cache size	None	Information only. Displays size in KB of the processor L1 Cache. Since L1 cache is not shared between cores, this is shown as the amount of L1 cache per core. There are two types of L1 cache, so this amount is the total of L1 Instruction Cache plus L1 Data Cache for each core.
L2 Cache RAM	L2 cache size	None	Information only. Displays size in KB of the processor L2 Cache. Since L2 cache is not shared between cores, this is shown as the amount of L2 cache per core.
L3 Cache RAM	L3 cache size	None	Information only. Displays size in MB of the processor L3 Cache. Since L3 cache is shared between all cores in a processor package, this is shown as the total amount of L3 cache per processor package.
Processor 1 Version	ID string from processor	None	Information only. Displays Brand ID string of processor with CPUID instruction.
Intel® Turbo Boost Technology	**Enabled** Disabled	Intel® Turbo Boost Technology allows the processor to automatically increase its frequency if it is running below power, temperature, and current specifications.	This option is only visible if the processor in the system support Intel® Turbo Boost Technology. In order for this option to be available, Enhanced Intel® SpeedStep® Technology must be Enabled.
Enhanced Intel SpeedStep® Technology	**Enabled** Disabled	Enhanced Intel SpeedStep® Technology allows the system to dynamically adjust processor voltage and core frequency, which can result in decreased average power consumption and decreased average heat production. Contact your OS vendor regarding OS support of this feature.	When Disabled, the processor setting reverts to running at Max TDP Core Frequency (rated frequency). This option is only visible if all processors installed in the system support Enhanced Intel® SpeedStep® Technology. In order for the Intel® Turbo Boost option to be available, Enhanced Intel® SpeedStep® Technology must be Enabled.
Processor C3	Enabled **Disabled**	Enable/Disable Processor C3 (ACPI C2/C3) report to OS	This is normally **Disabled,** but can be **Enabled** for improved performance on certain benchmarks and in certain situations.
Processor C6	**Enabled** Disabled	Enable/Disable Processor C6 (ACPI C3) report to OS	This is normally **Enabled** but can be **Disabled** for improved performance on certain benchmarks and in certain situations.

etup Item	Options	Help Text	Comments
Intel® Hyper-Threading Technology	**Enabled** Disabled	Intel® Hyper-Threading Technology allows multithreaded software applications to execute threads in parallel within each processor. Contact your OS vendor regarding OS support of this feature.	This option is only visible if all processors installed in the system support Intel® Hyper-Threading Technology.
Active Processor Cores	**All** 1 2 3 4 5 6 7	Number of cores to enable in each processor package.	e numbers of cores that appear as selections depends on the number of cores available in the processors installed. Boards may have as many as eight cores in each of 1, 2, or 4 processors. The same number of cores must be active in each processor package. This Setup screen should begin with the number of currently-active cores as the number displayed. See note below – this may be different from the number previously set by the user. **Note:** The ME can control the number of active cores independently of the BIOS Setup setting. If the ME disables or enables processor cores, that will override the BIOS setting, and the number selected by BIOS will be disregarded.
Execute Disable Bit	**Enabled** Disabled	Execute Disable Bit can help prevent certain classes of malicious buffer overflow attacks. Contact your OS vendor regarding OS support of this feature.	This option is only visible if all processors installed in the system support the Execute Disable Bit. The OS and applications installed must support this feature in order for it to be enabled.
Intel® Virtualization Technology	Enabled **Disabled**	Intel® Virtualization Technology allows a platform to run multiple operating systems and applications in independent partitions. Note: A change to this option requires the system to be powered off and then back on before the setting takes effect.	This option is only visible if all processors installed in the system support Intel® VT. The software configuration installed on the system must support this feature in order for it to be enabled.

etup Item	Options	Help Text	Comments
Intel® VT for Directed I/O	Enabled **Disabled**	Enable/Disable Intel® Virtualization Technology for Directed I/O. (Intel® VT-d) Report the I/O device assignment to VMM through DMAR ACPI Tables	This option is only visible if all processors installed in the system support Intel® VT-d. The software configuration installed on the system must support this feature in order for it to be enabled.
Interrupt Remapping	**Enabled** Disabled	Enable/Disable Intel® VT-d Interrupt Remapping support. For some processors, this option may be "always enabled".	This option only appears when Intel® Virtualization Technology for Directed I/O is Enabled. For some processors this will be enabled unconditionally whenever Intel® VT-d is enabled. In that case, this option will be shown as "Enabled", and grayed out and not changeable.
Coherency Support	Enabled **Disabled**	Enable/Disable Intel (R) VT-d Coherency support.	This option only appears when Intel® Virtualization Technology for Directed I/O is Enabled.
ATS Support	**Enabled** Disabled	Enable/Disable Intel (R) VT-d Address Translation Services (ATS) support.	This option only appears when Intel® Virtualization Technology for Directed I/O is Enabled.
Pass-through DMA Support	**Enabled** Disabled	Enable/Disable Intel (R) VT-d Pass-through DMA support. For some processors, this option may be "always enabled".	This option only appears when Intel® Virtualization Technology for Directed I/O is Enabled. For some processors this will be enabled unconditionally whenever Intel® VT-d is enabled. In that case, this option will be shown as "Enabled", and grayed out and not changeable.
Intel® TXT	Enabled **Disabled**	Enable/Disable Intel® Trusted Execution Technology. Takes effect after reboot.	Intel® TXT only appears with products and processors which has TXT support capability. This option is only available when both Intel® Virtualization Technology and Intel® VT for Directed IO are enabled and on models equipped with a TPM. The TPM must be active in order to support Intel® TXT. Changing the setting for Intel® TXT will require the system to perform a Hard Reset in order for the new setting to become effective.
Enhanced Error Containment Mode	Enabled **Disabled**	Enable Enhanced Error Containment Mode (Data Poisoning) - Erroneous data coming from memory will be poisoned. If disabled (default), will be in Legacy Mode - No data poisoning support available.	Enhanced Error Containment (Data Poisoning) is not supported by all models of processors, and this option will not appear unless all installed processors support Enhanced Error Containment. This option globally enables or disables both Core and Uncore Data Poisoning, for processors which support them

etup Item	Options	Help Text	Comments
MLC Streamer	**Enabled** Disabled	MLC Streamer is a speculative prefetch unit within the processor(s) **Note:** Modifying this setting may affect performance.	MLC Streamer is normally **Enabled**, for best efficiency in L2 Cache and Memory Channel use, but disabling it may improve performance for some processing loads and on certain benchmarks.
MLC Spatial Prefetcher	**Enabled** Disabled	[Enabled] – Fetches adjacent cache line (128 bytes) when required data is not currently in cache. [Disabled] – Only fetches cache line with data required by the processor (64 bytes).	MLC Spatial Prefetcher is normally **Enabled**, for best efficiency in L2 Cache and Memory Channel use, but disabling it may improve performance for some processing loads and on certain benchmarks.
DCU Data Prefetcher	**Enabled** Disabled	[Enabled] The next cache line will be prefetched into L1 data cache from L2 or system memory during unused cycles if it sees that the processor core has accessed several bytes sequentially in a cache line as data. [Disabled] – Only fetches cache line with data required by the processor (64 bytes).	DCU Data Prefetcher is normally **Enabled**, for best efficiency in L1 Data Cache and Memory Channel use, but disabling it may improve performance for some processing loads and on certain benchmarks.
DCU Instruction Prefetcher	**Enabled** Disabled	The next cache line will be prefetched into L1 instruction cache from L2 or system memory during unused cycles if it sees that the processor core has accessed several bytes sequentially in a cache line as data.	DCU Instruction Prefetcher is normally **Enabled**, for best efficiency in L1 I Cache and Memory Channel use, but disabling it may improve performance for some processing loads and on certain benchmarks.
Direct Cache Access (DCA)	**Enabled** Disabled	Allows processors to increase the I/O performance by placing data from I/O devices directly into the processor cache.	System performance is usually best with Direct Cache Access Enabled. In certain unusual cases, disabling this may give improved results.
Extended ATR	**0x03** 0x01	Extended Timeout value for PCIe tuning. 0x03 = default timeout. 0x01 = extended timeout.	Adjust ATR value to PCIe performance improvement.
PFloor tuning	Entry Field maximum Non-Turbo Frequency - 3 of installed Processors – 12, **12** is default	Adjustment of CPU idle frequency for PCIe Bus tuning between 12 and 3 less than CPU rated frequency	Adjustment of CPU idle frequency for PCIe performance tuning.

etup Item	Options	Help Text	Comments
SMM Wait Timeout	Entry Field 20 – 3000ms, **20** is default	Millisecond timeout waiting for BSP and APs to enter SMM. Range is 20ms to 3000ms	Amount of time to allow for the SMI Handler to respond to an SMI. If exceeded, BMC generates an SMI Timeout and resets the system **Note:** This field is temporary, and will be removed when no longer required.

5.4.2.5 Power and Performance policy

The Power and Performance screen allows the user to specify a profile which is optimized in the direction of either reduced power consumption or increased performance.

To access this screen from the Main screen, select Advanced > Power and Performance. To move to another screen, press the <Esc> key to return to the Advanced screen, then select the desired screen.

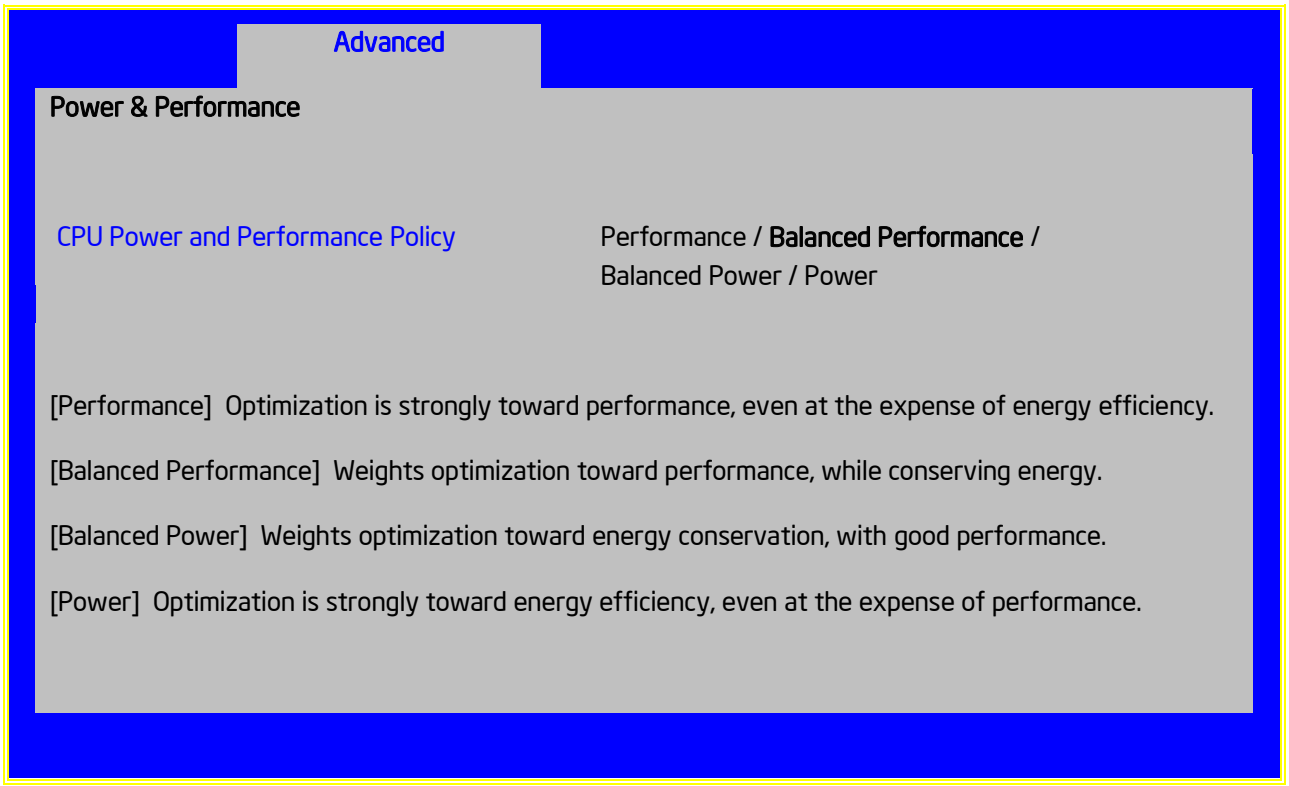


Figure 22. Power and Performance Configuration Screen

Table 31. Setup Utility – Power and Performance Configuration Screen Fields

Setup Item	Options	Help Text	Comments

Setup Item	Options	Help Text	Comments
CPU Power and Performance Policy	Performance **Balanced Performance** Balanced Power Power	Allows the user to set an overall power and performance policy for the system, and when changed will modify a selected list of options to achieve the policy. These options are still changeable outside of the policy but do reflect the changes that the policy makes when a new policy is selected.	Choosing one of these four Power and Performance Profiles implements a number of changes in BIOS settings, both visible settings in the Setup screens and non-visible internal settings. For detailed lists of settings affected by each profile, see Table 32.

When the user selects a “Power and Performance Policy” in Setup, there is a list of complementary settings which are made. These can be individually overridden after the policy setting has been selected and the profile settings performed. The profile settings are listed in the following table.

Table 32. Power/Performance Profiles

BIOS Features	Available Settings	Performance	Balanced Performance	Balanced Power	Power
Setup: Advanced > Power and Performance					
CPU Power and Performance Policy	Performance /**Balanced Performance** /Balanced Power /Power	Performance	(Balanced Performance)	Balanced Power	Power
Setup: Advanced > Processor Configuration					
Intel® QPI Frequency Select	**Auto Max** /6.4 GT/s /7.2 GT/s /8.0 GT/s	(Auto Max)	(Auto Max)	(Auto Max)	6.4 GT/s
Intel® Turbo Boost Technology	**Enabled**/Disabled	(Enabled)	(Enabled)	(Enabled)	(Enabled)
Enhanced Intel® SpeedStep® Technology	**Enabled**/Disabled	(Enabled)	(Enabled)	(Enabled)	(Enabled)
Processor C3	Enabled/**Disabled**	(Disabled)	(Disabled)	(Disabled)	(Disabled)
Processor C6	**Enabled**/Disabled	(Enabled)	(Enabled)	(Enabled)	(Enabled)
Intel® Hyper Threading	**Enabled**/Disabled	(Enabled)	(Enabled)	(Enabled)	(Enabled)

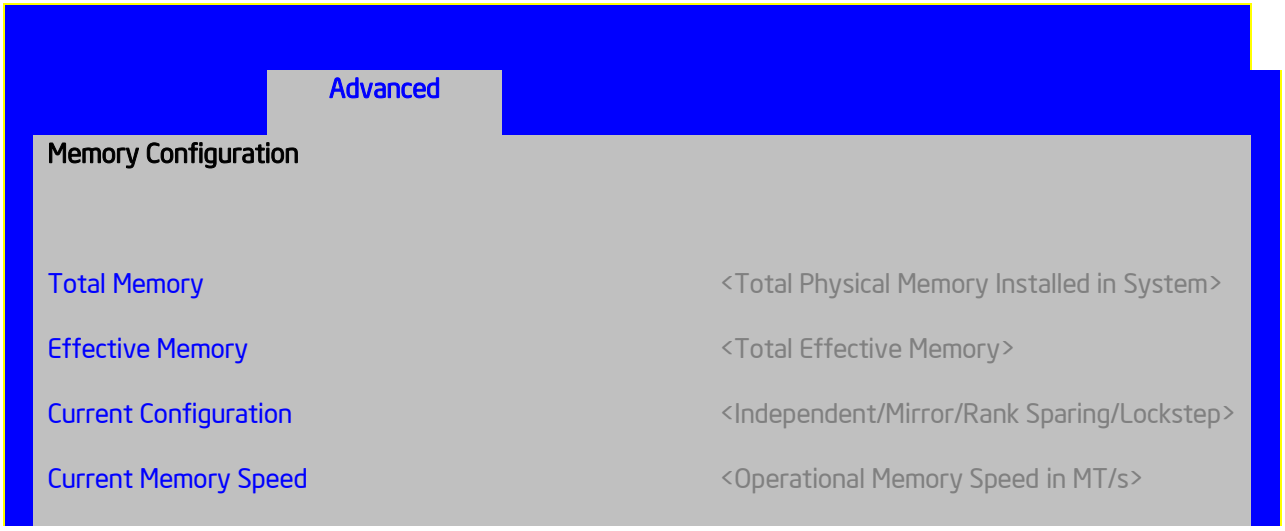
BIOS Features	Available Settings	Performance	Balanced Performance	Balanced Power	Power
Active Processor Cores	**All**/1/2/3/4/5/6/7	(All)	(All)	(All)	(All)
MLC Streamer	**Enabled**/Disabled	(Enabled)	(Enabled)	(Enabled)	(Enabled)
MLC Spatial Prefetcher	**Enabled**/Disabled	(Enabled)	(Enabled)	(Enabled)	(Enabled)
DCU Data Prefetcher	**Enabled**/Disabled	(Enabled)	(Enabled)	(Enabled)	(Enabled)
DCU Instruction Prefetcher	**Enabled**/Disabled	(Enabled)	(Enabled)	(Enabled)	(Enabled)
Direct Cache Access (DCA)	**Enabled**/Disabled	(Enabled)	(Enabled)	(Enabled)	(Enabled)
Setup: Advanced > Memory Configuration					
Memory Operating Speed Selection	**Auto**/800/1067 /1333/1600	(Auto)	(Auto)	(Auto)	(Auto)
Patrol Scrub	**Enabled**/Disabled	(Enabled)	(Enabled)	(Enabled)	(Enabled)
Demand Scrub	**Enabled**/Disabled	(Enabled)	(Enabled)	(Enabled)	(Enabled)
Setup: Advanced > System Acoustic and Performance Configuration					
Set Throttling Mode	**Auto**/DCLTT /SCLTT/SOLTT	(Auto)	(Auto)	(Auto)	(Auto)
Set Fan Profile	**Performance** /Acoustic	(Performance)	(Performance)	(Performance)	(Performance)
Quiet Fan Idle Mode	Enabled/**Disabled**	(Disabled)	(Disabled)	(Disabled)	(Disabled)
Setup: Server Management					
EuP LOT6 OFF-Mode	Enabled/**Disabled**	(Disabled)	(Disabled)	(Disabled)	(Disabled)
Internal BIOS Settings not displayed in BIOS Setup					
QPI Link L0S enable	**Auto**/Enabled /Disabled	Disabled	(Auto)	(Auto)	(Auto)
CKE Throttling	**Auto**/Enabled /Disabled	Disabled	(Auto)	(Auto)	Enabled
Memory Voltage	**Auto**/1.5V/1.35V	1.5v	(Auto)	(Auto)	(Auto)

BIOS Features	Available Settings	Performance	Balanced Performance	Balanced Power	Power
CPU PkgC State Limit	Disabled/C6 with no retention/**C6 with retention**	Disabled	(C6 with retention)	(C6 with retention)	(C6 with retention)
Processor C1 mapped to ACPI C1	**Enabled**/Disabled	(Enabled)	(Enabled)	(Enabled)	(Enabled)
Processor C6 with retention mapped to ACPI C2	**Enabled**/Disabled	(Enabled)	(Enabled)	(Enabled)	(Enabled)
ACPI C3	Enabled/**Disabled**	(Disabled)	(Disabled)	(Disabled)	(Disabled)
Processor C1/C3 Auto Demotion	**Enabled**/Disabled	(Enabled)	(Enabled)	(Enabled)	(Enabled)
Processor C1/C3 UnDemotion	**Enabled**/Disabled	(Enabled)	(Enabled)	(Enabled)	(Enabled)
ENERGY_PERF_BIAS mode	Performance/**Balanced Performance**/Balanced Power/Power	Performance	(Balanced Performance)	Balanced Power	Power

5.4.2.6 Memory Configuration

The Memory Configuration screen allows the user to view details about the DDRIII DIMMs that are installed as system memory, and alter BIOS Memory Configuration settings where appropriate.

To access this screen from the **Main** screen, select **Advanced > Memory Configuration**. To move to another screen, press the <Esc> key to return to the **Advanced** screen, then select the desired screen.



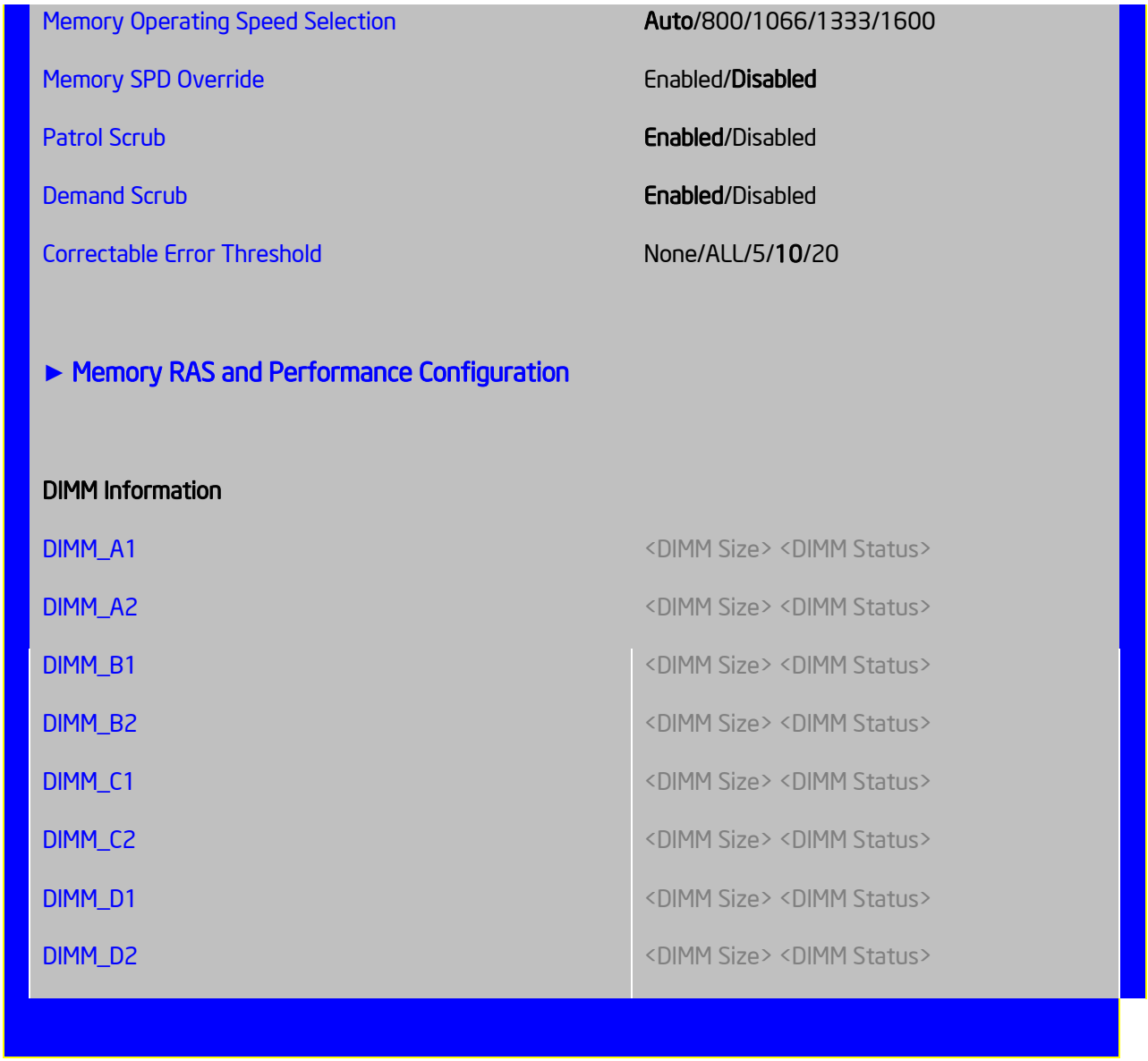


Figure 23. Memory Configuration Screen

Table 33. Setup Utility – Memory Configuration Screen Fields

Setup Item	Options	Help Text	Comments
Total Memory	Total Physical Memory installed in System	None	Information only. The amount of memory available in the system in the form of installed DDRIII DIMMs in units of GB.

Setup Item	Options	Help Text	Comments
Effective Memory	Total Effective Memory	None	Information only. Displays the amount of memory available to the OS in MB or GB. The Effective Memory is the Total Physical Memory minus the sum of all memory reserved for internal usage, RAS redundancy and SMRAM. **Note:** Some server operating systems do not display the total physical memory installed.
Current Configuration	Independent Channel Mirror Rank Sparing Lockstep	None	Information only: Displays one of the following: Independent Channel – DIMMs are operating in Independent Channel Mode, the default configuration when there is no RAS Mode configured. Mirror – Mirroring RAS Mode has been configured and is operational. Rank Sparing – Rank Sparing RAS Mode has been configured and is operational. Lockstep – Lockstep RAS Mode has been configured and is operational.
Current Memory Speed	Operational Memory Speed in MT/s	None	Information only. Displays the speed in MT/s at which the memory is currently running. The supported memory speeds are 800 MT/s, 1066 MT/s, 1333 MT/s, and 1600 MT/s. The actual memory speed capability depends on the memory configuration.
Memory Operating Speed Selection	**Auto** 800 1066 1333 1600	Force specific Memory Operating Speed or use Auto setting.	Allows the user to select a specific speed at which memory will operate. Only speeds that are legitimate are available, that is, the user can only specify speeds less than or equal to the auto-selected Memory Operating Speed. The default Auto setting will select the highest achievable Memory Operating Speed consistent with the DIMMs and processors installed.
Memory SPD Override	Enabled **Disabled**	When enabled, it extends the platform's capability to support higher Memory Frequency than the POR Settings; Disabling it keeps the POR settings.	None

Setup Item	Options	Help Text	Comments
Patrol Scrub	**Enabled** Disabled	When enabled, performs periodic checks on memory cells and proactively walks through populated memory space, to seek and correct soft ECC errors.	When enabled, Patrol Scrub is initialized to read through all of memory in a 24-hour period, correcting any Correctable ECC Errors it encounters by writing back the corrected data to memory.
Demand Scrub	**Enabled** Disabled	When enabled, executes when an ECC error is encountered during a normal read/write of data and corrects that data.	When enabled, Demand Scrub automatically corrects a Correctable ECC Error encountered during a fetch from memory by writing back the corrected data to memory.

Setup Item	Options	Help Text	Comments
Correctable Error Threshold	None All 5 **10** 20	Threshold value for logging Correctable Errors (CE) – Threshold of 10 (default) logs 10th CE, "All" logs every CE and “None”’ means no CE logging. All and None are not valid with Rank Sparing.	Specifies how many Correctable Errors must occur before triggering the logging of a SEL Correctable Error Event. Only the first threshold crossing is logged, unless “All” is selected. “All” causes every CE that occurs to be logged. “None” suppresses CE logging completely. When Rank Sparing RAS Mode is configured, “All” and “None” are not valid, so they will not be presented as choices. This threshold is applied on a per-rank basis. The Correctable Error occurrences are counted for each memory rank. When any one rank accumulates a CE count equal to the CE Threshold, then a single CE SEL Event is logged, and all further CE logging is suppressed. Note that the CE counts are subject to a “leaky bucket” mechanism that reduces the count as a function of time, to keep from accumulating counts unnecessarily over the term of a long operational run. This is also the Correctable Error threshold used when Rank Sparing RAS Mode is configured. When a CE threshold crossing occurs in Rank Sparing Mode on a channel which is in Redundant state, it causes a Sparing Fail Over (SFO) event to occur. That threshold crossing will also be logged as a Correctable Error event if it is the first to occur on the system. An SFO event causes the rank with the error to be replaced by the spare rank for that channel and the channel goes to a non-redundant state (with a “Redundancy Degraded” SEL Event logged). There may be an SFO for each channel in the system, although only the first one can be logged as a CE event.
Memory RAS and Performance Configuration	None	Configure memory RAS (Reliability, Availability, and Serviceability) and view current memory performance information and settings.	Selection only. Select this line and press the <Enter> key to go to the Memory RAS and Performance Configuration group of configuration settings.

Setup Item	Options	Help Text	Comments
DIMM_ XY	<DIMM Size> <DIMM Status> Where DIMM Size is: Size of DIMM in GB Where DIMM Status is: Installed and Operational Not Installed Failed/Disabled	None	Information only: Displays the status of each DIMM socket present on the board. There is one line for each DIMM socket present on the board. For each DIMM socket, the DIMM Status reflects one of the following three possible states: Installed and Operational – There is a DDRIII DIMM installed and operational in this slot. Not Installed – There is no DDRIII DIMM installed in this slot. Failed/Disabled – The DIMM installed in this slot has failed during initialization and/or was disabled during initialization. For each DIMM that is in the Installed & Operational state, the DIMM Size in GB of that DIMM is displayed. This is the physical size of the DIMM, regardless of how it is counted in the Effective Memory size.

5.4.2.7 Memory RAS and Performance Configuration

The Memory RAS and Performance Configuration screen allows the user to customize several memory configuration options, such as whether to use Memory Mirroring or Memory Sparing.

To access this screen from the **Main** screen, select **Advanced > Memory Configuration > Memory RAS and Performance Configuration**. To move to another screen, press the <Esc> key to return to the **Memory Configuration** screen, if necessary press the <Esc> key again to return to the **Advanced** screen, then select the desired screen.

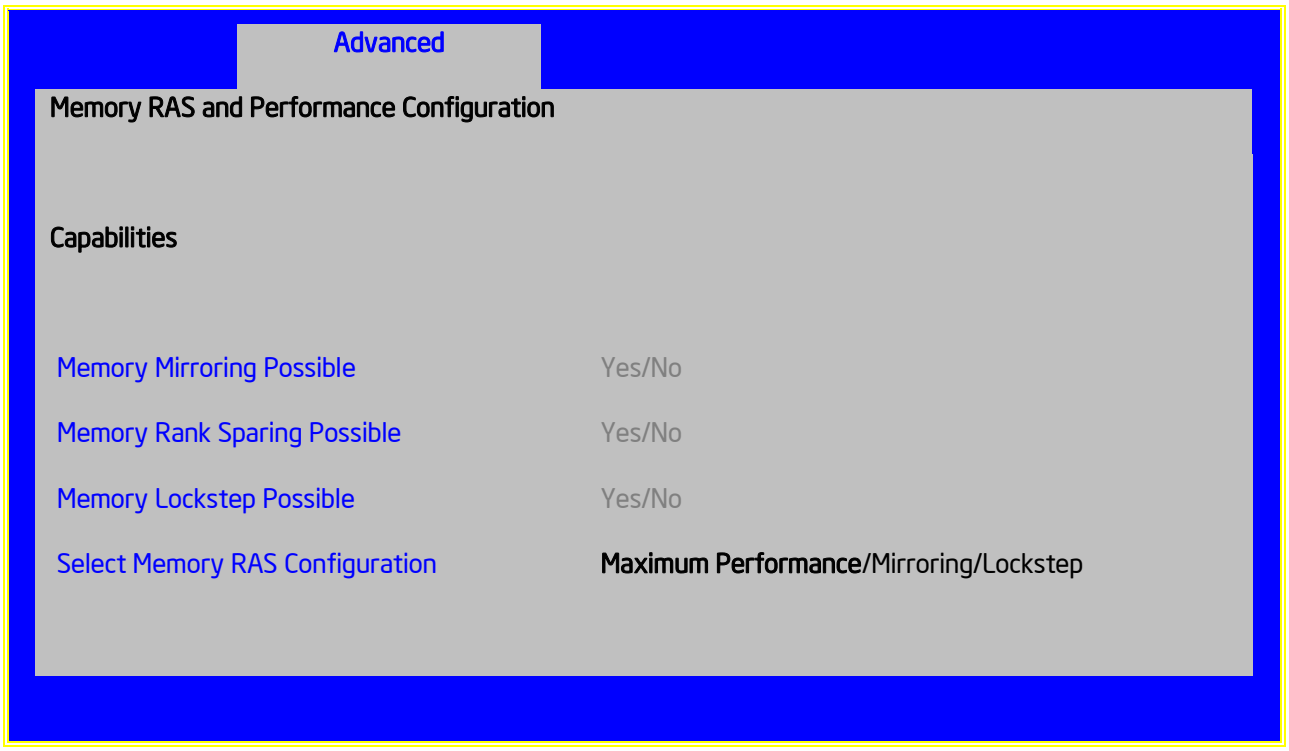


Figure 24. Memory RAS and Performance Configuration Screen

Table 34. Setup Utility – Memory RAS and Performance Configuration Fields

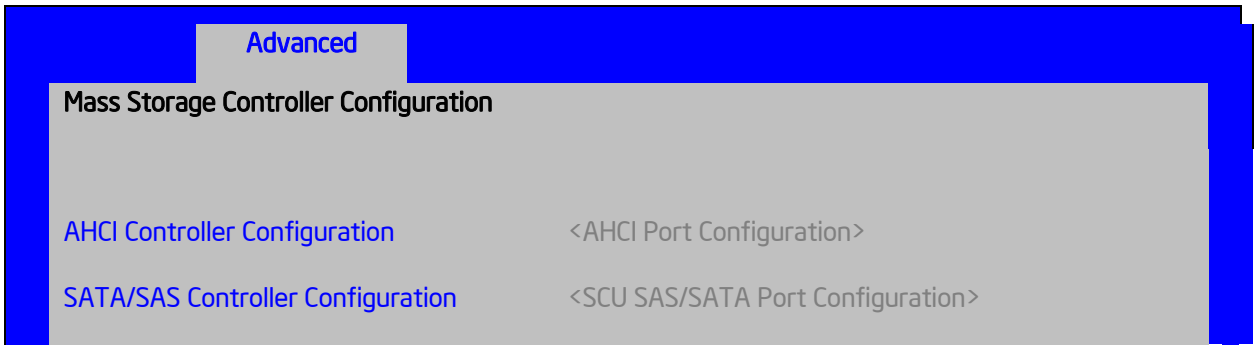
Setup Item	Options	Help Text	Comments
Memory Mirroring Possible	Yes No	None	Information only. Displays whether the current DIMM configuration is capable of Memory Mirroring. For Memory Mirroring to be possible, DIMM configurations on all paired channels must be identical between the channel pair (Mirroring Domain).
Memory Rank Sparing Possible	Yes No	None	Information only. Displays whether the current DIMM configuration is capable of Rank Sparing. For Rank Sparing to be possible, DIMM configurations on all channels must be capable of supporting Rank Sparing. **Note:** The Correctable Error Threshold value is also the Sparing Fail Over threshold value. Threshold values of “All” or “None” are not valid for Rank Sparing. If the Correctable Error Threshold is set to either of those values, Rank Spring will not be possible.

Setup Item	Options	Help Text	Comments
Memory Lockstep Possible	Yes No	None	Information only. Displays whether the current DIMM configuration is capable of Memory Lockstep. For Memory Lockstep to be possible, DIMM configurations on all paired channels must be identical between the channel pair.
Select Memory RAS Configuration	Maximum Performance Mirroring Rank Sparing Lockstep	Allows the user to select the memory RAS Configuration to be applied for the next boot.	Available modes depend on the current memory population. Modes which are not listed as "possible" should not be available as choices. If the only valid choice is "Maximum Performance", then this option should be grayed out and unavailable. Maximum Performance – (default) no RAS but best memory utilization since full amount of memory is available; operating in Independent Channel Mode. Mirroring - most reliability by using half of memory as a mirror image; can survive an Uncorrectable ECC Error. Rank Sparing – offers reliability by reserving spare ranks to replace failing ranks which are generating excessive Correctable ECC Errors. Lockstep – allows SDDC capability with x8 DIMMs installed. No memory size impact but does have a performance and power penalty. **Note:** since only RAS Modes which are listed as "possible" are available for selection, it is not possible to select a RAS Mode without first installing an appropriate DIMM configuration.

5.4.2.8 Mass Storage Controller Configuration

The Mass Storage Configuration screen allows the user to configure the Mass Storage controllers that are integrated into the server board on which the BIOS is executing.

To access this screen from the **Main** screen, select **Advanced** > **Mass Storage Controller Configuration**. To move to another screen, press the <Esc> key to return to the **Advanced** screen, then select the desired screen.



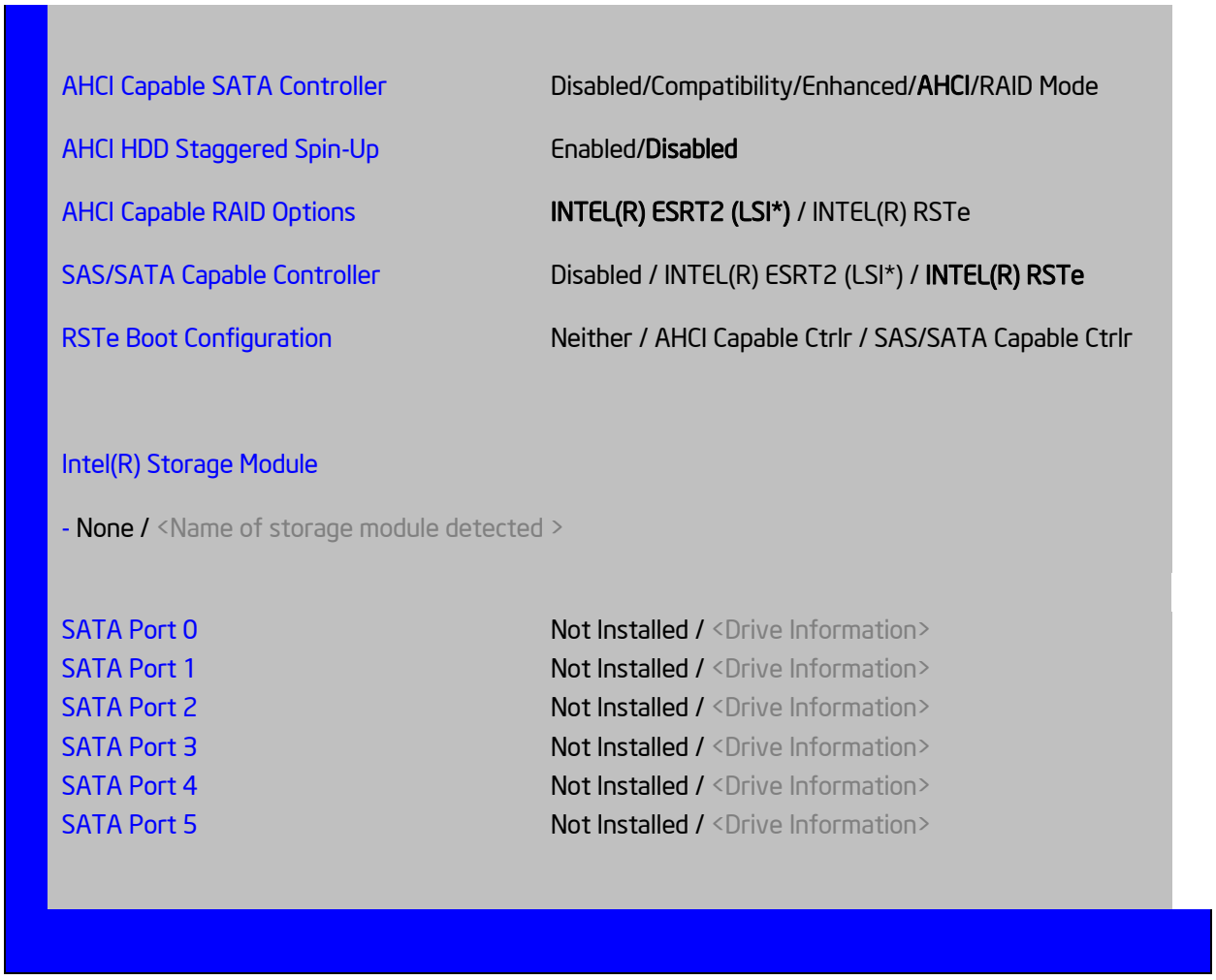


Figure 25. Mass Storage Controller Configuration Screen

Table 35. Mass Storage Controller Configuration Fields

Setup Item	Options	Help Text	Comments
AHCI Controller Configuration	AHCI Port Configuration	None	Information only. This is a display showing which ports are available through the onboard AHCI capable SATA controller, if the controller is enabled.
SATA/SAS Controller Configuration	SCU SAS/SATA Port Configuration	None	Information only. This is a display showing the number of ports which are available through the SCU controller, and whether they are configured for SATA or SAS.

Setup Item	Options	Help Text	Comments
AHCI Capable SATA Controller	Disabled Compatibility Enhanced **AHCI** RAID Mode	- Compatibility provides PATA emulation on the SATA device. - Enhanced provides Native SATA support. - AHCI enables the Advanced Host Controller Interface, which provides Enhanced SATA functionality. - RAID Mode provides host based RAID support on the onboard SATA ports.	This option configures the onboard AHCI-capable SATA controller, which is distinct from the SCU. If the SATA Controller is Disabled, the SATA Ports will not operate, and any installed SATA devices will be unavailable. Compatibility provides PATA emulation on the SATA device, allowing the use of legacy IDE/PATA drivers. Enhanced provides Native SATA support using native SATA drivers included with the vast majority of current OSes. AHCI enables the Advanced Host Controller Interface, which provides Enhanced SATA functionality plus possible additional functionality (Native Command Queuing, Hot Plug, Staggered Spin Up). It uses AHCI drivers available for the majority of current OSes. RAID Mode provides host based RAID support on the onboard SATA ports. RAID levels supported and required drivers depend on the RAID stack selected
AHCI HDD Staggered Spin-Up	Enabled **Disabled**	If enabled for the AHCI Capable SATA controller, Staggered Spin-Up will be performed on drives attached to it. Otherwise these drives will all spin up at boot.	This option enables or disables Staggered Spin-up only for disk drives attached to ports on the AHCI Capable SATA Controller. Disk drives attached to SATA/SAS ports on the Storage Control Unit are controlled by a different method for Staggered Spin-Up and this option does not affect them. This option is only visible when the SATA Controller is enabled and AHCI or RAID has been selected as the operational SATA Mode.
AHCI Capable RAID Options	**Intel® ESRT2 (LSI*)** Intel® RSTe	- Intel® ESRT2 (Powered By LSI*): Supports RAID 0/1/10 and optional RAID 5 with Intel® RAID C600 Upgrade Keys. Uses Intel® ESRT2 drivers (based on LSI* MegaSR). - Intel® RSTe: Provides pass-through drive support. Also provides host based RAID 0/1/10/5 support. Uses Intel® RSTe iastor drivers.	This option only appears when the SATA Controller is enabled, and RAID Mode has been selected as the operational SATA Mode. This setting selects the RAID stack to be used for SATA RAID with the onboard AHCI SATA controller. If a RAID Volume has not previously been created that is compatible with the RAID stack selected, it will be necessary to Save and Exit and reboot in order to create a RAID Volume.

Setup Item	Options	Help Text	Comments
SAS/SATA Capable Controller	Disabled Intel® ESRT2 (LSI*) **Intel® RSTe**	- Intel® ESRT2: Provides host based RAID 0/1/10 and optional RAID 5. Uses Intel®ESRT2 drivers (based on LSI* MegaSR). - Intel® RSTe: Provides pass-through drive support. Also provides host based RAID 0/1/10 support, and RAID 5 (in SATA mode only). Uses Intel® RSTe iastor drivers.	This option selects the RAID stack to be used with the SCU. If Disabled is selected, any drives connected to the SCU will not be usable. Intel® ESRT2 provides host based RAID 0/1/10 and optional RAID 5. For a RAID 5 configuration, this requires one of the Intel® RAID C600 Upgrade Keys uses Intel® ESRT2 drivers (based on LSI* MegaSR), and is also supported by Linux MDRAID*. Intel® RSTe provides pass-through drive support and provides host based RAID 0/1/10 support, and RAID 5 (in SATA mode only). Uses Intel® RSTe drivers in Windows*, and MDRAID stack in Linux*. The Intel® RSTe RAID stack is required if it is necessary to provide pass-through support for non-RAID drives, or if support is needed for more than eight drives.
RSTe Boot Configuration	Neither **AHCI Capable Ctrlr** SAS/SATA Capable Ctrlr	This selects the device that will support Bootable Drives, whether they are in RAID arrays or individual pass-through SAS/SATA drives. Once selected and set up (if necessary), individual bootable devices will be listed in the Bootable Devices menu display.	This option appears only when Intel® RSTe has been selected as the operational mode on both the AHCI and SCU controllers. In that case there is a conflict and only one controller can be selected as having bootable drives attached. Once selected and set up (if necessary), individual bootable logical or physical drives available on the selected controller will be listed in the Bootable Devices menu display. If only one device selects RSTe, it will be available as a boot device along with any other devices – this option is only necessary to distinguish between which the RSTe device runs the Option ROM instance. BIOS is required to designate the OPROM for the boot device selected here. Two iterations of the OPROM cannot fully load simultaneously, and the version fully loaded will only show devices connected to the given controller, so the OPROM load order is based on BIOS selecting the correct device. **Note:** If RSTe is selected, then only one CONTROLLER can be bootable, so there will be situations where the boot drive *OR* an optical device will be bootable but not both.

Setup Item	Options	Help Text	Comments
Intel® Storage Module	Name of Storage Module detected	None	Information Only. If no Intel® Storage Module is detected, then None is displayed. This shows the customer the product name of the module installed, which helps in identifying drivers, support, documentation, and so on.
SATA Port x	**Not Installed** Drive Information	None	Information only. The Drive Information, when present, will typically consist of the drive model identification and size for the disk drive installed on a particular port.

5.4.2.9 PCI Configuration

The PCI Configuration screen allows the user to configure the PCI memory space used for onboard and add-in adapters, configure video options, and configure onboard adapter options. It also displays the NIC MAC Addresses currently in use.

To access this screen from the **Main** screen, select **Advanced > PCI Configuration**. To move to another screen, press the <Esc> key to return to the **Advanced** screen, then select the desired screen.

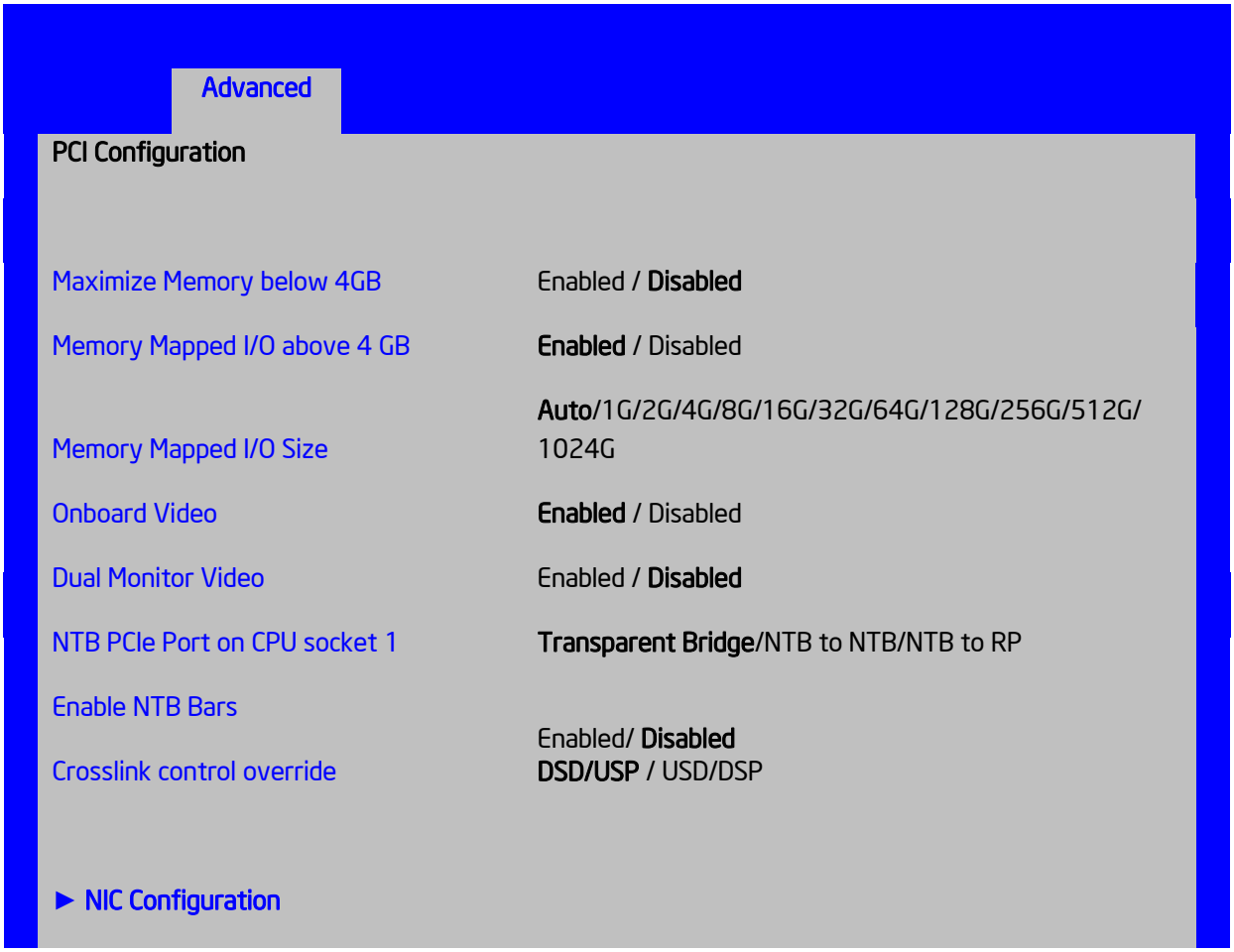


Figure 26. PCI Configuration Screen

Table 36. Setup Utility – PCI Configuration Screen Fields

Setup Item	Options	Help Text	Comments
Maximize Memory below 4GB	Enabled **Disabled**	BIOS maximizes memory usage below 4GB for an OS without PAE support, depending on the system configuration. Only enable for an OS without PAE support.	When this option is enabled, BIOS makes as much memory available as possible in the 32-bit (4GB) address space by limiting the amount of PCI/PCIe Memory Address Space and PCIe Extended Configuration Space to 64 buses rather than the standard 256 buses. This is done using the Bus Number limiting features offered by the processor and PCH and a variably sized Memory Mapped I/O region for the PCI Express functions This option should only be enabled for a 32-bit OS without PAE capability or without PAE enabled.
Memory Mapped I/O above 4GB	**Enabled** Disabled	Enable or disable memory mapped I/O of 64-bit PCI devices to 4 GB or greater address space.	When enabled, PCI/PCIe Memory Mapped I/O for devices capable of 64-bit addressing is allocated to address space above 4GB, in order to allow larger allocations and avoid impacting address space below 4GB.
Memory Mapped I/O Size	**Auto**/1G/2G/ 4G/8G/16/32G /64G/128G/ 256G/512G /1024G	Sets MMIO Size: Auto -> 2G(default).	When Memory Mapped I/O above 4GB option enabled, this option sets the preserved MMIO size as PCI/PCIe Memory Mapped I/O for devices capable of 64-bit addressing. This option is grayed out when Memory Mapped I/O above 4GB option is disabled.
Onboard Video	**Enabled** Disabled	Onboard video controller. Warning: System video is completely disabled if this option is disabled and an add-in video adapter is not installed.	When disabled, the system requires an add-in video card for the video to be seen. When there is no add-in video card installed, Onboard Video is set to Enabled and grayed out so it cannot be changed.

Setup Item	Options	Help Text	Comments
Dual Monitor Video	Enabled **Disabled**	If enabled, both the onboard video controller and an add-in video adapter are enabled for system video. The onboard video controller becomes the primary video device.	This option must be enabled to use an add-in card as a secondary POST Legacy Video device while also displaying on the Onboard Video device. If there is no add-in video card in any PCIe slot connected to CPU Socket 1, this option is set to *Disabled* and grayed out and unavailable.
NTB PCIe Port on CPU Socket 1	**Transparent Bridge/** NTB to NTB/NTB to RP	Configures port as TB, NTB-NTB, or NTB-RP.	This option selects the configuration mode of PCI Express Port 3A to support NTB configuration.
Enable NTB Bars	**Disabled** Enabled	If disabled, BIOS will not program NTB BAR size registers.	This option allow BIOS to program NTB BAR registers with default values when Enabled. If disabled, BIOS will not program NTB BARs registers and the task is left to drivers. This option only appears when NTB PCIe Port on CPU socket1 is not configured as 'Transparent Bridge'.
Crosslink control override	**DSD/USP** USD/DSP	Configure NTB port as DSP/USP, USD/DSP, or use external pins.	This option configures the Crosslink configuration of the NTB port. This option only appears when NTB PCIe Port on CPU socket1 is not configured as 'Transparent Bridge'.
NIC Configuration	None	View/Configure NIC information and settings	Selection only. Select this line and press the <Enter> key to go to the NIC Configuration group of configuration settings.
PCIe Port Oprom Contorl	None	View/Configure PCIe Port Oprom control settings.	Selection only. Select this line and press the <Enter> key to go to the PCIe Port Oprom Control Configuration group of configuration settings.

5.4.2.10 NIC Configuration

The NIC Configuration screen allows the user to configure on board NIC port1, port2, port3, and port4.

PXE 1GbE Option ROM	**Enabled** / Disabled
PXE 10GbE Option ROM	**Enabled** / Disabled
FCoE 10GbE Option ROM	Enabled / **Disabled**
iSCSI 1GbE/10GbE Option ROM	Enabled / **Disabled**
Onboard NIC1 Type	<Onboard NIC Description – Non-InfiniBand*>
NIC1 Controller	**Enabled** / Disabled
NIC1 Port1	**Enabled** / Disabled
NIC1 Port2	**Enabled** / Disabled
NIC1 Port3	**Enabled** / Disabled
NIC1 Port4	**Enabled** / Disabled
NIC1 Port1 PXE	**Enabled** / Disabled
NIC1 Port2 PXE	**Enabled** / Disabled
NIC1 Port3 PXE	**Enabled** / Disabled
NIC1 Port4 PXE	**Enabled** / Disabled
NIC1 Port1 MAC Address	<MAC Address display>
NIC1 Port2 MAC Address	<MAC Address display >
NIC1 Port3 MAC Address	<MAC Address display >
NIC1 Port4 MAC Address	<MAC Address display >
IO Module 1 Type	<IO Module Description – Non-InfiniBand*>
IOM1 Port1 PXE	**Enabled** / Disabled
IOM1 Port2 PXE	**Enabled** / Disabled
IOM1 Port3 PXE	**Enabled** / Disabled
IOM1 Port4 PXE	**Enabled** / Disabled

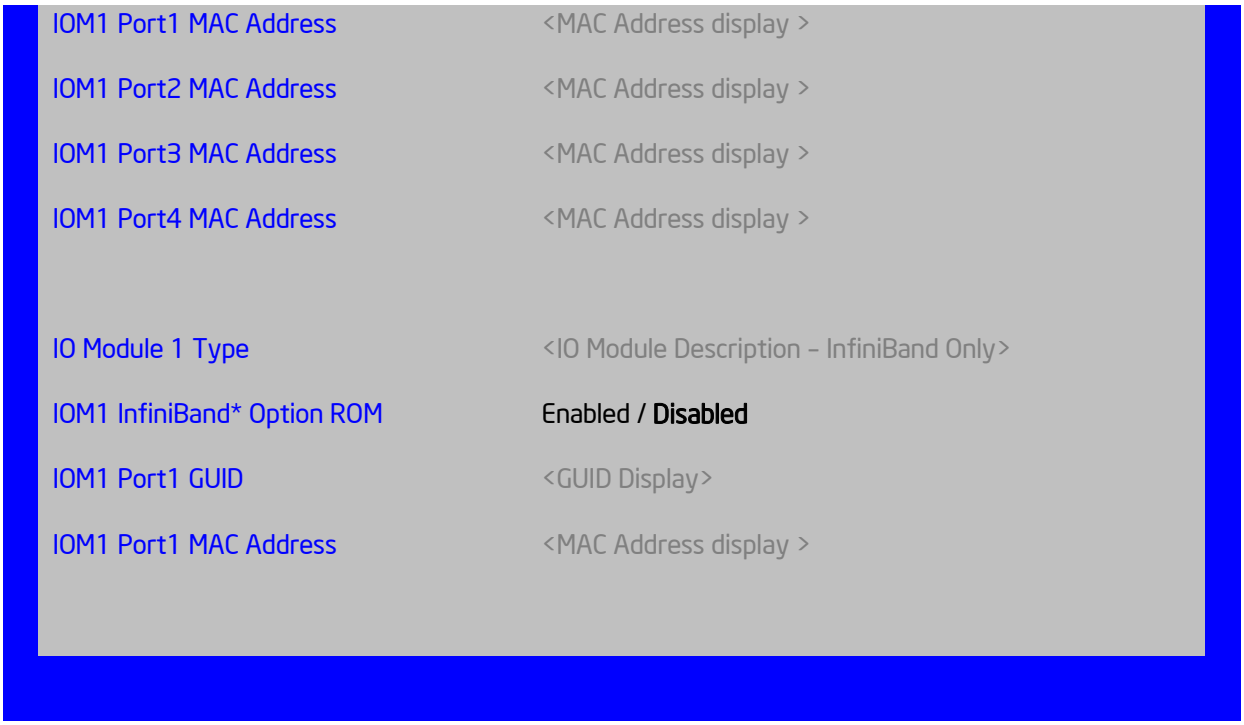


Figure 27. NIC Configuration Screen

Table 37. Setup Utility – NIC Configuration Screen Fields

Setup Item	Options	Help Text	Comments
Wake on LAN (PME)	**Enabled** Disabled	Enables or disables PCI PME function for Wake on LAN capability from LAN adapters.	Enables/disables PCI/PCIe PME# signal to generate Power Management Events (PME) and ACPI Table entries required for Wake on LAN (WOL). However, note that this will enable WOL only with an ACPI-capable Operating System which has the WOL function enabled.

Setup Item	Options	Help Text	Comments
PXE 1GbE Option ROM	**Enabled** Disabled	Enable/Disable Onboard/IOM NIC PXE Option ROM Load.	This selection is to enable/disable the 1GbE PXE Option ROM that is used by all Onboard and IO Module 1 GbE controllers. This option is grayed out and not accessible if the iSCSI Option ROM is enabled. It can co-exist with the 10 GbE PXE Option ROM, the 10 GbE FCoE Option ROM, or with an InfiniBand* controller Option ROM. If the 1GbE PXE Option ROM is disabled, and no other Option ROM is enabled, the system cannot perform a Network Boot and cannot respond for Wake-on-LAN. This 1GbE PXE option does not appear unless there is a 1 GbE NIC installed in the system as an Onboard or IO Module NIC.
PXE 10GbE Option ROM	**Enabled** Disabled	Enable/Disable Onboard/IOM NIC PXE Option ROM Load.	This selection is to enable/disable the 10GbE PXE Option ROM that is used by all Onboard and IO Module 10 GbE controllers. This option is grayed out and not accessible if the iSCSI Option ROM is enabled or the 10 GbE FCoE Option ROM is enabled. It can co-exist with the 1 GbE PXE Option ROM or with an InfiniBand* controller Option ROM. If the 10GbE PXE Option ROM is disabled, and no other Option ROM is enabled, the system cannot perform a Network Boot and cannot respond for Wake-on-LAN. This 10GbE PXE option does not appear unless there is a 10 GbE NIC installed in the system as an Onboard or IO Module NIC.
FCoE 10GbE Option ROM	Enabled **Disabled**	Enable/Disable Onboard/IOM NIC FCoE Option ROM Load.	This selection is to enable/disable the 10GbE FCoE Option ROM that is used by all Onboard and IO Module 10 GbE controllers capable of FCoE support. At the present time, only the Intel® 82599 10 Gigabit SFP+ NIC supports FCoE for this family of server boards. This option is grayed out and not accessible if the 10GbE PXE Option ROM is enabled or if the iSCSI Option ROM is enabled. It can co-exist with the 1GbE PXE Option ROM or with an InfiniBand* controller Option ROM. If the FCoE Option ROM is disabled, and no other Option ROM is enabled, the system cannot perform a Network Boot and cannot respond for Wake-on-LAN. This FCoE option does not appear unless there is a FCoE-capable 10GbE NIC installed in the system as an Onboard or IO Module NIC.

Setup Item	Options	Help Text	Comments
iSCSI 1GbE/10GbE Option ROM	Enabled **Disabled**	Enable/Disable Onboard/IOM NIC iSCSI Option ROM Load.	This selection is to enable/disable the iSCSI Option ROM that is used by all Onboard and IO Module 1 GbE and 10 GbE controllers. This option is grayed out and not accessible if the 1 GbE or 10GbE PXE Option ROM is enabled or if the 10 GbE FCoE Option ROM is enabled. It can co-exist with an InfiniBand* controller Option ROM. If the iSCSI Option ROM is disabled, and no other Option ROM is enabled, the system cannot perform a Network Boot and cannot respond for Wake-on-LAN. This iSCSI option does not appear unless there is an iSCSI -capable NIC installed in the system as an Onboard or IO Module NIC.
Onboard NIC1 Type	Onboard NIC Description	None.	rmation only. This is a display showing which NIC is available as Network Controllers integrated into the baseboard. Onboard NIC will be followed by a section including a group of options that are specific to the type of NIC.
NIC1 Controller	**Enabled** Disabled	Enable/Disable Onboard Network Controller.	This will completely disable Onboard Network Controller NIC1, along with all included NIC Ports and their associated options. That controller's NIC Ports, Port PXE options, and Port MAC Address displays will not appear. Ethernet controllers on IO Modules do not have a disabling function that can be controlled by BIOS, so there is no corresponding controller enable/disable option for an IOM Ethernet controller.
NIC1 Port x	**Enabled** Disabled	Enable/Disable NIC1 Port x	This will enable or disable Port <x, x = 1-4> of Onboard Network Controller 1, including associated Port PXE options. The NIC 1 Port x PXE option and MAC Address display will not appear when that port is disabled. The associated port enable/disable options will not appear when NIC 1 is disabled. Only ports which actually exist for a particular NIC will appear in this section. That is, Port1-Port4 will appear for a quad-port NIC, Port1-Port2 will appear for a dual-port NIC. Network controllers installed on an IO Module do not have a port disabling function that is controlled by BIOS, so there are no corresponding options for IO Module NICs.

Setup Item	Options	Help Text	Comments
NIC1 Port x PXE	Enable Disable	Enable/Disable NIC 1 Port x PXE Boot	This will enable or disable PXE Boot capability for Port<x, x = 1-4> of Onboard NIC 1. This option will not appear for ports on a NIC which is disabled, or for individual ports when the corresponding NIC Port is disabled. Only ports which actually exist for NIC1 will appear in this section. That is, Port1-Port4 will appear for a quad-port NIC, Port1-Port2 will appear for a dual-port NIC. The default state of each Port PXE Boot option is Enabled, if the corresponding PXE Boot OPROM of the same speed is Enabled. If a PXE Boot OPROM for 1 GbE or 10 GbE changes from Disabled to Enabled, then the Port PXE Boot option becomes Enabled for all ports of that speed. If the PXE Boot OPROM for1 GbE NICs or 10 GbE NICs is disabled, PXE Boot will be disabled and grayed out as unchangeable for all ports on NIC1 of that same speed. Conversely, if PXE Boot is disabled for all ports of a given speed, the corresponding PXE Option ROM will be disabled but not grayed out since it could be selected.
NIC 1 Port x MAC Address	Mac Address Display	None	Information only. 12 hex digits of the MAC address of Port<x, x = 1-4> of the NIC1. This display will appear only for ports which actually exist on the corresponding Network Controller. If the Network Controller or port is disabled, the port MAC Address will not appear.
IO Module 1 Type	IO Module Description	None	Information only. This is a display showing which Network Controllers on IO Modules are installed on the baseboard. Each of these IO Module NICs will be followed by a section including a group of options that are specific to the type of NIC, either as an Ethernet controller or an InfiniBand* controller. IO Module Type and following options section will only appear when an IO Module is installed,

Setup Item	Options	Help Text	Comments
IOM1 Portx PXE	**Enabled** Disabled	Enable/Disable IOM NIC Port PXE Boot	This will enable or disable PXE Boot capability for Port<x, x = 1-4> of IO Module 1. Only ports which actually exist for a particular IOM will appear in this section. That is, Port1-Port4 will appear for a quad-port NIC, Port1-Port2 will appear for a dual-port NIC, and only Port1 will appear for a single-port NIC. The default state of each Port PXE Boot option is Enabled, if the corresponding PXE Boot OPROM of the same speed is Enabled. If a PXE Boot OPROM for 1 GbE or 10 GbE changes from Disabled to Enabled, then the Port PXE Boot option becomes Enabled for all ports of that speed. If the PXE Boot OPROM for1 GbE NICs or 10 GbE NICs is disabled, PXE Boot will be disabled and grayed out as unchangeable for all ports on IO Modules of that same speed. Conversely, if PXE Boot is disabled for all ports of a given speed, the corresponding PXE Option ROM will be disabled but not grayed out since it could be selected.
IOM1 Portx MAC Address	Mac Address Display	None	Information only. 12 hex digits of the MAC address of Port1- Port4 of the IOM1.
IOM1 InfiniBand Option ROM	Enabled **Disabled**	Enable/Disable InfiniBand Controller Option ROM and FlexBoot.	This option will control whether the associated InfiniBand* Controller Option ROM is executed by BIOS during POST. This will also control whether the InfiniBand* controller FlexBoot program appears in the list of bootable devices. This option only appears for IO Module InfiniBand* controllers. It does not appear for Ethernet controllers.
IOM1 Port1 GUID	GUID Display	None	Information only. 16 hex digits of the Port1 GUID of the InfiniBand* controller for IOM1.

5.4.2.11 PCIe Port Oprom Control

The PCIe Root Port Expansion ROM configuration screen allows user to configure the Expansion ROM(Oprom) dispatching of the PCIe devices connected to the IIO PCIe root port during the BIOS POST.

To access this screen from the **Main** screen, select **Advanced > PCI Configuration > PCIe Port Oprom Contrl.** To move to another screen, press the <Esc> key to return to the **PCI Configuration** screen, if necessary press the <Esc> key again to return to the **Advanced** screen, then select the desired screen.

Figure 28 PCIe Port Oprom Control Screen

Table 38 Setup Utility – PCIe Port Oprom Control Screen Fields

Setup Item	Options	Help Text	Comments
PCIe Port xy OpROM control	**Enabled** Disabled	Enable or Disable Oprom dispatching of the PCIe Devices on this Root Port.	Disabling Oprom dispatching of the PCIe Devices on this Root Port will save the limited memory space for PCIe Oprom.

5.4.2.12 Serial Port Configuration

The Serial Port Configuration screen allows the user to configure the Serial A [COM 1]ports.

To access this screen from the **Main** screen, select **Advanced > Serial Port Configuration**. To move to another screen, press the <Esc> key to return to the **Advanced** screen, then select the desired screen.

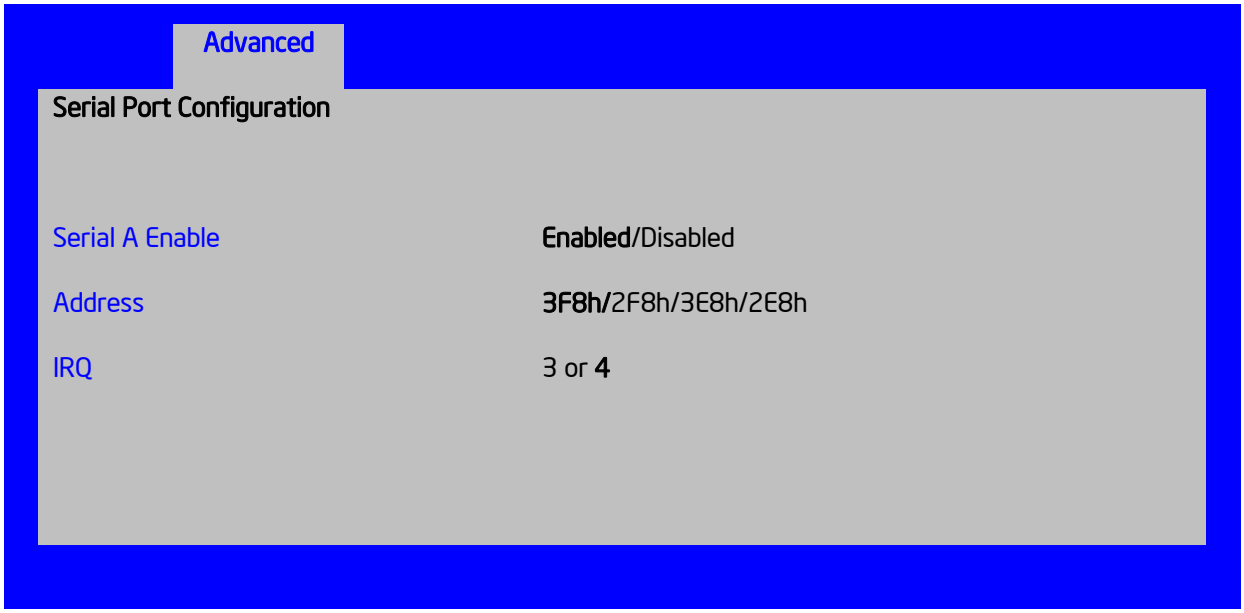


Figure 29. Serial Port Configuration Screen

Table 39. Setup Utility – Serial Ports Configuration Screen Fields

Setup Item	Options	Help Text	Comments
Serial A Enable	**Enabled** Disabled	Enable or Disable Serial port A.	Serial Port A can be used for either Serial Over LAN or Serial Console Redirection.
Address	**3F8h** 2F8h 3E8h 2E8h	Select Serial port A base I/O address.	Legacy I/O port address. This field should not appear when Serial A port enable/disable does not appear.
IRQ	3 **4**	Select Serial port A interrupt request (IRQ) line.	Legacy IRQ. This field should not appear when Serial A port enable/disable does not appear.

5.4.2.13 USB Configuration

The USB Configuration screen allows the user to configure the USB controller options.

To access this screen from the **Main** screen, select **Advanced > USB Configuration**. To move to another screen, press the <Esc> key to return to the **Advanced** screen, then select the desired screen.

Figure 30. USB Configuration Screen

Table 40. Setup Utility – USB Controller Configuration Screen Fields

Setup Item	Options	Help Text	Comments

Setup Item	Options	Help Text	Comments
Detected USB Devices	Number of USB devices detected in system	None	Information only. Displays the total number of USB devices of all types which have been detected in POST. **Note:** There is one USB keyboard and one USB mouse detected from the BMC KVM function under this item, even if no USB devices are connected to the system.
USB Controller	**Enabled** Disabled	[Enabled] - All onboard USB controllers are turned on and accessible by the OS. [Disabled] - All onboard USB controllers are turned off and inaccessible by the OS.	When the USB controllers are Disabled, there is no USB IO available for either POST or the OS. In that case, all following fields on this screen are grayed out and inactive.
Legacy USB Support	**Enabled** Disabled Auto	Enables Legacy USB support. AUTO option disables legacy support if no USB devices are connected. Disable option will only keep USB Keyboard devices available for EFI applications.	When Legacy USB Support is Disabled, USB devices are available only through OS drivers. If the USB controller setting is Disabled, this field is grayed out and inactive.
Port 60/64 Emulation	**Enabled** Disabled	Enables I/O port 60h/64h emulation support. This may be needed for legacy USB keyboard support when using an OS that is USB unaware.	If the USB controller setting is Disabled, this field is grayed out and inactive.
Make USB Devices Non-Bootable	**Enabled** Disabled	Exclude USB in Boot Table. [Enabled] - This removes all USB Mass Storage devices as Boot options. [Disabled] - This allows all USB Mass Storage devices as Boot options.	This is a security option. When Disabled, the system cannot be booted directly to a USB device of any kind. USB Mass Storage devices may still be used for data storage. If the USB controller setting is Disabled, this field is grayed out and inactive.

Setup Item	Options	Help Text	Comments
Device Reset timeout	10 seconds **20 seconds** 30 seconds 40 seconds	USB Mass Storage device Start Unit command timeout. Setting to a larger value provides more time for a mass storage device to be ready, if needed.	If the USB controller setting is Disabled, this field is grayed out and inactive.
Mass Storage Devices	**Auto** Floppy ForcedFDD Hard Disk CD-ROM	[Auto] - USB devices less than 530 MB are emulated as floppies. [Forced FDD] - HDD formatted drive is emulated as an FDD (For example, ZIP drive).	This field is hidden if no USB Mass Storage devices are detected. This setup screen can show a maximum of eight USB Mass Storage devices on the screen. If more than eight devices are installed in the system, the 'USB Devices Enabled' displays the correct count but only the first eight devices discovered are displayed in this list. If the USB controller setting is Disabled, this field is grayed out and inactive.

5.4.2.14 System Acoustic and Performance Configuration

The System Acoustic and Performance Configuration screen allows the user to configure the thermal control behavior of the system with respect to what parameters are used in the system's Fan Speed Control algorithms.

To access this screen from the **Main** screen, select **Advanced > System Acoustic and Performance Configuration**. To move to another screen, press the <Esc> key to return to the **Advanced** screen, then select the desired screen.

Figure 31. System Acoustic and Performance Configuration

Table 41. Setup Utility – System Acoustic and Performance Configuration Screen Fields

Setup Item	Options	Help Text	Comments
Set Throttling Mode	**Auto** DCLTT SCLTT SOLTT	Sets Thermal Throttling mode for memory, to control fans and DRAM power as needed to control DIMM temperatures. [Auto] –BIOS selects mode. [DCLTT] – Dynamic Closed Loop Thermal Throttling [SCLTT] – Static Closed Loop Thermal Throttling [SOLTT] – Static Open Loop Thermal Throttling	The Thermal Throttling Mode chosen reflects whether the DIMMs have Temperature Sensors (TSOD), and whether the chassis is an Intel chassis for which thermal data are available. Note that this is for thermal throttling only, independent of any controls imposed for the purpose of power limiting. DCLTT is the expected mode for a board in an Intel® chassis with inlet and outlet air temperature sensors and TSOD. The firmware can update the offset registers for closed loop during runtime, as BIOS sends the dynamic CLTT offset temperature data. SCLTT would be used with an OEM chassis and DIMMs with TSOD. The firmware does not change the offset registers for closed loop during runtime, although the Management Engine can do so. SOLTT is intended for a system with UDIMMs which do not have TSOD. The thermal control registers are configured during POST, and the firmware does not change them.
Altitude	300m or less **301m-900m** 901m-1500m Higher than 1500m	[300m or less] (980ft or less) Optimal performance setting near sea level. [301m - 900m] (980ft - 2950ft) Optimal performance setting at moderate elevation. [901m – 1500m] (2950ft – 4920ft) Optimal performance setting at high elevation. [Higher than 1500m] (4920ft or greater) Optimal performance setting at the highest elevations.	s option sets an altitude value in order to choose a Fan Profile that is optimized for the air density at the current altitude at which the system is installed.

Setup Item	Options	Help Text	Comments
Set Fan Profile	**Performance** Acoustics	[Performance] - Fan control provides primary system cooling before attempting to throttle memory. [Acoustic] - The system will favor using throttling of memory over boosting fans to cool the system if thermal thresholds are met.	This option allows the user to choose a Fan Profile that is optimized for maximizing performance or for minimizing acoustic noise. When *Performance* is selected, the thermal conditions in the system are controlled by raising fan speed when necessary to raise cooling performance. This provides cooling without impacting system performance, but may impact system acoustic performance – fans running faster are typically louder. When *Acoustic* is selected, then rather than increasing fan speed for additional cooling, the system will attempt first to control thermal conditions by throttling memory to reduce heat production. This regulates the system's thermal condition without changing the acoustic performance, but throttling memory may impact system performance.
Fan PWM Offset	Entry Field 0 – 100, **0** is default	Valid Offset 0 - 100. This number is added to the calculated PWM value to increase Fan Speed.	This is a percentage by which the calculated fan speed will be increased. The user can apply positive offsets that result in increasing the minimum fan speeds.
Quiet Fan Idle Mode	**Disabled** Enabled	Enabling this option allows the system fans to operate in Quiet 'Fan off' mode while still maintaining sufficient system cooling. In this mode, fan sensors become unavailable and cannot be monitored. There will be limited fan related event generation.	When enabled, this option allows fans to idle or turn off when sufficient thermal margin is available, decreasing the acoustic noise produced by the system and decreasing system power consumption. Fans will run as needed to maintain thermal control. The actual decrease in fan speed depends on the system thermal loading, which in turn depends on system configuration and workload. While Quiet Fan Idle Mode is engaged, fan sensors become unavailable and are not monitored by the BMC.

5.4.2.15 Security Screen (Tab)

The Security screen allows the user to enable and set the user and administrative password and to lock out the front panel buttons so that they cannot be used. This screen also allows the user to enable and activate the Trusted Platform Module (TPM) security settings on those boards that support TPM.

To access this screen from the **Main** screen or other top-level **Tab** screen, press the right or left arrow keys to traverse the tabs at the top of the **Setup** screen until the **Security** screen is selected.

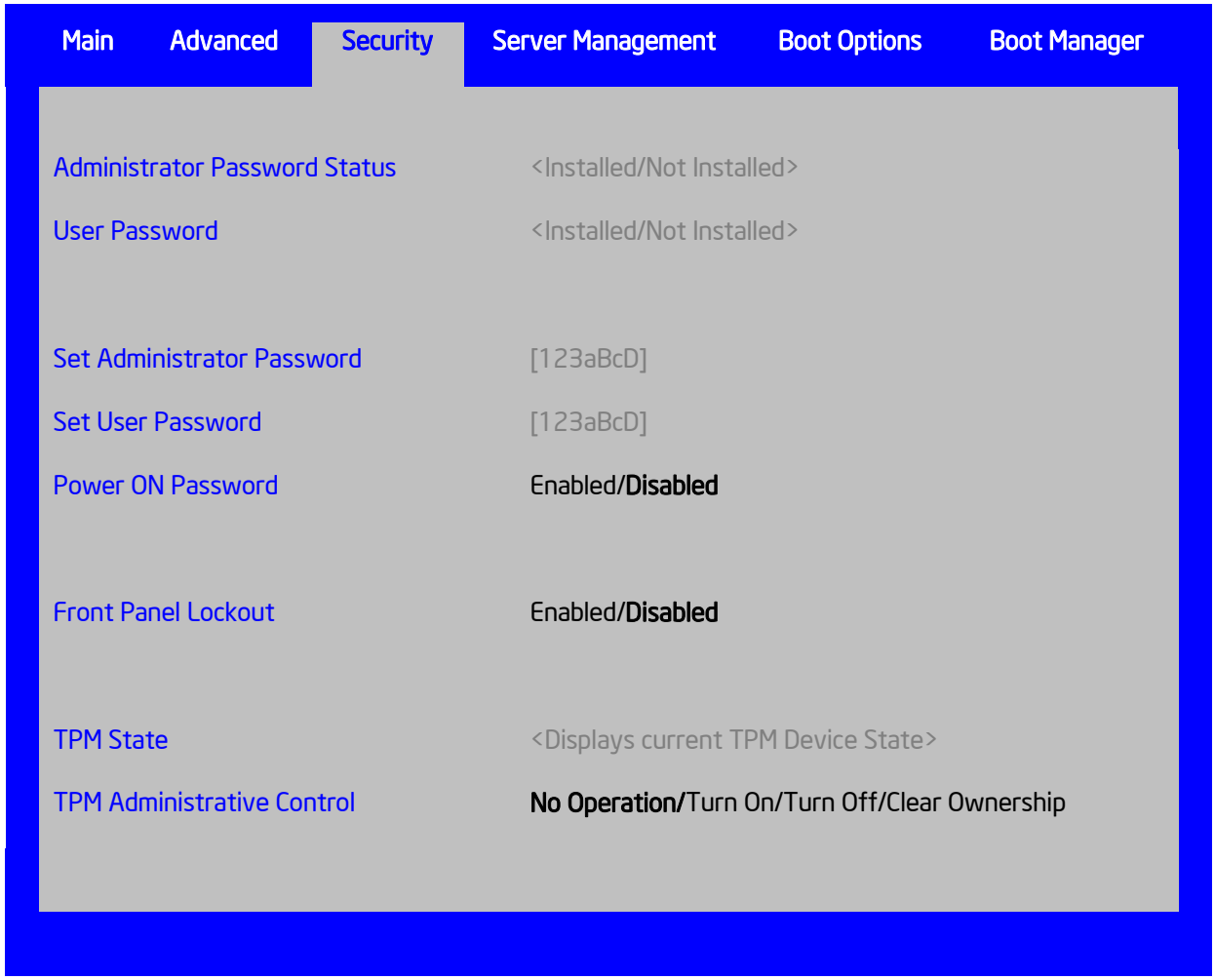


Figure 32. Security Screen

Table 42. Setup Utility – Security Configuration Screen Fields

Setup Item	Options	Help Text	Comments
Administrator Password Status	Installed Not Installed	None	Information only. Indicates the status of the administrator password.
User Password Status	Installed Not Installed	None	Information only. Indicates the status of the user password.

Setup Item	Options	Help Text	Comments
Set Administrator Password	Entry Field – 0-14 characters	Administrator password is used if Power On Password is enabled and to control change access in BIOS Setup. Length is 1-14 characters. Case sensitive alphabetic, numeric, and special characters !@#$%^&*()-_+=? are allowed. Note: Administrator password must be set in order to use the User account.	This password controls "change" access to Setup. The Administrator has full access to change settings for any Setup options, including setting the Administrator and User passwords. When Power On Password protection is enabled, the Administrator password may be used to allow the BIOS to complete POST and boot the system. Deleting all characters in the password entry field removes a password previously set. Clearing the Administrator Password also clears the User Password. If invalid characters are present in the password entered, it will not be accepted, and there will be popup error message: *Password entered is not valid. Only case sensitive alphabetic, numeric and special characters !@#$%^&*()-_+=? are allowed.* The Administrator and User passwords must be different. If the password entered is the same as the User password, it will not be accepted, and there will be popup error message: Password entered is not valid. Administrator and User passwords must be different. Strong passwords are encouraged, although not mandatory. If a password is entered which does not meet the "Strong Password" criteria, there will be a popup warning message: *Warning – a Strong Password should include at least one each case sensitive alphabetic, numeric, and special character. Length should be 8 to 14 characters.*

Setup Item	Options	Help Text	Comments
Set User Password	Entry Field – 0-14 characters	User password is used if Power On Password is enabled and to allow restricted access to BIOS Setup. Length is 1-14 characters. Case sensitive alphabetic, numeric, and special characters !@#$%^&*()-_+=? are allowed. **Note:** Removing the administrator password also removes the user password.	The User password is available only if the Administrator Password has been installed. This option protects Setup settings as well as boot choices. The User Password only allows limited access to the Setup options, and no choice of boot devices. When Power On Password protection is enabled, the User password may be used to allow the BIOS to complete POST and boot the system. The password format and entry rules and popup error and warning message are the same for the User password as for the Administrator password (see above).
Power ON Password	Enabled **Disabled**	Enable Power On Password support. If enabled, password entry is required in order to boot the system	When Power On Password security is enabled, the system will halt soon after power on and the BIOS will ask for a password before continuing POST and booting. Either the Administrator or User password may be used. If an Administrator password has not been set, this option will be grayed out and unavailable. If this option is enabled and the Administrator password is removed, that will also disable this option.
Front Panel Lockout	Enabled **Disabled**	If enabled, locks the power button OFF function and the reset and NMI Diagnostic Interrupt buttons on the system's front panel. If [Enabled] is selected, power off and reset must be controlled via a system management interface, and the NMI Diagnostic Interrupt is not available.	None

Setup Item	Options	Help Text	Comments
TPM State	<Displays current TPM Device State> May be: Enabled & Activated Enabled & Deactivated Disabled & Activated Disabled & Deactivated	None	Information only. Shows the current TPM device state. A Disabled TPM device does not execute commands that use the TPM functions and TPM security operations are not available. An Enabled & Deactivated TPM is in the same state as a disabled TPM, except that setting of the TPM ownership is allowed if it is not present already. An Enabled & Activated TPM executes all commands that use the TPM functions and TPM security operations are also available. **Note:** This option appears only on boards equipped with a TPM.
TPM Administrative Control	**No Operation** Turn On Turn Off Clear Ownership	[No Operation] - No changes to current state. [Turn On] - Enables and activates TPM. [Turn Off] - Disables and deactivates TPM. [Clear Ownership] - Removes TPM ownership & returns TPM to factory default state. **Note:** Setting returns to [No Operation] on every boot.	Any Administrative Control operation selected will require the system to perform a Hard Reset in order to become effective. **Note:** This option appears only on boards equipped with a TPM.

5.4.2.16 Server Management Screen (Tab)

The Server Management screen allows the user to configure several server management features. This screen also provides an access point to the screens for configuring console redirection, displaying system information, and controlling the BMC LAN configuration.

To access this screen from the **Main** screen or other top-level **Tab** screen, press the right or left arrow keys to traverse the tabs at the top of the **Setup** screen until the **Server Management** screen is selected.

Main | Advanced | Security | Server Management | Boot Options | Boot Manager

Assert NMI on SERR	**Enabled** / Disabled
Assert NMI on PERR	**Enabled** / Disabled
PCIe AER Support	**Enabled** / Disabled
Reset on CATERR	**Enabled** / Disabled
Reset on ERR2	**Enabled** / Disabled
Resume on AC Power Loss	**Stay Off** / Last state / Power On
Power Restore Delay	**Disabled**/Auto/Fixed
Power Restore Delay Value	25
Clear System Event Log	Enabled / **Disabled**
FRB-2 Enable	**Enabled** / Disabled
OS Boot Watchdog Timer	Enabled / **Disabled**
OS Boot Watchdog Timer Policy	**Power off** / Reset
OS Boot Watchdog Timer Timeout	5 minutes / **10 minutes** / 15 minutes / 20 minutes
Plug and Play BMC Detection	Enabled / **Disabled**
EuP LOT6 Off-Mode	Enabled / **Disabled**

► **Console Redirection**

► **System Information**

Figure 33. Server Management Screen

Table 43. Setup Utility – Server Management Configuration Screen Fields

Setup Item	Options	Help Text	Comments
Assert NMI on SERR	**Enabled** Disabled	On SERR, generate an NMI and log an error. **Note:** [Enabled] must be selected for the Assert NMI on PERR setup option to be visible.	This option allows the system to generate an NMI when an SERR occurs, which is a method Legacy Operating System error handlers may use instead of processing a Machine Check.
Assert NMI on PERR	**Enabled** Disabled	On PERR, generate an NMI and log an error. **Note:** This option is only active if the Assert NMI on SERR option is [Enabled] selected.	This option allows the system to generate an NMI when a PERR occurs, which is a method Legacy Operating System error handlers may use instead of processing a Machine Check.
PCIe AER Support	**Enabled** Disabled	[Enabled] – PCIe AER (Advanced Error Reporting) is enabled. [Disabled] – PCIe AER is disabled. All PCIe AER errors will be masked once PCIe AER is disabled.	This option allows the system to monitor and handle PCIe AER errors on PCIe devices with PCIe AER support. But as PCIe AER is described in *PCI Express* Base Specification*, any third party software or OS could override this BIOS policy and take ownership of PCIe AER handling after BIOS POST.
Reset on CATERR	**Enabled** Disabled	When enabled system gets reset upon encountering Catastrophic Error (CATERR); when disabled system does not get reset on CATERR.	This option controls whether the system will be reset when the “Catastrophic Error” CATERR# signal is held asserted, rather than just pulsed to generate an SMI. This indicates that the processor has encountered a fatal hardware error. **Note:** If “Reset on CATERR” is Disabled, this can result in a system hang for certain error conditions, possibly with the system unable to update the System Status LED or log an error to the SEL before hanging.

Setup Item	Options	Help Text	Comments
Reset on ERR2	**Enabled** Disabled	When enabled system gets reset upon encountering ERR2 (Fatal error); when disabled system does not get reset on ERR2.	This option controls whether the system will be reset if the BMC's ERR2 Monitor times out, that is, the ERR2 signal has been continuously asserted long enough to indicate that the SMI Handler is not able to service the condition. **Note:** If "Reset on ERR2" is Disabled, this can result in a system hang for certain error conditions, possibly with the system unable to update the System Status LED or log an error to the SEL before hanging.
Resume on AC Power Loss	**Stay Off** Last state Power on	System action to take on AC power loss recovery. [Stay Off] - System stays off. [Last State] - System returns to the same state before the AC power loss. [Power On] - System powers on.	This option controls the policy that the BMC will follow when AC power is restored after an unexpected power outage. The BMC will either hold DC power off or always turn it on to boot the system, depending on this setting – and in the case of Last State, depending on whether the power was on and the system was running before the AC power went off. When this setting is changed in Setup, the new setting will be sent to the BMC. However, the BMC maintains ("owns") this Power Restore Policy setting, and it can be changed independently with an IPMI command to the BMC. BIOS gets this setting from the BMC early in POST, and also for the Setup Server Management screen. **Note:** System will automatically power on after when AC is applied doing a CMOS clear because this option will not take effect at this situation.

Setup Item	Options	Help Text	Comments
Power Restore Delay	**Disabled** Auto Fixed	Allows a delay in powering up after a power failure, to reduce peak power requirements. The delay can be fixed or automatic between 25-300 seconds.	When the AC power resume policy (above) is either Power On or Last State, this option allows a delay to be taken after AC power is restored before the system actually begins to power up. This delay can be either a fixed time or an “automatic” time, where “automatic” means that the BIOS will select a randomized delay time of 25-300 seconds when it sends the Power Restore Delay setting to the BMC. This option will be grayed out and unavailable when the AC power resume policy is Stay Off. The Power Restore Delay setting is maintained by BIOS. This setting does not take effect until a reboot is done. Early in POST, the Power Restore Policy is read from the BMC, and if the policy is Power On or Last State, the delay settings are sent to the BMC. Bear in mind that even if the Power Restore Delay is Disabled, there will still be a delay of about 20 seconds while the BMC itself boots up after AC power is restored. **Note:** This Power Restore Delay option applies only to powering on when AC is applied. It has no effect on powering the system up using the Power Button on the Front Panel. A DC power on using the Power Button is not delayed. The purpose of this delay is to avoid having all systems draw “startup surge” power at the same time. Different systems or racks of systems can be set to different delay times to spread out the startup power draws. Alternatively, all systems can be set to Automatic, and then each system will wait for a random period before powering up.

Setup Item	Options	Help Text	Comments
Power Restore Delay Value	Entry Field 25 – 300, **25** is default	Fixed time period 25-300 seconds for Power Restore Delay	When the power restore policy is Power On or Last State, and the Power Restore Delay selection is Fixed, this field allows for specifying how long in seconds that fixed delay will be. When the Power Restore Delay is Disabled or Auto, this field will be grayed out and unavailable. The Power Restore Delay Value setting is maintained by BIOS. This setting does not take effect until a reboot is done. Early in POST, the Power Restore Policy is read from the BMC, and if the policy is Power On or Last State, the delay settings are sent to the BMC. When the Power Restore Delay setting is Fixed, this delay value is used to provide the length of the delay.
Clear System Event Log	Enabled **Disabled**	If enabled, clears the System Event Log. All current entries will be lost. **Note:** This option is reset to [Disabled] after a reboot.	This option sends a message to the BMC to request it to clear the System Event Log. The log will be cleared, and then the “Clear” action itself will be logged as an event. This gives the user a time/date for when the log was cleared.
FRB-2 Enable	**Enabled** Disabled	Fault Resilient Boot (FRB). BIOS programs the BMC watchdog timer for approximately 6 minutes. If BIOS does not complete POST before the timer expires, the BMC will reset the system.	This option controls whether the system will be reset if the BMC Watchdog Timer detects what appears to be a hang during POST. When the BMC Watchdog Timer is purposed as an FRB 2 timer, it is initially set to allow 6 minutes for POST to complete. However, the FRB 2 Timer is suspended during times when some lengthy operations are in progress, like executing Option ROMS, during Setup, and when BIOS is waiting for a password or for input to the F6 BBS Boot Menu. The FRB 2 Timer is also suspended while POST is paused with the <Pause> key.

Setup Item	Options	Help Text	Comments
O/S Boot Watchdog Timer	Enabled **Disabled**	If enabled, the BIOS programs the watchdog timer with the timeout value selected. If the OS does not complete booting before the timer expires, the BMC resets the system and an error is logged. Requires OS support or Intel® Management Software.	This option controls whether the system will set the BMC Watchdog to detect an apparent hang during OS boot. BIOS sets the timer before starting the OS bootstrap load procedure. If the OS Load Watchdog Timer times out, then presumably the OS failed to boot properly. If the OS does boot up successfully, it must be aware of the OS Load Watchdog Timer and immediately turn it off before it expires. The OS may turn off the timer, or more often the timer may be repurposed as an OS Watchdog Timer to protect against runtime OS hangs. Unless the OS does have timer-aware software to support the OS Load Watchdog Timer, the system will be unable to boot successfully with the OS Load Watchdog Timer enabled. When the timer expires without having been reset or turned off, the system will either reset or power off repeatedly.
O/S Boot Watchdog Timer Policy	**Power Off** Reset	If the OS boot watchdog timer is enabled, this is the system action taken if the watchdog timer expires. [Reset] - System performs a reset. [Power Off] - System powers off.	This option is grayed out and unavailable when the O/S Boot Watchdog Timer is disabled.
O/S Boot Watchdog Timer Timeout	5 minutes **10 minutes** 15 minutes 20 minutes	If the OS watchdog timer is enabled, this is the timeout value used by the BIOS to configure the watchdog timer.	This option is grayed out and unavailable when the O/S Boot Watchdog Timer is disabled.
Plug and Play BMC Detection	Enabled **Disabled**	If enabled, the BMC is detectable by OSs that support plug and play loading of an IPMI driver. Do not enable if your OS does not support this driver.	This option controls whether the OS Server Management Software will be able to find the BMC and automatically load the correct IPMI support software for it. If your OS does not support Plug & Play for the BMC, you will not have the correct IPMI driver software loaded.

Setup Item	Options	Help Text	Comments
EuP LOT6 Off-Mode	Enabled **Disabled**	Enable/disable Ecodesign EuP LOT6 “Deep Sleep” Off-Mode for near-zero energy use when powered off.	This option controls whether the system goes into “Deep Sleep” or more conventional S5 “Soft-Off” when powered off. “Deep Sleep” state uses less energy than S5 but S5 can start up faster and can allow a Wake on LAN action (which cannot be done from a Deep Sleep state). This option will not appear on platforms which do not support EuP LOT6 Off-Mode.
Console Redirection	None	View/Configure console redirection information and settings.	Selection only. Select this line and press the <Enter> key to go to the Console Redirection group of configuration settings.
System Information	None	View system information	Selection only. Select this line and press the <Enter> key to go to the System Information group of configuration settings.
BMC LAN Configuration	None	View/Configure BMC LAN channel and user settings	Selection only. Select this line and press the <Enter> key to go to the BMC LAN Configuration group of configuration settings.

5.4.2.17 Console Redirection

The Console Redirection screen allows the user to enable or disable Console Redirection for Remote Management, and to configure the connection options for this feature.

To access this screen from the **Main** screen, select **Server Management > Console Redirection.** To move to another screen, press the <Esc> key to return to the **Server Management** screen, then select the desired screen.

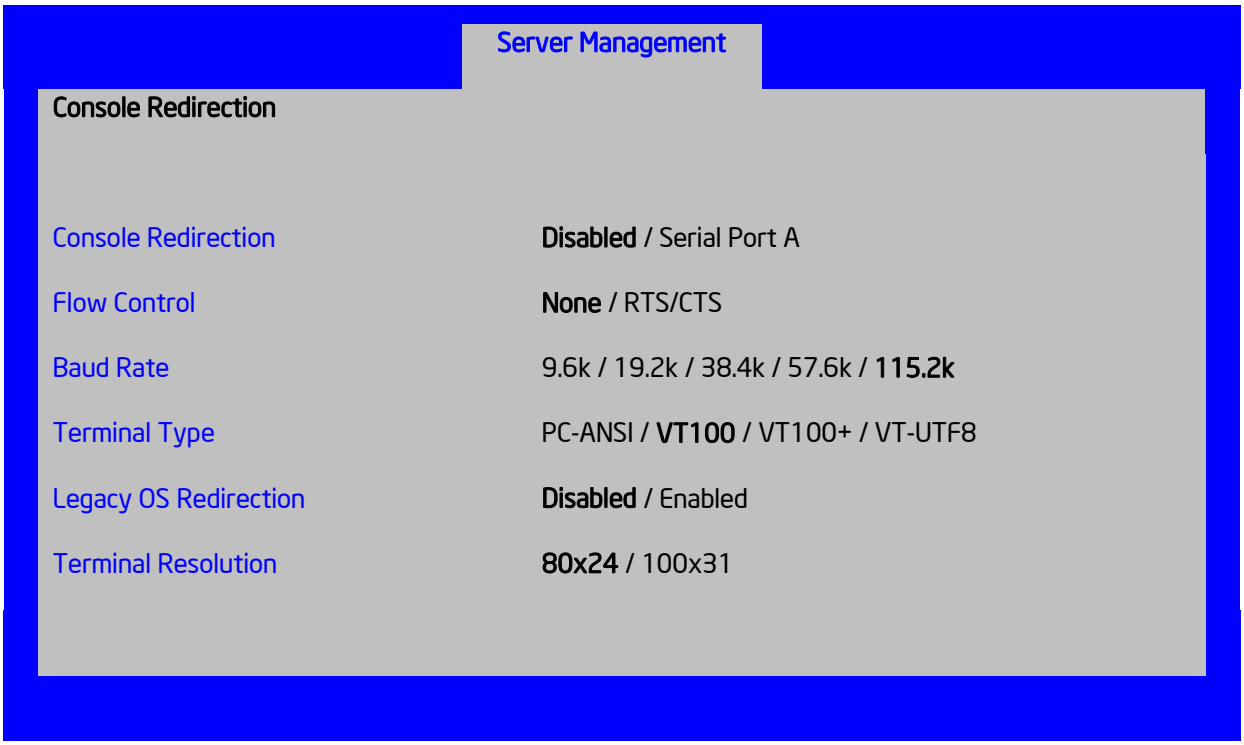


Figure 34. Console Redirection Screen

Table 44. Setup Utility – Console Redirection Configuration Fields

Setup Item	Options	Help Text	Comments
Console Redirection	**Disabled** Serial Port A	Console redirection allows a serial port to be used for server management tasks. [Disabled] - No console redirection. [Serial Port A] - Configure serial port A for console redirection. Enabling this option disables the display of the Quiet Boot logo screen during POST.	Serial Console Redirection can use Serial Port A. If SOL is also going to be configured, note that SOL is only supported through Serial Port A When Console Redirection is set to Disabled, all other options on this screen will be grayed out and unavailable. Only Serial Ports which are Enabled should be available to choose for Console Redirection. If Serial A is set to Enabled, then Console Redirection will be forced to Disabled, and grayed out as inactive. In that case, all other options on this screen will also be grayed
Flow Control	**None** RTS/CTS	Flow control is the handshake protocol. Setting must match the remote terminal application.	Flow control is necessary only when there is a possibility of data overrun. In that case the Request To Send/Clear to Send (RTS/CTS) hardware handshake is a relatively

Setup Item	Options	Help Text	Comments
		[None] - Configure for no flow control. [RTS/CTS] - Configure for hardware flow control.	conservative protocol which can usually be configured at both ends. When Console Redirection is set to Disabled, this option will be grayed out and unavailable.
Baud Rate	9600 19.2K 38.4K 57.6K **115.2K**	Serial port transmission speed. Setting must match the remote terminal application.	In most modern Server Management applications, serial data transfer is consolidated over an alternative faster medium like LAN, and 115.2k is the speed of choice. When Console Redirection is set to Disabled, this option will be grayed out and unavailable.
Terminal Type	PC-ANSI **VT100** VT100+ VT-UTF8	Character formatting used for console redirection. Setting must match the remote terminal application.	The VT100 and VT100+ terminal emulations are essentially the same. VT-UTF8 is a UTF8 encoding of VT100+. PC-ANSI is the native character encoding used by PC-compatible applications and emulators. When Console Redirection is set to Disabled, this option will be grayed out and unavailable.
Legacy OS Redirection	**Disabled** Enabled	This option enables legacy OS redirection (that is, DOS) on serial port. If it is enabled, the associated serial port is hidden from the legacy OS.	Operating Systems which are “redirection-aware” implement their own Console Redirection mechanisms. For a Legacy OS which is not “aware”, this option allows the BIOS to handle redirection. When Console Redirection is set to Disabled, this option will be grayed out and unavailable.
Terminal Resolution	**80x24** 100x31	Remote Terminal Resolution.	This option allows the use of a larger terminal screen area, although it does not change Setup displays to match. When Console Redirection is set to Disabled, this option will be grayed out and unavailable.

5.4.2.18 System Information

The System Information screen allows the user to view part numbers, serial numbers, and firmware revisions. This is an **Information Only** screen.

To access this screen from the **Main** screen, select **Server Management > System Information.** To move to another screen, press the <Esc> key to return to the **Server Management** screen, then select the desired screen.

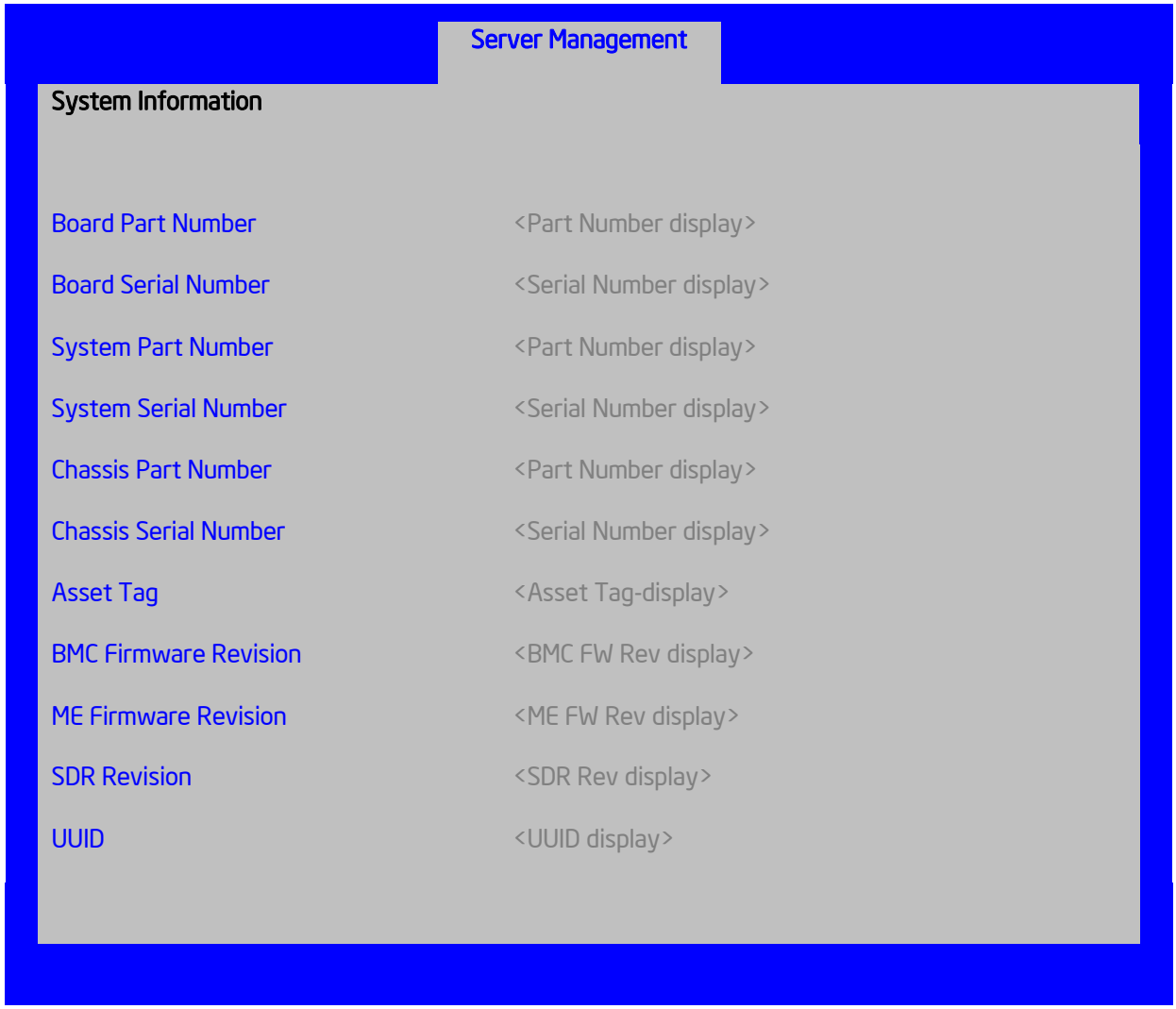


Figure 35. System Information Screen

Table 45. Setup Utility – Server Management System Information Fields

Setup Item	Options	Help Text	Comments
Board Part Number	Part Number display	None	Information only
Board Serial Number	Serial Number display	None	Information only
System Part Number	Part Number display	None	Information only
System Serial Number	Serial Number display	None	Information only

Setup Item	Options	Help Text	Comments
Chassis Part Number	Part Number display	None	Information only
Chassis Serial Number	Serial Number display>	None	Information only
Asset Tag	Asset Tag-display	None	Information only
BMC Firmware Revision	BMC FW Rev display	None	Information only
ME Firmware Revision	ME FW Rev display	None	Information only
SDR Revision	SDR Rev display	None	Information only
UUID	UUID display	None	Information only

5.4.2.19 BMC LAN Configuration

The BMC configuration screen allows the Setup user to configure the BMC Baseboard LAN channel and the RMM4 LAN channel, and to manage BMC User settings for up to five BMC Users.

To access this screen from the **Main** screen, select **Server Management > System Information.** To move to another screen, press the <Esc> key to return to the **Server Management** screen, then select the desired screen.

Server Management

BMC LAN Configuration

Baseboard LAN configuration

IP Source	Static/**Dynamic**
IP Address	[0.0.0.0]
Subnet Mask	[0.0.0.0]
Gateway IP	[0.0.0.0]

Baseboard LAN IPv6 configuration

IPv6	**Disable**/Enable
IPv6 source	Static/**Dynamic**/Auto
IPv6 address	[0000:0000:0000:0000:0000:0000:0000:0000]
Gateway IPv6	[0000:0000:0000:0000:0000:0000:0000:0000]
IPv6 Prefix Length	[0 – 128, **64** is default]

Intel(R) RMM4 IPv4 LAN configuration

Intel (R) RMM4	< Not Present/Intel(R) RMM4-Lite/Intel(R) RMM4 + DMN >
IP Source	Static/**Dynamic**
IP Address	[0.0.0.0]
Subnet Mask	[0.0.0.0]
Gateway IP	[0.0.0.0]

Intel(R) RMM4 IPv6 LAN configuration

IPv6 Source	Static/**Dynamic**/Auto
IPv6 Address	[0000:0000:0000:0000:0000:0000:0000:0000]
Gateway IPv6	[0000:0000:0000:0000:0000:0000:0000:0000]

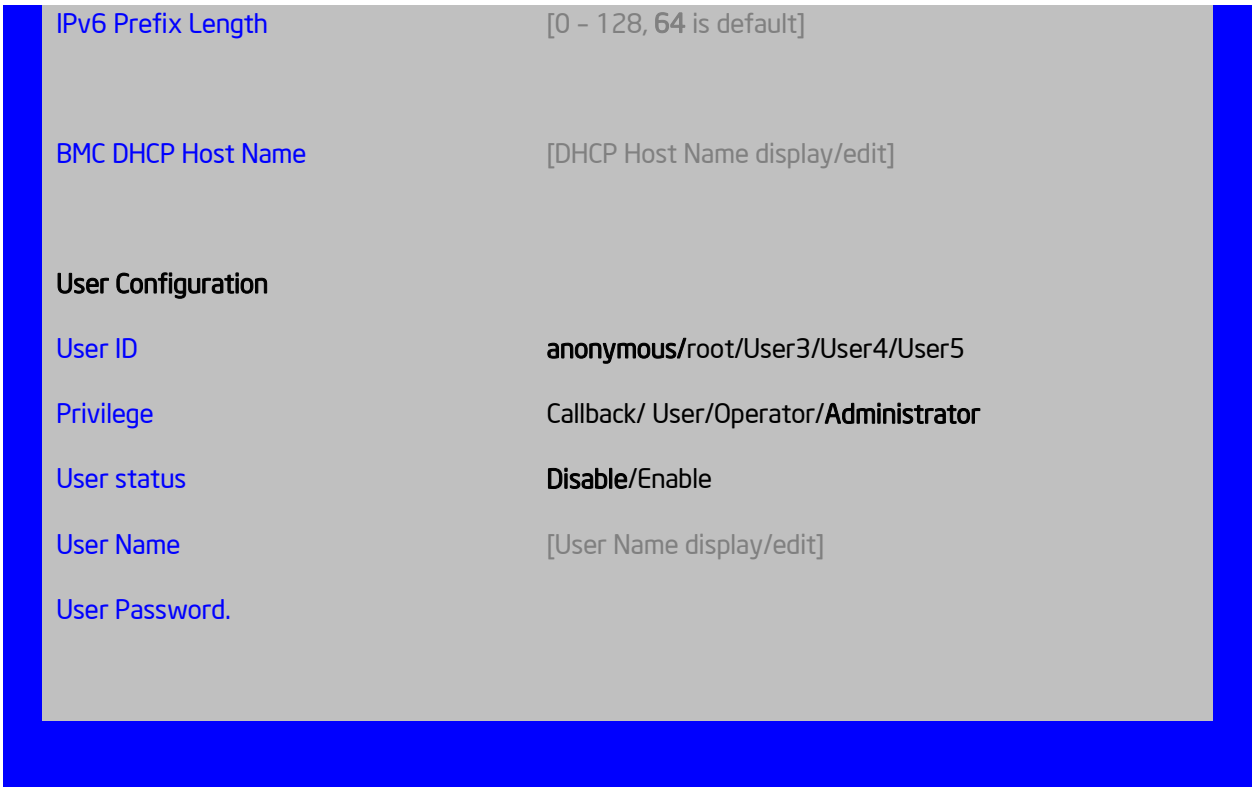


Figure 36. BMC LAN Configuration Screen

Table 46. Setup Utility – BMC configuration Screen Fields

Setup Item	Options	Help Text	Comments
IP source	Static **Dynamic**	Select BMC IP source. When Static option is selected, IP address, subnet mask and gateway are editable. When Dynamic option selected, these fields are read-only and IP is address acquired automatically (DHCP).	This specifies the IP Source for IPv4 addressing for the Baseboard LAN. There is a separate IP Source field for the Intel® RMM4 LAN configuration. When IPv4 addressing is used, the initial value for this field is acquired from the BMC, and its setting determines whether the other Baseboard LAN IPv4 addressing fields are display-only (when Dynamic) or can be edited (when Static).

Setup Item	Options	Help Text	Comments
IP address	Entry Field 0.0.0.0, **0.0.0.0** is default	View/Edit IP address. Press <Enter> to edit.	This specifies the IPv4 Address for the Baseboard LAN. There is a separate IPv4 Address field for the Intel® RMM4 LAN configuration. When IPv4 addressing is used, the initial value for this field is acquired from the BMC. The setting of IP Source determines whether this field is display-only (when Dynamic) or can be edited (when Static). When IPv6 addressing is enabled, this field is grayed out and inactive.
Subnet Mask	Entry Field 0.0.0.0, **0.0.0.0** is default	View/Edit subnet address. Press <Enter> to edit.	This specifies the IPv4 addressing Subnet Mask for the Baseboard LAN. There is a separate IPv4 Subnet Mask field for the Intel® RMM4 LAN configuration. When IPv4 addressing is used, the initial value for this field is acquired from the BMC. The setting of IP Source determines whether this field is display-only (when Dynamic) or can be edited (when Static). When IPv6 addressing is enabled, this field is grayed out and inactive.
Gateway IP	Entry Field 0.0.0.0, **0.0.0.0** is default	View/Edit Gateway IP address. Press <Enter> to edit.	This specifies the IPv4 addressing Gateway IP for the Baseboard LAN. There is a separate IPv4 Gateway IP field for the Intel® RMM4 LAN configuration. When IPv4 addressing is used, the initial value for this field is acquired from the BMC. The setting of IP Source determines whether this field is display-only (when Dynamic) or can be edited (when Static). When IPv6 addressing is enabled, this field is grayed out and inactive.
IPv6	Enabled **Disabled**	Option to Enable/Disable IPv6 addressing and any IPv6 network traffic on these channels.	The initial value for this field is acquired from the BMC. It may be changed in order to switch between IPv4 and IPv6 addressing technologies. When this option is set to Disabled, all other IPv6 fields will not be visible for the Baseboard LAN and Intel® RMM4 DMN

Setup Item	Options	Help Text	Comments
			(if installed). When IPv6 addressing is Enabled, all IPv6 fields for the Baseboard LAN and Intel® RMM4 DMN will become visible, and all IPv4 fields will be grayed out and inactive.
IPv6 Source	Static **Dynamic** Auto	Select BMC IPv6 source: If [Static], IPv6 parameters may be edited. If [Dynamic], these fields are display-only and IPv6 address is acquired automatically (DHCP). If [Auto], these fields are display-only and IPv6 address is acquired using ICMPv6 router / neighbor discovery.	This specifies the IP Source for IPv6 addressing for the Baseboard LAN configuration. There is a separate IPv6 Source field for the Intel® RMM4 LAN configuration. This option is only visible when the IPv6 option is set to Enabled. When IPv6 addressing is Enabled, the initial value for this field is acquired from the BMC, and its setting determines whether the other Baseboard LAN IPv6 addressing fields are display-only (when Dynamic or Auto) or can be edited (when Static).
IPv6 Address	Entry Field 0000:0000 0000:0000 0000:0000 0000:0000 **0000:0000** **0000:0000** **0000:0000** **0000:0000** is default	View/Edit IPv6 address. Press <Enter> to edit. IPv6 addresses consist of 8 hexadecimal 4 digit numbers separated by colons.	This specifies the IPv6 Address for the Baseboard LAN. There is a separate IPv6 Address field for the Intel® RMM4 LAN configuration. This option is only visible when the IPv6 option is set to Enabled. When IPv6 addressing is used, the initial value for this field is acquired from the BMC. The setting of IPv6 Source determines whether this field is display-only (when Dynamic or Auto) or can be edited (when Static).
Gateway IPv6	Entry Field 0000:0000 0000:0000 0000:0000 0000:0000 **0000:0000** **0000:0000**	View/Edit Gateway IPv6 address. Press <Enter> to edit. Gateway IPv6 addresses consist of 8 hexadecimal 4 digit numbers separated by colons.	This specifies the Gateway IPv6 Address for the Baseboard LAN. There is a separate Gateway IPv6 Address field for the Intel® RMM4 LAN configuration. This option is only visible when the IPv6 option is set to Enabled. When IPv6 addressing is used, the initial value for this field is acquired from the BMC. The setting of IPv6 Source determines whether this

Setup Item	Options	Help Text	Comments
	0000:0000 **0000:0000** is default		field is display-only (when Dynamic or Auto) or can be edited (when Static).
IPv6 Prefix Length	Entry Field 0 – 128, **64** is default	View/Edit IPv6 Prefix Length from zero to 128 (default 64). Press <Enter> to edit.	This specifies the IPv6 Prefix Length for the Baseboard LAN. There is a separate IPv6 Prefix Length field for the Intel® RMM4 LAN configuration. This option is only visible when the IPv6 option is set to Enabled. When IPv6 addressing is used, the initial value for this field is acquired from the BMC. The setting of IPv6 Source determines whether this field is display-only (when Dynamic or Auto) or can be edited (when Static).
Intel® RMM4	Not Present Intel(R) RMM4-Lite Intel(R) RMM4 + DMN	None	Information only. Displays whether an Intel® RMM4 component is currently installed. This information may come from querying the BMC. Intel® RMM4-Lite is the Management Module without the Dedicated Server Management NIC Module. When this is present, or if the Management Module is Not Present at all, the fields for Intel® RMM4 LAN Configuration will not be visible. When an Intel® RMM4 + DMN is installed, the options for Intel® RMM4 LAN Configuration will be visible. When IPv6 is Disabled, the IPv4 configuration fields will be visible and the IPv6 configuration fields will not be visible. When IPv6 is Enabled, the IPv4 fields will be grayed out and inactive, while the IPv6 Configuration fields will be visible. In either case, the Intel® RMM4 section IP Source or IPv6 Source will determine whether the IPv4 or IPv6 address fields are display-only or can be edited.

Setup Item	Options	Help Text	Comments
IP source	Static **Dynamic**	Select RMM4 IP source: If [Static], IP parameters may be edited. If [Dynamic], these fields are display-only and IP address is acquired automatically (DHCP).	This specifies the IP Source for IPv4 addressing for the Intel® RMM4 DMN LAN connection. There is a separate IP Source field for the Baseboard LAN configuration. When IPv4 addressing is used, the initial value for this field is acquired from the BMC, and its setting determines whether the other Intel® RMM4 DMN LAN IPv4 addressing fields are display-only (when Dynamic) or can be edited (when Static). When IPv6 addressing is enabled, this field is grayed out and inactive.
IP address	Entry Field 0.0.0.0, **0.0.0.0** is default	View/Edit IP address. Press <Enter> to edit.	This specifies the IPv4 Address for the Intel® RMM4 DMN LAN. There is a separate IPv4 Address field for the Baseboard LAN configuration. When IPv4 addressing is used, the initial value for this field is acquired from the BMC. The setting of IP Source determines whether this field is display-only (when Dynamic) or can be edited (when Static). When IPv6 addressing is enabled, this field is grayed out and inactive.
Subnet Mask	Entry Field 0.0.0.0, **0.0.0.0** is default	View/Edit subnet address. Press <Enter> to edit.	This specifies the IPv4 addressing Subnet Mask for the Intel® RMM4 DMN LAN. There is a separate IPv4 Subnet Mask field for the Baseboard LAN configuration. When IPv4 addressing is used, the initial value for this field is acquired from the BMC. The setting of IP Source determines whether this field is display-only (when Dynamic) or can be edited (when Static). When IPv6 addressing is enabled, this field is grayed out and inactive.
Gateway IP	Entry Field 0.0.0.0, **0.0.0.0** is default	View Edit Gateway IP address. Press <Enter> to edit.	This specifies the IPv4 addressing Gateway IP for the Intel® RMM4 DMN LAN. There is a separate IPv4 Gateway IP field for the Baseboard LAN configuration. When IPv4 addressing is used, the initial

Setup Item	Options	Help Text	Comments
			value for this field is acquired from the BMC. The setting of IP Source determines whether this field is display-only (when Dynamic) or can be edited (when Static). When IPv6 addressing is enabled, this field is grayed out and inactive.
IPv6 Source	Static **Dynamic** Auto	Select Intel(R) RMM4 IPv6 source: If [Static], IPv6 parameters may be edited. If [Dynamic], these fields are display-only and IPv6 address is acquired automatically (DHCP). If [Auto], these fields are display-only and IPv6 address is acquired using ICMPv6 router / neighbor discovery.	This specifies the IP Source for IPv6 addressing for the Intel® RMM4 DMN LAN configuration. There is a separate IPv6 Source field for the Baseboard LAN configuration. This option is only visible when the IPv6 option is set to Enabled. When IPv6 addressing is Enabled, the initial value for this field is acquired from the BMC, and its setting determines whether the other Intel® RMM4 DMN LAN IPv6 addressing fields are display-only (when Dynamic or Auto) or can be edited (when Static).
IPv6 Address	Entry Field 0000:0000 0000:0000 0000:0000 0000:0000 **0000:0000** **0000:0000** **0000:0000** **0000:0000** is default	View/Edit IPv6 address. Press <Enter> to edit. IPv6 addresses consist of 8 hexadecimal 4 digit numbers separated by colons.	This specifies the IPv6 Address for the Intel® RMM4 DMN LAN. There is a separate IPv6 Address field for the Baseboard LAN configuration. This option is only visible when the IPv6 option is set to Enabled. When IPv6 addressing is used, the initial value for this field is acquired from the BMC. The setting of IPv6 Source determines whether this field is display-only (when Dynamic or Auto) or can be edited (when Static).
Gateway IPv6	Entry Field 0000:0000 0000:0000 0000:0000	View/Edit Gateway IPv6 address. Press <Enter> to edit. Gateway IPv6 addresses consist of 8 hexadecimal 4 digit numbers separated by colons.	This specifies the Gateway IPv6 Address for the Intel® RMM4 DMN LAN. There is a separate Gateway IPv6 Address field for the Baseboard LAN configuration. This option is only visible when the IPv6 option is set to Enabled.

Setup Item	Options	Help Text	Comments
	0000:0000 **0000:0000** **0000:0000** **0000:0000** **0000:0000** is default		When IPv6 addressing is used, the initial value for this field is acquired from the BMC. The setting of IPv6 Source determines whether this field is display-only (when Dynamic or Auto) or can be edited (when Static).
IPv6 Prefix Length	Entry Field 0 – 128, **64** is default	View/Edit IPv6 Prefix Length from zero to 128 (default 64). Press <Enter> to edit.	This specifies the IPv6 Prefix Length for the Intel® RMM4 DMN LAN. There is a separate IPv6 Prefix Length field for the Baseboard LAN configuration. This option is only visible when the IPv6 option is set to Enabled. When IPv6 addressing is used, the initial value for this field is acquired from the BMC. The setting of IPv6 Source determines whether this field is display-only (when Dynamic or Auto) or can be edited (when Static).
BMC DHCP Host Name	Entry Field, 2-63 characters	View/Edit BMC DHCP host name. Press <Enter> to edit. Host name should start with an alphabetic, remaining can be alphanumeric characters. Host name length may be from 2 to 63 characters.	This field is active and may be edited whenever at least one of the IP Source or IPv6 Source options is set to Dynamic. This is the name of the DHCP Host from which dynamically assigned IPv4 or IPv6 addressing parameters are acquired. The initial value for this field is supplied from the BMC, if there is a DHCP Host available. The user can edit the existing Host or enter a different DHCP Host Name. If none of the IP/IPv6 Source fields is set to Dynamic, then this BMC DHCP Host Name field will be grayed out and inactive.
User ID	**anonymous** root User3 User4 User5	Select the User ID to configure: User1 (anonymous), User2 (root), and User3/4/5 are supported.	These 5 User IDs are fixed choices and cannot be changed. The BMC supports 15 User IDs natively but only the first 5 are supported through this interface.

Setup Item	Options	Help Text	Comments
Privilege	Callback User Operator **Administrator**	View/Select user privilege. User2 (root) privilege is "Administrator" and cannot be changed.	The level of privilege that is assigned for a User ID affects which functions that user may perform.
User Status	Enable **Disable**	Enable/Disable LAN access for selected user. Also enables/disables SOL, KVM media redirection.	Note that status setting is Disabled by default until set to Enabled.
User Name	Entry Field, 4 - 15 characters	Press <Enter> to edit user name. User name is string of 4 to 15 alphanumeric characters. User name must begin with an alphabetic character. User Name cannot be changed for User1 (anonymous) and User2 (root).	User Name can only be edited for users other than “anonymous” and “root”. Those two User Names may not be changed.
User Password	Popup Entry Field, 0 - 15 characters	Press <Enter> key to enter password. Maximum length is 15 characters. Any ASCII printable characters can be used: case-sensitive alphabetic, numeric, and special characters. **Note:** Password entered will override any previously set password.	This field will not indicate whether there is a password set already. There is no display - just press <Enter> for a popup with an entry field to enter a new password. Any new password entered will override the previous password, if there was one.

5.4.2.20 Boot Options Screen (Tab)

The Boot Options screen displays all bootable media encountered during POST, and allows the user to configure the desired order in which boot devices are to be tried.

The first boot device in the specified Boot Order which is present and is bootable during POST will be used to boot the system, and will continue to be used to reboot the system until the boot device configuration has changed (that is, which boot devices are present), or until the system has been powered down and booted in a “cold” power-on boot.

If all types of bootable devices are installed in the system, then the default boot order is as follows:

- CD/DVD-ROM
- Floppy Disk Drive
- Hard Disk Drive
- PXE Network Device
- BEV (Boot Entry Vector) Device
- EFI Shell and EFI Boot paths

To access this screen from the **Main** screen or other top-level “Tab” screen, press the right or left arrow keys to traverse the tabs at the top of the **Setup** screen until the **Boot Options** screen is selected.

Figure 37. Boot Options Screen

Table 47. Setup Utility – Boot Options Screen Fields

Setup Item	Options	Help Text	Comments
System Boot Timeout	Entry Field 0 – 65535, 0 is default	The number of seconds BIOS will pause at the end of POST to allow the user to press the [F2] key for entering the BIOS Setup utility. Valid values are 0-65535. Zero is the default. A value of 65535 causes the system to go to the Boot Manager menu and wait for user input for every system boot.	After entering the necessary timeout, press the **<Enter>** key to register that timeout value to the system. These settings are in seconds. The timeout value entered will take effect on the next boot. This timeout value is independent of the FRB2 setting for BIOS boot failure protection. The FBR2 countdown will be suspended during the time that the Boot Timeout countdown is active. Also, if the **<Pause>** key is pressed during the time that the Boot Timeout is active, the Boot Timeout countdown will be suspended until the Pause state has been dismissed and normal POST processing has resumed.
Boot Option #x	Available boot devices #n.	Set system boot order by selecting the boot option for this position.	When the Boot order has been chosen, it will take effect on the next boot. The system will go down the list and boot from the first device on the list which is available and bootable. This establishes the Boot Order only with respect to the normal boot path. This order has no effect on the Boot Manager selection list or the **<F6>** BIOS Boot Menu popup, both of which simply list all bootable devices available in the order in which they were detected. Whether or not a potential Boot Device is in this list has no bearing on the presence or order of Boot Devices shown for Boot Manager or the BIOS Boot Menu.
CDROM Order	None	Set the order of the legacy devices in this group.	Selection only. Select this line and press the **<Enter>** key to go to the CDROM Order Screen. This option appears when one or more bootable CDROM drives are available in the system. This includes USB CDROM devices but

Setup Item	Options	Help Text	Comments
			not USB Keys formatted for CRDOM emulation, which are seen as Hard Disk drives.
Hard Disk Order	None	Set the order of the legacy devices in this group.	Selection only. Select this line and press the **<Enter>** key to go to the Hard Disk Order Screen. This option appears when one or more bootable Hard Disk drives are available in the system. This includes USB Hard Disk devices and USB Keys formatted for Hard Disk or CRDOM emulation.
Floppy Order	None	Set the order of the legacy devices in this group.	Selection only. Select this line and press the **<Enter>** key to go to the Floppy Order Screen. This option appears when one or more bootable Floppy Disk drives are available in the system. This includes USB Floppy Disk devices and USB Keys formatted for Floppy Disk emulation.
Network Device Order	None	Set the order of the legacy devices in this group.	Selection only. Select this line and press the **<Enter>** key to go to the Network Device Order Screen. This option appears when one or more bootable Network Devices are available in the system.
BEV Device Order	None	Set the order of the legacy devices in this group.	Selection only. Select this line and press the **<Enter>** key to go to the BEV Device Order Screen. This option appears when one or more bootable BEV Devices are available in the system.
Add EFI Boot Option	None	Add a new EFI boot option to the boot order.	Selection only. Select this line and press the **<Enter>** key to go to the Add EFI Boot Option Screen. This option is only displayed if an EFI bootable device is available to the system.
Delete Boot Option	None	Remove an EFI boot option from the boot order.	Selection only. Select this line and press the **<Enter>** key to go to the Delete EFI Boot Option Screen.

Setup Item	Options	Help Text	Comments
			This option is only displayed if an EFI boot path is included in the Boot Order.
EFI Optimized Boot	Enabled **Disabled**	If enabled, the BIOS only loads modules required for booting EFI-aware Operating Systems.	If this option is enabled, the system will not boot successfully to a non-EFI-aware OS.
Use Legacy Video for EFI OS	Enabled **Disabled**	If enabled, the BIOS uses the legacy video ROM instead of the EFI video ROM.	This option appears only when EFI Optimized Boot is enabled.
Boot Option Retry	Enabled **Disabled**	If enabled, this continually retries non-EFI-based boot options without waiting for user input.	This option is intended to keep retrying for cases where the boot devices could possibly be slow to initially respond. For example, if the device were “asleep” and did not wake quickly enough. However, if none of the devices in the Boot Order ever responds, the BIOS will continue to reboot indefinitely.
USB Boot Priority	Enabled **Disabled**	If enabled, newly discovered USB devices are moved to the top of their boot device category. If disabled, newly discovered USB devices are moved to the bottom of their boot device category.	This option enables or disables the “USB Reorder” functionality. USB Boot Priority, if enabled, is intended for the case where a user wants to be able to plug in a USB device and immediately boot to it, for example in case of a maintenance or System Administration operation. If a User Password is installed, USB Boot Priority action is suspended when a User Password is installed.
Static Boot Ordering	Enabled **Disabled**	[Disabled] - Devices removed from the system are deleted from Boot Order Tables. [Enabled] - Devices removed have positions in Boot Order Tables retained for later reinsertion.	When the option changes to “Enabled” from “Disabled”, it will enable Static Boot Ordering (SBO) from the next boot onward, and also the current Boot Order will be stored as the SBO template. When the option changes to “Disabled” from “Enabled”, it will disable SBO and the SBO template will be cleared. Otherwise it will retain the current Enabled/Disabled state.
Reset Static Boot Order	Yes **No Action**	[Yes] Take snapshot of current boot order to save as Static Boot Order Template.	This option will allow you to save the Boot Order list as the Static Boot Order template without disabling and re-enabling the Static Boot

Setup Item	Options	Help Text	Comments
			Order option. Select Yes to take a snapshot of the current Boot Options list into the Static Boot Options list on the next boot. After saving Static Boot Options list, this option will change back to NoAction automatically. This option is available only when the Static Boot Order option is Enabled. Otherwise it will be grayed out and unavailable.

5.4.2.21 CDROM Order

The CDROM Order screen allows the user to control the order in which BIOS attempts to boot from the CDROM drives installed in the system. This screen is only available when there is at least one CDROM device available in the system configuration. Note that A USB attached CDROM device will appear in this section. However, a USB Key formatted as a CRDOM device will not – it will be detected as a Hard Disk device and will be included in the Hard Disk Order Screen.

To access this screen from the Main screen, select Boot Options > CDROM Order. To move to another screen, press the <Esc> key to return to the Boot Options screen, then select the desired screen.

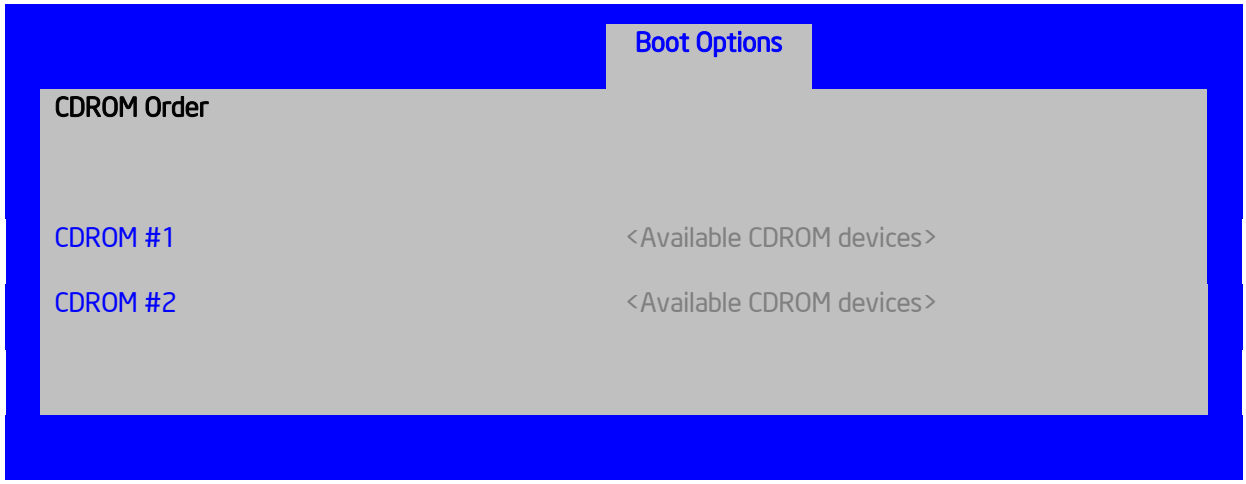


Figure 38. CDROM Order Screen

Table 48. Setup Utility – CDROM Order Fields

Setup Item	Options	Help Text	Comments

Setup Item	Options	Help Text	Comments
CDROM #1	Available CDROM devices.	Set system boot order by selecting the boot option for this position.	Choose the order of booting among CDROM devices by choosing which available CDROM device should be in each position in the order.
CDROM #2	Available CDROM devices.	Set system boot order by selecting the boot option for this position.	Choose the order of booting among CDROM devices by choosing which available CDROM device should be in each position in the order.

5.4.2.22 Hard Disk Order

The Hard Disk Order screen allows the user to control the order in which BIOS attempts to boot from the hard disk drives installed in the system. This screen is only available when there is at least one hard disk device available in the system configuration. Note that a USB attached Hard Disk drive or a USB Key device formatted as a hard disk will appear in this section.

To access this screen from the **Main** screen, select **Boot Options > Hard Disk Order**. To move to another screen, press the <Esc> key to return to the **Boot Options** screen, then select the desired screen.

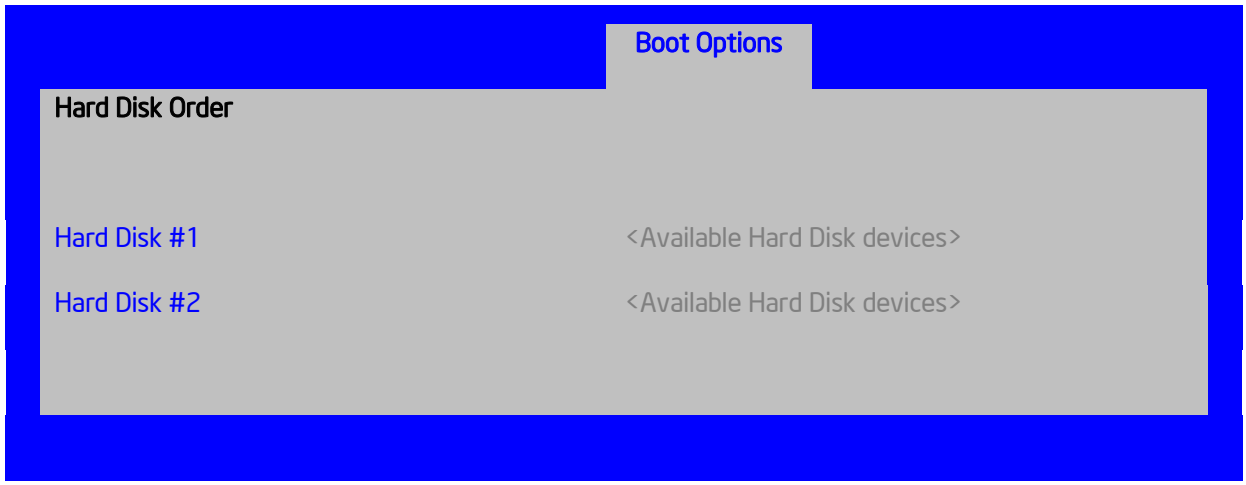


Figure 39. Hard Disk Order Screen

Table 49. Setup Utility – Hard Disk Order Fields

Setup Item	Options	Help Text	Comments

Setup Item	Options	Help Text	Comments
Hard Disk #1	Available Hard Disk devices.	Set system boot order by selecting the boot option for this position.	Choose the order of booting among Hard Disk devices by choosing which available Hard Disk device should be in each position in the order.
Hard Disk #2	Available Hard Disk devices.	Set system boot order by selecting the boot option for this position.	Choose the order of booting among Hard Disk devices by choosing which available Hard Disk device should be in each position in the order.

5.4.2.23 Floppy Order

The Floppy Order screen allows the user to control the order in which BIOS attempts to boot from the Floppy Disk drives installed in the system. This screen is only available when there is at least one Floppy Disk (diskette) device available in the system configuration. Note that a USB attached diskette drive or a USB Key device formatted as a diskette drive will appear in this section.

To access this screen from the Main screen, select Boot Options > Floppy Order. To move to another screen, press the <Esc> key to return to the Boot Options screen, then select the desired screen.

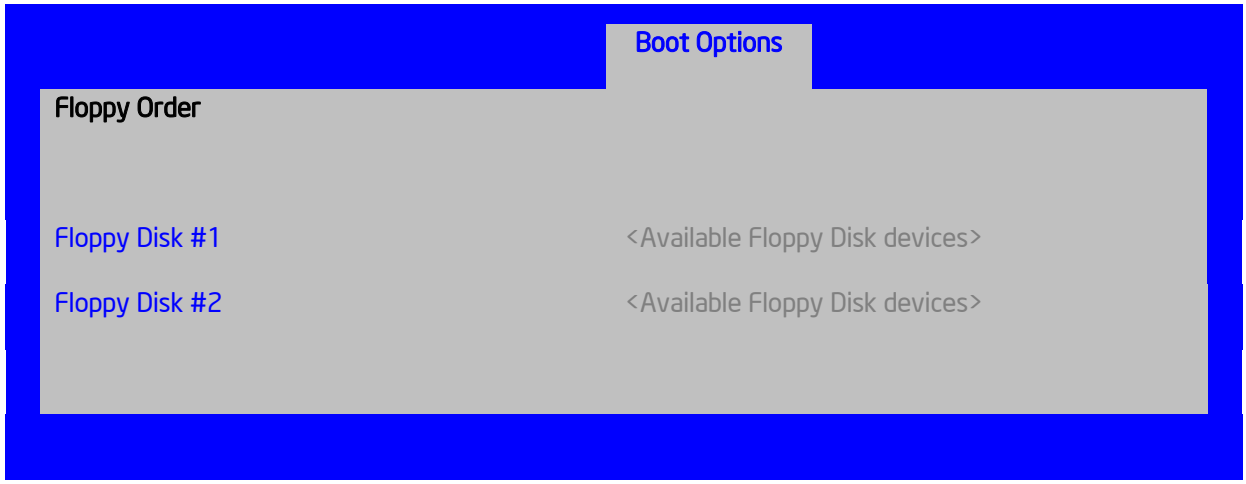


Figure 40. Floppy Order Screen

Table 50. Setup Utility – Floppy Order Fields

Setup Item	Options	Help Text	Comments

Setup Item	Options	Help Text	Comments
Floppy Disk #1	Available Floppy devices.	Set system boot order by selecting the boot option for this position.	Choose the order of booting among Floppy Disk devices by choosing which available Floppy Disk device should be in each position in the order.
Floppy Disk #2	Available Floppy devices.	Set system boot order by selecting the boot option for this position.	Choose the order of booting among Floppy Disk devices by choosing which available Floppy Disk device should be in each position in the order.

5.4.2.24 Network Device Order

The Network Device Order screen allows the user to control the order in which BIOS attempts to boot from the network bootable devices installed in the system. This screen is only available when there is at least one network bootable device available in the system configuration.

To access this screen from the **Main** screen, select **Boot Options > Network Device Order**. To move to another screen, press the <Esc> key to return to the **Boot Options** screen, then select the desired screen.

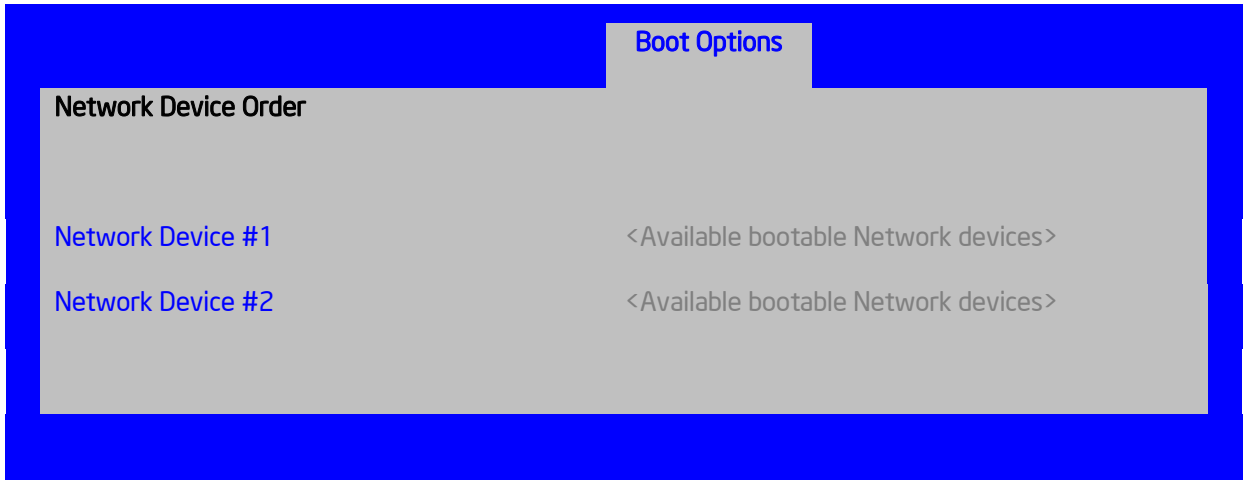


Figure 41. Network Device Order Screen

Table 51. Setup Utility – Network Device Order Fields

Setup Item	Options	Help Text	Comments
Network Device #1	Available Network Devices.	Set system boot order by selecting the boot option for this position.	Choose the order of booting among Network Devices by choosing which available Network Device should be in each position in the order.

Setup Item	Options	Help Text	Comments
Network Device #2	Available Network Devices.	Set system boot order by selecting the boot option for this position.	Choose the order of booting among Network Devices by choosing which available Network Device should be in each position in the order.

5.4.2.25 BEV Device Order

The BEV Device Order screen allows the user to control the order in which BIOS attempts to boot from the BEV Devices installed in the system. This screen is only available when there is at least one BEV device available in the system configuration.

To access this screen from the Main screen, select Boot Options > BEV Device Order. To move to another screen, press the <Esc> key to return to the Boot Options screen, then select the desired screen.

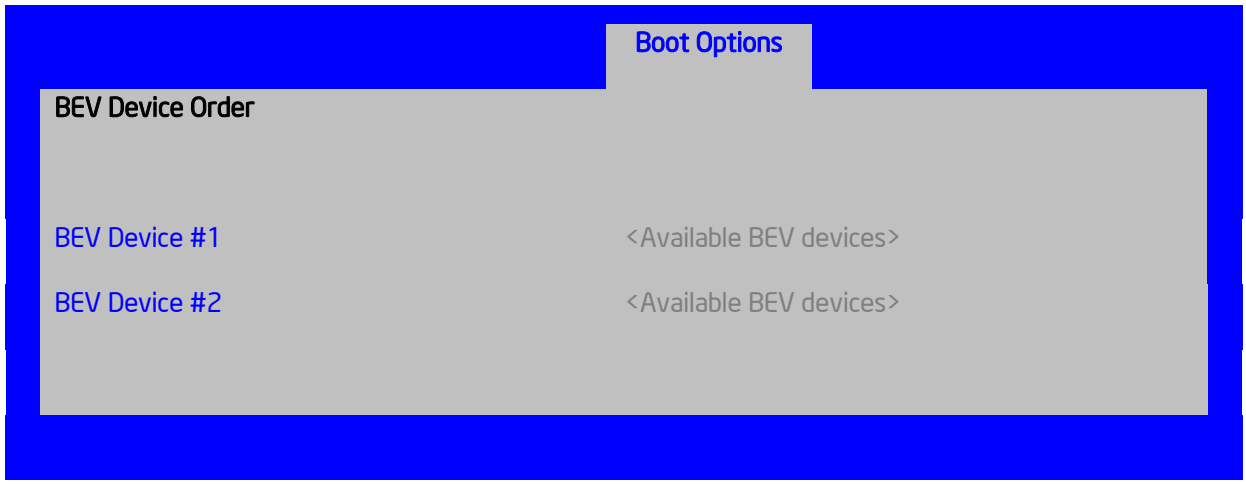


Figure 42. BEV Device Order Screen

Table 52. Setup Utility – BEV Device Order Fields

Setup Item	Options	Help Text	Comments
BEV Device #1	Available BEV Devices.	Set system boot order by selecting the boot option for this position.	Choose the order of booting among BEV Devices by choosing which available BEV Device should be in each position in the order.
BEV Device #2	Available BEV Devices.	Set system boot order by selecting the boot option for this position.	Choose the order of booting among BEV Devices by choosing which available BEV Device should be in each position in the order.

5.4.2.26 Add EFI Boot Option

The Add EFI Boot Option screen allows the user to add an EFI boot option to the boot order. This screen is only available when there is at least one EFI bootable device present in the system configuration. The “Internal EFI Shell” Boot Option is permanent and cannot be added or deleted.

To access this screen from the Main screen, select Boot Options > Add EFI Boot Option. To move to another screen, press the <Esc> key to return to the Boot Options screen, then select the desired screen.

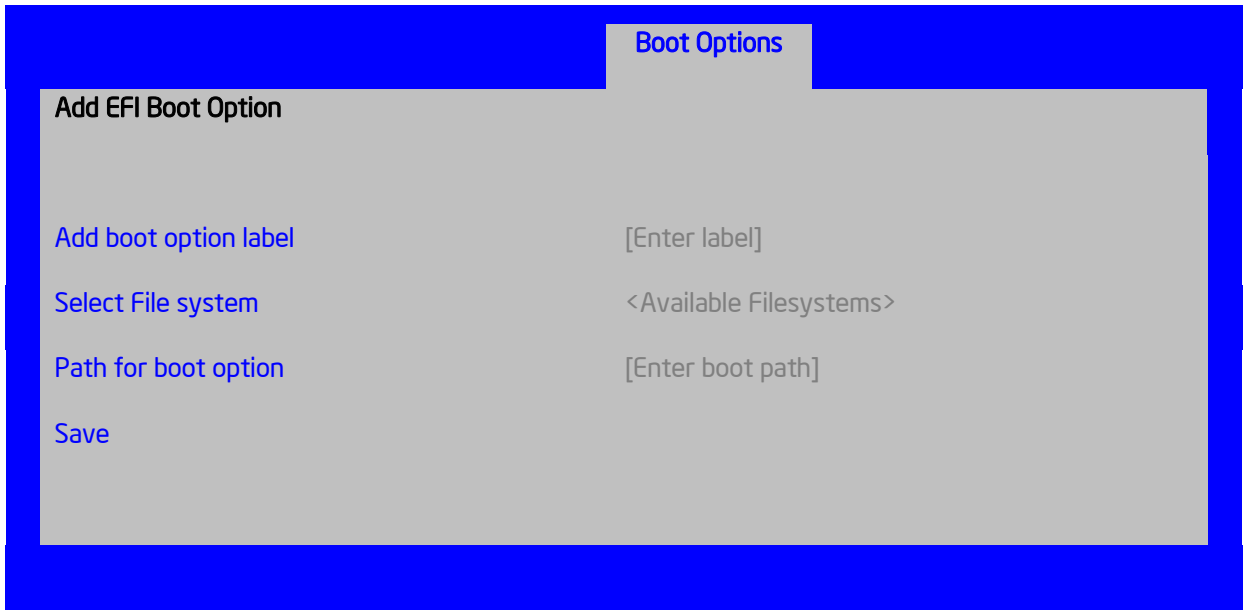


Figure 43. Add EFI Boot Option Screen

Table 53. Setup Utility – Add Boot Option Fields

Setup Item	Options	Help Text	Comments
Add boot option label	Enter Label	Create the label for the new boot option.	This label becomes an abbreviation for this Boot Path.
Select File system	Available Filesystems	Select one filesystem from this list.	Choose the filesystem on which this boot path resides.
Path for boot option	Enter boot path	Enter the path to the boot option in the format \path\filename.efi.	This will be the Boot Path, residing on the filesystem chosen, which will be entered into the Boot Order with the Label entered above.
Save	None	Save the boot option	Selection only. This will save the new Boot Option into the Boot Order.

5.4.2.27 Delete EFI Boot Option

The Delete EFI Boot Option screen allows the user to remove an EFI boot option from the boot order. The “Internal EFI Shell” Boot Option will not be listed, since it is permanent and cannot be added or deleted.

To access this screen from the **Main** screen, select **Boot Options > Delete EFI Boot Option**. To move to another screen, press the <Esc> key to return to the **Boot Options** screen, then select the desired screen.

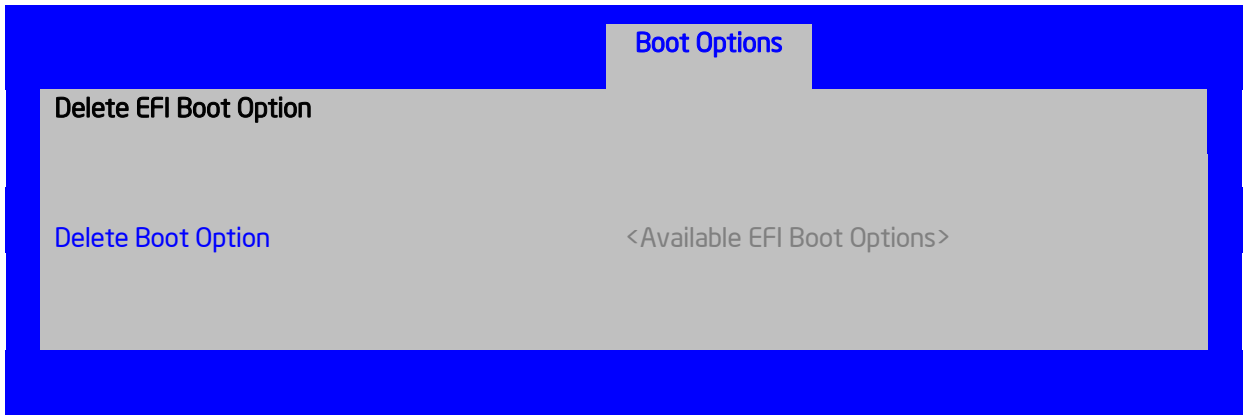


Figure 44. Delete EFI Boot Option Screen

Table 54. Setup Utility – Delete EFI Boot Option Fields

Setup Item	Options	Help Text	Comments
Delete Boot Option	Available EFI Boot Options	Select one to delete.	This will not allow a user to delete the EFI Shell.

5.4.2.28 Boot Manager Screen (Tab)

The Boot Manager screen allows the user to view a list of devices available for booting, and to select a boot device for immediately booting the system. There is no predetermined order for listing bootable devices. They are simply listed in order of discovery. Regardless of whether any other bootable devices are available, the “Internal EFI Shell” will always be available.

To access this screen from the **Main** screen or other top-level “Tab” screen, press the right or left arrow keys to traverse the tabs at the top of the Setup screen until the **Boot Manager** screen is selected.

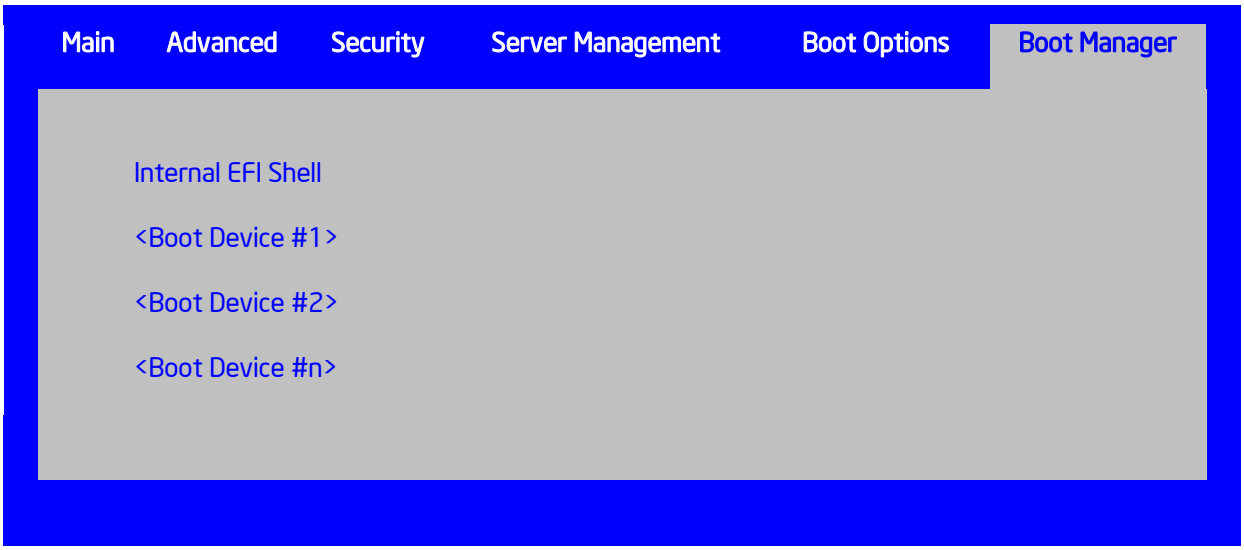


Figure 45. Boot Manager Screen

Table 55. Setup Utility – Boot Manager Screen Fields

Setup Item	Options	Help Text	Comments
Internal EFI Shell	None	Select this option to boot now. **Note:** This list is not the system boot option order. Use the Boot Options menu to view and configure the system boot option order.	The EFI Shell will always be present in the list of bootable devices.
Boot Device #n	None	Select this option to boot now. **Note:** This list is not the system boot option order. Use the Boot Options menu to view and configure the system boot option order.	These are names of bootable devices discovered in the system. The system user can choose any of them from which to initiate a one-time boot – that is, booting from any device in this list will not permanently affect the defined system Boot Order. These bootable devices are not displayed in any specified order, particularly not in the system Boot Order established by the Boot Options screen. This is just a list of bootable devices in the order in which they were enumerated.

5.4.2.29 Error Manager Screen (Tab)

The Error Manager screen displays any POST Error Codes encountered during BIOS POST, along with an explanation of the meaning of the Error Code in the form of a Help Text. This is an Information Only screen.

To access this screen from the Main screen or other top-level “Tab” screen, press the right or left arrow keys to traverse the tabs at the top of the Setup screen until the Error Manager screen is selected.

Figure 46. Error Manager Screen

Table 56. Setup Utility – Error Manager Screen Fields

Setup Item	Options	Help Text	Comments
ERROR CODE	Post Code	None	This is a POST Error Code – a BIOS-originated error that occurred during POST initialization.
SEVERITY	Minor Major Fatal	None	Each POST Error Code has a Severity associated with it.
INSTANCE	Depend on Error Code	None	Where applicable, this field shows a value indicating which one of a group of components was responsible for generating the POST Error Code that is being reported.
Description	None	Description of POST Error Code	This is a description of the meaning of the POST Error Code that is being reported. This text actually appears in the screen space that is usually reserved for “Help” messages.

5.4.2.30 Save and Exit Screen (Tab)

The Save and Exit screen allows the user to choose whether to save or discard the configuration changes made on other Setup screens. It also allows the user to restore the BIOS settings to the factory defaults or to save or restore them to a set of user-defined default values. If Load Default Values is selected, the factory default settings (noted in bold in the Setup screen images) are applied. If Load User Default Values is selected, the system is restored to previously saved User Default Values.

To access this screen from the **Main** screen or other top-level **Tab** screen, press the right or left arrow keys to traverse the tabs at the top of the Setup screen until the **Exit** screen is selected.

Note that there is a Legal Disclaimer footnote at the bottom of the Save & Exit screen:

*Certain brands and names may be claimed as the property of others.

This is reference to any instance in the Setup screens where names belonging to other companies may appear. For example, “LSI*” appears in Setup in the context of Mass Storage RAID options.

Figure 47. Save & Exit Screen

Table 57. Setup Utility – Exit Screen Fields

Setup Item	Options	Help Text	Comments

Setup Item	Options	Help Text	Comments
Save Changes and Exit	None	Exit the BIOS Setup utility after saving changes. The system reboots if required. The [F10] key can also be used.	Selection only. Select this line and press the <Enter> key to exit Setup with any changes in BIOS settings saved. If there have been no changes made in the settings, the BIOS will resume executing POST. If changes have been made in BIOS settings, a confirmation pop-up will appear. If the "Save Changes & Exit" action is positively confirmed, any persistent changes will applied and saved to the BIOS settings in NVRAM storage, then the system will reboot if necessary (which is normally the case). If the "Save Changes & Exit" action is not confirmed, BIOS will resume executing Setup. The **<F10>** function key may also be used from anyplace in Setup to initiate a "Save Changes & Exit" action.
Discard Changes and Exit	None	Exit the BIOS Setup utility without saving changes. The [Esc] key can also be used.	Selection only. Select this line and press the <Enter> key to exit Setup without saving any changes in BIOS settings. If there have been no changes made in the settings, the BIOS will resume executing POST. If changes have been made in BIOS settings, a confirmation pop-up will appear. If the "Discard Changes & Exit" action is positively confirmed, all pending changes will be discarded and BIOS will resume executing POST. If the "Discard Changes & Exit" action is not confirmed, BIOS will resume executing Setup without discarding any changes. The **<Esc>** key may also be used in Setup to initiate a "Discard Changes & Exit" action.
Save Changes	None	Save Changes made so far to any of the setup options.	Selection only. Select this line and press the **<Enter>** key to save any pending changes in BIOS settings. Also, the user should be aware that most changes require a reboot to become active. If changes have been made and saved, without exiting Setup, the system should be rebooted later even if no additional changes are made.

Setup Item	Options	Help Text	Comments
Discard Changes	None	Discard Changes made so far to any of the setup options.	Selection only. Select this line and press the <Enter> key to discard any pending unsaved changes in BIOS settings. If there have been no changes made in the settings, the BIOS will resume executing POST. If changes have been made in BIOS settings and not yet saved, a confirmation pop-up will appear. If the "Discard Changes" action is positively confirmed, all pending changes will be discarded and BIOS will resume executing POST. If the "Discard Changes" action is not confirmed, BIOS will resume executing Setup without discarding pending changes.
Load Default Values	None	Load Defaults Values for all the setup options.	Selection only. Select this line and press the <Enter> key to load default values for all BIOS settings. These are the initial factory settings ("failsafe" settings) for all BIOS parameters. There will be a confirmation popup to verify that the user really meant to take this action. After initializing all BIOS settings to default values, the BIOS will resume executing Setup, so the user may make additional changes in the BIOS settings if necessary (for example, Boot Order) before doing a "Save Changes and Exit" with a reboot to make the default settings take effect, including any changes made after loading the defaults. The **<F9>** function key may also be used from any place in Setup to initiate a "Load Default Values" action.

Setup Item	Options	Help Text	Comments
Save as User Default Values	None	Save the changes made so far as User Default Values.	Selection only. Select this line and press the <Enter> key to save the current state of the settings for all BIOS parameters as a customized set of "User Default Values". These are a user-determined set of BIOS default settings that can be used as an alternative instead of the initial factory settings ("failsafe" settings) for all BIOS parameters. By changing the BIOS settings to values that the user prefers to have for defaults, and then using this operation to save them as "User Default Values", that version of BIOS settings can be restored at any time by using the following "Load User Default Values" operation. There will be a confirmation popup to verify that the user really intended to take this action. Loading the "factory default" values with F9 or the "Load Default Values" – or by any other means – does not affect the User Default Values. They remain set to whatever values they were saved as.
Load User Default Values	None	Load user default values to all the set options.	Selection only. Select this line and press the <Enter> key to load User Default Values for all BIOS settings. These are user-customized BIOS default settings for all BIOS parameters, previously established by doing a "Save User Defaults" action (see above). There will be a confirmation popup to verify that the user really intended to take this action.

5.5 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.

You can send the request to reset the system to the defaults in the following ways:

- Pressing <F9> from within the BIOS Setup utility
- Moving the clear system configuration jumper
- IPMI command (set System Boot options command)
- Int15 AX=DA209
- Choosing Load User Defaults from the Exit page of the BIOS Setup loads user set defaults instead of the BIOS factory defaults

The recommended steps to load the BIOS defaults are:

1. Power down the system (Do not remove AC power)
2. Move the BIOS DFLT jumper from pins 1-2 to pins 2-3
3. Move the BIOS DFLT jumper from pins 2-3 to pins 1-2
4. Power up the system

.

6. Configuration Jumpers

The following table provides a summary and description of configuration, test, and debug jumpers on the Intel® Server Board S1600JP. The server board has several 3-pin jumper blocks that can be used.

Pin 1 on each jumper block can be identified by the following symbol on the silkscreen:

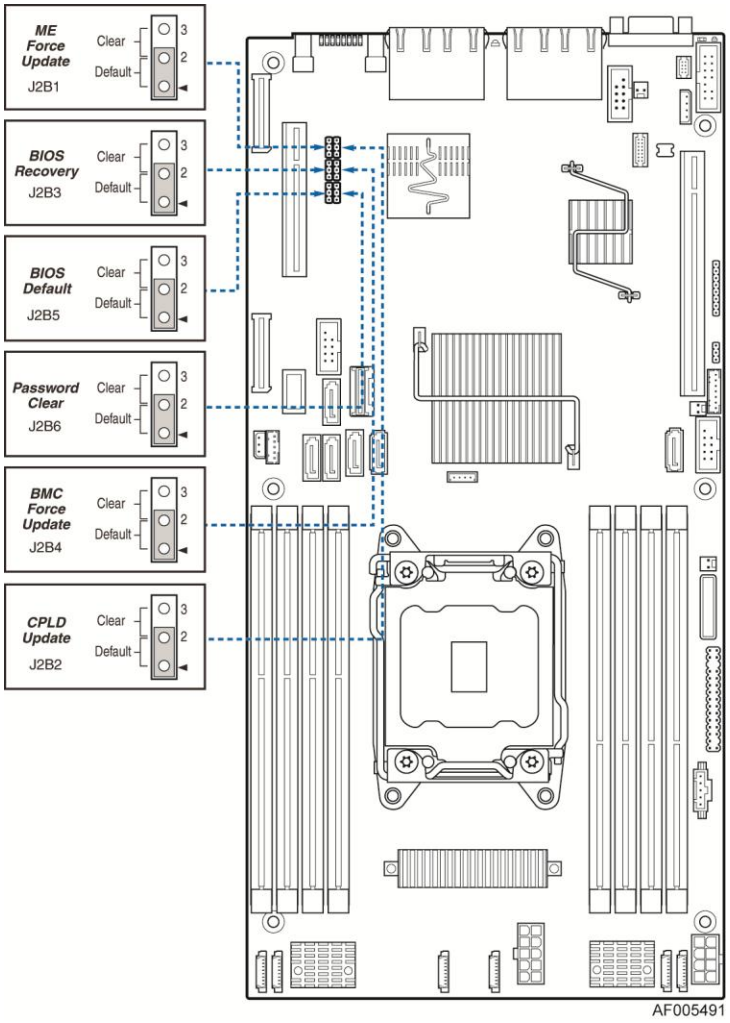


Figure 48. Jumper Blocks (J2B1, J2B3, J2B5, J2B6, J2B4, and J2B2)

Table 58. Server Board Jumpers (J6B1, J1E2, J1E3, J1E1, J1D5)

Jumper Name	Jumper Position	Mode of Operation	Note
J2B1: ME Force Update	1-2	Normal	Normal mode
	2-3	Update	ME in force update mode
J2B4: BMC Force Update jumper	1-2	Normal	Normal mode
	2-3	Update	BMC in force update mode

Jumper Name	Jumper Position	Mode of Operation	Note
J2B6: Password Clear	1-2	Normal	Normal mode, password in protection
	2-3	Clear Password	BIOS password is cleared
J2B3: BIOS Recovery Mode	1-2	Normal	Normal mode
	2-3	Recovery	BIOS in recovery mode
J2B2: CPLD Update	1-2	Normal	Normal mode
	2-3	Update	
J2B5: BIOS Default	1-2	Normal	Normal mode
	2-3	Clear BIOS Settings	BIOS settings are reset to factory default

6.1.1 Force Integrated BMC Update (J2B4)

When performing a standard BMC firmware update procedure, the update utility places the BMC into an update mode, allowing the firmware to load safely onto the flash device. In the unlikely event the BMC firmware update process fails due to the BMC not being in the proper update state, the server board provides a BMC Force Update jumper (J6B1) which will force the BMC into the proper update state. The following procedure should be followed in the event the standard BMC firmware update process fails.

Table 59. Force Integrated BMC Update Jumper

Jumper Position	Mode of Operation	Note
1-2	Normal	Normal operation
2-3	Update	BMC in force update mode

Steps to perform Force BMC Update:

1. Power down and remove the AC power cord.
2. Open the server chassis. See your server chassis documentation for instructions.
3. Move jumper from the default operating position, covering pins1 and 2, to the enabled position, covering pins 2 and 3.
4. Close the server chassis.
5. Reconnect the AC cord and power up the server.
6. Perform the BMC firmware update procedure as documented in the *ReleaseNote.TXT* file included in the given BMC firmware update package. After successful completion of the firmware update process, the firmware update utility may generate an error stating the BMC is still in update mode.
7. Power down and remove the AC power cord.
8. Open the server chassis.
9. Move the jumper from the enabled position, covering pins 2 and 3 to the disabled position, covering pins 1 and 2.
10. Close the server chassis.
11. Reconnect the AC cord and power up the server.

Note: Normal BMC functionality is disabled with the Force BMC Update jumper is set to the enabled position. You should never run the server with the BMC Force Update jumper set in this position. You should only use this jumper setting when the standard firmware update process fails. This jumper should remain in the default/disabled position when the server is running normally.

The server board has several 3-pin jumper blocks that can be used to configure, protect, or recover specific features of the server board.

6.1.2 Force ME Update (J2B1)

When this 3-pin jumper is set, it manually puts the ME firmware in update mode, which enables the user to update ME firmware code when necessary.

Table 60. Force ME Update Jumper

Jumper Position	Mode of Operation	Note
1-2	Normal	Normal operation
2-3	Update	ME in force update mode

Note: Normal ME functionality is disabled with the Force ME Update jumper is set to the enabled position. Never run the server with the ME Force Update jumper set in this position.

Only use this jumper setting when the standard firmware update process fails. This jumper should remain in the default/disabled position when the server is running normally.

Steps to perform the Force ME Update:

1. Power down and remove the AC power cord.
2. Open the server chassis. For instructions, see your server chassis documentation.
3. Move jumper from the default operating position (covering pins 1 and 2) to the enabled position (covering pins 2 and 3).
4. Close the server chassis.
5. Reconnect the AC cord and power up the server.
6. Perform the ME firmware update procedure as documented in the *README.TXT* file that is included in the given ME firmware update package (same package as BIOS).
7. Power down and remove the AC power cord.
8. Open the server chassis.
9. Move jumper from the enabled position (covering pins 2 and 3) to the disabled position (covering pins 1 and 2).
10. Close the server chassis.

6.1.3 Password Clear (J2B6)

The user sets this 3-pin jumper to clear the password.

Table 61. Password Clear Jumper

Jumper Position	Mode of Operation	Note
1-2	Normal	Normal mode, password in protection
2-3	Clear Password	BIOS password is cleared

Steps to clear the BIOS password:

1. Power down server. Do not unplug the power cord.
2. Open the chassis. For instructions, see your server chassis documentation.
3. Move jumper (J1B6) from the default operating position, covering pins 1 and 2, to the password clear position, covering pins 2 and 3.
4. Close the server chassis.
5. Power up the server, wait 10 seconds or until POST completes.
6. Power down the server.
7. Open the chassis and move the jumper back to default position, covering pins 1 and 2.
8. Close the server chassis.
9. Power up the server.

The password is now cleared and you can reset it by going into the BIOS setup.

6.1.4 BIOS Recovery Mode (J2B3)

The Intel® Server Board S1600JP uses BIOS recovery to repair the system BIOS from flash corruption in the main BIOS and Boot Block. This 3-pin jumper is used to reload the BIOS when the image is suspected to be corrupted. For directions on how to recover the BIOS, refer to the specific *BIOS release notes*.

Table 62. BIOS Recovery Mode Jumper

Jumper Position	Mode of Operation	Note
1-2	Normal	Normal mode
2-3	Recovery	BIOS in recovery mode

You can accomplish a BIOS recovery from the SATA CD and USB Mass Storage device. Please note that this platform does not support recovery from a USB floppy.

The recovery media must contain the following files under the root directory:

1. RML.ROM
2. UEFI iFlash32 11.0 Build 2 (including iFlash32.efi and ipmi.efi)
3. *Rec.CAP
4. Startup.nsh (update accordingly to use proper *Rec.CAP file)

The BIOS starts the recovery process by first loading and booting to the recovery image file (RML.ROM) on the root directory of the recovery media (USB disk). This process takes place before any video or console is available. Once the system boots to this recovery image file (FVMAIN.FV), it boots automatically into the EFI Shell to invoke the Startup.nsh script and start the flash update application (IFlash32.efi). IFlash32.efi requires the supporting BIOS Capsule image file (*Rec.CAP).

After the update is complete, a message displays, stating the “BIOS has been updated successfully”. This indicates the recovery process is finished.

The user should then switch the recovery jumper back to normal operation and restart the system by performing a power cycle.

The following steps demonstrate this recovery process:

1. Power OFF the system.
2. Insert recovery media.
3. Switch the recovery jumper. Details regarding the jumper ID and location can be obtained from the Board EPS for that Platform.
4. Power ON the system.
5. The BIOS POST screen will appear displaying the progress, and the system automatically boots to the EFI SHELL.
6. The Startup.nsh file executes, and initiates the flash update (IFlash32.efi) with a new capsule file (*Rec.CAP). The regular iFlash message displays at the end of the process—once the flash update succeeds.

7. Power OFF the system, and revert the recovery jumper position to "normal operation".
8. Power ON the system.
9. Do NOT interrupt the BIOS POST during the first boot.

6.1.5 Reset BIOS Settings (J2B5)

The former name for this jumper is CMOS Clear. It is used to be the BIOS reset jumper. Since the previous generation, the BIOS has moved CMOS data to the NVRAM region of the BIOS flash. The BIOS checks during boot to determine if the data in the NVRAM needs to be set to default. (Same function as F9 in BIOS that loads BIOS by default.)

Table 63. Reset BIOS Jumper

Jumper Position	Mode of Operation	Note
1-2	Normal	Normal mode
2-3	Clear BIOS settings	BIOS settings are reset to factory default

Steps to clear BIOS settings:

1. Power down server. Do not unplug the power cord.
2. Open the server chassis. For instructions, see your server chassis documentation.
3. Move jumper (J1D5) from the default operating position, covering pins 1 and 2, to the reset/clear position, covering pins 2 and 3.
4. Wait five seconds.
5. Remove AC power.
6. Move the jumper back to default position, covering pins 1 and 2.
7. Close the server chassis.
8. Power up the server.

The BIOS settings are now cleared and you can reset it by going into the BIOS setup.

Note: Removing AC Power before performing the BIOS settings Clear operation causes the system to automatically power up and immediately power down, after the procedure is followed and AC power is re-applied. If this happens, remove the AC power cord again, wait 30 seconds, and re-install the AC power cord. Power-up the system and proceed to the <F2> BIOS Setup Utility to reset the desired settings.

7. Connector/Header Locations and Pin-out

7.1 Power Connectors

To facilitate customers who want to cable to this board from a power supply, the power connectors are implemented through one 10-pin connector and one 8-pin connector.

Table 64. Main Power Supply Connector 10-pin 2x5 Connector Pin-Out (J4K1)

Pin	Signal Name	Pin	Signal Name
1	PSON	6	5VSB
2	GND	7	PWROK
3	GND	8	3.3V
4	GND	9	3.3V
5	5V	10	Reserved

Table 65. Main Power Supply Connector 8-pin 2x4 Connector Pin-Out (J6K1)

Pin	Signal Name	Pin	Signal Name
1	GND	5	+12V
2	GND	6	+12V
3	GND	7	+12V
4	GND	8	+12V

7.2 System Management Headers

7.2.1 Intel® Remote Management Module 4 (Intel® RMM4 Lite) Connector

A 7-pin Intel® RMM4 Lite connector (J6A2) is included on the server board to support the optional Intel® Remote Management Module 4. There is no support for third-party management cards on this server board.

Note: This connector is not compatible with the Intel® Remote Management Module 3 (Intel® RMM3).

Table 66. Intel® RMM4 Lite Connector Pin-out (J6A2)

Pin	Signal Description	Pin	Signal Description
1	P3V3_AUX	2	SPI_BMC_BK_DI
3	Key Pin	4	SPI_BMC_BK_CLK
5	SPI_BMC_BK_DO	6	GND
7	SPI_BMC_BK_CS_N	8	GND

7.2.2 IPMB Header

Table 67. IPMB Header Pin-Out (J6A4)

Pin	Signal Name
1	SMB_IPMB_5VSB_DAT
2	GND

Pin	Signal Name
3	SMB_IPMB_5VSB_CLK
4	P5V_STBY

7.2.3 Power Button

The BIOS supports a front control panel power button. Pressing the power button initiates a request that the Integrated BMC forwards to the ACPI power state machines in the chipset. It is monitored by the Integrated BMC and does not directly control power on the power supply.

- **Power Button — Off to On**
  The Integrated BMC monitors the power button and the wake-up event signals from the chipset. A transition from either source results in the Integrated BMC starting the power-up sequence. Since the processor is not executing, the BIOS does not participate in this sequence. The hardware receives the power good and reset signals from the Integrated BMC and then transitions to an ON state.
- **Power Button — On to Off (operating system absent)**
  The System Control Interrupt (SCI) is masked. The BIOS sets up the power button event to generate an SMI and checks the power button status bit in the ACPI hardware registers when an SMI occurs. If the status bit is set, the BIOS sets the ACPI power state of the machine in the chipset to the OFF state. The Integrated BMC monitors power state signals from the chipset and de-asserts PS_PWR_ON to the power supply. As a safety mechanism, if the BIOS fails to service the request, the Integrated BMC automatically powers off the system in four to five seconds.
- **Power Button — On to Off (operating system present)**
  If an ACPI operating system is running, pressing the power button switch generates a request through SCI to the operating system to shut down the system. The operating system retains control of the system and the operating system policy determines the sleep state into which the system transitions, if any. Otherwise, the BIOS turns off the system.

7.2.4 Reset Button

The platform supports a front control panel reset button. Pressing the reset button initiates a request forwarded by the Integrated BMC to the chipset. The BIOS does not affect the behavior of the reset button.

7.2.5 Chassis Identify Button

The front panel Chassis Identify button toggles the state of the chassis ID LED. If the LED is off, pushing the ID button lights the LED. It remains lit until the button is pushed again or until a *Chassis Identify* or a *Chassis Identify LED* command is received to change the state of the LED.

7.2.6 Power LED

The green power LED is active when the system DC power is on. The power LED is controlled by the BIOS. The power LED reflects a combination of the state of system (DC) power and the system ACPI state. The following table identifies the different states that the power LED can assume.

Table 68. Power LED Indicator States

State	ACPI	Power LED
Power off	No	Off
Power on	No	Solid on
S5	Yes	Off
S1 Sleep	Yes	~1 Hz blink
S0	Yes	Solid on

7.2.7 System Status LED

Note: The system status LED state shows the state for the current, most severe fault. For example, if there was a critical fault due to one source and a non-critical fault due to another source, the system status LED state would be solid on (the critical fault state).

The system status LED is a bicolor LED. Green (status) shows a normal operation state or a degraded operation. Amber (fault) shows the system hardware state and overrides the green status.

The Integrated BMC-detected state and the state from the other controllers, such as the SCSI/SATA hot-swap controller state, are included in the LED state. For fault states monitored by the Integrated BMC sensors, the contribution to the LED state follows the associated sensor state, with the priority going to the most critical state currently asserted.

When the server is powered down (transitions to the DC-off state or S5), the Integrated BMC is still on standby power and retains the sensor and front panel status LED state established prior to the power-down event.

The following table maps the system state to the LED state:

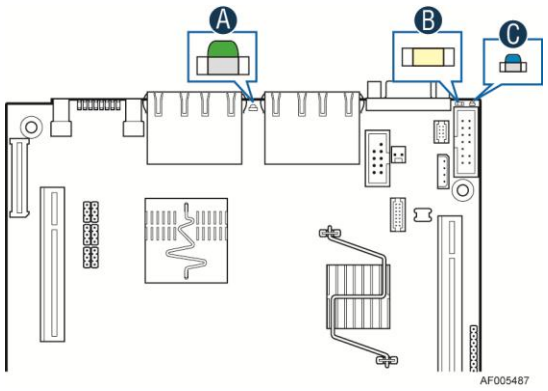


Figure 49. System Status LED (A), 5V StandBy LED (B), and ID LED (C)

Table 69. System Status LED

Color	State	System Status	Description
Green	Solid on	Ok	System ready

Color	State	System Status	Description
Green	~1 Hz blink	Degraded	BIOS detected ▪ Unable to use all of the installed memory (more than one DIMM installed).[1] ▪ In a mirrored configuration, when memory mirroring takes place and system loses memory redundancy. This is not covered by (2).[1] ▪ PCI Express* correctable link errors. Integrated BMC detected ▪ Redundancy loss such as a power supply or fan. Applies only if the associated platform subsystem has redundancy capabilities. ▪ CPU disabled – if there are two CPUs and one CPU is disabled. ▪ Fan alarm – Fan failure. Number of operational fans should be more than minimum number needed to cool the system. ▪ Non-critical threshold crossed – Temperature, voltage, power nozzle, power gauge, and PROCHOT2 (Therm Ctrl) sensors. ▪ Battery failure. ▪ Predictive failure when the system has redundant power supplies.
Amber	~1 Hz blink	Non-Fatal	Non-fatal alarm – system is likely to fail: BIOS Detected ▪ In non-mirroring mode, if the threshold of ten correctable errors is crossed within the window.[1] ▪ PCI Express* uncorrectable link errors. Integrated BMC Detected ▪ Critical threshold crossed – Voltage, temperature, power nozzle, power gauge, and PROCHOT (therm Ctrl) sensors. ▪ VRD Hot asserted. ▪ Minimum number of fans to cool the system are not present or have failed.
Amber	Solid on	Fatal	Fatal alarm – system has failed or shut down: BIOS Detected ▪ DIMM failure when there is one DIMM present and no good memory is present.[1] ▪ Run-time memory uncorrectable error in non-redundant mode.[1] ▪ CPU configuration error (for instance, processor stepping mismatch). Integrated BMC Detected ▪ CPU CATERR signal asserted. ▪ CPU 1 is missing. ▪ CPU THERMTRIP. ▪ No power good – power fault. ▪ Power Unit Redundancy sensor – Insufficient resources offset (indicates not enough power supplies are present).
Off	N/A	Not ready	Main power off

Notes:

1. The BIOS detects these conditions and sends a Set Fault Indication command to the Integrated BMC to provide the contribution to the system status LED.
2. Support for an upper, non-critical threshold limit is not provided in default SDR configuration. However if a user does enable this threshold in the SDR, then the system status LED should behave as described.

7.2.8 Chassis ID LED

The chassis ID LED provides a visual indication of a system being serviced. The state of the chassis ID LED is affected by the following:

- Toggled by the chassis ID button
- Controlled by the *Chassis Identify* command (IPMI)
- Controlled by the *Chassis Identify LED* command (OEM)

Table 70. Chassis ID LED Indicator States

State	LED State
Identify active through button	Solid on
Identify active through command	~1 Hz blink
Off	Off

There is no precedence or lock-out mechanism for the control sources. When a new request arrives, all previous requests are terminated. For example, if the chassis ID LED is blinking and the chassis ID button is pressed, then the chassis ID LED changes to solid on. If the button is pressed again with no intervening commands, the chassis ID LED turns off.

7.3 I/O Connectors

7.3.1 PCI Express* Connectors

The Intel® Server Board S1600JP uses three PCI Express* slots physically with different pint out definition. Each riser slot has dedicated usage and cannot be used for normal PCIe based add-in card.

- Riser Slot 1: Riser to support PCIe x16 add-in card
- Riser Slot 2: Riser to support PCIe x8 Intel® IOM card
- Riser Slot 3: Riser to support PCIe x16 add-in card or double width PCI Express* card

The pin-outs for the slots are shown in the following tables.

Table 71. PCI Express* x16 Riser Slot 1 Connector (J6B1)

Pin	Pin Name	Description	Pin	Pin Name	Description
B1	12V	66W for double width PCI Express*card	A1	Present1	
B2	12V	66W for double width PCI Express*card	A2	12V	66W for double width PCI Express*card
B3	12V	66W for double width PCI Express*card	A3	12V	66W for double width PCI Express*card
B4	GND		A4	GND	
B5	SMBUS_R4 CLK		A5	3.3V	
B6	SMBUS_R4 DAT	For wake on LAN	A6	spare	
B7	GND		A7	spare	
B8	3.3V		A8	3.3V	

Pin	Pin Name	Description	Pin	Pin Name	Description
B9	Spare		A9	3.3V	
B10	3.3VAUX	For wake on LAN	A10	3.3V	
B11	WAKE#	For wake on LAN	A11	PERST#	
KEY					
B12	3.3V		A12	GND	
B13	GND		A13	REFCLK1+	Clock pair 1
B14	PETxP0	Tx Lane 0+	A14	REFCLK1-	Clock pair 1
B15	PETxN0	Tx Lane 0+	A15	GND	
B16	GND		A16	PERxP0	Rx Lane 0+
B17	Present2		A17	PERxN0	Rx Lane 0-
B18	GND		A18	GND	
B19	PETxP1	Tx Lane 1+	A19	3.3V	
B20	PETxN1	Tx Lane 1-	A20	GND	
B21	GND		A21	PERxP1	Rx Lane 1+
B22	GND		A22	PERxN1	Rx Lane 1-
B23	PETxP2	Tx Lane 2+	A23	GND	
B24	PETxN2	Tx Lane 2-	A24	GND	
B25	GND		A25	PERxP2	Rx Lane 2+
B26	GND		A26	PERxN2	Rx Lane 2-
B27	PETxP3	Tx Lane 3+	A27	GND	
B28	PETxN3	Tx Lane 3-	A28	GND	
B29	GND		A29	PERxP3	Rx Lane 3+
B30	3.3V		A30	PERxN3	Rx Lane 3-
B31			A31	GND	
B32	GND		A32	REFCLK2+	Clock pair 2
B33	PETxP4	Tx Lane 4+	A33	REFCLK2-	Clock pair 2
B34	PETxN4	Tx Lane 4-	A34	GND	
B35	GND		A35	PERxP4	Rx Lane 4+
B36	GND		A36	PERxN4	Rx Lane 4-
B37	PETxP5	Tx Lane 5+	A37	GND	
B38	PETxN5	Tx Lane 5-	A38	GND	
B39	GND		A39	PERxP5	Rx Lane 5+
B40	GND		A40	PERxN5	Rx Lane 5-
B41	PETxP6	Tx Lane 6+	A41	GND	
B42	PETxN6	Tx Lane 6-	A42	GND	
B43	GND		A43	PERxP6	Rx Lane 6+
B44	GND		A44	PERxN6	Rx Lane 6-
B45	PETxP7	Tx Lane 7+	A45	GND	
B46	PETxN7	Tx Lane 7-	A46	GND	
B47	GND		A47	PERxP7	Rx Lane 7+
B48	Riser ID 0		A48	PERxN7	Rx Lane 7-
B49	GND		A49	GND	
B50	PETxP8	Tx Lane 8+	A50	Riser ID 1	
B51	PETxN8	Tx Lane 8-	A51	GND	
B52	GND		A52	PERxP8	Rx Lane 8+
B53	GND		A53	PERxN8	Rx Lane 8-
B54	PETxP9	Tx Lane 9+	A54	GND	
B55	PETxN9	Tx Lane 9-	A55	GND	
B56	GND		A56	PERxP9	Rx Lane 9+
B57	GND		A57	PERxN9	Rx Lane 9-
B58	PETxP10	Tx Lane 10+	A58	GND	

Pin	Pin Name	Description	Pin	Pin Name	Description
B59	PETxN10	Tx Lane 10-	A59	GND	
B60	GND		A60	PERxP10	Rx Lane 10+
B61	GND		A61	PERxN10	Rx Lane 10-
B62	PETxP11	Tx Lane 11+	A62	GND	
B63	PETxN11	Tx Lane 11-	A63	GND	
B64	GND		A64	PERxP11	Rx Lane 11+
B65	GND		A65	PERxN11	Rx Lane 11-
B66	PETxP12	Tx Lane 12+	A66	GND	
B67	PETxN12	Tx Lane 12-	A67	GND	
B68	GND		A68	PERxP12	Rx Lane 12+
B69	GND		A69	PERxN12	Rx Lane 12-
B70	PETxP13	Tx Lane 13+	A70	GND	
B71	PETxN13	Tx Lane 13-	A71	GND	
B72	GND		A72	PERxP13	Rx Lane 13+
B73	GND		A73	PERxN13	Rx Lane 13-
B74	PETxP14	Tx Lane 14+	A74	GND	
B75	PETxN14	Tx Lane 14-	A75	GND	
B76	GND		A76	PERxP14	Rx Lane 14+
B77	GND		A77	PERxN14	Rx Lane 14-
B78	PETxP15	Tx Lane 15+	A78	GND	
B79	PETxN15	Tx Lane 15-	A79	GND	
B80	GND		A80	PERxP15	Rx Lane 15+
B81	REFCLK3+	Clock pair 3	A81	PERxN15	Rx Lane 15-
B82	REFCLK3-	Clock pair 3	A82	GND	

Table 72. PCI Express* x8 Riser Slot 2 Connector (J1A2)

Pin	Pin Name	Description	Pin	Pin Name	Description
B1	12V		A1	3.3V	
B2	12V		A2	3.3V	for use by IB rIOM
B3	12V		A3	3.3V	
B4	12V		A4	SMDATA	for rIOM temp sensor
B5	SMCLK	for rIOM temp sensor	A5	5VAUX	For DNM & IOM wake on LAN
B6	3.3V Aux	For DNM & IOM wake on LAN	A6	PRESENT#	rIOM function present
B7	GND		A7	RIOM_ACT#	Drive generic Activity LED
B8	TXD_0	RGMII txmit data	A8	RXD_3	RGMII receive data
B9	TXD_1	RGMII txmit data	A9	RXD_2	RGMII receive data
B10	TXD_2	RGMII txmit data	A10	RXD_1	RGMII receive data
B11	TXD_3	RGMII txmit data	A11	RXD_0	RGMII receive data
KEY					
B12	GND		A12	RX_CTL	RGMII receive Cntrl
B13	TX_CLK	RGMII txmit Clock	A13	GND	
B14	TX_CTL	RGMII txmit Cntrl	A14	RX_CLK	RGMII receive Clock

Pin	Pin Name	Description	Pin	Pin Name	Description
B15	MDIO		A15	MDC	
B16	PERST#		A16	GND	
B17	WAKE#		A17	REFCLK+	Clock pair 1
B18	PETxP0		A18	REFCLK-	Clock pair 1
B19	PETxN0		A19	GND	
B20	GND		A20	PERxP0	
B21	GND		A21	PERxN0	
B22	PETxP1		A22	GND	
B23	PETxN1		A23	GND	
B24	GND		A24	PERxP1	
B25	GND		A25	PERxN1	
B26	PETxP2		A26	GND	
B27	PETxN2		A27	GND	
B28	GND		A28	PERxP2	
B29	GND		A29	PERxN2	
B30	PETxP3		A30	GND	
B31	PETxN3		A31	GND	
B32	GND		A32	PERxP3	
B33	GND		A33	PERxN3	
B34	PETxP4		A34	GND	
B35	PETxN4		A35	GND	
B36	GND		A36	PERxP4	
B37	GND		A37	PERxN4	
B38	PETxP5		A38	GND	
B39	PETxN5		A39	GND	
B40	GND		A40	PERxP5	
B41	GND		A41	PERxN5	
B42	PETxP6		A42	GND	
B43	PETxN6		A43	GND	
B44	GND		A44	PERxP6	
B45	GND		A45	PERxN6	
B46	PETxP7		A46	GND	
B47	PETxN7		A47	GND	
B48	GND		A48	PERxP7	
B49	GND		A49	PERxN7	

Table 73. PCI Express* x16 Riser Slot 3 Connector (J1B1 and J1D1)

Side Even	Pin Name	Side Odd	Pin Name
60	12V	59	12V
58	GND	57	12V
56	3.3V	55	GND
54	3.3V	53	REFCLK1+
52	gnd	51	REFCLK1-
50	PETxP0	49	GND

Side Even	Pin Name	Side Odd	Pin Name
48	PETxN0	47	PERxP0
46	GND	45	PERxN0
44	PETxP1	43	GND
42	PETxN1	41	PERxP1
40	GND	39	PERxN1
38	PETxP2	37	GND
36	PETxN2	35	PERxP2
34	GND	33	PERxN2
32	PETxP3	31	GND
30	PETxN3	29	PERxP3
28	GND	27	PERxN3
26	PETxP4	25	GND
24	PETxN4	23	PERxP4
22	GND	21	PERxN4
20	PETxP5	19	GND
18	PETxN5	17	PERxP5
16	GND	15	PERxN5
14	PETxP6	13	GND
12	PETxN6	11	PERxP6
10	GND	9	PERxN6
8	PETxP7	7	GND
6	PETxN7	5	PERxP7
4	GND	3	PERxN7
2	3.3VAUX	1	GND
60	WAKE#	59	GND
58	PERST#	57	REFCLK2+
56	GND	55	REFCLK2-
54	PETxP8	53	GND
52	PETxN8	51	PERxP8
50	GND	49	PERxN8
48	PETxP9	47	GND
46	PETxN9	45	PERxP9
44	GND	43	PERxN9
42	PETxP10	41	GND
40	PETxN10	39	PERxP10
38	GND	37	PERxN10
36	PETxP11	35	GND
34	PETxN11	33	PERxP11
32	GND	31	PERxN11
30	PETxP12	29	GND
28	PETxN12	27	PERxP12
26	GND	25	PERxN12
24	PETxP13	23	GND
22	PETxN13	21	PERxP13
20	GND	19	PERxN13
18	PETxP14	17	GND

Side Even	Pin Name	Side Odd	Pin Name
16	PETxN14	15	PERxP14
14	GND	13	PERxN14
12	PETxP15	11	GND
10	PETxN15	9	PERxP15
8	GND	7	PERxN15
6	SMBUS_R4 CLK	5	GND
4	Spare	3	SMBUS_R4 DAT
2	Spare	1	Riser ID

7.3.2 VGA Connector

The following table details the pin-out definition of the external VGA connector (J5A1).

Table 74. VGA External Video Connector Pin-Out (J5A1)

Pin	Signal Name	Description
1	CRT_RED	Red (analog color signal R)
2	CRT_GREEN	Green (analog color signal G)
3	CRT_BLUE	Blue (analog color signal B)
4	NC	No connection
5	GND	Ground
6	GND	Ground
7	GND	Ground
8	GND	Ground
9	NC	No connection
10	GND	Ground
11	NC	No connection
12	CRT_DDCDATA	DDCDAT
13	CRT_HSYNC	HSYNC (horizontal sync)
14	CRT_VSYNC	VSYNC (vertical sync)
15	CRT_DDCCLK	DDCCLK

7.3.3 Internal Video for the front video

The following table details the pin-out of the internal video for front connector (J6A1) found on the back edge of the server board.

Table 75. Internal Video Connector Pin-Out (J6A1)

Pin	Signal Name	Pin	Signal Name
1	Red	2	R_RTN (Red Return)
3	Green	4	G_RTN (Green Return)
5	Blue	6	B_RTN (Blue Return)

Pin	Signal Name	Pin	Signal Name
7	Vsync	8	GND
9	Hsync	10	KEY
11	DDC_SDA	12	VIDEO_IN_USE signal
13	DDC_SCL	14	+5V (fused, not populated)

7.3.4 NIC Connectors

The server board provides four RJ-45 connectors on the back edge of the board (JA4A1, JA3A1). The pin-out for NIC connectors are identical and are defined in the following table.

Table 76. RJ-45 10/100/1000 NIC Connector Pin-out (JA4A1, JA3A1)

Pin	Signal Name
1	NIC_0_0_DP
2	NIC_0_0_DN
3	NIC_0_CT1
4	NIC_0_1_DP
5	NIC_0_1_DN
6	NIC_0_CT2
7	NIC_0_2_DP
8	NIC_0_2_DN
9	NIC_0_CT3
10	NIC_0_3_DP
11	NIC_0_3_DN
12	NIC_0_CT4
13	LED_NIC_LINK0_100_N
14	LED_NIC_LINK0_1000_R_N
15	LED_NIC_LINK0_LNKUP_N
16	LED_NIC_LINK0_ACT_R_N

7.3.5 SATA Connectors

The server board provides six SATA port connectors which including two 6Gb/s SATA ports with white connectors (J6E1, J2E2) and four 3Gb/s SATA ports with black connectors (J2E1, J2E3, J1E3, and J2D3).

SATA_0 (J6E1) can support SATA DOM. The SATA_1 (J2E2) cannot support SATA DOM from the mechanical fitting with the board.

The pin configuration for each connector is identical and defined in the following table.

Table 77. SATA Connectors Pin-Out (J6E1, J2E2, J2E1, J2E3, J1E3, and J2D3)

Pin	Signal Name
1	GND
2	SATA_TX_DP
3	SATA_TX_DN
4	GND

Pin	Signal Name
5	SATA_RX_DN
6	SATA_RX_DP
7	GND

7.3.6 Mini SAS Connector

The server board provides one mini SAS port connector (J2D2).

Table 78. Mini SAS Connector Pin-Out (J2D2)

Pin	Signal Name	Pin	Signal Name
A1	GND	B1	GND
A2	RX0_P	B2	TX0_P
A3	RX0_N	B3	TX0_N
A4	GND	B4	GND
A5	RX1_P	B5	TX1_P
A6	RX1_N	B6	TX1_N
A7	GND	B7	GND
A8	BP_TYPE	B8	SGPIO_SAS_CLOCK
A9	GND	B9	SGPIO_SAS_LOAD
A10	SGPIO_SAS_DATAOUT	B10	GND
A11	SGPIO_SAS_DATAIN	B11	CNTRL_TYPE
A12	GND	B12	GND
A13	RX2_P	B13	TX2_P
A14	RX2_N	B14	TX2_N
A15	GND	B15	GND
A16	RX3_P	B16	TX3_P
A17	RX3_N	B17	TX3_N
A18	GND	B18	GND

7.3.7 SATA SGPIO Connector

The server board provides one SATA SGPIO connector (J1E1).

Table 79. SATA SGPIO Connector Pin-Out (J1E1)

Pin	Signal Name
1	SCLOCK
2	SLOAD
3	GND
4	SDOUT0
5	SDOUT1

7.3.8 Hard Drive Activity (Input) LED Header

Table 80. SATA HDD Activity (Input) LED Header (J6F1)

Pin	Description
1	LED_HD_ACTIVE_L
2	NC

7.3.9 Storage Upgrade Key Connector

The server board provides one SATA/SAS storage upgrade key connector (J3E1) on board. The Storage Upgrade Key is a small PCB board that has up to two security EEPROMs that are read by the system ME to enable different versions of LSI* RAID 5 software stack and/or upgrade from SATA to SAS storage functionality.

The pin configuration of connector is identical and defined in the following table.

Table 81. Storage Upgrade Key Connector Pin-Out (J3E1)

Pin	Signal Description
1	GND
2	FM_PBG_DYN_SKU_KEY_R
3	GND
4	FM_SSB_SAS_SATA_RAID_KEY_R

7.3.10 Serial Port Connectors

The server board provides one internal 9-pin serial A header (J5A2). The following tables define the pin-outs.

Table 82. Internal Serial Port Connecter Pin-Out (J5A2)

Pin	Signal Name	Pin	Signal Name
1	SPA_DCD	2	SPA_DSR
3	SPA_SIN_N	4	SPA_RTS
5	SPA_SOUT_N	6	SPA_CTS
7	SPA_DTR	8	SPA_RI
9	GND		

7.3.11 USB Connectors

The server board provides one two external USB headers, two internal USB connectors and one type A USB connector.

The following table defines the pin-out of the external USB port connectors (J1A1, J2A1) found on the back edge of the server board.

Table 83. External USB port Connector Pin-Out (J1A1, J2A1)

Pin	Signal Name
1	P5V_AUX
2	USB2_Px_REAR_DN
3	USB2_Px_REAR_DP

Pin	Signal Name
4	GND

One Type A USB connector on the server board provide an option to support UBS device. The pin-out is detailed in the following table.

Table 84. Type A USB connector Pin-Out (J1D2)

Pin	Signal Name
1	+5V
2	USB_N
3	USB_P
4	GND

Two 2x5 connectors on the server board provide an option to support four additional internal USB ports (J6E2, J2D1). The pin-out is detailed in the following table.

Table 85. Internal USB Connector Pin-Out (J6E2, J2D1)

Pin	Signal Name	Pin	Signal Name
1	+5V	2	+5V
3	USB_N	4	USB_N
5	USB_P	6	USB_P
7	GND	8	GND
9	Key Pin	10	NC

7.3.12 TPM Connector

The server board provides one TPM connector (J6B2) to support the TPM module. The pin-out is defined in the following table.

Table 86. TPM Connector Pin-Out (J6B2)

Pin	Signal Name	Pin	Signal Name
1	Key Pin	2	LPC_LAD<1>
3	LPC_LAD<0>	4	GND
5	IRQ_SERIAL	6	LPC_FRAME_N
7	P3V3	8	GND
9	RST_IBMC_NIC_N	10	CLK_33M_TPM
11	LPC_LAD<3>	12	GND
13	GND	14	LPC_LAD<2>

7.3.13 SSI Front Panel Header

The server board provides one front panel header (J6H1) to support the standard Scythe pin-out is defined in the following table.

Table 87. SSI Front Panel Header Pin-Out (J6H1)

Pin	SSI Signal name	Pin	SSI Signal Name
1	SB3.3V	2	SB3.3V
3	Key	4	SB5V
5	Power LED Cathode	6	System ID LED Cathode
7	3.3V	8	System Fault LED Anode
9	HDD Activity LED Cathode	10	System Fault LED Cathode
11	Power Switch	12	NIC#1 Activity LED
13	GND (Power Switch)	14	NIC#1 Link LED
15	Reset Switch	16	I^2C SDA
17	GND (Reset/ID/NMI Switch)	18	I^2C SCL
19	System ID Switch	20	Chassis Intrusion
21	Pull Down	22	NIC#2 Activity LED
23	NMI to CPU Switch	24	NIC#2 Link LED
1	NIC#3 Activity LED	2	NIC#4 Activity LED
3	NIC#3 Link LED	4	NIC#4 Link LED

7.3.14 SMB PMBus* Connector

The server board provides one SMB PMBus* Connector (J6H2). The pin-out is defined in the following table.

Table 88. PMBus* Connector Pin-Out (J6H2)

Pin	Signal Name
1	SMB_PWR_CLK
2	SMB_PWR_DAT
3	SMB_PWR_ALRT
4	GND
5	3.3V RS

7.3.15 HSBP I²C Connector

The server board provides one HSBP I^2C connector (J1E2). The pin-out is defined in the following table.

Table 89. HSBP I^2C Connector Pin-Out (J1E2)

Pin	Signal Name
1	SMB_HSBP_3V3STBY_DATA
2	GND
3	SMB_HSBP_3V3STBY_CLK

7.4 Fan Headers

The server board provides six 8 pin fan headers (J1K1, J1K2, J3K1, J4K2, J6K2, and J6K3). The following table defined the pin-out.

Table 90. Baseboard Fan Connector Pin-Out (J1K1, J1K2, J3K1, J4K2, J6K2, and J6K3)

Pin	Signal Name
1	GND
2	12V
3	Tachx
4	PWMy
5	GND
6	12V
7	Tachz
8	PWMy

7.5 Chassis Intrusion

The Chassis Intrusion header is connected through a two wire cable to a switch assembly that is mounted just under the chassis cover on systems that support this feature. When the chassis cover is removed, the switch and thus the electrical connection between the pins on this header become open allowing the Emulex* PILOT III BMC's CHASIS_N pin to be pulled LOW. The Emulex* PILOT III BMC's CHASIS_N pin is used by Firmware to note the change in the chassis cover status. Header on baseboard can be unstuffed by default a shorting resistor will be needed to close the circuit.

Table 91. Chassis Intrusion Header (J6A3)

Header state	Description
PINS 1 and 2 CLOSED	BMC CHASIS_N is pulled HIGH. Chassis cover is closed. Default position.
PINS 1 and 2 OPEN	BMC CHASIS_N is pulled LOW. Chassis cover is removed.

8. Intel® Light-Guided Diagnostics

Intel® Server Board S1600JP has several onboard diagnostic LEDs to assist in troubleshooting board-level issues. This section provides a description the location and function of each LED on the server board.

8.1 Front Panel Support

The Intel® Server Board S1600JP supports the front panel control signals are provided through bridge board.

Each Mini-FP provides the following switch and LED features:

- Power switch with integrated power LED (green): Includes clear button lens but painted black with laser etched power icon for light to shine through.
- Chassis ID switch with integrated ID LED (blue) Includes clear button lens but painted black with laser etched ID icon for light to shine through.
- Recessed reset switch with black actuator.
- Bi-color Status/Fault LED (green/amber): Includes a status/fault icon printed on cosmetic front panel label. Icon should be translucent (only shows when LED is on).
- Single network activity/link LED, hardware baseboard ORs Ethernet and Infiniband activity signals together into just one global signal. Includes a network activity/link icon printed on cosmetic front panel label. Icon should be translucent (only shows when LED is on).

8.1.1 System ID LED

The server board supports a blue system ID LED on the front panel, which is used to visually identify a specific server installed among many other similar servers. There are two options available for illuminating the System ID LED:

1. The front panel ID LED Button is pushed, which causes the LED to illuminate to a solid on state until the button is pushed again.
2. An IPMI “Chassis Identify” command is remotely entered, which causes the LED to blink.

The System ID LED on the server board is tied directly to the System ID LED on system front panel if present.

8.1.2 System Status LED

The server board supports status LED on the front panel, which acts as same as the status LED on the server board.

8.1.3 Network Link/Activity LED

The server board provides LED on the front panel for Network Link/Activity. The following table shows the LED details:

Table 92. Network link/activity LED

LED	Color	Condition	What It Means
LAN	Green	On	LAN link/no access
	Green	Blink	LAN access

LED	Color	Condition	What It Means
Link/Activity		Off	Idle

8.2 POST Code Diagnostic LEDs

Eight amber POST code diagnostic LEDs are located on the back-left-edge of the server board in the rear I/O area of the server board by the QSFP connector.

During the system boot process, the BIOS executes a number of platform configuration processes, each of which is assigned a specific hex POST code number. As each configuration routine is started, the BIOS displays the given POST code to the POST code diagnostic LEDs on the back edge of the server board. To assist in troubleshooting a system hang during the POST process, you can use the Diagnostic LEDs to identify the last POST process executed. For a complete description of how these LEDs are read and a list of all supported POST codes, refer to *Appendix A*.

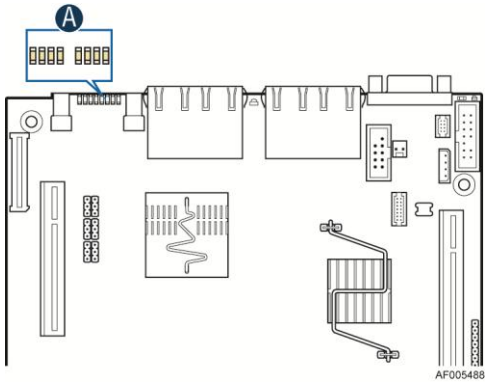


Figure 50. Rear Panel Diagnostic LEDs (Block A)

9. Environmental Limits Specifications

Operation of the server board at conditions beyond those shown in the following table may cause permanent damage to the system. Exposure to absolute maximum rating conditions for extended periods may affect long term system reliability.

Note: The **Energy Star** compliance is at the systems level and not the board level. Use of Intel® boards alone does not guarantee **Energy Star** compliance.

Table 93. Server Board Design Specifications

Operating Temperature	0ºC to 55ºC [1] (32ºF to 131ºF) at product airflow specification
Non-Operating Temperature	-40ºC to 70ºC (-40ºF to 158ºF)
DC Voltage	± 5% of all nominal voltages
Shock (Unpackaged)	Trapezoidal, 50 G, 170 inches/sec
Shock (Packaged)	
<20 pounds	36 inches
>= 20 to <40 pounds	30 inches
>= 40 to <80 pounds	24 inches
>= 80 to <100 pounds	18 inches
>= 100 to <120 pounds	12 inches
>= 120 pounds	9 inches
Vibration (Unpackaged)	5 Hz to 500 Hz 3.13 g RMS random

Note:

Chassis design must provide proper airflow to avoid exceeding the Intel® Xeon® processor maximum case temperature.

9.1 Processor Thermal Design Power (TDP) Support

To allow optimal operation and long-term reliability of Intel® processor-based systems, the processor must remain within the defined minimum and maximum case temperature (T_{CASE}) specifications. Thermal solutions not designed to provide sufficient thermal capability may affect the long-term reliability of the processor and system. The server board is designed to support the Intel® Xeon® Processor E5-2600 product family TDP guidelines up to and including 135W or Intel® Xeon® Processor E5-1600 product family TDP guidelines up to and including 130W.

Disclaimer Note: Intel Corporation server boards contain a number of high-density VLSI and power delivery components that need adequate airflow to cool. Intel® ensures through its own chassis development and testing that when Intel® server building blocks are used together, the fully integrated system will meet the intended thermal requirements of these components. It is the responsibility of the system integrator who chooses not to use Intel® developed server building blocks to consult vendor datasheets and operating parameters to determine the amount of airflow required for their specific application and environmental conditions. Intel Corporation cannot be held responsible, if components fail or the server board does not operate correctly when used outside any of their published operating or non-operating limits.

10. Power Supply Specification Guidelines

This section provides power supply specification guidelines recommended for providing the specified server platform with stable operating power requirements.

Note: The power supply data provided in this section is for reference purposes only. It reflects Intel®'s own AC power out requirements for a 750W power supply as used in an Intel® designed 1U server platform. The intent of this section is to provide customers with a guide to assist in defining and/or selecting a power supply for custom server platform designs that utilize the server boards detailed in this document.

10.1 Power Supply DC Output Connector

To facilitate customers who want to cable to this board from a power supply, the power connectors are implemented through one 10-pin connector and one 8-pin connector.

Table 94. Main Power Supply Connector 10-pin 2x5 Connector Pin-Out

Pin	Signal Name	Pin	Signal Name
1	PSON	6	5VSB
2	GND	7	PWROK
3	GND	8	3.3V
4	GND	9	3.3V
5	5V	10	Reserved

Table 95. Main Power Supply Connector 8-pin 2x4 Connector Pin-Out

Pin	Signal Name	Pin	Signal Name
1	GND	5	+12V
2	GND	6	+12V
3	GND	7	+12V
4	GND	8	+12V

10.2 Power Supply DC Output Specification

10.2.1 Output Power/Currents

The following tables define the minimum power and current ratings. The power supply must meet both static and dynamic voltage regulation requirements for all conditions.

Table 96. 750W Minimum Load Ratings

Parameter	Min	Max.	Peak [1,2]	Unit
12V main	0.0	62.0	70.0	A
12Vstby	0.0	2.1	2.4	A

Notes:

1) 12Vstby must provide 4.0A with two power supplies in parallel. The Fan may work when stby current >1.5A.
2) Length of time peak power can be supported is based on thermal sensor and assertion of the SMBAlert# signal. Minimum peak power duration shall be 20 seconds without asserting the SMBAlert# signal at maximum operating temperature.

10.2.2 Standby Output

The standby output shall be present when an AC input greater than the power supply turn on voltage is applied. There should be load sharing in the standby rail.

10.2.3 Voltage Regulation

The power supply output voltages must stay within the following voltage limits when operating at steady state and dynamic loading conditions. These limits include the peak-peak ripple/noise. These shall be measured at the output connectors.

Table 97. 750W Voltage Regulation Limits

Parameter	Tolerance	Min	Nom	Max	Units
+12V	- 5%/+5%	+11.40	+12.00	+12.60	V_{rms}
+12V stby	- 5%/+5%	+11.40	+12.00	+12.60	V_{rms}

10.2.4 Dynamic Loading

The output voltages shall remain within limits specified for the step loading and capacitive loading specified in the following table. The load transient repetition rate shall be tested between 50Hz and 5kHz at duty cycles ranging from 10%-90%. The load transient repetition rate is only a test specification. The step load may occur anywhere within the MIN load to the MAX load conditions.

Table 98. 750W Transient Load Requirements

Output	Step Load Size	Load Slew Rate	Test capacitive Load
+12VSB	1.0A	0.25 A/sec	20 F
+12V	60% of max load	0.25 A/sec	2000 F

Note: For dynamic condition +12V min loading is 1A.

10.2.5 Capacitive Loading

The power supply shall be stable and meet all requirements with the following capacitive loading ranges.

Table 99. 750W Capacitive Loading Conditions

Output	MIN	MAX	Units
+12VSB	20	3100	F
+12V	500	25000	F

10.2.6 Grounding

The output ground of the pins of the power supply provides the output power return path. The output connector ground pins shall be connected to the safety ground (power supply enclosure). This grounding should be well designed to ensure passing the max allowed Common Mode Noise levels.

The power supply shall be provided with a reliable protective earth ground. All secondary circuits shall be connected to protective earth ground. Resistance of the ground returns to chassis shall not exceed 1.0 m□. This path may be used to carry DC current.

10.2.7 Closed loop stability

The power supply shall be unconditionally stable under all line/load/transient load conditions including specified capacitive load ranges. A minimum of **45 degrees phase margin** and **10dB-gain margin** is required. Closed-loop stability must be ensured at the maximum and minimum loads as applicable.

10.2.8 Residual Voltage Immunity in Standby mode

The power supply should be immune to any residual voltage placed on its outputs (typically a leakage voltage through the system from standby output) up to **500mV**. There shall be no additional heat generated, nor stressing of any internal components with this voltage applied to any individual or all outputs simultaneously. It also should not trip the protection circuits during turn on.

The residual voltage at the power supply outputs for no load condition shall not exceed **100mV** when AC voltage is applied and the PSON# signal is de-asserted.

10.2.9 Common Mode Noise

The Common Mode noise on any output shall not exceed **350mV pk-pk** over the frequency band of 10Hz to 20MHz.

10.2.10 Soft Starting

The Power Supply shall contain control circuit which provides monotonic soft start for its outputs without overstress of the AC line or any power supply components at any specified AC line or load conditions.

10.2.11 Zero Load Stability Requirements

When the power subsystem operates in a no load condition, it does not need to meet the output regulation specification, but it must operate without any tripping of over-voltage or other fault circuitry. When the power subsystem is subsequently loaded, it must begin to regulate and source current without fault.

10.2.12 Hot Swap Requirements

Hot swapping a power supply is the process of inserting and extracting a power supply from an operating power system. During this process the output voltages shall remain within the limits with the capacitive load specified. The hot swap test must be conducted when the system is operating under static, dynamic, and zero loading conditions. The power supply shall use a

latching mechanism to prevent insertion and extraction of the power supply when the AC power cord is inserted into the power supply.

10.2.13 Forced Load Sharing

The +12V output will have active load sharing. The output will share within 10% at full load. The failure of a power supply should not affect the load sharing or output voltages of the other supplies still operating. The supplies must be able to load share in parallel and operate in a hot-swap/redundant **1+1** configurations. The 12VSB output is not required to actively share current between power supplies (passive sharing). The 12VSB output of the power supplies are connected together in the system so that a failure or hot swap of a redundant power supply does not cause these outputs to go out of regulation in the system.

10.2.14 Ripple/Noise

The maximum allowed ripple/noise output of the power supply is defined in the following table. This is measured over a bandwidth of 10Hz to 20MHz at the power supply output connectors. A 10□F tantalum capacitor in parallel with a 0.1□F ceramic capacitor is placed at the point of measurement.

Table 100. 750W Ripples and Noise

+12V main	+12VSB
120mVp-p	120mVp-p

10.2.15 Timing Requirement

These are the timing requirements for the power supply operation. The output voltages must rise from 10% to within regulation limits (T_{vout_rise}) within 5ms to 70ms. For 12VSB, it is allowed to rise from 1.0ms to 25ms. **All outputs must rise monotonically**. The following table shows the timing requirements for the power supply being turned on and off through the AC input, with PSON held low and the PSON signal, with the AC input applied.

Table 101. 750W Timing Requirements

Item	Description	Min	Max	Units
T_{vout_rise}	Output voltage rise time.	5.0 *	70 *	ms
$T_{sb\_on\_delay}$	Delay from AC being applied to 12VSB being within regulation.		1500	ms
$T_{ac\_on\_delay}$	Delay from AC being applied to all output voltages being within regulation.		3000	ms
T_{vout_holdup}	Time 12Vl output voltage stay within regulation after loss of AC.	13		ms
T_{pwok_holdup}	Delay from loss of AC to de-assertion of PWOK.	12		ms
$T_{pson\_on\_delay}$	Delay from PSON# active to output voltages within regulation limits.	5	400	ms
T_{pson_pwok}	Delay from PSON# deactivate to PWOK being de-asserted.		5	ms
T_{pwok_on}	Delay from output voltages within regulation limits to PWOK asserted at turn on.	100	500	ms
T_{pwok_off}	Delay from PWOK de-asserted to output voltages dropping out of regulation limits.	1		ms
T_{pwok_low}	Duration of PWOK being in the de-asserted state during an off/on cycle using AC or the PSON signal.	100		ms

T_{sb_vout}	Delay from 12VSB being in regulation to O/Ps being in regulation at AC turn on.	50	1000	ms
T_{12VSB_holdup}	Time the 12VSB output voltage stays within regulation after loss of AC.	70		ms

Note:

* The 12VSB output voltage rise time shall be from 1.0ms to 25ms.

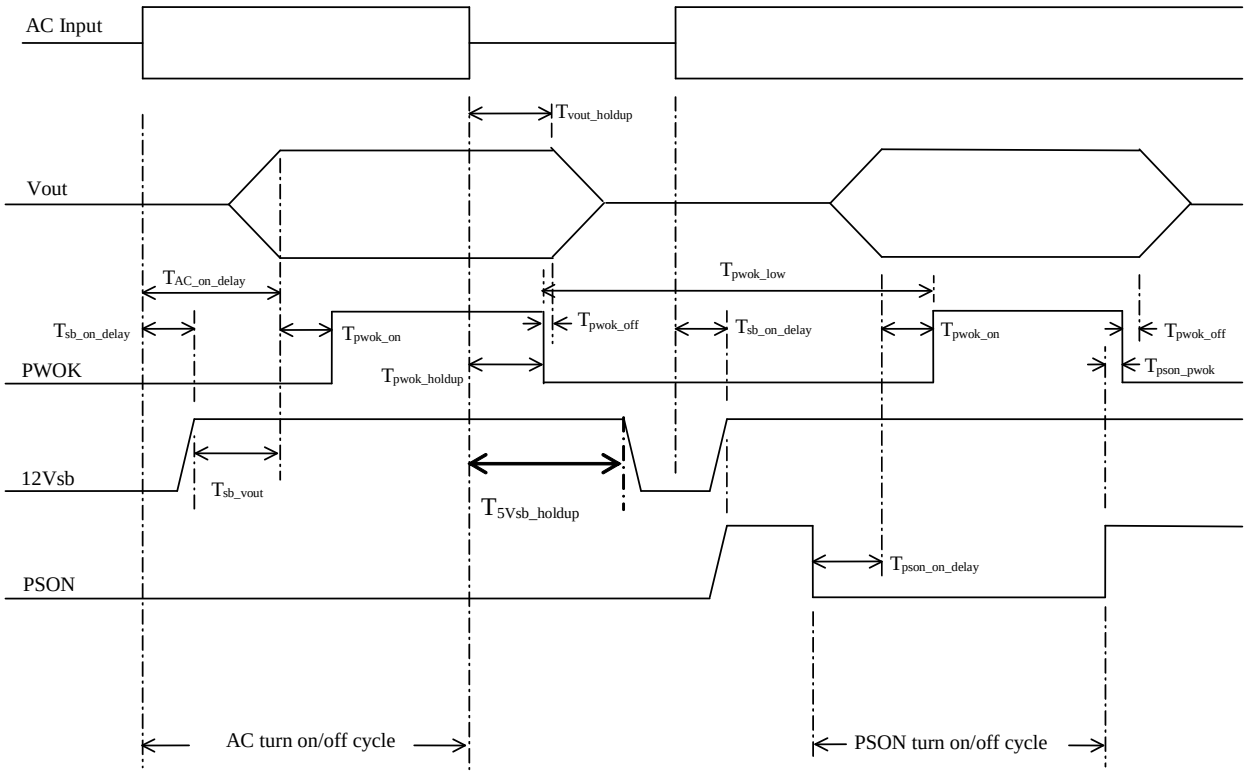


Figure 51. 750W Turn On/Off Timing (Power Supply Signals)

Appendix A: Integration and Usage Tips

- When adding or removing components or peripherals from the server board, AC power must be removed. With AC power plugged into the server board, 5-V standby is still present even though the server board is powered off.
- This server board supports the Intel® Xeon® Processor E5-2600 product family with a Thermal Design Power (TDP) of up to and including 135 Watts or Intel® Xeon® Processor E5-1600 product family with a Thermal Design Power (TDP) of up to and including 130 Watts. Previous generations of the Intel® Xeon® processors are not supported.
- The server board includes a pre-installed CPU power cable harness. The cable harness must be installed and fully seated in each connector for the server board to operate.
- On the back edge of the server board are eight diagnostic LEDs that display a sequence of amber POST codes during the boot process. If the server board hangs during POST, the LEDs display the last POST event run before the hang.
- This server board only supports registered DDRIII DIMMs (RDIMMs) and unbuffered DDRIII DIMMs (UDIMMs). Mixing of RDIMMs and UDIMMs is not supported.
- The Intel® Remote Management Module 4 (Intel® RMM4) connector is not compatible with any previous versions of the Intel® Remote Management Module (Product Order Code – AXXRMM, AXXRMM2, AXXRMM3).
- Clear the CMOS with AC power cord plugged. Removing the AC power before performing the CMOS clear operation causes the system to automatically power up and immediately power down after the CMOS clear procedure is followed and AC power is re-applied. If this happens, remove the AC power cord, wait 30 seconds, and then re-connect the AC power cord. Power up the system and proceed to the <F2> BIOS Setup utility to reset the desired settings.
- Normal Integrated BMC functionality is disabled with the BMC Force Update jumper set to the “enabled” position (pins 2-3). The server should never be run with the BMC Force Update jumper set in this position and should only be used when the standard firmware update process fails. This jumper should remain in the default (disabled) position (pins 1-2) when the server is running normally.
- When performing a normal BIOS update procedure, the BIOS recovery jumper must be set to its default position (pins 1-2).

Appendix B: Integrated BMC Sensor Tables

This appendix lists the sensor identification numbers and information about the sensor type, name, supported thresholds, assertion and de-assertion information, and a brief description of the sensor purpose. See the *Intelligent Platform Management Interface Specification, Version 2.0*, for sensor and event/reading-type table information.

- **Sensor Type**

  The Sensor Type values are the values enumerated in the *Sensor Type Codes* table in the *IPMI specification*. The Sensor Type provides the context in which to interpret the sensor, such as the physical entity or characteristic that is represented by this sensor.

- **Event/Reading Type**

  The Event/Reading Type values are from the *Event/Reading Type Code Ranges* and *Generic Event/Reading Type Codes* tables in the IPMI specification. Digital sensors are a specific type of discrete sensor, which have only two states.

- **Event Offset/Triggers**

  Event Thresholds are event-generating thresholds for threshold types of sensors.

  - [u,l][nr,c,nc]: upper non-recoverable, upper critical, upper non-critical, lower non-recoverable, lower critical, lower non-critical
  - uc, lc: upper critical, lower critical

  Event Triggers are supported event-generating offsets for discrete type sensors. The offsets can be found in the *Generic Event/Reading Type Codes* or *Sensor Type Codes* tables in the *IPMI specification*, depending on whether the sensor event/reading type is generic or a sensor-specific response.

- **Assertion/De-assertion Enables**

  Assertion and de-assertion indicators reveal the type of events the sensor generates:

  - As: Assertions
  - De: De-assertion

- **Readable Value/Offsets**

  - Readable Value indicates the type of value returned for threshold and other non-discrete type sensors.
  - Readable Offsets indicate the offsets for discrete sensors that are readable with the *Get Sensor Reading* command. Unless otherwise indicated, all event triggers are readable; Readable Offsets consist of the reading type offsets that do not generate events.

- **Event Data**

  Event data is the data that is included in an event message generated by the sensor. For threshold-based sensors, the following abbreviations are used:

  - R: Reading value
  - T: Threshold value

- **Rearm Sensors**

  The rearm is a request for the event status for a sensor to be rechecked and updated upon a transition between good and bad states. Rearming the sensors can be done manually or automatically. This column indicates the type supported by the sensor. The following abbreviations are used to describe a sensor:

  - A: Auto-rearm
  - M: Manual rearm

- **Default Hysteresis**

  The hysteresis setting applies to all thresholds of the sensor. This column provides the count of hysteresis for the sensor, which can be 1 or 2 (positive or negative hysteresis).

- **Criticality**

  Criticality is a classification of the severity and nature of the condition. It also controls the behavior of the Control Panel Status LED.

- **Standby**

  Some sensors operate on standby power. These sensors may be accessed and/or generate events when the main (system) power is off, but AC power is present.

Note: All sensors listed as follows may not be present on all platforms. Please check platform EPS section for platform applicability and platform chassis section for chassis specific sensors. Redundancy sensors will be only present on systems with appropriate hardware to support redundancy (for instance, fan or power supply).

Table 102. BMC Core Sensors

Full Sensor Name (Sensor name in SDR)	Sensor #	Platform Applicability	Sensor Type	Event/Reading Type	Event Offset Triggers	Contrib. To System Status	Assert/De-assert	Readable Value/ Offsets	Event Data	Rearm	Stand-by
Power Unit Status *(Pwr Unit Status)*	01h	All	Power Unit 09h	Sensor Specific 6Fh	00 - Power down	OK	As and De	–	Trig Offset	A	X
					02 - 240 VA power down	Fatal					
					04 - A/C lost	OK					
					05 - Soft power control failure	Fatal					
					06 - Power unit failure						
Power Unit Redundancy[Note1] *(Pwr Unit Redund)*	02h	Chassis-specific	Power Unit 09h	Generic 0Bh	00 - Fully Redundant	OK	As	–	Trig Offset	M	X
					01 - Redundancy lost	Degraded					
					02 - Redundancy degraded	Degraded					
					03 - Non-redundant: sufficient resources. Transition from full redundant state.	Degraded					

Full Sensor Name (Sensor name in SDR)	Sensor #	Platform Applicability	Sensor Type	Event/Reading Type	Event Offset Triggers	Contrib. To System Status	Assert/De-assert	Readable Value/ Offsets	Event Data	Rearm	Stand-by
					04 – Non-redundant: sufficient resources. Transition from insufficient state.	Degraded					
					05 - Non-redundant: insufficient resources	Fatal					
					06 – Redundant: degraded from fully redundant state.	Degraded					
					07 – Redundant: Transition from non-redundant state.	Degraded					
IPMI Watchdog *(IPMI Watchdog)*	03h	All	Watchdog 2 23h	Sensor Specific 6Fh	00 - Timer expired, status only	OK	As	–	Trig Offset	A	X
					01 - Hard reset						
					02 - Power down						
					03 - Power cycle						
					08 - Timer interrupt						

Full Sensor Name (Sensor name in SDR)	Sensor #	Platform Applicability	Sensor Type	Event/Reading Type	Event Offset Triggers	Contrib. To System Status	Assert/De-assert	Readable Value/ Offsets	Event Data	Rearm	Stand-by
Physical Security *(Physical Scrty)*	04h	Chassis Intrusion is chassis-specific	Physical Security 05h	Sensor Specific 6Fh	00 - Chassis intrusion 04 - LAN leash lost	Degraded OK	As and De	–	Trig Offset	A	X
FP Interrupt *(FP NMI Diag Int)*	05h	Chassis-specific	Critical Interrupt 13h	Sensor Specific 6Fh	00 - Front panel NMI/diagnostic interrupt	OK	As	–	Trig Offset	A	–
SMI Timeout *(SMI Timeout)*	06h	All	SMI Timeout F3h	Digital Discrete 03h	01 – State asserted	Fatal	As and De	–	Trig Offset	A	–
System Event Log *(System Event Log)*	07h	All	Event Logging Disabled 10h	Sensor Specific 6Fh	02 - Log area reset/cleared	OK	As	–	Trig Offset	A	X
System Event *(System Event)*	08h	All	System Event 12h	Sensor Specific 6Fh	– PEF action	OK	As	-	Trig Offset	A	X
Button Sensor *(Button)*	09h	All	Button/Switch 14h	Sensor Specific 6Fh	– Power Button 02 – Reset Button	OK	AS	–	Trig Offset	A	X
BMC Watchdog	0Ah	All	Mgmt System Health 28h	Digital Discrete 03h	01 – State Asserted	Degraded	As	–	Trig Offset	A	-

Full Sensor Name (Sensor name in SDR)	Sensor #	Platform Applicability	Sensor Type	Event/Reading Type	Event Offset Triggers	Contrib. To System Status	Assert/De-assert	Readable Value/ Offsets	Event Data	Rearm	Stand-by
Voltage Regulator Watchdog *(VR Watchdog)*	0Bh	All	Voltage 02h	Digital Discrete 03h	01 – State Asserted	Fatal	As and De	–	Trig Offset	M	X
Fan Redundancy[1] *(Fan Redundancy)*	0Ch	Chassis-specific	Fan 04h	Generic 0Bh	00 - Fully redundant	OK	As and De	–	Trig Offset	A	–
					01 - Redundancy lost	Degraded					
					02 - Redundancy degraded	Degraded					
					03 - Non-redundant: Sufficient resources. Transition from redundant	Degraded					
					04 - Non-redundant: Sufficient resources. Transition from insufficient.	Degraded					
					05 - Non-redundant: insufficient resources.	Non-Fatal					
					06 – Non-Redundant: degraded from fully redundant.	Degraded					

Full Sensor Name (Sensor name in SDR)	Sensor #	Platform Applicability	Sensor Type	Event/Reading Type	Event Offset Triggers	Contrib. To System Status	Assert/De-assert	Readable Value/ Offsets	Event Data	Rearm	Stand-by
					07 - Redundant degraded from non-redundant	Degraded					
SSB Thermal Trip *(SSB Therm Trip)*	0Dh	All	Temperature 01h	Digital Discrete 03h	01 – State Asserted	Fatal	As and De	–	Trig Offset	M	X
IO Module Presence *(IO Mod Presence)*	0Eh	Platform-specific	Module/Board 15h	Digital Discrete 08h	01 – Inserted/Present	OK	As and De	–	Trig Offset	M	-
SAS Module Presence (*SAS Mod Presence)*	0Fh	Platform-specific	Module/Board 15h	Digital Discrete 08h	01 – Inserted/Present	OK	As and De	–	Trig Offset	M	X
BMC Firmware Health (*BMC FW Health)*	10h	All	Mgmt Health 28h	Sensor Specific 6Fh	04 – Sensor Failure	Degraded	As	-	Trig Offset	A	X
System Airflow *(System Airflow)*	11h	All	Other Units 0Bh	Threshold 01h	–	–	–	Analog	–	–	–
FW Update Status	12h	All	Version Change 2Bh	OEM defined x70h	00h→Update started 01h→Update completed successfully. 02h→Update failure	OK	As	–	Trig Offset	A	–
IO Module2 Presence *(IO Mod2 Presence)*	13h	Platform-specific	Module/Board 15h	Digital Discrete 08h	01 – Inserted/Present	OK	As and De	–	Trig Offset	M	-

Full Sensor Name (Sensor name in SDR)	Sensor #	Platform Applicability	Sensor Type	Event/Reading Type	Event Offset Triggers	Contrib. To System Status	Assert/De-assert	Readable Value/ Offsets	Event Data	Rearm	Stand-by
Baseboard Temperature 5 *(Platform Specific)*	14h	Platform-specific	Temperature 01h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	X
Baseboard Temperature 6 *(Platform Specific)*	15h	Platform-specific	Temperature 01h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	X
IO Module2 Temperature *(I/O Mod2 Temp)*	16h	Platform-specific	Temperature 01h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	X
PCI Riser 3 Temperature *(PCI Riser 5 Temp)*	17h	Platform-specific	Temperature 01h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	X
PCI Riser 4 Temperature *(PCI Riser 4 Temp)*	18h	Platform-specific	Temperature 01h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	X
Baseboard +1.05V Processor3 Vccp *(BB +1.05Vccp P3)*	19h	Platform-specific	Voltage 02h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	–

Full Sensor Name (Sensor name in SDR)	Sensor #	Platform Applicability	Sensor Type	Event/Reading Type	Event Offset Triggers	Contrib. To System Status	Assert/De-assert	Readable Value/ Offsets	Event Data	Rearm	Stand-by
Baseboard +1.05V Processor4 Vccp *(BB +1.05Vccp P4)*	1Ah	Platform-specific	Voltage 02h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	–
Baseboard Temperature 1 *(Platform Specific)*	20h	Platform-specific	Temperature 01h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	X
Front Panel Temperature *(Front Panel Temp)*	21h	All	Temperature 01h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	X
SSB Temperature *(SSB Temp)*	22h	All	Temperature 01h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	X
Baseboard Temperature 2 *(Platform Specific)*	23h	Platform-specific	Temperature 01h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	X
Baseboard Temperature 3 *(Platform Specific)*	24h	Platform-specific	Temperature 01h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	X

Full Sensor Name (Sensor name in SDR)	Sensor #	Platform Applicability	Sensor Type	Event/Reading Type	Event Offset Triggers	Contrib. To System Status	Assert/De-assert	Readable Value/ Offsets	Event Data	Rearm	Stand-by
Baseboard Temperature 4 *(Platform Specific)*	25h	Platform-specific	Temperature 01h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	X
IO Module Temperature *(I/O Mod Temp)*	26h	Platform-specific	Temperature 01h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	X
PCI Riser 1 Temperature *(PCI Riser 1 Temp)*	27h	Platform-specific	Temperature 01h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	X
IO Riser Temperature *(IO Riser Temp)*	28h	Platform-specific	Temperature 01h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	X
Hot-swap Backplane 1 Temperature *(HSBP 1 Temp)*	29h	Chassis-specific	Temperature 01h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	X
Hot-swap Backplane 2 Temperature *(HSBP 2 Temp)*	2Ah	Chassis-specific	Temperature 01h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	X

Full Sensor Name (Sensor name in SDR)	Sensor #	Platform Applicability	Sensor Type	Event/Reading Type	Event Offset Triggers	Contrib. To System Status	Assert/De-assert	Readable Value/ Offsets	Event Data	Rearm	Stand-by
Hot-swap Backplane 3 Temperature *(HSBP 3 Temp)*	2Bh	Chassis-specific	Temperature 01h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	X
PCI Riser 2 Temperature *(PCI Riser 2 Temp)*	2Ch	Platform-specific	Temperature 01h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	X
SAS Module Temperature *(SAS Mod Temp)*	2Dh	Platform-specific	Temperature 01h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	X
Exit Air Temperature *(Exit Air Temp)*	2Eh	Chassis and Platform Specific	Temperature 01h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	X
Network Interface Controller Temperature *(LAN NIC Temp)*	2Fh	All	Temperature 01h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	X

Full Sensor Name (Sensor name in SDR)	Sensor #	Platform Applicability	Sensor Type	Event/Reading Type	Event Offset Triggers	Contrib. To System Status	Assert/De-assert	Readable Value/ Offsets	Event Data	Rearm	Stand-by
Fan Tachometer Sensors *(Chassis specific sensor names)*	30h–3Fh	Chassis and Platform Specific	Fan 04h	Threshold 01h	[l] [c,nc]	nc = Degraded c = Non-fatal[Note3]	As and De	Analog	R, T	M	-
Fan Present Sensors *(Fan x Present)*	40h–4Fh	Chassis and Platform Specific	Fan 04h	Generic 08h	01 - Device inserted	OK	As and De	-	Triggered Offset	Auto	-
Power Supply 1 Status[Note2] *(PS1 Status)*	50h	Chassis-specific	Power Supply 08h	Sensor Specific 6Fh	00 - Presence	OK	As and De	–	Trig Offset	A	X
					01 - Failure	Degraded					
					02 – Predictive Failure	Degraded					
					03 - A/C lost	Degraded					
					06 – Configuration error	OK					
Power Supply 2 Status[Note2] *(PS2 Status)*	51h	Chassis-specific	Power Supply 08h	Sensor Specific 6Fh	00 - Presence	OK	As and De	–	Trig Offset	A	X
					01 - Failure	Degraded					
					02 – Predictive Failure	Degraded					
					03 - A/C lost	Degraded					
					06 – Configuration error	OK					

Full Sensor Name (Sensor name in SDR)	Sensor #	Platform Applicability	Sensor Type	Event/Reading Type	Event Offset Triggers	Contrib. To System Status	Assert/De-assert	Readable Value/ Offsets	Event Data	Rearm	Stand-by
Power Supply 1 AC Power Input *(PS1 Power In)*	54h	Chassis-specific	Other Units 0Bh	Threshold 01h	[u] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	X
Power Supply 2 AC Power Input *(PS2 Power In)*	55h	Chassis-specific	Other Units 0Bh	Threshold 01h	[u] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	X
Power Supply 1 +12V % of Maximum Current Output (*PS1 Curr Out %*)	58h	Chassis-specific	Current 03h	Threshold 01h	[u] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	X
Power Supply 2 +12V % of Maximum Current Output (*PS2 Curr Out %*)	59h	Chassis-specific	Current 03h	Threshold 01h	[u] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	X
Power Supply 1 Temperature (*PS1 Temperature*)	5Ch	Chassis-specific	Temperature 01h	Threshold 01h	[u] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	X

Full Sensor Name (Sensor name in SDR)	Sensor #	Platform Applicability	Sensor Type	Event/Reading Type	Event Offset Triggers	Contrib. To System Status	Assert/De-assert	Readable Value/ Offsets	Event Data	Rearm	Stand-by
Power Supply 2 Temperature (*PS2 Temperature*)	5Dh	Chassis-specific	Temperature	Threshold 01h	[u] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	X
Hard Disk Drive 17 - 23 Status *(HDD 17 - 23 Status)*	60h – 68h	Chassis-specific	Drive Slot 0Dh	Sensor Specific 6Fh	00 - Drive Presence	OK	As and De	–	Trig Offset	A	X
					01- Drive Fault	Degraded					X
					07 - Rebuild/Remap in progress	Degraded					
Hot Swap Controller 1 - 3 Status *(HSC 1 - 3 Status)*	69h - 6Bh	Chassis-specific	Microcontroller 16h	Discrete 0Ah	04- transition to Off Line	Degraded	As and De	–	Trig Offset	A	X
Processor 1 Status *(P1 Status)*	70h	All	Processor 07h	Sensor Specific 6Fh	01 - Thermal trip	Fatal	As and De	–	Trig Offset	M	X
					07 - Presence	OK					
Processor 2 Status *(P2 Status)*	71h	All	Processor 07h	Sensor Specific 6Fh	01 - Thermal trip	Fatal	As and De	–	Trig Offset	M	X
					07 - Presence	OK					
Processor 3 Status *(P3 Status)*	72h	Platform-specific	Processor 07h	Sensor Specific 6Fh	01 - Thermal trip	Fatal	As and De	–	Trig Offset	M	X
					07 - Presence	OK					
Processor 4 Status *(P4 Status)*	73h	Platform-specific	Processor 07h	Sensor Specific 6Fh	01 - Thermal trip	Fatal	As and De	–	Trig Offset	M	X
					07 - Presence	OK					

Full Sensor Name (Sensor name in SDR)	Sensor #	Platform Applicability	Sensor Type	Event/Reading Type	Event Offset Triggers	Contrib. To System Status	Assert/De-assert	Readable Value/ Offsets	Event Data	Rearm	Stand-by
Processor 1 Thermal Margin *(P1 Therm Margin)*	74h	All	Temperature 01h	Threshold 01h	-	-	-	Analog	R, T	A	–
Processor 2 Thermal Margin *(P2 Therm Margin)*	75h	All	Temperature 01h	Threshold 01h	-	-	-	Analog	R, T	A	–
Processor 3 Thermal Margin *(P3 Therm Margin)*	76h	Platform-specific	Temperature 01h	Threshold 01h	-	-	-	Analog	R, T	A	–
Processor 4 Thermal Margin *(P4 Therm Margin)*	77h	Platform-specific	Temperature 01h	Threshold 01h	-	-	-	Analog	R, T	A	–
Processor 1 Thermal Control % (*P1 Therm Ctrl %*)	78h	All	Temperature 01h	Threshold 01h	[u] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	Trig Offset	A	–
Processor 2 Thermal Control % (*P2 Therm Ctrl %*)	79h	All	Temperature 01h	Threshold 01h	[u] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	Trig Offset	A	–

Full Sensor Name (Sensor name in SDR)	Sensor #	Platform Applicability	Sensor Type	Event/Reading Type	Event Offset Triggers	Contrib. To System Status	Assert/De-assert	Readable Value/ Offsets	Event Data	Rearm	Stand-by
Processor 3 Thermal Control % (*P3 Therm Ctrl %*)	7Ah	Platform-specific	Temperature 01h	Threshold 01h	[u] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	Trig Offset	A	–
Processor 4 Thermal Control % (*P4 Therm Ctrl %*)	7Bh	Platform-specific	Temperature 01h	Threshold 01h	[u] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	Trig Offset	A	–
Processor 1 ERR2 Timeout *(P1 ERR2)*	7Ch	All	Processor 07h	Digital Discrete 03h	01 – State Asserted	Fatal	As and De	–	Trig Offset	A	–
Processor 2 ERR2 Timeout *(P2 ERR2)*	7Dh	All	Processor 07h	Digital Discrete 03h	01 – State Asserted	Fatal	As and De	–	Trig Offset	A	–
Processor 3 ERR2 Timeout *(P3 ERR2)*	7Eh	Platform-specific	Processor 07h	Digital Discrete 03h	01 – State Asserted	Fatal	As and De	–	Trig Offset	A	–
Processor 4 ERR2 Timeout *(P4 ERR2)*	7Fh	Platform-specific	Processor 07h	Digital Discrete 03h	01 – State Asserted	Fatal	As and De	–	Trig Offset	A	–
Catastrophic Error *(CATERR)*	80h	All	Processor 07h	Digital Discrete 03h	01 – State Asserted	Fatal	As and De	–	Trig Offset	M	–

Full Sensor Name (Sensor name in SDR)	Sensor #	Platform Applicability	Sensor Type	Event/Reading Type	Event Offset Triggers	Contrib. To System Status	Assert/De-assert	Readable Value/ Offsets	Event Data	Rearm	Stand-by
Processor1 MSID Mismatch *(P1 MSID Mismatch)*	81h	All	Processor 07h	Digital Discrete 03h	01 – State Asserted	Fatal	As and De	–	Trig Offset	M	–
Processor Population Fault *(CPU Missing)*	82h	All	Processor 07h	Digital Discrete 03h	01 – State Asserted	Fatal	As and De	–	Trig Offset	M	–
Processor 1 DTS Thermal Margin *(P1 DTS Therm Mgn)*	83h	All	Temperature 01h	Threshold 01h	-	-	-	Analog	R, T	A	–
Processor 2 DTS Thermal Margin *(P2 DTS Therm Mgn)*	84h	All	Temperature 01h	Threshold 01h	-	-	-	Analog	R, T	A	–
Processor 3 DTS Thermal Margin *(P3 DTS Therm Mgn)*	85h	All	Temperature 01h	Threshold 01h	-	-	-	Analog	R, T	A	–
Processor 4 DTS Thermal Margin *(P4 DTS Therm Mgn)*	86h	All	Temperature 01h	Threshold 01h	-	-	-	Analog	R, T	A	–

Full Sensor Name (Sensor name in SDR)	Sensor #	Platform Applicability	Sensor Type	Event/Reading Type	Event Offset Triggers	Contrib. To System Status	Assert/De-assert	Readable Value/ Offsets	Event Data	Rearm	Stand-by
Processor2 MSID Mismatch *(P2 MSID Mismatch)*	87h	All	Processor 07h	Digital Discrete 03h	01 – State Asserted	Fatal	As and De	–	Trig Offset	M	–
Processor 1 VRD Temperature (*P1 VRD Hot*)	90h	All	Temperature 01h	Digital Discrete 05h	01 - Limit exceeded	Non-fatal	As and De	–	Trig Offset	A	–
Processor 2 VRD Temperature (*P2 VRD Hot*)	91h	All	Temperature 01h	Digital Discrete 05h	01 - Limit exceeded	Non-fatal	As and De	–	Trig Offset	A	–
Processor 3 VRD Temperature *(P3 VRD Hot)*	92h	All	Temperature 01h	Digital Discrete 05h	01 - Limit exceeded	Non-fatal	As and De	–	Trig Offset	A	–
Processor 4 VRD Temperature *(P4 VRD Hot)*	93h	All	Temperature 01h	Digital Discrete 05h	01 - Limit exceeded	Non-fatal	As and De	–	Trig Offset	A	–
Processor 1 Memory VRD Hot 0-1 *(P1 Mem01 VRD Hot)*	94h	All	Temperature 01h	Digital Discrete 05h	01 - Limit exceeded	Non-fatal	As and De	–	Trig Offset	A	–

Full Sensor Name (Sensor name in SDR)	Sensor #	Platform Applicability	Sensor Type	Event/Reading Type	Event Offset Triggers	Contrib. To System Status	Assert/De-assert	Readable Value/ Offsets	Event Data	Rearm	Stand-by
Processor 1 Memory VRD Hot 2-3 *(P1 Mem23 VRD Hot)*	95h	All	Temperature 01h	Digital Discrete 05h	01 - Limit exceeded	Non-fatal	As and De	–	Trig Offset	A	–
Processor 2 Memory VRD Hot 0-1 *(P2 Mem01 VRD Hot)*	96h	All	Temperature 01h	Digital Discrete 05h	01 - Limit exceeded	Non-fatal	As and De	–	Trig Offset	A	–
Processor 2 Memory VRD Hot 2-3 *(P2 Mem23 VRD Hot)*	97h	All	Temperature 01h	Digital Discrete 05h	01 - Limit exceeded	Non-fatal	As and De	–	Trig Offset	A	–
Processor 3 Memory VRD Hot 0-1 *(P3 Mem01 VRD Hot)*	98h	All	Temperature 01h	Digital Discrete 05h	01 - Limit exceeded	Non-fatal	As and De	–	Trig Offset	A	–
Processor 3 Memory VRD Hot 2-3 *(P4 Mem23 VRD Hot)*	99h	All	Temperature 01h	Digital Discrete 05h	01 - Limit exceeded	Non-fatal	As and De	–	Trig Offset	A	–

Full Sensor Name (Sensor name in SDR)	Sensor #	Platform Applicability	Sensor Type	Event/Reading Type	Event Offset Triggers	Contrib. To System Status	Assert/De-assert	Readable Value/ Offsets	Event Data	Rearm	Stand-by
Processor 4 Memory VRD Hot 0-1 *(P4 Mem01 VRD Hot)*	9Ah	All	Temperature 01h	Digital Discrete 05h	01 - Limit exceeded	Non-fatal	As and De	–	Trig Offset	A	–
Processor 4 Memory VRD Hot 2-3 *(P4 Mem23 VRD Hot)*	9Bh	All	Temperature 01h	Digital Discrete 05h	01 - Limit exceeded	Non-fatal	As and De	–	Trig Offset	A	–
Power Supply 1 Fan Tachometer 1 *(PS1 Fan Tach 1)*	A0h	Chassis-specific	Fan 04h	Generic – digital discrete	01 – State Asserted	Non-fatal	As and De	-	Trig Offset	M	-
Power Supply 1 Fan Tachometer 2 *(PS1 Fan Tach 2)*	A1h	Chassis-specific	Fan 04h	Generic – digital discrete	01 – State Asserted	Non-fatal	As and De	-	Trig Offset	M	-
Power Supply 2 Fan Tachometer 1 *(PS2 Fan Tach 1)*	A4h	Chassis-specific	Fan 04h	Generic – digital discrete	01 – State Asserted	Non-fatal	As and De	-	Trig Offset	M	-
Power Supply 2 Fan Tachometer 2 *(PS2 Fan Tach 2)*	A5h	Chassis-specific	Fan 04h	Generic – digital discrete	01 – State Asserted	Non-fatal	As and De	-	Trig Offset	M	-

Full Sensor Name (Sensor name in SDR)	Sensor #	Platform Applicability	Sensor Type	Event/Reading Type	Event Offset Triggers	Contrib. To System Status	Assert/De-assert	Readable Value/ Offsets	Event Data	Rearm	Stand-by
Processor 1 DIMM Aggregate Thermal Margin 1 *(P1 DIMM Thrm Mrgn1)*	B0h	All	Temperature 01h	Threshold 01h	[u] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	–
Processor 1 DIMM Aggregate Thermal Margin 2 *(P1 DIMM Thrm Mrgn2)*	B1h	All	Temperature 01h	Threshold 01h	[u] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	–
Processor 2 DIMM Aggregate Thermal Margin 1 *(P2 DIMM Thrm Mrgn1)*	B2h	All	Temperature 01h	Threshold 01h	[u] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	–
Processor 2 DIMM Aggregate Thermal Margin 2 *(P2 DIMM Thrm Mrgn2)*	B3h	All	Temperature 01h	Threshold 01h	[u] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	–

Full Sensor Name (Sensor name in SDR)	Sensor #	Platform Applicability	Sensor Type	Event/Reading Type	Event Offset Triggers	Contrib. To System Status	Assert/De-assert	Readable Value/ Offsets	Event Data	Rearm	Stand-by
Processor 3 DIMM Aggregate Thermal Margin 1 *(P3 DIMM Thrm Mrgn1)*	B4h	Platform Specific	Temperature 01h	Threshold 01h	[u] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	–
Processor 3 DIMM Aggregate Thermal Margin 2 *(P3 DIMM Thrm Mrgn2)*	B5h	Platform Specific	Temperature 01h	Threshold 01h	[u] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	–
Processor 4 DIMM Aggregate Thermal Margin 1 *(P4 DIMM Thrm Mrgn1)*	B6h	Platform Specific	Temperature 01h	Threshold 01h	[u] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	–
Processor 4 DIMM Aggregate Thermal Margin 2 *(P4 DIMM Thrm Mrgn2)*	B7h	Platform Specific	Temperature 01h	Threshold 01h	[u] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	–

Full Sensor Name (Sensor name in SDR)	Sensor #	Platform Applicability	Sensor Type	Event/Reading Type	Event Offset Triggers	Contrib. To System Status	Assert/De-assert	Readable Value/ Offsets	Event Data	Rearm	Stand-by
Fan Tachometer Sensors *(Chassis specific sensor names)*	BAh–BFh	Chassis and Platform Specific	Fan 04h	Threshold 01h	[l] [c,nc]	nc = Degraded c = Non-fatal[2]	As and De	Analog	R, T	M	-
Processor 1 DIMM Thermal Trip *(P1 Mem Thrm Trip)*	C0h	All	Memory 0Ch	Sensor Specific 6Fh	0A- Critical overtemperature	Fatal	As and De	–	Trig Offset	M	-
Processor 2 DIMM Thermal Trip *(P2 Mem Thrm Trip)*	C1h	All	Memory 0Ch	Sensor Specific 6Fh	0A- Critical overtemperature	Fatal	As and De	–	Trig Offset	M	-
Processor 3 DIMM Thermal Trip *(P3 Mem Thrm Trip)*	C2h	All	Memory 0Ch	Sensor Specific 6Fh	0A- Critical overtemperature	Fatal	As and De	–	Trig Offset	M	X
Processor 4 DIMM Thermal Trip *(P4 Mem Thrm Trip)*	C3h	All	Memory 0Ch	Sensor Specific 6Fh	0A- Critical overtemperature	Fatal	As and De	–	Trig Offset	M	X

Full Sensor Name (Sensor name in SDR)	Sensor #	Platform Applicability	Sensor Type	Event/Reading Type	Event Offset Triggers	Contrib. To System Status	Assert/De-assert	Readable Value/ Offsets	Event Data	Rearm	Stand-by
Global Aggregate Temperature Margin 1 *(Agg Therm Mrgn 1)*	C8h	Platform Specific	Temperature 01h	Threshold 01h	-	-	-	Analog	R, T	A	–
Global Aggregate Temperature Margin 2 *(Agg Therm Mrgn 2)*	C9h	Platform Specific	Temperature 01h	Threshold 01h	-	-	-	Analog	R, T	A	–
Global Aggregate Temperature Margin 3 *(Agg Therm Mrgn 3)*	CAh	Platform Specific	Temperature 01h	Threshold 01h	-	-	-	Analog	R, T	A	–
Global Aggregate Temperature Margin 4 *(Agg Therm Mrgn 4)*	CBh	Platform Specific	Temperature 01h	Threshold 01h	-	-	-	Analog	R, T	A	–
Global Aggregate Temperature Margin 5 *(Agg Therm Mrgn 5)*	CCh	Platform Specific	Temperature 01h	Threshold 01h	-	-	-	Analog	R, T	A	–

Full Sensor Name (Sensor name in SDR)	Sensor #	Platform Applicability	Sensor Type	Event/Reading Type	Event Offset Triggers	Contrib. To System Status	Assert/De-assert	Readable Value/ Offsets	Event Data	Rearm	Stand-by
Global Aggregate Temperature Margin 6 *(Agg Therm Mrgn 6)*	CDh	Platform Specific	Temperature 01h	Threshold 01h	-	-	-	Analog	R, T	A	–
Global Aggregate Temperature Margin 7 *(Agg Therm Mrgn 7)*	CEh	Platform Specific	Temperature 01h	Threshold 01h	-	-	-	Analog	R, T	A	–
Global Aggregate Temperature Margin 8 *(Agg Therm Mrgn 8)*	CFh	Platform Specific	Temperature 01h	Threshold 01h	-	-	-	Analog	R, T	A	–
Baseboard +12V *(BB +12.0V)*	D0h	All	Voltage 02h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	–
Baseboard +5V *(BB +5.0V)*	D1h	All	Voltage 02h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	–

Full Sensor Name (Sensor name in SDR)	Sensor #	Platform Applicability	Sensor Type	Event/Reading Type	Event Offset Triggers	Contrib. To System Status	Assert/De-assert	Readable Value/ Offsets	Event Data	Rearm	Stand-by
Baseboard +3.3V *(BB +3.3V)*	D2h	All	Voltage 02h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	–
Baseboard +5V Stand-by *(BB +5.0V STBY)*	D3h	All	Voltage 02h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	X
Baseboard +3.3V Auxiliary *(BB +3.3V AUX)*	D4h	All	Voltage 02h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	X
Baseboard +1.05V Processor1 Vccp *(BB +1.05Vccp P1)*	D6h	All	Voltage 02h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	–
Baseboard +1.05V Processor2 Vccp *(BB +1.05Vccp P2)*	D7h	All	Voltage 02h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	–
Baseboard +1.5V P1 Memory AB VDDQ *(BB +1.5 P1MEM AB)*	D8h	All	Voltage 02h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	–

Full Sensor Name (Sensor name in SDR)	Sensor #	Platform Applicability	Sensor Type	Event/Reading Type	Event Offset Triggers	Contrib. To System Status	Assert/De-assert	Readable Value/ Offsets	Event Data	Rearm	Stand-by
Baseboard +1.5V P1 Memory CD VDDQ *(BB +1.5 P1MEM CD)*	D9h	All	Voltage 02h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	–
Baseboard +1.5V P2 Memory AB VDDQ *(BB +1.5 P2MEM AB)*	DAh	All	Voltage 02h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	–
Baseboard +1.5V P2 Memory CD VDDQ *(BB +1.5 P2MEM CD)*	DBh	All	Voltage 02h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	–
Baseboard +1.8V Aux *(BB +1.8V AUX)*	DCh	All	Voltage 02h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	–
Baseboard +1.1V Stand-by *(BB +1.1V STBY)*	DDh	All	Voltage 02h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	–
Baseboard CMOS Battery *(BB +3.3V Vbat)*	DEh	All	Voltage 02h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	–

Full Sensor Name (Sensor name in SDR)	Sensor #	Platform Applicability	Sensor Type	Event/Reading Type	Event Offset Triggers	Contrib. To System Status	Assert/De-assert	Readable Value/ Offsets	Event Data	Rearm	Stand-by
Baseboard +1.35V P1 Low Voltage Memory AB VDDQ *(BB +1.35 P1LV AB)*	E4h	All	Voltage 02h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	–
Baseboard +1.35V P1 Low Voltage Memory CD VDDQ *(BB +1.35 P1LV CD)*	E5h	All	Voltage 02h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	–
Baseboard +1.35V P2 Low Voltage Memory AB VDDQ *(BB +1.35 P2LV AB)*	E6h	All	Voltage 02h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	–
Baseboard +1.35V P2 Low Voltage Memory CD VDDQ *(BB +1.35 P2LV CD)*	E7h	All	Voltage 02h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	–

Full Sensor Name (Sensor name in SDR)	Sensor #	Platform Applicability	Sensor Type	Event/Reading Type	Event Offset Triggers	Contrib. To System Status	Assert/De-assert	Readable Value/ Offsets	Event Data	Rearm	Stand-by
Baseboard +3.3V Riser 1 Power Good *(BB +3.3 RSR1 PGD)*	EAh	Platform Specific	Voltage 02h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	–
Baseboard +3.3V Riser 2 Power Good *(BB +3.3 RSR2 PGD)*	EBh	Platform Specific	Voltage 02h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	–
Baseboard +0.9V *(BB 0.9V Core IB)*	ECh	Platform Specific	Voltage 02h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	–
Baseboard +1.8V *(BB 1.8V IB I/O)*	EDh	Platform Specific	Voltage 02h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	–
Baseboard +1.1V *(BB 1.1V PCH)*	EEh	Platform Specific	Voltage 02h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	–

Full Sensor Name (Sensor name in SDR)	Sensor #	Platform Applicability	Sensor Type	Event/Reading Type	Event Offset Triggers	Contrib. To System Status	Assert/De-assert	Readable Value/ Offsets	Event Data	Rearm	Stand-by
Baseboard +1.2V *(BB +1.2V IB)*	EFh	Platform Specific	Voltage 02h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	–
Hard Disk Drive 0 -14 Status *(HDD 0 - 14 Status)*	F0h - FEh	Chassis-specific	Drive Slot 0Dh	Sensor Specific 6Fh	00 - Drive Presence	OK	As and De	–	Trig Offset	A	X
					01- Drive Fault	Degraded					
					07 - Rebuild/Remap in progress	Degraded					

Notes:

1. Redundancy sensors will be only present on systems with appropriate hardware to support redundancy (for instance, fan or power supply).
2. This is only applicable when the system does not support redundant Power supplies. When redundancy is supported, then the contribution to system state is driven by the power unit redundancy sensor.
3. This is only applicable when the system does not support redundant fans. When fan redundancy is supported, then the contribution to system state is driven by the fan redundancy sensor.

Appendix C: BIOS Sensors and SEL Data

BIOS owns a set of IPMI-compliant Sensors. These are actually divided in ownership between BIOS POST (GID = 01) and BIOS SMI Handler (GID = 33). The SMI Handler Sensors are typically for logging runtime error events, but they are active during POST and may log errors such as Correctable Memory ECC Errors if they occur.

It is important to remember that a Sensor is uniquely identified by the combination of Sensor Owner plus Sensor Number. There are cases where the same Sensor Number is used with different Sensor Owners – this is not a conflict. For example, in the BIOS Sensors list there is a Sensor Number 83h for Sensor Owner 01h (BIOS POST) as well as for Sensor Owner 33h (SMI Handler), but these are two distinct sensors reporting the same type of event from different sources (Generator IDs 01h and 33h).

On the other hand, each distinct Sensor (GID + Sensor Number) is defined by one specific Sensor Type describing the kind of data being reported, and one specific Event Type describing the type of event and the format of the data being reported.

Table 103. BIOS Sensor and SEL Data

Sensor Name	Sensor Number	Sensor Owner (GID)	Sensor Type	Event/Reading Type Offset Values	Event Data 2 Event Data 3
Mirroring Redundancy State	01h	33h (SMI Handler)	0Ch (Memory)	0Bh (Discrete, Redundancy State) 0h = Fully Redundant 2h = Redundancy Degraded	ED2 = [7:4] = Mirroring Domain 0-1 = Channel Pair for Socket [3:2] = Reserved [1:0] = Rank on DIMM 0-3 = Rank Number ED3 = [7:5]= Socket ID 0-3 = CPU1-4 [4:3] = Channel 0-3 = Channel A-D for Socket [2:0] = DIMM 0-2 = DIMM 1-3 on Channel

Sensor Name	Sensor Number	Sensor Owner (GID)	Sensor Type	Event/Reading Type Offset Values	Event Data 2 Event Data 3
Memory RAS Configuration Status	02h	01h (BIOS POST)	0Ch (Memory)	09h (Digital Discrete) 0h = RAS Configuration Disabled 1h = RAS Configuration Enabled	ED2 = [7:4] = Reserved [3:0] Config Err 0 = None 3 = Invalid DIMM Config for RAS Mode ED3 = [7:4] = Reserved [3:0] = RAS Mode 0 = None 1 = Mirroring 2 = Lockstep 4 = Rank Sparing
Memory ECC Error	02h	33h (SMI Handler)	0Ch (Memory)	6Fh (Sensor Specific Offset) 0h = Correctable Error 1h = Uncorrectable Error	ED2 = [7:2] = Reserved [1:0] = Rank on DIMM 0-3 = Rank Number ED3 = [7:5]= Socket ID 0-3 = CPU1-4 [4:3] = Channel 0-3 = Channel A-D for Socket [2:0] = DIMM 0-2 = DIMM 1-3 on Channel
Legacy PCI Error	03h	33h (SMI Handler)	13h (Critical Interrupt)	6Fh (Sensor Specific Offset) 4h = PCI PERR 5h = PCI SERR	ED2 = [7:0] = Bus Number ED3 = [7:3] = Device Number [2:0] = Function Number

Sensor Name	Sensor Number	Sensor Owner (GID)	Sensor Type	Event/Reading Type Offset Values	Event Data 2 Event Data 3
PCIe Fatal Error (Standard AER Errors) (see Sensor 14h for continuation)	04h	33h (SMI Handler)	13h (Critical Interrupt)	70h (OEM Discrete) 0h = Data Link Layer Protocol Error 1h = Surprise Link Down Error 2h = Completer Abort 3h = Unsupported Request 4h = Poisoned TLP 5h = Flow Control Protocol 6h = Completion Timeout 7h = Receiver Buffer Overflow 8h = ACS Violation 9h = Malformed TLP Ah = ECRC Error Bh = Received Fatal Message From Downstream Ch = Unexpected Completion Dh = Received ERR_NONFATAL Message Eh = Uncorrectable Internal Fh = MC Blocked TLP	ED2 = [7:0] = Bus Number ED3 = [7:3] = Device Number [2:0] = Function Number
PCIe Correctable Error (Standard AER Errors)	05h	33h (SMI Handler)	13h (Critical Interrupt)	71h (OEM Discrete) 0h = Receiver Error 1h = Bad DLLP 2h = Bad TLP 3h = Replay Num Rollover 4h = Replay Timer timeout 5h = Advisory Non-fatal 6h = Link BW Changed 7h = Correctable Internal 8h = Header Log Overflow	ED2 = [7:0] = Bus Number ED3 = [7:3] = Device Number [2:0] = Function Number
BIOS POST Error	06h	01h (BIOS POST)	0Fh (System Firmware Progress)	6Fh (Sensor Specific Offset) 0h = System Firmware Error (POST Error Code)	ED2 = [7:0] = LSB of POST Error Code ED3 = [7:0] MSB of POST Error Code

Sensor Name	Sensor Number	Sensor Owner (GID)	Sensor Type	Event/Reading Type Offset Values	Event Data 2 Event Data 3
QPI Correctable Errors (reserved for Validation)	06h	33h (SMI Handler)	13h (Critical Interrupt)	72h (OEM Discrete) Offset Reserved	ED2 = [7:0] = Node ID 0-3 = CPU1-4 ED3 = Reserved
QPI Fatal Error (see Sensor 17h for continuation)	07h	33h (SMI Handler)	13h (Critical Interrupt)	73h (OEM Discrete) 0h = Link Layer Uncorrectable ECC Error 1h = Protocol Layer Poisoned Packet Reception Error 2h = Link/PHY Init Failure with resultant degradation in link width 3h = PHY Layer detected drift buffer alarm 4h = PHY detected latency buffer rollover 5h = PHY Init Failure 6h = Link Layer generic control error (buffer overflow/underflow, credit underflow and so on.) 7h = Parity error in link or PHY layer 8h = Protocol layer timeout detected 9h = Protocol layer failed response Ah = Protocol layer illegal packet field, target Node ID Error, and so on. Bh = Protocol Layer Queue/table overflow/underflow Ch = Viral Error Dh = Protocol Layer parity error Eh = Routing Table Error Fh = (unused)	ED2 = [7:0] = Node ID 0-3 = CPU1-4 ED3 = No Data
Chipset Proprietary (reserved for Validation)	08h	33h (SMI Handler)	19h (Chipset)	75h (OEM Discrete) Offset Reserved	ED2 = Reserved ED3 = Reserved

Sensor Name	Sensor Number	Sensor Owner (GID)	Sensor Type	Event/Reading Type Offset Values	Event Data 2 Event Data 3
QPI Link Width Reduced	09h	01h (BIOS POST)	13h (Critical Interrupt)	77h (OEM Discrete) 1h = Reduced to ½ width 2h = Reduced to ¼ width	ED2 = [7:0] = Node ID 0-3 = CPU1-4 ED3 = No Data
Memory Error Extension (reserved for Validation)	10h	33h (SMI Handler)	0Ch (Memory)	7Fh (OEM Discrete) Offset Reserved	ED2 = Reserved ED3 = Reserved
Sparing Redundancy State	11h	33h (SMI Handler)	0Ch (Memory)	0Bh (Discrete, Redundancy State) 0h = Fully Redundant 2h = Redundancy Degraded	ED2 = [7:4] = Sparing Domain 0-3 = Channel A-D for Socket [3:2] = Reserved [1:0] = Rank on DIMM 0-3 = Rank Number ED3 = [7:5]= Socket ID 0-3 = CPU1-4 [4:3] = Channel 0-3 = Channel A-D for Socket [2:0] = DIMM 0-2 = DIMM 1-3 on Channel
Memory RAS Mode Select	12h	01h (BIOS POST)	0Ch (Memory)	09h (Digital Discrete) 0h = RAS Configuration Disabled 1h = RAS Configuration Enabled	ED2 = Prior Mode [7:4] = Reserved [3:0] = RAS Mode 0 = None 1 = Mirroring 2 = Lockstep 4 = Rank Sparing ED3 = Selected Mode [7:4] = Reserved [3:0] = RAS Mode 0 = None 1 = Mirroring 2 = Lockstep 4 = Rank Sparing

Sensor Name	Sensor Number	Sensor Owner (GID)	Sensor Type	Event/Reading Type Offset Values	Event Data 2 Event Data 3

Memory Parity Error	13h	33h (SMI Handler)	0Ch (Memory)	6Fh (Sensor Specific Offset)
				2h = Address Parity Error
					ED2 = Validity
					[7:5] = Reserved
					[4] = Channel Validity Check
					0 = ED3 Chan # Not Valid
					1 = ED3 Chan # Is Valid
					[3] = DIMM Validity Check
					0 = ED3 DIMM # Not Valid
					1 = ED3 DIMM # Is Valid
					[2:0] = Error Type
					0 = Not Known
					2 = Address Parity Error
					ED3 = Location
					[7:5]= Socket ID
					0-3 = CPU1-4
					[4:2] = Channel
					0-3 = Channel A-D for Socket
					[1:0] = DIMM
					0-2 = DIMM 1-3 on Channel

PCIe Fatal Error#2 (Standard AER Errors) (continuation of Sensor 04h)	14h	33h (SMI Handler)	13h (Critical Interrupt)	76h (OEM Discrete) 0h = Atomic Egress Blocked 1h = TLP Prefix Blocked Fh = Unspecified Non-AER Fatal Error	ED2 = [7:0] = Bus Number ED3 = [7:3] = Device Number [2:0] = Function Number

Sensor Name	Sensor Number	Sensor Owner (GID)	Sensor Type	Event/Reading Type Offset Values	Event Data 2 Event Data 3
QPI Fatal Error (continuation of Sensor 07h)	17h	33h (SMI Handler)	13h (Critical Interrupt)	74h (OEM Discrete) 0h = Illegal inbound request 1h = IIO Write Cache Uncorrectable Data ECC Error 2h = IIO CSR crossing 32-bit boundary Error 3h = IIO Received XPF physical/logical redirect interrupt inbound 4h = IIO Illegal SAD or Illegal or non-existent address or memory 5h = IIO Write Cache Coherency Violation	ED2 = [7:0] = Node ID 0-3 = CPU1-4 ED3 = No Data
System Event	83h	01h (BIOS POST)	12h (System Event)	6Fh (Sensor Specific Offset) 1h = System Boot Event 5h = Time Synch (EPSD)	ED2 = (only for Time Synch) [7:0] Synch # 00h = 1st in pair 80h = 2nd in pair ED3 = No Data
System Event	83h	33h (SMI Handler)	12h (System Event)	6Fh (Sensor Specific Offset) 5h = Time Synch (EPSD)	ED2 = (only for Time Synch) [7:0] Synch # 00h = 1st in pair 80h = 2nd in pair ED3 = No Data

Appendix D: POST Code LED Decoder

During the system boot process, the BIOS executes several platform configuration processes, each of which is assigned a specific hex POST code number. As each configuration routine is started, the BIOS displays the POST code on the POST code diagnostic LEDs found on the back edge of the server board. To assist in troubleshooting a system hang during the POST process, the diagnostic LEDs can be used to identify the last POST process to be executed.

Each POST code is represented by the eight amber diagnostic LEDs. The POST codes are divided into two nibbles, an upper nibble and a lower nibble. The upper nibble bits are represented by diagnostic LEDs #4, #5, #6, and #7. The lower nibble bits are represented by diagnostics LEDs #0, #1, #2, and #3. If the bit is set in the upper and lower nibbles, then the corresponding LED is lit. If the bit is clear, then the corresponding LED is off.

The diagnostic LED #7 is labeled as “MSB” (Most Significant Bit), and the diagnostic LED #0 is labeled as “LSB” (Least Significant Bit).

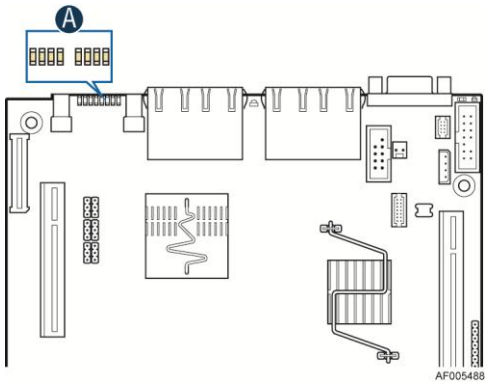


Figure 52. Diagnostic LED Placement Diagram

In the following example, the BIOS sends a value of ACh to the diagnostic LED decoder. The LEDs are decoded as follows:

Table 104. POST Progress Code LED Example

LEDs	Upper Nibble LEDs				Lower Nibble LEDs			
	MSB							LSB
	LED #7	LED #6	LED #5	LED #4	LED #3	LED #2	LED #1	LED #0
	8h	4h	2h	1h	8h	4h	2h	1h
Status	ON	OFF	ON	OFF	ON	ON	OFF	OFF
Results	1	0	1	0	1	1	0	0
	Ah				Ch			

Upper nibble bits = 1010b = Ah; Lower nibble bits = 1100b = Ch; the two are concatenated as ACh.

Table 105. Diagnostic LED POST Code Decoder

Checkpoint	Diagnostic LED Decoder = On, 0=Off								Description
	Upper Nibble				Lower Nibble				
	SB							LSB	
	8h	4h	2h	1h	8h	4h	2h	1h	
LED	#7	#6	#5	#4	#3	#2	#1	#0	
Host Processor									
0x10h	0	0	0	1	0	0	0	0	Power-on initialization of the host processor (bootstrap processor)
0x11h	0	0	0	1	0	0	0	1	Host processor cache initialization (including AP)
0x12h	0	0	0	1	0	0	1	0	Starting application processor initialization
0x13h	0	0	0	1	0	0	1	1	SMM initialization
Chipset									
0x21h	0	0	1	0	0	0	0	1	Initializing a chipset component
Memory									
0x22h	0	0	1	0	0	0	1	0	Reading configuration data from memory (SPD on FBDIMM)
0x23h	0	0	1	0	0	0	1	1	Detecting presence of memory
0x24h	0	0	1	0	0	1	0	0	Programming timing parameters in the memory controller
0x25h	0	0	1	0	0	1	0	1	Configuring memory parameters in the memory controller
0x26h	0	0	1	0	0	1	1	0	Optimizing memory controller settings
0x27h	0	0	1	0	0	1	1	1	Initializing memory, such as ECC in it
0x28h	0	0	1	0	1	0	0	0	Testing memory
0xE4h	1	1	1	0	0	1	0	0	BIOS cannot communicate with DIMM (serial channel hardware failure)
0xE6h	1	1	1	0	0	1	1	0	DIMM(s) failed Memory iBIST or Memory Link Training failure
0xE8h	1	1	1	0	1	0	0	0	No memory available (system halted)
0xE9h	1	1	1	0	1	0	0	1	Unsupported or invalid DIMM configuration (system halted)
0xEAh	1	1	1	0	1	0	1	0	DIMM training sequence failed (system halted)
0xEBh	1	1	1	0	1	0	1	1	Memory test failed (system halted)
0xECh	1	1	1	0	1	1	0	0	Unsupported or invalid DIMM configuration (system halted)
0xEDh	1	1	1	0	1	1	0	1	Unsupported or invalid DIMM configuration (system halted)
0xEBh	1	1	1	0	1	0	1	1	DIMM with corrupted SPD data detected (system halted)
QuickPath Interconnect (QPI)									
0xA0h	1	0	1	0	0	0	0	0	QPI Initialization
0xA1h	1	0	1	0	0	0	0	1	QPI Initialization
0xA2h	1	0	1	0	0	0	1	0	QPI Initialization
0xA3h	1	0	1	0	0	0	1	1	QPI Initialization
0xA4h	1	0	1	0	0	1	0	0	QPI Initialization
0xA5h	1	0	1	0	0	1	0	1	QPI Initialization
0xA6h	1	0	1	0	0	1	1	0	QPI Initialization
0xA7h	1	0	1	0	0	1	1	1	QPI Initialization
0xA8h	1	0	1	0	1	0	0	0	QPI Initialization
0xA9h	1	0	1	0	1	0	0	1	QPI Initialization
0xAAh	1	0	1	0	1	0	1	0	QPI Initialization
0xABh	1	0	1	0	1	0	1	1	QPI Initialization
0xACh	1	0	1	0	1	1	0	0	QPI Initialization
0xADh	1	0	1	0	1	1	0	1	QPI Initialization

Checkpoint	Diagnostic LED Decoder = On, 0=Off								Description
	Upper Nibble				Lower Nibble				
	SB							LSB	
	8h	4h	2h	1h	8h	4h	2h	1h	
LED	#7	#6	#5	#4	#3	#2	#1	#0	
0xAEh	1	0	1	0	1	1	1	0	QPI Initialization
0xAFh	1	0	1	0	1	1	1	1	QPI Initialization
Integrated Memory Controller (IMC)									
0xB0h	1	0	1	1	0	0	0	0	Memory Initialization of Integrated Memory Controller
0xB1h	1	0	1	1	0	0	0	1	Memory Initialization of Integrated Memory Controller
0xB2h	1	0	1	1	0	0	1	0	Memory Initialization of Integrated Memory Controller
0xB3h	1	0	1	1	0	0	1	1	Memory Initialization of Integrated Memory Controller
0xB4h	1	0	1	1	0	1	0	0	Memory Initialization of Integrated Memory Controller
0xB5h	1	0	1	1	0	1	0	1	Memory Initialization of Integrated Memory Controller
0xB6h	1	0	1	1	0	1	1	0	Memory Initialization of Integrated Memory Controller
0xB7h	1	0	1	1	0	1	1	1	Memory Initialization of Integrated Memory Controller
0xB8h	1	0	1	1	1	0	0	0	Memory Initialization of Integrated Memory Controller
0xB9h	1	0	1	1	1	0	0	1	Memory Initialization of Integrated Memory Controller
0xBAh	1	0	1	1	1	0	1	0	Memory Initialization of Integrated Memory Controller
0xBBh	1	0	1	1	1	0	1	1	Memory Initialization of Integrated Memory Controller
0xBCh	1	0	1	1	1	1	0	0	Memory Initialization of Integrated Memory Controller
0xBDh	1	0	1	1	1	1	0	1	Memory Initialization of Integrated Memory Controller
0xBEh	1	0	1	1	1	1	1	0	Memory Initialization of Integrated Memory Controller
0xBFh	1	0	1	1	1	1	1	1	Memory Initialization of Integrated Memory Controller
PCI Bus									
0x50h	0	1	0	1	0	0	0	0	Enumerating PCI buses
0x51h	0	1	0	1	0	0	0	1	Allocating resources to PCI buses
0x52h	0	1	0	1	0	0	1	0	Hot Plug PCI controller initialization
0x53h	0	1	0	1	0	0	1	1	Reserved for PCI bus
0x54h	0	1	0	1	0	1	0	0	Reserved for PCI bus
0x55h	0	1	0	1	0	1	0	1	Reserved for PCI bus
QuickPath Interconnect (QPI)									
0xA0h	1	0	1	0	0	0	0	0	QPI Initialization
0xA1h	1	0	1	0	0	0	0	1	QPI Initialization
0xA2h	1	0	1	0	0	0	1	0	QPI Initialization
0xA3h	1	0	1	0	0	0	1	1	QPI Initialization
0xA4h	1	0	1	0	0	1	0	0	QPI Initialization
0xA5h	1	0	1	0	0	1	0	1	QPI Initialization
0xA6h	1	0	1	0	0	1	1	0	QPI Initialization
0xA7h	1	0	1	0	0	1	1	1	QPI Initialization
0xA8h	1	0	1	0	1	0	0	0	QPI Initialization
0xA9h	1	0	1	0	1	0	0	1	QPI Initialization
0xAAh	1	0	1	0	1	0	1	0	QPI Initialization
0xABh	1	0	1	0	1	0	1	1	QPI Initialization
0xACh	1	0	1	0	1	1	0	0	QPI Initialization
0xADh	1	0	1	0	1	1	0	1	QPI Initialization
0xAEh	1	0	1	0	1	1	1	0	QPI Initialization
0xAFh	1	0	1	0	1	1	1	1	QPI Initialization
Integrated Memory Controller (IMC)									

Checkpoint	Diagnostic LED Decoder = On, 0=Off								Description
	Upper Nibble				Lower Nibble				
	SB							LSB	
	8h	4h	2h	1h	8h	4h	2h	1h	
LED	#7	#6	#5	#4	#3	#2	#1	#0	
0xB0h	1	0	1	1	0	0	0	0	Memory Initialization of Integrated Memory Controller
0xB1h	1	0	1	1	0	0	0	1	Memory Initialization of Integrated Memory Controller
0xB2h	1	0	1	1	0	0	1	0	Memory Initialization of Integrated Memory Controller
0xB3h	1	0	1	1	0	0	1	1	Memory Initialization of Integrated Memory Controller
0xB4h	1	0	1	1	0	1	0	0	Memory Initialization of Integrated Memory Controller
0xB5h	1	0	1	1	0	1	0	1	Memory Initialization of Integrated Memory Controller
0xB6h	1	0	1	1	0	1	1	0	Memory Initialization of Integrated Memory Controller
0xB7h	1	0	1	1	0	1	1	1	Memory Initialization of Integrated Memory Controller
0xB8h	1	0	1	1	1	0	0	0	Memory Initialization of Integrated Memory Controller
0xB9h	1	0	1	1	1	0	0	1	Memory Initialization of Integrated Memory Controller
0xBAh	1	0	1	1	1	0	1	0	Memory Initialization of Integrated Memory Controller
0xBBh	1	0	1	1	1	0	1	1	Memory Initialization of Integrated Memory Controller
0xBCh	1	0	1	1	1	1	0	0	Memory Initialization of Integrated Memory Controller
0xBDh	1	0	1	1	1	1	0	1	Memory Initialization of Integrated Memory Controller
0xBEh	1	0	1	1	1	1	1	0	Memory Initialization of Integrated Memory Controller
0xBFh	1	0	1	1	1	1	1	1	Memory Initialization of Integrated Memory Controller
PCI Bus									
0x50h	0	1	0	1	0	0	0	0	Enumerating PCI buses
0x51h	0	1	0	1	0	0	0	1	Allocating resources to PCI buses
0x52h	0	1	0	1	0	0	1	0	Hot Plug PCI controller initialization
0x53h	0	1	0	1	0	0	1	1	Reserved for PCI bus
0x54h	0	1	0	1	0	1	0	0	Reserved for PCI bus
0x55h	0	1	0	1	0	1	0	1	Reserved for PCI bus
USB									
0x56h	0	1	0	1	0	1	1	0	Initializing USB host controllers
0x57h	0	1	0	1	0	1	1	1	Detecting USB devices
0x58h	0	1	0	1	1	0	0	0	Resetting USB bus
0x59h	0	1	0	1	1	0	0	1	Reserved for USB devices
ATA/ATAPI/SATA									
0x5Ah	0	1	0	1	1	0	1	0	Resetting SATA bus and all devices
0x5Bh	0	1	0	1	1	0	1	1	Detecting the presence of ATA device
0x5Ch	0	1	0	1	1	1	0	0	Enable SMART if supported by ATA device
0x5Dh	0	1	0	1	1	1	0	1	Reserved for ATA
SMBUS*									
0x5Eh	0	1	0	1	1	1	1	0	Resetting SMBUS*
0x5Fh	0	1	0	1	1	1	1	1	Reserved for SMBUS*
I/O Controller Hub									
0x61h	0	1	1	0	0	0	0	1	Initializing I/O Controller Hub
uper I/O									
0x63h	0	1	1	0	0	0	1	1	Initializing Super I/O
Local Console									
0x70h	0	1	1	1	0	0	0	0	Resetting the video controller (VGA)
0x71h	0	1	1	1	0	0	0	1	Disabling the video controller (VGA)
0x72h	0	1	1	1	0	0	1	0	Enabling the video controller (VGA)

Checkpoint	Diagnostic LED Decoder = On, 0=Off								Description
	Upper Nibble				Lower Nibble				
	SB							LSB	
	8h	4h	2h	1h	8h	4h	2h	1h	
LED	#7	#6	#5	#4	#3	#2	#1	#0	
0x73h	0	1	1	1	0	0	1	1	Reserved for video controller (VGA)
Remote Console									
0x78h	0	1	1	1	1	0	0	0	Resetting the console controller
0x79h	0	1	1	1	1	0	0	1	Disabling the console controller
0x7Ah	0	1	1	1	1	0	1	0	Enabling the console controller
0x7Bh	0	1	1	1	1	0	1	1	Reserved for console controller
Keyboard (only USB)									
0x90h	1	0	0	1	0	0	0	0	Resetting the keyboard
0x91h	1	0	0	1	0	0	0	1	Disabling the keyboard
0x92h	1	0	0	1	0	0	1	0	Detecting the presence of the keyboard
0x93h	1	0	0	1	0	0	1	1	Enabling the keyboard
0x94h	1	0	0	1	0	1	0	0	Clearing keyboard input buffer
0x96h	1	0	0	1	0	1	1	0	Reserved for keyboard
Mouse (only USB)									
0x98h	1	0	0	1	0	0	1	0	Resetting the mouse
0x99h	1	0	0	1	0	0	1	1	Detecting the mouse
0x9Ah	1	0	0	1	0	1	1	0	Detecting the presence of mouse
0x9Bh	1	0	0	1	0	1	1	1	Enabling the mouse
0x9Ch	1	0	0	1	0	0	1	0	Reserved for mouse
Serial Port									
0xA8h	1	0	1	0	1	0	0	0	Resetting the serial port
0xA9h	1	0	1	0	1	0	0	1	Disabling the serial port
0xAAh	1	0	1	0	1	0	1	0	Detecting the presence of the serial port
0xABh	1	0	1	0	1	0	1	1	Clearing serial port buffer
0xACh	1	0	1	0	1	1	0	0	Enabling serial port
0xADh	1	0	1	0	1	1	0	1	Reserved for serial port
Fixed Media									
0xB0h	1	0	1	1	0	0	0	0	Resetting fixed media device
0xB1h	1	0	1	1	0	0	0	1	Disabling fixed media device
0xB2h	1	0	1	1	0	0	1	0	Detecting presence of a fixed media device (SATA hard drive detection, and so forth)
0xB3h	1	0	1	1	0	0	1	1	Enabling/configuring a fixed media device
0xB4h	1	0	1	1	0	1	0	0	Reserved for fixed media
Removable Media									
0xB8h	1	0	1	1	1	0	0	0	Resetting removable media device
0xB9h	1	0	1	1	1	0	0	1	Disabling removable media device
0xBAh	1	0	1	1	1	0	1	0	Detecting presence of a removable media device (SATA CDROM detection, and so forth)
0xBCh	1	0	1	1	1	1	0	0	Enabling/configuring a removable media device
0xBDh	1	0	1	1	1	1	0	1	Reserved for removable media device
Boot Device Selection (BDS)									
0xD0	1	1	0	1	0	0	0	0	Entered the Boot Device Selection phase (BDS)
0xD1	1	1	0	1	0	0	0	1	Return to last good boot device
0xD2	1	1	0	1	0	0	1	0	Setup boot device selection policy
0xD3	1	1	0	1	0	0	1	1	Connect boot device controller

Checkpoint	Diagnostic LED Decoder = On, 0=Off								Description
	Upper Nibble				Lower Nibble				
	SB							LSB	
	8h	4h	2h	1h	8h	4h	2h	1h	
LED	#7	#6	#5	#4	#3	#2	#1	#0	
0xD4	1	1	0	1	0	1	0	0	Attempt flash update boot mode
0xD5	1	1	0	1	0	1	0	1	Transfer control to EFI boot
0xD6	1	1	0	1	0	1	1	0	Trying to boot device selection
0xDF	1	1	0	1	1	1	1	1	Reserved for boot device selection
Pre-EFI Initialization (PEI) Core									
0xE0h	1	1	1	0	0	0	0	0	Entered Pre-EFI Initialization phase (PEI)
0xE1h	1	1	1	0	0	0	0	1	Started dispatching early initialization modules (PEIM)
0xE2h	1	1	1	0	0	0	1	0	Initial memory found, configured, and installed correctly
0xE3h	1	1	1	0	0	0	1	1	Transfer control to the DXE Core
PEI Modules									
0xF0h	1	1	1	1	0	0	0	0	Install PEIM for Platform Status Codes
0xF1h	1	1	1	1	0	0	0	1	Detecting Platform Type
0xF2h	1	1	1	1	0	0	1	0	Early Platform Initialization
0xF3h	1	1	1	1	0	0	1	1	PEI Modules initialized
Driver eXecution Environment (DXE) Core									
0xE4h	1	1	1	0	0	1	0	0	Entered EFI driver execution phase (DXE)
0xE5h	1	1	1	0	0	1	0	1	Started dispatching drivers
0xE6h	1	1	1	0	0	1	1	0	Started connecting drivers
DXE Drivers									
0xE7h	1	1	1	0	1	1	0	1	Waiting for user input
0xE8h	1	1	1	0	1	0	0	0	Checking password
0xE9h	1	1	1	0	1	0	0	1	Entering BIOS setup
0xEAh	1	1	1	0	1	1	0	0	Flash Update
0xEBh	1	1	1	0	1	1	0	1	Legacy Option ROM initialization
0xECh	1	1	1	0	1	0	0	0	DXE Drivers initialized
0xEDh	1	1	1	0	1	0	0	1	Transfer control to Boot Device Selection (BDS)
0xEEh	1	1	1	0	1	1	0	0	Calling Int 19. One beep unless silent boot is enabled.
0xEFh	1	1	1	0	1	1	0	1	Unrecoverable boot failure
Pre-EFI Initialization Module (PEIM)/Recovery									
0x30h	0	0	1	1	0	0	0	0	Crisis recovery initiated because of a user request
0x31h	0	0	1	1	0	0	0	1	Crisis recovery initiated by software (corrupt flash)
0x34h	0	0	1	1	0	1	0	0	Loading crisis recovery capsule
0x35h	0	0	1	1	0	1	0	1	Handing off control to the crisis recovery capsule
0x36h	0	0	1	1	0	1	1	0	Begin crisis recovery
0x3Eh	0	0	1	1	1	1	1	0	No crisis recovery capsule detected
0x3Fh	0	0	1	1	1	1	1	1	Crisis recovery capsule failed integrity check of capsule descriptors

Appendix E: Video POST Code Errors

Whenever possible, the BIOS outputs the current boot progress codes on the video screen. Progress codes are 32-bit quantities plus optional data. The 32-bit numbers include class, subclass, and operation information. The class and subclass fields point to the type of hardware being initialized. The operation field represents the specific initialization activity. Based on the data bit availability to display progress codes, a progress code can be customized to fit the data width. The higher the data bit, the higher the granularity of information that can be sent on the progress port. The progress codes may be reported by the system BIOS or option ROMs.

The Response section in the following table is divided into three types:

- **No Pause:** The message is displayed on the local Video screen during POST or in the Error Manager. The system continues booting with a degraded state. The user may want to replace the erroneous unit. The setup POST error Pause setting does not have any effect with this error.
- **Pause:** The message is displayed on the Error Manager screen, and an error is logged to the SEL. The setup POST error Pause setting determines whether the system pauses to the Error Manager for this type of error, where the user can take immediate corrective action or choose to continue booting.
- **Halt:** The message is displayed on the Error Manager screen, an error is logged to the SEL, and the system cannot boot unless the error is resolved. The user needs to replace the faulty part and restart the system. The setup POST error Pause setting does not have any effect with this error.

Table 106. POST Error Messages and Handling

Error Code	Error Message	Response
0012	CMOS date/time not set.	Major
0048	Password check failed.	Major
0108	Keyboard component encountered a locked error.	Minor
0109	Keyboard component encountered a stuck key error.	Minor
0113	Fixed Media The SAS RAID firmware cannot run properly. The user should attempt to reflash the firmware.	Major
0140	PCI component encountered a PERR error.	Major
0141	PCI resource conflict.	Major
0146	PCI out of resources error.	Major
0192	Processor 0x cache size mismatch detected.	Fatal
0193	Processor 0x stepping mismatch.	Minor
0194	Processor 0x family mismatch detected.	Fatal
0195	Processor 0x Intel(R) QPI speed mismatch.	Major
0196	Processor 0x model mismatch.	Fatal
0197	Processor 0x speeds mismatched.	Fatal
0198	Processor 0x family is not supported.	Fatal
019F	Processor and chipset stepping configuration is unsupported.	Major
5220	CMOS/NVRAM Configuration Cleared.	Major
5221	Passwords cleared by jumper.	Major

Error Code	Error Message	Response
5224	Password clear Jumper is Set.	Major
8160	Processor unable to apply microcode update.	Major
8180	Processor microcode update not found.	Minor
8190	Watchdog timer failed on last boot.	Major
8198	OS boot watchdog timer failure.	Major
8300	Baseboard management controller failed self-test.	Major
84F2	Baseboard management controller failed to respond.	Major
84F3	Baseboard management controller in update mode.	Major
84F4	Sensor data record empty.	Major
84FF	System event log full.	Minor
8500	Memory component could not be configured in the selected RAS mode.	Major
8501	DIMM Population Error.	Major
8502	CLTT Configuration Failure Error.	Major
8520	DIMM_A1 failed Self-Test (BIST).	Major
8521	DIMM_A2 failed Self-Test (BIST).	Major
8522	DIMM_B1 failed Self-Test (BIST).	Major
8523	DIMM_B2 failed Self-Test (BIST).	Major
8524	DIMM_C1 failed Self-Test (BIST).	Major
8525	DIMM_C2 failed Self-Test (BIST).	Major
8526	DIMM_D1 failed Self-Test (BIST).	Major
8527	DIMM_D2 failed Self-Test (BIST).	Major
8540	DIMM_A1 Disabled.	Major
8541	DIMM_A2 Disabled.	Major
8542	DIMM_B1 Disabled.	Major
8543	DIMM_B2 Disabled.	Major
8544	DIMM_C1 Disabled.	Major
8545	DIMM_C2 Disabled.	Major
8546	DIMM_D1 Disabled.	Major
8547	DIMM_D2 Disabled.	Major
8560	DIMM_A1 Component encountered a Serial Presence Detection (SPD) fail error.	Major
8561	DIMM_A2 Component encountered a Serial Presence Detection (SPD) fail error.	Major
8562	DIMM_B1 Component encountered a Serial Presence Detection (SPD) fail error.	Major
8563	DIMM_B2 Component encountered a Serial Presence Detection (SPD) fail error.	Major
8564	DIMM_C1 Component encountered a Serial Presence Detection (SPD) fail error.	Major
8565	DIMM_C2 Component encountered a Serial Presence Detection (SPD) fail error.	Major
8566	DIMM_D1 Component encountered a Serial Presence Detection (SPD) fail error.	Major
8567	DIMM_D2 Component encountered a Serial Presence Detection (SPD) fail error.	Major
85A0	DIMM_A1 Uncorrectable ECC error encountered.	Major
85A1	DIMM_A2 Uncorrectable ECC error encountered.	Major
85A2	DIMM_B1 Uncorrectable ECC error encountered.	Major
85A3	DIMM_B2 Uncorrectable ECC error encountered.	Major
85A4	DIMM_C1 Uncorrectable ECC error encountered.	Major
85A5	DIMM_C2 Uncorrectable ECC error encountered.	Major
85A6	DIMM_D1 Uncorrectable ECC error encountered.	Major

Error Code	Error Message	Response
85A7	DIMM_D2 Uncorrectable ECC error encountered.	Major
8604	Chipset Reclaim of non-critical variables complete.	Minor
9000	Unspecified processor component has encountered a nonspecific error.	Major
9223	Keyboard component was not detected.	Minor
9226	Keyboard component encountered a controller error.	Minor
9243	Mouse component was not detected.	Minor
9246	Mouse component encountered a controller error.	Minor
9266	Local Console component encountered a controller error.	Minor
9268	Local Console component encountered an output error.	Minor
9269	Local Console component encountered a resource conflict error.	Minor
9286	Remote Console component encountered a controller error.	Minor
9287	Remote Console component encountered an input error.	Minor
9288	Remote Console component encountered an output error.	Minor
92A3	Serial port component was not detected.	Major
92A9	Serial port component encountered a resource conflict error.	Major
92C6	Serial Port controller error.	Minor
92C7	Serial Port component encountered an input error.	Minor
92C8	Serial Port component encountered an output error.	Minor
94C6	LPC component encountered a controller error.	Minor
94C9	LPC component encountered a resource conflict error.	Major
9506	ATA/ATPI component encountered a controller error.	Minor
95A6	PCI component encountered a controller error.	Minor
95A7	PCI component encountered a read error.	Minor
95A8	PCI component encountered a write error.	Minor
9609	Unspecified software component encountered a start error.	Minor
9641	PEI Core component encountered a load error.	Minor
9667	PEI module component encountered a illegal software state error.	Fatal
9687	DXE core component encountered a illegal software state error.	Fatal
96A7	DXE boot services driver component encountered a illegal software state error.	Fatal
96AB	DXE boot services driver component encountered invalid configuration.	Minor
96E7	SMM driver component encountered a illegal software state error.	Fatal
0xA000	TPM device not detected.	Minor
0xA001	TPM device missing or not responding.	Minor
0xA002	TPM device failure.	Minor
0xA003	TPM device failed self-test.	Minor
0xA022	Processor component encountered a mismatch error.	Major
0xA027	Processor component encountered a low voltage error.	Minor
0xA028	Processor component encountered a high voltage error.	Minor
0xA421	PCI component encountered a SERR error.	Fatal
0xA500	ATA/ATPI ATA bus SMART not supported.	Minor
0xA501	ATA/ATPI ATA SMART is disabled.	Minor
0xA5A0	PCI Express* component encountered a PERR error.	Minor
0xA5A1	PCI Express* component encountered a SERR error.	Fatal
0xA5A4	PCI Express* IBIST error.	Major

Error Code	Error Message	Response
0xA6A0	DXE boot services driver. Not enough memory available to shadow a legacy option ROM.	Minor
0xB6A3	DXE boot services driver Unrecognized.	Major

Glossary

This appendix contains important terms used in the preceding chapters. For ease of use, numeric entries are listed first (for example, “82460GX”) with alpha entries following (for example, “AGP 4x”). Acronyms are then entered in their respective place, with non-acronyms following.

Table 107. Glossary

Term	Definition
ACPI	Advanced Configuration and Power Interface
AP	Application Processor
APIC	Advanced Programmable Interrupt Control
ARP	Address Resolution Protocol
ASIC	Application Specific Integrated Circuit
BIOS	Basic Input/Output System
BIST	Built-In Self Test
BMC	Baseboard Management Controller
Bridge	Circuitry connecting one computer bus to another, allowing an agent on one to access the other
BSP	Bootstrap Processor
Byte	8-bit quantity
CATERR	On a catastrophic hardware event the core signals CATERR to the uncore. The core enters a halted state that can only be exited by a reset
CBC	Chassis Bridge Controller (A microcontroller connected to one or more other CBCs, together they bridge the IPMB buses of multiple chassis.)
CEK	Common Enabling Kit
CHAP	Challenge Handshake Authentication Protocol
CMOS	In terms of this specification, this describes the PC-AT compatible region of battery-backed 128 bytes of memory, which normally resides on the server board
DCMI	Data Center Management Interface
DHCP	Dynamic Host Configuration Protocol
DPC	Direct Platform Control
EEPROM	Electrically Erasable Programmable Read-Only Memory
EHCI	Enhanced Host Controller Interface
EMP	Emergency Management Port
EPS	External Product Specification
FBD	Fully Buffered DIMM
F MB	Flexible Mother Board
FRB	Fault Resilient Booting
FRU	Field Replaceable Unit
FSB	Front Side Bus
GB	1024 MB
GPIO	General Purpose I/O
GTL	Gunning Transceiver Logic
GPA	Guest Physical Address
HSC	Hot-Swap Controller

Term	Definition
HPA	Host Physical Address
Hz	Hertz (1 cycle/second)
I^2C	Inter-Integrated Circuit Bus
IA	Intel® Architecture
IBF	Input Buffer
ICH	I/O Controller Hub
IC MB	Intelligent Chassis Management Bus
IFB	I/O and Firmware Bridge
ILM	Independent Loading Mechanism
IMC	Integrated Memory Controller
INTR	Interrupt
IP	Internet Protocol
IPMB	Intelligent Platform Management Bus
IPMI	Intelligent Platform Management Interface
IR	Infrared
ITP	In-Target Probe
KB	1024 bytes
KCS	Keyboard Controller Style
LAN	Local Area Network
LCD	Liquid Crystal Display
LED	Light Emitting Diode
LPC	Low Pin Count
LUN	Logical Unit Number
MAC	Media Access Control
MB	1024KB
ME	Management Engine
MD2	Message Digest 2 – Hashing Algorithm
MD5	Message Digest 5 – Hashing Algorithm – Higher Security
ms	Milliseconds
MTTR	Memory Type Range Register
Mux	Multiplexor
NIC	Network Interface Controller
NMI	Nonmaskable Interrupt
OBF	Output Buffer
OEM	Original Equipment Manufacturer
Ohm	Unit of electrical resistance
PECI	Platform Environment Control Interface
PEF	Platform Event Filtering
PEP	Platform Event Paging
PIA	Platform Information Area (This feature configures the firmware for the platform hardware)
PLD	Programmable Logic Device
PMI	Platform Management Interrupt
POST	Power-On Self Test
PSMI	Power Supply Management Interface

Term	Definition
PWM	Pulse-Width Modulation
QPI	QuickPath Interconnect
RAM	Random Access Memory
RASUM	Reliability, Availability, Serviceability, Usability, and Manageability
RISC	Reduced Instruction Set Computing
ROM	Read Only Memory
RTC	Real-Time Clock (Component of ICH peripheral chip on the server board)
RMM3	Remote Management Module 3
SDR	Sensor Data Record
SECC	Single Edge Connector Cartridge
SEEPROM	Serial Electrically Erasable Programmable Read-Only Memory
SEL	System Event Log
SIO	Server Input/Output
SMBUS*	System Management BUS
SMI	Server Management Interrupt (SMI is the highest priority nonmaskable interrupt)
SMM	Server Management Mode
SMS	Server Management Software
SNMP	Simple Network Management Protocol
TBD	To Be Determined
TDP	Thermal Design Power
TIM	Thermal Interface Material
UART	Universal Asynchronous Receiver/Transmitter
UDP	User Datagram Protocol
UHCI	Universal Host Controller Interface
URS	Unified Retention System
UTC	Universal time coordinate
UUID	Universally Unique Identifier
VID	Voltage Identification
VRD	Voltage Regulator Down
VT	Virtualization Technology
Word	16-bit quantity
ZIF	Zero Insertion Force

Reference Documents

- *ACPI 3.0*: http://www.acpi.info/spec.htm
- *IPMI 2.0*
- *Data Center Management Interface Specification v1.0*, May 1, 2008: www.intel.com/go/dcmi
- *PCI Bus Power Management Interface Specification 1.1*: http://www.pcisig.com/
- *PCI Express* Base Specification Rev 2.0 Dec 06*: http://www.pcisig.com/
- *PCI Express* Card Electromechanical Specification Rev 2.0*: http://www.pcisig.com/
- *PMBus**: http://pmbus.org
- *SATA 2.6*: http://www.sata-io.org/
- *SMBIOS 2.4*
- *SSI-EEB 3.0*: http://www.ssiforum.org
- *USB 1.1*: http://www.usb.org
- *USB 2.0*: http://www.usb.org
- *Windows* Logo/SDG 3.0*
- *Intel® Dynamic Power Technology Node Manager 1.5 External Interface Specification using IPMI, 2007*. Intel Corporation.
- *Node Power and Thermal Management Architecture Specification v1.5, rev.0.79. 2007*. Intel Corporation.
- *Intel® Server System Integrated Baseboard Management Controller Core External Product Specification, 2007.* Intel Corporation.
- *Intel® Thurley Server Platform Services IPMI Commands Specification 2007.* Intel Corporation.
- *Intel® Server Safety and Regulatory, 2011.* Intel Corporation. Order number: G23122-001.
- *Intelligent Platform Management Bus Communications Protocol Specification, Version 1.0, 1998*. Intel Corporation, Hewlett-Packard* Company, NEC* Corporation, Dell* Computer Corporation.
- *Platform Environmental Control Interface (PECI) Specification, Version 2.0*. Intel Corporation.
- *Platform Management FRU Information Storage Definition, Version 1.0, Revision 1.2, 2002.* Intel Corporation, Hewlett-Packard* Company, NEC* Corporation, Dell* Computer Corporation. http://developer.intel.com/design/servers/ipmi/spec.htm.