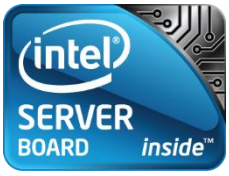
Intel® Server Board S1200V3RP

Technical Product Specification

Intel reference number G84364-004



Revision 2.0

June 2015

Revision History

Date	Revision Number	Modifications
November 2012	0.5	Preliminary release.
May 2013	1.0	▪ Updated BIOS Setup Interface ▪ Changed the chipset of S1200V3RPL to C226
October 2013	1.1	Updated Graphics Controller and Video output: Changed the supporting OS for pGFX Display Port video output to Microsoft Windows 7*.
January 2014	1.2	Added Backup BIOS update instruction.
July 2014	1.3	Updated TPM module information.
November 2014	1.4	Updated Figure 9.
June 2015	2.0	Added support for Intel® Xeon® processor E3-1200 v4 product family.

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.

A "Mission Critical Application" is any application in which failure of the Intel Product could result, directly or indirectly, in personal injury or death. SHOULD YOU PURCHASE OR USE INTEL'S PRODUCTS FOR ANY SUCH MISSION CRITICAL APPLICATION, YOU SHALL INDEMNIFY AND HOLD INTEL AND ITS SUBSIDIARIES, SUBCONTRACTORS AND AFFILIATES, AND THE DIRECTORS, OFFICERS, AND EMPLOYEES OF EACH, HARMLESS AGAINST ALL CLAIMS COSTS, DAMAGES, AND EXPENSES AND REASONABLE ATTORNEYS' FEES ARISING OUT OF, DIRECTLY OR INDIRECTLY, ANY CLAIM OF PRODUCT LIABILITY, PERSONAL INJURY, OR DEATH ARISING IN ANY WAY OUT OF SUCH MISSION CRITICAL APPLICATION, WHETHER OR NOT INTEL OR ITS SUBCONTRACTOR WAS NEGLIGENT IN THE DESIGN, MANUFACTURE, OR WARNING OF THE INTEL PRODUCT OR ANY OF ITS PARTS.

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. The information here is subject to change without notice. Do not finalize a design with this information.

The products described in 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.

Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order.

Copies of documents which have an order number and are referenced in this document, or other Intel literature, may be obtained by calling 1-800-548-4725, or go to: http://www.intel.com/design/literature.htm

Table of Contents

List of Figures

List of Tables

< This page intentionally left blank. >

1. Introduction

This *Technical Product Specification* (TPS) provides board specific information detailing the features, functionality, and high-level architecture of the Intel® Server Board series S1200V3RP family.

Design-level information related to specific server board components and subsystems can be obtained by ordering *External Product Specifications* (EPS) or *External Design Specifications* (EDS) related to this server generation. EPS and EDS documents are made available under NDA with Intel and must be ordered through your local Intel representative. See the Reference Documents section for a list of available documents.

1.1 Chapter Outline

This document is divided into the following chapters:

- Chapter 1 – Introduction
- Chapter 2 – Overview
- Chapter 3 – Functional Architecture
- Chapter 4 – System Security
- Chapter 5 –Intel® Technology Support
- Chapter 6 – Platform Management Functional Overview
- Chapter 7 – Advanced Management Feature Support (RMM4)
- Chapter 8 – On-board Connector/Header Overview
- Chapter 9 – BIOS Setup Interface
- Chapter 10 – Jumper Blocks
- Chapter 11 – Intel® Light Guided Diagnostics
- Chapter 12 – Environmental Limits Specifications
- Chapter 13 – Server Board Power Distribution
- Appendix A – Integration and Usage Tips
- Appendix B – Integrated BMC Sensor Tables
- Appendix C – POST Code Diagnostic LED Decoder
- Appendix D – POST Code Errors
- Appendix E – Supported Intel® Server Chassis
- Glossary
- Reference Documents

1.2 Server Board Use Disclaimer

Intel Corporation server boards support add-in peripherals and contain a number of high-density Very Large Scale Integration (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.

2. Overview

The Intel® Server Board S1200V3RPL, S1200V3RPS, S1200V3RPO, and S1200V3RPM are monolithic printed circuit boards (PCBs) with features designed to support the pedestal or rack server markets. These server boards are designed to support the Intel® Xeon® processor E3-1200 V3 product family and Intel® Xeon® processor E3-1200 V4 product family (only support Intel® C226 Platform Controller Hub (PCH) chipset). Previous generation Intel® Xeon® processors are not supported. Many of the features and functions of these four server boards are common. A board will be identified by name when a described feature or function is unique to it.

2.1 Intel® Server Boards S1200V3RP product family Feature Set

Table 1. Intel® Server Board S1200V3RP Feature Set

<table>
<tr><th>Feature</th><th>Description</th></tr>
<tr><td>Processor</td><td>▪ Support for one Intel® Xeon® processor E3-1200 V3 processor and Intel® Xeon® processor E3-1200 V4 product family (only support Intel® C226 Platform Controller Hub (PCH) chipset) in an LGA 1150 Socket H3 package with Thermal Design Power up to 95W.
▪ 5 GT/s point-to-point DMI 2.0 interface to PCH.</td></tr>
<tr><td>Memory</td><td>▪ Two memory channels, four memory DIMMs (Two memory DIMMs per channel).
▪ Support for 1333/1600 MT/s Unbuffered (UDIMM DDR3L ECC memory).
▪ No support for RDIMMs.
▪ No support for SODIMMs.
▪ No support for mixing ECC and non-ECC UDIMMs.</td></tr>
<tr><td>Chipset</td><td>▪ S1200V3RPO supports for Intel® C224 Platform Controller Hub (PCH) chipset.
▪ S1200V3RPS supports for Intel® C222 Platform Controller Hub (PCH) chipset.
▪ S1200V3RPL and S1200V3RPM support for Intel® C226 Platform Controller Hub (PCH) chipset.</td></tr>
<tr><td>Cooling Fan Support</td><td>Support for:
▪ One processor fan (4-pin header).
▪ Three front system fans (4-pin headers).
▪ One rear system fan (4-pin header).</td></tr>
<tr><td>Add-in PCI Express* Slots</td><td>Four expansion slots at most:
▪ Slot 7: PCI Express* Gen2 x1 electrical with x8 physical connector, from PCH.
▪ Slot 6: PCI Express* Gen3 x8 electrical with x16 physical connector, from processor.
▪ Slot 5: PCI Express* Gen2 x8 or x4 electrical with x8 physical connector, from processor.
▪ Slot 4: PCI Express* Gen2 x4 electrical with x8 physical connector, from PCH.
Slot Population Per SKU
<table>
<tr><th>Slot/SKU</th><th>S1200V3RPL</th><th>S1200V3RPS</th><th>S1200V3RPM</th><th>S1200V3RPO</th></tr>
<tr><td>Slot 7</td><td>Yes</td><td>Yes</td><td>NA</td><td>NA</td></tr>
<tr><td>Slot 6</td><td>Yes</td><td>Yes</td><td>Yes</td><td>Yes</td></tr>
<tr><td>Slot 5</td><td>Yes</td><td>Yes</td><td>NA</td><td>NA</td></tr>
<tr><td>Slot 4</td><td>Yes</td><td>Yes</td><td>NA</td><td>NA</td></tr>
</table></td></tr>
<tr><td>Hard Drive and Optical Drive Support</td><td>▪ Optical devices are supported.
▪ S1200V3RPO supports four SATA connectors at 6Gbps and two SATA connectors at 3Gbps through six onboard SATA connectors.</td></tr>
</table>

Feature	Description
	▪ **S1200V3RPL** and **S1200V3RPM** support six SATA connectors at 6Gbps through six onboard SATA connectors. ▪ **S1200V3RPS** supports two SATA connectors at 6Gbps and four SATA connectors at 3Gbps through six onboard SATA connectors.
RAID Support	▪ Intel® RSTe SW RAID through onboard SATA connectors provides SATA RAID 0/1/10/5. ▪ Intel® Embedded Server RAID Technology II through onboard SATA connectors provides SATA RAID 0/1/10 and optional RAID 5 support provided by the Intel® RAID Activation Key RKSATA4R5. ▪ S1200V3RPL, S1200V3RPO, and S1200V3RPM support one optional internal SAS module connector which supports Intel® SAS or ROC modules with the product code of RMS25CB080, RMS25JB080, RMS25CB040, and RMS25JB040.
External (Back Panel) I/O connections	External connections: ▪ DB9 serial port A connection. ▪ One DB-15 video connector. ▪ Two RJ-45 NIC connectors for 10/100/1000 Mb connections through the two Intel® Ethernet Controller I210. ▪ Two USB 3.0 ports at the back of the board. ▪ Two USB 2.0 ports at the back of the board.
Internal I/O connectors/ headers	▪ One 2x10 pin USB 3.0 header, providing front panel support for two USB ports respectively on S1200V3RPL, S1200V3RPO, and S1200V3RPM. ▪ One 2x5 pin USB 2.0 headers, providing front panel support for two USB ports respectively. ▪ One internal 2x5 pin serial port B header. ▪ One internal Type-A USB 2.0 port. ▪ One 9 pin USB header for eUSB SSD. ▪ One 1x7 pin header for optional Intel® Local Control Panel support. ▪ One combined header consists of a 24-pin SSI-EEB compliant front panel header.
Video Support	▪ Integrated 2D video controller. ▪ Dual monitor video mode is supported. ▪ 16 MB DDR3 Memory. ▪ Only S1200V3RPM supports integrated graphics support for processors with Intel® Graphics Technology. The processor graphics contains generation 7.5 graphics core architecture. This enables substantial gains in performance and lower power consumption over previous generations. Up to 20 EUs are supported depending on the processor SKU. The maximum resolution should be 3840x2160@60Hz, 24bpp.
LAN	Two Gigabit Ethernet Ports through the two Intel® Ethernet Controller I210 PHYs.
Security	Intel® TPM Module AXXTPME3 (Accessory Option).
Server Management	▪ Integrated Baseboard Management Controller, IPMI 2.0 compliant. ▪ Support for Intel® Remote Management Module 4 solutions (Optional except on S1200V3RPS). ▪ Support for Intel® Remote Management Module 4 Lite solutions (Optional except on S1200V3RPS). ▪ Support for Intel® System Management Software. ▪ Support for Intel® Intelligent Power Node Manager (Need PMBus*-compliant power supply).
Form Factor	microATX 9.6”x9.6” compliant form factor.
Compatible Intel® Server Chassis	Intel® Server Chassis P4000S for S1200V3RP.

2.2 Server Board Layout

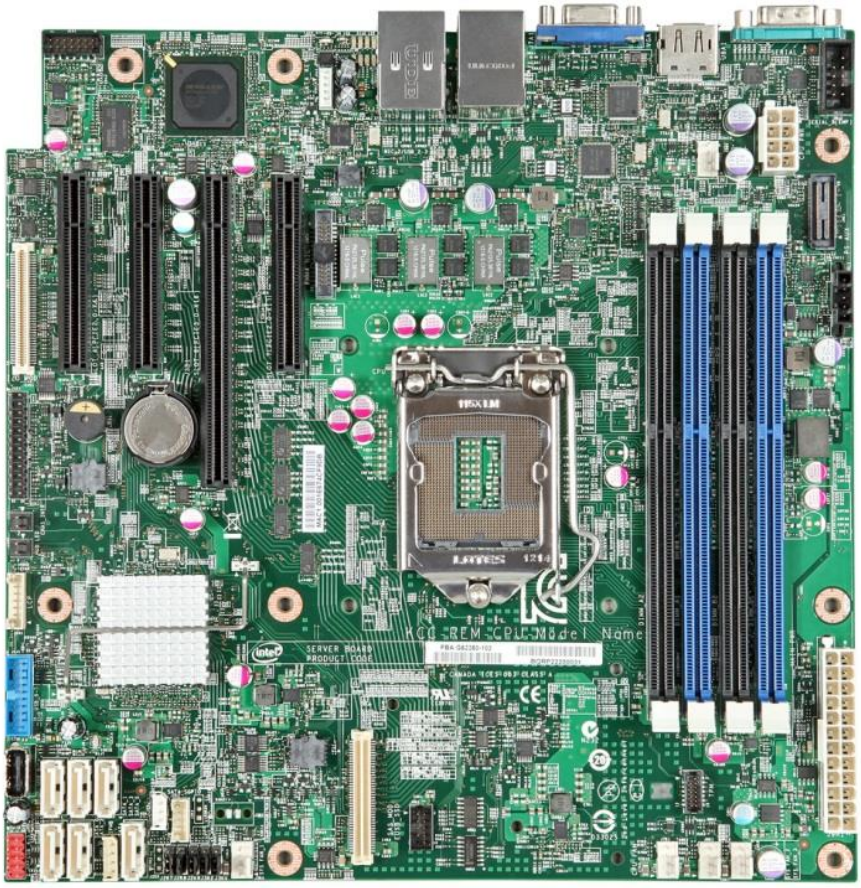


Figure 1. Intel® Server Board S1200V3RP Layout

2.2.1 Server Board Connector and Component Layout

The following figure shows the layout of the server board. Each connector and major component is identified by a number or letter, and a description is given in the figure below.

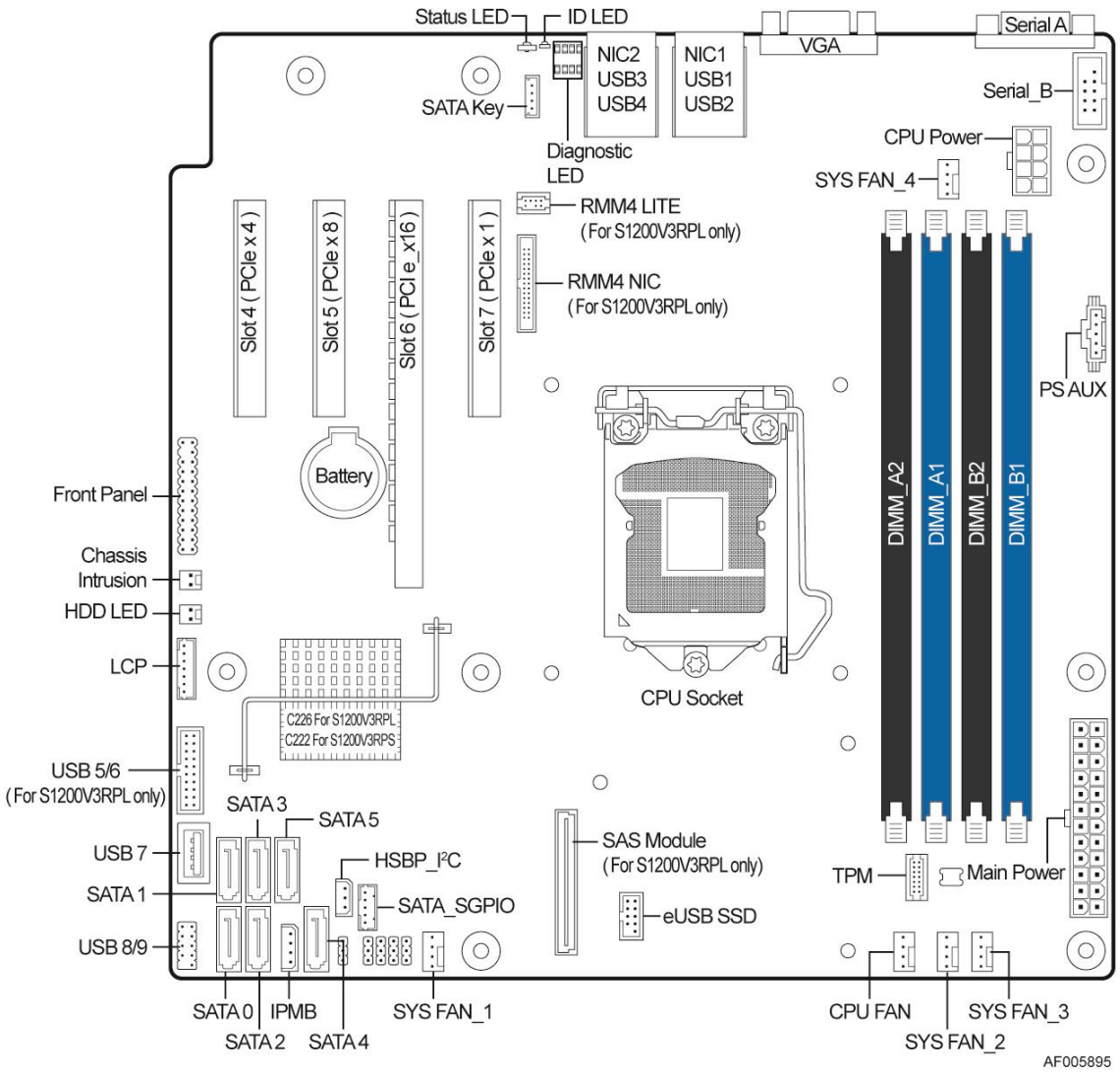


Figure 2. Intel® Server Board S1200V3RPL and S1200V3RPS Layout

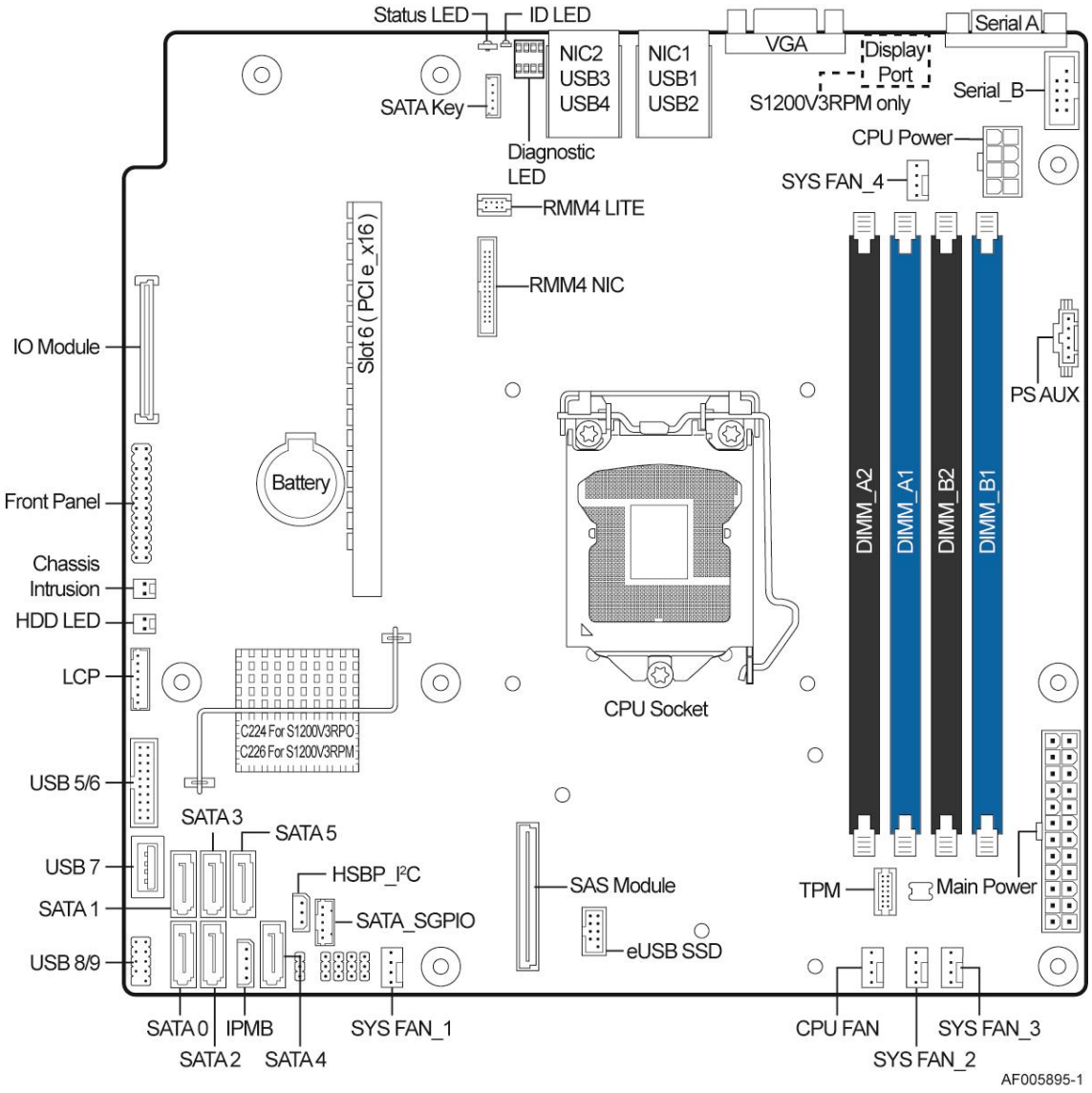


Figure 3. Intel® Server Board S1200V3RPO and S1200V3RPM Layout

2.2.2 Server Board Mechanical Drawings

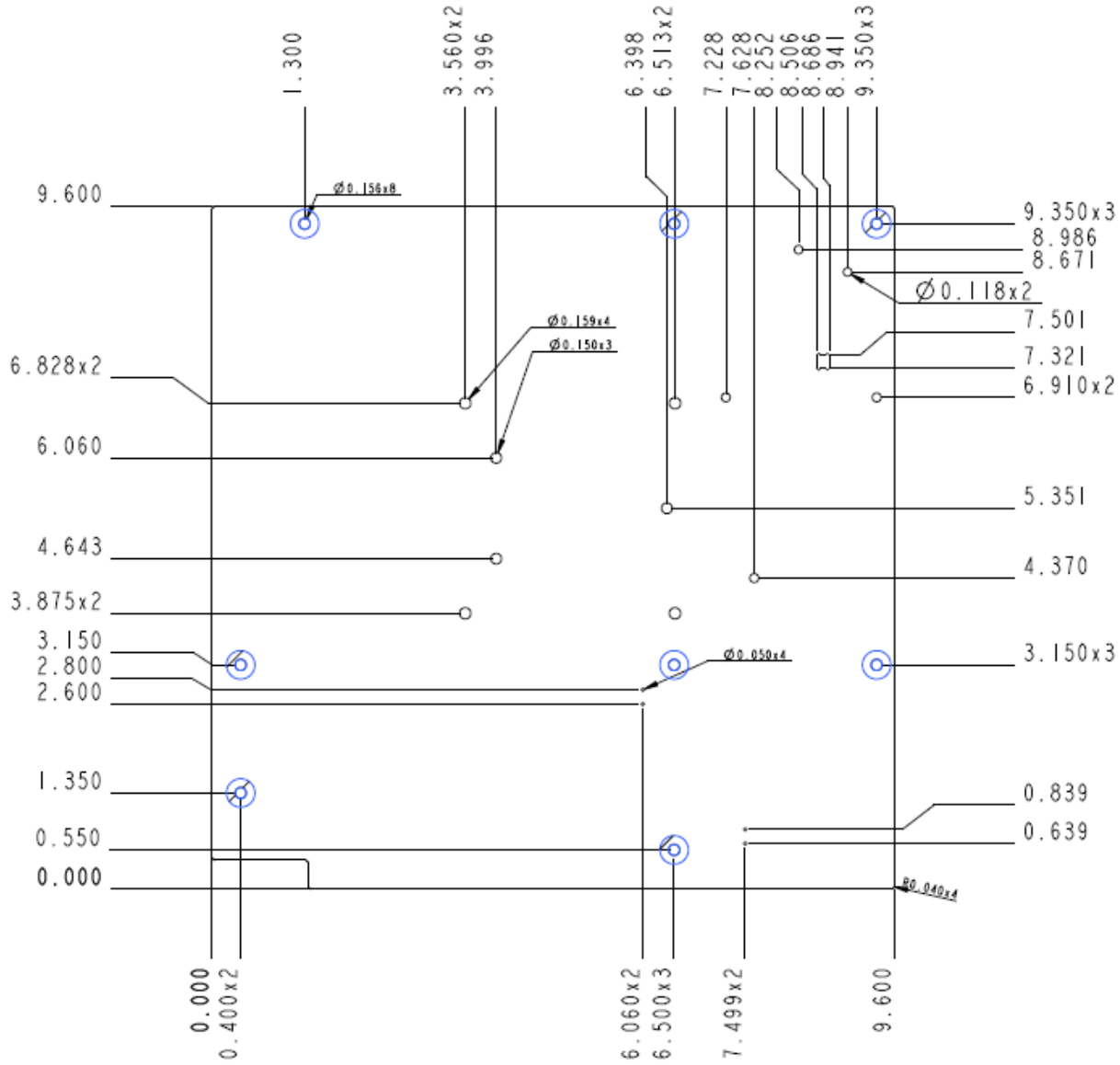


Figure 4. Intel® Server Board S1200V3RP – Mounting Hole Locations

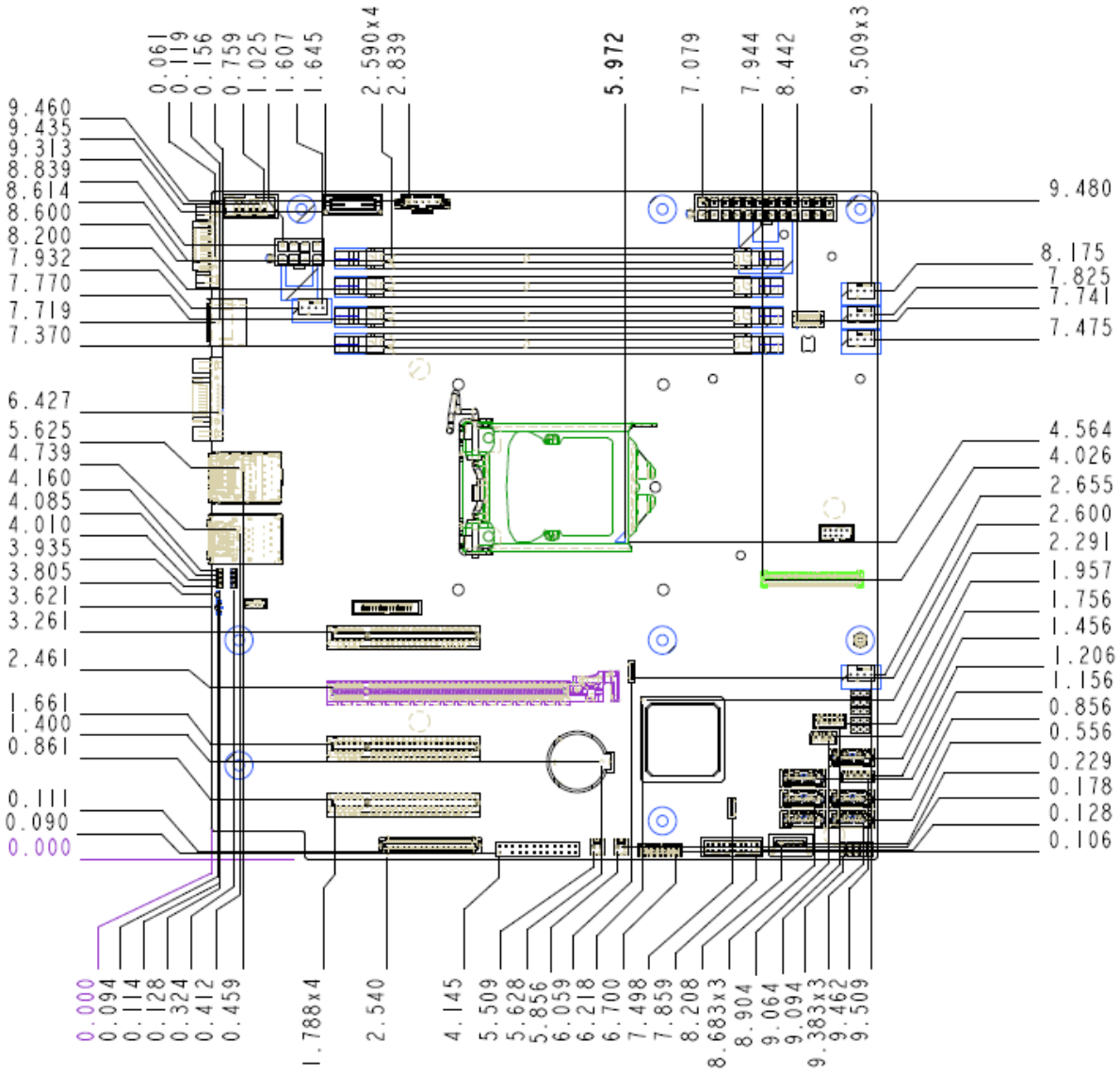


Figure 5. Intel® Server Board S1200V3RP – Major Connector Pin-1 Locations

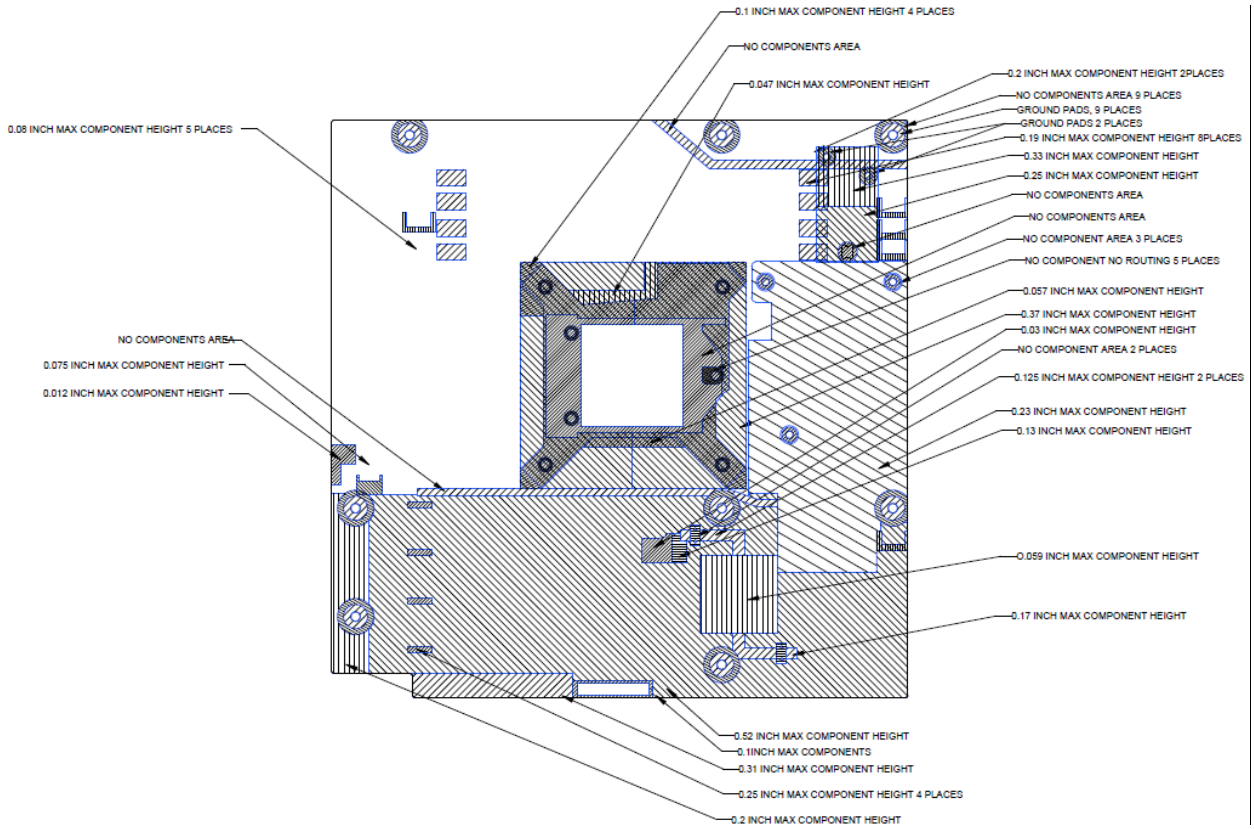


Figure 6. Intel® Server Board S1200V3RP – Primary Side Keepout Zone

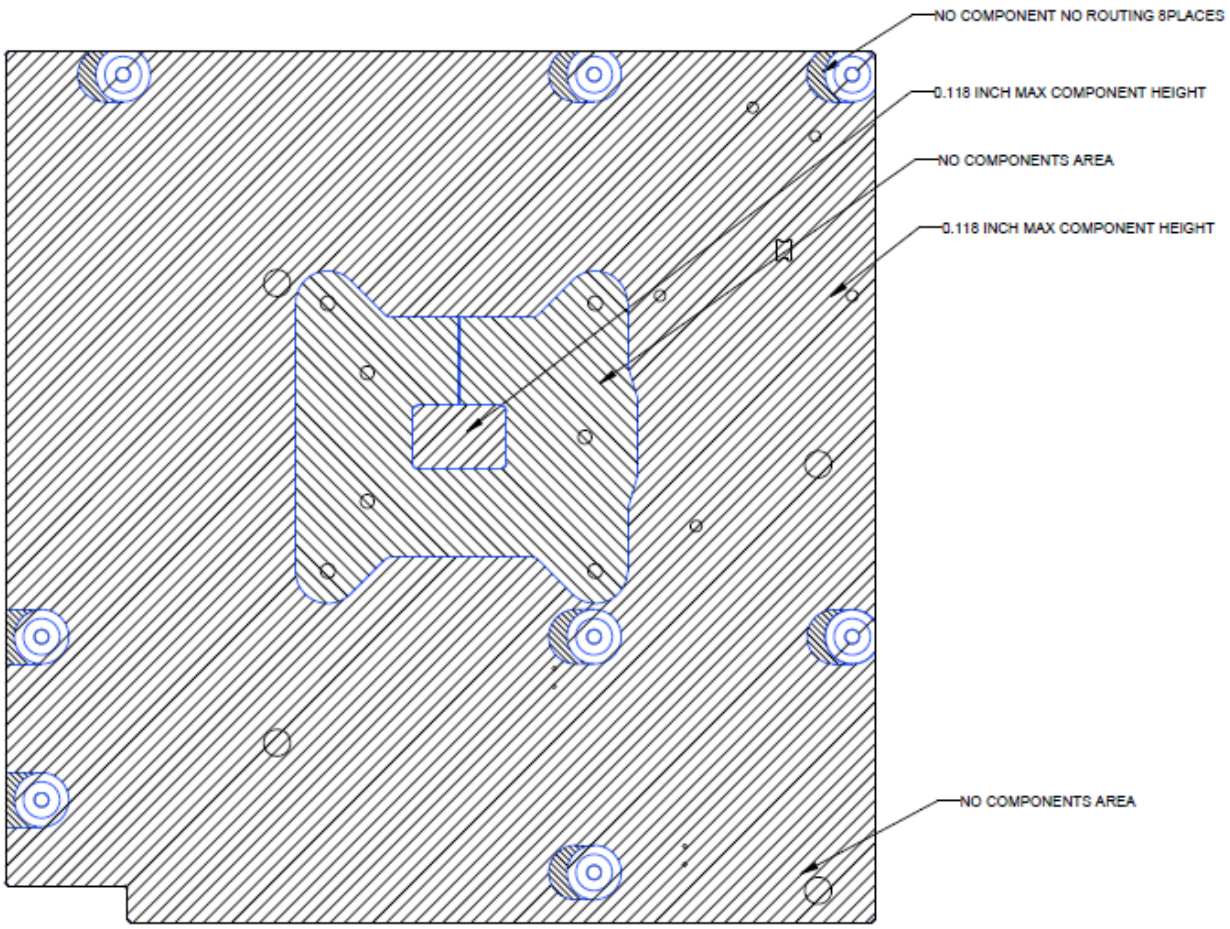


Figure 7. Intel® Server Board S1200V3RP – Second Side Keepout Zone

2.2.3 Server Board Rear I/O Layout

The following drawing shows the layout of the rear I/O components for the server board.

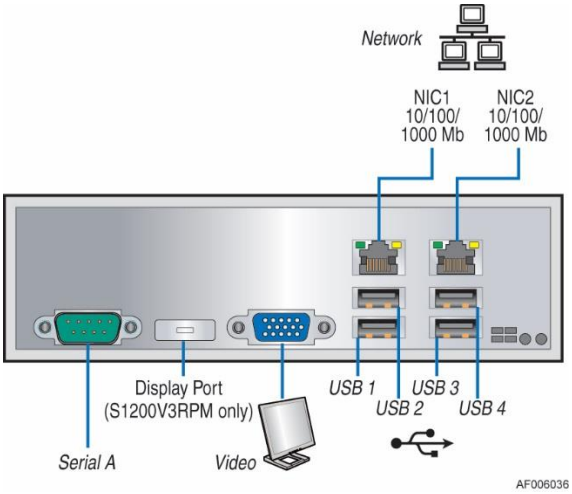


Figure 8. Intel® Server Board S1200V3RP Rear I/O Layout

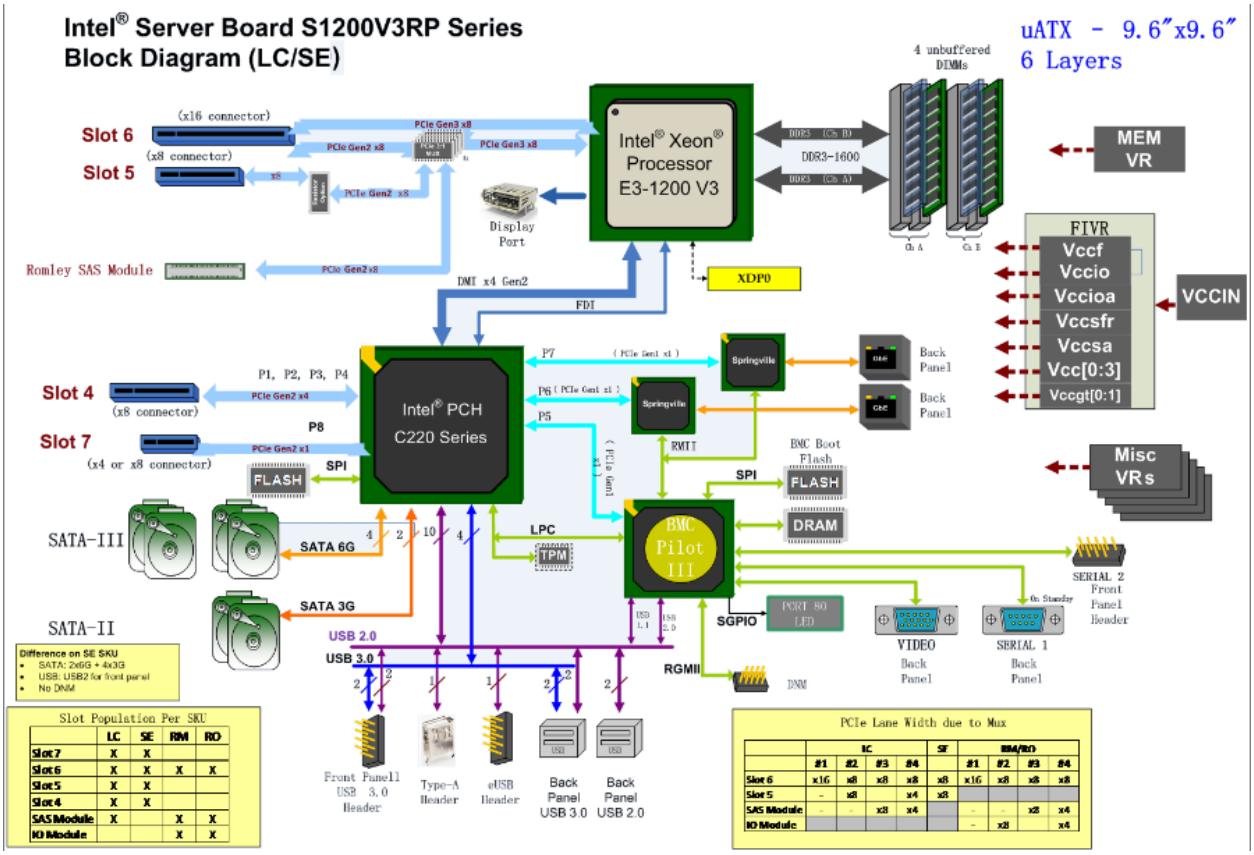
3. Functional Architecture

The architecture and design of the Intel® Server Board S1200V3RP is based on the Intel® C220 series chipset. The chipset is designed for systems based on the Intel® Xeon® processor in an LGA 1150 Socket H3 package.

The Intel® Server Board S1200V3RPO uses Intel® C224 chipset. The Intel® Server Board S1200V3RPS uses Intel® C222 chipset. The Intel® Server Board S1200V3RPL and S1200V3RPM use Intel® C226 chipset.

The Intel® Xeon® Processor E3-1200 V3 and Intel® Xeon® processor E3-1200 V4 Processors are made up of multi-core processors based on the 22nm processor technology. The 4th Intel® Core™ i3 Processors are made up of dual-core processors based on the 22nm processor technology.

This chapter provides a high-level description of the functionality associated with each chipset component and the architectural blocks that make up the server boards.



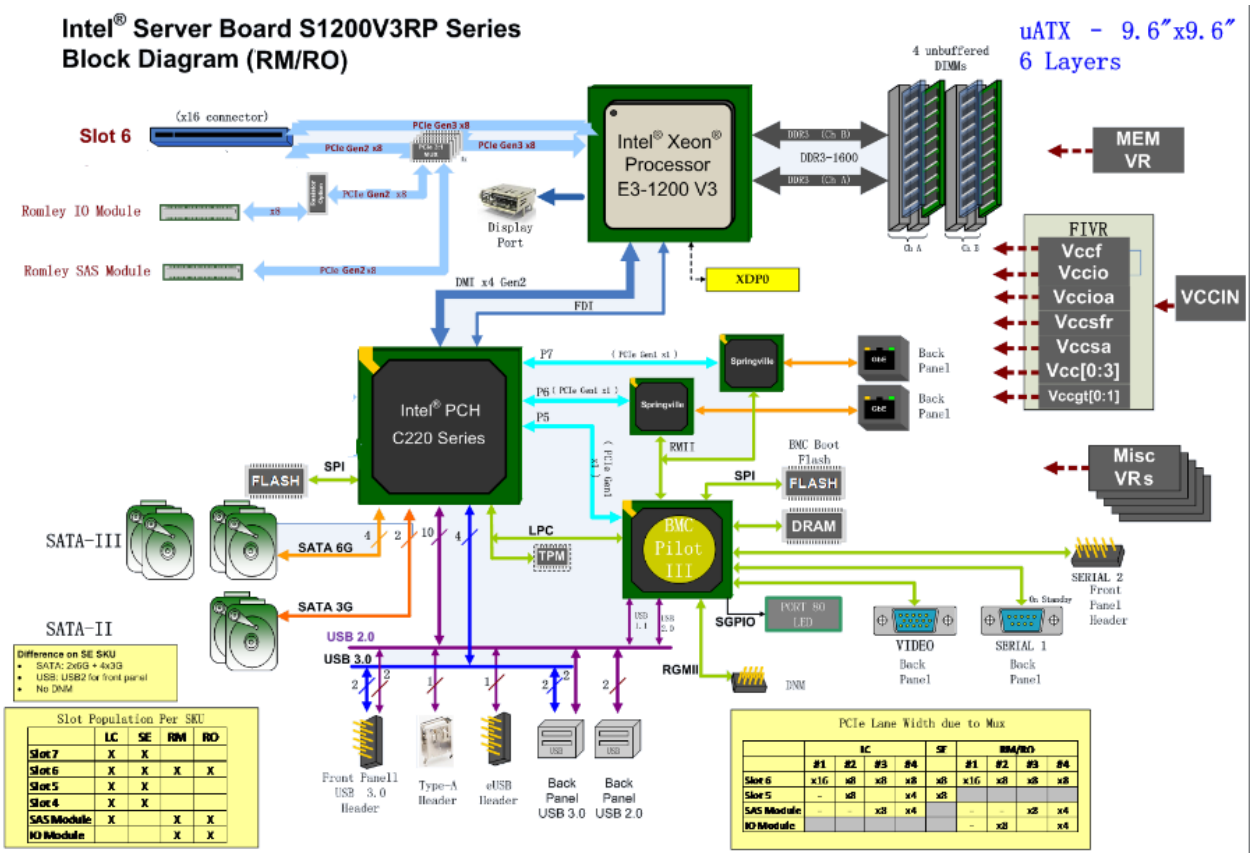


Figure 9. Intel® Server Board S1200V3RP Functional Block Diagram

3.1 Processor Subsystem

The Intel® Server Board S1200V3RP supports the following processor:

- Intel® Xeon® processor E3-1200 V3 product family
- Intel® Xeon® processor E3-1200 V4 product family (only support Intel® C226 Platform Controller Hub (PCH) chipset)
- The 4th Generation Intel® Core™ i3 processors

Note: The previous generation Intel® Xeon® processors are not supported on the Intel® server board described in this document.

3.1.1 Intel® Xeon® processor E3-1200 V3 product family

Intel® Xeon® processor E3-1200 v3 product family highly integrated solution variant is composed of quad processor cores:

- LGA 1150 socket package with 5 GT/s
- Up to 95 W Thermal Design Power (TDP)

The list of supported processors may be found at http://serverconfigurator.intel.com/sct_app.aspx.

3.1.2 Intel® Xeon® processor E3-1200 V4 product family

Intel® Xeon® processor E3-1200 v4 product family highly integrated solution variant is composed of quad processor cores:

- LGA 1150 socket package with 5 GT/s
- Up to 95 W Thermal Design Power (TDP)

The list of supported processors may be found at http://serverconfigurator.intel.com/sct_app.aspx.

Note: The workstation processor is not supported in this platform.

3.1.3 The 4th Generation Intel® Core™ i3 Processors

The 4th Generation Intel® Core™ i3 Processors highly integrated solution variant is composed of Duo cores:

- FC-LGA 1150 socket package with 5 GT/s
- Up to 65 W Thermal Design Power (TDP); processors with higher TDP are not supported

The list of supported processors may be found at http://serverconfigurator.intel.com/sct_app.aspx.

3.2 Processor Function Overview

With the release of the Intel® Xeon® processor E3-1200 V3/V4 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; up to 16 lanes of Gen 3 PCI Express* links. The FMA instruction has improved from 128 bit integer instruction to 256 bit integer, providing much better media processing performance.

The following sections 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 E3-1200 V3/V4 product family documents listed in the Reference Documents list.

Processor feature details:

- Up to four execution cores
- Each core supports two threads (Intel® Hyper-Threading Technology), up to 8 threads per socket

Supported technologies:

- Intel® Virtualization Technology (Intel® VT-x)
- Server Platform Services 3.0 (SPS3.0)
- Intel® Trusted Execution Technology (Intel® TXT)
- Intel® 64 Architecture

- Intel® Streaming SIMD Extensions 4.2 (Intel® SSE4.2)
- Intel® Advanced Vector Extensions 2.0 (Intel® AVX2)
- Advanced Encryption Standard New Instructions (AES-NI)
- Intel® Hyper-Threading Technology
- Execute Disable Bit
- Intel® Turbo Boost Technology
- PCLMULQDQ Instruction
- Intel® Transactional Synchronization Extensions (Intel® TSX)
- PAIR – Power Aware Interrupt Routing
- SMEP – Supervisor Mode Execution Protection

Note: The SR-IOV function is not supported because the hardware doesn't support ACS which is required to support SR-IOV.

3.3 Integrated Memory Controller (IMC) and Memory Subsystem

Integrated into the processor is a memory controller. Only ECC memory is supported on this platform. Each processor provides two DDR3L Unbuffered Dual In-Line Memory Modules (UDIMM) channels that support the following:

- ECC Unbuffered DDR3L
- Single-channel and dual-channel memory organization modes
- Data burst length of eight cycles for all memory organization modes
- Memory DDR3 data transfer rates of 1333, and 1600 MT/s
- 64-bit wide channels
- DDR3L I/O Voltage of 1.35 V
- Theoretical maximum memory bandwidth of:
  - 21.3 GB/s in dual-channel mode assuming 1333 MT/s
  - 25.6 GB/s in dual-channel mode assuming 1600 MT/s
- 1 Gb, 2 Gb, and 4 Gb DDR3L DRAM device technologies are supported
  - Using 4 Gb DRAM device technologies, the largest system memory capacity possible is 32 GB, assuming Dual Channel Mode with four x8 dual ranked DIMM memory configuration
- Up to 64 simultaneous open pages, 32 per channel (assuming 8 ranks of 8 bank devices)
- Processor on-die Vref generation for DDR DQ Read and Write as well as CMD/ADD
- Command launch modes of 1n/2n
- On-Die Termination (ODT)
- Asynchronous ODT
- Intel® Fast Memory Access (Intel® FMA):
  - Just-in-Time Command Scheduling
  - Command Overlap
  - Out-of-Order Scheduling
- The memory channels are named as *Channel A* and *Channel B*.

- The memory slots are named as *Slot1* and *Slot2* on each channel. Slot1 is the farthest from the processor socket.
- DIMMs are named to reflect the channel and slot in which they are installed:
  - Channel A, Slot1 is *DIMM_A1*.
  - Channel A, Slot2 is *DIMM_A2*.
  - Channel B, Slot1 is *DIMM_B1*.
  - Channel B, Slot2 is *DIMM_B2*.

3.3.1 Supported Memory

- Single Ranked x8 unbuffered ECC
- Dual Ranked x8 unbuffered ECC

Table 2. UDIMM Support Guidelines

Ranks Per DIMM and Data Width	Memory Capacity Per DIMM			Speed (MT/s) and Voltage Validated by Slot per Channel (SPC) and DIMM Per Channel (DPC)		
				1 Slot per Channel	2 Slots per Channel	
				1DPC	1DPC	2DPC
				1.35V	1.35V	1.35V
SRx8 ECC	1GB	2GB	4GB	1333, 1600	1333, 1600	1333, 1600
DRx8 ECC	2GB	4GB	8GB	1333, 1600	1333, 1600	1333, 1600

Notes:

1. No support for RDIMMs.
2. No support for SODIMM.
3. All channels in a system run at the fastest common frequency.
4. Mixing ECC and non-ECC UDIMMs anywhere on the platform is not supported.
5. Static CLTT supported using BMC (requires ECC DIMMs with thermal sensor).

3.3.1.1 Memory Population Rules

Note: Although mixed DIMM configurations are supported, Intel® only performs platform validation on systems that are configured with identical DIMMs installed.

The processor provides two channels of memory, each capable of supporting up to two DIMMs.

- DIMMs are organized into physical slots on DDR3L memory channels that belong to processor sockets.
- 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 on processor.
- Slot1 must be populated first before Slot2, on either channel.
- Channel A and Channel B are independent and are not required to have the same number of DIMMs installed. Either channel may be used for a single-DIMM configuration.

- When only one memory channel is populated, the memory runs in Single Channel mode, with no interleaving.

On the Intel® Server Board S1200V3RP, a total of 4 DIMM slots is provided. The nomenclature for DIMM sockets is detailed in the following table.

Table 3. Intel® Server Board S1200V3RP DIMM Nomenclature

(0) Channel A		(1) Channel B	
A1	A2	B1	B2

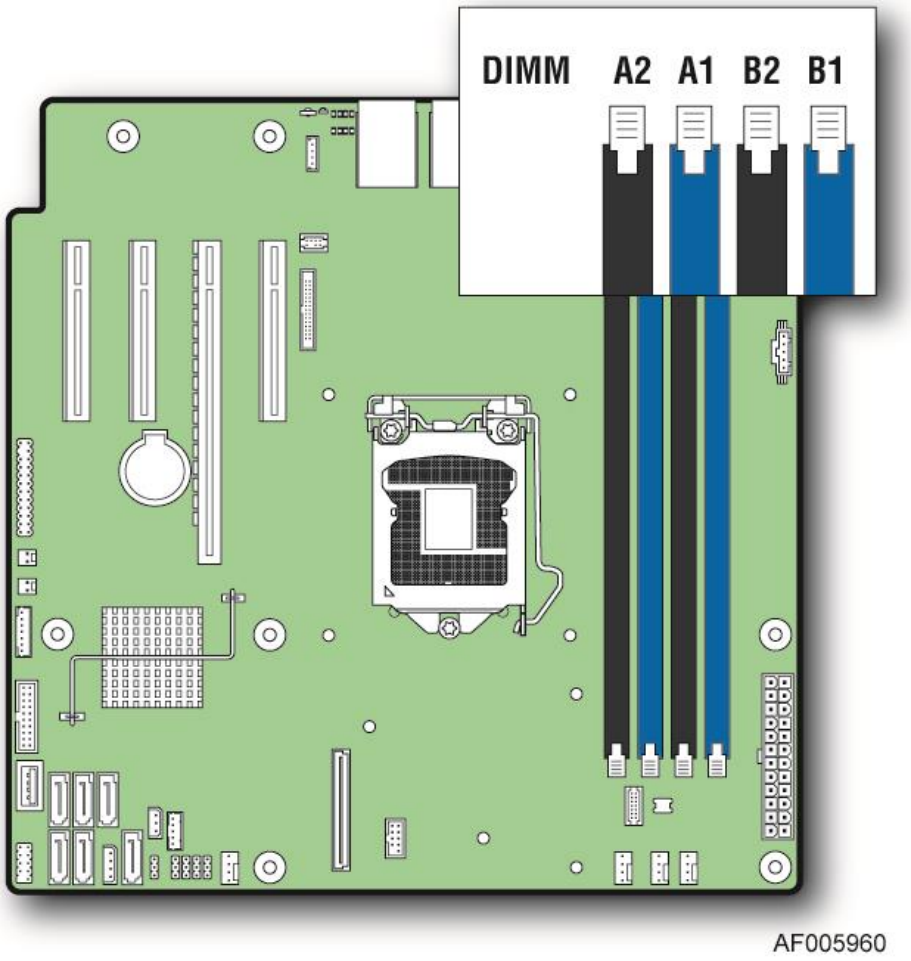


Figure 10. Intel® Server Board S1200V3RP DIMM Slot Layout

Table 4. Intel® Server Board S1200V3RP DIMM Maximum Configuration

Max Memory Possible	1Gb DRAM Technology	2Gb DRAM Technology	4Gb DRAM Technology
Single Rank UDIMM	4GB (4 x 1GB DIMMs)	8GB (4 x 2GB DIMMs)	16GB (4 x 4GB DIMMs)
Dual Rank UDIMMs	8GB (4 x 2GB DIMMs)	16GB (4x 4GB DIMMs)	32GB (4 x 8GB DIMMs)

3.3.1.2 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 DDR3 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 DDR3 DIMMs that are active (not disabled).
- 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.

Note: Some server operating systems do not display the total physical memory installed. What is displayed is the amount of physical memory minus the approximate memory space used by system BIOS components. These BIOS components include, but are not limited to:

1. *ACPI (may vary depending on the number of PCI devices detected in the system)*
2. *ACPI NVS table*
3. *Processor microcode*
4. *Memory Mapped I/O (MMIO)*
5. *Manageability Engine (ME)*
6. *BIOS flash*

3.3.2 Memory RAS Features

For Intel® Server Board S1200V3RP product family, the form of Memory RAS provided is Error Correction Code (ECC). ECC uses extra bits – 64-bit data in a 72-bit DRAM array – to add an 8-bit calculated Hamming Code to each 64 bits of data. This additional encoding enables the memory controller to detect and report single or double bit errors, and to correct single-bit errors.

There is a specific step in memory initialization in which all of memory is cleared to zeroes before the ECC function is enabled, in order to bring the ECC codes into agreement with memory contents.

During operation, in the process of every fetch from memory, the data and ECC bits are examined for each 64-bit data plus 8-bit ECC group. If the ECC computation indicates that a single bit Correctable Error has occurred, it is corrected and the corrected data is passed on to the processor. If a double-bit Uncorrectable Error is detected, it cannot be corrected. In each case, a Correctable or Uncorrectable ECC Error event is generated.

For Correctable Errors, there is a certain tolerance observed, since a Correctable Error can be generated by something as random as a stray Cosmic Ray impacting the DIMM. Correctable Errors are counted on a per-DIMM basis, but are just silently recorded until the tolerance threshold is crossed. The Correctable Error Threshold for Intel® Server Board S1200V3RP

product family board is set at 10 events. When the 10th CE occurs, a single Correctable Error event is logged.

3.3.3 Post Error Codes

The range {0xE0 - 0xEF} of POST codes is used for memory errors in early POST. In late POST, this same range of POST code values is used for reporting other system errors.

- **0xE8 - No Usable Memory Error**: If no usable memory is available, the BIOS emits a beep code and displays POST Diagnostic LED code 0xE8 and halts the system.

  This can also occur if all memory in the system fails and/or has become disabled during memory initialization. For example, if a DDR3 DIMM has no SPD information, the BIOS treats the DIMM slot as if no DDR3 DIMM is present on it. Therefore, if this is the only DDR3 DIMM installed in the system, there is no usable memory, and the BIOS goes to a memory error code 0xE8 as described above.
- **0x53/0x55/0XE8**: DIMM SPD does not respond or DIMM SPD Read Error, the DIMM will not be detected, if the SPD does not respond, which could result in No memory Installed or No Usable Memory Error Halt 0X53, 0x55, or 0xE8, or could result later in an invalid configuration if the no SPD DIMM is in Slot 1 on the channel.
- **0x51 – Memory SPD Error**: If the DIMM does respond but the SPD cannot be successfully read, that would cause a Memory SPD Error, memory error halt 0X51. For each memory channel, once the DIMM SPD parameters have been read, they are checked to verify that the DIMMs on the channel are a valid configuration, DIMM speed and size, ECC capability, and in which memory slot the DIMMs are installed. An invalid configuration will cause the system to halt.
- **0xEA - Channel Training Error**: If the memory initialization process is unable to properly perform the Data/Data Strobe timing training on a memory channel, the BIOS emits a beep code and displays POST Diagnostic LED code 0xEA momentarily during the beeping. If there is usable memory in the system on other channels, POST memory initialization continues. Otherwise, the system beeps and halts with POST Diagnostic LED code 0xEA staying displayed.
- **0x54/0xEB - Memory Test Erro**r: If a DDR3 DIMM or a set of DDR3 DIMMs on the same memory channel fails memory testing but usable memory remains available, the BIOS emits a beep code and displays POST Diagnostic LED code 0xEB momentarily during the beeping, then continues POST. If all of the memory fails memory testing, then system memory error code 0xE8 (No Usable Memory) as described above.
- **0xED - Population Error or Invalid DIMM**: If the installed memory contains an invalid DIMM configuration on any channel in the system, the system beeps and halts with POST Diagnostic LED code 0xED. The DIMM are installed incorrectly, not following the *Fill Farthest First* rule (Slot 1 must be filled before Slot 2). This will result in a DIMM Population Error, with a Memory Error Halt 0xED.

3.3.4 Processor Integrated I/O Module (IIO)

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 16 lanes of PCI Express*. Following are key attributes of the PCI Express* interface:

- Gen3 speeds at 8 GT/s (no 8b/10b encoding)
- Can operate at 2.5 GT/s, 5 GT/s, or 8 GT/s

The Intel® Server Board S1200V3RPL and S1200V3RPS support PCIe slots:

- Slot 7: PCI Express* Gen2 x1 electrical with x8 physical connector, from PCH.
- Slot 6: PCI Express* Gen2 x 16 or Gen3 x8 electrical with x16 physical connector, from processor.
- Slot 5: PCI Express* Gen2 x8 or x4 electrical with x8 physical connector, from processor.
- Slot 4: PCI Express* Gen2 x4 electrical with x8 physical connector, from PCH.

The Intel® Server Board S1200V3RPO and S1200V3RPM support PCIe slots:

- Slot 6: PCI Express* Gen3 x16 electrical with x16 physical connector, from processor.

Table 5. PCI Express* Speed Matrix for Each Configuration

<table>
<tr><td>Board Name</td><td colspan="5">PCI Express* Slot</td></tr>
<tr><td rowspan="2">S1200V3RPS</td><td>Slot4</td><td>Slot7</td><td colspan="2">Slot5</td><td>Slot6</td></tr>
<tr><td>PCI Express* Gen2 x4</td><td>PCI Express* Gen2 x1</td><td colspan="2">PCI Express* Gen2 x8</td><td>PCI Express* Gen3 x8</td></tr>
<tr><td rowspan="5">S1200V3RPL</td><td>Slot4</td><td>Slot7</td><td>Slot5</td><td>Slot6</td><td>SAS Module</td></tr>
<tr><td rowspan="4">PCI Express* Gen2 x4</td><td rowspan="4">PCI Express* Gen2 x1</td><td rowspan="2">No card installed</td><td>PCI Express* Gen3 x8 or Gen2 x16</td><td>No Card installed</td></tr>
<tr><td>PCI Express* Gen3 x8</td><td>PCI Express* Gen2 x8</td></tr>
<tr><td>PCI Express* Gen2 x8</td><td>PCI Express* Gen3 x8</td><td>No Card installed</td></tr>
<tr><td>PCI Express* Gen2 x4</td><td>Gen3 x8</td><td>PCI Express* Gen2 x4</td></tr>
<tr><td rowspan="4">S1200V3RPO
S1200V3RPM</td><td>Slot6</td><td colspan="2">IO Module</td><td colspan="2">SAS module</td></tr>
<tr><td>PCI Express* Gen2 x16 or Gen3 x8</td><td colspan="2">Don’t have add-in module</td><td colspan="2">Don’t have add-in module</td></tr>
<tr><td rowspan="3">PCI Express* Gen3 x8 or don’t have add-in card</td><td colspan="2">PCI Express* Gen2 x8</td><td colspan="2">Don’t have add-in module</td></tr>
<tr><td colspan="2">Don’t have add-in module</td><td colspan="2">PCI Express* Gen2 x8</td></tr>
<tr><td colspan="2">PCI Express* Gen2 x4</td><td colspan="2">PCI Express* Gen2 x4</td></tr>
</table>

Note: If no device is installed on IO Module connector or Slot5, the device connecting to Intel® SAS module connector can work as PCI Express Gen2 x4 electrical; if any device is installed on IO Module connector or Slot5, the Intel® SAS modules (RMS25JB080 and RMS25JB040) can work as PCI Express* Gen2 x4 electrical and the Intel® ROC modules (RMS25CB080 and RMS25CB040) cannot be detected.*

- **Direct Media Interface (DMI)**

  Direct Media Interface (DMI) connects the processor and the PCH. DMI2.0 is supported.

  Note: Only DMI x4 configuration is supported.

  - DMI 2.0 support.
  - Compliant to Direct Media Interface Second Generation (DMI2).
  - Four lanes in each direction.
  - 5 GT/s point-to-point DMI interface to PCH is supported.

3.3.5 Intel® Integrated RAID Option

The Intel® Server Board S1200V3RPL, S1200V3RPO, and S1200V3RPM provide a SAS/ROC Mezzanine slot (J4J1) to a high density 80-pin connector labeled *SAS_MOD* for the installation of an optional Intel® Integrated RAID Module. For more information, please refer to Table 5.

Features of this option include:

- SKU options to support full or entry level hardware RAID
- Dual-core 6Gb SAS ROC/IOC (LSI* 2208)
- 4 or 8 port and SAS/SATA or SATA – only ROC options
- SKU options to support 512MB or 1GB embedded memory
- Intel® designed flash plus optional support for Intel® RAID Maintenance Free Backup Units (AXXRMFBU2) or improved Lithium Polymer battery

Table 6. Supported Intel® Integrated RAID Modules

External Name	Description	Product Code
Intel® Integrated RAID Module RMS25CB080	8 Port SAS-2.1, Full HW RAID, 1GB, IOM Slot RAID Levels 0,1,10, 5, 50, 6, 60	RMS25CB080
Intel® Integrated RAID Module RMS25CB040	4 Port SAS-2.1, Full HW RAID, 1GB, IOM Slot RAID Levels 0,1,10, 5, 50, 6, 60	RMS25CB040
Intel® Integrated RAID Module RMT3CB080	8 Port SATA-3, Full HW RAID, 512MB, IOM Slot RAID Levels 0,1,10, 5, 50, 6, 60	RMT3CB080
Intel® Integrated RAID Module RMS25KB080	8 Port SAS-2.1, Entry-level HW RAID, IOM Slot RAID Levels 0,1,1E	RMS25KB080
Intel® Integrated RAID Module RMS25KB040	4 Port SAS-2.1, Entry-level HW RAID, IOM Slot RAID Levels 0,1,1E	RMS25KB040

For additional product information, refer to the document *Intel® Integrated RAID Module RMS25KB080, RMS25KB040, RMS25CB080, and RMS25CB040 Hardware User's Guide*.

3.3.6 Optional I/O Module Support

To broaden the standard on-board feature set, the Intel® Server Board S1200V3RPO and S1200V3RPM provide support for one of several available IO Module options. The I/O module

attaches to a high density 80-pin connector on the server board (J1C1) labeled *I/O_MOD* and is supported by up to x8 PCIe Gen3 signals from the IIO module of the processor.

3.3.7 Intel® I/O Acceleration Technolgy 2 (Intel® I/O AT2)

Intel® I/O AT2 is not supported.

3.3.7.1 Direct Cache Access (DCA)

Direct Cache Access (DCA) is not supported on Intel® Xeon® Processor E3-1200 V3/V4 series.

3.4 Intel® C220 series Chipset PCH Functional Overview

The following subsections provide an overview of the key features and functions of the Intel® C220 series chipset PCH used on the server board. For more comprehensive chipset specific information, refer to the Intel® C220 series chipset documents listed in the Reference Document list.

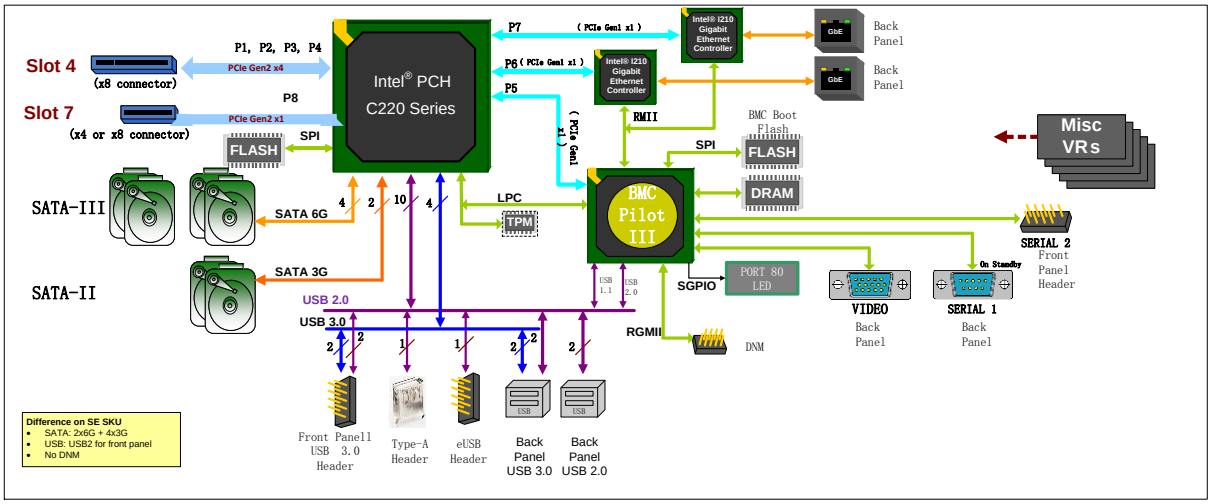


Figure 11. Functional Block Diagram – Chipset Supported Features and Functions

On the Intel® Server Boards S1200V3RP, the chipset provides support for the following on-board functions:

- Digital Media Interface (DMI) to Processor
- PCI Express* Interface
- Serial ATA (SATA) Controller
- AHCI
- Rapid Storage Technology enterprise (RSTe)
- Low Pin Count (LPC) interface
- Serial Peripheral Interface (SPI)
- Compatibility Modules (DMA Controller, Timer/Counters, Interrupt Controller)
- Advanced Programmable Interrupt Controller (APIC)
- Universal Serial Bus (USB) Controller

- Gigabit Ethernet Controller
- RTC
- GPIO
- Enhanced Power Management
- Manageability
- System Management Bus (SMBus* 2.0)
- Integrated NVSRAM controller
- Virtualization Technology for Direct I/O (Intel® VT-d)
- JTAG Boundary-Scan
- KVM/Serial Over LAN (SOL) Function

3.4.1 Digital Media Interface (DMI)

Digital Media Interface (DMI) is the chip-to-chip connection between the processor and the Intel® C220 series chipset. 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.

3.4.2 PCI Express* Interface

The Intel® C220 series chipset 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). On the Intel® Server Board S1200V3RPL and S1200V3RPS, PCI Express* Root Ports 1-4 is configured to support one Gen2 x4 port widths of slot 4; PCI Express* Root Port 8 is configured to support one Gen2 x1 port widths of slot 7. On the Intel® Server Boards S1200V3RP family product, PCI Express* Root Port 5 is configured to support one Gen1 x1 widths connection with the BMC chip; PCI Express* Root Port 5 and 6 are configured to support two Gen1 x1 widths connection with the two Intel® I210 Gigabit Ethernet Network controller.

3.4.3 Serial ATA (SATA) Controller

The Intel® C220 series chipset provides SATA host controllers that support independent DMA operation on up to six ports and supports data transfer rates of up to 6.0 Gb/s (600 MB/s) on up to six ports while all ports support rates up to 3.0 Gb/s. The SATA controller contains two modes of operation – a legacy mode using I/O space, and an AHCI mode using memory space. Software that uses legacy mode will not have AHCI capabilities. The Intel® C220 series chipset supports the Serial ATA Specification, Revision 3.0. The Intel® C220 series also supports 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).

Table 7. Intel® Server Board S1200V3RP SATA Data Transfer Rate

SKU Name	SATA Port 0, 1	SATA Port 2, 3	SATA Port 4, 5
S1200V3RPO	Up to 6.0 Gb/s	Up to 6.0 Gb/s	Up to 3.0 Gb/s
S1200V3RPS	Up to 6.0 Gb/s	Up to 3.0 Gb/s	Up to 3.0 Gb/s
S1200V3RPL S1200V3RPM	Up to 6.0 Gb/s	Up to 6.0 Gb/s	Up to 6.0 Gb/s

3.4.3.1 AHCI

The Intel® C220 series chipset provides hardware support for Advanced Host Controller Interface (AHCI), a standardized programming interface for SATA host controllers. Platforms supporting AHCI may take advantage of performance features such as no master/slave designation for SATA devices—each device is treated as a master—and hardware assisted native command queuing. AHCI also provides usability enhancements such as Hot-Plug. AHCI requires appropriate software support (for example, an AHCI driver) and for some features, hardware support in the SATA device or additional platform hardware.

The server board includes support for two embedded software RAID options:

- Intel® Embedded Server RAID Technology 2 (ESRT2) based on LSI* MegaRAID SW RAID technology
- Intel® Rapid Storage Technology (RSTe)

Using the <F2> BIOS Setup Utility, accessed during system POST, options are available to enable/disable SW RAID, and select which embedded software RAID option to use.

3.4.3.2 Intel® Rapid Storage Technology enterprise

The Intel® C220 series chipset provides support for Intel® Rapid Storage Technology enterprise, providing both AHCI (see above for details on AHCI) and integrated RAID functionality. The industry-leading RAID capability provides high-performance RAID 0, 1, 5, and 10 functionality on up to 6 SATA ports of the Intel® C220 series chipset. RSTe RAID support is provided to allow multiple RAID levels to be combined on a single set of hard drives, such as RAID 0 and RAID 1 on two disks. Other RAID features include hot-spare support, SMART alerting, and RAID 0 auto replace. Software components include an Option ROM for pre-boot configuration and boot functionality, a Microsoft Windows* compatible driver, and a user interface for configuration and management of the RAID capability of the Intel® C220 series chipset.

3.4.3.3 Intel® Embedded Server RAID Technology 2 (ESRT2)

Features of the embedded software RAID option Intel® Embedded Server RAID Technology 2 (ESRT2) include the following:

- Based on LSI* MegaRAID Software Stack
- Software RAID with system providing memory and CPU utilization
- Supported RAID Levels – 0, 1, 10, RAID 5 support provides with upgrade key of RKSATA4R5.
- Open Source Compliance = Binary Driver (includes Partial Source files) or Open Source using MDRAID layer in Linux*
- OS Support = Microsoft Windows 2012*, Microsoft Windows 2008*, RHEL*, SLES, and other Linux* variants using partial source builds
- Utilities = Microsoft Windows* GUI and CLI, Linux* GUI and CLI, DOS CLI, and EFI CLI

3.4.4 Low Pin Count (LPC) Interface

The Intel® C220 series chipset implements an LPC Interface as described in the *LPC 1.1 Specification* and provides support for up to two Master/DMI devices. On the server board, the LPC interface is utilized as an interconnection between the chipset and the Integrated Base

Board Management Controller as well as providing support for the optional Trusted Platform Module (TPM).

3.4.5 Serial Peripheral Interface (SPI)

The Intel® C220 series chipset implements an SPI Interface as an alternative interface for the BIOS flash device.

3.4.6 Universal Serial Bus (USB) Controller

The Intel® C220 series chipset has up to two Enhanced Host Controller Interface (EHCI) host controllers that support USB high-speed signaling. High-speed USB 2.0 allows data transfers up to 480 Mb/s which is 40 times faster than full-speed USB.

The Intel® C220 series chipset contains an eXtensible Host Controller Interface (xHCI) host controller which supports up to fourteen USB 2.0 ports of which up to six can be used as USB3.0 ports with board routing, ACPI table, and BIOS considerations. This controller allows data transfers of up to 5Gb/s. The controller supports SuperSpeed (SS), high-speed (HS), full-speed (FS), and low speed (LS) traffic on the bus.

Table 8. Intel® Server Board S1200V3RP series USB Ports Allocation

Board SKU	Rear USB Ports		Internal USB Headers			
	USB 1, 2 (USB2.0)	USB 3, 4 (USB3.0)	J1J1 (USB 5, 6) (USB3.0)	J1J4 (USB 7) (USB2.0 Type A)	J1K3 (USB 8,9) (USB2.0)	J5K1 eUSB (USB2.0)
S1200V3RPL S1200V3RPO S1200V3RPM	Yes	Yes	Yes	Yes	Yes	Yes
S1200V3RPS	Yes	Yes	No	Yes	Yes	Yes

3.4.6.1 Native USB Support

During the power-on self-test (POST), the BIOS initializes and configures the USB subsystem. The BIOS can initialize and use the following types of USB devices:

- USB Specification-compliant keyboards
- USB Specification-compliant mouse
- USB Specification-compliant storage devices that utilize bulk-only transport mechanism

USB devices are scanned to determine if they are required for booting.

The BIOS supports USB 2.0 mode of operation, and as such supports USB 1.1 and USB 2.0 compliant devices and host controllers.

During the pre-boot phase, the BIOS automatically supports the hot addition and hot removal of USB devices and a short beep is emitted to indicate such an action. For example, if a USB device is hot plugged, the BIOS detects the device insertion, initializes the device, and makes it available to the user. During POST, when the USB controller is initialized, it emits a short beep for each USB device in the system as if they were all just “hot added”.

Only on-board USB controllers are initialized by BIOS. This does not prevent the operating system from supporting any available USB controllers including add-in cards.

3.4.6.2 Legacy USB Support

The BIOS supports PS/2 emulation of USB keyboards and mouse. During POST, the BIOS initializes and configures the root hub ports and searches for a keyboard and/or a mouse on the USB hub and then enables the devices that are recognized.

3.4.6.3 eUSB SSD Support

The server board provides support for a low profile eUSB SSD storage device. A 2mm 2x5-pin connector labeled *eUSB SSD* near the rear I/O section of the server board is used to plug this small flash storage device into.

eUSB SSD features include:

- Two wire small form factor Universal Serial Bus 2.0 (Hi-Speed USB) interface to host
- Read Speed up to 35 MB/s and write Speed up to 24 MB/s
- Capacity range from 256 MB to 32 GB
- Support USB Mass Storage Class requirements for Boot capability

3.4.7 Gigabit Ethernet Controller

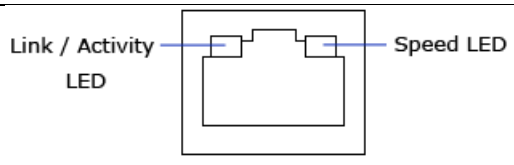
Network connectivity is provided by means of two onboard Intel® Ethernet Controller I210 providing up to two 10/100/1000 Mb Ethernet ports. The Intel® Ethernet Controller I210 is single, compact, low-power components that offer a fully-integrated Gigabit Ethernet Media Access Control (MAC) and Physical Layer (PHY) port. The Intel® Ethernet Controller I210 uses the PCI Express* architecture from the Intel® C220 series PCH and provides a single-port implementation in a relatively small area so it can be used for server and client configurations as a LAN on Motherboard (LOM) design.

External interfaces provided on the I210:

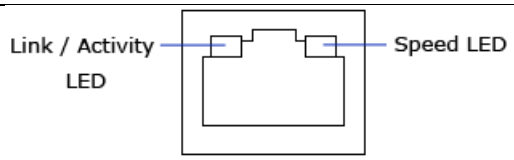
- PCIe Rev. 2.0 (2.5 GHz) x1
- MDI (Copper) standard IEEE 802.3 Ethernet interface for 1000BASE-T, 100BASETX, and 10BASE-T applications (802.3, 802.3u, and 802.3ab)
- NC-SI or SMBus* connection to a Manageability Controller (MC)
- EEE 1149.1 JTAG (note that BSDL testing is NOT supported)

Each Ethernet port drives two LEDs located on each network interface connector. The LED at the right of the connector is the link/activity LED and indicates network connection when on, and transmit/receive activity when blinking. The LED at the left of the connector indicates link speed as defined in the following table.

Table 9. External RJ45 NIC Port LED Definition



LED Color	LED State	NIC State
Green/Amber (Right)	Off	10 Mbps



LED Color	LED State	NIC State
	Amber	100 Mbps
	Green	1000 Mbps
Green (Left)	On	Active Connection
	Blinking	Transmit/Receive activity

3.4.7.1 MAC Address Definition

Each Intel® Server Board S1200V3RPL, S1200RPO, or S1200RPM has the following MAC addresses assigned to it at the factory:

- NIC 1 MAC address (for OS usage)
- NIC 2 MAC address – Assigned the NIC 1 MAC address +1 (for OS usage)
- Integrated BMC LAN Channel MAC address – Assigned the NIC 1 MAC address +2
- Intel® Remote Management Module 4 dedicated NIC MAC address – Assigned the NIC 1 MAC address +3

Each Intel® Server Board S1200V3RPS has the following MAC addresses assigned to it at the factory:

- NIC 1 MAC address
- NIC 2 MAC address – Assigned the NIC 1 MAC address +1
- Integrated BMC LAN Channel MAC address – Assigned the NIC 1 MAC address +2

3.4.8 Enhanced Power Management

The Intel® C220 series chipset's power management functions include enhanced clock control and various low-power (suspend) states (for example, Suspend-to-RAM and Suspend-to-Disk). A hardware-based thermal management circuit permits software-independent entrance to low-power states. The Intel® C220 series chipset contains full support for the *Advanced Configuration and Power Interface (ACPI) Specification, Revision 4.0a*.

3.4.9 Serial Ports

The server board provides two serial ports: an external DB9 serial port connector and an internal DH-10 serial header.

The rear DB9 Serial A port is a fully functional serial port that can support any standard serial device.

The Serial B port is an optional port accessed through a nine-pin internal DH-10 header (J9A2). You can use a standard DH-10 to DB9 cable to direct serial A port to the rear of a chassis.

3.4.10 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.

3.4.11 System Management Bus (SMBus* 2.0)

The Intel® C220 series chipset contains a SMBus* Host interface that allows the processor to communicate with SMBus* slaves. This interface is compatible with most I2C devices. Special I2C commands are implemented. The Intel® C220 series chipset's SMBus* host controller provides a mechanism for the processor to initiate communications with SMBus* peripherals (slaves). Also, the Intel® C220 series chipset 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® C220 series chipset'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.

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

The Intel® C220 series chipset provides hardware support for implementation of Intel® Virtualization Technology with Directed I/O (Intel® VT-d). Intel® VT-d Technology consists of technology components that support the virtualization of platforms based on Intel® Architecture Processors. Intel® VT-d Technology enables multiple operating systems and applications to run in independent partitions. A partition behaves like a Virtual Machine (VM) and provides isolation and protection across partitions. Each partition is allocated its own subset of host physical memory.

3.5 Integrated Baseboard Management Controller (BMC) Overview

The server board utilizes the I/O controller, Graphics Controller, and Baseboard Management features of the Emulex* Pilot-III Management Controller. The following is an overview of the features as implemented on the server board from each embedded controller.

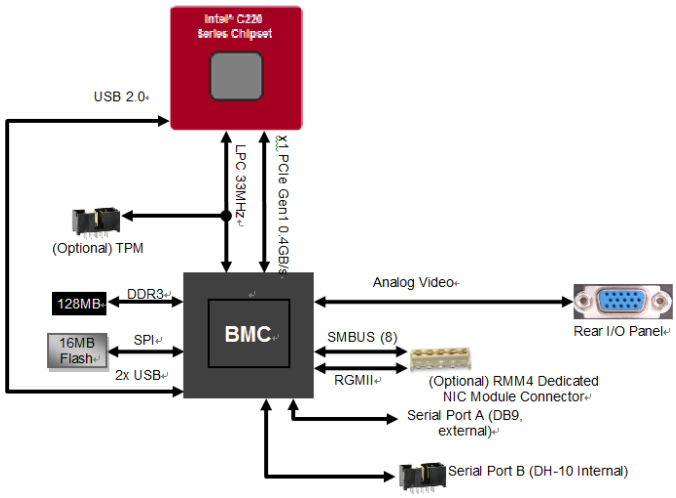


Figure 12. Integrated Baseboard Management Controller (BMC) Overview

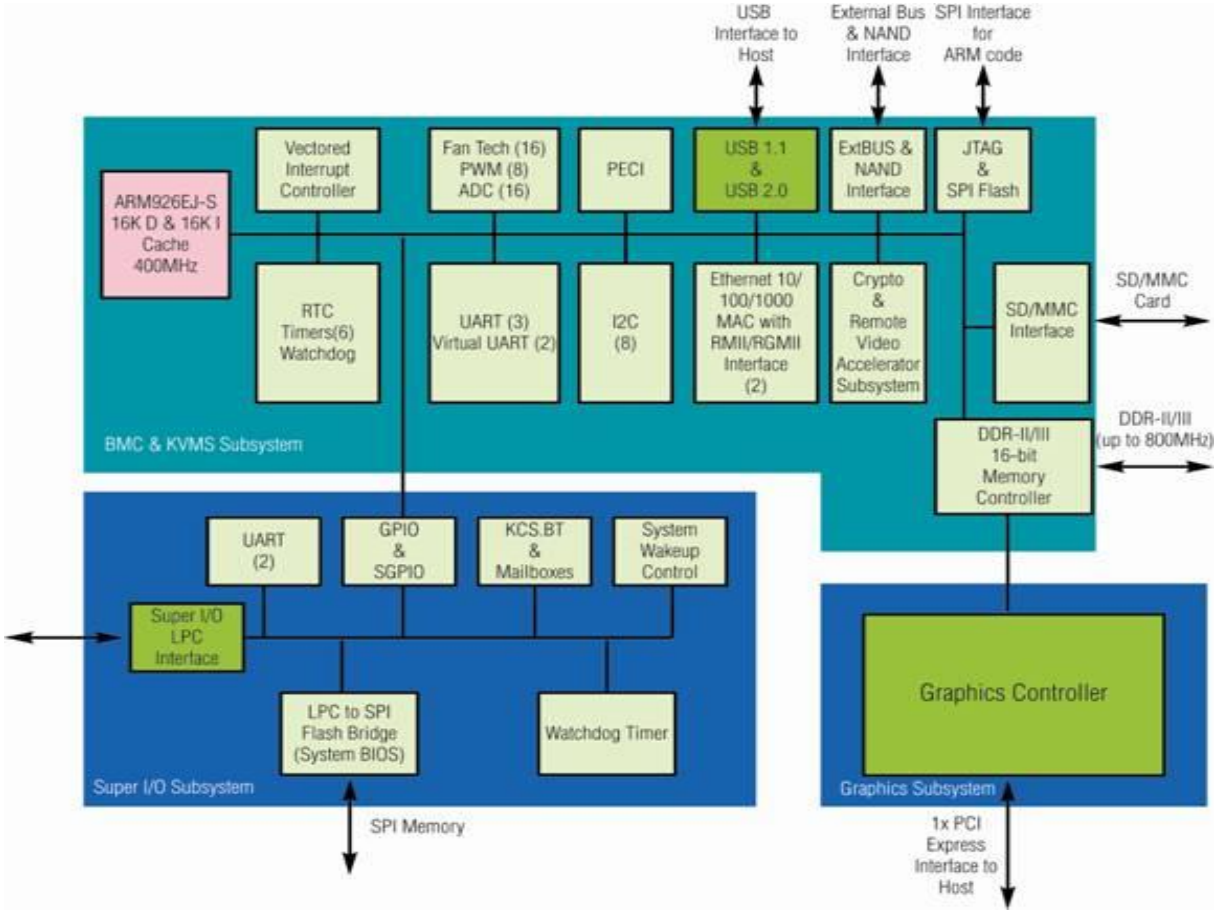


Figure 13. Integrated BMC Functional Block Diagram

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:

- Two Fully Functional Serial Ports, compatible with the 16C550
- Serial IRQ Support
- Up to 16 Shared direct GPIO's
- Serial GPIO support for 80 general purpose inputs and 80 general purpose outputs available for host processor
- Programmable Wake-up Event Support
- Plug and Play Register Set
- Power Supply Control
- Host SPI bridge for system BIOS support

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 keyboard 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-3 memory interface supporting up to 128MB of memory, 16MB allocated to graphic
- Supports display resolutions up to 1600 x 1200 16bpp @ 60Hz
- High speed Integrated 24-bit RAMDAC
- Single lane PCI Express* host interface running at Gen 1 speed

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

Table 10. Video Modes

2D Mode	2D Video Mode Support			
	8 bpp	16 bpp	24 bpp	32 bpp
640x480	X	X	X	X
800x600	X	X	X	X
1024x768	X	X	X	X
1152x864	X	X	X	X
1280x1024	X	X	X	X
1600x1200**	X	X		

** Video resolutions at 1600x1200 and higher are only supported through the external video connector located on the rear I/O section of the server 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 11. Video Mode

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

On Intel® Server Board S1200V3RPM, the display port is from the processor. The processor graphics contains a generation 7.5 graphics core architecture. This enables substantial gains in performance and lower power consumption over previous generations. Up to 20 EUs are supported depending on the processor SKU.

- Next Generation Intel® Clear Video Technology HD Support is a collection of video playback and enhancement features that improve the end user's viewing experience
  - Encode/transcode HD content
  - Playback of high definition content including Blu-ray Disc*
  - Superior image quality with sharper, more colorful images
  - Playback of Blu-ray* disc S3D content using HDMI (1.4a specification compliant with 3D)
- DirectX* Video Acceleration (DXVA) support for accelerating video processing
  - Full AVC/VC1/MPEG2 HW Decode
- Advanced Scheduler 2.0, 1.0, XPDM support

With display port, the maximum display resolution is 3840x2160@60Hz, 24bpp.

The supporting Operation System for display port Video output is Microsoft Windows 7*; other OS is not supported.

To use pGFX and BMC graphic as mixed (also known as: heterogeneous) graphic solution:

- Both BMC and Internal graphic need to be enabled/active in BIOS setup
- Select Internal graphic as primary display

Note: Internal graphic will not support local display unless it is set as primary display.

- Load add-in graphic driver for BMC and pGFX

For more information of pGFX on RBP RM SKU, refer to *3-Display Architecture and Configuration Overview (Supporting: 3rd Generation Intel® Core™ Processors and4th Generation Intel® Core™ Processors)*.

3.5.3 Baseboard Management Controller

The server board utilizes the following features of the embedded baseboard management controller:

- IPMI 2.0 Compliant
- 400MHz 32-bit ARM9 processor with memory management unit (MMU)
- Two independent10/100/1000 Ethernet Controllers with RMII/RGMII support
- DDR2/3 16-bit interface with up to 800 MHz operation
- 12 10-bit ADCs
- Fourteen fan tachometers
- Eight Pulse Width Modulators (PWM)
- Chassis intrusion logic
- JTAG Master
- Eight I2C 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.

3.5.3.1 Remote Keyboard, Video, Mouse, and Storage (KVMS) Support

- USB 2.0 interface for Keyboard, Mouse, and Remote storage such as CD/DVD ROM and USB Flash Drive
- 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

3.5.3.2 Integrated BMC Embedded LAN Channel

The Integrated BMC hardware includes two dedicated 10/100 network interfaces. These interfaces are not shared with the host system. At any time, only one dedicated interface may be enabled for management traffic. The default active interface is the NIC 1 port.

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

4. System Security

4.1 BIOS Password Protection

The BIOS uses passwords to prevent unauthorized tampering with the server setup. Passwords can restrict entry to the BIOS Setup, restrict use of the Boot Popup menu, and suppress automatic USB device reordering.

There is also an option to require a Power On password entry in order to boot the system. If the Power On Password function is enabled in Setup, the BIOS will halt early in POST to request a password before continuing POST.

Both Administrator and User passwords are supported by the BIOS. An Administrator password must be installed in order to set the User password. The maximum length of a password is 14 characters. A password can have alphanumeric (a-z, A-Z, 0-9) characters and it is case sensitive. Certain special characters are also allowed, from the following set:

! @ # $ % ^ & * ( ) - _ + = ?

The Administrator and User passwords must be different from each other. An error message will be displayed if there is an attempt to enter the same password for one as for the other.

The use of *Strong Passwords* is encouraged, but not required. In order to meet the criteria for a Strong Password, the password entered must be at least 8 characters in length, and must include at least one each of alphabetic, numeric, and special characters. If a weak password is entered, a popup warning message will be displayed, although the weak password will be accepted.

Once set, a password can be cleared by changing it to a null string. This requires the Administrator password, and must be done through BIOS Setup or other explicit means of changing the passwords. Clearing the Administrator password will also clear the User password.

Alternatively, the passwords can be cleared by using the Password Clear jumper if necessary. Resetting the BIOS configuration settings to default values (by any method) has no effect on the Administrator and User passwords.

Entering the User password allows the user to modify only the System Time and System Date in the Setup Main screen. Other setup fields can be modified only if the Administrator password has been entered. If any password is set, a password is required to enter the BIOS setup.

The Administrator has control over all fields in the BIOS setup, including the ability to clear the User password and the Administrator password.

It is strongly recommended that at least an Administrator Password be set, since not having set a password gives everyone who boots the system the equivalent of administrative access. Unless an Administrator password is installed, any User can go into Setup and change BIOS settings at will.

In addition to restricting access to most Setup fields to viewing only when a User password is entered, defining a User password imposes restrictions on booting the system. In order to simply boot in the defined boot order, no password is required. However, the F6 Boot popup

prompts for a password, and can only be used with the Administrator password. Also, when a User password is defined, it suppresses the USB Reordering that occurs, if enabled, when a new USB boot device is attached to the system. A User is restricted from booting in anything other than the Boot Order defined in the Setup by an Administrator.

As a security measure, if a User or Administrator enters an incorrect password three times in a row during the boot sequence, the system is placed into a halt state. A system reset is required to exit out of the halt state. This feature makes it more difficult to guess or break a password.

In addition, on the next successful reboot, the Error Manager displays a Major Error code 0048, which also logs a SEL event to alert the authorized user or administrator that a password access failure has occurred.

4.2 Trusted Platform Module (TPM) Support

Trusted Platform Module (TPM) option is a hardware-based security device that addresses the growing concern on boot process integrity and offers better data protection. TPM protects the system start-up process by ensuring it is tamper-free before releasing system control to the operating system. A TPM device provides secured storage to store data, such as security keys and passwords. In addition, a TPM device has encryption and hash functions. The server board implements TPM as per *TPM PC Client Specifications*, revision 1.2, by the Trusted Computing Group (TCG).

A TPM device is optionally installed onto a high density 14-pin connector labeled *TPM* and is secured from external software attacks and physical theft. A pre-boot environment, such as the BIOS and operating system loader, uses the TPM to collect and store unique measurements from multiple factors within the boot process to create a system fingerprint. This unique fingerprint remains the same unless the pre-boot environment is tampered with. Therefore, it is used to compare to future measurements to verify the integrity of the boot process.

After the system BIOS completes the measurement of its boot process, it hands off control to the operating system loader and in turn to the operating system. If the operating system is TPM-enabled, it compares the BIOS TPM measurements to those of previous boots to make sure the system was not tampered with before continuing the operating system boot process. Once the operating system is in operation, it optionally uses TPM to provide additional system and data security (for example, Microsoft Vista* supports Bitlocker drive encryption).

4.2.1 TPM security BIOS

The BIOS TPM support conforms to the *TPM PC Client Specific – Implementation Specification* for Conventional BIOS, version 1.2, and to the *TPM Interface Specification*, version 1.2. The BIOS adheres to the Microsoft Windows BitLocker* requirement. The role of the BIOS for TPM security includes the following:

- Measures and stores the boot process in the TPM microcontroller to allow a TPM enabled operating system to verify system boot integrity.
- Produces EFI and legacy interfaces to a TPM-enabled operating system for using TPM.
- Produces ACPI TPM device and methods to allow a TPM-enabled operating system to send TPM administrative command requests to the BIOS.
- Verifies operator physical presence. Confirms and executes operating system TPM administrative command requests.

- Provides BIOS Setup options to change TPM security states and to clear TPM ownership.

For additional details, refer to the *TCG PC Client Specific Implementation Specification*, the *TCG PC Client Specific Physical Presence Interface Specification*, and the *Microsoft BitLocker* Requirement* documents.

4.2.2 Physical Presence

Administrative operations to the TPM require TPM ownership or physical presence indication by the operator to confirm the execution of administrative operations. The BIOS implements the operator presence indication by verifying the setup Administrator password.

A TPM administrative sequence invoked from the operating system proceeds as follows:

1. User makes a TPM administrative request through the operating system's security software.

2. The operating system requests the BIOS to execute the TPM administrative command through TPM ACPI methods and then resets the system.

3. The BIOS verifies the physical presence and confirms the command with the operator.

4. The BIOS executes TPM administrative commands, inhibits BIOS Setup entry, and boots directly to the operating system which requested the TPM commands.

4.2.3 TPM Security Setup Options

The BIOS TPM Setup allows the operator to view the current TPM state and to carry out rudimentary TPM administrative operations. Performing TPM administrative options through the BIOS setup requires TPM physical presence verification.

Using BIOS TPM Setup, the operator can turn ON or OFF TPM functionality and clear the TPM ownership contents. After the requested TPM BIOS Setup operation is carried out, the option reverts to No Operation.

The BIOS TPM Setup also displays the current state of the TPM, whether TPM is enabled or disabled and activated or deactivated. Note that while using TPM, a TPM-enabled operating system or application may change the TPM state independent of the BIOS setup. When an operating system modifies the TPM state, the BIOS Setup displays the updated TPM state.

The BIOS Setup TPM Clear option allows the operator to clear the TPM ownership key and allows the operator to take control of the system with TPM. You use this option to clear security settings for a newly initialized system or to clear a system for which the TPM ownership security key was lost.

4.2.3.1 Security Screen

To enter the BIOS Setup, press the F2 function key during boot time when the OEM or Intel® logo displays. The following message displays on the diagnostics screen and under the Quiet Boot logo screen:

```
Press <F2> to enter setup
```

When the Setup is entered, the Main screen displays. The BIOS Setup utility provides the Security screen to enable and set the user and administrative passwords and to lock out the front panel buttons so they cannot be used. The Intel® Server Board S1200V3RP provides TPM settings through the security screen.

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

Figure 14. Setup Utility – TPM Configuration Screen

Table 12. TPM Setup Utility – Security Configuration Screen Fields

Setup Item	Options	Help Text	Comments
TPM State*	Enabled and Activated Enabled and Deactivated Disabled and Activated Disabled and Deactivated		Information only. Shows the current TPM device state. A disabled TPM device will not execute commands that use TPM functions and TPM security operations will not be available. An enabled and deactivated TPM

Setup Item	Options	Help Text	Comments
			is in the same state as a disabled TPM except setting of TPM ownership is allowed if not present already. An enabled and activated TPM executes all commands that use TPM functions and TPM security operations will be available.
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 the TPM ownership authentication and returns the TPM to a factory default state. **Note**: The BIOS setting returns to [No Operation] on every boot cycle by default.	

4.3 Intel® Trusted Execution Technology

The Intel® Xeon® Processor E3-1200 V3/V4 Product Family support Intel® Trusted Execution Technology (Intel® TXT), which is a robust security environment. Designed to help protect against software-based attacks, Intel® Trusted Execution Technology integrates new security features and capabilities into the processor, chipset, and other platform components. When used in conjunction with Intel® Virtualization Technology, Intel® Trusted Execution Technology provides hardware-rooted trust for your virtual applications.

This hardware-rooted security provides a general-purpose, safer computing environment capable of running a wide variety of operating systems and applications to increase the confidentiality and integrity of sensitive information without compromising the usability of the platform.

Intel® Trusted Execution Technology requires a computer system with Intel® Virtualization Technology enabled (both VT-x and VT-d), an Intel® Trusted Execution Technology-enabled processor, chipset, and BIOS, Authenticated Code Modules, and an Intel® Trusted Execution Technology compatible measured launched environment (MLE). The MLE could consist of a virtual machine monitor, an OS, or an application. In addition, Intel® Trusted Execution Technology requires the system to include a TPM v1.2, as defined by the *Trusted Computing Group TPM PC Client Specification*, Revision 1.2.

When available, Intel® Trusted Execution Technology can be enabled or disabled in the processor using a BIOS Setup option.

For general information about Intel® TXT, visit the Intel® Trusted Execution Technology website http://www.intel.com/technology/security/.

5. Intel® Technology Support

5.1 Intel® Trusted Execution Technology

The Intel® Xeon® Processor E3-1200 V3/V4 Product Families support Intel® Trusted Execution Technology (Intel® TXT), which is a robust security environment designed to help protect against software-based attacks. Intel® Trusted Execution Technology integrates new security features and capabilities into the processor, chipset, and other platform components. When used in conjunction with Intel® Virtualization Technology and Intel® VT for Directed IO, with an active TPM, Intel® Trusted Execution Technology provides hardware-rooted trust for your virtual applications.

5.2 Intel® Virtualization Technology – Intel® VT-x/VT-d/VT-c

Intel® Virtualization Technology consists of three components which are integrated and interrelated, but which address different areas of Virtualization.

- Intel® Virtualization Technology (VT-x) is processor-related and provides capabilities needed to provide hardware assist to a Virtual Machine Monitor (VMM).
- Intel® Virtualization Technology for Directed I/O (VT-d) is primarily concerned with virtualizing I/O efficiently in a VMM environment. This would generally be a chipset I/O feature, but in the Second Generation Intel® Core™ Processor Family there is an Integrated I/O unit embedded in the processor, and the IIO is also enabled for VT-d.
- Intel® Virtualization Technology for Connectivity (VT-c) is primarily concerned I/O hardware assist features, complementary to but independent of VT-d.

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

Intel® VT-d is supported jointly by the Intel® Xeon® Processor E3-1200 V3/V4 Product Families and The Intel® C220 series chipset. Both support 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.

The Intel® S1200V3RP Server Board Family BIOS publishes the DMAR table in the ACPI Tables. For each DMA Remapping Engine in the platform, one exact entry of DRHD (DMA Remapping Hardware Unit Definition) structure is added to the DMAR. The DRHD structure in turn contains a Device Scope structure that describes the PCI endpoints and/or sub-hierarchies handled by the particular DMA Remapping Engine.

Similarly, there are reserved memory regions typically allocated by the BIOS at boot time. The BIOS marks these regions as either reserved or unavailable in the system address memory map reported to the OS. Some of these regions can be a target of DMA requests from one or more devices in the system, while the OS or executive is active. The BIOS reports each such memory region using exactly one RMRR (Reserved Memory Region Reporting) structure in the DMAR. Each RMRR has a Device Scope listing the devices in the system that can cause a DMA request to the region.

For more information on the DMAR table and the DRHD entry format, refer to the *Intel® Virtualization Technology for Directed I/O Architecture Specification*. For more general information about VT-x, VT-d, and VT-c, a good reference is *Enabling Intel® Virtualization Technology Features and Benefits White Paper*.

5.3 Intel® Intelligent Power Node Manager

Data centers are faced with power and cooling challenges that are driven by increasing numbers of servers deployed and server density in the face of several data center power and cooling constraints. In this type of environment, Information Technology (IT) needs the ability to monitor actual platform power consumption and control power allocation to servers and racks in order to solve specific data center problems including the following issues.

Table 13. Intel® Intelligent Power Node Manager

IT Challenge	Requirement
Over-allocation of power	▪ Ability to monitor actual power consumption ▪ Control capability that can maintain a power budget to enable dynamic power allocation to each server
Under-population of rack space	Control capability that can maintain a power budget to enable increased rack population
High energy costs	Control capability that can maintain a power budget to ensure that a set energy cost can be achieved
Capacity planning	▪ Ability to monitor actual power consumption to enable power usage modeling over time and a given planning period ▪ Ability to understand cooling demand from a temperature and airflow perspective
Detection and correction of hot spots	▪ Control capability that reduces platform power consumption to protect a server in a hot-spot ▪ Ability to monitor server inlet temperatures to enable greater rack utilization in areas with adequate cooling

The requirements listed above are those that are addressed by the Intel® C220 series chipset Management Engine (ME) and Intel® Intelligent Power Node Manager (NM) technology. The ME/NM combination is a power and thermal control capability on the platform, which exposes external interfaces that allow IT (through external management software) to query the ME about platform power capability and consumption, thermal characteristics, and specify policy directives (for example, set a platform power budget).

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.

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 ACPI Source Language (ASL) code used by OS-Directed Power Management (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.

Following are the some of the applications of Intel® Intelligent Power Node Manager technology:

- **Platform Power Monitoring and Limiting**: The ME/NM monitors platform power consumption and holds average power over duration. It can be queried to return actual power at any given instance. The power limiting capability is to allow external management software to address key IT issues by setting a power budget for each server. For example, if there is a physical limit on the power available in a room, IT can decide to allocate power to different servers based on their usage – servers running critical systems can be allowed more power than servers that are running less critical workload.
- **Inlet Air Temperature Monitoring**: The ME/NM monitors server inlet air temperatures periodically. If there is an alert threshold in effect, ME/NM issues an alert when the inlet (room) temperature exceeds the specified value. The threshold value can be set by policy.
- **Memory Subsystem Power Limiting**: The ME/NM monitors memory power consumption. Memory power consumption is estimated using average bandwidth utilization information
- **Processor Power monitoring and limiting**: The ME/NM monitors processor or socket power consumption and holds average power over duration. It can be queried to return actual power at any given instant. The monitoring process of the ME will be used to limit the processor power consumption through processor P-states and dynamic core allocation.
- **Core allocation at boot time**: Restrict the number of cores for OS/VMM use by limiting how many cores are active at boot time. After the cores are turned off, the CPU will limit how many working cores are visible to BIOS and OS/VMM. The cores that are turned off cannot be turned on dynamically after the OS has started. It can be changed only at the next system reboot.
- **Core allocation at run-time**: This particular use case provides a higher level processor power control mechanism to a user at run-time, after booting. An external agent can dynamically use or not use cores in the processor subsystem by requesting ME/NM to control them, specifying the number of cores to use or not use.

Table 14. Intel® Intelligent Power Node Manager 2.0 Capabilities and Features

Value Vector	Capabilities and Features	2.0
Power and Thermal Monitoring	Platform power monitoring	✓
	Inlet Air temperature monitoring	✓
	Processor package power monitoring	✓
	Memory power monitoring	✓
Power Utilization Controls	Platform power limiting	✓
	Processor power limiting	✓
	Memory power limiting	✓
	Dynamic core allocation (core-Idling)	✓
	Configure core power off at boot time	✓
	Configure power-optimized boot at boot time	✓

Value Vector	Capabilities and Features	2.0
Power and Thermal Policies	Concurrent policies	16
	Power limiting – OS operational	✓
	Power limiting – during OS failure	✓
	Power reduction upon temperature excursion	✓
	Response SLA	1s(adj)
Avoid Triggering HW Protection	Reduce power consumption to prevent tripping DC circuit breaker	✓
	Reduce power consumption during SMART ride-through or overcurrent	✓
Interfaces	IPMI-based commands over SMBus* (monitoring, control, and alert)	✓

5.3.1 Hardware Requirements

NM is supported only on platforms that have the NM FW functionality loaded and enabled on the Management Engine (ME) in the SSB and that have a BMC present to support the external LAN interface to the ME. NM power limiting feature requires a means for the ME to monitor input power consumption for the platform. This capability is generally provided by means of PMBus*-compliant power supplies although an alternative model using a simpler SMBus* power monitoring device is possible (there is potential loss in accuracy and responsiveness using non-PMBus* devices). The NM SmaRT/CLST feature requires specific PMBus*-compliant power supplies as well as additional hardware on the baseboard.

6. 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 to the *BMC Core Firmware External Product Specification (EPS)* and *BIOS Core External Product Specification (EPS)* for Intel® Server products based on the Intel® Xeon® processor E3-1200 V3/V4 product families.

6.1 Baseboard Management Controller (BMC) Firmware Feature Support

The following sections outline features that the integrated BMC firmware can support. Support or 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.

6.1.1 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 including system management software (SMS) with receive message queue support, and server management mode (SMM)
  - IPMB interface
  - 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*.

6.1.2 Non-IPMI Features

The BMC supports the following non-IPMI features.

- 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
- 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.
- Local Control Display Panel support
- 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 online 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
- Embedded platform debug feature which allows capture of detailed data for later analysis
- Provisioning and inventory enhancements:
  - Inventory data/system information export (partial SMBIOS table)
- DCMI 1.1 compliance (product-specific)
- Management support for PMBus* rev1.2 compliant power supplies
- Energy Star Server Support
- Smart Ride Through (SmaRT)/Closed Loop System Throttling (CLST)
- Power Supply Cold Redundancy
- Power Supply FW Update
- Power Supply Compatibility Check

6.2 Basic and Advanced Features

The following table lists basic and advanced feature support. Individual features may vary by platform. See the appropriate Platform Specific EPS addendum for more information.

Table 15. Basic and Advanced Features

Feature	Basic*	Advanced**
IPMI 2.0 Feature Support	Yes	Yes
In-circuit BMC Firmware Update	Yes	Yes
FRB 2	Yes	Yes
Chassis Intrusion Detection	Yes	Yes
Fan Redundancy Monitoring	Yes	Yes
Hot-Swap Fan Support	Yes	Yes
Acoustic Management	Yes	Yes

Feature	Basic*	Advanced**
Diagnostic Beep Code Support	Yes	Yes
Power State Retention	Yes	Yes
ARP/DHCP Support	Yes	Yes
PECI Thermal Management Support	Yes	Yes
E-mail Alerting	Yes	Yes
Embedded Web Server	Yes	Yes
SSH Support	Yes	Yes
Integrated KVM		Yes
Integrated Remote Media Redirection		Yes
Lightweight Directory Access Protocol (LDAP)	Yes	Yes
Intel® Intelligent Power Node Manager Support***	Yes	Yes
SMASH CLP	Yes	Yes

* Basic management features provided by Integrated BMC

**Advanced management features available with optional Intel® Remote Management Module 4

*** Intel® Intelligent Power Node Manager Support requires PMBus*-compliant power supply

6.3 Advanced Configuration and Power Interface (ACPI)

The server board supports the following ACPI states.

Table 16. 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.
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.

6.4 Power Control Sources

The server board supports several power control sources which can initiate a power-up or power-down activity.

Table 17. Power Control Initiators

Source	External Signal Name or Internal Subsystem	Capabilities
Power button	Front panel power button	Turns power on or off
BMC watchdog timer	Internal BMC timer	Turns power off, or power cycle
Command	Routed through command processor	Turns power on or off, or power cycle
Power state retention	Implemented by means of BMC internal logic	Turns power on when AC power returns
Chipset	Sleep S4/S5 signal (same as *POWER_ON*)	Turns power on or off
CPU Thermal	CPU Thermtrip	Turns power off
WOL(Wake On LAN)	LAN	Turns power on

6.5 BMC Watchdog

The BMC FW is increasingly called upon to perform system functions that are time-critical in that failure to provide these functions in a timely manner can result in system or component damage. Intel® S1200V3RP Server Platforms introduce a BMC watchdog feature to provide a safe-guard against this scenario by providing an automatic recovery mechanism. It also can provide automatic recovery of functionality that has failed due to a fatal FW defect triggered by a rare sequence of events or a BMC hang due to some type of HW glitch (for example, power).

This feature is comprised of a set of capabilities whose purpose is to detect misbehaving subsections of BMC firmware, the BMC CPU itself, or HW subsystems of the BMC component, and to take appropriate action to restore proper operation. The action taken is dependent on the nature of the detected failure and may result in a restart of the BMC CPU, one or more BMC HW subsystems, or a restart of malfunctioning FW subsystems.

The BMC watchdog feature only allows up to three resets of the BMC CPU (such as HW reset) or entire FW stack (such as a SW reset) before giving up and remaining in the uBOOT code. This count is cleared upon cycling of power to the BMC or upon continuous operation of the BMC without a watchdog-generated reset occurring for a period of greater than 30 minutes. The BMC FW logs a SEL event indicating that a watchdog-generated BMC reset (either soft or hard reset) has occurred. This event may be logged after the actual reset has occurred. Refer to sensor section for details for the related sensor definition. The BMC will also indicate a degraded system status on the Front Panel Status LED after a BMC HW reset or FW stack reset. This state (which follows the state of the associated sensor) will be cleared upon system reset or (AC or DC) power cycle.

Note: A reset of the BMC may result in the following system degradations that will require a system reset or power cycle to correct:

1. *Timeout value for the rotation period can be set using this parameter. Potentially, there will be incorrect ACPI Power State reported by the BMC.*

2. Reversion of temporary test modes for the BMC back to normal operational modes.

3. FP status LED and DIMM fault LEDs may not reflect BIOS detected errors.

6.6 Fault Resilient Booting (FRB)

Fault resilient booting (FRB) is a set of BIOS and BMC algorithms and hardware support that allow a multiprocessor system to boot even if the bootstrap processor (BSP) fails. Only FRB2 is supported using watchdog timer commands.

FRB2 refers to the FRB algorithm that detects system failures during POST. The BIOS uses the BMC watchdog timer to back up its operation during POST. The BIOS configures the watchdog timer to indicate that the BIOS is using the timer for the FRB2 phase of the boot operation.

After the BIOS has identified and saved the BSP information, it sets the FRB2 timer use bit and loads the watchdog timer with the new timeout interval.

If the watchdog timer expires while the watchdog use bit is set to FRB2, the BMC (if so configured) logs a watchdog expiration event showing the FRB2 timeout in the event data bytes. The BMC then hard resets the system, assuming the BIOS-selected reset as the watchdog timeout action.

The BIOS is responsible for disabling the FRB2 timeout before initiating the option ROM scan and before displaying a request for a boot password. If the processor fails and causes an FRB2 timeout, the BMC resets the system.

The BIOS gets the watchdog expiration status from the BMC. If the status shows an expired FRB2 timer, the BIOS enters the failure in the system event log (SEL). In the OEM bytes entry in the SEL, the last POST code generated during the previous boot attempt is written. FRB2 failure is not reflected in the processor status sensor value.

The FRB2 failure does not affect the front panel LEDs.

6.7 Sensor Monitoring

The BMC monitors system hardware and reports system health. Some of the sensors include those for monitoring:

- Component, board, and platform temperatures
- Board and platform voltages
- System fan presence and tach
- Chassis intrusion
- Front Panel NMI
- Front Panel Power and System Reset Buttons
- SMI timeout
- Processor errors

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.

See *Appendix B – Integrated BMC Sensor Tables* for additional sensor information.

6.8 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.

6.9 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 (approximately 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).

Events logged to the SEL can be viewed using Intel's SELVIEW utility, Embedded Web Server, and Active System Console.

6.10 System Fan Management

The BMC controls and monitors the system fans. Each fan is associated with a fan speed sensor that detects fan failure and may also be associated with a fan presence sensor for hot-swap support. For redundant fan configurations, the fan failure and presence status determines the fan redundancy sensor state.

The system fans are divided into fan domains, each of which has a separate fan speed control signal and a separate configurable fan control policy. A fan domain can have a set of temperature and fan sensors associated with it. These are used to determine the current fan domain state.

A fan domain has three states: sleep, nominal, and boost. The sleep and boost states have fixed (but configurable through OEM SDRs) fan speeds associated with them. The nominal state has a variable speed determined by the fan domain policy. An OEM SDR record is used to configure the fan domain policy.

System fan speeds are controlled through pulse width modulation (PWM) signals, which are driven separately for each domain by integrated PWM hardware. Fan speed is changed by adjusting the duty cycle, which is the percentage of time the signal is driven high in each pulse.

6.10.1 Thermal and Acoustic Management

This feature refers to enhanced fan management to keep the system optimally cooled while reducing the amount of noise generated by the system fans. Aggressive acoustics standards

might require a trade-off between fan speed and system performance parameters that contribute to the cooling requirements, primarily memory bandwidth. The BIOS, BMC, and SDRs work together to provide control over how this trade-off is determined.

This capability requires the BMC to access temperature sensors on the individual memory DIMMs.

In order to maintain comprehensive thermal protection, deliver the best system acoustics, and improve fan power efficiency, an intelligent Fan Speed Control (FSC) and thermal management technology (mechanism) is used. Options in <F2> BIOS Setup (**BIOS** > **Advanced** > **System Acoustic and Performance Configuration**) allow for parameter adjustments based on the actual system configuration and usage:

- Set Throttling Mode
- Altitude
- Set Fan Profile
- Fan PWM Offset
- Quiet Fan Idle Mode

Note: The above features may or may not be in effective depends on the actual thermal characters of a specific system. Refer to Intel® Server System R1000RP product family Technical Product Specification and Intel® Server System P4000RP product family Technical Product Specification for system thermal and acoustic management.

6.10.2 Thermal Sensor Input to Fan Speed Control

The BMC uses various IPMI sensors as input to the fan speed control. Some of the sensors are IPMI models of actual physical sensors whereas some are virtual sensors whose values are derived from physical sensors using calculations and/or tabular information.

The following IPMI thermal sensors are used as input to the fan speed control:

- Front Panel Temperature Sensor[1]
- Baseboard Temperature Sensor[2]
- CPU Margin Sensors[3, 5, 6]
- DIMM Thermal Margin Sensors[3, 5]
- Exit Air Temperature Sensor[1, 4, 8]
- PCH Temperature Sensor[4, 6]
- On-board Ethernet Controller Temperature Sensors[4, 6]
- Add-In Intel® SAS/IO Module Temperature Sensors[4, 6]
- PSU Thermal Sensor[4, 9]
- CPU VR Temperature Sensors[4, 7]
- DIMM VR Temperature Sensors[4, 7]
- Integrated BMC Temperature Sensor[4, 7]
- Global Aggregate Thermal Margin Sensors[8]

Notes:

1. For fan speed control in Intel® chassis

2. For fan speed control in 3rd party chassis
3. Temperature margin from throttling threshold
4. Absolute temperature
5. PECI value or margin value
6. On-die sensor
7. On-board sensor
8. Virtual sensor
9. Available only when PSU has PMBus*

The following illustration provides a simple model showing the fan speed control structure that implements the resulting fan speeds.

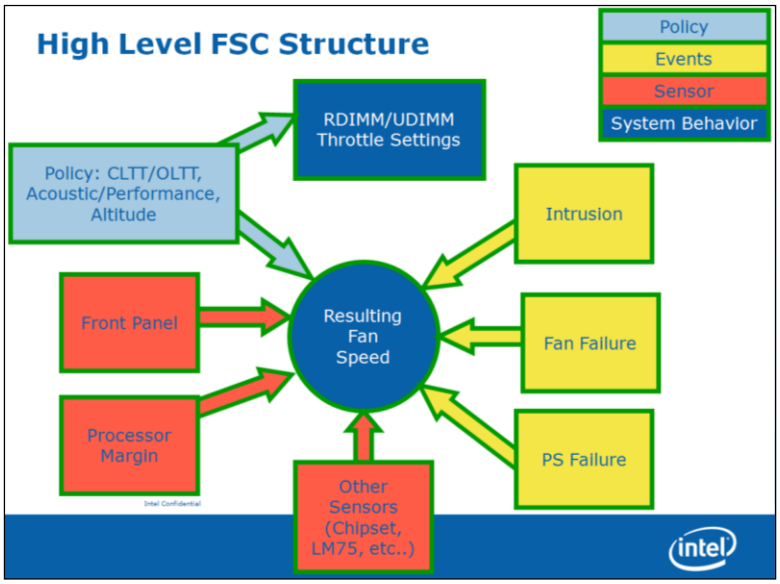


Figure 15. Fan Speed Control Process

6.10.3 Fan Profiles

The server system supports multiple fan control profiles to support acoustic targets and American Society of Heating, Refrigerating and Air Conditioning Engineers (ASHRAE) compliance. The BIOS Setup utility can be used to choose between meeting the target acoustic level or enhanced system performance. This is accomplished through fan profiles.

The BMC supports eight fan profiles, numbered from 0 to 7.

Table 18. Fan Profiles

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

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

Each group of profiles allows for varying fan control policies based on the altitude. For a given altitude, the Tcontrol SDRs associated with an acoustics-optimized profile generate less noise than the equivalent performance-optimized profile by driving lower fan speeds, and the BIOS reduces thermal management requirements by configuring more aggressive memory throttling.

The BMC only supports enabling a fan profile through the command if that profile is supported on all fan domains defined for the given system. It is important to configure platform Sensor Data Records (SDRs) so that all desired fan profiles are supported on each fan domain. If no single profile is supported across all domains, the BMC, by default, uses profile 0 and does not allow it to be changed.

6.10.4 Memory Thermal Throttling

The server board provides support for system thermal management through open loop throttling (OLTT) and closed loop throttling (CLTT) of system memory. Normal system operation uses closed-loop thermal throttling (CLTT) and DIMM temperature monitoring as major factors in overall thermal and acoustics management. In the event that BIOS is unable to configure the system for CLTT, it defaults to open-loop thermal throttling (OLTT). In the OLTT mode, it is assumed that the DIMM temperature sensors are not available for fan speed control. Throttling levels are changed dynamically to cap throttling based on memory and system thermal conditions as determined by the system and DIMM power and thermal parameters. The BMC's fan speed control functionality is linked 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 that 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).

Both Static and Dynamic CLTT modes implement a Hybrid Closed Loop Thermal Throttling mechanism whereby the Integrated Memory Controller estimates the DRAM temperature in between actual reads of the memory thermal sensors.

6.11 Messaging Interfaces

The BMC supports the following communications interfaces:

- 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) I2C interface
- LAN interface using the IPMI-over-LAN protocols

Every messaging interface is assigned an IPMI channel ID by IPMI 2.0. The following table shows the standard channel assignments.

Table 19. Messaging Interfaces

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
4	Reserved	Yes
5	USB[2]	No
6	Secondary IPMB	No
7	SMM	No
8 – 0Dh	Reserved	–
0Eh	Self[3]	–
0Fh	SMS/Receive Message Queue	No

Notes:

1. Optional hardware supported by the server system.

2. Reserve USB channel number, current BMC firmware does not support communication through a USB channel.

3. Refers to the actual channel used to send the request.

6.11.1 User Model

The BMC supports the IPMI 2.0 user model. 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.

2. User 2 (“root”) always has the administrator privilege level.

3. All user passwords (including passwords for 1 and 2) may be modified.

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.

6.11.2 IPMB Communication Interface

The IPMB communication interface uses the 100 KB/s version of an I^2C bus as its physical medium. For more information on I^2C specifications, see *The I^2C Bus and How to Use It*. The IPMB implementation in the BMC is compliant with the *IPMB v1.0*, revision 1.0.

The BMC IPMB slave address is 20h.

The BMC both sends and receives IPMB messages over the IPMB interface. Non-IPMB messages received by means of the IPMB interface are discarded.

Messages sent by the BMC can either be originated by the BMC, such as initialization agent operation, or by another source. One example is KCS-IPMB bridging.

6.11.3 LAN Interface

The BMC implements both the IPMI 1.5 and IPMI 2.0 messaging models. These provide out-of-band local area network (LAN) communication between the BMC and the network.

See the *Intelligent Platform Management Interface Specification Second Generation v2.0* for details about the IPMI-over-LAN protocol.

Run-time determination of LAN channel capabilities can be determined by both standard IPMI defined mechanisms.

6.11.3.1 RMCP/ASF Messaging

The BMC supports RMCP ping discovery in which the BMC responds with a pong message to an RMCP/ASF ping request. This is implemented per the *Intelligent Platform Management Interface Specification Second Generation v2.0*.

6.11.3.2 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 RMM4 add-in module.

6.11.3.2.1 Baseboard NICs

The on-board Ethernet controller provides support for a Network Controller Sideband Interface (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 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 NICs 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 1 master and up to 4 slaves. The logical layer (configuration commands) is incompatible with RMII.

The server board provides 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 using a BIOS setup option.

6.11.3.2.2 Dedicated Management Channel

An additional LAN channel dedicated to BMC usage and not available to host SW is supported using an optional RMM4 add-in card. There is only a PHY device present on the RMM4 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 RMM4 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 RMM4 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.

6.11.3.2.3 Concurrent Server Management Use of Multiple Ethernet Controllers

The BMC FW supports concurrent OOB LAN management sessions for the following combination:

- 2 on-board NIC ports
- 1 on-board NIC and the optional dedicated RMM4 add-in management NIC
- 2 on-board NICs and optional dedicated RMM4 add-in management NIC

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

MAC addresses are assigned for management NICs from a pool of up to 3 MAC addresses allocated specifically for manageability.

The server board has seven MAC addresses programmed at the factory. MAC addresses are assigned as follows:

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

The printed MAC address on the server board and/or server system is assigned to NIC1 on the server board.

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

- IP Address: Static
- All users disabled

IPMI-enabled network interfaces may not be placed on the same subnet. This includes the Intel® Dedicated Server Management NIC and either of the BMC's embedded network interfaces.

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

On server boards 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 LAN1 (Baseboard NIC port) – 100Mb (10Mb in DC off state)
- BMC LAN 2 (Baseboard NIC port) – 100Mb (10Mb in DC off state)
- BMC LAN 3 (Dedicated NIC) – 1000Mb

6.11.3.3 IPV6 Support

In addition to IPv4, the server board 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 vs. 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 are sent or received on that channel.
- There are two variants of automatic IP Address Source configuration vs. 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.

6.11.3.4 LAN Failover

The BMC FW provides a LAN failover capability so 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 using IPMI methods as well as 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 supports only an *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.

6.11.3.5 BMC IP Address Configuration

Enabling the BMC's network interfaces requires using the *Set LAN Configuration Parameter* command to configure LAN configuration parameter 4, *IP Address Source*. The BMC supports this parameter as follows:

- 1h, static address (manually configured): Supported on all management NICs. This is the BMC's default value.
- 2h, address obtained by BMC running DHCP: Supported only on embedded management NICs.

IP Address Source value 4h, address obtained by BMC running other address assignment protocol, is not supported on any management NIC.

Attempting to set an unsupported IP address source value has no effect, and the BMC returns error code 0xCC, Invalid data field-in request. Note that values 0h and 3h are no longer supported, and will return a 0xCC error completion code.

6.11.3.5.1 Static IP Address (IP Address Source Values 0h, 1h, and 3h)

The BMC supports static IP address assignment on all of its management NICs. The IP address source parameter must be set to *static* before the IP address; the subnet mask or gateway address can be manually set.

The BMC takes no special action when the following IP address source is specified as the IP address source for any management NIC:1h – Static address (manually configured).

The *Set LAN Configuration Parameter* command must be used to configure LAN configuration parameter 3, *IP Address*, with an appropriate value.

The BIOS does not monitor the value of this parameter, and it does not execute DHCP for the BMC under any circumstances, regardless of the BMC configuration.

6.11.3.5.2 Static LAN Configuration Parameters

When the IP Address Configuration parameter is set to 01h (static), the following parameters may be changed by the user:

- LAN configuration parameter 3 (IP Address)
- LAN configuration parameter 6 (Subnet Mask)
- LAN configuration parameter 12 (Default Gateway Address)

When changing from DHCP to Static configuration, the initial values of these three parameters will be equivalent to the existing DHCP-set parameters. Additionally, the BMC observes the following network safety precautions:

1. The user may only set a subnet mask that is valid, per IPv4 and RFC 950 (*Internet Standard Subnetting Procedure*). Invalid subnet values return a 0xCC (Invalid Data Field in Request) completion code, and the subnet mask is not set. If no valid mask has been previously set, default subnet mask is 0.0.0.0.

2. The user may only set a default gateway address that can potentially exist within the subnet specified above. Default gateway addresses outside the BMC's subnet are technically unreachable and the BMC will not set the default gateway address to an unreachable value. The BMC returns a 0xCC (Invalid Data Field in Request) completion code for default gateway addresses outside its subnet.

3. If a command is issued to set the default gateway IP address before the BMC's IP address and subnet mask are set, the default gateway IP address is not updated and the BMC returns 0xCC.

If the BMC's IP address on a LAN channel changes while a LAN session is in progress over that channel, the BMC does not take action to close the session except through a normal session timeout. The remote client must re-sync with the new IP address. The BMC's new IP address is only available in-band through the *Get LAN Configuration Parameters* command.

6.11.3.5.3 Enabling/Disabling Dynamic Host Configuration (DHCP) Protocol

The BMC DHCP feature is activated by using the *Set LAN Configuration Parameter* command to set LAN configuration parameter 4, *IP Address Sourc*e, to 2h: "address obtained by BMC

running DHCP". Once this parameter is set, the BMC initiates the DHCP process within approximately 100 ms.

If the BMC has previously been assigned an IP address through DHCP or the *Set LAN Configuration Parameter* command, it requests that same IP address to be reassigned. If the BMC does not receive the same IP address, system management software must be reconfigured to use the new IP address. The new address is only available in-band, through the IPMI *Get LAN Configuration Parameters* command.

Changing the *IP Address Source* parameter from 2h to any other supported value will cause the BMC to stop the DHCP process. The BMC uses the most recently obtained IP address until it is reconfigured.

If the physical LAN connection is lost (that is, the cable is unplugged), the BMC will not re-initiate the DHCP process when the connection is re-established.

6.11.3.5.4 DHCP-related LAN Configuration Parameters

Users may not change the following LAN parameters while the DHCP is enabled:

- LAN configuration parameter 3 (IP Address)
- LAN configuration parameter 6 (Subnet Mask)
- LAN configuration parameter 12 (Default Gateway Address)

To prevent users from disrupting the BMC's LAN configuration, the BMC treats these parameters as read-only while DHCP is enabled for the associated LAN channel. Using the *Set LAN Configuration Parameter* command to attempt to change one of these parameters under such circumstances has no effect, and the BMC returns error code 0xD5, "Cannot Execute Command. Command, or request parameter(s) are not supported in present state."

6.11.3.6 DHCP BMC Hostname

The BMC allows setting a DHCP Hostname using the *Set/Get LAN Configuration Parameters* command.

- DHCP Hostname can be set regardless of the IP Address source configured on the BMC. But this parameter is only used if the IP Address source is set to DHCP.
- When Byte 2 is set to *Update in progress*, all the 16 Block Data Bytes (Bytes 3 – 18) must be present in the request.
- When Block Size is less than 16, it must be the last Block request in this series. In other words Byte 2 is equal to *Update is complete* on that request.
- Whenever Block Size is less than 16, the Block data bytes must end with a NULL Character or Byte (=0).
- All Block write requests are updated into a local Memory byte array. When Byte 2 is set to *Update is Complete*, the Local Memory is committed to the NV Storage. Local Memory is reset to NULL after changes are committed.
- When Byte 1 (Block Selector = 1), firmware resets all the 64 bytes local memory. This can be used to undo any changes after the last *Update in Progress*.

- User should always set the hostname starting from block selector 1 after the last *Update is complete*. If the user skips block selector 1 while setting the hostname, the BMC will record the hostname as *NULL*, because the first block contains NULL data.
- This scheme effectively does not allow a user to make a partial Hostname change. Any Hostname change needs to start from Block 1.
- Byte 64 (Block Selector 04h byte 16) is always ignored and set to NULL by BMC which effectively means we can set only 63 bytes.
- User is responsible for keeping track of the Set series of commands and Local Memory contents.

While BMC firmware is in *Set Hostname in Progress* (Update not complete), the firmware continues using the Previous Hostname for DHCP purposes.

6.11.4 Address Resolution Protocol (ARP)

The BMC can receive and respond to ARP requests on BMC NICs. Gratuitous ARPs are supported, and disabled by default.

6.11.5 Internet Control Message Protocol (ICMP)

The BMC supports the following ICMP message types targeting the BMC over integrated NICs:

- Echo request (ping): The BMC sends an Echo Reply.
- Destination unreachable: If message is associated with an active socket connection within the BMC, the BMC closes the socket.

6.11.6 Virtual Local Area Network (VLAN)

The BMC supports VLAN as defined by IPMI 2.0 specifications. VLAN is supported internally by the BMC, not through switches. VLAN provides a way of grouping a set of systems together so that they form a logical network. This feature can be used to set up a management VLAN where only devices which are members of the VLAN will receive packets related to management and members of the VLAN will be isolated from any other network traffic. Note that VLAN does not change the behavior of the host network setting, and it only affects the BMC LAN communication.

LAN configuration options are now supported (by means of the *Set LAN Config Parameters* command, parameters 20 and 21) that allow support for 802.1Q VLAN (Layer 2). This allows VLAN headers/packets to be used for IPMI LAN sessions. VLAN IDs are entered and enabled by means of parameter 20 of the *Set LAN Config Parameters* IPMI command. When a VLAN ID is configured and enabled, the BMC only accepts packets with that VLAN tag/ID. Conversely, all BMC generated LAN packets on the channel include the given VLAN tag/ID. Valid VLAN IDs are 1 through 4094, and VLAN IDs of 0 and 4095 are reserved, per the 802.1Q VLAN specification. Only one VLAN can be enabled at any point in time on a LAN channel. If an existing VLAN is enabled, it must first be disabled prior to configuring a new VLAN on the same LAN channel.

Parameter 21 (VLAN Priority) of the *Set LAN Config Parameters* IPMI command is now implemented and a range from 0 to 7 will be allowed for VLAN Priorities. Note that bits 3 and 4 of Parameter 21 are considered Reserved bits.

Parameter 25 (VLAN Destination Address) of the *Set LAN Config Parameters* IPMI command is not supported and returns a completion code of 0x80 (parameter not supported) for any read/write of parameter 25.

If the BMC IP address source is DHCP, the following behavior is seen:

- If the BMC is first configured for DHCP (prior to enabling VLAN), when VLAN is enabled, the BMC performs a discovery on the new VLAN in order to obtain a new BMC IP address.
- If the BMC is configured for DHCP (before disabling VLAN), when VLAN is disabled, the BMC performs a discovery on the LAN in order to obtain a new BMC IP address.

If the BMC IP address source is Static, the following behavior is seen:

- If the BMC is first configured for static (prior to enabling VLAN), when VLAN is enabled, the BMC has the same IP address as configured before. It is left to the management application to configure a different IP address if that is not suitable for VLAN.
- If the BMC is configure for static (prior to disabling VLAN), when VLAN is disabled, the BMC has the same IP address as configured before. It is left to the management application to configure a different IP address if that is not suitable for LAN.

6.11.7 Secure Shell (SSH)

Secure Shell (SSH) connections are supported for SMASH-CLP sessions to the BMC.

6.11.8 Serial-over-LAN (SOL 2.0)

The BMC supports IPMI 2.0 SOL.

IPMI 2.0 introduced a standard serial-over-LAN feature. This is implemented as a standard payload type (01h) over RMCP+.

Three commands are implemented for SOL 2.0 configuration:

- Get SOL 2.0 Configuration Parameters and Set SOL 2.0 Configuration Parameters: These commands are used to get and set the values of the SOL configuration parameters. The parameters are implemented on a per-channel basis.
- Activating SOL: This command is not accepted by the BMC. It is sent by the BMC when SOL is activated to notify a remote client of the switch to SOL.
- Activating a SOL session requires an existing IPMI-over-LAN session. If encryption is used, it should be negotiated when the IPMI-over LAN session is established.

6.11.9 Platform Event Filter (PEF)

The BMC includes the ability to generate a selectable action, such as a system power-off or reset, when a match occurs to one of a configurable set of events. This capability is called *Platform Event Filtering*, or PEF. One of the available PEF actions is to trigger the BMC to send a LAN alert to one or more destinations.

The BMC supports 20 PEF filters. The first twelve entries in the PEF filter table are pre-configured (but may be changed by the user). The remaining entries are left blank, and may be configured by the user.

Table 20. Factory Configured PEF Table Entries

Event Filter Number	Offset Mask	Events
1	Non-critical, critical and non-recoverable	Temperature sensor out of range
2	Non-critical, critical and non-recoverable	Voltage sensor out of range
3	Non-critical, critical and non-recoverable	Fan failure
4	General chassis intrusion	Chassis intrusion (security violation)
5	Failure and predictive failure	Power supply failure
6	Uncorrectable ECC	BIOS
7	POST error	BIOS: POST code error
8	FRB2	Watchdog Timer expiration for FRB2
9	Policy Correction Time	Node Manager
10	Power down, power cycle, and reset	Watchdog timer
11	OEM system boot event	System restart (reboot)
12	Drive Failure, Predicted Failure	Hot Swap Controller

Additionally, the BMC supports the following PEF actions:

- Power off
- Power cycle
- Reset
- OEM action
- Alerts

The *Diagnostic interrupt* action is not supported.

6.11.10 LAN Alerting

The BMC supports sending embedded LAN alerts, called SNMP PET (Platform Event traps), and SMTP email alerts.

The BMC supports a minimum of four LAN alert destinations.

6.11.10.1 SNMP Platform Event Traps (PETs)

This feature enables a target system to send SNMP traps to a designated IP address by means of LAN. These alerts are formatted per the *Intelligent Platform Management Interface Specification Second Generation v2.0*. A Modular Information Block (MIB) file associated with the traps is provided with the BMC firmware to facilitate interpretation of the traps by external software. The format of the MIB file is covered under RFC 2578.

6.11.11 Alert Policy Table

Associated with each PEF entry is an alert policy that determines which IPMI channel the alert is to be sent. There is a maximum of 20 alert policy entries. There are no pre-configured entries in the alert policy table because the destination types and alerts may vary by user. Each entry in the alert policy table contains four bytes for a maximum table size of 80 bytes.

6.11.11.1 E-mail Alerting

The Embedded Email Alerting feature allows the user to receive e-mails alerts indicating issues with the server. This allows e-mail alerting in an OS-absent (for example, Pre-OS and OS-Hung) situation. This feature provides support for sending e-mail by means of SMTP, the Simple Mail Transport Protocol as defined in Internet RC 821. The e-mail alert provides a text string that describes a simple description of the event. SMTP alerting is configured using the embedded web server.

6.11.12 SM-CLP (SM-CLP Lite)

SMASH refers to Systems Management Architecture for Server Hardware. SMASH is defined by a suite of specifications, managed by the DMTF, that standardize the manageability interfaces for server hardware. CLP refers to Command Line Protocol. SM-CLP is defined by the *Server Management Command Line Protocol Specification (SM-CLP) ver1.0*, which is part of the SMASH suite of specifications. The specifications and further information on SMASH can be found at the DMTF website (http://www.dmtf.org/).

The BMC provides an embedded *lite* version of SM-CLP that is syntax-compatible but not considered fully compliant with the DMTF standards.

The SM-CLP utilized by a remote user by connecting a remote system using one of the system NICs. It is possible for third party management applications to create scripts using this CLP and execute them on server to retrieve information or perform management tasks such as reboot the server, configure events, and so on.

The BMC embedded SM-CLP feature includes the following capabilities:

- Power on/off/reset the server.
- Get the system power state.
- Clear the System Event Log (SEL).
- Get the interpreted SEL in a readable format.
- Initiate/terminate a Serial Over LAN session.
- Support “help” to provide helpful information.
- Get/set the system ID LED.
- Get the system GUID.
- Get/set configuration of user accounts.
- Get/set configuration of LAN parameters.
- Embedded CLP communication should support SSH connection.
- Provide current status of platform sensors including current values. Sensors include voltage, temperature, fans, power supplies, and redundancy (power unit and fan redundancy).

The embedded web server is supported over any system NIC port that is enabled for server management capabilities.

6.11.13 Embedded Web Server

BMC Base manageability provides an embedded web server and an OEM-customizable web GUI which exposes the manageability features of the BMC base feature set. It is supported over all on-board NICs that have management connectivity to the BMC as well as an optional RMM4 dedicated add-in management NIC. At least two concurrent web sessions from up to two different users is supported. The embedded web user interface supports 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. Embedded web server uses ports #80 and #443. The user interface presented by the embedded web user interface authenticates 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, the item will be displayed in grey-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.

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.
- Display BIOS, BMC, ME, and SDR version information.
- Display overall system health.
- Configuration of various IPMI over LAN parameters for both IPV4 and IPV6.
- 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.
- Provide ability to filter sensors based on sensor type (Voltage, Temperature, Fan, and Power supply related).
- Automatic refresh of sensor data with a configurable refresh rate.

- Online help.
- Display/clear SEL (display is in easily understandable human readable format).
- Support major industry-standard browsers (Microsoft Internet Explorer* and Mozilla Firefox*).
- Automatically log 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: Allows the user to initiate a *diagnostic dump* to a file that can be sent to Intel for debug purposes.
- Virtual Front Panel: The Virtual Front Panel provides the same functionality as the local front panel. The displayed LEDs match the current state of the local panel LEDs. The displayed buttons (for example, power button) can be used in the same manner as the local buttons.
- Severity level indication of SEL events: The web server UI displays the severity level associated with each event in the SEL. The severity level correlates with the front panel system status LED (*OK*, *Degraded*, *Non-Fatal*, or *Fatal*).
- Display of ME sensor data. Only sensors that have associated SDRs loaded are displayed.
- Ability to save the SEL to a file.
- Ability to force HTTPS connectivity for greater security. This is provided through a configuration option in the UI.
- Display of processor and memory information as is available over IPMI over LAN.
- Ability to get and set Node Manager (NM) power policies.
- Display of power consumed by the server.
- Ability to view and configure VLAN settings.
- Warn user the reconfiguration of IP address will cause disconnect.
- Capability to block logins for a period of time after several consecutive failed login attempts. The lock-out period and the number of failed logins that initiates the lock-out period are configurable by the user.
- Server Power Control: Ability to force into Setup on a reset.

6.11.14 Virtual Front Panel

- Virtual Front Panel is the module present as Virtual Front Panel on the left side in the embedded web server when remote Control tab is clicked.
- Main Purpose of the Virtual Front Panel is to provide the front panel functionality virtually.
- Virtual Front Panel (VFP) will mimic the status LED and Power LED status and Chassis ID alone. It is automatically in sync with BMC every 40 seconds.
- For any abnormal status LED state, Virtual Front Panel will get the reason behind the abnormal or status LED changes and displayed in VFP side.
- As Virtual Front Panel uses the *Chassis Control* command for power actions. It won't log the Front button press event since Logging the front panel press event for Virtual Front Panel press will mislead the administrator.
- For Reset from Virtual Front Panel, the reset will be done by a *Chassis Control* command.

- For Reset from Virtual Front Panel, the restart cause will be because of *Chassis Control* command.
- During Power action, Power button/Reset button will not accept the next action until current Power action is complete and the acknowledgment from BMC is received.
- EWS will provide a valid message during Power action until it completes the current Power action.
- The VFP does not have any effect on whether the front panel is locked by *Set Front Panel Enables* command.
- 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 actions:
  - Toggled by turning the chassis ID button on or off.
  - There is no precedence or lock-out mechanism for the control sources. When a new request arrives, previous requests are terminated. For example, if the chassis ID button is pressed, the chassis ID LED changes to solid on. If the button is pressed again, the chassis ID LED turns off.
  - Note that the chassis ID will turn on because of the original chassis ID button press and will reflect in the Virtual Front Panel after VFP sync with BMC. Virtual Front Panel will not reflect the chassis LED software blinking from the software command as there is no mechanism to get the chassis ID Led status.
  - Only Infinite chassis ID ON/OFF from the software command will reflect in EWS during automatic /manual EWS sync up with BMC.
- Virtual Front Panel help is available for virtual panel module.
- At present, NMI button in VFP is disabled. It can be used in future.

6.11.15 Embedded Platform Debug

The Embedded Platform Debug feature supports capturing low-level diagnostic data (applicable MSRs, PCI config-space registers, and so on). This feature allows a user to export this data into a file that is retrievable from the embedded web GUI, as well as through host and remote IPMI methods, for the purpose of sending to an Intel engineer for an enhanced debugging capability. The files are compressed, encrypted, and password protected. The file is not meant to be viewable by the end user but rather to provide additional debugging capability to an Intel support engineer.

A list of data that may be captured using this feature includes but is not limited to:

- Platform sensor readings – This includes all readable sensors that can be accessed by the BMC FW and have associated SDRs populated in the SDR repository. This does not include any event-only sensors. (All BIOS sensors and some BMC and ME sensors are event-only; meaning that they are not readable using an IPMI *Get Sensor Reading* command but rather are used just for event logging purposes).
- SEL – The current SEL contents are saved in both hexadecimal and text format.
- CPU/memory register data – Useful for diagnosing the cause of the following system errors: CATERR, ERR[2], SMI timeout, PERR, and SERR. The debug data is saved and timestamped for the last 3 occurrences of the error conditions.
  - PCI error registers
  - MSR registers
  - MCH registers

- BMC configuration data
  - BMC FW debug log (that is, SysLog) – Captures FW debug messages.
  - Non-volatile storage of captured data – Some of the captured data is stored persistently in the BMC's non-volatile flash memory and preserved across AC power cycles. Due to size limitations of the BMC's flash memory, it is not feasible to store all of the data persistently.
- SMBIOS table data – The entire SMBIOS table is captured from the last boot.
- PCI configuration data for on-board devices and add-in cards – The first 256 bytes of PCI configuration data is captured for each device for each boot.
- System memory map – The system memory map is provided by BIOS on the current boot. This includes the EFI memory map and the Legacy (E820) memory map depending on the current boot.
- Power supplies debug capability
  - Capture of power supply *black box* data and power supply asset information –Power supply vendors are adding the capability to store debug data within the power supply itself. The platform debug feature provides a means to capture this data for each installed power supply. The data can be analyzed by Intel for failure analysis and possibly provided to the power supply vendor as well. The BMC gets this data from the power supplied from the PMBus* manufacturer-specific commands.
  - Storage of system identification in power supply – The BMC copies board and system serial numbers and part numbers into the power supply whenever a new power supply is installed in the system or when the system is first powered on. This information is included as part of the power supply black box data for each installed power supply.
- Accessibility through IPMI interfaces – The platform debug file can be accessed using an external IPMI interface (KCS or LAN).
- POST code sequence for the two most recent boots – This is a best-effort data collection by the BMC as the BMC real-time response cannot guarantee that all POST codes are captured.
- Support for multiple debug files –The platform debug feature provides the ability to save data to two separate files that are encrypted with different passwords.
  - File #1 is strictly for viewing by Intel engineering and may contain BMC log messages (that is, syslog) and other debug data that Intel FW developers deem useful in addition to the data specified in this document.
  - File #2 can be viewed by Intel partners who have signed an NDA with Intel and its contents are restricted to specific data items specified in this with the exception of the BMC syslog messages and power supply *black box* data.

6.11.15.1 Output Data Format

The diagnostic feature outputs a password-protected compressed HTML file containing specific BMC and system information. This file is not intended for end-customer usage. This file is for customer support and engineering only.

6.11.15.2 Output Data Availability

The diagnostic data is available on-demand from the embedded web server, KCS, or IPMI *Over LAN* commands.

6.11.15.3 Output Data Categories

The following tables list the data to be provided in the diagnostic output.

Table 21. Diagnostic Data

Category	Data
Internal BMC Data	BMC uptime/load
	Process list
	Free Memory
	Detailed Memory List
	Filesystem List/Info
	BMC Network Info
	BMC Syslog
	BMC Configuration Data
External BMC Data	Hex SEL listing
	Human-readable SEL listing
	Human-readable sensor listing
External BIOS Data	BIOS configuration settings
	POST codes for the two most recent boots
System Data	SMBIOS table for the current boot
	256 bytes of PCI config data for each PCI device
	Memory Map (EFI and Legacy) for current boot

Table 22. Additional Diagnostics on Error

Category	Data
System Data	First 256 bytes of PCI config data for each PCI device
	PCI error registers
	MSR registers
	MCH registers

6.11.16 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. Intel® S1400/S1600/S2400/S2600 Server Platforms implement the mandatory DCMI features in the BMC firmware (DCMI 1.1 Errata 1 compliance). Refer to *DCMI 1.1 errata 1 spec* for details. Only mandatory commands are supported. No support for optional DCMI commands. Optional power management and SEL roll over feature is not supported. DCMI Asset tag is independent of baseboard FRU asset Tag. Refer to table DCMI Group Extension Commands for more details on DCMI commands.

6.11.17 Lightweight Directory Authentication Protocol (LDAP)

The Lightweight Directory Access Protocol (LDAP) is an application protocol supported by the BMC for the purpose of authentication and authorization. The 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) using the 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*. Only open LDAP is supported by BMC. Microsoft Windows* and Novell* LDAP are not supported.

7. Advanced Management Feature Support (RMM4)

The integrated baseboard management controller has support for advanced management features which are enabled when an optional Intel® Remote Management Module 4 (RMM4) is installed.

RMM4 is comprised of two boards: RMM4 lite and the optional Dedicated Server Management NIC (DMN).

Table 23. RMM4 Option Kits

Product Code	Description	Kit Contents	Benefits
AXXRMM4LITE	Intel® Remote Management Module 4 Lite	RMM4 Lite Activation Key	Enables KVM and media redirection from the onboard NIC.
AXXRMM4	Intel® Remote Management Module 4	RMM4 Lite Activation Key Dedicated NIC Port Module	Dedicated NIC for management traffic. Higher bandwidth connectivity for KVM and media Redirection with 100Mbe NIC.

On the server board each Intel® RMM4 component is installed at the following locations.

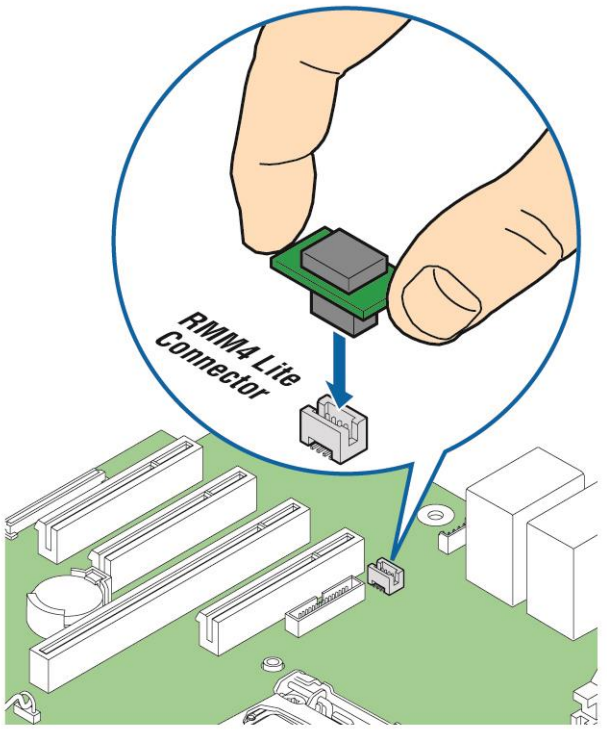


Figure 16. Intel® RMM4 Lite Activation Key Installation

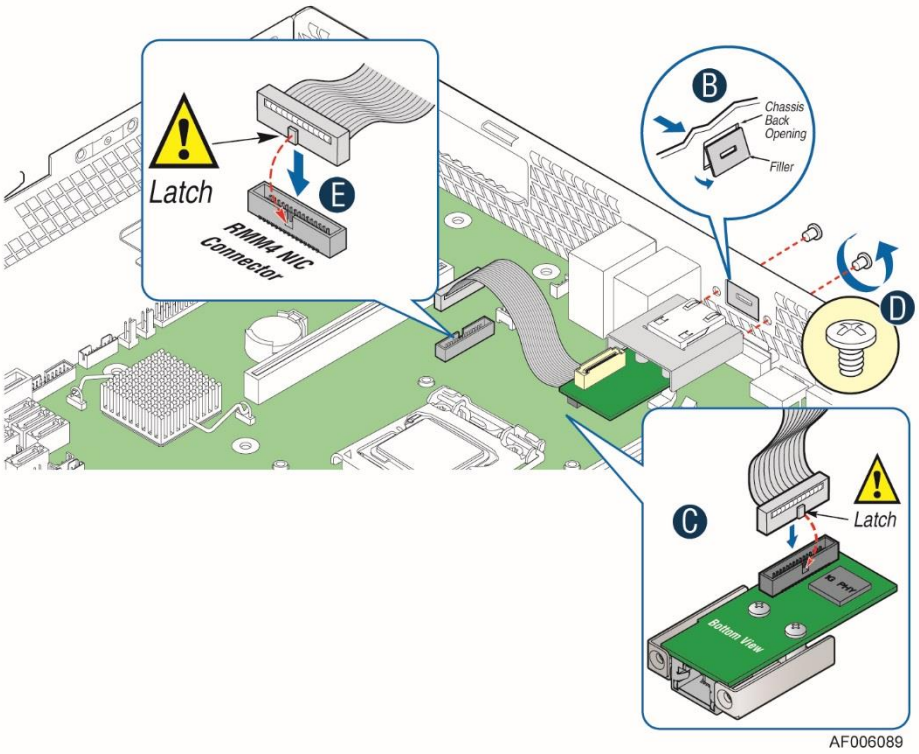


Figure 17. Intel® RMM4 Dedicated Management NIC Installation

Table 24. Enabling Advanced Management Features

Manageability Hardware	Benefits
Intel® Integrated BMC	Comprehensive IPMI based base manageability features
Intel® Remote Management Module 4 – Lite Package contains one module – ▪ Key for advance Manageability features.	No dedicated NIC for management Enables KVM and media redirection from onboard NIC
Intel® Remote Management Module 4 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.

If the optional Dedicated Server Management NIC is not used then the traffic can only go through the onboard Integrated BMC-shared NIC and will share network bandwidth with the host system. Advanced manageability features are supported over all NIC ports enabled for server manageability.

7.1 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 only enabled when the Intel® RMM4 lite is present. The client system must have a Java Runtime Environment* (JRE*) version 6.0 or later to run the KVM or media redirection applets.

The 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 functions of the remote server as if the user were physically at the managed server.

KVM redirection console supports the following keyboard layouts: English, Dutch, French, German, Italian, Russian, and Spanish.

KVM redirection includes a soft keyboard function. The soft keyboard is used to simulate an entire keyboard that is connected to the remote system. The soft keyboard functionality supports the following layouts: English, Dutch, French, German, Italian, Russian, and Spanish.

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
- Ability to select a mouse configuration based on the OS type
- Supports user definable keyboard macros

KVM redirection feature supports the following resolutions and refresh rates:

- 640x480 at 60Hz, 72Hz, 75Hz, 85Hz, 100Hz
- 800x600 at 60Hz, 72Hz, 75Hz, 85Hz
- 1024x768 at 60Hx, 72Hz, 75Hz, 85Hz
- 1280x960 at 60Hz
- 1280x1024 at 60Hz
- 1600x1200 at 60Hz
- 1920x1080 (1080p),
- 1920x1200 (WUXGA)
- 1650x1080 (WSXGA+)

7.1.1 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 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. When encryption is enabled, the protocol uses ports #7582 for KVM, #5124 for CDROM media redirection, and #5127 for Floppy/USB media redirection. The local network environment must permit these connections to be made, that is,

the firewall and, in case of a private internal network, the NAT (Network Address Translation) settings have to be configured accordingly.

7.1.2 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.

7.1.3 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.

7.1.4 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 is required during a server reset or power on/off. A BMC reset (for example, due to a BMC Watchdog initiated reset or BMC reset after BMC FW update) requires the session to be re-established.

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

7.1.5 Usage

As the server is powered up, the remote KVM session displays the complete BIOS boot process. The user can 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.

7.1.6 Force-enter BIOS Setup

KVM redirection can present an option to force-enter BIOS Setup. This enables the system to enter F2 setup while booting which is often missed by the time the remote console redirects the video.

7.2 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 IDE 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.
- Either IDE (CD-ROM, floppy) or USB devices can be mounted as a remote device to the server.
- 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 supports redirection for both a virtual CD device and a virtual Floppy/USB device concurrently. The CD device may be either a local CD drive or else an ISO image file; the Floppy/USB device may be a local Floppy drive, a local USB device, or a disk image file.
- 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. A BMC reset (for example, due to a BMC reset after BMC FW update) requires the session to be re-established
- The mounted device is visible to (and useable by) 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 appear as floppy disks over media redirection. This allows for the installation of device drivers during OS installation.

If either a virtual IDE or virtual floppy device is remotely attached during system boot, both the virtual IDE and virtual floppy are presented as bootable devices. It is not possible to present only a single-mounted device type to the system BIOS.

7.2.1 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.

7.2.2 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)

8. On-board Connector/Header Overview

The following section provides detailed information regarding all connectors, headers, and jumpers on the server boards.

8.1 Board Connector Information

The following table lists all connector types available on the board and the corresponding preference designators printed on the silkscreen.

Table 25. Board Connector Matrix

Connector	Quantity	Reference Designators	Connector Type	Pin Count
Power supply	3	J9H1 J9B1 J9C3	Main power CPU power PS AUX	24 8 5
CPU	1	U6F1	CPU sockets	1150
Main memory	4	J7C1, J8C1 J8C2, J9C2	DIMM sockets	240
PCI Express* x8 mechanical	3	J1B1, J2B1, J4B1	Card edge	98
PCI Express* x16 mechanical	1	J3B1	Card edge	164
Intel® RMM4 NIC	1	J4C1	Connector	30
Intel® RMM4 Lite	1	J4B1	Connector	7
SATA Key to enable ESRT2 RAID5	1	J4A1	Header	4
System fans	4	J3K4, J8K1, J8K2, J8B1	Header	4
CPU fan	1	J7K1	Header	4
Battery	1	BT2E1	Battery holder	2
Stacked RJ45/2xUSB	2	JA5A1, JA6A1	Dual USB/LAN (RJ45) Combo Connector	22
VGA	1	J7A1	Connector	15
Display Port	1	J8A1	Connector	4
Serial port A	1	J9A1	Connector	9
Serial port B	1	J9A2	Header	9
Front panel	1	J1E1	Header	24
Internal Dual USB 3.0	1	J1J1	Header	20
Internal Dual USB 2.0	1	J1K3	Header	10
eUSB SSD	1	J5K1	Header	9
Internal USB	1	J1J4	Type-A USB	4
HDD LED	1	J1G2	Header	2

Connector	Quantity	Reference Designators	Connector Type	Pin Count
SATA	6	J1K4, J1K1, J1K5, J1K2, J2K5, J2K3	Connector	7
HSBP_I2C	1	J2K4	Header	3
SATA SGPIO	1	J2K2	Header	5
LCP	1	J1G1	Header	7
IPMB	1	J2K1	Header	4
Configuration jumpers	5	J3K6 (Force Integrated BMC update), J2K9 (Password Clear), J2K8 (BIOS Recovery), J2K6 (Reset BIOS Configuration) J3K2 (ME Firmware Update)	Jumper	3
TPM	1	J8J1	Connector	14
Chassis Intrusion	1	J1F1	Header	2
I/O Module Connector	1	J1C1	Connector	80
SAS Module Connector	1	J4J1	Connector	80

8.2 Power Connectors

The main power supply connection uses an SSI-compliant 2x12 pin connector (J9H1).

Two additional power-related connectors also exist:

- One SSI-compliant 2x4 pin power connector (J9B1) to provide 12-V power to the CPU voltage regulators and memory.
- One SSI-compliant 1x5 pin connector (J9C3) to provide I2C monitoring of the power supply.

The following tables define these connector pin-outs:

Table 26. Main Power Connector Pin-out (J9H1)

Pin	Signal	Color	Pin	Signal	Color
1	+3.3 Vdc	Orange	13	+3.3 Vdc	Orange
2	+3.3 Vdc	Orange	14	-12 Vdc	Blue
3	GND	Black	15	GND	Black
4	+5 Vdc	Red	16	PS_ON#	Green
5	GND	Black	17	GND	Black
6	+5 Vdc	Red	18	GND	Black
7	GND	Black	19	GND	Black
8	PWR_OK	Gray	20	NC	White
9	5 VSB	Purple	21	+5 Vdc	Red
10	+12 Vdc	Yellow	22	+5 Vdc	Red
11	+12 Vdc	Yellow	23	+5 Vdc	Red
12	+3.3 Vdc	Orange	24	GND	Black

Table 27. CPU Power Connector Pin-out (J9B1)

Pin	Signal	Color
1	GND of Pin 5	Black
2	GND of Pin 6	Black
3	GND of Pin 7	Black
4	GND of Pin 8	Black
5	+12 Vdc CPU1	Yellow/black
6	+12 Vdc CPU1	Yellow/black
7	+12 Vdc DDR3_CPU1	Yellow/black
8	+12 Vdc DDR3_CPU1	Yellow/black

Table 28. Power Supply Auxiliary Signal Connector Pin-out (J9C3)

Pin	Signal	Color
1	SMB_CLK_FP_PWR_R	Orange
2	SMB_DAT_FP_PWR_R	Black
3	SMB_ALRT_3_ESB_R	Red
4	3.3 V SENSE-	Yellow
5	3.3 V SENSE+	Green

8.3 System Management Headers

8.3.1 Intel® Remote Management Module 4 Dedicated NIC Connector

A 30-pin Intel® RMM4 connector (J4C1) and a 7-pin Intel® RMM4 Lite connector (J4B1) are included on the server board to support the optional Intel® Remote Management Module 4 dedicated NIC module. This server board does not support third-party management cards.

Note: This connector is not compatible with the previous generation Intel® Remote Management Modules (Intel® RMM/RMM2/RMM3)

Table 29. Intel® RMM4 Dedicated NIC Module Connector Pin-out (J4C1)

Pin	Signal Name	Pin	Signal Name
1	3V3_AUX	2	MDIO
3	3V3_AUX	4	MDC
5	GND	6	TXD_0
7	GND	8	TXD_1
9	GND	10	TXD_2
11	GND	12	TXD_3
13	GND	14	TX_CTL
15	GND	16	RX_CTL
17	GND	18	RXD_0
19	GND	20	RXD_1
21	GND	22	RXD_2
23	GND	24	RXD_3

Pin	Signal Name	Pin	Signal Name
25	GND	26	TX_CLK
27	GND	28	RX_CLK
29	GND	30	PRESENT#

Table 30. Intel® RMM4 – Lite Connector Pin-out (J4B1)

Pin	Signal Name	Pin	Signal Name
1	3V3_AUX	2	SPI_RMM4_LITE_DI
3	KEY PIN	4	SPI_RMM4_LITE_CLK
5	SPI_RMM4_LITE_DO	6	GND
7	SPI_RMM4_LITE_CS_N	8	GND

8.3.2 TPM connector

Table 31. TPM connector Pin-out (J8J1)

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_CONN
11	LPC_LAD<3>	12	GND
13	GND	14	LPC_LAD<2>

8.3.3 Intel® ESRT2 RAID Upgrade Key Connector

The server board provides one connector to support Intel® ESRT2 RAID Upgrade Key. The I Upgrade Key is a small PCB board that enables RAID 5 software stack of ESRT2 SW RAID. The pin configuration of connector is identical and defined in the following table:

Table 32. Intel® ESRT2 RAID Upgrade Key Connector Pin-out (J4A1)

Pin	Signal Name
1	GND
2	FM_PBG_DYN_SKU_KEY
3	GND
4	FM_SSB_SAS_SATA_RAID_KEY

8.3.4 Local Control Panel Header

Table 33. LCP Header Pin-out (J1G1)

Pin	Signal Name
1	SMB_SENSOR_3V3STBY_DATA
2	GND
3	SMB_SENSOR_3V3STBY_CLK
4	P3V3_AUX
5	FM_LCP_ENTER_N

Pin	Signal Name
6	FM_LCP_LEFT_N
7	FM_LCP_RIGHT_N

8.3.5 HSBP_ I²C Header

Table 34. HSBP_ I²C Header Pin-out (J2K4)

Pin	Signal Name
1	SMB_HSBP_3V3STBY_DATA
2	GND
3	SMB_HSBP_3V3STBY_CLK

8.3.6 HDD LED Header

The server board includes a 2-pin hard drive activity LED header used with some SAS/SATA controller add-in cards. The header has the following pin-out.

Table 35. HDD LED Header Pin-out (J1G2)

Pin	Signal Name	Pin	Signal Name
1	LED_HDD_ACT_N	2	N/A

8.3.7 Chassis Intrusion Header

The server board includes a 2-pin chassis intrusion header which can be used when the chassis is configured with a chassis intrusion switch. The header has the following pin-out.

Table 36. Chassis Intrusion Header Pin-out (J1F1)

Header State	Description
Pins 1 and 2 closed	FM_INTRUDER_HDR_N is pulled HIGH. Chassis cover is closed.
Pins 1 and 2 open	FM_INTRUDER_HDR_N is pulled LOW. Chassis cover is removed.

8.3.8 SATA SGPIO Header

SGPIO uses a 5pin header, this is to incorporate a ground conductor as an SI improvement over previous generation products and based on measurement data indicating add the ground is strongly recommended. The 5pin connector will be consistent with other HSBPs, in this way cable commonality is improved.

Table 37. SATA SGPIO Header Pin-out (J2K2)

Pin	Signal Name
1	SCLK
2	SLOAD
3	GND
4	SDATAOUT0
5	SDATAOUT1

8.3.9 IPMB Connector

Table 38. IPMB Connector Pin-out (J2K1)

Pin	Signal Name
1	GND
2	P12V
3	FAN_PWM
4	FAN_TACH

8.4 Front Panel Connector

The server board provides a 24-pin front panel connector (J1E1) for use with Intel® and third-party chassis. The connector consists of a 24-pin SSI compatible front panel connector. The 24-pin SSI front panel connector provides various front panel features including:

- Power/Sleep Button
- System ID Button
- NMI Button
- NIC Activity LEDs
- Hard Drive Activity LEDs
- System Status LED
- System ID LED

The following table provides the pin-out for this connector:

Table 39. Front Panel 24-pin Connector Pin-out (J1E1)

Pin	Signal	Pin	Signal
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 (1/2) Activity LED
13	GND (Power Switch)	14	NIC#1 (1/2) Link LED
15	Reset Switch	16	I2C SDA
17	GND (Reset/ID/NMI Switch)	18	I2C 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

8.4.1 Power/Sleep Button and LED Support

Pressing the Power button will toggle the system power on and off. This button also functions as a sleep button if enabled by an ACPI compliant operating system. Pressing this button will send a signal to the integrated BMC, which will power on or power off the system. The power LED is a single color and is capable of supporting different indicator states as defined in the following table.

Table 40. Power/Sleep LED Functional States

State	Power Mode	LED	Description
Power-off	Non-ACPI	Off	System power is off, and the BIOS has not initialized the chipset.
Power-on	Non-ACPI	On	System power is on
S5	ACPI	Off	Mechanical is off, and the operating system has not saved any context to the hard disk.
S4	ACPI	Off	Mechanical is off. The operating system has saved context to the hard disk.
S3-S1	ACPI	Slow blink	DC power is still on. The operating system has saved context and gone into a level of low-power state.
S0	ACPI	Steady on	System and the operating system are up and running.

8.4.2 System ID Button and LED Support

Pressing the System ID Button will toggle both the ID LED on the front panel and the Blue ID LED on the server board on and off. The System ID LED is used to identify the system for maintenance when installed in a rack of similar server systems. The System ID LED can also be toggled on and off remotely using the *IPMI Chassis Identify* command which will cause the LED to blink for 15 seconds.

8.4.3 System Reset Button Support

When pressed, this button will reboot and re-initialize the system.

8.4.4 NMI Button Support

When the NMI button is pressed, it puts the server in a halt state and causes the BMC to issue a non-maskable interrupt (NMI). This can be useful when performing diagnostics for a given issue where a memory download is necessary to help determine the cause of the problem. 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:
- Receiving a *Chassis Control command* to pulse the diagnostic interrupt. This command does not cause an event to be logged in the SEL.

Watchdog timer pre-timeout expiration with NMI/diagnostic interrupt pre-timeout action enabled.

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

Table 41. NMI Signal Generation and Event Logging

Causal Event	NMI	
	Signal Generation	Front Panel Diag 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	X

8.4.5 NIC Activity LED Support

The Front Control Panel includes an activity LED indicator for each on-board Network Interface Controller (NIC). When a network link is detected, the LED will turn on solid. The LED will blink once network activity occurs at a rate that is consistent with the amount of network activity that is occurring.

8.4.6 Hard Drive Activity LED Support

The drive activity LED on the front panel indicates drive activity from the on-board hard disk controllers. The server board also provides a header giving access to this LED for add-in controllers.

8.4.7 System Status LED Support

The System Status LED is a bi-color (Green/Amber) indicator that shows the current health of the server system. The system provides two locations for this feature; one is located on the Front Control Panel, the other is located on the back edge of the server board, viewable from the back of the system. Both LEDs are tied together and will show the same state. The System Status LED states are driven by the on-board platform management sub-system.

8.5 I/O Connectors

8.5.1 VGA Connector

The following table details the pin-out definition of the VGA connector (J7A1).

Table 42. VGA Connector Pin-out (J7A1)

Pin	Signal Name	Description
1	V_IO_R_CONN	Red (analog color signal R)
2	V_IO_G_CONN	Green (analog color signal G)
3	V_IO_B_CONN	Blue (analog color signal B)
4	TP_VID_CONN_B4	No connection
5	GND	Ground
6	GND	Ground
7	GND	Ground
8	GND	Ground
9	P5V	+5V DC
10	GND	Ground
11	TP_VID_CONN_B11	No connection
12	V_IO_DDCDAT	DDCDAT
13	V_IO_HSYNC_CONN	HSYNC (horizontal sync)
14	V_IO_VSYNC_CONN	VSYNC (vertical sync)
15	V_IO_DDCCLK	DDCCLK

8.5.2 Display Port Connector

The following table details the pin-out definition of the Display Port connector (J8A1).

Table 43. Display Port Connector Pin-out (J8A1)

Pin	Signal Name	Description
1	OUT	ML_LANE 0 (P)
2	GND	Ground
3	OUT	ML_LANE 0 (N)
4	OUT	ML_LANE 1 (P)
5	GND	Ground
6	OUT	ML_LANE 1 (N)
7	OUT	ML_LANE 2 (P)
8	GND	Ground
9	OUT	ML_LANE 2 (N)
10	OUT	ML_LANE 3 (P)
11	GND	Ground
12	OUT	ML_LANE 3 (N)
13	GND	Ground
14	GND	Ground
15	I/O	AUX_CH (P)
16	GND	Ground
17	I/O	AUX_CH (N)
18	IN	HOT PLUG DETECT
19	PWR RTN	RETURN DP_PWR
20	PWR OUT	DP_PWR

8.5.3 SATA Connectors

The server board provides up to 6 SATA connectors: SATA-0 (J1K4), SATA-1 (J1K1), SATA-2 (J1K5), SATA-3 (J1K2), SATA-4 (J2K5), and SATA-5 (J2K3).

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

Table 44. SATA Connector Pin-out (J1K4, J1K1, J1K5, J1K2, J2K5, J2K3)

Pin	Signal Name
1	GND
2	TXP
3	TXN
4	GND
5	RXN
6	RXP
7	GND

8.5.4 Serial Port Connectors

The server board provides one external DB9 Serial A port (J9A1) and one internal 9-pin Serial B header (J9A2). The following tables define the pin-outs.

Table 45. External DB9 Serial A Port Pin-out (J9A1)

Pin	Signal Name	Description
1	SPA_DCD	DCD (carrier detect)
2	SPA_SIN_N	RXD (receive data)
3	SPA_OUT_N	TXD (Transmit data)
4	SPA_DTR	DTR (Data terminal ready)
5	GND	Ground
6	SPA_DSR	DSR (data set ready)
7	SPA_RTS	RTS (request to send)
8	SPA_CTS	CTS (clear to send)
9	SPA_RI	RI (Ring Indicate)

Table 46. Internal 9-pin Serial B Header Pin-out (J9A2)

Pin	Signal Name	Description
1	SPB_DCD	DCD (carrier detect)
2	SPB_DSR	DSR (data set ready)
3	SPB_SIN_N	RXD (receive data)
4	SPB_RTS	RTS (request to send)
5	SPB_OUT_N	TXD (Transmit data)
6	SPB_CTS	CTS (clear to send)
7	SPB_DTR	DTR (Data terminal ready)
8	SPB_RI	RI (Ring indicate)
9	GND	Ground
10	KEY PIN	No pin

8.5.5 USB Connector

One 2x5 connectors on the server board (J1K3) provides support for two additional USB 2.0 ports. J1K3 is recommended for front panel USB ports.

Table 47. Internal USB2.0 Connector Pin-out (J1K3)

Pin	Signal Name	Description
1	USB_PWR_5V	USB power
2	USB_PWR_5V	USB power
3	USB _PN_CONN	USB port negative signal
4	USB _PN_CONN	USB port negative signal
5	USB _PP_CONN	USB port positive signal
6	USB _PP_CONN	USB port positive signal
7	GND	Ground
8	GND	Ground
9	KEY PIN	No pin
10	TP_USB _NC	Test point

One 2x10 connectors on the server board (J1J1) provides support for two additional USB 3.0 ports. J1J1 is recommended for front panel USB ports.

Table 48. Internal USB3.0 Connector Pin-out (J1J1)

Pin	Signal	Description
1	Vbus	Power
2	IntA_P1_SSRX-	USB3 ICC Port1 SuperSpeed Rx-
3	IntA_P1_SSRX+	USB3 ICC Port1 SuperSpeed Rx+
4	GND	Ground
5	IntA_P1_SSTX-	USB3 ICC Port1 SuperSpeed Tx-
6	IntA_P1_SSTX+	USB3 ICC Port1 SuperSpeed Tx+
7	GND	Ground
8	IntA_P1_D-	USB3 ICC Port1 D- (USB2 Signal D-)
9	IntA_P1_D+	USB3 ICC Port1 D+ (USB2 Signal D+)
10	ID	Over Current Protection
11	IntA_P2_D+	USB3 ICC Port2 D+ (USB2 Signal D+)
12	IntA_P2_D-	USB3 ICC Port2 D- (USB2 Signal D-)
13	GND	Ground
14	IntA_P2_SSTX+	USB3 ICC Port2 SuperSpeed Tx+
15	IntA_P2_SSTX-	USB3 ICC Port2 Super Speed Tx-
16	GND	Ground
17	IntA_P2_SSRX+	USB3 ICC Port2 SuperSpeed Rx+
18	IntA_P2_SSRX-	USB3 ICC Port2 SuperSpeed Rx-
19	Vbus	Power
20	KEY PIN	No pin

The server board includes one 10-pin 2mm low-profile connector (J5K1) on the server boards provides an option to support a low-profile eUSB Solid State Drive.

Table 49. Pin-out of Internal Low-Profile USB Connector (eUSB) for Solid State Drive (J5K1)

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

The server board provides one additional Type A USB port (J1J4) to support the installation of a USB device inside the server chassis.

Table 50. Internal Type A USB Port Pin-out (J1J4)

Pin	Signal Name	Description
1	USB_PWR7_5V	USB_PWR
2	USB_PN	USB port negative signal
3	USB _PP	USB port positive signal
4	GND	Ground

8.5.6 I/O Module Connector

The following table details the pin-out definition of the I/O Module connector (J1C1).

Table 51. I/O Module Connector Pin-out (J1C1)

Pin	Signal Name	Pin	Signal Name
1	P3V3	2	P12V
3	P3V3	4	P12V
5	P3V3	6	P12V
7	P3V3	8	P12V
9	RSVD_PIN9	10	FRU_TEMP_ADDR
11	GND	12	P5V_AUX
13	RSVD_PIN13	14	FM_IOM_EN
15	RSVD_PIN15	16	P3V3_AUX
17	GND	18	LED _ACT_N
19	RSVD_PIN19	20	RPESENT_N
21	RSVD_PIN21	22	WAKE_N
23	GND	24	RESET_N
25	SMB_3V3SB_CLK	26	GND
27	SMB_3V3SB_DAT	28	CLK_100M_DP
29	GND	30	CLK_100M_DN
31	PE_TN_7	32	GND
33	PE_TP_7	34	PE_RN_7
35	GND	36	PE_RP_7
37	PE_TN_6	38	GND
39	PE_TP_6	40	PE_RN_6
41	GND	42	PE_RP_6
43	PE_TN_5	44	GND
45	PE_TP_5	46	PE_RN_5
47	GND	48	PE_RP_5
49	PE_TN_4	50	GND
51	PE_TP_4	52	PE_RN_4
53	GND	54	PE_RP_4
55	PE_TN_3	56	GND
57	PE_TP_3	58	PE_RN_3
59	GND	60	PE_RP_3
61	PE_TN_2	62	GND
63	PE_TP_2	64	PE_RN_2
65	GND	66	PE_RP_2
67	PE_TN_1	68	GND
69	PE_TP_1	70	PE_RN_1
71	GND	72	PE_RP_1
73	PE_TN_0	74	GND
75	PE_TP_0	76	PE_RN_0
77	GND	78	PE_RP_0
79	RSVD_PIN79	80	GND

8.5.7 SAS Module Connector

The following table details the pin-out definition of the SAS Module connector (J4J1).

Table 52. I/O Module Connector Pin-out (J4J1)

Pin	Signal Name	Pin	Signal Name
1	RSVD_PIN1	2	P12V
3	GND	4	P12V
5	PE_TP_7	6	P12V
7	PE_TN_7	8	GND
9	GND	10	PE_RP_7
11	PE_TP_6	12	PE_RN_7
13	PE_TN_6	14	GND
15	GND	16	PE_RP_6
17	PE_TP_5	18	PE_RN_6
19	PE_TN_5	20	GND
21	GND	22	PE_RP_5
23	PE_TP_4	24	PE_RN_5
25	PE_TN_4	26	GND
27	GND	28	PE_RP_4
29	PE_TP_3	30	PE_RN_4
31	PE_TN_3	32	GND
33	GND	34	PE_RP_3
35	PE_TP_2	36	PE_RN_3
37	PE_TN_2	38	GND
39	GND	40	PE_RP_2
41	PE_TP_1	42	PE_RN_2
43	PE_TN_1	44	GND
45	GND	46	PE_RP_1
47	PE_TP_0	48	PE_RN_1
49	PE_TN_0	50	GND
51	GND	52	PE_RP_0
53	SMD_3V3SB_DAT	54	PE_RN_0
55	SMD_3V3SB_CLK	56	GND
57	GND	58	RESET_N
59	RSVD_PIN59	60	WAKE_N
61	RSVD_PIN61	62	PRESENT_N
63	GND	64	LED_ACT_N
65	RSVD_PIN65	66	P3V3_AUX
67	RSVD_PIN67	68	FM_SAS_EN
69	GND	70	P5V_STBY
71	RSVD_PIN71	72	FRU_TEMP_ADDR
73	P3V3	74	P12V
75	P3V3	76	P12V
77	P3V3	78	P12V
79	P3V3	80	P12V

8.5.8 NIC1 with USB2.0 connector

Location: JA6A1

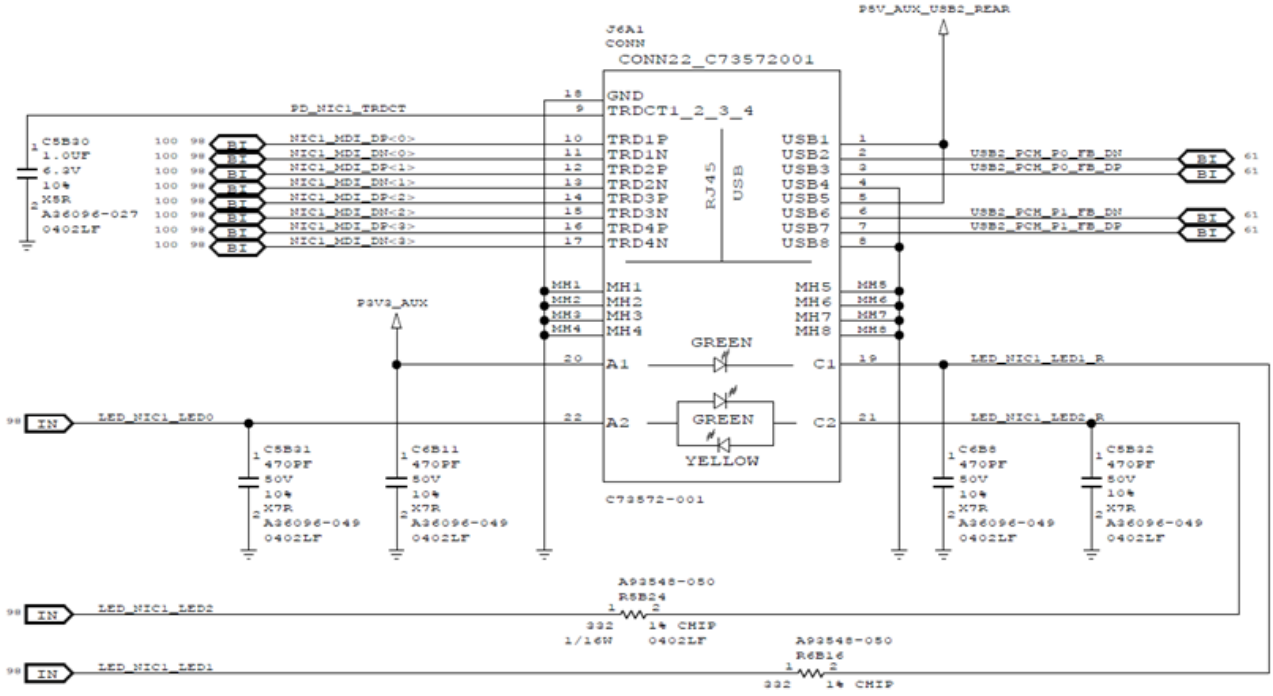


Figure 18. NIC1 with USB2.0 connector

8.5.9 NIC2 with USB3.0 connector

Location: JA5A1

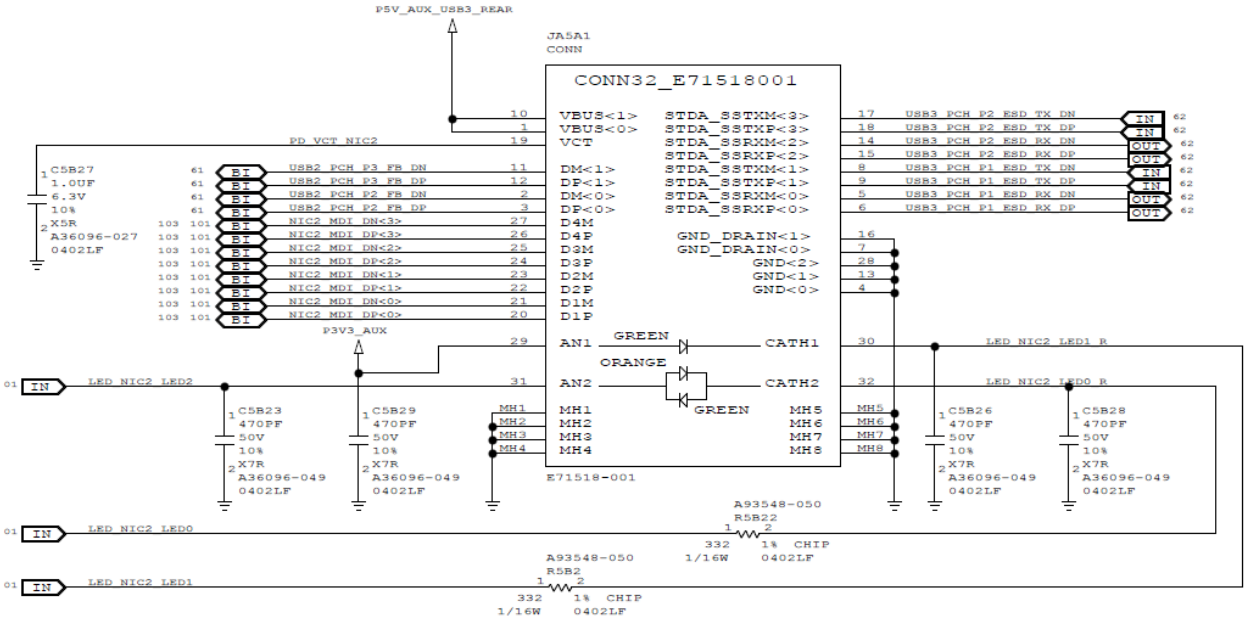


Figure 19. NIC2 with USB3.0 connector

8.6 Fan Headers

The server board provides five SSI-compliant 4-pin fans (J7K1, J3K4, J8K1, J8K2 and J8B1) to use as CPU and I/O cooling fans. 3-pin fans are supported on all fan headers. The pin configuration for each of the 4-pin fan headers is identical and defined in the following tables.

- One 4-pin fan header is designated as processor cooling fan:
  - CPU fan (J7K1)
- Three 4-pin fan headers are designated as system fans:
  - System fan 1 (J3K4)
  - System fan 2 (J8K1)
  - System fan 3 (J8K2)
- One 4-pin fan header is designated as a rear system fan:
  - System fan 4 (J8B1)

Table 53. SSI 4-pin Fan Header Pin-out (J7K1, J3K4, J8K1, J8K2, J8B1)

Pin	Signal Name	Type	Description
1	Ground	GND	Ground is the power supply ground
2	12V	Power	Power supply 12 V
3	Fan Tach Fan PWM	In Out	FAN_TACH signal is connected to the BMC to monitor the fan speed FAN_PWM signal to control fan speed
4	Fan PWM Fan Tach	Out In	FAN_PWM signal to control fan speed FAN_TACH signal is connected to the BMC to monitor the fan speed

Note: Intel Corporation server boards support peripheral components and can contain a number of high-density VLSI and power delivery components that need adequate airflow to cool. Intel's own chassis are designed and tested to meet the intended thermal requirements of these components when the fully integrated system is used together. It is the responsibility of the system integrator that 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 its published operating or non-operating limits.

9. BIOS Setup Interface

9.1 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 S1200V3RP 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 54. POST HotKeys Recognized

HotKey Combination	Function
<F2>	Enter Setup
<F6>	Pop up BIOS Boot Menu
<F12>	Network boot
<Esc>	Switch from Logo Screen to Diagnostic Screen
<Pause>	Stop POST temporarily

9.2 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

9.3 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.

9.4 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.

9.4.1 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.

9.4.1.1 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 55. 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, etc.
Keyboard Command Area	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

Functional Area	Description
	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 characters 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.

9.4.1.2 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.

9.4.1.3 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 56. 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.
↑	Select Item	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.

Key	Option	Description
↔	Select Menu	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.
<Tab>	Select Field	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.
-	Change Value	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.
<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.

9.4.1.4 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.

9.4.2 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 entry, 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.

9.4.2.1 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 57. Screen Map

Categories (Top Tabs)	2nd Level Screens	3rd Level Screens
Main Screen (Tab)		
Advanced Screen (Tab)		
↳	Processor Configuration	
↳		
↳	Memory Configuration	
	↳	
↳	Mass Storage Controller Configuration	
↳	PCI Configuration	
	↳	NIC Configuration
↳	Serial Port Configuration	
↳	USB Configuration	
↳	System Acoustic and Performance Configuration	
↳	Network Stack	

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

9.4.2.2 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.

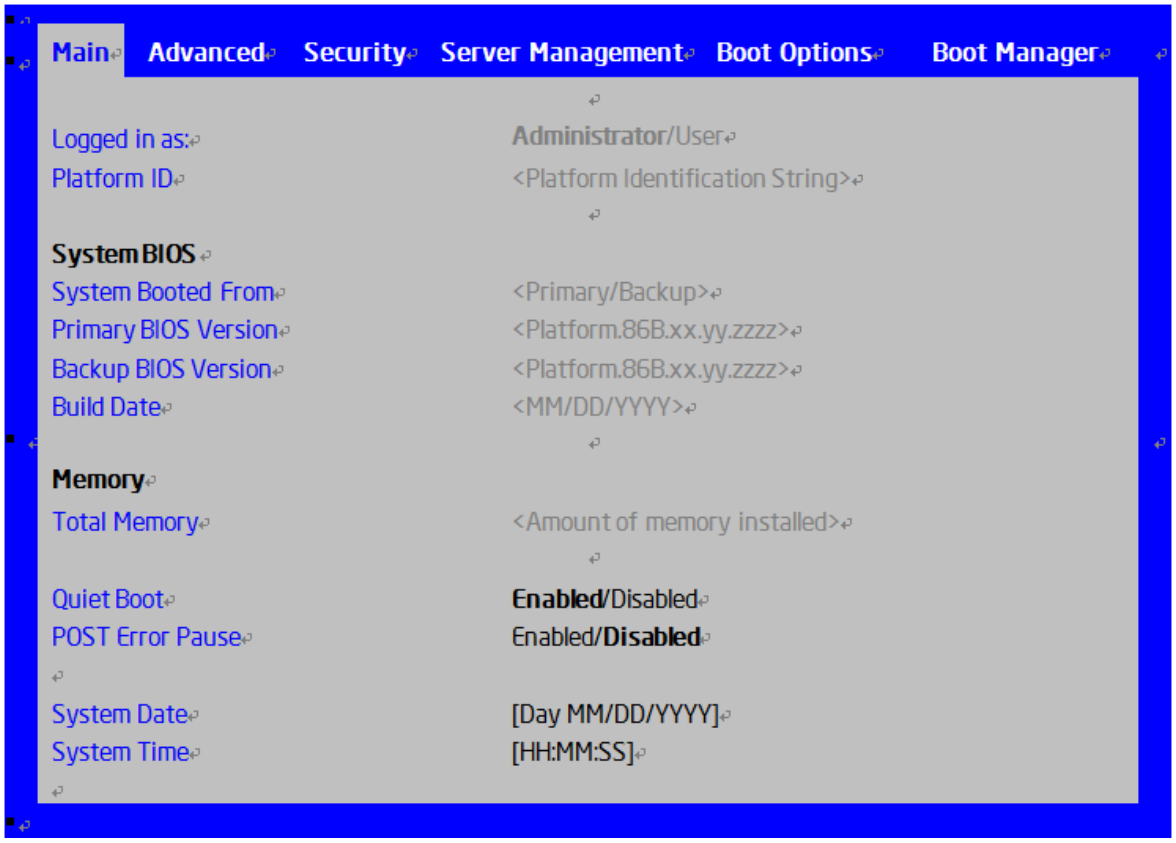


Figure 20. Main Screen

Screen Field Descriptions:

1. Logged in as:

   Option Values: *<Administrator / User>*

   Help Text: *<None>*

   Comments: *Information only.* Displays password level that setup is running in: Administrator or User. With no passwords set, Administrator is the default mode.

   Back to [Main Screen] — [Screen Map]

2. Platform ID

   Option Values: *< Platform ID>*

   Help Text: *<None>*

   Comments: *Information only.* Displays the Platform ID (Board ID) for the board on which the BIOS is executing POST.

   The Platform ID is limited to 8 characters, because it is also used in the ACPI Tables which have that limitation. In some cases, this means that the Platform ID is abbreviated from the marketing designation.

   Back to [Main Screen] — [Screen Map]

3. System Booted From

   Option Values: *< Primary/Backup>*

   Help Text: *<None>*

   Comments: *Information only*. Displays the exact BIOS portion on the board which is executing POST.

   Boot from Backup BIOS means the BIOS is running in Recovery mode and the Primary BIOS may be corrupted.

   Back to [Main Screen] — [Screen Map]

4. Primary BIOS Version

   Option Values: *<Current Primary BIOS version ID>*

   Help Text: *<None>*

   Comments: *Information only.* The primary BIOS version displayed uniquely identifies the primary BIOS 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 Intel Server BIOS

xx: Major Revision level of the BIOS

yy: Release Revision level for this BIOS

zzzz: Release Number for this BIOS

Back to [Main Screen] — [Screen Map]

5. Backup BIOS Version

   Option Values: *<Current Backup BIOS version ID>*

   Help Text: *<None>*

   Comments: *Information only.* The Backup BIOS version displayed uniquely identifies the backup 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 Intel Server BIOS

   xx: Major Revision level of the BIOS

   yy: Release Revision level for this BIOS

   zzzz: Release Number for this BIOS

   Back to [Main Screen] — [Screen Map]

6. Build Date

   Option Values: *<Date and time when the currently installed BIOS was created (built)>*

   Help Text: *<None>*

   Comments: *Information only.* The time and date displayed are taken from the timestamp segment of the BIOS ID String.

   Back to [Main Screen] — [Screen Map]

7. Total Memory

   Option Values: *<Amount of memory installed in the system>*

   Help Text: *<None>*

Comments: *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 DDR3 DIMMs.

Back to [Main Screen] — [Screen Map]

8. Quiet Boot

   Option Values: **Enabled**

   Disabled

   Help Text:

   [Enabled] – Display the logo screen during POST.

   [Disabled] – Display the diagnostic screen during POST.

   Comments: 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.

   Back to [Main Screen] — [Screen Map]

9. POST Error Pause

   Option Values: Enabled

   Disabled

   Help Text:

   [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.

   Comments: 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.

   Back to [Main Screen] — [Screen Map]

10. System Date

    Option Values: *<System Date initially displays the current system calendar date, including the day of the week>*

    Help Text:

    System Date has configurable fields for the current 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.

Comments: 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.

Back to [Main Screen] — [Screen Map]

11. System Time

Option Values: *<System Time initially displays the current system time of day, in 24-hour format>*

Help Text:

System Time has configurable fields for Hours, Minutes, and Seconds.

Hours are in 24-hour format.

Use the [Enter] or [Tab] key to select the next field.

Use the [+] or [-] key to modify the selected field.

Comments: 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 (although the time will be updated beginning from when it is reset early in POST).

Back to [Main Screen] — [Screen Map]

9.4.2.3 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.

This screen is the same for all board series, selecting between the same groups of options, although the options for different boards are not necessarily identical.

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.

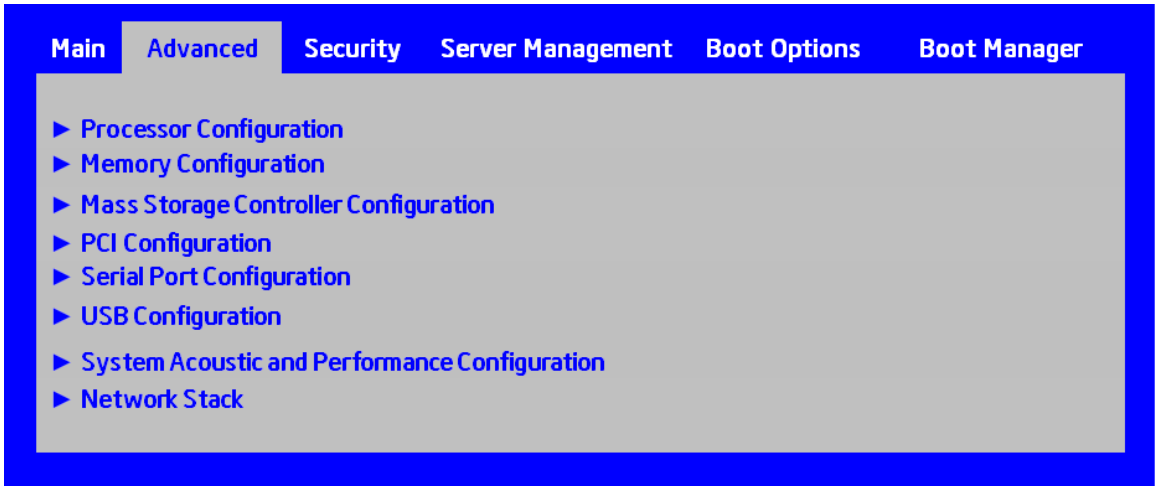


Figure 21. Advanced Screen

Screen Field Descriptions:

1. Processor Configuration

   Option Values: *<None>*

   Help Text:

   View/Configure processor information and settings.

   Comments: *Selection only.* Select this line and press the <Enter> key to go to the Processor Configuration group of configuration settings.

   Back to [Advanced Screen] — [Screen Map]

2. Memory Configuration

   Option Values: *<None>*

   Help Text:

   View/Configure memory information and settings.

   Comments: *Selection only.* Select this line and press the <Enter> key to go to the Memory Configuration group of configuration settings.

   Back to [Advanced Screen] — [Screen Map]

3. Mass Storage Controller Configuration

   Option Values: *<None>*

   Help Text:

   View/Configure mass storage controller information and settings.

Comments: *Selection only.* Select this line and press the <Enter> key to go to the Mass Storage Controller Configuration group of configuration settings.

Back to [Advanced Screen] — [Screen Map]

4. PCI Configuration

   Option Values: *<None>*

   Help Text:

   View/Configure PCI information and settings.

   Comments: *Selection only.* Select this line and press the <Enter> key to go to the PCI Configuration group of configuration settings.

   Back to [Advanced Screen] — [Screen Map]

5. Serial Port Configuration

   Option Values: *<None>*

   Help Text:

   View/Configure serial port information and settings.

   Comments: *Selection only.* Select this line and press the <Enter> key to go to the Serial Port Configuration group of configuration settings.

   Back to [Advanced Screen] — [Screen Map]

6. USB Configuration

   Option Values: *<None>*

   Help Text:

   View/Configure USB information and settings.

   Comments: *Selection only.* Select this line and press the <Enter> key to go to the USB Configuration group of configuration settings.

   Back to [Advanced Screen] — [Screen Map]

7. System Acoustic and Performance Configuration

   Option Values: *<None>*

   Help Text:

   View/Configure system acoustic and performance information and settings.

Comments: *Selection only.* Select this line and press the <Enter> key to go to the System Acoustic and Performance Configuration group of configuration settings.

Back to [Advanced Screen] — [Screen Map]

8. Network Stack

   Option Values: *<None>*

   Help Text:

   Network Stack Settings.

   Comments: *Selection only.* Select this line and press the <Enter> key to go to the Network Stack group of configuration settings.

   Back to [Advanced Screen] — [Screen Map]

9.4.2.4 Processor Configuration

The Processor Configuration screen displays the processor identification and microcode level, core frequency, cache sizes information 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.

The Processor Configuration screen will display different fields for single-socket, 2- socket and 4-socket boards shown as below Figures.

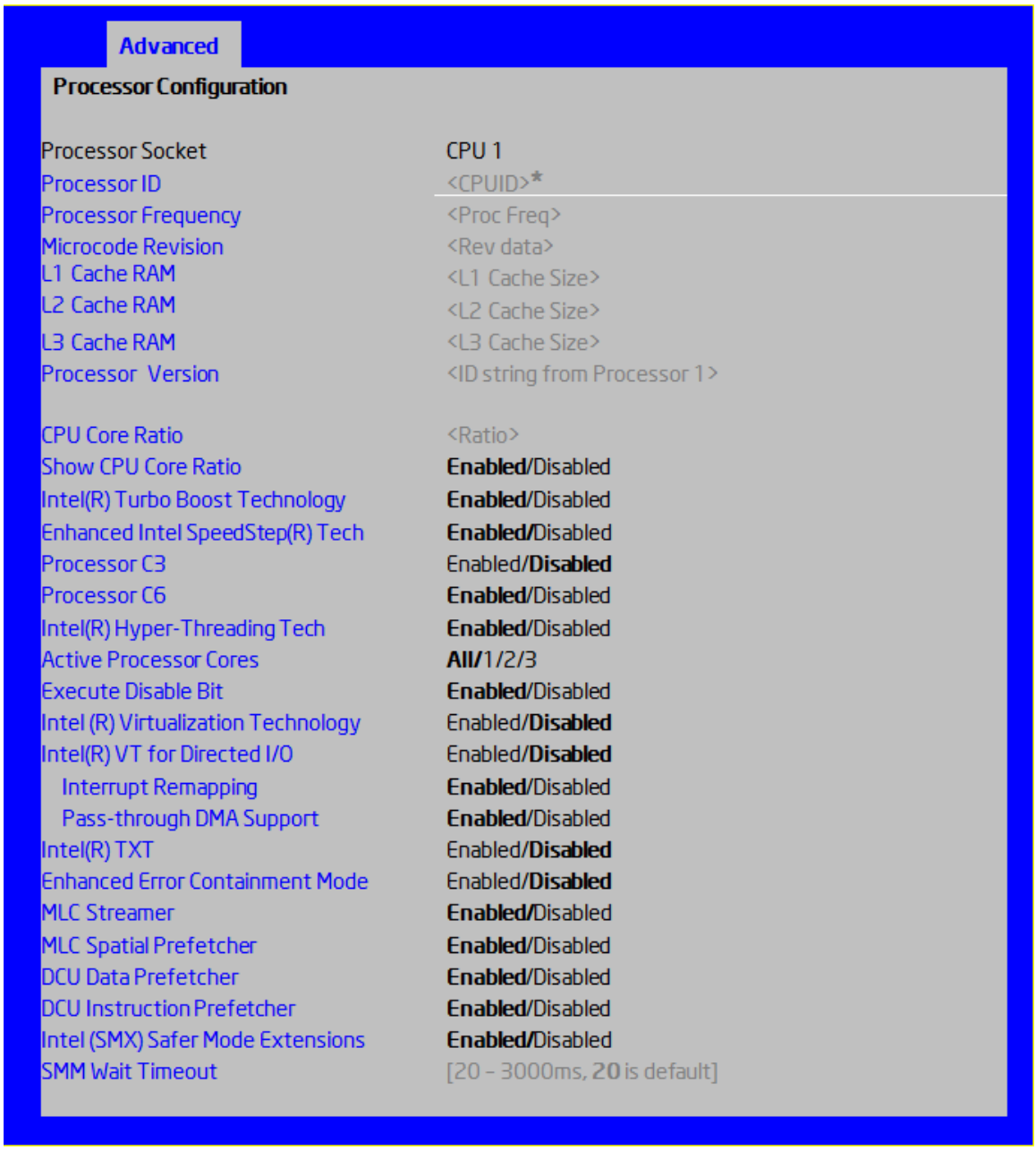


Figure 22. Processor Configuration Screen

Screen Field Descriptions:

1. Processor ID

   Option Values: *<CPUID>*

   Help Text: *<None>*

   Comments: *Information only.* Displays the Processor Signature value (from the CPUID instruction) identifying the type of processor and the stepping. S1200V3RP series boards have a single Processor ID display.

Back to [Advanced Screen] — [Screen Map]

2. Processor Frequency

   Option Values: *<Current Processor Operating Frequency>*

   Help Text: *<None>*

   Comments: *Information only.* Displays current operating frequency of the processor.

Back to [Advanced Screen] — [Screen Map]

3. Microcode Revision

   Option Values: *<Microcode Revision Number>*

   Help Text: *<None>*

   Comments: *Information only.* Displays Revision Level of the currently loaded processor microcode.

Back to [Advanced Screen] — [Screen Map]

4. L1 Cache RAM

   Option Values: *<L1 cache size>*

   Help Text: *<None>*

   Comments: *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.

Back to [Advanced Screen] — [Screen Map]

5. L2 Cache RAM

   Option Values: *<L2 cache size>*

   Help Text: *<None>*

   Comments: *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.

Back to [Advanced Screen] — [Screen Map]

6. L3 Cache RAM

   Option Values: *<L3 cache size>*

Help Text: *<None>*

Comments: *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.

Back to [Advanced Screen] — [Screen Map]

7. Processor Version

   Option Values: *<ID string from processor>*

   Help Text: *<None>*

   Comments: *Information only.* Displays Brand ID string read from processor with CPUID instruction.

   Back to [Advanced Screen] — [Screen Map]

8. CPU Core Ratio

   Option Values: [0 – 63]

   Help Text:

   Enter Core Ratio Multiplier. 0 - 63.

   Comments: In order for this option to be available, Show CPU Core Ratio must be Enabled.

   Back to [Advanced Screen] — [Screen Map]

9. Show CPU Core Ratio

   Option Values: Enabled

   Disabled

   Help Text:

   Allow Edits to Core Ratio Multiplier.

   Comments:

   Back to [Advanced Screen] — [Screen Map]

10. Intel(R) Turbo Boost Technology

    Option Values: **Enabled**

    Disabled

Help Text:

Intel(R) Turbo Boost Technology allows the processor to automatically increase its frequency if it is running below power, temperature, and current specifications.

Comments: This option is only visible if all processors installed in the system support Intel® Turbo Boost Technology. In order for this option to be available, Enhanced Intel® SpeedStep® Technology must be Enabled.

Back to [Advanced Screen] — [Screen Map]

11. Enhanced Intel SpeedStep(R) Tech

Option Values: **Enabled**

Disabled

Help Text:

Enhanced Intel SpeedStep (R) 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.

Comments: 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.

Back to [Advanced Screen] — [Screen Map]

12. Processor C3

Option Values: Enabled

Disabled

Help Text:

Enable/Disable Processor C3 (ACPI C2/C3) report to OS

Comments: This is normally Disabled but can be Enabled for improved performance on certain benchmarks and in certain situations.

Back to [Advanced Screen] — [Screen Map]

13. Processor C6

Option Values: **Enabled**

Disabled

Help Text:

Enable/Disable Processor C6 (ACPI C3) report to OS

Comments: This is normally Enabled but can be Disabled for improved performance on certain benchmarks and in certain situations.

Back to [Advanced Screen] — [Screen Map]

14. Intel(R) Hyper-Threading Tech

Option Values: **Enabled**

Disabled

Help Text:

Intel (R) 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.

Comments: This option is only visible if all processors installed in the system support Intel® Hyper-Threading Technology.

Back to [Advanced Screen] — [Screen Map]

15. Active Processor Cores

Option Values: **All**

1

2

3

4

5

6

7

Help Text:

Number of cores to enable in each processor package.

Comments: The numbers of cores that appear as selections depends on the number of cores available in the processors installed. Boards may have as many as 8 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.

Back to [Advanced Screen] — [Screen Map]

16. Execute Disable Bit

Option Values: **Enabled**

Disabled

Help Text:

Execute Disable Bit can help prevent certain classes of malicious buffer overflow attacks.

Contact your OS vendor regarding OS support of this feature.

Comments: 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.

Back to [Advanced Screen] — [Screen Map]

17. Intel (R) Virtualization Technology

Option Values: Enabled

Disabled

Help Text:

Intel (R) 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.

Comments: 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.

Back to [Advanced Screen] — [Screen Map]

18. Intel(R) VT for Directed I/O

    Option Values: Enabled

    Disabled

    Help Text:

    Enable/Disable Intel (R) Virtualization Technology for Directed I/O (Intel (R) VT-d).

    Report the I/O device assignment to VMM through DMAR ACPI Tables.

    Comments: 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.

    Back to [Advanced Screen] — [Screen Map]

19. Interrupt Remapping

    Option Values: **Enabled**

    Disabled

    Help Text:

    Enable/Disable Intel (R) VT-d Interrupt Remapping support. For some processors, this option may be "always enabled".

    Comments: 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.

    Back to [Advanced Screen] — [Screen Map]

20. Pass-through DMA Support

    Option Values: **Enabled**

    Disabled

    Help Text:

    Enable/Disable Intel (R) VT-d Pass-through DMA support. For some processors, this option may be "always enabled".

    Comments: 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.

Back to [Advanced Screen] — [Screen Map]

21. Intel(R) TXT

    Option Values: Enabled

    Disabled

    Help Text:

    Enable/Disable Intel(R) Trusted Execution Technology. Takes effect after reboot.

    Comments: Intel® TXT only appears when both Intel® Virtualization Technology and Intel® VT for Directed IO are enabled.

    This option appears only on models equipped with a TPM Module. The TPM Module must be active in order to support Intel® TXT.

    Note: Changing the setting for Intel® TXT will require the system to perform a Hard Reset in order for the new setting to become effective.

    Back to [Advanced Screen] — [Screen Map]

22. Enhanced Error Containment Mode

    Option Values: Enabled

    Disabled

    Help Text:

    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.

    Comments: 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.

    Back to [Advanced Screen] — [Screen Map]

23. MLC Streamer

    Option Values: **Enabled**

    Disabled

    Help Text:

MLC Streamer is a speculative prefetch unit within the processor(s).

Note: Modifying this setting may affect performance.

Comments: 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.

Back to [Advanced Screen] — [Screen Map]

24. MLC Spatial Prefetcher

Option Values: **Enabled**

Disabled

Help Text:

[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).

Comments: 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.

Back to [Advanced Screen] — [Screen Map]

25. DCU Data Prefetcher

Option Values: **Enabled**

Disabled

Help Text:

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).

Comments: 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.

Back to [Advanced Screen] — [Screen Map]

26. DCU Instruction Prefetcher

Option Values: **Enabled**

Disabled

Help Text:

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.

Comments: DCU Data Prefetcher is normally Enabled, for best efficiency in L1 Instruction Cache and Memory Channel use but disabling it may improve performance for some processing loads and on certain benchmarks.

Back to [Advanced Screen] — [Screen Map]

27. Intel (SMX) Safer Mode Extensions

Option Values: Enabled

Disabled

Help Text:

When Enabled, a SMX can utilize the additional hardware capabilities provided by Safer Mode Extensions.

Comments:

Back to [Advanced Screen] — [Screen Map]

28. SMM Wait Timeout

Option Values: *[Entry Field 20 – 3000ms, 20 is default]*

Help Text:

Millisecond timeout waiting for BSP and APs to enter SMM. Range is 20ms to 3000ms.

Comments: 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.

Back to [Advanced Screen] — [Screen Map]

9.4.2.5 Memory Configuration

The Memory Configuration screen allows the user to view details about the DDR3 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.

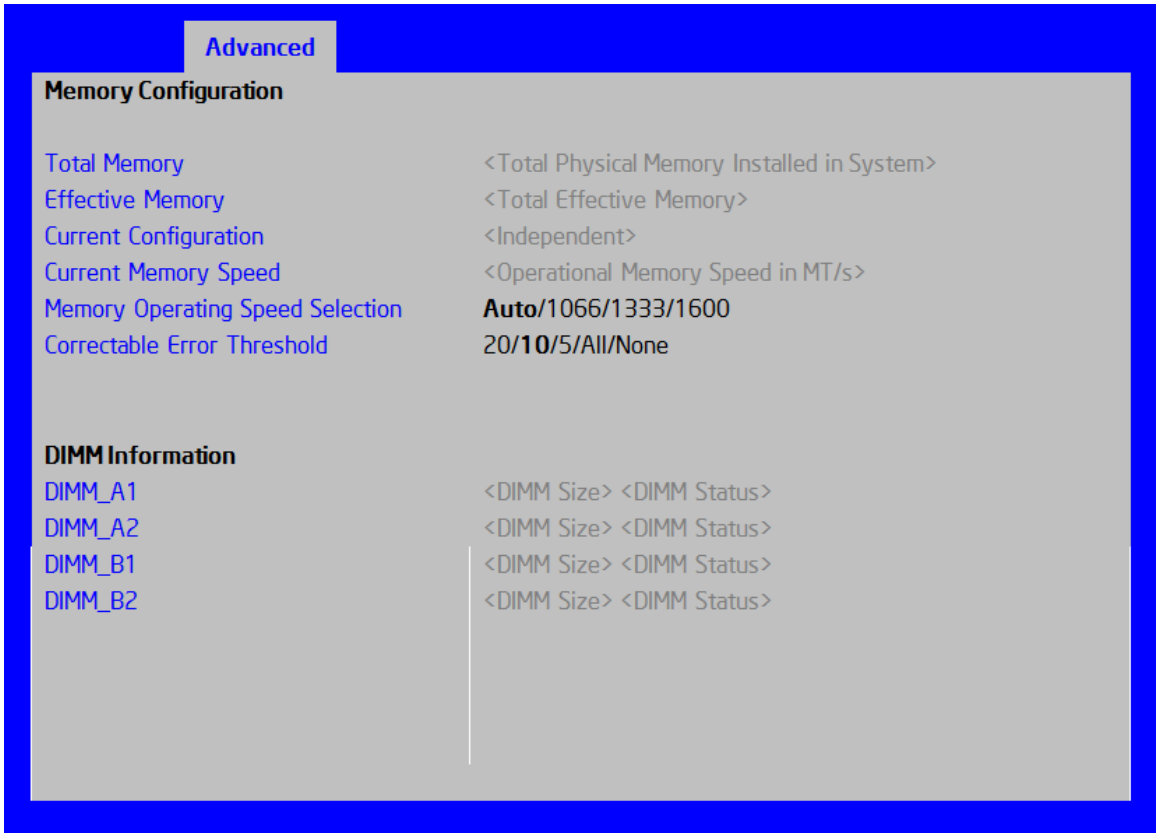


Figure 23. Memory Configuration Screen

Screen Field Descriptions:

1. Total Memory

   Option Values: *<Total Physical Memory Installed in System>*

   Help Text: *<None>*

   Comments: *Information only.* Displays the amount of memory available in the system in the form of installed DDR3 DIMMs, in units of GB.

   Back to [Memory Configuration Screen] — [Advanced Screen] — [Screen Map]

2. Effective Memory

   Option Values: *<Total Effective Memory>*

   Help Text: *<None>*

Comments: *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.

Back to [Memory Configuration Screen] — [Advanced Screen] — [Screen Map]

3. Current Memory Speed

   Option Values: *<Operational Memory Speed in MT/s>*

   Help Text: *<None>*

   Comments: *Information only.* Displays the speed in MT/s at which the memory is currently running.

   The supported memory speeds are 1066 MT/s, 1333 MT/s, and 1600 MT/s. The actual memory speed capability depends on the memory configuration.

   Back to [Memory Configuration Screen] — [Advanced Screen] — [Screen Map]

4. Memory Operating Speed Selection

   Option Values: **Auto**

   1066

   1333

   1600

   Help Text:

   Force specific Memory Operating Speed or use Auto setting.

   Comments: 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.

   1600 MT/s memory speed is available only on certain models.

   Back to [Memory Configuration Screen] — [Advanced Screen] — [Screen Map]

5. Correctable Error Threshold

   Option Values: 20

10

5

All

None

Help Text:

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.

Comments: 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.

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.

Back to [Memory Configuration Screen] — [Advanced Screen] — [Screen Map]

6. DIMM_A1
7. DIMM_A2
8. DIMM_B1
9. DIMM_B2

Help Text: *<None>*

Comments: *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 & Operational – There is a DDR3 DIMM installed and operational in this slot.
- Not Installed – There is no DDR3 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.

Note: In "DIMM_XY", X denotes the Channel Identifier A - P, and Y denotes the DIMM Slot identifier 1 - 3 within the Channel. DIMM_A2 is the DIMM socket on Channel A, Slot 2. Not all boards have the same number of channels and slots – this is dependent on the board features.

S1200V3RP boards can have DIMMs A1, A2 to B1, B2

Back to [Memory Configuration Screen] — [Advanced Screen] — [Screen Map]

9.4.2.6 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. This includes only onboard Mass Storage controllers. Mass Storage controllers on add-in cards are not included in this screen, nor are other storage mechanisms such as USB-attached storage devices or Network Attached Storage.

There is one types of onboard controller configured in this screen, the AHCI SATA controller with SATA drive support and RAID support. There are also informational displays of AHCI controller configuration, and SATA Drive Information when applicable. If the presence of an Intel® Storage Module is detected, the type of Storage Module is displayed as information-only.

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.

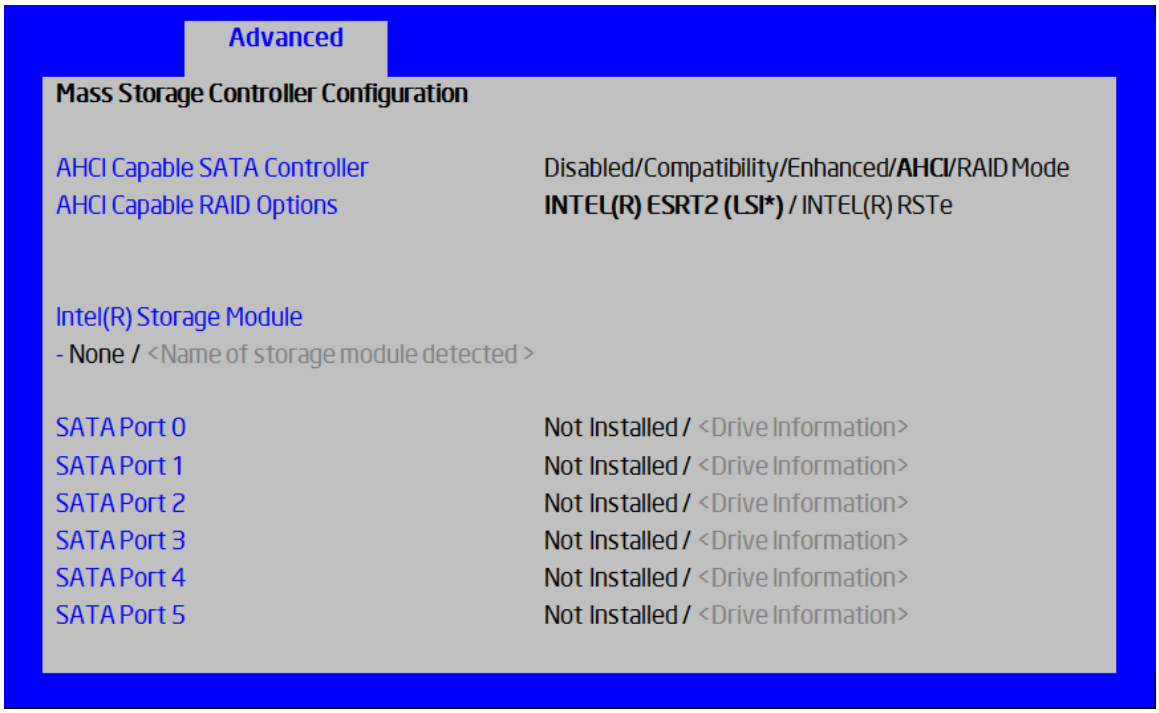


Figure 24. Mass Storage Controller Configuration Screen

Screen Field Descriptions:

1. AHCI Capable SATA Controller

   Option Values: Disabled

   Compatibility

   Enhanced

   AHCI

   RAID Mode

   Help Text:

   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

   Comments: This option configures the onboard AHCI-capable SATA controller. The number and type of ports it controls differs between board series.

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

Back to [Mass Storage Controller Configuration Screen] — [Screen Map]

2. AHCI Capable RAID Options

   Option Values: **Intel(R) ESRT2 (LSI*)**

   Intel(R) RSTe

   Help Text:

   Intel(R) ESRT2 (Powered by LSI): Supports RAID 0/1/10 and optional RAID 5 with Intel® RAID C220 Upgrade Keys. Uses Intel ESRT2 drivers (based on LSI* MegaSR).*

   Intel(R) RSTe: Provides pass-through drive support. Also provides host based RAID 0/1/10/5 support. Uses Intel(R) RSTe iastor drivers.

   Comments: 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.

   Note: This option does not appear on all boards.

   Back to [Mass Storage Controller Configuration Screen] — [Screen Map]

3. Intel(R) Storage Module

   Option Values: **None**

   <Name of Storage Module detected>

   Names of Storage Modules supported at this time are:

Intel(R) Integrated RAID Module

Intel(R) Integrated RAID Module RMS25PB040

Intel(R) Integrated RAID Module RMT3PB080

Intel(R) Integrated RAID Module RMS25CB080

Intel(R) Integrated RAID Module RMS25CB040

Intel(R) Integrated RAID Module RMT3CB080

Intel(R) Integrated RAID Module RMS25JB080

Intel(R) Integrated RAID Module RMS25JB040

Intel(R) Integrated RAID Module RMS25KB080

Intel(R) Integrated RAID Module RMS25KB040

Help Text: <None>

Comments: *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, etc.

Back to [Mass Storage Controller Configuration Screen] — [Screen Map]

4. SATA Port (For Port numbers 0-6)

   Option Values: **Not Installed**

   <Drive Information>

   Help Text: *<None>*

   Comments: *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.

   This Drive Information line is repeated for all 6 SATA Port for the onboard AHCI capable SATA Controller. However, for any given board, only the ports which are physically populated on the board are shown. That is, a board which only implements the two 6 GB/s ports 0 and 1 will only show those two ports in this Drive Information list.

   Back to [Mass Storage Controller Configuration Screen] — [Screen Map]

9.4.2.7 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 includes a selection option to go to the NIC Configuration screen.

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.

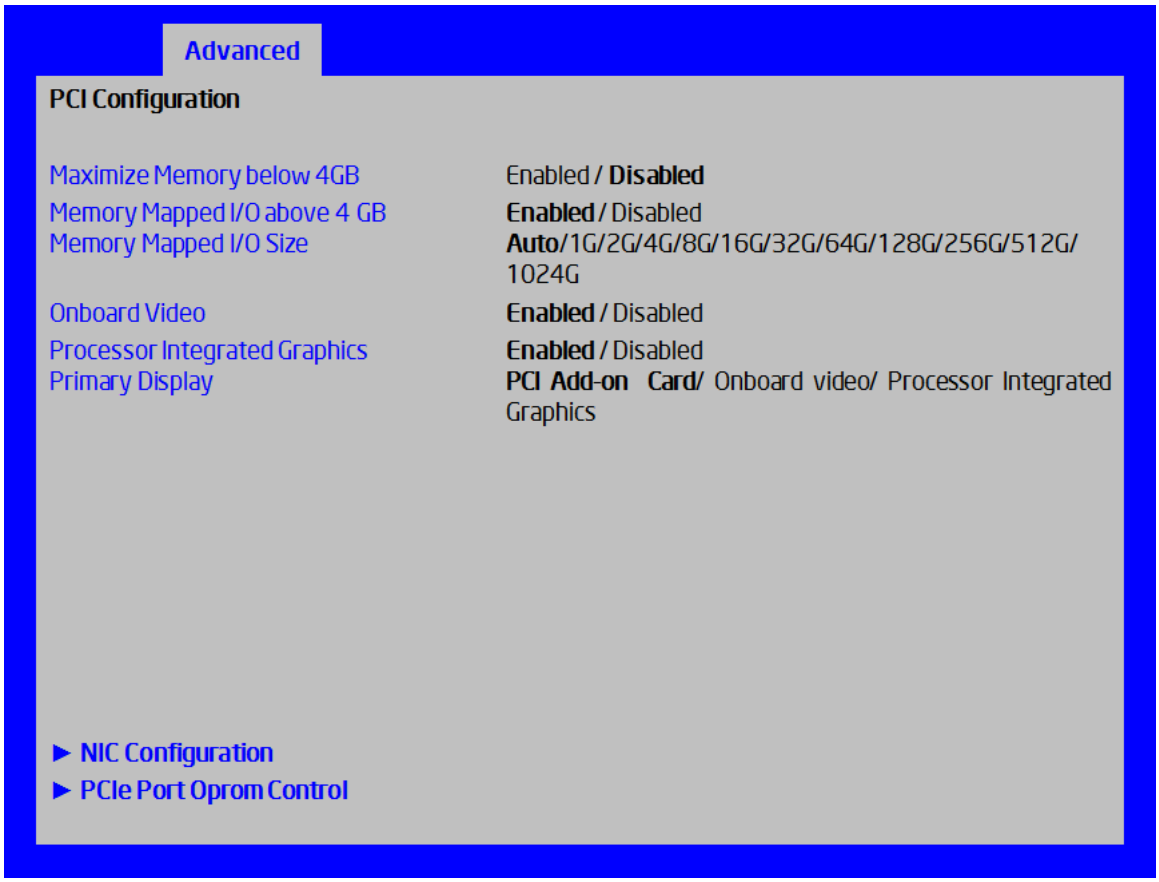


Figure 25. PCI Configuration Screen

Screen Field Descriptions:

1. Maximize Memory below 4GB

   Option Values: Enabled

   Disabled

   Help Text:

   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.

   Comments: 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. This option should only be enabled for a 32-bit OS without PAE capability or without PAE enabled.

Back to [PCI Configuration Screen] — [Advanced Screen] — [Screen Map]

2. Memory Mapped I/O above 4 GB

   Option Values: **Enabled**

   Disabled

   Help Text:

   Enable or disable memory mapped I/O of 64-bit PCI devices to 4 GB or greater address space.

   Comments: 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 4G.

   Back to [PCI Configuration Screen] — [Advanced Screen] — [Screen Map]

3. Memory Mapped I/O Size

   Option Values: **Auto**

   1G/2G/4G/8G/16G/32G/64G/128G/256G/512G/1024G

   Help Text:

   Sets MMIO Size: Auto -> 2G (default).

   Comments: 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.

   Back to [PCI Configuration Screen] — [Advanced Screen] — [Screen Map]

4. Onboard Video

   Option Values: **Enabled**

   Disabled

   Help Text:

   On-board video controller.

   Warning: System video is completely disabled if this option is disabled and an add-in video adapter is not installed and Processor Integrated graphics

Comments: When disabled, the system requires an add-in video card or Processor Integrated graphics for the video to be seen. When there is no add-in video card or Processor Integrated graphics installed, Onboard Video is set to Enabled and grayed out so it cannot be changed.

Back to [PCI Configuration Screen] — [Advanced Screen] — [Screen Map]

5. Processor Integrated Graphics

   Option Values: **Enabled**

   Disabled

   Help Text:

   Keep Processor Integrated Graphics enabled based on setup option.

   Comments: Processor Integrated Graphics is completely disabled if this option is disabled.

   Notes: This configuration page is only visible on RM SKU.

   Back to [PCI Configuration Screen] — [Advanced Screen] — [Screen Map]

6. Primary Display

   Option Values: **PCI Add-on Card**

   Onboard Video

   Processor Integrated graphics

   Help Text:

   Select which of Processor Integrated Graphics/Onboard Video/PCI Add-on Card Graphics device should be Primary Display or select SG for Switchable GFX.

   Comments:

   Back to [PCI Configuration Screen] — [Advanced Screen] — [Screen Map]

7. NIC Configuration

   Option Values: *<None>*

   Help Text:

   View/Configure NIC information and settings.

   Comments: *Selection only.* Select this line and press the <Enter> key to go to the NIC Configuration group of configuration settings.

Notes: This configuration page is not visible on some SKU.

Back to [PCI Configuration Screen] — [Advanced Screen] — [Screen Map]

9.4.2.8 NIC Configuration

The NIC Configuration screen allows the user to configure the NIC controller options for BIOS POST. It also displays the NIC MAC Addresses currently in use. This NIC Configuration screen handles network controllers built in on the baseboard ("onboard") or installed as an IO Module (IOM). It does not configure or report anything having to do with add-in network adapter cards.

To access this screen from the Main screen, select Advanced > PCI Configuration > NIC Configuration. 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.

There is usually one Onboard NIC built into the baseboard, although in some cases there are two Onboard NICs. There are several possible types of NICs which are incorporated into different boards. When an InfiniBand controller is on the baseboard, it appears as an Onboard NIC.

Most boards in this family also can have an IO Module that installs on the board in a specialized connector. There are boards which can have two IO Modules installed.

The descriptive names of the Onboard NIC types are:

Intel® I210 Dual-Port Gigabit Ethernet Controller

For boards with only one Onboard NIC, the "Onboard NIC2" entries are not present on the screen. The number of "Port" options which are displayed for each NIC will match the number of ports the Onboard NIC presents.

The IO Modules currently available are:

Intel® I350 Quad-Port Gigabit Ethernet Module

Intel® I540 Dual-Port X540 10 Gigabit RJ-45 Module

Intel® 82599 Dual-Port 10 Gigabit SFP+ Module

Intel® 82575EB Dual-Port Gigabit Module

Mellanox* ConnectX-3* Single-Port InfiniBand FD14 Module

For the IO Module entries on the NIC Configuration screen, only entries for modules which are currently installed will be appear, and only ports which exist on those IO Modules will appear.

If an IO Module which had been installed is no longer installed when the system is booted, all NIC Configuration entries which are specific to that IO Module will be reset to their default values and hidden. If a different IO Module is installed than had been previously installed, the module-specific settings will still be returned to defaults but not hidden. This will not necessarily

affect the Option ROM settings, which depend on the aggregate capabilities of all installed Onboard and IO Module NICs.

For each NIC port which is present on an Onboard NIC or IO Module other than InfiniBand controllers, there will be a port-specific PXE Boot enabling option and a MAC Address display. Onboard NICs and NIC ports also have enable/disable options. IO Modules and the ports on them cannot be disabled by BIOS.

InfiniBand controllers which appear as Onboard NICs or as IO Modules have a slightly different format. They do not have enable/disable options but they do have a choice of whether to enable loading and executing the embedded Option ROM for the controller, which will cause it to become bootable. For InfiniBand, both a GUID and a MAC Address are displayed. The GUID is used for InfiniBand Fabric operations, and the MAC Address is used when the controller is attached as an Ethernet device.

For non-InfiniBand NICs, there are different OPROMs for different protocols, which are also differentiated by speed, 1 Gb or 10 Gb. For a given protocol/speed, all Ethernet controllers of the same speed use the same Option ROM.

- PXE – there are two separate PXE Option ROMs, one for 1 Gb NICs and another for 10 Gb NICs. The two are independent of each other but each must be the only Option ROM enabled in its speed class. If 1 GbE PXE is enabled, then the iSCSI OPROM cannot be enabled. If 10 GbE PXE is enabled, then neither iSCSI nor 10 GbE FCoE may be enabled.
- iSCSI – there is only one iSCSI Option ROM for both 1 GbE and 10 GbE NICs. If iSCSI is enabled, then neither PXE nor FCoE OPROMs may be enabled for the 1 GbE or 10 GbE NICs.
- FCoE – there is a 10 GbE FCoE Option ROM that supports the Intel® 82599 NIC. When it is enabled, the iSCSI OPROM and the 10 GbE PXE OPROM must be disabled.

Note: These Option ROMs are only in support of onboard NICs and installed IO Modules. They do not support NICs on add-in network cards, even if the NIC on an add-in card is the same type of device as an onboard NIC or IO Module controller.

Only the Option ROMs for which controller capabilities are present are shown in the screen for selection. For example, if there are no 10 GbE NICs installed, then the 10 GbE OPROMs will not appear for selection. If controller capabilities are present but all controllers with those capabilities are disabled, then the relevant OPROM options will appear but will be disabled and grayed out and not changeable.

Similarly, when the PXE OPROM of a given speed is disabled, all PXE port enable/disable options using that OPROM will be disabled and grayed out. Conversely, if all ports are disabled for PXE, the PXE OPROM will be disabled and grayed out.

When a NIC Port is disabled, the PXE enable/disable option for it will be disabled and grayed out, and the MAC Address will be blank. When a NIC controller is disabled, all Ports and PXE options for that controller will become disabled and grayed out and all MAC Addresses for those ports will be blank. Conversely, if all ports for a given controller are disabled, the controller itself will appear as disabled.

Figure 26. NIC Configuration Screen

Screen Field Descriptions:

1. Wake on LAN (PME)

Option Values: **Enabled**

Disabled

Help Text:

Enables or disables PCI PME function for Wake on LAN capability from LAN adapters.

Comments: 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.

Back to [NIC Configuration Screen] — [PCI Configuration Screen] — [Advanced Screen] — [Screen Map]

2. PXE 1GbE Option ROM

Option Values: **Enabled**

Disabled

Help Text:

Enable/Disable Onboard/IOM NIC PXE Option ROM Load.

Comments: 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.

Back to [NIC Configuration Screen] — [PCI Configuration Screen] — [Advanced Screen] — [Screen Map]

3. PXE 10GbE Option ROM

Option Values: **Enabled**

Disabled

Help Text:

Enable/Disable Onboard/IOM NIC PXE Option ROM Load.

Comments: 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.

Back to [NIC Configuration Screen] — [PCI Configuration Screen] — [Advanced Screen] — [Screen Map]

4. FCoE 10GbE Option ROM

Option Values: Enabled

Disabled

Help Text:

Enable/Disable Onboard/IOM NIC FCoE Option ROM Load.

Comments: 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.

Back to [NIC Configuration Screen] — [PCI Configuration Screen] — [Advanced Screen] — [Screen Map]

5. iSCSI 1GbE/10GbE Option ROM

Option Values: Enabled

Disabled

Help Text:

Enable/Disable Onboard/IOM NIC iSCSI Option ROM Load.

Comments: 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.

Back to [NIC Configuration Screen] — [PCI Configuration Screen] — [Advanced Screen] — [Screen Map]

6. Onboard NIC1 Type

7. Onboard NIC2 Type

Option Values: *<Onboard NIC Description>*

string:

Intel(R) I210 Dual-Port Gigabit Ethernet Controller

Help Text: *<None>*

Comments: *Information only.* This is a display showing which NICs are available as Network Controllers integrated into the baseboard. Each of these Onboard 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.

If a board only has one onboard NIC, the second NIC Type and following options section will not appear.

Back to [NIC Configuration Screen] — [PCI Configuration Screen] — [Advanced Screen] — [Screen Map]

8. IO Module 1 Type

9. IO Module 2 Type

Option Values: *<IO Module Description>*

One of these strings:

Intel(R) I350 Quad-Port Gigabit Ethernet Module

Intel(R) I540 Dual-Port X540 10 Gigabit RJ-45 Module

Intel(R) 82599 Dual-Port 10 Gigabit SFP+ Module

Mellanox ConnectX-3* Single-Port InfiniBand FD14 Module*

Help Text: *<None>*

Comments: *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.

This descriptive screen image shows an example of an InifiniBand controller as IOM1. In a system with two IO Module connectors, an InfiniBand IO Module might be installed as either IOM1 or IOM2.

Most boards have only one IO Module connector. In any case, an IO Module Type and following options section will only appear when an IO Module is installed, and a second IO Module Type and options section will only appear if there are two IO Modules installed.

Back to [NIC Configuration Screen] — [PCI Configuration Screen] — [Advanced Screen] — [Screen Map]

10. NIC1 Controller

11. NIC2 Controller

    Option Values: **Enabled**

    Disabled

    Help Text:

    Enable/Disable Onboard Network Controller.

    Comments: This will completely disable Onboard Network Controller NIC1 or NIC2, 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.

    This option only appears for onboard Ethernet controllers. It does not appear for onboard InfiniBand controllers.

    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.

    Back to [NIC Configuration Screen] — [PCI Configuration Screen] — [Advanced Screen] — [Screen Map]

12. NIC2 InfiniBand Option ROM

13. IOM1 InfiniBand Option ROM

14. IOM2 InfiniBand Option ROM

    Option Values: Enabled

    Disabled

    Help Text:

    Enable/Disable InfiniBand Controller Option ROM and FlexBoot.

    Comments: 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 Onboard or IO Module InfiniBand controllers. It does not appear for Ethernet controllers.

    Back to [NIC Configuration Screen] — [PCI Configuration Screen] — [Advanced Screen] — [Screen Map]

15. NIC2 Port1 GUID

16. IOM1 Port1 GUID

17. IOM2 Port1 GUID

    Option Values: *<GUID Display>*

    Help Text: *<None>*

    Comments: *Information only.* 16 hex digits of the Port1 GUID of the InfiniBand controller for NIC2, IOM1, or IOM2.

    Back to [NIC Configuration Screen] — [PCI Configuration Screen] — [Advanced Screen] — [Screen Map]

18. NIC1 Port1 PXE

19. NIC2 Port1 PXE

20. IOM1 Port1 PXE

21. IOM1 Port2 PXE

22. IOM1 Port3 PXE

23. IOM1 Port4 PXE

24. IOM2 Port1 PXE

25. IOM2 Port2 PXE

26. IOM2 Port3 PXE

27. IOM2 Port4 PXE

    Option Values: **Enabled**

    Disabled

    Help Text:

    Enable/Disable Onboard/IOM NIC Port PXE Boot

    Comments: This will enable or disable PXE Boot capability for Port<x, x = 1-4> of Onboard NIC<n, n = 1-2> or IO Module<n, n = 1-2>.

    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 a particular NIC or 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 NICs or 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.

    Back to [NIC Configuration Screen] — [PCI Configuration Screen] — [Advanced Screen] — [Screen Map]

28. NIC1 Port1 MAC Address

29. NIC2 Port1 MAC Address

30. IOM1 Port1 MAC Address

31. IOM1 Port2 MAC Address

32. IOM1 Port3 MAC Address

33. IOM1 Port4 MAC Address

34. IOM2 Port1 MAC Address

35. IOM2 Port2 MAC Address

36. IOM2 Port3 MAC Address

37. IOM2 Port4 MAC Address

    Option Values: *<Mac Address Display>*

    Help Text: *<None>*

    Comments: *Information only.* 12 hex digits of the MAC address of Port1- Port4 of the Network Controller corresponding to NIC1, NIC2, IOM1, or IOM2.

    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.

    Back to [NIC Configuration Screen] — [PCI Configuration Screen] — [Advanced Screen] — [Screen Map]

9.4.2.9 Serial Port Configuration

The Serial Port Configuration screen allows the user to configure the Serial A and Serial B ports. In Legacy ISA nomenclature, these are ports COM1 and COM2 respectively.

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.

The primary usage for these serial ports is to enable Serial Console Redirection and Serial Over LAN (SOL) capabilities. Either port can be used for Serial Console Redirection but SOL is only supported on Serial A.

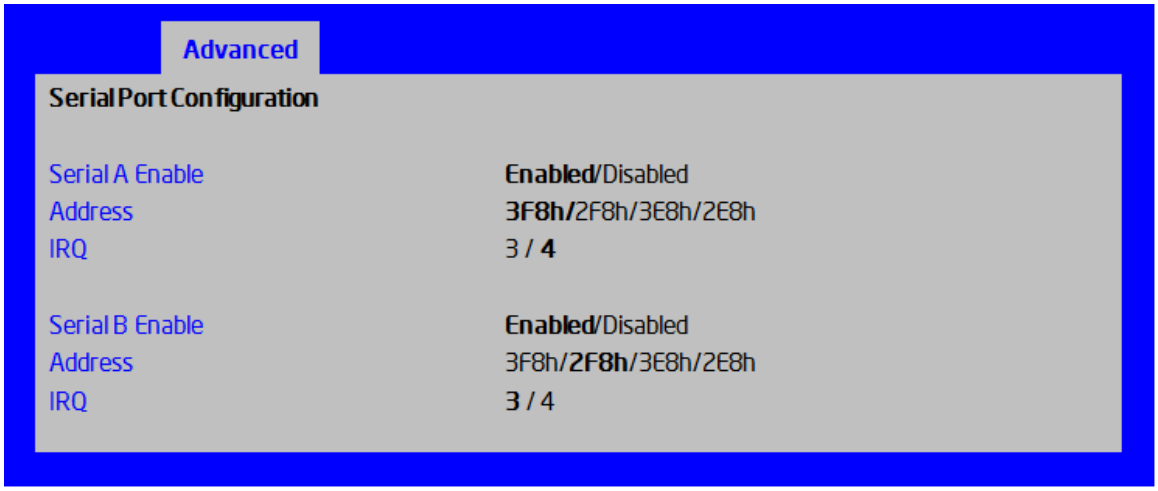


Figure 27. Serial Port Configuration Screen

Screen Field Descriptions:

1. Serial A Enable

Option Values: **Enabled**

Disabled

Help Text:

Enable or Disable Serial port A.

Comments: Serial Port A can be used for either Serial Over LAN or Serial Console Redirection.

Back to [Serial Port Configuration Screen] — [Screen Map]

2. Address

Option Values: **3F8h**

2F8h

3E8h

2E8h

Help Text:

Select Serial port A base I/O address.

Comments: Legacy I/O port address. This field should not appear when Serial A port enable/disable does not appear.

Back to [Serial Port Configuration Screen] — [Screen Map]

3. IRQ

Option Values: 3

4

Help Text:

Select Serial port A interrupt request (IRQ) line.

Comments: *Legacy IRQ.* This field should not appear when Serial A port enable/disable does not appear.

Back to [Serial Port Configuration Screen] — [Screen Map]

4. Serial B Enable

Option Values: **Enabled**

Disabled

Help Text:

Enable or Disable Serial port B.

Comments: Serial Port B can be used for Serial Console Redirection.

Back to [Serial Port Configuration Screen] — [Screen Map]

5. Address

Option Values: 3F8h

2F8h

3E8h

2E8h

Help Text:

Select Serial port B base I/O address.

Comments: Legacy I/O port address.

Back to [Serial Port Configuration Screen] — [Screen Map]

6. IRQ

Option Values: **3**

4

Help Text:

Select Serial port B interrupt request (IRQ) line.

Comments: *Legacy IRQ*

Back to [Serial Port Configuration Screen] — [Screen Map]

9.4.2.10 USB Configuration

The USB Configuration screen allows the user to configure the available 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.

This screen should display all USB Mass Storage devices which have been detected in the system. These include USB-attached Hard Disk Drives (HDDs), Floppy Disk Drives (FDDs), CDROM and DVDROM drives, and USB Flash Memory devices (USB Key, Keyfob, etc).

Each USB Mass Storage device may be set to allow the media emulation for which it is formatted, or an emulation may be specified. For USB Flash Memory devices in particular, there are some restrictions:

- A USB Key formatted as a CDROM drive will be recognized as an HDD.
- A USB Key formatted without a Partition Table will be forced to FDD emulation.
- A USB Key formatted with one Partition Table, and less than 528 MB in size, will be forced to FDD emulation – otherwise if it is 528 MB or greater in size, it will be forced to HDD emulation.

Note: USB devices can be "hotplugged" during POST, and will be detected and "beeped". They will be enumerated and displayed on this screen, though they may not be enumerated as bootable devices.

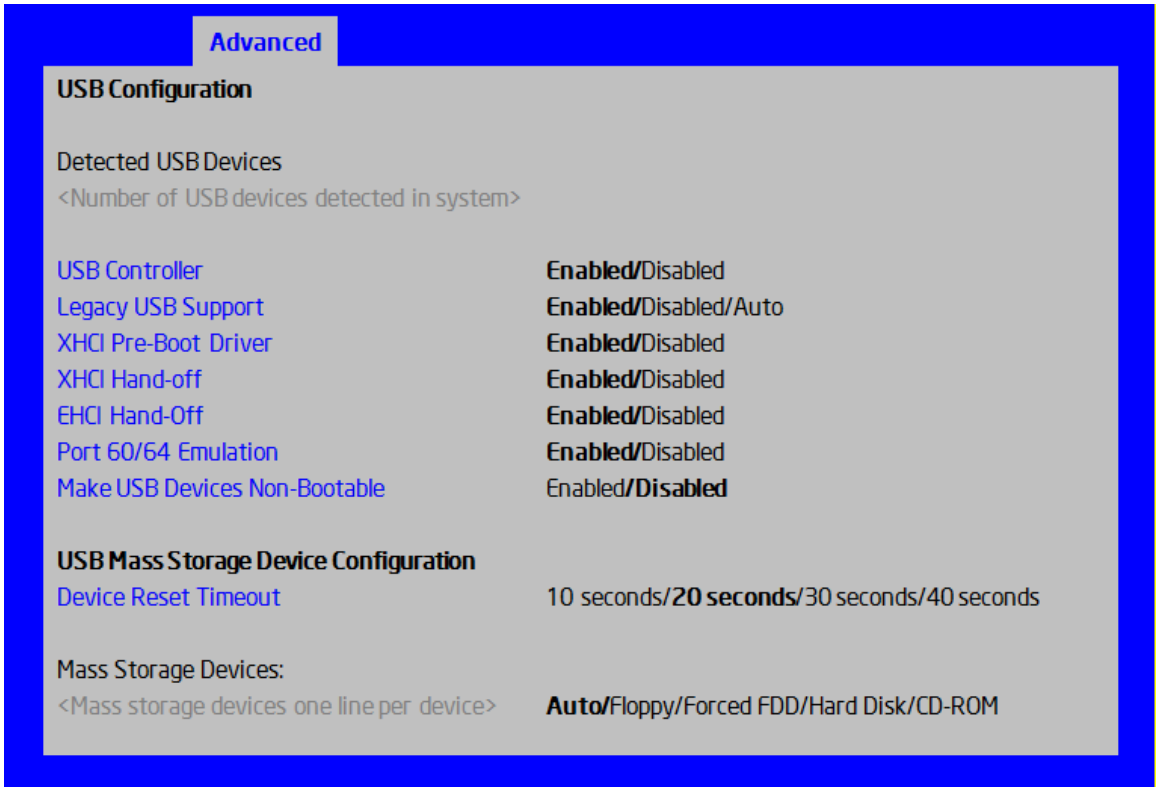


Figure 28. USB Configuration Screen

Screen Field Descriptions:

1. Detected USB Devices

   Option Values: *<Number of USB devices detected in system>*

   Help Text: *<None>*

Comments: *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 mice detected from the BMC KVM function under this item even no USB devices connected to the system.

Back to [USB Configuration Screen] — [Screen Map]

2. USB Controller

Option Values: **Enabled**

Disabled

Help Text:

[Enabled] - All on-board USB controllers are turned on and accessible by the OS.

[Disabled] - All on-board USB controllers are turned off and inaccessible by the OS.

Comments: 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.

Back to [USB Configuration Screen] — [Screen Map]

3. Legacy USB Support

Option Values: **Enabled**

Disabled

Auto

Help Text:

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.

Comments: 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.

Back to [USB Configuration Screen] — [Screen Map]

4. XHCI Pre-Boot Driver

Option Values: **Enabled**

Disabled

Help Text:

Enable/Disable XHCI Pre-Boot Driver support

Comments: If the USB controller setting is Disabled, this field is grayed out and inactive.

Back to [USB Configuration Screen] — [Screen Map]

5. XHCI Hand-off

Option Values: **Enabled**

Disabled

Help Text:

This is a workaround for OSes without XHCI hand-off support. The XHCI ownership change should be claimed by XHCI driver

Comments: If the USB controller setting is Disabled, this field is grayed out and inactive.

Back to [USB Configuration Screen] — [Screen Map]

6. EHCI Hand-off

Option Values: **Enabled**

Disabled

Help Text:

This is a workaround for OSes without EHCI hand-off support. The XHCI ownership change should be claimed by EHCI driver

Comments: If the USB controller setting is Disabled, this field is grayed out and inactive.

Back to [USB Configuration Screen] — [Screen Map]

7. Port 60/64 Emulation

Option Values: **Enabled**

Disabled

Help Text:

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.

Comments: If the USB controller setting is Disabled, this field is grayed out and inactive.

Back to [USB Configuration Screen] — [Screen Map]

8. Make USB Devices Non-Bootable

   Option Values: **Enabled**

   Disabled

   Help Text:

   Exclude USB in Boot Table.

   [Enabled]- This will remove all USB Mass Storage devices as Boot options.

   [Disabled] - This will allow all USB Mass Storage devices as Boot options.

   Comments: *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.

   Back to [USB Configuration Screen] — [Screen Map]

9. Device Reset Timeout

   Option Values: 10 seconds

   20 seconds

   30 seconds

   40 seconds

   Help Text:

   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.

   Comments: If the USB controller setting is Disabled, this field is grayed out and inactive.

   Back to [USB Configuration Screen] — [Screen Map]

10. Mass Storage Devices:

    Option Values: **Auto**

    Floppy

    Forced FDD

    Hard Disk

    CD-ROM

    Help Text:

    [Auto] - USB devices less than 530 MB are emulated as floppies.

    [Forced FDD] - HDD formatted drive is emulated as an FDD (e.g., ZIP drive).

    Comments: 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.

Back to [USB Configuration Screen] — [Screen Map]

9.4.2.11 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.

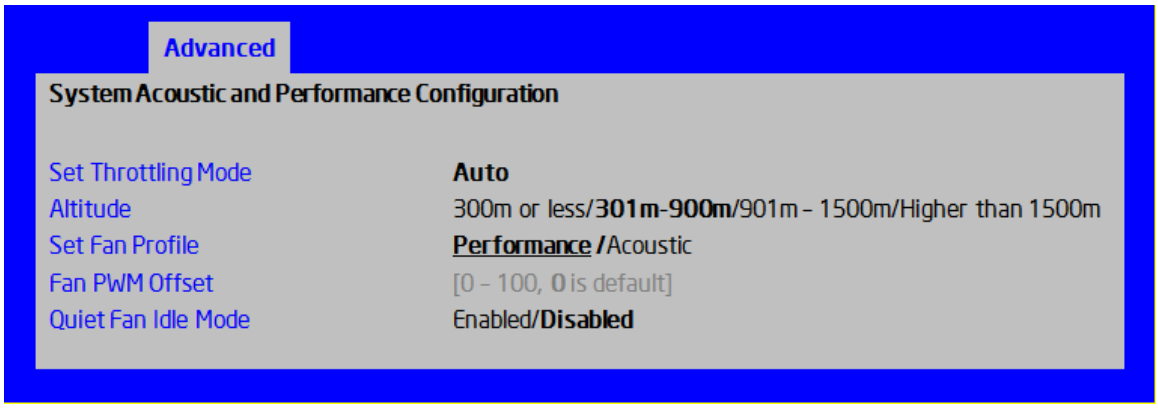


Figure 29. System Acoustic and Performance Configuration Screen

Screen Field Descriptions:

1. Set Throttling Mode

   Option Values: **Auto**

   Help Text:

   Sets Thermal Throttling mode for memory, to control fans and DRAM power as needed to control DIMM temperatures.

   [Auto] – Auto Throttling Mode

   [CLTM] - Closed Loop Thermal Management.

   [OLTM] - Open Loop Thermal Management.

   Closed Loop Thermal Management is supported only when ECC DIMM plugged. Open Loop Thermal Management is not supported.

   Comments: 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.

   - CLTM 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.

   - OLTM 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.

   Back to [System Acoustic and Performance Configuration] — [Screen Map]

2. Altitude

   Option Values: 300m or less

   301m-900m

   901m-1500m

   Higher than 1500m

   Help Text:

   [300m or less](980ft or less) Optimal near sea level.

   [301m-900m](980ft-2950ft) Optimal performance setting at moderate elevation.

   [901m-1500m](2950ft-4920ft) Optimal performance setting at high elevation.

[Above 1500m](above 4920ft) Optimal performance setting at the highest elevations.

Comments: This 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.

Back to [System Acoustic and Performance Configuration] — [Screen Map]

3. Set Fan Profile

Option Values: **Performance**

Acoustic

Help Text:

[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.

Comments: 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.

Back to [System Acoustic and Performance Configuration] — [Screen Map]

4. Fan PWM Offset

Option Values: *[Entry Field 0 – 100, 0 is default]*

Help Text:

Valid Offset 0 - 100.This number is added to the calculated PWM value to increase Fan Speed.

Comments: 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.

Back to [System Acoustic and Performance Configuration] — [Screen Map]

5. Quiet Fan Idle Mode

Option Values: Enabled

Disabled

Help Text:

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.

Comments: 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.

Quiet Fan Idle Mode does not conflict with Fan PWM Offset (above) – they work in concert, with Fan PWM Offset applied to fans in Quiet Fan Idle Mode just as when the fans are operating in "normal mode". A Fan PWM Offset of zero is necessary for fans to actually stop turning.

Back to [System Acoustic and Performance Configuration] — [Screen Map]

9.4.2.12 Network Stack

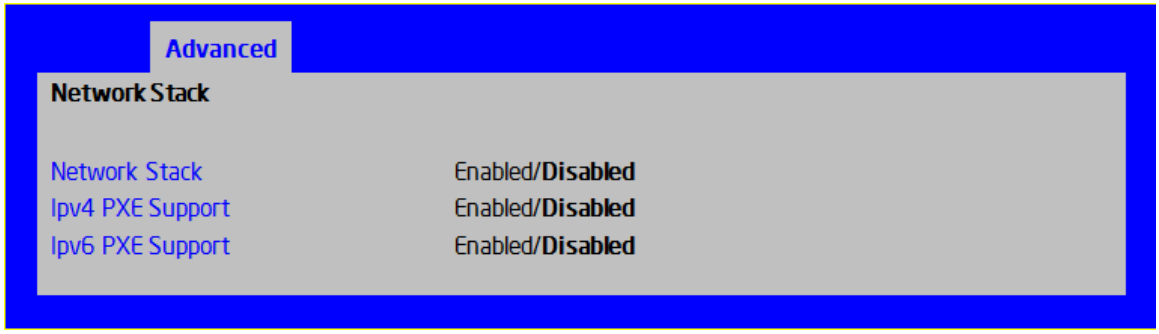


Figure 30. Network Stack Screen

Screen Field Descriptions:

1. Network Stack

Option Values: Enabled

Disabled

Help Text:

Enable/Disable UEFI network stack

Comments:

Back to [System Acoustic and Performance Configuration] — [Screen Map]

2. Ipv4 PXE support

   Option Values: Enabled

   Disabled

   Help Text:

   Enable Ipv4 PXE Boot Support. If disabled IPV4 PXE boot option will not be created.

   Comments:

   Back to [System Acoustic and Performance Configuration] — [Screen Map]

3. Ipv6 PXE support

   Option Values: Enabled

   Disabled

   Help Text:

   Enable Ipv6 PXE Boot Support. If disabled IPV6 PXE boot option will not be created

   Comments:

   Back to [System Acoustic and Performance Configuration] — [Screen Map]

9.4.2.13 Security Screen (Tab)

The Security screen allows the user to enable and set the Administrator and User passwords and to lock out the front panel buttons so 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.

Note that it is necessary to activate the TPM in order be able to enable Intel® Trusted Execution Technology (TXT) on boards that support it. Changing the TPM state in Setup will require a Hard Reset for the new state to become effective.

This BIOS supports (but does not require) “Strong Passwords” for security. The “Strong Password” criteria for both Administrator and User passwords require that passwords be between 8 and 14 characters at length, and a password must contain at least one case-sensitive alphabetic character, one numeric character, and one special character. A warning is given when a password is set which does not meet the Strong Password criteria but the password is accepted.

For further security, the BIOS optionally may require a Power on Password to be entered in early POST in order to boot the system. When Power On Password is enabled, POST is halted

soon after power on while the BIOS queries for a Power On Password. Either the Administrator or the User password may be entered for a Power on Password.

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.

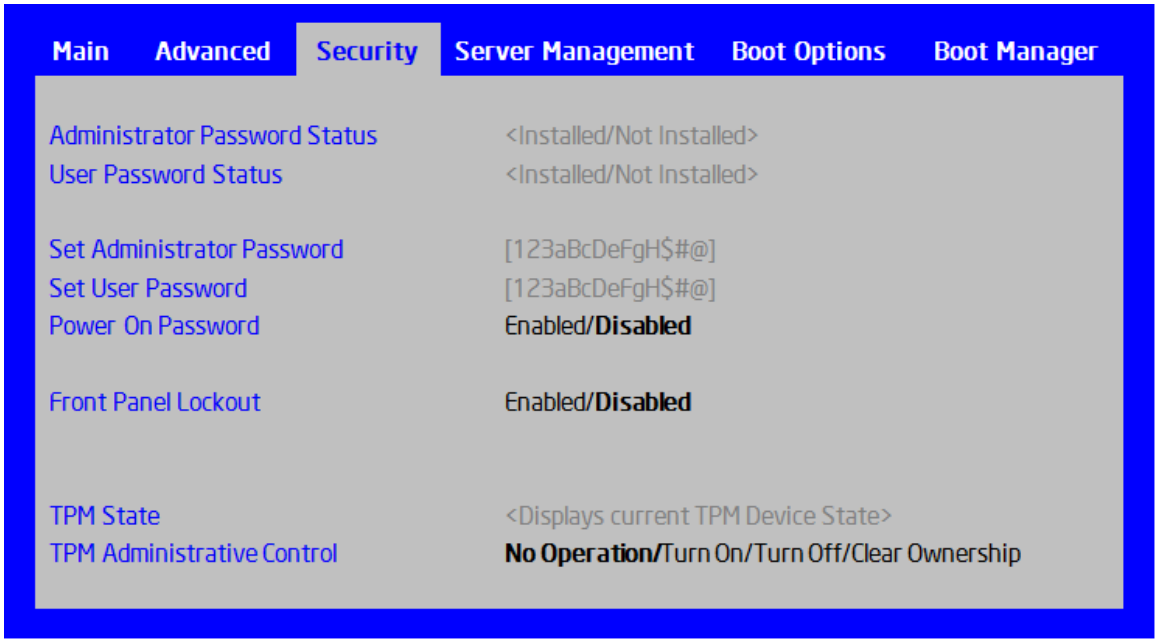


Figure 31. Security Screen

Screen Field Descriptions:

1. Administrator Password Status

   Option Values: Installed

   Not Installed

   Help Text: *<None>*

   Comments: *Information only.* Indicates the status of the Administrator Password.

   Back to [Security Screen] — [Screen Map]

2. User Password Status

   Option Values: Installed

   Not Installed

   Help Text: *<None>*

Comments: *Information only.* Indicates the status of the User Password.

Back to [Security Screen] — [Screen Map]

3. Set Administrator Password

   Option Values: [Entry Field – 0-14 characters]

   Help Text:

   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.

   Comments: 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.

   Back to [Security Screen] — [Screen Map]

4. Set User Password

   Option Values: *[Entry Field – 0-14 characters]*

Help Text:

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.

Comments: 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).

Back to [Security Screen] — [Screen Map]

5. Power On Password

   Option Values: Enabled

   Disabled

   Help Text:

   Enable Power On Password support. If enabled, password entry is required in order to boot the system.

   Comments: 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.

   Back to [Security Screen] — [Screen Map]

6. Front Panel Lockout

   Option Values: Enabled

   Disabled

   Help Text:

   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.

Note: This option is not visible on S1200V3RP Server Board.

Back to [Security Screen] — [Screen Map]

7. TPM State

   Option Values: *<Displays current TPM Device State>*

   May be:

   Enabled & Activated

   Enabled & Deactivated

   Disabled & Activated

   Disabled & Deactivated

   Help Text: *<None>*

   Comments: *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.

   Back to [Security Screen] — [Screen Map]

8. TPM Administrative Control

   Option Values: **No Operation**

   Turn On

   Turn Off

   Clear Ownership

   Help Text:

   [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.

Comments: 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.

Back to [Security Screen] — [Screen Map]

9.4.2.14 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.

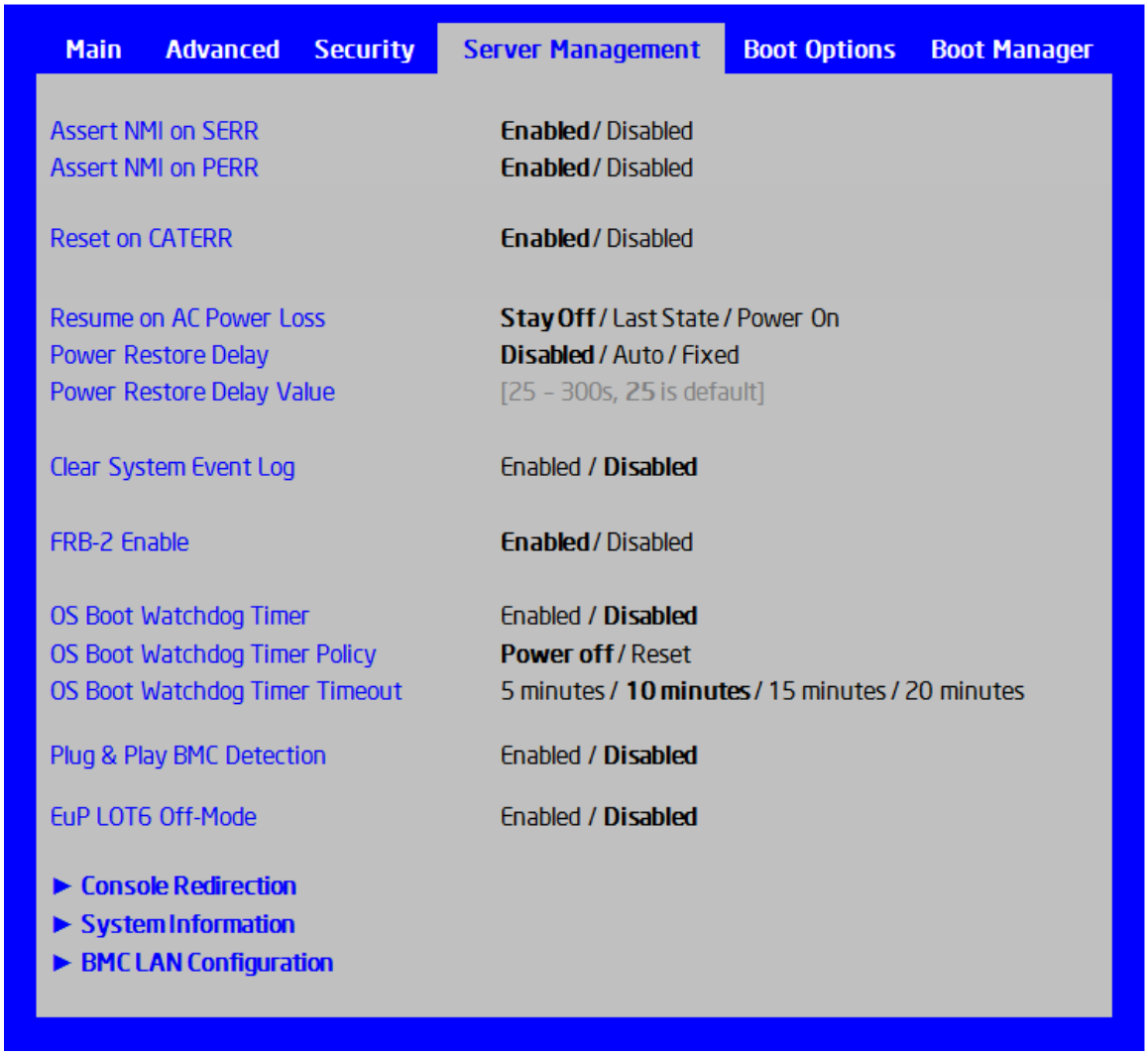


Figure 32. Server Management Screen

Screen Field Descriptions:

1. Assert NMI on SERR

   Option Values: **Enabled**

   Disabled

   Help Text:

   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.

   Comments: 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.

Back to [Server Management Screen] — [Screen Map]

2. Assert NMI on PERR

   Option Values: **Enabled**

   Disabled

   Help Text:

   On PERR, generate an NMI and log an error.

   Note: This option is only active if the Assert NMI on SERR option has [Enabled] selected.

   Comments: 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.

Back to [Server Management Screen] — [Screen Map]

3. Reset on CATERR

   Option Values: **Enabled**

   Disabled

   Help Text:

   When enabled system gets reset upon encountering Catastrophic Error (CATERR); when disabled system does not get reset on CATERR.

   Comments: 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.

Back to [Server Management Screen] — [Screen Map]

4. Resume on AC Power Loss

   Option Values: **Stay Off**

   Last State

   Power On

   Help Text:

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.

Comments: 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.

Back to [Server Management Screen] — [Screen Map]

5. Power Restore Delay

Option Values: **Disabled**

Auto

Fixed

Help Text:

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.

Comments: 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.

Back to [Server Management Screen] — [Screen Map]

6. Power Restore Delay Value

   Option Values: *[Entry Field 25 – 300, 25 is default]*

   Help Text:

   Fixed time period 25-300 seconds for Power Restore Delay.

   Comments: 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.

   Back to [Server Management Screen] — [Screen Map]

7. Clear System Event Log

   Option Values: Enabled

   Disabled

   Help Text:

   If enabled, clears the System Event Log. All current entries will be lost.

   Note: This option is reset to [Disabled] after a reboot.

   Comments: 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.

   Back to [Server Management Screen] — [Screen Map]

8. FRB-2 Enable

   Option Values: **Enabled**

   Disabled

   Help Text:

   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.

   Comments: 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.

   Back to [Server Management Screen] — [Screen Map]

9. OS Boot Watchdog Timer

   Option Values: Enabled

   Disabled

   Help Text:

   BIOS programs the watchdog timer with the timeout value selected. If the OS does not complete booting before the timer expires, the BMC will reset the system and an error will be logged.

   Requires OS support or Intel Management Software Support.

   Comments: 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.

Back to [Server Management Screen] — [Screen Map]

10. OS Boot Watchdog Timer Policy

    Option Values: **Power off**

    Reset

    Help Text:

    If the OS 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.

    Comments: This option is grayed out and unavailable when the O/S Boot Watchdog Timer is disabled.

    Back to [Server Management Screen] — [Screen Map]

11. OS Boot Watchdog Timer Timeout

    Option Values: 5 minutes

    10 minutes

    15 minutes

    20 minutes

    Help Text:

    If the OS watchdog timer is enabled, this is the timeout value BIOS will use to configure the watchdog timer.

    Comments: This option is grayed out and unavailable when the O/S Boot Watchdog Timer is disabled.

    Back to [Server Management Screen] — [Screen Map]

12. Plug & Play BMC Detection

    Option Values: Enabled

    Disabled

    Help Text:

If enabled, the BMC will be detectable by OSes which support plug and play loading of an IPMI driver. Do not enable this option if your OS does not support this driver.

Comments: 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.

Back to [Server Management Screen] — [Screen Map]

13. EuP LOT6 Off-Mode

Option Values: Enabled

Disabled

Help Text:

Enable/disable Ecodesign EuP LOT6 "Deep Sleep" Off-Mode for near-zero energy use when powered off.

Comments: 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.

Back to [Server Management Screen] — [Screen Map]

14. Console Redirection

Option Values: *<None>*

Help Text:

View/Configure Console Redirection information and settings.

Comments: *Selection only.* Select this line and press the <Enter> key to go to the Console Redirection group of configuration settings.

Back to [Server Management Screen] — [Screen Map]

15. System Information

Option Values: *<None>*

Help Text:

View System Information.

Comments: *Selection only.* Select this line and press the <Enter> key to go to the System Information group of configuration settings.

Back to [Server Management Screen] — [Screen Map]

16. BMC LAN Configuration

Option Values: *<None>*

Help Text:

View/Configure BMC LAN and user settings.

Comments: *Selection only.* Select this line and press the <Enter> key to go to the BMC LAN Configuration group of configuration settings.

Back to [Server Management Screen] — [Screen Map]

9.4.2.15 Console Redirection

The Console Redirection screen allows the user to enable or disable Console Redirection for Remote System 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.

When Console Redirection is active, all POST and Setup displays are in Text Mode. The Quiet Boot setting is disregarded, and the Text Mode POST Diagnostic Screen will be displayed regardless of the Quiet Boot setting. This is due to the limitations of Console Redirection, which is based on data terminal emulation using a serial data interface to transfer character data.

Console Redirection can use either of the two Serial Ports provided by the SuperIO in the BMC. However, if Console Redirection is to be coordinated with Serial Over LAN, the user should be aware that SOL is only supported through Serial Port A.

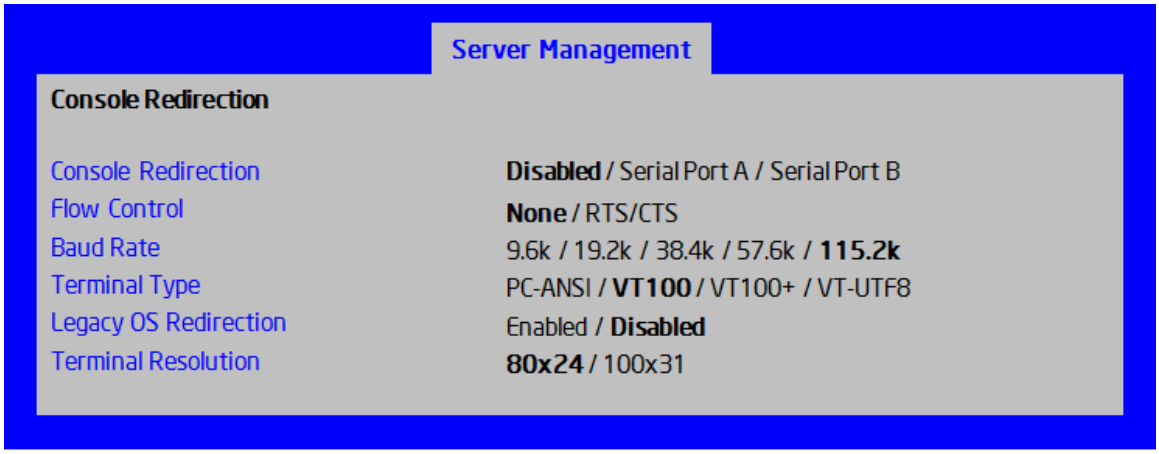


Figure 33. Console Redirection Screen

Screen Field Descriptions:

1. Console Redirection

   Option Values: **Disabled**

   Serial Port A

   Serial Port B

   Help Text:

   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 will disable display of the Quiet Boot logo screen during POST.

   Comments: Serial Console Redirection can use either Serial Port A or Serial Port B. 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 neither Serial A nor Serial B 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.

   Back to [Console Redirection Screen] — [Server Management Screen] — [Screen Map]

2. Flow Control

   Option Values: **None**

   RTS/CTS

   Help Text:

   Flow control is the handshake protocol.

   This setting must match the remote terminal application.

   [None] - Configure for no flow control.

   [RTS/CTS] - Configure for hardware flow control.

   Comments: 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 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.

Back to [Console Redirection Screen] — [Server Management Screen] — [Screen Map]

3. Baud Rate

Option Values: 9.6k

19.2k

38.4k

57.6k

115.2k

Help Text:

Serial port transmission speed. This setting must match the remote terminal application.

Comments: 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.

Back to [Console Redirection Screen] — [Server Management Screen] — [Screen Map]

4. Terminal Type

Option Values: PC-ANSI

VT100

VT100+

VT-UTF8

Help Text:

Character formatting used for console redirection. This setting must match the remote terminal application.

Comments: 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.

Back to [Console Redirection Screen] — [Server Management Screen] — [Screen Map]

5. Legacy OS Redirection

   Option Values: Enabled

   Disabled

   Help Text:

   This option enables legacy OS redirection (i.e., DOS) on serial port. If it is enabled, the associated serial port is hidden from the legacy OS.

   Comments: 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.

   Back to [Console Redirection Screen] — [Server Management Screen] — [Screen Map]

6. Terminal Resolution

   Option Values: **80x24**

   100x31

   Help Text:

   Remote Terminal Resolution.

   Comments: 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.

   Back to [Console Redirection Screen] — [Server Management Screen] — [Screen Map]

9.4.2.16 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.

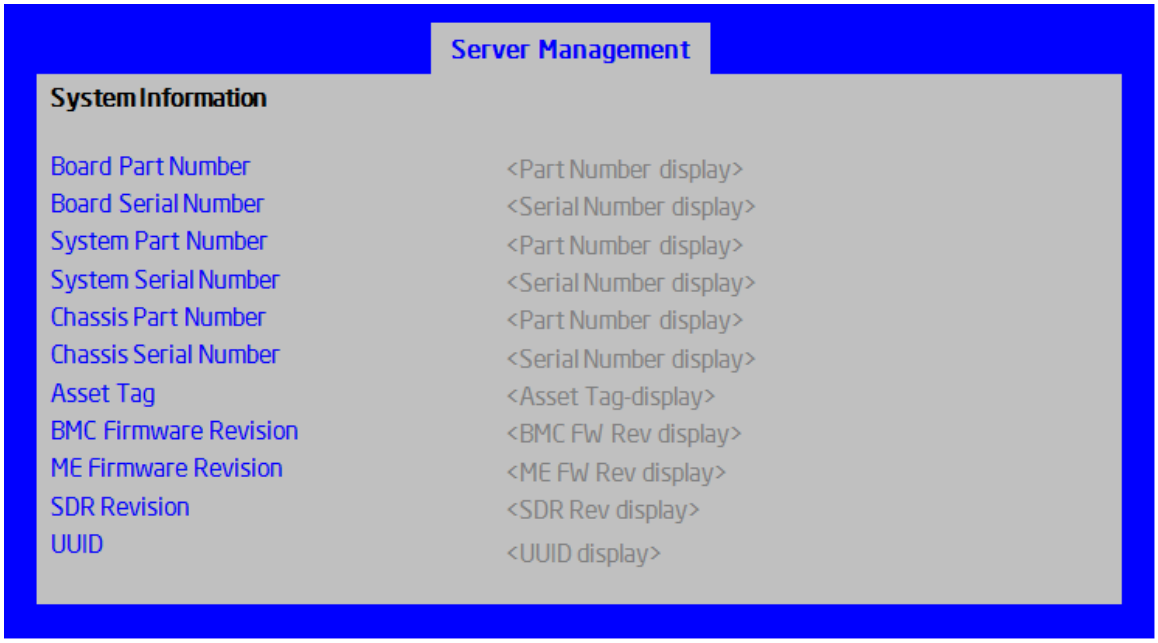


Figure 34. System Information Screen

Screen Field Descriptions:

1. Board Part Number

   Option Values: *<Part Number display>*

   Help Text: *<None>*

   Comments: *Information only.*

   Back to [System Information Screen] — [Server Management Screen] — [Screen Map]

2. Board Serial Number

   Option Values: <Serial Number display>

   Help Text: <None>

   Comments: Information only.

   Back to [System Information Screen] — [Server Management Screen] — [Screen Map]

3. System Part Number

   Option Values: *<Part Number display>*

   Help Text: *<None>*

   Comments: *Information only.*

Back to [System Information Screen] — [Server Management Screen] — [Screen Map]

4. System Serial Number

   Option Values: *<Serial Number display>*

   Help Text: *<None>*

   Comments: *Information only.*

   Back to [System Information Screen] — [Server Management Screen] — [Screen Map]

5. Chassis Part Number

   Option Values: *<Part Number display>*

   Help Text: *<None>*

   Comments: *Information only.*

   Back to [System Information Screen] — [Server Management Screen] — [Screen Map]

6. Chassis Serial Number

   Option Values: *<Serial Number display>*

   Help Text: *<None>*

   Comments: *Information only.*

   Back to [System Information Screen] — [Server Management Screen] — [Screen Map]

7. Asset Tag

   Option Values: *<Asset Tag-display>*

   Help Text: *<None>*

   Comments: *Information only.*

   Back to [System Information Screen] — [Server Management Screen] — [Screen Map]

8. BMC Firmware Revision

   Option Values: *<BMC FW Rev display>*

   Help Text: *<None>*

   Comments: *Information only.*

   Back to [System Information Screen] — [Server Management Screen] — [Screen Map]

9. ME Firmware Revision

   Option Values: *<ME FW Rev display>*

   Help Text: *<None>*

   Comments: *Information only.*

   Back to [System Information Screen] — [Server Management Screen] — [Screen Map]

10. SDR Revision

    Option Values: *<SDR Rev display>*

    Help Text: *<None>*

    Comments: *Information only.*

    Back to [System Information Screen] — [Server Management Screen] — [Screen Map]

11. UUID

    Option Values: *<UUID display>*

    Help Text: *<None>*

    Comments: *Information only.*

    Back to [System Information Screen] — [Server Management Screen] — [Screen Map]

9.4.2.17 BMC LAN Configuration

To access this screen from the Main screen, select Server Management > BMC LAN Configuration. To move to another screen, press the <Esc> key to return to the Server Management screen, then select the desired screen.

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

An Intel® RMM4 Management Module may be installed in the server system.

If the Management Module is installed, it may also have a Dedicated Server Management NIC Module (DMN) installed with it. In that case, the LAN settings for the Intel® RMM4 with Dedicated Server Management NIC may be configured.

When there is no Management Module installed in the system, or there is an Intel® RMM4-Lite without a DMN installed, the LAN settings specific to the Intel® RMM4 are grayed out and not available.

This screen has a choice of IPv4 or IPv6 addressing. When IPv6 is disabled, only the IPv4 addressing options appear. When IPv6 is enabled, the IPv4 options are grayed out and unavailable, and there is an additional section active for IPv6-addressing. This is true for both

the Baseboard LAN configuration and the Intel® RMM4 with Dedicated Server Management NIC Module.

IP addresses for either IPv4 or IPv6 addressing can be assigned by static IP addresses manually typed in, or by dynamic IP addresses supplied by a Dynamic Host Configuration Protocol (DHCP) server. IPv6 addressing can also be provided by “stateless autoconfiguration” which does not require a DHCP server.

The BMC LAN Configuration screen is unusual in that the LAN Configuration parameters are maintained by the BMC itself, so this screen is just a User Interface to the BMC configuration. As such, the initial values of the LAN options shown on the screen are acquired from the BMC when this screen is initially accessed by a user,. Any values changed by the user are communicated back to the BMC when a “Save Changes” or “Save Changes and Exit” action is performed. If a “Discard Changes” or “Discard Changes and Exit” action is performed instead, any accumulated changes from this screen will be disregarded and lost.

Figure 35. BMC LAN Configuration Screen

Screen Field Descriptions:

1. IP Source

   Option Values: Static

   Dynamic

   Help Text:

Select BMC IP Source: If [Static], IP parameters may be edited. If [Dynamic], these fields are display-only and IP address is acquired automatically (DHCP).

Comments: 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).

When IPv6 addressing is enabled, this field is grayed out and inactive.

Back to [BMC LAN Configuration Screen] — [Server Management Screen] — [Screen Map]

2. IP Address

Option Values: *[Entry Field 0.0.0.0, **0.0.0.0** is default]*

Help Text:

View/Edit IP Address. Press <Enter> to edit.

Comments: 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.

Back to [BMC LAN Configuration Screen] — [Server Management Screen] — [Screen Map]

3. Subnet Mask

Option Values: *[Entry Field 0.0.0.0, **0.0.0.0** is default]*

Help Text:

View/Edit Subnet Mask. Press <Enter> to edit.

Comments: 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.

Back to [BMC LAN Configuration Screen] — [Server Management Screen] — [Screen Map]

4. Gateway IP

   Option Values: *[Entry Field 0.0.0.0, **0.0.0.0** is default]*

   Help Text:

   View/Edit Gateway IP. Press <Enter> to edit.

   Comments: 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.

   Back to [BMC LAN Configuration Screen] — [Server Management Screen] — [Screen Map]

5. IPv6

   Option Values: Enabled

   Disabled

   Help Text:

   Option to Enable/Disable IPv6 addressing and any IPv6 network traffic on these channels.

   Comments: 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 (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.

   Back to [BMC LAN Configuration Screen] — [Server Management Screen] — [Screen Map]

6. IPv6 Source

   Option Values: Static

   Dynamic

Auto

Help Text:

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.

Comments: 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).

Back to [BMC LAN Configuration Screen] — [Server Management Screen] — [Screen Map]

7. IPv6 Address

   Option Values: *[Entry Field 0000:0000:0000:0000:0000:0000:0000:0000,*

   0000:0000:0000:0000:0000:0000:0000:0000 *is default]*

   Help Text:

   View/Edit IPv6 address. Press <Enter> to edit. IPv6 addresses consist of 8 hexadecimal 4 digit numbers separated by colons.

   Comments: 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).

   Back to [BMC LAN Configuration Screen] — [Server Management Screen] — [Screen Map]

8. Gateway IPv6

   Option Values: [Entry Field 0000:0000:0000:0000:0000:0000:0000:0000,

   0000:0000:0000:0000:0000:0000:0000:0000 is default]

   Help Text:

View/Edit Gateway IPv6 address. Press <Enter> to edit. Gateway IPv6 addresses consist of 8 hexadecimal 4 digit numbers separated by colons.

Comments: 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 field is display-only (when Dynamic or Auto) or can be edited (when Static).

Back to [BMC LAN Configuration Screen] — [Server Management Screen] — [Screen Map]

9. IPv6 Prefix Length

Option Values: [Entry Field 0 – 128, **64** is default]

Help Text:

View/Edit IPv6 Prefix Length from zero to 128 (default 64). Press <Enter> to edit.

Comments: 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).

Back to [BMC LAN Configuration Screen] — [Server Management Screen] — [Screen Map]

10. Intel(R) RMM4

Option Values: Not Present

Intel(R) RMM4-Lite

Intel(R) RMM4 + DMN

Help Text: *<None>*

Comments: *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.

Back to [BMC LAN Configuration Screen] — [Server Management Screen] — [Screen Map]

11. IP Source

    Option Values: Static

    Dynamic

    Help Text:

    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).

    Comments: 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.

    Back to [BMC LAN Configuration Screen] — [Server Management Screen] — [Screen Map]

12. IP Address

    Option Values: [Entry Field 0.0.0.0, **0.0.0.0** is default]

    Help Text:

    View/Edit IP Address. Press <Enter> to edit.

    Comments: 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.

Back to [BMC LAN Configuration Screen] — [Server Management Screen] — [Screen Map]

13. Subnet Mask

    Option Values: [Entry Field 0.0.0.0, **0.0.0.0** is default]

    Help Text:

    View/Edit Subnet Mask. Press <Enter> to edit.

    Comments: 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.

    Back to [BMC LAN Configuration Screen] — [Server Management Screen] — [Screen Map]

14. Gateway IP

    Option Values: [Entry Field 0.0.0.0, **0.0.0.0** is default]

    Help Text:

    View/Edit Gateway IP. Press <Enter> to edit.

    Comments: 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 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.

    Back to [BMC LAN Configuration Screen] — [Server Management Screen] — [Screen Map]

15. IPv6 Source

    Option Values: Static

    Dynamic

    Auto

Help Text:

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.

Comments: 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).

Back to [BMC LAN Configuration Screen] — [Server Management Screen] — [Screen Map]

16. IPv6 Address

Option Values: [Entry Field 0000:0000:0000:0000:0000:0000:0000:0000,

0000:0000:0000:0000:0000:0000:0000:0000 is default]

Help Text:

View/Edit IPv6 address. Press <Enter> to edit. IPv6 addresses consist of 8 hexadecimal 4 digit numbers separated by colons.

Comments: 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).

Back to [BMC LAN Configuration Screen] — [Server Management Screen] — [Screen Map]

17. Gateway IPv6

Option Values: [Entry Field 0000:0000:0000:0000:0000:0000:0000:0000,

0000:0000:0000:0000:0000:0000:0000:0000 is default]

Help Text:

View/Edit Gateway IPv6 address. Press <Enter> to edit. Gateway IPv6 addresses consist of 8 hexadecimal 4 digit numbers separated by colons.

Comments: 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.

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).

Back to [BMC LAN Configuration Screen] — [Server Management Screen] — [Screen Map]

18. IPv6 Prefix Length

    Option Values: [Entry Field 0 – 128, **64** is default]

    Help Text:

    View/Edit IPv6 Prefix Length from zero to 128 (default 64). Press <Enter> to edit.

    Comments: 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).

    Back to [BMC LAN Configuration Screen] — [Server Management Screen] — [Screen Map]

19. BMC DHCP Host Name

    Option Values: *[Entry Field, 2-63 characters]*

    Help Text:

    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.

    Comments: 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.

Back to [BMC LAN Configuration Screen] — [Server Management Screen] — [Screen Map]

20. User ID

    Option Values: **anonymous**

    root

    User3

    User4

    User5

    Help Text:

    Select the User ID to configure: User1 (anonymous), User2 (root), and User3/4/5 are supported.

    Comments: 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.

    Back to [BMC LAN Configuration Screen] — [Server Management Screen] — [Screen Map]

21. Privilege

    Option Values: Callback

    User

    Operator

    Administrator

    Help Text:

    View/Select user privilege. User2 (root) privilege is "Administrator" and cannot be changed.

    Comments: The level of privilege that is assigned for a User ID affects which functions that user may perform.

    Back to [BMC LAN Configuration Screen] — [Server Management Screen] — [Screen Map]

22. User Status

Option Values: Enabled

Disabled

Help Text:

Enable / Disable LAN access for selected user. Also enables/disables SOL, KVM, and media redirection.

Comments: Note that status setting is Disabled by default until set to Enabled.

Back to [BMC LAN Configuration Screen] — [Server Management Screen] — [Screen Map]

23. User Name

Option Values: *[Entry Field, 4 - 15 characters]*

Help Text:

Press <Enter> to edit User Name. User Name is a string of 4 to 15 alphanumeric characters, and must begin with an alphabetic character. User Name cannot be changed for User1 (anonymous) and User2 (root).

Comments: User Name can only be edited for users other than “anonymous” and “root”. Those two User Names may not be changed.

Back to [BMC LAN Configuration Screen] — [Server Management Screen] — [Screen Map]

24. User Password

Option Values: *[Popup Entry Field, 0 - 15 characters]*

Help Text:

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.

Comments: 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.

Back to [BMC LAN Configuration Screen] — [Server Management Screen] — [Screen Map]

9.4.2.18 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.

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.

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.

Note: USB devices can be “hotplugged” during POST, and will be detected and “beeped”. They will be enumerated and displayed on the USB Configuration Setup screen. However, they may not be enumerated as bootable devices, depending on when in POST they were hotplugged. If they were recognized before the enumeration of bootable devices, they will appear as Boot Devices if appropriate. If they were recognized after Boot Device enumeration, they will not appear as a bootable device for the Boot Options screen, the Boot Manager screen, or the F6 Boot Menu.

There are two main types of boot order control, Legacy Boot and EFI Optimized boot. These are mutually exclusive – when EFI Optimized Boot is enabled, Legacy Boot (the default) is disabled. Within Legacy Boot operation, there are two further methods of ordering boot devices, Dynamic Boot Order and Static Boot Order.

The default for Boot Order control is Legacy Boot, with Dynamic Boot Order. 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

In this default Boot Order, a USB device may appear in any of several Device Classes, due to the flexibility of USB connections and USB emulation of various types of devices.

Note: A USB Key (USB Flash Drive) can be formatted to emulate either a Floppy Drive or a Hard Drive, and will appear in that Boot Device Class. However, although it can be formatted as a CDROM Drive, it will not be detected as such. It will be treated as a Hard Disk and will appear in the list of available Hard Drives.

Figure 36. Boot Option Screen

Screen Field Descriptions:

1. System Boot Timeout

   Option Values: *[Entry Field 0 – 65535, **0** is default]*

   Help Text:

   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.

   Comments: After entering the desired 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.

Back to [Boot Options Screen] — Back to [Screen Map]

2. Boot Option #1

3. Boot Option #2

4. Boot Option <#n>

   Option Values: *<Available Boot Device #n>*

   Help Text:

   Set system boot order by selecting the boot option for this position.

   Comments: 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.

   Back to [Boot Options Screen] — Back to [Screen Map]

5. CDROM Order

   Option Values: *<None>*

   Help Text:

   Set the order of the legacy devices in this group.

   Comments: *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 not USB Keys formatted for CRDOM emulation, which are seen as Hard Disk drives.

   Back to [Boot Options Screen] — Back to [Screen Map]

6. Hard Disk Order

Option Values: *<None>*

Help Text:

Set the order of the legacy devices in this group.

Comments: *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.

Back to [Boot Options Screen] — Back to [Screen Map]

7. Floppy Order

   Option Values: *<None>*

   Help Text:

   Set the order of the legacy devices in this group.

   Comments: *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.

   Back to [Boot Options Screen] — Back to [Screen Map]

8. Network Device Order

   Option Values: *<None>*

   Help Text:

   Set the order of the legacy devices in this group.

   Comments: *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.

   Back to [Boot Options Screen] — Back to [Screen Map]

9. BEV Device Order

   Option Values: *<None>*

Help Text:

Set the order of the legacy devices in this group.

Comments: *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.

Back to [Boot Options Screen] — Back to [Screen Map]

10. Add EFI Boot Option

Option Values: *<None>*

Help Text:

Add a new EFI boot option to the boot order.

Comments: *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.

Back to [Boot Options Screen] — Back to [Screen Map]

11. Delete EFI Boot Option

Option Values: *<None>*

Help Text:

Remove an EFI boot option from the boot order.

Comments: *Selection only.* Select this line and press the <Enter> key to go to the Delete EFI Boot Option Screen.

This option is only displayed if an EFI boot path is included in the Boot Order.

Back to [Boot Options Screen] — Back to [Screen Map]

12. EFI Optimized Boot

Option Values: Enabled

Disabled

Help Text:

If enabled, the BIOS only loads modules required for booting EFI-aware Operating Systems.

Comments: If this option is enabled, the system will not boot successfully to a non EFI aware OS.

Back to [Boot Options Screen] — Back to [Screen Map]

13. Use Legacy Video for EFI OS

    Option Values: Enabled

    Disabled

    Help Text:

    If enabled, the BIOS uses the legacy video ROM instead of the EFI video ROM.

    Comments: This option appears only when EFI Optimized Boot is enabled.

    Back to [Boot Options Screen] — Back to [Screen Map]

14. Boot Option Retry

    Option Values: Enabled

    Disabled

    Help Text:

    If enabled, this continually retries non-EFI-based boot options without waiting for user input.

    Comments: This option is intended to keep retrying for cases where the boot devices could possibly be slow to initially respond, e.g. 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.

    Back to [Boot Options Screen] — Back to [Screen Map]

15. USB Boot Priority

    Option Values: Enabled

    Disabled

    Help Text:

    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.

Comments: 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.

Back to [Boot Options Screen] — Back to [Screen Map]

16. Static Boot Order

Option Values: Enabled

Disabled

Help Text:

[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.

Comments: When the option changes to “Enabled” from “Disabled”, it will enable Static Boot Order (SBO) from the next boot onward, and also the current Boot Order will be stored as the SBO template.

When the option changes from “Enabled” to “Disabled”, this will disable SBO and the SBO template will be cleared.

Otherwise it will retain the current Enabled/Disabled state.

Back to [Boot Options Screen]— Back to [Screen Map]

17. Reset Static Boot Order

Option Values: Yes

No Action

Help Text:

[Yes] Take snapshot of current boot order to save as Static Boot Order Template.

Comments: 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 Order option.

Select **Yes** to snapshot 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 grayed out and unavailable.

Back to [Boot Options Screen] — Back to [Screen Map]

9.4.2.19 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: 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.

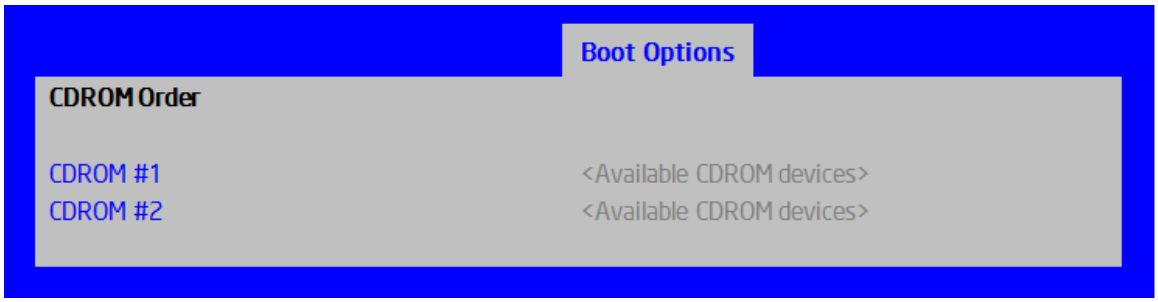


Figure 37. CDROM Order Screen

Screen Field Descriptions:

1. CDROM #1
2. CDROM #2

   Option Values: *<Available CDROM devices>*

   Help Text:

   Set system boot order by selecting the boot option for this position.

   Comments: Choose the order of booting among CDROM devices by choosing which available CDROM device should be in each position in the order.

   Back to [CDROM Order Screen] — [Boot Options Screen] — [Screen Map]

9.4.2.20 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.

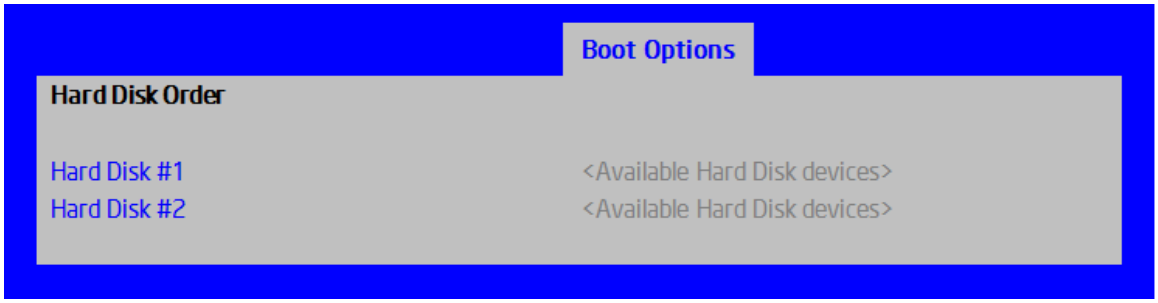


Figure 38. Hard Disk Order Screen

Screen Field Descriptions:

1. Hard Disk #1
2. Hard Disk #2

   Option Values: *<Available Hard Disk devices>*

   Help Text:

   Set system boot order by selecting the boot option for this position.

   Comments: Choose the order of booting among Hard Disk devices by choosing which available Hard Disk device should be in each position in the order.

Back to [Hard Disk Order Screen] — [Boot Options Screen] — [Screen Map]

9.4.2.21 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.

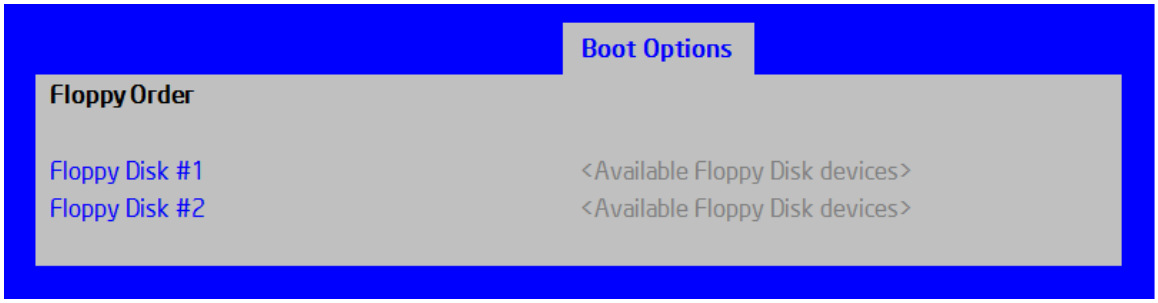


Figure 39. Floppy Order Screen

Screen Field Descriptions:

1. Floppy Disk #1
2. Floppy Disk #2

   Option Values: *<Available Floppy Disk devices>*

   Help Text:

   Set system boot order by selecting the boot option for this position.

   Comments: Choose the order of booting among Floppy Disk devices by choosing which available Floppy Disk device should be in each position in the order.

   Back to [Floppy Order Screen] — [Boot Options Screen] — [Screen Map]

9.4.2.22 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.

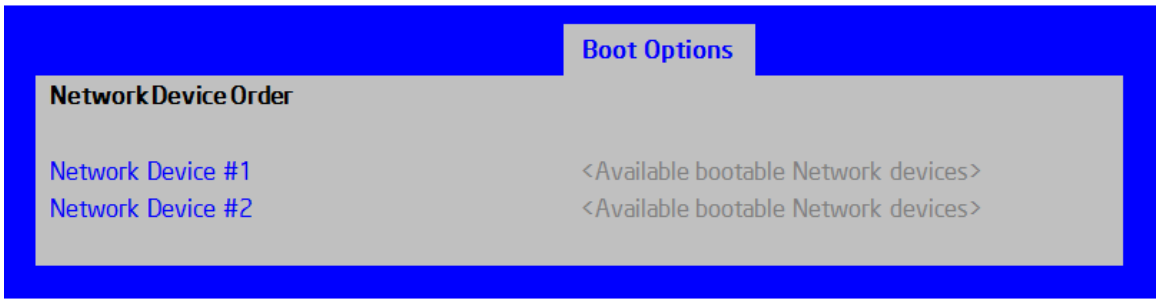


Figure 40. Network Device Order Screen

Screen Field Descriptions:

1. Network Device #1
2. Network Device #2

   Option Values: *<Available Network Devices>*

   Help Text:

   Set system boot order by selecting the boot option for this position.

   Comments: Choose the order of booting among Network Devices by choosing which available Network Device should be in each position in the order.

   Back to [Network Device Order Screen] — [Boot Options Screen] — [Screen Map]

9.4.2.23 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 41. BEV Device Order Screen

Screen Field Descriptions:

1. BEV Device #1
2. BEV Device #2

   Option Values: *<Available BEV Devices>*

   Help Text:

   Set system boot order by selecting the boot option for this position.

   Comments: Choose the order of booting among BEV Devices by choosing which available BEV Device should be in each position in the order.

   Back to [BEV Device Order Screen] — [Boot Options Screen] — [Screen Map]

9.4.2.24 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.

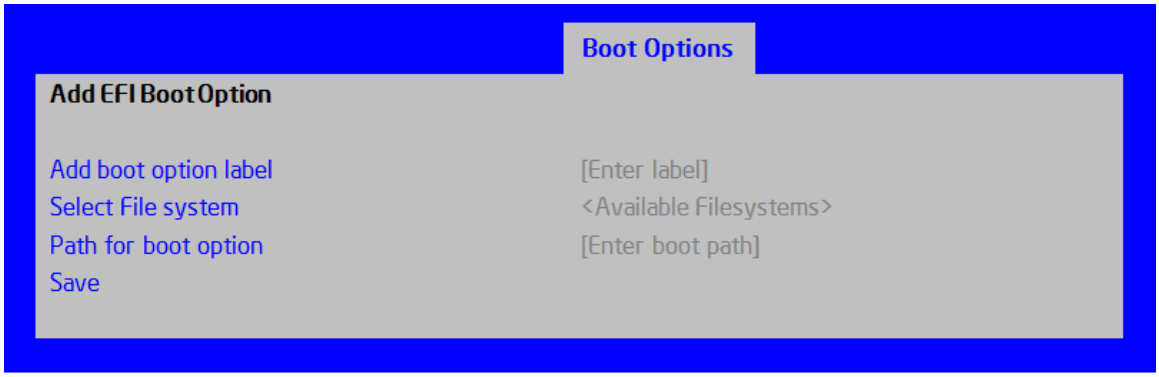


Figure 42. Add EFI Boot Option Screen

Screen Field Descriptions:

1. Add boot option label

   Option Values: *[Enter label]*

   Help Text:

   Create the label for the new boot option.

   Comments: This label becomes an abbreviation for this Boot Path.

   Back to [Add EFI Boot Option Screen] — [Boot Options Screen] — [Screen Map]

2. Select File system

   Option Values: *<Available Filesystems>*

   Help Text:

   Select one filesystem from this list.

   Comments: Choose the filesystem on which this boot path resides.

   Back to [Add EFI Boot Option Screen] — [Boot Options Screen] — [Screen Map]

3. Path for boot option

Option Values: *[Enter Boot Path]*

Help Text:

Enter the path to the boot option in the format \path\filename.efi.

Comments: This will be the Boot Path, residing on the filesystem chosen, which will enter into the Boot Order with the Label entered above.

Back to [Add EFI Boot Option Screen] — [Boot Options Screen] — [Screen Map]

4. Save

Option Values: *<None>*

Help Text:

Save the boot option.

Comments: *Selection only.* This will save the new Boot Option into the Boot Order.

Back to [Add EFI Boot Option Screen] — [Boot Options Screen] — [Screen Map]

9.4.2.25 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.

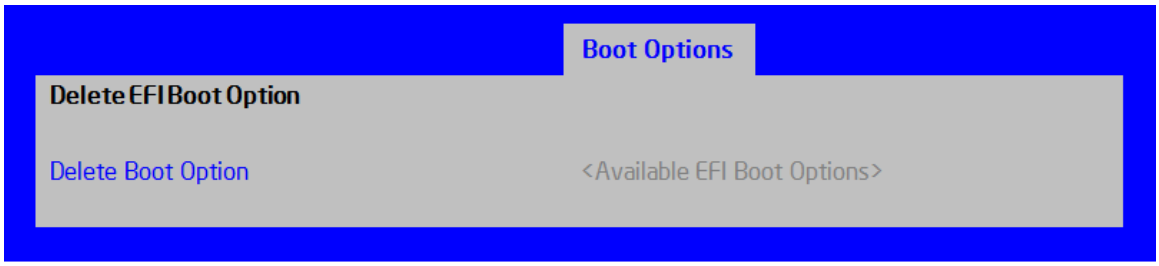


Figure 43. Delete EFI Boot Option Screen

Screen Field Descriptions:

1. Delete Boot Option

Option Values: *<Available EFI Boot Options>*

Help Text:

Select one to delete.

Comments: This will not allow a user to delete the EFI Shell.

Back to [Delete EFI Boot Option Screen] — [Boot Options Screen] — [Screen Map]

9.4.2.26 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.

Note: This list is not in order according to the system Boot Option order. Reordering Boot Devices or even removing them from the Boot Order completely has no effect on the Boot Manager.

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.

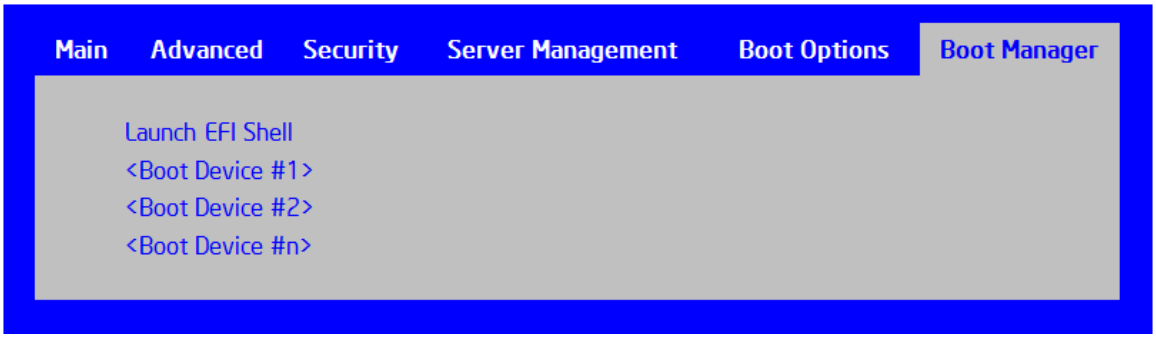


Figure 44. Boot Manager Screen

Screen Field Descriptions:

1. Launch EFI Shell

   Option Values: *<None>*

   Help Text:

   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.

   Comments: The EFI Shell will always be present in the list of bootable devices.

   Back to [Boot Manager Screen] — [Screen Map]

2. <Boot Device #1>
3. <Boot Device #2>
4. <Boot Device #n>

Option Values: *<None>*

Help Text:

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.

Comments: 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.

Back to [Boot Manager Screen] — [Screen Map]

9.4.2.27 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.

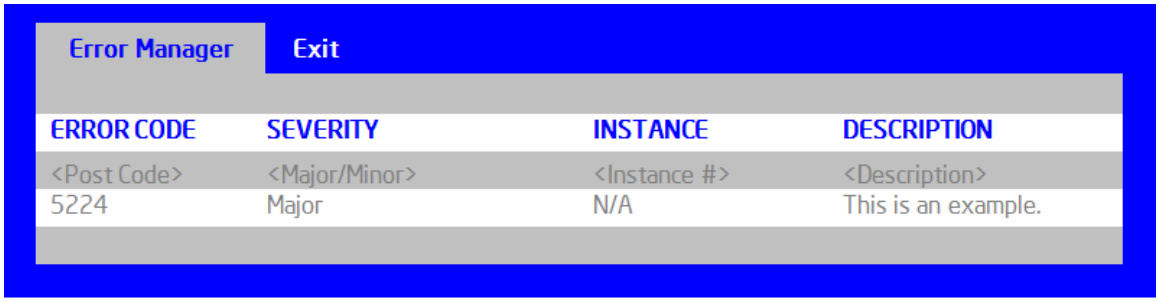


Figure 45. Error Manager Screen

Screen Field Descriptions:

1. ERROR CODE

Option Values: *<POST Error Code>*

Help Text: *<N/A>*

Comments: This is a POST Error Code – a BIOS-originated error that occurred during POST initialization.

Back to [Error Manager Screen] — [Screen Map]

2. SEVERITY

Option Values: Minor

Major

Fatal

Help Text: *<N/A>*

Comments: Each POST Error Code has a Severity associated with it.

Back to [Error Manager Screen] — [Screen Map]

3. INSTANCE

Option Values: *<Depends on error code>*

Help Text: *<N/A>*

Comments: 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.

Back to [Error Manager Screen] — [Screen Map]

4. DESCRIPTION

Option Values: *<N/A>*

Help Text: *<Description of POST Error Code>*

Comments: 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.

Back to [Error Manager Screen] — [Screen Map]

9.4.2.28 Save & Exit Screen (Tab)

The Save &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: 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 46. Save & Exit Screen

Screen Field Descriptions:

1. Save Changes and Exit

   Option Values: *<None>*

   Help Text:

   Exit BIOS Setup Utility after saving changes. The system will reboot if required.

   The [F10] key can also be used.

   Comments: *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.

Back to [Save & Exit Screen] — [Screen Map]

2. Discard Changes and Exit

   Option Values: *<None>*

   Help Text:

   Exit BIOS Setup Utility without saving changes.

   The [Esc] key can also be used.

   Comments: *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.

   Back to [Save & Exit Screen] — [Screen Map]

3. Save Changes

   Option Values: *<None>*

   Help Text:

   Save Changes made so far to any of the setup options.

   Comments: *Selection only.* Select this line and press the <Enter> key to save any pending changes in BIOS settings. If there have been no changes made in the 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.

   Back to [Save & Exit Screen] — [Screen Map]

4. Discard Changes

   Option Values: *<None>*

   Help Text:

   Discard Changes made so far to any of the setup options.

   Comments: *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.

   Back to [Save & Exit Screen] — [Screen Map]

5. Load Default Values

   Option Values: *<None>*

   Help Text:

   Load Defaults Values for all the setup options.

   Comments: *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 made 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 anyplace in Setup to initiate a “Load Default Values” action.

   Back to [Save & Exit Screen] — [Screen Map]

6. Save as User Default Values

   Option Values: *<None>*

   Help Text:

   Save the changes made so far as User Default Values.

Comments: *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.

Back to [Save & Exit Screen] — [Screen Map]

7. Load User Default Values

   Option Values: *<None>*

   Help Text:

   Load the User Default Values to all the setup options.

   Comments: *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.

   Back to [Save & Exit Screen] — [Screen Map]

9.5 BIOS Update Capability

The actual BIOS code that runs during POST is stored in Flash Memory on the baseboard. In general a user needs to interact with that code very little, other than when there is a BIOS problem to fix or new BIOS features or capabilities become available.

In order to bring those BIOS fixes or new features into the system, it is necessary to install updated BIOS in Flash Memory, replacing the current BIOS image. The user can do this either as a standalone process with a utility program running under the UEFI shell, or with an application program running under the OS.

The BIOS update is done using a “capsule” file which contains all relevant BIOS components. This capsule omits the NVRAM Firmware Volume, which retains its existing contents through the BIOS Update. There is a single BIOS capsule file for a given BIOS Release for updating the BIOS on all of the boards in the S1200RP Server Board Family.

It is also possible to completely reprogram the Flash Memory component using an EPROM Programmer and a binary BIOS image but this requires removing the Flash chip and is generally only done in a Development environment with a socketed Flash part. That is not discussed in this document.

9.5.1 Standalone BIOS Flash Update

The “IFlash32” BIOS Update Utility is a UEFI Shell application program used for updating the system BIOS using the capsule file from a BIOS release. This tool can also be used to update the ME but that is not discussed in this document (refer to ME Release Notes for update instructions).

There is an IFlash32 version available for WinPE* environments. This version requires that “Plug & Play BMC Detection” must be enabled in the Server Management tab in Setup (see Figure 32), and drivers must be installed. Refer to the IFlash32 program Release Notes for information on this.

The following procedure shows the steps necessary to update the BIOS using IFlash32 running under the UEFI Shell. The assumption is that the user has obtained a BIOS release in compressed (“Zip”) format, typically by downloading it from the Intel Support Website.

This is the general procedure for the UEFI BIOS Update – the BIOS Release Notes will include the most up-to-date procedure.

1. Unzip the compressed zip file on any Windows system and copy the UEFI folder (two required files: **iflash32.efi** and **ipmi.efi**) to any external medium, typically a USB Flash Drive (USB Key).

2. Copy the new capsule file to be updated (it has a file extension of “**.cap**”) to the same folder as **iflash32.efi**.

3. Boot to the EFI Shell on the system to be updated, and connect the external medium with the capsule file and IFlash32 to it.

4. Go to the directory where **iflash32.efi** is present on the external medium.

5. Run the command `iflash32 –u -ni [CapsuleFileName.cap]` where

   -u = update the System BIOS

   -ni = update will be in non-interactive mode

   [CapsuleFileName.cap] = replace with name of BIOS capsule file

6. At the end of the flash update, if the update is successful, a message will be displayed:

   `BIOS has been updated successfully.`

If the flash update fails for reasons of security compliance, a different message will be displayed:

Error: BIOS or ME update failure - the capsule file failed in the security compliance check. Please refer to BIOS Release Notes for details.

7. In order to properly complete the BIOS Update process, the system must perform a shutdown – DC power-off – then DC power-on and boot successfully to the EFI Shell or an OS environment.

In order to restore customer-determined BIOS setting defaults, another procedure is required after the BIOS update is successful:

1. Boot to the EFI Shell on the system just updated, and keep the external media with IFlash32 to it.

2. Go to the directory where **iflash32.efi** is present on the external medium.

3. Run the command `iflash32 -rd "[AdminPassword]"` where

   -rd = restore customer-determined BIOS setting defaults

   [AdminPassword] = BIOS Administer Password only if BIOS Administer Password was set.

4. Reset the system and the instruction returns success.

If there is a power loss during the IFlash32 BIOS Update:

- Try rebooting to the EFI Shell. If that is successful, restart the BIOS Update.
- If the boot to the EFI Shell fails, perform a Recovery Boot (see Section 9.6) using the Recovery capsule from the previously installed BIOS, that is, the BIOS version before the update.

Refer to the BIOS Release Notes and the IFlash32 program Release Notes for the most complete and accurate information, as well as additional information on the WinPE* version of IFlash32.

9.5.2 OS-Running BIOS Flash Update

The “One-Boot Flash Update” (OFU) Firmware Update Utility is an application program which can update the system BIOS while the system is in an “OS Running” state, so there is no need to take the system out of service to perform a BIOS update.

The OFU utility can actually update the ME, BMC, and SDR firmware as well as the BIOS. OFU is supported for both Windows and Linux (certain versions). It uses the BIOS capsule file for the BIOS update.

This utility requires that “Plug & Play BMC Detection” must be enabled in the Server Management tab in Setup (see Figure 32), and drivers must be installed depending on OS version. Refer to the One-Boot Flash Update program Release Notes for information on how to use it in different OS environments.

9.5.3 BIOS Backup Flash Update

The BIOS is also supported for updating the backup BIOS regions by update utility issues "UpdateBackupBios" command. After the BIOS receives request from utility, the backup BIOS update will be completed in next normal boot. It will show message "DO NOT REMOVE POWER! Now updating Backup BIOS region....." in update beginning, after backup update completed, will show "Done".

This is the general procedure for the UEFI backup BIOS Update – the BIOS Release Notes will include the most up-to-date procedure.

1. Unzip the compressed zip file on any Windows system and copy the UEFI folder (two required files: **iflash32.efi** and **ipmi.efi**) to any external medium, typically a USB Flash Drive (USB Key).

2. Copy the new capsule file to be updated (it has a file extension of "**.cap**") to the same folder as **iflash32.efi**.

3. Boot to the EFI Shell on the system to be updated, and connect the external medium with the capsule file and IFlash32 to it.

4. Go to the directory where **iflash32.efi** is present on the external medium.

5. Run the command `iflash32 –u -ni [CapsuleFileName.cap] UpdateBackupBios` where

   -u = update the System BIOS

   -ni = update will be in non-interactive mode

   [CapsuleFileName.cap] = replace with name of BIOS capsule file

   UpdateBackupBios = update the system backup BIOS

6. It will update primary BIOS with processed capsule. If the primary update is successful, then restart the system to complete backup BIOS update, and a message will be displayed:

   "Primary Update completed, Backup BIOS update will be completed in next boot."

9.6 BIOS Recovery

If a system is completely unable to boot successfully to an OS, hangs during POST, or even hangs and fails to start executing POST, it may be necessary to perform a BIOS Recovery procedure, which can replace a defective copy of the BIOS code.

This is intended to be a "last resort" method, and should not be used unless necessary.

Basically, this procedure involves opening the chassis, setting the BIOS Recovery jumper, and then following the instructions detailed in the current BIOS Release Notes.

The Recovery procedure is included here for general reference. However, if in conflict, the instructions in the BIOS Release Notes are the definitive version.

A BIOS recovery can be accomplished with images on backup flash blocks. The Recovery medium in USB Flash Drive must contain the following files in its root directory:

- UEFI iFlash32 (including **IFlash32.efi** and **ipmi.efi**)
- ***Rec.CAP** ("*" is a prefix depending on the BIOS Release number)
- **Startup.nsh** (edited as necessary to use the proper ***Rec.CAP** file)

The ***Rec.CAP** files should be from the BIOS version which is currently installed on the system. A mismatch between the Recovery files and the installed BIOS can cause unexpected failures in Recovery.

The BIOS starts the recovery process by first loading and booting to the recovery images from backup flash blocks. This process takes place before any video or console is available. Once the system boots to this recovery image file, it will boot automatically into 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, there will be a message displayed stating that the "BIOS has been updated successfully" indicating 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.

Step by step, this process goes as follows:

1. Power off the system. Removing AC power is not necessary but may be advisable due to safety considerations, or if a riser or other hardware must be moved for access to the BIOS Recovery jumper.

2. Open the chassis and move the BIOS Recovery jumper (marked BIOS RCVR) to its "Recovery" position on pins 2-3. Details regarding the jumper location can be obtained from the Technical Product Specification for the baseboard in the system. Restore any hardware to its correct position and close the chassis.

3. Insert recovery media (prepared previously as described above).

4. Power on the system. A beep code of 2 beeps should sound, indicating the start of Recovery.

5. If the Recovery Boot process fails prior to initializing video, there should be a 4-beep code and the system should halt with a Recovery Progress Code displayed in the Diagnostic LEDs.

6. The BIOS POST screen will appear displaying the progress, and the system will automatically boot to the EFI SHELL.

7. The **Startup.nsh** file will execute automatically, and will initiate the flash update (**IFlash32.efi**) with the new capsule file (***Rec.CAP**). The regular IFlash success message will be displayed at the end of the process, once the flash update succeeds.

8. Power off the system. Again, removing AC power is not necessary but may be advisable due to safety considerations, or if a riser or other hardware must be moved for access to the BIOS Recovery jumper.

9. Open the chassis, move hardware if necessary, and restore the recovery jumper position to "normal operation" pins 1-2. Replace any hardware moved, and close the chassis.

10. Remove Recovery medium.

11. Replug AC cords if removed, and power on the system.

12. Do NOT interrupt the BIOS POST during the first boot.

13. Boot the system into Setup. The Recovery Boot process will reset BIOS settings to default values.

14. Go to the Setup Main tab (see Figure 20), and set the System Date and System Time to the correct current settings. Make any other changes that are required in Setup – for example, Boot Order.

Again, before starting to perform a Recovery Boot, be sure to check the BIOS Release Notes and verify the Recovery procedure shown in the Release Notes.

10. Jumper Blocks

The server board includes several 3-pin jumper blocks which are used to as part of a process to restore a board function back to a normal functional state. The following diagram and sections identify the location of each jumper block and provides a description of their use.

The following symbol identifies Pin 1 on each jumper block on the silkscreen:

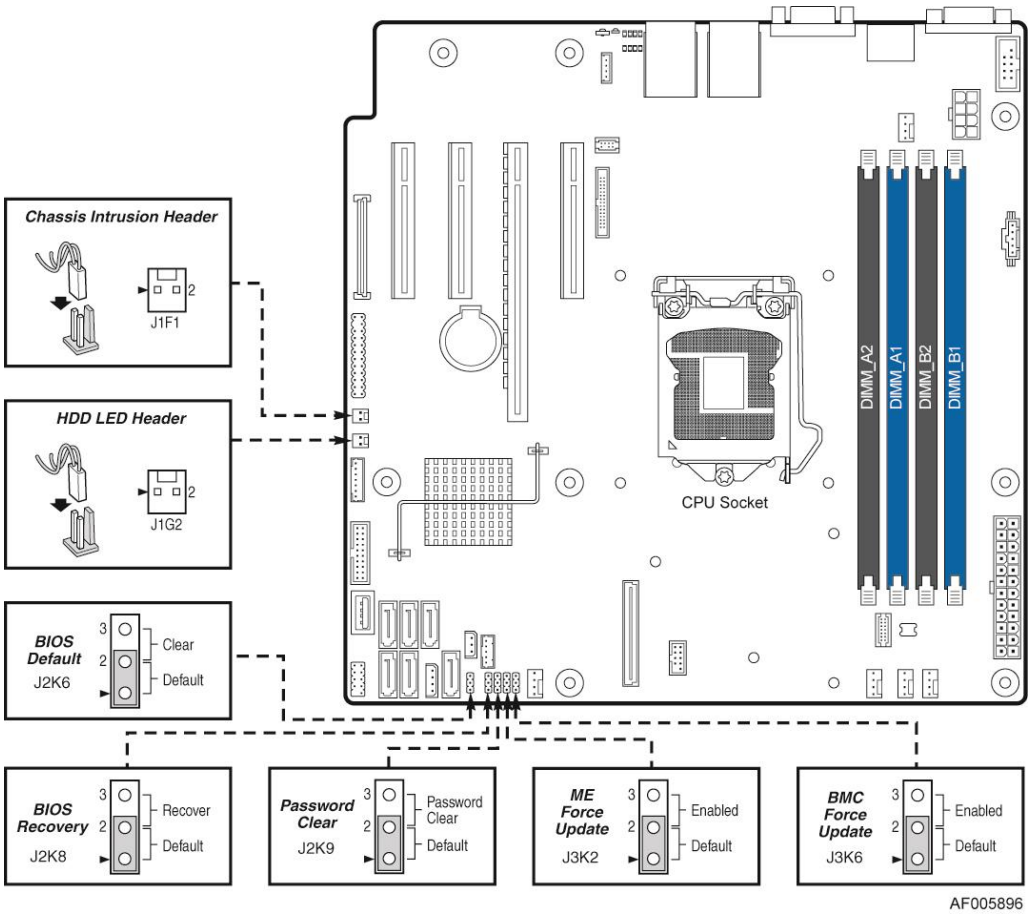


Figure 47. Jumper Blocks (J2K6, J2K8, J2K9, J3K2, J3K6)

Note:

1. *For safety purposes, the power cord should be disconnected from a system before removing any system components or moving any of the on-board jumper blocks.*

2. *System Update and Recovery files are included in the System Update Packages (SUP) posted to Intel's website.*

Table 58. Server Board Jumpers (J2K6, J2K8, J2K9, J3K2, J3K6)

Jumper Name	Pins	System Results
J2K6: BIOS Default	1-2	These pins should have a jumper in place for normal system operation. (**Default**)
	2-3	If pins 2-3 are jumpered with AC power plugged in, the CMOS settings clear in 5 seconds. Pins 2-3 should not be jumpered for normal system operation.
J2K8: BIOS Recovery	1-2	Pins 1-2 should be jumpered for normal system operation. (**Default**)
	2-3	The main system BIOS does not boot with pins 2-3 jumpered. The system only boots from EFI-bootable recovery media with a recovery BIOS image present.
J2K9: Password Clear	1-2	These pins should have a jumper in place for normal system operation.
	2-3	To clear administrator and user passwords, power on the system with pins 2-3 connected. The administrator and user passwords clear in 5-10 seconds after power on. Pins 2-3 should not be connected for normal system operation.
J3K2: ME Force Update	1-2	ME Firmware Force Update Mode – Disabled (**Default**)
	2-3	ME Firmware Force Update Mode – Enabled
J3K6: BMC Force Update	1-2	BMC Firmware Force Update Mode – Disabled (**Default**)
	2-3	BMC Firmware Force Update Mode – Enabled

10.1 BIOS Default Jumper Block

1. This jumper resets BIOS Setup options to their default factory settings.
2. Power down the server and unplug the power cords.
3. Open the chassis and remove the Riser #2 assembly.
4. Move BIOS DFLT jumper from the default (pins 1 and 2) position to the Set BIOS Defaults position (pins 2 and 3).
5. Wait 5 seconds then move the jumper back to the default position of pins 1 and 2.
6. Install riser card assembly.
7. Install Power Cords.
8. Power on system.

Note: BIOS Error Manager should report a 5220 error code (BIOS Settings reset to default settings).

10.2 BIOS Recovery Jumper

When the BIOS Recovery jumper block is moved from its default pin position, the system will boot into a BIOS Recovery Mode. It is used when the system BIOS has become corrupted and is non-functional, requiring a new BIOS image to be loaded on to the server board.

Note: The BIOS Recovery jumper is ONLY used to re-install a BIOS image in the event the BIOS has become corrupted. This jumper is NOT used when the BIOS is operating normally and you need to update the BIOS from one version to another.

The following steps demonstrate the BIOS recovery process:

1. After downloading the latest System Update Package (SUP) from the Intel® website, copy the following files to the root directory of a USB media device:

   - IPMI.EFI
   - IFlash32.EFI
   - RML.ROM
   - ####REC.CAP (where #### = BIOS revision number)
   - STARTUP.NSH
2. Power OFF the system
3. Locate the BIOS Recovery Jumper on the server board and move the jumper block from pins 1-2 (default) to pins 2-3 (recovery setting)
4. Insert the recovery media into a USB port
5. Power ON the system
6. The system will automatically boot into the embedded EFI Shell
7. The STARTUP.NSH file automatically executes and initiates the flash update. When complete, the IFlash utility will display a message
8. Power OFF the system and return the BIOS Recovery jumper to its default position
9. Power ON the system
10. Do *NOT* interrupt the BIOS POST during the first boot.
11. Configure desired BIOS settings

10.3 Password Clear Jumper Block

This jumper causes both the User password and the Administrator password to be cleared if they were set. The operator should be aware that this creates a security gap until passwords have been installed again through the BIOS Setup utility. This is the only method by which the Administrator and User passwords can be cleared unconditionally. Other than this jumper, passwords can only be set or cleared by changing them explicitly in BIOS Setup or by similar means. No method of resetting BIOS configuration settings to default values will affect either the Administrator or User passwords.

1. Power down the server and unplug the power cords.
2. Open the chassis and remove the Riser #2 assembly.
3. Move jumper from the default (pins 1 and 2) operating position to the password clear position (pins 2 and 3).
4. Close the server chassis and reattach the power cords.
5. Power up the server and wait until POST completes.

Note: BIOS Error Manager should report a 5224 and 5221 error codes (Password clear jumper is set and Passwords cleared by jumper).

6. Power down the server and unplug the power cords.
7. Open the chassis, remove the Riser #2 assembly, and move the jumper back to the default position (covering pins 1 and 2).
8. Reinstall the Riser #2 assembly.
9. Close the server chassis and reattach the power cords.
10. Power up the server.

10.4 Management Engine (ME) Firmware Force Update Jumper Block

When the ME Firmware Force Update jumper is moved from its default position, the ME is forced to operate in a reduced minimal operating capacity. This jumper should only be used if the ME firmware has gotten corrupted and requires re-installation. The following procedure should be followed.

Note: System Update and Recovery files are included in the System Update Packages (SUP) posted to Intel's website.

1. Turn off the system and remove power cords.
2. Remove Riser Card Assembly #2.
3. Move the ME FRC UPD Jumper from the default (pins 1 and 2) operating position to the Force Update position (pins 2 and 3).
4. Re-attach system power cords.
5. Power on the system.

Note: System Fans will boost and the BIOS Error Manager should report an 83A0 error code (ME in recovery mode).

6. Boot to the EFI shell and update the ME firmware using the "MEComplete####.cap" file (where #### = ME revision number) using the following command: iflash32 /u /ni MEComplete####.cap.
7. When update has successfully completed, power off system.
8. Remove AC power cords.
9. Move ME FRC UPD jumper back to the default position.

Note: If the ME FRC UPD jumper is moved with AC power applied, the ME will not operate properly. The system will need have the AC power cords removed, wait for at least 10 seconds and then reinstalled to ensure proper operation.

10. Install PCI Riser.

11. Install AC power cords.

12. Power on system.

10.5 BMC Force Update Jumper Block

The BMC Force Update jumper is used to put the BMC in Boot Recovery mode for a low-level update.

It is used when the BMC has become corrupted and is non-functional, requiring a new BMC image to be loaded on to the server board.

1. Turn off the system and remove power cords.

2. Move the BMC FRC UPDT Jumper from the default (pins 1 and 2) operating position to the Force Update position (pins 2 and 3).

3. Re-attach system power cords.

4. Power on the system.

   Note: System Fans will boost and the BIOS Error Manager should report an 84F3 error code (Baseboard Management Controller in update mode).

5. Boot to the EFI shell and update the BMC firmware using BMC####.NSH (where #### is the version number of the BMC).

6. When update has successfully completed, power off system.

7. Remove AC power cords.

8. Move BMC FRC UPDT jumper back to the default position.

9. Install AC power cords.

10. Power on system.

11. Boot to the EFI shell and update the FRU and SDR data using FRUSDR####.nsh (where #### is the version number of the FRUSDR package).

12. Reboot the system.

13. Configure desired BMC configuration settings.

11. Intel® Light Guided Diagnostics

The server board includes several on-board LED indicators to aid troubleshooting various board level faults. The following figure shows the location for each:

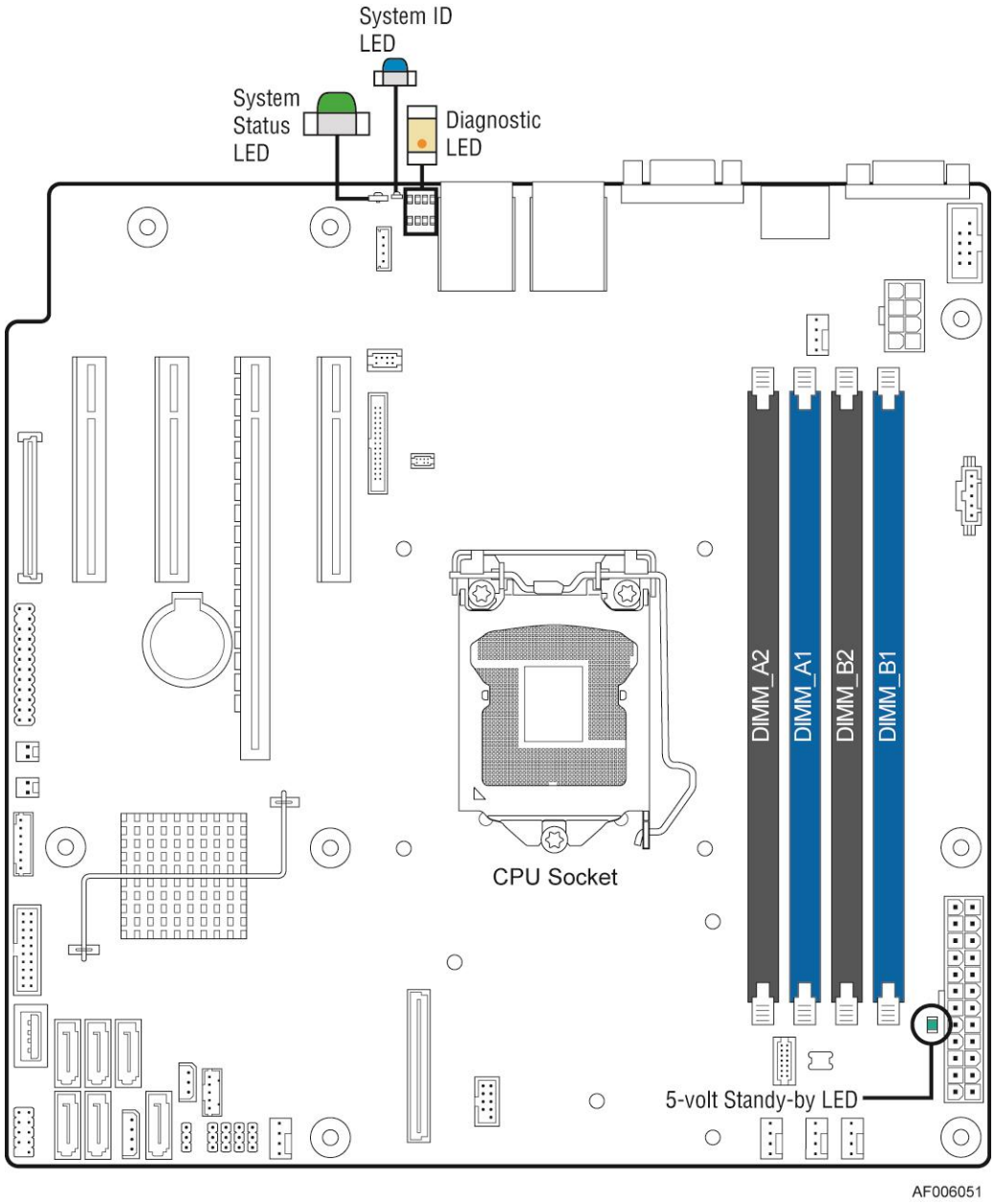


Figure 48. On-Board LED Placement

11.1 System ID LED

The server board includes a blue system ID LED 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.

11.2 System Status LED

The server board includes a bi-color System Status LED. The System Status LED on the server board is tied directly to the System Status LED on the front panel (if present). This LED indicates the current health of the server. Possible LED states include solid green, blinking green, blinking amber, and solid amber.

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

When AC power is first applied to the system, the status LED turns solid amber and then immediately changes to blinking green to indicate that the BMC is booting. If the BMC boot process completes with no errors, the status LED will change to solid green.

Table 59. System Status LED State Definitions

Color	State	Criticality	Description
Off	System is not operating	Not ready	1. System is powered off (AC and/or DC). 2. System is in EuP Lot6 Off Mode. 3. System is in S5 Soft-Off State. 4. System is in S4 Hibernate Sleep State.
Green	Solid on	Ok	Indicates that the System is running (in S0 State) and its status is 'Healthy'. The system is not exhibiting any errors. AC power is present and BMC has booted and manageability functionality is up and running.
Green	~1 Hz blink	Degraded - system is operating in a degraded state although still functional, *or* system is operating in a redundant state but with an impending failure warning	System degraded: Redundancy loss, such as power-supply or fan. Applies only if the associated platform sub-system has redundancy capabilities. Fan warning or failure when the number of fully operational fans is more than minimum number needed to cool the system. Non-critical threshold crossed – Temperature (including HSBP temp), voltage, input power to power supply, output current for main power rail from power supply and Processor Thermal Control (Therm Ctrl) sensors. Power supply predictive failure occurred while redundant power supply configuration was present. Unable to use all of the installed memory (one or more DIMMs

Color	State	Criticality	Description
			failed/disabled but functional memory remains available) Correctable Errors over a threshold and migrating to a spare DIMM (memory sparing). This indicates that the user no longer has spared DIMMs indicating a redundancy lost condition. Corresponding DIMM LED lit. Uncorrectable memory error has occurred in memory Mirroring Mode, causing Loss of Redundancy. Correctable memory error threshold has been reached for a failing DDR3 DIMM when the system is operating in fully redundant RAS Mirroring Mode. Battery failure. BMC executing in uBoot. (Indicated by Chassis ID blinking at Blinking at 3Hz). System in degraded state (no manageability). BMC uBoot is running but has not transferred control to BMC Linux*. Server will be in this state 6-8 seconds after BMC reset while it pulls the Linux* image into flash BMC booting Linux*. (Indicated by Chassis ID solid ON). System in degraded state (no manageability). Control has been passed from BMC uBoot to BMC Linux* itself. It will be in this state for ~10-~20 seconds. BMC Watchdog has reset the BMC. Power Unit sensor offset for configuration error is asserted. HDD HSC is off-line or degraded.
Amber	~1 Hz blink	Non-critical - System is operating in a degraded state with an impending failure warning, although still functioning	Non-fatal alarm – system is likely to fail: Critical threshold crossed – Voltage, temperature (including HSBP temp), input power to power supply, output current for main power rail from power supply and PROCHOT (Therm Ctrl) sensors. VRD Hot asserted. Minimum number of fans to cool the system not present or failed Hard drive fault Power Unit Redundancy sensor – Insufficient resources offset (indicates not enough power supplies present) In non-sparing and non-mirroring mode if the threshold of correctable errors is crossed within the window Correctable memory error threshold has been reached for a failing DDR3 DIMM when the system is operating in a non-redundant mode
Amber	Solid on	Critical, non-recoverable – System is halted	Fatal alarm – system has failed or shutdown: CPU CATERR signal asserted MSID mismatch detected (CATERR also asserts for this case). CPU 1 is missing CPU Thermal Trip No power good – power fault DIMM failure when there is only 1 DIMM present and hence no good memory present. Runtime memory uncorrectable error in non-redundant mode. DIMM Thermal Trip or equivalent SSB Thermal Trip or equivalent CPU ERR2 signal asserted BMC\Video memory test failed. (Chassis ID shows blue/solid-on for this condition) Both uBoot BMC FW images are bad. (Chassis ID shows blue/solid-on for this condition)

Color	State	Criticality	Description
			240VA fault Fatal Error in processor initialization: Processor family not identical Processor model not identical Processor core/thread counts not identical Processor cache size not identical Unable to synchronize processor frequency Unable to synchronize QPI link frequency

11.3 BMC Boot/Reset Status LED Indicators

During the BMC boot or BMC reset process, the System Status LED and System ID LED are used to indicate BMC boot process transitions and states. A BMC boot will occur when AC power is first applied to the system. A BMC reset will occur after: a BMC FW update, upon receiving a BMC cold reset command, and upon a BMC watchdog initiated reset. The following table defines the LED states during the BMC Boot/Reset process.

Table 60. BMC Boot/Reset Status LED Indicators

BMC Boot/Reset State	ID LED	Status LED	Comment
BMC/Video memory test failed	Solid Blue	Solid Amber	Nonrecoverable condition. Contact your Intel® representative for information on replacing this motherboard.
Both Universal Bootloader (u-Boot) images bad	Solid Blue	Solid Amber	Nonrecoverable condition. Contact your Intel® representative for information on replacing this motherboard.
BMC in u-Boot	Blink Blue 3Hz	Blink Green 1Hz	Blinking green indicates degraded state (no manageability), blinking blue indicates u-Boot is running but has not transferred control to BMC Linux*. Server will be in this state 6-8 seconds after BMC reset while it pulls the Linux* image into flash.
BMC Booting Linux*	Solid Blue	Solid Green	Solid green with solid blue after an AC cycle/BMC reset, indicates that the control has been passed from u-Boot to BMC Linux* itself. It will be in this state for ~10-~20 seconds.
End of BMC boot/reset process. Normal system operation	Off	Solid Green	Indicates BMC Linux* has booted and manageability functionality is up and running. Fault/Status LEDs operate as per usual.

11.4 Post Code Diagnostic LEDs

A bank of eight POST code diagnostic LEDs are located on the back edge of the server next to the stacked USB connectors. 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. The purpose of these LEDs is to assist in troubleshooting a system hang condition during the POST process. The diagnostic LEDs can be used to identify the last POST process to be executed. See Appendix D for a complete description of how these LEDs are read, and for a list of all supported POST codes.

11.5 5 Volt Stand-By Present LED

This LED is illuminated when a power cord (AC or DC) is connected to the server and the power supply is supplying 5 Volt Stand-by power to the server board. This LED is intended as a service caution indicator to anyone accessing the inside of the server system.

12. Environmental Limits Specification

The following table defines the Intel® Server Board S1200V3RP series operating and non-operating environmental limits. Operation of the Intel® Server Board S1200V3RP 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 system reliability.

Table 61. Server Board Design Specifications

Operating Temperature	0º C to 55º C 1 (32º F to 131º F)
Non-Operating Temperature	-40º C to 70º C (-40º F to 158º F)
DC Voltage	± 5% of all nominal voltages
Shock (Unpackaged)	Trapezoidal, 35g, 170 inches/sec
Shock (Packaged) < 20 pounds 20 to < 40 pounds 40 to < 80 pounds 80 to < 100 pounds 100 to < 120 pounds 120 pounds	 36 inches 30 inches 24 inches 18 inches 12 inches 9 inches
Vibration (Unpackaged)	5 Hz to 500 Hz 3.13 g RMS random

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 its published operating or non-operating limits.

Disclaimer Note: *Intel ensures the unpackaged server board and system meet the shock requirement mentioned above through its own chassis development and system configuration. It is the responsibility of the system integrator to determine the proper shock level of the board and system if the system integrator chooses different system configuration or different chassis. Intel Corporation cannot be held responsible if components fail or the server board does not operate correctly when used outside any of its published operating or non-operating limits.*

12.1 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 (TCASE) 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 E3-1200 V3/V4 product family TDP guidelines up to and including 95W.

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.

12.2 MTBF

The following is the calculated Mean Time Between Failures (MTBF) 40 degree C (ambient air). These values are derived using a historical failure rate and multiplied by factors for application, electrical and/or thermal stress and for device maturity. You should view MTBF estimates as "reference numbers" only.

- Calculate standard: Telcordia* issue 2
- Calculate Method: Method I-D
- Temperature = 40 degree C
- Environment = GB, GC – Ground Benign, Controlled
- Model = Serial
- Duty cycle = 100%
- Component Quality: Level II
- Adhere to De-rating data

Table 62. MTBF Estimate

Assembly Name	Temperature (Degree C)	MTBF (hours)
Intel® Server Board S1200V3RPL	40	283,887
Intel® Server Board S1200V3RPS	40	290,843
Intel® Server Board S1200V3RPO	40	286,078
Intel® Server Board S1200V3RPM	40	277,497

13. Server Board Power Distribution

This section provides power supply design guidelines for a system using the Intel® Server Board S1200V3RP. The following diagram shows the power distribution implemented on this server board.

The power supply data provided in this section is for reference purposes only. It reflects Intel's own DC power out requirements for a 365W power supply as used in an Intel designed 4U 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.

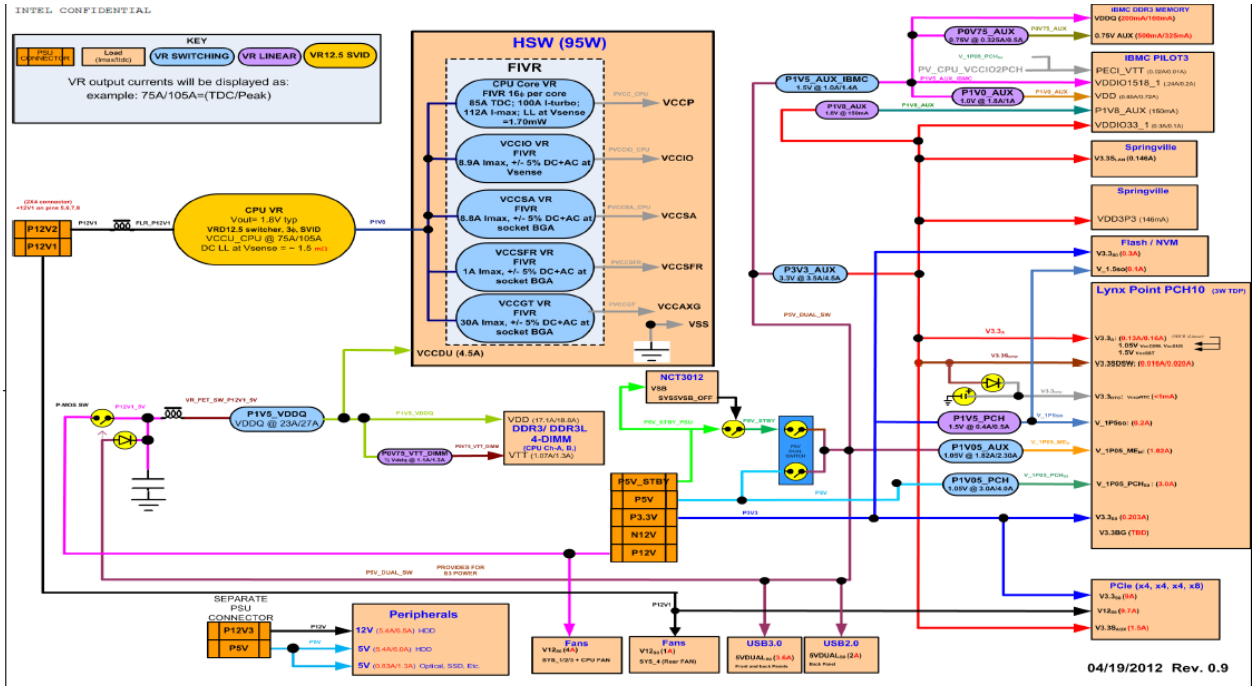


Figure 49. Power Distribution Block Diagram

13.1 DC Output Specification

13.1.1 Output Power/Currents

The following table defines the minimum power and current ratings. The power supply meets both static and dynamic voltage regulation requirements for all conditions.

Table 63. Over Voltage Protection Limits

Parameter	Min	Max.	Peak	Unit
5V	0.3	10.0		A
12V1	0.7	16.0	18.0	A
12V2	1.5	16.0	18.0	A
3.3V	0.5	18.0		A
– 12V	0.0	0.5		A

Parameter	Min	Max.	Peak	Unit
5Vstby	0.0	2.5	3.0	A

Note:

1. Max combined power for all output shall not exceed 350W.
2. Peak combined power for all outputs shall not exceed 400W.
3. Max combined power of 12V1 and 12V2 shall not exceed 318W.
4. Max combined power on 3.3V and 5V shall not exceed 100W.
5. Peak power and current loading shall be supported for a minimum of 12 second.

13.1.2 Cross Loading

The power supply maintains voltage regulation limit when operated over the following cross loading conditions.

Table 64. Loading Conditions

	3.3V	5.0V	12.0V	12.0V	12.0V	5.0V	Total Power	12V Power	3.3V/5V Power
Load1	10.8	2	16	10.5	0	0.3	365	318	46
Load2	18	4.1	7.6	16	0	0.3	365	283	80
Load3	18	4.1	16	7.6	0	0.3	365	283	80
Load4	13.6	7	10.2	12	0.5	2.5	365	266	80
Load5	0.5	0.3	0.7	1.5	0	0.3	31	26	3
Load6	16	4	0.7	2.6	0	0.3	114	40	73
Load7	1.2	2.7	14.5	7.1	0	1	282	259	17

13.1.3 Standby Output

The 5VSB output is present when an AC input greater than the power supply turn on voltage is applied.

13.1.4 Voltage Regulation

The power supply output voltages 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 65. Voltage Regulation Limits

PARAMETER	TOLERANCE	MIN	NOM	MAX	UNITS
+3.3V	- 5%/+5%	+3.14	+3.30	+3.46	V_{rms}
+5V	- 5%/+5%	+4.75	+5.00	+5.25	V_{rms}
+12V1	- 5%/+5%	+11.40	+12.00	+12.60	V_{rms}
+12V2	- 5%/+5%	+11.40	+12.00	+12.60	V_{rms}
- 12V	- 10%/+10%	- 13.20	-12.00	-10.80	V_{rms}
+5VSB	- 5%/+5%	+4.75	+5.00	+5.25	V_{rms}

13.1.5 Dynamic Loading

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

Table 66. Transient Load Requirements

Output	Δ Step Load Size (See note 2)	Load Slow Rate	Test capacitive Load
+3.3V	6.0A	0.5 A/μsec	970 μF
+5V	4.0A	0.5 A/μsec	400 μF
12V1+12V2	18.0A	0.5 A/μsec	2200 μF [1,2]
+5VSB	0.5A	0.5 A/μsec	20 μF

Note:

1. Step loads on each 12V output may happen simultaneously.

2. The +12V should be tested with 2200μF evenly split between the four +12V rails.

13.1.6 Capacitive Loading

The power supply is stable and meets all requirements with the following capacitive loading ranges.

Table 67. Capacitive Loading Conditions

Output	MIN	MAX	Units
+3.3V	250	5000	μF
+5V	400	5000	μF
+12V	500	8000	μF
-12V	1	350	μF
+5VSB	20	350	μF

13.1.7 Grounding

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

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

13.1.8 Residual Voltage Immunity in Standy mode

The power supply is immune to any residual voltage placed on its outputs (Typically a leakage voltage through the system from standby output) up to **500mV**. There is neither additional heat generated, nor stressing of any internal components with this voltage applied to any individual or all outputs simultaneously. It also does not trip the protection circuits during turn on.

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

13.1.9 Common Mode Noise

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

The measurement is made across a 100Ω resistor between each of DC outputs, including ground at the DC power connector and chassis ground (power subsystem enclosure).

The test set-up shall use a FET probe such as Tektronix* model P6046 or equivalent.

13.1.10 Ripple/Noise

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

Table 68. Ripples and Noise

+3.3V	+5V	+12V 1	+12V 2	-12V	+5VSB
50mVp-p	50mVp-p	120mVp-p	120mVp-p	200mVp-p	50mVp-p

The test set-up shall be as shown below.

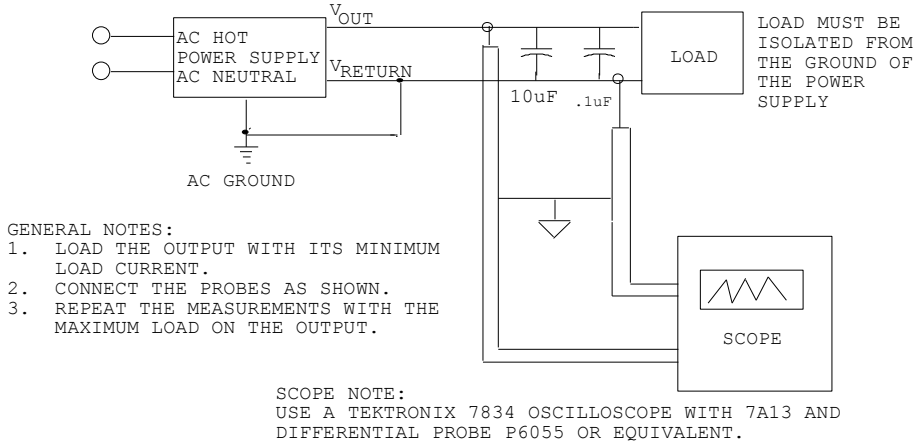


Figure 50. Differential Noise test setup

Note: When performing this test, the probe clips and capacitors should be located close to the load.

13.1.11 Timing Requirements

These are the timing requirements for the power supply operation. The output voltages rise from 10% to within regulation limits (T_{vout_rise}) within 2 to 50ms, except for 5VSB - it is allowed to rise from 1 to 25ms. The +3.3V, +5V and +12V1, +12V2 output voltages should start to rise approximately at the same time. All outputs must rise monotonically. Each output voltage reach regulation within 50ms (T_{vout_on}) of each other during turn on the power supply. Each output voltage fall out of regulation within 400ms (T_{vout_off}) of each other during turn off. The table below

shows the timing requirements for the power supply being turned on and off from the AC input, with PSON held low and the PSON signal, with the AC input applied.

Table 69. Output Voltage Timing

Item	Description	MIN	MAX	UNITS
T_{vout_rise}	Output voltage rise time from each main output.	2	50	ms
	Output rise time for the 5Vstby output.	1	25	ms
T_{vout_on}	All main outputs must be within regulation of each other within this time.		50	ms
T_{vout_off}	All main outputs must leave regulation within this time.		400	ms

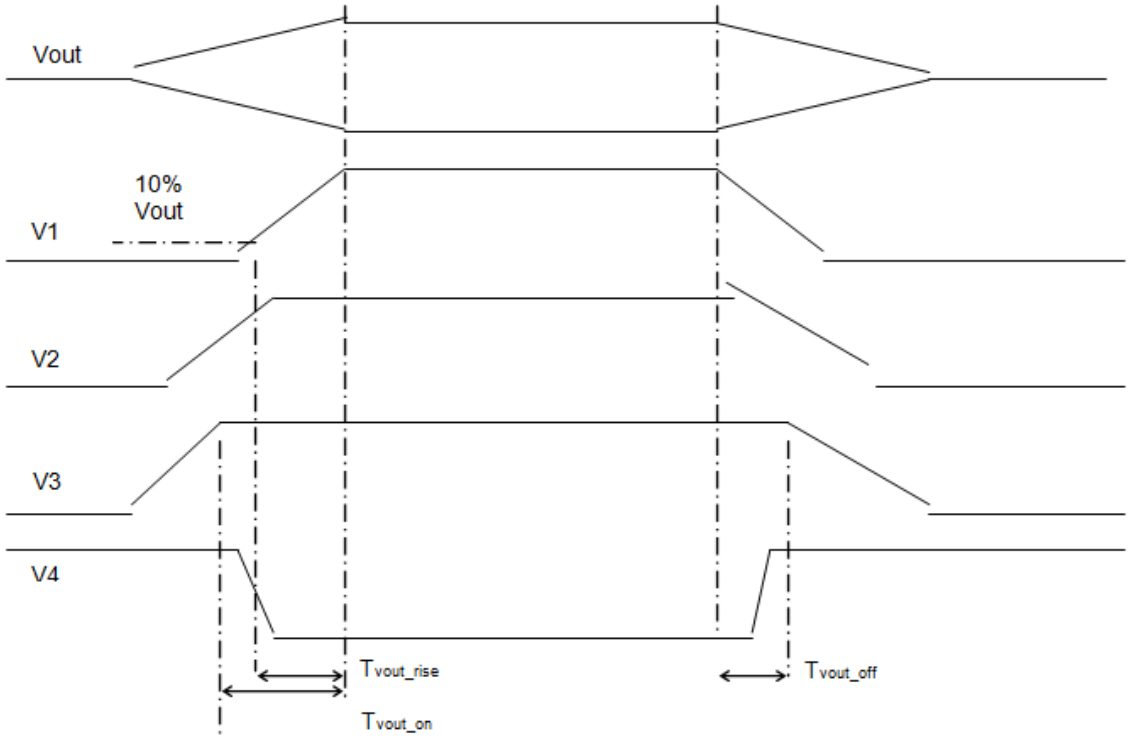


Figure 51. Output Voltage Timing

Table 70. Turn On/Off Timing

Item	Description	Min.	Max.	Units
$T_{sb\_on\_delay}$	Delay from AC being applied to 5VSB being within regulation.		1500	ms
$T_{ac\_on\_delay}$	Delay from AC being applied to all output voltages being within regulation.		2500	ms
T_{vout_holdup}	Time all output voltages stay within regulation after loss of AC. Tested at 75% of maximum load.	13		ms
T_{pwok_holdup}	Delay from loss of AC to de-assertion of PWOK. Tested at 75% of maximum load.	12		ms
$T_{pson\_on\_delay}$	Delay from PSON# active to output voltages within regulation limits.	5	400	ms

Item	Description	Min.	Max.	Units
T_{pson_pwok}	Delay from PSON# deactivate to PWOK being de-asserted.		50	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 (3.3V, 5V, 12V, -12V) 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 5VSB being in regulation to O/Ps being in regulation at AC turn on.	10	1000	ms
T_{5VSB_holdup}	Time the 5VSB output voltage stays within regulation after loss of AC.	70		ms

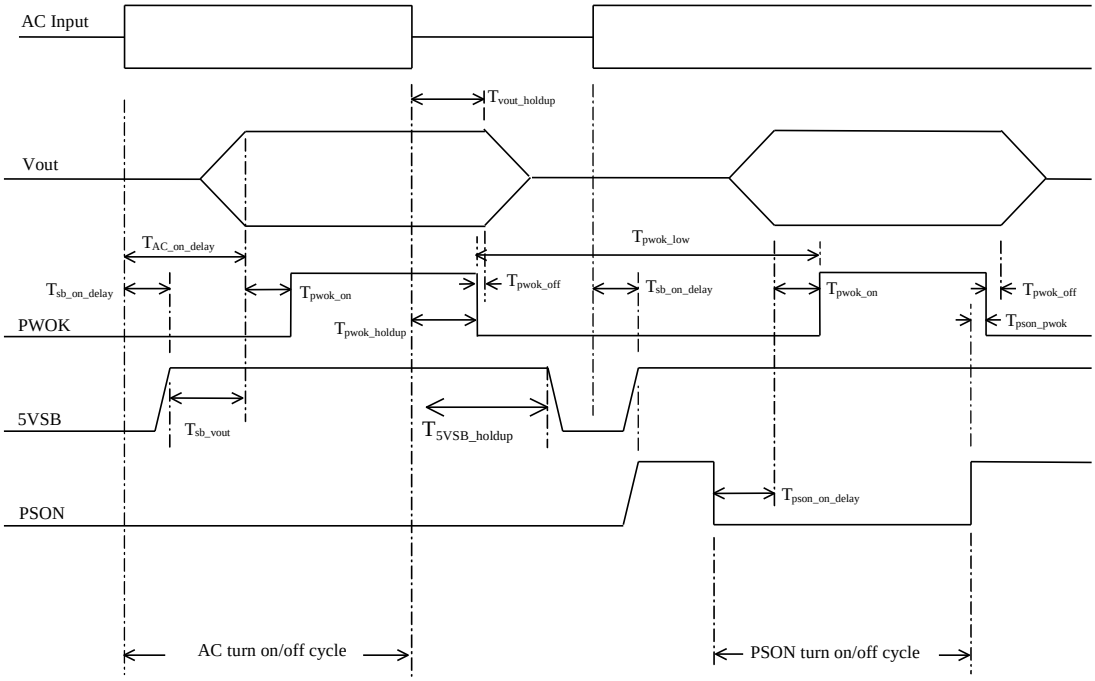


Figure 52. Turn On/Off Timing (Power Supply Signals)

Appendix A: Integration and Usage Tips

- When adding or removing components or peripherals from the server board, you must remove AC power cord. 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 Intel® Xeon® Processor E3-1200 V3/V4 product family with a Thermal Design Power (TDP) of up to and including 95 Watts. Previous generation Intel® Xeon® processors are not supported.
- The PCIe slot 4 does NOT support the Intel® PCIe gen3 ROC modules.
- The onboard SATA connectors 0 and 1 are designed to support the ODD or SSD, do NOT connect SATA connector 0 and 1 to the backplane. The onboard SATA connectors 2-5 are designed to support the backplane.
- 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.
- Only Unbuffered DDR3L DIMMs (UDIMMs) are supported on this server board. Mixing of RDIMMs and UDIMMs is not supported.
- The Intel® RMM4/RMM4 Lite connectors are not compatible with the previous Intel® Remote Management Modules
- Clear CMOS with the AC power cord plugged in. Removing 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 BMC functionality is disabled with the Force BMC Update jumper (J3K6) set to the “enabled” position (pins 2-3). You should never run the server with the Force BMC Update jumper set in this position and should only use the jumper in this position when the standard firmware update process fails. This jumper must remain in the default (disabled) position (pins 1-2) when the server is running normally.
- This server board no longer supports the Rolling BIOS (two BIOS banks). It implements the BIOS Recovery mechanism instead.
- When performing a normal BIOS update procedure, you must set the BIOS Recovery jumper (J2K8) 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 is the value 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 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 with only two states.

- **Event Offset/Triggers**

  Event Thresholds are event-generating thresholds for threshold type sensors.

  - [u,l][nr,c,nc]: upper nonrecoverable, upper critical, upper noncritical, lower nonrecoverable, lower critical, lower noncritical
  - uc, lc: upper critical, lower critical

  Event Triggers are supported, event-generating offsets for discrete type sensors. You can find the offsets 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 Values indicate 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 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 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 of a sensor to be rechecked and updated upon a transition between good and bad states. You can rearm the sensors manually or automatically. This column indicates the type supported by the sensor. The following abbreviations are used in the comment column 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 is 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. You can access these sensors and/or generate events when the main (system) power is off but AC power is present.

Table 71. Integrated 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	Standby
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 1 (Pwr Unit Redund)	02h	Chassis-specific	Power Unit 09h	Generic 0Bh	00 - Fully Redundant	OK	As and De	–	Trig Offset	M	X
					01 - Redundancy lost	Degraded					
					02 - Redundancy degraded	Degraded					
					03 - Non-redundant: sufficient resources. Transition from full redundant state.	Degraded					
					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	03h	All	Watchdog 2	Sensor Specifi	00 - Timer expired, status only	OK	As	–	Trig Offset	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	Standby
(IPMI Watchdog)			23h	c 6Fh	01 - Hard reset 02 - Power down 03 - Power cycle 08 - Timer interrupt						
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	02 - Undetermined system H/W failure 04 – PEF action	Fatal OK	As and De As	-	Trig Offset	A	X
Button Sensor (Button)	09h	All	Button/ Switch 14h	Sensor Specific 6Fh	00 – 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	-
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 01 - Redundancy lost 02 - Redundancy degraded 03 - Non-redundant:	OK Degraded Degraded Degrad	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	Standby
					Sufficient resources. Transition from redundant	ed					
					04 - Non-redundant: Sufficient resources. Transition from insufficient.	Degraded					
					05 - Non-redundant: insufficient resources.	Non-Fatal					
					06 – Non-Redundant: degraded from fully 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	-
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

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	Standby
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	–
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

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	Standby
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
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	2A	Chassis-specific	Temperature	Threshold	[u,l] [c,nc]	nc = Degrad	As and	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	Standby
Temperature (HSBP 2 Temp)	h		01h	01h		ed c = Non-fatal	De				
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
Fan Tachometer Sensors (Chassis specific sensor names)	30h–3Fh	Chassis and Platform Specific	Fan 04h	Threshold 01h	[l] [c,nc]	nc = Degraded c = Non-fatal2	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 (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	Degrad					

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	Standby
					Failure	ed					
					03 - A/C lost	Degraded					
					06 – Configuration error	OK					
Power Supply 2 Status (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					
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
Power	5	Chassis-	Temper	Thresh	[u] [c,nc]	nc =	As	Analo	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	Standby
Supply 2 Temperature (PS2 Temperature)	Dh	specific	ature	old 01h		Degraded c = Non-fatal	and De	g			
Hard Disk Drive 16 - 24 Status (HDD 16 - 24 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					
					07 - Rebuild/Remap in progress	Degraded		–	Trig Offset		X
					04- transition to Off Line	Degraded					
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					
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	77	Platform-	Temper	Thresh	-	-	-	Analo	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	Standby
Thermal Margin (P4 Therm Margin)	h	specific	ature 01h	old 01h				g			
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	–
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	–
Processor1	81	All	Proces	Digital	01 – State Asserted	fatal	As	–	Trig	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	Standby
MSID Mismatch (P1 MSID Mismatch)	h		sor 07h	Discrete 03h			and De		Offset		
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	–
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	M	–
Processor 2 VRD Temperature (P2 VRD Hot)	91h	All	Temperature 01h	Digital Discrete 05h	01 - Limit exceeded	Non-fatal	As and De	–	Trig Offset	M	–
Processor 3	92	All	Temper	Digital	01 - Limit exceeded	Fatal	As	–	Trig	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	Standby
VRD Temperature (P3 VRD Hot)	h		ature 01h	Discrete 05h			and De		Offset		
Processor 4 VRD Temperature (P4 VRD Hot)	93h	All	Temperature 01h	Digital Discrete 05h	01 - Limit exceeded	Fatal	As and De	–	Trig Offset	M	–
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	–
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	–
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	–

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	Standby
Power Supply 1 Fan Tachometer 1 (PS1 Fan Tach 1)	A 0h	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)	A 1h	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)	A 4h	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)	A 5h	Chassis-specific	Fan 04h	Generic – digital discrete	01 – State Asserted	Non-fatal	As and De	-	Trig Offset	M	-
Processor 1 DIMM Aggregate Thermal Margin 1 (P1 DIMM Thrm Mrgn1)	B 0h	All	Temperature 01h	Threshold 01h	[u,l] [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)	B 1h	All	Temperature 01h	Threshold 01h	[u,l] [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)	B 2h	All	Temperature 01h	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	Standby
Processor 2 DIMM Aggregate Thermal Margin 2 (P2 DIMM Thrm Mrgn2)	B 3h	All	Temperature 01h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	–
Processor 3 DIMM Aggregate Thermal Margin 1 (P3 DIMM Thrm Mrgn1)	B 4h	Platform Specific	Temperature 01h	Threshold 01h	[u,l] [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)	B 5h	Platform Specific	Temperature 01h	Threshold 01h	[u,l] [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)	B 6h	Platform Specific	Temperature 01h	Threshold 01h	[u,l] [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)	B 7h	Platform Specific	Temperature 01h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	–
Fan Tachometer Sensors (Chassis specific sensor names)	BAh–BFh	Chassis and Platform Specific	Fan 04h	Threshold 01h	[l] [c,nc]	nc = Degraded c = Non-fatal2	As and De	Analog	R, T	M	-
Processor 1 DIMM Thermal Trip (P1 Mem	C 0h	All	Memory 0Ch	Digital Discrete 03h	0A- Critical overtemperature	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	Standby
Thrm Trip)											
Processor 2 DIMM Thermal Trip (P2 Mem Thrm Trip)	C 1h	All	Memory 0Ch	Digital Discrete 03h	0A- Critical over temperature	Fatal	As and De	–	Trig Offset	M	-
Processor 3 DIMM Thermal Trip (P3 Mem Thrm Trip)	C 2h	All	Memory 0Ch	Digital Discrete 03h	0A- Critical overtemperature	Fatal	As and De	–	Trig Offset	M	X
Processor 4 DIMM Thermal Trip (P4 Mem Thrm Trip)	C 3h	All	Memory 0Ch	Digital Discrete 03h	0A- Critical overtemperature	Fatal	As and De	–	Trig Offset	M	X
Global Aggregate Temperature Margin 1 (Agg Therm Mrgn 1)	C 8h	Platform Specific	Temperature 01h	Threshold 01h	-	-	-	Analog	R, T	A	–
Global Aggregate Temperature Margin 2 (Agg Therm Mrgn 2)	C 9h	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	–
Global Aggregate Temperature	CDh	Platform Specific	Temperature	Threshold	-	-	-	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	Standby
Margin 6 (Agg Therm Mrgn 6)			01h	01h							
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	–
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	D6h	All	Voltage 02h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-	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	Standby
+1.05Vccp P1)						fatal					
Baseboard +1.05V Processor2 Vccp (BB +1.05Vccp P2)	D 7h	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)	D 8h	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 CD VDDQ (BB +1.5 P1MEM CD)	D 9h	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-	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	Standby
						fatal					
Baseboard +1.35V P1 Low Voltage Memory AB VDDQ (BB +1.35 P1LV AB)	E 4h	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)	E 5h	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)	E 6h	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)	E 7h	All	Voltage 02h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	–
Baseboard +3.3V Riser 1 Power Good (BB +3.3 RSR1 PGD)	EA h	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)	EB h	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 1 -15 Status (HDD 1 - 15 Status)	F 0h - FE h	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					

Note:

3. Redundancy sensors will be only present on systems with appropriate hardware to support redundancy (for instance, fan or power supply).

4. 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: POST Code Diagnostic LED Decoder

As an aid to assist in trouble shooting a system hang that occurs during a system's Power-On Self Test (POST) process, the server board includes a bank of eight POST Code Diagnostic LEDs on the back edge of the server board.

During the system boot process, Memory Reference Code (MRC) and System BIOS execute a number of memory initialization and platform configuration processes, each of which is assigned a specific hex POST code number. As each routine is started, the given POST code number is displayed to the POST Code Diagnostic LEDs on the back edge of the server board.

During a POST system hang, the displayed post code can be used to identify the last POST routine that was run prior to the error occurring, helping to isolate the possible cause of the hang condition.

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

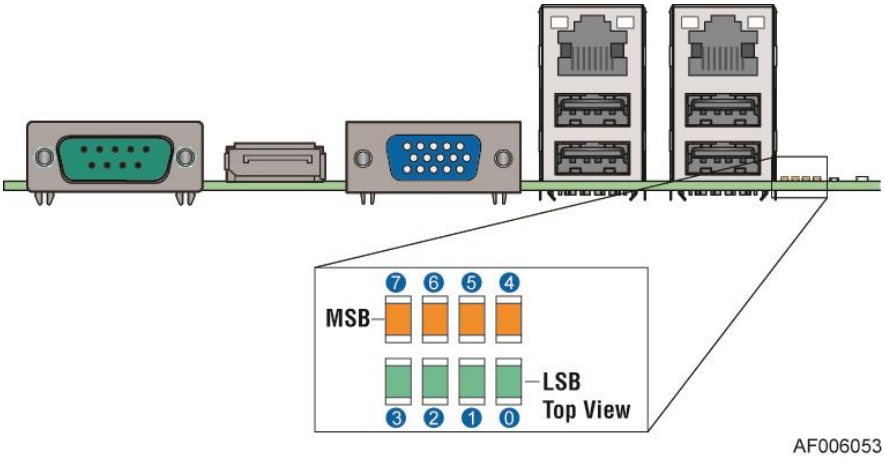


Figure 53. POST Code Diagnostic LEDs

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

Note: Diag LEDs are best read and decoded when viewing the LEDs from the back of the system.

Table 72. POST Progress Code LED Example

LEDs	Upper Nibble AMBER LEDs				Lower Nibble GREEN 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

The following table provides a list of all POST progress codes.

Table 73. POST Progress Codes

Checkpoint	Diagnostic LED Decoder 1 = LED On, 0 = LED Off								Description
	Upper Nibble				Lower Nibble				
	MSB							LSB	
	8h	4h	2h	1h	8h	4h	2h	1h	
LED #	#7	#6	#5	#4	#3	#2	#1	#0	
SEC Phase									
01h	0	0	0	0	0	0	0	1	First POST code after CPU reset
02h	0	0	0	0	0	0	1	0	Microcode load begin
03h	0	0	0	0	0	0	1	1	CRAM initialization begin
04h	0	0	0	0	0	1	0	0	Pei Cache When Disabled
05h	0	0	0	0	0	1	0	1	SEC Core At Power On Begin.
06h	0	0	0	0	0	1	1	0	Early CPU initialization during Sec Phase.
07h	0	0	0	0	0	1	1	1	Early SB initialization during Sec Phase.
08h	0	0	0	0	1	0	0	0	Early NB initialization during Sec Phase.
09h	0	0	0	0	1	0	0	1	End Of Sec Phase.
0Eh	0	0	0	0	1	1	1	0	Microcode Not Found.
0Fh	0	0	0	0	1	1	1	1	Microcode Not Loaded.
PEI Phase									
10h	0	0	0	1	0	0	0	0	PEI Core
11h	0	0	0	1	0	0	0	1	CPU PEIM
15h	0	0	0	1	0	1	0	1	NB PEIM
19h	0	0	0	1	1	0	0	1	SB PEIM
MRC Process Codes – MRC Progress Code Sequence is executed									
PEI Phase continued…									
31h	0	0	1	1	0	0	0	1	Memory Installed
32h	0	0	1	1	0	0	1	0	CPU PEIM (Cpu Init)
33h	0	0	1	1	0	0	1	1	CPU PEIM (Cache Init)
34h	0	0	1	1	0	1	0	0	CPU PEIM (BSP Select)
35h	0	0	1	1	0	1	0	1	CPU PEIM (AP Init)
36h	0	0	1	1	0	1	1	0	CPU PEIM (CPU SMM Init)
4Fh	0	1	0	0	1	1	1	1	Dxe IPL started
DXE Phase									
60h	0	1	1	0	0	0	0	0	DXE Core started
61h	0	1	1	0	0	0	0	1	DXE NVRAM Init
62h	0	1	1	0	0	0	1	0	SB RUN Init
63h	0	1	1	0	0	0	1	1	Dxe CPU Init
68h	0	1	1	0	1	0	0	0	DXE PCI Host Bridge Init
69h	0	1	1	0	1	0	0	1	DXE NB Init
6Ah	0	1	1	0	1	0	1	0	DXE NB SMM Init
70h	0	1	1	1	0	0	0	0	DXE SB Init

Checkpoint	Diagnostic LED Decoder 1 = LED On, 0 = LED Off								Description
	Upper Nibble				Lower Nibble				
	MSB							LSB	
	8h	4h	2h	1h	8h	4h	2h	1h	
LED #	#7	#6	#5	#4	#3	#2	#1	#0	
71h	0	1	1	1	0	0	0	1	DXE SB SMM Init
72h	0	1	1	1	0	0	1	0	DXE SB devices Init
78h	0	1	1	1	1	0	0	0	DXE ACPI Init
79h	0	1	1	1	1	0	0	1	DXE CSM Init
90h	1	0	0	1	0	0	0	0	DXE BDS Started
91h	1	0	0	1	0	0	0	1	DXE BDS connect drivers
92h	1	0	0	1	0	0	1	0	DXE PCI Bus begin
93h	1	0	0	1	0	0	1	1	DXE PCI Bus HPC Init
94h	1	0	0	1	0	1	0	0	DXE PCI Bus enumeration
95h	1	0	0	1	0	1	0	1	DXE PCI Bus resource requested
96h	1	0	0	1	0	1	1	0	DXE PCI Bus assign resource
97h	1	0	0	1	0	1	1	1	DXE CON_OUT connect
98h	1	0	0	1	1	0	0	0	DXE CON_IN connect
99h	1	0	0	1	1	0	0	1	DXE SIO Init
9Ah	1	0	0	1	1	0	1	0	DXE USB start
9Bh	1	0	0	1	1	0	1	1	DXE USB reset
9Ch	1	0	0	1	1	1	0	0	DXE USB detect
9Dh	1	0	0	1	1	1	0	1	DXE USB enable
A1h	1	0	1	0	0	0	0	1	DXE IDE begin
A2h	1	0	1	0	0	0	1	0	DXE IDE reset
A3h	1	0	1	0	0	0	1	1	DXE IDE detect
A4h	1	0	1	0	0	1	0	0	DXE IDE enable
A5h	1	0	1	0	0	1	0	1	DXE SCSI begin
A6h	1	0	1	0	0	1	1	0	DXE SCSI reset
A7h	1	0	1	0	0	1	1	1	DXE SCSI detect
A8h	1	0	1	0	1	0	0	0	DXE SCSI enable
A9h	1	0	1	0	1	0	0	1	DXE verifying SETUP password
ABh	1	0	1	0	1	0	1	1	DXE SETUP start
ACh	1	0	1	0	1	1	0	0	DXE SETUP input wait
ADh	1	0	1	0	1	1	0	1	DXE Ready to Boot
AEh	1	0	1	0	1	1	1	0	DXE Legacy Boot
AFh	1	0	1	0	1	1	1	1	DXE Exit Boot Services
B0h	1	0	1	1	0	0	0	0	RT Set Virtual Address Map Begin
B1h	1	0	1	1	0	0	0	1	RT Set Virtual Address Map End
B2h	1	0	1	1	0	0	1	0	DXE Legacy Option ROM init
B3h	1	0	1	1	0	0	1	1	DXE Reset system
B4h	1	0	1	1	0	1	0	0	DXE USB Hot plug
B5h	1	0	1	1	0	1	0	1	DXE PCI BUS Hot plug
B6h	1	0	1	1	0	1	1	0	DXE NVRAM cleanup
B7h	1	0	1	1	0	1	1	1	DXE Configuration Reset
00h	0	0	0	0	0	0	0	0	INT19

Checkpoint	Diagnostic LED Decoder 1 = LED On, 0 = LED Off								Description
	Upper Nibble				Lower Nibble				
	MSB							LSB	
	8h	4h	2h	1h	8h	4h	2h	1h	
LED #	#7	#6	#5	#4	#3	#2	#1	#0	
S3 Resume									
E0h	1	1	0	1	0	0	0	0	S3 Resume PEIM (S3 started)
E1h	1	1	0	1	0	0	0	1	S3 Resume PEIM (S3 boot script)
E2h	1	1	0	1	0	0	1	0	S3 Resume PEIM (S3 Video Repost)
E3h	1	1	0	1	0	0	1	1	S3 Resume PEIM (S3 OS wake)
BIOS Recovery									
F0h	1	1	1	1	0	0	0	0	PEIM which detected forced Recovery condition
F1h	1	1	1	1	0	0	0	1	PEIM which detected User Recovery condition
F2h	1	1	1	1	0	0	1	0	Recovery PEIM (Recovery started)
F3h	1	1	1	1	0	0	1	1	Recovery PEIM (Capsule found)
F4h	1	1	1	1	0	1	0	0	Recovery PEIM (Capsule loaded)

POST Memory Initialization MRC Diagnostic Codes

There are two types of POST Diagnostic Codes displayed by the MRC during memory initialization; Progress Codes and Fatal Error Codes.

The MRC Progress Codes are displays to the Diagnostic LEDs that show the execution point in the MRC operational path at each step.

Table 74. MRC Progress Codes

Checkpoint	Diagnostic LED Decoder 1 = LED On, 0 = LED Off								Description
	Upper Nibble				Lower Nibble				
	MSB							LSB	
	8h	4h	2h	1h	8h	4h	2h	1h	
LED	#7	#6	#5	#4	#3	#2	#1	#0	
MRC Progress Codes									
B0h	1	0	1	1	0	0	0	0	Detect DIMM population
B1h	1	0	1	1	0	0	0	1	Set DDR3 frequency
B2h	1	0	1	1	0	0	1	0	Gather remaining SPD data
B3h	1	0	1	1	0	0	1	1	Program registers on the memory controller level
B4h	1	0	1	1	0	1	0	0	Evaluate RAS modes and save rank information
B5h	1	0	1	1	0	1	0	1	Program registers on the channel level
B6h	1	0	1	1	0	1	1	0	Perform the JEDEC defined initialization sequence
B7h	1	0	1	1	0	1	1	1	Train DDR3 ranks
B8h	1	0	1	1	1	0	0	0	Initialize CLTT/OLTT
B9h	1	0	1	1	1	0	0	1	Hardware memory test and init
BAh	1	0	1	1	1	0	1	0	Execute software memory init
BBh	1	0	1	1	1	0	1	1	Program memory map and interleaving
BCh	1	0	1	1	1	1	0	0	Program RAS configuration

Checkpoint	Diagnostic LED Decoder 1 = LED On, 0 = LED Off Upper Nibble				Lower Nibble				Description
	MSB							LSB	
	8h	4h	2h	1h	8h	4h	2h	1h	
LED	#7	#6	#5	#4	#3	#2	#1	#0	
BFh	1	0	1	1	1	1	1	1	MRC is done

Memory Initialization at the beginning of POST includes multiple functions, including: discovery, channel training, validation that the DIMM population is acceptable and functional, initialization of the IMC and other hardware settings, and initialization of applicable RAS configurations.

When a major memory initialization error occurs and prevents the system from booting with data integrity, a beep code is generated, the MRC will display a fatal error code on the diagnostic LEDs, and a system halt command is executed. Fatal MRC error halts do NOT change the state of the System Status LED, and they do NOT get logged as SEL events. The following table lists all MRC fatal errors that are displayed to the Diagnostic LEDs.

Table 75. POST Progress LED Codes

Checkpoint	Diagnostic LED Decoder 1 = LED On, 0 = LED Off Upper Nibble				Lower Nibble				Description
	MSB							LSB	
	8h	4h	2h	1h	8h	4h	2h	1h	
LED	#7	#6	#5	#4	#3	#2	#1	#0	
MRC Fatal Error Codes									
E8h	1	1	1	0	1	0	0	0	No usable memory error 01h = No memory was detected from the SPD read, or invalid config that causes no operable memory. 02h = Memory DIMMs on all channels of all sockets are disabled due to hardware memtest error. 3h = No memory installed. All channels are disabled.
E9h	1	1	1	0	1	0	0	1	Memory is locked by Intel® Trusted Execution Technology and is inaccessible
EAh	1	1	1	0	1	0	1	0	DDR3 channel training error 01h = Error on read DQ/DQS (Data/Data Strobe) init 02h = Error on Receive Enable 3h = Error on Write Leveling 04h = Error on write DQ/DQS (Data/Data Strobe
EBh	1	1	1	0	1	0	1	1	Memory test failure 01h = Software memtest failure. 02h = Hardware memtest failed. 03h = Hardware Memtest failure in Lockstep Channel mode requiring a channel to be disabled. This is a fatal error which requires a reset and calling MRC with a different RAS mode to retry.

Checkpoint	Diagnostic LED Decoder								Description
	1 = LED On, 0 = LED Off								
	Upper Nibble				Lower Nibble				
	MSB							LSB	
	8h	4h	2h	1h	8h	4h	2h	1h	
LED	#7	#6	#5	#4	#3	#2	#1	#0	
EDh	1	1	1	0	1	1	0	1	DIMM configuration population error 01h = Different DIMM types (UDIMM, RDIMM, LRDIMM) are detected installed in the system. 02h = Violation of DIMM population rules. 03h = The 3rd DIMM slot cannot be populated when QR DIMMs are installed. 04h = UDIMMs are not supported in the 3rd DIMM slot. 05h = Unsupported DIMM Voltage.
EFh	1	1	1	0	1	1	1	1	Indicates a CLTT table structure error

Appendix D: POST Code Errors

Most error conditions encountered during POST are reported using POST Error Codes. These codes represent specific failures, warnings, or are informational. POST Error Codes may be displayed in the Error Manager display screen, and are always logged to the System Event Log (SEL). Logged events are available to System Management applications, including Remote and Out of Band (OOB) management.

There are exception cases in early initialization where system resources are not adequately initialized for handling POST Error Code reporting. These cases are primarily Fatal Error conditions resulting from initialization of processors and memory, and they are handed by a Diagnostic LED display with a system halt.

The following table lists the supported POST Error Codes. Each error code is assigned an error type which determines the action the BIOS will take when the error is encountered. Error types include Minor, Major, and Fatal. The BIOS action for each is defined as follows:

- **Minor**: The error message is displayed on the screen or on the Error Manager screen, and an error is logged to the SEL. The system continues booting in a degraded state. The user may want to replace the erroneous unit. The POST Error Pause option setting in the BIOS setup does not have any effect on this error.
- **Major:** The error message is displayed on the Error Manager screen, and an error is logged to the SEL. The POST Error **Pause** option setting in the BIOS setup determines whether the system pauses to the Error Manager for this type of error so the user can take immediate corrective action or the system continues booting.

  Note: For 0048 "Password check failed", the system halts, and then after the next reset/reboot will displays the error code on the Error Manager screen.

- **Fatal**: The system halts during post at a blank screen with the text **"Unrecoverable fatal error found. System will not boot until the error is resolved"** and **"Press <F2> to enter setup"** The POST Error Pause option setting in the BIOS setup does not have any effect with this class of error.

  When the operator presses the **F2** key on the keyboard, the error message is displayed on the Error Manager screen, and an error is logged to the SEL with the error code. The system cannot boot unless the error is resolved. The user needs to replace the faulty part and restart the system.

Note: The POST error codes in the following table are common to all current generation Intel® server platforms. Features present on a given server board/system will determine which of the listed error codes are supported.

Table 76. POST Error Codes and Messages

Error Code	Error Message	Response
0012	System RTC date/time not set	Major
0048	Password check failed	Major
0140	PCI component encountered a PERR error	Major
0141	PCI resource conflict	Major

Error Code	Error Message	Response
0146	PCI out of resources error	Major
0191	Processor core/thread count mismatch detected	Fatal
0192	Processor cache size mismatch detected	Fatal
0194	Processor family mismatch detected	Fatal
0195	Processor Intel® QPI link frequencies unable to synchronize	Fatal
0196	Processor model mismatch detected	Fatal
0197	Processor frequencies unable to synchronize	Fatal
5220	BIOS Settings reset to default settings	Major
5221	Passwords cleared by jumper	Major
5224	Password clear jumper is Set	Major
8130	Processor 01 disabled	Major
8131	Processor 02 disabled	Major
8132	Processor 03 disabled	Major
8133	Processor 04 disabled	Major
8160	Processor 01 unable to apply microcode update	Major
8161	Processor 02 unable to apply microcode update	Major
8162	Processor 03 unable to apply microcode update	Major
8163	Processor 04 unable to apply microcode update	Major
8170	Processor 01 failed Self Test (BIST)	Major
8171	Processor 02 failed Self Test (BIST)	Major
8172	Processor 03 failed Self Test (BIST)	Major
8173	Processor 04 failed Self Test (BIST)	Major
8180	Processor 01 microcode update not found	Minor
8181	Processor 02 microcode update not found	Minor
8182	Processor 03 microcode update not found	Minor
8183	Processor 04 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
8305	Hot Swap Controller failure	Major
83A0	Management Engine (ME) failed Self Test	Major
83A1	Management Engine (ME) Failed to respond.	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
8520	DIMM_A1 failed test/initialization	Major
8521	DIMM_A2 failed test/initialization	Major
8522	DIMM_A3 failed test/initialization	Major
8523	DIMM_B1 failed test/initialization	Major
8524	DIMM_B2 failed test/initialization	Major
8525	DIMM_B3 failed test/initialization	Major
8526	DIMM_C1 failed test/initialization	Major

Error Code	Error Message	Response
8527	DIMM_C2 failed test/initialization	Major
8528	DIMM_C3 failed test/initialization	Major
8529	DIMM_D1 failed test/initialization	Major
852A	DIMM_D2 failed test/initialization	Major
852B	DIMM_D3 failed test/initialization	Major
852C	DIMM_E1 failed test/initialization	Major
852D	DIMM_E2 failed test/initialization	Major
852E	DIMM_E3 failed test/initialization	Major
852F	DIMM_F1 failed test/initialization	Major
8530	DIMM_F2 failed test/initialization	Major
8531	DIMM_F3 failed test/initialization	Major
8532	DIMM_G1 failed test/initialization	Major
8533	DIMM_G2 failed test/initialization	Major
8534	DIMM_G3 failed test/initialization	Major
8535	DIMM_H1 failed test/initialization	Major
8536	DIMM_H2 failed test/initialization	Major
8537	DIMM_H3 failed test/initialization	Major
8538	DIMM_I1 failed test/initialization	Major
8539	DIMM_I2 failed test/initialization	Major
853A	DIMM_I3 failed test/initialization	Major
853B	DIMM_J1 failed test/initialization	Major
853C	DIMM_J2 failed test/initialization	Major
853D	DIMM_J3 failed test/initialization	Major
853E	DIMM_K1 failed test/initialization	Major
853F (Go to 85C0)	DIMM_K2 failed test/initialization	Major
8540	DIMM_A1 disabled	Major
8541	DIMM_A2 disabled	Major
8542	DIMM_A3 disabled	Major
8543	DIMM_B1 disabled	Major
8544	DIMM_B2 disabled	Major
8545	DIMM_B3 disabled	Major
8546	DIMM_C1 disabled	Major
8547	DIMM_C2 disabled	Major
8548	DIMM_C3 disabled	Major
8549	DIMM_D1 disabled	Major
854A	DIMM_D2 disabled	Major
854B	DIMM_D3 disabled	Major
854C	DIMM_E1 disabled	Major
854D	DIMM_E2 disabled	Major
854E	DIMM_E3 disabled	Major
854F	DIMM_F1 disabled	Major
8550	DIMM_F2 disabled	Major
8551	DIMM_F3 disabled	Major
8552	DIMM_G1 disabled	Major

Error Code	Error Message	Response
8553	DIMM_G2 disabled	Major
8554	DIMM_G3 disabled	Major
8555	DIMM_H1 disabled	Major
8556	DIMM_H2 disabled	Major
8557	DIMM_H3 disabled	Major
8558	DIMM_I1 disabled	Major
8559	DIMM_I2 disabled	Major
855A	DIMM_I3 disabled	Major
855B	DIMM_J1 disabled	Major
855C	DIMM_J2 disabled	Major
855D	DIMM_J3 disabled	Major
855E	DIMM_K1 disabled	Major
855F (Go to 85D0)	DIMM_K2 disabled	Major
8560	DIMM_A1 encountered a Serial Presence Detection (SPD) failure	Major
8561	DIMM_A2 encountered a Serial Presence Detection (SPD) failure	Major
8562	DIMM_A3 encountered a Serial Presence Detection (SPD) failure	Major
8563	DIMM_B1 encountered a Serial Presence Detection (SPD) failure	Major
8564	DIMM_B2 encountered a Serial Presence Detection (SPD) failure	Major
8565	DIMM_B3 encountered a Serial Presence Detection (SPD) failure	Major
8566	DIMM_C1 encountered a Serial Presence Detection (SPD) failure	Major
8567	DIMM_C2 encountered a Serial Presence Detection (SPD) failure	Major
8568	DIMM_C3 encountered a Serial Presence Detection (SPD) failure	Major
8569	DIMM_D1 encountered a Serial Presence Detection (SPD) failure	Major
856A	DIMM_D2 encountered a Serial Presence Detection (SPD) failure	Major
856B	DIMM_D3 encountered a Serial Presence Detection (SPD) failure	Major
856C	DIMM_E1 encountered a Serial Presence Detection (SPD) failure	Major
856D	DIMM_E2 encountered a Serial Presence Detection (SPD) failure	Major
856E	DIMM_E3 encountered a Serial Presence Detection (SPD) failure	Major
856F	DIMM_F1 encountered a Serial Presence Detection (SPD) failure	Major
8570	DIMM_F2 encountered a Serial Presence Detection (SPD) failure	Major
8571	DIMM_F3 encountered a Serial Presence Detection (SPD) failure	Major
8572	DIMM_G1 encountered a Serial Presence Detection (SPD) failure	Major
8573	DIMM_G2 encountered a Serial Presence Detection (SPD) failure	Major
8574	DIMM_G3 encountered a Serial Presence Detection (SPD) failure	Major
8575	DIMM_H1 encountered a Serial Presence Detection (SPD) failure	Major
8576	DIMM_H2 encountered a Serial Presence Detection (SPD) failure	Major
8577	DIMM_H3 encountered a Serial Presence Detection (SPD) failure	Major
8578	DIMM_I1 encountered a Serial Presence Detection (SPD) failure	Major
8579	DIMM_I2 encountered a Serial Presence Detection (SPD) failure	Major
857A	DIMM_I3 encountered a Serial Presence Detection (SPD) failure	Major
857B	DIMM_J1 encountered a Serial Presence Detection (SPD) failure	Major
857C	DIMM_J2 encountered a Serial Presence Detection (SPD) failure	Major
857D	DIMM_J3 encountered a Serial Presence Detection (SPD) failure	Major
857E	DIMM_K1 encountered a Serial Presence Detection (SPD) failure	Major

Error Code	Error Message	Response
857F (Go to 85E0)	DIMM_K2 encountered a Serial Presence Detection (SPD) failure	Major
85C0	DIMM_K3 failed test/initialization	Major
85C1	DIMM_L1 failed test/initialization	Major
85C2	DIMM_L2 failed test/initialization	Major
85C3	DIMM_L3 failed test/initialization	Major
85C4	DIMM_M1 failed test/initialization	Major
85C5	DIMM_M2 failed test/initialization	Major
85C6	DIMM_M3 failed test/initialization	Major
85C7	DIMM_N1 failed test/initialization	Major
85C8	DIMM_N2 failed test/initialization	Major
85C9	DIMM_N3 failed test/initialization	Major
85CA	DIMM_O1 failed test/initialization	Major
85CB	DIMM_O2 failed test/initialization	Major
85CC	DIMM_O3 failed test/initialization	Major
85CD	DIMM_P1 failed test/initialization	Major
85CE	DIMM_P2 failed test/initialization	Major
85CF	DIMM_P3 failed test/initialization	Major
85D0	DIMM_K3 disabled	Major
85D1	DIMM_L1 disabled	Major
85D2	DIMM_L2 disabled	Major
85D3	DIMM_L3 disabled	Major
85D4	DIMM_M1 disabled	Major
85D5	DIMM_M2 disabled	Major
85D6	DIMM_M3 disabled	Major
85D7	DIMM_N1 disabled	Major
85D8	DIMM_N2 disabled	Major
85D9	DIMM_N3 disabled	Major
85DA	DIMM_O1 disabled	Major
85DB	DIMM_O2 disabled	Major
85DC	DIMM_O3 disabled	Major
85DD	DIMM_P1 disabled	Major
85DE	DIMM_P2 disabled	Major
85DF	DIMM_P3 disabled	Major
85E0	DIMM_K3 encountered a Serial Presence Detection (SPD) failure	Major
85E1	DIMM_L1 encountered a Serial Presence Detection (SPD) failure	Major
85E2	DIMM_L2 encountered a Serial Presence Detection (SPD) failure	Major
85E3	DIMM_L3 encountered a Serial Presence Detection (SPD) failure	Major
85E4	DIMM_M1 encountered a Serial Presence Detection (SPD) failure	Major
85E5	DIMM_M2 encountered a Serial Presence Detection (SPD) failure	Major
85E6	DIMM_M3 encountered a Serial Presence Detection (SPD) failure	Major
85E7	DIMM_N1 encountered a Serial Presence Detection (SPD) failure	Major
85E8	DIMM_N2 encountered a Serial Presence Detection (SPD) failure	Major
85E9	DIMM_N3 encountered a Serial Presence Detection (SPD) failure	Major
85EA	DIMM_O1 encountered a Serial Presence Detection (SPD) failure	Major

Error Code	Error Message	Response
85EB	DIMM_O2 encountered a Serial Presence Detection (SPD) failure	Major
85EC	DIMM_O3 encountered a Serial Presence Detection (SPD) failure	Major
85ED	DIMM_P1 encountered a Serial Presence Detection (SPD) failure	Major
85EE	DIMM_P2 encountered a Serial Presence Detection (SPD) failure	Major
85EF	DIMM_P3 encountered a Serial Presence Detection (SPD) failure	Major
8604	POST Reclaim of non-critical NVRAM variables	Minor
8605	BIOS Settings are corrupted	Major
8606	NVRAM variable space was corrupted and has been reinitialized	Major
92A3	Serial port component was not detected	Major
92A9	Serial port component encountered a resource conflict error	Major
A000	TPM device not detected.	Minor
A001	TPM device missing or not responding.	Minor
A002	TPM device failure.	Minor
A003	TPM device failed self test.	Minor
A100	BIOS ACM Error	Major
A421	PCI component encountered a SERR error	Fatal
A5A0	PCI Express* component encountered a PERR error	Minor
A5A1	PCI Express* component encountered an SERR error	Fatal
A6A0	DXE Boot Service driver: Not enough memory available to shadow a Legacy Option ROM	Minor

POST Error Beep Codes

The following table lists the POST error beep codes. Prior to system video initialization, the BIOS uses these beep codes to inform users on error conditions. The beep code is followed by a user-visible code on the POST Progress LEDs.

Table 77. POST Error Beep Codes

Beeps	Error Message	POST Progress Code	Description
1	USB device action	NA	Short beep sounded whenever a USB device is discovered in POST, or inserted or removed during runtime
1 long	Intel® TXT security violation	0xAE, 0xAF	System halted because Intel® Trusted Execution Technology detected a potential violation of system security.
3	Memory error	See Tables 28 and 29	System halted because a fatal error related to the memory was detected.
2	BIOS Recovery started	NA	Recovery boot has been initiated
4	BIOS Recovery failure	NA	BIOS recovery has failed. This typically happens so quickly after recovery us initiated that it sounds like a 2-4 beep code.

The Integrated BMC may generate beep codes upon detection of failure conditions. Beep codes are sounded each time the problem is discovered, such as on each power-up attempt, but are not sounded continuously. Codes that are common across all Intel® server boards and systems that use same generation chipset are listed in the following table. Each digit in the code is represented by a sequence of beeps whose count is equal to the digit.

Table 78. Integrated BMC Beep Codes

Code	Reason for Beep	Associated Sensors
1-5-2-1	No CPUs installed or first CPU socket is empty.	CPU1 socket is empty, or sockets are populated incorrectly CPU1 must be populated before CPU2.
1-5-2-4	MSID Mismatch	MSID mismatch occurs if a processor is installed into a system board that has incompatible power capabilities.
1-5-4-2	Power fault	DC power unexpectedly lost (power good dropout) – Power unit sensors report power unit failure offset
1-5-4-4	Power control fault (power good assertion timeout).	Power good assertion timeout – Power unit sensors report soft power control failure offset
1-5-1-2	VR Watchdog Timer sensor assertion	VR controller DC power on sequence was not completed in time.
1-5-1-4	Power Supply Status	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.

Appendix E: Supported Intel® Server Chassis

The Intel® Server Board S1200V3RP requires a passive processor heat sink solution when integrated in the Intel® pedestal server chassis listed below. The Intel® Server Board S1200V3RP supports up to 95W TDP Intel® Xeon® Processor.

Table 79. Compatible Intel® Server Chassis P4000S family

Intel® Server Chassis SKU	System Fans	Storage Drives	Power Supply(s)
P4304XXSHDR	Two Fixed Fans	Four 3.5” Hotswap Drive Bay	Two 460W CRPS
P4304XXSFDR	Two Fixed Fans	Four 3.5” Fixed Drive Trays	Two 460W CRPS

You must install the active processor heat sink with the airflow direction as shown in the following figure.

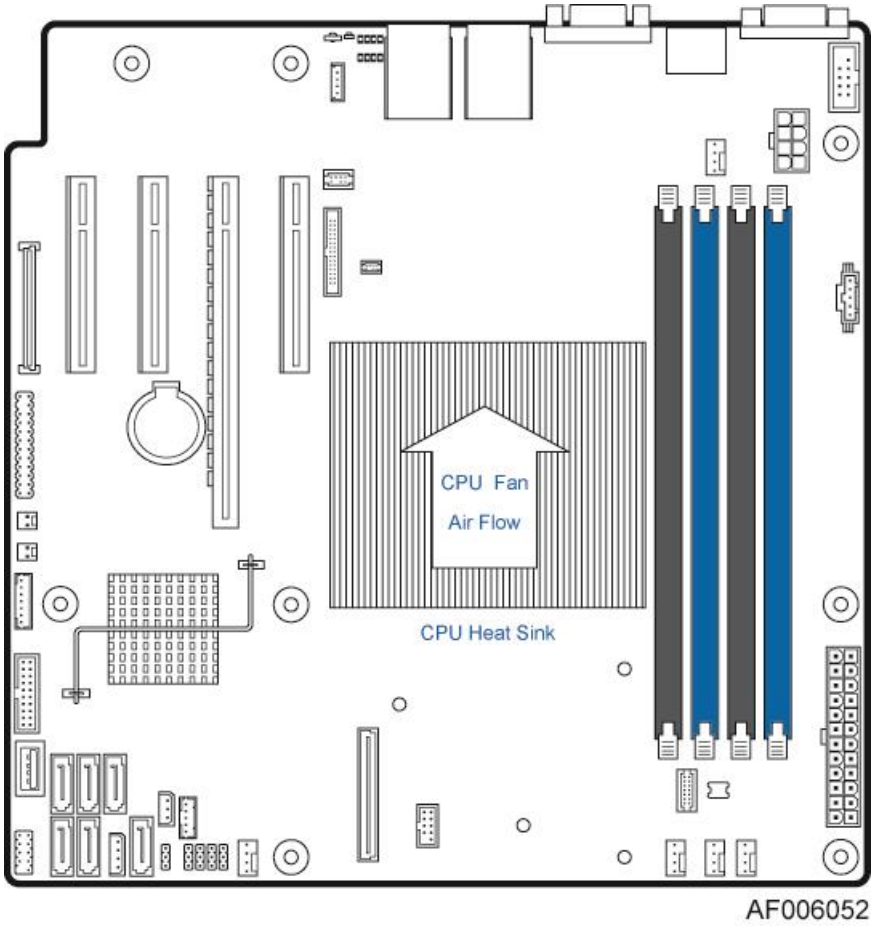


Figure 54. Processor Heatsink Installation

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.

Term	Definition
ACPI	Advanced Configuration and Power Interface
AES	Advanced Encryption Standard
AMB	Advanced Memory Buffer (there is an AMB on each FBDIMM)
APIC	Advanced Programmable Interrupt Controller
ARP	Address Resolution Protocol
ASF	Alert Standards Forum
ASIC	Application specific integrated circuit
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
CBC	Chassis bridge controller. A microcontroller connected to one or more other CBCs. Together they bridge the IPMB buses of multiple chassis.
CLI	Command-line interface
CLTT	Closed-loop thermal throttling (memory throttling mode)
CMOS	In terms of this specification, this describes the PC-AT compatible region of battery-backed 128 bytes of memory on the server board.
CSR	Control and status register
D-cache	Data cache. Processor-local cache dedicated for memory locations explicitly loaded and stored by running code.
DHCP	Dynamic Host Configuration Protocol
DIB	Device Information Block
DPC	Direct Platform Control
EEPROM	Electrically erasable programmable read-only memory
EMP	Emergency management port
EPS	External Product Specification
FML	Fast management link
FNI	Fast management link network interface
FRB	Fault resilient booting
FRU	Field replaceable unit
FSB	Front side bus
FTM	Firmware transfer mode
GPIO	General-purpose input/output
HSBP	Hot-swap backplane
HSC	Hot-swap controller
I-cache	Instruction cache. Processor-local cache dedicated for memory locations retrieved through instruction fetch operations.
I^2C	Inter-integrated circuit bus
IA	Intel® architecture

Term	Definition
IBF	Input buffer
ICH	I/O controller hub
IERR	Internal error
INIT	Initialization signal
IPMB	Intelligent Platform Management Bus
IPMI	Intelligent Platform Management Interface
ITP	In-target probe
KCS	Keyboard controller style
KT	Keyboard text
KVM	Keyboard, video, and mouse
LAN	Local area network
LCD	Liquid crystal display
LPC	Low pin count
LUN	Logical unit number
MAC	Media Access Control
MD5	Message Digest 5. A hashing algorithm that provides higher security than MD2.
MIB	Modular information block. A descriptive text translation of a PET event, contained in a MIB file for use by an SNMP agent hen decoding SEL entries.
ms	Millisecond
MUX	Multiplexer
NIC	Network interface card
NMI	Non-maskable interrupt
OBF	Output buffer
OEM	Original equipment manufacturer
OLTT	Open-loop thermal throttling (memory throttling mode)
PCI	Peripheral Component Interconnect
PECI	Platform Environmental Control Interface
PEF	Platform event filtering
PET	Platform event trap
PIA	Platform information area
PLD	Programmable logic device
POST	Power-on self-test
PROM	Programmable read-only memory
PSMI	Power Supply Management Interface
PWM	Pulse Width Modulation. The mechanism used to control the speed of system fans.
RAM	Random Access Memory
RAS	Reliability, availability, and serviceability
RC4	Rivest Cipher 4. A stream cipher designed by Rivest* for RSA data security, now RSA security. It is a variable key-size stream cipher with byte-oriented operations. The algorithm is based on a random permutation.
RMCP+	Remote Management Control Protocol
ROM	Read-only memory
RTC	Real-time clock
SCI	System Control Interrupt. A system interrupt used by hardware to notify the operating system of ACPI events.
SDR	Sensor data record

Term	Definition
SDRAM	Synchronous dynamic random access memory
SEL	System event log
SHA1	Secure Hash Algorithm 1
SIO	Server Input/Output
SMBus*	A two-wire interface based on the I^2C protocol. The SMBus* is a low-speed bus that provides positive addressing for devices and bus arbitration.
SMI	Server management interrupt. SMI is the highest priority non-maskable interrupt.
SMM	Server management mode
SMS	Server management software
SNMP	Simple Network Management Protocol
SOL	Serial-over-LAN
SPT	Straight pass-through
SRAM	Static random access memory
UART	Universal asynchronous receiver and transmitter
UDP	User Datagram Protocol
UHCI	Universal Host Controller Interface
VLAN	Virtual local area network

Reference Documents

See the following documents for additional information:

- *Advanced Configuration and Power Interface Specification, Revision 5.0*, http://www.acpi.info/.
- *Intelligent Platform Management Bus Communications Protocol Specification*, Version 1.0. 1998. Intel Corporation, Hewlett-Packard* Company, NEC* Corporation, Dell* Computer Corporation.
- *Intelligent Platform Management Interface Specification, Version 2.0*. 2004. Intel Corporation, Hewlett-Packard* Company, NEC* Corporation, Dell* Computer Corporation.
- *Platform Support for Serial-over-LAN (SOL), TMode, and Terminal Mode External Architecture Specification, Version 1.1*, 02/01/02, Intel Corporation.
- *Intel® Remote Management Module User's Guide*, Intel Corporation.
- *Alert Standard Format (ASF) Specification, Version 2.0*, 23 April 2003, ©2000-2003, Distributed Management Task Force, Inc., http://www.dmtf.org.
- *BIOS for PCSD Platforms Based on Intel® Xeon Processor E3-1200 V3/V4 Product Families External Product Specification*
- *PCSD Platforms Based On Intel Xeon® Processor E3-1200 V3/V4 Product Families BMC Core Firmware External Product Specification*