intel®

Intel® Server D40AMP Family

Technical Product Specification

An overview of product features, functions, architecture, and support specifications.

Rev 1.0

November 2021

D40AMP

Delivering Breakthrough Data Center System Innovation – Experience What's Inside!

< This page is intentionally left blank>

Document Revision History

Date	Revision	Changes
November 2021	1.0	Initial release.

Disclaimers

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software, or service activation. Performance varies depending on system configuration. No computer system can be absolutely secure. Check with your system manufacturer or retailer or learn more at intel.com.

You may not use or facilitate the use of this document in connection with any infringement or other legal analysis concerning Intel products described herein. You agree to grant Intel a non-exclusive, royalty-free license to any patent claim thereafter drafted which includes subject matter disclosed herein.

No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document.

The products described 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.

Intel disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade.

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

Intel, Xeon, Intel Optane, SpeedStep, and the Intel logo are trademarks of Intel Corporation or its subsidiaries in the U.S. and/or other countries.

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

© Intel Corporation

Table of Contents

List of Figures

List of Tables

1. Introduction

The Intel® Server D40AMP family is designed to support demanding hyperconverged infrastructure (HCI), high-performance computing (HPC) and artificial intelligence (AI) applications and workloads. It features the 3rd Gen Intel® Xeon® Scalable processor family, delivering new hardware-enhanced security features. Previous generation Intel® Xeon® processor and Intel® Xeon® Scalable processor families are not supported.

A fully configured 4-module system within the Intel® Server D40AMP family supports up to 24 NVMe* SSD drives in a 2.5" form factor, or up to 32 E1.L (EDSFF) NVMe* SSD drives (depending on chassis SKU) routed to the processors through PCIe* 4.0 lanes. It also supports up to 64 DDR4 DIMMs (up to 16 per compute module) with options to expand the amount of memory or add memory persistence by adding high capacity Intel® Optane™ persistent memory 200 series modules, for a total of up to 96 DIMMs (DDR4 + Intel® Optane™ PMem).

The product family includes the server board, the compute module and the server chassis. These building blocks are available separately, providing flexibility to build a multi-module system from the ground up. The product family also includes fully integrated 3U rack mount, multi-module systems.

This technical product specification (TPS) provides a high-level overview of the features, functions, architecture, and support specifications of the Intel® Server D40AMP family. This document is divided in two main parts, with the first four chapters providing feature information about the server board, the compute module, and the system separately. The rest of the chapters provide information about the technologies behind these features.

Note: In this document, the 3rd Gen Intel® Xeon® Scalable processor family may be referred to simply as "processor".

Note: This document includes several references to Intel websites where additional product information can be downloaded. However, these public Intel sites do not include content for products in development. Content for these products will be available on the public Intel websites after their public launch.
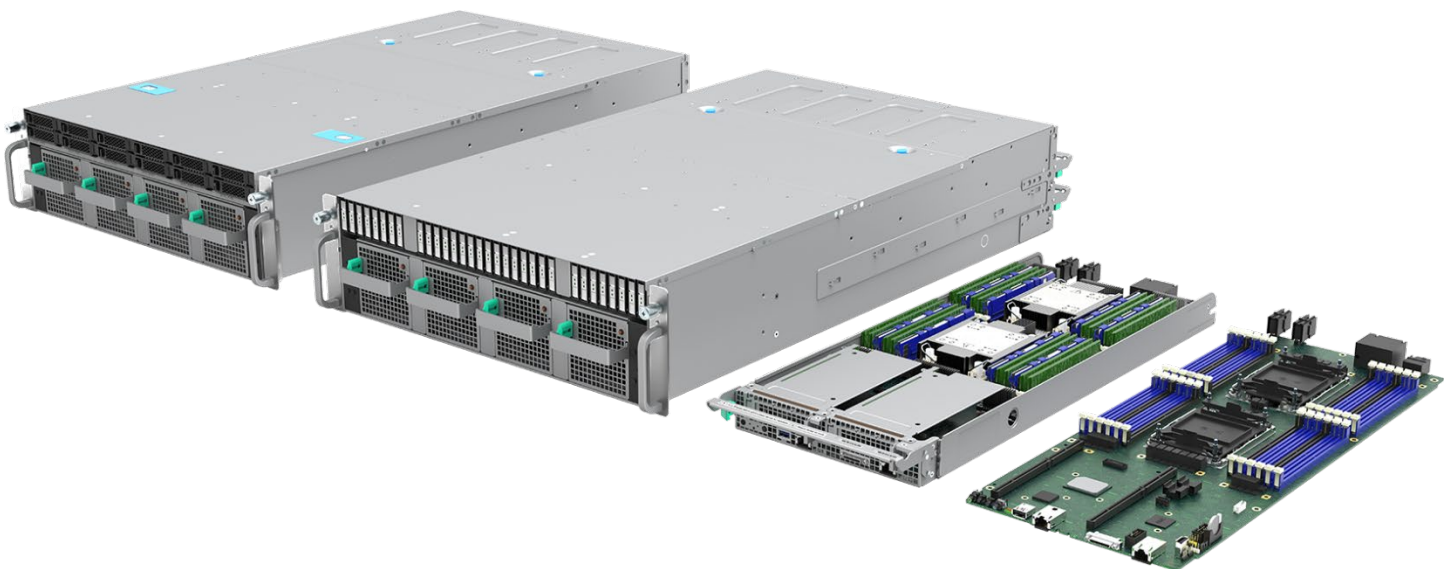
Figure 1. Intel® Server D40AMP Family

For a complete list of available documentation, see Table 1. Refer to the *Intel® Server D40AMP family Configuration Guide* for guidance to order fully configured systems and ordering information in general.

Table 1. Reference Documents

Document Title	Document Classification
Intel® Server D40AMP family Integration and Service Guide	Public - *link*
Intel® Server D40AMP family Configuration Guide	Public - *link*
3rd Generation Intel® Xeon® Processor Scalable Family BIOS Setup Specification	Intel Confidential
EPS Power Supply Specification	Intel Confidential
Intelligent Platform Management Interface Specification Second Generation v2.0	Intel Confidential
PCIe* Base Specification, Revision 4.0	http://www.pcisig.com/specifications
BIOS Firmware External Product Specification (EPS) For the Intel® Server Board D50TNP, M50CYP, and D40AMP Families	Intel Confidential
Integrated Baseboard Management Controller (BMC) Firmware External Product Specification (EPS) For the Intel® Server System D50TNP, M50CYP, and D40AMP Families	Intel Confidential
TPM PC Client Specifications revision 2.0	https://trustedcomputinggroup.org/resource/pc-client-platform-tpm-profile-ptp-specification/
3rd Generation Intel® Xeon® Scalable Processors, Code name Ice Lake-SP External Design Specification (EDS): Document IDs: 574451, 574942, 575291	Intel Confidential
Intel® Optane™ Persistent Memory Startup Guide	https://www.intel.com/content/dam/support/us/en/documents/memory-and-storage/data-center-persistent-mem/Intel_Optane_Persistent_Memory_Start_Up_Guide.pdf
Intel® Optane™ Persistent Memory 200 Series Operations Guide	Intel Confidential
3rd Generation Intel® Xeon® Scalable Processor, Code name Ice Lake-SP and Cooper Lake-SP - Thermal and Mechanical Specifications and Design Guide (TMSDG): Document ID 574080	Intel Confidential
Intel® Data Center Manager (Intel® DCM) Product Brief	Public - *link*
Intel® Data Center Manager (Intel® DCM) Console User Guide	Public - *link*

Disclaimer: Hyperlink references can change without notice. The provided hyperlinks in this document are tested to be functional at the time of publication.

2. Server Board Overview

This chapter provides information about the server board features and architecture. The Intel® Server Board D40AMP is a purpose built, rack-optimized server board ideal for use in HCI, HPC and AI applications. The architecture of the server board is developed around the features and functions of the 3rd Gen Intel® Xeon® Scalable processor family.
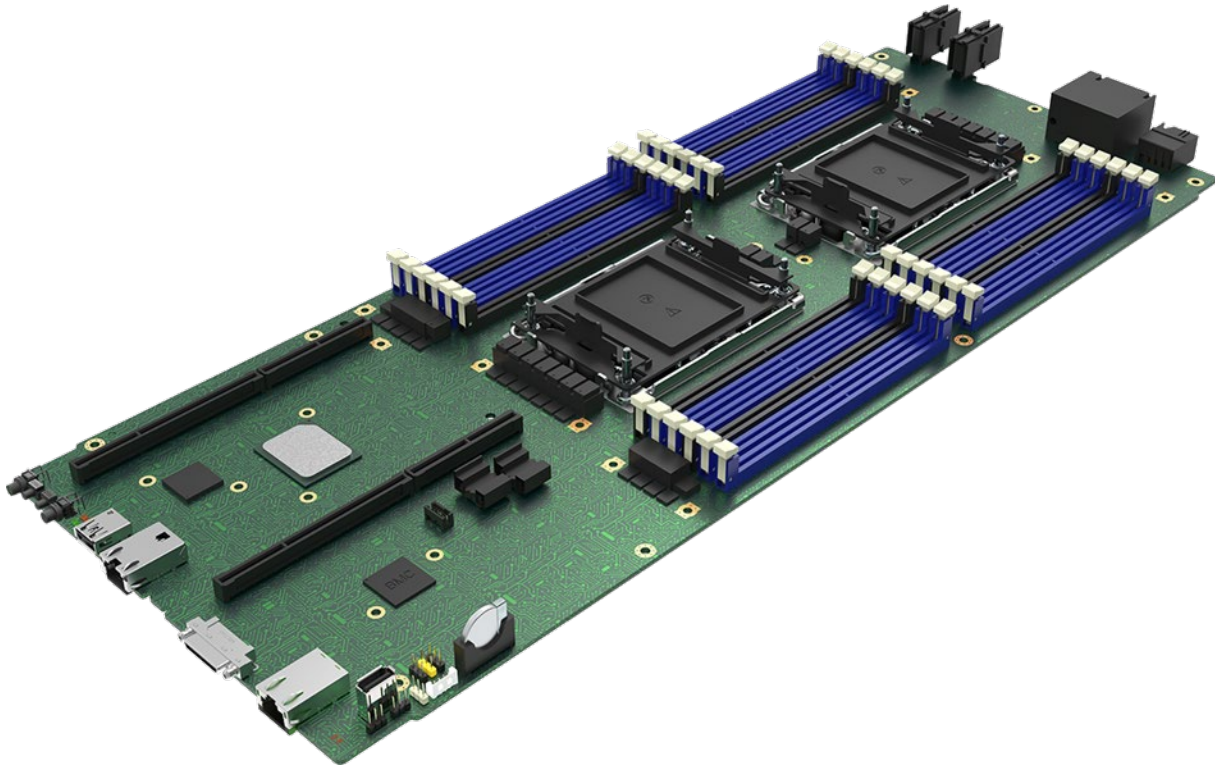
Figure 2. Intel® Server Board D40AMP

2.1 Server Board Features Overview

The following table lists the specifications of the server board. See Figure 3 for feature identification.

Table 2. Intel® Server Board D40AMP features

Feature	Description

Processor Support	• Supported 3rd Gen Intel® Xeon® Scalable processor family SKUs:
	    o Intel® Xeon® Platinum 8300 processor
	    o Intel® Xeon® Gold 6300 processor
	    o Intel® Xeon® Gold 5300 processor
	    o Intel® Xeon® Silver 4300 processor
	• UPI links: three at 11.2 GT/s (Platinum and Gold SKUs) or two at 10.4 GT/s (Silver SKU)
	
	Note: Supported 3rd Gen Intel® Xeon® Scalable processor SKUs must Not end in (H), (L), or (U). All other processor SKUs are supported.
	
	Note: Previous generation Intel® Xeon® processor and Intel® Xeon® processor Scalable families are not supported.
	
	Note: The 8351N SKU is a single-socket optimized SKU and is not supported on the Intel® Server D40AMP family.

Feature	Description
Maximum Processor Thermal Design Power (TDP)	3rd Gen Intel® Xeon® Scalable processors up to 205 W **Disclaimer:** Intel server boards contain and support several high-density VLSI and power delivery components that need adequate airflow to cool and remain within their thermal operating limits. Intel ensures through its own chassis development and testing that when an Intel server board and Intel chassis are used together, the fully integrated system meets the thermal requirements of these components. It is the responsibility of the system architect or system integrator who chooses to develop their own server system using an Intel server board and a non-Intel chassis, to consult relevant specifications and datasheets to determine thermal operating limits and necessary air flow to support intended system configurations and workloads when the system is operating within target ambient temperature limits. It is also their responsibility to perform adequate environmental validation testing to ensure reliable system operation. Intel cannot be held responsible if components fail or the server board does not operate correctly when published operating and non-operating limits are exceeded.
Processor Socket	Dual Socket-P4 4189
Chipset	Intel® C621A Chipset
Memory Support	• Up to 16 DDR4 DIMMs + up to 8 Intel® Optane™ persistent memory 200 series modules. See Chapter 6 for details. • All DDR4 DIMMs must support ECC • Registered DDR4 (RDIMM), 3DS-RDIMM, Load Reduced DDR4 (LRDIMM), 3DS-LRDIMM **Note**: 3DS = 3-dimensional Stacking • Up to 3200 MT/s memory data transfer rates • Up to 2 TB DDR4 memory capacity (1 TB per processor) for all processor SKUs • Up to 6 TB DDR4 and Intel® Optane™ PMem combined memory capacity (3 TB per processor), dependent on processor SKU • DDR4 standard voltage of 1.2 V **Note:** The maximum memory speed supported depends on the installed processor and population configuration. See Chapter 6 for details.
Video Support	• Integrated 2D video controller • 16 MB of DDR4 Memory • One VGA DB-15 external connector through I/O breakout cable
USB Support	• One external USB 3.0 port • Two external USB 3.0 ports (dual-stack) through I/O breakout cable
Serial Support	One external serial port connector through I/O breakout cable. The port follows Advanced Technology (AT) pinout specifications.
Networking	• One external 10GBASE-T Ethernet port (RJ45) • One external 1000BASE-T Ethernet port (RJ45) dedicated to server management
Riser Support	Two riser slots on the server board: **Riser Slot 1** • PCIe* x20 (x16 PCIe* 4.0 from CPU0, x4 PCIe* 3.0 from Chipset) - 1U single-PCIe* slot riser card option supporting one low profile PCIe* add-in card and one 80/110mm M.2 SSD **Riser Slot 2** • PCIe* x20 (x16 PCIe* 4.0 from CPU1, x4 PCIe* 3.0 from Chipset) - 1U single-PCIe* slot riser card option supporting one low profile PCIe* add-in card and one 80/110mm M.2 SSD **Note:** PCIe* lanes routed from processor/chipset support Intel® VROC 7.5 (VMD NVMe* RAID) when an Intel VROC key (accessory option) is installed.
Dedicated Connectors	One dedicated ExaMax* connector in the back of the server board supporting: • x16 PCIe* 4.0 from CPU0 • x16 PCIe* 4.0 from CPU1 • Hotplug signals for CPU0/1 • ID signals for Hot-swap backplane

Feature	Description
Security Features	• Intel® Platform Firmware Resilience (Intel® PFR) technology • Intel® Software Guard Extensions (Intel® SGX) • Intel® Total Memory Encryption (Intel® TME) • Intel® CBnT – Converged Intel® Boot Guard and Trusted Execution Technology (Intel® TXT) • Trusted platform module 2.0 (Rest of World) – iPC AXXTPMENC8 (accessory option) • Trusted platform module 2.0 (China Version) – iPC AXXTPMCHNE8 (accessory option) See Chapter 13 for more information.
Serviceability	
Server Management	• Integrated Baseboard Management Controller (BMC) based on the ASPEED* AST2500 Advanced PCIe* Graphics and Remote Management Processor • Intelligent Platform Management Interface (IPMI) 2.0 compliant • Redfish* compliant • Support for Intel® Data Center Manager (DCM) • Support for Intel® Server Debug and Provisioning Tool (SDPTool) • One external 1000BASE-T Ethernet port (RJ45) dedicated for server management • Onboard LEDs for Light Guided Diagnostics
Onboard Configuration and Service Jumpers	• BIOS defaults • BIOS Password clear • Intel® Management Engine (Intel® ME) firmware force update • BMC force update • BIOS Security Version Number (SVN) Downgrade • BMC Security Version Number (SVN) Downgrade
BIOS	• Unified Extensible Firmware Interface (UEFI)-based BIOS (legacy boot not supported)

Figure 3. Intel® Server Board D40AMP Feature Identification

The D40AMP server board includes several jumper blocks to configure, protect, or recover specific features of the server board. The following figure identifies the location of each jumper header on the server board. Pin 1 of each jumper can be identified by the arrowhead (▼) silkscreened on the server board next to the pin. See Chapter 14 for details on how to use each jumper.

Ref #: AMP10053
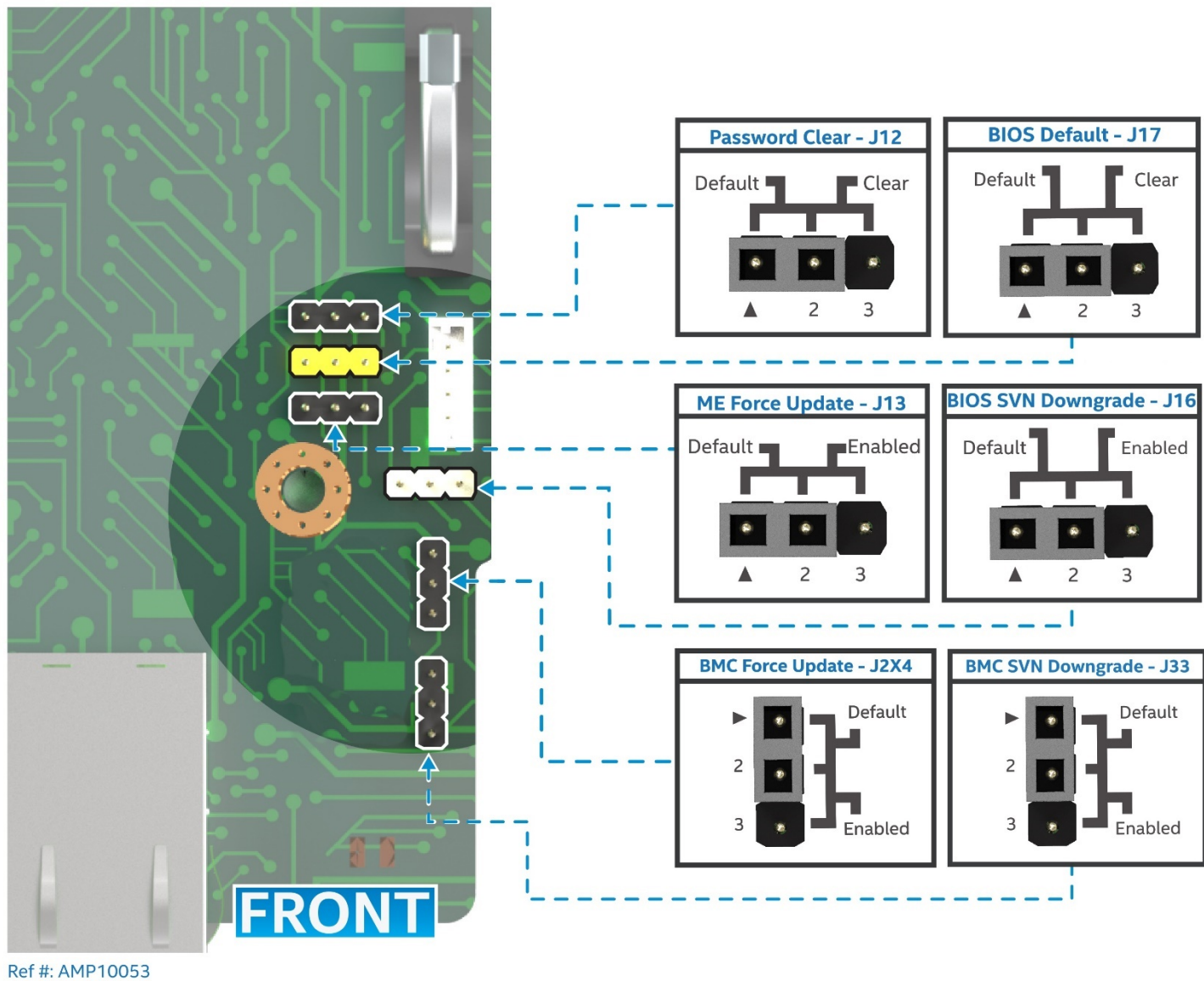
Figure 4. Reset and Recovery Jumper Header Location

A bank of eight diagnostic LEDs is located on the front edge of the server board (see Figure 5). During the boot process, the BIOS executes many module configuration steps, each of which is assigned a specific hex POST code number. As each configuration step is started, the BIOS displays the given POST code to the 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 executed. See Appendix C for a complete description of how these LEDs are read, and for a list of all supported POST codes.
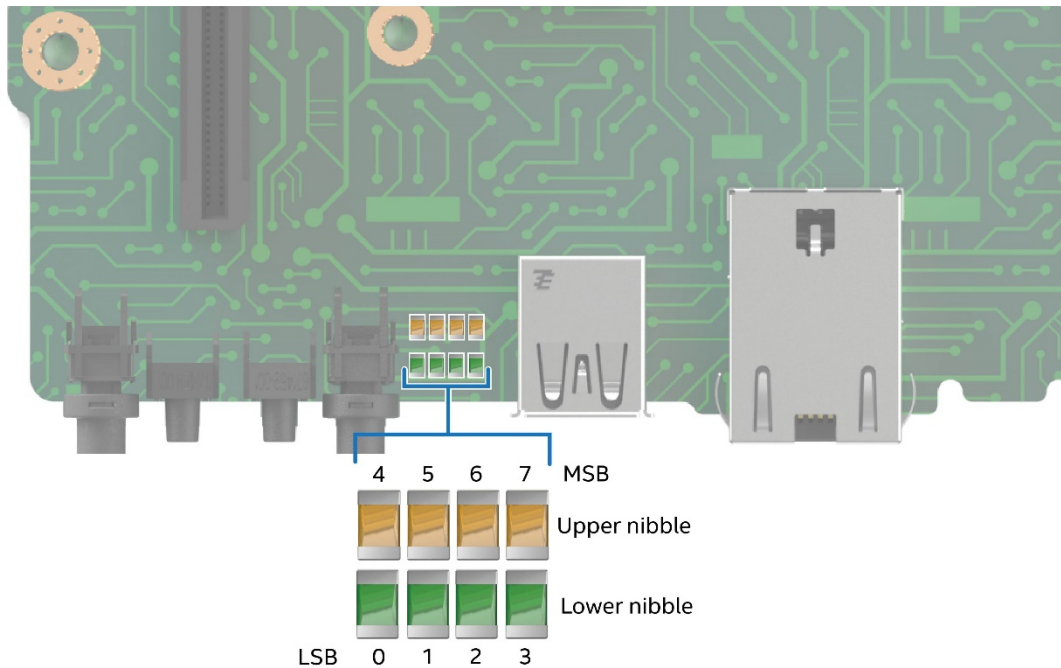
Ref #: AMP10012

Figure 5. Onboard LED Location

2.2   Server Board Architecture

The architecture of the Intel® Server Board D40AMP is developed around the integrated features and functions of the 3rd Gen Intel® Xeon® Scalable processor family, the Intel® C621A chipset, Intel® Ethernet Controller X550, and the ASPEED* AST2500 Server Board Management Processor.

The following figure provides an overview of the Intel® Server Board D40AMP architecture, showing the features and interconnects of each of the major subsystem components.
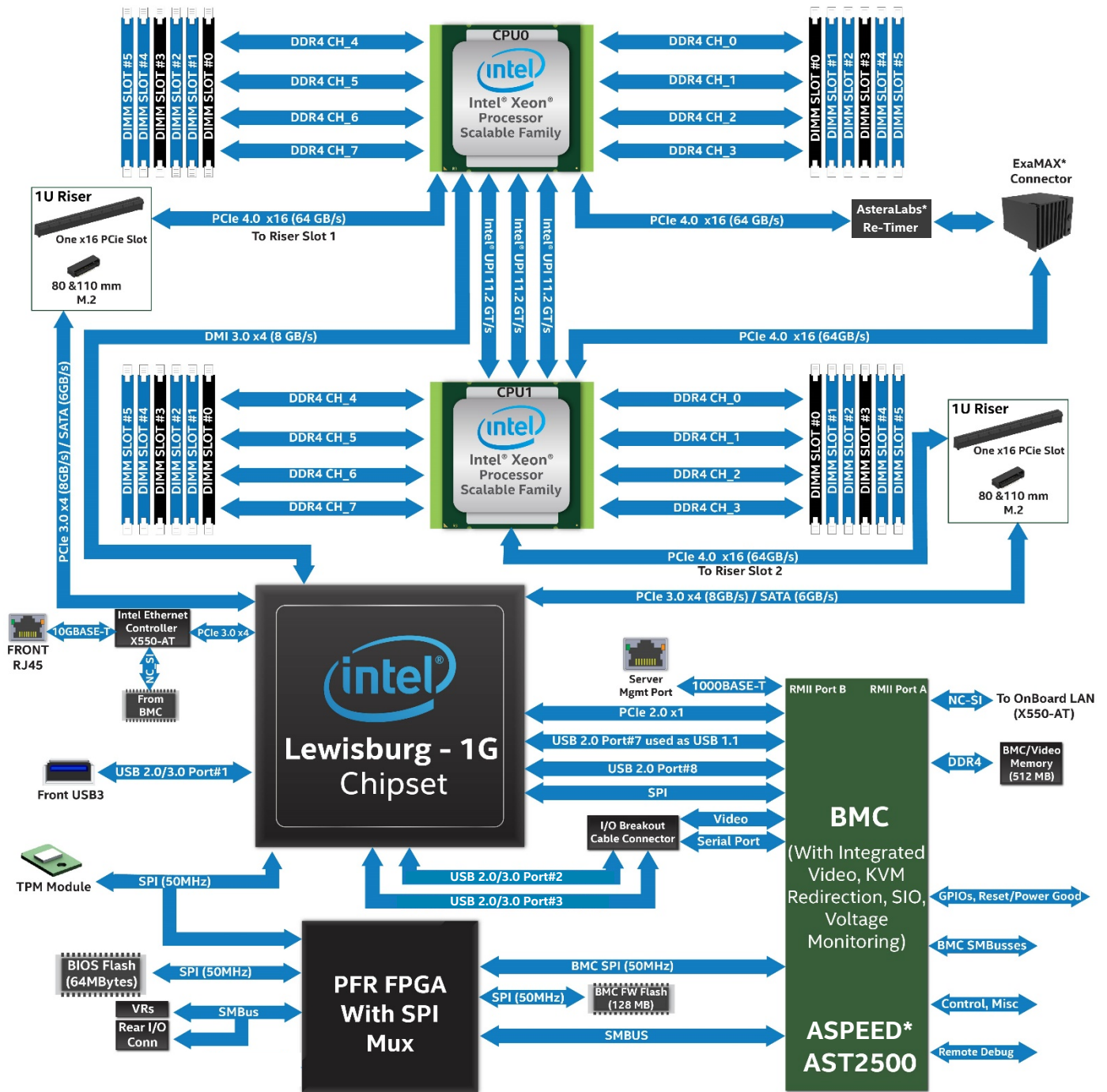
Figure 6. Intel® Server Board D40AMP Architectural Block Diagram

2.3   PCI Express (PCIe*)

The PCI Express (PCIe*) interfaces on the Intel® Server D40AMP family are fully compliant with the *PCI Express Base Specification, Revision 4.0* supporting the following PCIe* bit rates: 4.0 (16 GT/s), 3.0 (8.0 GT/s), 2.0 (5.0 GT/s), and 1.0 (2.5 GT/s). The interfaces supporting M.2 connectors from the Platform Controller Hub (PCH) chipset are fully compliant with the *PCI Express Base Specification, Revision 3.0* supporting the following PCIe* bit rates: 3.0 (8.0 GT/s), 2.0 (5.0 GT/s), and 1.0 (2.5 GT/s).

2.3.1   PCI Express Port Routing

The following table provides the PCIe* port routing for the supported riser slots and onboard ExaMAX* connector.

Table 3. PCIe* Port Routing

Host	Port	Width	Gen	Server Board Connector	Server System Usage
CPU0	Port 2A-2D	x16	4.0	ExaMAX* connector	U.2 HSBP / E1.L Midplane
	Port 3A-3D	x16	4.0	Riser Slot 1	x16 PCIe* slot in riser
CPU1	Port 2A-2D	x16	4.0	Riser Slot 2	x16 PCIe* slot in riser
	Port 3A-3D	x16	4.0	ExaMAX* connector	U.2 HSBP / E1.L Midplane
Chipset (PCH)	Port 4–7	x4	3.0	Riser Slot 1	M.2 SSD connector in riser
	Port 8–11	x4	3.0	Riser Slot 2	M.2 SSD connector in riser

2.3.2   PCI Express Enumeration and Allocation

The BIOS assigns PCI bus numbers in a depth-first hierarchy, in accordance with the *PCI Local Bus Specification, Revision 4.0*. The bus number is incremented when the BIOS encounters a PCI-PCI bridge device.

Scanning continues on the secondary side of the bridge until all subordinate buses are assigned numbers. PCI bus number assignments may vary from boot to boot with varying presence of PCI devices with PCI-PCI bridges.

If a bridge device with a single bus behind it is inserted into a PCI bus, all subsequent PCI bus numbers below the current bus are increased by one. The bus assignments occur once, early in the BIOS boot process, and never change during the pre-boot phase.

2.3.3   PCI Express Bifurcation

The Intel® Server Board D40AMP supports the following bifurcation of x16 PCIe* data lanes into smaller PCIe* groups:

- Riser Slot 1 – 1U PCIe* slot riser card: x16/x8x8/x8x4x4/x4x4x8/x4x4x4x4
- Riser Slot 2 – 1U PCIe* slot riser card: x16/x8x8/x8x4x4/x4x4x8/x4x4x4x4

Note: The Intel® Server Board D40AMP includes a clock signal for each PCIe* riser slot, which is used when the PCIe* slot is configured to work at full link width. When a PCIe* riser slot is configured with any of the available bifurcation options above, this clock signal is used for one of the PCIe* groups. The installed PCIe* add-in card must provide clock signals for the remaining PCIe* groups and all devices exposed to the system.

To change PCIe* bifurcation settings, access the BIOS Setup menu by pressing **<F2>** key during POST. Navigate to the following menu: **Advanced > Integrated IO Configuration > PCIe* Slot Bifurcation Setting**

2.4   Processor Cooling Requirements

In order to support optimal operation and long-term reliability for a server system configured with the Intel® Server Board D40AMP, the thermal management solution of the selected server chassis and/or module must dissipate enough heat generated from within to keep the processors and other system components within their specified thermal limits.

For optimal operation and long-term reliability, processors within the 3rd Gen Intel® Xeon® Scalable processor family must operate within their defined minimum and maximum case temperature (TCASE) limits. Refer to the 3rd Gen Intel® Xeon® Processor Scalable Family – Thermal Mechanical Specifications and Design Guide (TMSDG) for additional information concerning processor thermal limits.

Note: It is the responsibility of the system and components architects to ensure compliance with the processor thermal specifications. Compromising processor thermal requirements will impact the processor performance and reliability.

For details about Intel's air cooled solution, see Chapters 5 and 9.

3.   Intel® Compute Module D40AMP Overview

The Intel® Compute Module D40AMP is a 1U half-width compute module. With the Intel® Server Board D40AMP at its heart and supporting the 3rd Gen Intel® Xeon® Scalable processors, it builds upon its features to provide support for internal storage, and PCIe* 4.0 expansion options. A multi-module system within the Intel® Server D40AMP family supports up to four compute modules, that operate independently from each other. The installed modules within a system chassis share resources like power, storage and cooling.
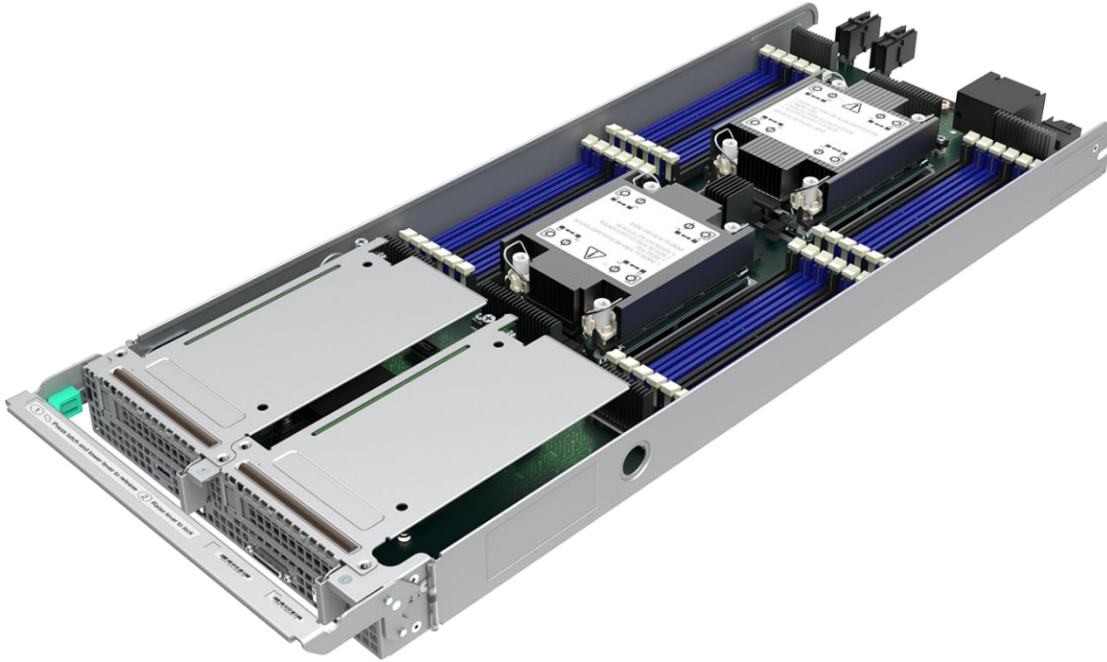
Figure 7. Intel® Compute Module D40AMP

The Compute Module supports up to 24 DIMMs (depending on configuration) and includes two riser card assemblies. Each riser card assembly includes a single, x16 PCIe* 4.0 slot compatible with low-profile PCIe* add-in cards. The riser assembly also supports a single 80/110 mm PCIe* or SATA M.2 SSD storage device.
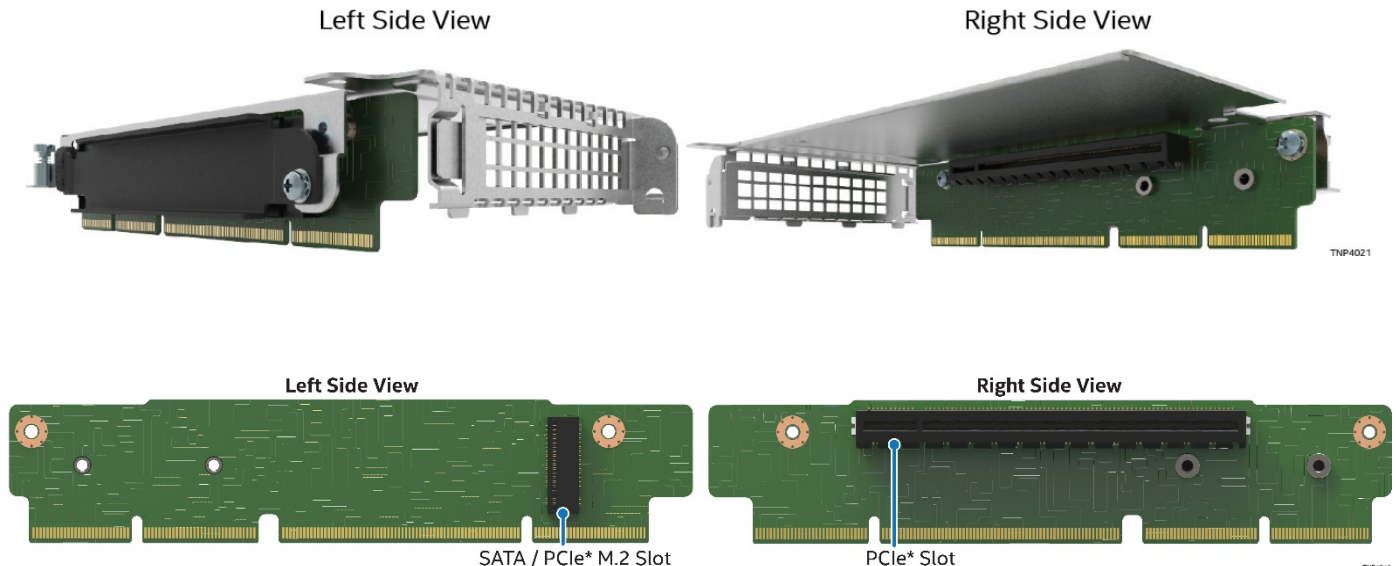
Figure 8. 1U Riser Card Assembly

3.1.1 Supported Features

The following table provides the Compute Module supported features.

Table 4. Compute Module supported features

Feature	Description
Processor Support	• Supported 3rd Gen Intel® Xeon® Scalable processor family SKUs: 　o　Intel® Xeon® Platinum 8300 processor 　o　Intel® Xeon® Gold 6300 processor 　o　Intel® Xeon® Gold 5300 processor 　o　Intel® Xeon® Silver 4300 processor • UPI links: three at 11.2 GT/s (Platinum and Gold SKUs) or two at 10.4 GT/s (Silver SKU) **Note:** Supported 3rd Gen Intel® Xeon® Scalable processor SKUs must Not end in (H), (L), or (U). All other processor SKUs are supported. **Note:** Previous generation Intel® Xeon® processor and Intel® Xeon® Scalable processor families are not supported. **Note:** The 8351N SKU is a single-socket optimized SKU and is not supported on the Intel® Server D40AMP family.
Maximum Processor TDP	• Up to 205 W **Note:** See Appendix E for details.
Processor Socket	• Dual Socket-P4 4189
Chipset	• Intel® C621A Chipset
Memory Support	• Up to 16 DDR4 DIMMs + up to 8 Intel® Optane™ persistent memory 200 series modules • All DDR4 DIMMs must support ECC • Registered DDR4 (RDIMM), 3DS-RDIMM, Load Reduced DDR4 (LRDIMM), 3DS-LRDIMM 　Note: 3DS = 3-dimensional Stacking • Intel® Optane™ persistent memory 200 series modules • Up to 3200 MT/s memory data transfer rates • Up to 2 TB DDR4 memory capacity (1 TB per processor) for all processor SKUs • Up to 6 TB DDR4 and Intel® Optane™ PMem combined memory capacity (3 TB per processor), dependent on processor SKU • DDR4 standard voltage of 1.2 V **Note:** The maximum memory speed supported depends on the installed processor and population configuration. See Chapter 6 for details.
Storage Support	**Via riser assemblies:** • Two 80/110mm M.2 SATA/PCIe* NVMe* SSDs with PCIe* 3.0 lanes routed from chipset **Note:** PCIe* lanes routed from processor/chipset have Intel® VROC 7.5 (VMD NVMe* RAID) support using Intel VROC key (accessory option).
	Accessible from the front of the compute module
I/O Ports	• One USB 3.0 port • One I/O breakout cable connector supporting the following: 　o　Two USB 3.0 ports (dual-stack) 　o　One VGA connector (routed to BMC VGA controller with 16 MB of DDR4 video memory) 　o　One serial port connector. The port follows AT pinout specifications

Feature	Description
	Note: The I/O breakout cable is available as an accessory option (iPC: **AXXCONNTDBG**).
Networking	• One external 10GBASE-T Ethernet port (RJ45) • One external 1000BASE-T Ethernet port (RJ45) dedicated for server management
LEDs	• Compute Module status • Compute Module ID
Expansion Options	
Riser 1	• PCIe* slot (from CPU0): x16 (mechanical/electrical) low-profile PCIe* 4.0 compatible • M.2 connector (from chipset): 80/110 mm SATA/PCIe* 3.0 NVMe*
Riser 2	• PCIe* slot (from CPU1): x16 (mechanical/electrical) low-profile PCIe* 4.0-compatible • M.2 connector (from chipset): 80/110 mm SATA/PCIe* 3.0-compatible NVMe* **Note:** The PCIe* slots in riser 1 and 2 provide up to 25 W of power.
Security	
Security Support	• Intel® Platform Firmware Resilience (Intel® PFR) technology • Intel® Software Guard Extensions (Intel® SGX) • Intel® Total Memory Encryption (Intel® TME) • Intel® CBnT – Converged Intel® Boot Guard and Trusted Execution Technology (Intel® TXT) • Trusted platform module 2.0 (Rest of World) – iPC AXXTPMENC8 (accessory option) • Trusted platform module 2.0 (China Version) – iPC AXXTPMCHNE8 (accessory option) See Chapter 13 for more information.
Serviceability	
Server Management	• Integrated baseboard management controller (BMC) based on the ASPEED* AST2500 Advanced PCIe* Graphics and Remote Management Processor • Intelligent Platform Management Interface (IPMI) 2.0 compliant • Redfish* compliant • Support for Intel® Data Center Manager (DCM) • Support for Intel® Server Debug and Provisioning Tool (SDPTool) • One external 1000BASE-T Ethernet port (RJ45) dedicated for server management • Onboard LEDs for Light Guided Diagnostics
Onboard Configuration and Service Jumpers	• BIOS Defaults • BIOS Password clear • Intel® Management Engine (Intel® ME) firmware force update • BMC force update • BIOS SVN Downgrade • BMC SVN Downgrade For more information, see Chapter 14.
BIOS	• Unified Extensible Firmware Interface (UEFI) –based BIOS (legacy boot not supported)

3.1.2 Feature identification
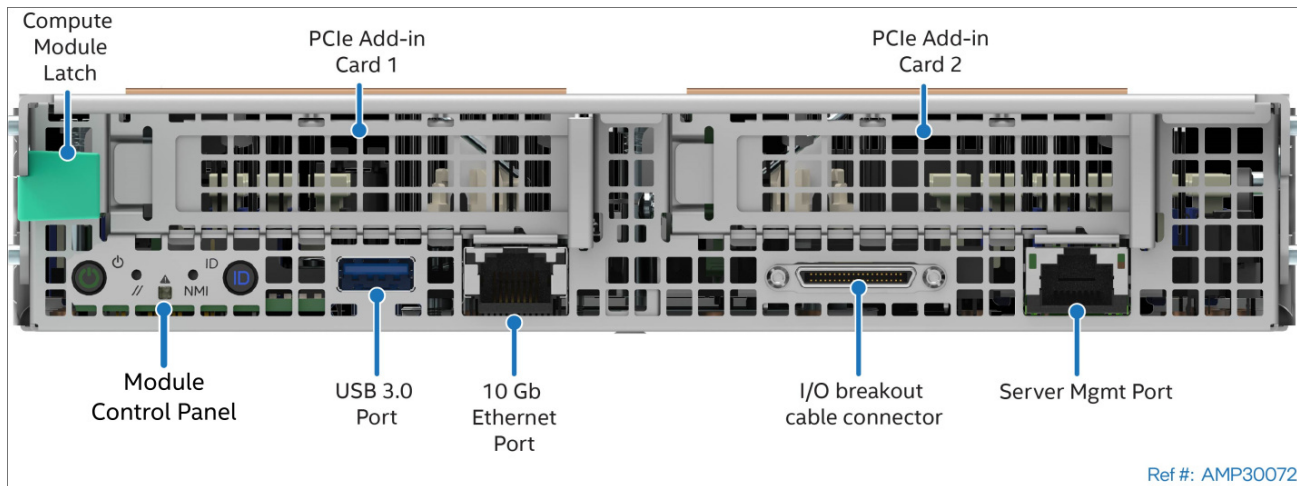
Figure 9. 1U Compute Module Front Panel Features
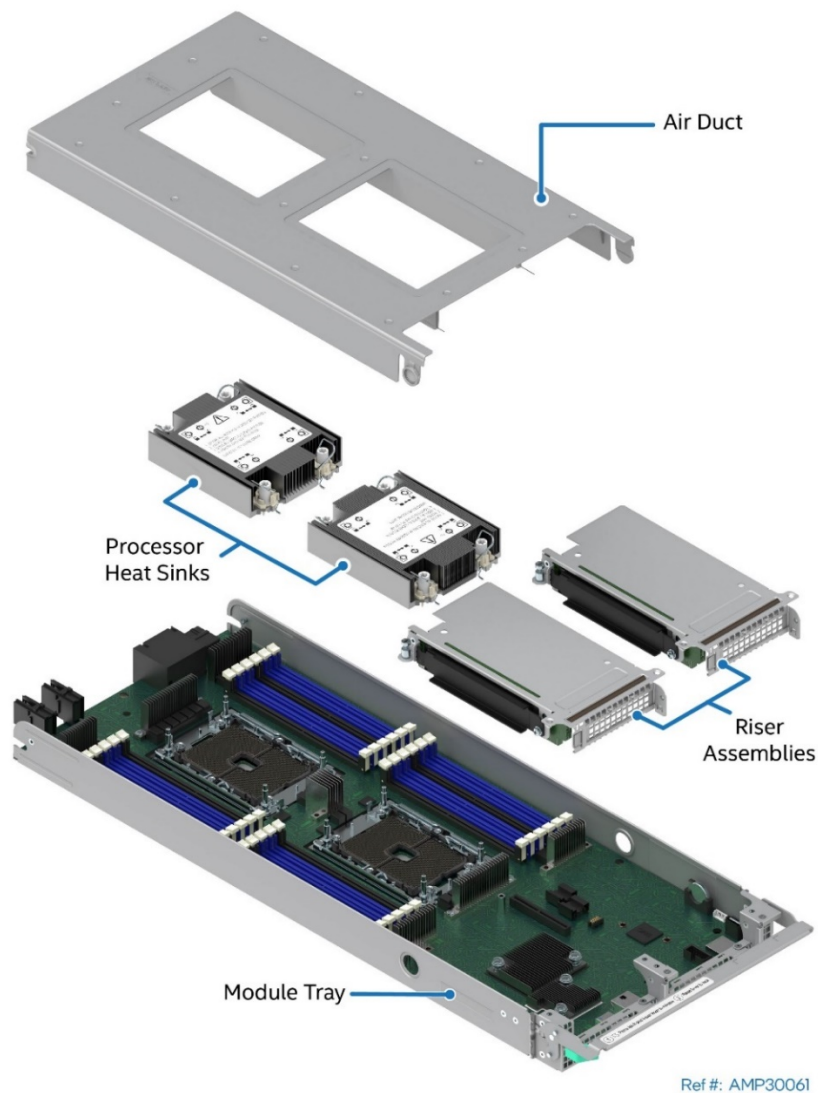
Figure 10. Compute Module Components

4.   System / Chassis Overview

This chapter provides an overview of the system and chassis features, dimensions, and environmental and packaging specifications.

4.1   System / Chassis Features

The Intel® Server D40AMP family provides flexibility for configuring fully integrated power-on ready system solutions. A power-on ready system can include chassis, modules, power supplies, storage, cooling components, and rails for rack or cabinet mounting. The modules are preconfigured and independent, allowing for a power-on ready installation, with configurable memory, internal storage, and network component options. Refer to the *Intel® Server System D40AMP Family Configuration Guide* for a complete list of available options.

The Intel® Server D40AMP family includes two chassis-only products that belong to the Intel® Server chassis VP3000 family. These chassis-only products are listed below.

- 3U air cooled, 2100 W PSU chassis supporting U.2 SSDs – iPC **VP3U2HAC21W0**
    - o Supports up to four 1U compute modules
    - o Supports up to 24x U.2 PCIe* 4.0 NVMe* SSDs
- 3U air cooled, 2100 W PSU chassis supporting E1.L SSDs – iPC **VP3E1HAC21W0**
    - o Supports up to four 1U compute modules
    - o Supports up to 32x E1.L (EDSFF) PCIe* 4.0 NVMe* SSDs

Refer to Table 5 for a feature list of system and chassis-only features.

Figure 11. Intel Server Chassis VP3U2HAC21W0

Figure 12. Intel® Server Chassis VP3E1HAC21W0

Table 5. Intel® Server Chassis / System D40AMP Feature Set

Feature	Description	
	Chassis SKU iPC VP3U2HAC21W0	**Chassis SKU iPC VP3E1HAC21W0**
Chassis Type	VP3000, 3U rack-mount, multi-module, air cooled, for 2.5" drives	VP3000, 3U rack-mount, multi-module, air cooled, for E1.L drives
Chassis Dimensions	• 736.6 mm x 440 mm x 130.8 mm (L x W x H)	
Packaging Dimensions	• 990 mm x 594 mm x 407 mm (L x W x H)	
Cooling	• Four dual-rotor 80 mm hot-swap fans with support for fan redundancy • Six hot-swap dual-rotor 40 mm fans with support for fan redundancy • One fan per installed power supply unit (PSU) See Chapter 9 for more information about cooling.	
Power	Up to four 2100-watt AC power supplies with power redundancy support (dependent on system configuration).	
Rack Mount Kit (VPXXRAILKIT)	• Tool-less installation • Travel distance: 536mm • Max supported weight: 60kg **Note:** Rack mount kit is included with chassis.	
Serviceability	Modular chassis features for simplified serviceability: • Fully independent warm-swappable Intel® D40AMP modules • Hot-swappable power supplies • Hot-swappable front fans • Hot-swappable U.2 solid state drive (SSD) storage (dependent on system configuration) • Hot-swappable full-length PCIe* NVMe* EDSFF SSDs (dependent on system configuration)	
Operating Temperature	10–35 °C ambient temperature	

4.2　System Feature Identification

All systems within the Intel® Server System D40AMP Family are designed for loading compute modules from the back. The following illustrations provide an overview of the rear features.
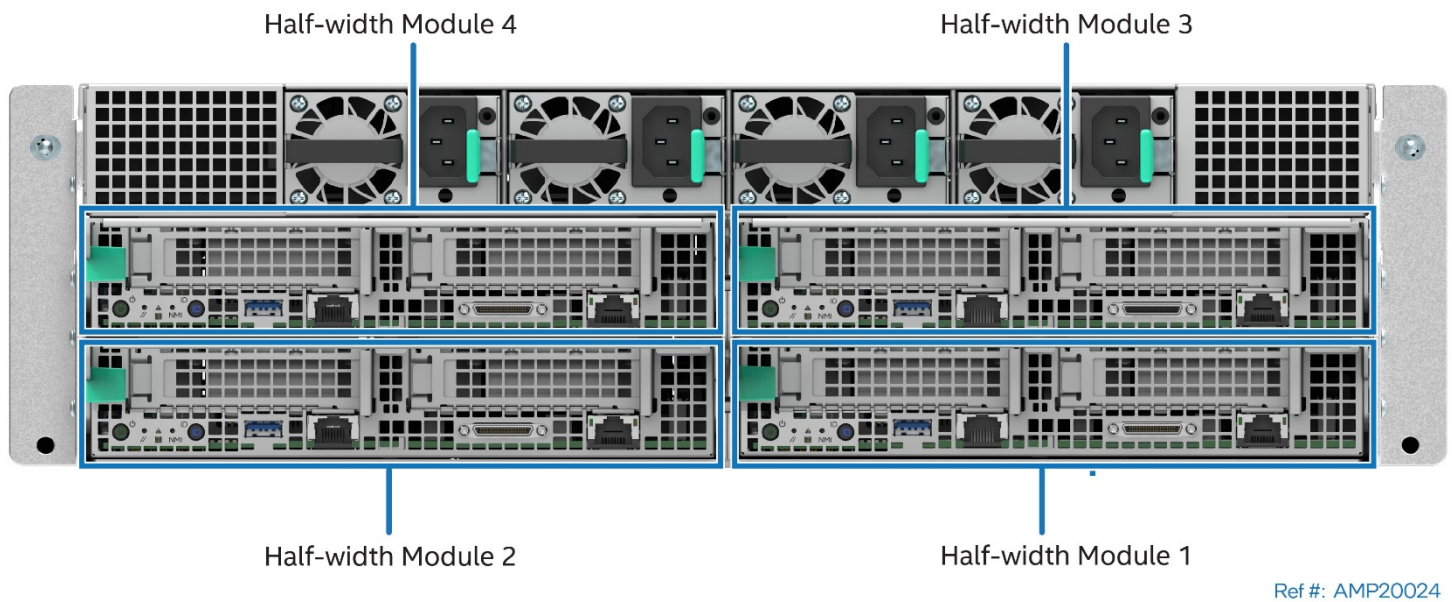
Figure 13. System Rear View - Module Identification

Chassis are offered with support for U.2 NVMe* SSDs or E1.L SSDs. The following illustrations identify key system features for both chassis options.
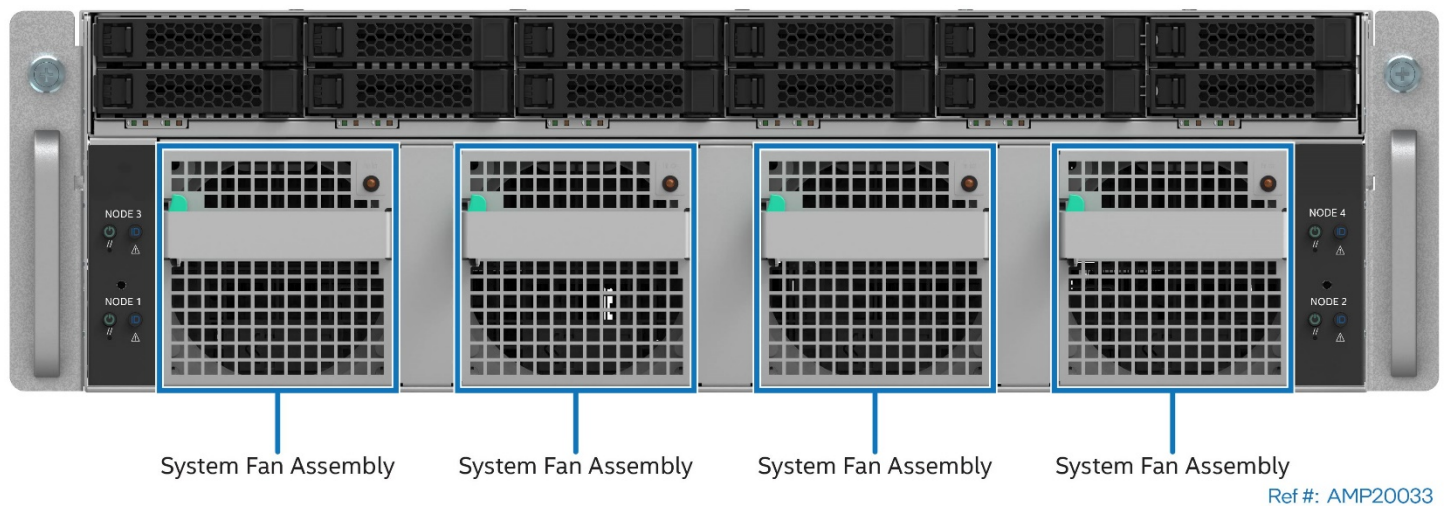
Figure 14. System Front View – Chassis VP3U2HAC21W0
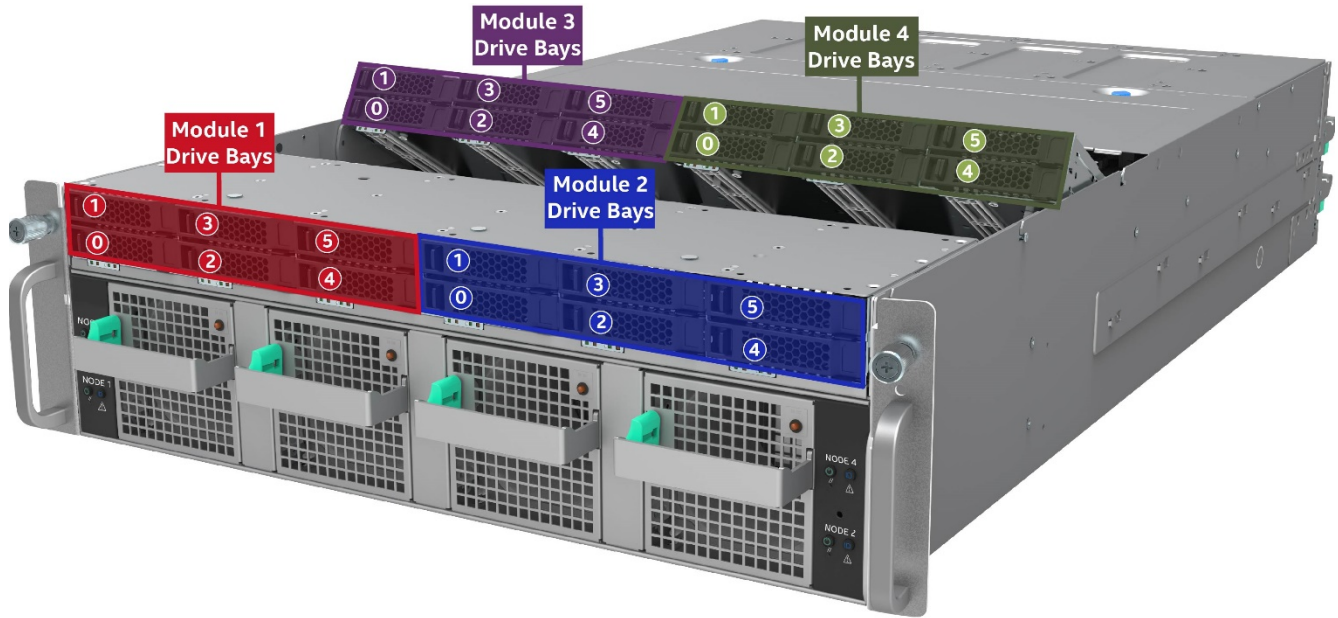
Figure 15. Expanded System Front View – Chassis VP3U2HAC21W0
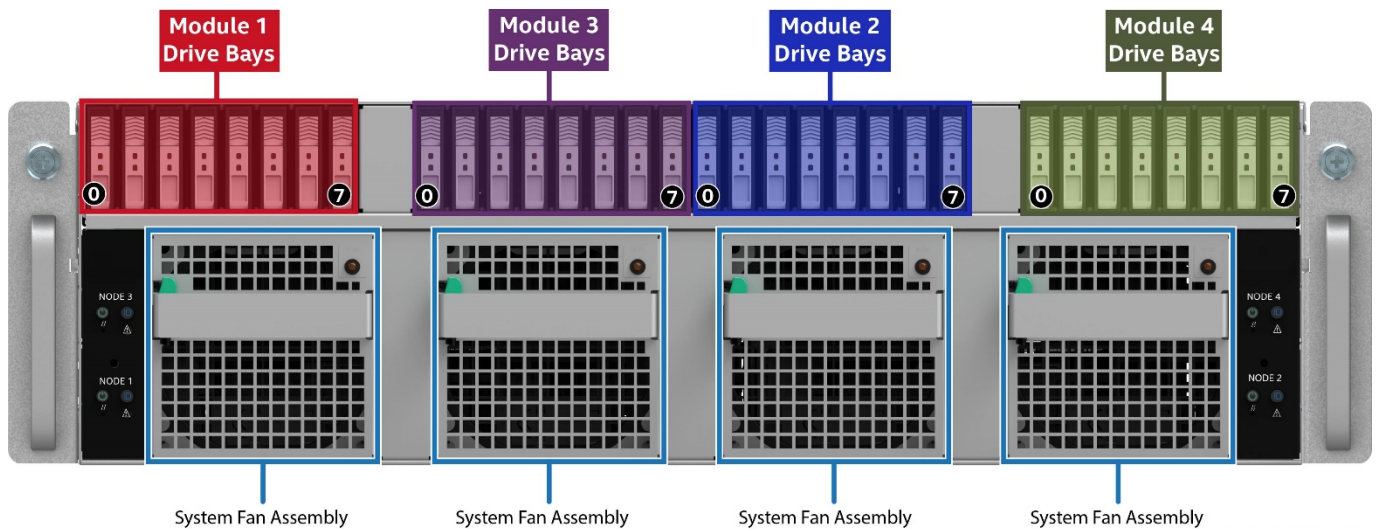
Figure 16. System Front View – Chassis VP3E1HAC21W0

4.3 Rack and Cabinet Mounting Kit

The Intel® Server System D40AMP supports a rail kit for installation into a four-post rack or cabinet. The following installation guidelines should be observed.

- For proper system ventilation, leave a minimum of 15 cm clearance in the front and rear of the system.
- Servers are high-power electrical appliances. They should be installed into dedicated cabinets with vents or professional water-cooled cabinets to prevent system failures caused by overheating.
- If installing more than one server or component into a given rack or cabinet, begin installing them from the bottom and load the heaviest items first.
- Note the cabinet's load-bearing capacity, power source capacity, and heat dissipation capacity. Be sure not to install devices that go beyond the cabinet's capacity thresholds.

- For the convenience of using the rear ports of the system and to allow for cabling, leave a minimum clearance of 150 mm between the back of the system and the inner side of the cabinet's back door.
- If your system has rack handles installed, do not lift, or carry the system solely by the rack handles. These handles are intended for the sole purpose of pulling a system from or pushing it into a rack.
- When lifting or moving a system, it is best to grasp and lift it by all four corners using two or more people. Do not grasp and lift the system by two opposing diagonal corners. Doing so will flex the chassis that may damage the internal system components.
- With no other option available but to lift the system using only two points of contact, grasp and lift the system at the mid-point of each side of the system.

Features and specifications for the rail kit are listed below:

- iPC **VPXXRAILKIT– Spare/Accessory** Rail Kit
  - o Tool-less installation
  - o Travel distance: 536mm
  - o Max supported weight: 60kg

Safety Note: Due to the weight of a fully configured system, Intel recommends using a mechanical lift to aid with the installation of the system into the rack, and/or use at least two people to install the system into the rack. Alternatively, remove all installed modules from the system before attempting to install the system into a rack or cabinet.

4.4   System / Chassis Level Environmental Limits

The following table defines the system level operating and non-operating environmental limits.

Table 6. System Environmental Limits Summary

Parameter		Limits
Temperature	Operating	ASHRAE Class A2 – Continuous Operation. 10 °C to 35 °C (50 °F to 95 °F) with the maximum rate of change not to exceed 10 °C per hour.
	Shipping	–40 °C to 70 °C (-40 °F to 158 °F)
Altitude	Operating	Support operation up to 3050 m with ASHRAE class de-ratings.
Humidity	Shipping	50% to 90%, non-condensing with a maximum wet bulb of 28 °C (at temperatures from 25 °C to 35 °C)
Shock	Operating	Half sine, 2 g, 11 msec
	Unpackaged	Trapezoidal, 25 g, velocity change is based on packaged weight
	Packaged	ISTA (International Safe Transit Association) Test Procedure 3A 2008
Vibration	Unpackaged	5 Hz to 500 Hz, 2.20 g RMS random
	Packaged	ISTA (International Safe Transit Association) Test Procedure 3A 2008
AC-DC	Voltage	200 V to 240 V
	Frequency	47 Hz to 63 Hz
	Source Interrupt	No loss of data for power line drop-out of 12 msec
	Surge Non-operating and operating	Unidirectional

Parameter		Limits
	Line to earth Only	AC Leads 2.0 kV I/O Leads 1.0 kV DC Leads 0.5 kV
ESD	Air Discharged	12.0 kV
	Contact Discharge	8.0 kV
Projected Sound Power (environmental condition: 23 C ±2°C)	Maximum	~ 8.9 BA
	Active	~ 7.7 BA
	Idle	~ 6.5 BA

Disclaimer: Intel Corporation server systems support add-in peripherals and contain several 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. 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.

For system configuration requirements and limitations, refer to Appendix E in this document or the Intel® Power Budget and Thermal Configuration Tool.

4.5   System / Chassis Packaging

The original Intel packaging is designed to provide protection to a fully configured system and tested to meet International Safe Transit Association (ISTA) Test Procedure 3A (2008). The packaging is designed to be re-used for shipment after system integration has been completed.

The original packaging includes two layers of boxes – an inner box and the outer shipping box – and various protective inner packaging components. The boxes and packaging components are designed to function together as a protective packaging system. When reused, all of the original packaging material must be used, including both boxes and each inner packaging component. In addition, all inner packaging components must be reinstalled in the proper location to ensure adequate protection of the system for subsequent shipment.

Note: The design of the inner packaging components does not prevent improper placement within the packaging assembly. There is only one correct packaging assembly that allows the package to meet the ISTA Test Procedure 3A (2008) limits. See the *Intel® Server System D40AMP Family System Integration and Service Guide* for complete packaging assembly instructions.

Failure to follow the specified packaging assembly instructions may result in damage to the system during shipment.

- **Outer shipping box external dimensions**
  - Length: 990 mm
  - Breadth: 594 mm
  - Height: 407 mm
- **Inner box internal dimension**
  - Length: 972 mm
  - Breadth: 579 mm
  - Height: 374 mm

5.   Processor Support

The Intel® Server Board D40AMP includes two Socket-P4 LGA4189 processor sockets compatible with the 3rd Gen Intel® Xeon® Scalable processor family. This chapter provides information on processor heat sinks, thermal design power (TDP), and population rules. The chapter also provides a processor family overview.

Note: Previous-generation Intel® Xeon® processors and Intel® Xeon® Scalable processor families and their supported processor heat sinks are not compatible with server boards described in this document.

Visit https://serverconfigurator.intel.com/exodus/page?eventType=11&targetPageId=120224
 for a complete list of supported processors.

5.1   Processor Heat Sink Module (PHM) Assembly and Processor Socket Assembly

This generation of server system requires that the processor be pre-assembled to the heat sink before installation on to the server board. The processor heat sink assembly is commonly referred to as the Processor Heat Sink Module or PHM. The assembly is installed onto the processor socket assembly (referred to as the loading mechanism) on the server board. The following figure identifies each component associated with the PHM and processor socket assembly.

Note: The following figure identifies the PHM components, not the processor installation process.
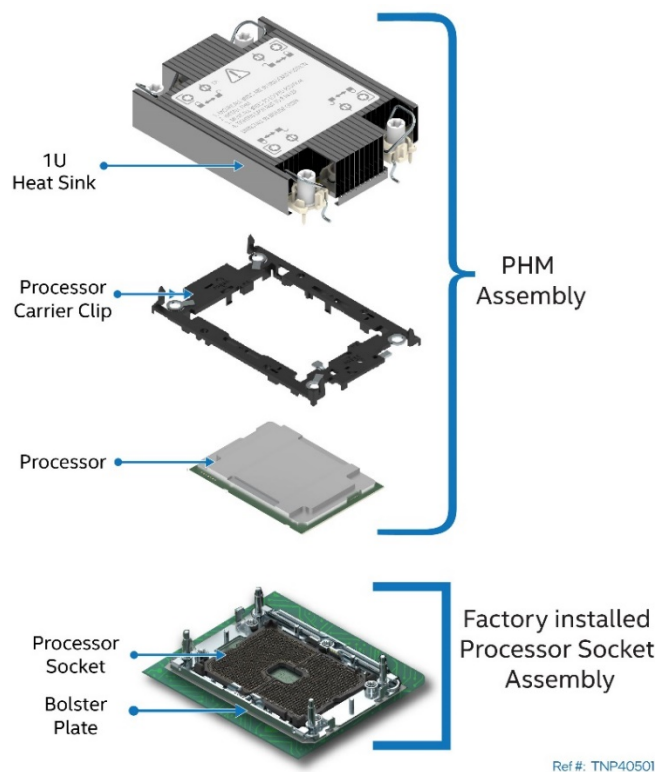
Figure 17. PHM Components and Processor Socket Reference Diagram

Note: For detailed processor assembly and installation instructions, see the *Intel® Server System D40AMP Integration and Service Guide*.

5.1.1   Processor Heat Sink

The Intel® Server D40AMP family supports 1U height heat sinks as shown in the following figures. There are two types of 1U heat sinks, a front heat sink and a back heat sink. The front heat sink type is used for CPU0 and the back heat sink type is used for CPU1. The exploded views in the figures show the difference. The front heat sink type has more heat venting fins. The front and back heatsinks are not interchangeable.

Note: references to front and back assume the compute module is out of the chassis and the reader is facing the external I/O ports.

1U Back Heat Sink   **1U Front Heat Sink**
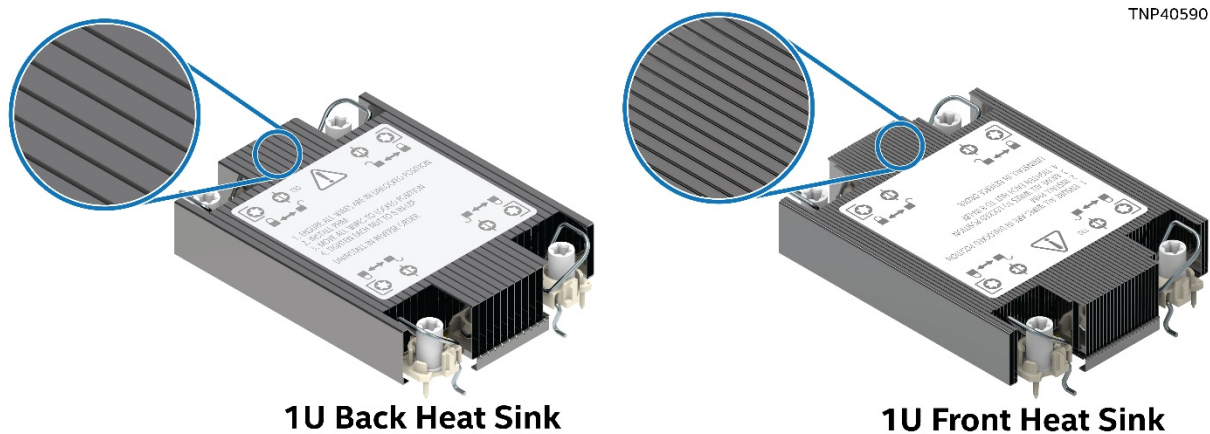
Figure 18. 1U Supported Processor Heat Sinks

The following figure shows a module with 1U front and back heat sinks installed.
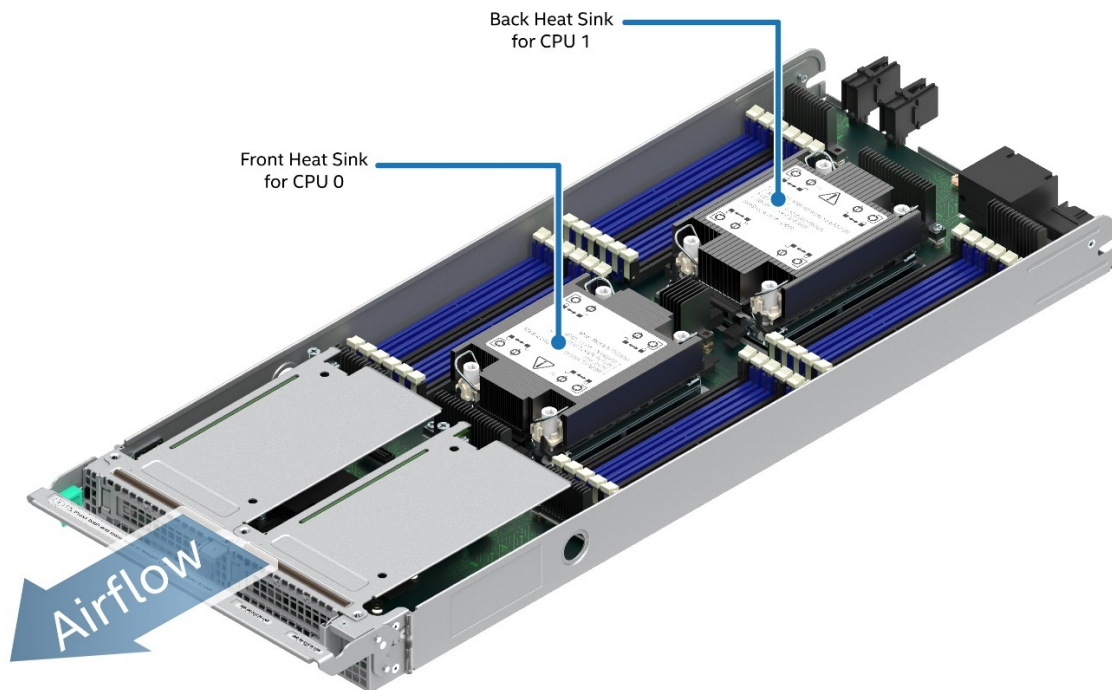
Figure 19. 1U Heat Sinks Installed in Compute Module

5.2   Processor Thermal Design Power (TDP) Support

To allow optimal operation and long-term reliability of systems within the Intel® Server D40AMP family, the processor must remain within the defined minimum and maximum case temperature (T_{CASE}) specifications. When installed in an Intel® D40AMP Compute Module, The Intel® Server Board D40AMP supports a maximum processor TDP up to and including 205 W. Depending on module and system configuration, the Intel® Server System D40AMP may support a TDP up to and including 205 W. For details, see Appendix E.

5.3   Processor Family Overview

The Intel® Server Board D40AMP supports the 3rd Gen Intel® Xeon® Scalable processor family. Processor shelves within the product family are identified as shown in the following figure.
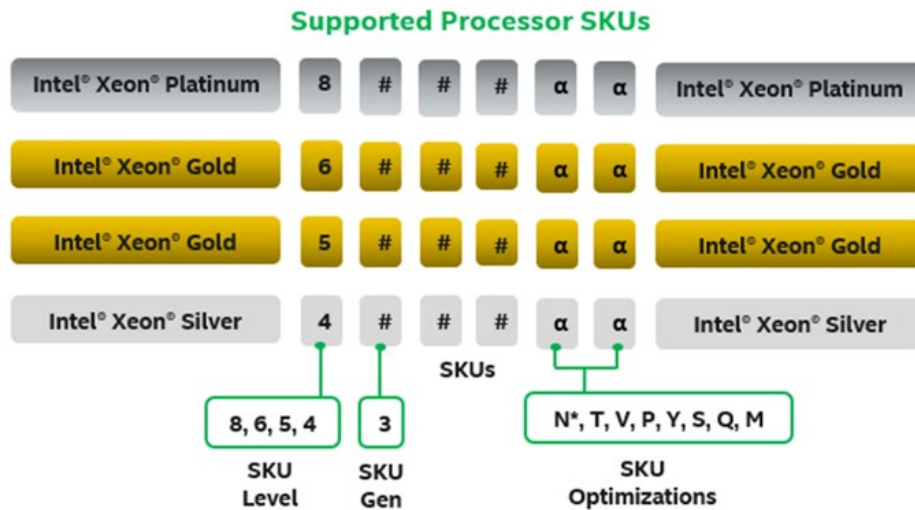
Figure 20. 3rd Gen Intel® Xeon® Scalable Processor Identification

Note: The 8351N SKU is a single-socket optimized SKU and is not supported on the Intel® Server D40AMP family.

Table 7. 3rd Gen Intel® Xeon® Scalable Processor Family Feature Comparison

Feature	Platinum 8300 Processors	Gold 6300 Processors	Gold 5300 Processors	Silver 4300 Processor
# of Intel® UPI Links	3	3	3	2
Intel® UPI Speed	11.2 GT/s	11.2 GT/s	11.2 GT/s	10.4 GT/s
Supported Topologies	2S–2UPI 2S–3UPI	2S–2UPI 2S–3UPI	2S–2UPI 2S–3UPI	2S–2UPI
Node Controller Support	No	No	No	No
Processor RAS Capability	Advanced	Advanced	Advanced	Standard
# of DDR4 Integrated Memory Controllers (IMC)	4	4	4	4
# DDR4 Channels	8	8	8	8
Intel® Turbo Boost Technology	Yes	Yes	Yes	Yes
Intel® HT Technology	Yes	Yes	Yes	Yes
Intel® AVX-512 ISA Support	Yes	Yes	Yes	Yes

Feature	Platinum 8300 Processors	Gold 6300 Processors	Gold 5300 Processors	Silver 4300 Processor
Intel® AVX-512 - # of 512b FMA Units	2	2	2	2
# of PCIe* Lanes	64	64	64	64
Intel® VMD 2.0	Yes	Yes	Yes	Yes

Note: Feature may vary between processor SKUs.

Reference 3rd Gen Intel® Xeon® Scalable processor specification sheets and product briefs for additional information.

5.4 Processor Population Rules

When two processors are installed, both processors must have identical extended family, extended model number and processor type.

Note: Processors with different steppings can be mixed in a system as long as the rules mentioned above are met.

Population rules are applicable to any combination of processors within the 3rd Gen Intel® Xeon® Scalable processor family.

For additional information on processor population rules, refer to the *BIOS Firmware External Product Specification (EPS) for the Intel® Server Board D50TNP, M50CYP, and D40AMP Families.*

Note: The server board may support dual-processor configurations consisting of different processors that meet the defined criteria. However, Intel does not perform validation testing of these configurations. In addition, Intel does not ensure that a server system configured with unmatched processors will operate reliably. The system BIOS attempts to operate with processors that are not matched but are generally compatible. For optimal system performance in dual-processor configurations, Intel recommends that identical processors be installed.

6.   System Memory

This chapter describes the architecture that drives the memory subsystem, supported memory types, memory population rules, and supported memory RAS features.

6.1   Memory Subsystem Architecture

The Intel® Server Board D40AMP includes 8 DDR4 DIMM slots and 4 Intel® Optane™ PMem DIMM slots, for a total of 12 DIMM slots per processor.

Each 3rd Gen Intel® Xeon® Scalable processor supports eight memory channels using four integrated memory controllers (IMCs). Each memory channel is assigned an identifying letter from A to H. Channels A, C, E, and G each provide two DIMM slots – slot 1 (blue slot supporting DDR4 DIMMs) and slot 2 (black slot supporting Intel® Optane™ PMem DIMMs). The remaining channels each provide one DIMM slot (blue slot supporting DDR4 DIMMs).

Figure 21. Memory Slot Connectivity Diagram

6.2   Supported Memory

The Intel® Server D40AMP family supports standard DDR4 RDIMMs and LDRIMMs. Aside from Standard DDR4, the Intel® Server D40AMP family supports Intel® Optane™ persistent memory 200 series modules.

Note: Previous generation Intel® Optane™ persistent memory modules are not supported.

6.2.1   Standard DDR4 DIMM Support

The following figure shows a standard DDR4 DIMM.
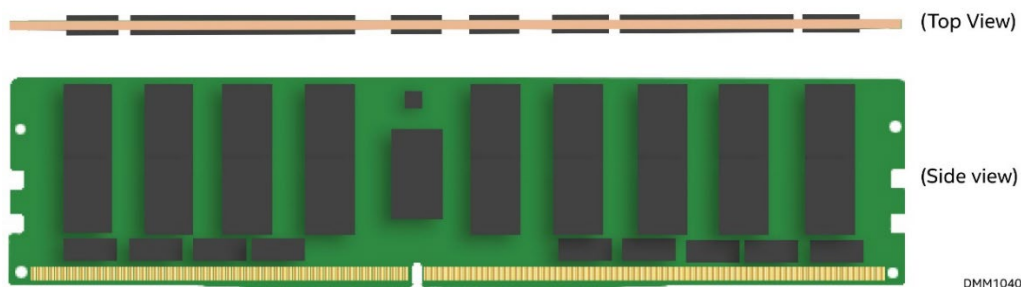
Figure 22. Standard DRAM DDR4 DIMM

The Intel® Server D40AMP family supports DDR4 DIMMs with the following features:

- All DDR4 DIMMs must support ECC
- Registered DDR4 (RDIMM), 3DS-RDIMM, Load Reduced DDR4 (LRDIMM), 3DS-LRDIMM

Note: 3DS = 3-dimensional Stacking

- RDIMMs and LRDIMMs with thermal sensor on-DIMM (TSOD)
- DIMM capacities of 8 GB, 16 GB, 32 GB, 64 GB, and 128 GB
- RDIMMs organized as Single Rank (SR), Dual Rank (DR)
- 3DS-RDIMM organized as Quad Rank (QR), or Oct Rank (OR)
- LRDIMMs organized as Quad Rank (QR)
- 3DS-LRDIMM organized as Quad Rank (QR), or Oct Rank (OR)

The following tables list the DDR4 DIMM support guidelines.

Table 8. Supported DDR4 DIMM Memory

Type	Ranks per DIMM and Data Width	DIMM Capacity (GB)		Maximum Speed (MT/s) at 1.2 V
		8 Gb DDR4 Density	16 Gb DDR4 Density	1 DPC
RDIMM	SR x8	8	16	3200
	SR x4	16	32	3200
	DR x8	16	32	3200
	DR x4	32	64	3200
3DS-RDIMM	QR/OR x4	64 (2H) 128 (4H)	128 (2H)	3200
LRDIMM	QR x4	64	128	3200
3DS-LRDIMM	QR/OR x4	128 (4H)	128 (2H)	3200

Note: SR = Single Rank, DR = Dual Rank, QR = Quad Rank, OR = Oct Rank, H = Stack Height, DPC = DIMMs Per Channel

---

The maximum supported DRAM DIMM speed depends on the processor tier as shown in the following table.

Table 9. Maximum Supported Standard DRAM DIMM Speed by Processor Shelf

Processor Family	Maximum DIMM Speed (MT/s) by processor Shelf			
	Platinum 8300 Processors	Gold 6300 Processors	Gold 5300 Processors	Silver 4300 Processors
3rd Gen Intel® Xeon® Scalable processors	3200	3200	2933	2666

Notes:
1. Specification applies only to memory chips mounted by the surface mounted technology (SMT) method.
2. Gold processor SKU 6330 maximum speed is 2933 (MT/s).

6.2.2　　　Intel® Optane™ Persistent Memory 200 Series Support

The Intel® Compute Module D40AMP supports Intel® Optane™ persistent memory 200 series.

Note: Previous generation Intel® Optane™ persistent memory modules are not supported.
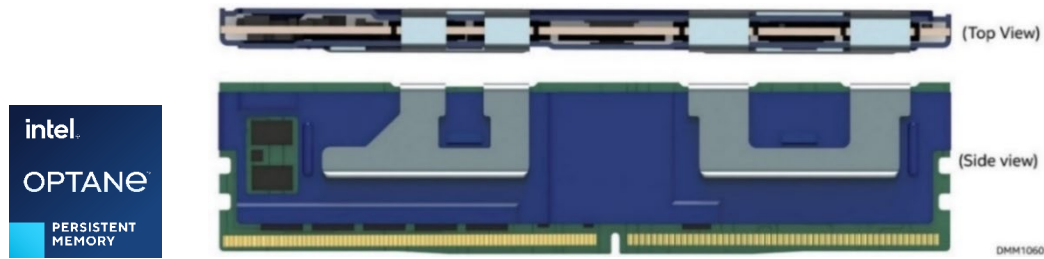
Figure 23. Intel® Optane™ Persistent Memory 200 Series Module

Intel® Optane™ PMem is an innovative technology that delivers a unique combination of affordable large memory capacity and data persistence (non-volatility). It represents a new class of memory and storage technology architected specifically for data center usage. Intel® Optane™ PMem 200 series enables higher density (capacity per DIMM) DDR4-compatible memory modules with near-DRAM performance and advanced features not found in standard DRAM.

Intel® Optane™ PMem 200 Series modules support the following features:

- DDR4 Pin Compatible
- Available PMem Capacities – 128, 256, 512 GB
- Up to 2 TB per processor socket
- Up to 3200 MT/sec
- TDP = 15 W
- AES256 Bit Encryption
- Secure Erase
- Data persistence in power failure event – – ADR, eADR (optional)

See Section 6.4 for memory RAS features and Intel® Optane™ PMem 200 series compatibility with security features Intel® Software Guard Extensions (Intel® SGX), Intel® Total Memory Encryption (Intel® TME), and Intel® Total Memory Encryption – Multi-Tenant (Intel® TME-MT).

Supported operating modes:

- Memory mode (MM)
- App Direct (AD) mode

6.2.2.1　　　Intel® Optane™ Persistent Memory 200 Series – Memory Mode (MM)

In Memory mode, the standard DDR4 DRAM acts as a cache for the most frequently accessed data, while Intel® Optane™ persistent memory 200 series modules provide large memory capacity by acting as direct load/store memory. In this mode, applications and operating system are explicitly aware that the Intel® Optane™ persistent memory 200 series is the only type of direct load/store memory in the system. Cache management operations are handled by the integrated memory controller in the 3rd Gen Intel® Xeon® Scalable processor.

When data is requested from memory, the memory controller first checks the DRAM cache. If the data is present, the response latency is identical to DRAM. If the data is not in the DRAM cache, it is read from the Intel® Optane™ persistent memory 200 series modules with slightly longer latency. The applications with consistent data retrieval patterns that the memory controller can predict, will have a higher cache hit rate.

Data is volatile in Memory mode. It will not be saved in the event of power loss. Persistence is enabled in App Direct mode.

6.2.2.2 Intel® Optane™ Persistent Memory 200 Series – App Direct (AD) Mode

In App Direct mode, the operating system sees Intel® Optane™ persistent memory and DDR4 DRAM DIMMs as two separate pools of memory. App Direct mode can direct which type of data read or write is suitable for DRAM or Intel® Optane™ PMem. Operations that require the lowest latency and do not need permanent data storage can be executed on DRAM DIMMs, such as database "scratch pads". Data that needs to be made persistent or structures that are very large can be routed to Intel® Optane™ persistent memory. The App Direct mode must be used to make data persistent in memory. This mode requires an operating system or virtualization environment enabled with a persistent memory-aware file system.

App Direct mode requires both driver and explicit software support. To ensure operating system compatibility, visit https://www.intel.com/content/www/us/en/products/details/memory-storage/optane-dc-persistent-memory.html

6.2.2.3 Intel® Optane™ PMem configuration using the BIOS Setup Utility

Following the installation of Intel® Optane™ PMem devices into the system, they need to be configured using the BIOS Setup utility. The BIOS Setup utility includes several Intel® Optane™ PMem configuration options across multiple BIOS Setup screens. The following illustration provides a BIOS Setup screen navigation directing the user to the main Intel® Optane™ PMem configuration screen.
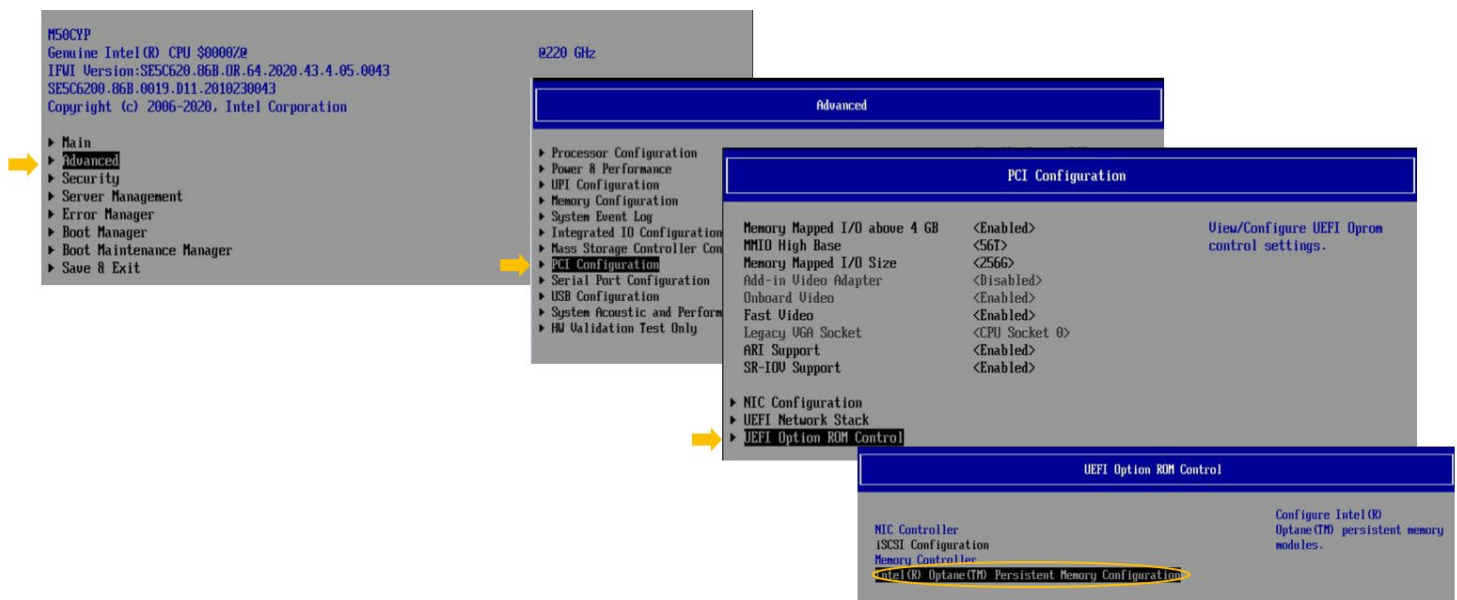
Figure 24. BIOS Setup Utility Screen Navigation for Intel® Optane™ PMem Setup Options

From the main BIOS Setup page navigate to Advanced > PCI Configuration > UEFI Option ROM Control > Intel® Optane™ Persistent Memory Configuration. The main Intel® Optane™ PMem Configuration screen provides links to the various device information and setup screens.
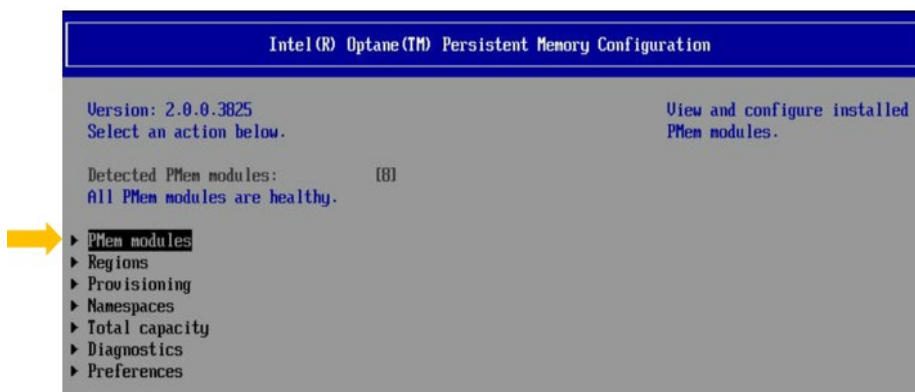
Figure 25. Intel® Optane™ PMem Configuration Menu in BIOS Setup Utility

Refer to the *Intel® Optane™ Persistent Memory Startup Guide* and the *Intel® Optane™ Persistent Memory 200 Series Operations Guide* for details on how to configure Intel® Optane™ PMem on the Intel® Server D40AMP family. See Table 1 for details.

6.3   Memory Population

The Intel® Server Board D40AMP, as well as the Intel® Compute Module D40AMP support memory configurations that consist of both standard DDR4 DIMMs and Intel® Optane™ persistent memory 200 series modules. With two processors installed, 8 memory slots are available for Intel® Optane™ persistent memory 200 series and 16 memory slots are available for DDR4 DIMMs.

This section provides memory population rules and recommendations for standard DIMMs and Intel® Optane™ persistent memory 200 series modules. The following figure shows the full board layout for all memory slots on both processor sockets.

Figure 26. Intel® Server Board D40AMP Memory Slot Layout

6.3.1   Standard DDR4 DIMM Population Rules

Intel DDR4 DIMM Support Disclaimer:

Intel validates and will only provide support for system configurations where all installed DDR4 DIMMs have matching "Identical" or "Like" attributes. See Table 10. A system configured concurrently with DDR4 DIMMs from different vendors will be supported by Intel if all other DDR4 "Like" DIMM attributes match.

Intel does not perform system validation testing nor will it provide support for system configurations where all populated DDR4 DIMMs do not have matching "Like" DIMM attributes as listed in Table 10.

Intel will only provide support for Intel server systems configured with DDR4 DIMMs that have been validated by Intel and are listed on Intel's Tested Memory list for the given Intel server product family.

Intel configures and ships pre-integrated L9 server systems. All DDR4 DIMMs within a given L9 server system as shipped by Intel will be identical. All installed DIMMs will have matching attributes as those listed in the *"Identical" DDR4 DIMM4 Attributes* column in Table 10.

When purchasing more than one integrated L9 server system with the same configuration from Intel, Intel reserves the right to use "Like" DIMMs between server systems. At a minimum, "Like" DIMMS will have matching DIMM attributes as listed in the table below. However, the DIMM model #, revision #, or vendor may be different.

For warranty replacement, Intel will make every effort to ship back an exact match to the one returned. However, Intel may ship back a validated "Like" DIMM. A "Like" DIMM may be from the same vendor but may not be the same revision # or model #, or it may be an Intel validated DIMM from a different vendor. At a minimum, all "Like" DIMMs shipped from Intel will match attributes of the original part according to the definition of "Like" DIMMs in the following table.

Table 10. DDR4 DIMM Attributes Table for "Identical" and "Like" DIMMs

• DDR4 DIMMs are considered "Identical" when ALL listed attributes between the DIMMs match • Two or more DDR4 DIMMs are considered "Like" DIMMs when all attributes minus the Vendor, and/or DIMM Part # and/or DIMM Revision#, are the same.			
Attribute	**"Identical" DDR4 DIMM Attributes**	**"Like" DDR4 DIMM Attributes**	**Possible DDR4 Attribute Values**
Vendor	**Match**	**Maybe Different**	Memory Vendor Name
DIMM Part #	**Match**	**Maybe Different**	Memory Vendor Part #
DIMM Revision #	**Match**	**Maybe Different**	Memory Vendor Part Revision #
DRAM Type	**Match**	**Match**	DDR4
DIMM Type	**Match**	**Match**	RDIMM, LRDIMM
Speed (MHz)	**Match**	**Match**	2666, 2933, 3200
Voltage	**Match**	**Match**	1.2V
DIMM Size (GB)	**Match**	**Match**	8GB, 16GB, 32GB, 64GB, 128GB, 256GB
Organization	**Match**	**Match**	1Gx72; 2Gx72; 4Gx72; 8Gx72; 16Gx72; 32Gx72
DIMM Rank	**Match**	**Match**	1R, 2R, 4R, 8R
DRAM Width	**Match**	**Match**	x4, x8
DRAM Density	**Match**	**Match**	8Gb, 16Gb

Note: Intel only supports mixed DDR4 DRAM DIMM configurations as defined in the Intel DDR4 Support Disclaimer above.

The following DDR4 DIMM population rules apply for best operation. However, see the *Intel DDR4 DIMM Support Disclaimer* above for Intel support guidelines.

- DDR4 DIMMs can only be installed in blue slots
- Mixed DDR4 DIMM rules:
  - Mixing DDR4 DIMMs of different speeds and latencies is not supported within or across processors. If a mixed configuration is encountered, the BIOS attempts to operate at the highest common speed and the lowest latency possible.
  - Mixing of DDR4 DIMM types (RDIMM, LRDIMM, 3DS-RDIMM, 3DS-LRDIMM) within or across processors is not supported. This is a Fatal Error Halt in Memory Initialization.
- When channels A, C, E, and G are populated, they must be populated with same total DDR4 DIMM capacity per channel for a balanced performance.
- When channels B, F, D, and H are populated, they must be populated with same total DDR4 DIMM capacity per channel for a balanced performance.
- Memory slots associated with a given processor are unavailable if the corresponding processor socket is not populated
- Processor sockets are self-contained and autonomous. However, all memory subsystem support (such as memory RAS and error management) in the BIOS Setup are applied commonly for each installed processor.
- For best system performance, memory must be installed in all eight channels for each installed processor.
- For best system performance in dual processor configurations, installed DDR4 DIMM type and population for DDR4 DIMMs configured to CPU1 must match DDR4 DIMM type and population configured to CPU0. For additional information, refer to Section 6.3.3.

6.3.2 Intel® Optane™ Persistent Memory 200 Series Module Rules

All operating modes:

- Only Intel® Optane™ persistent memory 200 series modules are supported.
- Intel® Optane™ persistent memory 200 series modules are only supported in DIMM slot 2 (black slot), and DIMM slot 1 (blue slot) in the same memory channel must be populated with one DDR4 DIMM.
- Mixing of different DDR4 DIMM types on the system is not supported nor validated.
  - Intel® Optane™ persistent memory 200 series modules must have the same capacity and type across or within all sockets.
  - DDR DIMMs must have the same capacity and type across or within all sockets.

Memory mode:
- Populate each memory channel with at least one DDR4 to maximize bandwidth.
- Intel® Optane™ persistent memory 200 series modules must be populated symmetrically for each installed processor (corresponding slots populated on either side of each processor) and across both processors.

App Direct mode:
- Minimum of one Intel® Optane™ persistent memory 200 series module for the board.
- Intel® Optane™ persistent memory 200 series modules must be populated symmetrically for each installed processor (corresponding slots populated on either side of each processor) and across both processors.

Table 11. Intel® Optane™ Persistent Memory 200 Series Module Support

Processor SKU Level	Intel® Optane™ Persistent Memory 200 Series Capacity (GB)	Max Speed (MT/s)
Silver 4300 processors (Silver 4314 processor SKU only)	128 256 512	2666
Gold 5300 processors	128 256 512	2933
Gold 6300 processors	128 256 512	3200
Platinum 8300 processors	128 256 512	3200

Table 12. Standard DDR4 DIMMs Compatible with Intel® Optane™ Persistent Memory 200 Series Modules

Type	Ranks per DIMM and Data Width	DIMM Size (GB)	
		8 Gb DRAM Density	16 Gb DRAM Density
RDIMM (PTH – up to 2933 MT/s) (SMT – up to 3200 MT/s)	SR x8	N/A	N/A
	SR x4	16	32
	DR x8	16	32
	DR x4	32	64
3DS-RDIMM (PTH – up to 2933 MT/s) (SMT – up to 3200 MT/s)	QR x4 (2H)	N/A	128
	OR x4 (4H)	N/A	N/A
LRDIMM (PTH/SMT – up to 3200 MT/s)	QR x4	64	128
3DS-LRDIMM (PTH/SMT – up to 3200 MT/s)	QR x4 (2H)	N/A	128
	OR x4 (4H)	128	N/A

Note: SR = Single Rank, DR = Dual Rank, QR = Quad Rank, OR = Oct Rank, H = Stack Height, PTH = Plated Through Hole, SMT = Surface-Mount Technology

6.3.3 Recommended Memory Configurations

This section provides the recommended memory population configurations for the Intel® Server D40AMP family. For best system performance in dual-processor configurations, installed memory type and population should be the same for both processors.

See the following figures and tables to identify the memory slot locations and recommended population configurations.
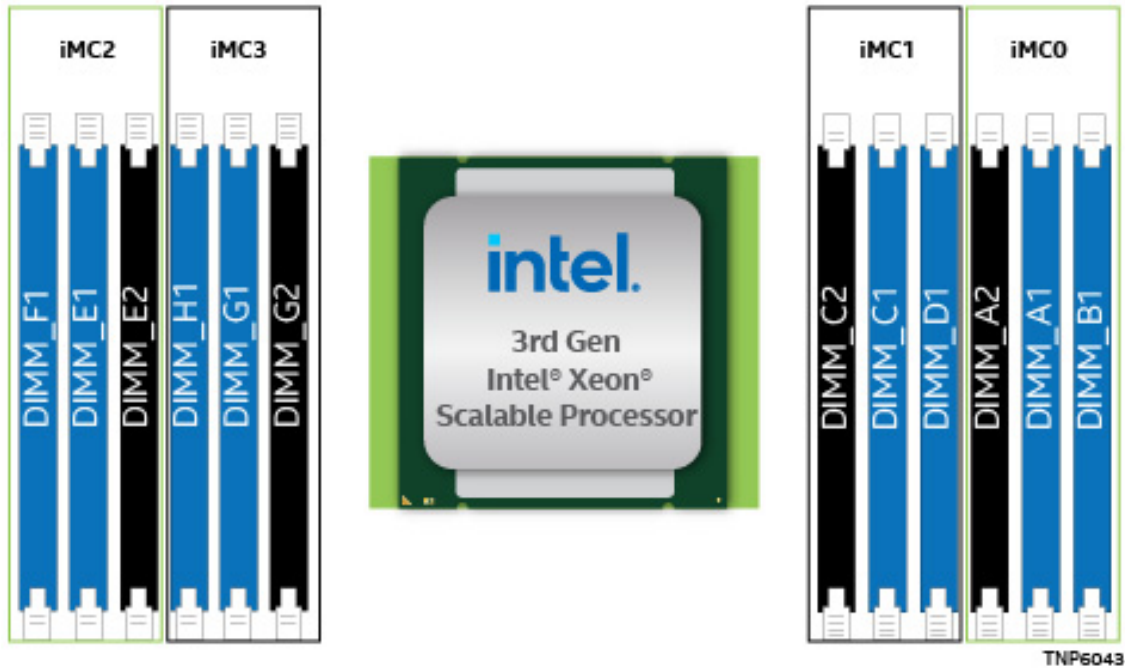
Figure 27. Intel® Server Board D40AMP Memory Slot Identification

Table 13. Standard DDR4 DIMM-only per Socket Population Configurations

# of DIMMs	IMC 2			IMC 3			IMC 1			IMC 0		
	CH F	CH E		CH H	CH G		CH C		CH D	CH A		CH B
	Slot 1	Slot 1	Slot 2	Slot 1	Slot 1	Slot 2	Slot 2	Slot 1	Slot 1	Slot 2	Slot 1	Slot 1
1	-	-	-	-	-	-	-	-	-	-	DDR4 [1]	-
2	-	DDR4	-	-	-	-	-	-	-	-	DDR4	-
2	-	-	-	-	DDR4	-	-	DDR4	-	-	-	-
2	-	-	-	-	-	-	-	DDR4	-	-	DDR4	-
2	-	DDR4	-	-	DDR4	-	-	-	-	-	-	-
2	-	-	-	-	-	-	-	-	DDR4	-	DDR4	-
4	-	DDR4	-	-	DDR4	-	-	DDR4	-	-	DDR4	-
6	DDR4	DDR4	-	-	DDR4	-	-	DDR4	-	-	DDR4	DDR4
8	DDR4	DDR4	-	DDR4	DDR4	-	-	DDR4	DDR4	-	DDR4	DDR4

[1] Recommended location. DDR4 may be populated in slot 1 on any channel.

Table 14. Standard DDR4 DIMM and Intel® Optane™ Persistent Memory 200 Series Module (PMem) per Socket Population Configurations

# of DIMMs	Mode	IMC 2			IMC 3			IMC 1			IMC 0		
		CH F	CH E		CH H	CH G		CH C		CH D	CH A		CH B
		Slot 1	Slot 1	Slot 2	Slot 1	Slot 1	Slot 2	Slot 2	Slot 1	Slot 1	Slot 2	Slot 1	Slot 1
8 DDR4 / 1 PMem	AD	DDR4	DDR4	-	DDR4	DDR4	-	-	DDR4	DDR4	PMem	DDR4	DDR4
	AD	DDR4	DDR4	-	DDR4	DDR4	-	PMem	DDR4	DDR4	-	DDR4	DDR4
	AD	DDR4	DDR4	PMem	DDR4	DDR4	-	-	DDR4	DDR4	-	DDR4	DDR4
	AD	DDR4	DDR4	-	DDR4	DDR4	PMem	-	DDR4	DDR4	-	DDR4	DDR4
8 DDR4 / 4 PMem	AD or MM	DDR4	DDR4	PMem	DDR4	DDR4	PMem	PMem	DDR4	DDR4	PMem	DDR4	DDR4

Note: AD = App Direct mode, MM = Memory Mode, PMem = Persistent Memory

Notes on Intel® Optane™ persistent memory 200 series module population:

- For MM, standard DDR4 / Intel® Optane™ persistent memory 200 series module capacity recommended ratio is 1 GB: 8 GB.
- For each individual population, rearrangements between channels are allowed as long as the resulting population is consistent with defined memory population rules.
- For each individual population, the same type and capacity of DDR4 DIMM must be used in all slots, as specified by the defined memory population rules.

6.4   Memory RAS Support

Processors within the 3rd Gen Intel® Xeon® Scalable processor family support standard or advanced memory RAS features, depending on processor SKU, defined in Table 15. This table lists the RAS features pertaining to system memory that consists of standard DDR4 DIMMs or a combination of standard DDR4 DIMMs and Intel® Optane™ persistent memory 200 series modules. These features are managed by the processor's IMC.

Table 15. Memory RAS Features

Memory RAS Feature	Description	Standard	Advanced
Partial Cache-Line Sparing (PCLS)	Allows replacing failed single bit within a device using spare capacity available within the processor's integrated memory controller (IMC). Up to 16 failures allowed per memory channel and no more than one failure per cache line. After failure is detected, replacement is performed at a nibble level. Supported with x4 DIMMs only.	√	√
Device Data Correction	Single Device Data Correction (SDDC) via static virtual lockstep Supported with x4 DIMMs only.	√	√
	Adaptive Data Correction – Single Region (ADC-SR) via adaptive virtual lockstep (applicable to x4 DDR4 DIMMs). Cannot be enabled with "Memory Multi-Rank Sparing" or "Write Data CRC Check and Retry."	√	√
	Adaptive Double Data Correction – Multiple Regions (ADDDC-MR, + 1) Supported with x4 DIMMs only.	–	√
DDR4 Command/Address (CMD/ADDR) Parity Check and Retry	DDR4 technology based CMD/ADDR parity check and retry with CMD/ADDR parity error "address" logging and CMD/ADDR retry.	√	√
DDR4 Write Data CRC Check and Retry	Checks for CRC mismatch and sends a signal back to the processor for retry. Cannot be enabled with "ADC-SR" or "ADDDC-MR, +1."	√	√

Memory RAS Feature	Description	Standard	Advanced
Memory Data Scrambling with Command and Address	Scrambles the data with address and command in "write cycle" and unscrambles the data in "read cycle". Addresses reliability by improving signal integrity at the physical layer. Additionally, assists with detection of an address bit error.	√	√
Memory Demand and Patrol Scrubbing	Demand scrubbing is the ability to write corrected data back to the memory once a correctable error is detected on a read transaction. Patrol scrubbing proactively searches the system memory, repairing correctable errors. Prevents accumulation of single-bit errors.	√	√
Memory Mirroring	Full memory mirroring: An intra-IMC method of keeping a duplicate (secondary or mirrored) copy of the contents of memory as a redundant backup for use if the primary memory fails. The mirrored copy of the memory is stored in memory of the same processor socket's IMC. Dynamic (without reboot) failover to the mirrored DIMMs is transparent to the OS and applications.	√	√
	Address range/partial memory mirroring: Provides further intra socket granularity to mirroring of memory. It does this by allowing the firmware or OS to determine a range of memory addresses to be mirrored, leaving the rest of the memory in the socket in non-mirror mode.	–	√
DDR Memory Multi-Rank Memory Sparing	Up to two ranks out of a maximum of eight ranks can be assigned as spare ranks. Cannot be enabled with "ADC-SR", "ADDDC-MR, +1", and "Memory Mirroring".	√	√
Memory SMBus* Hang Recovery	Allows system recovery if the SMBus* fails to respond during runtime thus preventing system crash.	√	√
Memory Disable and Map Out for Fault Resilient Boot (FRB)	Allows memory initialization and booting to OS even when memory fault occurs.	√	√
Post Package Repair (PPR)	PPR offers additional spare capacity within the DDR4 that can be used to replace faulty cell areas detected during system boot time.	√	√
Memory Thermal Throttling	Management controller monitors the memory DIMM temperature and can temporarily slow down the memory access rates to reduce the DIMM temperature if needed.	√	√
MEMHOT Pin Support for Error Reporting	MEMHOT pin can be configured as an output and used to notify if DIMM is operating within the target temperature range. Used to implement "Memory Thermal Throttling".	√	√

Notes: Population Rules and BIOS Setup for Memory RAS
- Memory sparing and memory mirroring options are enabled in BIOS Setup.
- Memory sparing and memory mirroring options are mutually exclusive in this product. Only one operating mode at a time may be selected in BIOS Setup.
- If a RAS mode has been enabled and the memory configuration is not able to support it during boot, the system will fall back to independent channel mode and log and display errors.
- Rank sparing mode is only possible when all channels that are populated with memory have at least two single-rank or double-rank DIMMs installed, or at least one quad-rank DIMM installed, on each populated channel.
- Memory mirroring mode requires that for any channel pair that is populated with memory, the memory population on both channels of the pair must be identically sized.
- The Intel® Optane™ persistent memory 200 series RAS features listed in the following table are integrated into the system memory RAS features.

The following table lists additional memory RAS features specific to the Intel® Optane™ persistent memory 200 series memory. These features are managed by the processor's IMC.

Table 16. Intel® Optane™ Persistent Memory 200 Series RAS Features

Memory RAS Feature	Description
DIMM Error Detection and Correction	Protects against random bit failures across media devices.
DIMM Device Failure Recovery (Single Device Data Correction (SDDC)	Corrects errors resulting from the failure of a single media device.
DIMM Package Sparing (Double Device Data Correction (DDDC)	Achieved by a spare device on the DIMM and erasure decoding.
DIMM Patrol Scrubbing	Proactively searches the DIMM memory, repairing correctable errors. This can prevent correctable errors from becoming uncorrectable due to accumulation of failed bits.
DIMM Address Error Detection	Ensures the correctness of addresses when data is read from media devices.
DIMM Data Poisoning	Mechanism to contain, and possibly recover from, uncorrectable data errors. Depending on the mode used, poisoning has different reset behavior: • • In memory mode, poison is cleared after reset. • • In App Direct, poison is not cleared with reset.
DIMM Viral	Ensures that potentially corrupted data is not committed to persistent memory in App Direct and is supported only in tandem with poison. Viral mode does not apply to memory mode.
DIMM Address Range Scrub (ARS)	Obtains the healthy memory media range before assigning it to a persistent memory region.
DDR-T Command and Address Parity Check and Retry	Host retries a CMD/ADDR transaction if the DIMM controller detects a parity error and initiates an error flow.
DDR-T Read Write Data ECC Check and Retry	Host continuously retries a data transaction as long as the DIMM controller detects an ECC error and initiates an error flow.
Faulty DIMM Isolation	Identifies a specific failing DIMM enabling replacement of only the DIMM that has failed.

The Intel® Server D40AMP family security features include support for Intel® Software Guard Extensions (Intel® SGX), Intel® Total Memory Encryption (Intel® TME), and Intel® Total Memory Encryption – Multi-Tenant (Intel® TME-MT). When any of these security features are enabled, Intel® Optane™ PMem 200 series will be disabled. In addition, some of the memory RAS features will be disabled as indicated in the following table.

Table 17. Compatibility of RAS features and Intel® SGX, Intel® TME, and Intel® TME-MT

Feature/Technology	Intel® SGX	Intel® TME, Intel® TME-MT
Intel® Optane™ persistent memory 200 series	No	No
ADC(SR)/ADDDC(MR)	No	Yes
MCA Recovery – Execution Path	No	Yes
MCA Recovery – Non-execution Path	Yes	Yes
Address Range Mirroring	No	Yes
Dynamic Capacity change: CPU/Memory/IIO, Physical CPU Board Hot Add/Remove, OS CPU/Memory/IIO On-lining (Capacity change), OS CPU off-lining (Capacity change), Intel® UPI link Hot pluggability, and Intel® UPI System Quiescence.	No	Yes
Static/Hard Partitioning, Electronically Isolated (Static/Hard) Partitioning, Dynamic Partitioning (Via Resource/Capacity Addition), Multiple South Bridge (PCH) Presence for supporting system partitioning	No	Yes

7.   System Storage

This chapter provides an overview of the available storage options for the Intel® Server D40AMP family.

7.1   M.2 SSD Storage Support

All modules in the Intel® Server D40AMP family include support for up to two M.2 storage devices via riser assemblies as shown in the following figure. The M.2 connectors are labeled "M.2_x4_PCIE/SATA" on risers 1 and 2. Each M.2 connector supports a PCIe* NVMe* or SATA drive that conforms to a 2280 (80 mm) or 22110 (110 mm) form factor.
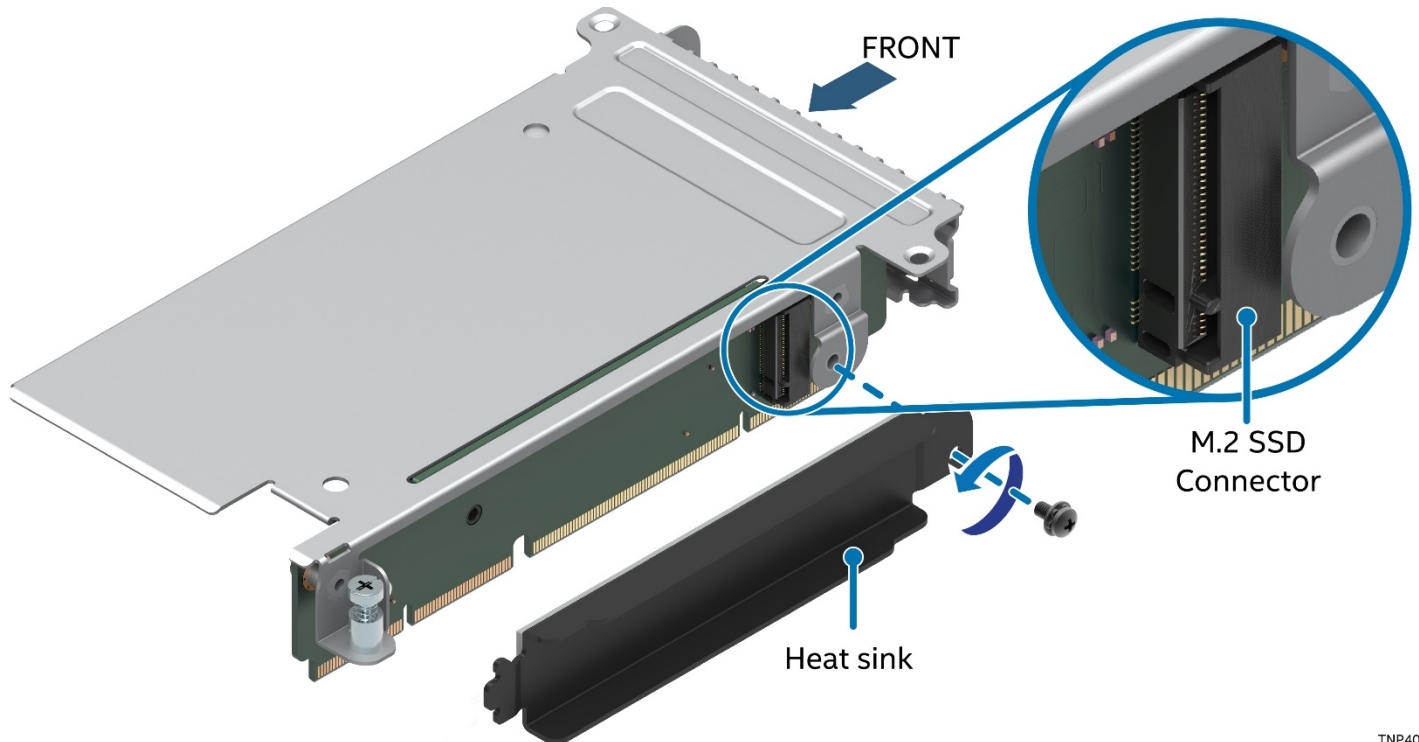
Figure 28. M.2 Connector Location on Riser Card

The M.2 connectors on both risers provide four PCIe* lanes routed from the chipset embedded controller. Both risers include a heat sink for M.2 SSDs that must be installed whether an M.2 SSD is present or not.

The compute modules in the Intel® Server D40AMP family support Intel® VROC (VMD NVMe* RAID) for PCIe* NVMe* devices installed in the M.2 connectors. Refer to Section 7.5 for more information on Intel® VROC and Intel® VMD.

The M.2 connectors also support SATA drives with speeds of up to 6 Gb/sec. The M.2 connectors on both risers are routed to the chipset embedded sSATA controller. Therefore, the M.2 storage devices support Intel® VROC SATA RAID. Refer to Section 7.6 for more information on Intel® VROC SATA RAID.

Note: The Intel® Server D40AMP family only supports SATA devices on the M.2 connectors. Check Section 8.

Table 21 lists the supported features by the embedded sSATA controller.

7.2   U.2 SSD Storage Support – VP3U2HAC21W0 Chassis Only

Systems configured with a VP3U2HAC21W0 chassis, support up to 24 hot-swappable 2.5" U.2 PCIe* NVMe* SSDs trough two common backplanes. Each compute module is connected to a group of 6 dedicated hot-swap drive bays.

Figure 29. Intel Server Chassis VP3U2HAC21W0

The drive bays are organized in two banks of 12, with the bays for modules 1 and 2 at the front of the chassis, and the bays for modules 3 and 4 behind them. The hot-swap drive bays for modules 3 and 4 are accessible by sliding the chassis out of the rack, removing the front top cover, and lifting the hot-swap drive bay assembly as shown in the following figures.
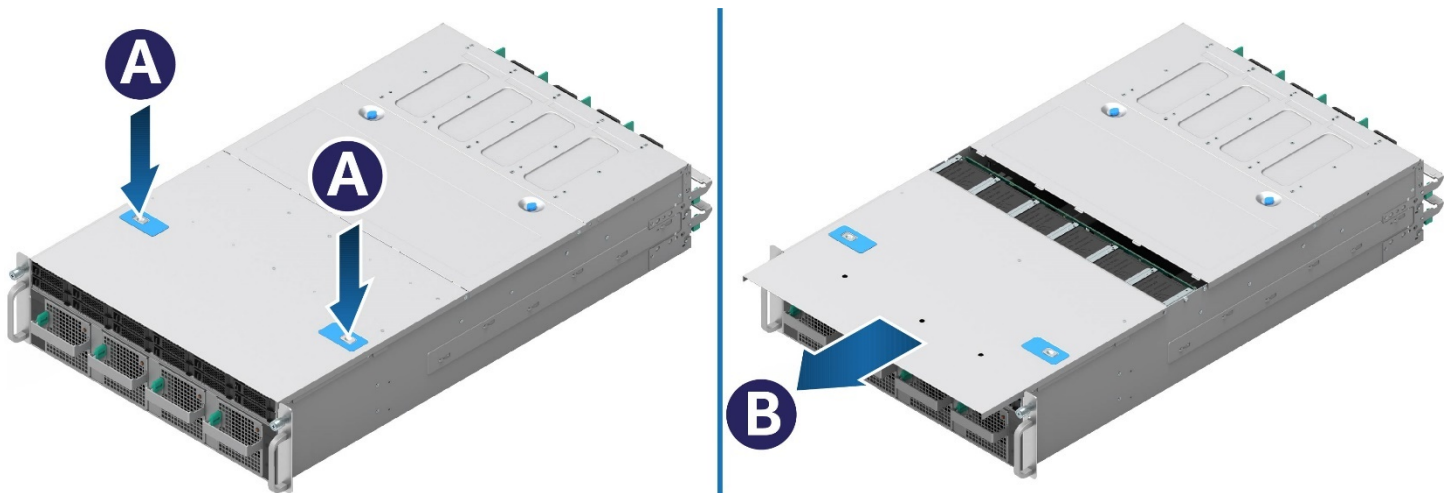
Ref #: AMP20171

Figure 30. Removing the Front Top Cover
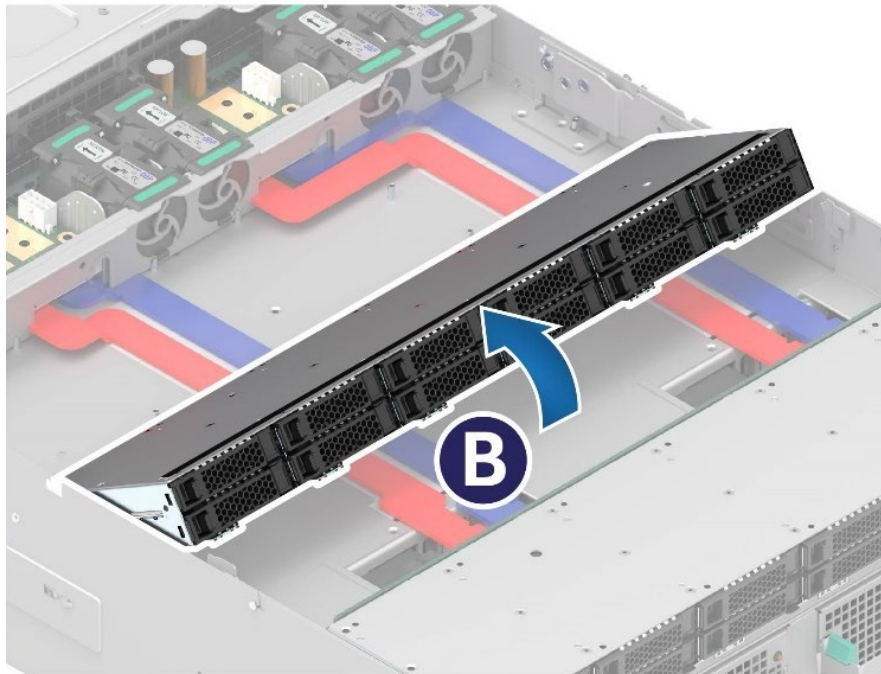
Ref #: AMP20220

Figure 31. Accessing U.2 Hot-Swap Drive Bays for Modules 3 and 4
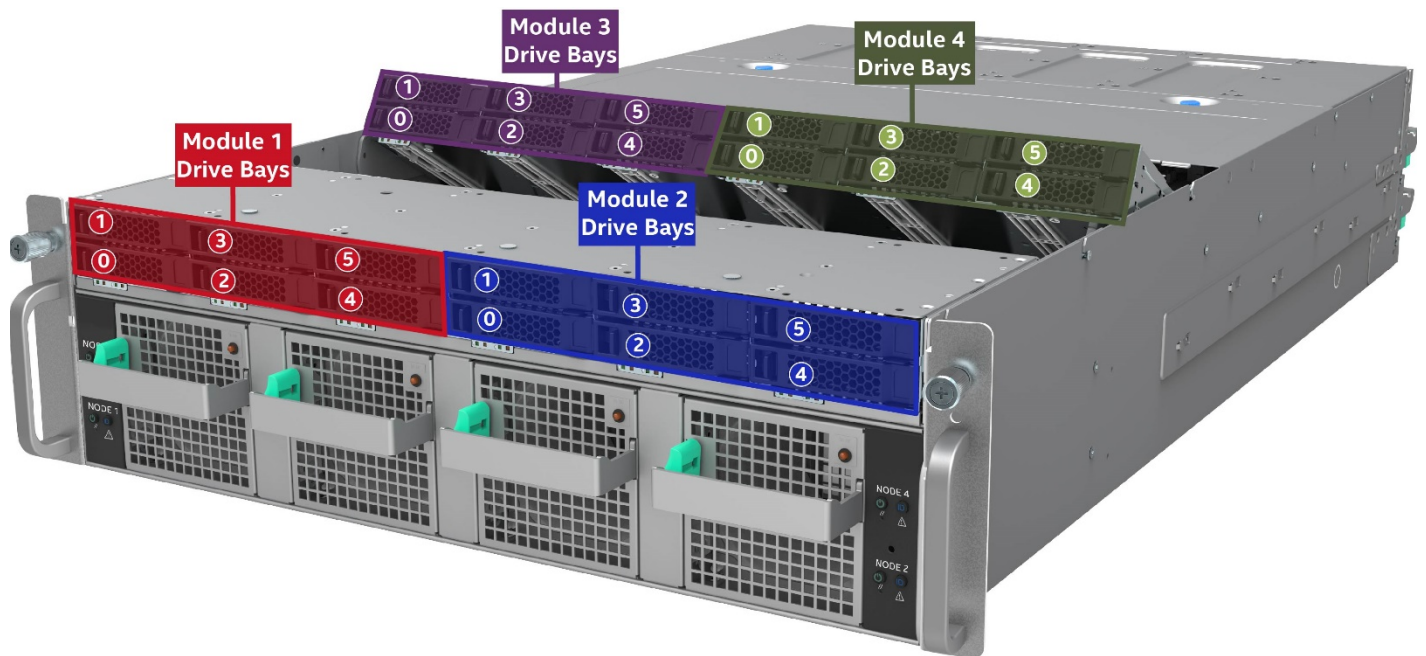
Ref #: AMP20104

Figure 32. U.2 Hot-Swap Drive Bay Identification

Each drive slot pair includes LED indicators below them for drive activity and drive status. There are two LEDs for each drive bay: Amber Status LED and Green Activity LED. The LEDs are identified with an arrow indicating the drive bay they are connected to. The following tables provide the LED states.

Top Bay **Bottom Bay**
LEDs **LEDs**

Ref #: AMP40251
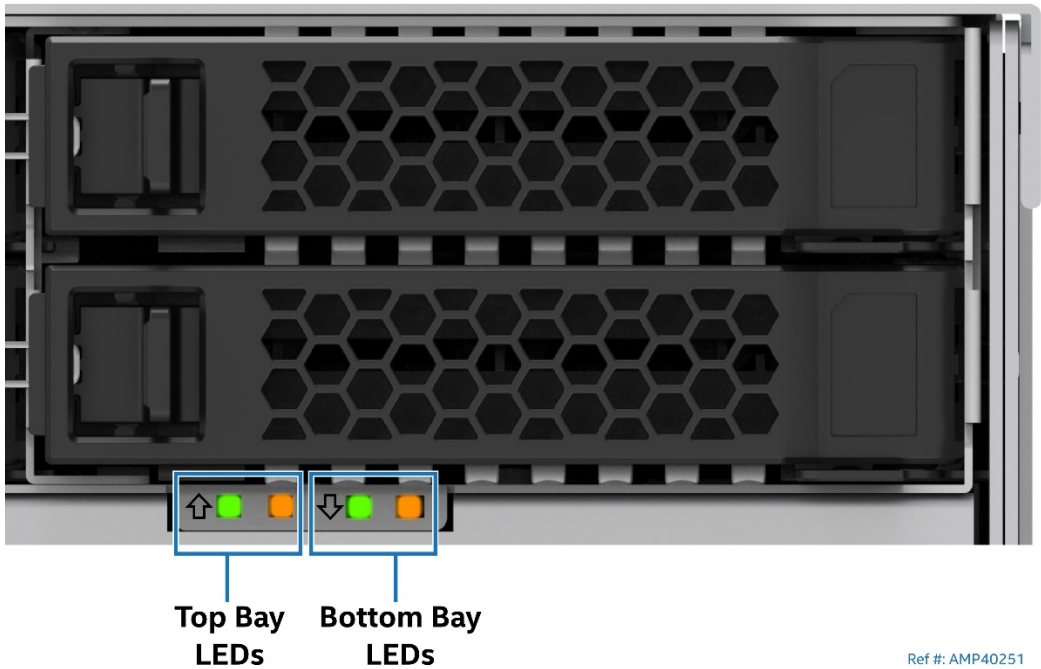
Figure 33. Drive Bay LED Identification

Table 18. Drive Activity LED states

	LED State	Condition
Green	Stays on	Drive present, no activity
	4Hz Blinking	LED blinks off when processing a command
	Off	Drive not present
	4Hz Blinking	Locate drive (identify)

Table 19. Drive Status LED States

	LED State	Drive Status
Amber	Off	No fault, OK
	4 Hz blinking	Locate (identify)
	Stays on	Fault/fail
	1 Hz blinking	Rebuild

Note: The drive activity LED is driven by signals coming from the drive itself. Drive vendors may choose to operate the activity LED different from what is described in the table above. If the activity LED on a given drive type behaves differently than what is described, customers should reference the drive vendor specifications for the specific drive model to determine the expected drive activity LED operation.

7.3 NVMe* Enterprise Data Center SSD Form Factor (EDSFF) Storage Support – VP3E1HAC21W0 Chassis Only

Systems configured with a VP3E1HAC21W0 chassis support up to 32 hot-swappable E1.L (full-length) PCIe* EDSFF NVMe* SSDs as shown in the following figure. Each installed compute module is connected to a group of 8 hot-swap drives through a common mid-plane.

Figure 34. Intel® Server Chassis VP3E1HAC21W0

The drive bays are organized in four groups of 8, with the bays for modules 1 and 3 to the left of the chassis, and the bays for modules 2 and 4 to the right. The following figure identifies the SSD groups as seen from the front of the chassis.
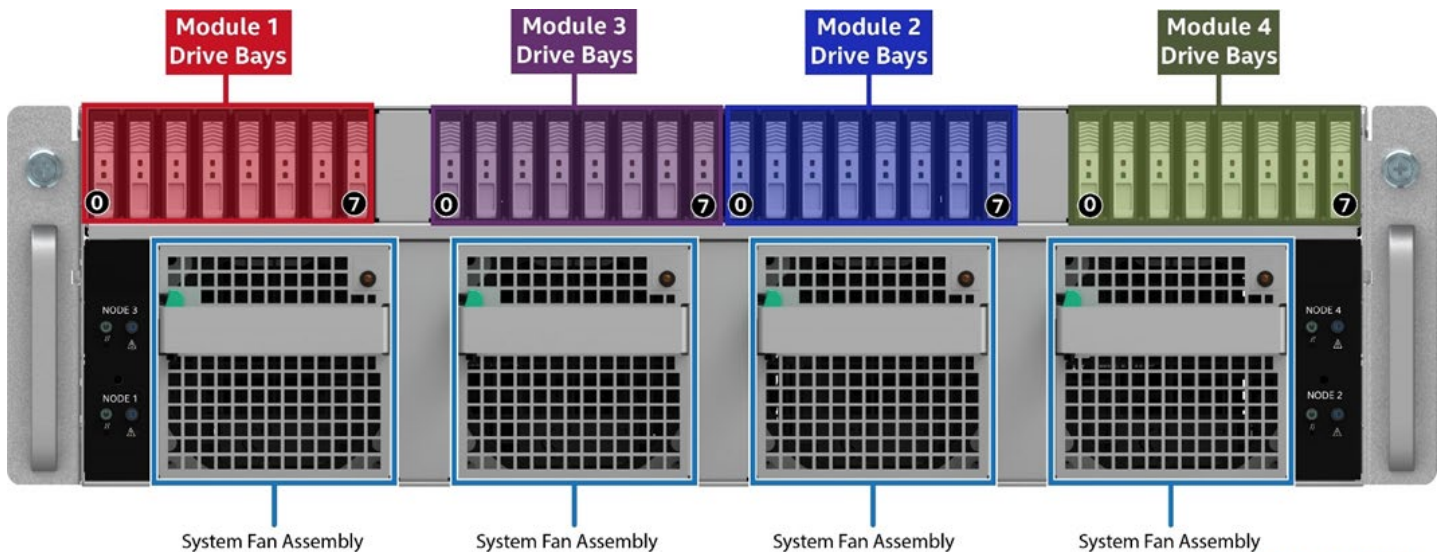
Figure 35. EDSFF NVMe* Drive Bay Identification

7.4 Intel® Volume Management Device 2.0 (Intel® VMD 2.0) for NVMe*

Intel® Volume Management Device (Intel® VMD) is hardware logic inside the processor root complex to help manage PCIe* NVMe* SSDs. It provides robust hot plug support and status LED management. This allows servicing of storage system NVMe* SSD media without fear of system crashes or hangs when ejecting or inserting NVMe* SSD devices on the PCIe* bus.
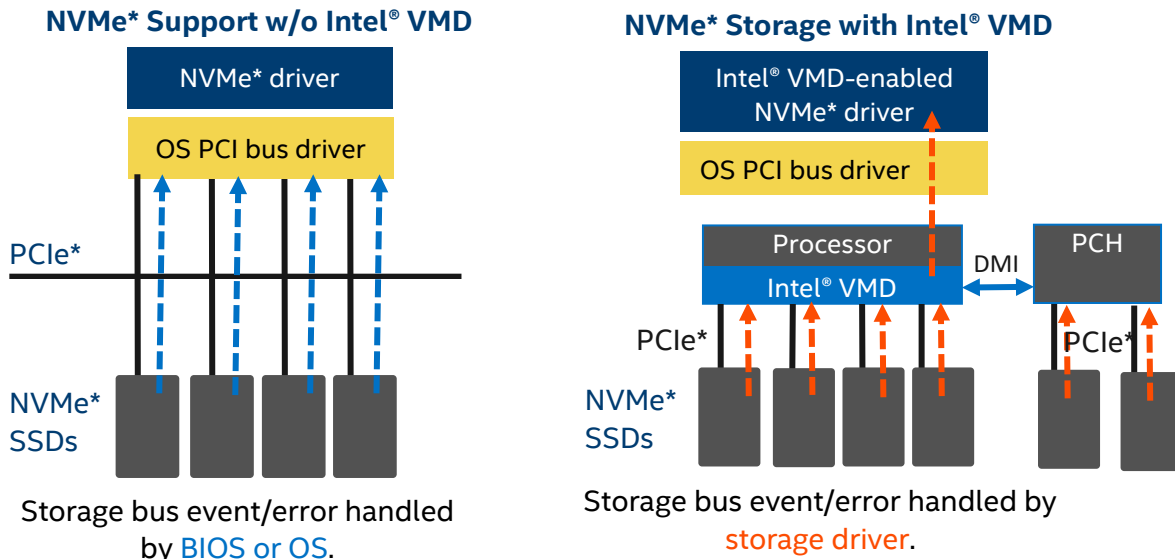
Figure 36. NVMe* Storage Bus Event/error Handling

Intel® VMD handles the physical management of NVMe* storage devices as a stand-alone function but can be enhanced when Intel® VROC support options are enabled to implement RAID based storage systems. See Section 7.5 for more information.

7.4.1 Intel® VMD 2.0 Features

The modules within the Intel® Server D40AMP family support the following Intel® VMD features and capabilities:

- The hardware to enable Intel® VMD is integrated inside the processor's PCIe* root complex
- Entire PCIe* trees are mapped into their own address spaces (domains).
- Each domain manages x16 PCIe* lanes.
- Can be enabled/disabled in BIOS Setup at x4 lane granularity.
- Driver sets up/manages the domain (enumerate, event/error handling).
- May load an additional child device driver that is Intel® VMD aware.
- Hot plug support – hot insert array of PCIe* NVMe* SSDs.
- Support for PCIe* NVMe* SSDs only (no network interface controllers (NICs), graphics cards, and so on)
- Support for MMIO only (no port-mapped I/O).
- Does not support NTB, Quick Data Tech, Intel® Omni-Path Architecture, or SR-IOV.
- Correctable errors do not bring down the system.
- Intel® VMD only manages devices on PCIe* lanes routed from the processor directly or via supported PCIe* switch or routed from the PCH chipset
- When Intel® VMD is enabled, the BIOS does not enumerate devices that are behind Intel® VMD. The Intel® VMD-enabled driver is responsible for enumerating these devices and exposing them to the host.

7.4.2   Enabling Intel® VMD support

By default, Intel® VMD support is disabled on all processor PCIe* root ports in BIOS. To enable Intel® VMD support on the appropriate CPU PCIe* root port navigate to **Advanced > PCI Configuration > Volume Management Device** in the BIOS Setup menu.

Table 3 in Section 2.4.1 provides the PCIe* root port mapping for all onboard PCIe* devices and riser card slots.

7.5   Intel® Virtual RAID on Chip (Intel® VROC) for NVMe*

The Intel® Compute Module D40AMP supports the following Intel® VROC features:

- Bootable RAID
- Self encrypting drive (SED) key management in UEFI
- Integrated caching with Intel Optane* SSDs
- RAID5 power loss protection for degraded volumes (double fault protection)
- Isolated storage devices from operating system for error handling
- NVMe* SSD hot plug and surprise removal on CPU PCIe* lanes
- LED management for PCIe* attached storage
- Hot spare and auto-rebuild
- Bad block management
- Email notifications for RAID events
- Configurable strip sizes (4k, 8k, 16k, 32k, 64k, 128k)
- RAID/storage management using representational state transfer (RESTful) application programming interfaces (APIs).
- Graphical user interface (GUI) for Windows*
- 4Kn native NVMe* SSD support

Intel® VROC (VMD NVMe* RAID) offers several options for RAID to meet the needs of the end user. Supported RAID levels include:

- **RAID 0** – Uses striping to provide high data throughput, especially for large files in an environment that does not require fault tolerance.
- **RAID 1** – Uses mirroring so that data written to one disk drive is simultaneously written to another disk drive. This is good for small databases or other applications that require small capacity but complete data redundancy.
- **RAID 5** – Uses disk striping and parity data across all drives (distributed parity) to provide high data throughput, especially for small random access. A minimum of three drives required.
- **RAID 10** – A combination of RAID 0 and RAID 1 on four drives, consists of striped data across mirrored drives. It provides high data throughput and complete data redundancy but uses a larger number of drives.

Enabling Intel® VROC support requires the installation of an optional upgrade key in the Intel® D40AMP modules as shown in Figure 37. Table 20 identifies the supported RAID features by the optional upgrade keys.
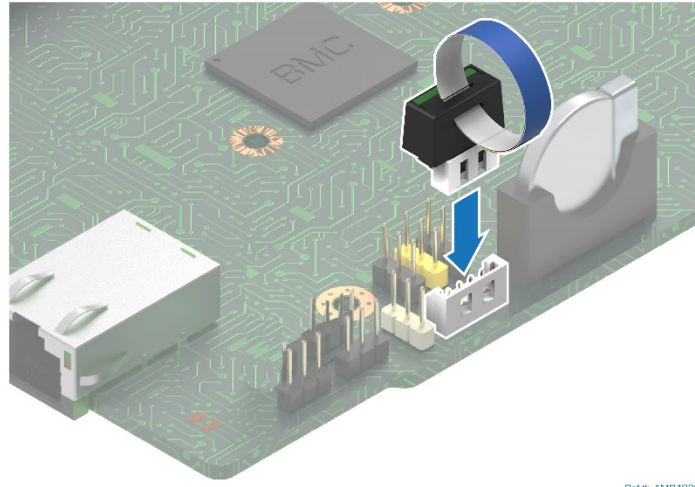
Ref #: AMP40221

Figure 37. Intel® VROC upgrade key

Table 20. Optional VROC Upgrade Keys – Supported NVMe* Features

Features	Standard Intel® VROC 7.5 Key (iPC – VROCSTANMOD)	Premium Intel® VROC 7.5 Key (iPC – VROCPREMMOD)
Processor/chipset-attached NVMe* SSD – high performance	√	√
Boot on RAID volume	√	√
Third party vendor SSD support	√	√
RAID 0/1	√	√
RAID 10	√	√
RAID 5	–	√
RAID write hole closed	–	√
Hot plug/ surprise removal	√	√
Enclosure LED management	√	√

7.6 Intel® Virtual RAID on Chip (Intel® VROC) for SATA

Intel® VROC (SATA RAID) provides an enterprise RAID solution for SATA devices connected to the sSATA controller on the Intel® Platform Control Hub (PCH).

By default, onboard RAID options are disabled in BIOS Setup. To enable onboard RAID support, access the BIOS Setup utility by pressing **<F2>** key during POST. Navigate to the onboard RAID configuration menu: **Advanced** > **Mass Storage Controller Configuration > sSATA Controller.**

From the options available in the menu, select the RAID mode to enable the RAID support.

Note: The Intel® Compute Module D40AMP only supports SATA III devices on the M.2 connectors in the riser assemblies.

Supported SATA RAID levels on the Intel® Compute Module D40AMP include RAID 0 and RAID 1.

- **RAID 0** – Uses striping to provide high data throughput, especially for large files in an environment that does not require fault tolerance.
- **RAID 1** – Uses mirroring so that data written to one disk drive is simultaneously written to another disk drive. This is good for small databases or other applications that require small capacity but complete data redundancy.

Intel® VROC 7.5 functionality requires the following:

- The embedded RAID option must be enabled in BIOS Setup.
- Intel® VROC 7.5 option must be selected in BIOS Setup.
- Intel® VROC 7.5 drivers must be loaded for the installed operating system.
- At least two SATA drives needed to support RAID 0 or RAID 1.
- NVMe* SSDs and SATA drives must not be mixed within a single RAID volume.

7.7   Onboard SATA Support

The sSATA controller can be enabled, disabled, or configured through the BIOS Setup utility under the **Mass Storage Controller Configuration** menu screen. The following table lists the supported features by the embedded sSATA controller.

Table 21. sSATA controller feature support

Feature	Description	AHCI Mode	RAID Mode Intel® VROC (SATA RAID)
Native Command Queuing (NCQ)	Allows the device to reorder commands for more efficient data transfers	Supported	Supported
Auto Activate for DMA	Improves efficiency of data transfer by skipping DMA Activate command after DMA Setup command	Supported	Supported
Asynchronous Signal Recovery	Provides a recovery from a loss of signal or establishing communication after hot plug	Supported	Supported
6 Gb/s Transfer Rate	Capable of data transfers up to 6 Gb/s	Supported	Supported
ATAPI Asynchronous Notification	A mechanism for a device to send a notification to the host that the device requires attention	Supported	Supported
Host & Link Initiated Power Management	Capability for the host controller or device to request Partial and Slumber interface power states	Supported	Supported
Staggered Spin-Up	Enables the host to spin up hard drives sequentially to prevent power load problems on boot	Supported	Supported
Command Completion Coalescing	Reduces interrupt and completion overhead by allowing a specified number of commands to complete and then generating an interrupt to process the commands	Supported	N/A

8. Chassis and Module Control Panel and I/O

This chapter provides information on the control panel and I/O available on the Intel® Compute Module D40AMP and at the front of the Intel® Server Chassis VP3000 family.

8.1 Compute Module Control Panel Features

The Intel® Compute Module D40AMP includes a control panel with push button controls and LED indicators. This section provides a description for each control panel feature.
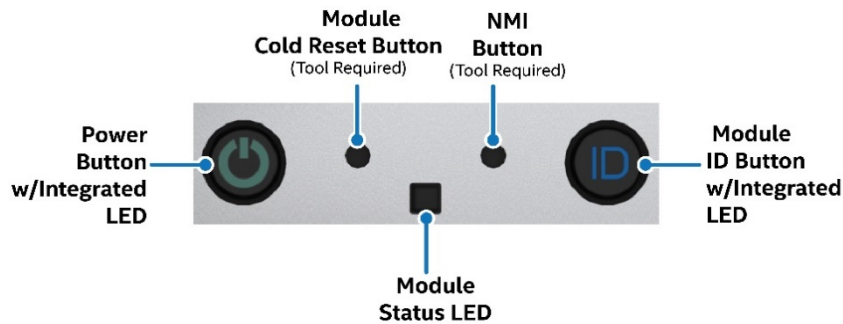
Figure 38. Compute Module Control Panel Features

- **Power button with integrated LED** – Toggles the module power on and off. This button also functions as a sleep button if enabled by an ACPI compliant operating system. Pressing this button sends a signal to the Integrated BMC that either powers on or powers off the module. The integrated LED is a single color (green) and supports different indicator states as defined in the following table.

Note: After AC power is connected, several subsystems are initialized and low-level FRU discovery is performed. This process can take up to 90 seconds. When this process is completed, the ID LED will turn solid on, indicating that the system is ready to be powered on.

Table 22. Power / Sleep LED Functional States

Power Mode	LED	Module State	Description
Non-ACPI	Off	Power-off	Module power is off, and the BIOS has not initialized the chipset.
	On	Power-on	Module power is on
ACPI	Off	S5	Mechanical is off and the operating system has not saved any context to the hard disk.
	On	S0	Module and the operating system are up and running.

- **Module ID button w/ integrated LED** – Toggles the integrated blue ID LED on and off. The module ID LED is used to identify an Intel® Compute Module D40AMP within a chassis for maintenance when installed in a rack of similar server systems. The module ID LED can also be toggled on and off remotely using the IPMI "Chassis Identify" command that causes the LED to blink for 15 seconds.
- **NMI Button** – When the NMI button is pressed, it puts the Intel® Compute Module D40AMP in a halt state and issues 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. To prevent an inadvertent module halt, the actual NMI button is located behind the control panel faceplate where it is only accessible with the use of a small-tipped tool like a pin or paper clip.

- **Module cold reset button** – When pressed, this button reboots and re-initializes the Intel® Compute Module D40AMP. Unlike the power button, the reset button does not disconnect the power to the module. It just starts the module's Power-On Self-Test (POST) sequence over again.
- **Module status LED** – The module status LED is a bi-color (green/amber) indicator that shows the current health of the module. The module status LED states are driven by the integrated platform management subsystem. Table 23 provides a description of each supported LED state.

Table 23. Intel® Compute Module D40AMP Status LED State Definitions

LED State	Module State	BIOS Status Description
Off	No AC Power to system	- System power is not present. - Module is in EuP Lot6 off mode. - Module is in S5 soft-off state.
Solid green	Module is operating normally.	- Module is running (in S0 State) and its status is healthy. The module is not exhibiting any errors. Source power is present BMC has booted and manageability functionality is up and running. - After a BMC reset, and in conjunction with the module ID LED solid on, the BMC is booting Linux*. Control has been passed from BMC uBoot to BMC Linux*. It is in this state for roughly 10–20 seconds.
Blinking green	Module is operating in a degraded state although still functioning, or module is operating in a redundant state but with an impending failure warning.	- Redundancy loss such as power-supply or fan. Applies only if the associated platform subsystem has redundancy capabilities. - Fan warning or failure when the number of fully operational fans is more than the minimum number needed to cool the system. - Non-critical threshold crossed – Temperature, 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 installed memory (more than 1 DIMM installed). - Correctable Errors over a threshold and migrating to a spare DIMM (memory sparing). This indicates that the module no longer has spared DIMMs (a redundancy lost condition). - In mirrored configuration, when memory mirroring takes place and the module loses memory redundancy. - Battery failure. - BMC executing in uBoot. (Indicated by module ID LED blinking at 3 Hz while Status blinking at 1 Hz). Module in degraded state (no manageability). BMC uBoot is running but has not transferred control to BMC Linux*. The module will be in this state 6–8 seconds after BMC reset while it pulls the Linux* image into flash. - BMC Watchdog has reset the BMC. - Power Unit sensor offset for configuration error is asserted. - SSD Hot Swap Controller (HSC) is off-line or degraded.
Blinking amber and green alternatively	Module is initializing after AC power is applied	- PFR in the process of updating/authenticating/recovering when AC power is connected, module firmware being updated. - Module not ready to take power button event/signal.
Blinking amber	Module is operating in a degraded state with an impending failure warning, although still functioning. Module is likely to fail.	- Critical threshold crossed – Voltage, temperature, 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. - Storage 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. - Invalid firmware image detected during boot up or firmware update.

LED State	Module State	BIOS Status Description

Solid amber	Critical/non-recoverable – module is halted. Fatal alarm – module has failed or shut down.	• CPU CATERR signal asserted.
		• MSID mismatch detected (CATERR also asserts for this case).
		• CPU 0 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.
		• Processor ERR2 signal asserted.
		• BMC/Video memory test failed (module ID LED shows blue/solid-on for this condition).
		• Both uBoot BMC firmware images are bad (module ID LED shows blue/solid-on for this condition).
		• 240 VA fault.
		• Fatal Error in processor initialization:
		   o Processor family not identical
		   o Processor model not identical
		   o Processor core/thread counts not identical
		   o Processor cache size not identical
		   o Unable to synchronize processor frequency
		   o Unable to synchronize UPI link frequency
		• BMC fail authentication with non-recoverable condition, system hang at T-1; boot PCH only, system hang; PIT failed, system lockdown

8.2 Compute Module External I/O

Several connectors are accessible from the outside of the compute module. The following sections describe each of the available connectors.

8.2.1 Networking

The Intel® Compute Module D40AMP includes two RJ45 connectors:

- 10 Gb Ethernet port (10GBASE-T)
- 1 Gb Ethernet port (1000BASE-T) dedicated to server management

The following figures show the location of the ports on the compute module.

Ref #: AMP30092

10 Gb Ethernet Port   Server Mgmt Port
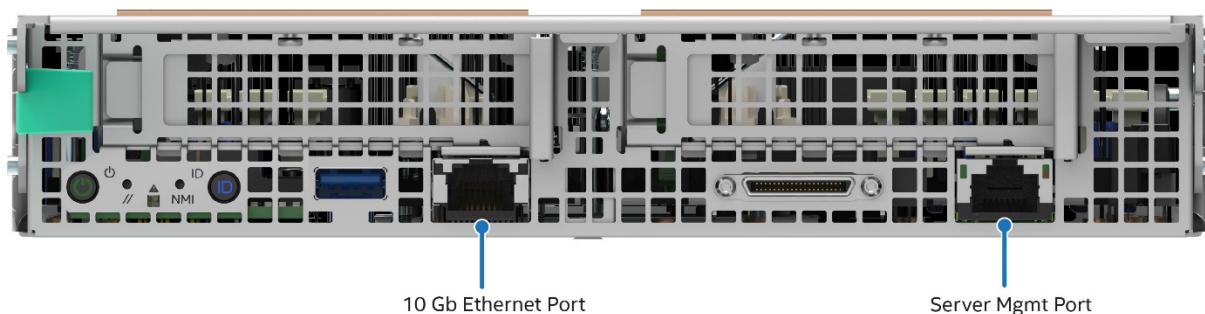
Figure 39. RJ45 Connectors Identification

8.2.1.1   10GbE Network Port

Network connectivity is provided by the onboard Intel® Ethernet Controller X550 supporting 1/2.5/5/10 Gb transfer rates. The Intel® Ethernet Controller X550 is a single, compact, low-power component that offers a fully-integrated Gigabit Ethernet Media Access Control (MAC) and Physical Layer (PHY) port. The Intel® Ethernet Controller X550 is connected via the PCIe* interface to the Intel® C621A PCH chipset and provides a single-port implementation.

See the respective product datasheet for a complete list of supported features.

The RJ45 network interface connector includes two LEDs. The LED at the left of the connector is the link/activity LED and indicates a network connection when on and transmit/receive activity when blinking. The LED at the right of the connector indicates link speed as defined in Table 24.

Figure 40. 10Gb RJ45 Connector LEDs

Table 24. 10Gb RJ45 Connector LED Definition

LED	LED State	NIC State
Link/activity (left)	Off	LAN link not established
	Solid green	LAN link is established
	Blinking green	Transmit/receive activity
Transmit/receive (right)	Solid amber	1 Gb data rate
	Solid green	10 Gb data rate

8.2.1.2   Server Management Port

Each compute module within a system chassis includes a 1 GbE RJ45 port for server management. See Chapter 11 for additional information about server management support.

The server management port includes two LEDs. The behavior of the LEDs is defined in Table 25.

Figure 41. 1Gb RJ45 Connector LEDs

Table 25. 1Gb RJ45 Connector LED Definition

Left LED	Right LED	Network Status
Off	Off	No link
Solid on	Solid on	10 Mbps link
Blinking	Blinking	10 Mbps activity
Solid on	Off	100 Mbps link
Blinking	Off	100 Mbps activity
Off	Solid on	1 Gpbs link
Off	Blinking	1 Gbps activity

8.2.1.3   MAC Address Definition

The modules in the Intel® Server D40AMP family have the following MAC addresses assigned at the factory:

- 10Gb network interface (base MAC address)
- 1Gb network interface (base MAC address + 1)

8.2.2   I/O Breakout Cable

Each Intel® D40AMP Module contains a 40-pin connector supporting an I/O breakout cable as shown in Figure 42. Each system configuration includes one I/O breakout cable providing a single module with additional support for one serial port, one VGA port, and two USB 3.0 ports as needed.
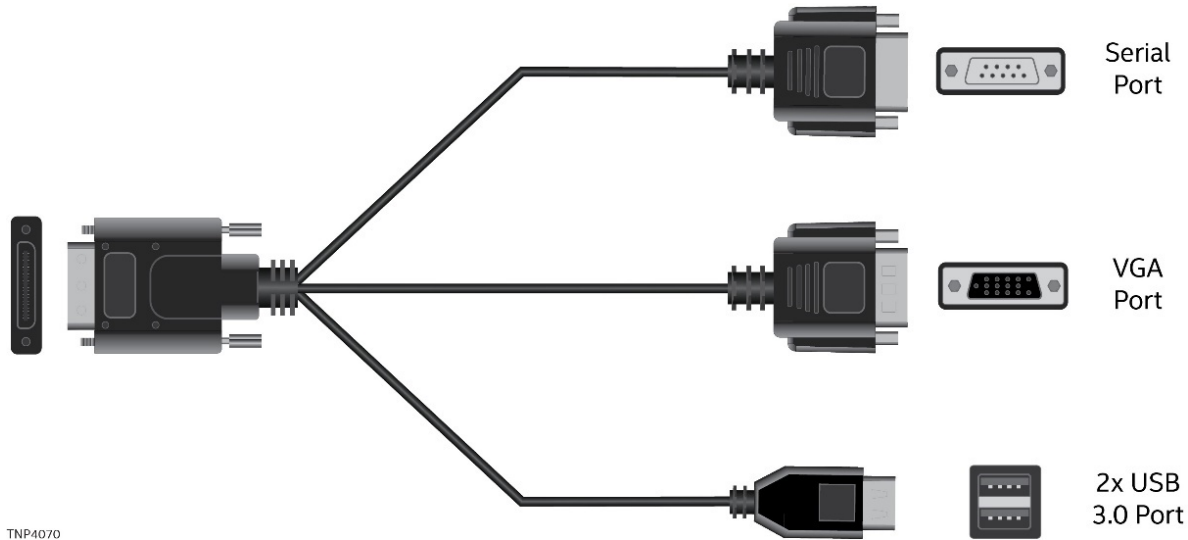
Figure 42. I/O Breakout Cable Port Identification

8.2.3   USB Support

The compute modules provide one external USB 3.0 port. There are two other USB 3.0 ports available through the dedicated I/O breakout cable (see Section 8.2.2). The following figures show the location of the USB port.
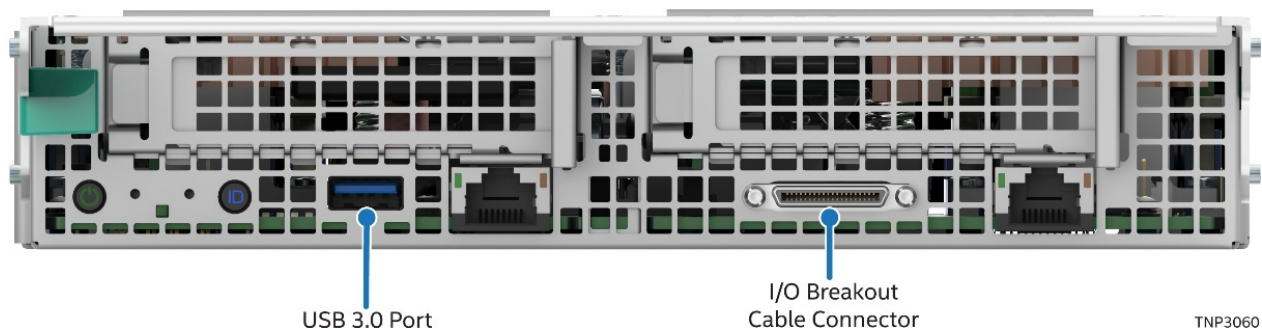
Figure 43. USB Port and I/O Breakout Cable Connector Location on Compute Module

8.3   Chassis Front Control Panel Features Overview

The Intel® Server Chassis VP3000 family includes two control panels located at the front side of the chassis enabling basic interaction with the installed compute modules. This section provides a description for each front control panel feature.

The chassis front control panels are connected to each of the compute modules, in the same layout they are installed. The following figure identifies the features of the control panel for modules 1 and 3.
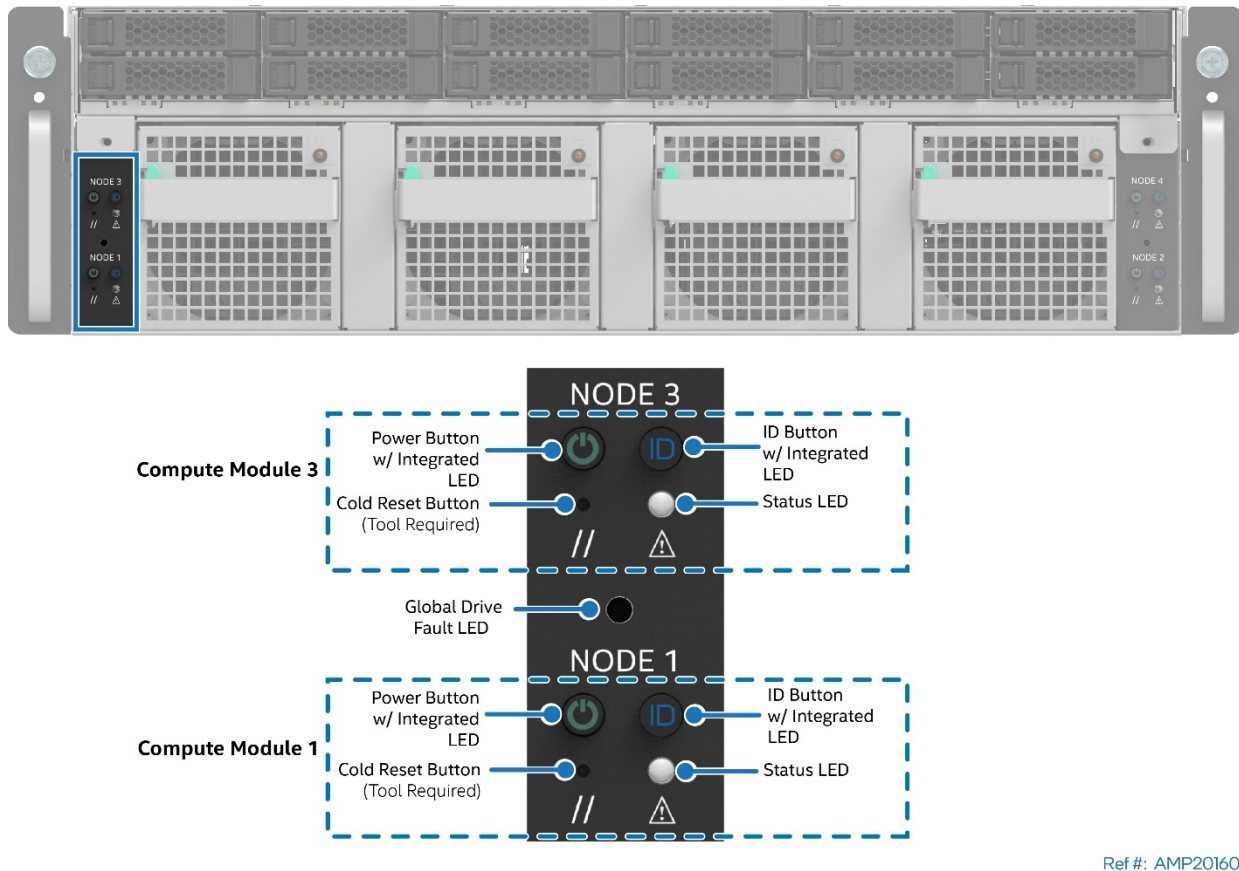
Figure 44. Chassis Front Control Panel Features

The push button controls and LED indicators in the chassis front control panel are assigned to a corresponding compute module bay. If a compute module is not installed in the corresponding module bay (see Figure 13), accidental activation of these controls will have no impact on the overall system functionality.

The features and functions of the front control panel in the chassis, are the same as those of the compute module control panel, with the exception of the NMI function and the Global Drive Fault LED. The NMI function is only available from the specific compute module control panel. Refer to Section 8.1 for details about the functionality of the available controls.

8.3.1   Global Drive Fault LED

The left control panel at the front of the chassis includes a Global Fault LED as shown in Figure 44. In the case of a failure of any installed SSD this LED turns on with an amber light, providing a visual alert about a drive failure. If no failure is present in any of the installed SSDs, this LED remains off.

9.   Thermal Management

The Intel® Server D40AMP family supports air-cooling for all installed compute modules and the chassis. This chapter provides an overview of the thermal management features and capabilities of the system.

The fully integrated system is designed to operate at external ambient temperatures between 10–35 °C. Working with integrated platform management, several features are designed to move air from the front to the back of the system and over critical components to prevent them from overheating, allowing the system to operate optimally.

Ref #: AMP40245
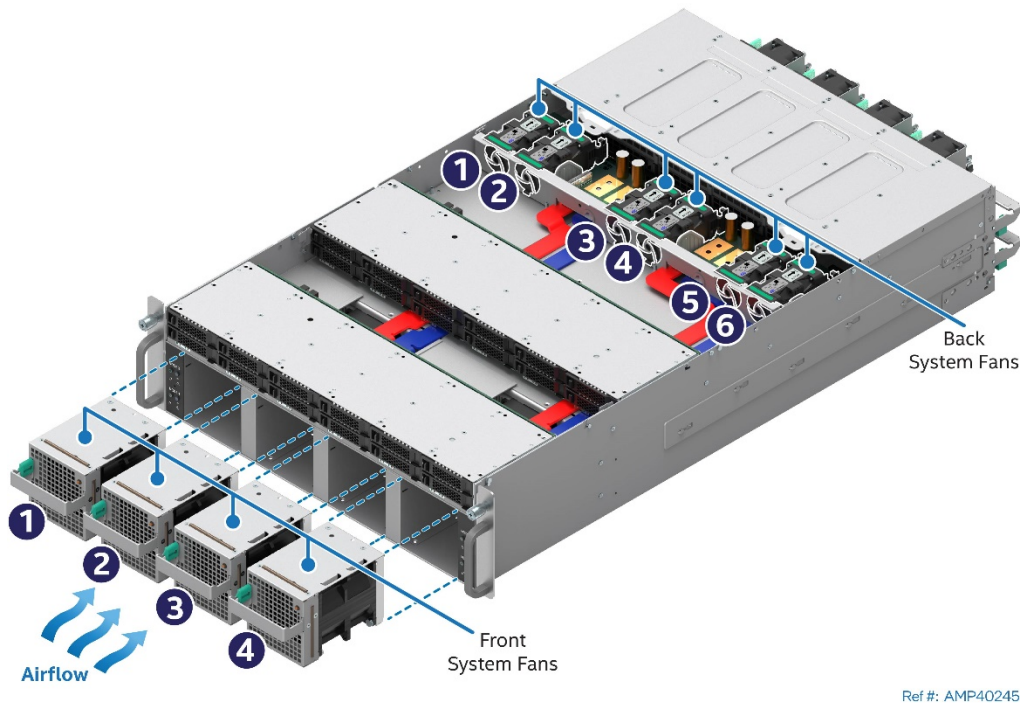
Figure 45. Air-Cooled System Airflow and Fan Identification

The following table shows airflow data for the Intel® Server D40AMP family and is provided for reference purposes only. The data was derived from actual wind tunnel test methods and measurements using fully configured (worst case) system configurations. In addition, the cubic feet per minute (CFM) data obtained using server management utilities that use platform sensor data may vary slightly from the data listed in the tables. Different system configurations may produce slightly different data results.

Note: For system BTU data, see the Intel® Server D40AMP Power Budget and Thermal Configuration Tool.

Table 26. System Volumetric Airflow, Intel® Server D40AMP Family

System Fans Speed	PSU Fan Speed	Airflow (CFM) – Systems Configured with Chassis VP3U2HAC21W0	Airflow (CFM) – Systems Configured with Chassis VP3E1HAC21W0
100%		424	411
50%	Auto	231	221
30%		151	146

The installation and functionality of several system components is used to maintain system thermals. These components are listed below:

- Four managed 80-mm dual rotor hot-swap system fans located at the front of the chassis
- Six managed 40-mm dual rotor hot-swap system fans located behind the storage bays
- Fans integrated into each installed power supply module
- Server board component heat sinks
- Drive bays. Drive bays must be populated with either an SSD or supplied drive blank.
- Installed DIMMs and DIMM blanks
- Processor heat sinks
- Air duct on installed compute modules
- Compute Module bays. Compute module bays must be populated with a blank when a compute module is not installed.

In addition, it is necessary to have all blue DIMM slots populated with either DIMMs or DIMM blanks. Pre-installed DIMM blanks should only be removed when installing a memory module in its place.

9.1 Thermal Operation and Configuration Requirements

The system is designed to support long term reliability targets when operated at an external ambient temperature of up to 35 °C (ASHRAE A2).

Specific configuration requirements and limitations are documented in the system configuration table for thermal compatibility in Appendix E or in the Intel® Server D40AMP Power Budget and Thermal Configuration Tool. The tool is available as a download at https://downloadcenter.intel.com/

9.2 Thermal Management Overview

To maintain the necessary airflow within the system, the previously listed components and top cover need to be properly installed. For optimal system performance, the external ambient temperature should remain below 35 °C and all system fans should be operational. System fan rotor redundancy allows server to operate in case of single fan failure with limited performance for some components in the system. See Appendix E for performance in fan failed mode.

If a single fan rotor failure occurs (within a system fan or a power supply fan), integrated platform management does the following:

- Changes the state of the system status LED to blinking green,
- Reports an error to the system event log, and
- Automatically adjusts fan speeds of operational fans as needed to maintain system temperatures below maximum thermal limits.

Fan redundancy is lost if more than one fan rotor, in the same fan or different fans, are in a failed state.

Note: All system fans are controlled independently of each other. The fan control system may adjust fan speeds for different fans based on increasing/decreasing temperatures in different thermal zones within the chassis.

If system temperatures continue to increase with the system fans operating at their maximum speed, platform management may begin to throttle bandwidth of either the memory subsystems, the processors, or both to keep components from overheating and keep the system operational. Throttling of these subsystems continues until system temperatures are reduced below preprogrammed limits.

If system thermals increase to a point beyond the maximum thermal limits, the system shuts down, the system status LED changes to solid amber, and the event is logged to the system event log.

If power supply thermals increase to a point beyond their maximum thermal limits or if a power supply fan should fail, the power supply shuts down.

For proper system thermal management, sensor data records (SDRs) for any given system configuration must be loaded by the system integrator as part of the initial system integration process. SDRs are loaded using the FRUSDR utility that is part of the system update package (SUP) or System Firmware Update Package (SFUP) utility that can be downloaded from http://downloadcenter.intel.com.

9.3   System Fans

The system includes the following fans:

- Four managed 80-mm dual rotor hot-swap system fans located at the front of the chassis
- Six managed 40-mm dual rotor hot-swap system fans located behind the storage bays
- Fans integrated into each installed power supply module

The system fans and power supply module fans provide the primary airflow for the system.

The system is designed for fan redundancy when configured with four power supply modules. That is, all system fan rotors are operational and ambient air remains at or below ASHRAE class 2 limits. Should a single system fan rotor fail, platform management will adjust airflow of the remaining system fans and manage other platform features to maintain system thermals. Fan redundancy is lost if more than one fan rotor, in the same fan or different fans, are in a failed state.

The 80-mm system fans are mounted inside a fan cage assembly that can be removed from the front of the system chassis. The fan cage assembly includes a fan fail LED visible from the front of the system chassis. The 40-mm system fans located behind the storage bays are mounted directly on the main power distribution board. A fan fail LED is located to the right of each fan connector in the main power distribution board. Each system fan:

- Is hot-swappable.
- Is designed for tool-less insertion and extraction from the system chassis.
- Has a tachometer signal that allows the Integrated BMC to monitor its status.
- Has its fan speed controlled by integrated platform management. As system thermals fluctuate high and low, the Integrated BMC firmware increases and decreases the speeds to specific fans within the fan assembly to regulate system thermals.

The connector pinouts for the different system fans are listed in Table 27 and Table 28.
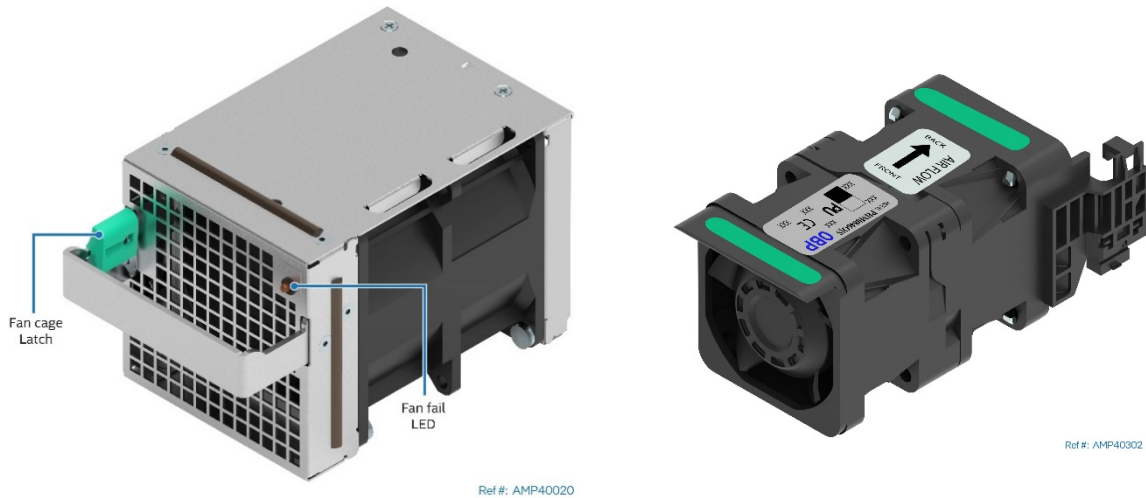
80-mm System Fan   40-mm System Fan

Figure 46. 80-mm and 40-mm System Fans

Table 27. 80-mm System Fan Connector Pinout

Pin #	Signal Name	Pin #	Signal Name
1	P12V_FAN	6	FAN_PRSNT_N
2	GND	7	FAN_CATH_LED
3	FAN_TACH1_FLT	8	FAN_ANODE_LED3
4	FAN_TACH2_FLT	9	P12V_FAN
5	FAN_PWM_FLT	10	GND

Table 28. 40-mm System Fan Connector Pinout

Pin #	Signal Name	Pin #	Signal Name
1	FAN_TACH1_FLT	5	FAN_TACH2_FLT
2	FAN_PWM_FLT	6	GND
3	P12V_FAN	7	GND
4	P12V_FAN	8	FAN_PRSNT_N

9.4 Power Supply Module Fans

Each installed power supply module includes embedded (non-removable) 40-mm fans. These fans are responsible for airflow through the power supply module and are managed by the fan control system of the power supply. Should a fan fail, the power supply shuts down.

9.5 Fan Speed Control

The BMC controls and monitors 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 determine 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 sensors are used to determine the current fan domain state.

A fan domain has three states: sleep, boost, and nominal. 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.

The fan domain state is controlled by several factors, listed below in order of precedence from high to low. If any of these conditions apply, the fans are set to a fixed boost state speed.

- An associated fan is in a critical state or missing. The SDR describes which fan domains are boosted in response to a fan failure or removal in each domain. If a fan is removed when the system is in a DC-off state, it is not detected and there is no fan boost until the system comes out of DC-off mode.
- Any associated temperature sensor is in a critical state. The SDR describes which temperature-threshold violations cause fan boost for each fan domain.
- The BMC is in firmware update mode, or the operational firmware is corrupted.
- If any of the above conditions apply, the fans are set to a fixed boost state speed.

For more information on nominal fan speed, see Section 9.5.5.

9.5.1   Programmable Fan Pulse Width Modulation (PWM) Offset

The system provides a BIOS Setup option to boost the system fan speed by a programmable positive offset setting. Enabling the **Fan PWM Offset** option causes the BMC to add the offset to the fan speeds to which it would otherwise be driving the fans. This setting causes the BMC to replace the domain minimum speed with alternate domain minimums that are also programmable through SDRs.

This capability is offered to provide system administrators the option to manually configure fan speeds in instances where the fan speed optimized for a given platform may not be sufficient when a high-end add-in adapter is configured into the system.

9.5.2   Hot-Swappable Fans

Hot-swap fans are supported and can be removed and replaced while the system is powered on and operating. The BMC implements fan presence sensors (sensor type = Fan (04h), event / reading type = Generic (08h) for each hot-swappable fan.

When a fan is not present, the associated fan speed sensor is put into the reading/unavailable state, and any associated fan domains are put into the boost state. The fans may already be boosted due to a previous fan failure or fan removal.

When a removed fan is inserted, the associated fan speed sensor is re-armed. If there are no other critical conditions causing a fan boost condition, the fan speed returns to the nominal state. Power cycling or resetting the system re-arms the fan speed sensors and clears fan failure conditions. If the failure condition is still present, the fan returns to its boosted state once the sensor has re-initialized and the threshold violation is detected again.

9.5.3   Fan Redundancy Detection

The BMC supports redundant fan monitoring and implements a fan redundancy sensor. A fan redundancy sensor generates events when its associated set of fans transitions between redundant and non-redundant states, as determined by the number and health of the fans.

Note: The definition of fan redundancy is system-configuration dependent. The Integrated BMC allows for redundancy to be configured on a per-fan redundancy sensor basis through OEM SDR records. The shipping configuration from Intel allows for optimal system performance within the operational limits defined in this document.

A fan failure or removal of hot-swap fans up to the number of redundant fans specified in the SDR in a fan configuration is a non-critical failure and is reflected in the front panel status. A fan failure or removal that

exceeds the number of redundant fans is a non-fatal, insufficient-resources condition and is reflected in the front panel status as a non-fatal error. In the front control panel, a blinking green system status LED indicates non-critical error and a blinking amber LED indicates non-fatal error.

Redundancy is checked only when the system is in the DC-on state. Fan redundancy changes that occur when the system is DC-off or when AC is removed, will not be logged until the system is turned on.

9.5.4   Fan Control Mechanism

System fan speeds are controlled through Pulse Width Modulation (PWM) signals that 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.

The BMC controls the average duty cycle of each PWM signal through direct manipulation of the integrated PWM control registers.

The same device may drive multiple PWM signals.

9.5.5   Nominal Fan Speed

A fan domain's nominal fan speed can be configured as static (fixed value) or controlled by the state of one or more associated temperature sensors.

OEM SDR records are used to configure which temperature sensors are associated with which fan control domains and the algorithmic relationship between the temperature and fan speed. Multiple OEM SDRs can reference or control the same fan control domain and multiple OEM SDRs can reference the same temperature sensors.

Hysteresis can be specified to minimize fan speed oscillation and to smooth fan speed transitions. If a Tcontrol SDR record does not contain a hysteresis definition (for example, an SDR adhering to a legacy format), the BMC assumes a hysteresis value of zero.

9.5.6   Thermal and Acoustic Management

This feature allows for 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 individual memory DIMMs. Additionally, closed-loop thermal throttling is only supported with DIMMs containing temperature sensors.

9.5.7   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 fan speed control:

- Front panel temperature sensor [1]
- Processor margin sensors [2, 4, 5]
- DIMM thermal margin sensors [2, 4]
- Exit air temperature sensor [1, 7, 9]
- PCH temperature sensor [3, 5]
- Onboard Ethernet controller temperature sensors [3, 5]
- PSU thermal sensor [3, 8]
- Processor VR temperature sensors [3, 6]

- DIMM VR temperature sensors [3, 6]
- BMC temperature sensor [3, 6]
- Global aggregate thermal margin sensors [7]
- Riser card temperature sensors

Notes:

[1] For fan speed control in Intel® chassis

[2] Temperature margin to max junction temp

[3] Absolute temperature

[4] PECI value or margin value

[5] On-die sensor

[6] Onboard sensor

[7] Virtual sensor

[8] Available only when a PSU is connected through PMBus

[9] Calculated estimate

The following figure shows a high-level representation of the fan speed control structure that determines fan speed.
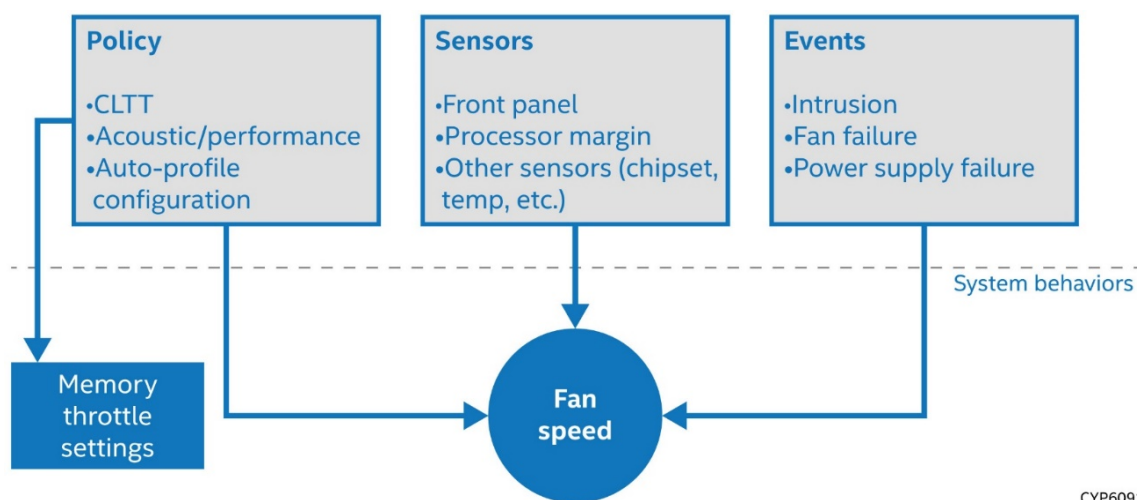
Figure 47. High-Level Fan Speed Control Model

9.6   FRUSDR Utility

The purpose of the embedded platform management and fan control systems is to monitor and control various system features, and to maintain an efficient operating environment. Platform management is also used to communicate system health to supported platform management software and support mechanisms. The FRUSDR utility is used to program the server board with platform specific environmental limits, configuration data, and the appropriate sensor data records (SDRs) for use by these management features.

As part of the system manufacturing process, a default software stack is loaded that contains FRU and SDR data. However, this software may not be the latest available version. Intel recommends updating the SDR to the latest available as part of a planned system software update.

The FRUSDR utility for the given server platform can be downloaded as part of the System Update Package (SUP) or System Firmware Update Package (SFUP) from http://downloadcenter.intel.com.

Note: The embedded platform management system may not operate as expected if the platform is not updated with accurate system configuration data. The FRUSDR utility must be run with the system fully configured during the initial system integration process for accurate system monitoring and event reporting.

---

10. System Power

The Intel® Server D40AMP family supports up to four AC 2100 W (80 Plus Platinum) power supplies. Each power supply is hot-swappable and allows tool-less insertion and extraction from the rear of the chassis.

Disclaimer: The Intel® Server D40AMP family is designed to operate as described in this Technical Product Specification when connected to a 220–240 V power source. Connecting to a lower voltage power line is not supported and may result in an unreliable system operation. If a 220–240 V power source is not available, it is the responsibility of the system integrator to recalculate the total power consumption of the system.
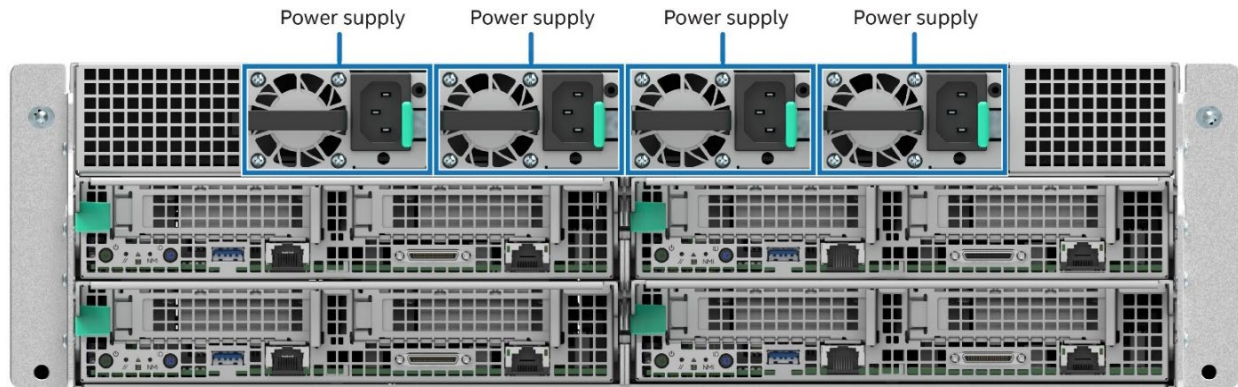
Figure 48. Power Supply Module Identification
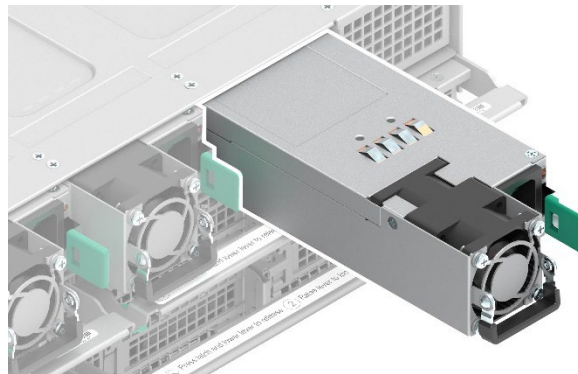
Figure 49. Power Supply Module Partially Out of Chassis

Figure 50. Power Supply Module

To minimize the risk of accidental power cord extraction, each power supply supports a power cord retention strap.
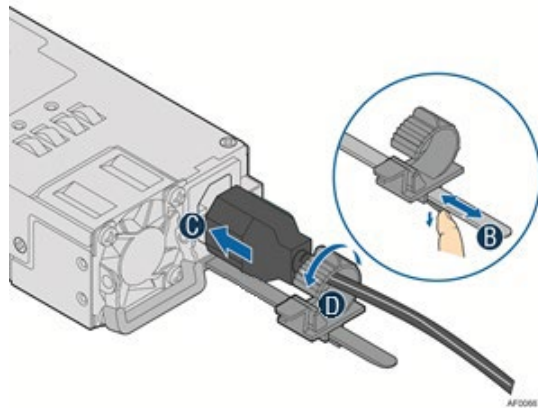
Figure 51. Power Cord Retention Strap

10.1 Power Supply Configurations

The Intel® Server Chassis VP3000 family can have up to four power supply modules installed. The Integrated BMC calculates the total power demand at the chassis level and distributes the power load among the installed power supply modules. A fully configured 4-module system supporting 24 U.2 or 32 E1.L NVMe* SSDs supports the following power supply configurations:

- 4+0 combined power (non-redundant)
- 3+1 redundant power

Redundant power and combined power configurations are automatically configured depending on the number of modules in the system. Should system thermal levels exceed programmed limits, platform management attempts to keep the system operational. For details, see Section 10.2 and Chapter 11.

In the event of a power supply failure, the redundant power configurations support hot-swap extraction and replacement of the failed power supply. The AC input is auto-ranging and power factor corrected. In the event of a power supply failure in a 4+0 configuration, the other three power supplies provide the power and the system may throttle.

Note: Other power supply configurations may be supported depending on system configuration. Refer to the *Intel® Server D40AMP Power Budget and Thermal Configuration Tool* for more details.

10.2 Closed Loop System Throttling (CLST)

The server system supports Closed Loop System Throttling (CLST) that prevents the system from crashing if a power supply module is overloaded or overheats. If the system power reaches a pre-programmed power limit, CLST throttles system memory and/or processors to reduce power. System performance is degraded if this event occurs.

10.3 Smart Ride Through (SmaRT) Throttling

The server system supports Smart Ride Through (SmaRT) throttling. This increases the reliability of a system operating in a heavy power load condition and to remain operational during an AC line dropout event.

When AC voltage is too low, a fast AC loss detection circuit inside each installed power supply asserts an SMBALERT# signal to initiate a throttle condition in the system. System throttling reduces the bandwidth to both system memory and processors, which, in turn, reduces the power load during the AC line drop out event.

10.4 Cold Redundancy Support

10.4.1   Powering on Cold Standby Power Supplies to Maintain Best Efficiency

The system assigns a cold standby state for each installed power supply, depending on the power demand for operation. The assigned state or position can be 1, 2, or 3. The BMC uses a signal that can be identified by the power supplies to enter an active state, should the system power demand rise above a predefined threshold. Depending on which position (1, 2, or 3) the system defines a power supply to be in, the cold standby configuration slightly changes the system power demand threshold that the power supply will power on at.

When a power supply changes its state from cold standby to active or vice versa these events are logged in the System event log as CR_BUS asserted or de-asserted states.

10.4.2   Powering on Cold Standby Power Supplies During a Fault or Over Current Condition

In the event of a power supply failure, the CR_BUS signal for it will change to a fault state. When this happens, all installed power supplies in cold standby mode will power on within 100 µsec.

10.4.3   BMC Requirements

The BMC uses the `Cold_Redundancy_Config` command to define and configure the power supply's role in the cold redundancy scheme and to turn on/off cold redundancy.

To allow for equal usage over the lifetime of installed power supplies, the BMC schedules a rolling re-configuration of installed power supplies. Each one is rotated between being an "Active" power supply and a "Cold Stby" power supply as needed.

Events that trigger a re-configuration of the power supplies using the `Cold_Redundancy_Config` command are listed below.

- AC power ON
- PSON power ON
- Power supply failure
- Power supply inserted into system

10.4.4   Power Supply Turn on Function

Powering on and off the cold standby power supplies is controlled by each PSU. The system defines the position of each power supply in the cold redundant operation. It does this each time the system is powered on, a power supply fails, or a power supply is added to the system.

The system is relied upon to tell each power supply where it resides in the cold redundancy scheme.

10.5 Power Supply Specification Overview

The Intel® Server D40AMP family supports the following power supply:

- AC 2100 W (80 Plus Platinum)

AC power supplies are auto-ranging and power factor corrected.

The following sections provide an overview of select power supply features and functions.

Note: Full power supply specification documents are available upon request. Power supply specification documents are classified as Intel Confidential and will require a signed non-disclosure agreement (NDA) with Intel before being made available.

10.5.1   Power Supply Module Efficiency

Each power supply option is rated to meet specific power efficiency limits based on their 80 PLUS power efficiency rating: Titanium, Platinum, or Gold.

The following tables define the required minimum power efficiency levels based on their 80 PLUS efficiency rating at specified power load conditions: 100%, 50%, 20%, and 10%

Table 29. 2100 W AC Power Supply Efficiency (80 PLUS* Platinum)

Loading	100% of maximum	50% of maximum	20% of maximum	10% of maximum
Minimum Efficiency	91%	94%	90%	82%

10.5.2   AC Power Cord Specifications
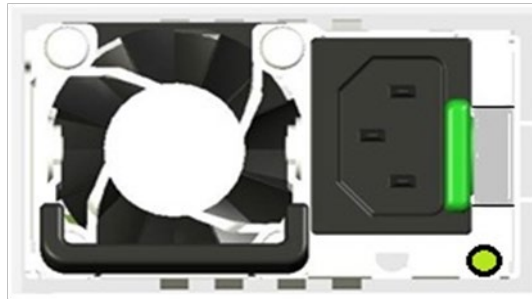
Figure 52. AC Power Cable Connector

CYP41880
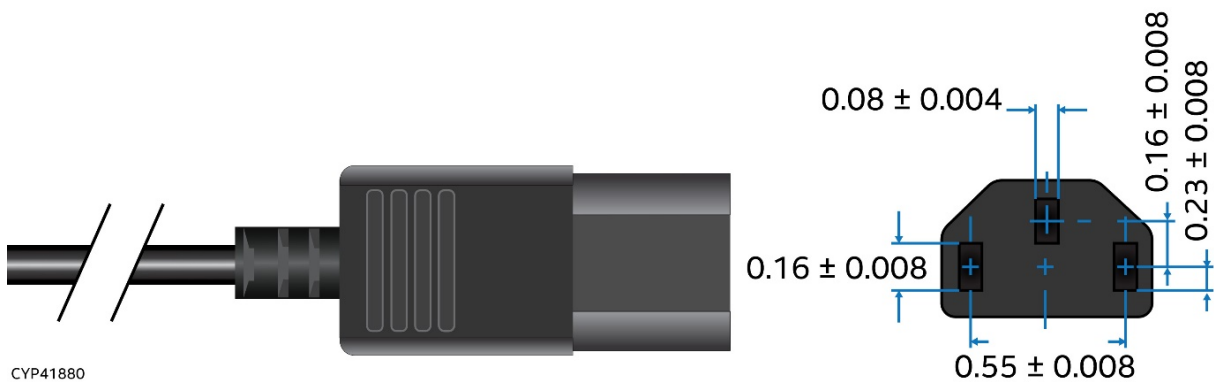
Figure 53. AC Power Cord Specification

The AC power cord used must meet the specification requirements listed in the following table.

Table 30. AC Power Cord Specifications

Item	Description
Cable Type	SJT
Wire Size	14 AWG
Temperature Rating	105 ºC
Amperage Rating	10 A at 240 V
Voltage Rating	240 VAC

10.6 Power Supply Features

The following sections describe features supported by the AC power supply options.

10.6.1   Power Supply Status LED

A single bi-color LED indicates power supply status. The operational states of this bi-color LED are defined in the following table.

Table 31. LED Indicators

LED State	Power Supply Condition
Off	No source power.
Solid green	Output ON and OK.
1 Hz blinking green	Source power present/only 12 VSB on (PS off) or PS in cold redundant state.
Solid amber	Source power cord unplugged or source power lost; with a second power supply in parallel still with AC input power. Or power supply critical event causing a shutdown; failure, OCP, OVP, fan fail.
1 Hz blinking amber	Power supply warning events where the power supply continues to operate; high temp, high power, high current, slow fan.
2 Hz blinking green	Power supply firmware updating.

10.6.2   Protection Circuits

Each installed power supply module includes several protection circuits that will shut down the power supply in the event a defined operating threshold is exceeded.

10.6.2.1   Over Current Protection (OCP)

Each installed power supply is protected against over current. The power supply unit shuts down for a specific time period after crossing current thresholds. A power supply that is shut down due to an exceeded protection circuit threshold can be reset by removing source power for 15 seconds.

Table 32. Over Current Protection for 2100 W Power Supplies

Output Voltage	Input Voltage Range	Over Current Limits	Over Current Protection Delay
+12 V	180–264 VAC	252 A minimum / 258 A maximum	50 msec minimum / 200 msec maximum
		269 A minimum / 277 A maximum	5 msec minimum / 20 msec maximum
12 VSB	90–264 VAC	3.6 A minimum / 4 A maximum	10 msec minimum / 20 msec maximum

Table 33. Over Voltage Protection (OVP) Limits

Output Voltage	Minimum (V)	Maximum (V)
+12 V	13.5	14.5

+12 VSB	13.5	14.5

10.6.2.2   Over Temperature Protection (OTP)

Each installed power supply is protected against over temperature conditions caused by loss of fan cooling or excessive ambient temperature. The power supply unit shuts down during an OTP condition. Once the power supply temperature drops to within specified limits, the power supply restores power automatically.

Note: The 12 VSB always remains on while the power supply is connected to the power source.

10.7 Power Distribution Board (PDB)

The Intel® Server D40AMP family includes two power distribution boards (PDBs) providing power and management connections for several components in the system. The following figure shows the location of the PDBs in the system.

Primary Power Distribution Board

Secondary Power Distribution Board
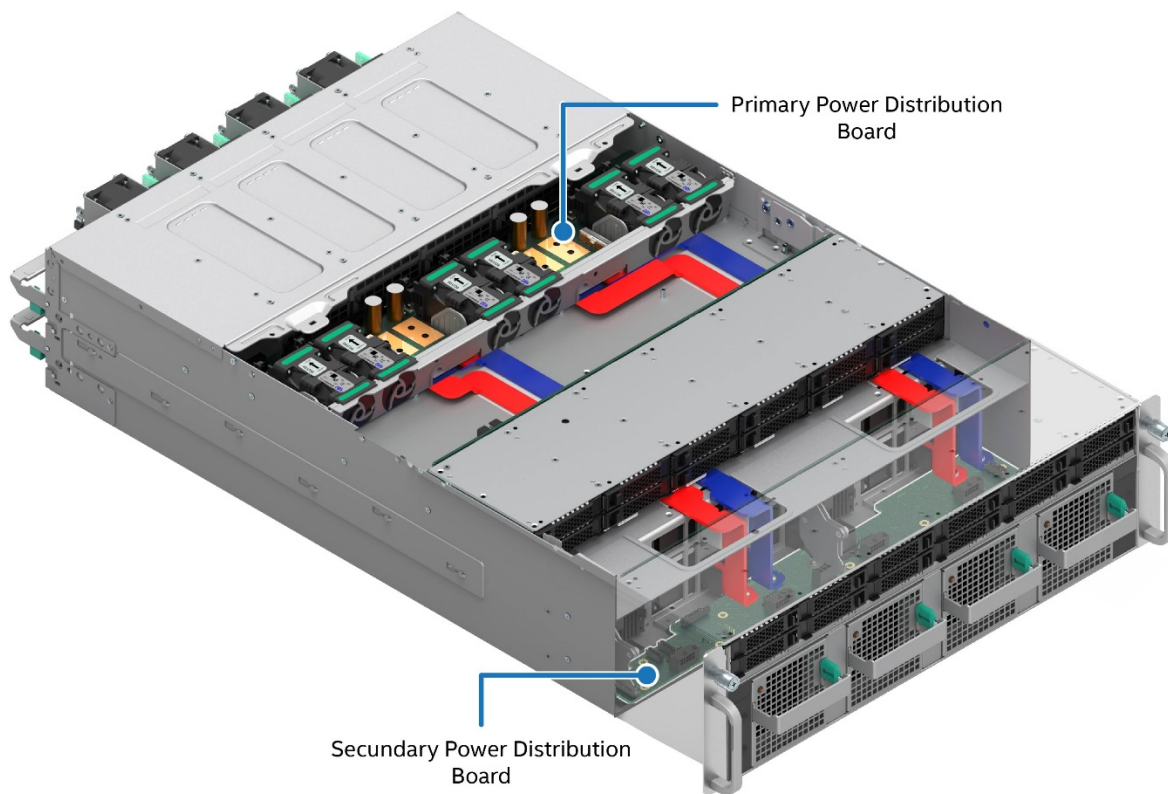
Ref #: AMP40480

Figure 54. Power Distribution Board Identification

10.7.1   Primary Power Distribution Board

The primary power distribution board is located in the back of the chassis and it is the entry point for all power in the system. It provides power directly for the 40 mm system fans in the back of the chassis, and one of the backplanes or midplane, depending on system configuration. It is connected to the secondary power distribution board through bus bars.

The primary power distribution board includes the following features:

- Four power supply interface connectors in the rear
- Backplane power connectors
- Six system fan connectors on top

- Six fan fault LEDs each associated to a system fan connector
- Mount points for bus bars for connecting to the secondary PDB

Figure 55 identifies the connectors in the secondary power distribution board.
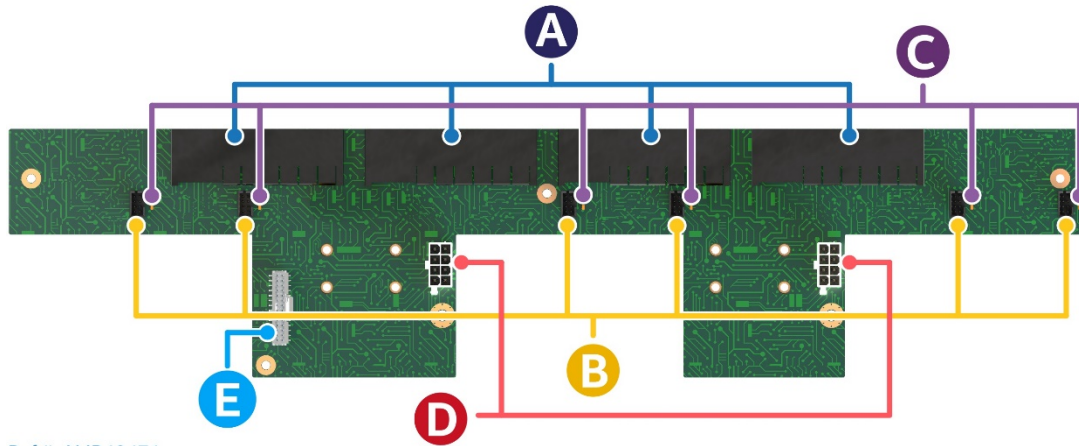
Ref #: AMP40471

Figure 55. Primary Power Distribution Board Connector Identification

Table 34. Primary Power Distribution Board Connector Identifiers

Connector Identifier	Description
A	Power supply connectors
B	40 mm system fan connectors
C	Fan fault LEDs
D	Backplane power connector
E	Sideband connector

10.7.2 Secondary Power Distribution Board

The secondary power distribution board receives power from the primary PDB through four bus bars. It provides power to the installed compute modules, the front system fans, and provides power and communication signals for the chassis front control panels.

Aside from these general features, the secondary PDB also supports specific features depending on system configuration:

- Systems configured with chassis VP3U2HAC21W0: provides power to the hot-swap backplane located at the front of the chassis and I2C signals for the installed hot-swap backplanes.
- Systems configured with chassis VP3E1HAC21W0: provides I2C signals for the installed midplane.

The following figure identifies the connectors in the secondary power distribution board.
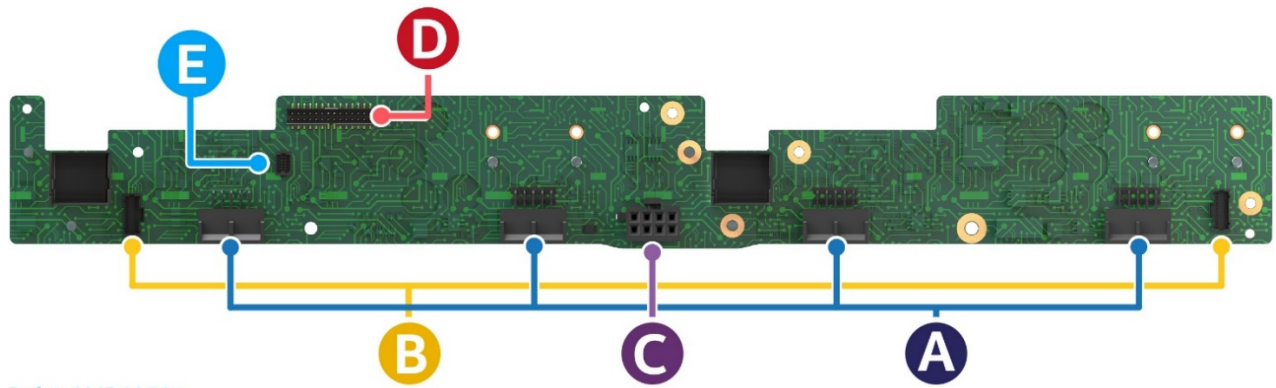
Ref #: AMP40501

Figure 56. Secondary Power Distribution Board Connector Identification

Table 35. Secondary Power Distribution Board Connector Identifiers

Connector Identifier	Description
A	80 mm front system fan connectors
B	Chassis front control panel connectors
C	Backplane power connector
D	Sideband connector
E	I2C Cable Connector

11. Platform Management

The Intel® Server D40AMP family uses an ASPEED* AST2500 server management processor as the baseboard management controller (BMC). The BMC supports multiple system management features including intra-system sensor monitoring, fan speed control, system power management, and system error handling and messaging. It also provides remote platform management capabilities including remote access, monitoring, logging, and alerting features.

All server management capabilities can be split in two groups:
- Standard management features (Included)
- Optional advanced management features that can be enabled with the purchase of advanced management license

In addition, BMC integrates with the Intel® Data Center Manager (DCM) software to provide unified management at Data Center level.

The following subsections provide a brief description of each.

11.1 Management Port

The Intel® Compute Module D40AMP includes a 1 Gb/s Ethernet RJ45 port used to access embedded system management features remotely.

Note: The management port is for system management access purposes only. The port is not intended or designed to support standard LAN data traffic.

For more information on the server management port, including LED definition, see Chapter 8.

TNP3070

Dedicated Management Port
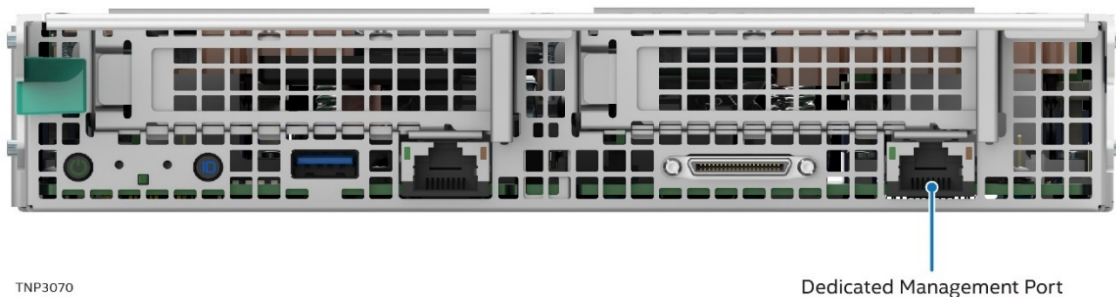
Figure 57. Server Management Port Location in Compute Modules

Before the 1 GbE Ethernet port can be used for remote management, it must be configured in the BIOS Setup Utility.

11.1.1   Configuring System Management Port Using BIOS Setup

1. After the server completes the POST process, press the <F2> key on keyboard when prompted to go to the BIOS Setup utility.
2. Navigate to the **Server Management** tab and select **BMC LAN Configuration** to enter the BMC LAN Configuration screen (Figure 58).
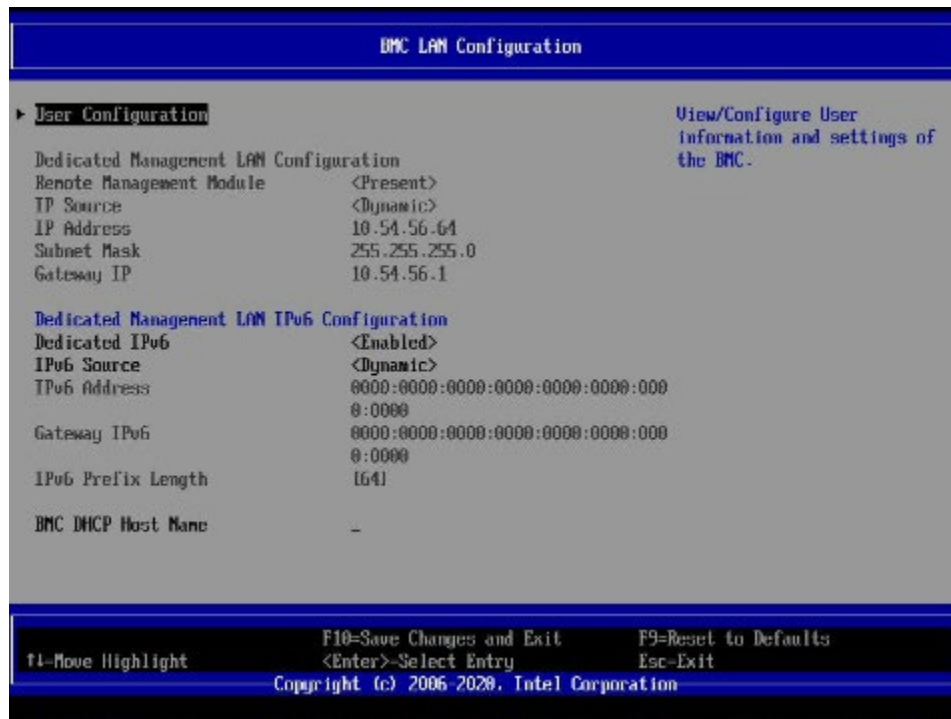
Figure 58. BIOS Setup BMC LAN Configuration Screen

The system is configured using the **BMC LAN Configuration**

3. Use the Server Management LAN configuration section to set parameters for an IPv4 network:
   o If Static is selected as the IP source, configure the IP address, Subnet mask, and Gateway IP as needed.
4. Use the Server Management LAN IPv6 configuration section to set parameters for an IPv6 network:
   o Navigate to the Dedicated IPv6 field and then select Enabled. Then scroll to IPV6 source and select either Static or Dynamic. If Static is selected, configure the IPV6 address, Gateway IPV6, and IPV6 Prefix Length as needed.
5. Select **BMC User Configuration** to enter the User Configuration screen (Figure 59).
6. Under **User ID**, set the following settings as desired:
   o **Privilege** – Select the privilege to be used. (Administrator privilege is required to use KVM or media redirection).
   o **User Status** – Select **Enabled**.
   o **User Name** – Enter the desired name. Note that the anonymous user cannot be changed.
   o **User password** – Enter the desired password twice.
7. Press **<F10>** to save the configured settings and exit BIOS Setup. The server reboots with the new LAN settings.

Figure 59. BIOS Setup User Configuration Screen

Once the management port is configured, the server can be accessed remotely to perform system management functions defined in the following sections.

11.2 Standard System Management Features

The following system management features are supported on the Intel® Server D40AMP family by default.

- Integrated BMC Web Console
- Virtual KVM over HTML5
- Redfish*
- IPMI 2.0
  o Node Manager
- Out-of-band BIOS/BMC Update and Configuration
- System Inventory
- Autonomous Debug Log

The following subsections provide a brief description for each feature.

11.2.1 Integrated BMC Web Console

The BMC firmware includes an embedded web server that can serve web pages to any supported browser. This web console is designed to be fully a functional server administration tool and allows a system administrator to:

- View system information including firmware versions, server health, diagnostic information, and power statistics.
- Configure BMC and BIOS options
- Perform power actions (power on, power off, etc.)
- Launch the KVM and media redirection application

To access Integrated BMC Web Console enter the configured IP address of the BMC management port (see Section 11.1.1) into the web browser in the URL field. The Integrated BMC Web Console login page will be shown (See Figure 60).

Enter the username and password and select a language option. For example:

- Username: `root`
- Password: `superuser`
- Language: **English**
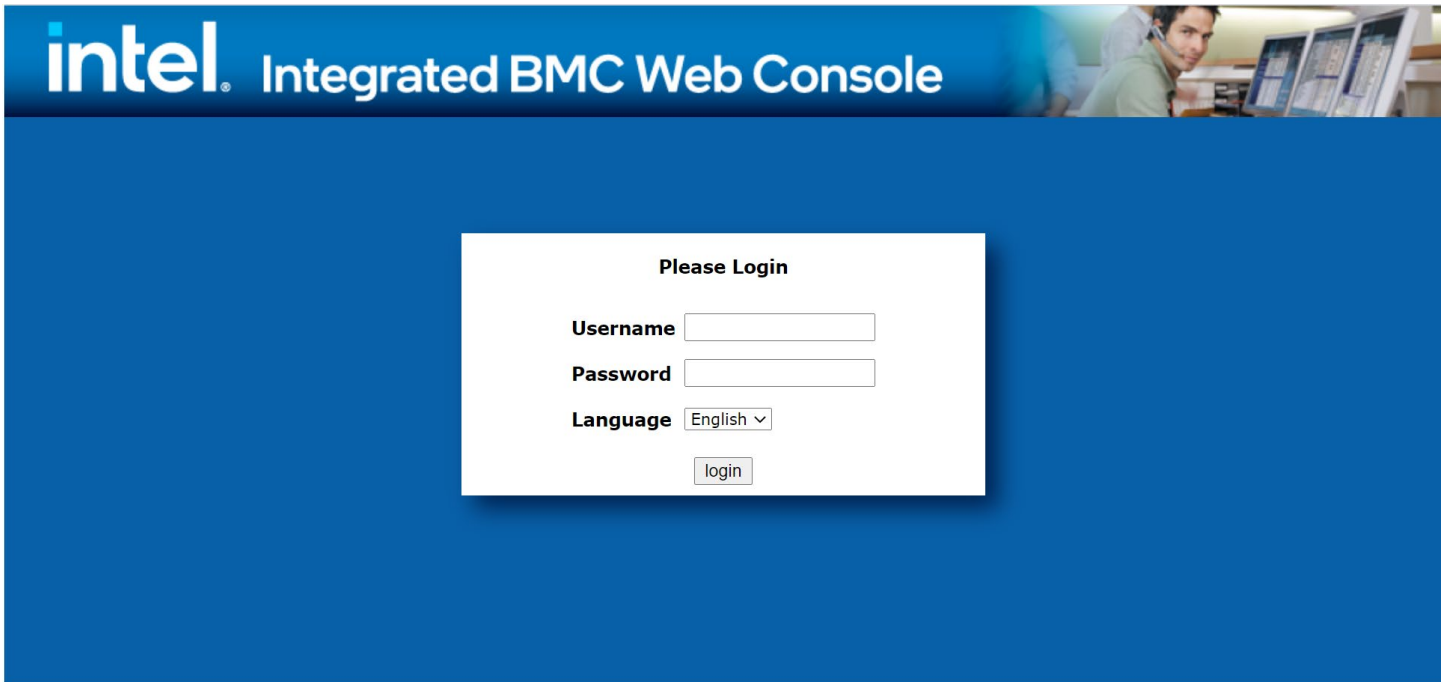
Figure 60. Integrated BMC Web Console Login Page

Click the **Login** button to view the "System" page.
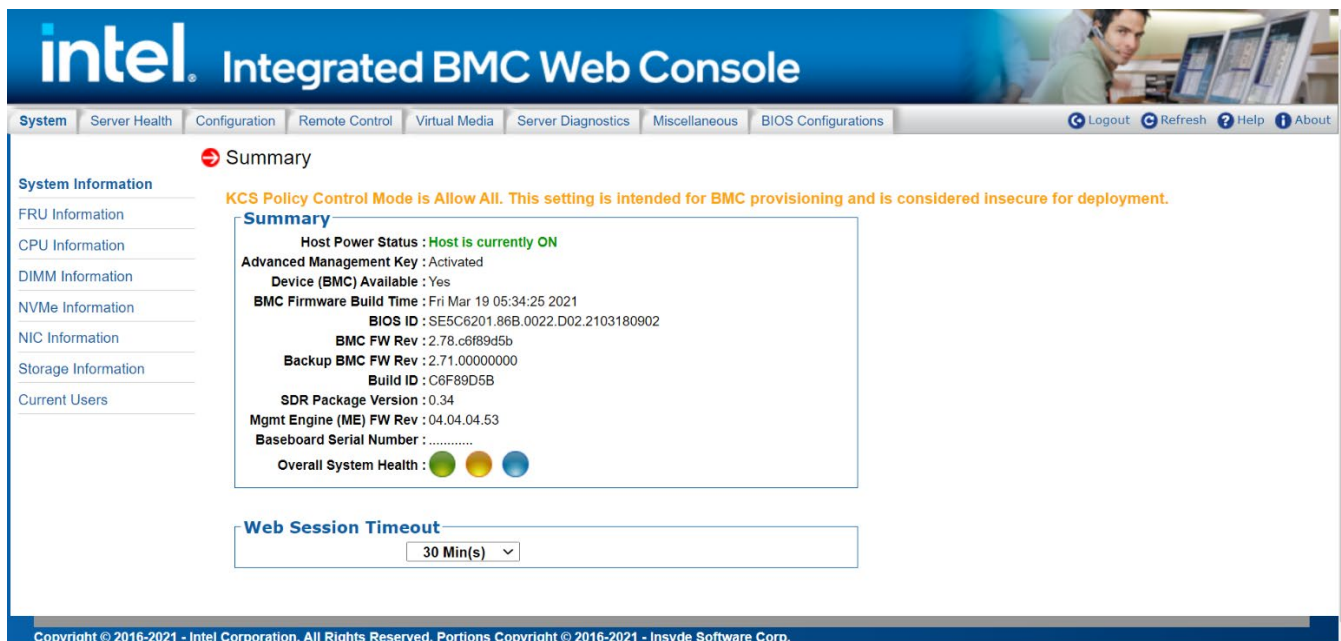
Figure 61. Integrated BMC Web Console – System Tab View

For additional information about the BMC Web Console, refer to the *Intel® Integrated Baseboard Management Controller Web Console (Intel® BMC Web Console) User Guide.*

11.2.2   Virtual KVM over HTML5

The BMC firmware supports keyboard, video, and mouse redirection (KVM) over LAN. This feature allows a user to interact with a remote server using the keyboard, video, and mouse (KVM) of the local computer as if the user were physically at the managed server. This feature is available as an HTML5 application of the embedded web server. 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).

KVM redirection supports the following keyboard layouts: English, Chinese (traditional), Japanese, German, French, Spanish, Korean, Italian, and United Kingdom. The KVM redirection application also includes a "soft keyboard" function emulating an entire keyboard on the screen. 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.

11.2.3   Redfish* Support

DMTF's Redfish* is a standard designed to deliver simple and secure management for converged, hybrid IT and the Software Defined Data Center (SDDC). Both human readable and machine capable, Redfish* leverages common Internet and web services standards to expose information directly to the modern tool chain. The BMC currently supports version 1.7 and schema version 2019.1.

11.2.4   IPMI 2.0 Support

The BMC is IPMI 2.0 compliant including support for Intel® Dynamic Power Node Manager. IPMI defines a set of interfaces used by system administrators for out-of-band management of computer systems and monitoring of their operation.

11.2.5   Out-of-Band BIOS / BMC Update and Configuration

The BMC supports Redfish* schemas and embedded web console features that allow administrators to update the BMC, BIOS, Intel® ME and SDR firmware. The BMC firmware also includes Power Supply and Backplane firmware. The BMC update will happen immediately and cause a BMC reset to occur at the end. The BIOS and Intel® ME firmware is staged in the BMC and will be updated on the next reboot. The BMC also allows to view and modify BIOS settings using Redfish or the embedded web console. On each boot, BIOS provides all its settings and active value to the BMC to be displayed. BIOS also checks if any changes are requested and performs those changes.

11.2.6   System Inventory

The BMC supports Redfish* schemas and embedded web console pages to display system inventory. This inventory includes FRU information, CPU, Memory, NVMe*, networking, and storage. When applicable, the firmware version will also be provided.

11.2.7   Autonomous Debug Log

The BMC has a debug log that can be downloaded to facilitate support issues. This debug log can be downloaded from the embedded web console or via syscfg and SDPTool utilities. The debug log contains configuration data including SDR, SEL, BMC configuration, PCI configuration, power supply configuration and power supply black box data. The debug log also contains SMBIOS data and the POST codes from the last two system boots. Finally, when the system has a catastrophic error condition leading to a system shutdown, the BMC will hold the CPU in reset long enough to collect processor machine check registers, memory controller machine check registers, I/O global error registers, and other processor state info.

11.2.8   Security Features

The BMC supports several security features including OpenLDAP and Active Directory, security logs, ability to turn off any remote port, SSL certificates, traffic encryption, VLANs, and KCS control. The BMC also supports full user management with password defined privileges and the ability to define password complexity rules. Each BMC release is given a security version number to prevent firmware downgrades to lower security versions. Intel provides a best practices security guide, available at https://www.intel.com/content/www/us/en/support/articles/000055785/server-products.html

11.3 Advanced System Management Features

Purchasing an optional Advanced System Management product key (iPC **ADVSYSMGMTKEY**), unlocks the following advanced system management features:

- Virtual Media Image Redirection (HTML5 and Java)
- Virtual Media over network share and local folder
- Active Directory support
- Included single system license for Intel® Data Center Manager (Intel® DCM)
  - Intel® Data Center Manager (Intel® DCM) is a software solution that collects and analyzes the real-time health, power, and thermals of a variety of devices in data centers helping you improve the efficiency and uptime. For more information, go to https://software.intel.com/content/www/us/en/develop/download/dcm-product-brief.html
- Future Feature Additions
  - Full system firmware update including drives, memory, and RAID
  - Storage and network device monitoring
  - Out-of-band hardware RAID Management for latest Intel RAID cards

The Advanced System Management product key can be purchased and pre-loaded onto the system when ordering a fully integrated server system directly from Intel using its online Configure-to-Order (CTO) tool. Or the Advanced System Management product key can be purchased separately and installed later. When purchasing the product key separately from the system, instructions will be provided on where to register the product key with Intel. A license file is then downloaded onto the system where the Integrated BMC Web Console or the SYSCFG utility are used to upload the key to the BMC firmware to unlock the advanced features.

11.3.1   Virtual Media Image Redirection (HTML5 and Java)

The BMC supports media redirection of local folders and .IMG or .ISO image files. This redirection is supported in both HTML5 and Java console clients. When the user selects "Virtual Media over HTML5", a new web page will be displayed. This web page provides the user interface to select which type of source media (image file or file folder*) to mount, and the location of the desired media to make available to the server system. After the type and specific media are selected, the interface provides a mount/unmount interface so the user can connect the media to or disconnect the media from the server system. Once connected, the selected image file or file folder is presented in the server system as standard removable media. This feature gives system administrators the ability to install software (including operating system installation), copy files, perform firmware updates, and so on from media on their remote workstation.

Note: The shared file/folder is presented to the server system as a UDF file system; the operating system of the server must support UDF file systems for this feature to work.

11.3.2   Virtual Media over network share and local folder

In addition to supporting media redirection from the administrator's workstation (see Section 11.3.1), the BMC also supports media redirection of file folders and .IMG or .ISO files hosted on a file server accessible to the BMC via network interface. The current version supports Samba shares (Microsoft Windows* file shares). Future versions will add support for NFS shares. This virtual media redirection is more effective for mounting virtual media at scale, instead of processing all files from the workstation's drive through the HTML5 application and over the workstation's network. Each BMC makes a direct network file share connection to the file server and accesses files across that network share directly.

11.3.3   Active Directory support

The BMC supports Active Directory. Active Directory (AD) is a directory service developed by Microsoft* for Windows domain networks. This feature allows users to login to the BMC web console or Redfish* using an active directory authentication instead of local credentials. The feature allows administrators to only change passwords on this single domain account instead on every remote system.

11.4 Intel® Data Center Manager (DCM) Support

Intel® DCM is a solution for out-of-band monitoring and managing the health, power, and thermals of servers and a variety of other types of devices.

What can you do with Intel® DCM?

- Automate health monitoring
- Improve system manageability
- Simplify capacity planning
- Identify underutilized servers
- Measure energy use by device
- Pinpoint power/thermal issues
- Create power-aware job scheduling tasks
- Increase rack densities
- Set power policies and caps
- Improve data center thermal profile
- Optimize application power consumption
- Avoid expensive PDUs and smart power strips

For more information, go to:

https://software.intel.com/content/www/us/en/develop/download/dcm-product-brief.html

12. System Software Stack

The Intel® Server Board D40AMP and Intel® Compute Module D40AMP include a system software stack that consists of the following components:

- System BIOS
- BMC firmware
- Intel® Management Engine (Intel® ME) firmware / Intel® Server Platform Services (Intel® SPS)
- Field replaceable unit (FRU) and sensor data record (SDR) data

Together, they configure and manage features and functions of the server system.

Many features and functions of the server system are managed jointly by the system BIOS and the BMC firmware, including:

- IPMI watchdog timer
- Messaging support, including command bridging and user/session support
- BIOS boot flags support
- Event receiver device: The BMC receives and processes events from the BIOS.
- Serial-over-LAN (SOL)
- ACPI state synchronization: The BMC tracks ACPI state changes that are provided by the BIOS.
- Fault resilient booting (FRB): Fault resistant boot level 2 (FRB-2) is supported by the watchdog timer functionality.
- Front panel management: The BMC controls the system status LED and system ID LED. It supports secure lockout of certain front panel functionality and monitors button presses. The system ID LED is turned on using a front panel button or a command
- DIMM temperature monitoring: New sensors and improved acoustic management using closed-loop fan control algorithm comprehending DIMM temperature readings
- Integrated KVM (Keyboard, Video, and Mouse) redirection application
- Integrated remote media redirection application
- Intel® Intelligent Power Node Manager support
- Sensor and system event log (SEL) logging additions/enhancements (e.g., additional thermal monitoring capability)
- Embedded platform debug feature that allows capture of detailed data for later analysis by Intel

A factory installed system software stack is pre-programmed on each server board and compute module within the Intel® Server D40AMP family. However, later revisions may be available. To ensure optimal system operation, Intel recommends the following:

- Power up the Intel® Compute Module D40AMP or system configured with a Intel® Server Board D40AMP and access the onboard BIOS Setup utility to verify the version numbers of the installed system software stack: BIOS, BMC firmware, Intel® ME firmware, FRU and SDR.
- Check the following Intel website for possible updates: http://downloadcenter.intel.com
- Download and update the software stack if later revisions are available.

System updates can be performed in several operating environments, including the UEFI shell using the UEFI-only system update package (SUP), or under different operating systems using the System Firmware Update Package(SFUP) utility.

Refer to the following Intel documents for more in depth information concerning the system software stack and its functions:

- *BIOS Firmware External Product Specification (EPS) for the Intel® Server Board D50TNP, M50CYP, and D40AMP Families* – Intel NDA Required
- *Integrated Baseboard Management Controller Firmware External Product Specification (EPS) for the Intel® Server System D50TNP, M50CYP, and D40AMP Families* – Intel NDA Required

12.1 Hot Keys Supported During POST

Certain hot keys are recognized during power-on self-test (POST). A hot key is a key or key combination that is recognized as an unprompted command input. In most cases, hot keys are recognized even while other processing is in progress.

BIOS supported hot keys are only recognized by the system BIOS during the system boot time POST process. Once the POST process has completed and transitions the system boot process to the operating system, BIOS supported hot keys are no longer recognized.

Table 36 provides a list of available POST hot keys along with a description for each.

Table 36. POST hot keys

Hot Key	Function
<F2>	Enter the BIOS Setup utility
<F6>	Pop-up BIOS boot menu
<F12>	Network boot
<Esc>	Switch from logo screen to diagnostic screen
<Pause>	Stop POST temporarily (press any key to resume)

12.1.1   POST Logo/Diagnostic Screen

If quiet boot is enabled in the BIOS Setup utility, a splash screen is displayed with the standard Intel logo screen or a customized original equipment manufacturer (OEM) logo screen if one is present in the designated flash memory location. By default, quiet boot is enabled in the BIOS Setup utility and the logo screen is the default POST display. However, pressing **<Esc>** hides the logo screen and displays the diagnostic screen instead during the current boot.

If a logo is not present in the BIOS flash memory space, or if quiet boot is disabled in the system configuration, the POST diagnostic screen is displayed with a summary of system configuration information. The POST diagnostic screen is purely a text mode screen, as opposed to the graphics mode logo screen.

If console redirection is enabled in the BIOS Setup utility, the quiet boot setting is disregarded, and the text mode diagnostic screen is displayed unconditionally. This is due to the limitations of console redirection that transfers data in a mode that is not graphics-compatible.

12.1.2   BIOS Boot Pop-Up Menu

The BIOS boot selection (BBS) menu provides a boot device pop-up menu that is 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 utility. The pop-up menu simply lists all 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 configured in the BIOS Setup utility, the administrator password is required to access the boot pop-up menu. If a user password is entered, the user is taken directly to the boot manager in the BIOS Setup utility, only allowing booting in the order previously defined by the administrator.

12.1.3   Entering BIOS Setup

To enter the BIOS Setup utility using a keyboard (or emulated keyboard), press the **<F2>** function key during boot time when the OEM or Intel logo screen or the POST diagnostic screen is displayed.

The following instructional message is displayed on the diagnostic screen or above the quiet boot logo screen:

<div align="center">

Press <F2> to enter setup, <F6> Boot Menu, <F12> Network Boot

</div>

Note: With a USB keyboard, it is important to wait until the BIOS discovers the keyboard. Until the USB controller has been initialized and the keyboard activated, key presses are not read by the system.

When the BIOS Setup utility is entered, the main screen is displayed initially. However, if a serious error occurs during POST, the system enters the BIOS Setup utility and displays the error manager screen instead of the main screen.

For additional BIOS Setup utility information, see the *Intel® Server Board D40AMP BIOS Setup User Guide*.

12.1.4   BIOS Update Capability

To bring BIOS fixes or new features into the system, it is necessary to replace the current installed BIOS image with an updated one. Full BIOS update instructions are provided with update packages downloaded from the Intel website.

12.2 Field Replaceable Unit (FRU) and Sensor Data Record (SDR) Data

As part of the manufacturing process, FRU and SDR data is loaded into the Intel® Server Board D40AMP and Intel® Compute Module D40AMP. This ensures that the embedded platform management system can monitor the appropriate sensor data and operate the system with best cooling and performance. This also ensures that auto-configuration occurs without the need to perform additional SDR updates or provide other user input to the system when any of the following components are added or removed:

- Module
- Memory
- Power supply
- Fans
- Power distribution boards

Intel recommends updating the SDR to the latest available version whenever a system software update is performed.

12.2.1   Loading FRU and SDR Data

The FRU and SDR data can be updated using a stand-alone FRUSDR utility in the UEFI shell or can be done using the Intel OFU utility program under a supported operating system. Full FRU and SDR update instructions are provided with the appropriate system update package (SUP) or System Firmware Update Package (SFUP) utility that can be downloaded from http://downloadcenter.intel.com.

13. System Security

The Intel® Compute Module D40AMP supports a variety of security options designed to prevent unauthorized access to or tampering with system settings. Security options supported include:

- Password protection
- Front panel lockout
- Intel® Platform Firmware Resilience (Intel® PFR)
- Intel® Software Guard Extensions (Intel® SGX)
- Trusted Platform Module (TPM) support
- Intel® CBnT – Converged Boot Guard and Trusted Execution Technology (Intel® TXT)
- Unified Extensible Firmware Interface (UEFI) Secure Boot Technology

13.1 Password Protection

The BIOS Setup utility includes a Security tab where options to configure passwords, front panel lockout, and TPM settings are found.
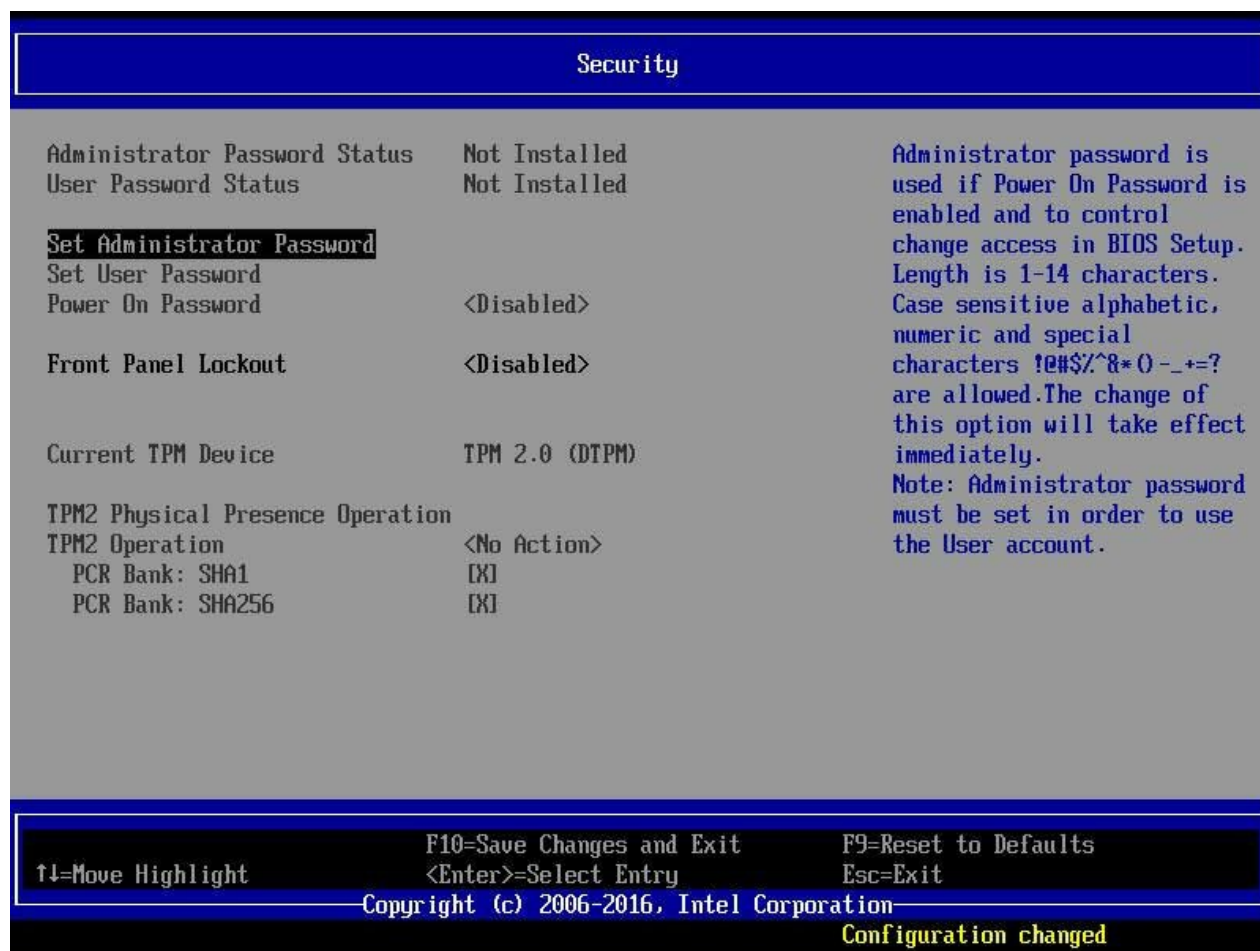
Figure 62. BIOS Setup Security Tab

13.1.1   Password Setup

The BIOS uses passwords to prevent unauthorized access to the Intel® D40AMP modules. Passwords can restrict entry to the BIOS Setup utility, restrict use of the Boot Device popup menu during POST, suppress automatic USB device re-ordering, and prevent unauthorized system power on. It is strongly recommended that an administrator password be set. A system with no administrator password set allows anyone who has access to the server to change BIOS settings.

An administrator password must be set, in order to set the user password.

The maximum length of a password is 14 characters. The minimum length is one character. The password can be made up of a combination of alphanumeric (a-z, A-Z, 0–9) characters and any of the following special characters:

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

Passwords are case-sensitive.

The administrator and user passwords must be different from each other. An error message is displayed, and a different password must be entered if there is an attempt to enter the same password for both. The use of strong passwords is encouraged, but not required. To meet the criteria for a strong password, the password entered must be at least eight characters in length, and must include at least one each of alphabetical, numeric, and special characters. If a weak password is entered, a warning message is displayed, and the weak password is 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. Clearing the administrator password also clears the user password. Passwords can also be cleared by using the password clear jumper on the server board. For more information on the password clear jumper, see Section 14.2.

Resetting the BIOS configuration settings to default values (by any method) has no effect on the administrator and user passwords.

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.

13.1.2   System Administrator Password Rights

When the correct administrator password is entered, the user may perform the following actions:

- Access the BIOS Setup utility.
- Configure all BIOS Setup options in the BIOS Setup utility.
- Clear both the administrator and user passwords.
- Access the Boot Menu during POST.

If the Power On Password function is enabled in BIOS Setup, the BIOS halts early in POST to request a password (administrator or user) before continuing POST.

13.1.3   Authorized System User Password Rights and Restrictions

When the correct user password is entered, the user can perform the following actions:

- Access the BIOS Setup utility.
- View, but not change, any BIOS Setup options in the BIOS Setup utility.
- Modify system time and date in the BIOS Setup utility.

If the Power On Password function is enabled in BIOS Setup, the BIOS halts early in POST to request a password (administrator or user) before continuing POST.

Configuring an administrator password imposes restrictions on booting the system and configures most setup fields to read-only if the administrator password is not provided. The boot popup menu requires the administrator password to function, and the USB reordering is suppressed as long as the administrator password is enabled. Users are restricted from booting in anything other than the boot order defined in setup by an administrator.

13.2 Front Panel Lockout

If enabled in BIOS Setup from the Security screen, this option disables the following front panel features:

- The off function of the power button.
- System reset button.

If front panel lockout is enabled, power off and reset must be controlled via a system management interface.

13.3 Intel® Platform Firmware Resilience (Intel® PFR)

As the intensity, sophistication, and disruptive impact of security attacks continue to escalate, data centers are driving a holistic approach to protect their critical infrastructure. This includes protecting server systems at the firmware level, the lowest layers of the platform, where threats are most difficult to detect. To address this, Intel has developed Intel® Platform Firmware Resilience (Intel® PFR) technology where platforms can provide security starting with power-on, system boot, and OS load activities.

The Intel® Server D40AMP family supports Intel® PFR technology, a hardware-enhanced platform security that uses an Intel® FPGA to protect, detect, and correct platform firmware.

- **Protect:** Monitors and filters malicious traffic on system buses. All platform firmware is attested safe before code execution.
- **Detect:** Verifies integrity of platform firmware images before executing. Performs boot and runtime monitoring to assure server is running a known good firmware.
- **Correct:** Automatically restores corrupted firmware from a protected gold recovery image within minutes

Critical firmware elements protected in an Intel® Server D40AMP system include: BIOS, SPI Descriptor, BMC, Intel® Management Engine (Intel® ME), and Power Supply firmware. This capability to mitigate firmware corruption is an important industry innovation and provides an optimal solution for security-sensitive organizations.

Intel® PFR fully supports the National Institute of Standards and Technology (NIST*) proposed firmware resiliency guidelines (800-193) that have wide industry support.

13.4 Intel® Total Memory Encryption (Intel® TME)

To better protect computer system memory, the 3rd Gen Intel® Xeon® Scalable processor has a security feature called Intel® Total Memory Encryption (Intel® TME). This feature is supported on the Intel® Server D40AMP family. Intel® TME helps ensure that all memory accessed from the Intel® processors is encrypted, including customer credentials, encryption keys, and other IP or personal information. Intel® TME is also available for multi-tenant server applications, called Intel® Total Memory Encryption – Multi-Tenant (Intel® TME-MT).

Intel developed this feature to provide greater protection for system memory against hardware attacks, such as removing and reading the dual in-line memory module (DIMM) after spraying it with liquid nitrogen or installing purpose-built attack hardware. Using the National Institute of Standards and Technology (NIST) storage encryption standard AES XTS, an encryption key is generated using a hardened random number generator in the processor without exposure to software. This allows existing software to run unmodified while better protecting memory.

Intel® TME can be enabled directly in the server BIOS and is compatible with Intel® Software Guard Extensions application enclave solutions.

Intel® TME has the following characteristics:

- **Encrypts** the entire memory using a NIST standard "storage-class" algorithm for encryption: AES-XTS
- **Transparent to software**, it encrypts data before writing to server memory and then decrypts on read.
- **Easy enablement** that requires no operating system or application modification and is applicable to all operating systems.

To enable/disable Intel® TME, access the BIOS Setup menu by pressing **<F2>** key during POST. Navigate to the following menu: **Advanced > Processor Configuration**

Important Note: When either Intel® TME or Intel® TME-MT is enabled, Intel® Optane™ persistent memory 200 series (if installed) will be disabled. See Table 17 for details.

For more information on Intel® TME, see the *BIOS Setup Utility User Guide for the Intel® Server Board D50TNP, M50CYP, and D40AMP Families* and *BIOS Firmware External Product Specification (EPS) for the Intel® Server Board D50TNP, M50CYP, and D40AMP Families .*

13.5 Intel® Software Guard Extensions (Intel® SGX)

Intel® Software Guard Extensions (Intel® SGX) is a set of instructions that increases the security of application code and data, giving them more protection from disclosure or modification. Developers can partition sensitive information into enclaves that are areas of execution in memory with more security protection.

Intel® SGX helps protect selected code and data from disclosure or modification. Intel® SGX helps partition applications into enclaves in memory that increase security. Enclaves have hardware-assisted confidentiality and integrity-added protections to help prevent access from processes at higher privilege levels. Through attestation services, a relying party can receive some verification on the identity of an application enclave before launch.

The Intel® Server D40AMP family provides Intel® SGX as part of the platform system security. Intel® SGX provides fine grain data protection via application isolation in memory. Data protected includes: code, transactions, IDs, keys, key material, private data, algorithms. Intel® SGX provides enhanced security protections for application data independent of operating system or hardware configuration. Intel® SGX provides the following security features:

- **Helps protect against attacks on software,** even if OS/drivers/BIOS/VMM/SMM are compromised.
- **Increases protections for secrets,** even when the attacker has full control of platform.
- **Helps prevent attacks**, such as memory bus snooping, memory tampering, and "cold boot" attacks, against memory contents in RAM.
- **Provides an option for hardware-based attestation** capabilities to measure and verify valid code and data signatures.

Intel® SGX for Intel® Xeon® Scalable processors are optimized to meet the application isolation needs of server systems in cloud environments:

- Massively increased Enclave Page Cache (EPC) size (up to 1 TB for typical 2-socket server system).
- Significant performance improvements: minimal impact vs native non-encrypted execution (significantly reduced overhead depending on workload).
- Fully software and binary-compatibility with applications written on other variants of Intel® SGX.
- Support for deployers to control which enclaves can be launched.
- Provides deployers full control over Attestation stack, compatible with Intel® Datacenter Attestation primitives.
- Full protection against cyber (software) attacks, some reduction in protection against physical attacks (no integrity/anti-replay protections) vs other Intel SGX variants.
- Designed for environments where the physical environment is still trusted.

Note: Intel® SGX can only be enabled when Intel® TME is enabled. See Section 13.4 to enable Intel® TME

To enable/disable Intel® SGX, access the BIOS Setup menu by pressing the **<F2>** key during POST. Navigate to the following menu: **Advanced > Processor Configuration**

Important Note: When either Intel® TME or Intel® TME-MT is enabled, a subset of memory RAS features and Intel® Optane™ persistent memory 200 series (if installed) will be disabled. See Table 17 for details.

For more information on Intel® SGX, see the *BIOS Setup Utility User Guide for the Intel® Server Board D50TNP, M50CYP, and D40AMP Families* and *BIOS Firmware External Product Specification (EPS) for the Intel® Server Board D50TNP, M50CYP, and D40AMP Families.*

13.6 Trusted Platform Module (TPM) Support

The Trusted Platform Module (TPM) option is a hardware-based security device that addresses the growing concern about boot process integrity and offers better data protection. TPM protects the system startup process by ensuring it is tamper-free before releasing system control to the operating system. A TPM device provides secured storage for data, such as security keys and passwords. In addition, a TPM device has encryption and hash functions. The Intel® Server Board D40AMP and Intel® Compute Module D40AMP support TPM in compliance with the *TPM PC Client Specifications revision 2.0*, published by the Trusted Computing Group (TCG).

A TPM device 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 with future measurements to verify the integrity of the boot process.

After the 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 running, it optionally uses the TPM to provide additional system and data security (for example, the BitLocker* drive encryption utility in Microsoft Windows* uses the TPM to store cryptographic keys).

Intel offers the following TPM kits for the Intel® Server Board D40AMP and Intel® Compute Module D40AMP:

- Trusted platform module 2.0 (Rest of World) – iPC **AXXTPMENC8 (accessory part)**
- Trusted platform module 2.0 (China Version) – iPC **AXXTPMCHNE8 (accessory part)**

13.6.1   Trusted Platform Module (TPM) Security BIOS

The BIOS TPM support conforms to the TCG (Trusted Computing Group) PC Client Specific Implementation Specification for Conventional BIOS, the TCG PC Client Specific TPM Interface Specification, and the Microsoft Windows BitLocker Requirements. 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 Extensible Firmware Interface (EFI) to a TPM-enabled operating system for using TPM.
- Produces Advanced Configuration and Power Interface (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 Platform Physical Presence Interface Specification*, and the *Microsoft Windows* BitLocker* Requirements* documents.

13.6.2   Physical Presence

Before administrative operations to the TPM can be executed, the operator must confirm TPM ownership by verifying their physical presence. The BIOS implements the operator presence indication by verifying the administrator password.

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

1. A 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 command, inhibits BIOS Setup entry, and boots directly to the operating system that requested the TPM command.

13.6.3   TPM Security Setup Options

The Security page in the BIOS setup utility 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.

The operator can turn TPM functionality on or off and clear the TPM ownership contents. After the requested TPM BIOS Setup operation is carried out, the TPM2 Operation field in the BIOS Setup utility 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. While using TPM, a TPM-enabled operating system or application may change the TPM state independently 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. This option is used to clear security settings for a newly initialized system or to clear a system for which the TPM ownership security key was lost.

13.7 Intel® CBnT – Converged Intel® Boot Guard and Trusted Execution Technology (Intel® TXT)

Previous generation Intel servers supported Intel® Boot Guard and Intel® Trusted Execution Technology (Intel® TXT).

<table>
<tr><td>

Intel® Boot Guard

- Provides mechanism to authenticate the initial BIOS Code, before BIOS starts
- Hardware-based Static Root of Trust for Measurement (SRTM)
- Defends against attackers replacing/modifying the platform firmware

</td><td>

Intel® TXT

- Provides the ability to attest the authenticity of a platform configuration and OS environment; Establish trust
- Hardware-based Dynamic Root of Trust for Measurement (DRTM)
- Defends against software-based attacks aimed at stealing sensitive information

</td></tr>
</table>

The two security features combined included some redundancies and inefficiencies between them. With this product generation, Intel rearchitected and fused together the two technologies into Intel® CBnT (Converged Intel® Boot Guard and Trusted Execution Technology). Combining the two technologies into one made them more efficient, eliminated redundancies between them, simplified their implementation, and provided stronger protections.

For more information, visit
https://www.intel.com/content/www/us/en/support/articles/000025873/technologies.html

13.8 Unified Extensible Firmware Interface (UEFI) Secure Boot Technology

UEFI secure boot technology defines how a platform's firmware can authenticate a digitally signed UEFI image, such as an operating system loader or a UEFI driver stored in an option ROM. This provides the capability to ensure that those UEFI images are only loaded in an owner authorized fashion and provides a common means to ensure platform security and integrity over systems running UEFI-based firmware. The Intel® Server Board D40AMP BIOS is compliant with the UEFI Specification 2.3.1 Errata C for UEFI secure boot feature.

UEFI secure boot requires native UEFI boot mode and it disables legacy Option ROM dispatch. By default, secure boot on the Intel® Server D40AMP family is disabled.

To enable / disable UEFI Secure Boot, access the BIOS Setup menu by pressing **<F2>** key during POST. Navigate to the following menu: **Boot Maintenance Manager** > **Advanced Boot Options** > **Secure Boot Configuration**.

For more information on UEFI Secure Boot Technology, see the *BIOS Setup Utility User Guide for the Intel® Server Board D50TNP, M50CYP, and D40AMP Families* and the *BIOS Firmware External Product Specification (EPS) for the Intel® Server Board D50TNP, M50CYP, and D40AMP Families.*

14. Onboard Configuration and Service Jumpers

The Intel® Server Board D40AMP includes several jumper blocks to configure, protect, or recover specific features of the server board. See the following figure to identify the location of each jumper block on the server board. The following sections describe how each jumper is used. Pin 1 of each jumper is identified by the arrowhead (▼) silkscreened on the server board next to the pin.

Ref #: AMP10053
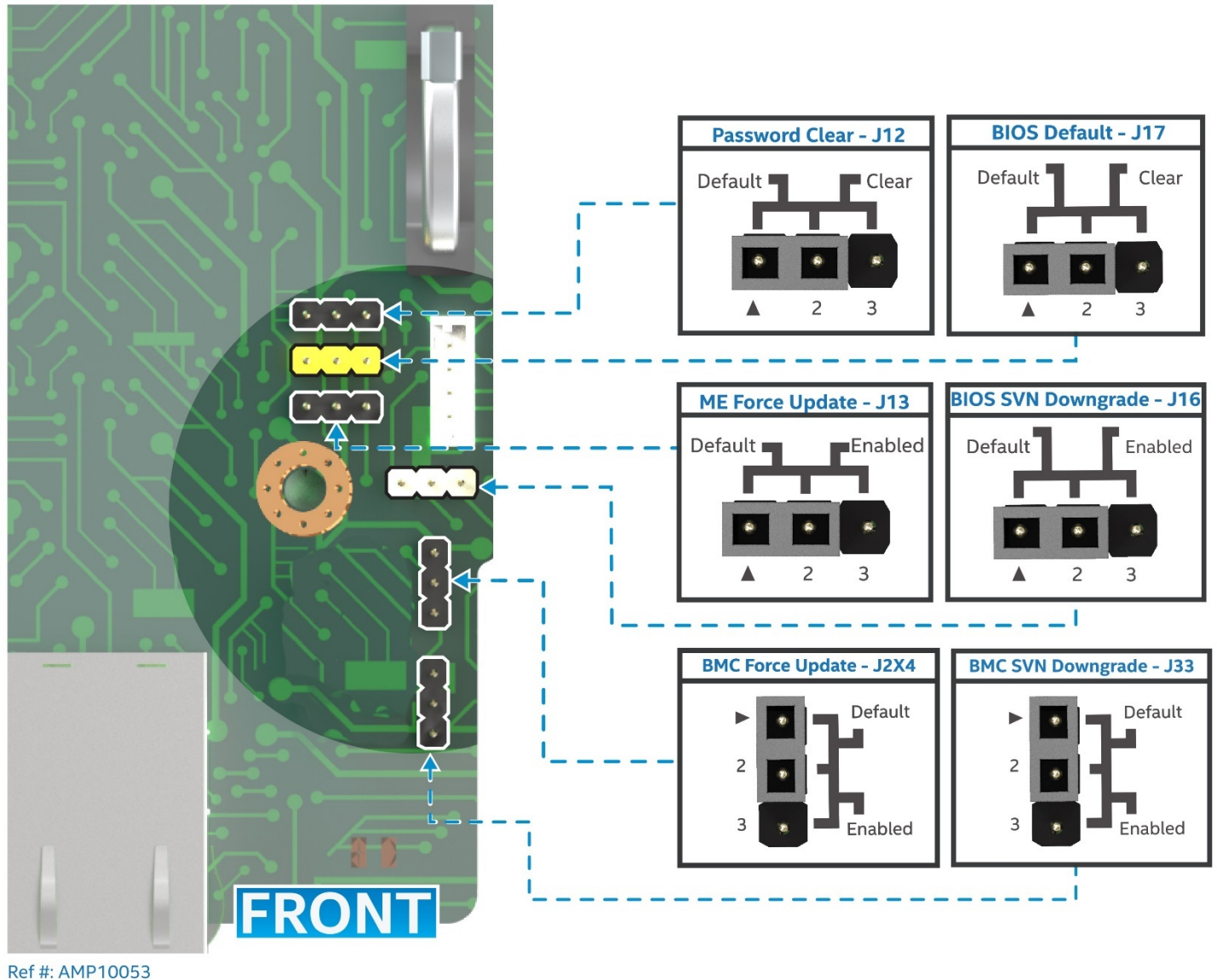
Figure 63. Reset and Recovery Jumper Block Location

14.1 BIOS Default Jumper (BIOS DFLT – J17)

This jumper resets BIOS options, configured using the BIOS Setup utility, back to their original default factory settings.

Note: This jumper does not reset administrator or user passwords. To reset passwords, the password clear jumper must be used.

To use the BIOS default jumper, perform the following steps:

1. Power down the selected compute module.
2. Remove the compute module from the chassis
3. Remove the riser assembly for riser slot #2 from the compute module.
   Refer to the *Intel® Server D40AMP family Installation and Service Guide* for instructions.
4. Move the "BIOS DFLT" (J17) jumper from pins 1–2 (normal operation) to pins 2–3 (set BIOS defaults).
5. Wait five seconds then move the "BIOS DFLT" (J17) jumper back to pins 1–2.
6. Reinstall the riser assembly.
7. Reinstall the compute module in the chassis.
8. Power on the compute module and press **<F2>** during POST to access the BIOS Setup utility to configure and save desired BIOS options.

After resetting BIOS options using the BIOS default jumper, the Error Manager Screen in the BIOS Setup utility displays two errors:

- 0012   System RTC date/time not set
- 5220   BIOS Settings reset to default settings

The system time and date will need to be reset.

14.2 Password Clear Jumper (PASSWD_CLR – J12)

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 configured 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. No method of resetting BIOS configuration settings to default values affects either the administrator or user passwords.

To use the password clear jumper, perform the following steps:

1. Power down the compute module.
2. Remove the compute module from the chassis
3. Remove the riser assemblies from the compute module.
   Refer to the *Intel® Server D40AMP family Installation and Service Guide* for instructions.
4. Move the "PASSWD_CLR" (J12) jumper from pins 1–2 (default) to pins 2–3 (password clear position).
5. Reinstall the compute module in the chassis.
6. Power on the compute module and press **<F2>** during POST to access the BIOS Setup utility.
7. Verify the password clear operation was successful by viewing the Error Manager screen. Two errors should be logged:
   o 5221   Passwords cleared by jumper
   o 5224   Password clear jumper is set
8. Exit the BIOS Setup utility and power down the compute module.
9. Remove the compute module from the chassis.

10. Move the "PASSWD_CLR" (J12) jumper back to pins 1–2 (default).
11. Reinstall the riser assemblies
12. Reinstall the compute module in the chassis.
13. Power up the module.
14. It is strongly recommended to boot into BIOS Setup immediately, navigate to the Security tab, and set the administrator and user passwords if intending to use BIOS password protection.

14.3 Intel® Management Engine (Intel® ME) Firmware Force Update Jumper (ME_FRC_UPDT – J13)

When the Intel® ME firmware force update jumper is moved from its default position, the Intel® ME is forced to operate in a reduced minimal operating capacity. This jumper should only be used if the Intel® ME firmware has gotten corrupted and requires reinstallation.

Note: The Intel® ME firmware update files are included in the system update packages (SUP) posted to Intel's download center website at http://downloadcenter.intel.com.

To use the Intel® ME firmware force update jumper, perform the following steps:

1. Power down the selected compute module.
2. Remove the compute module from the chassis
3. Remove the riser assemblies from the compute module.
   Refer to the *Intel® Server D40AMP family Installation and Service Guide* for instructions.
4. Move the "ME FRC UPDT" (J13) jumper from pins 1–2 (default) to pins 2–3 (force update position).
5. Reinstall the compute module in the chassis.
6. Power on the compute module.
7. Boot to the EFI shell.
8. Change directories to the folder containing the update files.
9. Update the Intel® ME firmware following the instructions provided with the system update package.
10. When the update has successfully completed, power off the compute module.
11. Remove the compute module from the chassis
12. Move the "ME FRC UPDT" (J13) jumper back to pins 1–2 (default).
13. Reinstall the riser assemblies.
14. Reinstall the compute module in the chassis.
15. Power on the compute module.

14.4 BMC Force Update Jumper (BMC_FRC_UPDT – J2X4)

The BMC force update jumper is used to put the BMC in boot recovery mode for a low-level update. It causes the BMC to abort its normal boot process and stay in the boot loader without executing any Linux* code. This jumper should only be used if the BMC firmware has become corrupted and requires reinstallation.

Note: The BMC firmware update files are included in the SUP posted to Intel's download center website at http://downloadcenter.intel.com.

To use the BMC force update jumper, perform the following steps:

1. Power down the selected compute module.
2. Remove the compute module from the chassis
3. Remove the riser assemblies from the compute module.
   Refer to the *Intel® Server D40AMP family Installation and Service Guide* for instructions.

4. Using tweezers, move the "BMC FRC UPDT" (J2X4) jumper from pins 1–2 (default) to pins 2–3 (force update position).
5. Reinstall the compute module in the chassis.
6. Power on the compute module.
7. Boot to the EFI shell.
8. Change directories to the folder containing the update files.
9. Update the BMC firmware following the instructions provided in the system update package.
10. When the update has successfully completed, power down the compute module.
11. Remove the compute module from the chassis.
12. Using tweezers, move the "BMC FRC UPDT" (J2X4) jumper back to pins 1–2 (default).
13. Reinstall the riser assemblies.
14. Reinstall the compute module in the chassis.
15. Power on the compute module.
16. Boot to the EFI shell.
17. Change directories to the folder containing the update files.
18. Reinstall the board/system SDR data by running the FRUSDR utility.
19. After the SDR data has been loaded, reboot the compute module.

14.5 BIOS SVN Downgrade (SVN_Bypass – J16)

The BIOS SVN Downgrade Jumper is labeled SVN_BYPASS on the server board. When this jumper is moved from its default pin position (pins 1–2), it allows the module firmware (including BIOS) in the PFR-controlled PCH capsule file to be downgraded to a lower Security Version Number (SVN). This jumper is used when there is a need for the compute module to power on using a BIOS revision with a lower SVN.

Caution: Downgrading to an older version of BIOS may result in the loss of functionality and security features that are present in a higher SVN.

Caution: When downgrading to an older version of BIOS, compute modules may end up with a firmware stack combination that is not supported, and therefore could experience unpredictable behavior.

Note: Latest system update packages are included in the SUP posted to Intel's download center website at http://downloadcenter.intel.com – When available

To use the SVN Bypass jumper, perform the following steps:

1. Power down the selected compute module.
2. Remove the compute module from the chassis
3. Remove the riser assemblies from the compute module.
   Refer to the *Intel® Server D40AMP family Installation and Service Guide* for instructions.
4. Move the "SVN_Bypass" (J16) jumper from pins 1–2 (default) to pins 2–3 (Enabled).
5. Reinstall the compute module in the chassis.
6. Power on the compute module. The system automatically boots to the EFI shell.
7. Update the BIOS using the recovery BIOS update instructions provided with the system update package.
8. After the BIOS update has successfully completed, power down the compute module.
9. Remove the compute module from the chassis.
10. Move the "SVN_Bypass" (J16) jumper back to pins 1–2 (default).
11. Reinstall the riser assemblies.
12. Reinstall the compute module in the chassis.
13. Power on the compute module. During POST, press **<F2>** to access the BIOS Setup utility to configure and save desired BIOS options.

14.6 BMC SVN Downgrade (J33)

When this jumper is moved from its default pin position (pins 1–2), it allows the compute module BMC firmware in the PFR-controlled BMC capsule file to be downgraded to a lower Security Version Number (SVN). This jumper is used when there is a need for the compute module to power on using a BMC revision with a lower SVN.

Caution: Downgrading to a BMC version with lower SVN may result in the loss of functionality and security features that are present in a higher SVN but were not implemented in the lower SVN.

Caution: When downgrading to an older version of BMC, modules may end up with a firmware stack combination that is not supported, and therefore could experience unpredictable behavior.

Note: Latest system update packages are included in the SUP posted to Intel's download center website at http://downloadcenter.intel.com – When available

To use the BMC SVN Downgrade jumper, perform the following steps:

1. Power down the selected compute module.
2. Remove the compute module from the chassis
3. Remove the riser assemblies from the compute module.
   Refer to the *Intel® Server D40AMP family Installation and Service Guide* for instructions.
4. Using tweezers, move the BMC SVN Downgrade jumper (J33) from pins 1–2 (default) to pins 2–3 (Enabled).
5. Reinstall the compute module in the chassis.
6. Power on the compute module. The system automatically boots to the EFI shell.
7. Update the BMC using the recovery BMC update instructions provided with the system update package.
8. After the BMC update has successfully completed, power down the compute module.
9. Remove the compute module from the chassis and remove the riser assemblies from the compute module.
10. Using tweezers, move the BMC SVN Downgrade jumper (J33) jumper back to pins 1–2 (default).
11. Reinstall the riser assemblies
12. Reinstall the compute module in the chassis.
13. Power on the compute module.

Appendix A. Getting Help

Available Intel support options with your Intel Server System:

1. 24x7 support through Intel's support webpage at
   https://www.intel.com/content/www/us/en/support/products/1201/server-products.html

   Information available at the support site includes:

   - Latest BIOS, firmware, drivers, and utilities
   - Product documentation, setup, and service guides
   - Full product specifications, technical advisories, and errata
   - Compatibility documentation for memory, hardware add-in cards, and operating systems
   - Server and chassis accessory parts list for ordering upgrades or spare parts
   - A searchable knowledge base to search for product information throughout the support site

   Quick Links:

Use the following links for support on Intel Server Boards and Server Systems	**Download Center** http://www.intel.com/support/downloadserversw	**BIOS Support Page** http://www.intel.com/support/serverbios	**Troubleshooting Boot Issue** http://www.intel.com/support/tsboot
Use the following links for support on Intel® Data Center Block (DCB) Integrated Systems* * Intel DCB comes pre-populated with processors, memory, storage, and peripherals based on how it was ordered through the Intel Configure to Order tool.	**Download Center** http://www.intel.com/support/downloaddcbsw	**Technical Support Documents** http://www.intel.com/support/dcb	**Warranty and Support** Infohttp://www.intel.com/support/dcbwarranty

2. If a solution cannot be found at Intel's support site, submit a service request via Intel's online service center at https://supporttickets.intel.com/servicecenter?lang=en-US. In addition, you can also view previous support requests. (Login required to access previous support requests)

3. Contact an Intel support representative using one of the support phone numbers available at https://www.intel.com/content/www/us/en/support/contact-support.html (charges may apply).

Intel also offers Partner Alliance Program members around-the-clock 24x7 technical phone support on Intel® server boards, server chassis, server RAID controller cards, and Intel® Server Management at https://www.intel.com/content/www/us/en/partner-alliance/overview.html

Note: The 24x7 support number is available after logging in to the Intel Partner Alliance website.

Warranty Information

To obtain warranty information, visit http://www.intel.com/p/en_US/support/warranty.

Appendix B. Mechanical Dimension Diagrams

This appendix provides server board, compute module, and server system dimensions. Other details like the pull out tab location for the chassis are included.

B.1   Intel® Server Board D40AMP Mechanical Dimension Diagrams

The following figure provides the server board dimensional data for the Intel® Server Board D40AMP.
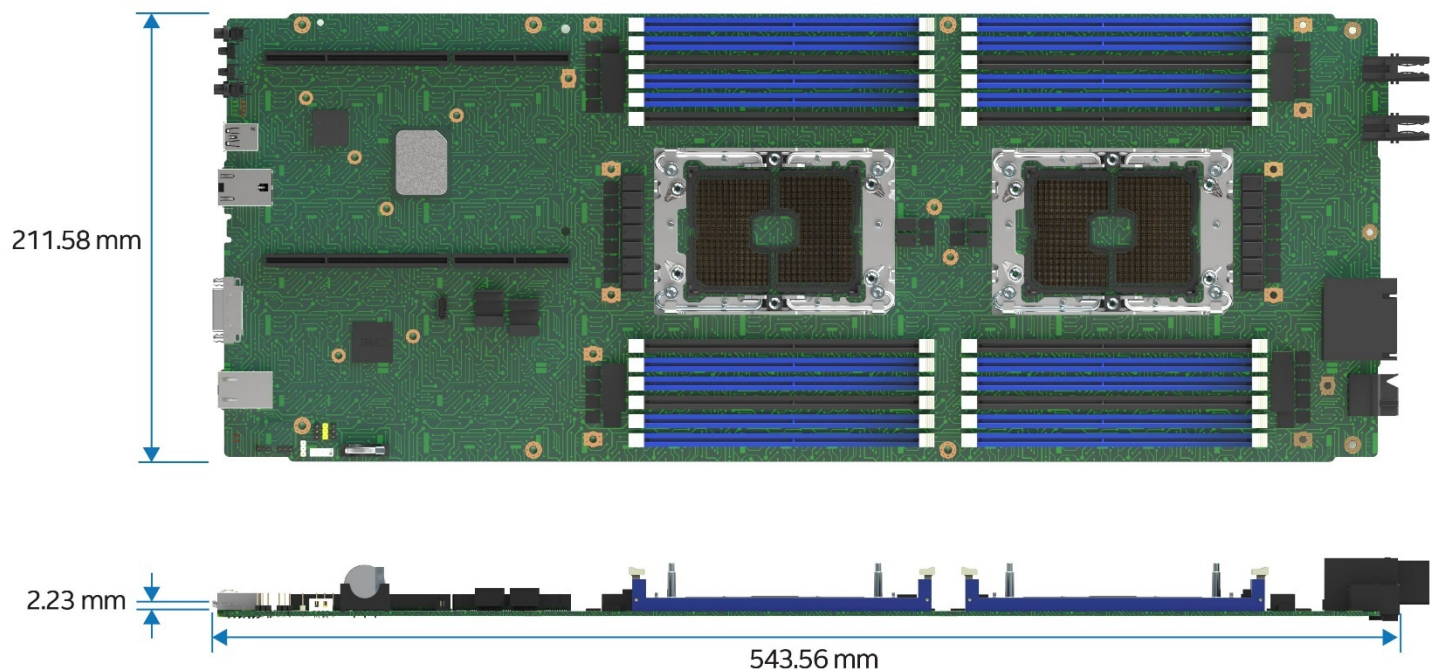
Ref #: AMP10062

Figure 64. Intel® Server Board D40AMP Dimensions

B.2 Intel® Compute Module D40AMP Dimension Diagrams

The following figure provides the dimensions for the Intel® Compute Module D40AMP.
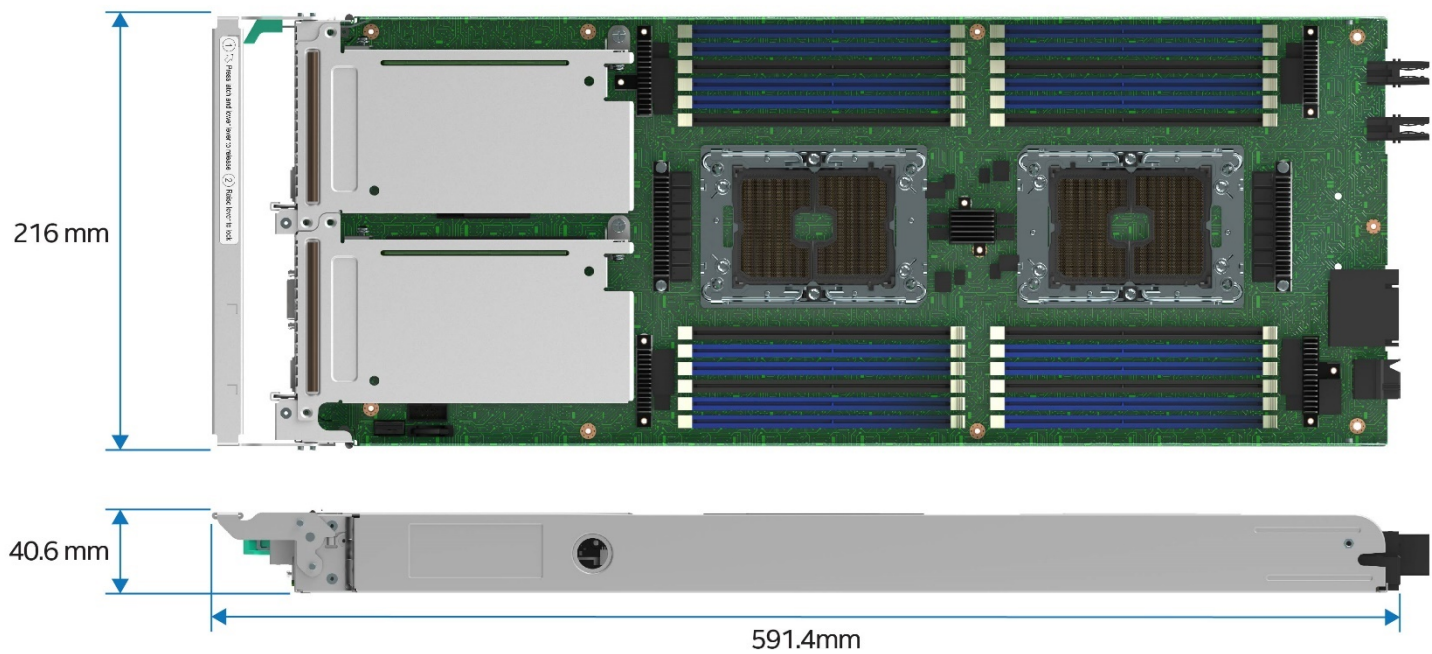
Ref #: AMP30111

Figure 65. Intel® Compute Module D40AMP Dimensions

B.3   System Chassis Dimension Diagrams

The following figure provides the server chassis dimensional data for chassis VP3U2HAC21W0 and VP3E1HAC21W0.
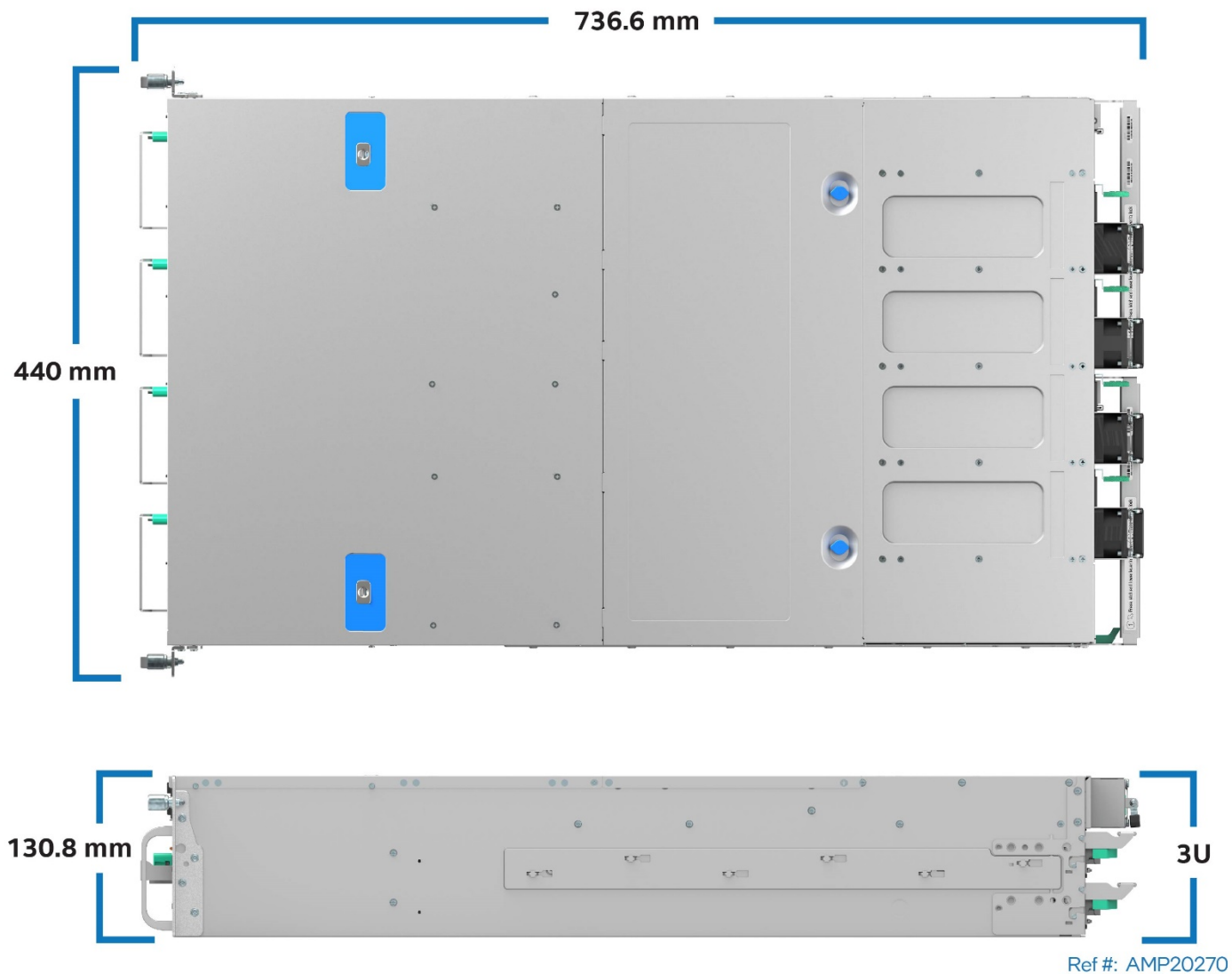
Figure 66. Intel® Server Chassis VP3000 Family Dimensions

Note: Chassis VP3U2HAC21W0 shown.

B. 4 Server Board Mechanical Drawings
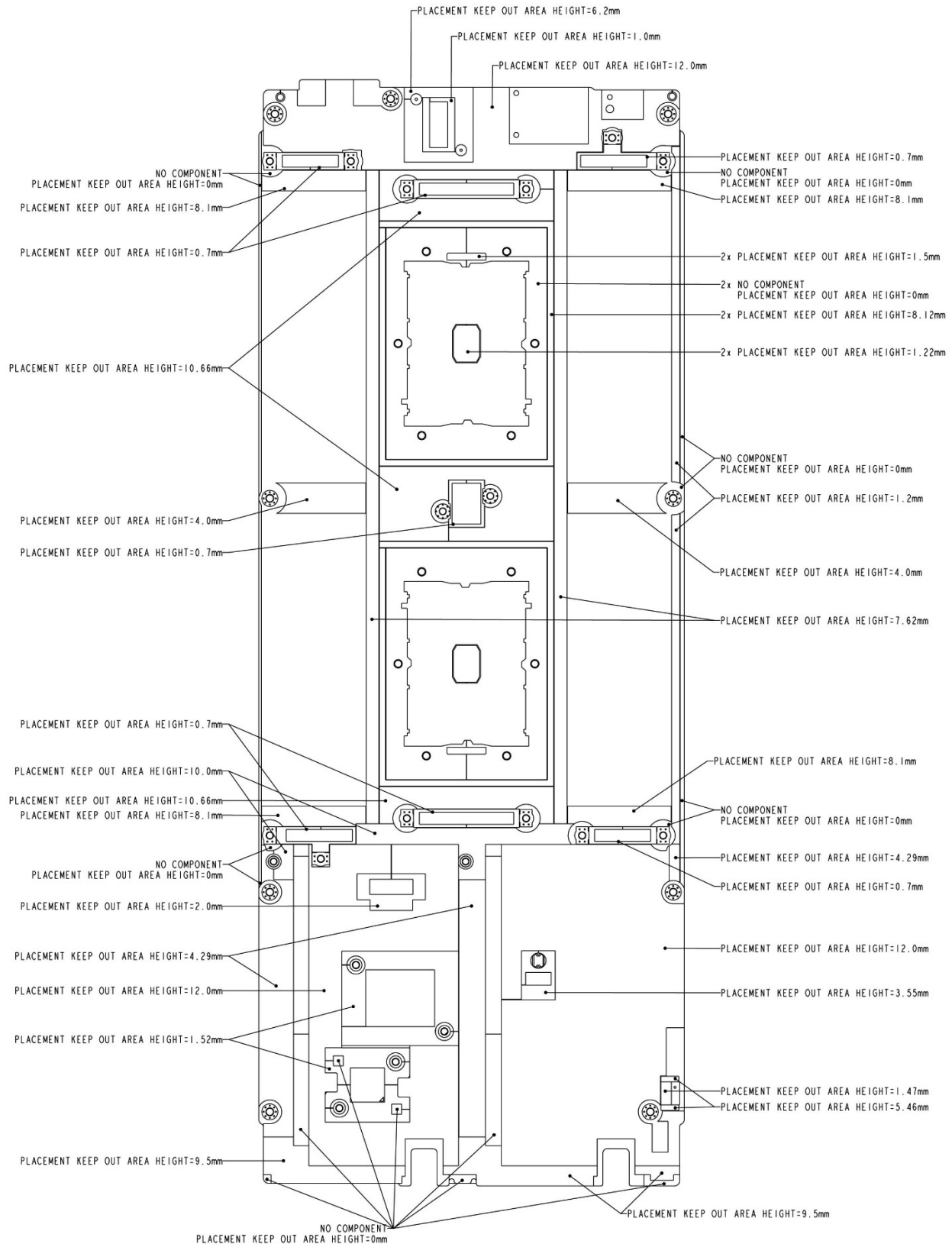
Figure 67. Intel® Server Board D40AMP Top Surface Keep Out Zone
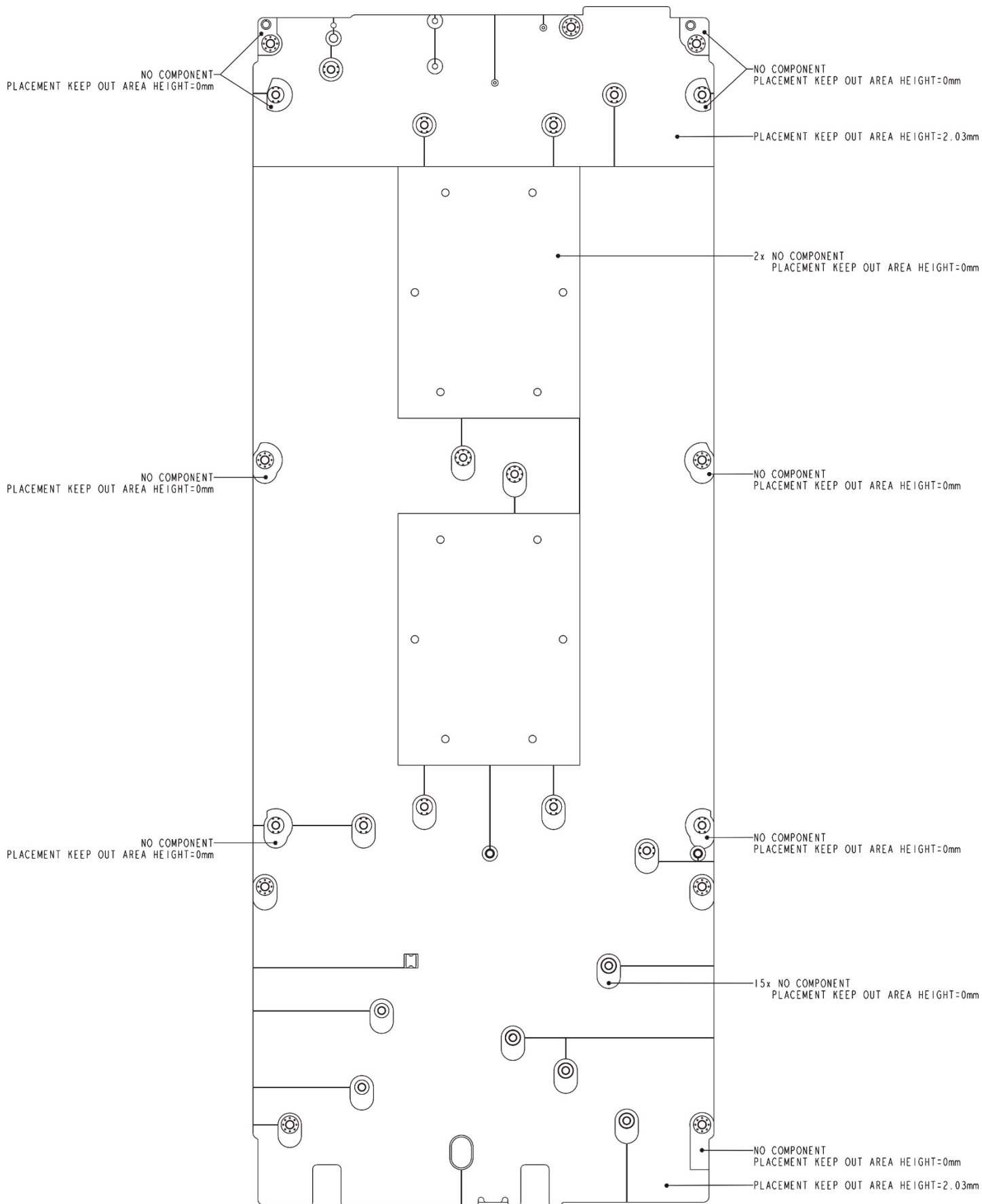
Ref #: AMP10110

Figure 68. Intel® Server Board D40AMP Bottom Surface Keep Out Zone

Figure 69. Intel® Server Board D40AMP Components Position

Figure 70. Intel® Server Board D40AMP Holes Position

113

Appendix C. Diagnostic LED Decoder

As an aid in troubleshooting a system hang that occurs during a system POST process, the server board includes a bank of eight diagnostic LEDs on the back edge of the server board.

During the system boot process, Memory Reference Code (MRC) and system BIOS execute several memory initialization and platform configuration routines, each of which is assigned a hexadecimal POST code number.

As each routine is started, the given POST code number is displayed to the 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 before the error occurred, helping to isolate the possible cause of the hang condition.

Each POST code is represented by eight LEDs, four green LEDs and four amber LEDs. 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 and the lower nibble bits are represented by green diagnostic LEDs. If the bit is set, the corresponding LED is lit. If the bit is clear, the corresponding LED is off. For each set of nibble bits, LED 0 represents the least significant bit (LSB) and LED 3 represents the most significant bit (MSB).
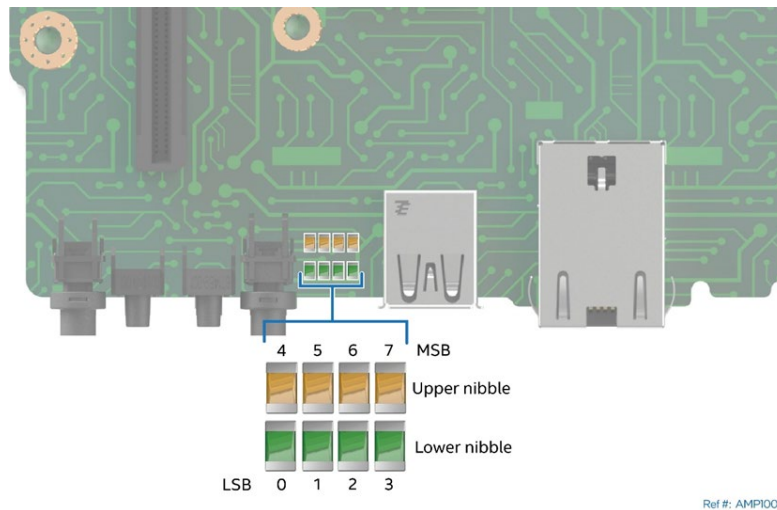
Figure 71. Onboard Diagnostic LEDs

In the following example, the BIOS sends a hexadecimal value of `AC` to the diagnostic LEDs. The LEDs are decoded as shown in the following table.

Table 37. 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**
Read Value	Binary	1	0	1	0	1	1	0	**0**
	Hexadecimal	**A**h				**C**h			
	Result	AC**h**							

Upper nibble bits = 1010b = **A**h; Lower nibble bits = 1100b = **C**h; the two Hex Nibble values are combined to create a single **AC**h POST Progress Code.

C.1   Early POST Memory Initialization MRC Diagnostic Codes

Memory initialization at the beginning of POST includes multiple functions: 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.

The MRC progress codes are displayed to the diagnostic LEDs that show the execution point in the MRC operational path at each step.

Table 38. MRC progress codes

POST Code (Hex)	Upper Nibble				Lower Nibble				Description
	8h	4h	2h	1h	8h	4h	2h	1h	
B0	1	0	1	1	0	0	0	0	Detect DIMM population
B1	1	0	1	1	0	0	0	1	Set DDR4 frequency
B2	1	0	1	1	0	0	1	0	Gather remaining SPD data
B3	1	0	1	1	0	0	1	1	Program registers on the memory controller level
B4	1	0	1	1	0	1	0	0	Evaluate RAS modes and save rank information
B5	1	0	1	1	0	1	0	1	Program registers on the channel level
B6	1	0	1	1	0	1	1	0	Perform the JEDEC defined initialization sequence
B7	1	0	1	1	0	1	1	1	Train DDR4 ranks
1	0	0	0	0	0	0	0	1	Train DDR4 ranks
2	0	0	0	0	0	0	1	0	Train DDR4 ranks – Read DQ/DQS training
3	0	0	0	0	0	0	1	1	Train DDR4 ranks – Receive enable training
4	0	0	0	0	0	1	0	0	Train DDR4 ranks – Write DQ/DQS training
5	0	0	0	0	0	1	0	1	Train DDR4 ranks – DDR channel training done
B8	1	0	1	1	1	0	0	0	Initialize CLTT/OLTT
B9	1	0	1	1	1	0	0	1	Hardware memory test and init
BA	1	0	1	1	1	0	1	0	Execute software memory init
BB	1	0	1	1	1	0	1	1	Program memory map and interleaving
BC	1	0	1	1	1	1	0	0	Program RAS configuration
BE	1	0	1	1	1	1	1	0	Execute BSSA RMT
BF	1	0	1	1	1	1	1	1	MRC is done

If a major memory initialization error occurs, preventing the system from booting with data integrity, the MRC displays 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. Table 39 lists all MRC fatal errors that are displayed to the diagnostic LEDs.

Note: Fatal MRC errors display POST error codes that may be the same as BIOS POST progress codes displayed later in the POST process.

Table 39. MRC fatal error codes

POST Code (Hex)	Upper Nibble				Lower Nibble				Description
	8h	**4h**	**2h**	**1h**	**8h**	**4h**	**2h**	**1h**	
E8	1	1	1	0	1	0	0	0	No usable memory error 01h = No memory was detected from 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. 03h = No memory installed. All channels are disabled.
E9	1	1	1	0	1	0	0	1	Memory is locked by Intel® TXT and is inaccessible
EA	1	1	1	0	1	0	1	0	DDR4 channel training error 01h = Error on read DQ/DQS (Data/Data Strobe) init 02h = Error on Receive Enable 03h = Error on Write Leveling 04h = Error on write DQ/DQS (Data/Data Strobe)
EB	1	1	1	0	1	0	1	1	Memory test failure 01h = Software memtest failure. 02h = Hardware memtest failed.
ED	1	1	1	0	1	1	0	1	DIMM configuration population error 01h = Different DIMM types (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. 05h = Unsupported DIMM Voltage.
EF	1	1	1	0	1	1	1	1	Indicates a CLTT table structure error

C.2 BIOS POST Progress Codes

The following table provides a list of all POST progress codes.

Table 40. POST progress codes

POST Code (Hex)	Upper Nibble				Lower Nibble				Description
	8h	4h	2h	1h	8h	4h	2h	1h	
SEC Phase									
01	0	0	0	0	0	0	0	1	First POST code after CPU reset
02	0	0	0	0	0	0	1	0	Microcode load begin
03	0	0	0	0	0	0	1	1	CRAM initialization begin
04	0	0	0	0	0	1	0	0	PEI Cache When Disabled
05	0	0	0	0	0	1	0	1	SEC Core At Power On Begin.
06	0	0	0	0	0	1	1	0	Early CPU initialization during SEC Phase.
UPI RC (Fully leverage without platform change)									
A1	1	0	1	0	0	0	0	1	Collect info such as SBSP, boot mode, reset type, etc.
A3	1	0	1	0	0	0	1	1	Setup minimum path between SBSP and other sockets
A6	1	0	1	0	0	1	1	0	Sync up with PBSPs
A7	1	0	1	0	0	1	1	1	Topology discovery and route calculation
A8	1	0	1	0	1	0	0	0	Program final route
A9	1	0	1	0	1	0	0	1	Program final IO SAD setting
AA	1	0	1	0	1	0	1	0	Protocol layer and other uncore settings
AB	1	0	1	0	1	0	1	1	Transition links to full speed operation
AE	1	0	1	0	1	1	1	0	Coherency settings
AF	1	0	1	0	1	1	1	1	KTI initialization done
PEI Phase									
10	0	0	0	1	0	0	0	0	PEI Core
11	0	0	0	1	0	0	0	1	CPU PEIM
15	0	0	0	1	0	1	0	1	Platform Type Init
19	0	0	0	1	1	0	0	1	Platform PEIM Init
IIO Progress Codes									
E0	1	1	1	0	0	0	0	0	Iio Early Init Entry
E1	1	1	1	0	0	0	0	1	Iio Pre-link Training
E2	1	1	1	0	0		1	0	Iio EQ Programming
E3	1	1	1	0	0	0	1	1	Iio Link Training
E4	1	1	1	0	0	1	0	0	Internal Use
E5	1	1	1	0	0	1	0	1	Iio Early Init Exit
E6	1	1	1	0	0	1	1	0	Iio Late Init Entry
E7	1	1	1	0	0	1	1	1	Iio PCIe* Ports Init
E8	1	1	1	0	1	0	0	0	Iio IOAPIC init
E9	1	1	1	0	1	0	0	1	Iio VTD Init
EA	1	1	1	0	1	0	1	0	Iio IOAT Init
EB	1	1	1	0	1	0	1	1	Iio DXF Init
EC	1	1	1	0	1	1	0	0	Iio NTB Init
ED	1	1	1	0	1	1	0	1	Iio Security Init
EE	1	1	1	0	1	1	1	0	Iio Late Init Exit
EF	1	1	1	0	1	1	1	1	Iio ready to boot

POST Code (Hex)	Upper Nibble				Lower Nibble				Description
	8h	4h	2h	1h	8h	4h	2h	1h	
MRC Progress Codes – At this point the MRC Progress Code sequence is executed.									
31	0	0	1	1	0	0	0	1	Memory Installed
32	0	0	1	1	0	0	1	0	CPU PEIM (CPU Init)
33	0	0	1	1	0	0	1	1	CPU PEIM (Cache Init)
34	0	0	1	1	0	1	0	0	CPU BSP Select
35	0	0	1	1	0	1	0	1	CPU AP Init
36	0	0	1	1	0	1	1	0	CPU SMM Init
4F	0	1	0	0	1	1	1	1	DXE IPL started
Memory Feature Progress Codes									
C1	1	1	0	0	0	0	0	1	Memory POR check
C2	1	1	0	0	0	0	1	0	Internal Use
C3	1	1	0	0	0	0	1	1	Internal Use
C4	1	1	0	0	0	1	0	0	Internal Use
C5	1	1	0	0	0	1	0	1	Memory Early Init
C6	1	1	0	0	0	1	1	0	Display DIMM info in debug mode
C7	1	1	0	0	0	1	1	1	JEDEC Nvdimm training
C9	1	1	0	0	1	0	0	1	Setup SVL and Scrambling
CA	1	1	0	0	1	0	1	0	Internal Use
CB	1	1	0	0	1	0	1	1	Check RAS support
CC	1	1	0	0	1	1	0	0	Pmem ADR Init
CD	1	1	0	0	1	1	0	1	Internal Use
CE	1	1	0	0	1	1	1	0	Memory Late Init
CF	1	1	0	0	1	1	1	1	Determine MRC boot mode
D0	1	1	0	1	0	0	0	0	MKTME Early Init
D1	1	1	0	1	0	0	0	1	SGX Early Init
D2	1	1	0	1	0	0	1	0	Memory Margin Test
D3	1	1	0	1	0	0	1	1	Internal Use
D5	1	1	0	1	0	1	0	1	Internal Use
D6	1	1	0	1	0	1	1	0	Offset Training Result
DXE Phase									
60	0	1	1	0	0	0	0	0	DXE Core started
62	0	1	1	0	0	0	1	0	DXE Setup Init
68	0	1	1	0	1	0	0	0	DXE PCI Host Bridge Init
69	0	1	1	0	1	0	0	1	DXE NB Init
6A	0	1	1	0	1	0	1	0	DXE NB SMM Init
70	0	1	1	1	0	0	0	0	DXE SB Init
71	0	1	1	1	0	0	0	1	DXE SB SMM Init
72	0	1	1	1	0	0	1	0	DXE SB devices Init
78	0	1	1	1	1	0	0	0	DXE ACPI Init
79	0	1	1	1	1	0	0	1	DXE CSM Init
7D	0	1	1	1	1	1	0	1	DXE Removable Media Detect
7E	0	1	1	1	1	1	1	0	DXE Removable Media Detected
90	1	0	0	1	0	0	0	0	DXE BDS started
91	1	0	0	1	0	0	0	1	DXE BDS connect drivers

POST Code (Hex)	Upper Nibble				Lower Nibble				Description
	8h	4h	2h	1h	8h	4h	2h	1h	
92	1	0	0	1	0	0	1	0	DXE PCI bus begin
93	1	0	0	1	0	0	1	1	DXE PCI Bus HPC Init
94	1	0	0	1	0	1	0	0	DXE PCI Bus enumeration
95	1	0	0	1	0	1	0	1	DXE PCI Bus resource requested
96	1	0	0	1	0	1	1	0	DXE PCI Bus assign resource
97	1	0	0	1	0	1	1	1	DXE CON_OUT connect
98	1	0	0	1	1	0	0	0	DXE CON_IN connect
99	1	0	0	1	1	0	0	1	DXE SIO Init
9A	1	0	0	1	1	0	1	0	DXE USB start
9B	1	0	0	1	1	0	1	1	DXE USB reset
9C	1	0	0	1	1	1	0	0	DXE USB detect
9D	1	0	0	1	1	1	0	1	DXE USB enable
A1	1	0	1	0	0	0	0	1	DXE IDE begin
A2	1	0	1	0	0	0	1	0	DXE IDE reset
A3	1	0	1	0	0	0	1	1	DXE IDE detect
A4	1	0	1	0	0	1	0	0	DXE IDE enable
A5	1	0	1	0	0	1	0	1	DXE SCSI begin
A6	1	0	1	0	0	1	1	0	DXE SCSI reset
A7	1	0	1	0	0	1	1	1	DXE SCSI detect
A8	1	0	1	0	1	0	0	0	DXE SCSI enable
AB	1	0	1	0	1	0	1	1	DXE SETUP start
AC	1	0	1	0	1	1	0	0	DXE SETUP input wait
AD	1	0	1	0	1	1	0	1	DXE Ready to Boot
AE	1	0	1	0	1	1	1	0	DXE Legacy Boot
AF	1	0	1	0	1	1	1	1	DXE Exit Boot Services
B0	1	0	1	1	0	0	0	0	RT Set Virtual Address Map Begin
B1	1	0	1	1	0	0	0	1	RT Set Virtual Address Map End
B2	1	0	1	1	0	0	1	0	DXE Legacy Option ROM init
B3	1	0	1	1	0	0	1	1	DXE Reset system
B4	1	0	1	1	0	1	0	0	DXE USB Hot plug
B5	1	0	1	1	0	1	0	1	DXE PCI BUS Hot plug
B8	1	0	1	1	1	0	0	0	PWRBTN Shutdown
B9	1	0	1	1	1	0	0	1	SLEEP Shutdown
C0	1	1	0	0	0	0	0	0	End of DXE
C7	1	1	0	0	0	1	1	1	DXE ACPI Enable
0	0	0	0	0	0	0	0	0	Clear POST Code
S3 Resume									
E0	1	1	1	0	0	0	0	0	S3 Resume PEIM (S3 started)
E1	1	1	1	0	0	0	0	1	S3 Resume PEIM (S3 boot script)
E2	1	1	1	0	0	0	1	0	S3 Resume PEIM (S3 Video Repost)
E3	1	1	1	0	0	0	1	1	S3 Resume PEIM (S3 OS wake)

Appendix D. POST Code Errors

Most error conditions encountered during POST are reported using POST error codes. These codes represent specific failures, warnings, or information. 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 handled by a diagnostic LED display with a system halt.

Table 41 lists the supported POST error codes. Each error code is assigned an error type that determines the action the BIOS takes when the error is encountered. Error types include minor, major, and fatal. The BIOS action for each is defined as follows:

- **Minor**: An error message may be displayed to the screen or to the BIOS Setup error manager and the POST error code 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**: An error message is displayed to the error manager screen and an error is logged to the SEL. If the BIOS Setup option "POST Error Pause" is enabled, operator intervention is required to continue booting the system. If the BIOS Setup option "POST Error Pause" is disabled, the system continues to boot.

  Note: For 0048 "Password check failed", the system halts and then, after the next reset/reboot, displays the error code on the error manager screen.

- **Fatal**: If the system cannot boot, POST halts and displays the following message: `Unrecoverable fatal error found. System will not boot until the error is resolved. Press <F2> to enter setup.`
  When the **<F2>** key on the keyboard is pressed, the error message is displayed on the error manager screen and an error is logged to the system event log (SEL) with the POST error code. The system cannot boot unless the error is resolved. The faulty component must be replaced. The "POST Error Pause" option setting in the BIOS Setup does not have any effect on this error.

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 determine which of the listed error codes are supported.

Table 41. POST Error Messages and Handling

Error Code	Error Message	Action message	Type
0012	System RTC date/time not set		Major
0048	Password check failed	Put right password.	Major
0140	PCI component encountered a PERR error		Major
0141	PCI resource conflict		Major
0146	PCI out of resources error	Enable Memory Mapped I/O above 4 GB item at SETUP to use 64-bit MMIO.	Major
0191	Processor core/thread count mismatch detected	Use identical CPU type.	Fatal
0192	Processor cache size mismatch detected	Use identical CPU type.	Fatal
0194	Processor family mismatch detected	Use identical CPU type.	Fatal

Error Code	Error Message	Action message	Type
0195	Processor Intel(R) UPI link frequencies unable to synchronize		Fatal
0196	Processor model mismatch detected	Use identical CPU type.	Fatal
0197	Processor frequencies unable to synchronize	Use identical CPU type.	Fatal
5220	BIOS Settings reset to default settings		Major
5221	Passwords cleared by jumper		Major
5224	Password clear jumper is Set	Recommend reminding user to install BIOS password as BIOS admin password is the master keys for several BIOS security features.	Major
8130	CPU0 disabled		Major
8131	CPU1 disabled		Major
8160	CPU0 unable to apply microcode update		Major
8161	CPU1 unable to apply microcode update		Major
8170	CPU0 failed Self-Test (BIST)		Major
8171	CPU1 failed Self-Test (BIST)		Major
8180	CPU0 microcode update not found		Minor
8181	CPU1 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	Baseboard Management Controller Sensor Data Record empty.	Update right SDR.	Major
84FF	System Event Log full	Clear SEL through EWS or SELVIEW utility.	Minor
85FC	Memory component could not be configured in the selected RAS mode		Major
8501	Memory Population Error	Plug DIMM at right population.	Major
8502	PMem invalid DIMM population found on the system.	Populate valid POR pmem DIMM population.	Major
8520	Memory failed test/initialization CPU0_DIMM_A1	Remove the disabled DIMM.	Major
8521	Memory failed test/initialization CPU0_DIMM_A2	Remove the disabled DIMM.	Major
8522	Memory failed test/initialization CPU0_DIMM_A3	Remove the disabled DIMM.	Major
8523	Memory failed test/initialization CPU0_DIMM_B1	Remove the disabled DIMM.	Major
8524	Memory failed test/initialization CPU0_DIMM_B2	Remove the disabled DIMM.	Major
8525	Memory failed test/initialization CPU0_DIMM_B3	Remove the disabled DIMM.	Major
8526	Memory failed test/initialization CPU0_DIMM_C1	Remove the disabled DIMM.	Major
8527	Memory failed test/initialization CPU0_DIMM_C2	Remove the disabled DIMM.	Major
8528	Memory failed test/initialization CPU0_DIMM_C3	Remove the disabled DIMM.	Major
8529	Memory failed test/initialization CPU0_DIMM_D1	Remove the disabled DIMM.	Major
852A	Memory failed test/initialization CPU0_DIMM_D2	Remove the disabled DIMM.	Major
852B	Memory failed test/initialization CPU0_DIMM_D3	Remove the disabled DIMM.	Major
852C	Memory failed test/initialization CPU0_DIMM_E1	Remove the disabled DIMM.	Major

Error Code	Error Message	Action message	Type
852D	Memory failed test/initialization CPU0_DIMM_E2	Remove the disabled DIMM.	Major
852E	Memory failed test/initialization CPU0_DIMM_E3	Remove the disabled DIMM.	Major
852F	Memory failed test/initialization CPU0_DIMM_F1	Remove the disabled DIMM.	Major
8530	Memory failed test/initialization CPU0_DIMM_F2	Remove the disabled DIMM.	Major
8531	Memory failed test/initialization CPU0_DIMM_F3	Remove the disabled DIMM.	Major
8532	Memory failed test/initialization CPU0_DIMM_G1	Remove the disabled DIMM.	Major
8533	Memory failed test/initialization CPU0_DIMM_G2	Remove the disabled DIMM.	Major
8534	Memory failed test/initialization CPU0_DIMM_G3	Remove the disabled DIMM.	Major
8535	Memory failed test/initialization CPU0_DIMM_H1	Remove the disabled DIMM.	Major
8536	Memory failed test/initialization CPU0_DIMM_H2	Remove the disabled DIMM.	Major
8537	Memory failed test/initialization CPU0_DIMM_H3	Remove the disabled DIMM.	Major
8538	Memory failed test/initialization CPU1_DIMM_A1	Remove the disabled DIMM.	Major
8539	Memory failed test/initialization CPU1_DIMM_A2	Remove the disabled DIMM.	Major
853A	Memory failed test/initialization CPU1_DIMM_A3	Remove the disabled DIMM.	Major
853B	Memory failed test/initialization CPU1_DIMM_B1	Remove the disabled DIMM.	Major
853C	Memory failed test/initialization CPU1_DIMM_B2	Remove the disabled DIMM.	Major
853D	Memory failed test/initialization CPU1_DIMM_B3	Remove the disabled DIMM.	Major
853E	Memory failed test/initialization CPU1_DIMM_C1	Remove the disabled DIMM.	Major
853F (Go to 85C0)	Memory failed test/initialization CPU1_DIMM_C2	Remove the disabled DIMM.	Major
8540	Memory disabled.CPU0_DIMM_A1	Remove the disabled DIMM.	Major
8541	Memory disabled.CPU0_DIMM_A2	Remove the disabled DIMM.	Major
8542	Memory disabled.CPU0_DIMM_A3	Remove the disabled DIMM.	Major
8543	Memory disabled.CPU0_DIMM_B1	Remove the disabled DIMM.	Major
8544	Memory disabled.CPU0_DIMM_B2	Remove the disabled DIMM.	Major
8545	Memory disabled.CPU0_DIMM_B3	Remove the disabled DIMM.	Major
8546	Memory disabled.CPU0_DIMM_C1	Remove the disabled DIMM.	Major
8547	Memory disabled.CPU0_DIMM_C2	Remove the disabled DIMM.	Major
8548	Memory disabled.CPU0_DIMM_C3	Remove the disabled DIMM.	Major
8549	Memory disabled.CPU0_DIMM_D1	Remove the disabled DIMM.	Major
854A	Memory disabled.CPU0_DIMM_D2	Remove the disabled DIMM.	Major
854B	Memory disabled.CPU0_DIMM_D3	Remove the disabled DIMM.	Major
854C	Memory disabled.CPU0_DIMM_E1	Remove the disabled DIMM.	Major
854D	Memory disabled.CPU0_DIMM_E2	Remove the disabled DIMM.	Major
854E	Memory disabled.CPU0_DIMM_E3	Remove the disabled DIMM.	Major
854F	Memory disabled.CPU0_DIMM_F1	Remove the disabled DIMM.	Major
8550	Memory disabled.CPU0_DIMM_F2	Remove the disabled DIMM.	Major
8551	Memory disabled.CPU0_DIMM_F3	Remove the disabled DIMM.	Major
8552	Memory disabled.CPU0_DIMM_G1	Remove the disabled DIMM.	Major
8553	Memory disabled.CPU0_DIMM_G2	Remove the disabled DIMM.	Major
8554	Memory disabled.CPU0_DIMM_G3	Remove the disabled DIMM.	Major
8555	Memory disabled.CPU0_DIMM_H1	Remove the disabled DIMM.	Major
8556	Memory disabled.CPU0_DIMM_H2	Remove the disabled DIMM.	Major
8557	Memory disabled.CPU0_DIMM_H3	Remove the disabled DIMM.	Major
8558	Memory disabled.CPU1_DIMM_A1	Remove the disabled DIMM.	Major
8559	Memory disabled.CPU1_DIMM_A2	Remove the disabled DIMM.	Major

Error Code	Error Message	Action message	Type
855A	Memory disabled.CPU1_DIMM_A3	Remove the disabled DIMM.	Major
855B	Memory disabled.CPU1_DIMM_B1	Remove the disabled DIMM.	Major
855C	Memory disabled.CPU1_DIMM_B2	Remove the disabled DIMM.	Major
855D	Memory disabled.CPU1_DIMM_B3	Remove the disabled DIMM.	Major
855E	Memory disabled.CPU1_DIMM_C1	Remove the disabled DIMM.	Major
855F (Go to 85D0)	Memory disabled.CPU1_DIMM_C2	Remove the disabled DIMM.	Major
8560	Memory encountered a Serial Presence Detection(SPD) failure.CPU0_DIMM_A1		Major
8561	Memory encountered a Serial Presence Detection(SPD) failure.CPU0_DIMM_A2		Major
8562	Memory encountered a Serial Presence Detection(SPD) failure.CPU0_DIMM_A3		Major
8563	Memory encountered a Serial Presence Detection(SPD) failure.CPU0_DIMM_B1		Major
8564	Memory encountered a Serial Presence Detection(SPD) failure.CPU0_DIMM_B2		Major
8565	Memory encountered a Serial Presence Detection(SPD) failure.CPU0_DIMM_B3		Major
8566	Memory encountered a Serial Presence Detection(SPD) failure.CPU0_DIMM_C1		Major
8567	Memory encountered a Serial Presence Detection (SPD) failure.CPU0_DIMM_C2		Major
8568	Memory encountered a Serial Presence Detection (SPD) failure.CPU0_DIMM_C3		Major
8569	Memory encountered a Serial Presence Detection(SPD) failure.CPU0_DIMM_D1		Major
856A	Memory encountered a Serial Presence Detection(SPD) failure.CPU0_DIMM_D2		Major
856B	Memory encountered a Serial Presence Detection(SPD) failure.CPU0_DIMM_D3		Major
856C	Memory encountered a Serial Presence Detection(SPD) failure.CPU0_DIMM_E1		Major
856D	Memory encountered a Serial Presence Detection(SPD) failure.CPU0_DIMM_E2		Major
856E	Memory encountered a Serial Presence Detection(SPD) failure.CPU0_DIMM_E3		Major
856F	Memory encountered a Serial Presence Detection(SPD) failure.CPU0_DIMM_F1		Major
8570	Memory encountered a Serial Presence Detection(SPD) failure.CPU0_DIMM_F2		Major
8571	Memory encountered a Serial Presence Detection(SPD) failure.CPU0_DIMM_F3		Major
8572	Memory encountered a Serial Presence Detection(SPD) failure.CPU0_DIMM_G1		Major
8573	Memory encountered a Serial Presence Detection(SPD) failure.CPU0_DIMM_G2		Major
8574	Memory encountered a Serial Presence Detection(SPD) failure.CPU0_DIMM_G3		Major
8575	Memory encountered a Serial Presence Detection(SPD) failure.CPU0_DIMM_H1		Major

Error Code	Error Message	Action message	Type
8576	Memory encountered a Serial Presence Detection(SPD) failure.CPU0_DIMM_H2		Major
8577	Memory encountered a Serial Presence Detection(SPD) failure.CPU0_DIMM_H3		Major
8578	Memory encountered a Serial Presence Detection(SPD) failure.CPU1_DIMM_A1		Major
8579	Memory encountered a Serial Presence Detection(SPD) failure.CPU1_DIMM_A2		Major
857A	Memory encountered a Serial Presence Detection(SPD) failure.CPU1_DIMM_A3		Major
857B	Memory encountered a Serial Presence Detection(SPD) failure.CPU1_DIMM_B1		Major
857C	Memory encountered a Serial Presence Detection(SPD) failure.CPU1_DIMM_B2		Major
857D	Memory encountered a Serial Presence Detection(SPD) failure.CPU1_DIMM_B3		Major
857E	Memory encountered a Serial Presence Detection(SPD) failure.CPU1_DIMM_C1		Major
857F (Go to 85E0)	Memory encountered a Serial Presence Detection(SPD) failure.CPU1_DIMM_C2		Major
85C0	Memory failed test/initialization CPU1_DIMM_C3	Remove the disabled DIMM.	Major
85C1	Memory failed test/initialization CPU1_DIMM_D1	Remove the disabled DIMM.	Major
85C2	Memory failed test/initialization CPU1_DIMM_D2	Remove the disabled DIMM.	Major
85C3	Memory failed test/initialization CPU1_DIMM_D3	Remove the disabled DIMM.	Major
85C4	Memory failed test/initialization CPU1_DIMM_E1	Remove the disabled DIMM.	Major
85C5	Memory failed test/initialization CPU1_DIMM_E2	Remove the disabled DIMM.	Major
85C6	Memory failed test/initialization CPU1_DIMM_E3	Remove the disabled DIMM.	Major
85C7	Memory failed test/initialization CPU1_DIMM_F1	Remove the disabled DIMM.	Major
85C8	Memory failed test/initialization CPU1_DIMM_F2	Remove the disabled DIMM.	Major
85C9	Memory failed test/initialization CPU1_DIMM_F3	Remove the disabled DIMM.	Major
85CA	Memory failed test/initialization CPU1_DIMM_G1	Remove the disabled DIMM.	Major
85CB	Memory failed test/initialization CPU1_DIMM_G2	Remove the disabled DIMM.	Major
85CC	Memory failed test/initialization CPU1_DIMM_G3	Remove the disabled DIMM.	Major
85CD	Memory failed test/initialization CPU1_DIMM_H1	Remove the disabled DIMM.	Major
85CE	Memory failed test/initialization CPU1_DIMM_H2	Remove the disabled DIMM.	Major
85CF	Memory failed test/initialization CPU1_DIMM_H3	Remove the disabled DIMM.	Major
85D0	Memory disabled.CPU1_DIMM_C3	Remove the disabled DIMM.	Major
85D1	Memory disabled.CPU1_DIMM_D1	Remove the disabled DIMM.	Major
85D2	Memory disabled.CPU1_DIMM_D2	Remove the disabled DIMM.	Major
85D3	Memory disabled.CPU1_DIMM_D3	Remove the disabled DIMM.	Major
85D4	Memory disabled.CPU1_DIMM_E1	Remove the disabled DIMM.	Major
85D5	Memory disabled.CPU1_DIMM_E2	Remove the disabled DIMM.	Major
85D6	Memory disabled.CPU1_DIMM_E3	Remove the disabled DIMM.	Major
85D7	Memory disabled.CPU1_DIMM_F1	Remove the disabled DIMM.	Major
85D8	Memory disabled.CPU1_DIMM_F2	Remove the disabled DIMM.	Major
85D9	Memory disabled.CPU1_DIMM_F3	Remove the disabled DIMM.	Major
85DA	Memory disabled.CPU1_DIMM_G1	Remove the disabled DIMM.	Major
85DB	Memory disabled.CPU1_DIMM_G2	Remove the disabled DIMM.	Major

Error Code	Error Message	Action message	Type
85DC	Memory disabled.CPU1_DIMM_G3	Remove the disabled DIMM.	Major
85DD	Memory disabled.CPU1_DIMM_H1	Remove the disabled DIMM.	Major
85DE	Memory disabled.CPU1_DIMM_H2	Remove the disabled DIMM.	Major
85DF	Memory disabled.CPU1_DIMM_H3	Remove the disabled DIMM.	Major
85E0	Memory encountered a Serial Presence Detection(SPD) failure.CPU1_DIMM_C3		Major
85E1	Memory encountered a Serial Presence Detection (SPD) failure. CPU1_DIMM_D1		Major
85E2	Memory encountered a Serial Presence Detection (SPD) failure.CPU1_DIMM_D2		Major
85E3	Memory encountered a Serial Presence Detection(SPD) failure.CPU1_DIMM_D3		Major
85E4	Memory encountered a Serial Presence Detection(SPD) failure.CPU1_DIMM_E1		Major
85E5	Memory encountered a Serial Presence Detection(SPD) failure.CPU1_DIMM_E2		Major
85E6	Memory encountered a Serial Presence Detection(SPD) failure.CPU1_DIMM_E3		Major
85E7	Memory encountered a Serial Presence Detection (SPD) failure.CPU1_DIMM_F1		Major
85E8	Memory encountered a Serial Presence Detection(SPD) failure.CPU1_DIMM_F2		Major
85E9	Memory encountered a Serial Presence Detection(SPD) failure.CPU1_DIMM_F3		Major
85EA	Memory encountered a Serial Presence Detection(SPD) failure.CPU1_DIMM_G1		Major
85EB	Memory encountered a Serial Presence Detection (SPD) failure. CPU1_DIMM_G2		Major
85EC	Memory encountered a Serial Presence Detection(SPD) failure.CPU1_DIMM_G3		Major
85ED	Memory encountered a Serial Presence Detection(SPD) failure.CPU1_DIMM_H1		Major
85EE	Memory encountered a Serial Presence Detection(SPD) failure.CPU1_DIMM_H2		Major
85EF	Memory encountered a Serial Presence Detection(SPD) failure.CPU1_DIMM_H3		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
8607	Recovery boot has been initiated. Note: The Primary BIOS image may be corrupted or the system may hang during POST. A BIOS update is required.		Fatal
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 Services driver: Not enough memory available to shadow a Legacy Option ROM.	Disable oprom at SETUP to save runtime memory.	Minor

D.1   Processor Initialization Error Summary

Table 42 describes mixed processor conditions and actions for all Intel server boards and Intel server systems designed with the Intel® Xeon® Scalable processor family architecture. The errors fall into one of the following categories:

- **Fatal**: If the system cannot boot, POST halts and displays the following message:

  ```
  Unrecoverable fatal error found. System will not boot until the error is resolved
  Press <F2> to enter setup
  ```

  When the **<F2>** key on the keyboard is pressed, the BIOS Setup Error Message is displayed on the BIOS Setup Error Manager screen. An error is logged to the system event log (SEL) with the POST error code.

  The "POST Error Pause" option setting in the BIOS Setup does not have any effect on this error.

  If the system is not able to boot, the system generates a beep code consisting of three long beeps and one short beep. The system cannot boot unless the error is resolved. The faulty component must be replaced.

  The system status LED is set to a steady amber color for all fatal errors that are detected during processor initialization. A steady amber system status LED indicates that an unrecoverable system failure condition has occurred.

- **Major**: An error message is displayed to the BIOS Setup Error Message screen and an error is logged to the SEL. If the BIOS Setup option "POST Error Pause" is enabled, operator intervention is required to continue booting the system. If the BIOS Setup option "POST Error Pause" is disabled, the system continues to boot.

- **Minor**: An error message may be displayed to the screen or to the BIOS Setup Error Manager and the POST error code 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.

Table 42. Mixed Processor Configurations Error Summary

Error	Severity	System Action when BIOS Detects the Error Condition
Processor family not identical	Fatal	• Halts at POST code 0xE6. • Halts with three long beeps and one short beep. • Takes fatal error action (see above) and does not boot until the fault condition is remedied.
Processor model not identical	Fatal	• Logs the POST error code into the SEL. • Alerts the BMC to set the system status LED to steady amber. • Displays 0196: Processor model mismatch detected message in the error manager. • Takes fatal error action (see above) and does not boot until the fault condition is remedied.
Processor cores/threads not identical	Fatal	• Halts at POST code 0xE5. • Halts with three long beeps and one short beep. • Takes fatal error action (see above) and does not boot until the fault condition is remedied.
Processor cache or home agent not identical	Fatal	• Halts at POST code 0xE5. • Halts with three long beeps and one short beep. • Takes fatal error action (see above) and does not boot until the fault condition is remedied.

Error	Severity	System Action when BIOS Detects the Error Condition
Processor frequency (speed) not identical	Fatal	If the frequencies for all processors can be adjusted to be the same: • Adjusts all processor frequencies to the highest common frequency. • Does not generate an error – this is not an error condition. • Continues to boot the system successfully. If the frequencies for all processors cannot be adjusted to be the same: • Logs the POST error code into the SEL. • Alerts the BMC to set the system status LED to steady amber. • Does not disable the processor. • Displays 0197: Processor speeds unable to synchronize message in the error manager. • Takes fatal error action (see above) and does not boot until the fault condition is remedied
Processor Intel® UPI link frequencies not identical	Fatal	If the link frequencies for all Intel® Ultra Path Interconnect (Intel® UPI) links can be adjusted to be the same: • Adjusts all Intel® UPI interconnect link frequencies to highest common frequency. • Does not generate an error – this is not an error condition. • Continues to boot the system successfully. If the link frequencies for all Intel® UPI links cannot be adjusted to be the same: • Logs the POST error code into the SEL. • Alerts the BMC to set the system status LED to steady amber. • Does not disable the processor. • Displays 0195: Processor Intel(R) UPII link frequencies unable to synchronize message in the error manager. • Takes fatal error action (see above) and does not boot until the fault condition is remedied.
Processor microcode update failed	Major	• Logs the POST error code into the SEL. • Displays 816x: Processor 0x unable to apply microcode update message in the error manager or on the screen. • Takes major error action. The system may continue to boot in a degraded state, depending on the "POST Error Pause" setting in setup, or may halt with the POST error code in the error manager waiting for operator intervention.
Processor microcode update missing	Minor	• Logs the POST error code into the SEL. • Displays 818x: Processor 0x microcode update not found message in the error manager or on the screen. • The system continues to boot in a degraded state, regardless of the "POST Error Pause" setting in setup.

Appendix E. System Configuration Table for Thermal Compatibility

This appendix provides tables listing system configuration compatibility data based on various supported system operating thermal limits. Section E.1 identifies supported system configurations while the system is in "normal" operating mode, meaning that all systems fans are present, on-line, and operational. Section E.2 identifies supported system configurations while the system is in a "fan fail" mode, meaning more than one fan rotor in the same fan or different fans are no longer operational and fan redundancy is lost.

E.1   Normal Operating Mode

For the tables in this section, a bullet (●) indicates full support without limitation. A cell with a number indicates conditional support. See the following notes. A blank cell indicates that the configuration is not supported.

The following list of notes support criteria associated with specific configurations identified in the following tables.

Notes:
1. The 27°C configuration guidance is limited to be used at an altitude of 900m or less. When operating at an altitude higher than 900m, The ASHRAE Class2 guidance must be followed.
2. Processor and Memory throttling (over spec ≦10C) may occur which may impact system performance.
3. Processor and Memory heavy throttling (over spec >10C) may occur, which may impact system performance.
4. SSD Throughput throttling is expected when the SSD SMART thermal sensor exceeds 70C.

Table 43. Thermal Configuration Matrix – Normal Operating Mode

Thermal Configuration Matrix – Normal Operating Mode "●" = Full Support without limitation "4,5" (Cell with number) = Conditional support with limitation (See notes above) " " (Blank) = No support			Systems Configured with chassis VP3U2HAC21W0							Systems Configured with chassis VP3E1HAC21W0							
ASHRAE (See Note 1)	Classifications		15°C	20°C	25°C	27°C	32°C	A2	A3	A4	15°C	20°C	25°C	27°C	32°C	A2	A3	A4
	Max Ambient		15°C	20°C	25°C	27°C(1)	32°C	35°C	40°C	45°C	15°C	20°C	25°C	27°C(1)	32°C	35°C	40°C	45°C
PSU	2100W		●	●	●	●	●	●			●	●	●	●	●	●		
3rd Gen Intel® Xeon® Scalable Processors	205W	18C Intel(R) Xeon(R) Gold 6354	●	●	2	2					●	●	2	2				
		16C Intel(R) Xeon(R) Gold 6346	●	●	2	2					●	●	2	2				
		32C Intel(R) Xeon(R) Gold 6338	●	●	●	●					●	●	●	●				
		28C Intel(R) Xeon(R) Gold 6330	●	●	●	●					●	●	●	●				

Thermal Configuration Matrix – Normal Operating Mode "●" = Full Support without limitation "4,5" (Cell with number) = Conditional support with limitation (See notes above) " " (Blank) = No support		Systems Configured with chassis VP3U2HAC21W0								Systems Configured with chassis VP3E1HAC21W0							
ASHRAE (See Note 1)	Classifications	15°C	20°C	25°C	27°C	32°C	A2	A3	A4	15°C	20°C	25°C	27°C	32°C	A2	A3	A4
	Max Ambient	15°C	20°C	25°C	27°C(1)	32°C	35°C	40°C	45°C	15°C	20°C	25°C	27°C(1)	32°C	35°C	40°C	45°C
	32C Intel(R) Xeon(R) Gold 6314U	●	●	●	●					●	●	●	●				
	32C Intel(R) Xeon(R) Platinum 8352Y	●	●	●	●					●	●	●	●				
	32C Intel(R) Xeon(R) Platinum 8352S	●	●	●	●					●	●	●	●				
195W	36C Intel(R) Xeon(R) Platinum 8352V, CSP	●	●	●	●	2	2			●	●	●	●	2	2		
185W	32C Intel(R) Xeon(R) Gold 6338N, NFV	●	●	●	●	●	●			●	●	●	●	●	●		
	32C Intel(R) Xeon(R) Gold 8352M	●	●	●	●	2	2			●	●	●	●	2	2		
165W	28C Intel(R) Xeon(R) Gold 6330N, NFV	●	●	●	●	●	●			●	●	●	●	●	●		
	26C Intel(R) Xeon(R) Gold 5320	●	●	●	●	2	2			●	●	●	●	2	2		
185W	24C Intel(R) Xeon(R) Gold 6336Y	●	●	●	●	●	2			●	●	●	●	2	2		
	24C Intel(R) Xeon(R) Gold 6312U	●	●	●	●	●	2			●	●	●	●	2	2		
	16C Intel(R) Xeon(R) Gold 6326	●	●	●	●	2	2			●	●	●	●	2	2		
	8C Intel(R) Xeon(R) Gold 6334	●	●	2	2	3	3			●	●	2	2	3			
165W	24C Intel(R) Xeon(R) Gold 5318S	●	●	●	●	●	●			●	●	●	●	●	●		
	24C Intel(R) Xeon(R) Gold 5118Y	●	●	●	●	●	●			●	●	●	●	●	●		
	24C Intel(R) Xeon(R) Gold 6338T, 10-year use + NEBS-friendly	●	●	●	●	2	2			●	●	●	2	2	2		
	20C Intel(R) Xeon(R) Gold 5320T	●	●	●	●	2	2			●	●	●	●	2	2		
150W	20C Intel(R) Xeon(R) Silver 4316	●	●	●	●	●	●			●	●	●	●	●	●		
	12C Intel(R) Xeon(R) Gold 5317	●	●	●	●	●	●			●	●	●	●	●	●		
	24C Intel(R) Xeon(R) Gold 5318N	●	●	●	●	●	●			●	●	●	●	●	●		

Thermal Configuration Matrix – Normal Operating Mode "●" = Full Support without limitation "4,5" (Cell with number) = Conditional support with limitation (See notes above) " " (Blank) = No support			Systems Configured with chassis VP3U2HAC21W0								Systems Configured with chassis VP3E1HAC21W0							
ASHRAE (See Note 1)	Classifications		15°C	20°C	25°C	27°C	32°C	A2	A3	A4	15°C	20°C	25°C	27°C	32°C	A2	A3	A4
	Max Ambient		15°C	20°C	25°C	27°C(1)	32°C	35°C	40°C	45°C	15°C	20°C	25°C	27°C(1)	32°C	35°C	40°C	45°C
	140W	8C Intel(R) Xeon(R) Gold 5315Y	●	●	●	●	●	●			●	●	●	●	●	●		
	135W	16C Intel(R) Xeon(R) Silver 4314	●	●	●	●	●	●			●	●	●	●	●	●		
	120W	12C Intel(R) Xeon(R) Silver 4310	●	●	●	●	●	●			●	●	●	●	●	●		
	105W	8C Intel(R) Xeon(R) Silver 4309Y	●	●	●	●	●	●			●	●	●	●	●	●		
		10C Intel(R) Xeon(R) Silver 4310T, 10-year use + NEBS-friendly	●	●	●	●	●	●			●	●	●	●	●	●		
Memory Type	LRDIMM QRx4 (16Gb) - 2DPC 13w		●	●	●	●	●	●			●	●	●	●	●	●		
	LR-DIMM 8Rx4 - 2DPC 16w		●	●	●	●	●	●			●	●	●	●	●	●		
	LRDIMM QRx4 - 2DPC 12w		●	●	●	●	●	●			●	●	●	●	●	●		
	RDIMM-DRx4 - 2DPC 7w		●	●	●	●	●	●			●	●	●	●	●	●		
	RDIMM-DRx8 - 2DPC 4w		●	●	●	●	●	●			●	●	●	●	●	●		
	RDIMM SRx4 - 2DPC 5w		●	●	●	●	●	●			●	●	●	●	●	●		
	RDIMM SRx8 -2DPC 3w		●	●	●	●	●	●			●	●	●	●	●	●		
Intel® Optane™ PMem 200 series	128 Gb (TDP=12W)		●	●	●	●	●	●			●	●	●	●	●	●		
	256 GB (TDP=15W)		●	●	●	●	●	●			●	●	●	●	●	●		
	512 GB (TDP=15W)		●	●	●	●	●	●			●	●	●	●	●	●		
Add-in Cards	Riser #1 - 100LFM		●	●	●	●	●	●			●	●	●	●	●	●		
	Riser #1 - 200LFM		●	●	●	●	●	●			●	●	●	●	●	●		
	Riser #1 - 300LFM		●	●	●	●	●	●			●	●	●	●	●	●		
	Riser #2 - 100LFM		●	●	●	●	●	●			●	●	●	●	●	●		
	Riser #2 - 200LFM		●	●	●	●	●	●			●	●	●	●	●	●		
	Riser #2 - 300LFM		●	●	●	●	●	●			●	●	●	●	●	●		
M.2 SSD (rated to 70C)	Riser #1		●	●	●	●	●	●			●	●	●	●	●	●		
	Riser #2		●	●	●	●	●	4			●	●	●	●	●	4		
Intel® SSD DC (E1.L)	D5-P4326 Series (rated to 70C)		N/A	N/A	N/A	N/A	N/A	N/A			●	●	●	●	●	●		
	DC P4510 Series (rated to 70C)		N/A	N/A	N/A	N/A	N/A	N/A			●	●	●	●	●	●		
2.5" PCIe* NVMe* SSD (rated to 70C)	U.2 SSD (TDP=25W)		●	●	●	●	●	●			N/A	N/A	N/A	N/A	N/A	N/A		

E.2 Fan Fail Mode

For the tables in this section, a bullet (●) indicates full support without limitation. A cell with a number indicates conditional support. See the following notes. A blank cell indicates that the configuration is not supported.

The following list of notes support criteria associated with specific configurations identified in the following tables.

Notes:

1. The 27°C configuration guidance is limited to be used at an altitude of 900m or less. When operating at an altitude higher than 900m, The ASHRAE Class2 guidance must be followed.
2. Processor and Memory throttling (over spec ≦10C) may occur which may impact system performance.
3. Processor and Memory heavy throttling (over spec >10C) may occur, which may impact system performance.
4. SSD Throughput throttling is expected when the SSD SMART thermal sensor exceeds 70C.

Table 44. "Thermal Configuration Matrix – Fan Fail Mode

Thermal Configuration Matrix – Fan Fail Mode "●" = Full Support without limitation "2,3" (Cell with number) = Conditional support with limitation (See notes above) " " (Blank) = No support		Systems Configured with chassis VP3U2HAC21W0								Systems Configured with chassis VP3E1HAC21W0 (TBD)							
ASHRAE (See note 1)	**Classifications**	15°C	20°C	25°C	27°C	32°C	A2	A3	A4	15°C	20°C	25°C	27°C	32°C	A2	A3	A4
	Max Ambient	15°C	20°C	25°C	27°C(1)	32°C	35°C	40°C	45°C	15°C	20°C	25°C	27°C(1)	32°C	35°C	40°C	45°C
PSU	2100W	●	●	●	●	●	●										
205W	18C Intel(R) Xeon(R) Gold 6354	●	2	3	3												
	16C Intel(R) Xeon(R) Gold 6346	●	2	3	3												
	32C Intel(R) Xeon(R) Gold 6338	●	●	2	3												
	28C Intel(R) Xeon(R) Gold 6330	●	●	2	2												
	32C Intel(R) Xeon(R) Gold 6314U	●	●	2	2												
	32C Intel(R) Xeon(R) Platinum 8352Y	●	●	2	2												
	32C Intel(R) Xeon(R) Platinum 8352S	●	●	2	2												
195W	36C Intel(R) Xeon(R) Platinum 8352V, CSP	●	●	2	2	3											

Thermal Configuration Matrix – Fan Fail Mode "●" = Full Support without limitation "2,3" (Cell with number) = Conditional support with limitation (See notes above) " " (Blank) = No support			Systems Configured with chassis VP3U2HAC21W0								Systems Configured with chassis VP3E1HAC21W0 (TBD)							
ASHRAE (See note 1)	**Classifications**		15°C	20°C	25°C	27°C	32°C	A2	A3	A4	15°C	20°C	25°C	27°C	32°C	A2	A3	A4
	Max Ambient		15°C	20°C	25°C	27°C(1)	32°C	35°C	40°C	45°C	15°C	20°C	25°C	27°C(1)	32°C	35°C	40°C	45°C
	185W	32C Intel(R) Xeon(R) Gold 6338N, NFV	●	●	●	●	2	2										
		32C Intel(R) Xeon(R) Gold 8352M	●	●	2	2	3											
	165W	28C Intel(R) Xeon(R) Gold 6330N, NFV	●	●	●	●	●	●										
	185W	26C Intel(R) Xeon(R) Gold 5320	●	●	2	2	3											
		24C Intel(R) Xeon(R) Gold 6336Y	●	●	2	2	3											
		24C Intel(R) Xeon(R) Gold 6312U	●	●	2	2	3											
		16C Intel(R) Xeon(R) Gold 6326	●	●	2	2	3											
	165W	8C Intel(R) Xeon(R) Gold 6334	●	2	3													
		24C Intel(R) Xeon(R) Gold 5318S	●	●	●	●	●	●										
		24C Intel(R) Xeon(R) Gold 5118Y	●	●	●	●	●	●										
		24C Intel(R) Xeon(R) Gold 6338T, 10-year use + NEBS-friendly	●	●	2	2	3											
	150W	20C Intel(R) Xeon(R) Gold 5320T	●	●	2	2	3											
		20C Intel(R) Xeon(R) Silver 4316	●	●	●	●	●	●										
		12C Intel(R) Xeon(R) Gold 5317	●	●	●	●	●	●										
		24C Intel(R) Xeon(R) Gold 5318N	●	●	●	●	●	●										
	140W	8C Intel(R) Xeon(R) Gold 5315Y	●	●	●	●	●	●										
	135W	16C Intel(R) Xeon(R) Silver 4314	●	●	●	●	●	●										
	120W	12C Intel(R) Xeon(R) Silver 4310	●	●	●	●	●	●										

Thermal Configuration Matrix – Fan Fail Mode "●" = Full Support without limitation "2,3" (Cell with number) = Conditional support with limitation (See notes above) " " (Blank) = No support			Systems Configured with chassis VP3U2HAC21W0								Systems Configured with chassis VP3E1HAC21W0 (TBD)							
ASHRAE (See note 1)	**Classifications**		15°C	20°C	25°C	27°C	32°C	A2	A3	A4	15°C	20°C	25°C	27°C	32°C	A2	A3	A4
	Max Ambient		15°C	20°C	25°C	27°C(1)	32°C	35°C	40°C	45°C	15°C	20°C	25°C	27°C(1)	32°C	35°C	40°C	45°C
	105W	8C Intel(R) Xeon(R) Silver 4309Y	●	●	●	●	●	●										
	105W	10C Intel(R) Xeon(R) Silver 4310T, 10-year use + NEBS-friendly	●	●	●	●	●	●										
Memory Type	LRDIMM QRx4 (16Gb) - 2DPC 13w		●	●	●	●	●	●										
	LR-DIMM 8Rx4 - 2DPC 16w		●	●	●	●	2	3										
	LRDIMM QRx4 - 2DPC 12w		●	●	●	●	●	2										
	RDIMM-DRx4 - 2DPC 7w		●	●	●	●	●	●										
	RDIMM-DRx8 - 2DPC 4w		●	●	●	●	●	●										
	RDIMM SRx4 - 2DPC 5w		●	●	●	●	●	●										
	RDIMM SRx8 -2DPC 3w		●	●	●	●	●	●										
Intel® Optane™ PMem 200 series	128 Gb (TDP=12W)		●	●	●	●	●	●										
	256 GB (TDP=15W)		●	●	●	●	2	2										
	512 GB (TDP=15W)		●	●	●	●	2	2										
Add-in Cards	Riser #1 - 100LFM		●	●	●	●	●	●										
	Riser #1 - 200LFM		●	●	●	●	●											
	Riser #1 - 300LFM		●	●	●													
	Riser #2 - 100LFM		●	●	●	●	●	●										
	Riser #2 - 200LFM		●	●	●	●	●											
	Riser #2 - 300LFM		●	●	●													
M.2 SSD (rated to 70C)	Riser #1		●	●	●	●	●	4										
	Riser #2		●	●														
Intel® SSD DC (E1.L)	D5-P4326 Series (rated to 70C)		N/A	N/A	N/A	N/A	N/A	N/A										
	DC P4510 Series (rated to 70C)		N/A	N/A	N/A	N/A	N/A	N/A										
2.5" PCIe* NVMe* SSD (rated to 70C)	U.2 SSD (TDP=25W)		●	●	●	●	4	4										

Appendix F. Board Sensors

The following figure provides the location of the sensors on the Intel® Server Board D40AMP. The following table provides a list of the sensors.
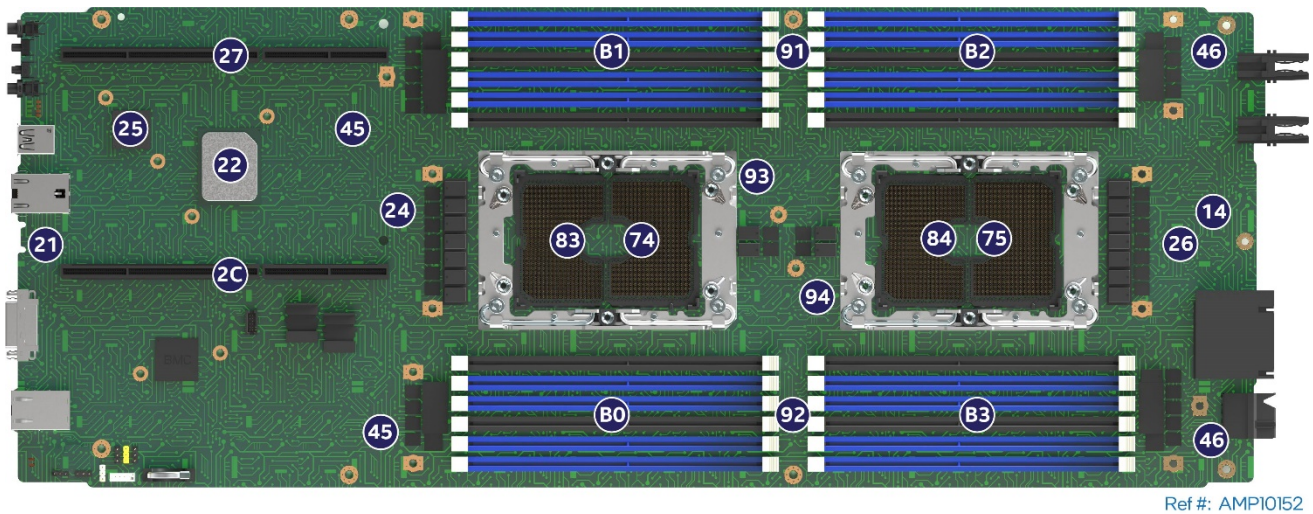
Figure 72. Board Sensor Map

Note: Numbers in the figure are hexadecimal numbers.

Table 45. Available Sensors Monitored by the BMC

Sensor Number	Sensor Name
14h	Baseboard Inlet Temperature
21h	Baseboard Outlet Temperature
22h	PCH Temp
24h	CPU0 VCCIN
26h	CPU1 VCCIN
25h	Integrated LAN controller Temperature
27h	PCI Riser 1 Temperature
2Ch	PCI Riser 2 Temperature
45h	Memory CPU0 VR Temperature
46h	Memory CPU1 VR Temperature
74h	CPU0 Therm Margin
75h	CPU1 Therm Margin
83h	CPU0 DTS Therm Margin
84h	CPU1 DTS Therm Margin
91h	CPU0 VCCIO
92h	CPU1 VCCIO
93h	CPU0 VCCANA
94h	CPU1 VCCANA
B0h	DIMM Aggregate Margin CPU0 ABCD
B1h	DIMM Aggregate Margin CPU0 EFGH
B2h	DIMM Aggregate Margin CPU1 ABCD
B3h	DIMM Aggregate Margin CPU1 EFGH

Appendix G. Server Board Installation and Component Replacement

This appendix provides general information necessary to install the server board into a server chassis. The system integrator should reference and follow all available system assembly instructions provided by the chassis manufacturer for full system assembly instructions.

This appendix also provides instructions for processor and memory replacement. Replacement instructions for all other system options should be provided by the chassis or system manufacturer.

Safety Warnings

Heed safety instructions: Before working with your server product, whether you are using this guide or any other resource as a reference, pay close attention to the safety instructions. You must adhere to the assembly instructions in this guide to ensure and maintain compliance with existing product certifications and approvals. Use only the described, regulated components specified in this guide. Use of other products/components will void the UL listing and other regulatory approvals of the product and will most likely result in noncompliance with product regulations in one or more regions in which the product is sold.

System power on/off: The power button DOES NOT turn off the system AC power. To remove power from the system, you must unplug the AC power cord. Make sure the AC power cord is unplugged before you open the chassis, add, or remove any components.

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

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

Electrostatic Discharge (ESD)

Electrostatic discharge can damage the computer or the components within it. ESD can occur without the user feeling a shock while working inside the system chassis or while improperly handling electronic devices like processors, memory or other storage devices, and add-in cards.


Intel recommends the following steps be taken when performing any procedures described within this document or while performing service to any computer system.

- Where available, all system integration and/or service should be performed at a properly equipped ESD workstation

- Wear ESD protective gear like a grounded antistatic wrist strap, sole grounders, and/or conductive shoes
- Wear an anti-static smock or gown to cover any clothing that may generate an electrostatic charge
- Remove all jewelry
- Disconnect all power cables and cords attached to the server before performing any integration or service
- Touch any unpainted metal surface of the chassis before performing any integration or service
- Hold all circuit boards and other electronic components by their edges only
- After removing electronic devices from the system or from their protective packaging, place them component side up on to a grounded anti-static surface or conductive workbench pad. Do not place electronic devices on to the outside of any protective packaging.

G.1   Server Board Installation Guidelines

This section provides general guidelines and recommendations for installing the server board into a server chassis. However, Intel highly recommends that system integrators follow all installation guidelines and instructions provided by the chassis manufacturer when integrating the server board into the chosen chassis.

Ref #:AMP10160
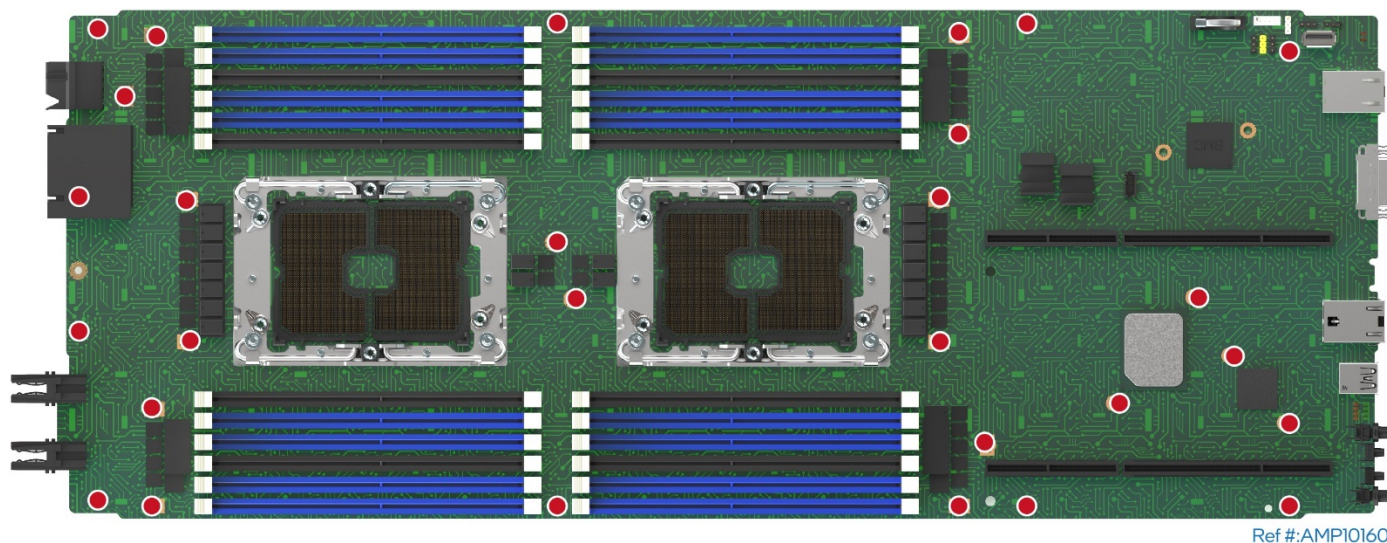
Figure 73. Server Board Mounting Hole Locations

Server chassis may use different methods for securing the server board to the chassis. The selected chassis may have integrated mounting features or they may include separate mounting stand-offs that must be installed.

The following illustration identifies possible mounting options that can be used.
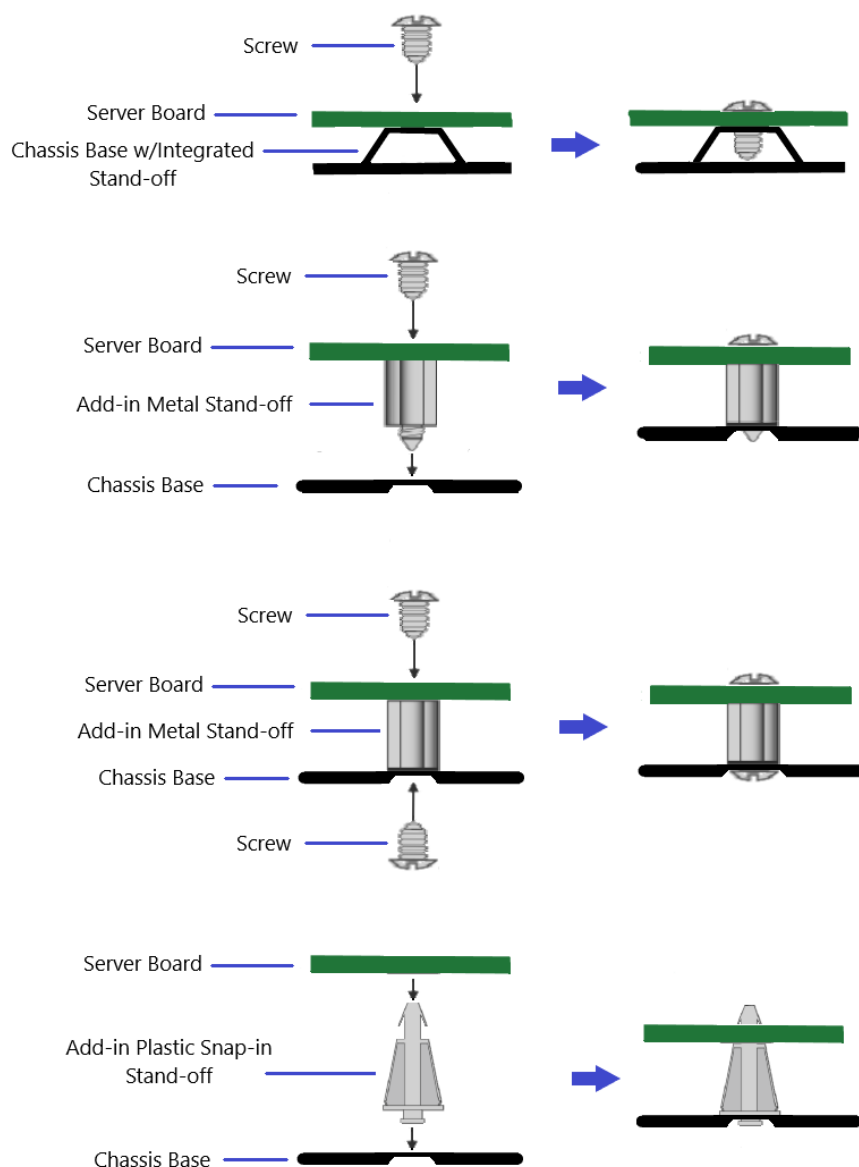
Figure 74. Possible Server Board Mounting Options

For mounting options that require the server board to be secured to the chassis using screws, Intel recommends tightening the screws using a torque or pneumatic screwdriver. The recommended torque setting is dependent on the screw type used. See the following table.

Table 46. Server Board Mounting Screw Torque Requirements

Screw Size	Torque Value	Tolerance ±
6–32	8 in-lb	1
M3	5 in-lb	1

G.2   Processor Replacement

Processors are part of an assembly referred to as a PHM (Processor Heat sink Module). A PHM consists of a processor, a processor carrier clip, and the processor heat sink that is preassembled into a single module before placement onto the processor socket assembly on the server board. The PHM concept reduces the risk of damaging pins within the processor socket during the replacement process.

The following procedure applies to processor heat sinks that are used by Intel for use in its server systems. If the processor heat sink is different from those depicted in the following procedures, Intel recommends following the processor replacement procedures included within documentation supplied with the chosen non-Intel server system.

Components Required for each faulty processor:

- New 3rd Gen Intel® Xeon® Scalable processor + included shipping tray
- Existing processor carrier clip
- New processor heat sink or existing processor heat sink + new thermal interface material (TIM)

Required Tools and Supplies:

- Anti-static wrist strap and conductive workbench pad (recommended)
- ESD Gloves (recommended)
- T-30 Torx* screwdriver

Note: The installation figures in this section only display the front heat sink. However, the processor installation procedure is the same, regardless of the position of the heat sink.

Caution: Fin edges of the processor heat sink are very sharp. Intel recommends wearing thin ESD protective gloves when handling the PHM during the following procedures.

Caution: Processor heat sinks are easily damaged if handled improperly. See the following figure for proper handling.
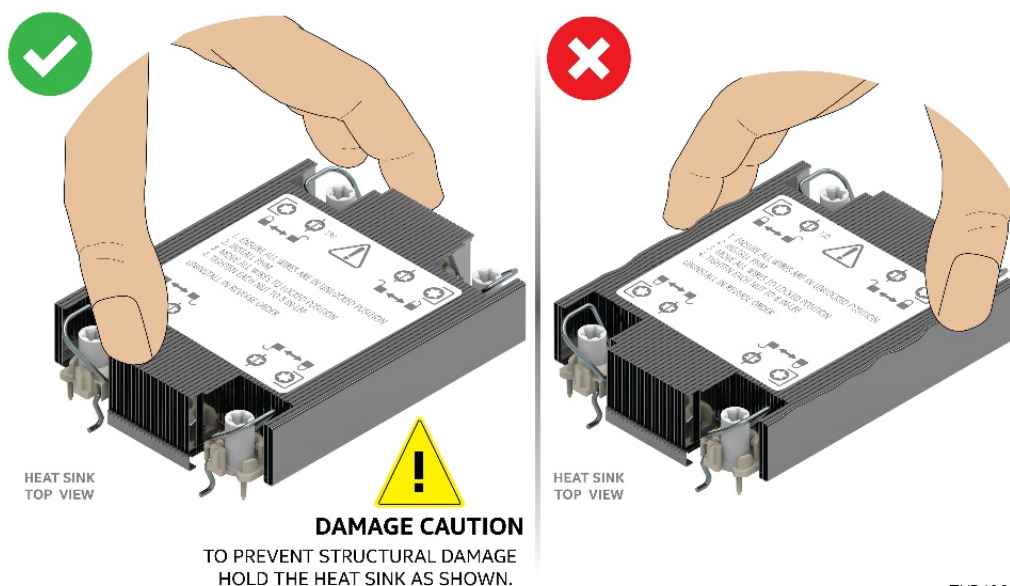
Figure 75. Processor Heat Sink Handling

G.2.1   Processor Heat Sink Module (PHM) Removal

1. Identify and locate the faulty processor.
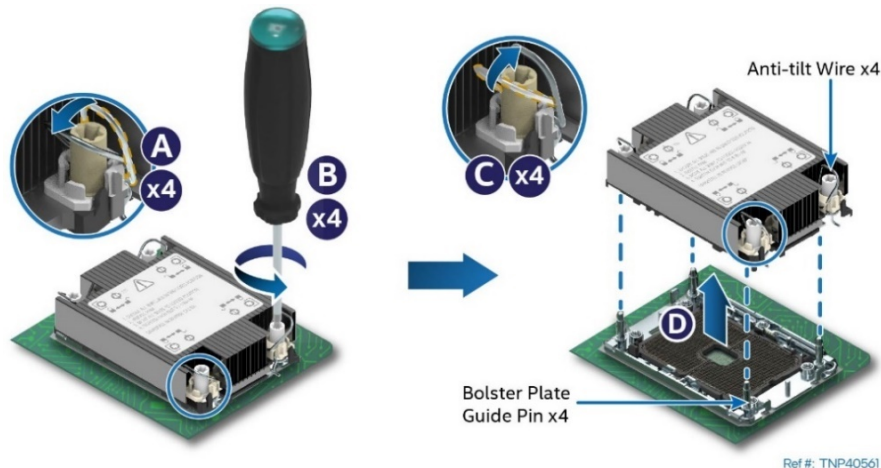
Figure 76. PHM Assembly Removal from Processor Socket

2. Ensure the heat sink anti-tilt wires located over each of the four heat sink fasteners are in the outward position (see Letter A).
3. Using T-30 Torx* screwdriver, fully loosen all four heat sink fasteners in any order (see Letter B).
4. Set all four anti-tilt wires on the heat sink to the inward position (see Letter C).
5. Carefully grasp the PHM and lift it straight up and off the server board (see Letter D).
6. With the processor facing up, set the PHM down onto a flat surface.
7. Visually inspect that the processor socket is free of damage or contamination.

Caution: If debris is observed, blow it away gently. Do not use tweezers or any other hard tools to remove the debris.

8. If not replacing the processor, install the original plastic socket cover over the processor socket.
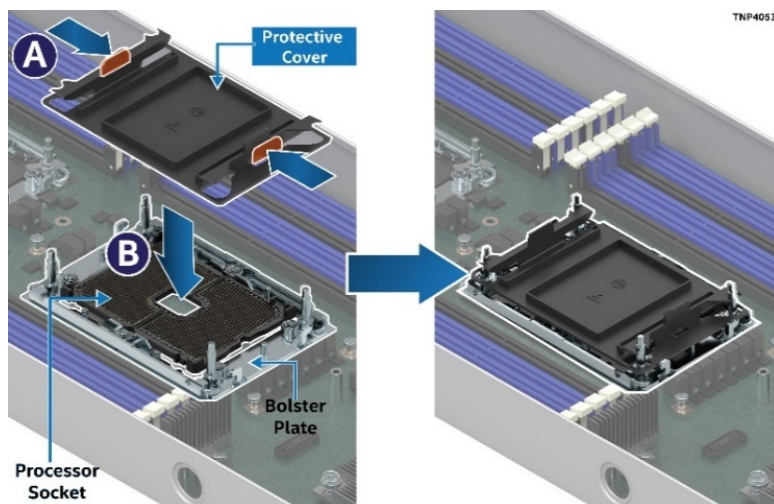
Figure 77. Reinstall the Socket Cover

- Squeeze the finger grips at each end of the cover (see Letter A).
- Carefully lower the cover over the four alignment pins of the bolster plate and onto the processor socket (see Letter B).

- Release finger grips to lock the cover in place.
- Ensure the socket cover is locked in place.

Caution: Do not press down on the center of the socket cover.

G.2.2   PHM Disassembly
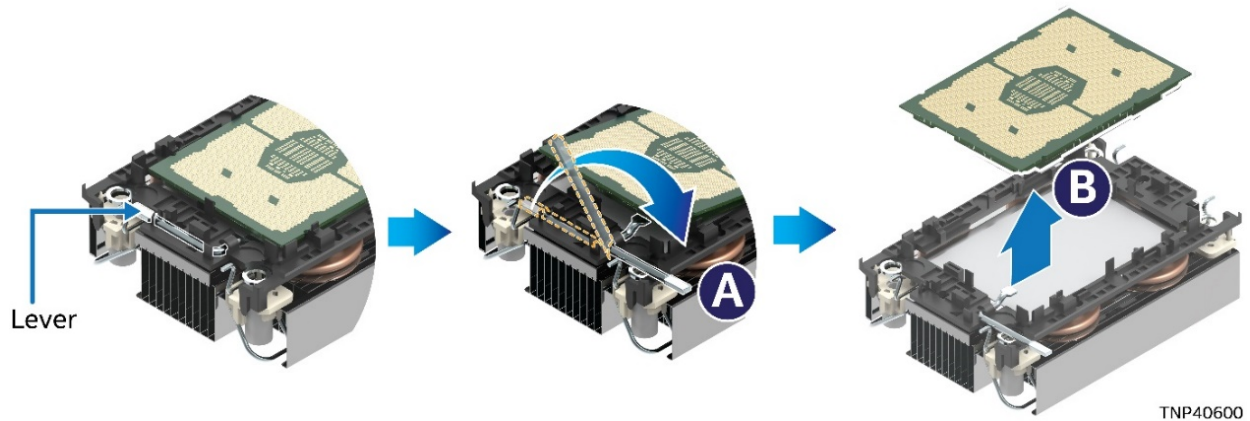
Figure 78. Processor Removal from PHM Assembly

1. While holding down the PHM, rotate the lever (see Letter A) from left to right until the processor lifts free from the processor carrier clip.
2. Holding down the processor carrier clip, carefully lift the processor and slide it out of the processor carrier clip (see Letter B).
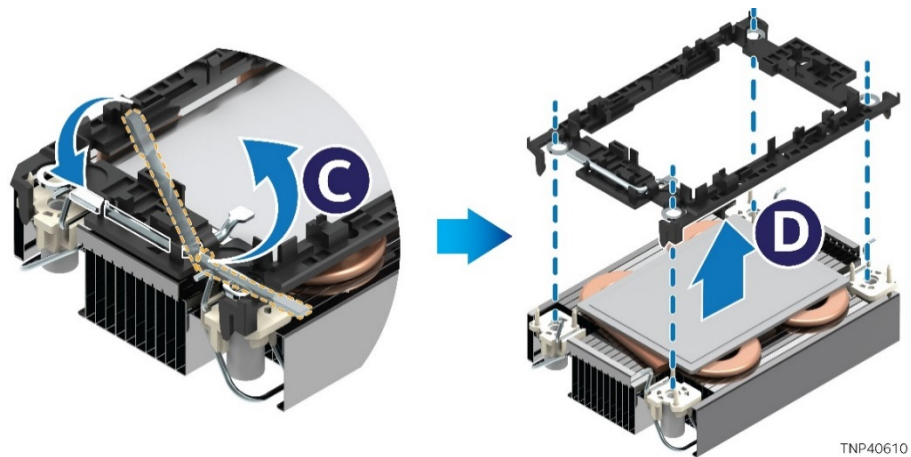
Figure 79. Processor Carrier Clip Removal from PHM Assembly

3. Return the lever to the original position (see Letter C).
4. Detach the processor carrier clip from the heat sink.
   - Unlatch the hook on each corner of the processor carrier clip and lift it from the heat sink (see Letter D).

G.2.3 PHM Reassembly

To properly reassemble the PHM and install it onto the server board, the procedures described in the following sections must be followed in the order specified. These instructions assume that the processor heat sink (new or reuse of existing) has the necessary Thermal Interface Material (TIM) (Honeywell* PTM7000) already applied to the bottom of the heat sink.

Caution: Full ESD precautions should be followed to perform reassembly of the PHM and reinstallation of the PHM to the server board. The processor itself should Not be handled.

Each component within the PHM assembly includes a Pin 1 indicator. Pin 1 indicator alignment between all components is required throughout the assembly process.
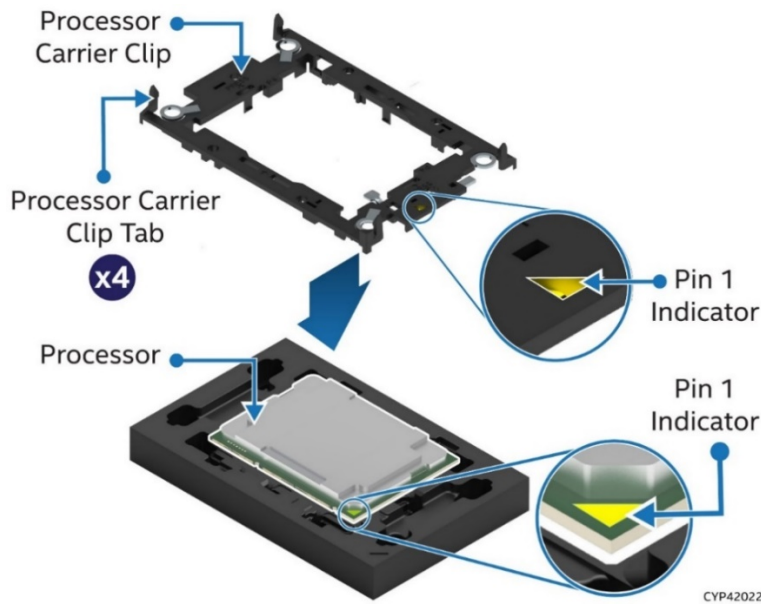
Figure 80. Installing Processor Carrier Clip onto Processor – Part 1
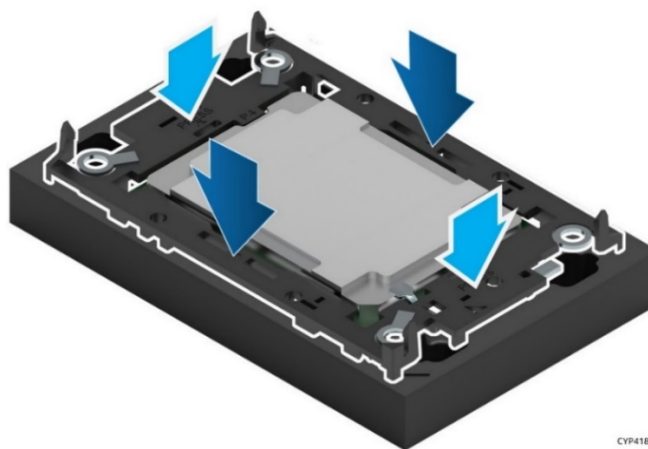
Figure 81. Installing Processor Carrier Clip onto Processor – Part 2

1. With the processor still in its tray, place the processor carrier clip over the processor.
2. Ensure the Pin 1 indicator on the processor carrier clip is aligned with the Pin 1 indicator of the processor.

3. Gently press down simultaneously on two opposite sides of the processor carrier clip until it clicks in place.
4. Repeat step 3 for the other two sides.
5. Locate the processor heat sink. To avoid damage, grasp it by its narrower sides as shown below.
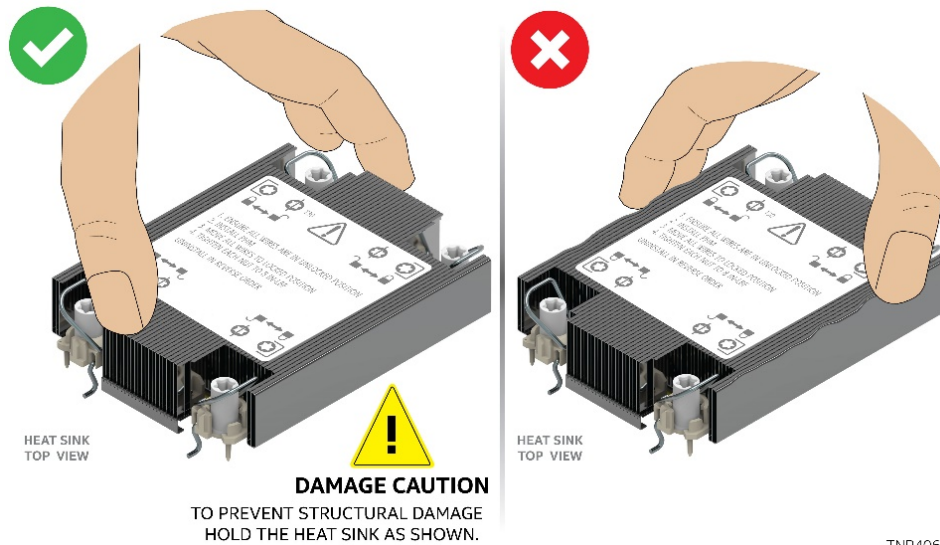
Figure 82. Processor Heat Sink Handling

6. Place the heat sink bottom side up onto a flat surface.

If reusing an existing heat sink:

- Properly clean off existing thermal interface material (TIM) from the bottom of the heat sink
- Apply new TIM (Honeywell* PTM7000)

If using a new heat sink:

- Remove the plastic protective film (if present) from the Thermal Interface Material (TIM).
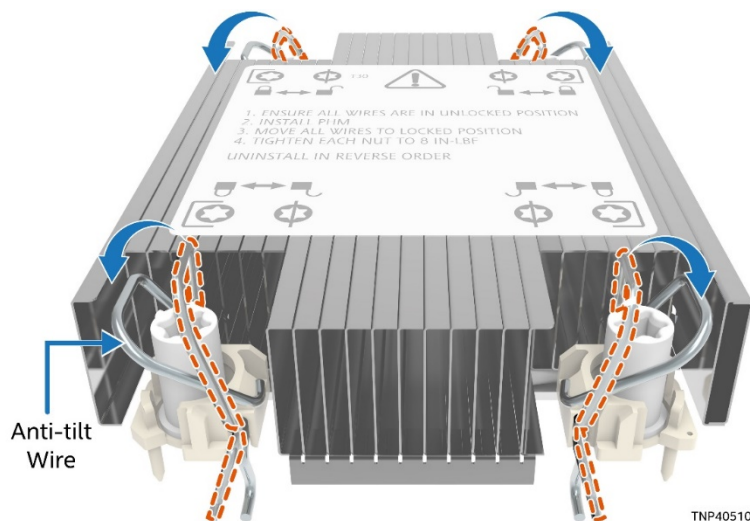
Figure 83. Processor Heat Sink Anti-tilt Wires in the Outward Position

7. Set the anti-tilt wire over each of the four heat sink fasteners to their outward position.
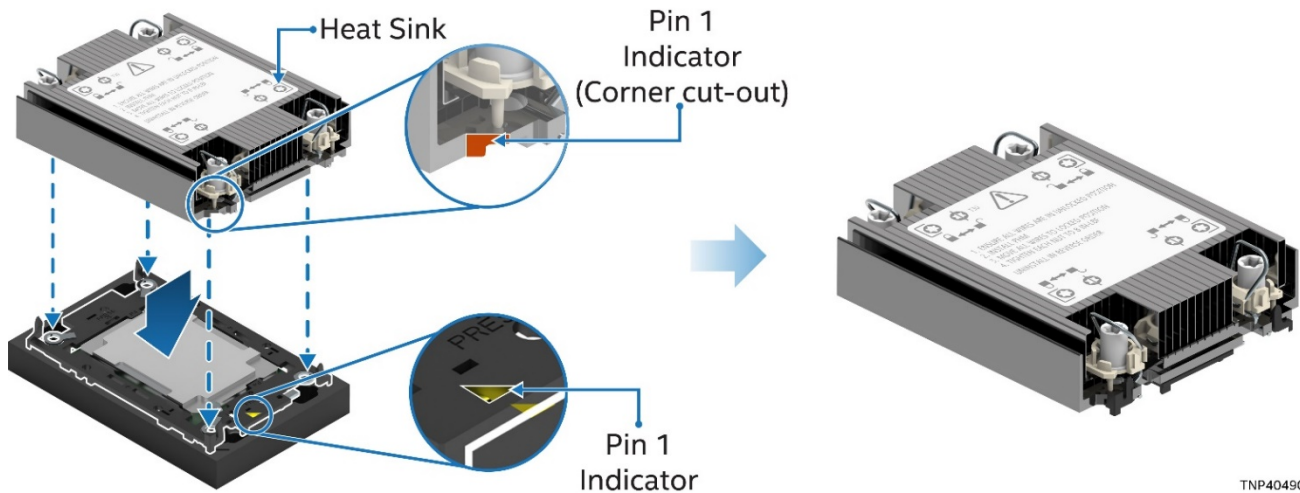
Figure 84. Pin 1 Indicator of Processor Carrier Clip

8. Align the Pin 1 indicator of processor carrier clip with one of the diagonally cut corners on the base of the heat sink. Or (if present) look for the Pin 1 indicator on the corner of the heat sink label.
9. Gently press down the heat sink onto the processor carrier clip until it clicks into place.
10. Ensure all four heat sink corners are securely latched to the processor carrier clip tabs.

G.2.4   PHM Installation

1. If installed, remove the plastic cover from the processor socket.

Caution: Do not touch the socket pins. The pins inside the processor socket are extremely sensitive. A damaged processor socket may produce unpredictable system errors.
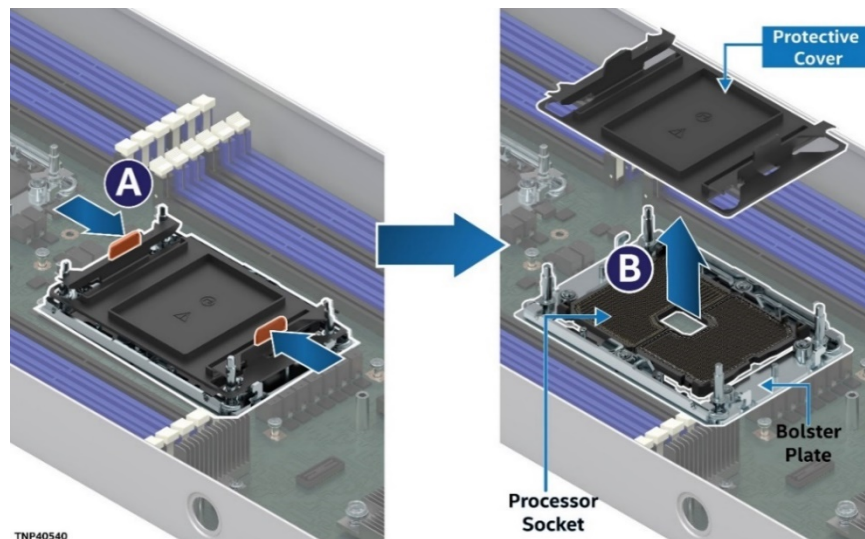
Figure 85. Socket Protective Cover Removal

2. Remove the protective cover by squeezing the finger grips (see Letter A) and pulling the cover up (see Letter B).
3. Ensure the socket is free of damage or contamination before installing the PHM.

Caution: If debris is observed, blow it away gently. Do not remove it manually, such as with tweezers.
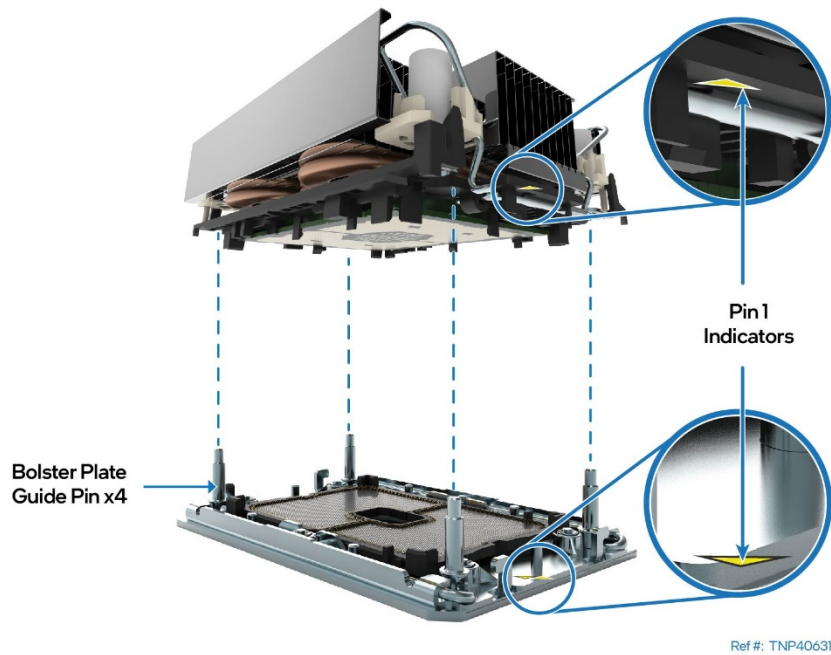
Figure 86. PHM Alignment with Socket Assembly

Caution: Processor socket pins are delicate and bend easily. Use extreme care when placing the PHM onto the processor socket. Do not drop it.
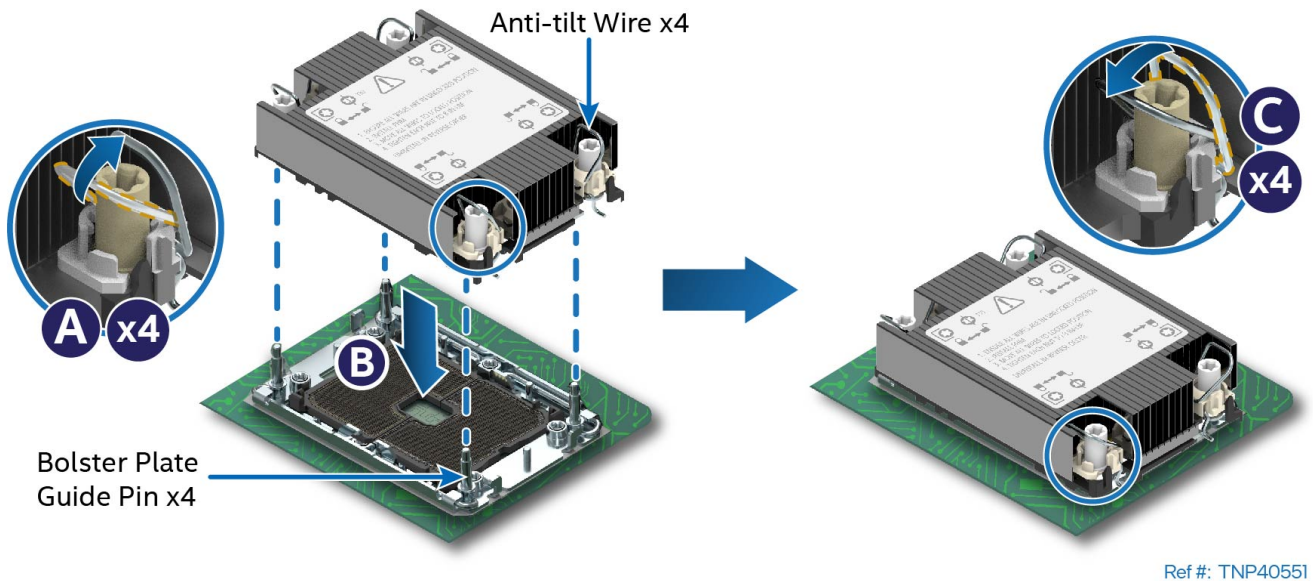
Figure 87. PHM Installation onto Server Board

4. Set all four anti-tilt wires on the heat sink to the inward position (see Letter A).
5. Align the Pin 1 indicators of the processor carrier clip and processor with the Pin 1 indicator on the socket assembly bolster plate.
6. Carefully lower the PHM over the four bolster plate alignment pins (see Letter B).
7. Ensure the PHM is sitting flat and even on the bolster plate.
8. Set all four anti-tilt wires on the heat sink to the outward position (see Letter C).

Figure 88. Tighten Heat Sink Fasteners

9. Using a T30 Torx* screwdriver, tighten the heat sink fasteners to 8 in-lb. No specific sequence is needed for tightening.

Note: Intel strongly recommends that both processors are installed. If only one processor is installed, do not install a processor heat sink on an empty socket.

G.3　　　DIMM / Intel® Optane™ PMem Replacement Instructions

The Intel® Server Boards D50TNP1SB and D50TNP1SBCR support standard DDR4, RDIMMs, and LDRIMMs. In addition, the D50TNP1SB server board supports Intel® Optane™ persistent memory 200 series modules (also known as, Intel® Optane™ PMem).

Required Tools and Supplies:

- Anti-static wrist strap and conductive workbench pad (recommended)

The figures below show standard DDR4 DIMMs but the steps of DDR4 DIMM installation and replacement are the same between standard DDR4 DIMMs and Intel® Optane™ PMem modules.

Standard DDR4 DIMMs and Intel® Optane™ PMem devices will be commonly referred to as "memory device" in the following instructions.
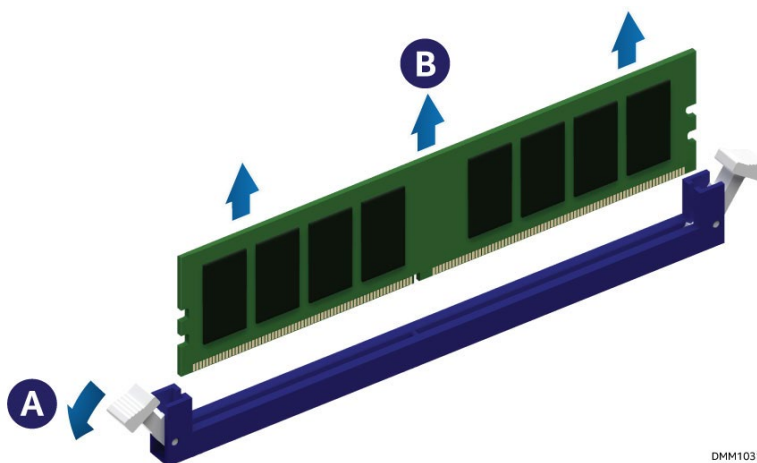
Figure 89. Removing the DIMM

1. Identify and locate the memory module to be replaced.
2. Ensure that the ejection tabs of adjacent memory slots are closed.
3. Open the ejection tabs at both ends of the selected memory slot (see Letter A). The memory module will slightly lift from the slot.
4. Holding the memory module by its edges, lift it away from the slot (see Letter B).
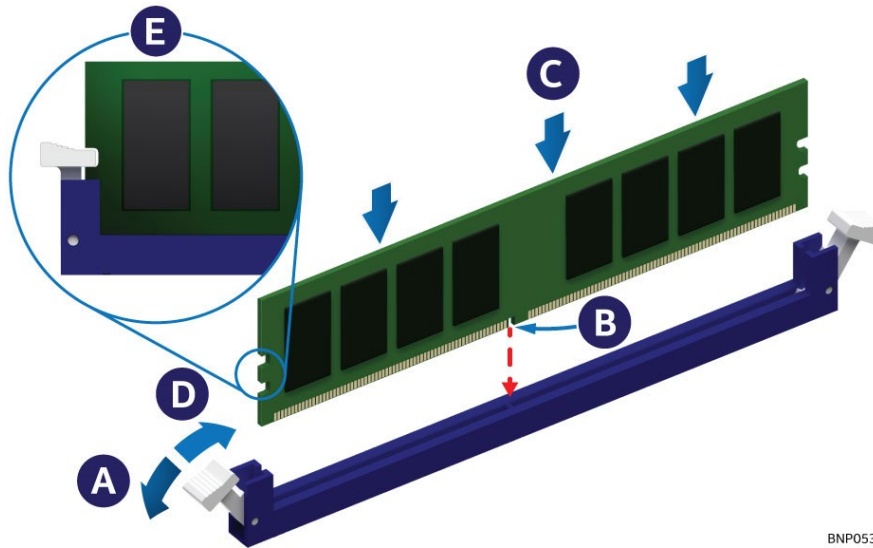
Figure 90. Installing the DIMM

5. Ensure that the ejection tabs at both ends of the memory slot are pushed outward to the open position (see Letter A).
6. Carefully unpack the replacement memory module, taking care to only handle the device by its outer edges.
7. Align the notch at the bottom edge of the memory module with the key in the memory slot (see Letter B).
8. Insert the memory module into the memory slot:
   a. Using even pressure along the top edge, push down on the memory module (see letter C) until the ejection tabs of the memory slot snap into place (see Letter D).

Ensure that the ejection tabs are firmly in place (see Letter E)

Appendix H. Statement of Volatility

This appendix describes the volatile and non-volatile components on the Intel® Server D40AMP family. It is not the intention of this document to include any components not directly mounted to the server board in the Intel® Compute Module D40AMP or riser cards used within the Intel® D40AMP modules or supported Intel chassis. These may include processors, memory, storage devices, or add-in cards.

The tables in this appendix provide the following data for each identified component.

Component Type

Three types of memory components are used on the Compute Module server board assembly. These include:

- **Non-volatile:** Non-volatile memory is persistent and is not cleared when power is removed from the system. Non-Volatile memory must be erased to clear data. The exact method of clearing these areas varies by the specific component. Some areas are required for normal operation of the server and clearing these areas may render the server board inoperable.
- **Volatile:** Volatile memory is cleared automatically when power is removed from the system.
- **Battery powered RAM:** Battery powered RAM is similar to volatile memory; however, is powered by a battery on the server board. Data in Battery powered RAM is persistent until the battery is removed from the server board.

Size

The size of each component includes sizes in bits, Kbits, bytes, kilobytes (KB) or megabytes (MB).

Board Location

The physical location of each component is specified in the Board Location column. The board location information corresponds to information on the silkscreen in the Compute Module server board.

User Data

The flash components on the Intel® Server D40AMP family do not store user data from the operating system. No operating system level data is retained in any listed components after AC power is removed. The persistence of information written to each component is determined by its type as described in the table.

Each component stores data specific to its function. Some components may contain passwords that provide access to that device's configuration or functionality. These passwords are specific to the device and are unique and unrelated to operating system passwords. The specific components that may contain password data are:

- **BIOS**: The BIOS provides the capability to prevent unauthorized users from configuring BIOS settings when a BIOS password is set. This password is stored in BIOS flash and is only used to set BIOS configuration access restrictions.
- **BMC**: The Intel® Server Board D40AMP and Intel® Compute Module D40AMP support an Intelligent Platform Management Interface (IPMI) 2.0 conformant baseboard management controller (BMC). The BMC provides health monitoring, alerting and remote power control capabilities for the Intel® Server Board D40AMP and Intel® Compute Module D40AMP. The BMC does not have access to operating system level data.

The BMC supports the capability for remote software to connect over the network and perform health monitoring and power control. This access can be configured to require authentication by a password. If configured, the BMC will maintain user passwords to control this access. These passwords are stored in the BMC flash.

The Intel® Server Board D40AMP includes several components that can be used to store data. A list of those components is included in the following table.

Table 47. Components in The Intel® Server Board D40AMP

Component Type	Size	Board Location	User Data	Name
Non-Volatile	256 Mb	U111X1	No (BIOS)	BIOS Flash
Non-Volatile	256 Mb	U62X1	No (FW)	BMC FW
Non-Volatile	16 Mb	U25X1	No	LAN Flash
Non-Volatile	768 B	EU63X1	No (TPM)	TPM
Non-Volatile	–	U37X1	No	FPGA
Volatile	4 Gb	E29X1	No	BMC DRAM
Non-Volatile	256 KB	U72	No	Retimer SW EEPROM

The riser cards within Intel® Compute Module D40AMP may include components used to store data. The following table provides a list of components associated with them. For server board components, see the section above.

Table 48. Components for Riser Cards in the Intel® Compute Module D40AMP

Component Type	Size	Board Location	User Data	Name
Non-Volatile	2 KB	U1	No	1U riser card FRU

System boards within the Intel® Server Chassis VP3000 family contain components used to store data. A list of components for the system boards in the chassis is included in the following table. For server board components and compute module components, see the sections above.

Table 49. Components for System Boards in Intel® Server Chassis VP3000 family

Component Type	Size	Board Location	User Data	Name
Non-Volatile	256 B	U25	No	Primary PDB FRU
Non-Volatile	128 KB + 3 KB	U30	No	Primary PDB PIC MCU (boot)
Non-Volatile	256 B	U25	No	Secondary PDB FRU
Non-Volatile	128 KB + 3 KB	U30	No	Secondary PDB PIC MCU (boot)
Non-Volatile	256 B	U10, U12	No	U.2 HSBP FRU
Non-Volatile	256 B	U9, U10, U11, U12	No	E1.L Midplane FRU

Appendix I.   Product Regulatory Compliance

This product has been evaluated and certified as Information Technology Equipment (ITE) that may be installed in offices, schools, computer rooms, and similar commercial type locations. The suitability of this product for other product certification categories and/or environments (such as: medical, industrial, telecommunications, NEBS, residential, alarm systems, test equipment, and so on), other than an ITE application, will require further evaluation and may require additional regulatory approvals.

Intel has verified that all L3, L6, and L9 server products[1] **as configured and sold by Intel** to its customers comply with the requirements for all regulatory certifications defined in the following table. It is the Intel customer's responsibility to ensure their final server system configurations are tested and certified to meet the regulatory requirements for the countries to which they plan to ship and or deploy server systems into.

	Intel® Server Board D40AMP	Intel® Server D40AMP family	Notes
	"American Pass"	"American Pass"	Intel Project Code Name
	L3 Board	L6/L9 System	Product integration level
	D40AMP	VP3000	Product family identified on certification
Regulatory Certification			
TBD			

Table Key

Not Tested / Not Certified	○
Tested / Certified – Limited OEM SKUs only	●
Testing / Certification (Planned)	(Date)
Tested / Certified	✓

---

[1] An L9 system configuration is a power-on ready server system with NO operating system installed. An L6 system configuration requires additional components to be installed to make it power-on ready. L3 are component building block options that require integration into a chassis to create a functional server system.

EU Directive 2019/424 (Lot 9)

Beginning on March 1, 2020, an additional component of the European Union (EU) regulatory CE marking scheme, identified as EU Directive 2019/424 (Lot 9), went into effect. After this date, all new server systems shipped into or deployed within the EU must meet the full CE marking requirements including those defined by the additional EU Lot 9 regulations.

Intel has verified that all L3, L6, and L9 server products[2] **as configured and sold by Intel** to its customers comply with the full CE regulatory requirements for the given product type, including those defined by EU Lot 9. It is the Intel customer's responsibility to ensure their final server system configurations are SPEC® SERT™ tested and meet the new CE regulatory requirements.

Visit the following website for additional EU Directive 2019/424 (Lot9) information:

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019R0424

In compliance with the EU Directive 2019/424 (Lot 9) materials efficiency requirements, Intel makes available all necessary product collaterals as identified below:

- **System Disassembly Instructions**
    - *Intel® Server D40AMP Family System Integration and Service Guide*
    - See Section 1 for link to document.
- **Product Specifications**
    - *Intel® Server D40AMP Family Technical Product Specification (TPS)*
    - See Section 1 for link to document.
- **System BIOS/Firmware and Security Updates – Intel® Server D40AMP family**
    - System Update Package (SUP) – uEFI only
    - See Section 1.
- **Intel® Solid State Drive (SSD) Secure Data Deletion and Firmware Updates**
    - Note: for system configurations that may be configured with an Intel SSD
    - The Intel® Memory and Storage Tool (Intel® MAS)
      https://downloadcenter.intel.com/product/35125/Memory-and-Storage
- **Intel® RAID Controller Firmware Updates and other support collaterals**
    - **Note**: for system configurations that may be configured with an Intel® RAID Controller
      https://www.intel.com/content/www/us/en/support/products/43732/server-products/raid-products.html

---

[2] An L9 system configuration is a power-on ready server system with NO operating system installed. An L6 system configuration requires additional components to be installed to make it power-on ready. L3 are component building block options that require integration into a chassis to create a functional server system

EU Lot9 Support Summary – VP3000 – Intel® Server D40AMP Family ("American Pass")

DISCLAIMER – The information contained within the following tables is for reference purposes only and is intended to provide Intel customers with a template to report product information necessary for (EU) 2019/424 (Lot 9) server conformity assessment. The information provided herein does not represent any final shipping server system test results, and customer's actual test results for shipping server configurations may differ from the information provided. Use of this information is at the sole risk of the user, and Intel assumes no responsibility for customers server system level regulation compliance with EU 2019/424 (Lot 9).

Product Info.					
Product Type	Server				
Manufacturer Name	Intel Corporation				
Registered trade name and address	Intel 2200 Mission College Blvd, Santa Clara, CA 95054-1594, USA				
Product model number and model numbers for low end performance and high-end performance configure if applicable	VP3000				
Year Of Manufacture	2021				
PSU efficiency at 10%, 20%, 50% and 100% of rated output power	**2100W PSU AXX2100TCRPS (FF185) Titanium**				
	Model	**10%**	**20%**	**50%**	**100%**
	AXX2100TCRPS	90%	94%	96%	91%
PSU factor at 50% of rated load level	AXX2100TCRPS	0.95			
PSU Rated Power Output (Server Only)	AXX2100TCRPS	2100 Watts			
Idle state power (Server only) (Watts)	Refer to the following table				
List of all components for additional idle power allowances (server only)	Refer to the following table				
Maximum power (Server only)	Refer to the following table				
Declared operating condition class	ASHRAE Class A2-Continuous Operation 10 ℃ to 35 ℃ with the maximum rate of change not to exceed 10 ℃ per hour				
Idle State Power (watts) at the higher boundary temp (Server Only)	Refer to the following table				
the active state efficiency and the performance in active state of the server (server only)	Refer to the following table				
Information on the secure data deletion functionality	Refer to the following table				
for blade server, a list of recommended combinations with compatible chassis (Server only)	Not Applicable				
If Product Model Is Part Of A Server Product Family, a list of all model configurations that are represented by the model shall be supplied (Server only)	TBD				

Energy Efficiency Data of FC2H – 2 (Dual) CPUs Installed Configuration

	Configuration		TBD.	TBD.
Details	Chassis	Model		
	Node/MB	Quantity		
		Model		
	CPU	Quantity		
		Model		
	Memory	Quantity		
		Capacity per DIMM (GB)		
		Total Memory Amount (GB)		
	SSD	SSD Quantity		
	PSU	Quantity		
		Model		
	FW			
Measured and Calculated Server Allowance	P Base			
	Additional CPU			
	Additional Power Supply			
	Storage Devices			
	Additional Memory			
	Additional I/O Device (10Gx 15W/2Port on MB)			
	Perfcpu			
Limits/ Results	Idle power allowances (W)			
	Idle power tested (W) Per node			
	Minimum Eff$_{ACTIVE}$			
	Eff$_{ACTIVE}$ tested			
Other test result	Idle Power at Higher Temp. (per Node) @ 35 degree C			
	Max Power (Per Node)			

Other Information:

Chemical Declaration
• Neodymium Not Applicable. (No HDD offered by Intel) • Cobalt Not Applicable. (No BBUs. Coin battery is out of scope)

Appendix J. Glossary

Term	Definition
ACPI	Advanced Configuration and Power Interface
Intel® AES-NI	Intel® Advanced Encryption Standard New Instructions. See also AES.
AI	Artificial Intelligence
ASHRAE	American Society of Heating, Refrigerating and Air Conditioning Engineers
Intel® AVX-512	Intel® Advanced Vector Extensions 512
BBS	BIOS Boot Selection
BMC	Baseboard Management Controller
BIOS	Basic Input/Output System
Intel® CBnT	Converged Intel® Boot Guard and Trusted Execution Technology (Intel® TXT)
CFM	Cubic Feet per Minute
CLST	Closed Loop System Throttling
CMOS	Complementary Metal-Oxide-Semiconductor
DDR4	Double Data Rate 4
DIMM	Dual In-line Memory Module
DMI	Direct Media Interface
DPC	DIMMs per Channel
DR	Dual Rank
ECC	Error Correction Code
EFI	Extensible Firmware Interface
EMP	Ethernet Management Port
EPS	External Product Specification
FRB	Fault Resilient Boot
FRU	Field Replaceable Unit
GUI	Graphical User Interface
HPC	High-Performance Computing
Intel® HT Technology	Intel® Hyper-Threading Technology
IDE	Integrated Drive Electronics
IMC	Integrated Memory Controller
IIO	Integrated Input/Output
iPC	Intel Product Code
IPMI	Intelligent Platform Management Interface
ISTA	International Safe Transit Association
KVM	Keyboard, Video, and Mouse
KVM-r	Keyboard/Video/Mouse Redirection
LFM	Linear Feet per Minute (airflow measurement)
LLC	Last Level Cache
LRDIMM	Load Reduced DIMM
LSB	Least Significant Bit
Intel® ME	Intel® Management Engine
MKTME	Multi-Key Total Memory Encryption
MM	Memory Mode
MRC	Memory Reference Code
MSB	Most Significant Bit

Term	Definition
NAT	Network Address Translation
NIC	Network Interface Controller
NMI	Non-maskable Interrupt
NTB	Non-Transparent Bridge
OEM	Original Equipment Manufacturer
OR	Oct (8) Rank
OTP	Over Temperature Protection
OVP	Over-voltage Protection
PCH	Peripheral Controller Hub
PCI	Peripheral Component Interconnect
PCIe*	Peripheral Component Interconnect Express*
PDB	Power Distribution Board
PECI	Platform Environment Control Interface
Intel® PFR	Intel® Platform Firmware Resilience
PHM	Processor Heat sink Module
PMem	Persistent Memory
POST	Power-on self-test
PSU	Power Supply Unit
PWM	Pulse Width Modulation
QR	Quad (8) Rank
RAID	Redundant Array of Independent Disks
RAS	Reliability, Availability, and Serviceability
RDIMM	Registered DIMM
SATA	Serial Advanced Technology Attachment
SEL	System Event Log
SDR	Sensor Data Record
SmaRT	Smart Ride Through
Intel® SGX	Intel® Software Guard Extensions
SMBus*	System Management Bus
SMM	Server Management Mode
SMP	Server Management Processor
SOL	Serial-Over-LAN
SR	Single Rank
SSD	Solid State Device
SSL	Secure Sockets Layer
TCG	Trusted Computing Group
TDP	Thermal Design Power
TIM	Thermal Interface Material
Intel® TME	Intel® Total Memory Encryption
TPM	Trusted Platform Module
Intel® TXT	Intel® Trusted Execution Technology
UEFI	Unified Extensible Firmware Interface
Intel® UPI	Intel® Ultra Path Interconnect
Intel® VMD	Intel® Volume Management Device
Intel® VROC	Intel® Virtual RAID on CPU
VSB	Voltage Standby