



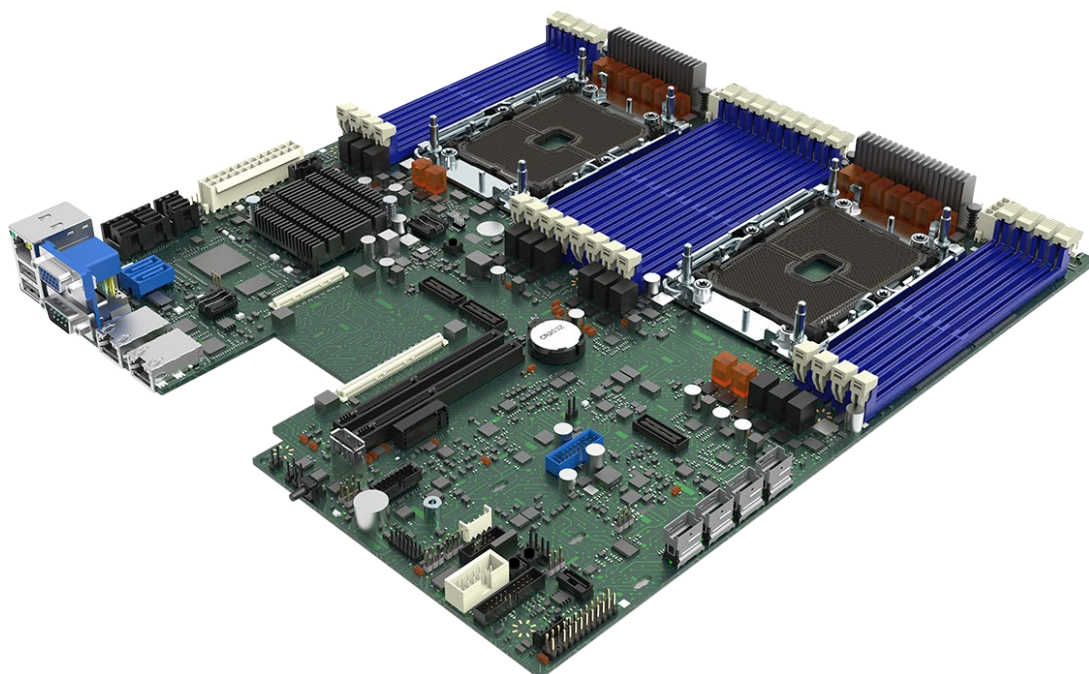
# Intel® Server Board M20NTP2SB

## *Technical Product Specification*

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

Rev. 1.2

September 2022



# M20NTP2SB

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

<This page is intentionally left blank>

## Document Revision History

Date	Revision	Changes
October 2021	1.0	Production release.
May 2022	1.1	<ul style="list-style-type: none"><li>• Correction made to Figure 7 – Architectural Block Diagram.</li><li>• Correction made to Table 37 – Statement of Volatility Server Board Components.</li></ul>
September 2022	1.2	<ul style="list-style-type: none"><li>• Minor edits throughout the document for clarity.</li><li>• Updated Section 5.1- Remote Management Port. figures 25 and 26.</li><li>• Added section 5.1.1.1 - IPMI Command Execution Required to Enable the Integrated BMC Web Console.</li><li>• Updated content in Table 35. Onboard LED Descriptions</li></ul>

## 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](http://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 that 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](http://www.intel.com/design/literature.htm).

Intel, Xeon, 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

<b>1. Introduction</b>	<b>12</b>
1.1 Reference Documents	12
<b>2. Server Board Overview</b>	<b>15</b>
2.1 Server Board Feature Set	16
2.2 Server Board Component / Feature Identification	18
2.3 Server Board Architecture Overview	21
<b>3. Server Chassis Development Guidance</b>	<b>22</b>
3.1 Server Board Dimensions	22
3.2 Server Board Mechanical Drawing	23
3.3 Rear I/O Connector and OCP* Add-in Card Support	24
3.4 PCIe* Add-in Card Support	25
3.4.1 1U 1-Slot PCIe* Riser Card (Riser Slot 1) – iPC M20NTP1URISER1	26
3.4.2 1U 1-Slot PCIe* Riser Card (Riser Slot 2) – iPC M20NTP1URISER2	26
3.5 Server Board Power	27
3.6 Thermal Management	28
3.6.1 Platform Management Support Using Non-Intel Chassis	31
3.6.2 System Fan Connectors	32
<b>4. System Software and Utilities</b>	<b>33</b>
4.1 Hot Keys Supported During POST	33
4.1.1 POST Logo / Diagnostic Screen	34
4.1.2 BIOS Boot Pop-Up Menu	34
4.2 <F2> BIOS Setup Utility	34
4.3 AMI* BIOS Configuration Program (AMIBCP) – Creating a BIOS Image for Customized Settings	35
4.4 AMI* ChangeLogo Utility – Customizing the BIOS Splash Screen	35
4.5 Intel Server Configuration Utility ( <i>syscfg</i> )	35
4.6 System Update Package (SUP) for Intel® Server System M20NTP2SB	35
4.7 Intel Server Firmware Update Utility ( <i>sysfwupdt</i> )	35
4.8 Intel Server Information Retrieval Utility ( <i>sysinfo</i> )	36
4.9 Intel® Server Debug and Provisioning Tool (Intel® SDP Tool)	36
<b>5. Server Management</b>	<b>37</b>
5.1 Remote Management Port	38
5.1.1 Configuring System Management Port Using <F2> BIOS Setup	38
5.2 Standard System Management Features	41
5.2.1 Virtual KVM over HTML5	41
5.2.2 Integrated Baseboard Management Controller Web Console (Integrated BMC Web Console) ...	41
5.2.3 Redfish* Support	42
5.2.4 IPMI 2.0 Support	43
5.2.5 Out-of-Band BIOS / BMC Update and Configuration	43
5.2.6 System Inventory	43

5.2.7	Autonomous Debug Log .....	43
5.2.8	Security Features.....	43
5.3	Advanced System Management Features .....	44
5.3.1	Virtual Media Image Redirection (HTML5 and Java) .....	44
5.3.2	Virtual Media over Network Share and Local Folder .....	45
5.3.3	Active Directory* Support.....	45
5.4	Intel® Data Center Manager (Intel® DCM) Support.....	45
<b>6.</b>	<b>Processor Support.....</b>	<b>46</b>
6.1	Processor Cooling Overview .....	46
6.1.1	Processor Cooling Requirements.....	47
6.2	Supported Processor Overview .....	47
6.2.1	Processor Thermal Design Power (TDP) .....	48
6.2.2	Supported Technologies .....	49
6.3	Processor Population Rules.....	50
<b>7.</b>	<b>Memory Support.....</b>	<b>51</b>
7.1	Supported Memory .....	51
7.2	Memory Subsystem Architecture.....	52
7.2.1	Recommended Memory Configurations .....	55
7.3	Memory RAS Support.....	56
<b>8.</b>	<b>PCI Express (PCIe*) Subsystem Overview .....</b>	<b>58</b>
8.1	PCIe* Enumeration and Allocation .....	59
8.2	PCIe* Riser Card Support.....	60
8.3	Network Connectivity.....	61
8.3.1	OCP* Mezzanine Card 2.0 Support.....	62
<b>9.</b>	<b>Storage Interface Support Options .....</b>	<b>63</b>
9.1	Internal USB 3.0 Type A Connector.....	64
9.2	Internal M.2 SSD Storage Support.....	64
9.3	SATA Support.....	65
9.3.1	Staggered Disk Spin-Up Option.....	66
9.1	Intel® Virtual RAID on CPU 7.5 (Intel® VROC) for SATA .....	67
9.2	NVMe* Support.....	68
9.2.1	Intel® Volume Management Device (Intel® VMD) 2.0 for NVMe* .....	68
9.2.2	Intel® Virtual RAID on CPU 7.5 (Intel® VROC) for NVMe* .....	70
<b>10.</b>	<b>Video Support .....</b>	<b>71</b>
10.1	Video Resolutions.....	71
10.2	Server Board Video and Add-in Video Adapter Support .....	71
<b>11.</b>	<b>System Security .....</b>	<b>73</b>
11.1	Password Protection.....	73
11.1.1	Password Setup .....	74
11.1.2	System Administrator Password Rights .....	74
11.1.3	Authorized System User Password Rights and Restrictions.....	75

11.2	Front Panel Lockout.....	75
11.3	Intel® Total Memory Encryption (Intel® TME) .....	75
11.4	Intel® Software Guard Extensions (Intel® SGX).....	76
11.5	Trusted Platform Module (TPM) Support .....	77
11.5.1	Trusted Platform Module (TPM) Security BIOS.....	78
11.5.2	Physical Presence .....	78
11.5.3	TPM Security Setup Options .....	78
11.6	Converged Intel® Boot Guard and Trusted Execution Technology (Intel® TXT).....	79
11.7	Unified Extensible Firmware Interface (UEFI) Secure Boot Technology.....	79
<b>12.</b>	<b>Server Board Connectors and Headers .....</b>	<b>80</b>
12.1	PCIe* Riser Card Slots.....	80
12.2	Main Power and CPU Power Cable Connectors .....	80
12.3	System Fan Cable Connectors.....	80
12.4	Front Panel Cable Header.....	81
12.5	Onboard USB 3.0 Cable Connector.....	82
12.6	Onboard Serial COM2 Cable Connector .....	83
12.7	Onboard VGA Cable Header.....	84
12.8	Power Supply Management Interface (PSMI) Cable Connector .....	85
12.9	Intelligent Platform Management Bus (IPMB) Cable Connector .....	85
12.10	sSATA SGPIO Cable Header .....	86
12.11	sSATA Ports 4 and 5 Cable Connectors .....	86
12.12	sSATA Ports 0–3 Mini-SAS* HD Cable Connector.....	87
12.13	SATA Ports 0–7 Dual Mini-SAS* HD Cable Connector .....	88
12.14	NVMe* Port Cable Connectors .....	89
<b>13.</b>	<b>Intel® Light Guided Diagnostics.....</b>	<b>91</b>
<b>14.</b>	<b>Server Board Jumpers Blocks and Service Buttons .....</b>	<b>93</b>
14.1	Onboard Service Buttons .....	93
14.1.1	Clear CMOS Button.....	93
14.2	Onboard Jumper Blocks .....	94
14.2.1	PC Beep Jumper .....	94
14.2.2	BMC COM Port Configuration Jumpers.....	94
14.2.3	ME Recovery Jumper.....	94
<b>15.</b>	<b>Server Board Installation and Component Replacement.....</b>	<b>95</b>
15.1	Server Board Installation Guidelines .....	97
15.2	Processor Replacement Instructions.....	100
15.2.1	Processor Heat Sink Module (PHM) Removal .....	101
15.2.2	PHM Disassembly.....	102
15.2.3	PHM Reassembly.....	103
15.2.4	PHM Installation .....	105
15.3	DIMM Replacement Instructions .....	107
<b>Appendix A.</b>	<b>Getting Help .....</b>	<b>109</b>

Warranty Information.....	109
<b>Appendix B. Integration and Usage Tips.....</b>	<b>110</b>
<b>Appendix C. POST Code Errors .....</b>	<b>111</b>
<b>Appendix D. Statement of Volatility.....</b>	<b>116</b>
<b>Appendix E. Regulatory Information .....</b>	<b>117</b>
<b>Appendix F. Glossary .....</b>	<b>119</b>

## List of Figures

Figure 1. Intel® Server Board M20NTP2SB.....	12
Figure 2. Intel® Server Board M20NTP2SB Overview .....	15
Figure 3. Intel® Server Board M20NTP2SB Component / Feature Identification .....	18
Figure 4. Back Panel Features Identification.....	19
Figure 5. Intel® Light-Guided Diagnostics – LED Identification .....	19
Figure 6. System Configuration and Recovery Features.....	20
Figure 7. Intel® Server Board M20NTP2SB Architectural Block Diagram .....	21
Figure 8. Intel® Server Board M20NTP2SB Board Dimensions.....	22
Figure 9. Server Board Mechanical Drawing.....	23
Figure 10. Optional EATX Compatible Rear I/O Shield .....	24
Figure 11. PCIe Riser Card Slots.....	25
Figure 12. 1U Chassis Example – Add-in Card Orientation .....	25
Figure 13. 1U PCIe* Riser Card (Riser Slot 1).....	26
Figure 14. 1U PCIe* Riser Card (Riser Slot 1) Mechanical Drawing.....	26
Figure 15. 1U PCIe* Riser Card (Riser Slot 2).....	26
Figure 16. 1U PCIe* Riser Card (Riser Slot 2) Mechanical Drawing.....	26
Figure 17. Power Connectors.....	27
Figure 18. ATX 24-Pin Main Power Connector (PWR1).....	27
Figure 19. SS1 8-Pin CPU 0 Power Connector (PW1).....	28
Figure 20. SSI 8-Pin CPU 1 Power Connector (PW2) .....	28
Figure 21. Onboard Temperature Sensor Locations.....	29
Figure 22. System Fan Connectors.....	32
Figure 23. 4-Pin System Fan Connector Pinout .....	32
Figure 24. Remote Management Port.....	38
Figure 25. BIOS Setup Utility's BMC LAN Configuration Screen .....	38
Figure 26. BIOS Setup Utility's User Configuration Screen .....	39
Figure 27. Example of BMC Station IP Address in the BIOS Setup Utility .....	40
Figure 28. Integrated BMC Web Console – Login Screen.....	40
Figure 29. Integrated BMC Web Console Login Page .....	42
Figure 30. Integrated BMC Web Console – Main Console View .....	42
Figure 31. Component Reference Diagram for PHM and Processor Socket Assemblies .....	46
Figure 32. PHM Placement onto Processor Socket.....	47
Figure 33. 3 <sup>rd</sup> Gen Intel® Xeon® Scalable Processor Identification.....	48
Figure 34. Processor Socket Identification.....	50
Figure 35. Standard SDRAM DDR4 DIMM.....	51
Figure 36. Server Board Memory Slot Association by CPU .....	52
Figure 37. Processor Memory Slot Support Overview .....	52
Figure 38. PCIe* Subsystem Architecture Block Diagram .....	58
Figure 39. Riser Card Slots .....	60

Figure 40. Back Panel Network Connectivity.....	61
Figure 41. OCP* Mezzanine 2.0 Add-in Card Support.....	62
Figure 42. Storage Interface Support Architecture.....	63
Figure 43. Internal USB 3.0 Type A connector.....	64
Figure 44. M.2 SSD Placement .....	64
Figure 45. M.2 NVMe* SSD Accessory Clip Placement.....	64
Figure 46. SATA Interface Cable Connectors .....	65
Figure 47. PCIe* SlimSAS* Connectors .....	68
Figure 48. NVMe* Storage Bus Event / Error Handling.....	68
Figure 49. Intel® VROC Key Insertion.....	70
Figure 50. BIOS Setup Utility Security Tab.....	73
Figure 51. TPM Module Placement.....	77
Figure 52. Intel® Light-Guided Diagnostics – LED Identification .....	91
Figure 53. CPU Fault LED Identification.....	91
Figure 54. Reset and Recovery Jumper Header Locations.....	93
Figure 55. Server Board Mounting Hole Locations .....	97
Figure 56. Possible Server Board Mounting Options.....	98
Figure 57. Server Board Rear I/O Connectors.....	99
Figure 58. Rear I/O Shield Placement.....	99
Figure 59. Processor Heat Sink Handling.....	100
Figure 60. PHM Assembly Removal from Processor Socket.....	101
Figure 61. Processor Socket Cover Installation.....	101
Figure 62. Processor Removal from PHM Assembly.....	102
Figure 63. Processor Carrier Clip Removal from PHM Assembly.....	102
Figure 64. Installing Processor Carrier Clip onto Processor – Part 1.....	103
Figure 65. Installing Processor Carrier Clip onto Processor – Part 2.....	103
Figure 66. Processor Heat Sink Handling.....	104
Figure 67. Processor Heat Sink Anti-tilt Wires in the Outward Position.....	104
Figure 68. Pin 1 Indicator of Processor Carrier Clip.....	105
Figure 69. Processor Socket Cover Removal.....	105
Figure 70. PHM Alignment with Processor Socket Assembly .....	106
Figure 71. PHM Installation onto Server Board.....	106
Figure 72. Tighten Heat Sink Fasteners.....	107
Figure 73. Memory Module Removal.....	107
Figure 74. DIMM Installation.....	108

## List of Tables

Table 1. Intel® Server M20NTP Family Reference Documents and Support Collaterals .....	13
Table 2. Intel® Server Board M20NTP2SB Features .....	16
Table 3. Thermal Sensor List.....	30
Table 4. POST Hot Keys.....	33
Table 5. 3 <sup>rd</sup> Gen Intel® Xeon® Scalable Processor Family Feature Comparison .....	49
Table 6. Supported DDR4 DIMM Memory .....	51
Table 7. Maximum Supported Standard SDRAM DIMM Speeds by Processor Shelf .....	52
Table 8. DDR4 DIMM Attributes Table for “Identical” and “Like” DIMMs .....	54
Table 9. Recommended DDR4 DIMM per Socket Population Configurations.....	55
Table 10. Memory RAS Features .....	56
Table 11. Compatibility of RAS Features Intel® SGX, Intel® TME, and Intel® TME-MT .....	57
Table 12. Processor / PCH PCIe* Port Routing.....	59
Table 13. RJ45 LAN Connector Link/Activity LEDs.....	61
Table 14. SATA and sSATA Controller Feature Support.....	66
Table 15. CPU to PCIe* NVMe* SlimSAS* Connector Routing .....	69
Table 16. Optional Intel® VROC for NVMe Upgrade Key Features.....	70
Table 17. Supported Video Resolutions .....	71
Table 18. Orderable TPM Accessory Kits.....	77
Table 19. Control Panel Cable Header Pinout.....	81
Table 20. Onboard USB 3.0 Cable Connector Pinout.....	82
Table 21. Onboard DH10 Serial COM2 Connector Pinout .....	83
Table 22. Serial COM2 Configuration Jumpers.....	84
Table 23. Onboard VGA Cable Header Pinout.....	84
Table 24. PSMI Cable Connector Pinout.....	85
Table 25. IPMB Cable Connector Pinout.....	85
Table 26. sSATA (4 and 5) SGPIO Cable Header Pinout.....	86
Table 27. sSATA Port 4 Cable Connector Pinout .....	86
Table 28. sSATA Port 5 Cable Connector Pinout .....	87
Table 29. sSATA Ports 0–3 Mini-SAS* HD Cable Connector Pinout.....	87
Table 30. SATA Ports 0–7 Dual Mini-SAS* HD Cable Connector Pinout .....	88
Table 31. PCIe* NVMe* Port 0 Cable Connector Pinout .....	89
Table 32. PCIe* NVMe* Port 1 Cable Connector Pinout .....	90
Table 33. PCIe* NVMe* Port 2 Cable Connector Pinout .....	90
Table 34. PCIe* NVMe* Port 3 Cable Connector Pinout .....	90
Table 35. Onboard LED Descriptions .....	92
Table 36. Server Board Mounting Screw Torque Requirements .....	98
Table 37. Server Board Components the Store Volatile/Non-Volatile Data.....	116

# 1. Introduction

---

This technical product specification (TPS) describes the features, functions, architecture, and support specifications of the Intel® Server Board M20NTP2SB.

---

**Note:** The Intel Server Board M20NTP2SB is available as a board only product or as a system component within the Intel® Server System M20NTP1UR. This document provides information related to the server board only. For complete Intel server system information, reference content from this document in addition to information in the appropriate Intel system TPS.

---

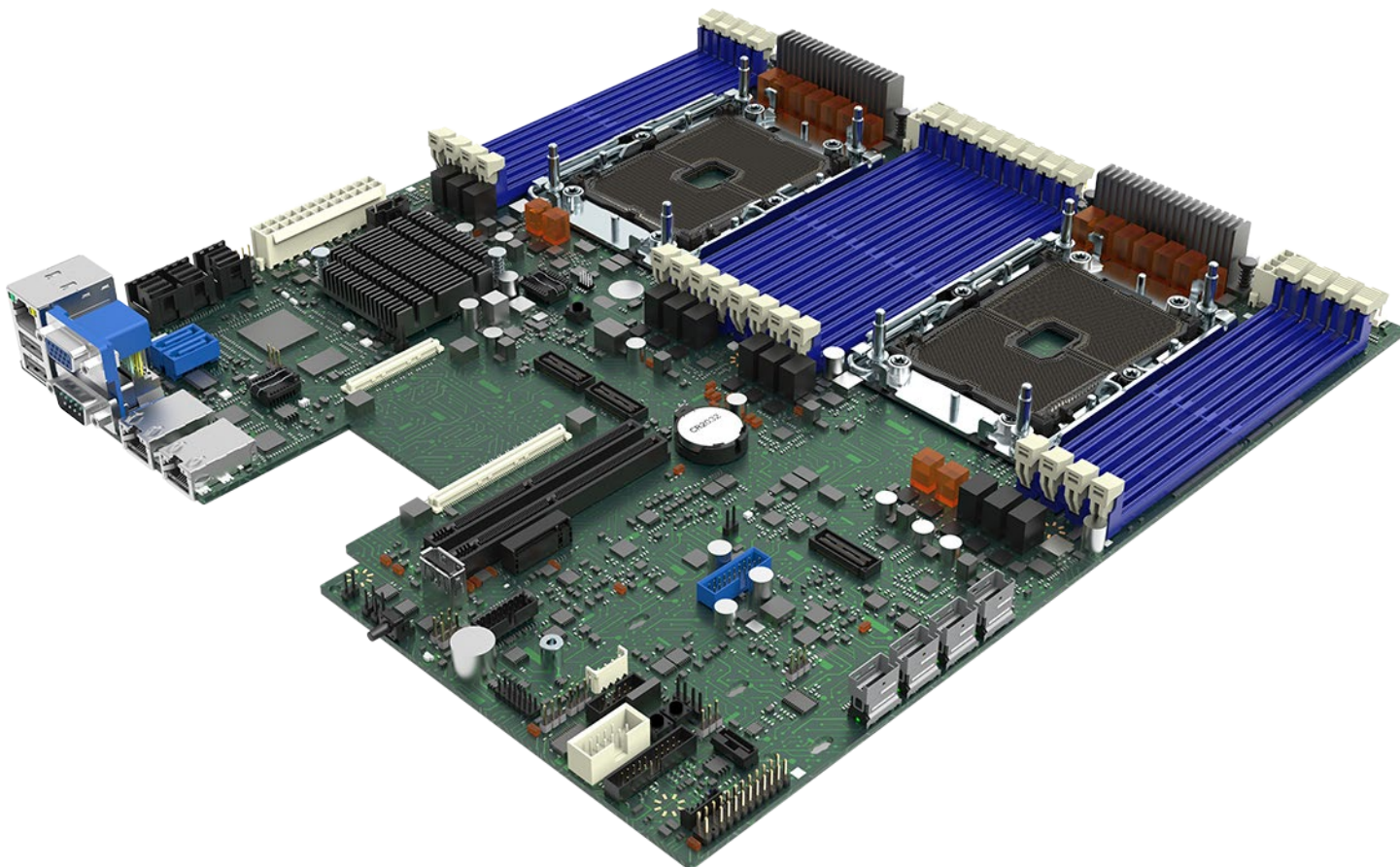


Figure 1. Intel® Server Board M20NTP2SB

## 1.1 Reference Documents

For additional information and other support collaterals related to this Intel server product, see [Table 1](#). Listed documents and utilities can be downloaded from the following Intel web sites or can be ordered through your local Intel support representative.

<https://www.intel.com/content/www/us/en/design/resource-design-center.html>

---

**Note:** Some of the Intel documents listed in [Table 1](#) are classified as “Intel Confidential”. These documents are only made available under a nondisclosure agreement (NDA) with Intel. With an appropriate NDA in place, listed classified documents can be downloaded from the Intel Resource and Design Center web site at the following link: <https://www.intel.com/content/www/us/en/design/resource-design-center.html>

---



**Table 1. Intel® Server M20NTP Family Reference Documents and Support Collaterals**

Topic	Document Title or Support Collateral	Document Classification
Server-board-level architectural and features overview	<i>Intel® Server Board M20NTP Technical Product Specification</i>	Public
System-level architectural and features overview	<i>Intel® Server System M20NTP1UR Technical Product Specification</i>	Public
System integration and service instructions	<i>Intel® Server System M20NTP1UR System Integration and Service Guide</i>	Public
Available options, spares, accessories.	<i>Intel® Server M20NTP Family Configuration Guide</i>	Public
BIOS setup utility overview	<i>Intel® Server M20NTP Family BIOS Setup Utility User Guide</i>	Public
Integrated BMC Web Console	<i>Integrated Baseboard Management Controller Web Console (Integrated BMC Web Console) User Guide for Intel® Server Boards</i>	Public
Base specifications for the IPMI architecture and interfaces	<i>Intelligent Platform Management Interface Specification Second Generation, version 2.0</i>	Intel Confidential
Specifications for the PCIe* 3.0 architecture and interfaces	<i>PCIe Base Specification, revision 3.0</i> <a href="http://www.pcisig.com/specifications">http://www.pcisig.com/specifications</a>	Public
Specifications for the PCIe* 4.0 architecture and interfaces	<i>PCIe Base Specification, revision 4.0</i> <a href="http://www.pcisig.com/specifications">http://www.pcisig.com/specifications</a>	Public
Specification for OCP*	<i>Open Compute Project (OCP) Specification</i>	Intel Confidential
TPM for PC Client specifications	<i>TPM PC Client Specifications, revision 2.0</i>	Intel Confidential
Functional specifications of 3 <sup>rd</sup> Gen Intel® Xeon® Scalable processor family	<i>3<sup>rd</sup> Generation Intel® Xeon® Scalable Processors, Codename Ice Lake-SP External Design Specification (EDS) – Documents IDs: 574451, 574942, 575291</i>	Intel Confidential
Processor thermal design specifications and recommendations	<i>3<sup>rd</sup> Generation Intel® Xeon® Scalable Processor, Codename Ice Lake-SP and Cooper Lake-SP – Thermal and Mechanical Specifications and Design Guide (TMSDG) – Document ID 574080</i>	Intel Confidential
Intel® Virtual RAID on CPU (VROC)	<i>Intel® Virtual RAID on CPU (VROC) Technical Product Specification (TPS)</i>	Intel Confidential
	<i>Intel® Virtual RAID on CPU (VROC) User Guide</i>	Public
BIOS and BMC security best practices	<i>Intel® Server Systems Baseboard Management Controller (BMC) and BIOS Security Best Practices White Paper</i> <a href="https://www.intel.com/content/www/us/en/support/articles/000055785/server-products.html">https://www.intel.com/content/www/us/en/support/articles/000055785/server-products.html</a>	Public
Managing an Intel server overview	<i>Managing an Intel® Server System 2020</i> <a href="https://www.intel.com/content/www/us/en/support/articles/000057741/server-products.html">https://www.intel.com/content/www/us/en/support/articles/000057741/server-products.html</a>	Public
Latest system software updates: BIOS and firmware	<i>Intel® Server Update Package (SUP) for Intel® Server M20NTP Family</i>	Public
	<i>Intel® Server Firmware Update Utility – Various operating system support</i>	
	<i>Intel® Server Firmware Update Utility User Guide</i>	
To obtain full system information	<i>Intel® Server Information Utility</i>	Public
	<i>Intel® Server Information Utility User Guide</i>	
To configure, save, and restore various system options	<i>Intel® Server Configuration Utility – Various operating system support</i>	Public
	<i>Intel® Server Configuration Utility User Guide</i>	
Product warranty information	<i>Warranty Terms and Conditions</i> <a href="https://www.intel.com/content/www/us/en/support/services/000005886.html">https://www.intel.com/content/www/us/en/support/services/000005886.html</a>	Public

Intel® Server Board M20NTP2SB Technical Product Specification

Topic	Document Title or Support Collateral	Document Classification
Intel® Data Center Manager (Intel® DCM) information	<i>Intel® Data Center Manager (Intel® DCM) Product Brief</i> <a href="https://software.intel.com/content/www/us/en/develop/download/dcm-product-brief.html">https://software.intel.com/content/www/us/en/develop/download/dcm-product-brief.html</a>	Public
	<i>Intel® Data Center Manager (Intel® DCM) Console User Guide</i> <a href="https://software.intel.com/content/www/us/en/develop/download/dcm-user-guide.html">https://software.intel.com/content/www/us/en/develop/download/dcm-user-guide.html</a>	Public

## 2. Server Board Overview

The Intel® Server Board M20NTP2SB is a monolithic printed circuit board assembly with features that are intended for high density rack mount server systems. This server board is designed to support the 3rd Gen Intel® Xeon® Scalable processor family. Previous generation Intel® Xeon® processor and Intel® Xeon® Scalable processor families are not supported.

This chapter provides an overview of the Intel® Server Board M20NTP2SB. It identifies board features, provides mechanical dimensional diagrams, and provides a general overview of the board architecture.

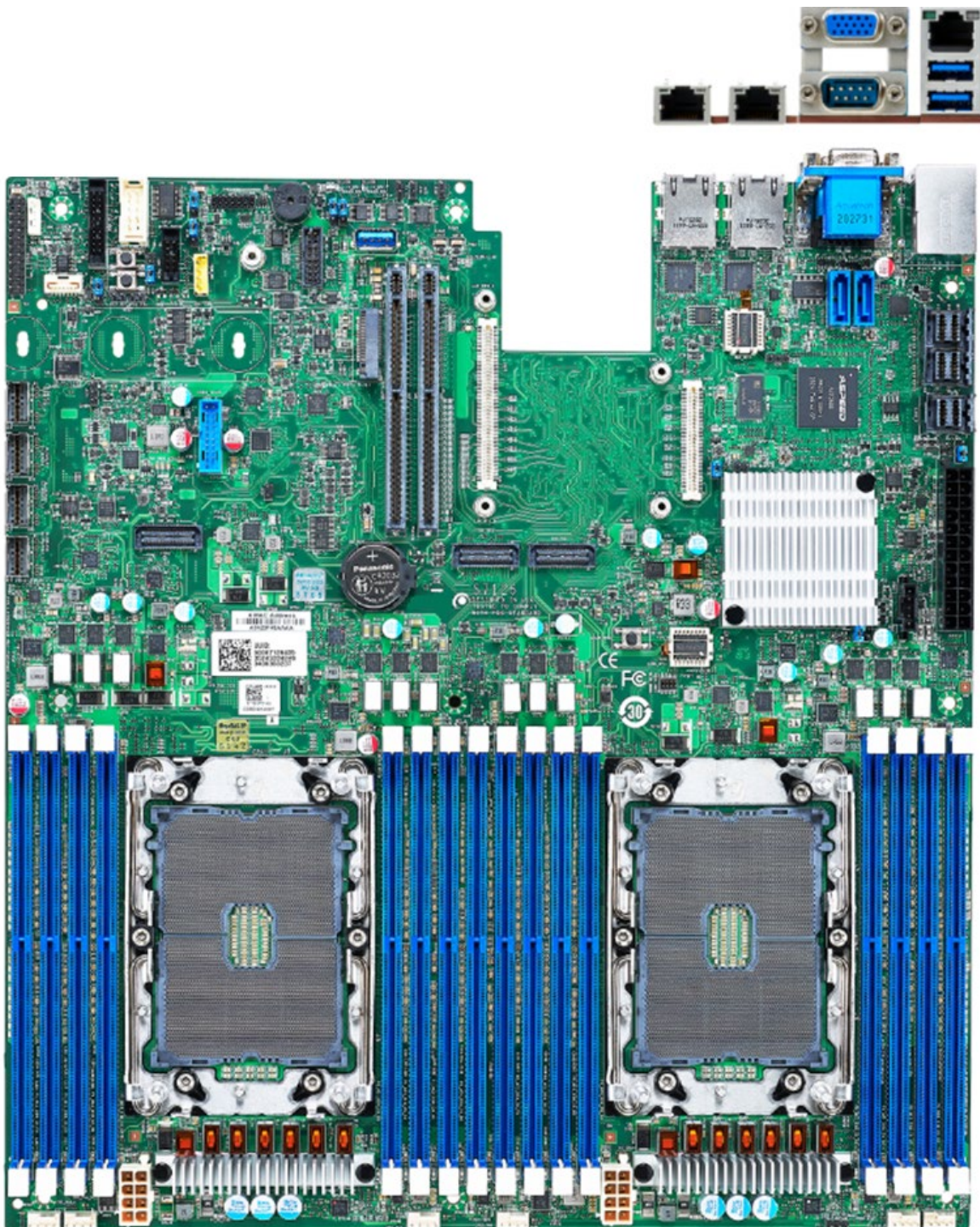


Figure 2. Intel® Server Board M20NTP2SB Overview

## 2.1 Server Board Feature Set

The following table provides a high-level feature overview of the Intel® Server Board M20NTP2SB.

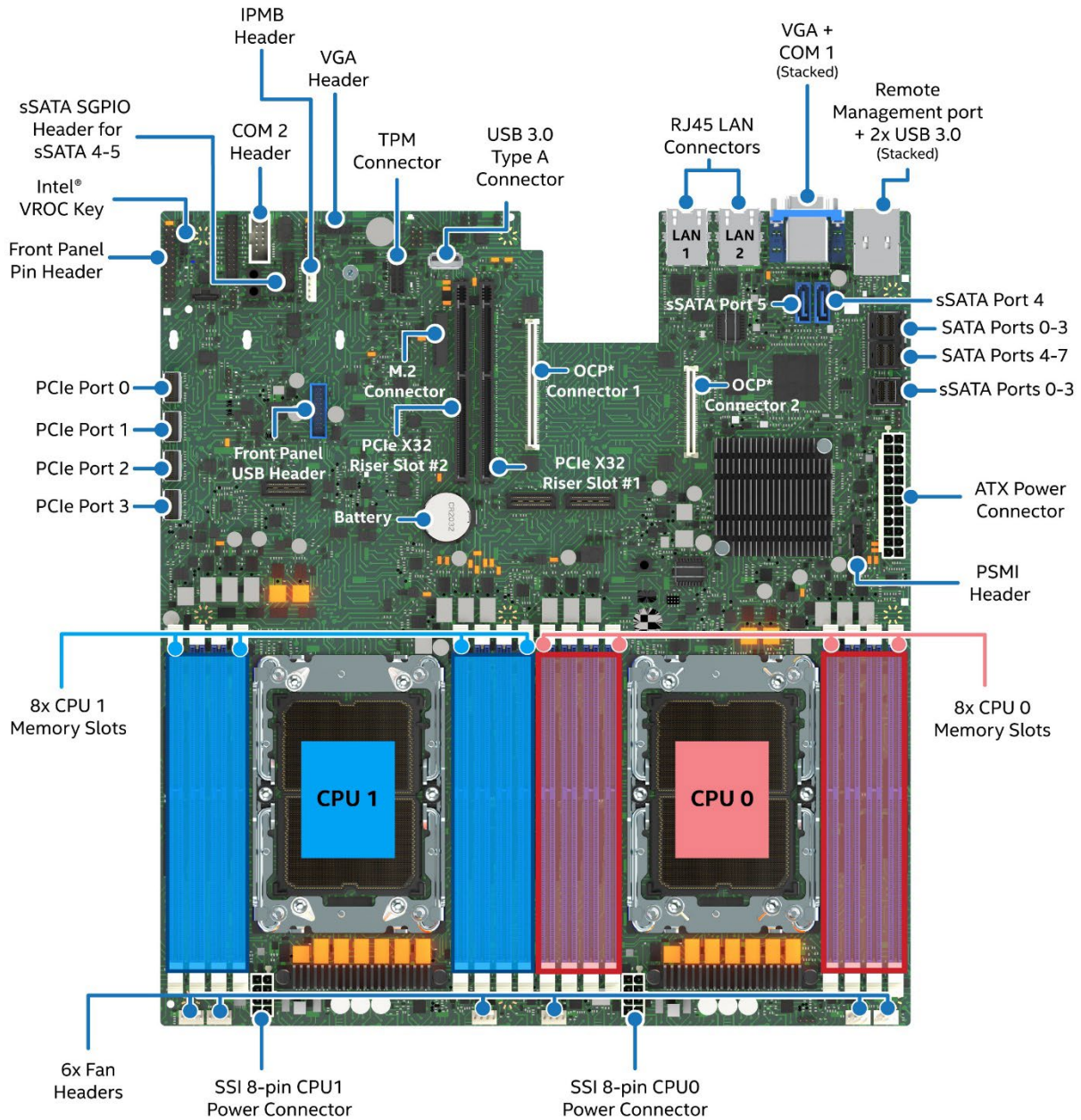
**Table 2. Intel® Server Board M20NTP2SB Features**

Feature	Details
<b>Server Board</b>	Intel® Server Board M20NTP2SB
<b>Server Board Dimensions</b>	333.2 mm X 306.8 mm (13.1" X 12")
<b>Processor Support</b>	<ul style="list-style-type: none"> <li>• Dual Socket-P4 LGA4189</li> <li>• 3<sup>rd</sup> Gen Intel Xeon Scalable processor family:               <ul style="list-style-type: none"> <li>• Intel® Xeon® Platinum 8300 processor</li> <li>• Intel® Xeon® Gold 6300 processor</li> <li>• Intel® Xeon® Gold 5300 processor</li> <li>• Intel® Xeon® Silver 4300 processor</li> </ul> </li> <li>• <b>Note:</b> 3<sup>rd</sup> Gen Intel® Xeon® Scalable processor SKUs ending in (H), (L), (U), or (Q) are not supported.</li> <li>• Intel® UPI links: up to three at 11.2 GT/s (Platinum and Gold families) or up to two at 10.4 GT/s (Silver family)</li> </ul> <p><b>Note:</b> Previous generation Intel® Xeon® processors are not supported.</p>
<b>Maximum Supported Processor Thermal Design Power (TDP)</b>	<ul style="list-style-type: none"> <li>• 250 W (Server board only)</li> </ul> <p><b>Note:</b> The maximum supported processor TDP at the system level may be lower than what the server board can support. Design limits of the chosen server chassis / system will determine the maximum processor TDP that can be supported up to the 250W processor TDP limit of the server board. Reference the chosen server chassis/system documentation for specific processor support limits.</p>
<b>PCH Chipset</b>	<ul style="list-style-type: none"> <li>• Intel® C621A Platform Controller Hub (PCH) chipset</li> <li>• Embedded features enabled on this server board:               <ul style="list-style-type: none"> <li>• SATA support</li> <li>• USB support</li> <li>• PCIe support</li> </ul> </li> </ul>
<b>Server Management Processor (SMP)</b>	<ul style="list-style-type: none"> <li>• Aspeed AST2500* Advanced PCIe Graphics and Remote Management Processor</li> <li>• Embedded features enabled on this server board:               <ul style="list-style-type: none"> <li>• Baseboard Management Controller (BMC)</li> <li>• 2D Video Graphics Adapter</li> </ul> </li> </ul>
<b>Memory Support</b>	<ul style="list-style-type: none"> <li>• 16 memory slots</li> <li>• 8 DIMM slots per processor (2 processors)</li> <li>• Eight memory channels per processor</li> <li>• One slot per memory channel</li> <li>• Registered DDR4 (RDIMM), 3DS-RDIMM, Load Reduced DDR4 (LRDIMM), 3DS-LRDIMM</li> <li>• <b>Note:</b> 3DS = 3-Dimensional Stacking</li> <li>• All DDR4 DIMMs must support ECC</li> <li>• Up to 3200 MT/s (processor SKU dependent)</li> <li>• Memory voltage = 1.2 V</li> </ul>
<b>Network Connectivity</b>	<ul style="list-style-type: none"> <li>• Onboard Intel® Ethernet Controller I210-AT</li> <li>• Two (2) RJ45 1000 Base-T ports (Back panel I/O)</li> </ul>
<b>PCIe* Expansion</b>	<ul style="list-style-type: none"> <li>• Two (2) X32 PCIe 4.0 Riser Card slots</li> </ul> <p>Refer to the <i>Intel® Server M20NTP Family Configuration Guide</i> for available 1U PCIe riser card accessory options for Intel server products.</p> <ul style="list-style-type: none"> <li>• Support for one (1) OCP 2.0 Mezzanine add-in card</li> </ul> <p>Refer to the <i>Intel® Server M20NTP Family Configuration Guide</i> for supported OCP add-in options</p>



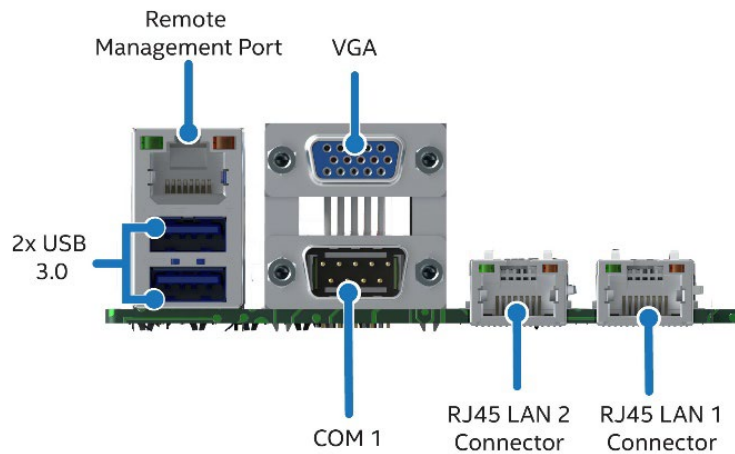
Feature	Details
<b>Storage Connectivity Options</b>	<p><b>NVMe* support</b></p> <ul style="list-style-type: none"> <li>• Four (4) onboard SFF-8654 SlimSAS* cable connectors. Each connector supports backplane connectivity for one PCIe NVMe SSD</li> <li>• One (1) onboard PCIe NVMe M.2 SSD connector. Supports 42 mm, 80 mm, or 110 mm SSD</li> <li>• Embedded support for Intel® Volume Management Device (Intel® VMD) 2.0 for NVMe</li> <li>• Optional support for Intel® Virtual RAID on CPU 7.5 (Intel® VROC) for NVMe. (Accessory option)</li> </ul> <p><b>SATA Support – Up to 14 SATA 6 GB/s drives</b></p> <ul style="list-style-type: none"> <li>• Three (3) onboard quad port SFF-8643 Mini-SAS* HD cable connectors. Each connector supports backplane connectivity for 4 SATA devices</li> <li>• Two (2) onboard single port 7-pin cable connectors</li> <li>• Embedded support for Intel® Virtual RAID on CPU 7.5 (Intel® VROC) for SATA. Supported RAID Levels: 0, 1, 5, 10</li> </ul>
<b>Video Support</b>	<ul style="list-style-type: none"> <li>• Embedded 2D video controller</li> <li>• One (1) VGA DB-15 cable connector (Back panel I/O)</li> <li>• One (1) VGA 14-pin onboard cable header (Front Panel VGA support)</li> <li>• 128 MB of DDR4 video memory</li> <li>• Up to 1920 x 1200 resolution</li> </ul>
<b>USB Support</b>	<ul style="list-style-type: none"> <li>• Two (2) external USB 3.0 connectors (Back panel I/O)</li> <li>• One (1) USB 3.0 internal onboard Type-A connector</li> <li>• One (1) onboard 20-pin cable connector for optional front panel 2x USB 3.0 ports</li> </ul>
<b>Serial Ports</b>	<ul style="list-style-type: none"> <li>• One (1) DB-9 Serial COM1 port cable connector (Back panel I/O)</li> <li>• One (1) onboard DH-10 Serial COM2 port header for optional front or rear serial port support. The port follows DTK pinout specifications.</li> </ul>
<b>Fan Support</b>	<ul style="list-style-type: none"> <li>• Six (6) 4-pin system fan connectors</li> <li>• Managed fan speed control</li> <li>• Enabled (Default) with Intel Server Systems</li> <li>• Disabled (Default) for system using Non-Intel chassis. Can be configured using embedded server management features of the BMC. See <a href="#">Section 3.6</a></li> </ul>
<b>Server Management</b>	<ul style="list-style-type: none"> <li>• Integrated Baseboard Management Controller (BMC)</li> <li>• Dedicated RJ45 1 GbE remote management port (Back panel I/O)</li> <li>• Onboard Light Guided Diagnostics</li> <li>• Integrated BMC Web Console for Intel server products</li> <li>• Intelligent Platform Management Interface (IPMI) 2.0 compliant</li> <li>• Support for Intel® Data Center Manager (DCM)</li> <li>• Support for Intel® Server Debug and Provisioning Tool (Intel® SDP Tool)</li> <li>• Redfish* compliant</li> <li>• Customizable BMC management support for server systems using non-Intel server chassis</li> <li>• Sensor monitoring</li> <li>• Fan speed control</li> </ul>
<b>Security</b>	<ul style="list-style-type: none"> <li>• Intel® Software Guard Extensions (Intel® SGX)</li> <li>• Converged Intel® Boot Guard and Trusted Execution Technology (Intel® TXT)</li> <li>• Intel® Total Memory Encryption (Intel® TME)</li> <li>• Trusted platform module (TPM 2.0) Support</li> <li>• Accessory option: Standard – iPC <b>JNPTPM</b> (Not compatible in China)</li> <li>• Accessory option: China Compatible – iPC <b>JNPTPMCH</b></li> </ul> <p><b>Note:</b> Available TPM Accessories are not supported by Microsoft* Windows Server 2022</p>
<b>Onboard Jumper Blocks and Buttons</b>	<ul style="list-style-type: none"> <li>• System Buzzer Configuration Jumper</li> <li>• Serial Port Configuration Jumpers</li> <li>• Intel ME Recovery Jumper</li> <li>• Clear CMOS Button</li> <li>• System Reset Button</li> <li>• Power Button</li> </ul>
<b>Environment Limits</b>	<ul style="list-style-type: none"> <li>• Operating Temp: 10–35 °C (50–95 °F)</li> <li>• Non-Operating Temp: -40–70 °C (-40–158 °F)</li> <li>• Non-Operating Humidity: 90%, non-condensing at 35 °C</li> </ul>
<b>RoHS</b>	<ul style="list-style-type: none"> <li>• RoHS 6/6 Compliant: Yes</li> </ul>

## 2.2 Server Board Component / Feature Identification



Ref #: NTP10012

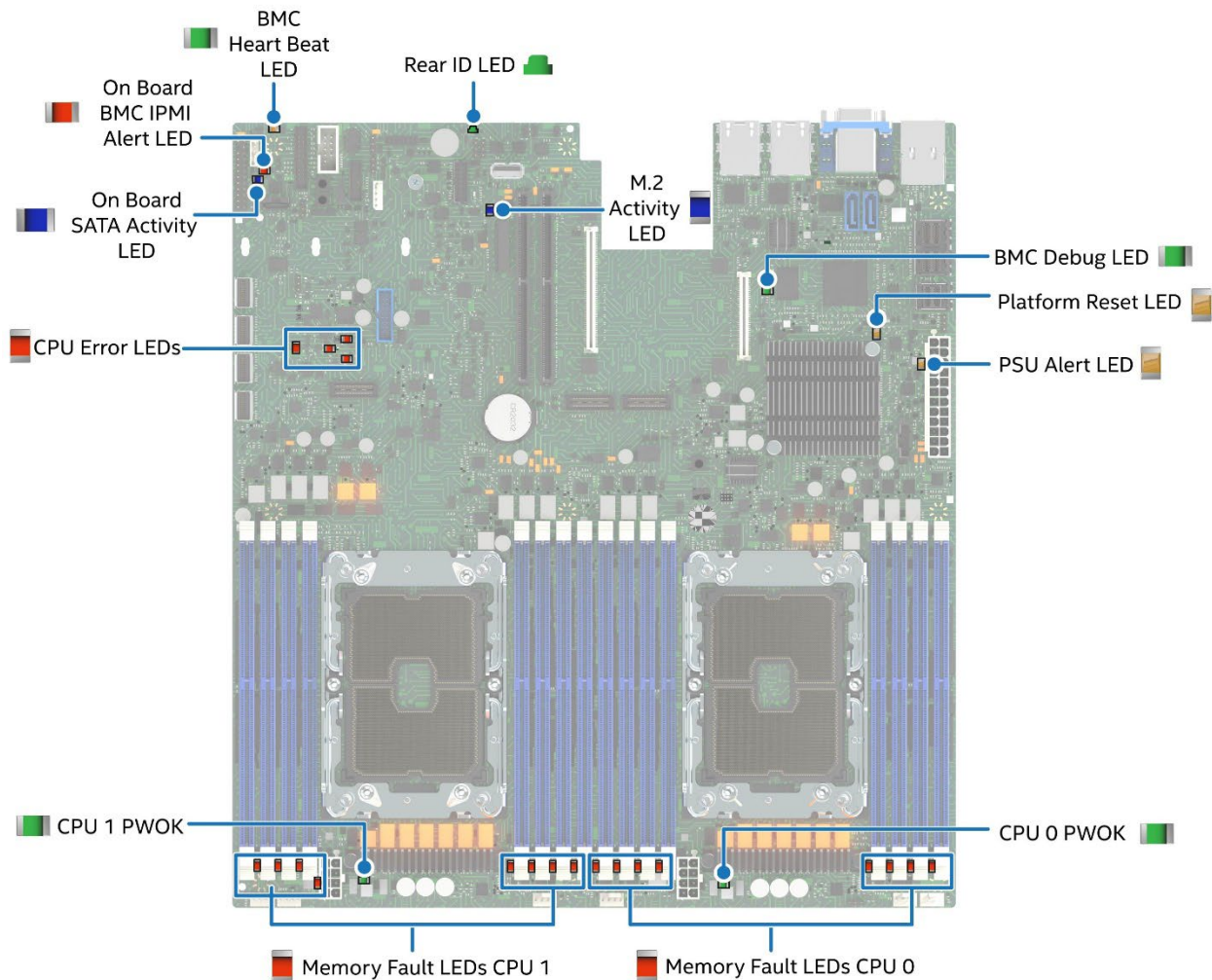
Figure 3. Intel® Server Board M20NTP2SB Component / Feature Identification



Ref #: NTP10021

**Figure 4. Back Panel Features Identification**

The server board includes LEDs to identify system status and/or indicate a component fault. For additional information, see [Chapter 13](#).

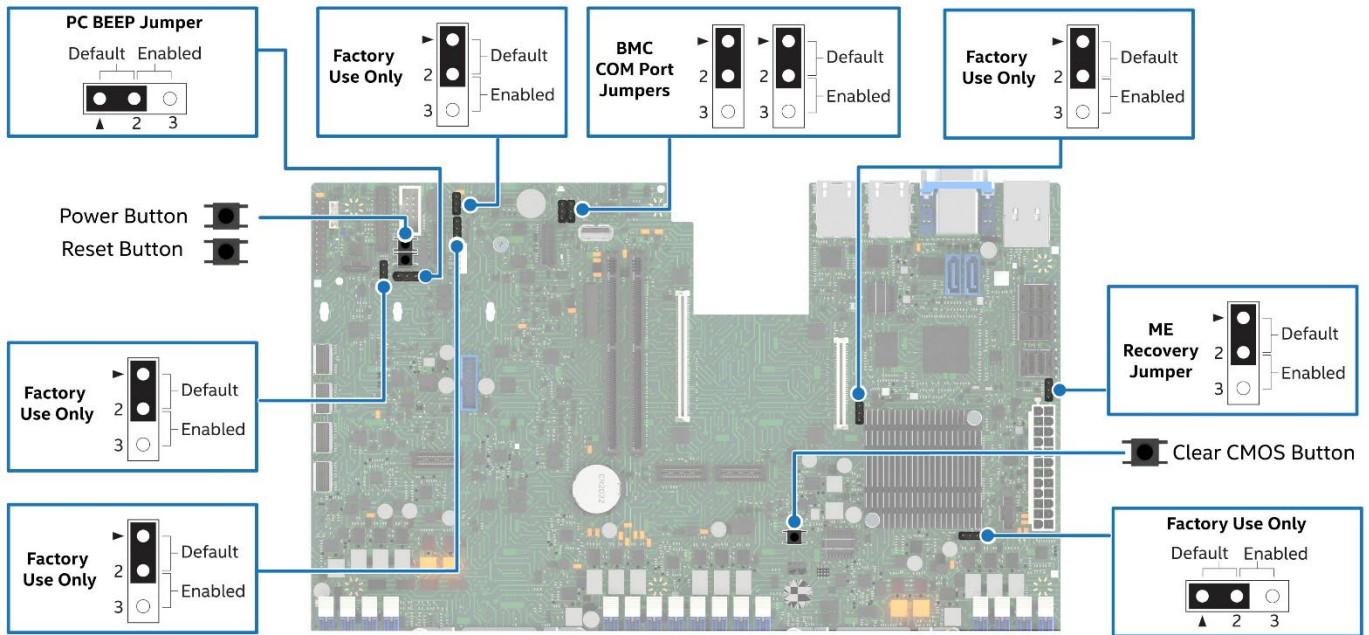


Ref #: NTP10082

**Figure 5. Intel® Light-Guided Diagnostics – LED Identification**



The server board includes several jumper blocks and onboard buttons (see [Figure 6](#)) that can be used to configure, protect, or recover specific features of the server board. For additional information, see [Chapter 14](#).



Ref #: NTP10092

**Figure 6. System Configuration and Recovery Features**



## 2.3 Server Board Architecture Overview

The architecture of the Intel® Server Board M20NTP2SB was developed around the integrated features and functions of the 3<sup>rd</sup> Gen Intel Xeon Scalable processor family, Intel® C621A PCH chipset, and the Aspeed® AST2500 Server Management Processor (SMP).

Figure 7 provides an overview of the Intel® Server Board M20NTP2SB architecture showing the features and interconnects of the major subsystem components. Refer to Figure 3 for an overview of the server board, identifying the physical location of these key feature and components.

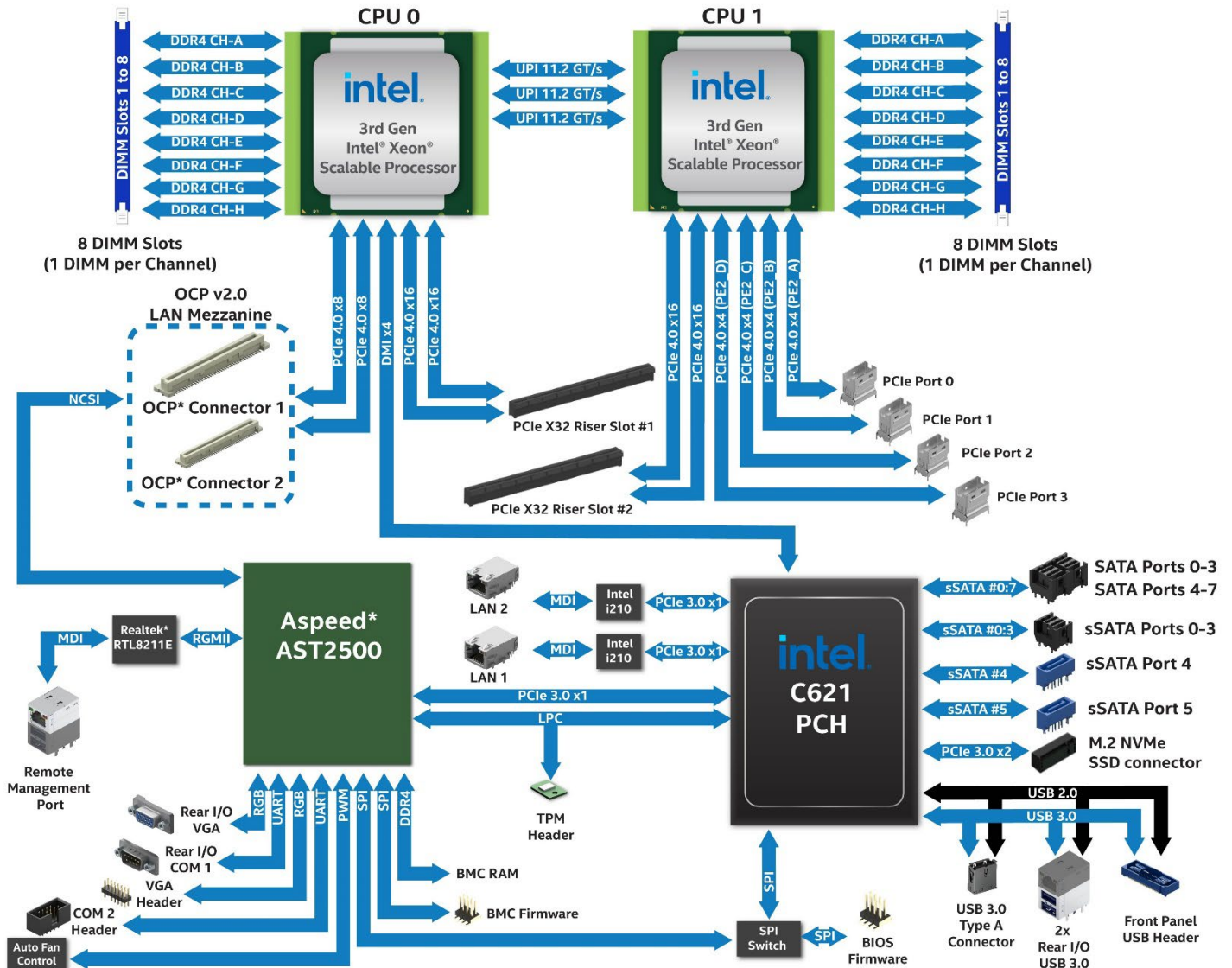


Figure 7. Intel® Server Board M20NTP2SB Architectural Block Diagram

### 3. Server Chassis Development Guidance

The Intel® Server Board M20NTP2SB is available as a board only product (Intel - iPC M20NTP2SB) allowing system architects and integrators to use it along with a non-Intel chassis to develop a customized server system. This chapter provides information that may be useful towards planning and development of these systems.

The Intel® Server Board M20NTP2SB was designed with features and architecture to be supported within a 1U rack mount server chassis.

---

**Note:** To support the design efforts of system architects and integrators with the development of a server chassis that is compatible with the Intel Server Board M20NTP2SB, Intel offers a 3D CAD assembly file (.STP format only) of the server board. The file is “Intel Confidential” and requires a signed NDA. Contact your local Intel representative for download access to this file.

---

#### 3.1 Server Board Dimensions

The dimensions of the Intel® Server Board M20NTP2SB conform to the Extended ATX (EATX) form factor: 13.1" x 12" (333.2 mm x 306.8 mm).

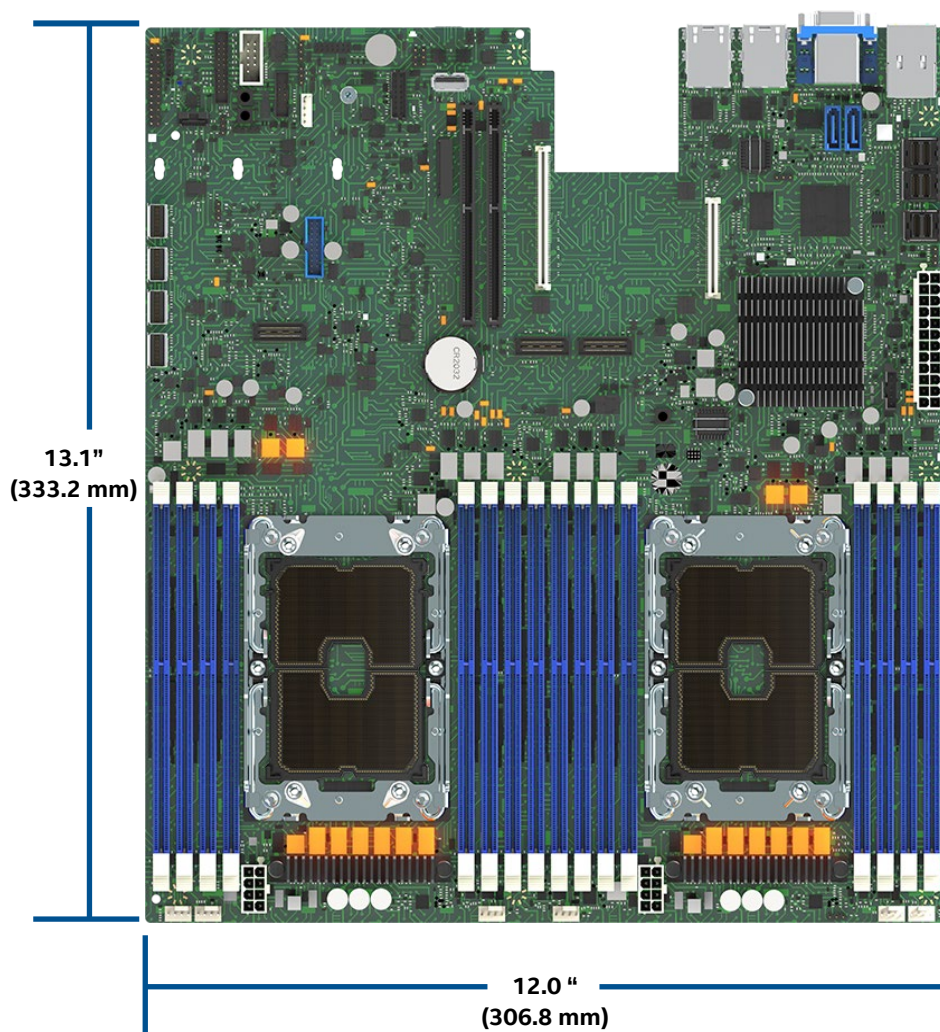


Figure 8. Intel® Server Board M20NTP2SB Board Dimensions

### 3.2 Server Board Mechanical Drawing

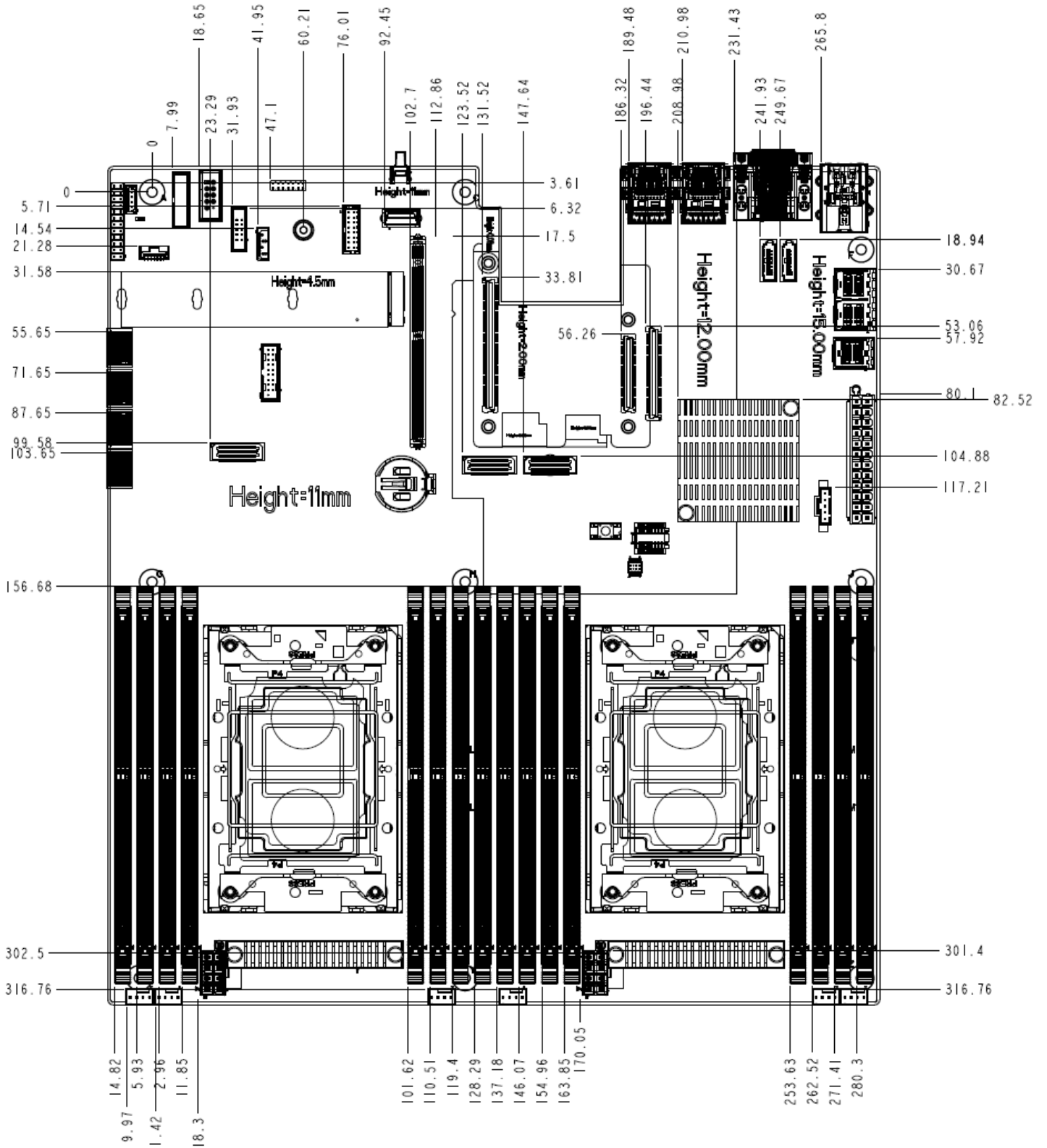
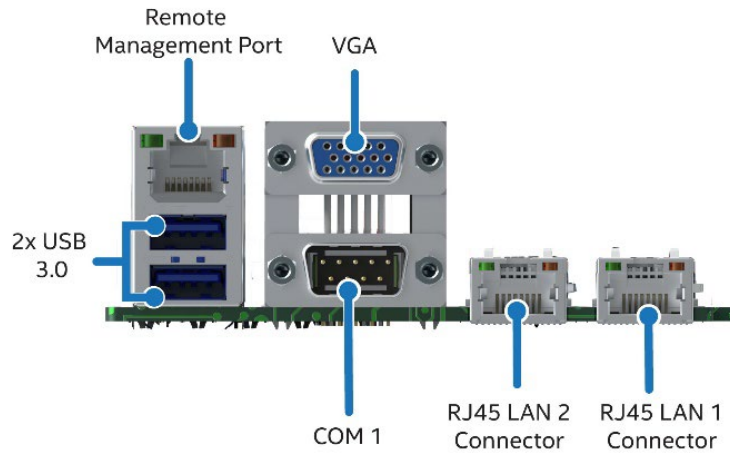


Figure 9. Server Board Mechanical Drawing

### 3.3 Rear I/O Connector and OCP\* Add-in Card Support

The selected server chassis must support one of two back panel design options to support the I/O features found on the back edge of the server board.



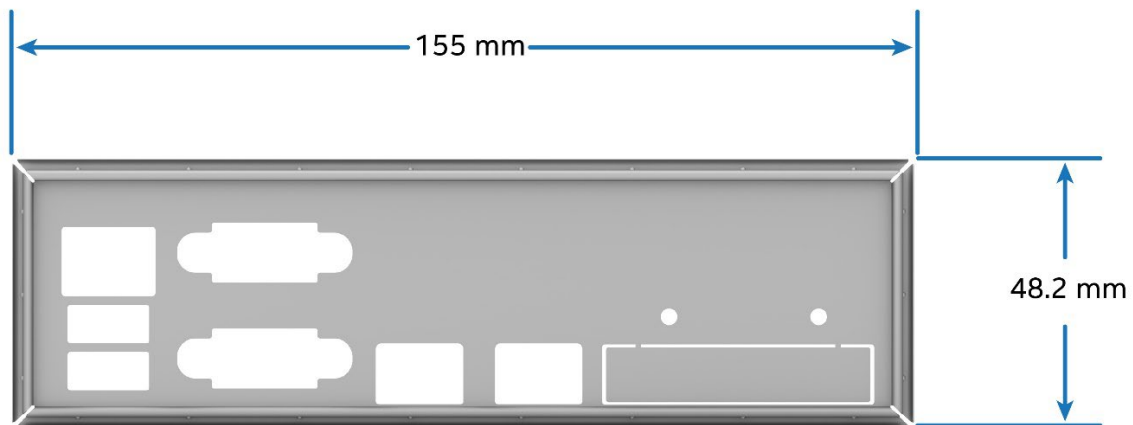
Ref #: NTP10021

- Option 1:** The chassis will have support for the installation of an I/O Shield with EATX defined X,Y dimensions as shown in the following figure. The I/O shield will include cut-outs for each external I/O connector found on the back edge of the server board. An additional knock-out panel can be included to support an optionally installed OCP Mezzanine add-in card.

---

**Note:** The server board (Intel - iPC M20NTP2SB) includes an EATX compatible I/O shield (as shown in the following figure) for use in non-Intel server chassis that support it.

---



Ref #: NTP40010

**Figure 10. Optional EATX Compatible Rear I/O Shield**

- Option 2:** The chassis back panel will include through hole mounting locations for each external rear I/O connector on the back edge of the server board. If OCP Mezzanine add-in card support is planned, then an additional cut-out must be included to support access to the ports of the OCP option as well.



### 3.4 PCIe\* Add-in Card Support

The server board has two PCIe X32 riser card slots. These slots are designed to support PCIe riser cards only. Attempting to install a PCIe add-in card directly into one of these slots may cause damage to the server board, the add-in card, or both.

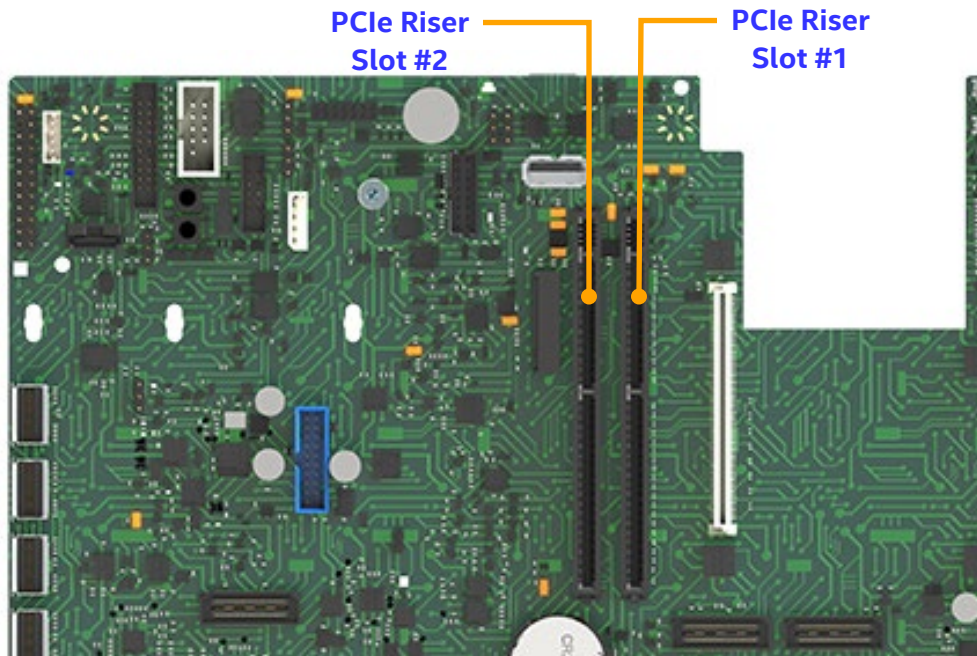


Figure 11. PCIe Riser Card Slots

PCIe add-in card(s) are oriented horizontally to the server board when installed to a riser card as shown in the following example.

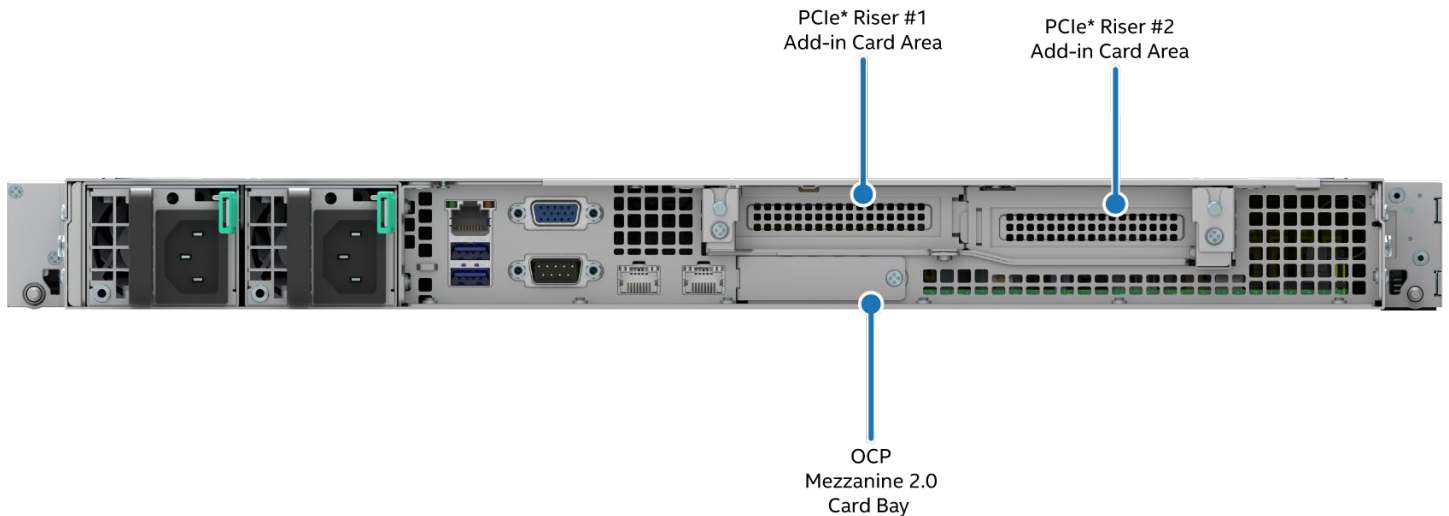


Figure 12. 1U Chassis Example – Add-in Card Orientation

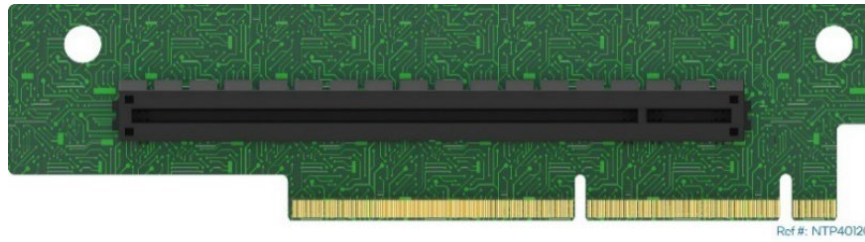
Ref #: NTP20211

**Note:** Riser Slot schematics are available by request under NDA.

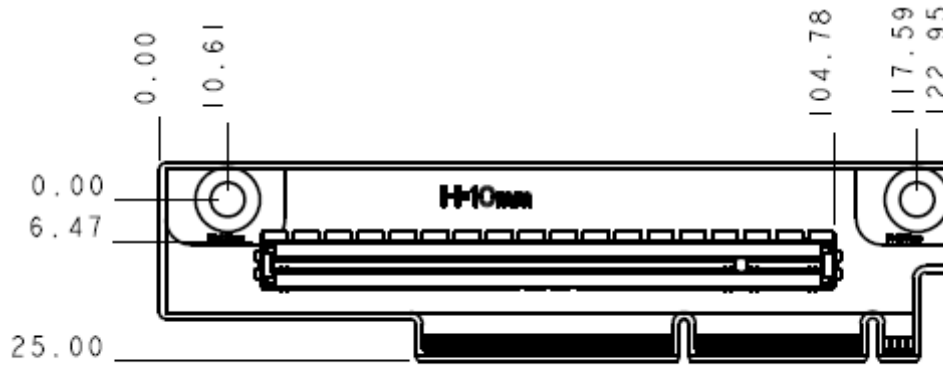
Riser cards developed for this server board are not interchangeable between the two riser card slots. Riser cards are specifically designed to be supported by Riser Slot 1 or Riser Slot 2.

Intel offers PCIe riser card accessory kits shown in the following subsections.

**3.4.1 1U 1-Slot PCIe\* Riser Card (Riser Slot 1) – iPC M20NTP1URISER1**



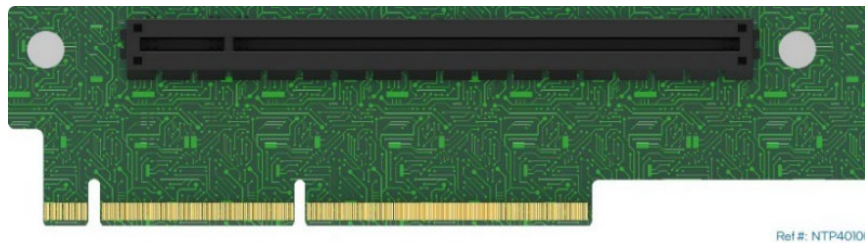
**Figure 13. 1U PCIe\* Riser Card (Riser Slot 1)**



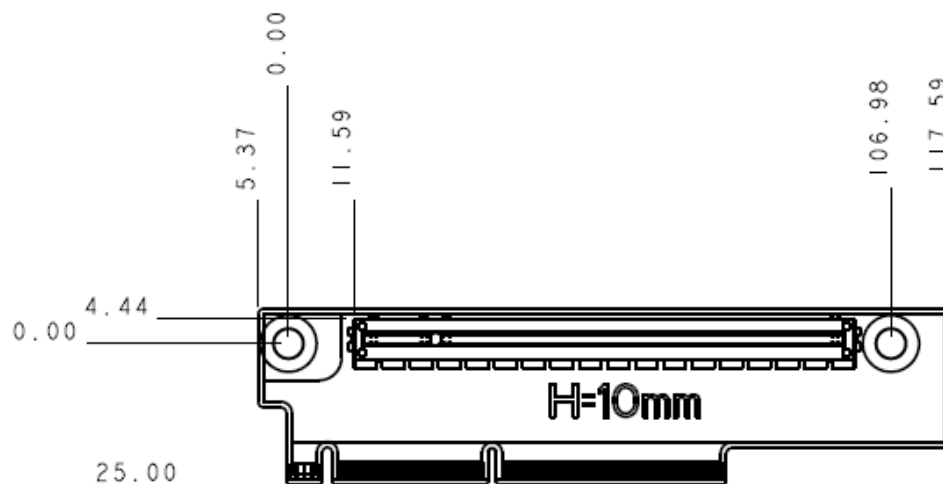
SCALE 1.000

**Figure 14. 1U PCIe\* Riser Card (Riser Slot 1) Mechanical Drawing**

**3.4.2 1U 1-Slot PCIe\* Riser Card (Riser Slot 2) – iPC M20NTP1URISER2**



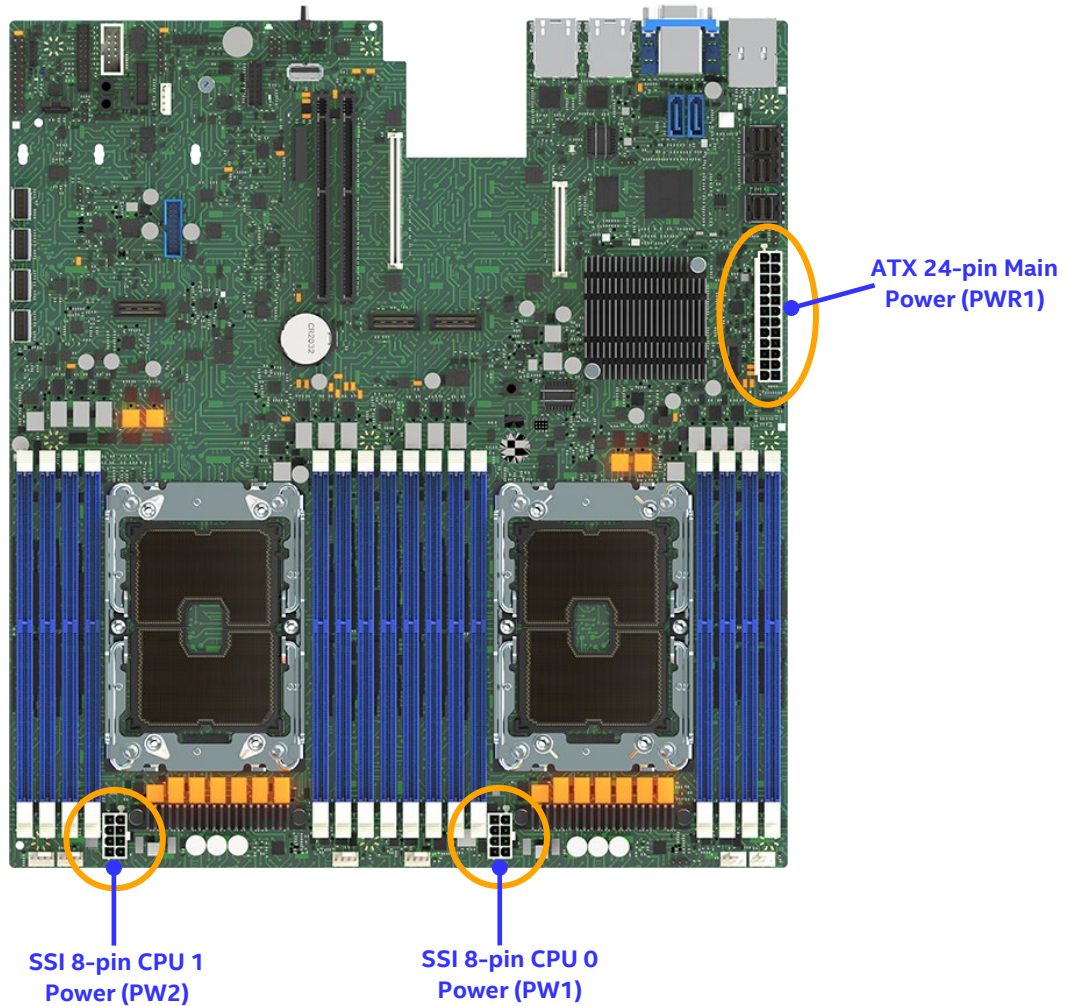
**Figure 15. 1U PCIe\* Riser Card (Riser Slot 2)**



**Figure 16. 1U PCIe\* Riser Card (Riser Slot 2) Mechanical Drawing**

### 3.5 Server Board Power

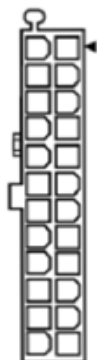
Power to support the features of the server board is supplied by three (3) onboard power-in connectors.



**Figure 17. Power Connectors**

The following figures provide the pinout definition for each power connector. The illustrations and pinout definition tables match the orientation and pin locations of the physical connectors on the server board. The Pin 1 location for each connector is identified by a black triangle.

▼ = Pin 1



Signal	Pin	Pin	Signal
VCC3	13	1	VCC3
VCC12N	14	2	VCC3
GND	15	3	GND
ATX_PS_ON_N	16	4	VCC5
GND	17	5	GND
GND	18	6	VCC5
GND	19	7	GND
NC_PWR1_20	20	8	ATX_PG
VCC5	21	9	VCC5_SB
VCC5	22	10	P12V_IN
VCC5	23	11	P12V_IN
GND	24	12	VCC3

**Figure 18. ATX 24-Pin Main Power Connector (PWR1)**

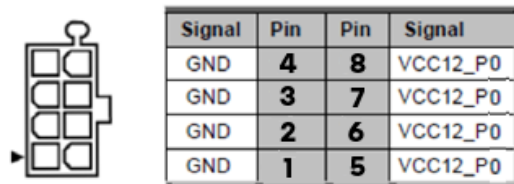


Figure 19. SS1 8-Pin CPU 0 Power Connector (PW1)

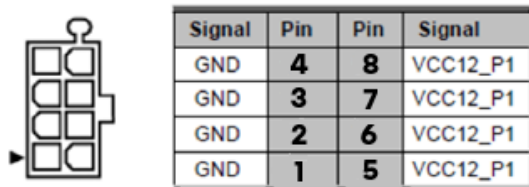


Figure 20. SSI 8-Pin CPU 1 Power Connector (PW2)

All three power connectors must be used to support all onboard features.

### 3.6 Thermal Management

---

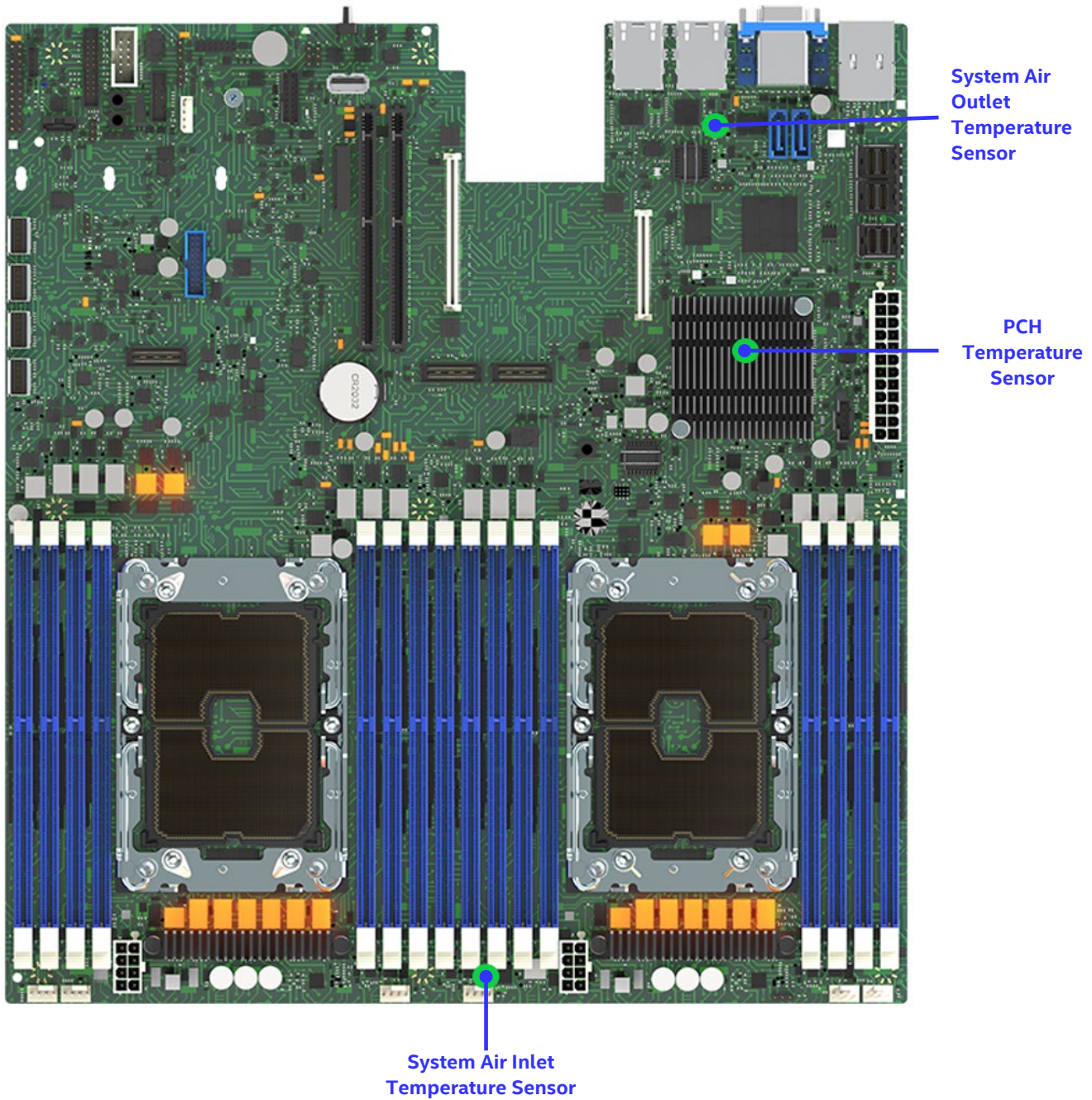
**Disclaimer:** Intel server boards contain and support several high-density VLSI and power delivery components that need adequate airflow to cool and remain within their thermal operating limits. Intel ensures through its own chassis development and testing that when an Intel server board and Intel 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 airflow 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.

---

The Intel® Server Board M20NTP2SB supports platform and thermal management using the features of the embedded baseboard management controller (BMC) of the Aspeed AST2500\* Advanced PCIe Graphics and Remote Management Processor.

The server board includes thermal sensors that can be monitored by the BMC. Some are mounted directly on to the server board (as shown in [Figure 21](#)), others are embedded within integrated peripheral components like processors, memory, and some system boards.





**Figure 21. Onboard Temperature Sensor Locations**

Additionally, the BMC can be programmed to monitor other sensor types within a system to support the desired thermal profiles of the chosen server configuration and operating environment. The following table lists all sensor types that can be monitored by the BMC for thermal management.

**Table 3. Thermal Sensor List**

Sensor Name String (SDR)	Sensor Description	SDR loaded using Generic Chassis Profile (Y/N)
P0 Abs Temp	CPU 0 Absolute Temperature	Y
P0 DTS Temp	CPU 0 DTS Temperature	Y
P1 Abs Temp	CPU 1 Absolute Temperature	Y
P1 DTS Temp	CPU 1 DTS Temperature	Y
PCH Temp	Chipset Temp sensor	Y
DIMM Thrm Mgn 1	DIMM Aggregate margin CPU0 ABCD (Max.)	Y
DIMM Thrm Mgn 2	DIMM Aggregate margin CPU0 EFGH (Max.)	Y
DIMM Thrm Mgn 3	DIMM Aggregate margin CPU1 ABCD (Max.)	Y
DIMM Thrm Mgn 4	DIMM Aggregate margin CPU1 EFGH (Max.)	Y
P0 Vcore VR Temp	P0 Vcore VR Temp	Y
P0 Vcore VR Mgn	P0 Vcore VR Thermal Margin	Y
P0 Vccio VR Temp	P0 Vccio VR Temp	Y
P0 Vccio VR Mgn	P0 Vccio VR Thermal Margin	Y
P1 Vcore VR Temp	P1 Vcore VR Temp	Y
P1 Vcore VR Mgn	P1 Vcore VR Thermal Margin	Y
P1 Vccio VR Temp	P1 Vccio VR Temp	Y
P1 Vccio VR Mgn	P1 Vccio VR Thermal Margin	Y
P0 DIMM VR Mgn 1	P0 DIMM ABCD VR Thermal Margin	Y
P0 DIMM VR Mgn 2	P0 DIMM EFGH VR Thermal Margin	Y
P1 DIMM VR Mgn 1	P1 DIMM ABCD VR Thermal Margin	Y
P1 DIMM VR Mgn 2	P1 DIMM EFGH VR Thermal Margin	Y
Front Panel Temp	Front Panel Temp	Y
OCP Air Temp	OCP Air Inlet Temp	Y
OCP Mod Temp	OCP Card Temp	Y
HSBP Temp	1U Hot-swap Backplane Temperature	Y
Riser R Temp	PCI Riser 1 Temperature	Y
Riser L Temp	PCI Riser 2 Temperature	Y
NVMe* Thrm Mgn	NVMe Aggregate Thermal Margin (Max.)	Y
SYS_FAN_1	Fan Speed of SYS_FAN_1	Y
SYS_FAN_2	Fan Speed of SYS_FAN_2	Y
SYS_FAN_3	Fan Speed of SYS_FAN_3	Y
SYS_FAN_4	Fan Speed of SYS_FAN_4	Y
SYS_FAN_5	Fan Speed of SYS_FAN_5	Y
SYS_FAN_6	Fan Speed of SYS_FAN_6	Y
PSU0_STATUS	Current status of PSU0	Y

Sensor Name String (SDR)	Sensor Description	SDR loaded using Generic Chassis Profile (Y/N)
PSU0_Temp	Temperature of PSU0	Y
PSU0_FAN	Fan Speed of PSU0	Y
PSU1_STATUS	Current status of PSU1	Y
PSU1_Temp	Temperature of PSU1	Y
PSU1_FAN	Fan Speed of PSU1	Y

BMC monitored sensors for a given server system configuration are enabled through .INI configuration files embedded within the BMC firmware.

The factory installed BMC firmware (and all subsequent BMC firmware updates released by Intel) will include system configuration files to support the Intel® Server System M20NTP1UR and generic (non-Intel) server systems.

When the server board is first integrated into a server chassis, the system integrator must configure the BMC with a specific chassis identifier for it to load the appropriate embedded system configuration and sensor data record (SDR) files. See [Appendix C](#).

These files are used by the BMC to enable the appropriate platform management support. The SDRs will include pre-determined operational limits data for each sensor type. For thermal management, this data is used to determine fan speed control and other system actions when operational and critical limits are exceeded.

If the BMC is not configured with a specific chassis identifier, then by default, generic chassis configuration files and SDRs are loaded (see [Table 3](#)). In this operating mode, platform management has no support for fan speed control and all installed system fans will operate at 100% Pulse Width Modulation (PWM) all the time.

For Intel server systems, the BMC supports fan speed control that uses a fan speed stepping schema to raise and lower fan speeds as internal temperatures fluctuate. As temperatures within the system rise, so too will the speed of one or more system fans, up to 100% of their design limit.

By default, when the normal operational thermal limits for processors and/or memory are exceeded, the system will initiate power throttling to these devices. Throttling can also be programmed to occur if other thermal sensors exceed their normal operating thermal limits. Power throttling reduces the heat generated by these devices by capping their power usage.

System performance will be degraded when processor and/or memory throttling is initiated. Throttling will continue until the temperature of the monitored thermal sensors fall back to within normal operational limits. Should processor temperatures continue to rise beyond critical limits, the processor will initiate a system shutdown to prevent component damage.

### 3.6.1 Platform Management Support Using Non-Intel Chassis

When the Intel server board is integrated into a non-Intel chassis, support for available sensors types (see [Table 3](#)) and fan speed control can be enabled by creating a custom .INI configuration file and embedding it within the BMC firmware.

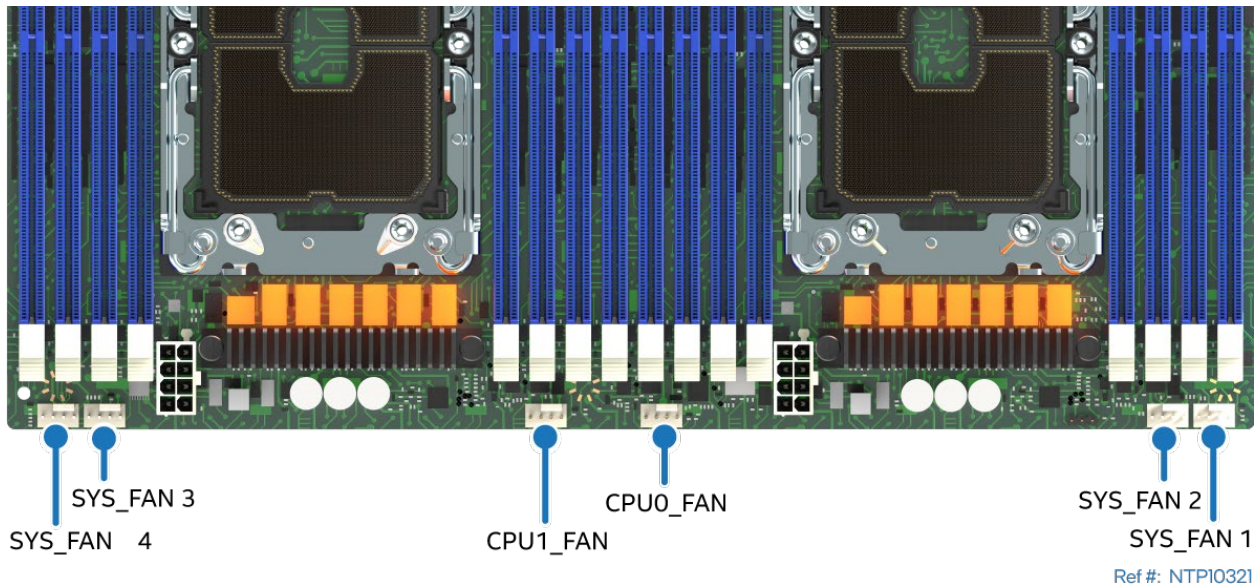
---

**Note:** Contact your local Intel representative to request support.

---

### 3.6.2 System Fan Connectors

The server board includes six (6) 4-pin fan connectors. Each fan connector supports a single system fan with a maximum current draw of 3 Amps.



**Figure 22. System Fan Connectors**

The following figure provides the pinout definition for each system fan connector.

▼ = Pin 1

Pin	4	3	2	1
Signal	FAN_PWM	FAN_TACH	P12V	GND

**Figure 23. 4-Pin System Fan Connector Pinout**

The BMC monitors the FAN\_TACH signal to determine the speed of the given system fan.



## 4. System Software and Utilities

The server board includes a system software stack that consists of the following components:

- System BIOS
- BMC firmware
- Intel® ME firmware

Together, the software components configure and manage features and functions of the server system. A factory installed software stack is pre-programmed on the server board during the board assembly process, making the server board functional at first power on.

However, to ensure the most reliable system operation, Intel highly recommends checking <http://downloadcenter.intel.com> for the latest available system updates and applying them before production deployment.

Several POST accessible hot keys and embedded and stand-alone software utilities are available to configure, customize, support, and update the Intel® Server Board M20NTP2SB. These utilities include:

- BIOS setup utility
- AMI\* BIOS Configuration Program (AMIBCP)
- AMI ChangeLogo\* utility
- Intel® System Configuration Utility (*syscfg*)
- System Update Package (*sup*)
- Intel® Server Firmware Update Utility (*sysfwupdt*)
- Intel® Server Information Retrieval Utility (*sysinfo*)
- Intel SDP Tool

The following sections provide a brief description of each.

### 4.1 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.

The following table provides a list of available POST hot keys along with a description for each.

**Table 4. 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)

### 4.1.1 POST Logo / Diagnostic Screen

If Quiet Boot is enabled in the BIOS setup utility, a splash screen is displayed. The screen contains 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 action is due to the limitations of console redirection that transfers data in a mode that is not graphics compatible.

### 4.1.2 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 the system to boot in the order previously defined by the administrator.

## 4.2 <F2> BIOS Setup Utility

The BIOS setup utility is an embedded text-based utility used to:

- View and configure system settings that determine how the system operates
- Set security features
- Set remote server management access parameters
- Set boot management options
- Access the error management display screen

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

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

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

When the BIOS setup utility is first entered, the utility's Main Menu page is displayed, providing system information and access to various sub-menus. However, should a serious POST error occur, accessing the BIOS setup utility will automatically redirect the initial display to the Error Manager screen within the BIOS setup utility, where additional error information can be found.

It is also possible to boot directly to the BIOS setup utility using the IPMI 2.0 command *Get/Set System Boot Options*. For details, see the IPMI 2.0 specification.

Reference the *Intel® Server M20NTP Family BIOS Setup Utility User Guide* for additional information.

### 4.3 AMI\* BIOS Configuration Program (AMIBCP) – Creating a BIOS Image for Customized Settings

The AMI\* BIOS Configuration Program (AMIBCP) is a powerful customization utility that enables OEMs/ODMs to customize the BIOS ROM image without intervening on the source code and rebuilding the BIOS. With AMIBCP, it is possible to obtain multiple ROM image flavors ready for production.

The AMIBCP utility for this system is custom and is only available under NDA and upon request from Intel.

### 4.4 AMI\* ChangeLogo Utility – Customizing the BIOS Splash Screen

The AMI\* ChangeLogo utility allows developers to easily change splash screen logos displayed by BIOS at boot using the GUI or CLI. The full screen “splash” logo and small logos appearing on the main screen during POST can be replaced with custom logos. The ChangeLogo utility for this system is custom and is only available under NDA and upon request from Intel.

### 4.5 Intel Server Configuration Utility (`syscfg`)

The Intel® System Configuration Utility (`syscfg`) is a command-line tool that supports the following features:

- Save selective BIOS and/or firmware settings to a file
- Write BIOS and Firmware settings from a file to a server
- Configure selected firmware settings
- Configure selected BIOS settings
- Configure selected system settings
- Display selected firmware settings
- Display selected BIOS settings

For further information, download the *Intel® Server Configuration Utility User Guide*.

### 4.6 System Update Package (SUP) for Intel® Server System M20NTP2SB

The SUP is a set of UEFI-based utilities and files bundled together and used to update the system BIOS and other embedded system firmware. Included within the compressed file package is a `README` file providing complete system update instructions and a `STARTUP.NSH` script file that automates the entire system update process with little or no user intervention.

### 4.7 Intel Server Firmware Update Utility (`sysfwupd`)

The Intel Server Firmware Update utility provides the ability to update the system BIOS and Firmware while the server is running its host operating system. This utility is a command-line tool and it requires users to have administrator (Windows\*) or root (Linux\*) privileges.

The Intel Server Firmware Update Utility supports the following features.

- BIOS Update – tool transfers the bin file to BMC and the real update will start on next reboot by default.
- BMC Update - Update Server Management (SM) firmware (FW) of the Baseboard Management Controller (BMC), and on next BMC reset the new BMC firmware will be loaded.
- Recovery Update
- Modify specific FRU field
- Display BIOS/Intel ME/BMC/Base Board/System/FRU/SDR/SMBIOS information
- Restore BIOS Default setting

For further information, download the *Intel® Server Firmware Update Utility User Guide*.

## 4.8 Intel Server Information Retrieval Utility (`sysinfo`)

The Intel Server Information Retrieval Utility is a command-line tool that provides the ability to collect system information, as fully described in the IPMI and BMC specifications. Running the utility requires that the user have Windows\* administrator or Linux\* root permissions.

The Intel Server Information Retrieval Utility collects the following system information and writes the data to a log file:

- Platform Firmware Inventory
- Sensors
- Sensor Data Records (SDR)
- Baseboard FRU
- System Boot Order
- BMC User Settings
- BMC LAN Channel Settings
- BMC SOL Channel Settings
- BMC Power Restore Policy Settings
- BMC channel settings
- SMBIOS Type 1, Type 2, Type 3
- Memory
- Processor
- Storage Devices - Hard Disk Drives (HDD) and solid-state drives (SSD)
- Operating System Information
- Device Manager Information (such as drivers)
- List of Software Installed
- Operating System Event Log
- PCI Bus Device Information
- RAID settings and RAID log
- BIOS Settings (per the BIOS setup utility)
- Power Telemetry (if available)

For further information, download the *Intel® Server Information Retrieval Utility User Guide*.

## 4.9 Intel® Server Debug and Provisioning Tool (Intel® SDP Tool)

The Intel Server Debug and Provisioning Tool (Intel SDP Tool) is a single server command line tool that communicates with the BMC out-of-band to perform debug and provisioning tasks. It does not require any agents, operating system or host network on the remote server and can be scripted to run on multiple systems at the same time. The Intel SDP Tool is also used by Intel Data Center Manager and other software plugins to perform provisioning tasks.

Supported features include:

- Update BMC, BIOS, ME, and SDR
- Deploy an EFI based custom payload. Custom payloads can perform firmware updates of other components, configure RAID, or collect logs
- Configure BIOS and BMC settings
- Download/View System Event Log, Sensors and Debug Log
- Mount virtual media images (ISO and USB)
- Check online for latest BIOS and BMC versions for given platform
- View system inventory (CPU, Memory, Storage, Networking)
- View firmware versions
- Perform power actions



## 5. Server Management

---

The Intel® Server Board M20NTP2SB uses the baseboard management controller (BMC) features of an Aspeed AST2500\* Advanced PCIe Graphics and Remote Management Processor.

The BMC is IPMI 2.0 compliant and supports the following:

- Advanced configuration and power interface (ACPI), system reset control, system initialization, front panel control, and system event log.
- Monitors various board and system sensors and regulates platform thermals and performance to maintain (when possible) server functionality in the event of component failure and/or environmentally stressed conditions.
- Monitor and report system health.
- In-Circuit BMC firmware update
- Chassis intrusion detection
- FRU information
- Error logging and reporting
- Remote control
- Image redirection
- Power control
- Chassis identify
- Front panel control
- Configuration backup
- External user services
- Platform event filtering
- SMTP messaging
- Video recording
- User management
- Embedded firewall

The server board supports the following:

- One (1) Dedicated 1Gb/s RJ45 Management Port – (External Rear I/O Panel)
- Standard management features (Included)
- Advanced management features (\$\$ Optional)
- Intel® Data Center Manager (Intel® DCM) support (\$\$ Optional)

The following subsections provide a brief description of each.

## 5.1 Remote Management Port

The server board includes a dedicated 1 Gb/s RJ45 management port used to access embedded system management features remotely.

---

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

---



Figure 24. Remote Management Port

To access the server remotely using the management port requires network parameters to be configured using the <F2> BIOS setup utility.

### 5.1.1 Configuring System Management Port Using <F2> BIOS Setup

1. During the system power-on POST process, press <F2> when prompted to go to the BIOS setup utility main menu page.
2. Navigate to the **Server Management** tab and select **BMC Network Configuration** to enter the BMC LAN Configuration screen (Figure 25).

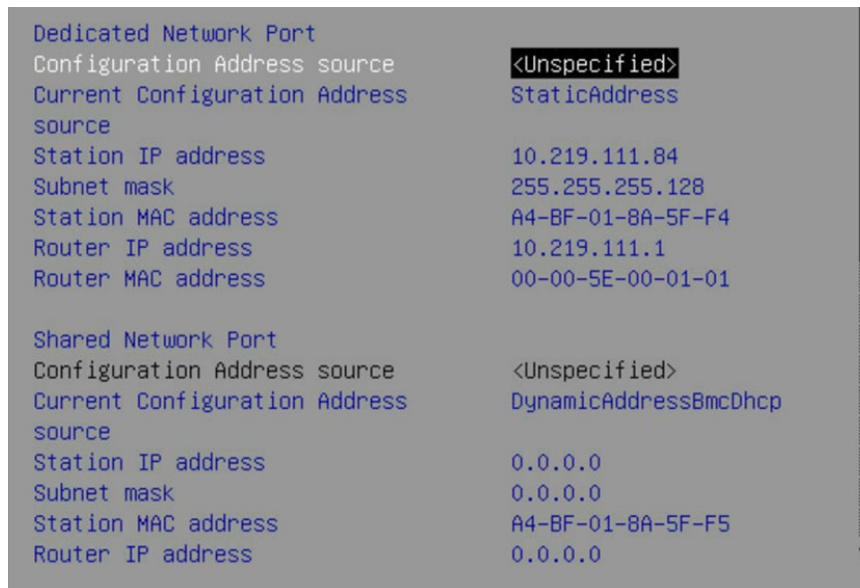
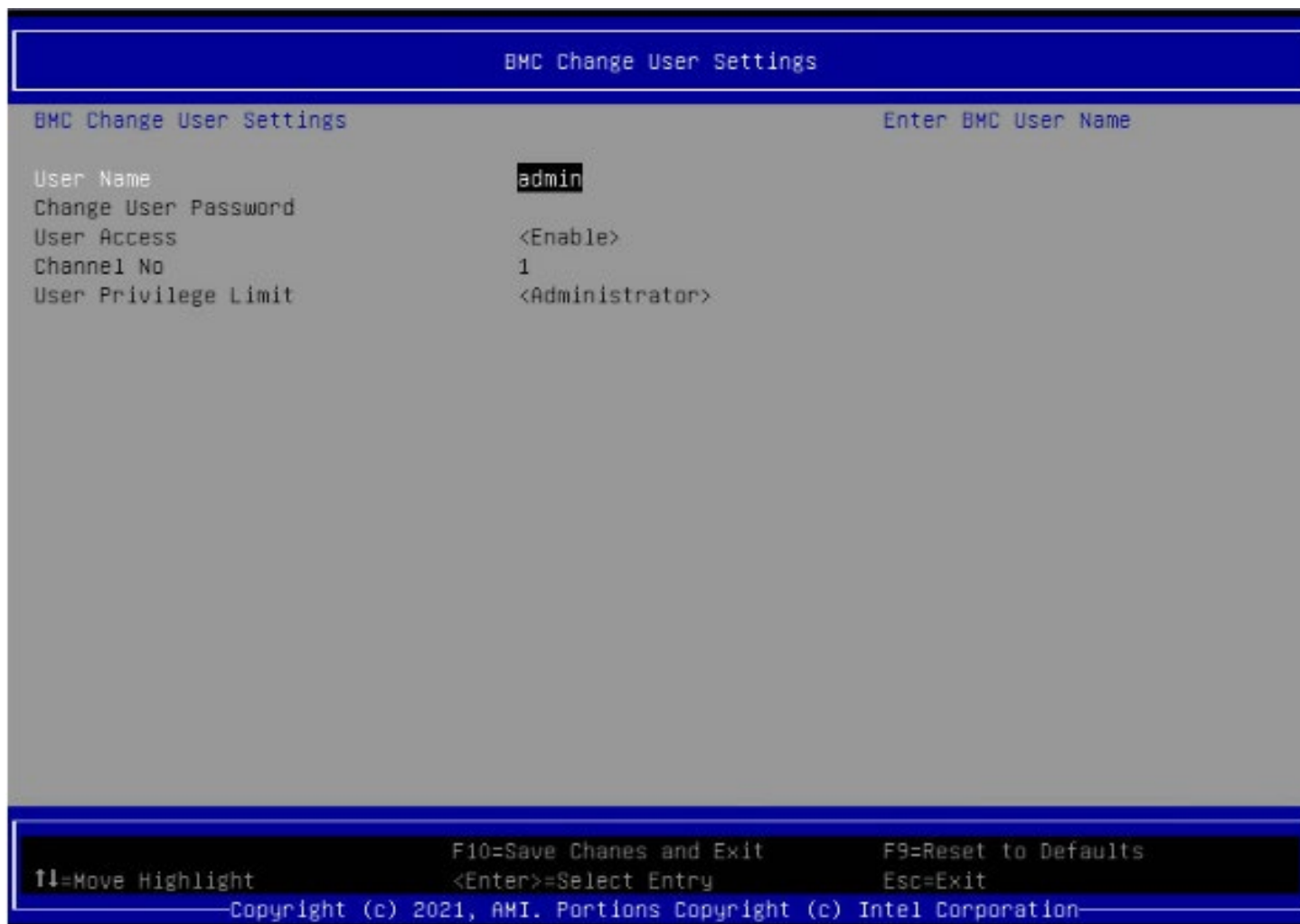


Figure 25. BIOS Setup Utility's BMC LAN Configuration Screen

3. For an IPv4 network:
  - If configuring the server management BMC LAN, scroll to > **Current Configuration Address Source** and then select either **Static** or **Dynamic**. If **Static** is selected, configure the **IP address**, **Subnet mask**, and **Gateway IP** as needed.
4. For an IPv6 network:
  - If configuring the server management BMC LAN, scroll to **Baseboard LAN IPv6 configuration > IP source** 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. The default **User Name** and **Password** is **admin/admin**.
6. If there is a need to change the User and Password, select **BMC User Settings** to enter the User Configuration screen (see [Figure 26](#)).
7. Under **Add User**, set the following settings as desired:
  - **User Name** – Enter the desired name.  
**Note:** The anonymous user cannot be changed.
  - **User password** – Enter the desired password twice.
  - **Channel No** – Select the Channel 1.
  - **Privilege** – Select the privilege to be used. (Administrator privilege is required to use KVM or media redirection)
8. Press <F10> to save the configured settings and exit BIOS setup utility. The server reboots with the new LAN settings.



**Figure 26. BIOS Setup Utility's User Configuration Screen**

### 5.1.1.1 IPMI Command Execution Required to Enable the Integrated BMC Web Console

To enable the Integrated BMC Web Console once the management port is configured, the following procedure should be followed to execute the required IPMI command.

1. In the BIOS setup utility, locate the BMC **Station IP address** (the following figure shows an example).

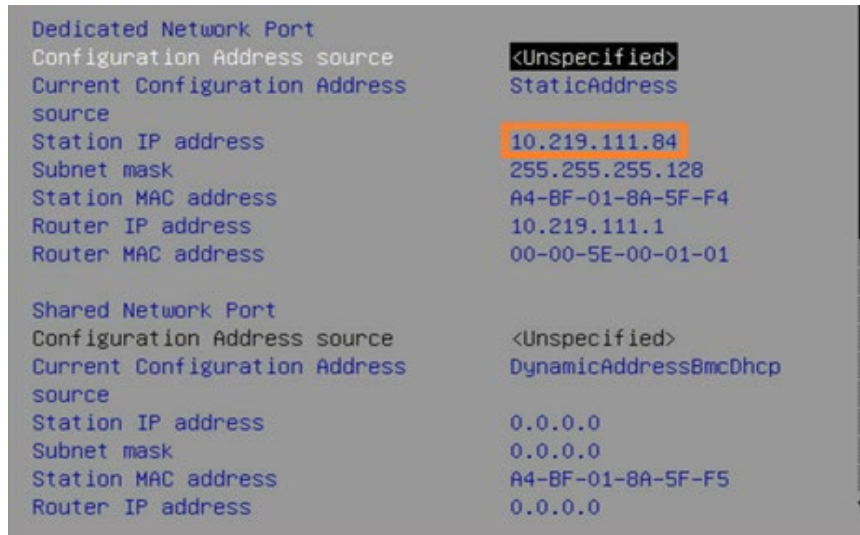


Figure 27. Example of BMC Station IP Address in the BIOS Setup Utility

2. Install the IPMI tool onto the system.
3. Go back to the host and execute the following command using the BMC user and password created within the BIOS setup utility.
 

Note: The following commands can be executed via Linux\*, Windows\* or EFI shell

  - o `ipmitool -I lanplus -H<IP Address> -U<user name> -P<password> raw 6 0x40 1 0x42 4` – If the command execution is successful, no error message is displayed.
  - o Then, run: `ipmitool -I lanplus -H<IP Address> -U<user name> -P<password> raw 0x32 0x6a 0x01 0x00 0x00 0x00 0x01 0x62 0x6f 0x74 0x68 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0xff 0xff 0xff 0xff 0xbb 1 0 0 8 7 0 0 0 0` – If the command execution is successful, no error message is displayed.
4. Open a **web browser** and enter the **Station IP address** to access the Integrated BMC Web Console.
5. Enter the BMC user and password in the corresponding fields of the login screen (see Figure 28). After signing in, the Integrated BMC Web Console is enabled and ready to use.

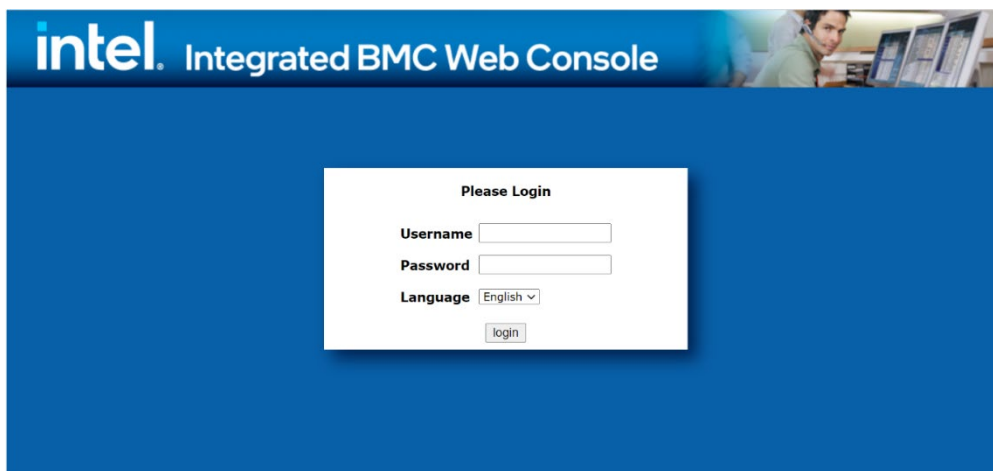


Figure 28. Integrated BMC Web Console – Login Screen

## 5.2 Standard System Management Features

The following system management features are supported on the Intel® Server Board M20NTP2SB.

- Virtual KVM over HTML5
- Integrated BMC Web Console
- Redfish
- IPMI 2.0
  - 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.

### 5.2.1 Virtual KVM over HTML5

The BMC firmware supports keyboard, video, and mouse redirection (KVM) over LAN. This feature is available remotely from the Integrated BMC Web Console as an HTML5 application. USB1.1 or USB 2.0 based mouse and keyboard redirection are supported. The KVM-redirection (KVM-r) session can be used concurrently with media-redirection (media-r). This feature allows a user to interactively use the keyboard, video, and mouse (KVM) functions of the remote server as if the user were physically at the managed server.

KVM redirection consoles support the following keyboard layouts: English, Chinese (traditional), Japanese, German, French, Spanish, Korean, Italian, and United Kingdom. KVM redirection includes a “soft keyboard” function. The “soft keyboard” is used to simulate an entire keyboard that is connected to the remote system. The “soft keyboard” functionality supports the following layouts: English, Dutch, French, German, Italian, Russian, and Spanish.

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

### 5.2.2 Integrated Baseboard Management Controller Web Console (Integrated BMC Web Console)

The BMC firmware has an embedded web server that can remotely serve web pages to any supported browser. This web console allows the administrator to view system information including firmware versions, server health, diagnostic information, power statistics.

The web console enables configuration of the BMC and BIOS. It provides the ability for users to perform power actions, launch KVM, and set up virtual media redirection.

Enter the configured IP address of the BMC management port into the web browser to open the Integrated BMC Web Console module login page (see [Figure 29](#)). To use a secure connection, type:

```
https://<IPaddress_or_Hostname>/
```

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

- Username: `root`
- Password: `superuser`
- Language: **English**

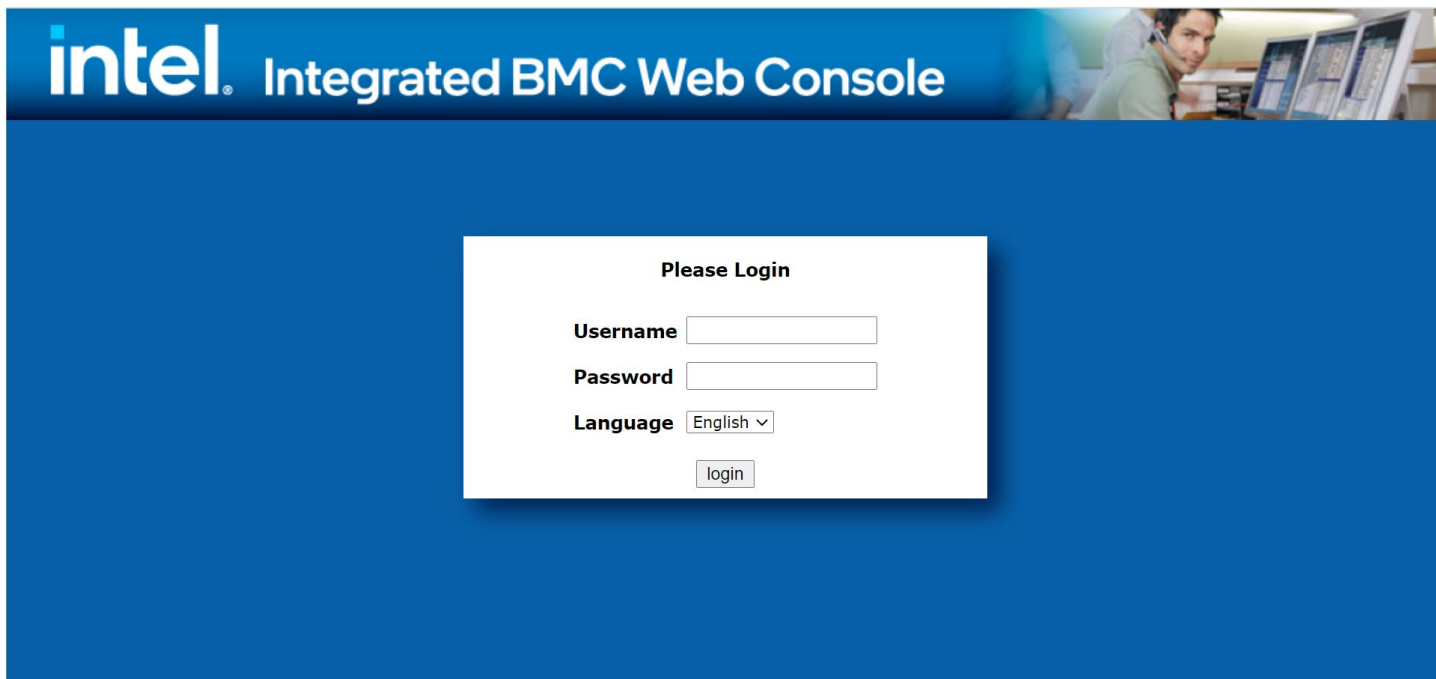


Figure 29. Integrated BMC Web Console Login Page

Click the **Login** button to view the homepage.

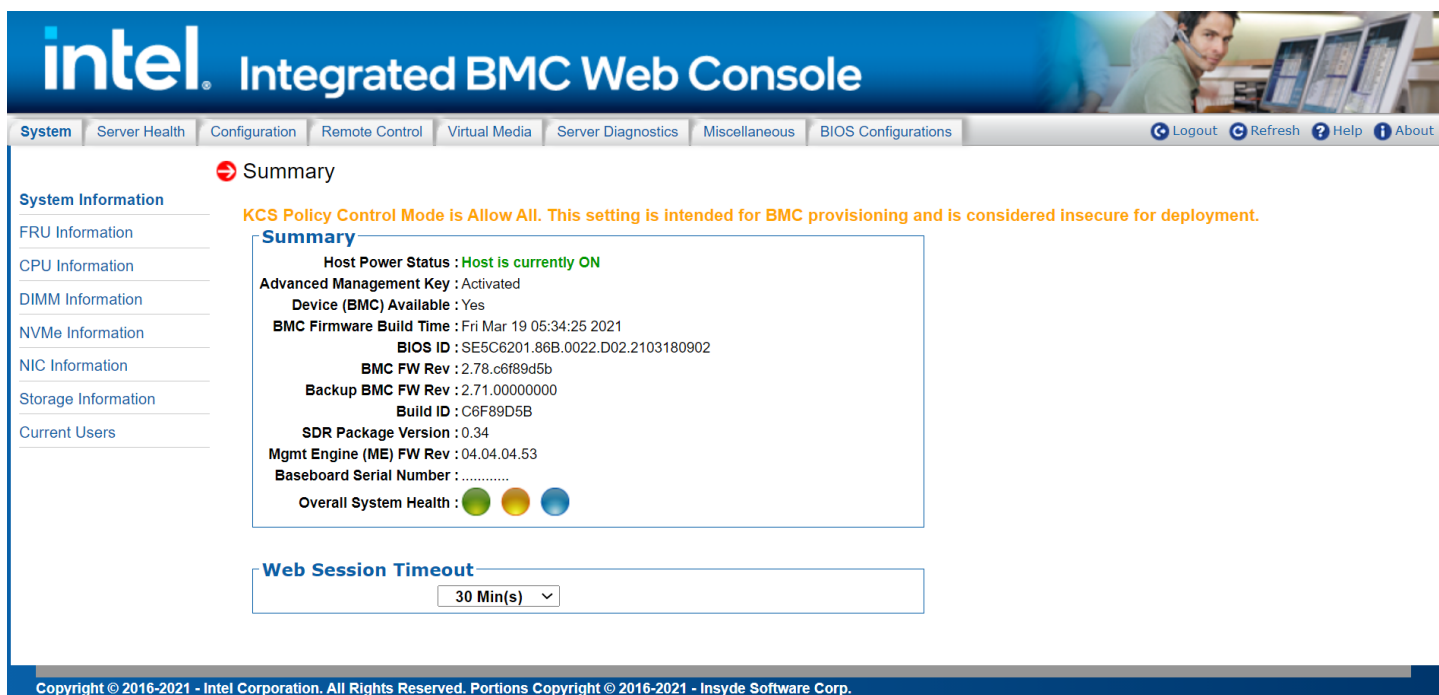


Figure 30. Integrated BMC Web Console – Main Console View

For setup and additional information about this utility, download the *Integrated Baseboard Management Controller Web Console (Integrated BMC Web Console) User Guide*.

### 5.2.3 Redfish\* Support

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



### 5.2.4 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.

### 5.2.5 Out-of-Band BIOS / BMC Update and Configuration

The BMC supports Redfish schemas and Integrated BMC Web Console features that allow administrators to update the BMC, BIOS, Intel ME, and SDR firmware. The BMC firmware also includes Power Supply and Back plan 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 supports Redfish and Integrated BMC Web Console feature to view and modify BIOS settings. 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.

### 5.2.6 System Inventory

The BMC supports Redfish schemas and Integrated BMC Web Console pages to display system inventory. This inventory includes FRU information, Processor, Memory, NVMe, networking, and storage. When applicable, the firmware version will also be provided.

### 5.2.7 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 Integrated BMC Web Console or using Intel Server Configuration Utility and Intel SDP Tool 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 processor in reset long enough to collect processor machine check registers, memory controller machine check registers, I/O global error registers, and other processor state information.

### 5.2.8 Security Features

The BMC contains several security features including: OpenLDAP\* and Active Directory\*, security logs, ability to turn off any remote port, SSL certificate upload, VLAN support, and KCS control. The BMC also supports full user management with the ability to define password complexity rules.

Each BMC release is given a security version number to prevent firmware downgrades from going 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>

## 5.3 Advanced System Management Features

Purchasing an optional Advanced System Management product key (iPC **ADVSYSTEMGMTKEY**) 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 to improve the efficiency and uptime. For more information, go to <https://www.intel.com/content/www/us/en/software/intel-dcm-product-detail.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 Intel Server Configuration Utility are used to upload the key to the BMC firmware to unlock the advanced features.

### 5.3.1 Virtual Media Image Redirection (HTML5 and Java)

The BMC supports media redirection of local folders and .IMG and .ISO image files. This redirection is supported in both HTML5 and Java remote 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. The web page then allows the user to select 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 may be interacted within the normal fashion, based on the operating system running on the server system. The feature allows 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 file folder share is presented to the server system as a UDF file system. The server system operating system must be able to interact with UDF file systems for this feature to be used with the operating system.

---

### 5.3.2 Virtual Media over Network Share and Local Folder

In addition to supporting virtual media redirection from the remote workstation (see [Section 5.3.1](#)), the BMC also supports media redirection of file folders and .IMG and .ISO files hosted on a network file server accessible to the BMC 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.

### 5.3.3 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 log in to the web console or Redfish\* using an Active Directory username instead of local authentication. The feature allows administrators to change only passwords on this single domain account instead of on every remote system.

## 5.4 Intel® Data Center Manager (Intel® 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://www.intel.com/content/www/us/en/software/intel-dcm-product-detail.html>

## 6. Processor Support

The server board includes two Socket-P4 LGA4189 processor sockets compatible with the 3<sup>rd</sup> Gen Intel® Xeon® Scalable processor family.

**Note:** Previous generations Intel® Xeon® processor and Intel® Xeon® Scalable processor families and their supported processor heat sinks are not compatible on the server board described in this document.

### 6.1 Processor Cooling Overview

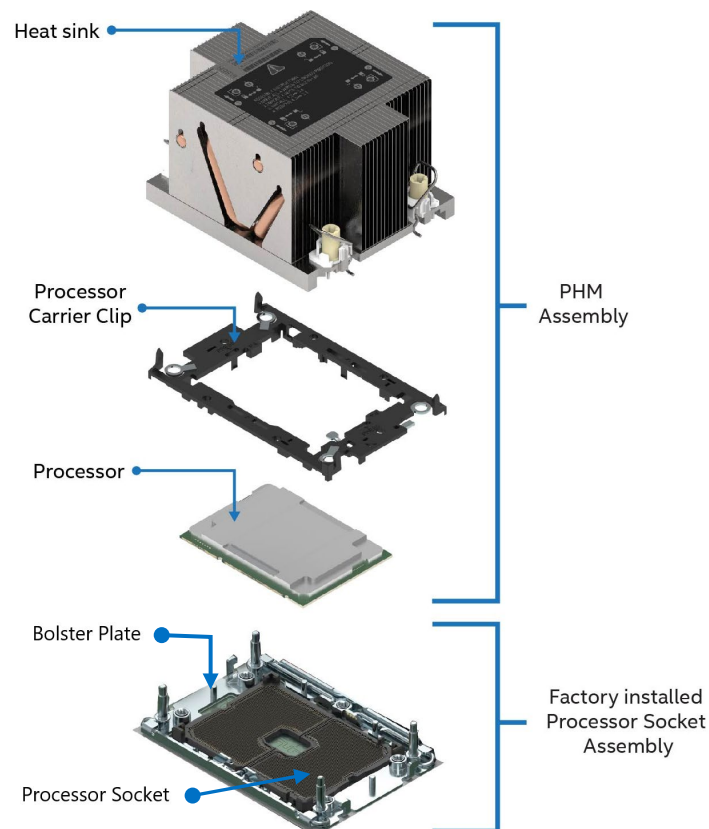
The server board includes two processor socket assemblies, each consisting of a processor socket and bolster plate. The factory installed bolster plate is secured to the server board. It is generally used to align the processor cooling hardware over the processor socket and secure it to the server board.

Processor cooling options in a server system may use a passive or active heat sink that use airflow to dissipate heat generated by the processors. Other processor cooling options may use liquid cooling plates, where cool liquid is pumped through the cooling plates to dissipate the heat from the processor.

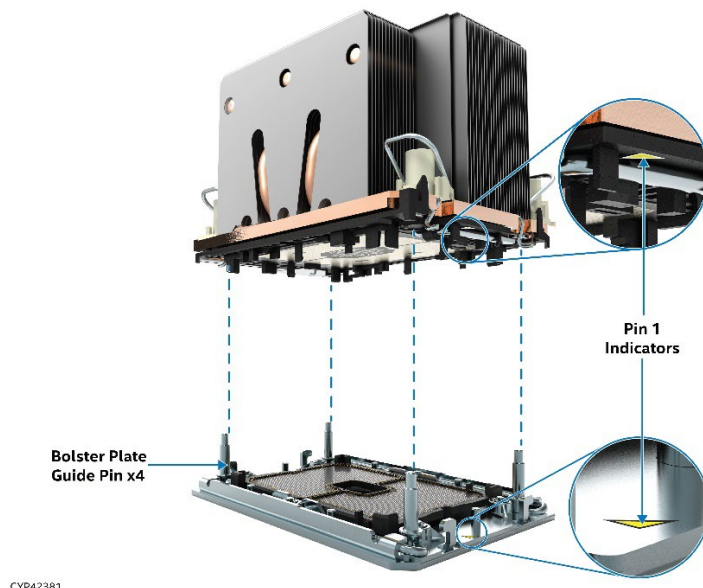
For air cooled systems, the processor and heat sink are generally pre-assembled into a single Processor Heat-sink Module (PHM) before being installed onto the processor socket assembly. The PHM concept reduces the risk of damaging pins within the processor socket during the processor installation process.

A PHM assembly consists of a processor, a processor carrier clip, and the processor heat sink.

The following figure identifies each component associated with the PHM and processor socket assembly.



**Figure 31. Component Reference Diagram for PHM and Processor Socket Assemblies**



**Figure 32. PHM Placement onto Processor Socket**

---

**Note:** Figure 31 and Figure 32 are intended as a general reference to components that make up the PHM and processor socket assemblies. The components shown may or may not match exactly what may be used. The diagrams do NOT define the process necessary to assemble the PHM or install it onto the processor socket. See Section 15.2.3 for recommended PHM assembly and installation instructions.

---

For details supporting liquid cooling solutions, refer to the documentation supplied with the chosen liquid cooling solution or system.

### 6.1.1 Processor Cooling Requirements

For the server system to support optimal operation, performance, and long-term reliability, the chosen thermal management solution must expel enough heat generated from within the chassis to keep the processors and other system components within their specified thermal operating limits.

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

---

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

---

## 6.2 Supported Processor Overview

The Intel® Server Board M20NTP2SB supports processors within the 3<sup>rd</sup> Gen Intel® Xeon® Scalable processor family.

---

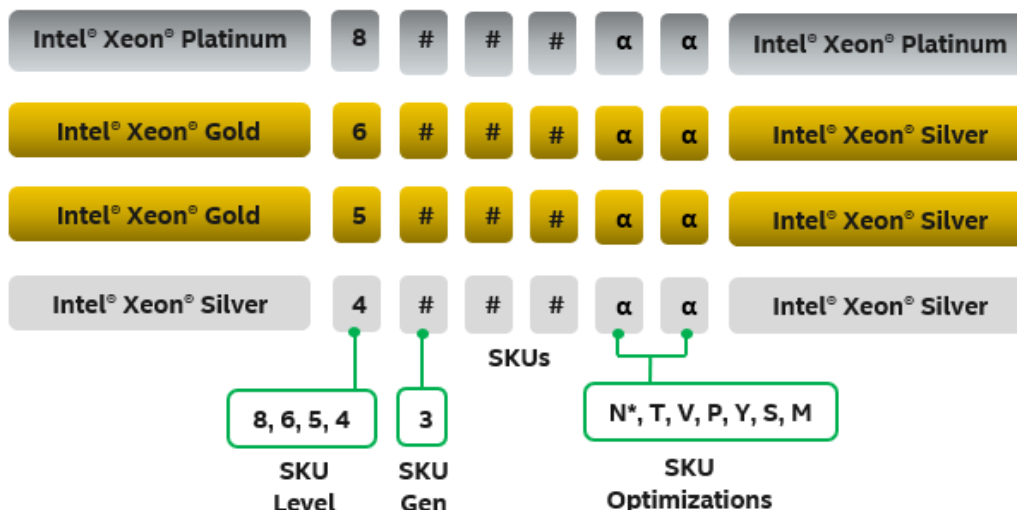
**Note:** Previous generations Intel® Xeon® processor and Intel® Xeon® Scalable processor families and their supported processor heat sinks are not compatible on the server board described in this document.

---

The 3<sup>rd</sup> Gen Intel® Xeon® Scalable processor family includes many different processor SKUs. However, some are not compatible for use on the Intel® Server Board M20NTP2SB. The following figure provides guidance to determine which processor SKUs are supported and which are not.



### Supported Processor SKUs



### Processor SKUs Not Supported

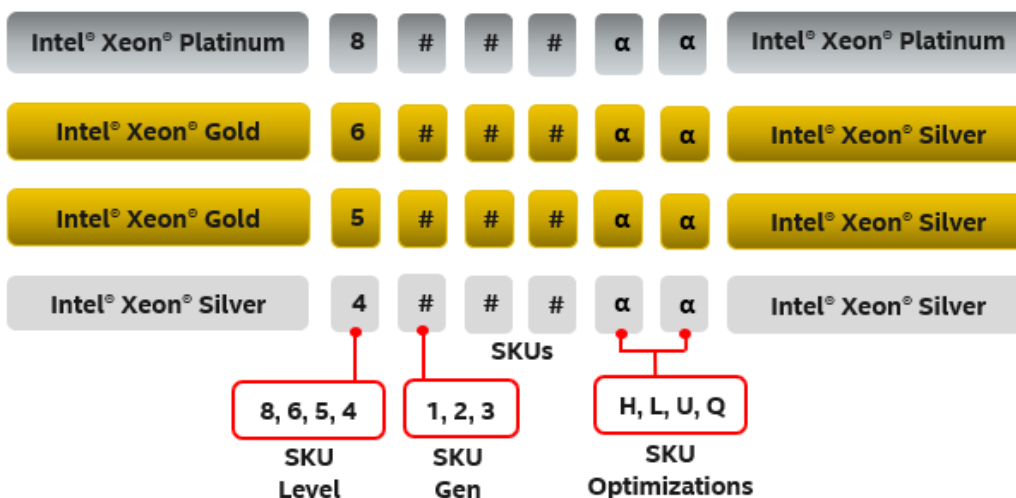


Figure 33. 3<sup>rd</sup> Gen Intel® Xeon® Scalable Processor Identification

#### Notes:

- Supported 3<sup>rd</sup> Gen Intel® Xeon® Scalable processor SKUs cannot end in (H), (L), (U), or (Q). All other processor SKUs are supported.
- The 8351N SKU is a single-socket optimized SKU and is not supported on the Intel® Server Board M20NTP2SB.

#### 6.2.1 Processor Thermal Design Power (TDP)

Voltage regulators on the Intel® Server Board M20NTP2SB support processors that have a thermal design power (TDP) of 250W or less. Processors with a TDP greater than 250W cannot be supported.

**Note:** The maximum supported processor TDP at the system level may be lower than what the server board can support. Design limits of the chosen server chassis / system will determine the maximum processor TDP that can be supported up to the 250W processor TDP limit of the server board. Reference the chosen server chassis/system documentation for specific processor support information.

**Table 5. 3<sup>rd</sup> Gen Intel® Xeon® Scalable Processor Family Feature Comparison**

Feature	Platinum 8300 series Processors	Gold 6300 series Processors	Gold 5300 series Processors	Silver 4300 series Processors
# 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
RAS Capability	Advanced	Advanced	Advanced	Standard
Intel® Turbo Boost Technology	Yes	Yes	Yes	Yes
Intel® HT Technology	Yes	Yes	Yes	Yes
Intel® AVX-512 ISA Support	Yes	Yes	Yes	Yes
Intel® AVX-512 - # of 512b FMA Units	2	2	2	2
# of PCIe* Lanes	64	64	64	64
Intel® VMD	Yes	Yes	Yes	Yes

**Note:** Features may vary between processor SKUs.

See 3<sup>rd</sup> Gen Intel® Xeon® Scalable processor specifications and product briefs for additional information.

## 6.2.2 Supported Technologies

The 3<sup>rd</sup> Gen Intel® Xeon® Scalable processors combine several key system components into a single processor package including the processor cores, Integrated Memory Controller (IMC), and Integrated IO Module.

The core features and technologies for the processor family include:

- Intel® Ultra Path Interconnect (Intel® UPI) – supports up to 11.2 GT/s
- Intel® Speed Shift Technology
- Intel® 64 Architecture
- Enhanced Intel® SpeedStep® Technology
- Intel® Turbo Boost Technology 2.0
- Intel® Hyper-Threading Technology (Intel® HT Technology)
- Intel® Virtualization Technology (Intel® VT-x)
- Intel® Virtualization Technology for Directed I/O (Intel® VT-d)
- Execute Disable Bit
- Intel® Trusted Execution Technology (Intel® TXT)
- Intel® Advanced Vector Extensions (Intel® AVX-512)
- Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI)
- Intel® Deep Learning through VNNI
- Intel® Speed Select Technology on select processor SKUs
- Intel® Resource Director Technology

## 6.3 Processor Population Rules

---

**Note:** The server board may support dual-processor configurations consisting of different processors that meet the following defined criteria. However, Intel does not perform validation testing of this configuration. 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.

---

For single processor configurations, the processor must be installed into the processor socket labeled “CPU\_0”.

---

**Note:** Some server board features may not be functional unless two processors are installed. For an architectural block diagram of the Intel® Server Board M20NTP2SB, see [Figure 7](#).

---

When two processors are installed, the following population rules apply:

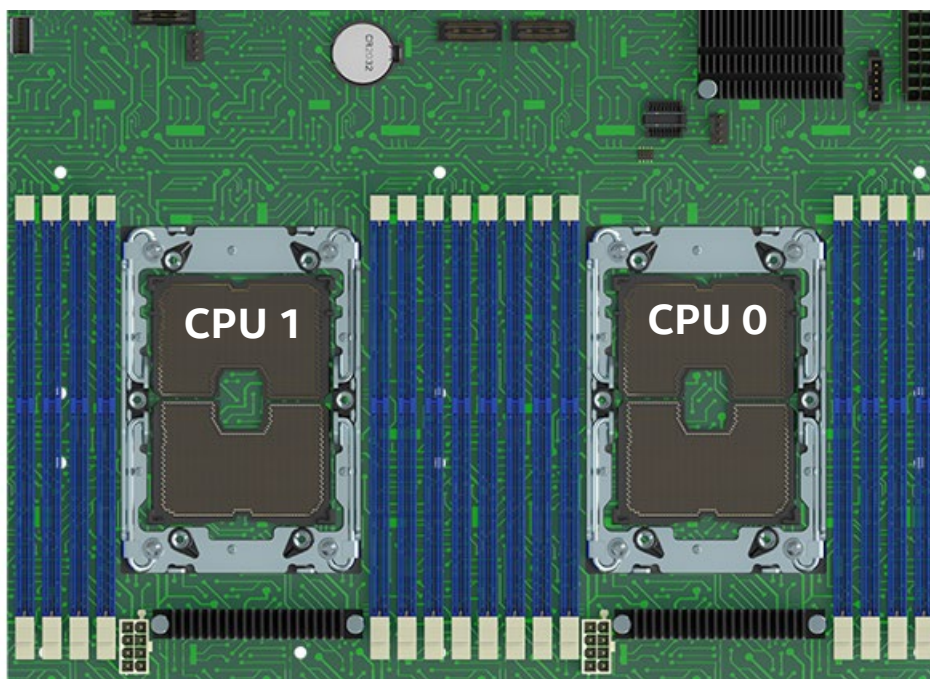
- Both processors must have identical extended family, extended model number and processor type
- Both processors must have the same number of cores
- Both processors must have the same cache sizes for all levels of processor cache memory
- Both processors must support identical DDR4 memory frequencies

---

**Note:** Processors with different steppings can be mixed in a system if the previously mentioned rules are met.

---

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



**Figure 34. Processor Socket Identification**

## 7. Memory Support

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

### 7.1 Supported Memory

The Intel® Server Board M20NTP2SB supports standard DDR4 RDIMMs and LDRIMMs.

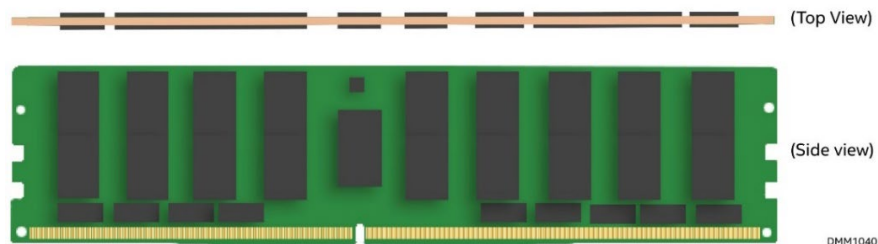


Figure 35. Standard SDRAM DDR4 DIMM

Supported DDR4 DIMMs must have the following attributes:

- 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 speeds of up to 3200 MT/s
- DIMM capacities of 8 GB, 16 GB, 32 GB, 64 GB, 128 GB, and 256 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 supported DDR4 DIMM types.

Table 6. 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) 256 (4H)	3200
LRDIMM	QR x4	64	128	3200
3DS-LRDIMM	QR/OR x4	128 (4H)	128 (2H) 256 (4H)	3200

**Note:** SR = Single Rank, DR = Dual Rank, QR = Quad Rank, OR = Oct Rank.

**Note:** Specification applies only to memory chips mounted by surface mounted technology (SMT) method. Refer to the DIMM datasheets for more information.

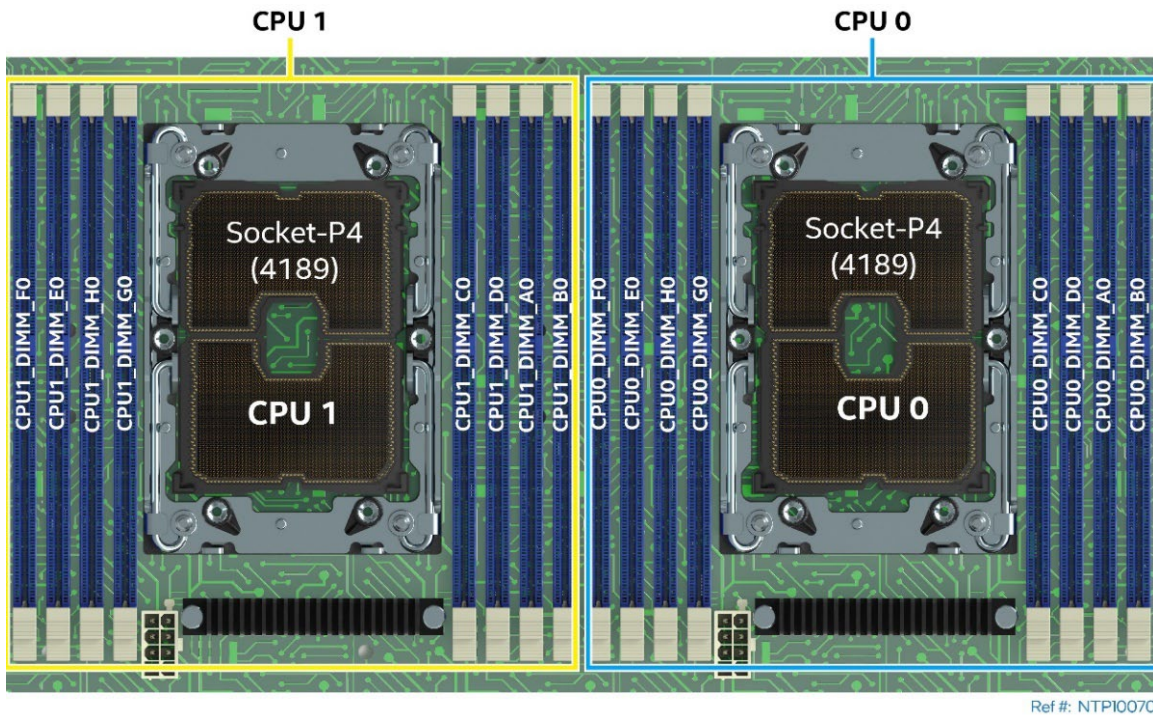


**Table 7. Maximum Supported Standard SDRAM DIMM Speeds by Processor Shelf**

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

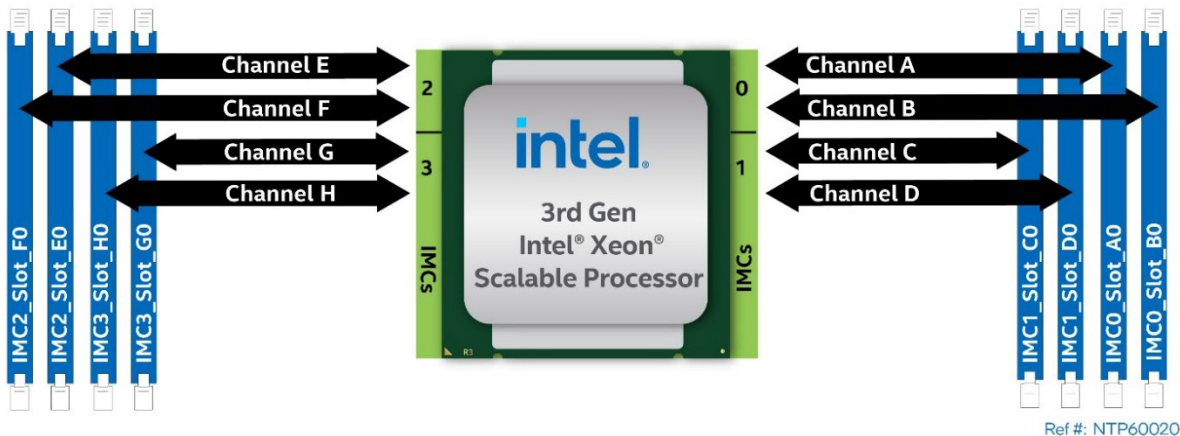
## 7.2 Memory Subsystem Architecture

The Intel® Server Board M20NTP2SB includes a total of 16 memory slots, 8 memory slots supported by each processor.



**Figure 36. Server Board Memory Slot Association by CPU**

Each processor has four integrated memory controllers (IMCs) (see Figure 37), each supporting two memory channels. Memory channels are identified A through H. Each memory channel supports one memory slot.



**Figure 37. Processor Memory Slot Support Overview**



The following applies to the memory architecture of the server board:

- 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 utility are applied commonly for each installed processor.
- For best system performance in dual processor configurations, installed DDR4 DIMM type and population configured to CPU 1 must match DDR4 DIMM type and population configured to CPU 0.
- For best system performance, memory should be installed in all eight channels for each installed processor.
- Mixed DDR4 DIMM population rules:
  - Mixing DDR4 DIMMs of different frequencies and latencies is not supported within or across processors. If a mixed configuration is encountered, the BIOS attempts to operate at the highest common frequency and the lowest latency possible.
  - Mixing of DDR4 DIMM types (RDIMM, LRDIMM, 3DS-RDIMM, 3DS-LRDIMM) within or across processors is not supported. This condition is a Fatal Error Halt in Memory Initialization.

---

**Note:** Intel does not support nor will it provide support for systems populated with “Un-like” (non-matching) DIMMs. However, the system may still operate if all the mixed DDR4 DIMM population rules are followed. Validation and support of these configurations is the sole responsibility of the original system integrator.

For best compatibility and system operation, Intel highly recommends that all installed DIMMs have “identical” or “like” attributes as defined in the following Intel DDR4 support disclaimer.

---

**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 8](#). 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 8](#).

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 8](#).

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 following table. 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.

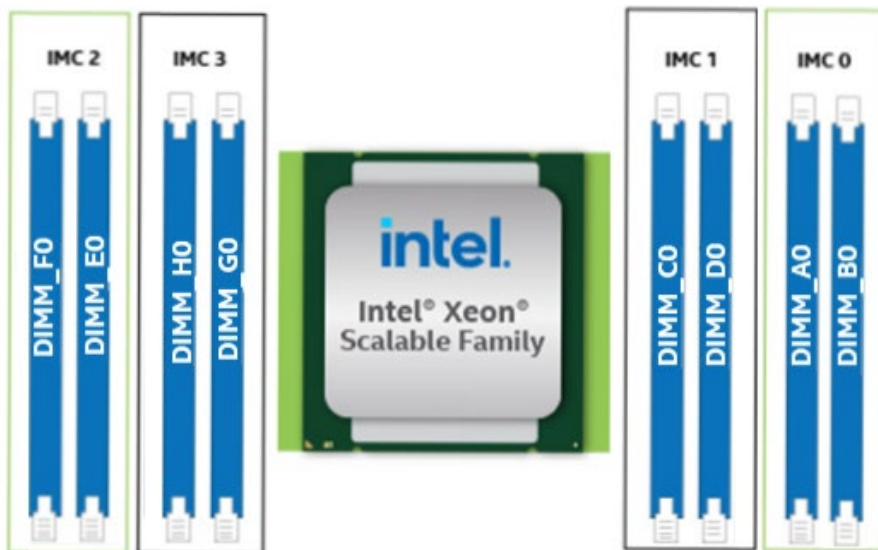
**Table 8. DDR4 DIMM Attributes Table for “Identical” and “Like” DIMMs**

<ul style="list-style-type: none"> <li>• DDR4 DIMMs are considered “Identical” when ALL listed attributes between the DIMMs match.</li> <li>• 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.</li> </ul>			
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 #
SDRAM 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

### 7.2.1 Recommended Memory Configurations

The following table identifies the recommended DIMM population configurations by memory slot based on the desired number of DIMMs to be supported by each installed processor. For best system performance in a dual processor configuration, installed memory type and population configured to CPU 1 must match memory type and population configured to CPU 0.

**Table 9. Recommended DDR4 DIMM 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 0	Slot 0	Slot 0	Slot 0	Slot 0	Slot 0	Slot 0	Slot 0
1	-	-	-	-	-	-	DIMM	-
2	-	DIMM	-	-	-	-	DIMM	-
4	-	DIMM	-	DIMM	DIMM	-	DIMM	-
6	DIMM	DIMM	-	DIMM	DIMM	-	DIMM	DIMM
8	DIMM	DIMM	DIMM	DIMM	DIMM	DIMM	DIMM	DIMM

## 7.3 Memory RAS Support

Processors shelves within the 3<sup>rd</sup> Gen Intel® Xeon® Scalable processor family have support for either the standard or advanced memory RAS features defined in the following table. See [Table 5](#) to determine which Memory RAS tier is supported by each supported processor shelf.

**Table 10. Memory RAS Features**

Memory RAS Feature	Description	Standard	Advanced
<b>Partial Cache-Line Sparing (PCLS)</b>	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.	✓	✓
<b>Device Data Correction</b>	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 DRAM DIMMs). Cannot be enabled with “Memory Multi-Rank Sparing” or “Write Data CRC Check and Retry.”	✓	✓
	Adaptive Double Data Correction – Multiple Region (ADDDC-MR, + 1) Supported with x4 DIMMs only.	–	✓
<b>DDR4 Command/Address (CMD/ADDR) Parity Check and Retry</b>	DDR4 technology based CMD/ADDR parity check and retry with CMD/ADDR parity error “address” logging and CMD/ADDR retry.	✓	✓
<b>DDR4 Write Data CRC Check and Retry</b>	Checks for CRC mismatch and sends a signal back to the processor for retry. Cannot be enabled with “ADC-SR” or “ADDDC-MR, +1.”	✓	✓
<b>Memory Data Scrambling with Command and Address</b>	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.	✓	✓
<b>Memory Demand and Patrol Scrubbing</b>	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.	✓	✓
<b>Memory Mirroring</b>	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 operating system and applications.	✓	✓
	Address range/partial memory mirroring: Provides further intra socket granularity to mirroring of memory. This allows 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.	–	✓
<b>DDR Memory Multi-Rank Memory Sparing</b>	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”.	✓	✓
<b>Memory SMBus* Hang Recovery</b>	Allows system recovery if the SMBus fails to respond during runtime, thus, preventing system crash.	✓	✓
<b>Memory Disable and Map Out for Fault Resilient Boot (FRB)</b>	Allows memory initialization and booting to the operating system even when memory fault occurs.	✓	✓

Memory RAS Feature	Description	Standard	Advanced
<b>Post Package Repair (PPR)</b>	PPR offers additional spare capacity within the DDR4 DRAM that can be used to replace faulty cell areas detected during system boot time.	✓	✓
<b>Memory Thermal Throttling</b>	Management controller monitors the memory DIMM temperature and can temporarily slow down the memory access rates to reduce the DIMM temperature if needed.	✓	✓
<b>MEMHOT Pin Support for Error Reporting</b>	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 utility for Memory RAS
- Memory sparing and memory mirroring options are enabled in BIOS setup utility.
- 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 utility.
- 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® Server Board M20NTP2SB includes support for Intel® Software Guard Extensions (Intel® SGX), Intel® Total Memory Encryption (Intel® TME), and Intel® Total Memory Encryption – Multi-Tenant (Intel® TME-MT). In addition, some of the memory RAS features are disabled as indicated in the following table.

**Table 11. Compatibility of RAS Features Intel® SGX, Intel® TME, and Intel® TME-MT**

Feature/Technology	Intel® SGX	Intel® TME, Intel® TME-MT
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 Southbridge (PCH) Presence for supporting system partitioning	No	Yes



## 8. PCI Express (PCIe®) Subsystem Overview

The 3rd Gen Intel® Xeon® Scalable processors provide up to 48 PCIe 4.0 bus lanes to the host system. PCIe bus lanes from each processor are used to support various system features as shown in the following diagram. The system must be configured with two processors to support all possible PCIe functionality of the server board.

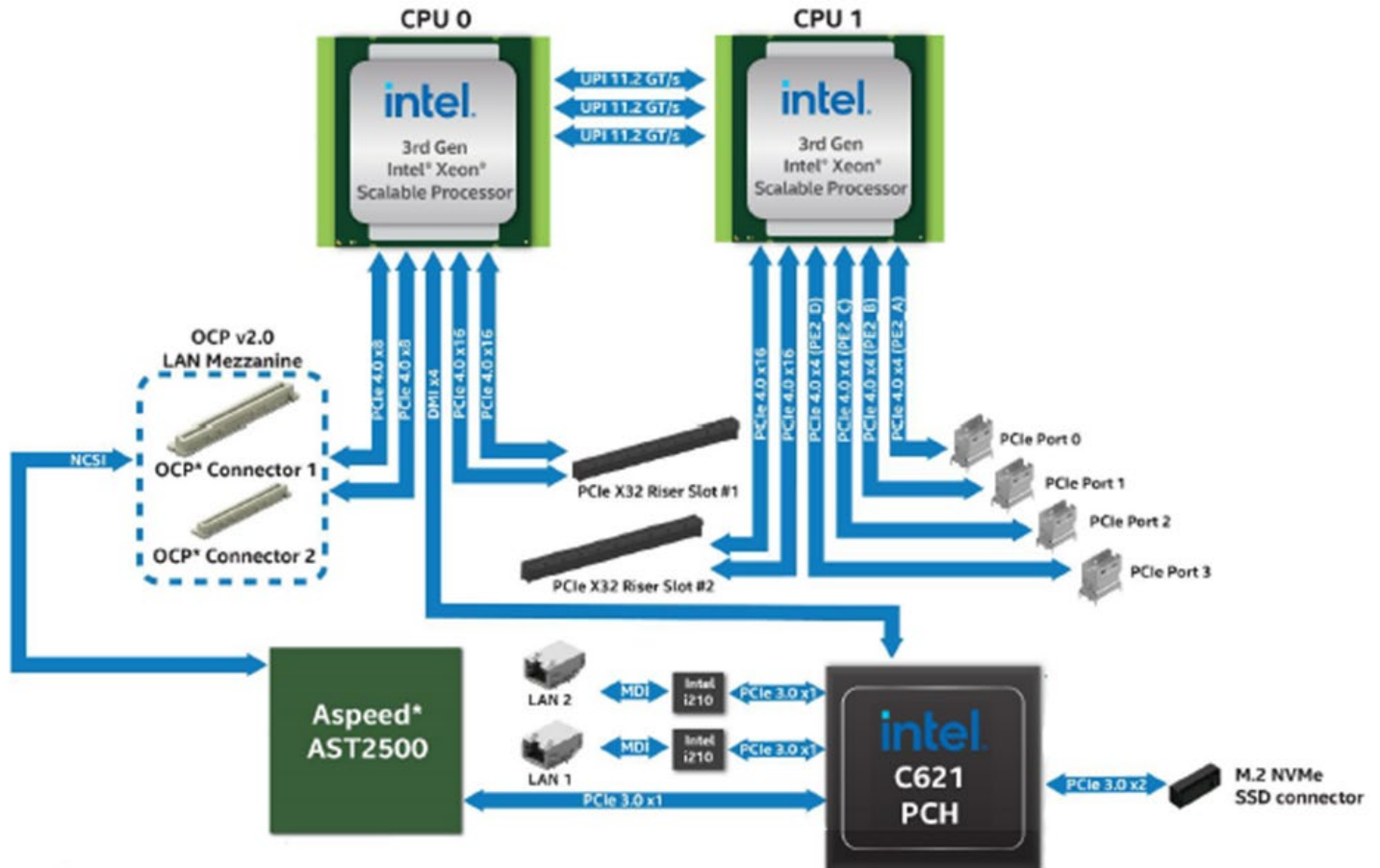


Figure 38. PCIe\* Subsystem Architecture Block Diagram

The PCIe bus lanes from each processor are fully compliant with the *PCIe 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 PCIe bus lanes routed from the PCH are fully compliant with the *PCIe 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).

The following table provides the PCIe port routing from each processor and the PCH.

**Table 12. Processor / PCH PCIe\* Port Routing**

CPU #	Port #	Port Range	# Bus lanes	Onboard PCIe* Connector
CPU 0	Port 0	CPU 0 PE0 <15:0>	PCIe 4.0 X16	OCP Connector
	Port 1	CPU 0 PE1 <15:0>	PCIe 4.0 X16	Riser Slot 1
	Port 2	CPU 0 PE2 <15:0>	PCIe 4.0 X16	Riser Slot 1
CPU 1	Port 0	CPU 1 PE0 <15:0>	PCIe 4.0 X16	Riser Slot 2
	Port 1	CPU 1 PE1 <15:0>	PCIe 4.0 X16	Riser Slot 2
	Port 2	CPU 1 PE2 <15:0>	PCIe 4.0 X16	4 x PCIe SlimSAS* Connectors X4 PCIe Ports 1–4
PCH			PCIe 3.0 X1	Intel® I210
			PCIe 3.0 X1	Intel® I210
			PCIe 3.0 X1	Aspeed AST2500* - BMC
			PCIe 3.0 X2	PCIe M.2 SSD Connector

## 8.1 PCIe\* Enumeration and Allocation

The BIOS assigns PCIe bus numbers in a depth-first hierarchy, in accordance with the *PCIe Local Specification, Revision 4.0*. The bus number is incremented when the BIOS encounters a PCI-PCI bridge device. Scanning continues onto the secondary side of the bridge until all subordinate buses are assigned numbers. PCI bus number assignments may change if the PCI-PCI bridge configuration is changed between boot cycles.

If a bridge device with a single bus behind it is inserted into a PCIe bus, all subsequent PCIe bus numbers below the current bus are increased by one. The bus assignments occur once, early in the BIOS boot process, and will not change during the pre-boot phase.

## 8.2 PCIe\* Riser Card Support

The server board provides two PCIe X32 riser card slots identified as: Riser Slot #1 and Riser Slot #2. The PCIe bus lanes for Riser Slot #1 are supported by CPU 0. The PCIe bus lanes for Riser Slot #2 are supported by CPU 1. A dual processor configuration is required to enable support for Riser Slot #2.

The riser card slots are specifically designed to support riser cards only. Attempting to install a PCIe add-in card directly into a riser card slot on the server board may damage the server board, the add-in card, or both.

Riser cards developed for this server board are not interchangeable between the two riser card slots. Riser cards are specifically designed to be supported by Riser Slot 1 or Riser Slot 2.

See [Section 3.4](#) for available Intel Riser Card accessory kits.

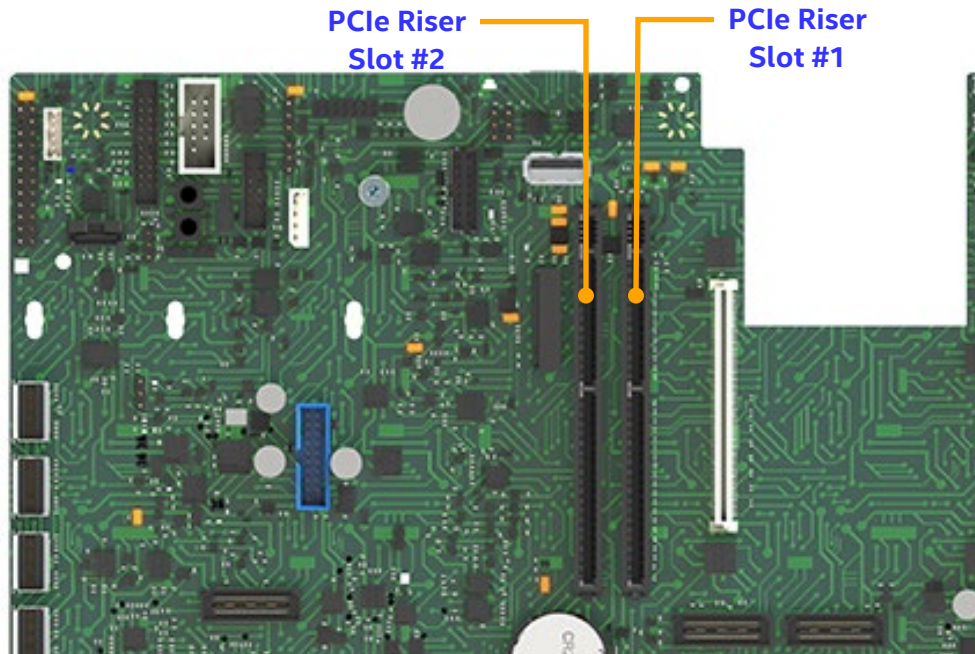
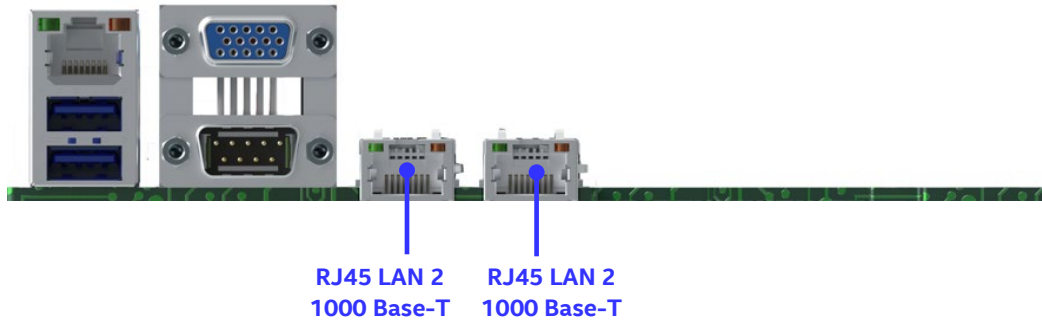


Figure 39. Riser Card Slots

### 8.3 Network Connectivity

The server board includes two Intel® I210-AT Ethernet Controllers. The I210 supports advanced features such as Audio-Video Bridging (AVB), IEEE 802.1AS precision timestamping, Error Correcting Code (ECC) Packet Buffers, and Enhanced Management Interface options.

Each Ethernet controller is supported by one external RJ45 1000Base-T Ethernet connector.



**Figure 40. Back Panel Network Connectivity**

Each RJ45 LAN connector includes two Link/Activity LEDs that function as defined in the following table.

**Table 13. RJ45 LAN Connector Link/Activity LEDs**

10Mbps/100Mbps/1Gbps LAN Link/Activity LED Scheme		
	Left LED	Right LED
No Link	Off	Off
10Mbps	Link	Off
	Active	Blinking Green
100Mbps	Link	Solid Green
	Active	Solid Green
1Gbps	Link	Solid Yellow
	Active	Solid Yellow

### 8.3.1 OCP\* Mezzanine Card 2.0 Support

The server board supports one (1) OCP Mezzanine 2.0 compliant add-in card. Refer to the *Intel® Server M20NTP Family Configuration Guide* for a list of validated cards.

Supported OCP 2.0 Mezzanine cards may include one or two interface connectors that install to matching connectors on the server board.



OCP\* Mezzanine Card 2.0 (Option)

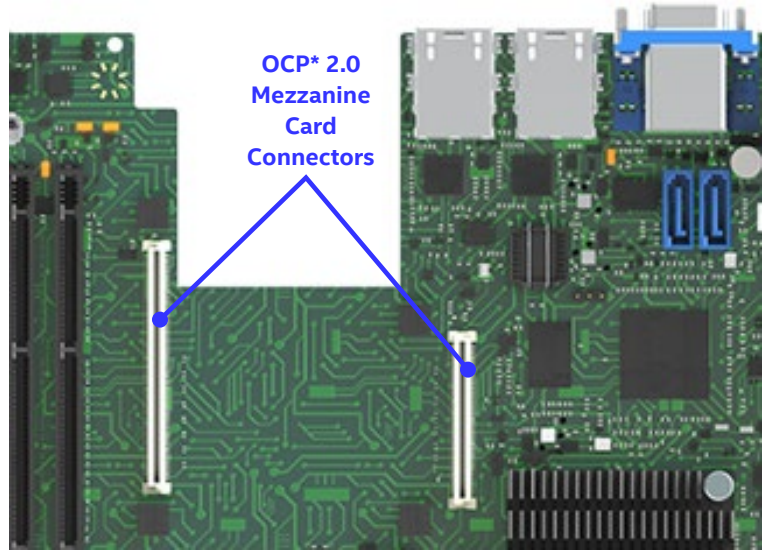


Figure 41. OCP\* Mezzanine 2.0 Add-in Card Support



## 9. Storage Interface Support Options

The server board supports the following PCIe NVMe and SATA storage interface connectors.

- One (1) onboard M.2 NVMe SSD connector
- Three (3) Multi-port SATA Mini-SAS\* HD cable connectors
- Two (2) Single-port SATA cable connectors
- Four (4) PCIe X4 SlimSAS\* cable connectors for NVMe support
- One (1) internal USB 3.0 Type A connector

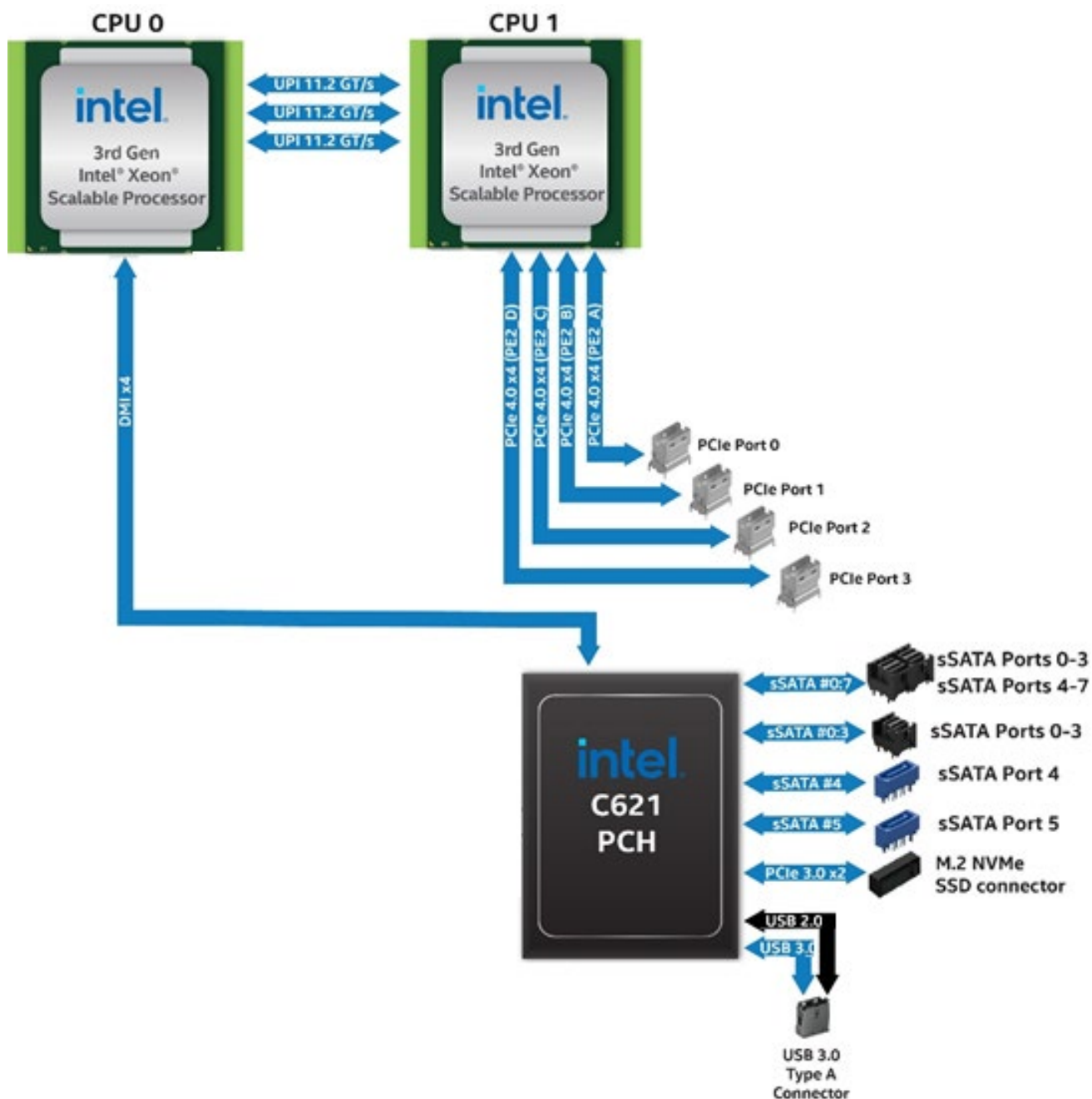


Figure 42. Storage Interface Support Architecture

## 9.1 Internal USB 3.0 Type A Connector

The server board includes a USB 3.0 Type A connector allowing support for a single internally mounted USB storage device.



Figure 43. Internal USB 3.0 Type A connector

## 9.2 Internal M.2 SSD Storage Support

The server board includes a single M.2 SSD connector allowing support for a single internally mounted M.2 NVMe SSD option. Supported M.2 SSD form factors include: 2242 (42 mm), 2280 (80 mm), and 22110 (110 mm).

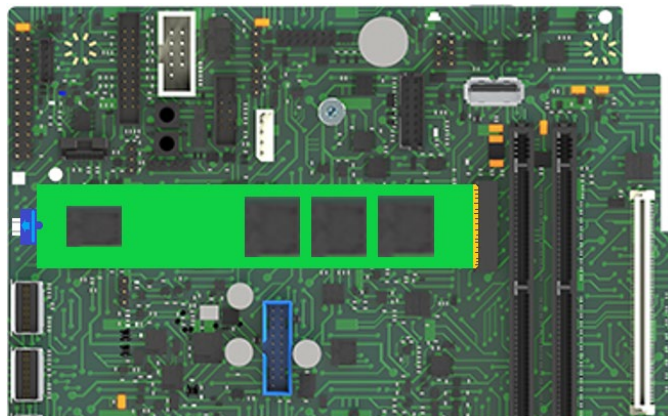


Figure 44. M.2 SSD Placement

When installed into the connector, the M.2 SSD is secured to the server board using an accessory clip that slides over the far edge of the device.

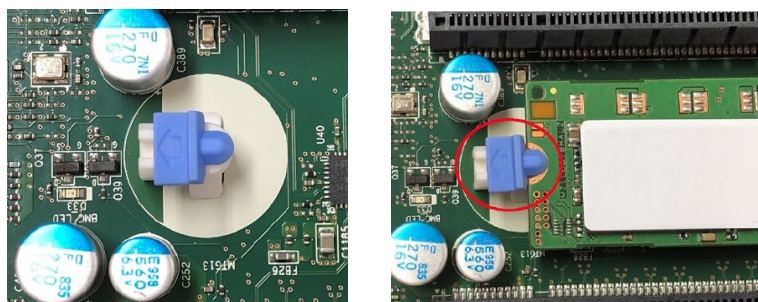


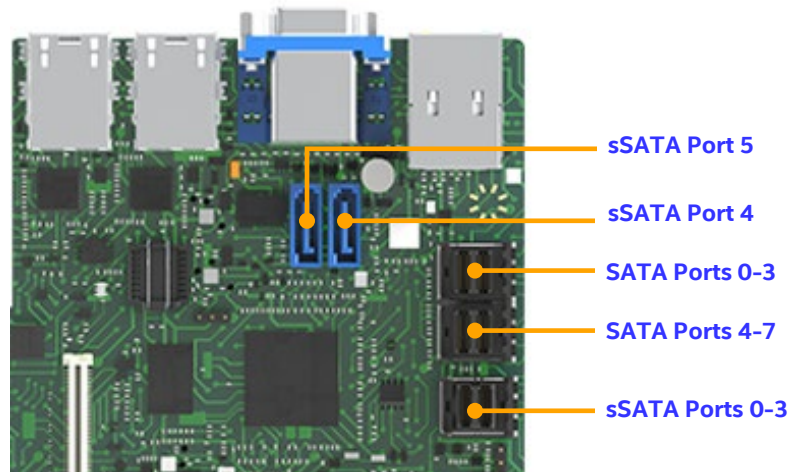
Figure 45. M.2 NVMe\* SSD Accessory Clip Placement

### 9.3 SATA Support

The Intel® C621 PCH includes two embedded AHCI SATA controllers, identified as “SATA” and “sSATA”, which provide the server board support for up to fourteen 6 GB/s SATA 3.0 devices.

SATA interface cable connectors on the server board are as follows:

- Four SATA ports from the Mini-SAS HD (SFF-8643) cable connector labeled “SATA\_0–3”
- Four SATA ports from the Mini-SAS HD (SFF-8643) cable connector labeled “SATA\_4–7”
- Four SATA ports from the Mini-SAS HD (SFF-8643) cable connector labeled “sSATA\_0-3”
- One SATA port from the 7-pin SATA cable connector labeled “sSATA\_4”
- One SATA port from the 7-pin SATA cable connector labeled “sSATA\_5”



**Figure 46. SATA Interface Cable Connectors**

Both embedded SATA controllers can be independently enabled or disabled and can be configured to support the following operating modes: AHCI mode or RAID mode. The SATA controllers can be configured using the <F2> BIOS setup utility under the **Advanced > Mass Storage Controller Configuration** menu screen.

The following table describes the features supported by both embedded SATA controllers.

**Table 14. SATA and 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 direct memory access (DMA)	Collapses a DMA Setup, then DMA Activate sequence into a DMA Setup only	Supported	Supported
Hot Plug Support (U.2 Drives Only)	Allows for device detection without power being applied and ability to connect and disconnect devices without prior notification to the system	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 and 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 the ability 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

### 9.3.1 Staggered Disk Spin-Up Option

For server systems configured with many SATA disk drives, the initial power on requirements needed to spin up all drives at once may be too high for a power supply to support, causing it to shut down prematurely.

To mitigate this condition and reduce the peak power demand during system startup, the embedded SATA controllers support a staggered spin-up option. Each installed SATA drive is initiated one at a time, with a short delay in between each startup. By default, this option is set to “Disabled” in BIOS setup utility. To enable this support, access the <F2> BIOS setup utility and enable the “AHCI HDD Staggered Spin-up” option found on the Mass Storage Controller Configuration menu.

## 9.1 Intel® Virtual RAID on CPU 7.5 (Intel® VROC) for SATA

Intel® VROC (SATA RAID) provides an enterprise RAID solution for SATA devices connected to the embedded SATA controllers of the Intel Platform Control Hub (PCH).

By default, onboard RAID options are disabled in BIOS setup utility. 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 or SATA Controller**.

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

Supported SATA RAID levels include RAID 0, RAID 1, RAID 5, and RAID 10.

- **RAID 0 (striping)** – RAID level 0 combines at least two (up to the maximum number) drives supported by the embedded SATA and sSATA controllers, so that all data is divided into manageable blocks called strips. The strips are distributed across the array members on which the RAID 0 volume resides. Data stored in a RAID 0 volume is not redundant. Therefore, if one drive fails, all data on the volume is lost.
- **RAID 1 (mirroring)** – Data is concurrently written to two drives creating real-time redundancy of all data written to the first drive. This condition is good for small databases or other applications that require small capacity but complete data redundancy. The maximum number of drives supported in a RAID 1 volume is two drives. The RAID 1 volume appears as a single physical drive with a capacity equal to that of the smaller drive.
- **RAID 5 (striping with parity)** – A RAID 5 volume provides the capacity of  $(N - 1) \times$  smallest size of the drives, where  $N \geq 3$  and  $\leq$  maximum number of drives supported by the SATA or sSATA controller. All data is divided into manageable blocks called strips. RAID 5 also stores parity, a mathematical method for recreating lost data on a single drive. The data and parity are striped across array members. Because of parity, it is possible to rebuild the data after replacing a failed drive with a new one. The maximum number of drives supported in a RAID 5 is the maximum number of drives supported by the platform.
- **RAID 10 (striping and mirroring)** – RAID level 10 uses four drives to create a combination of RAID levels 0 and 1. The data is striped across a two-disk array forming a RAID 0 component. Each of the drives in the RAID 0 array is mirrored to form a RAID 1 component. This condition provides the performance benefits of RAID 0 and the redundancy of RAID 1. The RAID 10 volume appears as a single physical drive with a capacity equal to the two smallest drives of the four-drive configuration. The space on the remaining two drives will be used for mirroring. The maximum number of drives supported in a RAID 10 is four.

Intel VROC 7.5 for SATA functionality requires the following:

- The embedded RAID option must be enabled in BIOS setup utility.
- Intel VROC 7.5 drivers must be loaded for the installed operating system.
- At least two SATA drives are needed to support RAID 0 or Raid 1.
- At least three SATA drives are needed to support RAID 5.
- Four SATA drives are needed to support RAID 10.



## 9.2 NVMe\* Support

The server board includes four PCIe X4 SlimSAS cable connectors providing the PCIe interface to support up to four NVMe SSDs (one NVMe SSD per connector). X16 PCIe lanes from CPU 1 are bifurcated to support each PCIe SlimSAS connector with X4 PCIe lanes.

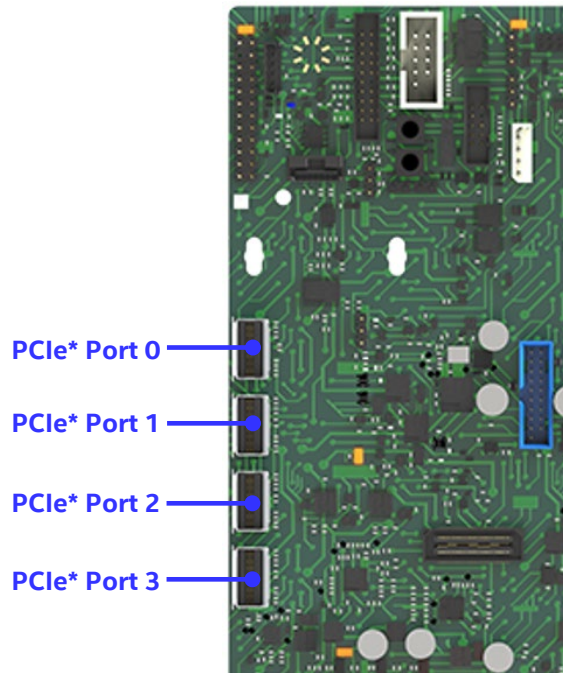


Figure 47. PCIe\* SlimSAS\* Connectors

### 9.2.1 Intel® Volume Management Device (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. Intel® VMD provides robust hot plug support and status LED management. This allows servicing of storage system NVMe SSD media without system crashes or hangs when ejecting or inserting NVMe SSD devices on the PCIe bus.

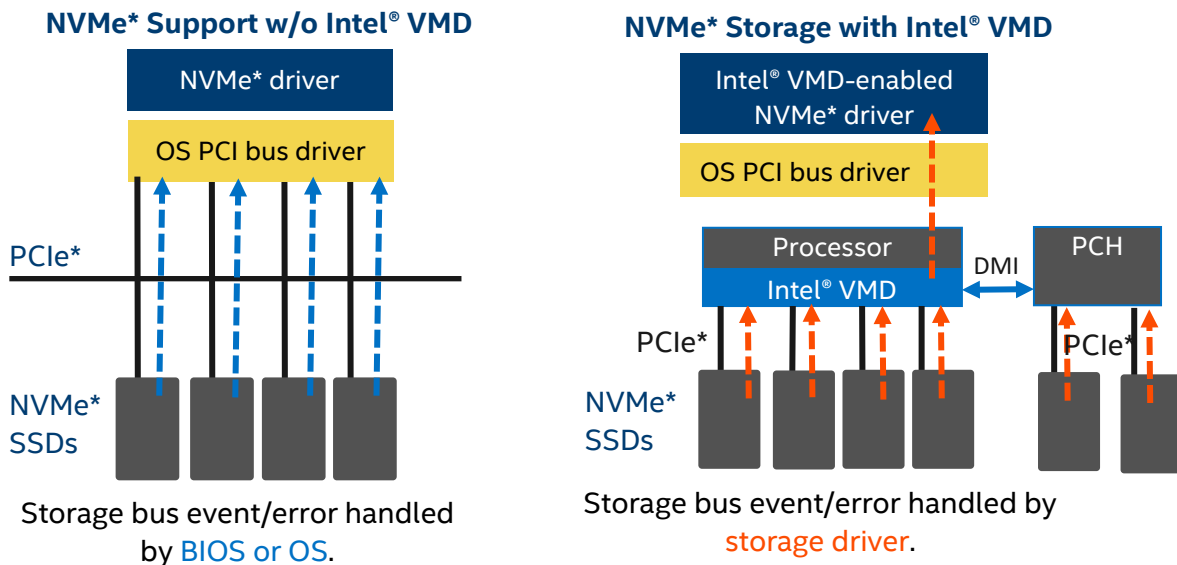


Figure 48. NVMe\* Storage Bus Event / Error Handling

Intel® VMD handles the physical management of NVMe storage devices as a stand-alone function. However, Intel® VMD can be enhanced when Intel® Virtual RAID on CPU (Intel® VROC) support options are enabled to implement RAID based storage systems.

Intel® VMD 2.0 includes the following features and capabilities:

- Hardware is integrated inside the processor 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 utility 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)
- Maximum of 128 PCIe bus numbers per domain.
- Support for Management Component Transport Protocol (MCTP) over SMBus\* only.
- Support for MMIO only (no port-mapped I/O).
- Does not support NTB, Quick Data Tech, Intel® Omni-Path Architecture (Intel® OPA), or SR-IOV.
- Correctable errors do not bring down the system.
- Intel VMD only manages devices on PCIe lanes routed directly from the processor or 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.

### 9.2.1.1 Enabling Intel® VMD 2.0 for NVMe\* Support

For installed NVMe devices to use the Intel® VMD features in the system, Intel® VMD must be enabled on the appropriate processor PCIe root ports in BIOS setup utility. By default, Intel® VMD support is disabled on all processor PCIe root ports in BIOS setup utility.

The following table provides the PCIe port routing information for the server board PCIe SlimSAS connectors.

**Table 15. CPU to PCIe\* NVMe\* SlimSAS\* Connector Routing**

Host	CPU Port	SlimSAS* Connector
CPU 1	PE2 A	PCIe_Port 0
	PE2 B	PCIe_Port 1
	PE2 C	PCIe_Port 2
	PE2 D	PCIe_Port 3

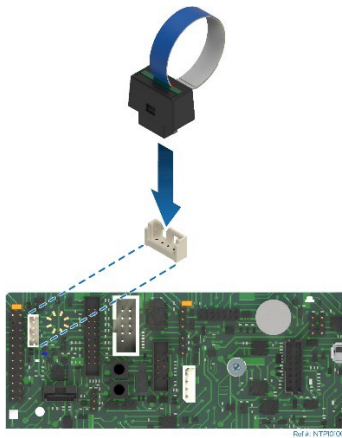
In BIOS setup utility, the Intel VMD support menu is on the following menu tab: **Advanced > PCI Configuration > Volume Management Device.**

## 9.2.2 Intel® Virtual RAID on CPU 7.5 (Intel® VROC) for NVMe\*

NVMe drives interfaced through the onboard PCIe SlimSAS connectors have optional support for RAID using Intel® Virtual RAID on CPU (Intel® VROC for NVMe) 7.5 technology. Intel® VROC 7.5 supports the following:

- I/O processor with controller (ROC) and DRAM.
- Protected write-back cache – software and hardware that allows recovery from a double fault.
- Isolated storage devices from operating system for error handling.
- Protected R5 data from operating system crash.
- NVMe SSD hot plug and surprise removal on processor PCIe lanes.
- LED management for PCIe attached storage.
- RAID/storage management using Representational State Transfer (RESTful) application programming interfaces (APIs).
- Graphical user interface (GUI) for Linux\*.
- 4K built-in NVMe SSD support.

Enabling Intel® VROC 7.5 support requires installation of an optional upgrade key on the server board as shown in [Figure 49](#).



**Figure 49. Intel® VROC Key Insertion**

The following table identifies available Intel VROC upgrade key options.

**Table 16. Optional Intel® VROC for NVMe Upgrade Key Features**

Intel® VROC for NVMe* RAID Features	Standard Intel® VROC Key (iPC – VROCSTANMOD)	Premium Intel® VROC Key (iPC – VROCPREMMOD)	Intel® SSD Only VROC Key (iPC – VROCISSDMOD)
Processor-attached NVMe* SSD – high performance	Yes	Yes	Yes
Boot on RAID volume	Yes	Yes	Yes
Third party vendor SSD support	Yes	Yes	No
RAID 0/1/10	Yes	Yes	Yes
RAID 0/1/5/10	No	Yes	Yes
RAID write hole closed (RMFBU replacement)	No	Yes	Yes
Hot plug/ surprise removal (2.5" SSD form factor only)	Yes	Yes	Yes
Enclosure LED management	Yes	Yes	Yes

## 10. Video Support

A standard 15-pin video connector is on the back edge of the server board.

### 10.1 Video Resolutions

The graphics controller of the Aspeed AST2500\* BMC is a VGA-compliant controller with 2D hardware acceleration and full bus primary support. With 16 MB of memory reserved, the video controller supports the resolutions in the following table.

**Table 17. Supported Video Resolutions**

2D Mode Resolution	2D Video Support (Color Bit)			
	8 bpp	16 bpp	24 bpp	32 bpp
640 x 480	60, 72, 75, 85	60, 72, 75, 85	Not Supported	60, 72, 75, 85
800 x 600	60, 72, 75, 85	60, 72, 75, 85	Not Supported	60, 72, 75, 85
1024 x 768	60, 72, 75, 85	60, 72, 75, 85	Not Supported	60, 72, 75, 85
1152 x 864	75	75	75	75
1280 x 800	60	60	60	60
1280 x 1024	60	60	60	60
1440 x 900	60	60	60	60
1600 x 1200	60	60	Not Supported	Not Supported
1680 x 1050	60	60	Not Supported	Not Supported
1920 x 1080	60	60	Not Supported	Not Supported
1920 x 1200	60	60	Not Supported	Not Supported

### 10.2 Server Board Video and Add-in Video Adapter Support

BIOS setup utility includes options to support the desired video operation.

#### 1. BIOS setup option: **Onboard Video**

Value: **Enabled/Disabled**

Help text: Enable or disable onboard video controller.

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

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

If there is an add-in video card installed in a PCIe slot connected to CPU Socket 0, and the Legacy VGA Socket option is set to CPU Socket 0, then this Onboard Video option is available to be set and default as Disabled.

If there is an add-in video card installed on a PCIe slot connected to CPU Socket 1, and the Legacy VGA Socket option is set to CPU Socket 1, this option is grayed out and unavailable, with a value set to Disabled. This is because the Onboard Video is connected to CPU Socket 0, and is not functional when CPU Socket 1 is the active path for video. When Legacy VGA Socket is set back to CPU Socket 0, this option becomes available again and is set to its default value of Enabled.

**2. BIOS setup option: Add-in Video Adapter**Value: **Enabled/Disabled**

Help text: When Onboard Video is Enabled, and Add-in Video Adapter is also Enabled, both can be active. The onboard video is still the primary console and active during BIOS POST; the add-in video adapter would be active under an OS environment with the video driver support.

When Onboard Video is Enabled, and Add-in Video Adapter is Disabled, then only the onboard video would be active.

When Onboard Video is Disabled, and Add-in Video Adapter is Enabled, then only the add-in video adapter would be active.

Comments: This option must be enabled to use an add-in card as a primary POST legacy video device.

If there is no add-in video card in any PCIe slot connected to CPU Socket 0 with the Legacy VGA Socket option set to CPU Socket 0, this option is set to Disabled and grayed out and unavailable.

If there is no add-in video card in any PCIe slot connected to CPU Socket 1 with the Legacy VGA Socket option set to CPU Socket 1, this option is set to Disabled and grayed out and unavailable.

If the Legacy VGA Socket option is set to CPU Socket 0 with both Add-in Video Adapter and Onboard Video enabled, the onboard video device works as primary video device while add-in video adapter as secondary Dual Monitor Support.

**3. BIOS setup option: Fast Video**Value: **Enabled/Disabled**

Help text: Fast video allows the screen light up in early phase.

---

**Note:** Fast Video only appears when Onboard Video is Enabled.

---

**4. BIOS setup option: Legacy VGA Socket**Value: **CPU Socket 0/CPU Socket 1**

Help text: Determines whether Legacy VGA video output is enabled for PCIe slots attached to Processor Socket 0 or 1. Socket 0 is the default.

Comments: This option is necessary when using an add-in video card on a PCIe slot attached to CPU Socket 1, due to a limitation of the processor IIO. This option allows the switch to use a video card in a slot connected to CPU Socket 1.

This option does not appear unless the BIOS is running on a board that has one processor installed on CPU Socket 1 and can potentially have a video card installed in a PCIe slot connected to CPU Socket 1.

This option is grayed out as unavailable and set to CPU Socket 0 unless there is a processor installed on CPU Socket 1 and a video card installed in a PCIe slot connected to CPU Socket 1. When this option is active and is set to CPU Socket 1, then both Onboard Video and Dual Monitor Video are set to Disabled and grayed out as unavailable. This is because the Onboard Video is a PCIe device connected to CPU Socket 0 and is unavailable when the Legacy VGA Socket is set to Socket 1.





### 11.1.1 Password Setup

The BIOS uses passwords to prevent unauthorized access to the server board. 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.

Intel strongly recommends that an administrator password be set. A system with no administrator password set allows anyone who has access to the server board to change BIOS settings.

An administrator password must be set 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. It 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 action requires the administrator password and must be done through BIOS setup utility. 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 [Chapter 14](#).

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. A SEL event is also logged to alert the authorized user or administrator that a password access failure has occurred.

### 11.1.2 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 utility, the BIOS halts early in POST to request a password (administrator or user) before continuing POST.

### 11.1.3 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 utility, 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 if the administrator password is enabled. Users are restricted from booting in anything other than the boot order defined in setup by an administrator.

## 11.2 Front Panel Lockout

If enabled in BIOS setup utility 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, system power off and reset must be controlled via a system management interface.

## 11.3 Intel® Total Memory Encryption (Intel® TME)

To better protect computer system memory, the 3<sup>rd</sup> Gen Intel Xeon Scalable processor supports Intel® Total Memory Encryption (Intel® TME). 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 on the external memory bus. Intel® TME is also available for multi-tenant server platforms, 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 situation 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 enabling and is applicable to all operating systems.

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

## 11.4 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.

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 is optimized to meet the application isolation needs of server systems in cloud environments:

- Massively increased electronic product code (enclave) size (up to 1 TB for typical dual-socket server system).
- Significant performance improvements: minimal impact vs built-in 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 Data Center 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 11.3](#) to enable Intel TME.

---

To enable/disable Intel® SGX, access the BIOS setup utility 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 will be disabled. See [Table 11](#) for details.

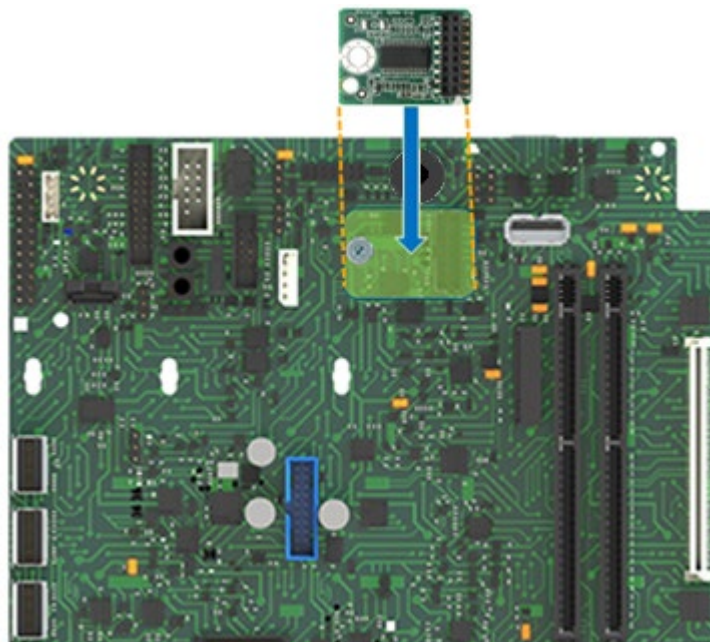
---

## 11.5 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. A TPM protects the system startup process by ensuring that it is tamper-free before releasing system control to the operating system.

A TPM device provides secured storage to store data, such as security keys and passwords. In addition, a TPM device has encryption and hash functions. The server board implements TPM as per *TPM PC Client Specifications revision 2.0*, published by the Trusted Computing Group (TCG).

A TPM device is optionally installed on the server board and is secured from external software attacks and physical theft.



**Figure 51. TPM Module Placement**

A pre-boot environment, such as the BIOS and operating system loader, uses the TPM to collect and store unique measurements from multiple factors within the boot process to create a system fingerprint. This unique fingerprint remains the same unless the pre-boot environment is tampered with. Therefore, it is used to compare to future measurements to verify the integrity of the boot process.

After the system BIOS completes the measurement of its boot process, it hands off control to the operating system loader and, in turn, to the operating system. If the operating system is TPM-enabled, it compares the BIOS TPM measurements to those of previous boots to make sure that the system was not tampered with before continuing the operating system boot process. Once the operating system is in operation, it optionally uses the TPM to provide additional system and data security (for example, Microsoft Windows\* 10 supports BitLocker\* drive encryption).

Intel offers two orderable TPM accessory kits for this product family:

**Table 18. Orderable TPM Accessory Kits**

Intel Product Code	MM#	Description
JNPTPM	999PLH	TPM 2.0 Module (ROW) - TM-TPM2-I-3353-JNP
JNPTPMCH	999PM2	TPM 2.0 Module (China) - TM-TPM2-Z-JNP

**Note:** Available TPM Accessories are not supported by Microsoft\* Windows Server 2022.



### 11.5.1 Trusted Platform Module (TPM) Security BIOS

The BIOS TPM support conforms to the TPM PC Client Implementation Specification for Conventional BIOS the 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, see the *TCG PC Client Specific Implementation Specification*, the *TCG PC Client Specific Physical Presence Interface Specification*, and the *Microsoft Windows\* BitLocker\* Requirements* documents.

### 11.5.2 Physical Presence

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

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

1. 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 utility entry, and boots directly to the operating system that requested the TPM command.

### 11.5.3 TPM Security Setup Options

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

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

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

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

## 11.6 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). The two security features combined included some redundancies and inefficiencies between them.

### 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

### 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

With this product generation, Intel rearchitected and fused together the two technologies into 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>.

## 11.7 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 technology provides the capability to ensure that those UEFI images are only loaded in an owner authorized fashion.

The technology also provides a common means to ensure platform security and integrity over systems running UEFI-based firmware. The Intel Server Board BIOS is compliant with the UEFI Specification 2.3.1 Errata C for UEFI secure boot feature.

UEFI secure boot requires built-in UEFI boot mode and it disables legacy Option ROM dispatch. By default, secure boot on Intel server boards is disabled as the default boot mode is legacy mode.

To enable / disable UEFI Secure Boot in the BIOS setup utility menu, select **Boot Maintenance Manager > Advanced Boot Options > Secure Boot Configuration**.

## 12. Server Board Connectors and Headers

---

This chapter identifies the location and pinout for most connectors and headers on the server board. Information for some connectors and headers is found elsewhere in the document where the feature is described in more detail.

---

**Note:** Pinout definition tables included in this section will show an image of the specified connector/header in the same orientation as is mounted on the server board. Pin-1 on both the connector/header image and its pinout definition table will be identified using a black triangle. The pinout definition within a given table will match the orientation of the pins of the given connector/header.

---

### 12.1 PCIe\* Riser Card Slots

Riser Card Slot schematics are available upon request (Intel NDA Required). See [Section 3.4](#) for additional information.

### 12.2 Main Power and CPU Power Cable Connectors

See [Section 3.5](#).

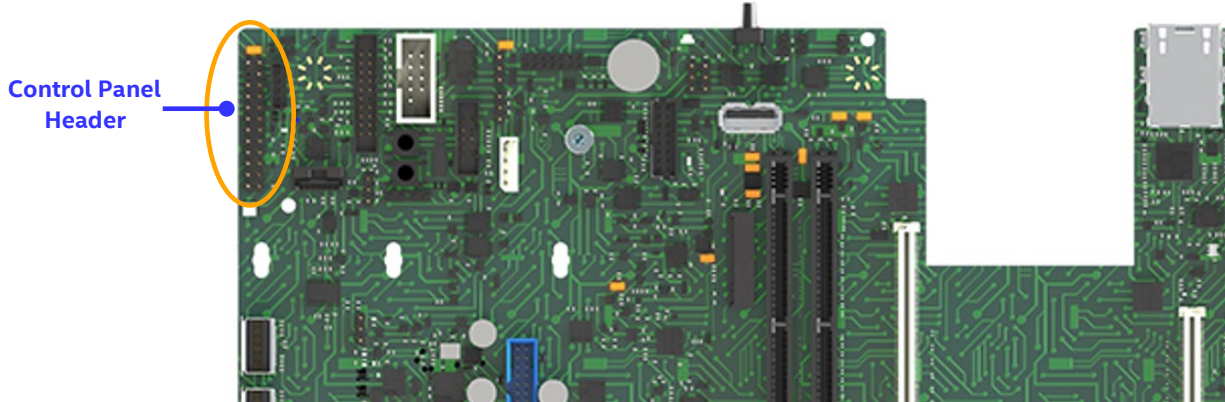
### 12.3 System Fan Cable Connectors

See [Section 3.6](#).

## 12.4 Front Panel Cable Header

The server board includes an SSI compatible 24-pin Front Panel cable header supporting the following features:

- System Power LED
- System ID LED
- Hard Drive Activity LED
- System Fault LED
- LAN 0 Activity LED
- LAN 1 Activity LED
- System Power Button
- System ID LED Button
- NMI Reset Button
- System Reset Button
- Support for a chassis intrusion switch
- Support for a front panel temperature sensor

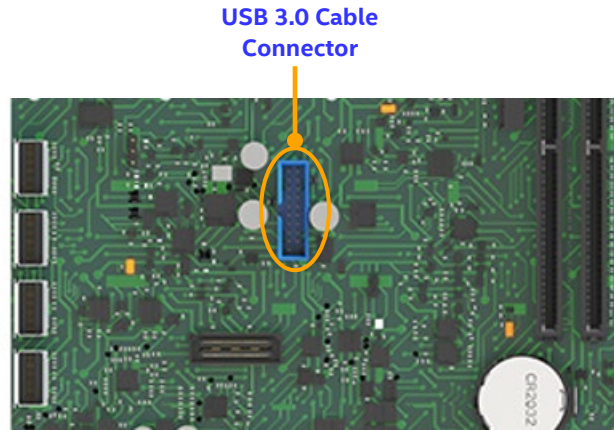


**Table 19. Control Panel Cable Header Pinout**

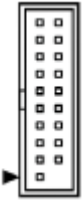
	Signal	Pin	Pin	Signal
	FP_PW_LED_PW	1	2	FP_PWER (VCC3_Aux)
	KEY	3	4	FP_ID_LED_PW
	FP_PW_LED_GND	5	6	FP_ID_LED_N
	HDD_LED_PW	7	8	BMC_HW_FAULT_N
	HDD_ACT_LED_N	9	10	BMC_SYS_FAULT_N
	FP_PWR_BTN_N	11	12	LAN0_LED_P
	GND	13	14	LAN0_LED_N
	FP_RST_BTN_JP_N	15	16	FP_SMB_DAT
	GND	17	18	FP_SMB_CLK
	FP_IDLED_BTN_N	19	20	FP_INTRUSION_N
	SYS_AIR_INLET	21	22	LAN1_LED_P
	FP_NMI_BTN_N	23	24	LAN1_LED_N

## 12.5 Onboard USB 3.0 Cable Connector

The server board includes a Blue 20-pin cable connector providing optional support for up to two USB 3.0 ports.



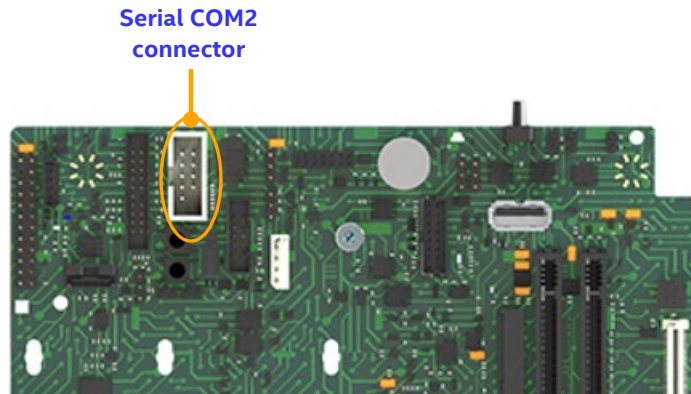
**Table 20. Onboard USB 3.0 Cable Connector Pinout**

	Signal	Pin	Pin	Signal
	OC_N	10	11	P1_P
	PO_P	9	12	P1_N
	PO_N	8	13	GND
	GND	7	14	P1_TX_P
	PO_TX_P	6	15	P1_TX_N
	PO_TX_N	5	16	GND
	GND	4	17	P1_RX_P
	PO_RX_P	3	18	P1_RX_N
	PO_RX_N	2	19	+5V
	+5V	1 (▽)	20	Key



## 12.6 Onboard Serial COM2 Cable Connector

The server board includes a 10-pin DH-10 cable connector providing optional support for a 2<sup>nd</sup> serial port. On the server board, the connector is labeled as “COM 2”. The pinout for this connector adheres to the DTK pinout specification.

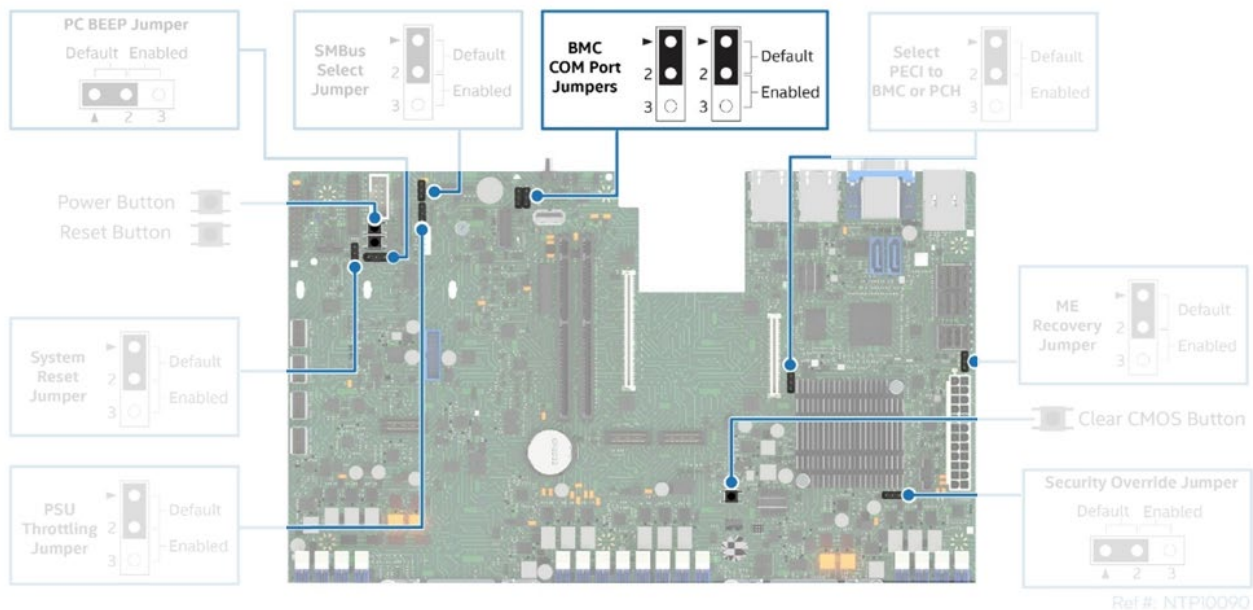


**Table 21. Onboard DH10 Serial COM2 Connector Pinout**

	Signal	Pin	Pin	Signal
	COM2_DCD	1 (∇)	2	COM2_DSR
	COM2_RXD	3	4	COM2_RTS
	COM2_TXD	5	6	COM2_CTS
	COM2_DTR	7	8	COM2_NRI
	GND	9	10	KEY



Changing the jumper blocks labeled as J118 and J119 on the server board will change the RXD and TXD signals of COM2 to support a COM5 configuration as shown in the following figure.

**Note:** COM5 support is generally used for debug purposes only. Intel recommends keeping the jumper blocks connected to J118 and J119 in their default positions.





**Table 22. Serial COM2 Configuration Jumpers**

**J118: BMC COM Port Jumper**

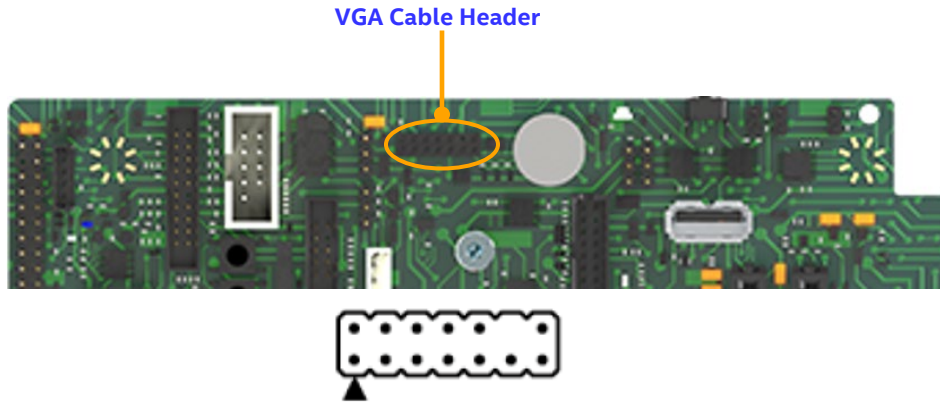
	Signal	Pin	Pin	Signal
	BMC_COM2_RXD	1	2	RXD_2
	BMC_COM5_RXD	3		
	Pin1-2 closed: BMC COM PORT2 (Default) Pin2-3 closed: BMC CONSOLE PORT5			

**J119: BMC COM Port Jumper**

	Signal	Pin	Pin	Signal
	BMC_COM2_TXD	1	2	TXD_2
	BMC_COM5_TXD	3		
	Pin1-2 closed: BMC COM PORT2 (Default) Pin2-3 closed: BMC CONSOLE PORT5			

## 12.7 Onboard VGA Cable Header

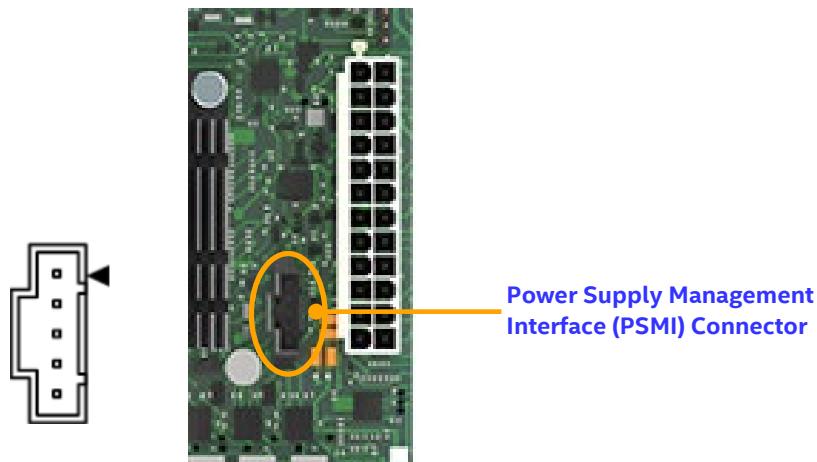
The server board includes a 14-pin cable header providing optional support for a front panel VGA connector.



**Table 23. Onboard VGA Cable Header Pinout**

Signal	VGA2_5V	HD_VGA_R	HD_VGA_G	HD_VGA_B	HD_VGA_DAT	Key	HD_VGA_VS
Pin	2	4	6	8	10	12	14
Pin	1 (∇)	3	5	7	9	11	13
Signal	GND	GND	GND	GND	GND	HD_VGA_HS	HD_VGA_CLK

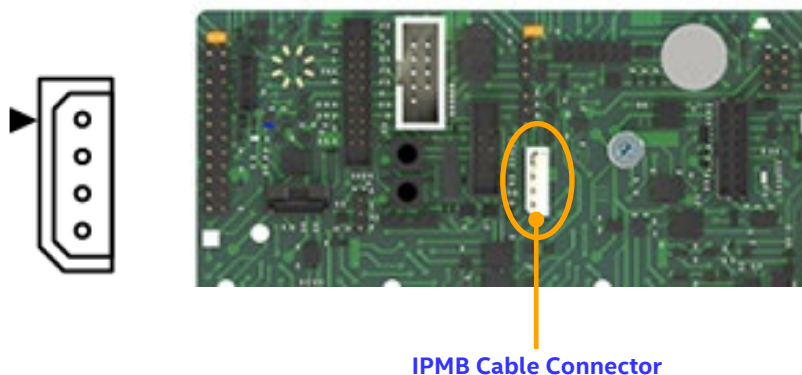
## 12.8 Power Supply Management Interface (PSMI) Cable Connector



**Table 24. PSMI Cable Connector Pinout**

Pin	Signal
1 (▽)	SMB_CLK
2	SMB_DAT
3	PSU_SMBALERT_N
4	GND
5	V3.3

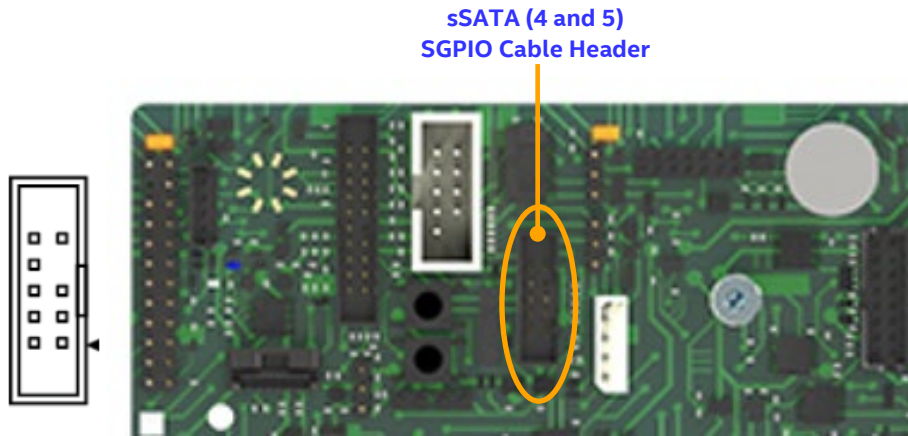
## 12.9 Intelligent Platform Management Bus (IPMB) Cable Connector



**Table 25. IPMB Cable Connector Pinout**

Pin	Signal
1 (▽)	IPMB_DAT
2	GND
3	IPMB_CLK
4	VCC3_AUX

## 12.10 sSATA SGPIO Cable Header

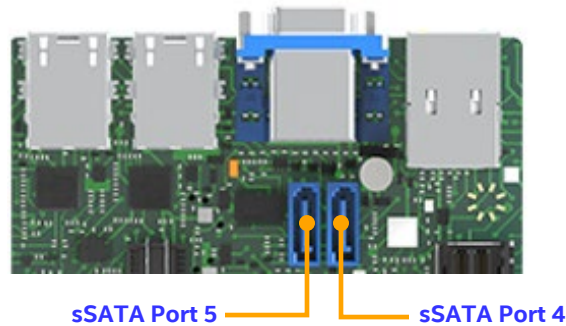


**Table 26. sSATA (4 and 5) SGPIO Cable Header Pinout**


Signal	Pin	Pin	Signal
No connect	10	9	VCC3_AUX
SCLOCK	8	7	Key
SLOAD	6	5	GND
SDATA OUT	4	3	SDA
No connect	2	1	SCL

## 12.11 sSATA Ports 4 and 5 Cable Connectors


The server board includes two 7-pin SATA cable connectors supporting sSATA ports 4 and 5.



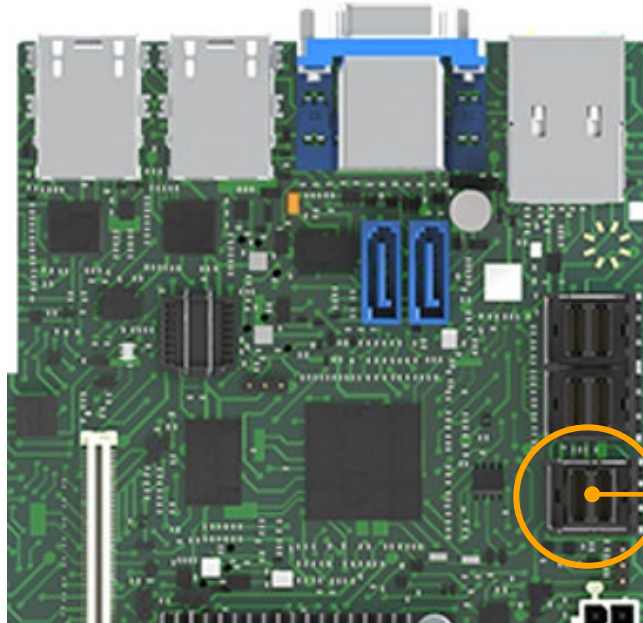
**Table 27. sSATA Port 4 Cable Connector Pinout**

	PIN Define	Pin
		1
2		SSATA4_TXP_C
3		SSATA4_TXN_C
4		GND
5		SSATA4_RXN_C
6		SSATA4_RXP_C
7		GND

**Table 28. sSATA Port 5 Cable Connector Pinout**

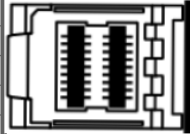
	PIN Define	Pin
	1	GND
	2	SSATA5_TXP_C
	3	SSATA5_TXN_C
	4	GND
	5	SSATA5_RXN_C
	6	SSATA5_RXP_C
7	GND	

## 12.12 sSATA Ports 0–3 Mini-SAS\* HD Cable Connector



sSATA Ports 0 – 3 Mini-SAS\* HD Cable Connector

**Table 29. sSATA Ports 0–3 Mini-SAS\* HD Cable Connector Pinout**

	Signal	Pin	Pin	Signal
	PCH_SSATA_0-3_A1	A1	B1	GND
	SGPIO_SSATA_CLK	A2	B2	SGPIO_SSATA_LOAD
	GND	A3	B3	GND
	SSATA1_RXP_C	A4	B4	SSATA0_RXP_C
	SSATA1_RXN_C	A5	B5	SSATA0_RXN_C
	GND	A6	B6	GND
	SSATA3_RXP_C	A7	B7	SSATA2_RXP_C
	SSATA3_RXN_C	A8	B8	SSATA2_RXN_C
	GND	A9	B9	GND
	SSGPIO_DO_0R	C1	D1	SSGPIO_DI_0R
	GND	C2	D2	SAS1_CTYPE
	GND	C3	D3	GND
	SSATA1_TXP_C	C4	D4	SSATA0_TXP_C
	SSATA1_TXN_C	C5	D5	SSATA0_TXN_C
	GND	C6	D6	GND
	SSATA3_TXP_C	C7	D7	SSATA2_TXP_C
	SSATA3_TXN_C	C8	D8	SSATA2_TXN_C
	GND	C9	D9	GND



## 12.13 SATA Ports 0–7 Dual Mini-SAS\* HD Cable Connector

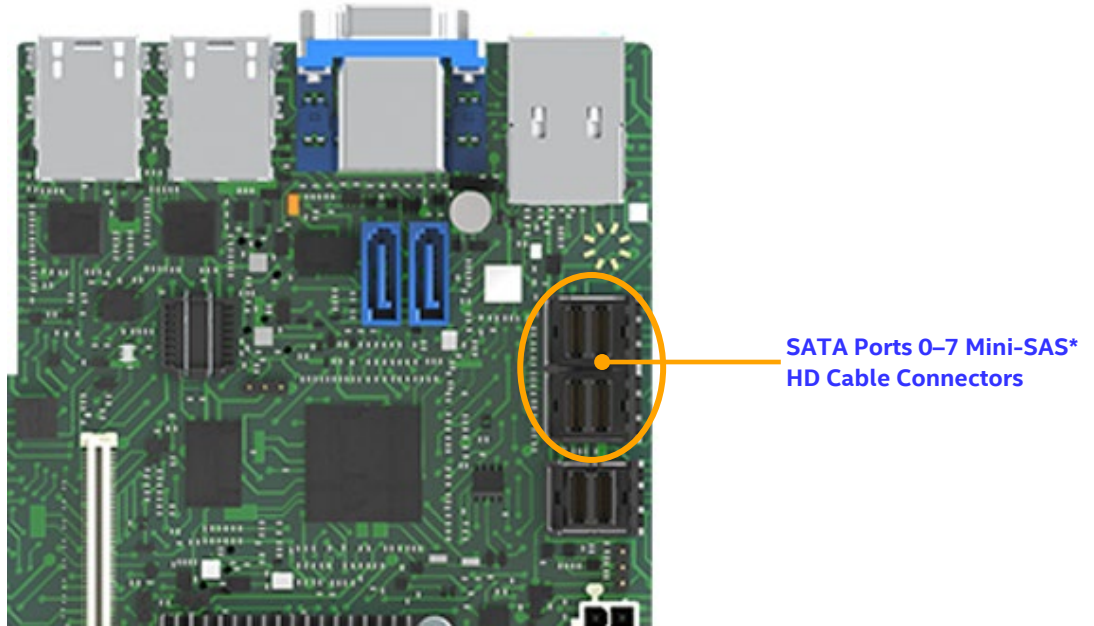
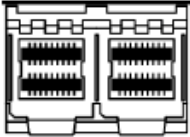
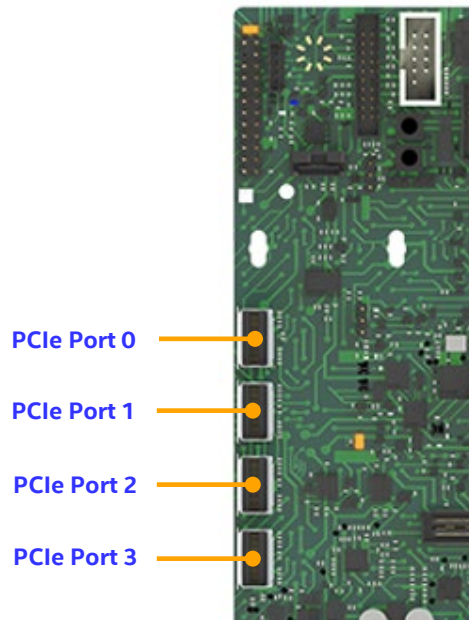


Table 30. SATA Ports 0–7 Dual Mini-SAS\* HD Cable Connector Pinout

	Signal	Pin	Pin	Signal
	PCH_SATA_0-7_A1	A1	B1	GND
	SGPIO_SATA_CLK	A2	B2	SGPIO_SATA_LOAD
	GND	A3	B3	GND
	SATA1_RXP_C	A4	B4	SATA0_RXP_C
	SATA1_RXN_C	A5	B5	SATA0_RXN_C
	GND	A6	B6	GND
	SATA3_RXP_C	A7	B7	SATA2_RXP_C
	SATA3_RXN_C	A8	B8	SATA2_RXN_C
	GND	A9	B9	GND
	SGPIO_DO_0R	C1	D1	SGPIO_DI_0R
	GND	C2	D2	SAS0_CTYPE
	GND	C3	D3	GND
	SATA1_TXP_C	C4	D4	SATA0_TXP_C
	SATA1_TXN_C	C5	D5	SATA0_TXN_C
	GND	C6	D6	GND
	SATA3_TXP_C	C7	D7	SATA2_TXP_C
	SATA3_TXN_C	C8	D8	SATA2_TXN_C
	GND	C9	D9	GND
	NC_PCH_SATA_0-7_A10	A10	B10	GND
	SGPIO_SATA_CLK	A11	B11	SGPIO_SATA_LOAD
	GND	A12	B12	GND
	SATA5_RXP_C	A13	B13	SATA4_RXP_C
	SATA5_RXN_C	A14	B14	SATA4_RXN_C
	GND	A15	B15	GND
	SATA7_RXP_C	A16	B16	SATA6_RXP_C
	SATA7_RXN_C	A17	B17	SAA6_RXN_C
	GND	A18	B18	GND
	SGPIO_DO_1R	C10	D10	SGPIO_DI_1R
	GND	C11	D11	SAS1_CTYPE
	GND	C12	D12	GND
	SATA5_TXP_C	C13	D13	SATA4_TXP_C
	SATA5_TXN_C	C14	D14	SATA4_TXN_C
	GND	C15	D15	GND
	SATA7_TXP_C	C16	D16	SATA6_TXP_C
SATA7_TXN_C	C17	D17	SATA6_TXN_C	
GND	C18	D18	GND	

## 12.14 NVMe\* Port Cable Connectors


The server board includes four PCIe X4 SlimSAS cable connectors identified as NVMe Ports 1–4.




**Table 31. PCIe\* NVMe\* Port 0 Cable Connector Pinout**

	Signal Name	Pin	Pin	Signal Name
	GND	A1	B1	GND
	CPU1_PE2_ABCD_RX_DN0	A2	B2	CPU1_PE2_ABCD_TX_DP0_C
	CPU1_PE2_ABCD_RX_DP0	A3	B3	CPU1_PE2_ABCD_TX_DN0_C
	GND	A4	B4	GND
	CPU1_PE2_ABCD_RX_DN1	A5	B5	CPU1_PE2_ABCD_TX_DP1_C
	CPU1_PE2_ABCD_RX_DP1	A6	B6	CPU1_PE2_ABCD_TX_DN1_C
	GND	A7	B7	GND
	BP_TYPEA	A8	B8	PE_HD0_SMB_CLK
	PE_WAKE_N0	A9	B9	PE_HD0_SMB_DAT
	GND	A10	B10	GND
	SLIMSAS_NVME0_DP	A11	B11	PCIE_SLIMSAS_RST_N
	SLIMSAS_NVME0_DN	A12	B12	CPRSNTA-
	GND	A13	B13	GND
	CPU1_PE2_ABCD_RX_DN2	A14	B14	CPU1_PE2_ABCD_TX_DP2_C
	CPU1_PE2_ABCD_RX_DP2	A15	B15	CPU1_PE2_ABCD_TX_DN2_C
	GND	A16	B16	GND
	CPU1_PE2_ABCD_RX_DN3	A17	B17	CPU1_PE2_ABCD_TX_DP3_C
	CPU1_PE2_ABCD_RX_DP3	A18	B18	CPU1_PE2_ABCD_TX_DN3_C
	GND	A19	B19	GND


**Table 32. PCIe\* NVMe\* Port 1 Cable Connector Pinout**

	Signal Name	Pin	Pin	Signal Name
		GND	A1	B1
	CPU1_PE2_ABCD_RX_DN4	A2	B2	CPU1_PE2_ABCD_TX_DP4_C
	CPU1_PE2_ABCD_RX_DP4	A3	B3	CPU1_PE2_ABCD_TX_DN4_C
	GND	A4	B4	GND
	CPU1_PE2_ABCD_RX_DN5	A5	B5	CPU1_PE2_ABCD_TX_DP5_C
	CPU1_PE2_ABCD_RX_DP5	A6	B6	CPU1_PE2_ABCD_TX_DN5_C
	GND	A7	B7	GND
	BP_TYPEB	A8	B8	PE_HD1_SMB_CLK
	PE_WAKE_N1	A9	B9	PE_HD1_SMB_DAT
	GND	A10	B10	GND
	SLIMSAS_NVME1_DP	A11	B11	PCIE_SLIMSAS_RST_N
	SLIMSAS_NVME1_DN	A12	B12	CPRSNTA-
	GND	A13	B13	GND
	CPU1_PE2_ABCD_RX_DN6	A14	B14	CPU1_PE2_ABCD_TX_DP6_C
	CPU1_PE2_ABCD_RX_DP6	A15	B15	CPU1_PE2_ABCD_TX_DN6_C
	GND	A16	B16	GND
	CPU1_PE2_ABCD_RX_DN7	A17	B17	CPU1_PE2_ABCD_TX_DP7_C
	CPU1_PE2_ABCD_RX_DP7	A18	B18	CPU1_PE2_ABCD_TX_DN7_C
	GND	A19	B19	GND

**Table 33. PCIe\* NVMe\* Port 2 Cable Connector Pinout**

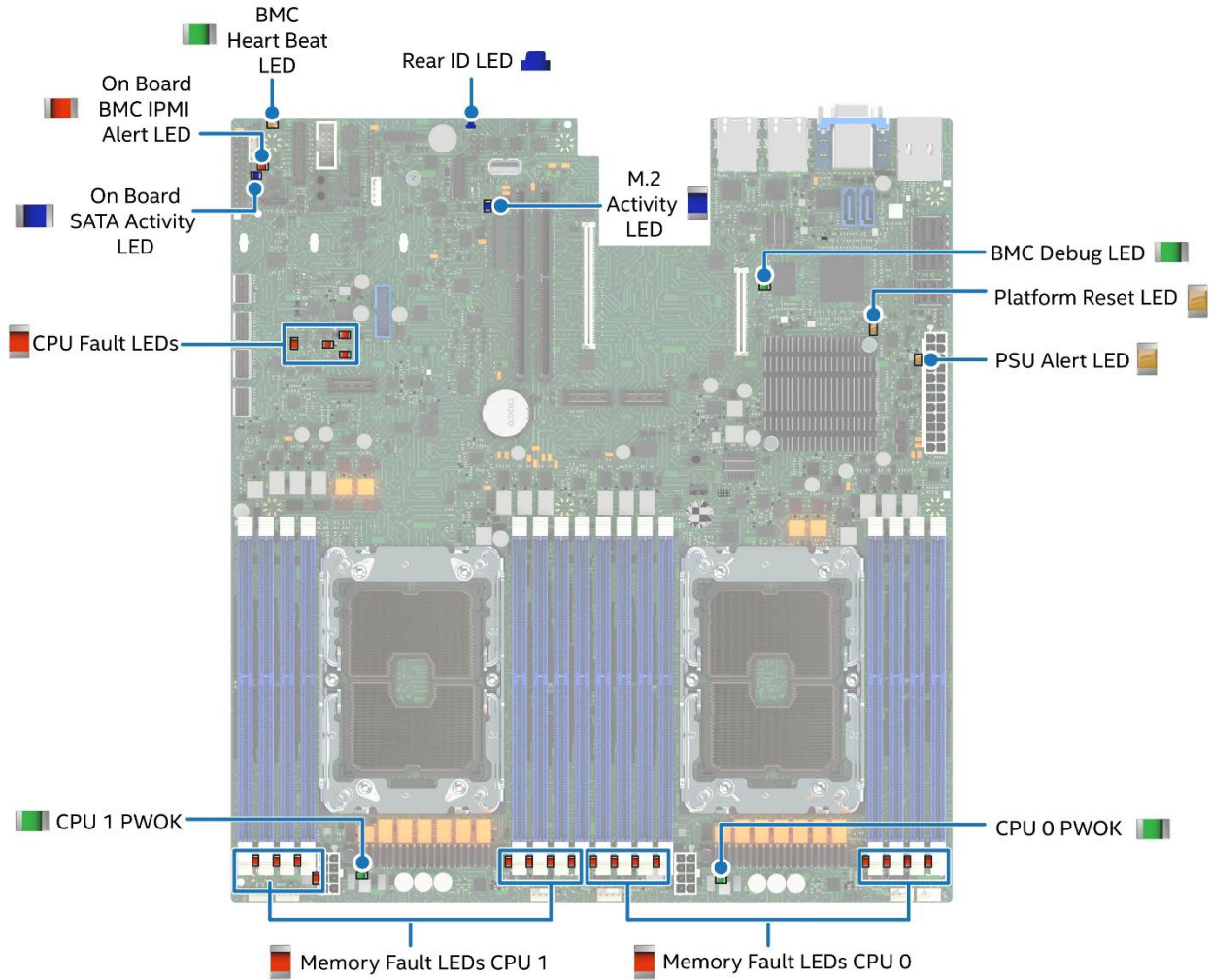
	Signal Name	Pin	Pin	Signal Name
		GND	A1	B1
	CPU1_PE2_ABCD_RX_DN8	A2	B2	CPU1_PE2_ABCD_TX_DP8_C
	CPU1_PE2_ABCD_RX_DP8	A3	B3	CPU1_PE2_ABCD_TX_DN8_C
	GND	A4	B4	GND
	CPU1_PE2_ABCD_RX_DN9	A5	B5	CPU1_PE2_ABCD_TX_DP9_C
	CPU1_PE2_ABCD_RX_DP9	A6	B6	CPU1_PE2_ABCD_TX_DN9_C
	GND	A7	B7	GND
	BP_TYPEC	A8	B8	PE_HD2_SMB_CLK
	PE_WAKE_N2	A9	B9	PE_HD2_SMB_DAT
	GND	A10	B10	GND
	SLIMSAS_NVME2_DP	A11	B11	PCIE_SLIMSAS_RST_N
	SLIMSAS_NVME2_DN	A12	B12	CPRSNTA-
	GND	A13	B13	GND
	CPU1_PE2_ABCD_RX_DN10	A14	B14	CPU1_PE2_ABCD_TX_DP10_C
	CPU1_PE2_ABCD_RX_DP10	A15	B15	CPU1_PE2_ABCD_TX_DN10_C
	GND	A16	B16	GND
	CPU1_PE2_ABCD_RX_DN11	A17	B17	CPU1_PE2_ABCD_TX_DP11_C
	CPU1_PE2_ABCD_RX_DP11	A18	B18	CPU1_PE2_ABCD_TX_DN11_C
	GND	A19	B19	GND

**Table 34. PCIe\* NVMe\* Port 3 Cable Connector Pinout**

	Signal Name	Pin	Pin	Signal Name
		GND	A1	B1
	CPU1_PE2_ABCD_RX_DN12	A2	B2	CPU1_PE2_ABCD_TX_DP12_C
	CPU1_PE2_ABCD_RX_DP12	A3	B3	CPU1_PE2_ABCD_TX_DN12_C
	GND	A4	B4	GND
	CPU1_PE2_ABCD_RX_DN13	A5	B5	CPU1_PE2_ABCD_TX_DP13_C
	CPU1_PE2_ABCD_RX_DP13	A6	B6	CPU1_PE2_ABCD_TX_DN13_C
	GND	A7	B7	GND
	BP_TYPED	A8	B8	PE_HD3_SMB_CLK
	PE_WAKE_N3	A9	B9	PE_HD3_SMB_DAT
	GND	A10	B10	GND
	SLIMSAS_NVME3_DP	A11	B11	PCIE_SLIMSAS_RST_N
	SLIMSAS_NVME3_DN	A12	B12	CPRSNTA-
	GND	A13	B13	GND
	CPU1_PE2_ABCD_RX_DN14	A14	B14	CPU1_PE2_ABCD_TX_DP14_C
	CPU1_PE2_ABCD_RX_DP14	A15	B15	CPU1_PE2_ABCD_TX_DN14_C
	GND	A16	B16	GND
	CPU1_PE2_ABCD_RX_DN15	A17	B17	CPU1_PE2_ABCD_TX_DP15_C
	CPU1_PE2_ABCD_RX_DP15	A18	B18	CPU1_PE2_ABCD_TX_DN15_C
	GND	A19	B19	GND

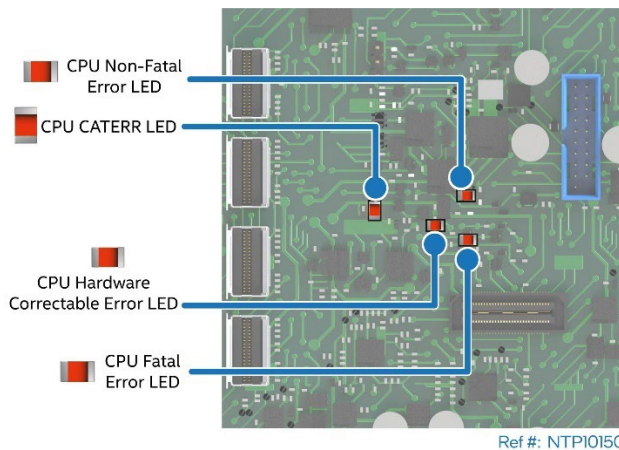
## 13. Intel® Light Guided Diagnostics

This chapter identifies and provides a descriptive overview for each LED found on the server board.



Ref #: NTP10082

**Figure 52. Intel® Light-Guided Diagnostics – LED Identification**



Ref #: NTP10150

**Figure 53. CPU Fault LED Identification**



Table 35. Onboard LED Descriptions

LED	State	Description
BMC Debug LED	Off	BMC Firmware not running
	Blinking Green	<b>10 Hz:</b> ARM Running on Flash <b>2 Hz:</b> ARM Running on DRAM without interrupt enabled <b>0.5 Hz:</b> ARM Running on DRAM with interrupt monitor enabled (normal operating mode) <b>0.1 Hz:</b> Abnormal mode, some interrupts are not serviced for over 2 seconds
BMC Heart Beat LED	Off	BMC has not initialized and cannot be detected
	Blinking Green	<b>Normal State</b> – LED blinks once per sec to indicate that the BMC is functioning normally
CPU 0 Power Status LED (PWOK)	Off	Power to CPU 0 is faulty
	On Green	Power to CPU 0 is OK
CPU 1 Power Status LED (PWOK)	Off	Power to CPU 1 is faulty
	On Green	Power to CPU 1 is OK
PSU Alert LED	Off	Power supply normal
	On Orange	Power supply fault
Rear ID LED	Off	
	On Blue	Used to identify system in rack
CPU CATERR LED	Off	Normal state
	On Red	CPU CAT Error has occurred
CPU Hardware Correctable Error LED	Off	Normal State
	On Red	A CPU hardware correctable error has occurred
CPU Non-Fatal Error LED	Off	Normal State
	On Red	A CPU Non-fatal error has occurred
CPU Fatal Error LED	Off	Normal State
	On Red	A CPU Fatal error has occurred
M.2 SSD Activity LED	Off	No activity on SSD
	Blinking Blue	Activity on M.2 SSD is occurring
SATA Drive Activity LED	Off	No activity on any SATA drive attached to onboard SATA connectors
	Blinking Blue	Activity on SATA drive attached to onboard SATA connector
Memory Fault LEDs (1 LED per DIMM Slot)	Off	DIMM functioning properly
	On Red	Memory fault has occurred
IPMI Hardware Sensor Alert LED	Off	System is operating in a degraded state with an impending failure warning, although still functioning. System is likely to fail.
	Solid Amber	System is operating normally.
	Blinking Amber	System is operating in a degraded state although still functioning, or system is operating in a redundant state but with an impending failure warning.



## 14. Server Board Jumpers Blocks and Service Buttons

The server board includes several jumper blocks and service buttons that can be used to configure, protect, reset, or recover specific features of the server board. The following figure identifies the location of each jumper block and service button on the server board. Pin 1 of each jumper can be identified by the arrowhead (▼) silkscreened on the server board next to the pin. The following sections describe how each jumper is used.

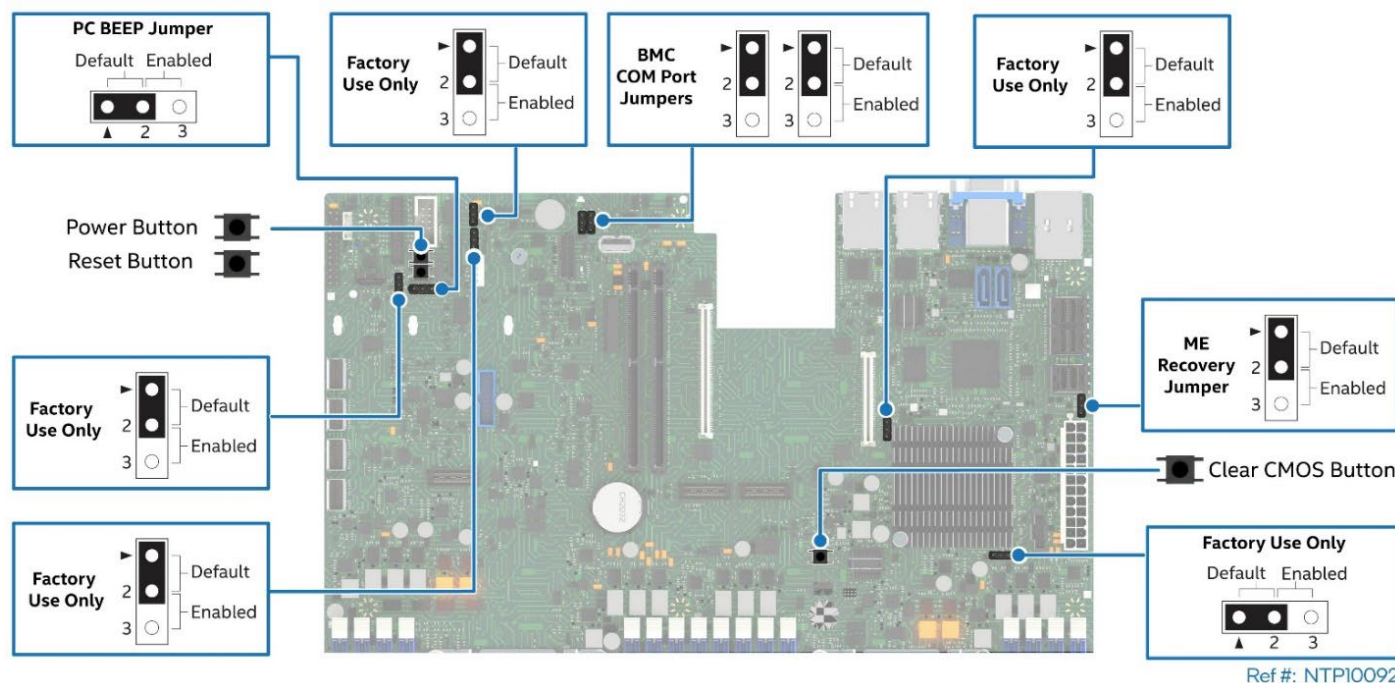


Figure 54. Reset and Recovery Jumper Header Locations

### 14.1 Onboard Service Buttons

The server board includes three surface mount buttons. The Power and Reset buttons can be used to power down or cold reset the system if no control panel is present.

#### 14.1.1 Clear CMOS Button

The Clear CMOS button is used to:

- Reset the BIOS to its original default settings
- Reset the Real time clock
- Clear any BIOS security passwords

To use this feature:

1. Power off the system and disconnect the power cord(s) from the system. Wait 30 seconds
2. Press the Clear CMOS button
3. Reconnect the power cord(s) to the system and power on the system
4. During POST, enter <F2> BIOS setup utility to reconfigure desired BIOS Settings and set the system time and date
5. Save settings, exit BIOS setup utility, and reboot the system

**Note:** This same procedure should be performed when updating the system BIOS.

## 14.2 Onboard Jumper Blocks

The server board includes several 3-pin jumper blocks. Most are used for factory support purposes and should not be changed from their default settings. The following can be used as needed.

### 14.2.1 PC Beep Jumper

The server board includes a small surface mount speaker near the back edge of the server board. The speaker is used to generate auditory beep codes when the BIOS or BMC detects an error during the power on POST process. The PC Beep Jumper can be set to enable or disable the auditory beep codes.

### 14.2.2 BMC COM Port Configuration Jumpers

See [Section 12.6](#).

### 14.2.3 ME Recovery Jumper

The ME Recovery jumper is used to place the embedded Intel® Management Engine (Intel® ME) into a force update mode. This jumper can be used should the Intel ME firmware fail to operate due to some type of firmware corruption. Placing the Intel ME into a recovery mode disables the Intel ME operation allowing the firmware to be updated.

## 15. Server Board Installation and Component Replacement

---

This chapter 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 chapter 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 that 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.

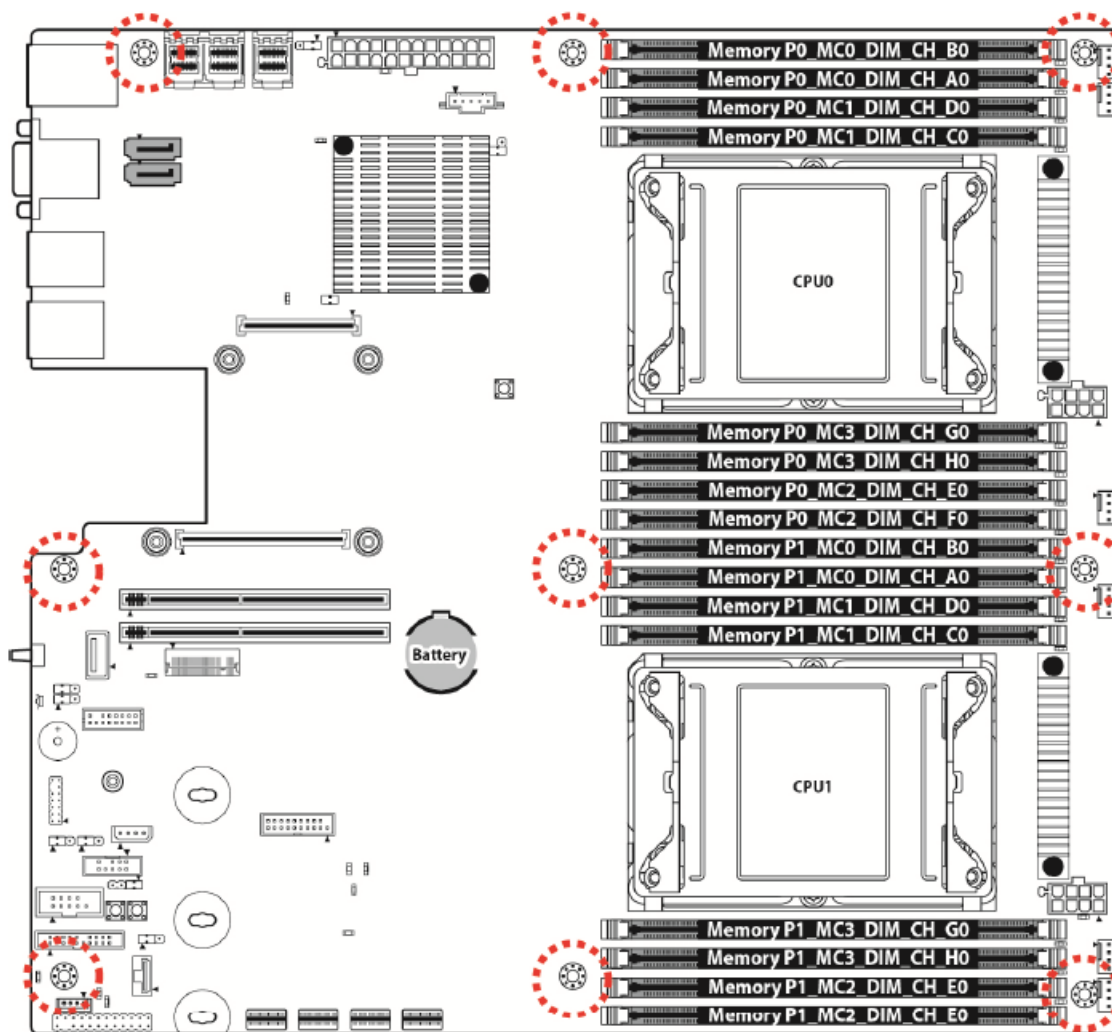


Intel recommends that the following steps be taken when performing any procedures described within this document or while performing service to any computer system.

- 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

## 15.1 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.



**Figure 55. Server Board Mounting Hole Locations**

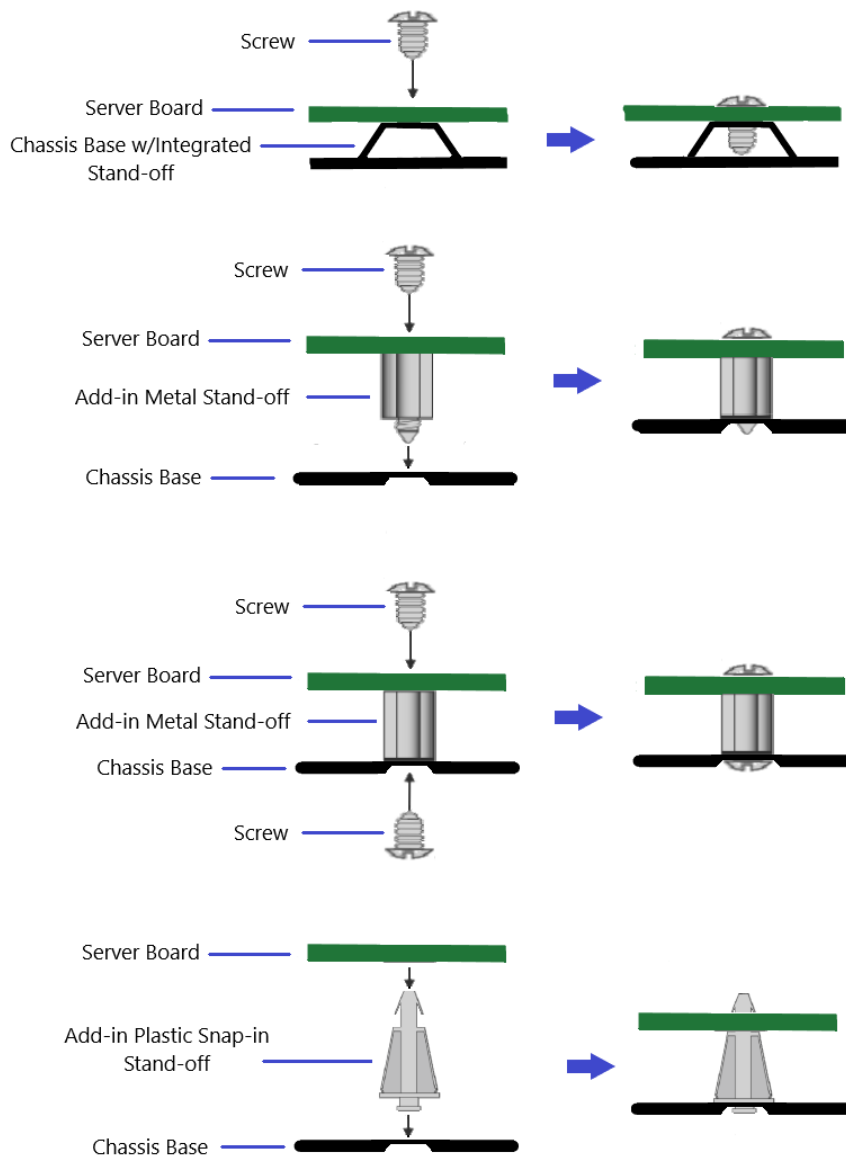
This server board generally conforms to the industry standard extended ATX (EATX) form factor, except that its architecture and feature set were developed to be supported by a rack mount 1U server chassis. This form factor should be considered when selecting a server chassis to mount the server board into.

Server boards and server chassis' that conform to the EATX form factor will share compatible mounting features that match the server board mounting holes to fastener locations on the chassis base plate.

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.





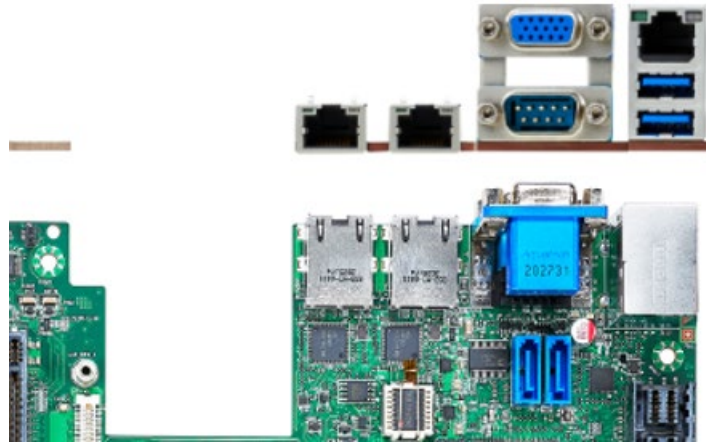
**Figure 56. Possible Server Board Mounting Options**

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 36. Server Board Mounting Screw Torque Requirements**

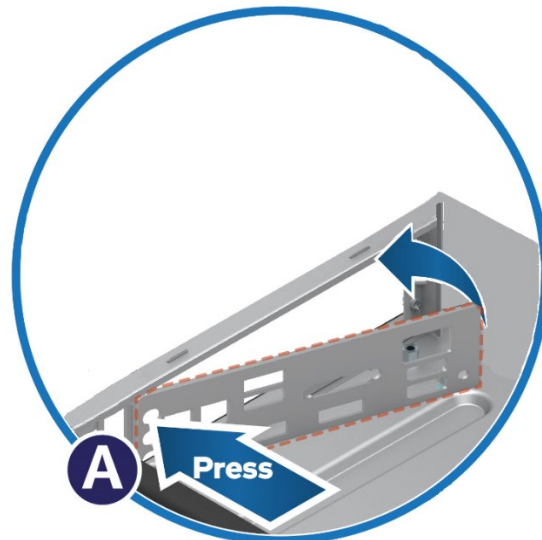
Screw Size	Torque Value	Tolerance $\pm$
6-32	8 in-lb.	1
M3	5 in-lb.	1

The chosen chassis may or may not have a back panel with matching I/O port cut-outs to accommodate the rear I/O connectors found on the back edge of the server board.



**Figure 57. Server Board Rear I/O Connectors**

Most extended ATX server chassis include a standard sized cut-out on the back panel that allows for an I/O shield to be installed. As shipped by Intel, the server board will include an optional rear I/O shield with matching connector cut-outs that snap into the back-panel cut-out of the chassis. Should the I/O shield be necessary, it must be installed into the chassis before the installation of the server board.



**Figure 58. Rear I/O Shield Placement**

## 15.2 Processor Replacement Instructions

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 server board can support 1U (low-profile) or 2U processor heat sinks. Illustrations used in the following instructions show a 2U processor heat sink. The instructions can be applied to either type.

---

**Note:** These instructions assume the processor heat sinks match those that ship with Intel server systems. If the heat sinks being used appear different than those illustrated, then Intel recommends following the processor replacement procedures included within documentation supplied with the chosen non-Intel server system.

---

### Components Required:

- New matching 3<sup>rd</sup> Gen Intel Xeon processor 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, an ESD safe workbench, and other anti-ESD precautions (recommended)
- ESD Gloves (recommended)
- T-30 Torx\* screwdriver

**Average Time to Complete:** ~10+ minutes

### Procedure Prerequisites

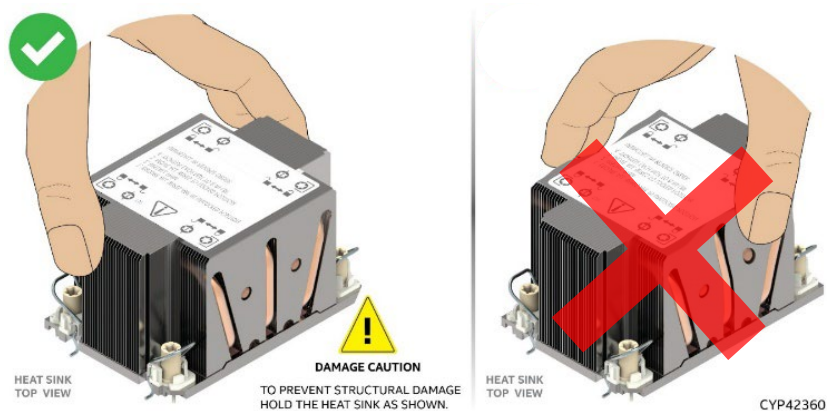
- The system must be powered off for at least 5 minutes allowing the heatsinks to cool.
- AC Power cord(s) must be disconnected from the system

---

**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 image for proper handling.

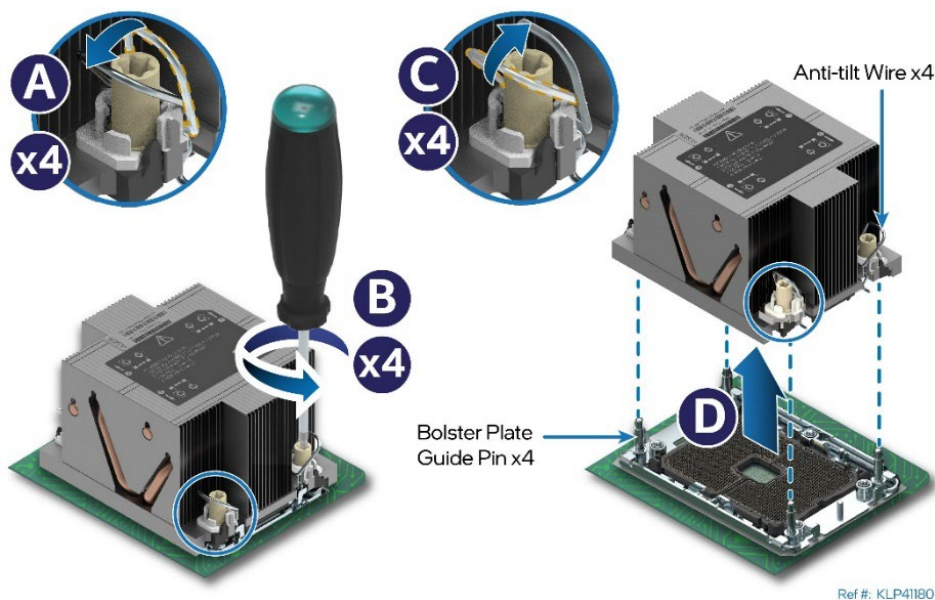
---



**Figure 59. Processor Heat Sink Handling**

## 15.2.1 Processor Heat Sink Module (PHM) Removal

1. Identify and locate the faulty processor.

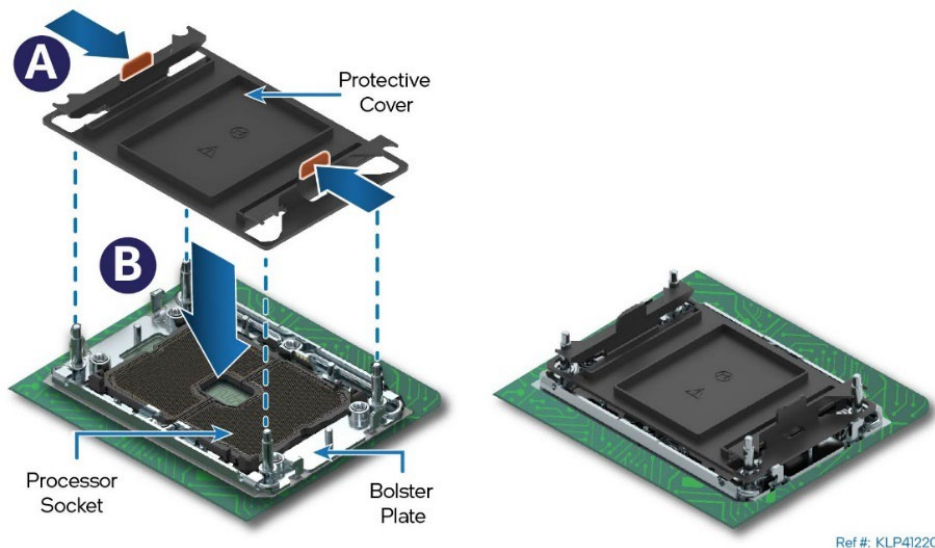


**Figure 60. PHM Assembly Removal from Processor Socket**

2. Ensure the anti-tilt wires located over each of the four heat sink fasteners are in the outward position (see Letter A).
3. Fully loosen all four heat sink fasteners in the following order – 4, 3, 2, 1 (see Letter B).
  - Reference the label atop of the heat sink for fastener numbering
4. Set all four anti-tilt wires 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. Turn over the PHM. 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.

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

If not replacing the processor, install the original plastic socket cover over the processor socket.

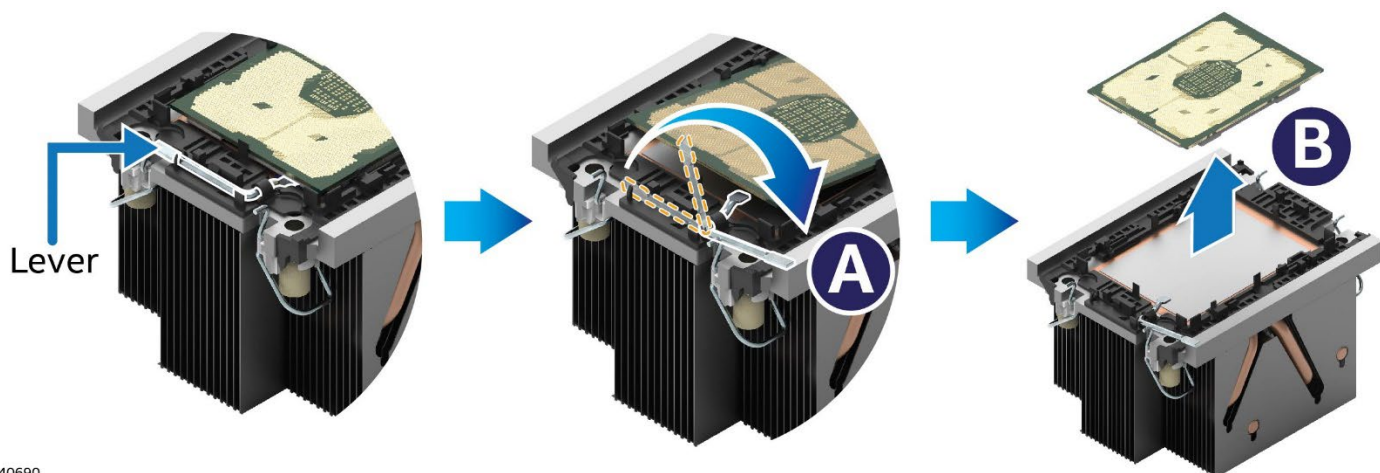


**Figure 61. Processor Socket Cover Installation**

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

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

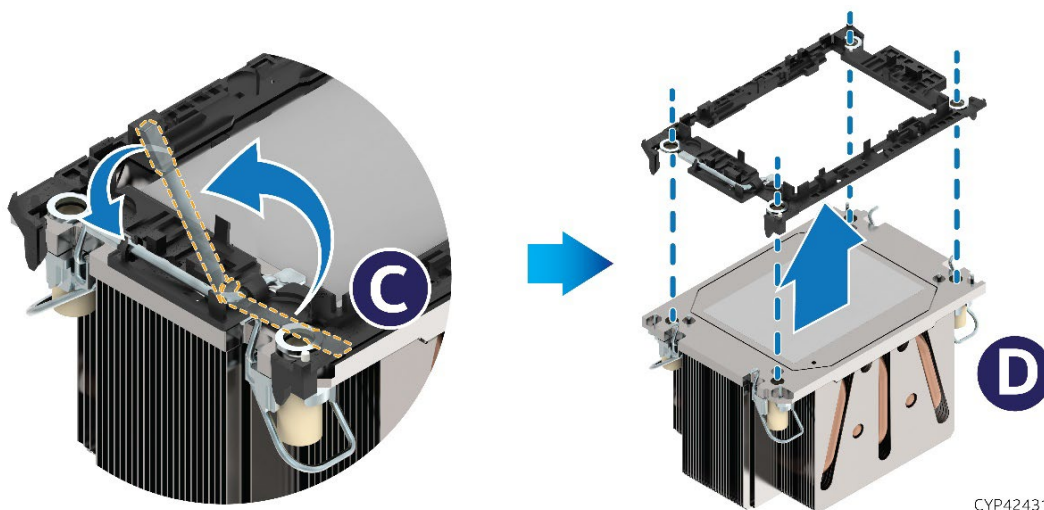
## 15.2.2 PHM Disassembly



KLP40690

**Figure 62. Processor Removal from PHM Assembly**

1. While holding down the PHM, rotate the processor release lever (see Letter A) until the processor lifts free from the processor carrier clip.
2. Holding down the processor carrier clip, carefully lift out the processor (see Letter B).



CYP42431

**Figure 63. 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).



### 15.2.3 PHM Reassembly

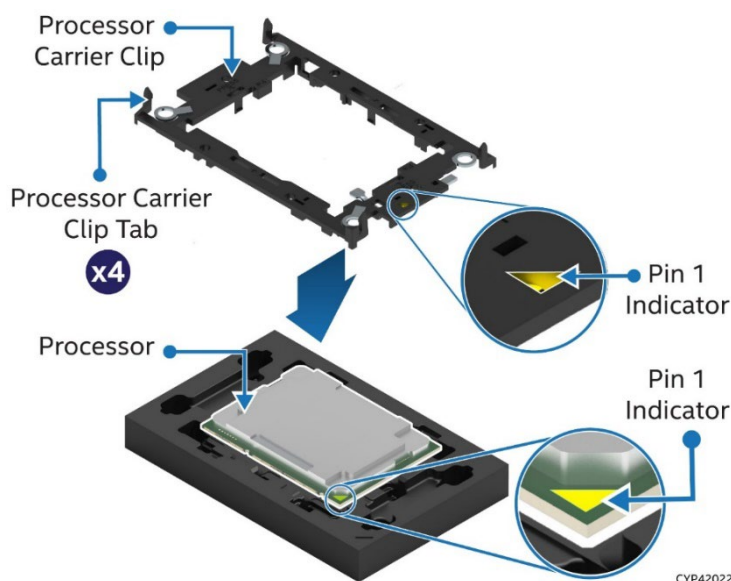
To properly assemble the PHM and install it onto the server board, the procedures described in the following sections must be followed in the order specified. These instructions assume that the processor heat sink (New or reuse of existing) has the necessary Thermal Interface Material (TIM) (DOWSIL\* TC-5888) already applied.

---

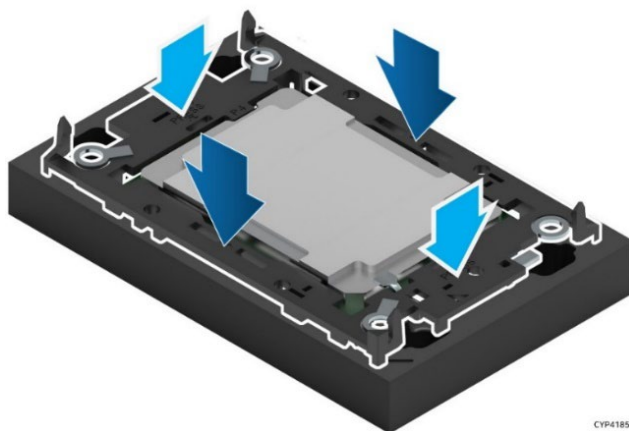
**Note:** Full ESD precautions should be followed to perform reassembly of the PHM and reinstallation of the PHM to the server board. At no time should the processor itself be handled.

---

Each component within the PHM assembly includes a Pin 1 indicator. Pin 1 indicator alignment between all components is required throughout the assembly process.



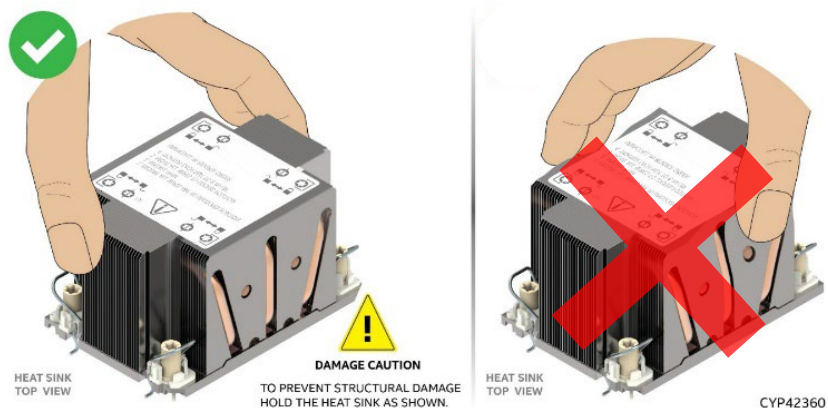
**Figure 64. Installing Processor Carrier Clip onto Processor – Part 1**



**Figure 65. 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 that 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 in [Figure 66](#).



**Figure 66. 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 (DOWSIL\* TC-5888).

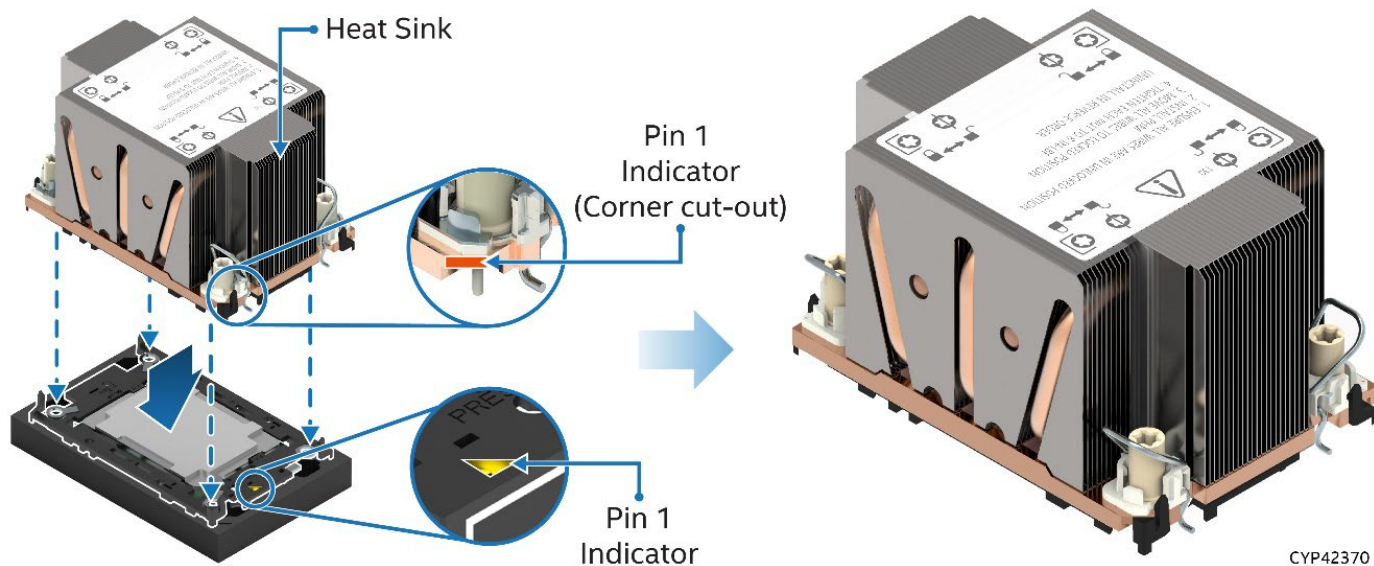
If using a new heat sink

- Remove the plastic protective film (if present) from the Thermal Interface Material (TIM).



**Figure 67. 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 68. 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 that all four heat sink corners are securely latched to the carrier clip tabs.

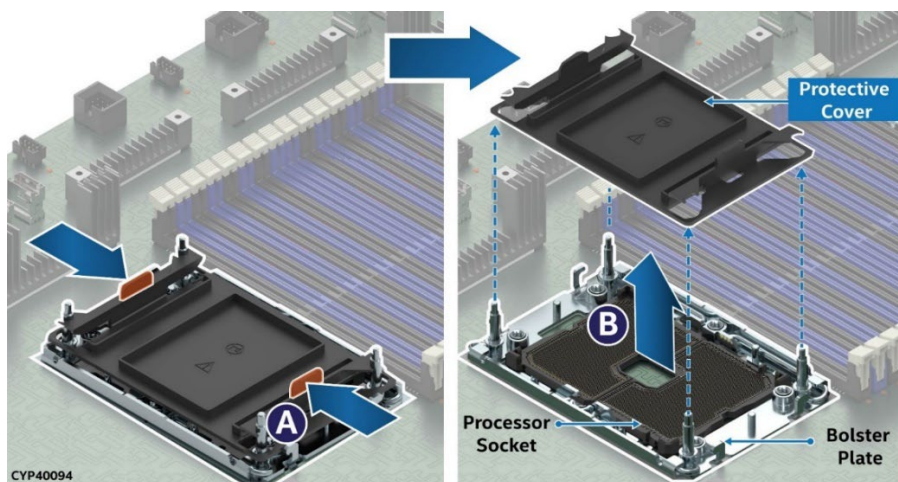
#### 15.2.4 PHM Installation

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. Damaged socket pins may produce unpredictable system errors.

---



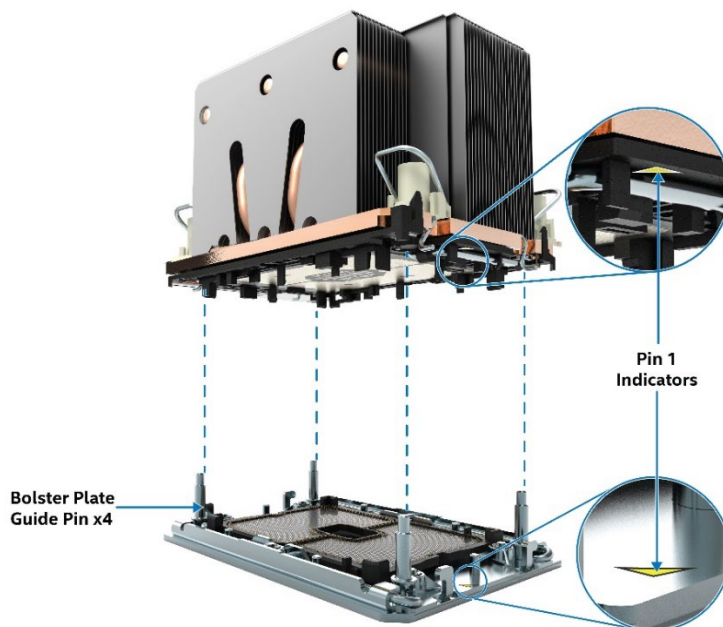
**Figure 69. Processor Socket Cover Removal**

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

---

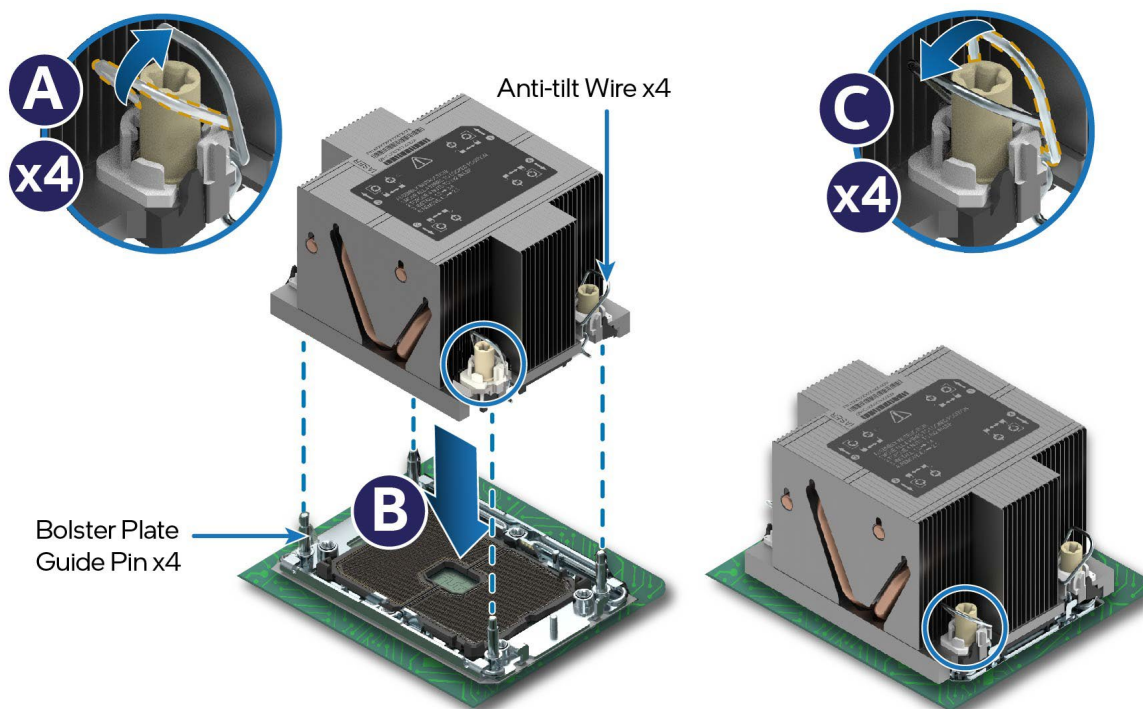
**Caution:** If debris is observed, blow it away gently. Do not remove it manually, such as with tweezers.

---



CYP42381  
**Figure 70. PHM Alignment with Processor 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.



Ref #: KLP41190

**Figure 71. PHM Installation onto Server Board**

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





**Figure 72. Tighten Heat Sink Fasteners**

- Using a T30 Torx\* screwdriver, tighten (in order 1,2,3,4) the heat sink fasteners to 8 in-lb.

## 15.3 DIMM Replacement Instructions

### Required Tools and Supplies

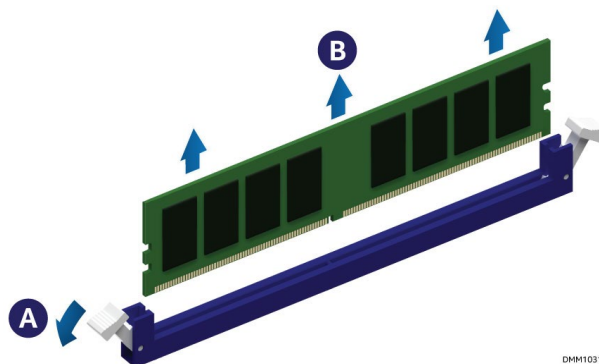
- Anti-static wrist strap and conductive workbench pad (recommended)
- Replacement equivalent memory module

**Average Time to Complete:** ~ 5 minutes

### Procedure Prerequisites

- Memory modules are NOT hot-swappable. The system must be powered down and unplugged from the AC power source before replacing a faulty memory module from the system.

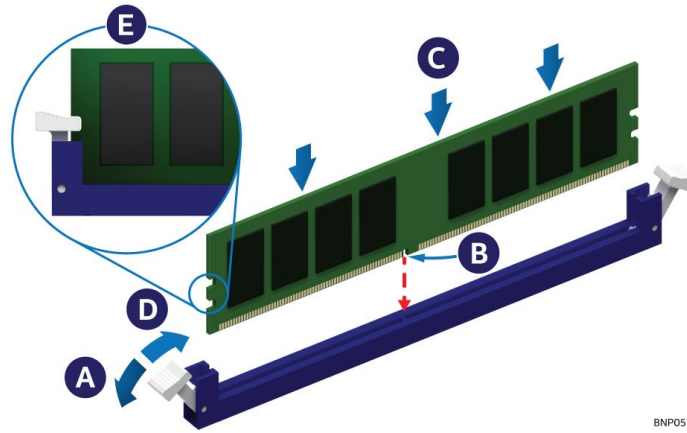
For the following procedure, Standard DDR4 DIMMs are commonly referred to as “Memory Module”.



**Figure 73. Memory Module Removal**

- Identify and locate the faulty memory module.
- Ensure that the ejection tabs of adjacent memory slots are fully closed.
- Open the ejection tabs at both ends of the selected memory slot (see Letter A). The memory module will lift out from the memory slot.
- Holding the memory module by its edges, lift it away from the slot (see Letter B).





**Figure 74. DIMM Installation**

5. Ensure that the ejector 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.
  - Using even pressure along the top edge, push down on the memory module (see Letter C) until the ejector tabs of the memory slot snap into place (see Letter D).
9. Ensure that the ejector tabs are firmly in place (see Letter E).

## Appendix A. Getting Help


Available Intel support options with your Intel Server System:

- 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	<p style="text-align: center;"><b>Download Center</b></p>  <p style="text-align: center;"><a href="http://www.intel.com/support/downloadserversw">http://www.intel.com/support/downloadserversw</a></p>	<p style="text-align: center;"><b>BIOS Support Page</b></p>  <p style="text-align: center;"><a href="http://www.intel.com/support/serverbios">http://www.intel.com/support/serverbios</a></p>	<p style="text-align: center;"><b>Troubleshooting Boot Issue</b></p>  <p style="text-align: center;"><a href="http://www.intel.com/support/tsboot">http://www.intel.com/support/tsboot</a></p>
<p>Use the following links for support on Intel® Data Center Block (DCB) Integrated Systems*</p> <p>* Intel DCB comes pre-populated with processors, memory, storage, and peripherals based on how it was ordered through the Intel Configure to Order tool.</p>	<p style="text-align: center;"><b>Download Center</b></p>  <p style="text-align: center;"><a href="http://www.intel.com/support/downloadddcbw">http://www.intel.com/support/downloadddcbw</a></p>	<p style="text-align: center;"><b>Technical Support Documents</b></p>  <p style="text-align: center;"><a href="http://www.intel.com/support/dcb">http://www.intel.com/support/dcb</a></p>	<p style="text-align: center;"><b>Warranty and Support Info</b></p>  <p style="text-align: center;"><a href="http://www.intel.com/support/dcbwarranty">http://www.intel.com/support/dcbwarranty</a></p>

- 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)
- 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](http://www.intel.com/p/en_US/support/warranty).

## Appendix B. Integration and Usage Tips

This appendix provides a list of useful information that is unique to the Intel Server Board M20NTB2SB and should be kept in mind while configuring your server system.

- When adding or removing components or peripherals from the server board, power cords must be disconnected from the server. With power cords connected to the server, standby voltages are still present even though the server board is powered off.
- The server board supports the 3<sup>rd</sup> Gen Intel® Xeon® Scalable processor family with a Thermal Design Power (TDP) of 250 Watts or less. Previous generations of the Intel® Xeon® processor and Intel® Xeon® Scalable processor families are not supported. Server systems using this server board may or may not meet the TDP design limits of the server board. Validate the TDP limits of the server system before selecting a processor.
- Processors must be installed in order. CPU 0 must be populated for the server board to operate.
- Riser Card Slot #2 on the server board can only be used in dual processor configurations.
- The riser card slots are specifically designed to support riser cards only. Attempting to install a PCIe add-in card directly into a riser card slot on the server board may damage the server board, the add-in card, or both.
- For the best performance, the number of DDR4 DIMMs installed should be balanced across both processor sockets and memory channels.
- RAID partitions created using Intel VROC for SATA cannot span across the two embedded SATA controllers. Only drives attached to a common SATA controller can be included in a RAID partition.
- Make sure that the latest system software is loaded on the server. This includes system BIOS and BMC firmware. The latest system software can be downloaded from <http://downloadcenter.intel.com>.

## Appendix C. 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.

### Checkpoint Ranges

Status Code Range	Description
0x01 – 0x0B	SEC execution
0x0C – 0x0F	SEC errors
0x10 – 0x2F	PEI execution up to and including memory detection
0x30 – 0x4F	PEI execution after memory detection
0x50 – 0x5F	PEI errors
0x60 – 0x8F	DXE execution up to BDS
0x90 – 0xCF	BDS execution
0xD0 – 0xDF	DXE errors
0xE0 – 0xE8	S3 Resume (PEI)
0xE9 – 0xEF	S3 Resume errors (PEI)
0xF0 – 0xF8	Recovery (PEI)
0xF9 – 0xFF	Recovery errors (PEI)

### Standard Checkpoints

#### Security (SEC) Phase

Status Code	Description
0x00	Not used
<b>Progress Codes</b>	
0x01	Power on. Reset type detection (soft/hard).
0x02	AP initialization before microcode loading
0x03	Northbridge initialization before microcode loading
0x04	Southbridge initialization before microcode loading
0x05	OEM initialization before microcode loading
0x06	Microcode loading
0x07	AP initialization after microcode loading
0x08	Northbridge initialization after microcode loading
0x09	Southbridge initialization after microcode loading
0x0A	OEM initialization after microcode loading
0x0B	Cache initialization
<b>SEC Error Codes</b>	
0x0C – 0x0D	Reserved for future AMI SEC error codes
0x0E	Microcode not found
0x0F	Microcode not found

#### SEC Beep Codes

- None

## Pre-EFI Initialization (PEI) Phase

Status Code	Description
<b>Progress Codes</b>	
0x10	PEI Core is started
0x11	Pre-memory CPU initialization is started
0x12	Pre-memory CPU initialization (CPU module specific)
0x13	Pre-memory CPU initialization (CPU module specific)
0x14	Pre-memory CPU initialization (CPU module specific)
0x15	Pre-memory northbridge initialization is started
0x16	Pre-Memory northbridge initialization (northbridge module specific)
0x17	Pre-memory northbridge initialization (northbridge module specific)
0x18	Pre-Memory northbridge initialization (northbridge module specific)
0x19	Pre-memory southbridge initialization is started
0x1A	Pre-Memory southbridge initialization (southbridge module specific)
0x1B	Pre-memory southbridge initialization (southbridge module specific)
0x1C	Pre-Memory southbridge initialization (southbridge module specific)
0x1D – 0x2A	OEM pre-memory initialization codes
0x2B	Memory initialization. Serial Presence Detect (SPD) data reading
0x2C	Memory initialization. Memory presence detection
0x2D	Memory initialization. Programming memory timing information
0x2E	Memory initialization. Configuring memory
0x2F	Memory initialization (other)
0x30	Reserved for ASL (see <a href="#">ACPI/ASL Checkpoints</a> )
0x31	Memory Installed
0x32	CPU post-memory initialization is started
0x33	CPU post-memory initialization. Cache initialization
0x34	CPU post-memory initialization. Application Processor(s) (AP) initialization
0x35	CPU post-memory initialization. Bootstrap processor (BSP) selection
0x36	CPU post-memory initialization. System Management Mode(SMM) initialization
0x37	Post-Memory northbridge initialization is started
0x38	Post-Memory northbridge initialization (northbridge module specific)
0x39	Post-Memory northbridge initialization (northbridge module specific)
0x3A	Post-Memory northbridge initialization (northbridge module specific)
0x3B	Post-Memory southbridge initialization is started
0x3C	Post-Memory southbridge initialization (southbridge module specific)
0x3D	Post-Memory southbridge initialization (southbridge module specific)
0x3E	Post-Memory southbridge initialization (southbridge module specific)
0x3F – 0x4E	OEM post memory initialization codes
0x4F	DXE IPL is started
<b>PEI Error Codes</b>	
0x50	Memory initialization error. Invalid memory type or incompatible memory speed
0x51	Memory initialization error. SPD reading has failed
0x52	Memory initialization error. Invalid memory size or memory modules do not match
0x53	Memory initialization error. No usable memory detected
0x54	Unspecified memory initialization error
0x55	Memory not installed
0x56	Invalid CPU type or speed
0x57	CPU mismatch
0x58	CPU self-test failed or possible CPU cache error
0x59	CPU microcode is not found or microcode update is failed
0x5A	Internal CPU error
0x5B	Reset PPI is not available
0x5C – 0x5F	Reserved for future AMI error codes



Status Code	Description
<b>S3 Resume Progress Codes</b>	
0xE0	S3 Resume is started (S3 Resume PPI is called by the DXE IPL)
0xE1	S3 Boot Script execution
0xE2	Video repost
0xE3	OS S3 wake vector call
0xE4 – 0xE7	Reserved for future AMI progress codes
<b>S3 Resume Error Codes</b>	
0xE8	S3 Resume Failed
0xE9	S3 Resume PPI not Found
0xEA	S3 Resume Boot Script Error
0xEB	S3 OS Wake Error
0xEC – 0xEF	Reserved for future AMI error codes
<b>Recovery Progress Codes</b>	
0xF0	Recovery condition triggered by firmware (Auto recovery)
0xF1	Recovery condition triggered by user (Forced recovery)
0xF2	Recovery process started
0xF3	Recovery firmware image is found
0xF4	Recovery firmware image is loaded
0xF5 – 0xF7	Reserved for future AMI progress codes
<b>Recovery Error Codes</b>	
0xF8	Recovery PPI is not available
0xF9	Recovery capsule is not found
0xFA	Invalid recovery capsule
0xFB – 0xFF	Reserved for future AMI error codes

## Driver Execution Environment (DXE) Phase

Status Code	Description
0x60	DXE Core is started
0x61	NVRAM initialization
0x62	Installation of the southbridge Runtime Services
0x63	CPU DXE initialization is started
0x64	CPU DXE initialization (CPU module specific)
0x65	CPU DXE initialization (CPU module specific)
0x66	CPU DXE initialization (CPU module specific)
0x67	CPU DXE initialization (CPU module specific)
0x68	PCI host bridge initialization
0x69	Northbridge DXE initialization is started
0x6A	Northbridge DXE SMM initialization is started
0x6B	Northbridge DXE initialization (northbridge module specific)
0x6C	Northbridge DXE initialization (northbridge module specific)
0x6D	Northbridge DXE initialization (northbridge module specific)
0x6E	Northbridge DXE initialization (northbridge module specific)
0x6F	Northbridge DXE initialization (northbridge module specific)
0x70	Southbridge DXE initialization is started
0x71	Southbridge DXE SMM initialization is started
0x72	Southbridge devices initialization
0x73	Southbridge DXE initialization (southbridge module specific)
0x74	Southbridge DXE initialization (southbridge module specific)
0x75	Southbridge DXE initialization (southbridge module specific)
0x76	Southbridge DXE initialization (southbridge module specific)
0x77	Southbridge DXE initialization (southbridge module specific)
0x78	ACPI module initialization
0x79	CSM initialization
0x7A – 0x7F	Reserved for future AMI DXE codes
0x80 – 0x8F	OEM DXE initialization codes
0x90	Boot Device Selection (BDS) phase is started
0x91	Driver connecting is started
0x92	PCI Bus initialization is started
0x93	PCI Bus Hot Plug Controller initialization
0x94	PCI Bus Enumeration
0x95	PCI BUS Request Resources
0x96	PCI Bus Assign Resources
0x97	Console Output devices connect
0x98	Console Input devices connect
0x99	Super IO initialization
0x9A	USB initialization is started
0x9B	USB Reset
0x9C	USB Detect
0x9D	USB Enable
0x9E – 0x9F	Reserved for future AMI codes
0xA0	IDE initialization is started
0xA1	IDE Reset
0xA2	IDE Detect
0xA3	IDE Enable
0xA4	SCSI initialization is started
0xA5	SCSI Reset
0xA6	SCSI Detect
0xA7	SCSI Enable
0xA8	Setup Verifying Password

Status Code	Description
0xA9	Start of Setup
0xAA	Reserved for ASL (see <a href="#">ACPI/ASL Checkpoints</a> )
0xAB	Setup Input Wait
0xAC	Reserved for ASL (see <a href="#">ACPI/ASL Checkpoints</a> )
0xAD	Ready To Boot event
0xAE	Legacy Boot event
0xAF	Exit Boot Services event
0xB0	Runtime Set Virtual Address MAP Begin
0xB1	Runtime Set Virtual Address MAP End
0xB2	Legacy Option ROM initialization
0xB3	System Reset
0xB4	USB hot plug
0xB5	PCI bus hot plug
0xB6	Clean-up of NVRAM
0xB7	Configuration Reset (reset of NVRAM settings)
0xB8 – 0xBF	Reserved for future AML codes
0xC0 – 0xCF	OEM BDS initialization codes
<b>DXE Error Codes</b>	
0xD0	CPU initialization error
0xD1	Northbridge initialization error
0xD2	Southbridge initialization error
0xD3	Some of the Architectural Protocols are not available
0xD4	PCI resource allocation error. Out of Resources
0xD5	No Space for Legacy Option ROM
0xD6	No Console Output Devices are found
0xD7	No Console Input Devices are found
0xD8	Invalid password
0xD9	Error loading Boot Option (LoadImage returned error)
0xDA	Boot Option is failed (StartImage returned error)
0xDB	Flash update is failed
0xDC	Reset protocol is not available

## ACPI/ASL Checkpoints

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

## Appendix D. Statement of Volatility

The tables in this section are used to identify the volatile and non-volatile memory components of the Intel Server Board M20NTP2SB.

The tables provide the following data for each identified component.

- **Component Type:** Three types of components are on the server board assembly:
  - **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 but 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:** Size of each component in bits, kilobits (Kb), megabits (Mb), bytes, kilobytes (KB), or megabytes (MB).
- **Board Location:** Board location is the physical location of each component corresponding to information on the server board silkscreen.
- **User Data:** The flash components on the server board 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 the following:

- **BIOS:** The server board 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 server board supports 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. The BMC does not have access to operating system level data.

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

The Intel Server Board M20NTP2SB includes several components that can be used to store data. A list of these components is included in the following table.

**Table 37. Server Board Components the Store Volatile/Non-Volatile Data**

Component	Size	Board location	User Data	Name
Non-Volatile	32 MB	BIOS_SPI1	Yes	BIOS Flash
Non-Volatile	64 MB	BMC_SPI1	Yes	BMC FW
Non-Volatile	4 MB	U396, U398	No	Lan1 & LAN 2 EEPROM Flash
Volatile	4 Gb	BMC_MEM1	No	BMC Firmware SDRAM

## Appendix E. Regulatory Information

This product has been evaluated and certified as Information Technology Equipment (ITE), which may be installed in offices, schools, computer rooms, and similar commercial type locations. The suitability of this product for other product 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 **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.

**Note:** 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.

Regulatory Certification	Intel® Server Board M20NTP2SB Family	Notes
	"North Pass"	Intel Project Code Name
	L3 Board Only	Product integration level
	M20NTP	Product family identified on certification
Australia & New Zealand ACMA DoC	✓	
Canada ICES – 003 Certification	✓	
CB Certification & Report (International – report to include all CB country national deviations)	✓	
China CCC certification	○	
CU Certification & DoC (Russia/Belarus/Kazakhstan)	○	
Europe CE DoC	✓	
FCC Part 15 Emissions Verification (USA)	✓	
Germany GS Certification	○	
India BIS Certification	○	
International Compliance – CISPR32 & CISPR35	✓	
Japan VCCI Certification	○	
Korea KC Certification	✓	
Mexico NOM Certification	○	
NRTL Certification (USA & Canada)	✓	
South Africa Certification	○	
Taiwan BSMI Certification & DoC	✓	
United Kingdom UKCA DoC	✓	
Ukraine Certification	○	

### Table Key

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



## 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), will go 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 **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.**

---

**Note:** 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.

---

Visit the following website for additional EU Directive 2019/424 (Lot 9) 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 in these documents:

- **Service Instructions**  
Server board only – See [Chapter 15](#)  
1U Server System – *Intel® Server System M20NTP1UR Family System Integration and Service Guide*
- **Product Specifications**  
Server board only – This document  
1U Server System – Intel® Server System M20NTP1UR Family Technical Product Specification (TPS)
- **BIOS/Firmware and Security Updates – Intel® Server Board M20NTP2SB**
  - System Update Package (SUP) – UEFI only. Available for download at:  
<http://downloadcenter.intel.com>

## Appendix F. Glossary

Term	Definition
<b>ACPI</b>	Advanced Configuration and Power Interface
<b>ARP</b>	Address Resolution Protocol
<b>ASHRAE</b>	American Society of Heating, Refrigerating, and Air-Conditioning Engineers
<b>AVB</b>	Audio-Video Bridging
<b>BBS</b>	BIOS Boot Selection
<b>BMC</b>	Baseboard Management Controller
<b>BIOS</b>	Basic Input/Output System
<b>CFM</b>	Cubic Feet per Minute
<b>CLI</b>	Command-line interface
<b>CLST</b>	Closed Loop System Throttling
<b>CMOS</b>	Complementary Metal-oxide-semiconductor
<b>CPU</b>	Central Processing Unit
<b>DDR4</b>	Double Data Rate 4
<b>DHCP</b>	Dynamic Host Configuration Protocol
<b>DIMM</b>	Dual In-line Memory Module
<b>DPC</b>	DIMMs per Channel
<b>DR</b>	Dual Rank
<b>EATX</b>	Extended Advanced Technology eXtended
<b>EDS</b>	External Design Specification
<b>EFI</b>	Extensible Firmware Interface
<b>FP</b>	Front Panel
<b>FRB</b>	Fault Resilient Boot
<b>FRU</b>	Field Replaceable Unit
<b>GPGPU</b>	General Purpose Graphic Processing Unit
<b>GPIO</b>	General Purpose Input/Output
<b>GUI</b>	Graphical User Interface
<b>I<sup>2</sup>C</b>	Inter-integrated Circuit bus
<b>IMC</b>	Integrated Memory Controller
<b>IIO</b>	Integrated Input/Output
<b>iPC</b>	Intel Product Code
<b>IPMI</b>	Intelligent Platform Management Interface
<b>LED</b>	Light Emitting Diode
<b>LFM</b>	Linear Feet per Minute – Airflow measurement
<b>LPC</b>	Low-pin Count
<b>LRDIMM</b>	Load Reduced DIMM
<b>LSB</b>	Least Significant Bit
<b>MSB</b>	Most Significant Bit
<b>MKTME</b>	Multi-key Total Memory Encryption
<b>MLE</b>	Measured Launched Environment
<b>MM</b>	Memory Mode
<b>MRC</b>	Memory Reference Code
<b>MTBF</b>	Mean Time Between Failure
<b>NAT</b>	Network Address Translation
<b>NIC</b>	Network Interface Controller

Term	Definition
<b>NMI</b>	Non-maskable Interrupt
<b>NTB</b>	Non-Transparent Bridge
<b>OEM</b>	Original Equipment Manufacturer
<b>OCP*</b>	Open Compute Project*
<b>OR</b>	Oct Rank
<b>OTP</b>	Over Temperature Protection
<b>OVP</b>	Over-voltage Protection
<b>PCH</b>	Peripheral Controller Hub
<b>PCI</b>	Peripheral Component Interconnect
<b>PCB</b>	Printed Circuit Board
<b>PCIe*</b>	Peripheral Component Interconnect Express*
<b>PECI</b>	Platform Environment Control Interface
<b>PFC</b>	Power Factor Correction
<b>PHM</b>	Processor Heat sink Module
<b>PMBus</b>	Power Management Bus
<b>PMem</b>	Persistent Memory Module
<b>POST</b>	Power-on self-test
<b>PSMI</b>	Power Supply Management Interface
<b>PSU</b>	Power Supply Unit
<b>PWM</b>	Pulse Width Modulation
<b>QR</b>	Quad (8) Rank
<b>RAID</b>	Redundant Array of Independent Disks
<b>RAM</b>	Random Access Memory
<b>RAS</b>	Reliability, Availability, and Serviceability
<b>RCiEP</b>	Root Complex Integrated Endpoint
<b>RDIMM</b>	Registered DIMM
<b>RMCP</b>	Remote Management Control Protocol
<b>ROC</b>	RAID On Chip
<b>SAS*</b>	Serial Attached SCSI
<b>SATA</b>	Serial Advanced Technology Attachment
<b>SEL</b>	System Event Log
<b>SCA</b>	Single Connector Attachment
<b>SCSI</b>	Small Computer System Interface
<b>SDR</b>	Sensor Data Record
<b>SFF</b>	Small Form Factor
<b>SFP</b>	Small Form-factor Pluggable
<b>SFUP</b>	System Firmware Update Package
<b>SMBus</b>	System Management Bus
<b>SMTP</b>	Simple Mail Transfer Protocol
<b>SNMP</b>	Simple Network Management Protocol
<b>SOL</b>	Serial-over-LAN
<b>SR</b>	Single Rank
<b>SSD</b>	Solid State Device
<b>TCG</b>	Trusted Computing Group
<b>TDP</b>	Thermal Design Power
<b>TPM</b>	Trusted Platform Module

## Intel® Server Board M20NTP2SB Technical Product Specification

Term	Definition
<b>TPS</b>	Technical Product Specification
<b>Intel® TXT</b>	Intel Trusted Execution Technology
<b>Intel® VMD</b>	Intel Volume Management Device
<b>UEFI</b>	Unified Extensible Firmware Interface
<b>Intel® UPI</b>	Intel Ultra Path Interconnect
<b>VLSI</b>	Very Large Scale Integration
<b>VSB</b>	Voltage Standby
<b>Intel® VROC</b>	Intel Virtual RAID on CPU
<b>Intel® VT-d</b>	Intel Virtualization Technology for Directed I/O
<b>Intel® VT-x</b>	Intel Virtualization Technology for IA-32, Intel® 64 and Intel® Architecture