BIOS Release Notes Form

Supermicro 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. All products, computer systems, dates, and figures specified are preliminary based on current expectations, and are subject to change without notice. Supermicro and the Supermicro logo are trademarks of Super Micro Computer, Inc. in the U.S. and/or other countries. Copyright © 2018 Super Micro Computer, Inc. All rights reserved.

Product Name	**X14DBT-B**
Release Version	**1.2**
Release Date	**01/24/2025**
Previous Version	**1.0b**
Update Category	**Recommended**
Dependencies	**None**
Important Notes	**None**
Enhancements	**1. Updated the code base to 5.35_0ACQZ_3544P15_GNRAP_GNRSP_069 GNR PV.** **2. Added SMC_ONLY_LOG_CORRECTED_MCE_WITH_YELLOW_STATUS support.** **3. Fixed how the DNS IP would show up incorrectly when setting the DNS IP on the web.** **4. Enabled 'Latency Optimized Mode' for workload profiles (HPC, Virtualization) and ENERGY_PERF_BIAS_CFG modes (Maximum, Extreme Performance).** **5. Configured "Thread Enabled" in SBMIOS type 4.** **6. Implemented the TPM Redfish MeasurementSet feature.** **7. Updated code base to 5.35_0ACQZ_3544P15_GNRAP_GNRSP_068 GNR PC+3, SRF PLR1.** **8. Fixed the system hang with the KioXia NVMe driver. Integrated EIF812015 solution.** **9. Updated the IMC/CHANNEL/DIMM number to fit BirchStream spec and SMBIOS Type17 update method.** **10. Enabled "Adv MemTest Reset Failure Tracking List" as the default.**

	11. Added enhancements for INTEL-SA-00390 Security Advisory to address CVE-2020-8738,CVE-2020-8739,CVE-2020-8740,CVE-2020-8764 security issues. 12. After TC 4113 - Multiple - TpmManage failed, fixed it with a SAA ECO SMSTC test. 13. Fixed the failed TXT test with GNR QS CPU. 14. Added the mechanism to reset MMIO of MMBI when time out occurs. 15. Enhanced Microcode_support module to refer to Microcode2_support. 16. Updated smbios type 17 Memory Technology for MRDIMM (SMBIOS 3.8). 17. Fixed how some setup items would change to unexpected settings when using the ipmitool to change boot order and if the system had an additional reset during the change boot order process. 18. Exposed "Secure Boot Mode" setup item to SAA. 19. Supported Rocky and Alma Linux. 20. Disabled SMBIOS type 18 memory error info display. 21. Supported multi-layer USB device boot options. 22. Detected IIO port link status even in VMD mode. 23. Updated the SmcOob module to SMCOOBV2.01.06 to enhance the previously hidden items when it is exposed in the page.
New features	**None**
Fixes	1. Fixed the dependency issues with 'Hardware P-States' and Maximum Performance. 2. Fixed the dependency issues with 'Intel SST-PP', 'Dynamic SST-PP', and 'SST-BF' settings and workload profiles. 3. Fixed the HttpBootCheckSpaceToDeleteAllHttp problem. 4. Fixed the BMC IPV6 setup items that wouldn’t work. 5. Resolved the issue where the system would hang when restoring the Secure Boot keys. 6. Fixed the processor configuration error where SEL would use the incorrect type by injecting IERR via Cscript. 7. Fixed how there was no mapped out SEL after injecting memory UECC.

	8. Fixed the POST hang 0xB9 where the Enhanced PPR would be set to Persistent and the keyboard reset on the shell. **9. Fixed the problem where firmware protection and memory integrity could not enable simultaneously. (AMI EIP #800598)** **10. Fixed the issue where the HTTPs boot TLS certificate via BMC Redfish API would fail to delete.** **11. Runtime updated the smbios date to ROMHOLE.** **12. Fixed how the system would hang when installing a SAS3916 card.**

Release Notes from Previous Release(s)

1.0b (09/25/2024)

1. *Corrected SCC-P2NM2G5-B1 and SCC-A2NM2241GH-B1 M.2 type 9 information.*

1.0a (07/09/2024)

1. *Updated code base to 5.35_0ACQZ_3218D03_SRFAP_55_BETA for WW25 BKC.*
2. *Updated Intel Giga LAN uEFI driver to BootUtil 29.1.*
3. *Updated AST2600 VGA uEFI driver to 1.13.04.*
4. *Changed PCI_DO_NOT_RESET_VC_MAPPING to enable.*
5. *[SmcVPD] Patch for Mellanox InfiniBand Controller MAC Address issue.*
6. *Filled DUID with UUID to avoid making all systems' DUID in IPv6 DHCP the same.*
7. *Assigned unique display name for "Security Function" and "Password" published by SMC secure erase module.*

1. *Changed callback protocol from gEfiRestProtocolGuid to SmcMmbiHostInterfaceAccessGuid since RNDIS may not be ready during POST.*
2. *[SmcEarlyConsoleStatus] Modified and updated SmcEarlyConsoleStatus to show EarlyVideo and Status messages in SOL and console during POST.*
3. *Fixed duplicate ACPI objects.*
4. *Fixed the VideoSelect abnormal problem.*
5. *Fixed how the SAA reported garbage in the string SMC_STR_BOOT_DESCRIPTION_HELP.*
6. *Patch M.2 device could not be detected after BKC WW23.*
7. *Fixed the ITOS memory error check failure issue.*
8. *Corrected the memory address of the ErrorRecord.*
9. *Overwrote AmiPcdChassisType to sync SYS_CHASSIS_TYPE_1 setting.*

1.0 (05/24/2024)

1. *First release based on:*
    1. *SRFAP/GNRAP/GNRSP BKCWW19*
    2. *SRF-SP BKCWW19 PC components*
    3. *VROC 9.0 PC*
    4. *BHS_SRF_SP_PRE_BKC/2024.WW21 microcode.*

____ ____________________

Product Manager *Date*