BIOS Release Notes Form

Product Name	**X12DDW-A6**
Release Version	**1.4 SPS: 4.4.4.202**
Build Date	**8/4/2022**
Previous Version	**1.2**
Update Category	**Recommended**
Dependencies	**None**
Important Notes	**None**
Enhancements	**1. Updated 5.22_WhitleyCrb_0ACMS_ICX_72 Intel BKC WW23 PLR3 to address the following issues:** **a. A security update that includes INTEL-SA-00657: CVE-2022-21233 (6.0 Medium), INTEL-TA-00613: CVE-2022-0004 (7.3 High), INTEL-TA-00615: CVE-2022-21166 (5.5 Medium), INTEL-TA-00616: CVE-2022-21136 (2.7 Low), INTEL-TA-00617: CVE-2022-21151 (5.3 Medium), and INTEL-TA-00601:CVE-2021-33060 (7.8 High).** **2. Updated VROC SATA/sSATA EFI driver to VROC PreOS v7.7.6.1004 to address INTEL-TA-00692. Updated CVE-2022-29919(7.8 High), CVE-2022-30338(6.7 Medium), CVE-2022-29508(6.3 Medium), CVE-2022-25976(5.5 Medium). Updated VROC SATA/sSATA legacy driver to VROC PreOS v6.3.5.1003 Hot Fix to fix 10TB or higher volume drive issue.** **3. Added "CSM Support" setup item into SMCISBForm page.** **4. Filtered the Dynamic TCG Security pages to fix the SUM ChangeBiosCfg command.**

	5. Enabled SUM ChangeBiosCfg command to update PchSetup variable. **6. Enhanced the VPD data routines for the network controller E810.** **7. Added support for IPMI PXE boot to all LAN port feature for both Legacy and UEFI PXE.** **8. Applied a workaround to fix Linux OS showing the incorrect CPU maximum frequency.** **9. Updated SmcOOB to the version "_SMCOOBV1.01.25_" to fix the system resetting when loading NVRAM defaults.** **10. Exposed the BIOS settings Link Retrain per port, MCTP for CPU1 slot1, and CPU2 slot2.** **11. If the FRU0 chassis type is not 1 or 2, synchronize the FRU0 chassis type to SMBIOS type 3.** **12. Updated the VPD routine to read the AOC-ATG-b2Tm LAN MAC address.**
New features	**N/A**
Fixes	**N/A**

Release Notes from Previous Release(s)

1.2 (2/15/2022)

1. Updated AMI 5.22_WhitleyCrb_0ACMS_ICX_070 RC27P52 for BKC 2021_WW52 (PLR1).
2. Changed string "VMX" to "Intel Virtualization Technology".
3. Added 12+2 NVMe config support.
4. Removed 1G option from MMCFG base to avoid system hang.
5. Fixed the SMBIOS event log ERROR CODE, which not display correctly under BIOS menu issue (EFI error type).
6. Added "Preserve_SMBIOS", "Preserve_OA" into FlashFlag when in the condition "NvramDefaultMode".
7. Fixed the setup item "Lockdown Mode" which is always gray-out.

1.1b (09/18/2021)

1. Enabled 2U non-NVMe system support with 668 RSC.

1.1a (8/18/2021)

1. Updated 5.22_WhitleyCrb_0ACMS_ICX_067 Intel BKCWW32 2021 PV MR5.
2. Updated Dx/Mx microcode from Intel-Generic-Microcode-20210701_NDA.
3. Updated SATA/sSATA EFI driver to VROC PreOS v7.6.0.1012.
4. Fixed failure of SUM Test case 254 SecureEraseDisk test.
5. Added support for SUM upload/delete HTTPS TLS certificate.
6. Changed "Hard Drive Security Frozen" default setting to disabled.
7. Prevented system entering to BIOS recovery mode when implanting runtime OA 2.0 software license key under EFI shell on the system that enables chain of trust for Intel boot guard (POST F2->07 and shutdown).
8. Applied workaround for system hang at 68 during cburn power cycle long run.
9. Fixed iPXE GPF when Redfish HI is disabled.
10. Set TOKEN "Sum_UploadTlsKey_SUPPORT" default to enabled to support SUM upload/deletion of HTTPS TLS certificate.
11. Added support for SmcRedfishHostInterface EUI-48 Locally Administered MAC Address.
12. Added support for RSC-D2-666.
13. Added support for BPN-SAS3-LB16A-N10 rev. 2.00.
14. Patched X550 drop issue for dual chip AIOM.
15. Fixed inability to modify NumLock item by SmcPostHotKey.sd.
16. Fixed failure of SUM TC 221 when installing multiple NICs on system.
17. Fixed inability to preserve SGX settings after updating BIOS.
18. Fixed PSOD of VMWare with TPM.
19. Fixed problem of the system hanging during POST when building BIOS with the token "SMC_SETUP_STYLE" as 0.
20. Fixed malfunction of Patrol Scrub on Dx ICX.

1.1 (4/20/2021)

1. Set default Boot Guard profile to 5.
2. Set all OPROM control items to Legacy when boot mode is set to Dual.
3. Updated CPLD Signature table 101 and tool to 1.30.24 for CPLD Signature table 101.
4. Added support for 6+4 NVMe solution.
5. Added new CPU power spec profiles.

6. Fixed problem of T-states always showing 15 levels even when T-state is disabled.
7. Fixed missing offboard output in Setup if limited to 4G in Non-EFI mode.
8. Fixed failure of Microsoft HLK certification and TPM 2.0 UEFI Preboot Interface Test on Microsoft Server 2019.
9. Fixed problem with a CPU exception.
10. Fixed failure to hide the SmcSecureErase setup page when no HDD devices are plugged in.
11. Corrected display of UEFI OS boot option name in BIOS setup.
12. Fixed inability to upload all OOB files on the first BMC boot.
13. Corrected iSCSI Configuration page.
14. Set DIMM size to recalibrate when rank is disabled.

1.0b (3/3/2021)

1. Updated BKCWW09 2021 (PCIe recipe 3.8).
2. Updated Intel-Generic-Microcode-20210226a_NDA and Intel AE.
3. Updated ASPEED VBIOS and EFI driver to 1.11.03.
4. Updated SATA/sSATA EFI driver to VROC PreOS v7.5.0.1152.
5. Kept value of setup string of Manufacturer and Product according to priority "modification of AmiBcp, FUR1, and then SMBIOS Table".
6. Added code to stop AFU support.
7. Added HCC Mx stepping CPU check for CPU stepping display.
8. Automatically disabled and hid ADDDC with x8 width DIMM.
9. Set "NVMe Firmware Source" to auto-hide when AOC-SMG3-2M2-B is plugged in.
10. Disabled MCTP for M.2 slots to prevent system hang with Micron 2300.
11. Removed 4G limit of Intel LAN memory if boot mode is not legacy.
12. Automatically disabled and grayed out ADDDC, UMA-Base Clustering, and mirror mode and enabled NUMA when SGX is enabled.
13. Enhanced SMCI HDD Security feature.
14. Extended memory DIMM serial number information (Samsung, Micron, Hynix).
15. Enhanced SMC DCPMM feature.
16. Added RSC-D2-666-G4 and RSC-D2R-666-G4.
17. Fixed failure of SUT to prompt "Enter User password" screen after setting a password when plugging in SED device.
18. Corrected display of IPv4 address source status after updating BIOS.
19. Fixed missing SMBIOS type 17 BPS information when plugged in at P1-DIMMC2 or P2-DIMMC2.
20. Corrected location of RT UECC log.
21. Fixed failure of RT UECC to be mapped out.
22. Fixed problem of BIOS initialization showing IPV6 address when IPV6 is disabled in the IPMI GUI.
23. Filtered Dynamic HDD Security pages to patch failure of SUM ChangeBiosCfg.
24. Fixed GPU sensor issue with 2U riser.

1.0a (1/4/2021)

1. Updated Intel BKC to WW51 PC2.
2. Added retraining for X550 AIOM link drop.
3. Added F1 reboot function after 3 password attempts.
4. Added NVMe VMD auto mode with enabled VMD when VROC key is present and disabled VMD when VROC key is absent.