IPMI Firmware / BIOS Release Notes Form

Product Name	**X11SCL-LN4F**
Release Version	**1.1**
Release Date	**8/28/2019**
Build Date	**8/28/2019**
Previous Version	**1.0b**
Update Category	**Critical**
Dependencies	**None**
Important Notes	**None**
Enhancements	**1. Changed the BIOS version to 1.1.** **2. Set memory uncorrectable error to always be recorded, regardless of METW and MECI.** **3. Updated SPS firmware to SPS_E3_05.01.03.078.0.** **4. Added "SATA Frozen" function.** **5. Updated SMC OOB module to 1.01.08, added Redfish/SUM Secure Boot feature, and updated OOB for secure boot and reserve Key.** **6. Updated RC to Mehlow Refresh PV version 7.0.58.42.** **7. Implemented dynamic change for Secure Boot Mode default value.** **8. Fixed inability of BIOS to get SMBIOS type 39 power supply FRU data.** **9. Updated Coffee Lake-S R-0 stepping CPU microcode M22906ED_000000BE and Coffee Lake-S P-0 stepping CPU microcode M22906EC_000000BE.**

	10. Displayed setup item "BME DMA Mitigation" on the Advanced -> PCIe/PCI/PnP Configuration page.
New features	N/A
Fixes	1. Fixed problem of SATA Configuration page showing 1TB for 8TB 4KN HDDs. 2. Fixed problem of key details showing "Security Violation" after loading Factory secure boot keys. 3. Fixed problem of two boot devices occurring in the boot order when installing UEFI CentOS. 4. Fixed inability to enable TPM in the BIOS setup menu when plugging in TPM device and then disabling it. 5. Fixed problem of some items being adjusted when user adjusts dual boot order in BIOS setup. 6. Fixed inability to identify duplicated NVMe boot option with more than one of the same NVMe drives on an add-on card. 7. Fixed failure of OPROM control item if CSM is disabled.

1.0b (5/17/2019)

1. Updated BIOS version to 1.0b.

2. Updated RC to version 7.0.58.41.

3. Updated Coffee Lake-S R-0 stepping CPU microcode M22906ED_000000B0.

4. Updated MCU 906EA-U0 + 906EB-B0 + 906EC-P0) for INTEL-SA-00233 Security Advisory to address CVE-2018-12126, CVE-2018-12127, and CVE-2018-12130.

5. Update SPS 5.1.03.62 for INTEL-SA-00213 Security Advisory to address CVE-2019-0089, CVE-2019-0090, CVE-2019-0086, CVE-2019-0091, CVE-2019-0092, CVE-2019-0093, CVE-2019-0094, CVE-2019-0096, CVE-2019-0097, CVE-2019-0098, and CVE-2019-0099.

6. Update SPS 5.1.03.62 for INTEL-SA-00213 Security Advisory to address CVE-2019-0089, CVE-2019-0090, CVE-2019-0086, CVE-2019-0091, CVE-2019-0092, CVE-2019-0093, CVE-2019-0094, CVE-2019-0096, CVE-2019-0097, CVE-2019-0098, and CVE-2019-0099.

7. Updated Intel RSTe RAID Option ROM/UEFI Driver to 6.1.0.1017.

8. Updated USB and Fastboot module.

9. Enhanced the solution for the error/warning message from dmidecode after a modification by AMIDE.

10. Exposed the CPU's PL1 and PL2 items of Advanced -> CPU Configuration page in the BIOS setup menu.

11. Renamed "AC Loss Policy Depend on" back to "Restore on AC Power Loss".

12. Updated to avoid inability to flash OA License Key randomly.

13. Added Driver Health setup item.

14. Added driver health warning message.

15. Added OEM strings to 50 bytes in Type 11.

16. Updated IPv4 and IPv6 setup items string.

17. Updated BIOS Setup Menu for the item "Always Turbo Mode" in Advanced/CPU Configuration page.

18. Added code for Consistent Device Name support.

19. Added support for Linux built-in utility efibootmgr.

20. Set default setting Power Limit 2 to 150W when 8 Core CPU is used in the system.

21. Set OptionRom and boot mode select to EFI while CSM is disabled.

22. Changed UEFI Lan Boot option name format for SUM requirement.

23. Added RFC3021 solution for the network stack (/32 subnet mask support).

24. Exposed the setup item "BME DMA Mitigation" in the Advanced -> PCIe/PCI/PnP Configuration page.

25. Fixed issue of DIMM location to show "¡§No DIMM info¡" in Event Logs when ECC error occurs.

26. Fixed issue of DIMM location to always show "DIMMA1" in BIOS Event log when ECC error occurs.

27. Fixed issue of ""?[1;31;40m" being shown on POST screen when EFI driver is "unhealthy".

28. Fixed issue of BMC VGA status showing Enabled in SMBIOS Type 41 when JPG1 is disabled (In 2-3).

29. Fixed issue of onboard video having an output when JPG1 is disabled.

30. Fixed problem of hot-plug being registered when the PCH root port bridge is without a PCI-E device.

31. Updated "Restore Optimized Defaults" string for Mehlow Server template.

32. Modified UEFI network description as IPv4/IPv6 to follow Industry Standard.

33. Added workaround for BIOS flash failure with 156 bytes PubKey (Error: "Secure Flash Rom Verify Fail").

34. Fixed problem of the system hanging in CP: 0xF4 when the system recovery occurs in BIOS with TPM module.

35. Fixed problem of the value of Power Limit 2 displaying as 0 in setup menu when setup menu is set to 0 (AUTO).

36. Fixed issue of system may or may not hanging up when LAN1 is disabled.

37. Fixed DIMM location of ECC error to show "NO DIMM INFO" in Event log when Multi-Bit ECC error occurs.

1.0a (2/26/2019)

1. Updated BIOS revision to 1.0a.

2. Updated Intel Reference Code to version 7.0.51.40.

3. Updated CPU MCU (906EA, U0 + 906EB, B0 + 906EC, P0).

4. Hid LAN OPROM Control items when LAN#1 OPROM is set to iSCSI.

5. Added Early Video messages when BIOS is in recovery mode.

6. Added "ACPI T-States" setup item.

7. Displayed "AERON" and "MCEON" strings during POST when "PCI AER Support" or "Memory Corrected Error" is enabled.

8. Hide "ECC Support" item.

9. Set the default of "Memory Corrected Error Enabling" to disabled.

10. Updated the Intel BIOS ACM version to 1.5.0 and SINIT ACM to 1.6.0.

11. Added "SMC SMBIOS Measurement" feature for PCR#1 measurement and enabled "Measure_Smbios_Tables".

12. Updated RAID option ROM and UEFI driver to 5.5.1028.

13. Added "MCEON" and "AERON" POST strings for SOL console when items are enabled.

14. Enhanced JPG1 function for running SUM with JPG1 2-3.

15. Added support for RFC4122 UUID format feature so that RFC4122 encoding from build time is produced by IPMICFG 1.29 tool or newer version.

16. Added "SATA Frozen" function.

17. Added support for Linux built-in utility efibootmgr.

18. Hid "Always Turbo Mode" when "Turbo Mode" setting is set to Disable in Advanced/CPU Configuration page.

19. Updated IPv4 and IPv5 setup item strings.

20. Added OEM strings to 50 bytes in Type 11.

21. Added Disabled option for "Onboard Video Option ROM" setup item.

22. Added "Driver Health" setup item.

23. Added Driver Health warning message.

24. Renamed "AC Loss Policy Depend on" to "Restore on AC Power Loss".

25. Enhanced the solution for the error/warning message from dmidecode after AMIDE modification.

26. Updated SMBIOS Type 9 for AOC Sensor Reading.

27. Fixed inability to Boot Option of UEFI Application Boot Priorities to load default via Afu tool with command "/N".

28. Changed the "SATA Interrupt Selection" default value to MSI.

29. Fixed problem of Chassis Intrusion status in BMC clearing every time system boots.

30. Fixed issue of serial port UID order to follow COM port order after BIOS update.

31. Fixed issue of PCR#1 value to be changed during Legacy boot with TPM 2.0 when Measure_Smbios_tables is disabled.

32. Fixed problem of the system having an exception while entering BIOS Setup with NVMe M2*1 + SATA M2*1.

33. Fixed problem of InBand receiving incorrect OEM FID size.

34. Fixed problem of system hanging in CP during system recovery BIOS with TPM module.

35. Updated "Restore Optimized Defaults" string for Mehlow Server template.

36. Modified UEFI network description to IPv4/IPv6 to follow Industry Standard.

37. Removed processor version "Type" string for Mehlow Server template.

38. Fixed issue of onboard video output displaying screen on DXE stage when JPG1 is disabled.

39. Updated "Redirection After BIOS POST" string for Mehlow Server template.

40. Fixed problem of BMC VGA status being enabled in SMBIOS Type 41 when JPG1 is disabled (In 2-3).

41. Fixed lack of onboard VGA information in Type 40.