NUC BIOS ENGINEERING

5200 NE Elam Young Parkway
Hillsboro, OR 97124-6497

BIOS Update Release Notes

Alder Lake-P Standard BIOS
PRODUCTS: LAPAC71G, LAPAC71H (Alder County)

ACADL357.0069.2025.0916.1436 Production BIOS

About This Release:

- Date: Sep 16, 2025
- ROM Image Checksum: 0XA5BA70A4
- EC Firmware: 1.12.00.000
- ME Firmware: 16.1.38.2676
- PCH Configuration Firmware: 16.1.0.1014
- PMC Firmware: 160.1.0.1030
- iTBT Firmware: 16.0.0.2102
- IOM Firmware: 36.7.0.0000
- Retimer Firmware in BIOS capsule: 3.9
- SPHY Firmware: N/A
- NPHY Firmware: 14.531.509.8259
- Platform Properties Assessment Module: 11.22a.7
- I225 NVM: N/A
- CRB Label: ADL_052
- Boot Guard ACM: 1.18.16
- Bios Guard: BiosGuard_035
- Silicon Initialization Code: Based on 0C.00.69.74
- Memory Reference Code: Based on 0.0.4.60
- Integrated Graphics GOP
  - UEFI Driver: 21.0.1054
- Intel RST Pre-OS:
  - VMD UEFI Driver: 19.0.0.5428
- AHCI Code: Based on AHCI_30
- Supported Flash Devices:

WinBond	W25Q256FV	32MB
GigaDevice	GD25B256D	32MB

- Microcode Updates included in .ROM & .CAP Files:
  M80906A3_00000437.pdb

Feature Changes/Updates/Security Patches

Based on AC0068

1. Update:[AMI Changes][EIP 849222] 2025.2 Intel Platform Update
2. Update:[AMI Changes][EIP 849223] [SA50315] SecureBoot DBX Update 06102025

Known Errata:

- Bitlocker Recovery will be occurred after reload Secureboot key in Setup since L30048 has updated Secure Boot DBX.
- **WU files for test use only.**

ACADL357.0068.2025.0507.1432 Production BIOS

About This Release:

- Date: May 07, 2025
- ROM Image Checksum: 0XA5C48ACF
- EC Firmware: 1.12.00.000
- ME Firmware: 16.1.35.2557
- PCH Configuration Firmware: 16.1.0.1014
- PMC Firmware: 160.1.0.1030
- iTBT Firmware: 16.0.0.2102
- IOM Firmware: 36.7.0.0000
- Retimer Firmware in BIOS capsule: 3.9
- NPHY Firmware: 14.531.509.8259
- Platform Properties Assessment Module: 11.22a.7
- CRB Label: ADL_052
- Boot Guard ACM: 1.18.16
- BIOS Guard: BiosGuard_035
- Silicon Initialization Code: Based on 0C.00.69.74
- Memory Reference Code: Based on 0.0.4.60
- Integrated Graphics:
    - UEFI Driver: 21.0.1054
- Intel RST Pre-OS:
    - VMD UEFI Driver: 19.0.0.5428
- Wired LAN Adapter:
    - UEFI Driver: 0.9.03
- AHCI Code: Based on AHCI_30
- Visual BIOS: Intel AptioV

- Supported Flash Devices:

WinBond	W25Q256FV	32MB
GigaDevice	GD25B256D	32MB

- Microcode Updates included in .BIN & .CAP Files:

  M80906A3_00000437.pdb

Feature Changes/Updates/Security Patches

Based on AC0067

1. Fixed: [AMI Changes][EIP 837831] Run “BCDEDIT /set {fwbootmgr}” timeout fail under OS
2. Updated: [AMI Changes][EIP 837826][IPU][SA50278] 2025.1 Intel Platform Update
3. Updated: [AMI Changes][EIP None] Update CPU Microcode to revision 0x437
4. Added: [AMI Changes][EIP 837826][[Security] Implement S3 reboot code in MS support project

Known Errata:

- AC0061 remains using the TCSS FW package, and only updates the ME FW.
- Intel signed BIOS and NvRAM have been locked in AC0037, do not downgrade BIOS to previous versions.
- Both BIOS Lock and ME Pre-Lock are active in AC0043, user cannot flash BIOS using FPT tool.
- **WU files for test use only.**

ACADL357.0067.2025.0115.1505 Production BIOS

About This Release:

- Date: Jan 15, 2025
- ROM Image Checksum: 0XA5CB813E
- EC Firmware: 1.12.00.000
- ME Firmware: **16.1.35.2557**
- PCH Configuration Firmware: 16.1.0.1014
- PMC Firmware: 160.1.0.1030
- iTBT Firmware: 16.0.0.2102
- IOM Firmware: 36.7.0.0000
- Retimer Firmware in BIOS capsule: 3.9
- NPHY Firmware: 14.531.509.8259
- Platform Properties Assessment Module: 11.22a.7
- CRB Label: ADL_052
- Boot Guard ACM: 1.18.16
- BIOS Guard: BiosGuard_035
- Silicon Initialization Code: Based on 0C.00.69.74
- Memory Reference Code: Based on 0.0.4.60
- Integrated Graphics:
  - UEFI Driver: 21.0.1054
- Intel RST Pre-OS:
  - VMD UEFI Driver: 19.0.0.5428
- Wired LAN Adapter:
  - UEFI Driver: 0.9.03
- AHCI Code: Based on AHCI_30
- Visual BIOS: Intel AptioV

- Supported Flash Devices:

WinBond	W25Q256FV	32MB
GigaDevice	GD25B256D	32MB

- Microcode Updates included in .BIN & .CAP Files:
  M80906A3_00000436.pdb

Feature Changes/Updates/Security Patches

Based on AC0066

1. Updated: [AMI Changes][EIP 828191][Intel/NUC-G][TF][AC][IPU][SA50253] 2024.2 Intel Platform Update.
2. Updated: [AMI Changes][EIP 828192][Intel/NUC-G][TF][AC][IPU][SA50254] 2024.3 Intel Platform Update.
3. Updated: [AMI Changes][EIP 828193][Intel/NUC-G][TF][AC][IPU][SA50269] 2024.4 Intel Platform Update.
4. Updated: [AMI Changes][EIP None] Update ME to 16.1.35.2557
5. Updated: [AMI Changes][EIP None] Update CPU Microcode to revision 0x436
6. Updated: [AMI Changes][EIP 828185][Intel/NUC-G][TF][AC] Align MRC to IPU 2024.1 from RPL CRB048
7. Fixed: [AMI Changes][EIP 828187][Intel/NUC-G][TF][AC] After re-plugging TYPE-C/DP/HDMI, the secure boot violation message screen shows noise
8. Fixed: [AMI Changes][EIP 828188][Intel/NUC-G][TF][AC] Setting the Hard Disk pre-delay will cause a black screen for a period of time during the POST process.
9. Fixed: [AMI Changes][EIP 828190][Intel/NUC-G][TF][AC] SUT could not boot into OS on NVMe ports in config mode of Security Jumper
10. Fixed: [AMI Changes][EIP 808580][Intel/NUC-G][TF][AC] No matter “Re-size Bar Support” in AC0065 is set to enable or disable, the function is always enable

Known Errata:

- AC0061 remains using the TCSS FW package, and only updates the ME FW.
- Intel signed BIOS and NvRAM have been locked in AC0037, do not downgrade BIOS to previous versions.
- Both BIOS Lock and ME Pre-Lock are active in AC0043, user cannot flash BIOS using FPT tool.
- **WU files for test use only.**

ACADL357.0066.2024.0702.1615 Production BIOS

About This Release:

- Date: July 02, 2024
- ROM Image Checksum: 0XA609F89B
- EC Firmware: 1.12.00.000
- ME Firmware: **16.1.32.2418**
- PCH Configuration Firmware: 16.1.0.1014
- PMC Firmware: 160.1.0.1030
- iTBT Firmware: **16.0.0.2102**
- IOM Firmware: **36.7.0.0000**
- Retimer Firmware in BIOS capsule: 3.9
- NPHY Firmware: 14.531.509.8259
- Platform Properties Assessment Module: 11.22a.7
- CRB Label: ADL_052
- Boot Guard ACM: 1.18.16
- BIOS Guard: BiosGuard_035
- Silicon Initialization Code: Based on 0C.00.69.74
- Memory Reference Code: Based on 0.0.4.60
- Integrated Graphics:
    - UEFI Driver: 21.0.1054
- Intel RST Pre-OS:
    - VMD UEFI Driver: 19.0.0.5428
- Wired LAN Adapter:
    - UEFI Driver: 0.9.03
- AHCI Code: Based on AHCI_30
- Visual BIOS: Intel AptioV

- Supported Flash Devices:

WinBond	W25Q256FV	32MB
GigaDevice	GD25B256D	32MB

- Microcode Updates included in .BIN & .CAP Files:
  M80906A3_00000434.pdb

Feature Changes/Updates/Security Patches

Based on AC0065

1. Fixed: [AMI Changes][EIP 806375][Intel/NUC-G][TF][AC][SA50209] TOCTOU Vulnerability in SmiFlash (Enhancement)
2. Updated: [AMI Changes][EIP None] Update ME to 16.1.32.2418
3. Updated: [AMI Changes][EIP None] Update CPU Microcode to revision 0x434
4. Fixed: [AMI Changes][EIP 799655][Intel/NUC-G][TF][AC] EBU will fail if rerunning the EBU program after closed it
5. Fixed: [AMI Changes][EIP 806376][New patch][Intel/NUC-G][TF][AC] The POST screen is not correct after the BIOS block downgrade message is displayed.

Known Errata:

- AC0061 remains using the TCSS FW package, and only updates the ME FW.
- Intel signed BIOS and NvRAM have been locked in AC0037, do not downgrade BIOS to previous versions.
- Both BIOS Lock and ME Pre-Lock are active in AC0043, user cannot flash BIOS using FPT tool.
- **WU files for test use only.**

ACADL357.0065.2024.0409.1723 Production BIOS

About This Release:

- Date: Apr 09, 2024
- ROM Image Checksum: 0XA60DFF6C
- EC Firmware: 1.12.00.000
- ME Firmware: **16.1.30.2307**
- PCH Configuration Firmware: 16.1.0.1014
- PMC Firmware: **160.1.0.1030**
- iTBT Firmware: **16.0.0.0202**
- IOM Firmware: **36.6.0.0000**
- Retimer Firmware in BIOS capsule: 3.9
- NPHY Firmware: **14.531.509.8259**
- Platform Properties Assessment Module: 11.22a.7
- CRB Label: ADL_052
- Boot Guard ACM: **1.18.16**
- BIOS Guard: BiosGuard_035
- Silicon Initialization Code: Based on 0C.00.69.74
- Memory Reference Code: Based on 0.0.4.60
- Integrated Graphics:
  - o UEFI Driver: 21.0.1054
- Intel RST Pre-OS:
  - o VMD UEFI Driver: 19.0.0.5428
- o Wired LAN Adapter:
  - ▪ UEFI Driver: 0.9.03
- AHCI Code: Based on AHCI_30
- Visual BIOS: Intel AptioV

- Supported Flash Devices:

WinBond	W25Q256FV	32MB
GigaDevice	GD25B256D	32MB

- Microcode Updates included in .BIN & .CAP Files:
  M80906A3_00000433.pdb

Feature Changes/Updates/Security Patches

Based on AC0064

11. Fixed: [AMI Changes][EIP 795118][Intel/NUC-G][TF][AC][PTK4413][SA50189] Flash driver security review
12. Fixed: [AMI Changes][EIP 795115][Intel/NUC-G][TF][AC][PTK4469][SA50243] UsbRt TOCTOU Vulnerability
13. Fixed: [AMI Changes][EIP 795120][Intel/NUC-G][TF][AC][PTK4132/4135][SA50232] Vulnerabilities in EDK2 NetworkPkg
14. Fixed: [AMI Changes][EIP 795119][Intel/NUC-G][TF][AC][SA50235] Extended Image Parser Corruption Correction
15. Fixed: [AMI Changes][EIP 795126][Intel/NUC-G][TF][AC][SA50230] Image Parser Corruption Vulnerability
16. Updated: [AMI Changes][EIP 795114][Intel/NUC-G][TF][AC][IPU][SA50211/SA50217] 2024.1 Intel Platform Update
17. Updated: [AMI Changes][EIP 795113][Intel/NUC-G][TF][AC][IPU][SA50204] 2023.4 Intel Platform Update
18. Updated: [AMI Changes][EIP None] Update ME to 16.1.30.2307
19. Updated: [AMI Changes][EIP None] Update CPU Microcode to 0x433
20. Fixed: [AMI Changes][EIP 795122][Intel/NUC-G][ECS][AC] The POST screen is not correct after the BIOS block downgrade message is displayed.

Known Errata:

- AC0061 remains using the TCSS FW package, and only updates the ME FW.
- Intel signed BIOS and NvRAM have been locked in AC0037, do not downgrade BIOS to previous versions.
- Both BIOS Lock and ME Pre-Lock are active in AC0043, user cannot flash BIOS using FPT tool.
- **WU files for test use only.**

ACADL357.0064.2024.0110.1510 Production BIOS

About This Release:

- Date: Jan 10, 2024
- ROM Image Checksum: 0XA6141EDB
- EC Firmware: 1.12.00.000
- ME Firmware: 16.1.27.2176
- PCH Configuration Firmware: 16.1.0.1014
- PMC Firmware: 160.1.0.1029
- iTBT Firmware: 16.0.0.0117
- IOM Firmware: 34.12.0.0000
- Retimer Firmware in BIOS capsule: 3.9
- NPHY Firmware: 14.528.505.8210
- Platform Properties Assessment Module: 11.22a.7
- CRB Label: ADL_052
- Boot Guard ACM: 1.18.15
- BIOS Guard: BiosGuard_035
- Silicon Initialization Code: Based on 0C.00.69.74
- Memory Reference Code: Based on 0.0.4.60
- Integrated Graphics:
  - UEFI Driver: 21.0.1054
- Intel RST Pre-OS:
  - VMD UEFI Driver: 19.0.0.5428
- Wired LAN Adapter:
  - UEFI Driver: 0.9.03
- AHCI Code: Based on AHCI_30
- Visual BIOS: Intel AptioV

- Supported Flash Devices:

WinBond	W25Q256FV	32MB
GigaDevice	GD25B256D	32MB

- Microcode Updates included in .BIN & .CAP Files:

  M80906A3_00000432.pdb

Feature Changes/Updates/Security Patches

Based on AC0063

21. Fixed: [AMI Changes][EIP 782956][Intel/NUC-G][TF][AC][PTK4040][SA50216] LogoFAIL Vulnerability
22. Fixed: [AMI Changes][EIP 782960][Intel/NUC-G][TF][AC][PTK4157][SA50212] EDK2 PEI-Phase Denial of Service Vulnerability
23. Fixed: [AMI Changes][EIP 782958][Intel/NUC-G][TF][AC][SA50218] NetworkPkg EDK2
24. Fixed: [AMI Changes][EIP 782959][Intel/NUC-G][TF][AC][PTK4208][SA50221] UsbSmmRt vulnerability
25. Updated: [AMI Changes][EIP 782963] [Intel/NUC-G][TF][AC] Update Intel KEK/DB keys to support MSFT CA 2023
26. Updated: [AMI Changes][EIP None] CPU Microcode to M80906A3_00000432.pdb

Known Errata:

- AC0061 remains using the TCSS FW package, and only updates the ME FW.
- Intel signed BIOS and NvRAM have been locked in AC0037, do not downgrade BIOS to previous versions.
- Both BIOS Lock and ME Pre-Lock are active in AC0043, user cannot flash BIOS using FPT tool.

- **WU files for test use only.**

Alder Lake-P Standard BIOS
PRODUCTS: LAPAC71G, LAPAC71H (Alder County)

ACADL357.0063.2023.1003.1426 Production BIOS

About This Release:

- Date: Oct 03, 2023

- ROM Image Checksum: 0XA6293D7C
- EC Firmware: 1.12.00.000
- ME Firmware: 16.1.27.2176
- PCH Configuration Firmware: 16.1.0.1014
- PMC Firmware: 160.1.0.1029
- iTBT Firmware: 16.0.0.0117
- IOM Firmware: 34.12.0.0000
- Retimer Firmware in BIOS capsule: 3.9
- NPHY Firmware: 14.528.505.8210
- Platform Properties Assessment Module: 11.22a.7
- CRB Label: ADL_052
- Boot Guard ACM: 1.18.15
- BIOS Guard: BiosGuard_035
- Silicon Initialization Code: Based on 0C.00.69.74
- Memory Reference Code: Based on 0.0.4.60
- Integrated Graphics:
    - UEFI Driver: 21.0.1054
- Intel RST Pre-OS:
    - VMD UEFI Driver: 19.0.0.5428
- Wired LAN Adapter:
    - UEFI Driver: 0.9.03
- AHCI Code: Based on AHCI_30
- Visual BIOS: Intel AptioV

- Supported Flash Devices:

WinBond	W25Q256FV	32MB
GigaDevice	GD25B256D	32MB

- Microcode Updates included in .BIN & .CAP Files:
  M80906A3_00000430.pdb

Feature Changes/Updates/Security Patches

Based on AC0062

27. Fixed: [AMI Changes][EIP 767734] [Intel/NUC-G][TF][AC][PTK3792][SA50209] TOCTOU Vulnerability in "SmiFlash".
28. Updated: [AMI Changes] CPU Microcode to M80906A3_00000430.pdb.
29. Fixed: [AMI Changes][EIP 767737] [Intel/NUC-G][TF][AC] The values of iSetupCfg password check setting are not saved when pressing the SAVE icon in the upper right corner.

Known Errata:

- AC0061 remains using the TCSS FW package, and only updates the ME FW.
- Intel signed BIOS and NvRAM have been locked in AC0037, do not downgrade BIOS to previous versions.
- Both BIOS Lock and ME Pre-Lock are active in AC0043, user cannot flash BIOS using FPT tool.
- **WU files for test use only.**

Alder Lake-P Standard BIOS
PRODUCTS: LAPAC71G, LAPAC71H (Alder County)

ACADL357.0062.2023.0724.1432 Production BIOS

About This Release:

- Date: July 24, 2023

- ROM Image Checksum: 0XA644BBCA
- EC Firmware: 1.12.00.000
- **ME Firmware: 16.1.27.2176**
- PCH Configuration Firmware: 16.1.0.1014
- PMC Firmware: 160.1.0.1029
- iTBT Firmware: 16.0.0.0117
- IOM Firmware: 34.12.0.0000
- Retimer Firmware in BIOS capsule: 3.9
- NPHY Firmware: 14.528.505.8210
- Platform Properties Assessment Module: 11.22a.7
- CRB Label: ADL_052
- **Boot Guard ACM: 1.18.15**
- BIOS Guard: BiosGuard_035
- Silicon Initialization Code: Based on 0C.00.69.74
- Memory Reference Code: Based on 0.0.4.60
- Integrated Graphics:
    - UEFI Driver: 21.0.1054
- Intel RST Pre-OS:
    - VMD UEFI Driver: 19.0.0.5428
- AHCI Code: Based on AHCI_30
- Wired LAN Adapter:
    - UEFI Driver: 0.9.03
- Visual BIOS: Intel AptioV

- Supported Flash Devices:

WinBond	W25Q256FV	32MB
GigaDevice	GD25B256D	32MB

- Microcode Updates included in .BIN & .CAP Files:

  M80906A3_0000042C.pdb

Feature Changes/Updates/Security Patches

Based on AC0061

30. Updated: [AMI Changes][EIP 755471][Intel/NUC-G][TF][AC][IPU][SA50184] 2023.3 Intel Platform update.
31. Updated: [AMI Changes][EIP 755464][Intel/NUC-G][TF][AC][PTK3596][Utility] Updated support for iFlashV flash tool versions 5.13.00.2106 (X64) / 5.13.00.2106 (Ia32).
32. Updated: [AMI Changes][EIP 755473][Intel/NUC-G][TF][AC][SA50197] BlackLotus-SecureBoot DBX update.
33. Fixed: [AMI Changes][EIP 755456][Intel/NUC-G][TF][AC][PTK2793] Intel NUC information leak vulnerability.
34. Fixed: [AMI Changes][EIP 755460][Intel/NUC-G][TF][AC][SA50136] GenericSio Information Disclosure vulnerability.
35. Fixed: [AMI Changes][EIP 755458][Intel/NUC-G][TF][AC][SA50179/CVE] EDK2 vulnerabilities.
36. Added: [AMI Changes][EIP 755462][Intel/NUC-G][TF][AC][SA50158] PlatformLang Timeout Variable Access.
37. Updated: [AMI Changes][EIP 755466][Intel/NUC-G][TF][AC][SA50193] OpenSSL Policy Constraints.
38. Fixed: [AMI Changes][EIP 755468][Intel/NUC-G][TF][AC][PTK3750/PTK3756][SA50198] Heap Buffer Overflow in TCG2MeasurePeImage.
39. Updated: [AMI Changes][EIP 755461][Intel/NUC-G][TF][AC] ADL RC 0C.00.74.20 (3365.00) partial update: Variable buffer overflow.
40. Updated: [AMI Changes][EIP 755475][Intel/NUC-G][TF][AC][SA50183] Harden SMM Write Flash area.
41. Fixed: [AMI Changes][EIP 742566][Intel/NUC-G][TF][AC][SA50186] OpenSSL vulnerabilities.
42. **Updated: [AMI Changes][Intel/NUC-G][TF][AC] ME FW to 16.1.27.2176 (v2).**
43. **Updated: [AMI Changes][Intel/NUC-G][TF][AC] CPU Microcode to 0x42C.**
44. Added: [AMI Changes][EIP 755482][Intel/NUC-G][TF][AC] "Extend CSME Measurement to TPM-PCR”.
45. Fixed: [AMI Changes][EIP 755484][Intel/NUC-G][TF][AC] When the Intel i219 LAN and Thunderbolt support items are disabled in the BIOS, the system cannot update the BIOS through the Power Button Menu [F7] Flash option.

Known Errata:

- AC0061 remains with the same TCSS FW package, only ME FW has been updated.
- Intel Signed BIOS and NvRAM have been locked in AC0037, do not downgrade BIOS to previous versions.
- Both BIOS Lock and ME Pre-Lock are active in AC0043, user cannot flash BIOS using FPT tool.
- **WU files for test use only.**

Alder Lake-P Standard BIOS
PRODUCTS: LAPAC71G, LAPAC71H (Alder County)

ACADL357.0061.2023.0427.1553 Production BIOS

About This Release:

- Date: 04/27/2023

- ROM Image Checksum: 0xA6E91251
- **EC Firmware: 1.12.00.000**
- **ME Firmware: 16.1.25.2124**
- **PCH Configuration Firmware: 16.1.0.1014**
- **PMC Firmware: 160.1.0.1029**
- iTBT Firmware: 16.0.0.0117
- **IOM Firmware: 34.12.0.0000**
- Retimer Firmware in BIOS capsule: 3.9
- NPHY Firmware: 14.528.505.8210
- Platform Properties Assessment Module: 11.22a.7
- CRB Label: ADL_052
- **Boot Guard ACM: 1.18.12**
- BIOS Guard: BiosGuard_035
- Silicon Initialization Code: Based on 0C.00.69.74
- Memory Reference Code: Based on 0.0.4.60
- Integrated Graphics:
  - UEFI Driver: 21.0.1054
- Intel RST Pre-OS:
  - VMD UEFI Driver: 19.0.0.5428
- AHCI Code: Based on AHCI_30
- Wired LAN Adapter:
  - UEFI Driver: 0.9.03
- Visual BIOS: Intel AptioV

- Supported Flash Devices:

WinBond	W25Q256FV	32MB
GigaDevice	GD25B256D	32MB

- Microcode Updates included in .BIN & .CAP Files:

  M80906A3_0000042A.pdb

Feature Changes/Updates/Security Patches：

Based on AC0060

1. Updated: [AMI Changes][Intel/NUC-G][TF][AC] IPU 2023.1 Update.
2. Fixed: [AMI Changes][Intel/NUC-G][TF][AC][PTK2712/SA50175] UEFI Variable access vulnerability.
3. Fixed: [AMI Changes][SA50170][Intel/NUC-G][TF][AC] “SmmEntryPoint” Underflow Vulnerability.
4. Fixed: [AMI Changes][Intel/NUC-G][TF][AC][PTK2427/SA50140] The Stack Buffer Overflow vulnerability can lead to arbitrary code execution in DXE driver on select Intel platforms.
5. **Updated: [AMI Changes] ME FW to 16.1.25.2124.**
6. **Updated: [AMI Changes] EC FW to v1.12.00.000**
7. **Updated: [AMI Changes] CPU Microcode to M80906A3_0000042A.pdb**

Known Errata:

- AC0061 remains with the same TCSS FW package, only ME FW has been updated.
- Intel Signed BIOS and NvRAM locked in AC0037, do not downgrade BIOS to previous versions.
- Both BIOS Lock and ME Pre-Lock are active in AC0043, user cannot flash BIOS using FPT tool.
- **WU files for test use only.**

ACADL357.0060.2023.0110.1333 Production BIOS

About This Release:

- Date: Jan 09, 2023
- ROM Image Checksum: 0xA734ABEF
- **EC Firmware: 1.11.00**
- ME Firmware: 16.0.15.1810 (v5)
- PCH Configuration Firmware: 16.0.0.1012
- PMC Firmware: 160.01.00.1027
- iTBT Firmware: TBT_ADL_MP_ALL_17.1V1_Rel
- IOM Firmware: 22.000c.0.0000
- Retimer Firmware in BIOS capsule: 3.9
- NPHY Firmware: 14.528.505.8210
- Platform Properties Assessment Module: 11.22a.7
- CRB Label: ADL_052
- Boot Guard ACM: 1.18.10
- BIOS Guard: 2.0.5021
- Silicon Initialization Code: Based on 0C.00.69.74
- Memory Reference Code: Based on 0.0.4.60
- Integrated Graphics:
  - o UEFI Driver: 21.0.1054
- Intel RST Pre-OS:
  - o VMD UEFI Driver: 19.0.0.5428

o Wired LAN Adapter:
  - ▪ UEFI Driver: 0.9.03

- AHCI Code: Based on AHCI_30
- Visual BIOS: Intel AptioV

- Supported Flash Devices:

WinBond	W25Q256FV	32MB
GigaDevice	GD25B256D	32MB

- Microcode Updates included in .BIN & .CAP Files:
  M80906A3_00000420.pdb

Feature Changes/Updates/Security Patches：
Based on AC0059

1. Fixed: [AMI Changes][Intel/NUC-G][TF][AC][SA50085] GRUB Bootloader Vulnerability.
2. Fixed: [AMI Changes][Intel/NUC-G][TF][AC][PTK2712/SA50151] SIO_DEV_STATUS_VAR_NAME Information Leakage_PTK2712#12.
3. Fixed: [AMI Changes][Intel/NUC-G][TF][AC]][SA50148] SDIO_DEV_CONFIGURATION SetVariable NVRAM Corruption.
4. Updated: [AMI Changes][Intel/NUC-G][TF][AC][IPU] 2022 IPU update: 2022.3.
5. Fixed: [AMI Changes][Intel/NUC-G][TF][AC][PTK2828/PTK2829] Intel NUC 8 vulnerability/Intel NUC 8 info leak vulnerability.
6. Fixed: [AMI Changes][Intel/NUC-G][TF][AC][SA50157] UEFI Boot Variables Access.
7. Fixed: [AMI Changes][Intel/NUC-G][TF][AC][SA50088] TianoCore Security Issues.
8. Updated: [AMI Changes][General] Building Process optimized.
9. Updated: [AMI Changes] Changed "Press F8 to Activate Windows Recovery Mode" Boot Flow for "BOOT_FLOW_CONDITION_OEM_KEY3" to "BOOT_FLOW_CONDITION_OEM_KEY4".
10. Added: [AMI Changes][Intel/NUC-G][TF][AC] BIOS WU setup addition.
11. **Updated: [AMI_Changes] EC FW to v1.11.00**

12. Fixed: [AMI Changes] OemPL1Time size in stddefault was not correct.

Known Errata:

1. Supplemental BIOS starts from AC0033 and does not work on QS K Stepping CPU. **DO NOT FLASH** this BIOS on older platform. If you need to build BIOS for K stepping CPU, please modify TOKEN “SUPPLEMENTAL_BOARD_SUPPORT” as 0.
2. Intel signed BIOS and NvRAM locked in AC0037, do not downgrade BIOS to a previous version.
3. BIOS Lock and ME Pre-Lock in AC0043 and cannot flash BIOS using FPT tool.
4. **WU files for test use only.**

ACADL357.0059.2022.1205.2222 Production BIOS

About This Release:

- Date: Dec 05, 2022
- ROM Image Checksum: 0xA749E082
- EC Firmware: 1.09.00.000
- ME Firmware: 16.0.15.1810 (v5)
- PCH Configuration Firmware: 16.0.0.1012
- PMC Firmware: 160.01.00.1027
- iTBT Firmware: TBT_ADL_MP_ALL_17.1V1_Rel
- IOM Firmware: 22.000c.0.0000
- Retimer Firmware in BIOS capsule: 3.9
- NPHY Firmware: 14.528.505.8210
- Platform Properties Assessment Module: 11.22a.7
- CRB Label: ADL_052
- Boot Guard ACM: 1.18.10
- BIOS Guard: 2.0.5021
- Silicon Initialization Code: Based on 0C.00.69.74
- Memory Reference Code: Based on 0.0.4.6
- Integrated Graphics:
  - UEFI Driver: 21.0.1054
- Intel RST Pre-OS:
  - VMD UEFI Driver: 19.0.0.5428
- AHCI Code: Based on AHCI_30
- Visual BIOS: Intel AptioV

- Supported Flash Devices:

WinBond	W25Q256FV	32MB
GigaDevice	GD25B256D	32MB

- Microcode Updates included in .BIN & .CAP Files:
  M80906A3_00000420.pdb

Feature Change/Updates:
Based on AC0058

13. Fixed: [AMI_Changes][Intel/NUC-G][TF][AC][Security][PTK1931] Privilege escalation vulnerability from kernel to SMM in multiple devices.
14. Fixed: [AMI_Changes][Intel/NUC-G][TF][AC][PTK2696] Intel NUC information disclosure vulnerability.
15. Fixed: [AMI_Changes][Intel/NUC-G][TF][AC][PTK2872] Potential hack of BIOS EBU DLL.
16. Fixed: [AMI_Changes][Intel/NUC-G][TF][AC][Security] “OpenSSL” (CVE-2022-3786 & CVE-2022-3602) security vulnerabilities.
17. Fixed: [AMI_Changes][EIP 713339][Intel/NUC-G][TF][AC] iSetupCfg not able to change default value of PLx/Fan curve parameters due to stdDefault override mechanism.
18. Updated: [AMI_Changes] Remove Exit button in capsule update page because it is not used.
19. Updated: [AMI_Changes] Follow RC0C.00.71.76 (3275.00) to revert TME TPM log change.
20. Added: [AMI_Changes] Added StdDefaults into ProtectedNvVariableForRuntime ELink.
21. Fixed: [AMI_Changes] BIOS WU:DF - InfVerif INF Verification-Fails

Known Errata:

5. Supplemental BIOS starts from AC0033 and does not work on QS K Stepping CPU. **DO NOT FLASH** this BIOS on older

platform. If you need to build BIOS for K stepping CPU, please modify TOKEN “SUPPLEMENTAL_BOARD_SUPPORT” as 0.

6. Intel signed BIOS and NvRAM locked in AC0037, do not downgrade BIOS to a previous version.
7. BIOS Lock and ME Pre-Lock in AC0043 and cannot flash BIOS using FPT tool.
8. **WU files for test use only.**

ACADL357.0058.2022.0914.1524 Production BIOS

About This Release:

- Date: Sep 14, 2022
- ROM Image Checksum: 0xA74E9909
- **EC Firmware: 1.09.00.000**
- ME Firmware: 16.0.15.1810 (v5)
- PCH Configuration Firmware: 16.0.0.1012
- PMC Firmware: 160.01.00.1027
- iTBT Firmware: TBT_ADL_MP_ALL_17.1V1_Rel
- IOM Firmware: 22.000c.0.0000
- Retimer Firmware in BIOS capsule: 3.9
- NPHY Firmware: 14.528.505.8210
- Platform Properties Assessment Module: 11.22a.7
- CRB Label: ADL_052
- Boot Guard ACM: 1.18.10
- BIOS Guard: 2.0.5021
- Silicon Initialization Code: Based on 0C.00.69.74
- Memory Reference Code: Based on 0.0.4.6
- Integrated Graphics:
  - UEFI Driver: 21.0.1054
- Discrete Graphics:
  - UEFI Driver: 20.1046.0.0
- Intel RST Pre-OS:
  - VMD UEFI Driver: 19.0.0.5428
- AHCI Code: Based on AHCI_30
- Visual BIOS: Intel AptioV

- Supported Flash Devices:

* WinBond	W25Q256FV	32MB
* GigaDevice	GD25B256D	32MB

- Microcode Updates included in .BIN & .CAP Files:
  M80906A3_00000420.pdb

Feature Change/Update:

1. Fixed: Windows 11 22H2 WHQL camera related test failure.
2. **Updated: [AMI_Changes][AC0057] EC FW to v01.09.00**

Known Errata:

9. Supplemental BIOS starts from AC0033 and does not work on QS K Stepping CPU. DO NOT FLASH this BIOS on older platform. If you need to build BIOS for K stepping CPU, please modify TOKEN "SUPPLEMENTAL_BOARD_SUPPORT" as 0.
10. Intel signed BIOS and NvRAM locked in AC0037, do not downgrade BIOS to a previous version.
11. BIOS Lock and ME Pre-Lock in AC0043 and cannot flash BIOS using FPT tool.
12. **WU files for test use only.**

ACADL357.0057.2022.0905.1533 Development BIOS

About This Release:

- Date: Sept 05, 2022
- ROM Image Checksum: 0xA7473FBB
- **EC Firmware: 1.09.00.000**
- ME Firmware: 16.0.15.1810 (v5)
- PCH Configuration Firmware: 16.0.0.1012
- PMC Firmware: 160.01.00.1027
- iTBT Firmware: TBT_ADL_MP_ALL_17.1V1_Rel
- IOM Firmware: 22.000c.0.0000
- Retimer Firmware in BIOS capsule: 3.9
- NPHY Firmware: 14.528.505.8210
- Platform Properties Assessment Module: 11.22a.7
- CRB Label: ADL_052
- Boot Guard ACM: 1.18.10
- Bios Guard: 2.0.5021
- Silicon Initialization Code: Based on 0C.00.69.74
- Memory Reference Code: Based on 0.0.4.6
- Integrated Graphics:
    - UEFI Driver: 21.0.1054
- Discrete Graphics:
    - UEFI Driver: 20.1046.0.0
- Intel RST Pre-OS:
    - VMD UEFI Driver: 19.0.0.5428
- AHCI Code: Based on AHCI_30
- Visual BIOS: Intel AptioV

- Supported Flash Devices:

WinBond	W25Q256FV	32MB
GigaDevice	GD25B256D	32MB

- Microcode Updates included in .BIN & .CAP Files:
  M80906A3_00000420.pdb

Feature Change/Update:

1. **Updated: [AMI_Changes] EC FW to v01.09.00**
2. Fixed: [PTK2778] Stack overflow vulnerability in SMI handler.

Known Errata:

1. Supplemental BIOS starts from AC0033 and cannot work on QS K stepping CPU. Please do not flash this BIOS on old platform. If need to build BIOS for K stepping CPU, please modify TOKEN “SUPPLEMENTAL_BOARD_SUPPORT” as 0.
2. Intel signed BIOS and NvRAM locked in AC0037, please do not downgrade BIOS before it.
3. BIOS lock and ME per-lock in AC0043 and cannot flash BIOS by FTP tool.

ACADL357.0056.2022.0803.1442 Development BIOS

About This Release:

- Date: Aug 01, 2022
- ROM Image Checksum: 0xA7496689
- ME Firmware: 16.0.15.1810
- EC Firmware: 1.08.00.000
- PMC Firmware: 160.01.00.1027
- Boot Guard ACM: 1.18.10
- Reference Code: Based on 0C.00.69.74
- Memory Reference Code: Based on 0.0.4.6
- Integrated Graphics:
  - UEFI Driver: 21.0.1054
- Discrete Graphics:
  - UEFI Driver: 20.1046.0.0
- AHCI Code: Based on AHCI_30
- Wired LAN Adapter:
  - UEFI Driver: 0.9.03
- Visual BIOS: Intel AptioV

- Supported Flash Devices:
  - WinBond   W25Q256FV   32MB
  - GigaDevice GD25B256D   32MB

- Microcode Updates included in .BIN & .CAP Files:
  - M80906A3_00000420.pdb

New Fixes/Features:

1. [PTK2703] The arbitrary code execution in DXE driver
2. [PTK2617] SMM memory corruption vulnerability in SMM driver on Intel platforms
3. Remove Undervolting page from Setup
4. System will hang when do recovery.
5. [AMI_Changes]Update CRB to ADL_052

Known Errata:

1. Supplemental BIOS starts from AC0033 and cannot work on QS K stepping CPU. Please do not flash this BIOS on old platform. If need to build BIOS for K stepping CPU, please modify TOKEN “SUPPLEMENTAL_BOARD_SUPPORT” as 0.
2. Intel signed BIOS and NvRAM locked in AC0037, please do not downgrade BIOS before it.
3. BIOS lock and ME per-lock in AC0043 and cannot flash BIOS by FTP tool.

ACADL357.0055.2022.0725.2251 Production BIOS

About This Release:

- Date: July 25 2022
- ROM Image Checksum: 0xA77F1121
- **ME Firmware: 16.0.15.1810 (v5)**
- **EC Firmware: 1.08.00.000**
- PMC Firmware: 160.01.00.1027
- Boot Guard ACM: 1.18.07
- Reference Code: Based on 0C.00.65.70
- Memory Reference Code: Based on 0.0.3.128
- Integrated Graphics:
  - UEFI Driver: 21.0.1054
- Discrete Graphics:
  - UEFI Driver: 20.1046.0.0
- AHCI Code: Based on AHCI_29
- Wired LAN Adapter:
  - UEFI Driver: 0.9.03
- Visual BIOS: Intel AptioV
- Supported Flash Devices:
  - WinBond W25Q256FV 32MB
  - GigaDevice GD25B256D 32MB
- Microcode Updates included in .BIN & .CAP Files:
  - M80906A3_00000420.pdb

New Fixes/Features:
Based on AC0054

- **Updated: [ODM_Changes][BKC WW25] ME FW to 16.0.15.1810 (v5)**
- **Updated: [AMI_Changes] EC FW to v1.08.00.000**

  1. For EC 1.08.00.000:
  Improved Thermal performance.
  Improved DC Boot Battery power.
  Improved CPU/GPU Temperature processed.

Known Errata:

13. Supplemental BIOS starts from AC0033 and does not work on QS K Stepping CPU. DO NOT FLASH this BIOS on older platform. If you need to build BIOS for K stepping CPU, please modify TOKEN “SUPPLEMENTAL_BOARD_SUPPORT” as 0.
14. Intel Signed BIOS and NvRAM locked in AC0037, do not downgrade BIOS to a previous version.
15. BIOS Lock and ME Pre-Lock in AC0043 and cannot flash BIOS using FPT tool.
16. **WU files for test use only.**

ACADL357.0054.2022.0704.2053 Development BIOS

About This Release:

- Date: July 04 2022
- ROM Image Checksum: 0xA779F9FD
- **ME Firmware: 16.0.15.1810**
- **EC Firmware: 1.07.00.000**
- PMC Firmware: 160.01.00.1027
- Boot Guard ACM: 1.18.07
- Reference Code: Based on 0C.00.65.70
- Memory Reference Code: Based on 0.0.3.128
- Integrated Graphics:
  - UEFI Driver: 21.0.1054
- Discrete Graphics:
  - UEFI Driver: 20.1046.0.0
- AHCI Code: Based on AHCI_29
- Wired LAN Adapter:
  - UEFI Driver: 0.9.03
- Visual BIOS: Intel AptioV

- Supported Flash Devices:

WinBond	W25Q256FV	32MB
GigaDevice	GD25B256D	32MB

- Microcode Updates included in .BIN & .CAP Files:
  - M80906A3_00000420.pdb

New Fixes/Features:

1. [ODM_Changes] BIOS mailbox enabled (#723158)
2. [AMI_Changes][EIP None] Separate MCU for K stepping and L stepping in BIOS
3. [AMI_Changes][EIP 688856][Intel/NUC-G][TF][AC][ADL][PTK2699] Fastboot module solution
4. [AMI_Changes][EIP None][Intel][NUC-G][TF][AC] Disable Setup item “USB2 PHY Sus Well Power Gating” for item 2
5. [AMI_Changes][EIP 688683][Intel][NUC-G][TF][AC] Remove jumper system will hang
6. [AMI_Changes][EIP None] Update for the F6 exit MFG mode message.
7. [AMI_Changes][EIP 690967][Intel/NUC-G][TF][AC][ADL][PTK2702] Vulnerability in PEI module.

1. [ODM_Changes] Update ME FW 16.0.15.1810v5 (BKC WW25)

2. [AMI_Changes][EIP None] Update EC to v1.07

For EC 1.07.00.000:

a. Take the place of TccOffset with CpuPL1_Tcc
b. Disable CpuPL1_Tcc @Benchmark
c. Modify GpuPL of SAPC table
d. Modify Peci/OOB GpuPL4
e. Support ecSysPower calculate
f. Modify AC unplug to DC prochot check with ecSysPower
g. Modify SAPC charger current
h. Disable VRT while DTT on

Known Errata:

1. Supplemental BIOS starts from AC0033 and cannot work on QS K stepping CPU. Please do not flash this BIOS on old platform. If need to build BIOS for K stepping CPU, please modify TOKEN “SUPPLEMENTAL_BOARD_SUPPORT” as 0.
2. Intel signed BIOS and NvRAM locked in AC0037, please do not downgrade BIOS before it.
3. BIOS lock and ME per-lock in AC0043 and cannot flash BIOS by FTP tool.
4. **AC0054 based on AC0052 integrate AC0053 display issue solution and other code change.**

ACADL357.0053.2022.0627.1006 Pilot Production BIOS

About This Release:

- Date: Jun 27 2022
- ROM Image Checksum: 0xA7852804
- ME Firmware: 16.0.15.1778
- EC Firmware: 1.04.00.000
- PMC Firmware: 160.01.00.1026
- Boot Guard ACM: 1.18.07
- Reference Code: Based on 0C.00.65.70
- Memory Reference Code: Based on 0.0.3.128
- Integrated Graphics:
  - UEFI Driver: 21.0.1046
- Discrete Graphics:
  - UEFI Driver: 20.1046.0.0
- AHCI Code: Based on AHCI_29
- Wired LAN Adapter:
  - UEFI Driver: 0.9.03
- Visual BIOS: Intel AptioV

- Supported Flash Devices:
  - WinBond W25Q256FV 32MB
  - GigaDevice GD25B256D 32MB

- Microcode Updates included in .BIN & .CAP Files:
  - **M80906A3_00000420.pdb**

New Fixes/Features:

Based on AC0052

- Updated: [AMI Changes] Disable Setup item “USB2 PHY Sus Well Power Gating”.
- **Updated: [AMI Changes][BIOS 0052] Updated CPU L Stepping Only Microcode to M80906A3_00000420.**

Known Errata:

17. Supplemental BIOS starts from AC0033 and does not work on QS K Stepping CPU. DO NOT FLASH this BIOS on older platform. If you need to build BIOS for K stepping CPU, please modify TOKEN “SUPPLEMENTAL_BOARD_SUPPORT” as 0.
18. Intel Signed BIOS and NvRAM locked in AC0037, do not downgrade BIOS to a previous version.
19. BIOS Lock and ME Pre-Lock in AC0043 and cannot flash BIOS using FPT tool.
20. **AC0053 is based on AC0048 and integrates solution for display issue.**
21. **WU files for test use only.**

ACADL357.0052.2022.0622.1910 Development BIOS

About This Release:

- Date: Jun 20 2022
- ROM Image Checksum: 0xA787DAA1
- ME Firmware: 16.0.15.1778
- EC Firmware: 1.06.00.000
- PMC Firmware: 160.01.00.1026
- Boot Guard ACM: 1.18.07
- Reference Code: Based on 0C.00.65.70
- Memory Reference Code: Based on 0.0.3.128
- Integrated Graphics:
  - UEFI Driver: 21.0.1046
- AHCI Code: Based on AHCI_29
- Wired LAN Adapter:
  - UEFI Driver: 0.9.03

- Supported Flash Devices:
  - WinBond W25Q256FV 32MB
  - GigaDevice GD25B256D 32MB

- Microcode Updates included in .BIN & .CAP Files:
  - M80906A3_00000420.pdb

New Fixes/Features:

1. [ODM_Changes] 60ms delay after DG2 off
2. [AMI_Changes][EIP None] Correct L10 sku number
3. [AMI_Changes][EIP None] Some platform has cut string in POST
4. [AMI_Changes][EIP None] Message warning when upgrade results means a downgrade is no possible

Changes:

1. [AMI_Changes][EIP None] Update L stepping MCU to 0x420

Known Errata:

1. Supplemental BIOS starts from AC0033 and cannot work on QS K stepping CPU. Please do not flash this BIOS on old platform. If need to build BIOS for K stepping CPU, please modify TOKEN “SUPPLEMENTAL_BOARD_SUPPORT” as 0.
2. Intel signed BIOS and NvRAM locked in AC0037, please do not downgrade BIOS before it.
3. BIOS lock and ME per-lock in AC0043 and cannot flash BIOS by FPT tool.

ACADL357.0051.2022.0614.0934 Development BIOS

About This Release:

- Date: Jun 13 2022
- ROM Image Checksum: 0xA45CD57D
- ME Firmware: 16.0.15.1778
- EC Firmware: 1.06.00.000
- PMC Firmware: 160.01.00.1026
- Boot Guard ACM: 1.18.07
- Reference Code: Based on 0C.00.65.70
- Memory Reference Code: Based on 0.0.3.128
- Integrated Graphics:
  - UEFI Driver: 21.0.1046
- AHCI Code: Based on AHCI_29
- Wired LAN Adapter:
  - UEFI Driver: 0.9.03
  - N/A
- Supported Flash Devices:
  - WinBond   W25Q256FV   32MB
  - GigaDevice GD25B256D   32MB
- Microcode Updates included in .ROM & .BIO Files:
  - M80906A2_0000030E.pdb
  - M80906A3_0000041C.pdb

New Fixes/Features:

5. [ODM_Changes] Add 60ms delay before DG2 off
6. [AMI_Changes][EIP None] fTPM is not shown at the very first boot with the clean SPI image
7. [AMI_Changes][EIP None] Layout the F6 string.
8. [AMI_Changes][EIP 685711] [Intel][NUC-G][TF][AC] Comment Out The PCON bit11 and bit12 Settings In BIOS Setup

Known Errata:

1. Supplemental BIOS starts from AC0033 and can not work on QS K stepping CPU. Please do not flash this BIOS on old platform. If need to build BIOS for K stepping CPU, please modify TOKEN “SUPPLEMENTAL_BOARD_SUPPORT” as 0.
2. Intel signed BIOS and NvRAM locked in AC0037, please do not downgrade BIOS before it.
3. BIOS lock and ME per-lock in AC0043 and cannot flash BIOS by FTP tool.

ACADL357.0050.2022.0607.1352 Development BIOS

About This Release:

- Date: Jun 06 2022
- ROM Image Checksum: 0xA45C3008
- ME Firmware: 16.0.15.1778
- EC Firmware: 1.06.00.000
- PMC Firmware: 160.01.00.1026
- Boot Guard ACM: 1.18.07
- Reference Code: Based on 0C.00.65.70
- Memory Reference Code: Based on 0.0.3.128
- Integrated Graphics
    - UEFI Driver: 21.0.1046
- AHCI Code: Based on AHCI_29
- Wired LAN Adapter:
    - UEFI Driver: 0.9.03
    - N/A
- Supported Flash Devices:
    - WinBond W25Q256FV 32MB
    - GigaDevice GD25B256D 32MB
- Microcode Updates included in .ROM & .BIO Files:
    - M80906A2_0000030E.pdb
    - M80906A3_0000041C.pdb

New Fixes/Features:

1. [AMI_Changes][EIP None] Support injecting OA3 keys and updating OEMID and OEMTableID at the same time
2. [AMI_Changes][EIP None] Fix system always reset loop after RTC power loss
3. [AMI_Changes][EIP None] Hard coding to modify PC00.PEG0 _S0W to 0, PC00.PEG0.PEGP _S0W to 3

Changes:

1. [AMI_Changes][EIP None] Update EC to v1.06

EC Changes:

For EC 1.06.00.000:

1. Support Gpu DG2 FW Unlock by GPIO

Known Errata:

1. Supplemental BIOS starts from AC0033 and can not work on QS K stepping CPU. Please do not flash this BIOS on old platform. If need to build BIOS for K stepping CPU, please modify TOKEN “SUPPLEMENTAL_BOARD_SUPPORT” as 0.
2. Intel signed BIOS and NvRAM locked in AC0037, please do not downgrade BIOS before it.
3. BIOS lock and ME per-lock in AC0043 and cannot flash BIOS by FTP tool.

ACADL357.0049.2022.0530.2132 Development BIOS

About This Release:

- Date: May 30 2022
- ROM Image Checksum: 0xA464CF52
- ME Firmware: 16.0.15.1778
- EC Firmware: 1.05.00.000
- PMC Firmware: 160.01.00.1026
- Boot Guard ACM: 1.18.07
- Reference Code: Based on 0C.00.65.70
- Memory Reference Code: Based on 0.0.3.128
- Integrated Graphics
  - UEFI Driver: 21.0.1046
- AHCI Code: Based on AHCI_29
- Wired LAN Adapter:
  - UEFI Driver: 0.9.03
  - N/A
- Supported Flash Devices:
  - WinBond W25Q256FV 32MB
  - GigaDevice GD25B256D 32MB
- Microcode Updates included in .ROM & .BIO Files:
  - M80906A2_0000030E.pdb
  - M80906A3_0000041C.pdb

New Fixes/Features:

1. [AMI_Changes][EIP None] Correct NSS memory region
2. [AMI_Changes][EIP None] Fixed CppCheck Error and Waring issues.
3. [AMI_Changes][EIP 682652][Intel][NUC-G][TF][AC] Hidden Power setting items in Power page - Revert re-size bar support setup item

Changes:

1. [AMI_Changes][EIP None] Update EC to v1.05

EC Changes:

For EC 1.05.00.000:

1. Modify Battery Temp Protect point
2. Modify charging LEDModify Battery Temp Protect point

Known Errata:

1. Supplemental BIOS starts from AC0033 and can not work on QS K stepping CPU. Please do not flash this BIOS on old platform. If need to build BIOS for K stepping CPU, please modify TOKEN “SUPPLEMENTAL_BOARD_SUPPORT” as 0.
2. Intel signed BIOS and NvRAM locked in AC0037, please do not downgrade BIOS before it.
3. BIOS lock and ME per-lock in AC0043 and cannot flash BIOS by FTP tool.

ACADL357.0048.2022.0524.1116 Development BIOS

About This Release:

- Date: May 23 2022
- ROM Image Checksum: 0xA463A901
- ME Firmware: 16.0.15.1778
- EC Firmware: 1.04.00.000
- PMC Firmware: 160.01.00.1026
- Boot Guard ACM: 1.18.07
- Reference Code: Based on 0C.00.65.70
- Memory Reference Code: Based on 0.0.3.128
- Integrated Graphics
  - UEFI Driver: 21.0.1046
- AHCI Code: Based on AHCI_29
- Wired LAN Adapter:
  - UEFI Driver: 0.9.03
  - N/A
- Supported Flash Devices:
  - WinBond W25Q256FV 32MB
  - GigaDevice GD25B256D 32MB
- Microcode Updates included in .ROM & .BIO Files:
  - M80906A2_0000030E.pdb
  - M80906A3_0000041C.pdb

New Fixes/Features:

1. [AMI_Changes][EIP None] Update Setup stddefault value
2. [AMI_Changes][EIP 682652][Intel][NUC-G][TF][AC] Hidden Power setting items in Power page
3. [AMI_Changes][EIP 682460][Intel][NUC-G][TF][AC] BlueTooth is not disable when Disable WLAN setup item.

Changes:

1. [AMI_Changes][EIP None] Update EC to v1.04

EC Changes:

For EC 1.04.00.000:

1. Modify/Enable VR Thermal Alert protect
2. Modify to avoid charging LED on @DC
3. Modify Tcc offset
4. Modify Battery Temp Protect point
5. Reset Modern Standby flag (factory checking) when MODS start

Known Errata:

1. Supplemental BIOS starts from AC0033 and can not work on QS K stepping CPU. Please do not flash this BIOS on old platform. If need to build BIOS for K stepping CPU, please modify TOKEN “SUPPLEMENTAL_BOARD_SUPPORT” as 0.
2. Intel signed BIOS and NvRAM locked in AC0037, please do not downgrade BIOS before it.
3. BIOS lock and ME per-lock in AC0043 and cannot flash BIOS by FTP tool.

ACADL357.0047.2022.0516.2050 Development BIOS

About This Release:

- Date: May 16 2022
- ROM Image Checksum: 0xA4624B07
- ME Firmware: 16.0.15.1778
- EC Firmware: 1.03.00.000
- PMC Firmware: 160.01.00.1026
- Boot Guard ACM: 1.18.07
- Reference Code: Based on 0C.00.65.70
- Memory Reference Code: Based on 0.0.3.128
- Integrated Graphics
  - UEFI Driver: 21.0.1046
- AHCI Code: Based on AHCI_29
- Wired LAN Adapter:
  - UEFI Driver: 0.9.03
  - N/A
- Supported Flash Devices:
  - WinBond   W25Q256FV   32MB
  - GigaDevice GD25B256D   32MB
- Microcode Updates included in .ROM & .BIO Files:
  - M80906A2_0000030E.pdb
  - M80906A3_0000041C.pdb

New Fixes/Features:

1. [ODM_Changes] Memory corruption vulnerability on Intel platforms PTK2616
2. [ODM_Changes] Sync up with SN for long run setting
3. [ODM_Changes] Directed FX System Verification Test fail
4. [AMI_Changes][EIP 681406][Intel][NUC-G][TF][AC] BIOS setup item default modify
5. [AMI_Changes][EIP 680831][Intel/NUC-G][TF][AC][ADL][PTK1433] PEI memory corruption on server boards and on majority of NUCsTF

Changes:

1. [ODM_Changes] Update ME FW 16.0.15.1778v3 (BKC WW18)
2. [AMI_Changes][EIP None] Update L stepping MCU to 41C
3. [AMI_Changes][EIP None] Update EC to v1.03

EC Changes:

For EC 1.03.00.000:

1. Modify SAPC PL (Disable DC Protect)
2. Modify Throttling Protect
3. Modify Battery Temp Protect
4. Modify GPU PLx Reset after Gpu Off
5. Modify Tccoffset
6. Support Gpu PL4
7. Enable Efficiency Turbo @Battery Saver
8. Disable VR Thermal Alert

Known Errata:

1. Supplemental BIOS starts from AC0033 and can not work on QS K stepping CPU. Please do not flash this BIOS on old platform. If need to build BIOS for K stepping CPU, please modify TOKEN “SUPPLEMENTAL_BOARD_SUPPORT” as 0.
2. Intel signed BIOS and NvRAM locked in AC0037, please do not downgrade BIOS before it.
3. BIOS lock and ME per-lock in AC0043 and cannot flash BIOS by FTP tool.

ACADL357.0046.2022.0509.1913 Development BIOS

About This Release:

- Date: May 09 2022
- ROM Image Checksum: 0xA4747D42
- ME Firmware: 16.0.15.1735
- EC Firmware: 1.02.00.000
- PMC Firmware: 160.01.00.1023
- Boot Guard ACM: 1.18.07
- Reference Code: Based on 0C.00.65.70
- Memory Reference Code: Based on 0.0.3.128
- Integrated Graphics
  - UEFI Driver: 21.0.1046
- AHCI Code: Based on AHCI_29
- Wired LAN Adapter:
  - UEFI Driver: 0.9.03
  - N/A
- Supported Flash Devices:
  - WinBond W25Q256FV 32MB
  - GigaDevice GD25B256D 32MB
- Microcode Updates included in .ROM & .BIO Files:
  - M80906A2_0000030E.pdb
  - M80906A3_00000416.pdb

New Fixes/Features:

1. [ODM_Changes] Disable Hot plug support in VBT for fixed plugged in HDMI the panel will flicker issue.
2. [AMI_Changes][EIP None] BIOS Warning message during BIOS WU.
3. [AMI_Changes][EIP None] Force enable Tco Timers

Changes:

1. [AMI_Changes][EIP None] Update EC to v1.02

EC Changes:

For EC 1.02.00.000:

1. Modify DC PL
2. Modify Battery Temp Protect
3. Fix Modern Standby wake up @BatTemp protect
4. Fix Jp Keyboard table
5. Fix key repeat @Setup menu

Known Errata:

1. Supplemental BIOS starts from AC0033 and can not work on QS K stepping CPU. Please do not flash this BIOS on old platform. If need to build BIOS for K stepping CPU, please modify TOKEN “SUPPLEMENTAL_BOARD_SUPPORT” as 0.
2. Intel signed BIOS and NvRAM locked in AC0037, please do not downgrade BIOS before it.
3. BIOS lock and ME per-lock in AC0043 and cannot flash BIOS by FTP tool.

ACADL357.0045.2022.0429.1927 Development BIOS

About This Release:

- Date: Apr 29 2022
- ROM Image Checksum: 0xA473FF9B
- ME Firmware: 16.0.15.1735
- EC Firmware: 1.01.00.000
- PMC Firmware: 160.01.00.1023
- Boot Guard ACM: 1.18.07
- Reference Code: Based on 0C.00.65.70
- Memory Reference Code: Based on 0.0.3.128
- Integrated Graphics
  - UEFI Driver: 21.0.1046
- AHCI Code: Based on AHCI_29
- Wired LAN Adapter:
  - UEFI Driver: 0.9.03
  - N/A
- Supported Flash Devices:
  - WinBond W25Q256FV 32MB
  - GigaDevice GD25B256D 32MB
- Microcode Updates included in .ROM & .BIO Files:
  - M80906A2_0000030E.pdb
  - M80906A3_00000416.pdb

New Fixes/Features:

1. [AMI_Changes][EIP None]Revert EIP660942 for not lock MSR 601h and 610h
2. [AMI_Changes][EIP 678685][Intel][NUC-G][TF][AC] Plug-in AC will auto power on after load default
3. [AMI_Changes][EIP None] Force reboot after exit Setup

Changes:

1. N/A

EC Changes:

N/A

Known Errata:

1. Supplemental BIOS starts from AC0033 and can not work on QS K stepping CPU. Please do not flash this BIOS on old platform. If need to build BIOS for K stepping CPU, please modify TOKEN "SUPPLEMENTAL_BOARD_SUPPORT" as 0.
2. Intel signed BIOS and NvRAM locked in AC0037, please do not downgrade BIOS before it.
3. BIOS lock and ME per-lock in AC0043 and cannot flash BIOS by FTP tool.

ACADL357.0044.2022.0427.1818 Development BIOS

About This Release:

- Date: Apr 25 2022
- ROM Image Checksum: 0xA47A4EB8
- ME Firmware: 16.0.15.1735
- EC Firmware: 1.01.00.000
- PMC Firmware: 160.01.00.1023
- Boot Guard ACM: 1.18.07
- Reference Code: Based on 0C.00.65.70
- Memory Reference Code: Based on 0.0.3.128
- Integrated Graphics
  - UEFI Driver: 21.0.1046
- AHCI Code: Based on AHCI_29
- Wired LAN Adapter:
  - UEFI Driver: 0.9.03
  - N/A
- Supported Flash Devices:
  - WinBond W25Q256FV 32MB
  - GigaDevice GD25B256D 32MB
- Microcode Updates included in .ROM & .BIO Files:
  - M80906A2_0000030E.pdb
  - M80906A3_00000416.pdb

New Fixes/Features:

1. [AMI_Changes][EIP 677069][Intel/NUC-G][TF][AC] ASPM setting of PCIE PEG port
2. [AMI_Changes][EIP None] Correct PCIe storage device _S0W

Changes:

1. [AMI_Changes][EIP None] Update EC to v1.00
2. [AMI_Changes][EIP None] Update EC to v1.01

EC Changes:

For EC 1.00.00.000:
1. Modify SAPC PL
2. Modify BatSav mode Fan Table
3. Fix Prochot clear once AC plug in
4. Disable Auto MPS updated with version check

For EC 1.01.00.000:
1. Modify SAPC PL
2. Modify Fan Table
3. Modify VR Thermal Alert protect

Known Errata:

1. Supplemental BIOS starts from AC0033 and can not work on QS K stepping CPU. Please do not flash this BIOS on old platform. If need to build BIOS for K stepping CPU, please modify TOKEN “SUPPLEMENTAL_BOARD_SUPPORT” as 0.
2. Intel signed BIOS and NvRAM locked in AC0037, please do not downgrade BIOS before it.
3. BIOS lock and ME per-lock in AC0043 and cannot flash BIOS by FTP tool.

ACADL357.0043.2022.0419.1618 Development BIOS

About This Release:

- Date: Apr 19 2022
- ROM Image Checksum: 0xA472F55D
- ME Firmware: 16.0.15.1735
- EC Firmware: 0.44.00.000
- PMC Firmware: 160.01.00.1023
- Boot Guard ACM: 1.18.07
- Reference Code: Based on 0C.00.65.70
- Memory Reference Code: Based on 0.0.3.128
- Integrated Graphics
  - UEFI Driver: 21.0.1046
- AHCI Code: Based on AHCI_29
- Wired LAN Adapter:
  - UEFI Driver: 0.9.03
  - N/A
- Supported Flash Devices:
  - WinBond   W25Q256FV   32MB
  - GigaDevice GD25B256D   32MB
- Microcode Updates included in .ROM & .BIO Files:
  - M80906A2_0000030E.pdb
  - M80906A3_00000416.pdb

New Fixes/Features:

1. [AMI_Changes][EIP 671005][Intel][NUC-G][TF][AC] When press F9 load default, F2 can't work
2. [AMI_Changes][EIP 674716] EIP674716 Reduce POST time when i225 PXE boot is enabled.
3. [AMI_Changes][EIP None] Common solution for system hangs during boot if NVRAM is exactly full
4. [AMI_Changes][EIP 668189][Intel][NUC-G][TF][AC] Hidden unknown device in Device Manager
5. [AMI_Changes][EIP 660942][Intel][NUC-G][TF][AC] Modify single core CPU, the frequency can't up to 4.7Mhz
6. [AMI_Changes][EIP 649515][Intel/NUC-G][TF][AC][PT_WHQL] Modern Standby Basic Requirement Test on ACDC-power Source fail
7. [AMI_Changes][EIP None] Enable BIOS lock and ME per lock

Changes:

1. [AMI_Changes][EIP None] Update EC to v0.43
2. [AMI_Changes][EIP None] Update EC to v0.44

EC Changes:

For EC 0.43.00.000:

1. Modify SAPC PL
2. Modify Fan Table
3. Modify Tthrottling Protect
4. Modify Remote Temp Over Protect (CC33)
5. Modify Thermal Safety Mode Protect
6. Support VR Thermal Alert
7. Workaround for KB abnormal no work
8. Delay power sequence PCH_PWOK 500ms

For EC 0.44.00.000:

1. Modify SAPC PL
2. Modify Throttling Protect

Known Errata:

1. Supplemental BIOS starts from AC0033 and can not work on QS K stepping CPU. Please do not flash this BIOS on old platform. If need to build BIOS for K stepping CPU, please modify TOKEN “SUPPLEMENTAL_BOARD_SUPPORT” as 0.
2. Intel signed BIOS and NvRAM locked in AC0037, please do not downgrade BIOS before it.
3. **BIOS lock and ME per-lock in this version. Please update BIOS by FPT to lock ME.**

ACADL357.0042.2022.0411.2110 Development BIOS

About This Release:

- Date: Apr 11 2022
- ROM Image Checksum: 0xA4826925
- ME Firmware: 16.0.15.1735
- EC Firmware: 0.42.00.000
- PMC Firmware: 160.01.00.1023
- Boot Guard ACM: 1.18.07
- Reference Code: Based on 0C.00.65.70
- Memory Reference Code: Based on 0.0.3.128
- Integrated Graphics
  - UEFI Driver: 21.0.1046
- AHCI Code: Based on AHCI_29
- Wired LAN Adapter:
  - UEFI Driver: 0.9.03
  - N/A
- Supported Flash Devices:
  - WinBond W25Q256FV 32MB
  - GigaDevice GD25B256D 32MB
- Microcode Updates included in .ROM & .BIO Files:
  - M80906A2_0000030E.pdb
  - M80906A3_00000416.pdb

New Fixes/Features:

1. [AMI_Changes][EIP None] Change SSID setting

Changes:

1. [AMI_Changes][EIP None] Update EC to v0.42

EC Changes:

For EC 0.42.00.000:

1. Update PD fw (3.01)(WHQL UCSI commands - Get Alternate Modes, SOP-DoublePrime failed)
2. Support VR Thermal Alert
3. Disable USB Retimer patch
4. Delay QEvent @Gpu Off->On avoid QEvent while power off
5. Modify Tcc offset switch by Gpu Temp (instead Gpu On/Off)

Known Errata:

1. Supplemental BIOS starts from AC0033 and can not work on QS K stepping CPU. Please do not flash this BIOS on old platform. If need to build BIOS for K stepping CPU, please modify TOKEN “SUPPLEMENTAL_BOARD_SUPPORT” as 0.
2. **Intel signed BIOS and NvRAM locked in AC0037, please do not downgrade BIOS before it.**

ACADL357.0041.2022.0406.1530 Development BIOS

About This Release:

- Date: Apr 06 2022
- ROM Image Checksum: 0xA47862AE
- ME Firmware: 16.0.15.1735
- EC Firmware: 0.41.00.000
- PMC Firmware: 160.01.00.1023
- Boot Guard ACM: 1.18.07
- Reference Code: Based on 0C.00.65.70
- Memory Reference Code: Based on 0.0.3.128
- Integrated Graphics
  - UEFI Driver: 21.0.1046
- AHCI Code: Based on AHCI_29
- Wired LAN Adapter:
  - UEFI Driver: 0.9.03
  - N/A
- Supported Flash Devices:
  - WinBond W25Q256FV 32MB
  - GigaDevice GD25B256D 32MB
- Microcode Updates included in .ROM & .BIO Files:
  - M80906A2_0000030E.pdb
  - M80906A3_00000416.pdb

New Fixes/Features:

1. [AMI_Changes][EIP None] Fix build fail when disable bios guard
2. [AMI_Changes][EIP 662085][Intel][NUC-G][TF][AC] BlInitializeLibrary failed 0xc0000001 Error message still seen if exiting BIOS without saving
3. [AMI_Changes][EIP None] Load safe setting porting

Changes:

1. [AMI_Changes][EIP None] Update EC to v0.41

EC Changes:

For EC 0.41.00.000:

1. Modify Support Crucial DDR5
2. Modify SAPC PL
3. Disable PD FW1 Updated

Known Errata:

1. Supplemental BIOS starts from AC0033 and can not work on QS K stepping CPU. Please do not flash this BIOS on old platform. If need to build BIOS for K stepping CPU, please modify TOKEN “SUPPLEMENTAL_BOARD_SUPPORT” as 0.
2. **Intel signed BIOS and NvRAM locked in AC0037, please do not downgrade BIOS before it.**

ACADL357.0040.2022.0328.2028 Development BIOS

About This Release:

- Date: Mar 28 2022
- ROM Image Checksum: 0xA47C1C00
- ME Firmware: 16.0.15.1735
- EC Firmware: 0.36.00.000
- PMC Firmware: 160.01.00.1023
- Boot Guard ACM: 1.18.07
- Reference Code: Based on 0C.00.65.70
- Memory Reference Code: Based on 0.0.3.128
- Integrated Graphics
  - UEFI Driver: 21.0.1046
- AHCI Code: Based on AHCI_29
- Wired LAN Adapter:
  - UEFI Driver: 0.9.03
  - N/A
- Supported Flash Devices:
  - WinBond W25Q256FV 32MB
  - GigaDevice GD25B256D 32MB
- Microcode Updates included in .ROM & .BIO Files:
  - M80906A2_0000030E.pdb
  - M80906A3_00000416.pdb

New Fixes/Features:

1. [ODM_Changes] Update WLAN power table (SAR)
2. [ODM_Changes] Modify CPU tau value to 64
3. [AMI_Changes][EIP 668637][Intel][NUC-G][TF][AC] BIOS setup no intel DG2 information and Frequency
4. [AMI_Changes][EIP 642482][Intel][NUC-G][TF][AC] Host NVM Update is fail.
5. [AMI_Changes][EIP None] Correct ME version in K0 stepping

Changes:

1. [AMI_Changes][EIP None] Update EC to v0.36
2. [AMI_Changes][EIP None] Update CRB to ADL_040

EC Changes:

For EC 0.36.00.000:

1. Update PD fw (3.00)
2. Support Power Menu LED
3. Support Fn Lock @Shell mode
4. Support PL in difference three mode @DC
5. Modify PL @AC
6. Modify TccOffset
7. Enable PD FW1 Updated

Known Errata:

1. AC will reboot 4 or 5 times after flash BIOS for rebuild NVRAM and this situation will be gone in PP stage.
2. Supplemental BIOS starts from AC0033 and can not work on QS K stepping CPU. Please do not flash this BIOS on old platform. If need to build BIOS for K stepping CPU, please modify TOKEN “SUPPLEMENTAL_BOARD_SUPPORT” as 0.
3. **Intel signed BIOS and NvRAM locked in AC0037, please do not downgrade BIOS before it.**

ACADL357.0039.2022.0321.1941 Development BIOS

About This Release:

- Date: Mar 21 2022
- ROM Image Checksum: 0xA4B3781D
- ME Firmware: 16.0.15.1735
- EC Firmware: 0.35.00.000
- PMC Firmware: 160.01.00.1023
- Boot Guard ACM: 1.18.07
- Reference Code: Based on 0C.00.65.70
- Memory Reference Code: Based on 0.0.3.96
- Integrated Graphics
  - UEFI Driver: 21.0.1046
- AHCI Code: Based on AHCI_29
- Wired LAN Adapter:
  - UEFI Driver: 0.9.03
  - N/A
- Supported Flash Devices:
  - WinBond W25Q256FV 32MB
  - GigaDevice GD25B256D 32MB
- Microcode Updates included in .ROM & .BIO Files:
  - M80906A2_0000030E.pdb
  - M80906A3_00000416.pdb

New Fixes/Features:

1. [ODM_Changes] Modify debug token setting
2. [AMI_Changes][EIP None] Update Boot Guard ACM for QS/production sku
3. [AMI_Changes][EIP None] Fix system will trigger WDT after enter power button menu

Changes:

1. [AMI_Changes][EIP None] Update EC to v0.35

EC Changes:

For EC 0.35.00.000:

1. Modify OOB PLx & CpuTemp
2. Modify PECI PLx & GpuTemp
3. Modify SAPC PLx
4. Modify TccOffset
5. Modify CPU/GPU Throttling point
6. Disable KB Back Light @LidClose
7. Update MPS GPU_2979_V7/GPU_2950_V9
8. Support AP override PL @DC

Known Errata:

1. AC will reboot 4 or 5 times after flash BIOS for rebuild NVRAM and this situation will be gone in PP stage.
2. Supplemental BIOS starts from AC0033 and can not work on QS K stepping CPU. Please do not flash this BIOS on old platform. If need to build BIOS for K stepping CPU, please modify TOKEN “SUPPLEMENTAL_BOARD_SUPPORT” as 0.
3. **Intel signed BIOS and NvRAM locked in AC0037, please do not downgrade BIOS before it.**

ACADL357.0038.2022.0314.1823 Development BIOS

About This Release:

- Date: Mar 14 2022
- ROM Image Checksum: 0xA4B3BD62
- ME Firmware: 16.0.15.1735
- EC Firmware: 0.34.00.000
- PMC Firmware: 160.01.00.1023
- Boot Guard ACM: 1.18.07
- Reference Code: Based on 0C.00.65.70
- Memory Reference Code: Based on 0.0.3.96
- Integrated Graphics
  - UEFI Driver: 21.0.1046
- AHCI Code: Based on AHCI_29
- Wired LAN Adapter:
  - UEFI Driver: 0.9.03
  - N/A
- Supported Flash Devices:
  - WinBond W25Q256FV 32MB
  - GigaDevice GD25B256D 32MB
- Microcode Updates included in .ROM & .BIO Files:
  - M80906A2_0000030E.pdb
  - M80906A3_00000416.pdb

New Fixes/Features:

1. [ODM_Changes] Update ME FW 16.0.15.1735v1.1 (BKC WW09)
2. [ODM_Changes] Update WLAN power table (SAR)
3. [ODM_Changes] Fixed Right USB2.0 can't work.
4. [AMI_Changes][EIP 668663][Intel][NUC-G][TF][AC] USB information not correct
5. [AMI_Changes][EIP None]Setup "exit & boot" page should not be hidden
6. [AMI_Changes][EIP 668642][Intel][NUC-G][TF][AC] iSetupCfg Password Check and Fast Boot default setting

Changes:

1. [AMI_Changes][EIP None] Update EC to v0.34

EC Changes:

For EC 0.34.00.000:

1. Support APP to set GPU PECI PL1/2
2. Support Read GPU PECI PL1/2
3. Fix GPU PECI PL1/2 not setting @AC boot
4. Add GPU Temp && GPU PECI PL1/2 retry
5. Modify PECI Read/Write Time Sharing
6. Modify GPU PL1/2 value @230W/180W
7. Modify Thermal Safety/FanLock/Remote protect
8. Modify DC Suicide to avoid power button on
9. Reset OOB PECI PLx Index @S5
10. Fix Battery saver mode efficient turbo @DC
11. Fix JP KB Alt
12. Disable PD FW1 Updated

Known Errata:

1. AC will reboot 4 or 5 times after flash BIOS for rebuild NVRAM and this situation will be gone in PP stage.
2. Supplemental BIOS starts from AC0033 and can not work on QS K stepping CPU. Please do not flash this BIOS on old platform. If need to build BIOS for K stepping CPU, please modify TOKEN “SUPPLEMENTAL_BOARD_SUPPORT” as 0.
3. **Intel signed BIOS and NvRAM locked in AC0037, please do not downgrade BIOS**

before it.

ACADL357.0037.2022.0308.1520 Development BIOS

About This Release:

- Date: Mar 08 2022
- ROM Image Checksum: 0xA4B5A3CB
- ME Firmware: 16.0.15.1662
- EC Firmware: 0.33.00.000
- PMC Firmware: 160.01.00.1019
- Boot Guard ACM: 1.18.07
- Reference Code: Based on 0C.00.65.70
- Memory Reference Code: Based on 0.0.3.96
- Integrated Graphics
  - UEFI Driver: 21.0.1046
- AHCI Code: Based on AHCI_29
- Wired LAN Adapter:
  - UEFI Driver: 0.9.03
  - N/A
- Supported Flash Devices:
  - WinBond W25Q256FV 32MB
  - GigaDevice GD25B256D 32MB
- Microcode Updates included in .ROM & .BIO Files:
  - M80906A2_0000030E.pdb
  - M80906A3_00000416.pdb

New Fixes/Features:

1. [ODM_Changes] Change EC to use H2RAM
2. [ODM_Changes] Support debug token function
3. [ODM_Changes] Update WLAN power table (SAR)
4. [AMI_Changes][EIP None] Update for the re-sign package.
5. [AMI_Changes][EIP None] WA for SUT hang if TP is not connected.
6. [AMI_Changes][EIP None] Reserve setup structure for NVRAM lock
7. [AMI_Changes][EIP None] CRB Setup need to be hidden when ESA interface enable

Changes:

1. [AMI_Changes][EIP None] Update BiosGuard to BiosGuard_032
2. [AMI_Changes][EIP None] Update EC to v0.33

EC Changes:

For EC 0.33.00.000:

1. Support PD multi zone Updated (update Boot loader table)
2. Updated PD FW1
3. Modify ROM MEMORY load default with Signature magic key
4. Workaround for DG2 reset @Sleep
5. Modify SAPC DG2 PL table
6. Modify Thermal Safety protect
7. Modify Power on Fan up for noise

Known Errata:

1. Because boot guard and BIOS guard is enabled in AC0009, please use FPT tool update BIOS from AC0008 and previous versions to this version for avoid any unexpected behavior.
2. Please do not downgrade BIOS to AC0008 and previous versions by F7/exe/iflashV to avoid any unexpected behavior.
3. AC will reboot 4 or 5 times after flash BIOS for rebuild NVRAM and this situation will be gone in PP stage.
4. AC formal BIOS is QS SKU BIOS in AC0024, please do not flash BIOS from AC0023 and above.
5. Supplemental BIOS starts from AC0033 and can not work on QS K stepping CPU. Please do not flash this BIOS on old platform. If need to build BIOS for K stepping CPU, please modify TOKEN “SUPPLEMENTAL_BOARD_SUPPORT” as 0.
6. **AC0037 is Intel signed BIOS and NvRAM is locked, please only update BIOS to this version by FPT tool for avoid any unexpected issue and do not downgrade BIOS from this version.**

ACADL357.0036.2022.0225.2209 Development BIOS

About This Release:

- Date: Feb 25 2022
- ROM Image Checksum: 0xA4B7E096
- ME Firmware: 16.0.15.1662
- EC Firmware: 0.32.00.000
- PMC Firmware: 160.01.00.1019
- Boot Guard ACM: 1.18.07
- Reference Code: Based on 0C.00.65.70
- Memory Reference Code: Based on 0.0.3.96
- Integrated Graphics
  - UEFI Driver: 21.0.1046
- AHCI Code: Based on AHCI_29
- Wired LAN Adapter:
  - UEFI Driver: 0.9.03
  - N/A
- Supported Flash Devices:
  - WinBond   W25Q256FV   32MB
  - GigaDevice GD25B256D   32MB
- Microcode Updates included in .ROM & .BIO Files:
  - M80906A2_0000030E.pdb
  - M80906A3_00000416.pdb

New Fixes/Features:

1. [AMI_Changes][EIP 665589][Intel][NUC-G][TF][AC] Include SSID module

Changes:

1. N/A

EC Changes:

1. N/A

Known Errata:

1. Because boot guard and BIOS guard is enabled in AC0009, please use FPT tool update BIOS from AC0008 and previous versions to this version for avoid any unexpected behavior.
2. Please do not downgrade BIOS to AC0008 and previous versions by F7/exe/iflashV to avoid any unexpected behavior.
3. AC will reboot 4 or 5 times after flash BIOS for rebuild NVRAM and this situation will be gone in PP stage.
4. AC formal BIOS is QS SKU BIOS in AC0024, please do not flash BIOS from AC0023 and above.
5. **Supplemental BIOS starts from AC0033 and can not work on QS K stepping CPU. Please do not flash this BIOS on old platform. If need to build BIOS for K stepping CPU, please modify TOKEN "SUPPLEMENTAL_BOARD_SUPPORT" as 0.**

ACADL357.0035.2022.0221.XXXX Development BIOS

About This Release:

- Date: Feb 21 2022
- ROM Image Checksum: 0xA4B9D10E
- ME Firmware: 16.0.15.1662
- EC Firmware: 0.31.00.000
- PMC Firmware: 160.01.00.1019
- Boot Guard ACM: 1.18.07
- Reference Code: Based on 0C.00.65.70
- Memory Reference Code: Based on 0.0.3.96
- Integrated Graphics
  - UEFI Driver: 21.0.1046
- AHCI Code: Based on AHCI_29
- Wired LAN Adapter:
  - UEFI Driver: 0.9.03
  - N/A
- Supported Flash Devices:
  - WinBond W25Q256FV 32MB
  - GigaDevice GD25B256D 32MB
- Microcode Updates included in .ROM & .BIO Files:
  - M80906A2_0000030E.pdb
  - M80906A3_00000416.pdb

New Fixes/Features:

1. [ODM_Changes] Disable DTT setting
2. [AMI_Changes][EIP None] Fix supplemental QS BIOS include wrong ME

Changes:

1. [AMI_Changes][EIP None] Update EC to v0.32
2. [AMI_Changes][EIP 665643][Intel/NUC-G][TF][AC] DBIOS for CRB038 update
3. [AMI_Changes][EIP None] Update L stepping MCU to 416

EC Changes:

For EC 0.32.00.000:

1. Update PD fw (2.00) (New SDK)
2. Modify GPIO for Fab D MB
3. Modify ROM Memory Load Default (Timing & Rom Writing)
4. Modify Power Mode no reset @S5/Restart

Known Errata:

1. Because boot guard and BIOS guard is enabled in AC0009, please use FPT tool update BIOS from AC0008 and previous versions to this version for avoid any unexpected behavior.
2. Please do not downgrade BIOS to AC0008 and previous versions by F7/exe/iflashV to avoid any unexpected behavior.
3. AC will reboot 4 or 5 times after flash BIOS for rebuild NVRAM and this situation will be gone in PP stage.
4. AC formal BIOS is QS SKU BIOS in AC0024, please do not flash BIOS from AC0023 and above.
5. **Supplemental BIOS starts from AC0033 and can not work on QS K stepping CPU. Please do not flash this BIOS on old platform. If need to build BIOS for K stepping CPU, please modify TOKEN "SUPPLEMENTAL_BOARD_SUPPORT" as 0.**

ACADL357.0034.2022.0214.XXXX Development BIOS

About This Release:

- Date: Feb 14 2022
- ROM Image Checksum: 0xA4CBE656
- ME Firmware: 16.0.15.1662
- EC Firmware: 0.31.00.000
- PMC Firmware: 160.01.00.1016
- Boot Guard ACM: 1.18.07
- Reference Code: Based on 0C.00.65.70
- Memory Reference Code: Based on 0.0.3.74
- Integrated Graphics
  - UEFI Driver: 21.0.1046
- AHCI Code: Based on AHCI_29
- Wired LAN Adapter:
  - UEFI Driver: 0.9.03
  - N/A
- Supported Flash Devices:
  - WinBond W25Q256FV 32MB
  - GigaDevice GD25B256D 32MB
- Microcode Updates included in .ROM & .BIO Files:
  - M80906A2_0000030E.pdb
  - M80906A3_00000413.pdb

New Fixes/Features:

1. [AMI_Changes][EIP None] Add common solution for blank Line ESA issue

Changes:

1. [AMI_Changes][EIP None] Update EC to v0.31

EC Changes:

For EC 0.31.00.000:
1. Support Read MPS temperature
2. Support monitor CPU Thermal trip to force shutdown.
3. Modify Low Bat Breath LED @Modern Standby
4. Fix Cpu/Gpu Temp Tthrottling release lock

Known Errata:

1. Because boot guard and BIOS guard is enabled in AC0009, please use FPT tool update BIOS from AC0008 and previous versions to this version for avoid any unexpected behavior.
2. Please do not downgrade BIOS to AC0008 and previous versions by F7/exe/iflashV to avoid any unexpected behavior.
3. AC will reboot 4 or 5 times after flash BIOS for rebuild NVRAM and this situation will be gone in PP stage.
4. AC formal BIOS is QS SKU BIOS in AC0024, please do not flash BIOS from AC0023 and above.
5. DTT is enabled in AC0030 which cause CPU frequency will be 400 MHz.
6. **Supplemental BIOS starts from AC0033 and can not work on QS K stepping CPU. Please do not flash this BIOS on old platform. If need to build BIOS for K stepping CPU, please modify TOKEN "SUPPLEMENTAL_BOARD_SUPPORT" as 0.**

ACADL357.0033.2022.0207.XXXX Development BIOS

About This Release:

- Date: Feb 07 2022
- ROM Image Checksum: 0xA4CF0C73
- ME Firmware: 16.0.15.1662
- EC Firmware: 0.30.00.000
- PMC Firmware: 160.01.00.1016
- Boot Guard ACM: 1.18.07
- Reference Code: Based on 0C.00.65.70
- Memory Reference Code: Based on 0.0.3.74
- Integrated Graphics
  - UEFI Driver: 21.0.1046
- AHCI Code: Based on AHCI_29
- Wired LAN Adapter:
  - UEFI Driver: 0.9.03
  - N/A
- Supported Flash Devices:
  - WinBond   W25Q256FV   32MB
  - GigaDevice GD25B256D   32MB
- Microcode Updates included in .ROM & .BIO Files:
  - M80906A2_0000030E.pdb
  - M80906A3_00000413.pdb

New Fixes/Features:

1. [ODM_Changes] Update BKC WW03
2. [ODM_Changes] Fixed PL1/2/4 value when DTT Enable
3. [ODM_Changes] If receive PLx=0 form EC, write PLx value to maximum
4. [AMI_Changes][EIP 659836][Intel][NUC-G][TF][AC] BIOS setup item "PCIE Resizable BAR Support" moves to previous page
5. [AMI_Changes][EIP None] Add supplemental BIOS support

Changes:

1. [AMI_Changes][EIP None] Update EC to v0.30

EC Changes:

For EC 0.30.00.000:

1. Fix PL12 Lock after LCD Display Off
2. Fix WHQL "Modern Standby Check Thermal Zones"
3. Modify BatI Throttling to improve DC drop
4. Modify Low PL DC boot
5. Delay Q70 2sec avoid Q70 too often @ApcOn PL change often

Known Errata:

1. Because boot guard and BIOS guard is enabled in AC0009, please use FPT tool update BIOS from AC0008 and previous versions to this version for avoid any unexpected behavior.
2. Please do not downgrade BIOS to AC0008 and previous versions by F7/exe/iflashV to avoid any unexpected behavior.
3. AC will reboot 4 or 5 times after flash BIOS for rebuild NVRAM and this situation will be gone in PP stage.
4. AC formal BIOS is QS SKU BIOS in AC0024, please do not flash BIOS from AC0023 and above.
5. DTT is enabled in AC0030 which cause CPU frequency will be 400 MHz.
6. **AC0033 is supplemental BIOS and can not work on QS K stepping CPU. Please do not flash this BIOS on old platform. If need to build BIOS for K stepping CPU, please modify TOKEN "SUPPLEMENTAL_BOARD_SUPPORT" as 0.**

ACADL357.0032.2022.0124.2008 Development BIOS

About This Release:

- Date: Jan 24 2022
- ROM Image Checksum: 0xA4D6F964
- ME Firmware: 16.0.15.1620
- EC Firmware: 0.29.00.000
- PMC Firmware: 160.01.00.1016
- Boot Guard ACM: 1.18.07
- Reference Code: Based on 0C.00.65.70
- Memory Reference Code: Based on 0.0.3.74
- Integrated Graphics
  - UEFI Driver: 21.0.1044
- AHCI Code: Based on AHCI_29
- Wired LAN Adapter:
  - UEFI Driver: 0.9.03
  - N/A
- Supported Flash Devices:
  - WinBond W25Q256FV 32MB
  - GigaDevice GD25B256D 32MB
- Microcode Updates included in .ROM & .BIO Files:
  - M80906A2_0000030E.pdb
  - M80906A3_00000413.pdb

New Fixes/Features:

1. [AMI_Changes][EIP None] Update common solution for in setup of TCG Storage device Security Configuration page to set user password, password cannot be processed by “Enter” prompt.

Changes:

1. [AMI_Changes][EIP None] Update EC to v0.29
2. [ODM_Changes] Update ME FW 16.0.15.1620v3.2 (BKC WW02)

EC Changes:

For EC 0.29.00.000:

1. Modify Modern Standby
2. Modify Smart APC table && GPUPL12 adjust @ApcOn
3. Modify Throttling protect
4. Disable Q70 @DTT On
5. Enable Thermo Fanlock & RemoteTemp Protect
6. Create WarmBootLock Count
7. Reset Power Sense state @S5 @Warmboot
8. Patch SWG Battery error count RET

Known Errata:

7. Because boot guard and BIOS guard is enabled in AC0009, please use FPT tool update BIOS from AC0008 and previous versions to this version for avoid any unexpected behavior.
8. Please do not downgrade BIOS to AC0008 and previous versions by F7/exe/iflashV to avoid any unexpected behavior.
9. AC will reboot 4 or 5 times after flash BIOS for rebuild NVRAM and this situation will be gone in PP stage.
10. AC formal BIOS is QS SKU BIOS in AC0024, please do not flash BIOS from AC0023 and above.
11. DTT is enabled in AC0030 which cause CPU frequency will be 400 MHz.

ACADL357.0031.2022.0117.2022 Development BIOS

About This Release:

- Date: Jan 17 2022
- ROM Image Checksum: 0xA4E0A721
- ME Firmware: 16.0.15.1605
- EC Firmware: 0.28.00.000
- PMC Firmware: 160.01.00.1016
- Boot Guard ACM: 1.18.07
- Reference Code: Based on 0C.00.65.70
- Memory Reference Code: Based on 0.0.3.74
- Integrated Graphics
  - UEFI Driver: 21.0.1044
- AHCI Code: Based on AHCI_29
- Wired LAN Adapter:
  - UEFI Driver: 0.9.03
  - N/A
- Supported Flash Devices:
  - WinBond   W25Q256FV   32MB
  - GigaDevice GD25B256D   32MB
- Microcode Updates included in .ROM & .BIO Files:
  - M80906A2_0000030E.pdb
  - M80906A3_00000413.pdb

New Fixes/Features:

1. [ODM_Changes] Update WLAN power table (SAR)
2. [ODM_Changes] Dsiable TCC offset lock
3. [ODM_Changes] Inculd Q71 event
4. [AMI_Changes][EIP 634641] Smoke test- Power Button Menu failure

Changes:

1. [AMI_Changes][EIP None] Update EC to v0.28
2. [AMI_Changes][EIP None] Update CRB to ADL_036

EC Changes:

For EC 0.28.00.000:

1. Update PD fw (1.05) (Support Power Sense TypeC 5V3A<->5V0.9A)
2. Modify TypeC 5V3A<->5V0.9A relate to (DC)BatI Tthrottling and (AC)SAPC
3. Modify PD command structure
4. Modify Fan table (Performance mode)
5. Modify Fan mode relate to PxFx
6. Modify BatI Tthrottling time delay
7. Modify TccOffset
8. Enable TccOffset Q71
9. Enable Hybrid On condiction for SAPC trigger
10. Relate Lan power On/Off to BIOS setup menu "Lan Enable"
11. Fix DC no suicide @S5

Known Errata:

1. Because boot guard and BIOS guard is enabled in AC0009, please use FPT tool update BIOS from AC0008 and previous versions to this version for avoid any unexpected behavior.
2. Please do not downgrade BIOS to AC0008 and previous versions by F7/exe/iflashV to avoid any unexpected behavior.
3. AC will reboot 4 or 5 times after flash BIOS for rebuild NVRAM and this situation will be gone in PP stage.
4. AC formal BIOS is QS SKU BIOS in AC0024, please do not flash BIOS from AC0023 and above.
5. DTT is enabled in AC0030 which cause CPU frequency will be 400 MHz.
6. For EC 0.28, LAN power On/Off have to run with BIOS version 30 or later. Otherwise it will auto reboot after power off.

ACADL357.0030.2022.0110.2118 Development BIOS

About This Release:

- Date: Jan 10 2022
- ROM Image Checksum: 0xA5334C9F
- ME Firmware: 16.0.15.1605
- EC Firmware: 0.27.00.000
- PMC Firmware: 160.01.00.1016
- Boot Guard ACM: 1.18.05
- Reference Code: Based on 0C.00.60.10
- Memory Reference Code: Based on 0.0.3.9
- Integrated Graphics
  - UEFI Driver: 21.0.1044
- AHCI Code: Based on AHCI_28
- Wired LAN Adapter:
  - UEFI Driver: 0.9.03
  - N/A
- Supported Flash Devices:
  - WinBond W25Q256FV 32MB
  - GigaDevice GD25B256D 32MB
- Microcode Updates included in .ROM & .BIO Files:
  - M8290671_0000001C.pdb
  - M80906A2_0000030E.pdb

New Fixes/Features:

1. [ODM_Changes] Enable RPMC
2. [ODM_Changes] Modify DTT and Smart APC setting
3. [AMI_Changes][EIP 650571][Intel][NUC-G][TF][AC] LAN power setting sync up with EC

Changes:

1. [AMI_Changes][EIP None] Update EC to v0.27

EC Changes:

For EC 0.27.00.000:
1. Enable Auto RTC reset
2. Updated SAPC table
3. Modify SW_Release (HW_PROCHOT) & CPU/GPU PROCHOT
4. Modify BatI (Discharge) Tthrottling
5. Modify BatTemp Tthrottling

Known Errata:

1. Because boot guard and BIOS guard is enabled in AC0009, please use FPT tool update BIOS from AC0008 and previous versions to this version for avoid any unexpected behavior.
2. Please do not downgrade BIOS to AC0008 and previous versions by F7/exe/iflashV to avoid any unexpected behavior.
3. AC will reboot 4 or 5 times after flash BIOS for rebuild NVRAM and this situation will be gone in PP stage.
4. AC formal BIOS is QS SKU BIOS in AC0024, please do not flash BIOS from AC0023 and above.
5. AutoRtcReset is ready in EC0.27 and it need to work with BIOS AC0028 or later or platform will auto reboot in 60 seconds after power on. If run this EC with older BIOS, it can be cancelled by press power button again before Intel logo show on display while power on.

ACADL357.0029.2022.0103.2017 Development BIOS

About This Release:

- Date: Jan 03 2022
- ROM Image Checksum: 0xA5379860
- ME Firmware: 16.0.15.1605
- EC Firmware: 0.26.00.000
- PMC Firmware: 160.01.00.1016
- Boot Guard ACM: 1.18.05
- Reference Code: Based on 0C.00.60.10
- Memory Reference Code: Based on 0.0.3.9
- Integrated Graphics
  - UEFI Driver: 21.0.1044
- AHCI Code: Based on AHCI_28
- Wired LAN Adapter:
  - UEFI Driver: 0.9.03
  - N/A
- Supported Flash Devices:
  - WinBond W25Q256FV 32MB
  - GigaDevice GD25B256D 32MB
- Microcode Updates included in .ROM & .BIO Files:
  - M8290671_0000001C.pdb
  - M80906A2_0000030E.pdb

New Fixes/Features:

1. [ODM_Changes] Add ODM UpdateMsr function
2. [ODM_Changes] Support SMAPC
3. [ODM_Changes] Create token for support Enable / Disable DTT function
4. [AMI_Changes][EIP 615063][Intel][NUC-G][TF][AC][WHQL] Verify Post Device Supports Display And Render fail

Changes:

1. [AMI_Changes][EIP None] Update EC to v0.26

EC Changes:

For EC 0.26.00.000:

1. Modify SMAPC
2. Modify Tthrottling
3. Support NV DState (Disable)
4. Support NV Whisper mode(Disable)

Known Errata:

1. Because boot guard and BIOS guard is enabled in AC0009, please use FPT tool update BIOS from AC0008 and previous versions to this version for avoid any unexpected behavior.
2. Please do not downgrade BIOS to AC0008 and previous versions by F7/exe/iflashV to avoid any unexpected behavior.
3. AC will reboot 4 or 5 times after flash BIOS for rebuild NVRAM and this situation will be gone in PP stage.
4. AC formal BIOS is QS SKU BIOS in AC0024, please do not flash BIOS from AC0023 and above.

ACADL357.0028.2021.1227.2116 Development BIOS

About This Release:

- Date: Dec 27 2021
- ROM Image Checksum: 0xA537D127
- ME Firmware: 16.0.15.1605
- EC Firmware: 0.25.00.000
- PMC Firmware: 160.01.00.1016
- Boot Guard ACM: 1.18.05
- Reference Code: Based on 0C.00.60.10
- Memory Reference Code: Based on 0.0.3.9
- Integrated Graphics
  - UEFI Driver: 21.0.1044
- AHCI Code: Based on AHCI_28
- Wired LAN Adapter:
  - UEFI Driver: 0.9.03
  - N/A
- Supported Flash Devices:
  - WinBond W25Q256FV 32MB
  - GigaDevice GD25B256D 32MB
- Microcode Updates included in .ROM & .BIO Files:
  - M8290671_0000001C.pdb
  - M80906A2_0000030E.pdb

New Fixes/Features:

1. [ODM_Changes] Review HW design and modify GPIO pin
2. [ODM_Changes] AutoRTC can't clear EC timer
3. [AMI_Changes][EIP 650415][Intel][NUC-G][TF][AC][WHQL] Bluetooth - Initiate platform-level device reset fail

Changes:

1. [AMI_Changes][EIP None] Update EC to v0.25

EC Changes:

For EC 0.25.00.000:

1. Support EC Chip version EX (Exculd DX)
2. Modify SAPC AC/DC (New C Code @PPC.C)
3. Modify Throttling (New C Code @PPC.C)
4. Turn Off USB power @BatI>5.8A
5. Enable PLx Q70, Disable Q71 Q72
6. Modify Dumb Battery Helth Low Level
7. Update MPS CPU_2960_V5/GPU_256_V7

Known Errata:

1. Because boot guard and BIOS guard is enabled in AC0009, please use FPT tool update BIOS from AC0008 and previous versions to this version for avoid any unexpected behavior.
2. Please do not downgrade BIOS to AC0008 and previous versions by F7/exe/iflashV to avoid any unexpected behavior.
3. AC will reboot 4 or 5 times after flash BIOS for rebuild NVRAM and this situation will be gone in PP stage.
4. AC formal BIOS is QS SKU BIOS in AC0024, please do not flash BIOS from AC0023 and above.

ACADL357.0027.2021.1222.1439 Development BIOS

About This Release:

- Date: Dec 22 2021
- ROM Image Checksum: 0xA532A31D
- ME Firmware: 16.0.15.1605
- EC Firmware: 0.24.00.000
- PMC Firmware: 160.01.00.1016
- Boot Guard ACM: 1.18.05
- Reference Code: Based on 0C.00.60.10
- Memory Reference Code: Based on 0.0.3.9
- Integrated Graphics
  - UEFI Driver: 21.0.1044
- AHCI Code: Based on AHCI_28
- Wired LAN Adapter:
  - UEFI Driver: 0.9.03
  - N/A
- Supported Flash Devices:
  - WinBond W25Q256FV 32MB
  - GigaDevice GD25B256D 32MB
- Microcode Updates included in .ROM & .BIO Files:
  - M8290671_0000001C.pdb
  - M80906A2_0000030E.pdb

New Fixes/Features:

1. [ODM_Changes] WHQL - Fixed Profile Interrupt Test fail
2. [AMI_Changes][EIP 649753][Intel][NUC-G][TF][AC] Type10 to 19 display empty
3. [AMI_Changes][EIP 648909][Intel/NUC-G][TF][AC] JP Keyboard layout detection for EC control.

Changes:

1. [AMI_Changes][EIP None] Update EC to v0.24

EC Changes:

For EC 0.24.00.000:

1. Update PD fw (1.04) (TBT device lost from S4/S5 resume @DC)
2. Support Gpu DG2 PL12 @SAPC
3. Modify SAPC structure & condiction table
4. Modify Get PL minimum calculation
5. Modify GPU Throttling @BatI BatV GpuT
6. Modify AC->DC unplug Adaptor prochot condiction
7. Modify TypeC 5V3A<->5V0.9A condiction
8. Modify PECI VTT Level 1.1V->1.05V
9. Modify Jap Keyboard matrix
10. Modify Battery ERM

Known Errata:

1. Because boot guard and BIOS guard is enabled in AC0009, please use FPT tool update BIOS from AC0008 and previous versions to this version for avoid any unexpected behavior.
2. Please do not downgrade BIOS to AC0008 and previous versions by F7/exe/iflashV to avoid any unexpected behavior.
3. AC will reboot 4 or 5 times after flash BIOS for rebuild NVRAM and this situation will be gone in PP stage.
4. AC formal BIOS is QS SKU BIOS in AC0024, please do not flash BIOS from AC0023 and above.

ACADL357.0026.2021.1213.2115 Development BIOS

About This Release:

- Date: Dec 13 2021
- ROM Image Checksum: 0xA53869A4
- ME Firmware: 16.0.15.1605
- EC Firmware: 0.23.00.000
- PMC Firmware: 160.01.00.1016
- Boot Guard ACM: 1.18.05
- Reference Code: Based on 0C.00.60.10
- Memory Reference Code: Based on 0.0.3.9
- Integrated Graphics
  - UEFI Driver: 21.0.1044
- AHCI Code: Based on AHCI_28
- Wired LAN Adapter:
  - UEFI Driver: 0.9.03
  - N/A
- Supported Flash Devices:
  - WinBond W25Q256FV 32MB
  - GigaDevice GD25B256D 32MB
- Microcode Updates included in .ROM & .BIO Files:
  - M8290671_0000001C.pdb
  - M80906A2_0000030E.pdb

New Fixes/Features:

1. [ODM_Changes] Fixed HDMI can't display
2. [ODM_Changes] Modify ME setting
3. [AMI_Changes][EIP 642549][Intel][NUC-G][TF][AC][PT][WHQL] Hardware Security Testability Interface Test fail - WA for Error 0x00110001 - RollBack Firmware Error

Changes:

1. [AMI_Changes][EIP None] Update EC to v0.23

EC Changes:

For EC 0.23.00.000:

2. Support EC Chip version EX
3. Modify Fan delay count for GPU Fan
4. Modify Passive Cooling Mode @Fan NonSync
5. Add dummy.txt in empty folder for Git

Known Errata:

1. Because boot guard and BIOS guard is enabled in AC0009, please use FPT tool update BIOS from AC0008 and previous versions to this version for avoid any unexpected behavior.
2. Please do not downgrade BIOS to AC0008 and previous versions by F7/exe/iflashV to avoid any unexpected behavior.
3. AC will reboot 4 or 5 times after flash BIOS for rebuild NVRAM and this situation will be gone in PP stage.
4. AC formal BIOS is QS SKU BIOS in AC0024, please do not flash BIOS from AC0023 and above.

ACADL357.0025.2021.1206.2158 Development BIOS

About This Release:

- Date: Dec 06 2021
- ROM Image Checksum: 0xA53B026D
- ME Firmware: 16.0.15.1605
- EC Firmware: 0.22.00.000
- PMC Firmware: 160.01.00.1016
- Boot Guard ACM: 1.18.05
- Reference Code: Based on 0C.00.60.10
- Memory Reference Code: Based on 0.0.3.9
- Integrated Graphics
  - UEFI Driver: 21.0.1043
- AHCI Code: Based on AHCI_28
- Wired LAN Adapter:
  - UEFI Driver: 0.9.03
  - N/A
- Supported Flash Devices:
  - WinBond   W25Q256FV   32MB
  - GigaDevice GD25B256D   32MB
- Microcode Updates included in .ROM & .BIO Files:
  - M8290671_0000001C.pdb
  - M80906A2_0000030E.pdb

New Fixes/Features:

1. [ODM_Changes] When BIOS load default, set EC bit
2. [ODM_Changes] Remove GPP_D9, FAB D not use.
3. [ODM_Changes] Audio can't normal on QS board.
4. [ODM_Changes] VCCST Status to disable
5. [ODM_Changes] Sync DTT OEM Variable with AP
6. [AMI_Changes][EIP None]Update retimer fw update feature
7. [AMI_Changes][EIP None]Add Setup item Deep S4/S5 for Intel request
8. [AMI_Changes][EIP 649727][Intel][NUC-G][TF][AC] BIOS Setup MENU > Advanced > USB : Right USB Port & Left USB Front Port & Left USB Rear Port setup Fail
9. [AMI_Changes][EIP 649729][Intel][NUC-G][TF][AC] BIOS SETUP MENU>Advanced>ON BOARD DEVICES :[HD Audio][LAN][Bluetooth][Webcam] Setup Disable Fail
10. [AMI_Changes][EIP 652496][Intel][NUC-G][TF][AC] BIOS AC0024 formal release ME FW version display 0.0.0.0
11. [AMI_Changes][EIP 650274][Intel][NUC-G][TF][AC] Front-panel Power LED Blink Codes

Changes:

1. [ODM_Changes] Update ME FW 16.0.15.1605 (BKC WW49)
2. [AMI_Changes][EIP None] Update EC to v0.22

EC Changes:

For EC 0.22.00.000:

1. Update PD fw (1.03) for WHQL (UCSI USB Operation role command - Accept Swap)
2. Modify Compiler Build setting
3. Modify Lan Power On @S5->S0 Sequence
4. Modify OOB Peci set PL124
5. Disable PECI PL124 @DTT On
6. Diable PECI PL124 by set 0
7. Fix Gpu DG2 PL12 setting
8. Support AP/BIOS change PxFx(Power/Fan) Mode

Known Errata:

1. Because boot guard and BIOS guard is enabled in AC0009, please use FPT tool update BIOS from AC0008 and previous versions to this version for avoid any unexpected behavior.
2. Please do not downgrade BIOS to AC0008 and previous versions by F7/exe/iflashV to avoid any unexpected behavior.
3. AC will reboot 4 or 5 times after flash BIOS for rebuild NVRAM and this situation will be gone in PP stage.
4. AC formal BIOS is QS SKU BIOS in AC0024, please do not flash BIOS from AC0023 and above.
5. **Need to wait 20 sec after first time update EC for flash new PD fw (Amber LED twinkle in FAB D)**

ACADL357.0024.2021.1130.0109 Development BIOS

About This Release:

- Date: Nov 29 2021
- ROM Image Checksum: 0xA414C96B
- ME Firmware: 16.0.15.1597
- EC Firmware: 0.21.00.000
- PMC Firmware: 160.01.00.1016
- Boot Guard ACM: 1.18.05
- Reference Code: Based on 0C.00.60.10
- Memory Reference Code: Based on 0.0.3.9
- Integrated Graphics
  - UEFI Driver: 21.0.1042
- AHCI Code: Based on AHCI_28
- Wired LAN Adapter:
  - UEFI Driver: 0.9.03
  - N/A
- Supported Flash Devices:
  - WinBond   W25Q256FV   32MB
  - GigaDevice GD25B256D   32MB
- Microcode Updates included in .ROM & .BIO Files:
  - M8290671_0000001C.pdb
  - M80906A2_0000030E.pdb

New Fixes/Features:

1. [ODM_Changes] Enable Re-Size BAR Support
2. [AMI_Changes][EIP None] Change default build as QS SKU
3. [AMI_Changes][EIP None] Remove Deep S4/S5 Setup item
4. [AMI_Changes][EIP 649773][Intel][NUC-G][TF][AC] Audio KeyHash

Changes:

1. [ODM_Changes] Update ME FW 16.0.15.1597
2. [AMI_Changes][EIP None] Update CRB to ADL_031
3. [AMI_Changes][EIP None] Update EC to v0.21

EC Changes:

For EC 0.21.00.000:

1. Modify Lan Power On/Off
2. Modify PECI VTT Level 1.05V->1.1V
3. Support Rom Memory load default by BIOS setup menu
4. Support Gpu PL12 setting by manual
5. Fix DTT PSRC wrong setting
6. Workaround to prevent Battery RC abnormal Zero
7. Workaround to prevent Battery FCC abnormal Zero

Known Errata:

1. Because boot guard and BIOS guard is enabled in AC0009, please use FPT tool update BIOS from AC0008 and previous versions to this version for avoid any unexpected behavior.
2. Please do not downgrade BIOS to AC0008 and previous versions by F7/exe/iflashV to avoid any unexpected behavior.
3. AC will reboot 4 or 5 times after flash BIOS for rebuild NVRAM and this situation will be gone in PP stage.
4. **AC formal BIOS is QS SKU BIOS in this version, please do not flash BIOS from previous version.**

ACADL357.0023.2021.1122.2158 Development BIOS

About This Release:

- Date: Nov 22 2021
- ROM Image Checksum: 0xA44CDDE7
- ME Firmware: 16.0.15.1545
- EC Firmware: 0.20.00.000
- PMC Firmware: 160.01.00.1013
- Boot Guard ACM: 1.18.1
- Reference Code: Based on 0C.00.5D.30
- Memory Reference Code: Based on 0.0.2.232
- Integrated Graphics
  - UEFI Dri ver: 21.0.1040
- AHCI Code: Based on AHCI_28
- Wired LAN Adapter:
  - UEFI Driver: 0.9.03
  - N/A
- Supported Flash Devices:
  - WinBond W25Q256FV 32MB
  - GigaDevice GD25B256D 32MB
- Microcode Updates included in .ROM & .BIO Files:
  - M8290671_0000001C.pdb
  - M80906A2_0000030E.pdb

New Fixes/Features:

1. [ODM_Changes] Verb table update for fix before installing the driver, unit will be noise.
2. [ODM_Changes] Fix TBT dock will cause system auto resume from S4 when system unplug TBT
3. [AMI_Changes][EIP 648119][Intel][NUC-G][TF][AC] BIOS Chassis Info_Version string -> BIOS shows 2.0, PRD shows 3.0; BIOS shows Intel (R), PRD shows Intel (without R)
4. [AMI_Changes][EIP 643698][Intel][NUC-G][TF][AC] Display DG2 GPU device type and VBIOS version.
5. [AMI_Changes][EIP None] Weird BIOS Message when Recovering BIOS

Changes:

1. [AMI_Changes][EIP None] Update EC to v0.20

EC Changes:

For EC 0.20.00.000:

1. Support BIOS updated/Memory Error LED
2. Support Factory ecUtil -MODS test
3. Modify Battery Safty protect charge current to 4.5A
4. Monitor CPU Thermal Trip @Normal shutdown (CC C6)
5. Modify Power Button Leakage @S0->S5
6. Fix TBT lost device once wake from S4/S5 @DC
7. Disable Caps LED @Modern standby

Known Errata:

1. Because boot guard and BIOS guard is enabled in AC0009, please use FPT tool update BIOS from AC0008 and previous versions to this version for avoid any unexpected behavior.
2. Please do not downgrade BIOS to AC0008 and previous versions by F7/exe/iflashV to avoid any unexpected behavior.
3. AC will reboot 4 or 5 times after flash BIOS for rebuild NVRAM and this situation will be gone in PP stage.

ACADL357.0022.2021.1115.2208 Development BIOS

About This Release:

- Date: Nov 15 2021
- ROM Image Checksum: 0xA44DCDEB
- ME Firmware: 16.0.15.1545
- EC Firmware: 0.19.00.000
- PMC Firmware: 160.01.00.1013
- Boot Guard ACM: 1.18.1
- Reference Code: Based on 0C.00.5D.30
- Memory Reference Code: Based on 0.0.2.232
- Integrated Graphics
  - UEFI Dri ver: 21.0.1040
- AHCI Code: Based on AHCI_28
- Wired LAN Adapter:
  - UEFI Driver: 0.9.03
  - N/A
- Supported Flash Devices:
  - WinBond W25Q256FV 32MB
  - GigaDevice GD25B256D 32MB
- Microcode Updates included in .ROM & .BIO Files:
  - M8290671_0000001C.pdb
  - M80906A2_0000030E.pdb

New Fixes/Features:

1. [ODM_Changes] Update GDDV to fix PL setting are incorrect during DTT mode change
2. [ODM_Changes] Fix DTT ARTG for AC/DC change
3. [ODM_Changes] Fix TBT dock will cause system auto resume from S4
4. [AMI_Changes][EIP None] Correct USB port string in Setup
5. [AMI_Changes][EIP 648119][Intel][NUC-G][TF][AC] BIOS Chassis Info_Version string -> BIOS shows 2.0, PRD shows 3.0 - Update BIOS Chassis Info_Version

Changes:

1. [AMI_Changes][EIP None] Update EC to v0.19

EC Changes:

For EC 0.19.00.000:

1. Support JP Keyboard switch by BIOS DMI
2. Modify ExGPIO code (Mute/LID/USB_PW)
3. Modify Breath Amber->White @AC Modern Standby
4. Fix Abnormal Amber LED on @S5
5. Fix EC->BIOS 230W/180W DTT setting

Known Errata:

1. Because boot guard and BIOS guard is enabled in AC0009, please use FPT tool update BIOS from AC0008 and previous versions to this version for avoid any unexpected behavior.
2. Please do not downgrade BIOS to AC0008 and previous versions by F7/exe/iflashV to avoid any unexpected behavior.
3. AC will reboot 4 or 5 times after flash BIOS for rebuild NVRAM and this situation will be gone in PP stage.

ACADL357.0021.2021.1108.2205 Development BIOS

About This Release:

- Date: Nov 08 2021
- ROM Image Checksum: 0xA452CFAC
- ME Firmware: 16.0.15.1545
- EC Firmware: 0.18.00.000
- PMC Firmware: 160.01.00.1013
- Boot Guard ACM: 1.18.1
- Reference Code: Based on 0C.00.5D.30
- Memory Reference Code: Based on 0.0.2.232
- Integrated Graphics
  - UEFI Dri ver: 21.0.1040
- AHCI Code: Based on AHCI_28
- Wired LAN Adapter:
  - UEFI Driver: 0.9.03
  - N/A
- Supported Flash Devices:
  - WinBond W25Q256FV 32MB
  - GigaDevice GD25B256D 32MB
- Microcode Updates included in .ROM & .BIO Files:
  - M8290671_0000001C.pdb
  - M80906A2_0000030E.pdb

New Fixes/Features:

1. [ODM_Changes] Fix DTT BAT show unknown device
2. [ODM_Changes] Fix DG2 Bus1 cannot enter into RTD3
3. [ODM_Changes] Correct DTT Battery participant _UID
4. [AMI_Changes][EIP None] Adjust FSP S FV size for debug mode build fail
5. [AMI_Changes][EIP 647158] [Intel/NUC-G][TF][AC] PTK1885: Unauthorized modification of UEFI variables could disable the protect mechanism of SMM

Changes:

1. [ODM_Changes] Update GOP 21.0.1040
2. [ODM_Changes] Add 1xDMIC verbtable on Fab D
3. [ODM_Changes] Update ME FW 16.0.15.1545v2
4. [AMI_Changes][EIP None] Update EC to v0.18

EC Changes:

For EC 0.18.00.000:

1. Modify RGB Lightbat code
2. Modify GPIO code
3. Support MPS update w/ check version
4. Fix Passive Cooling Mode no work @DTT on
5. Inhibit Touch pad On/Of @Modern Standby
6. Modify RSMRST# track on SLP_SUS# @S5->DeepS5

Known Errata:

1. Because boot guard and BIOS guard is enabled in AC0009, please use FPT tool update BIOS from AC0008 and previous versions to this version for avoid any unexpected behavior.
2. Please do not downgrade BIOS to AC0008 and previous versions by F7/exe/iflashV to avoid any unexpected behavior.
3. AC will reboot 4 or 5 times after flash BIOS for rebuild NVRAM and this situation will be gone in PP stage.

ACADL357.0020.2021.1101.2135 Development BIOS

About This Release:

- Date: Nov 01 2021
- ROM Image Checksum: 0xA4656545
- ME Firmware: 16.0.15.1545
- EC Firmware: 0.17.00.000
- PMC Firmware: 160.01.00.1013
- Boot Guard ACM: 1.18.1
- Reference Code: Based on 0C.00.5D.30
- Memory Reference Code: Based on 0.0.2.232
- Integrated Graphics
  - UEFI Dri ver: 21.0.1038
- AHCI Code: Based on AHCI_28
- Wired LAN Adapter:
  - UEFI Driver: 0.9.03
  - N/A
- Supported Flash Devices:
  - WinBond W25Q256FV 32MB
  - GigaDevice GD25B256D 32MB
- Microcode Updates included in .ROM & .BIO Files:
  - M8290671_0000001C.pdb
  - M80906A2_0000030E.pdb

New Fixes/Features:

1. [AMI_Changes][EIP 642552][Intel][NUC-G][TF][AC][PT][WHQL] ACPI Logo Test fail
2. [AMI_Changes][EIP None] Linux ACPI BIOS error
3. [AMI_Changes][EIP None] Remove QR code in POST since AC will not support it

Changes:

1. [ODM_Changes] Update ME FW 16.0.15.1545
2. [ODN_Changes] Update Micorcode K0 0x30E
3. [AMI_Changes][EIP None] Update EC to 0.17
4. [AMI_Changes][EIP None] Update CRB to ADL_030

EC Changes:

For EC 0.17.00.000:

1. Fix Fan no Start Up once Stop
2. Fix Fan boost block by DTT
3. Modify RGB KB Backlight for NSS new spec.
4. Modify OOB read GPU Temp (old+new)/2
5. Modify Peci read GPU temp (old+new)/2
6. Modify SMBus block read/write for waiting finish

Known Errata:

1. Because boot guard and BIOS guard is enabled in AC0009, please use FPT tool update BIOS from AC0008 and previous versions to this version for avoid any unexpected behavior.
2. Please do not downgrade BIOS to AC0008 and previous versions by F7/exe/iflashV to avoid any unexpected behavior.
3. AC will reboot 4 or 5 times after flash BIOS for rebuild NVRAM and this situation will be gone in PP stage.

ACADL357.0019.2021.1025.2214 Development BIOS

About This Release:

- Date: Oct 25 2021
- ROM Image Checksum: 0xA44BB18A
- ME Firmware: 16.0.10.1473
- EC Firmware: 0.16.00.000
- PMC Firmware: 160.01.00.1013
- Boot Guard ACM: 1.18.1
- Reference Code: Based on 0C.00.5B.10
- Memory Reference Code: Based on 0.0.2.206
- Integrated Graphics
  - UEFI Dri ver: 21.0.1038
- AHCI Code: Based on AHCI_26
- Wired LAN Adapter:
  - UEFI Driver: 0.9.03
  - N/A
- Supported Flash Devices:
  - WinBond   W25Q256FV   32MB
  - GigaDevice GD25B256D   32MB
- Microcode Updates included in .ROM & .BIO Files:
  - M8290671_0000001C.pdb

New Fixes/Features:

1. [ODM_Changes] Update QS/ES build control for ME FW
2. [ODM_Changes] Update DTT ARTG return value
3. [ODM_Changes] Correct ES ME build error
4. [ODM_Changes] Update DTT GDDV 10/22

Changes:

1. [ODM_Changes] Update GOP 21.0.1038
2. [AMI_Changes][EIP None] Update EC to 0.16
3. [AMI_Changes][EIP None] Update CRB to ADL_029

EC Changes:

For EC 0.16.00.000:

1. Fix Power LED abnormal
2. Fix ramdebug memory conflict
3. Modiify Fn+F2 == FnLock (Record in ROM MEMORY)
4. Modify Charger Psys low power setting @DC
5. Modify PECI GPU temp reading
6. Modify OOB PsysPL1 PsysPL2 writing
7. Modify SAPC (Enable@DTTOff / Disable@DTTOn)
8. Modify Shipping mode
9. Modify Fan kick off
10. Modify Display detect

Known Errata:

1. Because boot guard and BIOS guard is enabled in AC0009, please use FPT tool update BIOS from AC0008 and previous versions to this version for avoid any unexpected behavior.
2. Please do not downgrade BIOS to AC0008 and previous versions by F7/exe/iflashV to avoid any unexpected behavior.
3. AC will reboot 4 or 5 times after flash BIOS for rebuild NVRAM and this situation will be gone in PP stage.

ACADL357.0018.2021.1018.2202 Development BIOS

About This Release:

- Date: Oct 18 2021
- ROM Image Checksum: 0xA4704E0F
- ME Firmware: 16.0.10.1473
- EC Firmware: 0.15.00.000
- PMC Firmware: 160.01.00.1013
- Boot Guard ACM: 1.17.97
- Reference Code: Based on 0C.00.57.10
- Memory Reference Code: Based on 0.0.2.171
- Integrated Graphics
  - UEFI Dri ver: 21.0.1036
- AHCI Code: Based on AHCI_26
- Wired LAN Adapter:
  - UEFI Driver: 0.9.03
  - N/A
- Supported Flash Devices:
  - WinBond W25Q256FV 32MB
  - GigaDevice GD25B256D 32MB
- Microcode Updates included in .ROM & .BIO Files:
  - M8290671_0000001C.pdb

New Fixes/Features:

1. [ODM_Changes] Sync DTT OEM Variable with AP
2. [ODM_Changes] Add QS/ES build control for ME FW

Changes:

1. [AMI_Changes][EIP None] Update EC to 0.14
2. [AMI_Changes][EIP None] Update EC to 0.15

EC Changes:

For EC 0.14.00.000:

1. Modify Battery Charge Voltage protect point to Charger Voltage+300mV
2. Updated Fan Table
3. Tccoffset fixed 5
4. Remove Power on PL124 double setting

For EC 0.15.00.000:

1. Modify LED behavior for PRD 1.09
2. Modify EC RAM MAP (0x0700~0x072F -> 0x91xx)
3. Modify Passive Cooling Mode
4. Fix DTT battery polling event abnormal
5. Fix Battery Charge Time out fail cause by Hybrid on
6. Enable TBT Retimer update command
7. Remove WorkAround for current noise (Charger 400K/800KHz)

Known Errata:

1. Because boot guard and BIOS guard is enabled in AC0009, please use FPT tool update BIOS from AC0008 and previous versions to this version for avoid any unexpected behavior.
2. Please do not downgrade BIOS to AC0008 and previous versions by F7/exe/iflashV to avoid any unexpected behavior.
3. AC will reboot 4 or 5 times after flash BIOS for rebuild NVRAM and this situation will be gone in PP stage.

ACADL357.0017.2021.1008.2156 Development BIOS

About This Release:

- Date: Oct 08 2021
- ROM Image Checksum: 0xA4741FCC
- ME Firmware: 16.0.10.1473
- EC Firmware: 0.12.00.000
- PMC Firmware: 160.01.00.1013
- Boot Guard ACM: 1.17.97
- Reference Code: Based on 0C.00.57.10
- Memory Reference Code: Based on 0.0.2.171
- Integrated Graphics
    - UEFI Dri ver: 21.0.1036
- AHCI Code: Based on AHCI_26
- Wired LAN Adapter:
    - UEFI Driver: 0.9.03
    - N/A
- Supported Flash Devices:
    - WinBond W25Q256FV 32MB
    - GigaDevice GD25B256D 32MB
- Microcode Updates included in .ROM & .BIO Files:
    - M8290671_0000001C.pdb

New Fixes/Features:

1. [ODM_Changes] Update DTT ARTG report
2. [ODM_Changes] Update thermal table 10/08
3. [AMI_Changes][EIP 641191] [Intel-SPG][TF][AC] Smoke test - NVMe Port Check failure
4. [AMI_Changes][EIP None] Add lost change for update CRB to ADL_026
5. [AMI_Changes][EIP None] FailSafe watchdog function fail

Changes:

1. N/A

EC Changes:

2. N/A

Known Errata:

1. Because boot guard and BIOS guard is enabled in AC0009, please use FPT tool update BIOS from AC0008 and previous versions to this version for avoid any unexpected behavior.
2. Please do not downgrade BIOS to AC0008 and previous versions by F7/exe/iflashV to avoid any unexpected behavior.
3. AC will reboot 4 or 5 times after flash BIOS for rebuild NVRAM and this situation will be gone in PP stage.

ACADL357.0016.2021.1004.2226 Development BIOS

About This Release:

- Date: Oct 04 2021
- ROM Image Checksum: 0xA472E035
- ME Firmware: 16.0.10.1473
- EC Firmware: 0.12.00.000
- PMC Firmware: 160.01.00.1013
- Boot Guard ACM: 1.17.97
- Reference Code: Based on 0C.00.57.10
- Memory Reference Code: Based on 0.0.2.171
- Integrated Graphics
  - UEFI Dri ver: 21.0.1036
- AHCI Code: Based on AHCI_26
- Wired LAN Adapter:
  - UEFI Driver: 0.9.03
  - N/A
- Supported Flash Devices:
  - WinBond   W25Q256FV   32MB
  - GigaDevice GD25B256D   32MB
- Microcode Updates included in .ROM & .BIO Files:
  - M8290671_0000001C.pdb

New Fixes/Features:

1. [ODM_Changes] Follow RC to correct UCSI device
2. [ODM_Changes] Update GDDV to improve FAN control by DTT
3. [AMI_Changes][EIP 637083][Intel-SPG][TF][AC] CCD shows mirroring side image
4. [AMI_Changes][EIP None] Sync PLx value
5. [AMI_Changes][EIP None] Enable ESA support
6. [AMI_Changes][EIP None] Temp enable CRB Setup when ESA support

Changes:

1. [AMI_Changes][EIP None] Update EC to 0.12

EC Changes:

1. Fix plug in AC and it will automatically turn on at battery mode.
2. Power LED off when Modern standby
3. Power LED Blink when Charging status
4. RGB keyboard Black Light welcome function
5. Support tool can system shutdown in shell mode
6. Support Factor FanPWM
7. Fix battery charge fail while RSOC 100%->90% self discharge
8. Disable PL124 control by MSR(Q70)
9. Disable FANLOCK protect by thermo fan table
10. Disable REMOTETEMP protect by thermo fan table

Known Errata:

1. Because boot guard and BIOS guard is enabled in AC0009, please use FPT tool update BIOS from AC0008 and previous versions to this version for avoid any unexpected behavior.
2. Please do not downgrade BIOS to AC0008 and previous versions by F7/exe/iflashV to avoid any unexpected behavior.
3. AC will reboot 4 or 5 times after flash BIOS for rebuild NVRAM and this situation will be gone in PP stage.
4. Camera need to be updated or reset in Win 11 for EIP637083.

ACADL357.0015.2021.0927.2235 Development BIOS

About This Release:

- Date: Sep 27 2021
- ROM Image Checksum: 0xAF1D087C
- ME Firmware: 16.0.10.1473
- EC Firmware: 0.11.00.000
- PMC Firmware: 160.01.00.1013
- Boot Guard ACM: 1.17.97
- Memory Reference Code: Based on 0.0.2.171
- Integrated Graphics
  - UEFI Dri ver: 21.0.1036
- AHCI Code: Based on AHCI_26
- Wired LAN Adapter:
  - UEFI Driver: 0.9.03
  - N/A
- Supported Flash Devices:
  - WinBond   W25Q256FV   32MB
  - GigaDevice GD25B256D   32MB
- Microcode Updates included in .ROM & .BIO Files:
  - M8290671_0000001C.pdb

New Fixes/Features:

1. [ODM_Changes] Set Tcc Offset by thermal request
2. [AMI_Changes][EIP638906][Intel-SPG][TF][AC] Boot time over 13s - Skip loading PCI PXE ROM when BIOS setup item "Network Boot" is disabled.

Changes:

1. [AMI_Changes][EIP None] Update CRB to ADL 026
2. [AMI_Changes][EIP None] Update EC to 0.11

EC Changes:

1. Fix Caps LED default ON when Power on and rearrange IT8308 function code.
2. Modify Fan table follow thermal table R01 and fix sometimes Fan full run after modern standby wakeup.

Known Errata:

1. Because boot guard and BIOS guard is enabled in AC0009, please use FPT tool update BIOS from AC0008 and previous versions to this version for avoid any unexpected behavior.
2. Please do not downgrade BIOS to AC0008 and previous versions by F7/exe/iflashV to avoid any unexpected behavior.
3. AC will reboot 4 or 5 times after flash BIOS for rebuild NVRAM and this situation will be gone in PP stage.

ACADL357.0014.2021.0917.2029 Development BIOS

About This Release:

- Date: Sep 17 2021
- ROM Image Checksum: 0xAF8CB2F9
- ME Firmware: 16.0.10.1473
- EC Firmware: 0.10.00.000
- PMC Firmware: 160.01.00.1013
- Boot Guard ACM: 1.17.97
- Memory Reference Code: Based on 0.0.2.159
- Integrated Graphics
  - UEFI Dri ver: 21.0.1036
- AHCI Code: Based on AHCI_26
- Wired LAN Adapter:
  - UEFI Driver: 0.9.03
  - N/A
- Supported Flash Devices:
  - WinBond W25Q256FV 32MB
  - GigaDevice GD25B256D 32MB
- Microcode Updates included in .ROM & .BIO Files:
  - M8290671_0000001C.pdb

New Fixes/Features:

1. [ODM_Changes] For EC DTT sync
2. [AMI_Changes][EIP637085][Intel-SPG][TF][AC] Memory size is incorrect on F2 bios setup

Changes:

1. [AMI_Changes][EIP None] Update CRB to ADL 024
2. [AMI_Changes][EIP None] Update EC to 0.10

EC Changes:

1. Fix boot fail after 10Sec PCH Force shutdown.
2. Add key Fn+up (Page-up)/Fn+down (Page-down)/Fn+left (Home)/Fn+right (End)
3. Add key Fn+PRT SC (Insert)
4. Add Fn+F2 lock system
5. Fix power ON fail after GReset.
6. Remove "V0.06.00 release item 2: FAN Table fix 80% "

Known Errata:

1. Because boot guard and BIOS guard is enabled in AC0009, please use FPT tool update BIOS from AC0008 and previous versions to this version for avoid any unexpected behavior.
2. Please do not downgrade BIOS to AC0008 and previous versions by F7/exe/iflashV to avoid any unexpected behavior.
3. AC will reboot 4 or 5 times after flash BIOS for rebuild NVRAM and this situation will be gone in PP stage.

ACADL357.0013.2021.0913.2052 Development BIOS

About This Release:

- Date: Sep 13 2021
- ROM Image Checksum: 0xAFA50538
- ME Firmware: 16.0.10.1473
- EC Firmware: 0.09.00.000
- PMC Firmware: 160.01.00.1010
- Boot Guard ACM: 1.17.97
- Memory Reference Code: Based on 0.0.2.134
- Integrated Graphics
  - UEFI Dri ver: 21.0.1036
- AHCI Code: Based on AHCI_26
- Wired LAN Adapter:
  - UEFI Driver: 0.9.02
  - N/A
- Supported Flash Devices:
  - WinBond W25Q256FV 32MB
  - GigaDevice GD25B256D 32MB
- Microcode Updates included in .ROM & .BIO Files:
  - M8290671_0000001C.pdb

New Fixes/Features:

1. [ODM_Changes] Sync BIOS Info to EC for AP use
2. [AMI_Changes][EIP None] Remove SD card 3.0 controller from Setup
3. [AMI_Changes][EIP 627686] RTC wake from S5 fail
4. [AMI_Changes][EIP 618736] BIOS Debug Build Release Package

Changes:

1. [ODM_Changes] Update thermal GDDV 0907
2. [ODM_Changes] Update GOP 21.0.1036
3. [ODM_Changes] Update ME FW 16.0.10.1473 (BKC WW37)
4. [AMI_Changes][EIP None] Update EnhancePeiVariable module to label_11

Known Errata:

1. Because boot guard and BIOS guard is enabled in AC0009, please use FPT tool update BIOS from AC0008 and previous versions to this version for avoid any unexpected behavior.
2. Please do not downgrade BIOS to AC0008 and previous versions by F7/exe/iflashV to avoid any unexpected behavior.

ACADL357.0012.2021.0906.1952 Development BIOS

About This Release:

- Date: Sep 06 2021
- ROM Image Checksum: 0xAFBA6757
- ME Firmware: 16.0.10.1394
- EC Firmware: 0.09.00.000
- PMC Firmware: 160.01.00.1010
- Boot Guard ACM: 1.17.97
- Memory Reference Code: Based on 0.0.2.134
- Integrated Graphics
  - UEFI Dri ver: 21.0.1028
- AHCI Code: Based on AHCI_26
- Wired LAN Adapter:
  - UEFI Driver: 0.9.02
  - N/A
- Supported Flash Devices:
  - WinBond W25Q256FV 32MB
  - GigaDevice GD25B256D 32MB
- Microcode Updates included in .ROM & .BIO Files:
  - M8290671_0000001C.pdb

New Fixes/Features:

1. [ODM_Changes][EIP None] Update thermal GDDV (PL1=40W, Power Share Policy enable)
2. [ODM_Changes][EIP None] Fix connect LAN cable in windows cannot wake
3. [AMI_Changes][EIP None] Update CRB to ADL022
4. [AMI_Changes][EIP None] Temp disable OC item for Caterr and CPU frequency issue after update CRB to ADL022
5. [AMI_Changes][EIP None] Fix press F8 no function
6. [AMI_Changes][EIP None] Temp disable deep Sx
7. [AMI_Changes][EIP None] Update for abnormal shutdown form when do S4 (need Plug in TBT device)

Changes:

1. [ODM_Changes][EIP None] Update EC to 0.09

Known Errata:

1. Because boot guard and BIOS guard is enabled in AC0009, please use FPT tool update BIOS from AC0008 and previous versions to this version for avoid any unexpected behavior.
2. Please do not downgrade BIOS to AC0008 and previous versions by F7/exe/iflashV to avoid any unexpected behavior.

ACADL357.0011.2021.0830.2134 Development BIOS

About This Release:

- Date: Aug 30 2021
- ROM Image Checksum: 0xB0627C86
- ME Firmware: 16.0.10.1394
- EC Firmware: 0.08.00.000
- PMC Firmware: 160.01.00.1007
- Boot Guard ACM: 1.17.65
- Memory Reference Code: Based on 0.0.2.52
- Integrated Graphics
  - UEFI Dri ver: 21.0.1028
- AHCI Code: Based on AHCI_26
- Wired LAN Adapter:
  - UEFI Driver:
  - N/A
- Supported Flash Devices:
  - WinBond W25Q256FV 32MB
  - GigaDevice GD25B256D 32MB
- Microcode Updates included in .ROM & .BIO Files:
  - M8290671_0000001A.pdb

New Fixes/Features:

1. [ODM_Changes][EIP None] Update DigitalMicrophone enable/disable
2. [AMI_Changes][EIP None] Update power check support
3. [AMI_Changes][EIP None] Update for security jumper cannot enter recovery
4. [AMI_Changes][EIP None] Update for patch ME region is too slow to update in recovery mode after enable BIOSGuard

Changes:

1. N/A

Known Errata:

1. Because boot guard and BIOS guard is enabled in AC0009, please use FPT tool update BIOS from AC0008 and previous versions to this version for avoid any unexpected behavior.
2. Please do not downgrade BIOS to AC0008 and previous versions by F7/exe/iflashV to avoid any unexpected behavior.

ACADL357.0010.2021.0823.2133 Development BIOS

About This Release:

- Date: Aug 23 2021
- ROM Image Checksum: 0xB074D090
- ME Firmware: 16.0.10.1394
- EC Firmware: 0.08.00.000
- PMC Firmware: 160.01.00.1007
- Boot Guard ACM: 1.17.65
- Memory Reference Code: Based on 0.0.2.52
- Integrated Graphics
  - UEFI Dri ver: 21.0.1028
- AHCI Code: Based on AHCI_26
- Wired LAN Adapter:
  - UEFI Driver:
  - N/A
- Supported Flash Devices:
  - WinBond   W25Q256FV   32MB
  - GigaDevice GD25B256D   32MB
- Microcode Updates included in .ROM & .BIO Files:
  - M8290671_0000001A.pdb

New Fixes/Features:

1. [AMI_Changes][EIP None] Update for SMBIOS table function
2. [AMI_Changes][EIP None] Update USB map table
3. [AMI_Changes][EIP None] Skip loading i225 PXE ROM if the BIOS setup item "Network Boot" is disabled
4. [AMI_Changes][EIP None] Update stddefault function

Changes:

1. N/A

Known Errata:

1. Because boot guard and BIOS guard is enabled in AC0009, please use FPT tool update BIOS from AC0008 and previous versions to this version for avoid any unexpected behavior.
2. Please do not downgrade BIOS to AC0008 and previous versions by F7/exe/iflashV to avoid any unexpected behavior.

ACADL357.0009.2021.0817.1011 Development BIOS

About This Release:

- Date: Aug 17 2021
- ROM Image Checksum: 0xB071FA34
- ME Firmware: 16.0.10.1394
- EC Firmware: 0.08.00.000
- PMC Firmware: 160.01.00.1007
- Boot Guard ACM: 1.17.65
- Memory Reference Code: Based on 0.0.2.52
- Integrated Graphics
  - UEFI Dri ver: 21.0.1028
- AHCI Code: Based on AHCI_26
- Wired LAN Adapter:
  - UEFI Driver:
  - N/A
- Supported Flash Devices:
  - WinBond W25Q256FV 32MB
  - GigaDevice GD25B256D 32MB
- Microcode Updates included in .ROM & .BIO Files:
  - M8290671_0000001A.pdb

New Fixes/Features:

1. [ODM_Changes][EIP None] Update Thermal GDDV and enhance FAN participants.
2. [AMI_Changes][EIP None] Active internal UEFI Shell.
3. [AMI_Changes][EIP None] Update DG2 Setup string.
4. [AMI_Changes][EIP None] Update for SMBIOS table.
5. [AMI_Changes][EIP None] Enable and update EC FW update.
6. [AMI_Changes][EIP None] Update for Energy Star.
7. [AMI_Changes][EIP None] Enable boot guard.
8. [AMI_Changes][EIP None] Enable BIOS guard.
9. [AMI_Changes][EIP None] Enable and update Self-healing.

Changes:

1. [ODM_Changes][EIP None] Update EC to 0.08.00.000.

Known Errata:

1. **Because boot guard and BIOS guard is enabled in this version, please use FPT tool update BIOS to this version for avoid any unexpected behavior.**
2. **Please do not downgrade BIOS from this version by F7/exe/iflashV to avoid any unexpected behavior.**

ACADL357.0008.2021.0809.2210 Development BIOS

About This Release:

- Date: Aug 09 2021
- ROM Image Checksum: 0xB2997A76
- ME Firmware: 16.0.10.1394
- EC Firmware: 0.07.00.000
- PMC Firmware: 160.01.00.1007
- Boot Guard ACM: None
- Memory Reference Code: Based on 0.0.2.52
- Integrated Graphics
  - UEFI Dri ver: 21.0.1028
- AHCI Code: Based on AHCI_26
- Wired LAN Adapter:
  - UEFI Driver:
  - N/A
- Supported Flash Devices:
  - WinBond W25Q256FV 32MB
  - GigaDevice GD25B256D 32MB
- Microcode Updates included in .ROM & .BIO Files:
  - M8290671_0000001A.pdb

New Fixes/Features:

1. [ODM_Changes][EIP None] Update ODM change for Update PsysPL2=290W and add EC to feedback TZ00._TMP for NSS.
2. [AMI_Changes][EIP None] Update for Deep Sx support.
3. [AMI_Changes][EIP None] Disable SGX Setup item.
4. [AMI_Changes][EIP None] Update for SMBIOS table.

Changes:

1. [ODM_CHANGE][EIP None] Update EC to 0.07.000

Known Errata:

1. System cannot power on after BIOS downgrade to AC0003 by F7/exe/iflashV.

ACADL357.0007.2021.0802.2257 Development BIOS

About This Release:

- Date: Aug 02 2021
- ROM Image Checksum: 0xB29C1256
- ME Firmware: 16.0.10.1394
- EC Firmware: 0.06.00.000
- PMC Firmware: 160.01.00.1007
- Boot Guard ACM: None
- Memory Reference Code: Based on 0.0.2.52
- Integrated Graphics
    - UEFI Driver: 21.0.1028
- AHCI Code: Based on AHCI_26
- Wired LAN Adapter:
    - UEFI Driver:
    - N/A
- Supported Flash Devices:
    - WinBond W25Q256FV 32MB
    - GigaDevice GD25B256D 32MB
- Microcode Updates included in .ROM & .BIO Files:
    - M8290671_0000001A.pdb

New Fixes/Features:

1. [ODM_Changes][EIP None] Update ODM change for Disable DeepSx, DTT update and Reserve GPIO_SSD_RST.
2. [AMI_Changes][EIP None] Update for BIOS cannot boot to OS in Debug mode.
3. [AMI_Changes][EIP None] Update for XMP support.
4. [AMI_Changes][EIP None] Update for Hot Key F8 Active Windows Recovery Mode.
5. [AMI_Changes][EIP None] Update for TBT support.

Changes:

1. N/A

Known Errata:

1. System cannot power on after BIOS downgrade to AC0003 by F7/exe/iflashV.

ACADL357.0006.2021.0726.2309 Development BIOS

About This Release:

- Date: July 26 2021
- ROM Image Checksum: 0xB2A5B1C9
- ME Firmware: 16.0.10.1394
- EC Firmware: 0.06.00.000
- PMC Firmware: 160.01.00.1007
- Boot Guard ACM: None
- Memory Reference Code: Based on 0.0.2.52
- Integrated Graphics
  - UEFI Driver: 21.0.1028
- AHCI Code: Based on AHCI_26
- Wired LAN Adapter:
  - UEFI Driver:
  - N/A
- Supported Flash Devices:
  - WinBond W25Q256FV 32MB
  - GigaDevice GD25B256D 32MB
- Microcode Updates included in .ROM & .BIO Files:
  - M8290671_0000001A.pdb

New Fixes/Features:

1. [ODM_Changes][EIP None] Update ODM change for DG2_delay, Disable EVL MSG, LID status, PS2 KB and VMD setting
2. [AMI_Changes][EIP None] Update wireless control porting
3. [AMI_Changes][EIP None] Update for WOL from S5 porting
4. [AMI_Changes][EIP None] Update for touchpad cannot used in ESA Setup

Changes:

1. [ODM_CHANGE][EIP None] Update EC to 0.06.000

Known Errata:

1. System cannot power on after BIOS downgrade to AC0003 by F7/exe/iflashV.

ACADL357.0005.2021.0719.2050 Development BIOS

About This Release:

- Date: July 19 2021
- ROM Image Checksum: 0xB2AC7EE6
- ME Firmware: 16.0.10.1394
- EC Firmware: 0.05.00.000
- PMC Firmware: 160.01.00.1007
- Boot Guard ACM: None
- Memory Reference Code: Based on 0.0.2.52
- Integrated Graphics
  - UEFI Driver: 21.0.1028
- AHCI Code: Based on AHCI_26
- Wired LAN Adapter:
  - UEFI Driver:
  - N/A
- Supported Flash Devices:
  - WinBond W25Q256FV 32MB
  - GigaDevice GD25B256D 32MB
- Microcode Updates included in .ROM & .BIO Files:
  - M8290671_0000001A.pdb

New Fixes/Features:

1. [ODM Changes][EIP NONE] Update ODM change for Disable SPI1, ME_HDA_GPIO, Restart Fail by LAN, USB_UPD_PLD
2. [AMI Changes][EIP NONE] Remove WA for AC cannot boot to OS.
3. [AMI Changes][EIP NONE] Update change for WHQL test fail - BitLocker Tpm And Recovery Password tests for AOAC devices with PCR[7].
4. [AMI Changes][EIP NONE] Update ME_FW_IMAGE_VERSION to prevent ME from always following the BIOS update.
5. [AMI Changes][EIP NONE] Update for ME/EC recovery.
6. [AMI Changes][EIP NONE] Update for Memory size decrease and CPU ThermalTrip error log report code.
7. [AMI Changes][EIP NONE] Follow KC to integrate change for AutoRTCReset to meet EC behavior

Changes:

1. N/A

Known Errata:

1. System cannot power on after BIOS downgrade to AC0003 by F7/exe/iflashV.

ACADL357.0004.2021.0712.2200 Development BIOS

About This Release:

- Date: July 12 2021
- ROM Image Checksum: 0xB2BB0554
- ME Firmware: 16.0.10.1394
- EC Firmware: 0.05.00.000
- PMC Firmware: 160.01.00.1007
- Boot Guard ACM: None
- Memory Reference Code: Based on 0.0.2.52
- Integrated Graphics
  - UEFI Driver: 21.0.1028
- AHCI Code: Based on AHCI_26
- Wired LAN Adapter:
  - UEFI Driver:
  - N/A
- Supported Flash Devices:
  - WinBond W25Q256FV 32MB
  - GigaDevice GD25B256D 32MB
- Microcode Updates included in .ROM & .BIO Files:
  - M8290671_0000001A.pdb

New Fixes/Features:

1. [ODM Changes][EIP NONE] Implement ODM solution
2. [AMI Changes][EIP 623099][Intel-SPG][TF][AC] AC9002 will BSOD.
3. [AMI Changes][EIP NONE] Update CRB to CRB019.
4. [AMI Changes][EIP NONE] Update ME to 16.0.10.1394.
5. [AMI Changes][EIP NONE] Update auto RTC reset function.
6. [AMI Changes][EIP NONE] Dynamic update EC version for SMBIOS and OS.

Changes:

1. N/A

Known Errata:

1. System cannot power on after AC0004 downgrade to AC0003 by F7/exe/iflashV.

ACADL357.0003.2021.0705.2205 Development BIOS

About This Release:

- Date: July 05 2021
- ROM Image Checksum: 0xB3401FB3
- ME Firmware: 16.0.0.1318
- EC Firmware: 0.05.00.000
- PMC Firmware: 160.1.0.1007
- Boot Guard ACM: None
- Memory Reference Code: Based on 0.0.1.232
- Integrated Graphics
  - UEFI Driver: 21.0.1028
- AHCI Code: Based on AHCI_26
- Wired LAN Adapter:
  - UEFI Driver:
  - N/A
- Supported Flash Devices:
  - WinBond W25Q256FV 32MB
  - GigaDevice GD25B256D 32MB
- Microcode Updates included in .ROM & .BIO Files:
  - M8290671_00000017.pdb

New Fixes/Features:

1. [ODM Changes][EIP NONE] Implement ODM solution for disable unused devices.
2. [AMI Changes][EIP NONE] Disable BIOS Guard for FPT cannot flash.
3. [AMI Changes][EIP NONE] Add Setup Real-Time Performance Tuning item.
4. [AMI Changes][EIP NONE] Correct GPIO pin for security jumper.
5. [AMI Changes][EIP NONE] Update EC FW update porting.
6. [AMI Changes][EIP NONE] Update for PXE boot porting.
7. [AMI Changes][EIP619761][Intel-SPG][TF][AC] OFBD module SMI handler vulnerabilities.

Changes:

1. [AMI Changes][EIP NONE] Update EC to 0.05.00.000

Known Errata:

2. AC cannot reboot due to HW issue.

ACADL357.0002.2021.0629.0048 Development BIOS

About This Release:

- Date: Jun 28 2021
- ROM Image Checksum: 0xB2344440
- ME Firmware: 16.0.0.1318
- EC Firmware: 0.04.00.000
- PMC Firmware: 160.1.0.1007
- Boot Guard ACM: None
- Memory Reference Code: Based on 0.0.1.232
- Integrated Graphics
  - UEFI Driver: 21.0.1028
- AHCI Code: Based on AHCI_26
- Wired LAN Adapter:
  - UEFI Driver:
  - N/A
- Supported Flash Devices:
  - WinBond W25Q256FV 32MB
  - GigaDevice GD25B256D 32MB
- Microcode Updates included in .ROM & .BIO Files:
  - M8290671_00000017.pdb

New Fixes/Features:

1. [ODM Changes][EIP NONE] Implement ODM solution.
2. [AMI Changes][EIP NONE] Update CRB to CRB015.
3. [AMI Changes][EIP NONE]Enable BIOS guard.
4. [AMI Changes][EIP NONE]Update EC version in Setup.
5. [AMI Changes][EIP NONE]Update Setup for USB and Storage page.

Changes:

1. [ODM Changes][EIP NONE] Update EC to 0.04.00.000

Known Errata:

1. USB cannot be used since EC is not ready.
2. AC cannot reboot due to HW issue.

ACADL357.0001.2021.0621.2252 Development BIOS

About This Release:

- Date: Jun 21 2021
- ROM Image Checksum: 0xB657E495
- ME Firmware: 16.0.0.1318
- EC Firmware: 0.02.00.000
- PMC Firmware: 160.1.0.1007
- Boot Guard ACM: None
- Memory Reference Code: Based on 0.0.1.212
- Integrated Graphics
  - UEFI Driver: 21.0.1028
- AHCI Code: Based on AHCI_26
- Wired LAN Adapter:
  - UEFI Driver:
  - N/A
- Supported Flash Devices:
  - WinBond W25Q256FV 32MB
  - GigaDevice GD25B256D 32MB
- Microcode Updates included in .ROM & .BIO Files:
  - M8290671_00000017.pdb

New Fixes/Features:

1. [AMI Changes][EIP NONE] Update SPG module into AC project
2. [ODM Changes][EIP NONE] Implement ODM solution for AC power on.

Changes:

1.

Known Errata:

1. USB cannot be used since EC is not ready.