



BIOS Update Release Notes

PRODUCTS: NUC11TNBi3/K/H, NUC11TNBi5/K/H, NUC11TNBi7/K/H

BIOS Version 0058 - TNTGL357.0058.2021.0813.1709

About This Release:

- Date: Aug 13, 2021
- ROM Image Checksum: 683d13cf
- ME Firmware: 15.0.10.1574v1.2
- EC Firmware: TIGA370000
- PMC Firmware: PMC_B0_150.01.20.1032_prod
- Boot Guard ACM: 1.14.15
- Memory Reference Code: Based on 0A.00.38.51
- Integrated Graphics
 - UEFI Driver: 17.0.1052
- Intel RST Pre-OS:
 - VMD UEFI Driver: 18.0.5.5115
- AHCI Code: Based on AHCI_24
- Wired LAN Adapter:
 - UEFI Driver: 0.8.05
- Visual BIOS: Intel AptioV
- Supported Flash Devices:
 - MACRONIX MX25L25645G 32MB
- Microcode Updates included in .BIN & .CAP Files:
 - m80806c1_0000008a
 - m80806c1_0000007e

New Fixes/Features:

- Fixed EC Firmware text typo during BIOS flash update.
- Updated CPU Microcode to m80806c1_0000008a, m80806c1_0000007e.
- Updated ME Firmware to 15.0.10.1574v1.2
- Added event log support for Auto RTC feature.
- Fixed issue where Virtual Display emulation did not allow BIOS KVM access.
- Added pop-up warning message to user when transition BIOS is necessary.
- Added new BIOS item: Force-enable power to 2242 m.2 slot.

Known Errata:

- Flashing from TN0052/TN0053 to TN0054 still stay on POST logo for about 4mins, TN0054 to TN0054 will not see this.
- TN0032 added code change for new DmiEdit tool, please use latest version of AMI/Intel tools.

BIOS Version 0057 - TNTGL357.0057.2021.0609.1511

About This Release:

- Date: Jun 9, 2021
- ROM Image Checksum: 7f54fc8b

*Other names and brands may be claimed as the property of others.

- ME Firmware: 15.0.10.1469
- EC Firmware: TIGA360000
- PMC Firmware: 150.01.20.1028
- Boot Guard ACM: 1.14.15
- Memory Reference Code: Based on 0A.00.38.51
- Integrated Graphics:
 - UEFI Driver: 17.0.1052
- Intel RST Pre-OS:
 - VMD UEFI Driver: 18.0.5.5115
- AHCI Code: Based on AHCI_24
- Wired LAN Adapter:
 - UEFI Driver: 0.8.05
- Visual BIOS: Intel AptioV
- Supported Flash Devices:
 - MACRONIX MX25L25645G 32MB
- Microcode Updates included in .BIN & .CAP Files:
 - M80806C1_00000072.pdb

New Fixes/Features:

- Disabled BIOS Manufacturing mode.

BIOS Version 0056 - TNTGL357.0056.2021.0513.1618

About This Release:

- Date: May 13, 2021
- ROM Image Checksum: baf92c8f
- ME Firmware: 15.0.10.1469
- EC Firmware: TIGA360000
- PMC Firmware: 150.01.20.1028
- Boot Guard ACM: 1.14.15
- Memory Reference Code: Based on 0A.00.38.51
- Integrated Graphics:
 - UEFI Driver: 17.0.1052
- Intel RST Pre-OS:
 - VMD UEFI Driver: 18.0.5.5115
- AHCI Code: Based on AHCI_24
- Wired LAN Adapter:
 - UEFI Driver: 0.8.05
- Visual BIOS: Intel AptioV
- Supported Flash Devices:
 - MACRONIX MX25L25645G 32MB
- Microcode Updates included in .BIN & .CAP Files:
 - M80806C1_00000072.pdb

New Fixes/Features:

- Fixed issue where help text was missing after loading "F9" defaults.
- Updated EC Firmware to TIGA360000.
- Fixed issue where after re-plugging HDMI/Type-C cable on the boot menu screen, the screen was abnormal.
- Fixed issue when Fan control mode was set to "Custom", CPU fan was not spinning.

*Other names and brands may be claimed as the property of others.

BIOS Version 0054 - TNTGL357.0054.2021.0316.1417

About This Release:

- Date: Mar, 16 2021
- ROM Image Checksum: 934ba40c
- ME Firmware: 15.0.10.1469
- EC Firmware: TIGA340000
- PMC Firmware: 150.01.20.1028
- Boot Guard ACM: 1.14.15
- Memory Reference Code: Based on 0A.00.38.51
- Integrated Graphics:
 - UEFI Driver: 17.0.1052
- Intel RST Pre-OS:
 - VMD UEFI Driver: 18.0.5.5115
- AHCI Code: Based on AHCI_24
- Wired LAN Adapter:
 - UEFI Driver: 0.8.05
- Visual BIOS: Intel AptioV

- Supported Flash Devices:
 - MACRONIX MX25L25645G 32MB

- Microcode Updates included in .BIN & .CAP Files:
 - M80806C1_00000072.pdb

New Fixes/Features:

- Fixed POST display emulation after HDMI reconnection.
- Updated Retimer dynamic function.
- Updated EC firmware to TIGA340000
- Updated ME firmware to 15.0.10.1469
- Updated Retimer firmware to 2.17
- Changed virtual display setup.
- Fixed ME upgrade failure using security jumper recovery.
- Updated TXT version to 1.14.15
- Fixed issue with USB2.0 port functionality after disabling Thunderbolt™ Support in the BIOS.
- Changed Cooling-Balanced Fan Off Temperature of CPUVR default.
- Enabled "TCO Timer" setup option.
- Adjusted POST screen QRCode position.
- Added Self-Healing module.
- Updated CPU Microcode to m80806c1_00000072.
- Fixed issue where system would stay on POST logo screen for about 4 minutes before flash update started.
- Updated NTFS DXE driver regarding parsing NTFS file system partition.
- Fixed issue with display emulation missing POST information after HDMI re-plug in.
-

BIOS Version 0043 - TNTGL357.0043.2020.1223.1022

About This Release:

- Date: Dec 23, 2020

*Other names and brands may be claimed as the property of others.

- ROM Image Checksum: 41AA299A
- ME Firmware: 15.0.10.1414
- EC Firmware: TIGA320000
- PMC Firmware: 150.01.20.1026
- Boot Guard ACM: 1.14.12
- Memory Reference Code: Based on 0A.00.30.51
- Integrated Graphics:
 - UEFI Driver: 17.0.1045
- Intel RST Pre-OS:
 - VMD UEFI Driver: 18.0.2.5008
- AHCI Code: Based on AHCI_24
- Wired LAN Adapter:
 - UEFI Driver: 0.8.05
- Visual BIOS: Intel AptioV
- Supported Flash Devices:
 - MACRONIX MX25L25645G 32MB
- Microcode Updates included in .BIN & .CAP Files:
 - M80806C1_0000006C.pdb

New Fixes/Features:

- Fixed issue with active/link LED still on when LAN is disabled in BIOS.
- Fixed modern standby blinking behavior.

BIOS Version 0038 - TNTGL357.0038.2020.1124.1648

About This Release:

- Date: Nov 24, 2020
- ROM Image Checksum: c01834bb
- ME Firmware: 15.0.10.1414
- EC Firmware: TIGA300000
- PMC Firmware: 150.01.20.1026
- Boot Guard ACM: 1.14.12
- Memory Reference Code: Based on 0A.00.30.51
- Integrated Graphics:
 - UEFI Driver: 17.0.1045
- Intel RST Pre-OS:
 - VMD UEFI Driver: 18.0.2.5008
- AHCI Code: Based on AHCI_24
- Wired LAN Adapter:
 - UEFI Driver: 0.8.05
- Visual BIOS: Intel AptioV
- Supported Flash Devices:
 - MACRONIX MX25L25645G 32MB
- Microcode Updates included in .BIN & .CAP Files:
 - M80806C1_0000006C.pdb

New Fixes/Features:

*Other names and brands may be claimed as the property of others.

- Initial production BIOS release

LEGAL INFORMATION

Information in this document is provided in connection with Intel Products and for the purpose of supporting Intel developed server/desktop boards and systems.

No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted by this document. Except as provided in Intel's Terms and Conditions of Sale for such products, Intel assumes no liability whatsoever, and Intel disclaims any express or implied warranty, relating to sale and/or use of Intel products including liability or warranties relating to fitness for a particular purpose, merchantability, or infringement of any patent, copyright or other intellectual property right. Intel Corporation may have patents or pending patent applications, trademarks, copyrights, or other intellectual property rights that relate to the presented subject matter. The furnishing of documents and other materials and information does not provide any license, express or implied, by estoppel or otherwise, to any such patents, trademarks, copyrights, or other intellectual property rights. Intel products are not intended for use in medical, life saving, or life sustaining applications. Intel may make changes to specifications and product descriptions at any time, without notice.

Intel is a trademark of Intel Corporation in the US and other countries.
Copyright (c) 2021 Intel Corporation.