Skylake Desktop

BIOS Release Document

Designed by Fujitsu

- D3400-A/B1
- D3401-A/B1
- D3402-A/B1
- D3410-B1
- D3417-A/B1

Content

Revision History:

Date	BIOS Version	Notes
18.03.2020	R1.29.0	Added new BIOS version Changed whole document to Kontron design Reordered some chapters
22.08.2019	R1.28.0	Added new BIOS version (R1.28.0).
06.11.2018	R1.27.0	Added new BIOS version (R1.27.0).
02.07.2018	R1.26.0	Added new BIOS version (R1.26.0). Updated hyperlinks.
17.04.2018	R1.24.0	Updated CVE number for Reference Code
20.02.2017	R1.25.0	Added new BIOS version (R1.25.0)
15.12.2017	R1.24.0	Added new BIOS version (R1.24.0)
31.08.2017	R1.22.0	Added new BIOS version (R1.21.0) only for D3402-B1 & D3417-B1
26.06.2017	R1.21.0	Updated CPU Microcode Patch version number
20.06.2017	R1.21.0	Updated Known Issus for Bios R1.20.0 and R1.21.0
02.06.2017	R1.21.0	Added new BIOS version (R1.21.0)
02.05.2017	R1.20.0	Added new BIOS version (R1.20.0)
03.11.2016	R1.17.0	Added new BIOS version (R1.16.0 and R1.17.0)
13.07.2016	R1.15.0	Added new BIOS version (R1.15.0)
04.07.2016	R1.14.0	Added new BIOS version (R1.14.0)
02.03.2016	R1.13.0	Added new BIOS version (R1.13.0)
26.02.2016	R1.12.0	Added new BIOS version only for D3417 (R1.12.0) Updated Chapter 1.3: Added tool BIOSSET
17.02.2016	R1.11.0	Added new BIOS version (R1.11.0)
02.12.2015	R1.8.0	Added new BIOS version (R1.8.0)
06.11.2015 13.11.2015	R1.6.0	Added new BIOS version (R1.6.0) Updated chapter 1 Updated BIOS 1.6.0 known issues
30.10.2015	R1.4.0	Added new BIOS version (R1.4.0) Updated chapters 1, 1.2 and 1.3
05.10.2015	R1.3.0	Initial mass production release

1. General Notes

- AMI Aptio V5.0.0.11

Caution: These BIOS updates are only for mass production version mainboards (GS1 and newer).

All preproduction mainboards (GS5x, GS6x) were manufactured with BIOS version lower than 1.3.0 and should not be updated to BIOS version 1.3.0 or newer - this might cause problems. Please scrap these old mainboards.

1.1 Released OS Versions

- MS Windows 7 (32/64bit)
- MS Windows 8.1 (64bit)
- MS Windows 10 (64bit)

1.2 BIOS Update Options

DOS Flash Update

Use ZIP-files for DOS-based BIOS Update
→ Copy related files (folder "DOS") to a DOS-bootable device and run <DosFlash.BAT>

Please see the BIOS-Flash-Tools documentation for more information:
ftp://ftp.kontron.com/Services/Software_Tools/BIOS-Flash-Tools/

Windows Flash Update

Use Dxxx-xyz.DFI.$xe for Windows-based BIOS update
→ Rename file to *.exe after download and run exe-file from MS Windows

Auto BIOS Update

With Auto BIOS Update it is possible to check a Fujitsu server automatically to see if there is a new BIOS version for the system. For the update, no operating system or external storage medium is required. This feature must be enabled in BIOS Setup first.
For details on the Auto BIOS Update function please see the BIOS manual.

BIOS Recovery

Please see the BIOS-Flash-Tools documentation for more information:
ftp://ftp.kontron.com/Services/Software_Tools/BIOS-Flash-Tools/

Additional information

If you have any problems after a BIOS flash please try if “Load Optimized Default Values” (F3) in BIOS setup solves the problem.

1.3 FTP BIOS Folder

The released BIOS version is available here:

D3400:
ftp://ftp.kontron.com/Products/Motherboards/EoL_Motherboards/EoL_ClassicDesktop/D34xx/D3400_D3410/BIOS_D3400/

D3410:
ftp://ftp.kontron.com/Products/Motherboards/EoL_Motherboards/EoL_ClassicDesktop/D34xx/D3400_D3410/BIOS_D3410/

D3401 / D3402-A / D3417-A:
ftp://ftp.kontron.com/Products/Motherboards/EoL_Motherboards/EoL_ClassicDesktop/D34xx/D3401_D3402-A_D3417-A/BIOS_D3401_D3402-A_D3417-A/

D3402-B1 / D3417-B1:
ftp://ftp.kontron.com/Products/Motherboards/ExtendedLifeCycle/D3402-B_D3417-B/BIOS/

1.4 How to create a DOS bootable USB stick?

You can use the Fujitsu tool FTS_Basic-BootStick.EXE to easily create a Free-DOS bootable Stick:
ftp://ftp.kontron.com/Services/Software_Tools/Common-Mainboard-Tools/USB-FreeDOS-Bootstick/
Rename file from *.$xe to *.exe and run tool in Windows.

1.5 Modify BIOS Setup Settings and Defaults (Tool EditCMOS / BIOSSET) [updated]

The file D34**-***.R1.x.0.SetupItemId.txt provides the list of BIOS Setup items that this BIOS version allows to be modified by the DOS tool EditCMOS (Modify BIOS Setup Settings and Defaults).

See EditCMOS tool for further details:
ftp://ftp.kontron.com/Services/Software_Tools/Common-Mainboard-Tools/EditCMOS_UEFI/

For Windows/Linux the Tool BIOSSET can be used instead, it is part of this package:
ftp://ftp.kontron.com/Services/Software_Tools/Common-Mainboard-Tools/BiosSet/

Both tools are also described in our Manufacturing-Tools HowTo document:
ftp://ftp.kontron.com/Services/Software_Tools/Common-Mainboard-Tools/

1.6 Note: Customer Service Release BIOS

Besides the released BIOS versions there may be additional BIOS versions
(Customer Service Release BIOS = CSR BIOS) that solve specific customer problems.
Please note: These versions are available via OEM FTP only and they are not pre-installed ex factory.

2. BIOS R1.3.0

First released mass production BIOS

Known Issues and Limitations:

3. BIOS R1.4.0

Changes vs. previous released BIOS

- Improved: now TXT can only be enabled if VT-d and TPM support is enabled.
- Solved (D3417 only): TXT hang when using E3 CPU.
- Solved: POST hang with Matrox ExtIo cards.
- Solved: “Device found” message was shown in Setup when TPM is disabled.
- Feature: Update Microcode for CPUID 506E3 to version 4A. This enables SGX support on supported CPUs
- Solved: System showed “ERROR – FAN fault: SYS2” and beeps.
- Solved: HCT Resstomp Test failed in Win7 32-bit.
- Solved: Issue with Emulex FCoE adapter.
- Solved: Entering Setup or boot menu wasn’t working reliably when system holds due to HDD SMART error.
- Solved: System boot was hanging if an M.2 PCIe NVMe card was plugged
- Solved: Sensor name of SMBIOS “Battery voltage errors” corrected.
- Solved: If User Password is the same as HDD password, HDD password was also required.

Known Issues and Limitations:

- In the Boot Option Priorities list some options might be shown multiple times
- Bitlocker Drive Encyption doesn’t work with Win7 32Bit and TPM 1.2
- (D3417 only) Error Beep doesn't sound for No Memory
- After TPM clear, during POST the system may be reset by watchdog if waiting too long for user input.

4. BIOS R1.6.0

Changes vs. previous released BIOS

- Solved: Bitlocker Drive Encyption problem with Win7 32Bit and TPM 1.2
- Improved (D3417 only): ECC Memory Error Logging
- Solved: USB port description was not correct for D3400A/B. This meant one WHQL test couldn't pass.
- Solved: Some function keys caused incorrect behavior of POST if pressed at legacy OPROM scan.
- Solved: ME Update issues after Setup Load Defaults and sporadically under other circumstances
- Solved: There was no Error Beep for No Memory
- Feature (D34xx-B only): Updated Thermal management firmware to also allow battery measurement with additional load. AC fail is necessary to activate new the firmware.
- Solved: After TPM clear, during POST the system could be reset by watchdog if waiting too long for user input.
- Improved: Prevent setting Internal Graphics to Disabled if no graphics card is plugged
- Solved: Over temperature event was not logged in BIOS event log
- Solved: ASPM Setup item couldn't be changed via EditCMOS/BIOSSET
- Solved: Write Read Verify-Feature was not working after S3 resume
- Solved: PowerCycle-Reset after BIOS update didn't work
- Solved: BIOS didn't control serial port signals by ACPI method
- Solved: Console Redirection stayed with black screen when entering Setup (keyboard still works)
- Solved: In Boot Option Priorities List some options could be shown multiple times
- Solved: ACPI-RSDP table was present even if CSM was disabled

Known Issues and Limitations:

- D3410-B only: USB port description is not correct. This means one WHQL test cannot pass. This is fixed in BIOS 1.8.0.
- The feature "fan startup check" (default: disabled) might warn in POST that some fans are missing. To fix this, enter setup and save & reset. This will save which fans are actually attached.
- Under some circumstances WOL may not work for onboard LAN when system enters S3 or S4. This issue is fixed in BIOS 1.8.0.
- Boot logo position may not be correct in Legacy/CSM boot mode with some external graphics cards. This issue is fixed in BIOS 1.8.0.

5. BIOS R1.8.0

Changes vs. previous released BIOS

- Solved: Under some circumstances WOL from S3 or S4 was not working for onboard LAN.
- Solved: OS could not be installed using SATA DVD ROM in Secure Boot UEFI mode.
- Solved (D3410-B only): USB port description was not correct. This meant one WHQL test could not pass.
- Solved: The feature “fan startup check” (default: disabled) might warn in POST that some fans are missing. To fix this, enter setup and save & reset. This will save which fans are actually attached.
- Solved: Boot logo position was not correct in Legacy/CSM boot mode with some external graphics cards.
- Solved: System fan ran with full speed after changing fan control from “Enhanced” to “Auto”
- Improvement: Updated UEFI LAN Option ROM to version E0009X7. Now UEFI PXE Boot is available also without active link.
- Improvement: PS/2 keyboard LEDs are switched off when system enters S3.
- Improvement: Updated TXT support.
- Improvement: Updated CPU Microcode Patch for Skylake DT R-0/S-0 CPUs (CPU-ID 506E3) to version 00000056h.

Known Issues and Limitations:

- none

6. BIOS R1.11.0

Changes vs. previous released BIOS

- Updated to Management Engine Firmware version 11.0.0.1205
- Updated to CPU Microcode Patch 0x74
- Feature: Added support for NVMe SSDs to HDD Security Feature
- Feature: Added PS/2 Emulation setup option in USB configuration page which allows USB Keyboard/Mouse to be used in Windows 7 install before XHCI driver is installed
- Feature: USB Keyboard supports wake-up/power on via any key
- Feature: Setup items [Intel ATM] and [USB Provisioning of AMT] added. Note: BSI Saftey Warning / Vulnerability of unprovisioned Intel-AMT Platforms
- Feature: Added support to control setup options using EditCMOS/BIOSSET:
    - DASH
    - SATA Controller
    - Intel® AMT (0x1C2h)
    - USB Provisioning of AMT (0x1C3h)
    - PS/2 Emulation (0x1C4h)
    - Usb Port Control (0xC5)
- Solved: ODD auto playback under OS did not work
- Solved: Keystrokes were not detected during Auto BIOS Update
- Solved: Press <F2> to enter Setup is in Japanese if Quiet Boot and Boot Menu are disabled
- Solved: Change behavior of F4 and ESC hot keys in SETUP to always reset the mainboard
- Solved: It was possible to set password for disks within RAID which results in a non-bootable OS
- Solved: Fix issue with multiple UEFI boot order entry on external USB hard drive.
- Solved: Sometimes no beep code during BIOS recovery
- Solved: SSDs could not be deleted using optional BIOS feature Erase Disk
- Solved: Fix sporadic error in intrusion detection
- Solved: Onboard WOL was not working reliably for some USB xHCI settings

Known Issues and Limitations:

- none

7. BIOS R1.12.0

Changes vs. previous released BIOS

- Improvement: Updated Thermal management firmware to solve issues in cases where fan speeds increase very fast. AC fail is necessary to activate new the firmware.

Known Issues and Limitations:

- none

8. BIOS R1.13.0

Changes vs. previous released BIOS

- Updated to Management Engine Firmware version 11.0.1.1001
- Updated to CPU Microcode Patch 0x74
- Solved: POST hang with 64GB RAM populated and both internal graphics and PCIe graphics card enabled
- Feature: prevent power-button switch off and CTRL+ALT+DEL during BIOS update in POST.
- Solved: POST hang with some types of USB Cardreaders
- Solved: Sporadic Display Flickering with internal graphics
- Solved: Corrected HDD password behavior during POST if Setup entry is requested via F2 key
- Solved: Platform boots with TXT enabled although TPM is not provisioned.
- Solved: Grayout "TPM Disable" if TXT is enabled
- Solved: Hang after PME/WOL Wakeup of devices behind a PCIe-to-PCI Bridge
- Feature: Idle mode power optimization for M.2 PCIe slots. This requires loading of defaults in BIOS Setup.

Known Issues and Limitations:

- none

9. BIOS R1.14.0

Changes vs. previous released BIOS

- Updated to Management Engine Firmware version 11.0.12.1008
- Updated to CPU Microcode Patch 0x8A
- Updated System monitoring characteristics for D3400-B1, D3401-B1 and D3410-B1
- Feature: “Intel TXT support” option is now visible in Advanced -> CPU Configuration
- Feature: USB Keyboard wake up on any key is disabled for Fujitsu USB keyboards equipped with Power Button. For these keyboards the dedicated Power Button is the only key that can start a system.
- Fixed: Beep on POST did not work on some boards
- Fixed: TPM 2.0 SHA2 setting did not work
- Fixed: Correction of periodic timer inaccuracy on Skylake platforms
- Fixed: Windows 10 goes to OS recovery mode with certain Setup configuration
- Fixed: The SystemLock 3 PIN dialog box has been skipped in POST if no monitor was attached
- Fixed: With TXT enabled and a discrete TPM1.2 (in state unowned) a POST error message will be shown
- Fixed: Sytem does not boot from a RAID volume of the PCH-RAID when a HDD Password is set and the legacy RAID OPROM is active.
- Fixed: The PS2 wake up should only wake from S3. It was also possible to wake the System from S4 and hybrid S5. Now the system can only be waken in S3.
- Fixed (B150 chipset only): Not supported AMT features turned off in Advanced AMT configuration menu.

Known Issues and Limitations:

- System does not boot from HDD when press Ctrl+Alt+Del in BIOS POST. All SATA devices are disabled until next reset.

10. BIOS R1.15.0

Changes vs. previous released BIOS – only released for D3402 and D3417

- Updated System monitoring characteristics for D3402-B1 and D3417-B1
- Fixed: BIOS did not start on boards equipped with Infinion TPM2.0 when TXT was enabled

Known Issues and Limitations:

- System does not boot from HDD when press Ctrl+Alt+Del in BIOS POST. All SATA devices are disabled until next reset.

11. BIOS R1.16.0

Changes vs. previous released BIOS

- Updated to Management Engine Firmware version 11.0.17.1002
- Updated to CPU Microcode Patch 0xA2
- Fixed: Sporadically the fan was running with wrong speed after ACPI-S3 resume
- Fixed: Configuration of Intel TXT Support now is only possible with discrete TPM
- Fixed: 'Force LAN Boot' sometimes did not work
- Fixed: Headless RAID HDD boot was not possible
- Fixed: BIOS setting “Restore User Defaults” was showing a wrong dialog box

Known Issues and Limitations:

- System does not boot from HDD when press Ctrl+Alt+Del in BIOS POST. All SATA devices are disabled until next reset.

12. BIOS R1.17.0

Changes vs. previous released BIOS

- Updated to Management Engine Firmware version 11.0.18.1002
- Updated to CPU Microcode Patch 0xA6
- Fixed: Unsupported iAMT message from POST diagnostic screen removed
- Fixed: Possible BIOS POST hangs with BIOS setup setting “Intel TXT Support: Enabled” (at “Advanced – CPU Configuration” submenu)
- Fixed: Windows recovery mode started when using BIOS setup setting “Boot Removable Media: Disabled” (at “Boot” submenu) and connected USB media.
- Fixed: Internal USB devices show up as removable in Windows
- Fixed: Mainboard automatically switches on after AC fail if “Power-On Source” is set to “ACPI Controlled” an “Power Failure Recovery” is disabled

Known Issues and Limitations:

- System does not boot from HDD when press Ctrl+Alt+Del in BIOS POST. All SATA devices are disabled until next reset.

13. BIOS R1.20.0

Changes vs. previous released BIOS

- Updated to Management Engine Firmware version 11.0.22.1000.
- Updated to CPU Microcode Patch 0xB2 for Skylake R0/S0.
- Updated to System Management Controller (Teutates) Firmware 46.
- Updated Intel PXE Oprom to V.0.1.10 and UEFI driver E0014X7.
- Fixed: URL to the Fujitsu Open Source Software License Information was missing.
- Fixed: Confirmation of detected intrusion ("Housing monitoring: Enabled") via Administrator password was not working properly.
- Fixed: UEFI PXE boot devices were visible in Setup even if "Launch PXE OpROM Policy" was set to "Do not launch" or "Legacy only".
- Fixed: Sporadic speaker beep while power button was pressed quite long (e.g. 2 seconds) to resume from sleep (S3).
- Fixed: BIOS update at Windows with Hyper V / DeviceGuard enabled not working.
- Fixed: System hang occurred if Hyper V is enabled.
- Fixed: Adjustment of watchdog operation during F12 Boot Menu display.
- Fixed: Setup option "HDD Password on Boot" = "Disabled" was ignored in case of NVMe drives.
- Fixed: If “Secure Boot Control” set to Enabled in BIOS Setup and execute Load Setup Default by BiosSet.exe. Afterwards “Secure Boot Control” was not set back to default value “Disabled”
- Fixed: BiosSet.exe /wakeonrtc did not return status “ON”.
- Fixed: BiosSet.exe command for setting a password did not work.
- Fixed: Speed of setup page “Acoustic Management Configuration” was increased and unexpected items are removed.
- Fixed: Fan, sensor and voltage names will be displayed correctly at BIOS Event Log.
- Fixed: Intel display audio device disappeared after resume from S3.
- Fixed: TPM PPI Clear failed with BiosSet.
- Fixed: Sporadically some M.2 NVMe drives disappears after reboot

Known Issues and Limitations:

- System does not boot from HDD when press Ctrl+Alt+Del in BIOS POST. All SATA devices are disabled until next reset.
- When using USB keyboard and starting some programs at FreeDOS installation, <Enter> key is auto-repeated.
- BIOS sporadically recognizes non-connected FANs (e.g. FAN PSU).
    - Workaround: To prevent, that the BIOS POST will stop with the error message “ERROR – FAN absent: PSU”, change the BIOS setting [Boot > Boot error handling] to “Continue”.

14. BIOS R1.21.0

Changes vs. previous released BIOS

- Updated to Management Engine Firmware version 11.0.25.3001.
    - Fix for INTEL-SA-00075 / CVE-2017-5689
- Updated CPU Microcode (0xBA) for Skylake R0/S0.
- Updated System monitoring characteristics for D3402-A1 only.

Known Issues and Limitations:

- System does not boot from HDD when press Ctrl+Alt+Del in BIOS POST. All SATA devices are disabled until next reset.
- When using USB keyboard and starting some programs at FreeDOS installation, <Enter> key is auto-repeated.
- BIOS sporadically recognizes non-connected FANs (e.g. FAN PSU).
    - Workaround: To prevent, that the BIOS POST will stop with the error message "ERROR – FAN absent: PSU", change the BIOS setting [Boot > Boot error handling] to "Continue".

15. BIOS R1.22.0

Changes vs. previous released BIOS

- Updated System monitoring characteristics (only D3402-B1 and D3417-B1).
- Updated “Auto BIOS Update” functionality
- Fixed: When using USB keyboard and starting some programs at FreeDOS installation, <Enter> key is auto-repeated.
- Fixed: BIOS setup defaults are set after several BIOS Updates.
- Fixed: “Secure Boot” was always prevented from being restored to default “Disabled” value.
- Fixed: Teutates system monitoring runtime sensor event logging not functional.
- Feature: “Secure Boot Control” will not change during battery removal.
- Feature: Allow beep at the end of POST

Known Issues and Limitations:

- System does not boot from HDD when press Ctrl+Alt+Del in BIOS POST. All SATA devices are disabled until next reset.

16. BIOS R1.24.0

Changes vs. previous released BIOS

- Updated to Management Engine Firmware version 11.8.50.3425.
    - Fix for INTEL-SA-00086
- Updated GOP/VBT
- Updated Intel Reference Code (CVE-2017-5703)
- Fixed: WOL does not work with PCI LAN card FMV-1813
- Fixed: PXE boot failures with IPv6 occurred.

Known Issues and Limitations:

- System does not boot from HDD when press Ctrl+Alt+Del in BIOS POST. All SATA devices are disabled until next reset.
- Not all BIOS Setup settings are reset to default values via CMOS battery removal.
- First HDD password entry was "Invalid Password" when BIOS setup setting "Password on Boot" is "On Every Boot" or "On First Boot".

17. BIOS R1.25.0

Changes vs. previous released BIOS

- Updated CPU Microcode (0xC2) for Skylake R0/S0.
    - Needed for Intel-SA-00088 (CVE2017-5715)

Known Issues and Limitations:

- System does not boot from HDD when press Ctrl+Alt+Del in BIOS POST. All SATA devices are disabled until next reset.
- Not all BIOS Setup settings are reset to default values via CMOS battery removal.
- First HDD password entry was "Invalid Password" when BIOS setup setting "Password on Boot" is "On Every Boot" or "On First Boot".

18. BIOS R1.26.0

Changes vs. previous released BIOS

- Updated CPU Microcode (0xC6) for Skylake R0/S0.
    - Needed for Intel-SA-00115 (CVE2018-3639, CVE2018-3640)

Known Issues and Limitations:

- System does not boot from HDD when press Ctrl+Alt+Del in BIOS POST. All SATA devices are disabled until next reset.
- Not all BIOS Setup settings are reset to default values via CMOS battery removal.
- First HDD password entry was "Invalid Password" when BIOS setup setting "Password on Boot" is "On Every Boot" or "On First Boot".

19. BIOS R1.27.0

Changes vs. previous released BIOS

- Updated to Management Engine Firmware version 11.8.55.3510.
    - Fix for CVE-2018-3616, CVE-2018-3643, CVE-2018-3644, CVE-2018-3655, CVE-2018-3657, CVE-2018-3658, CVE-2018-3659
- Feature: Updated EraseDisk to version 4.6
- Feature: Improved Auto BIOS Update

Known Issues and Limitations:

- System does not boot from HDD when press Ctrl+Alt+Del in BIOS POST. All SATA devices are disabled until next reset.
- Not all BIOS Setup settings are reset to default values via CMOS battery removal.
- First HDD password entry was "Invalid Password" when BIOS setup setting "Password on Boot" is "On Every Boot" or "On First Boot".

20. BIOS R1.28.0

Changes vs. previous released BIOS

- Updated CPU Microcode (0xCC) for Skylake R0/S0 and (0x200005E) for Skylake XEON
  - INTEL-SA-00115, CVE-2018-12126, CVE-2018-12127, CVE-2018-12130
- Updated Management Engine Firmware version 11.8.65.3590
  - INTEL-SA-00185, PSIRT-TA-201810-004, PSIRT-TA-201901-002, CVE-2018-12188, CVE-2018-12189, CVE-2018-12190, CVE-2018-12191, CVE-2018-12192, CVE-2018-12199, CVE-2018-12198, CVE-2018-12200, CVE-2018-12187, CVE-2018-12196, CVE-2018-12185, CVE-2019-0089, CVE-2019-0090, CVE-2019-0086, CVE-2019-0091, CVE-2019-0092, CVE-2019-0093, CVE-2019-0094, CVE-2019-0096, CVE-2019-0097, CVE-2019-0098, CVE-2019-0099)
- Fixed: Linux Deskflash update problems occurred
- Fixed: Windows Boot Manager was missing under some circumstances.
- Fixed: 14TB hard disk sporadically not recognized at SATA port 2.
- Feature: BIOS option “Launch Storage OpRom” added [Advanced > CSM Configuration]

Known Issues and Limitations:

- System does not boot from HDD when press Ctrl+Alt+Del in BIOS POST. All SATA devices are disabled until next reset.
- Not all BIOS Setup settings are reset to default values via CMOS battery removal.
- First HDD password entry was "Invalid Password" when BIOS setup setting "Password on Boot" is "On Every Boot" or "On First Boot".

21. BIOS R1.29.0 [new]

Changes vs. previous released BIOS

- Intel IPU 2019 Q2 Security Update - Integrated Fixes for CVE-2019-0117, CVE-2019-0123, CVE-2019-0124, CVE-2019-0131, CVE-2019-0151, CVE-2019-0166, CVE-2019-0168, CVE-2019-0169, CVE-2019-0184, CVE-2019-11087, CVE-2019-11088, CVE-2019-11090, CVE-2019-11097, CVE-2019-11100, CVE-2019-11100, CVE-2019-11101, CVE-2019-11102, CVE-2019-11104, CVE-2019-11106, CVE-2019-11157, CVE-2019-11157
- Updated CPU Microcode for Skylake R0/S0 (0xD6) and for Skylake Xeon (0x65)
- Updated to Management Engine Firmware version 11.8.71.3630

Known Issues and Limitations:

- System does not boot from HDD when press Ctrl+Alt+Del in BIOS POST. All SATA devices are disabled until next reset.
- Not all BIOS Setup settings are reset to default values via CMOS battery removal.
- First HDD password entry was "Invalid Password" when BIOS setup setting "Password on Boot" is "On Every Boot" or "On First Boot".

Global Headquarters

Kontron S&T AG

Lise-Meitner-Str. 3-5
86156 Augsburg, Germany
Tel.: +49 821 4086 0
Fax: +49 821 4086 111
info@kontron.com
www.kontron.com