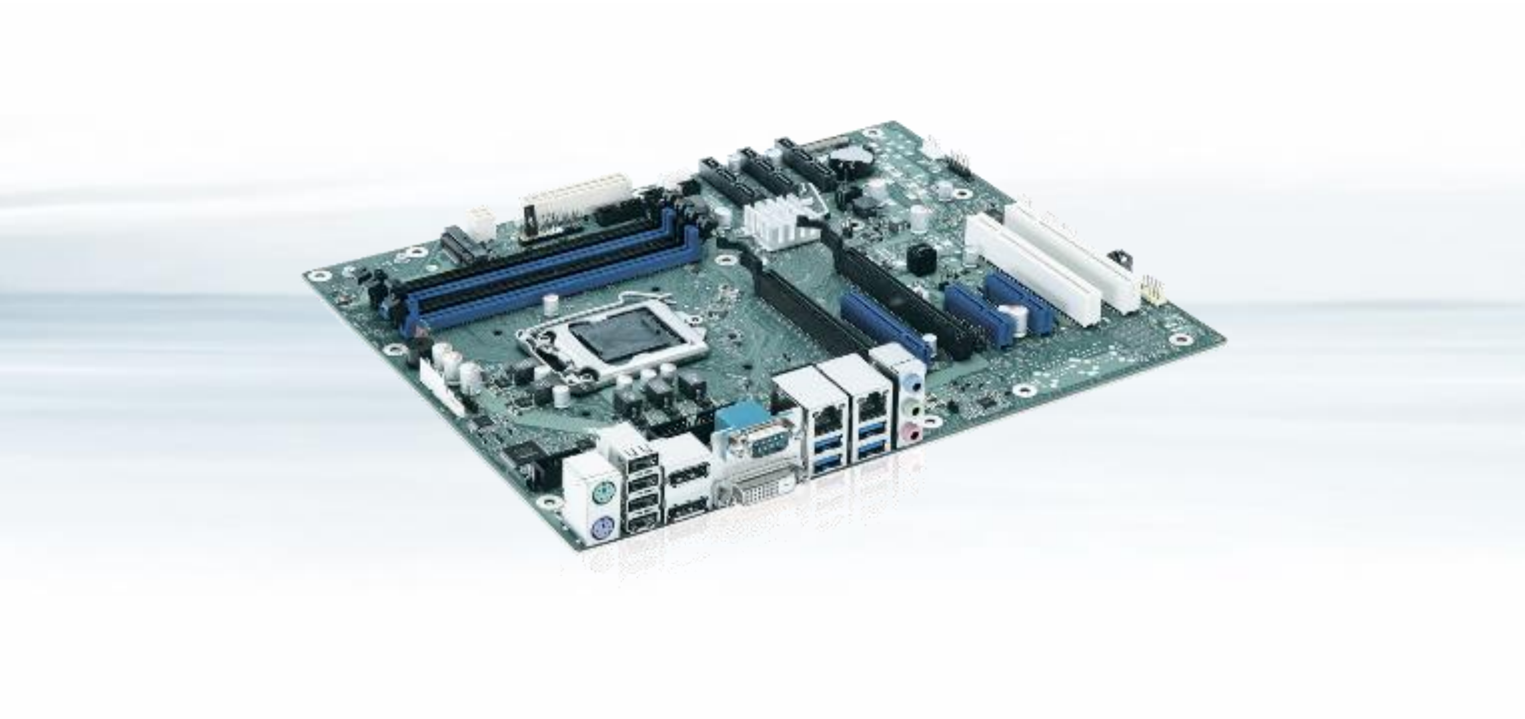
Kabylake Industrial

BIOS Release Document



Designed by Fujitsu

- D3433-S2
- D3434-S2
- D3441-S2
- D3446-S2

Content

Revision History:

Date	BIOS Version	Notes
09.03.2020	R1.26.0	Added new BIOS version Changed whole document to Kontron design Reordered some chapters
05.08.2019	R1.22.0	Added new BIOS version, Links adjusted
05.10.2018	R1.20.0	Added new BIOS version
13.07.2018	R1.17.0	Added new BIOS version
11.05.2018	R1.16.0	Added new BIOS version (R1.16.0)
27.09.2017	R1.13.0	Added new BIOS version (R1.13.0) for D3446-S2 only
12.09.2017	R1.12.0	Initial mass production release for D3446-S2
28.08.2017	R1.12.0	Initial mass production release (only D3434-S2 and D3441-S2)
31.07.2017	R1.10.0	Initial mass production release (only D3433-S2)

1. General Notes

- AMI Aptio V5.0.0.12

1.1 Released OS Versions [updated]

- MS Windows 7 (32/64bit) 1)
- MS Windows 8.1 (64bit) 1)
- MS Windows 10 (64bit)

1) Requires Skylake (= 6th gen.) processor!

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:

D3433 / D3434:
ftp://ftp.kontron.com/Products/Motherboards/Industrial/D343x-S_Mini-ITX/BIOS_D343x-S/

D3441 / D3446:
ftp://ftp.kontron.com/Products/Motherboards/Industrial/D344x-S/BIOS_D344x-S/

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 R1.10.0

First released mass production BIOS only for D3433-S2

Known Issues and Limitations:

- Housing Monitoring always shows error, even if the housing is closed.
- BIOS Recovery Flash does not terminate. After successfully BIOS Recovery Flash Update the system keeps on beeping and rebooting.
- POST hang (PC=B2h) with LVDS, eDP and external monitor plugged at the same time.
- Wake on LAN via I219LM onboard LAN controller from ACPI S3/S4 is possible even when the I219LM is disabled in device manager
- Wake up from RTC after Power Button Overwrite does not work. Issue related to ME/PMC Firmware. This issue will not be solved on the Skylake/Kabylake platform from Intel side.
- Windows 7 only: no TPM2.0 support for legacy installed OS

3. BIOS R1.12.0

First released mass production BIOS only for D3434-S2, D3441-S2 and D3446-S2

Known Issues and Limitations:

- Housing Monitoring is not usable. Switch is not recognized even if connected.
- BIOS Recovery Flash does not terminate. After successfully BIOS Recovery Flash Update the system keeps on beeping and rebooting.
- D3433-S2 and D3434-S2 only: POST hang (PC=B2h) with LVDS, eDP and external monitor plugged at the same time.
- Wake on LAN via I219LM onboard LAN controller from ACPI S3/S4 is possible even when the I219LM is disabled in device manager
- Wake up from RTC after Power Button Overwrite does not work. Issue related to ME/PMC Firmware. This issue will not be solved on the Skylake/Kabylake platform from Intel side.
- Windows 7 only: no TPM2.0 support for legacy installed OS
- Additional "Virtual Display" available after unplug and plug external monitor

4. BIOS R1.13.0

Changes vs. previous released BIOS (only released for D3446-S2)

- Fixed: SM-Bus errors due to enabled PCIe ASPM support. ASPM has disabled completely. Prevents the Pericom PCIe-PCI bridge from going into sleep state.

Known Issues and Limitations:

- Housing Monitoring is not usable. Switch is not recognized even if connected.
- BIOS Recovery Flash does not terminate. After successfully BIOS Recovery Flash Update the system keeps on beeping and rebooting.
- D3433-S2 and D3434-S2 only: POST hang (PC=B2h) with LVDS, eDP and external monitor plugged at the same time.
- Wake on LAN via I219LM onboard LAN controller from ACPI S3/S4 is possible even when the I219LM is disabled in device manager
- Wake up from RTC after Power Button Overwrite does not work. Issue related to ME/PMC Firmware. This issue will not be solved on the Skylake/Kabylake platform from Intel side.
- Windows 7 only: no TPM2.0 support for legacy installed OS
- Additional "Virtual Display" available after unplug and plug external monitor

5. BIOS R1.16.0

Changes vs. previous released BIOS

- Updated CPU Microcode for Skylake R0/S0 (0xC2) and Kabylake B-0 (0x84).
  - INTEL-SA-00088, CVE2017-5715
- Updated Management Engine Firmware version 11.8.50.3460 (INTEL-SA-00086)
- Updated Intel Reference Code (INTEL-SA-00087, CVE-2017-5703)
- Updated legacy VBIOS and UEFI GOP driver
- Fixed: It was not possible to activate and use iTCO watchdog timer within Linux.
- Fixed: LVDS EDID communication not working.
- Fixed: BIOS setting “Native PCIe Enable” has wrong default. New default value: “Disabled”.
- Fixed: BIOS setting “PERR” and “SERR” not configurable.
- Fixed: Housing Monitoring is not usable. Switch is not recognized even if connected.
- Fixed: Some PCIe cards (Dual LAN RTL8111F and mPCIe Dual LAN with i211) did not work properly. Added enhanced PCIe support.
- Fixed: Even if [System Firmware Update] is set to Restricted, System Firmware device appears in Device Manager.
- Fixed: PXE boot failures with IPv6 occurred.
- Fixed: WOL was working even when disabled in Setup and USB keyboard wakeup set to enabled.
- Fixed: USB Power is enabled even if BIOS setting is "Always off"
- Fixed: TXT is not working - GetSec results in reboot
- Updated BIOS flash interface (Gabi).
  - Added SetupItemID for “MiniCard Mode”: 0x01F5
  - Added SetupItemID for "Intel ® Speed Shift Technology": 0x025B
  - Added SetupItemID for “High Precision Event Timer”: 0x025C
  - Fixed (D343x-S2 only): SettingID 0xC2 (“Adjusted Parameters”) cannot be set for SetupItemID 0xC7 (“Panel Config Select”)

Changes vs. previous released BIOS - continued (R1.13.0)

- Feature: Added Setup Settings:
  - Advanced > Onboard Devices Configuration > High Precision Event Timer
    - Note: If “High Precision Event Timer” is disabled, BIOS flash update is not possible anymore.
  - Advanced > CPU Configuration > Intel ® Speed Shift Technology
- Feature: Improve 3rd party Option ROM launch prior to end of DXE.
- Feature (D343x-S2 only): Added support for “LVDS BacklightApp” (Windows)
  - BacklightApp can be downloaded from our FTP server: ftp://ftp.kontron.com/Services/Software_Tools/LVDS_Brightness-Tool/
- Feature: Reduced runtime SMIs to improve real-time performance

Known Issues and Limitations:

- BIOS Recovery Flash does not terminate. After successfully BIOS Recovery Flash Update the system keeps on beeping and rebooting.
- D3433-S2 and D3434-S2 only: POST hang (PC=B2h) with LVDS, eDP and external monitor plugged at the same time.
- Wake on LAN via I219LM onboard LAN controller from ACPI S3/S4 is possible even when the I219LM is disabled in device manager
- Wake up from RTC after Power Button Overwrite does not work. Issue related to ME/PMC Firmware. This issue will not be solved on the Skylake/Kabylake platform from Intel side.
- Windows 7 only: no TPM2.0 support for legacy installed OS
- Additional "Virtual Display" available after unplug and plug external monitor

6. BIOS R1.17.0

Changes vs. previous released BIOS

- Updated CPU Microcode. Fix for Intel-SA-00115 (CVE2018-3639, CVE2018-3640)
  - 0xC6 for Skylake R0/S0 and Skylake Xeon E3
  - 0x8E for Kaby Lake H/S/X/G and Kaby Lake Xeon E3

Known Issues and Limitations:

- BIOS Recovery Flash does not terminate. After successfully BIOS Recovery Flash Update the system keeps on beeping and rebooting.
- D3433-S2 and D3434-S2 only: POST hang (PC=B2h) with LVDS, eDP and external monitor plugged at the same time.
- Wake on LAN via I219LM onboard LAN controller from ACPI S3/S4 is possible even when the I219LM is disabled in device manager
- Wake up from RTC after Power Button Overwrite does not work. Issue related to ME/PMC Firmware. This issue will not be solved on the Skylake/Kabylake platform from Intel side.
- Windows 7 only: no TPM2.0 support for legacy installed OS
- Additional "Virtual Display" available after unplug and plug external monitor

7. BIOS R1.20.0

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
- Updated System Management Controller Firmware to Teutates V56
- Improved fan characteristic (SystemGuard version 4.16 or newer required)
- Fixed: Windows 10 System Firmware Update – Progress bar is missing
- Fixed: Trusted Module BIOS entry was still visible if TPM license flag disabled with OEMIdent.
- Fixed: Mainboards sporadically hang at POST with some PCIe cards due to PCIe runtime error logging being enabled. Default is now “Disabled”
- Feature: Enhance Setup Password Severity Options (Standard, Strong, Stringent)
- Feature: Show "Launch Storage OpROM policy" in [BIOS > Advanced > CSM Configuration]
  - Feature: Added SetupItemID for “SATA Controller Speed”: 0x01BA

Known Issues and Limitations:

- BIOS Recovery Flash does not terminate. After successfully BIOS Recovery Flash Update the system keeps on beeping and rebooting.
- D3433-S2 and D3434-S2 only: POST hang (PC=B2h) with LVDS, eDP and external monitor plugged at the same time.
- Wake on LAN via I219LM onboard LAN controller from ACPI S3/S4 is possible even when the I219LM is disabled in device manager
- Wake up from RTC after Power Button Overwrite does not work. Issue related to ME/PMC Firmware. This issue will not be solved on the Skylake/Kabylake platform from Intel side.
- Windows 7 only: no TPM2.0 support for legacy installed OS
- Additional "Virtual Display" available after unplug and plug external monitor

8. BIOS R1.22.0

Changes vs. previous released BIOS

- Integrated Fixes for
  - PSIRT-TA-201810-007, PSIRT-TA-201810-004 (INTEL-SA-00185), PSIRT-TA-201901-002,
  - CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2018-12178, CVE-2018-12179, CVE-2018-12180, CVE-2018-12181, CVE-2018-12182, CVE-2018-12185, CVE-2018-12187, CVE-2018-12188, CVE-2018-12189, CVE-2018-12190, CVE-2018-12191, CVE-2018-12192, CVE-2018-12196, CVE-2018-12199, CVE-2018-12198, CVE-2018-12200, CVE-2018-12201, CVE-2018-12202, CVE-2018-12203, CVE-2018-12204, CVE-2018-12205
  - 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
- Updated CPU Microcode (0xCC) for Skylake-S0/R0 and (0xB4) for Kabylake-B-0
- Updated to Management Engine Firmware version 11.8.65.3590
- Fixed: Wake from S3 was not possible with 'Above 4G Decoding' being enabled in SETUP.
- Fixed: HDD Password input box was black after set HDD password.
- Fixed: Windows Boot Manager was missing under some circumstances.
- Fixed: Drive size of disks with native 4k sectors was not shown correctly in BIOS setup.
- Fixed: Boot from removable media was possible although disabled in BIOS setup.
- Feature: “Erase Disk” license enabled by default. This only takes effect for newly produced mainboards. Not possible to activate “Erase Disk” license via BIOS update flash.

Known Issues and Limitations:

- BIOS Recovery Flash does not terminate. After successfully BIOS Recovery Flash Update the system keeps on beeping and rebooting.
- D3433-S2 and D3434-S2 only: POST hang (PC=B2h) with LVDS, eDP and external monitor plugged at the same time.
- Wake on LAN via I219LM onboard LAN controller from ACPI S3/S4 is possible even when the I219LM is disabled in device manager
- Wake up from RTC after Power Button Overwrite does not work. Issue related to ME/PMC Firmware. This issue will not be solved on the Skylake/Kabylake platform from Intel side.
- Windows 7 only: no TPM2.0 support for legacy installed OS
- Additional "Virtual Display" available after unplug and plug external monitor

9. BIOS R1.26.0 [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-2019-0165, CVE-2019-0166, CVE-2019-0168, CVE-2019-0169, CVE-2019-0184, CVE-2019-11086, CVE-2019-11087, CVE-2019-11088, CVE-2019-11090, CVE-2019-11097, CVE-2019-11100, CVE-2019-11101, CVE-2019-11102, CVE-2019-11103, CVE-2019-11104, CVE-2019-11105, CVE-2019-11106, CVE-2019-11107, CVE-2019-11108, CVE-2019-11110, CVE-2019-11131, CVE-2019-11132, CVE-2019-11147, CVE-2019-11157, CVE-2019-11157
- Updated CPU Microcode for Skylake-S0/R0 (0xD6) and Kabylake-B-0 (0xCA)
- Updated to Management Engine Firmware version 11.8.70.3626
- Updated Intel Raid & RST UEFI driver – Fixes boot issues in RAID1, if one drive was removed.
- Fixed: “Windows Boot Manager” entry in boot menu missing after reboot

Known Issues and Limitations:

- BIOS Recovery Flash does not terminate. After successfully BIOS Recovery Flash Update the system keeps on beeping and rebooting.
- D3433-S2 and D3434-S2 only: POST hang (PC=B2h) with LVDS, eDP and external monitor plugged at the same time.
- Wake on LAN via I219LM onboard LAN controller from ACPI S3/S4 is possible even when the I219LM is disabled in device manager
- Wake up from RTC after Power Button Overwrite does not work. Issue related to ME/PMC Firmware. This issue will not be solved on the Skylake/Kabylake platform from Intel side.
- Windows 7 only: no TPM2.0 support for legacy installed OS
- Additional "Virtual Display" available after unplug and plug external monitor

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