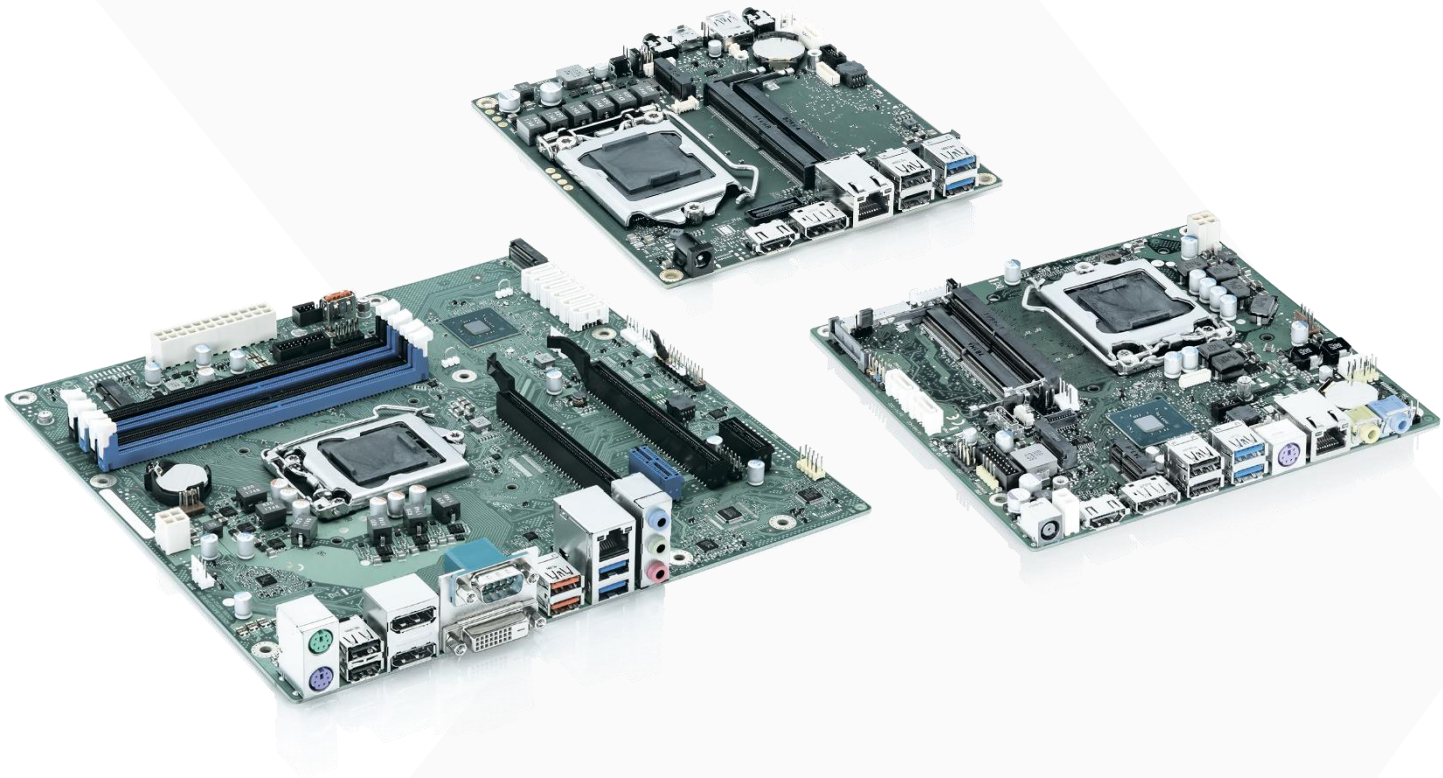
Bios Release Document

Intel® Coffee Lake-S



Extended Lifecycle Series

- D3642-B
- D3643-H
- D3644-B
- D3654-B
- D3664-B
- D3674-B

kontron
The Power of IoT

Content

1. GENERAL NOTES 2

1.1 RELEASED OS VERSIONS 2
1.2 BIOS UPDATE OPTIONS 3
1.3 FTP BIOS FOLDER 4
1.4 MODIFY BIOS SETUP SETTINGS AND DEFAULTS (TOOL BIOSSET) 4
1.5 WHAT'S ABOUT DOS SUPPORT AND WHERE ARE THE DOS TOOLS? 4
1.6 NOTE: CUSTOMER SERVICE RELEASE BIOS 4

2. PREVIOUS BIOS RELEASES 5

3. BIOS R1.25.0 6

4. BIOS R1.26.0 7

5. BIOS R1.28.0 8

6. BIOS R1.29.0 [NEW] 9

ABOUT KONTRON 11

Revision History:

Date	BIOS Version	Notes
26.03.2025	R1.29.0	Added new BIOS version
20.03.2023	R1.28.0	Updated Info regarding SCD/NVUX archive update on R1.28.0
07.03.2023	R1.28.0	Updated EFI flash update information
21.12.2022	R1.28.0	Added new BIOS version; Updated FTP links
12.04.2021	R1.26.0	Added new BIOS version
02.09.2020	R1.25.0	Added new BIOS version (R1.25.0). New document due to consolidation of D354x-B/H and D36x4-B (STX, ThinMiniITX).

1. General Notes

- AMI Aptio V5.0.0.13

1.1 Released OS Versions

- MS Windows 10 (64bit)
- MS Windows 11 (64bit)*

*) Not validated by Kontron. “Runnable”. Please check official Microsoft and Intel sites to get an overview about supported processor and graphic products on Windows 11:

- https://www.intel.co.uk/content/www/uk/en/support/articles/000005526/graphics.html
- https://www.intel.co.uk/content/www/uk/en/support/articles/000087875/processors.html
- https://learn.microsoft.com/en-us/windows-hardware/design/minimum/windows-processor-requirements

1.2 BIOS Update Options

EFI Flash Update

Use ZIP-files for EFI-based BIOS Update

1. Copy all content of *Dxxxx-Yzz.R1.*.0.zip* to any FAT32 formatted USB drive/stick:
2. Switch on system and boot to UEFI shell. Included autostart script (startup.nsh) will automatically select the BIOS update stick and starts the BIOS update.
3. Follow the screen instructions.
   Do not touch or power off the system during BIOS update!

If you want to use the "Fujitsu Update Utility" available in Boot menu (F12 key during start up) then you need to copy "Efiflash.efi" tool from the root directory to "/EFI/FUJITSU". Now a new boot entry is visible and can be selected in boot menu.

Please see the BIOS-Flash-Tools documentation for more information:
https://ftp.kontron.com/main.html?download&weblink=3cb83a90a99c51160d2aa1f1f34cc340&subfolder=Services/Software%5FTools/BIOS%2DFlash%2DTools

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:
https://ftp.kontron.com/main.html?download&weblink=3cb83a90a99c51160d2aa1f1f34cc340&subfolder=Services/Software%5FTools/BIOS%2DFlash%2DTools

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:

D3642-B:
https://ftp.kontron.com/main.html?download&weblink=e4315cc5b33af153f710143f716d6e4d&subfolder=BIOS_D364x-B/BIOS_D3642-B

D3643-H:
https://ftp.kontron.com/main.html?download&weblink=c934078bda798814e7317195dabbc55e&subfolder=BIOS_D3643-H

D3644-B:
https://ftp.kontron.com/main.html?download&weblink=e4315cc5b33af153f710143f716d6e4d&subfolder=BIOS_D364x-B/BIOS_D3644-B

D3654-B:
https://ftp.kontron.com/main.html?download&weblink=b5fb923cb7593911f1a3206f54cff47e&subfolder=BIOS_D3654-B

D3664-B:
https://ftp.kontron.com/main.html?download&weblink=f402db65df7b7f4dc45c1f53623b1db0&subfolder=BIOS_D3664-B

D3674-B:
https://ftp.kontron.com/main.html?download&weblink=4d6f100d56746eeea42f9a850905bd0f&subfolder=BIOS_D3674-B

1.4 Modify BIOS Setup Settings and Defaults (Tool BIOSSET)

BIOS settings can be modified by the Windows and Linux tool BIOSSET (Modify BIOS Setup Settings and Defaults). See BIOSSET tool help (parameter –h) for further details.

The tool is also described in our Manufacturing-Tools HowTo document:
https://ftp.kontron.com/main.html?download&weblink=3cb83a90a99c51160d2aa1f1f34cc340&subfolder=Services/Software%5FTools/Common%2DMainboard%2DTools

1.5 What's about DOS support and where are the DOS tools?

Due to Intel's and Microsoft's decision, there is no "Legacy" OS support (CSM mode) implemented anymore. So only usage of UEFI operating systems is possible. We will provide the necessary tools and documentation for Windows and Linux.

Editcmos (DOS) -> Biosset (Windows and Linux)
EfiFlash.exe (DOS) -> Efiflash.efi (EFI environment) or Dskflash/Deskflash (Windows/Linux)
SMCO, LVDS tool, OEMIdent are also available for Windows and Linux.

https://ftp.kontron.com/main.html?download&weblink=3cb83a90a99c51160d2aa1f1f34cc340&subfolder=Services/Software%5FTools

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. Previous BIOS releases

Since BIOS version R1.25.0 we have consolidated BIOS-Info document for D364x-B/H and D36x4-B (STX, Thin-MiniITX). You can find the revision history for previous released BIOS versions within the “Previous_Versions” subfolder:

D364x-B/H:
https://ftp.kontron.com/main.html?download&weblink=e4315cc5b33af153f710143f716d6e4d&subfolder=BIOS%5FD364x%2DB/BIOS%5FD3644%2DB/Previous%5FVersions&realfilename=BIOS%2DRelease%2DDocument%5FCoffeelake%2DXLC%5FD364x%2DB%5F%2DH%5FR1%2E8%2E0%2Epdf

D36x4-B:
https://ftp.kontron.com/main.html?download&weblink=4d6f100d56746eeea42f9a850905bd0f&subfolder=BIOS%5FD3674%2DB/Previous%5FVersions&realfilename=BIOS%2DRelease%2DDocument%5FCoffeelake%2DMini%2DSTX%5FThinMini%5FD36x4%5FR1%2E23%2E0%2Epdf

3. BIOS R1.25.0

Changes vs. previous released BIOS

- Integrated fixes for “Ripple20” (INTEL-SA-00295)
- Updated CPU Microcode for CoffeeLake-S U-0 (0xD6) and for CoffeeLake-S R-0 (0xD6)
- Updated to Management Engine Firmware version 12.0.64.1551
- Info: LVDS backlight inverting is not working if set to OS controlled. Option therefore is greyed out now.
- Info: Replaced Fujitsu logos with Kontron logos.
    - Diagnostic screen logo (Quiet Boot = Disabled) removal takes immediate effect after BIOS update.
    - Silent boot logo will not be replaced during BIOS updates in field (logo preserve function). It just takes effect on newly produced or RMA processed motherboards. To activate the logo on “old” motherboards, you can use the Logo file from: https://ftp.kontron.com/main.html?download&weblink=3cb83a90a99c51160d2aa1f1f34cc340&subfolder=Services/Software_Tools/Miscellaneous
        - Kontron_QuietBootBIOSLogo.zip
- Info: BIOS Feature “Auto BIOS Update” not working with the Fujitsu default server address. The server infrastructure at Fujitsu does not contain data for Kontron Extended Lifecycle and Industrial motherboards anymore. Therefore, the address was removed. Kontron will not provide an update server. Custom TFTP server solutions are still possible.

Known Issues and Limitations:

- No legacy OS support (UEFI only due to Intel restrictions)!
- No beep code prior to Capsule Update.
- Default value for “Intel ® Speed Shift Technology” (Hardware P-State control) had been changed to “Disabled” This will only take effect, if you load “Optimized Defaults” after BIOS update.
- [D3674-B1 only] In Linux a “ghost screen” is visible with a resolution of 1024x786 which mainly gets the “main” screen. You have to switch the main screen manually to the real connected monitors.
- Integrated Intel TPM is high sporadically disappearing after combined S3 / Reboot cycles.
- BIOS downgrade to a version prior R1.6.0 (D3642, D3643, D3644) / R1.13.0 (D3654, D3664, D3674) is blocked due to security reasons and the support of 9th gen Intel CPUs!

4. BIOS R1.26.0

Changes vs. previous released BIOS

- Intel IPU 2020.2 Security Update - Integrated Fixes for CVE-2020-587, -588, -590, -591, -592, -593, -8694, -8695, -8696, -8698, -8705, -8744, -8745, -8746, -8747, -8749, -8750, -8751, -8752, -8753, -8754, -8755, -8761, -12297, -12303, -12304, -12354, -12355, -12356
- Integrated fixes for INTEL-SA-00404 (CVE-2020-8758)
- Updated CPU Microcode for CoffeeLake-S U-0 (0xDE) and for CoffeeLake-S R-0 (0xDE)
- Updated to Management Engine Firmware version 12.0.72.1757
- Fixed: BIOS setting “System Power Limit” visible on not supported system configurations.
- Fixed: BIOS setting “CPU TDP” was grayed out by default after flash to R1.8.0 or later.
- Fixed: Unexpected POST message "Intel AMT SOL operational mode" after BIOS update

Known Issues and Limitations:

- No legacy OS support (UEFI only due to Intel restrictions)!
- No beep code prior to Capsule Update.
- Default value for “Intel ® Speed Shift Technology” (Hardware P-State control) had been changed to “Disabled” This will only take effect, if you load “Optimized Defaults” after BIOS update.
- [D3674-B1 only] In Linux a “ghost screen” is visible with a resolution of 1024x786 which mainly gets the “main” screen. You have to switch the main screen manually to the real connected monitors.
- Integrated Intel TPM is high sporadically disappearing after combined S3 / Reboot cycles.
- BIOS downgrade to a version prior R1.6.0 (D3642, D3643, D3644) / R1.13.0 (D3654, D3664, D3674) is blocked due to security reasons and the support of 9th gen Intel CPUs!

5. BIOS R1.28.0

Changes vs. previous released BIOS

- Intel IPU 2021.1 Security Update - Integrated Fixes for CVE-2020-8670, -8673, -8700, -8703, -8704, -12357, -12358, -12359, -12360, -24486, -24489, -24506, -24507, -24509, -24511, -4512, -24513, -24516, CVE-2021-0095, - 33107
- Updated CPU Microcode for CoffeeLake-S U-0 (0xF0) and for CoffeeLake-S R-0 (0xF4)
- Updated to Management Engine Firmware version 12.0.92.2145.
- Fixed: OemIdent corrupts link to SMBIOS Type 3 within Type 2 structure.
- Fixed: Possible Memory Exception while BIOS update in POST
- Feature: New password type “Boot Menu password” [BIOS > Security] to protect only the Boot menu by a separate password.
    - Note: No tool support to add the new password type!
    - Important: BIOS archive files (*.SCD / *.NVUX) which were created with an older BIOS version, cannot be used for combined update+restore process to R1.28.0 BIOS! Create a new settings archive file on a system with at least R1.28.0 BIOS version and use the new SCD/NVUX file for the combined update process.
- [D364x only] Feature: Added PCIe speed options for bifurcated PEG slots

Known Issues and Limitations:

- No legacy OS support (UEFI only due to Intel restrictions)!
- No beep code prior to Capsule Update.
- No POST beep “At start of POST” – deprecated function.
- Default value for “Intel ® Speed Shift Technology” (Hardware P-State control) had been changed to “Disabled” This will only take effect, if you load “Optimized Defaults” after BIOS update.
- [D3674-B1 only] In Linux a “ghost screen” is visible with a resolution of 1024x786 which mainly gets the “main” screen. You have to switch the main screen manually to the real connected monitors.
- Integrated Intel TPM is high sporadically disappearing after combined S3 / Reboot cycles.
- Do not use SCD files created with BIOS version ≤ R1.26.0 on systems with BIOS ≥ R1.28.0. Otherwise, the system configuration is corrupted and leads to an unexpected behaviour.
- BIOS downgrade to a version prior R1.6.0 (D3642, D3643, D3644) / R1.13.0 (D3654, D3664, D3674) is blocked due to security reasons and the support of 9th gen Intel CPUs!

6. BIOS R1.29.0 [new]

Changes vs. previous released BIOS (Not released for D3674-B)

- Intel IPU 2021.2: Integrate fixes for CVE-2021-0060, -0091, -0092, -0093, -0099, -0103, -0107, -0111, -0114, -0115, -0116, -0117, -0118, -0119, -0124, -0125, -0127, -0145, -0146, -0147, -0156, -0157, -0158
- Intel IPU 2022.1: Integrate fixes for CVE-2021-0153,-0154,-0155,-0159,-0188,-0189,-0190,-21131,-21136,-33060,-33103,-33122,-33123, -33124,-33159,CVE-2022-0004,-0005,-21123, -21125, -21127, -21151,-21166
- Intel IPU 2022.3: Integrate fixes for CVE-2021-0187, CVE-2022-21198, CVE-2022-26006, CVE-2022-26343, CVE-2022-26837, CVE-2022-26845, CVE-2022-27497, CVE-2022-29466, CVE-2022-29515, CVE-2022-29893, CVE-2022-33159
- Intel IPU 2023.1: Integrate fixes for CVE-2021-0187, CVE-2022-21216, CVE-2022-26343, CVE-2022-26837, CVE-2022-30539, CVE-2022-30704, CVE-2022-32231, CVE-2022-33196, CVE-2022-33894, CVE-2022-33972, CVE-2022-36348, CVE-2022-36794, CVE-2022-38090
- Intel IPU 2023.2: Integrate fixes for CVE-2022-33894, CVE-2022-38087
- Intel IPU 2023.3: Integrate fixes for CVE-2022-27879, CVE-2022-29871, CVE-2022-36392, CVE-2022-37343, CVE-2022-38083, CVE-2022-38102, CVE-2022-40982, CVE-2022-41804, CVE-2022-43505, CVE-2022-44611, CVE-2023-23908
- Intel IPU 2023.4: Integrate fixes for CVE-2023-25756, CVE-2023-22329
- Intel IPU 2024.3: Integrate fixes for CVE-2023-22351, -23904, -25546, -34424, -34440, -38655, -40067, -41833, -42772, -43626, -43753, -43758, -48361, CVE-2024-21781, -21820, -21829, -21844, -21871, -23599, -23918, -23984, -24853, -24968, -24980, -35061
- Intel IPU 2025.1: Integrate fixes for CVE-2024-24582, CVE-2024-26021, CVE-2024-28047, CVE-2024-28127, CVE-2024-28956, CVE-2024-29214, CVE-2024-30211, CVE-2024-31157, CVE-2024-36293, CVE-2024-38307, CVE-2024-39279, CVE-2024-39355
- Security: Integrate fixes for CVE-2017-5721, CVE-2020-0572, CVE-2020-12301, CVE-2021-26943, CVE-2022-24415, CVE-2022-24416, CVE-2022-24419, CVE-2022-24420, CVE-2022-24421, CVE-2020-8670, CVE-2020-10255, CVE-2022-36372, CVE-2021-38578, CVE-2023-28005, CVE-2022-43505, CVE-2022-4303, CVE-2022-4450, CVE-2023-0215, CVE-2023-0286, CVE-2023-0465, CVE-2023-0464, CVE-2022-21894, CWE-506, CVE-2022-36763, CVE-2022-36764, CVE-2023-27504, CVE-2023-28383, CVE-2023-28402, CVE-2020-0570, CVE-2020-0571, CVE-2019-14556, CVE-2019-14557, CVE-2019-14558, CVE-2020-8671, CVE-2020-8672
- Updated CPU Microcode for CoffeeLake-S U-0 (0xF4)
- Updated to Management Engine Firmware version 12.0.93.2331V4.
- Updated Memory Reference code to 0.7.1.121
- [D364x only] Fixed: Disabled PCIe x1 slot 2 and PCIe x1 Slot 4 can still be used
- Fixed: TPM PCR7 Binding issue

BIOS R1.29.0 (cont')

- [D3674 only] Fixed: "LVDS adjusted parameters" cannot be deleted from LVDS configuration BIOS setup.
- Fixed: Unknown BIOS Password required after BIOS flash via combined BUP with Deskflash.
- Fixed: Console Redirection options in BIOS Setup can be changed with User rights.
- Feature: Added missing SetupItemID 0x00B5 (Watchdog Timeout)
- Feature: New Kontron Logo 2023 for BIOS POST Screen. (Only on new produced motherboards).
- Fixed: BIOS can be accessed with Administrator rights by using the User Password at boot via boot menu.
- Fixed: BIOS settings (current/default) cannot be changed via tool (Biosset, Gabisettings).
- Fixed: Description for Password handling (BIOS > Security) is different from the current implementation.
- Fixed: Onboard LAN port i210 cannot be disabled from BIOS Setup
- Fixed: LAN Boot is triggered when waking the system via USB Keyboard
- Fixed: Erase disk utility cannot read Setup Variable
- Fixed: BIOS Password is not required after opening the Housing when User Password is enabled
- Fixed: Boot hang up on boot logo, with battery warning and specific CPU (e.g. i3-9100) only.
- Fixed: Physical Memory information are missing in SMBIOS data

Known Issues and Limitations:

- No legacy OS support (UEFI only due to Intel restrictions)!
- No beep code prior to Capsule Update.
- No POST beep "At start of POST" – deprecated function.
- Default value for "Intel ® Speed Shift Technology" (Hardware P-State control) had been changed to "Disabled" This will only take effect, if you load "Optimized Defaults" after BIOS update.
- [D3674-B1 only] In Linux a "ghost screen" is visible with a resolution of 1024x786 which mainly gets the "main" screen. You have to switch the main screen manually to the real connected monitors.
    - Workaround: Disable int. display by kernel option: `video=eDP-1:d` (check monitor name by `xrandr –listmonitors`)
- Integrated Intel TPM is high sporadically disappearing after combined S3 / Reboot cycles.
- Do not use SCD files created with BIOS version ≤ R1.26.0 on systems with BIOS ≥ R1.28.0. Otherwise, the system configuration is corrupted and leads to an unexpected behaviour.
- BIOS downgrade to a version prior R1.6.0 (D3642, D3643, D3644) / R1.13.0 (D3654, D3664, D3674) is blocked due to security reasons and the support of 9th gen Intel CPUs!

About Kontron

Kontron AG (www.kontron.com, ISIN AT0000A0E9W5, WKN A0X9EJ, KTN) is a leading IoT technology company. For more than 20 years, Kontron has been supporting companies from a wide range of industries to achieve their business goals with intelligent solutions. From automated industrial operations, smarter and safer transport to advanced communications, connectivity, medical, and energy solutions, the company delivers technologies that add value for its customers. With the acquisition of Katek SE in early 2024, Kontron significantly strengthens its portfolio with the new GreenTec division, focusing on solar energy and eMobility, and grows to around 8,000 employees in over 20 countries worldwide. Kontron is listed on the SDAX® and TecDAX® of the German Stock Exchange.

For more information, please visit: www.kontron.com

Global Headquarters

Kontron Europe GmbH

Gutenbergstraße 2
85737 Ismaning, Germany
Tel.: + 49 821 4086 0
Fax: + 821 4086 111
pcmb-sales@kontron.com

Copyright © 2023 Kontron. All rights reserved. All data is for information purposes only and not guaranteed for legal purposes. Information has been carefully checked and is believed to be accurate; however, no responsibility is assumed for inaccuracies. Kontron and the Kontron logo and all other trademarks or registered trademarks are the property of their respective owners and are recognized. Specifications are subject to change without notice.