Intel® Firmware Support Package (Intel® FSP) for with Intel® Atom™ processor E3900 product family (formerly Apollo Lake), MR9

Release Notes

January 2021

Document Number: 634529

Contents

Tables

Revision History

These are the main releases of Intel® Firmware Support Package (Intel® FSP) for the Intel® Atom™ processor E3900 product family (formerly Apollo Lake):

Date	Revision	Description
November 2, 2015	ALPHA	Alpha Release
February 17, 2016	BETA1	Beta 1 Release
May 13, 2016	BETA2	Beta 2 Release with Intel® FSP 0.8.1
July 27, 2016	GOLD	Gold Release with Intel® FSP 1.1.0
September 9, 2016	MR1	MR1 Release with IOTG FSP 1.1.4.1
January 27, 2017	MR2	MR2 Release with Intel® FSP 1.3.1.0
April 28, 2017	MR3	MR3 Release with Intel® FSP 1.4.1.0
December 15, 2017	MR4	MR4 Release with Intel® FSP 1.4.3.0
February 12, 2018	MR5	MR5 Release with Intel® FSP 1.4.3.1
September, 2019	MR6	MR6 Release with Intel® FSP 1.4.3.1 (SIC 1.1.1)
	MR7	Skipped (internal evaluation purpose)
	MR8	Skipped (internal evaluation purpose)
October 2020	MR9	Intel® FSP Release with FSP/SIC 1.5.2.0

§

1.0 Introduction

This package contains required binary image(s) and collateral for the Intel® Firmware Support Package (Intel® FSP) for the Intel® Atom™ processor E3900 product family (formerly Apollo Lake). The Intel® FSP packaged in this release is intended for IOTG usage only.

This document provides system requirements, installation instructions, issues and limitations, and legal information.

To learn more about this product, see:

- New and previously new features listed in Section 2.0, New in This Release.
- Reference documentation listed in Section 1.2, Related Documentation, Tools, and Packages.

This release provides support for Intel® FSP EAS 2.0, for more information please view the related document *Intel® Firmware Support Package (Intel® FSP) External Architecture Specification (EAS) v2.0.*

The following table lists the relevant platform software components used during development and validation of this release.

Table 1. Platform Software Component Information

Component	MR9
Microcode Update (Bx/Dx-stepping)	M_03_506C9_00000040
Microcode Update (Ex-stepping)	M_03_506CA_0000001e

Table 2. Intel® FSP Included Components

Component	MR9
SIC/FSP	1.5.2.0
MRC Version	0.56.43 / 89.27
GOP/VBT	10.0.1036 / 207

1.1 Terminology

The following terms are used in this document.

Table 3. Terminology

Term	Description
API	Application Programming Interface
BSF	Binary Settings File
BCT	Binary Configuration Tool
CRB	Customer Reference Board
Intel® EDC	Intel® Embedded Design Center
Intel® FSP	Intel® Firmware Support Package
SoC	System on Chip

1.2 Related Documentation, Tools, and Packages

Table 4. Related Documentation, Tools, and Packages

Document	Location
Intel® Firmware Support Package (Intel® FSP) for the Apollo Lake Platform Integration Guide	Available in this release package
Intel® Binary Configuration Tool for Intel® Firmware Support Package	-www.intel.com/fsp - https://github.com/intel/BCT
Intel® Firmware Support Package (Intel® FSP) External Architecture Specification (EAS) v2.0	www.intel.com/content/dam/www/public/us/en/documents/technical-specifications/fsp-architecture-spec-v2.pdf
Intel® Atom™ Processor E3900 Series BIOS Writer's Guide Addendum	CDI # 570618

1.3 Intended Audience

The intended audience is for platform and system developers who intends to use an Intel® FSP-based boot loader for the firmware solution for their overall design based on the Intel® Atom™ processor E3900 product family (formerly Apollo Lake). This group includes, but is not limited to, system BIOS developers, boot loader developers, and system integrators.

1.4 Customer Support

Intel offers support for this software at the API level only, defined in the *Intel® FSP Integration Guide* and reference manuals listed in Section 1.2, Related Documentation, Tools, and Packages.

§

2.0 New in This Release

2.1 MR9 Features

- Add options to reduce susceptibility to DDR4 Rowhammer-style Attacks [MRC 0.56.43/MMRC 89.27].
- Fixed for contexts are not saved in OS after resuming from hibernate (S4).3
- Fix to P2SB security Hole **[#CVE: CVE-2020-0599]**
    - Added silicon Upd "P2sbSecEn" to disable/enable P2SB security option, Default zero to disable.
- MRC DDR PHY DLL parameters improvement (Rev.5a) for F1 stepping [MRC 0.56.42/MMRC 89.26].
- Added HKDF-SHA256(RFC 5869) support in Edk2 Crypto library to enable for Seed derivation.
- Added initial support for Seed Protocol DXE driver.
- A/E SKU D0 stepping detection.

MR7 and MR8 Release - skipped (internal evaluation) purpose

2.2 MR6 Features

- Update MRC/MMRC to 0.56.41/89.24
    - Resolved QH-MGU_Start-up problem with negative temperatures.
    - Resolved MRC hang at A8.
    - Resolved ECC boot hangs at MRC checkpoint 30.
    - Update swizzle calculator spreadsheet
- Added silicon Upd-PwmEnabled to disable/enable PWM config space and Upd-DptfEnabled to disable/enable Dptf config space. Default zero to disable.
- Correction of FspS upd variable from USB2_PER_PORT_2_PPX to USB2_PER_PORT_PPX

2.3 MR5 Features

- N/A (Bug fixes only)

2.4 MR4 Features

- N/A (Bug fixes only)

2.5 MR3 Features

- Real Time processing mode enabled (FSP-S UPD RtEn). Refer to document *Intel® Atom™ Processor E3900 Series BIOS Writer's Guide Addendum* for more information on how to enable this in platform code.

2.6 MR2 Features

- Intel® FSP OBB loading is capable of loading from BP1 or BP2 partitions and specific sub-partitions by specifying path to OBB filename in FSP-M OemFileName UPD value (ex: "BP2\\OBB\\OBB", "BP1\\IBB\\OBB", etc.).

2.7 MR1 Features

- N/A

2.8 Gold Features

- N/A

2.9 Beta 2 Features

- Intel® FSP BCT configuration support (via BCT 3.2.2 or newer versions)
- Support for eMMC firmware boot

2.10 Beta 1 Features

- Intel® FSP BCT configuration support (via BCT 3.2.1)

2.11 Alpha Features

- Initial release

- Support for SPI firmware boot
- Support for Intel® Firmware Support Package (Intel® FSP) FVs: FVIBBL.Fv, FVIBBM.Fv, and FVOBB.Fv

§

3.0 Limitations

3.1 Current Release

- CRB Power button is not responding to Windows* power button settings (choose what the power buttons do).

3.2 Previous Releases

- The default MR6 Intel® FSP release package was not working with MR4 Coreboot, hence 2 Intel® FSP binaries are released for both MR4 and Latest Open source Coreboot. **This Limitation has been addressed as of Intel® FSP MR9.**
- The BCT tool used with this release must be version 3.2.2 or newer, older versions of BCT tool may not be compatible with the newer Intel® FSP 2.0 architecture. For more information please view the related document *Intel® Firmware Support Package (Intel® FSP) External Architecture Specification (EAS) v2.0.*
- This Intel® FSP does not support full RMT data output for compatibility with RMT analysis tool. This support is planned to be enabled in the next release. **This limitation has been addressed as of MR1, using the debug Intel® FSP binary and enabling the FSP-M UPD RmtMode (For example, set to 0x3) will yield RMT data printing for use with RMT analysis tool.**
- When configuring the provided Fsp.fd binary using BCT tool the setting for DDR3L Page Size will show a blank field with default value 0x0 but should only show 1KB or 2KB option. The behavior of the 0x0 value results in the same behavior as when 1KB is selected. **This limitation has been addressed as of Beta 2.**
- Rebasing of Intel® Firmware Support Package (Intel® FSP) via Intel® Binary Configuration Tool is not supported in this release. Support is expected in the Beta release. **This limitation has been addressed as of Beta 1.**
- Memory parameters in this Intel® FSP release are not configurable. This release can support only the same memory configuration as that of the Leaf Hill CRB at this time. **This limitation has been addressed as of Beta 1.**

§

4.0 *Known Issues*

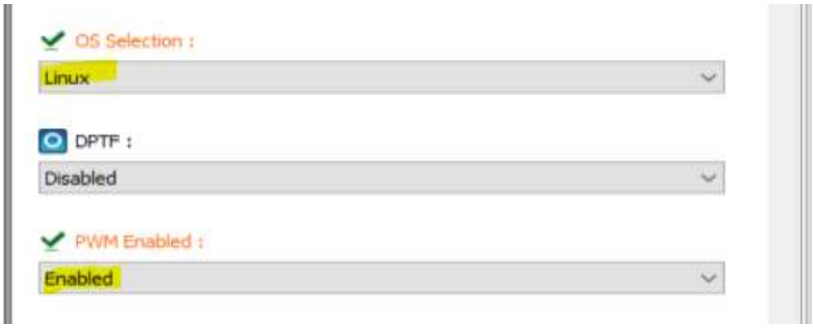
4.1 Current Release

- OS boot issue observed on internal MR4 Coreboot with MR3 UEFI as payload.
    - ➢ The modification shown below in MR3 payload source required for successful Boot to Windows /Yocto Linux*.

```
CorebootPayloadPkg/CorebootPayloadPkgIa32X64.dsc

DEFINE EMU_VARIABLE_ENABLE     = TRUE
```

- PWM controller CPU fan is not spinning with default MR4 CB Release. Required to set UPD's using BCT tool as show below in order to CPU fan to spin.



✓ OS Selection :
Linux

DPTF :
Disabled

✓ PWM Enabled :
Enabled

4.2 Previous Releases

- Definition error in Intel® FSP integration guide at session 6.2.2.181 where USB2_PER_PORT_2_PPX [19:17] should be USB2_PER_PORT_PPX [19:17]. **Resolved in MR6 Release**.

- The **pre-MR6** prior releases **could not be forward compatible** to the **F1-stepping** SoC. **Resolved in MR6 Release**.

- **This issue has been resolved in MR5 (this) release.** When setting the FSP-S UPD for SkipMpInit to enable the Intel® FSP will reference a NULL pointer inside of Intel® FSP code causing a hang during FspSiInit. The fix required for this was to not reference the pointer when SkipMpInit is enabled.

- Issue of determining reset type from OS layer; some write-one clear bits in GEN_PMCON1 will be cleared unexpectedly in Intel® FSP, which results in unable to obtain reset type in OS layer. **Resolved in MR4 release.**

- MRC profile for memory down and ECC (e.g. 0x5) was note enabled properly. **Resolved in MR3 release.**

- If using the FSPT_COMMON_UPD structure defined in FsptUpd.h with the FSP API call for FSP_TEMP_RAM_INIT there is a mismatch between the structure defined within Intel® FSP and the structure defined in FsptUpd.h. In order to remedy this issue, the FSPT_COMMON_UPD structure defined in FsptUpd.h should remove the Revision and Reserved [3] fields to match the structure used within Intel® FSP. This will be addressed in a future release of Intel® FSP. **Resolved in MR3 release.**

- The Intel® Atom™ Processor A3940 SKU has issue to boot using the Leaf Hill CRB due to an MRC limitation in this release of Intel® FSP. The issue will be resolved in a future release of Intel® FSP. **This issue has been resolved as of MR2.**

- There is a mistake regarding the NPK Enable Mode configurable option displayed when using BCT tool to configure the Intel® FSP binary. The duplicate of default option will appear blank, but it should be displaying 3 for Auto, which is the default setting. The valid list of options for this field are 0: Disable, 1: Enable, 2:Debugger, 3:Auto(Default). This will be fixed in the next release of Intel® FSP. **This issue has been resolved as of MR1.**

- There is some issue with Intel® FSP performing OBB loading and TPM initialization when using Micron (Numonyx) N25Q128A11 SPI chip. Recommend to either use eMMC firmware booting or Winbond W25Q128FW SPI chip. No plan to investigate a solution to this. **Tip to resolve this issue** "**GP_SSP_1_CLK** needs to be pulled down after Intel® FSP memory init is completed, not at boot time."

- There is a duplicate of ISH Controller configurable option displayed when using BCT tool to configure the Intel® FSP binary. The duplicate of ISH Controller is supposed to be for "Enable/Disable BIOS Interface Lock Down bit to prevent writes to the Backup Control Register. 0:Disable, 1:Enable(Default)." This will be fixed in the next release of Intel® FSP. **This issue has been resolved as of Gold.**

- Issue configuring xHCI option in BCT issue; the default value is set as "Auto" but only allows to be set as enabled or disabled, should be changed to be a 4-option type field: {Mode of operation of xHCI controller. 0: Disable, 1:Enable, 2:Auto(Default), 3:SmartAuto.}. Can be worked around by overriding the UPD value in boot loader code before calling Intel® FSP silicon initialization if desired. Will be fixed to provide correct configurable options via BCT in a future release. **This issue has been resolved as of Gold.**

- The most current release of Intel® Binary Configuration Tool (3.2.0) is incompatible with the Intel® Firmware Support Package (Intel® FSP) binary included in this release. Settings can be overridden from within the boot loader call prior to Intel® FSP API calls. **This issue has been resolved as of Beta 1.**

§

5.0 Where to Find the Release

This package can be found at https://github.com/IntelFsp/FSP/tree/master/ApolloLakeFspBinPkg .

§

6.0 Release Content

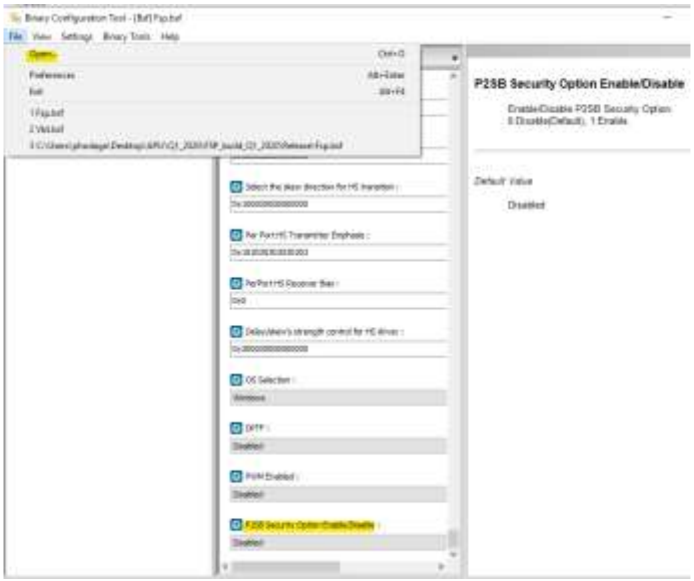
This release contains:

- Intel® FSP Integration Guide
- Intel® FSP Binary
- Binary Settings File (BSF)
- Graphics VBT and BSF file
- Release Notes

§

7.0 Steps to differentiate MR9 and MR6

- The Intel® FSP for MR9 and MR6 can be differentiate by reading the config using BCT tools since MR9 contain features that are not included in MR6.
- See 9.0 Configuration to get BCT tools.
- Open Fsp.bsf in BCT tools.



Select the skew direction for HS transition :
Per Port HS Transmitter Emphasis :
Per Port HS Receiver Bias :
Delay/skew's strength control for HS driver :
OS Selection :
Windows
DPTF :
Disabled
PAVP Enabled :
Disabled
P2SB Security Option Enable/Disable :
Disabled

P2SB Security Option Enable/Disable

Enable/Disable P2SB Security Option
0:Disable(Default), 1:Enable

Default Value

Disabled

- Check whether there is config of ‘**Refresh Watermark**’ in FSP_M settings and ‘**P2SB security option**’ in FSP_S settings.
- If yes, it is MR9.

§

8.0 Hardware and Software Compatibility

8.1 Supported Hardware

This Intel® Firmware Support Package (Intel® FSP) release is specifically targeted for the Intel® Atom™ processor E3900 product family (formerly Apollo Lake).

8.2 Supported Operating Systems

This release can be installed on either a Windows* or a Linux* system. However, the Intel® FSP binary itself can be used with any software development environment to generate a complete boot loader solution.

The software in this release has been validated on customer reference boards (CRBs) with the boot loader and operating systems listed in the following table.

Table 5. Operating System/Boot Loader Support

Product Family	Boot Loader	Operating System
Intel® Atom™ processor E3900 product family (formerly Apollo Lake)	1) Open source Coreboot (commit: **645d2a817a)** with the open source UEFI payload 2) Internal release MR4 Coreboot with internal Release UEFI payload.	Yocto Project* Windows 10 (Core and IOT)

§

9.0 Configuration

Intel® Binary Configuration Tool (BCT) for Intel® Firmware Support Package (Intel® FSP) is provided as a companion tool and is intended to be used to:

- Customize the Intel® FSP binary configuration options based on the Binary Settings File (BSF).
- Rebase the Intel® FSP binary to a different base address.

It is recommended to use the latest version of Intel® Binary Configuration Tool with this release.

See *Intel® Binary Configuration Tool User Guide* for the usage instructions. See Section 1.2, Related Documentation, Tools, and Packages, for information on where to download the tool.

9.1 Rebasing

When integrating Intel® FSP with a boot loader, place Intel® FSP at the same base address that it is configured to. Intel® Binary Configuration Tool can be used to rebase the Intel® FSP binary.

9.2 Microcode

Use the latest microcode when integrating Intel® FSP. Any processor that does not have the correct updated microcode loaded, is considered to be operating out of specification. See the integration guide for more details regarding microcode loading.

Microcode is now released at GitHub: https://github.com/otcshare/Intel-Generic-Microcode

Refer to Doc#: in GitHub (R) MCU Repository Training v1.3 on how to obtain the Microcode patch from GitHub.

§

10.0 Stitching Ingredients

Updated stitching ingredients listed below:

Package	Kit #
Apollo Lake-I Intel® Trusted Execution Engine 3.1.76.2356 Production Version Release	VIP 136210
PMC - Apollo Lake Intel® PMC Firmware Version 03.21.00_PROD Hot Fix Release	VIP 135401
Intel® Integrated Sensor Solution 4.1.0.3364_PROD kit	VIP 122769
BpmGen Tool version 2.4 **-Copy "BpmGen2.exe" to BlStitch\Signing\GenBPM.exe**	bpmgen2release2019-08-30.zip
Apollo Lake Soc B0/B1/B2/D0 CPU Signature 506c9 Microcode Punit Patch m_03_506c9_00000040	https://github.com/otcshare/Intel-Generic-Microcode/tree/master/NDA/repository/soc/production
Apollo Lake I E0/F1 CPU Signature 506ca Ex Microcode Punit Patch m_03_506ca_0000001e	https://github.com/otcshare/Intel-Generic-Microcode/tree/master/NDA/repository/soc/production

Tested version:

- **Apollo Lake-I Intel® Trusted Execution Engine PV 3.1.76.2356_B0_PROD**
- **PMC - Apollo Lake Intel® PMC Firmware Version 03.21.00_PROD Hot Fix Release**
- **Intel® Integrated Sensor Solution 4.1.0.3364_PROD kit**
- **Apollo Lake soc CPU Signature 506c9 Ex Microcode Punit Patch m_03_506c9_0000003e.inc**
- **Apollo Lake I CPU Signature 506ca Ex Microcode Punit Patch m_03_506ca_0000001c.inc**

§