Intel® Xeon® D-2700 Processor Family Intel® Firmware Support Package (Intel® FSP)

Release Notes

September 2022

Revision 001US

Document Number: 742659

Notice: This document contains information on products in the design phase of development. The information here is subject to change without notice. Do not finalize a design with this information.

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software, or service activation. Learn more at intel.com, or from the OEM or retailer.

No computer system can be absolutely secure. Intel does not assume any liability for lost or stolen data or systems or any damages resulting from such losses.

You may not use or facilitate the use of this document in connection with any infringement or other legal analysis concerning Intel products described herein. You agree to grant Intel a non-exclusive, royalty-free license to any patent claim thereafter drafted which includes subject matter disclosed herein.

No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document. The products described may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

This document contains information on products, services and/or processes in development. All information provided here is subject to change without notice. Contact your Intel representative to obtain the latest Intel product specifications and roadmaps.

Intel disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade.

Intel does not control or audit third-party benchmark data or the web sites referenced in this document. You should visit the referenced web site and confirm whether referenced data are accurate.

Copies of documents which have an order number and are referenced in this document may be obtained by calling 1-800-548-4725 or by visiting www.intel.com/design/literature.htm.

Intel, the Intel logo, and Xeon are trademarks of Intel Corporation in the U.S. and/or other countries.

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

Copyright © 2022, Intel Corporation. All Rights Reserved.

Contents

1 Introduction 5
1.1 Component Information 5
1.2 Bootloader Requirements 5
1.3 Acronyms and Terms 6
1.4 Related Documentation, Tools, and Packages 7
1.5 Intended Audience 7
1.6 Customer Support 8

2 New in This Release 9
2.1 New Feature 9

3 Software Issues and Limitations 10
3.1 Known Issues 10
3.2 Resolved Issues 10
3.3 Limitations 10

4 Where to Find the Release 11
4.1 How to Unpack This Release 11
4.1.1 For Linux* 11
4.2 Microcode Update 11
4.3 Debug 11
4.4 BIOS Shared Software Architecture (BSSA) Rank Margining Tool (RMT) 12
4.5 Component Extraction 12

5 Release Content 13

6 Hardware and Software Compatibility 14
6.1 Supported Hardware 14
6.2 Supported Operating Systems 14

7 Configuration 15
7.1 Intel Firmware Support Package Information 15

Tables

Table 1. Intel FSP Component Information 5
Table 2. Terminology 6
Table 3. Intel Firmware Support Package Documentation 7
Table 4. Tool Versions 7
Table 5. Package Contents 13
Table 6. Operating System/Bootloader Support 14

Revision History

Revision Number	Description	Date
001US	• Initial release of the document.	September 2022

1 Introduction

This package contains required binary image(s) and collateral for the Intel® Xeon® D-2700 Processor Family Intel® Firmware Support Package (Intel® FSP).

This Intel® Firmware Support Package (Intel® FSP) is compliant with the *Intel® Firmware Support Package External Architecture Specification v2.1*.

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

To learn more about this product, refer to:

- New features listed in Section 2.0 or in the help
- Reference documentation listed in Section 1.4
- Installation instructions listed in Section 4.1

1.1 Component Information

The software in this release has been developed and validated using the following information as shown in Table 1.

Table 1. Intel FSP Component Information

Component	Version
Code Base	EDKII
Core Version	edk2-stable202102
Memory Reference Code Version	
Reference Code Build Version	0023.D.57

1.2 Bootloader Requirements

It is expected that the bootloader performs the following:

- Configure the HSUART device for the serial port. Refer to the UPD Data Region section of the *Intel® Xeon® D-2700 Processor Family Intel® Firmware Support Package (Intel® FSP) Integration Guide*.

Note: Intel Xeon D-2700 Processor Family Intel FSP does NOT support a legacy serial port.

- Implement the following functions depending on the specific platform requirements:
  - Addition of support for the (A0 stepping) silicon
  - Addition of support for required boards/platforms

- Set up of the operating environment for the Intel FSP Application Programming Interfaces (APIs) that includes, but is not limited to, the following:
  - CPU initialization
  - Loading microcode
  - Board-specific initialization including PCI enumeration and post-PCI enumeration initialization
  - Serial AT Attachment (SATA) initialization
  - Peripheral Component Interconnect Express* (PCIe*) initialization
  - Universal Serial Bus (USB) initialization
  - Power management initialization (S-states, P-states, wake events, and thermal)
  - Advanced Configuration and Power Interface (ACPI) support
  - Payload to load/boot the OS
  - Port 80 display
  - Fast boot support
  - Booting from USB2/USB3 storage devices
  - Booting from eMMC* storage device
  - IA64 mode support

1.3 Acronyms and Terms

Table 2 lists the acronyms and terms used in this document (in alphabetic order).

Table 2. Terminology

Term	Description
ACPI	Advanced Configuration and Power Interface
API	Application Programming Interface
BCT	Binary Configuration Tool
BIOS	Basic Input Output System
BKC	Best Know Configuration
BSF	Boot Settings File
CPU	Central Processing Unit
CRB	Customer Reference Board
eMMC	embedded Multi-Media-Card
FIA	Flexible I/O Adapter
Intel® FSP	Intel® Firmware Support Package
IBL	Intel® Business Link
MOW	Message of the Week
NS	Network Solutions

Term	Description
OS	Operating System
PCD	Platform Configuration Database
PCIe*	Peripheral Component Interconnect Express
RMT	Rank Margining Tool
SATA	Serial AT Attachment
SoC	System on a Chip
UPD	Updatable Product Data
USB	Universal Serial Bus

1.4 Related Documentation, Tools, and Packages

Table 3 lists the processor family documentation.

Table 3. Intel Firmware Support Package Documentation

Document Name	Reference Number
Intel® FSP External Architecture Specification v2.1 https://www.intel.com/content/www/us/en/intelligent-systems/intel-firmware-support-package/intel-fsp-overview.html	
Boot Setting File (BSF) Specification https://software.intel.com/content/www/us/en/develop/download/boot-setting-file-specification-release-10.html	
Binary Configuration Tool (BCT) for Intel® FSP https://github.com/IntelFsp/BCT	
Intel® Xeon® D-2700 Processor Family Intel® Firmware Support Package (Intel® FSP) Integration Guide	742659

Table 4 lists the tools applicable to this Intel FSP release.

Table 4. Tool Versions

Tool	Version
EDKII BaseTools	edk2-stable202102
Binary Configuration Tool (BCT)	3.4.1
Intel® Server Platform Services (Intel® SPS) FW (CRB) version	SPS_SoC-X_05.00.04.032.0

1.5 Intended Audience

This document is for platform and system developers who intend to use an Intel FSP based bootloader for the firmware solution for their overall design based on the Intel® Xeon® D-2700 Processor Family. This group includes system BIOS developers, bootloader developers, and system integrators.

1.6 Customer Support

Intel offers support for this software at the API level only, defined in the *Intel® Xeon® D-2700 Processor Family Intel® Firmware Support Package (Intel® FSP) Integration Guide*. If your field representative has created an account for you, support requests can be submitted at https://premiersupport.intel.com.

2 New in This Release

2.1 New Feature

This release includes the following new feature and product change:

- Build version 23.D.57

3 Software Issues and Limitations

Known and resolved issues relating to the Intel Firmware Support Package are described in this section.

3.1 Known Issues

None

3.2 Resolved Issues

None

3.3 Limitations

None

4 Where to Find the Release

This package can be found at https://github.com/intel/FSP.

4.1 How to Unpack This Release

This release can be unpacked on a Linux* or Windows* system.

4.1.1 For Linux*

1. Clone IdavilleFspBinPkg from GitHub.

Note: For guidance on how to add the Intel FSP APIs into the bootloader code, refer to the *Intel® Xeon® D-2700 Processor Family Intel® Firmware Support Package (Intel® FSP) Integration Guide* (refer to Table 3 for more information).

4.2 Microcode Update

The IA-32 processors have the capability to correct specific errata through the loading of an Intel supplied data block. This data block is referred to as a microcode update or system configuration data.

Each unique processor stepping/package combination has an associated microcode update that, when applied, constitutes a supported processor (that is, Specified Processor = Processor Stepping + Microcode Update). The proper microcode update must be loaded on each processor in a system. The proper microcode update is defined as the latest microcode update available from Intel for a given family, model, and stepping of the processor. Any processor that does not have the correct microcode update loaded is operating out of specification.

Intel recommends that future microcode updates are done as soon as the latest ones are released.

4.3 Debug

Debug messages are the primary way of debugging the Intel FSP. Debug messages are suppressed for production binary and enabled by default in the debug binary.

4.4 BIOS Shared Software Architecture (BSSA) Rank Margining Tool (RMT)

The RMT can flag areas of concern for platform developers and is disabled by default in this Intel FSP release.

4.5 Component Extraction

The Intel FSP binary is released as a single binary. Use the Python* script, SplitFspBin.py, to split the binary into the different components.

SplitFspBin.py is available at:
https://github.com/IntelFsp/FSP/blob/master/Tools/SplitFspBin.py

The sample command shown next creates three binaries named after the inputting the Intel FSP binary and appending with "_M", "_S", and "_T", respectively.

```
python SplitFspBin.py split -f <FSP Binary>
```

Example: `python IntelFsp2Pkg\Tools\SplitFspBin.py split -f FspRel.bin`

Example Output:

- `FspRel_M.bin`
- `FspRel_S.bin`
- `FspRel_T.bin`

5 Release Content

This release package contains the following contents.

Table 5. Package Contents

Description	Filename	Path
Intel FSP Binary File	FspRel.bin	ICELAKE-D_FSP_KIT/ IdavilleFspBinPkg/Hcc/FspBin
Boot Setting File (BSF)	FspRel.bsf	ICELAKE-D_FSP_KIT/ IdavilleFspBinPkg/Hcc/FspBin
Documents	IcelakeDEFsp IntegrationGuide.pdf IcelakeDEFsp ReleaseNotes.pdf	ICELAKE-D_FSP_KIT/ IdavilleFspBinPkg/Hcc/Docs
Sample File	FsptUpd.h FspmUpd.h FspsUpd.h FspUpd.h	ICELAKE-D_FSP_KIT/ IdavilleFspBinPkg/Hcc/Include

6 Hardware and Software Compatibility

6.1 Supported Hardware

The Intel FSP included in this release is specifically targeted for the Intel® Xeon® D-2700 Processor Family.

6.2 Supported Operating Systems

This release installs 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 bootloader solution.

The software in this release has been validated against the operating systems given in Table 6 on the Customer Reference Boards (CRBs) for the Intel® Xeon® D-2700 Processor Family.

Note: While the Intel FSP is validated on the slim bootloader and Fedora* operating systems on the respective platforms, it is designed to work without any changes on some other bootloader and operating systems.

Table 6. Operating System/Bootloader Support

Software Type	Name	Version
Bootloader	Slim Boot	SBID: SB_IDV ISVN: 001 IVER: 001.000.001.000.00000
Firmware Component	Intel SPS Intel ME Firmware	SoC-X_05.00.04.032.0
Firmware Component	Intel FSP	23.D.57
Operating System	Yocto*	Yocto version
Tool	BCT	3.4.1

NOTE: Validation was done on Moro City with Intel Xeon D-2700 Processor Family QYDX and QYDZ QDFs only. ***

7 Configuration

A Binary Configuration Tool (BCT) for the 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 Boot Setting File (BSF).
- Rebase the Intel FSP binary to a different base address (the default base address of the Intel FSP for Intel® Xeon® D-2700 Processor Family is 0xFFF85000 for FSP-T, 0xFFDA8000 for FSP-M and 0xFFD3A000 for FSP-S).

Intel recommends using the latest BCT with this release.

Refer to the BCT User Guide for usage instructions. Refer to Section 1.4 to obtain the BCT.

7.1 Intel Firmware Support Package Information

To obtain the Intel FSP binary information:

1. Run the Binary Configuration Tool.
2. Click the Show Binary Description command button.
3. Select the Intel FSP binary. For this release, the binary included is named as:

   FspRel.bin (release version)
4. Click Open. Another window will open and show the Intel FSP binary information.
5. Click OK to close the window.

This Intel FSP release has the following Binary Description.

```
FSP-T Header Details.................

This FSP supports the following:

ICXD



Build: 0023.D57

FSP Version: 0.0.23.57

FSP Header:
```

```
  Signature: FSPH
  Header Length: 0x50
  Header Revision: 0x4
  SpecVersion: 0x21
  Image Revision: 0x2357
  Image ID: ICXD-FSP
  Image Size: 0x6000
  Image Base: 0xfff96000
  Image Attribute: 0x10030002
  Configuration Region Offset: 0x184
  Configuration Region Size: 0x80
  API Entry Num: 0x0
  Temp RAM Init Entry: 0x549
  FSP Init Entry: 0x0
  Notify Phase Entry: 0x0
  FSP Memory Init Entry: 0x0
  Temp RAM Exit Entry: 0x0
  FSP Silicon Init Entry: 0x0

FSP Extended Header:
  Signature: FSPE
  Header Length: 0x18
  Header Revision: 0x1
  FSP Producer Id: INTELC
  FSP Producer Revision: 0x1

FSP-M Header Details.................
This FSP supports the following:
ICXD
```

```
Build: 0023.D57

FSP Version: 0.0.23.57

FSP Header:

  Signature: FSPH

  Header Length: 0x50

  Header Revision: 0x4

  SpecVersion: 0x21

  Image Revision: 0x2357

  Image ID: ICXD-FSP

  Image Size: 0x1e5000

  Image Base: 0xffdb1000

  Image Attribute: 0x20030002

  Configuration Region Offset: 0x184

  Configuration Region Size: 0x20d

  API Entry Num: 0x0

  Temp RAM Init Entry: 0x0

  FSP Init Entry: 0x0

  Notify Phase Entry: 0x0

  FSP Memory Init Entry: 0x488

  Temp RAM Exit Entry: 0x492

  FSP Silicon Init Entry: 0x0


FSP Extended Header:

  Signature: FSPE

  Header Length: 0x18

  Header Revision: 0x1

  FSP Producer Id: INTELC

  FSP Producer Revision: 0x1
```

```
FSP-S Header Details.................
This FSP supports the following:
ICXD



Build: 0023.D57
FSP Version: 0.0.23.57
FSP Header:
  Signature: FSPH
  Header Length: 0x50
  Header Revision: 0x4
  SpecVersion: 0x21
  Image Revision: 0x2357
  Image ID: ICXD-FSP
  Image Size: 0x91000
  Image Base: 0xffd20000
  Image Attribute: 0x30030002
  Configuration Region Offset: 0x184
  Configuration Region Size: 0x125
  API Entry Num: 0x0
  Temp RAM Init Entry: 0x0
  FSP Init Entry: 0x0
  Notify Phase Entry: 0x370
  FSP Memory Init Entry: 0x0
  Temp RAM Exit Entry: 0x0
  FSP Silicon Init Entry: 0x37a

FSP Extended Header:
  Signature: FSPE
  Header Length: 0x18
```

```
Header Revision: 0x1

FSP Producer Id: INTELC

FSP Producer Revision: 0x1
```