Intel® Firmware Support Package (Intel® FSP) for Intel® Xeon® Processor D Product Family, Gold 001

Release Notes

October 2015

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.

All information provided here is subject to change without notice. Contact your Intel representative to obtain the latest Intel product specifications and roadmaps.

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.

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: http://www.intel.com/design/literature.htm

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

Contents

Tables

Revision History

Date	Revision	Description
October 16, 2015	GOLD1	Gold 001 Release
May 27, 2015	BETA1	Beta 001 Release
March 6, 2015	ALPHA1	Alpha 001 Release

§

1.0 Introduction

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

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

To learn more about this product, see:

- New features are listed in the New in This Release, or in the help.
- Reference documentation listed in the Related Documentation, Tools, and Packages section.
- Installation instructions can be found in the How to Install this Release section.

Table 1 lists the relevant platform software components used during development and validation of this release.

Table 1. Platform Software Component Information

Component	GOLD
Reference Code Version	01.80.20.00
SPS FW Version	SPS_SoC-X_03.00.03.009.0_PC-GVL_REL
Microcode Update (U0-stepping)	MFF50661_F1000008
Microcode Update (V1-stepping)	M1050662_0000000A
Microcode Update (V2-stepping)	M1050663_07000001

1.1 Terminology

The following acronyms and terms are used in this document.

Table 2. Terminology

Term	Description
BCT	Binary Configuration Tool
BSF	Binary Settings File
CRB	Customer Reference Board
EDC	Embedded Design Center

Term	Description
FSP	Firmware Support Package
SoC	System on a Chip
TXE	Trusted Execution Engine
UPD	Updatable Product Data
VPD	Vital Product Data

1.2 Related Documentation, Tools, and Packages

Table 3. Related Documentation, Tools, and Packages

Document #	Document	Location
-	*Intel® Firmware Support Package (Intel® FSP) for Intel® Xeon® Processor D Product Family Integration Guide*	Available in this release package
-	*Binary Configuration Tool (BCT) for Intel® FSP*	www.intel.com/fsp

1.3 Intended Audience

The intended audience is platform and system developers who intend to use an Intel® FSP-based boot loader for the firmware solution for their overall design based on the Intel® Xeon® Processor D Product Family. 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 FSP Integration guide and reference manuals listed in the Related Documentation, Tools, and Packages section.

For technical support, see the Intel Embedded Design Center (Intel EDC) Support website at:

http://www.intel.com/content/www/us/en/intelligent-systems/embedded-design-center-contact-us.html

§

2.0 New in This Release

2.1 New Features

This release includes the following new features and product changes:

- Updated to reference code (RC) version 01.80.20.00.
- Added UPD option to Enable/Disable Turbo Mode.
- Added UPD option for basic ASPM configuration.
- Added UPD option to enable FSP to switch to the max non-turbo frequency.
- Added UPD option to enable EV DFx features, for testing purposes.
- Added UPD option to selectively hide the PCH thermal device (D31:F6).

§

3.0 Fixed Issues

The following table contains the fixed issues in this release:

Reference No.	Description	Impact	Affected Component(s)	Affected OS(s)	Resolution
N/A	XHCI BAR being destroyed.	USB 3.0 devices not working in OS.	USB	Fedora 21	Fixed in FSP.
N/A	EOP message not being sent to ME.	Out of specification and potential system security/stability problem.	System	N/A	Enabled sending of EOP message from FSP on the ReadyToBoot API call.
N/A	Incorrect SPD page being read from.	System may fail during memory training failure with message “DIMM not supported.”	MRC	N/A	Always reset SPD page back to 0 in FSP.
N/A	Watchdog timer resets system if verbose output is enabled.	System may reset unexpectedly.	System	N/A	Halt WDT earlier in boot process in FSP.
N/A	LPC UART not functional when SerialPortConfigure UPD parameter is set to 0.	External LPC UART may not function as expected.	UART	N/A	Fixed in FSP.

§

4.0 Limitations

- The Fast Boot feature is only supported on ES2 and later steppings.

§

5.0 Known Issues

None.

§

6.0 Where to Find the Release

This package can be found at www.intel.com/fsp.

6.1 How to Install this Release

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

For Windows*:

1. Download the Windows .exe file from www.intel.com/fsp.
2. Run the .exe file to perform the installation.

For Linux*:

1. Download the Linux* .tgz file from www.intel.com/fsp.
2. Extract the contents of the .tgz file.
3. See the Readme_Extract.txt file for further instructions to complete the installation.

Note: For the guide to integrate the Intel® FSP APIs into the boot loader code, please refer to the *Intel® Firmware Support Package (Intel® FSP) for Intel® Xeon® Processor D Product Family Integration Guide.*

§

7.0 Release Content

This release contains:

- FSP Integration Guide
- FSP Binary
- Boot Settings File (BSF)
- Release Notes
- Sample Code

§

8.0 Hardware and Software Compatibility

8.1 Supported Hardware

The FSP included in this release is specifically targeted for the Intel® Xeon® Processor D Product Family System on a Chip (SoC).

8.2 Supported Operating Systems

This release installs on either a Windows or a Linux system. However, the 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 against the boot loader and operating systems given in the following table on the Customer Reference Boards (CRBs).

Table 4. Operating System/Boot Loader Support

Product Family	Boot loader	Operating System
Intel® Xeon® Processor D Product Family	Coreboot with the U-boot payload.	Fedora 21

§

9.0 Configuration

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

- Customize the FSP binary configuration options based on the Boot Setting File (BSF).
- Rebase the FSP binary to a different base address.

It is recommended to use latest version of the BCT with this release.

Please refer to the BCT User Guide for the usage instructions. See the Related Documentation, Tools, and Packages to for information on where to download the BCT.

9.1 Rebasing

When integrating with a bootloader, the FSP should be placed at the same base address that it is configured to. The BCT can be used to rebase the FSP binary.

9.2 Microcode

The latest microcode should be used when integrating FSP. Any processor that does not have the correct microcode update loaded is considered to be operating out of specification. Please consult the integration guide for more details regarding microcode loading.