Intel® Server Platform Services Manageability Engine Firmware for Lewisburg Product Line Full, SiEn

Customer Release Notes

PV RC1 Release for Purley-Refresh Platforms

Document Version 1.0

January 2019

Contents

List of Tables

1. Introduction

These release notes are intended for the PV RC1 release of the Intel® Server Platform Services Manageability Engine Firmware for the Lewisburg Product Line.

The product name is abbreviated to SPS in the remainder of this document.

SPS Firmware for Purley-Refresh platform can be configured in 2 different SKUs: Full, SiEn. Please refer to Intel® SPS External Product Specification [555192] for information regarding the Firmware SKU definition.

1.1. Revision Numbers of SPS Package Components

Table 1.1: Revision numbers of PV RC1 release components included in SPS_E5_04.01.04.251.0.zip package.

Subproject (component)	Location	Revision
Intel(R) SPS ME Firmware	/spsOperational.bin	SPS_E5_04.01.04.251.0
Intel(R) SPS ME Recovery Boot Loader	/spsRecovery.bin	SPS_E5_04.01.04.251.0
Intel(R) SPS ME Pure Recovery Boot Loader	/spsPureRecovery.bin	SPS_E5_04.01.04.251.0
Intel Flash Image Tool for Server Platform Services only	/Tools/FlashImageTool	SPS_E5_04.01.04.251.0

Table 1.2: Revision numbers of PV RC1 release components included in SPS_EPO_04.01.04.251.0.zip package.

Subproject (component)	Location	Revision
Intel(R) SPS ME Firmware	/spsOperational.bin	SPS_EPO_04.01.04.251.0
Intel(R) SPS ME Recovery Boot Loader	/spsRecovery.bin	SPS_EPO_04.01.04.251.0
Intel(R) SPS ME Pure Recovery Boot Loader	/spsPureRecovery.bin	SPS_EPO_04.01.04.251.0
Intel Flash Image Tool for Server Platform Services only	/Tools/FlashImageTool	SPS_EPO_04.01.04.251.0

Table 1.3: Revision numbers of PV RC1 release components included in SPS_Tools_4.2.97.99.zip package.

Subproject (component)	Location	Revision
Intel® Flash Programming Tool	/FlashProgrammingTool	SPS_Tools_4.2.97.99
SPS ME SMBus Diagnostic Console	/MeDiagnosticConsole	SPS_Tools_4.2.97.99
SPS ME SMBus Diagnostic Console	/MeDiagnosticConsoleAgent	SPS_Tools_4.2.97.99
Intel® ME Info with support for SPS	/SpsInfo	SPS_Tools_4.2.97.99
SPS FW Manufacturing Tool	/SpsManuf	SPS_Tools_4.2.97.99
Sample Update Tool for SPS	/SampleUpdateTool	SPS_Tools_4.2.97.99
NULL Heci Driver	/NullHeciDriver	SPS_Tools_4.2.97.99
Compliance Tests IPMI Tool Scripts	/ComplianceTestsScripts	SPS_Tools_4.2.97.99

Table 1.4: Revision numbers of PV RC1 release components included in SPS_Tools_4.2.61.89_epo.zip package.

Subproject (component)	Location	Revision
SPS ME SMBus Diagnostic Console	/MeDiagnosticConsole	SPS_Tools_4.2.61.89_epo

Table 1.5: Revision numbers visible in component properties, on the console, or over IPMI included in SPS_E5_04.01.04.251.0.zip package.

Console-Component	Revision
ME SPS Firmware Get Device Id response	50 01 04 14 02 21 57 01 00 0A 0B 04 25 10 01
ME SPS Recovery Boot Loader Get Device Id response	50 01 84 14 02 20 57 01 00 0A 0B 00 25 10 00
ME SPS Pure Recovery Boot Loader Get Device Id response	50 01 84 14 02 20 57 01 00 0A 0B 00 25 10 00
HECI MKHI_GET_FW_VERSION response	04.01.04.251
spsFITc.exe	4.1.4.251
SPS NM PTU option ROM SHA-256 hash to support UEFI Secure Boot : : :	0.2 D0 1D 14 F7 E8 93 7B B1 42 C3 0B 8F 5A 3B CA 40 1C 59 DD 6E CA 7C 22 08 40 5A BF E3 AB 68 6D A1

Table 1.6: Revision numbers visible in component properties, on the console, or over IPMI included in SPS_EPO_04.01.04.251.0.zip package.

Console-Component	Revision
ME SPS Firmware Get Device Id response	50 01 04 14 02 21 57 01 00 0C 0B 00 25 10 01
ME SPS Recovery Boot Loader Get Device Id response	————————
ME SPS Pure Recovery Boot Loader Get Device Id response	————————
HECI MKHI_GET_FW_VERSION response	04.01.04.251
spsFITc.exe	4.1.4.251

Table 1.7: Revision numbers visible in component properties, on the console, or over IPMI included in SPS_Tools_4.2.97.99.zip package.

Console-Component	Revision
spsFPT.efi, spsFPTW64.exe	SPS_Tools_4.2.97.99
MESDC.exe	SPS_Tools_4.2.97.99
RemoteAgentLinux64, RemoteAgentWin64.exe	SPS_Tools_4.2.97.99
spsInfoWin64.exe, spsInfoLinux64, spsInfo.efi	SPS_Tools_4.2.97.99
spsManufWin64.exe, spsManuf.efi, spsManufLinux64	SPS_Tools_4.2.97.99

Table 1.8: Revision numbers visible in component properties, on the console, or over IPMI included in SPS_Tools_4.2.61.89_epo.zip package.

Console-Component	Revision
MESDC.exe	SPS_Tools_4.2.61.89_epo

2. SPS Package Contents

Table 2.1 lists the contents of the release package.

Note: All of this software needs Intel® compatible PC with Microsoft Windows 7® x64, Microsoft Windows 8.1® x86/x64, Microsoft Windows 10® x64, Microsoft Windows Server 2012® R2 SP1 x64 or Microsoft Windows Server 10® x64 operating system installed depending on the specific tool requirements listed below.

Note: The release package contains one license file placed in the main directory. This license is specified for PV RC1 release firmware.

Table 2.1: Software package

No.	Package	Contents
1	ReleaseNotes.pdf	This file.
2	Tools User Guide.pdf	User Guide for Tools package.
3	SPS_E5_04.01.04.251.0	This is a release package with Intel SPS ME Firmware and Tools for Lewisburg platform. Uncompress the package. The package will uncompress into SPS_E5_04.01.04.251.0 directory. SPSOperational - Uncompressed SPS firmware binary for Lewisburg stepping of silicon located in the main directory. SPSRecovery - Uncompressed SPS firmware binary for Lewisburg stepping of silicon located in the main directory. SPSPureRecovery - Uncompressed SPS firmware binary for Lewisburg stepping of silicon located in the main directory. Intel Flash Image Tool for Server Platform Services only - Microstoft Windows* tool: This is a tool to create SPI Flash image and to modify SPS Firmware factory configuration. This tool is unpacked into the /Tools/FlashImageTool directory with dedicated license.

Table 2.1: Software package

No.	Package	Contents
4	SPS_EPO_04.01.04.251.0	This is a release package with Intel SPS ME Firmware and Tools for Lewisburg Endpoint Only platform. Uncompress the package. The package will uncompress into SPS_EPO_04.01.04.251.0 directory. SPSOperational - Uncompressed SPS firmware binary for Lewisburg stepping of silicon located in the main directory. SPSRecovery - Uncompressed SPS firmware binary for Lewisburg stepping of silicon located in the main directory. SPSPureRecovery - Uncompressed SPS firmware binary for Lewisburg stepping of silicon located in the main directory. Intel Flash Image Tool for Server Platform Services only - Microstoft Windows* tool: This is a tool to create SPI Flash image and to modify SPS Firmware factory configuration. This tool is unpacked into the /Tools/FlashImageTool directory with dedicated license.

Table 2.1: Software package

No.	Package	Contents
5	SPS_Tools_4.2.97.99	This is a release package with Intel SPS Tools. Tools from this package will work with -Refresh platform. The package will uncompress into zip directory. Flash Programming Tool - Microsoft Windows* tool: Flash Programming Tool for PCH attached SPI Flash. This tool is unpacked into the /FlashProgrammingTool directory with dedicated license. ME SMBus Diagnostic Console Application. This tool is used to diagnose ME Firmware through SMBus interface. The main purpose of this tool is to provide live feedback from ME FW. ME SMBus Diagnostic Console Application is unpacked into the /MeDiagnosticConsole directory. MESDC Agent. This tool is a proxy application for MESDC. It connects MESDC using the LAN connection with the SPS FW using the HECI connection. MESDC Agent is unpacked into the /MeDiagnosticConsoleAgent directory. SPS Info tool for checking basic ME health and supported features list in /SpsInfo directory. SPS Manuf tool for validation ME functionality on the manufacturing line in /SpsManuf directory. SiEn specific Sample Update Tool source code for online update over IPMI interface in /SampleUpdateTool directory. Null HECI driver - Windows setup provides null driver removing unknown device warning from Device manager in /NullHeciDriver directory. Compliance Tests IPMI Tool Scripts in /ComplianceTestsScripts directory.
6	SPS_Tools_4.2.61.89_epo	This is a release package with Intel SPS Tools. Tools from this package will work with -Refresh platform. The package will uncompress into zip directory. ME SMBus Diagnostic Console Application. This tool is used to diagnose ME Firmware through SMBus interface. The main purpose of this tool is to provide live feedback from ME FW. ME SMBus Diagnostic Console Application is unpacked into the /MeDiagnosticConsole directory.

3. New/Changed Features

3.1. New/Changed Features

Purley-Refresh platforms (SiEn and Full) introduces the following new features.

- New firmware version SPS_E5_04.01.04.251.0 is provided.
- **This version of FW can be used on PRQ PCH. When running this firmware on PRQ PCH silicon, Field Programmable Fuses (FPFs) will be permanently and irreversibly set as per Intel End of Manufacturing (EOM) process flow guidelines. Please refer to Purley Manufacturing Test (document 569314) for details on the EOM process.**

3.2. Limitations

The following list describes all the limitations for this SPS release
This code was tested in the following configuration:

- Neon City RP
  - Firmware: SiEn, Full
  - PCH: LBG B0, B1, B2 also S0 and S1.
  - CPU: CLX A0 and B0
  - Various memory configs: from 1 to max platform capacity RDIMMs
- Lightning Ridge
  - Firmware: SiEn, Full
  - PCH: LBG B0 and B1
  - CPU: SKX B0 and H0
  - Various memory configs: from 1 to max platform capacity RDIMMs
- Taliverde CRB
  - PCH: LBG B0 and B1

This release was tested with the following operating systems:

- Microsoft Windows 2012 R2
- RHEL 7.22 x64*

This release was tested with the following versions:

- BIOS version: PLYXCRB1.SBT.0566.D03.1812120917
- mPhy table version: RC8

- PMC version: a0-16ww39a; b0-18ww34a
- PTT version: 302.8

To enable SMBus diagnostic interface using spsFITc:

- PCH Strap 54 -> SMTEN = 0x1
- Configuration -> MESDC -> SMT config -> Diagnostic/Tracing SMT Device set to SMBus
- Configuration -> MESDC -> SMT config -> I2C Address set to 0x38

For executing Online Flash Update on Taliverde platform, dual image option is required:

- DualImage value = 0x1

Unexpected reboots on some platforms can be avoided by changing strap:

- PCH Strap119 -> CPUPWRGDStretchingWDTimerEnable to enabled

In recovery the PTT works in Failure Mode only. To exit from PTT Failure Mode, platform or host reset is required.
MESDC Diagnostic Console Application does not fully support Purley End Point Only mode platform.
Booting in recovery (via jumper) might cause missing of some PCI devices.
Access to RF-NVRAM memory through PECI Proxy is available only for SKX H0.
Slave Attached Flash (SAF) mode does not support eSPI configurations single 20 MHz and single 30 MHz.
MESDC SMBus tracing when enabled may cause an exception during shutdown triggered by a ME Reset.
On Windows 2012R2 with Hyper-V role installed there is no possibility to change available cores number in runtime. This is OS limitation.
To disable global reset generated by ME during UMA Timeout, open your SPSfitc XML file and add the following lines immediately before </spsfiles>

```
<file name="SPS Special Options 1" enabled="true">

  <variable name="Option01" value="0x2FA332E6" />

</file>
```

Save the XML file and use it as input to SPSfitc to generate your SPI chip binary file image. NOTE: this manual edit overrides the UmaTimeoutGlobalResetDelay parameter in SPSfitc GUI.
ME doesn‘t comply to requirement of maximum frame length on IPMB interface equal to 80 bytes. ME can send IPMB frames of up to 137 bytes long. OEM FW should be prepared to handle IPMB frames of up to that length.
When PECI trust is disabled in BIOS it could impact to:

- memory utilization returns 0
- NM Prochot Assertion Ratio may not work

It will not change until 10nm CPU.

With NMPTU OPROM version 0.1 new CERT has been introduced. OPROM CERT file change could lead to conflict of secure boot process. User needs to take the corresponding actions to update the CERT file according to their platform and software design.

When downgrading to SPS_E5_04.01.02.161.0 or earlier Firmware Exception (A00901) and Manufacturing Error (A00705) will occur.

3.3. XML Changes

Initial XML version compilant with SPI Programming Guide - Revision 1.0 - document number: 574431

3.4. Documentation Updates

Table 3.1: Current SPS Firmware Documentation.

Document Title	Revision	Ref.
SPS 4.0 External Product Specification	2.20	555192
SPS 4.0 Services Integration Guide	2.05	550581
NM 4.0 External Interface Specification	2.07	550710
SPS 4.0 ME-to-BIOS Specification	1.0.15	548530
SPS 4.0 Tools Guide	2.3	Released with the kit
SPS 4.0 Tools Guide EPO	1.1	Released with the kit
SPS 4.0 Diagnostics Guide	2.0	554904
SPS 4.0 Purley Platform Integration Guide	1.1	560168

4. Known Issues

Table 4.1: Disposition field definition.

State	Definition
Under Investigation	The sighting is being investigated.
Root Cause Identified	The root cause for the defect is identified.
Workaround Available	A temporary solution to the defect is provided until the defect is fixed.

Table 4.2: Known Issues.

Issue Id	Description
124376	**Uefi PTU does not load DCPMEM memory in mixed mode**
Description	No stress is observed in memory domain when running UEFI PTU on system with DCPMEM modules with pool configured for volatile and non-volatile memory at the same time.
Root Cause	Virus Library used in Uefi Ptu does not support DCPMEM in mixed mode yet.
Status	Rootcause identified
Workaround	Sps NMPTU in current version will not support Mixed or AppDirect configurations - loading memory used as storage is not available. To measure maximum power consumption in memory domain OS PTU should be used. It can gain access to storage reserved memory from OS side.
128060	**Multiple UMA timeout SEL events when DCPMMs are mounted**
Description	Using DCPMMs in 2LM mode during OS boot ME hits multiple exceptions with ~0,5s interval between each one. In the result ME is put to the restricted mode.
Root Cause	Exceptions are the result of exceeding predefined UMA timeout during write transaction to UMA. Three UMA related exceptions same type hit within 30s period between each cause ME to go to restricted mode.
Status	Under Investigation.
Workaround	The UMA timeout value has been increased.
129718	**Exceptions in PTU with 8S and 18TB of Memory**
Description	Exceptions were observed, when ruuning the PTU on 8S system with large amounts of memory, 18TB in this case with SPS_E5_04.01.02.161.0.
Root Cause	Unknown.

Table 4.2: Known Issues.

Issue Id	Description
Status	Under Investigation.

5. Fixed Issues

Table 5.1: Disposition field definition.

State	Definition
As Designed	The issue reported is not a defect and the behavior will not be modified.
Closed no repro	The situation was not observed anymore and no further investigation is scheduled.
Fixed	Already fixed.

Table 5.2: Fixed Issues.

Issue Id	Description
129554	**Non-aggressive power limiting failure when using HWP.OOB mode.**
Description	When using non-aggressive power limiting with Hardware P-States set to Out of Band Mode, the moment of going into T-States will be detected earlier, and as a result limit will be kept higher than intended. The problem is caused by BIOS supplying Node Manager with Number of P-States = 0 when HWP is set to OOB, and NM not calculating the real number of P-States (based on the P-State ratio table), which is needed for non-aggressive limiting.
Root Cause	Legacy behavior that was incorrectly updated when the Host Configuration Message frame format was changed. When HWP.OOB was set and Turbo Mode was enabled, NM treated this configuration as invalid, sent an error to BIOS, and recalculated the number of P-States based on CPU parameters; side effect of the latter was that non-aggressive limiting worked, because NM created full P-State configuration for itself. When defect 127798 was fixed, the above configuration was made to be treated as valid, and therefore Number of P-States received from BIOS (= 0) was not updated, which broke non-aggressive limiting.
Status	Fixed. Node Manager will now properly update Number of P-States value
Workaround	Use aggressive limiting instead of non-aggressive.
129604	**PCH staps 128 and 129 not aligned with spec in extrnal ICC profile**
Description	After switching to External ICC Profile in Configuration/Silicon Enabling/Integrated Clock Controller, values of PCH straps 128 and 129 have invalid values
Root Cause	FITc and ICC documentation not inline

Table 5.2: Fixed Issues.

Issue Id	Description
Status	Fixed.