



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

Customer Release Notes

IPU 2022.2 PV Release for Purley-Refresh Platforms

Document Version 1.0

February 2022

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

UNLESS OTHERWISE AGREED IN WRITING BY INTEL, THE INTEL PRODUCTS ARE NOT DESIGNED NOR INTENDED FOR ANY APPLICATION IN WHICH THE FAILURE OF THE INTEL PRODUCT COULD CREATE A SITUATION WHERE PERSONAL INJURY OR DEATH MAY OCCUR.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined." Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.

The products described in this document 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.

Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order.

Copies of documents which have an order number and are referenced in this document, or other Intel literature, may be obtained by calling 1-800-548-4725, or go to: http://www.intel.com/#/en_US_01

Copyright©2022, Intel Corporation

Intel, the Intel logo are trademarks or registered trademarks of Intel Corporation.

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

Contents

1	Introduction	5
1.1	Revision Numbers of SPS Package Components	5
2	SPS Package Contents	8
3	New/Changed Features	11
3.1	New/Changed Features	11
3.2	Limitations	11
3.3	XML Changes	13
3.4	Documentation Updates	14
4	Known Issues	15
5	Fixed Issues	17

List of Tables

1.1	Revision numbers of IPU 2022.2 PV release components included in SPS_E5_04.01.04.804.0.zip package.	5
1.2	Revision numbers of IPU 2022.2 PV release components included in SPS_EPO_04.01.04.804.0.zip package.	6
1.3	Revision numbers visible in component properties, on the console, or over IPMI included in SPS_E5_04.01.04.804.0.zip package.	6
1.4	Revision numbers visible in component properties, on the console, or over IPMI included in SPS_EPO_04.01.04.804.0.zip package.	7
2.1	Software package	8
3.1	XML changes.	13
3.2	Current SPS Firmware Documentation.	14
4.1	Disposition field definition.	15
4.2	Known Issues.	15
5.1	Disposition field definition.	17
5.2	Fixed Issues.	17

1. Introduction

These release notes are intended for the IPU 2022.2 PV 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 IPU 2022.2 PV release components included in SPS_E5_04.01.04.804.0.zip package.

Subproject (component)	Location	Revision
Intel(R) SPS ME Firmware	/spsOperational.bin	SPS_E5_04.01.04.804.0
Intel(R) SPS ME Recovery Boot Loader	/spsRecovery.bin	SPS_E5_04.01.04.804.0
Intel(R) SPS ME Pure Recovery Boot Loader	/spsPureRecovery.bin	SPS_E5_04.01.04.804.0
Intel Flash Image Tool for Server Platform Services only	/Tools/FlashImageTool	SPS_E5_04.01.04.804.0
Intel® Flash Programming Tool	/Tools/FlashProgramming-Tool	SPS_Tools_4.2.97.451
SPS ME SMBus Diagnostic Console	/Tools/MeDiagnosticConsole	SPS_Tools_4.2.97.451
SPS ME SMBus Diagnostic Console	/Tools/MeDiagnostic-ConsoleAgent	SPS_Tools_4.2.97.451
Intel® ME Info with support for SPS	/Tools/SpsInfo	SPS_Tools_4.2.97.451
SPS FW Manufacturing Tool	/Tools/SpsManuf	SPS_Tools_4.2.97.451
Sample Update Tool for SPS	/Tools/SampleUpdateTool	SPS_Tools_4.2.97.451
NULL Heci Driver	/Tools/NullHeciDriver	SPS_Tools_4.2.97.451

Table 1.1: Revision numbers of IPU 2022.2 PV release components included in SPS_E5_04.01.04.804.0.zip package.

Subproject (component)	Location	Revision
Compliance Tests IPMI Tool Scripts	/Tools/ComplianceTestsScripts	SPS_Tools_4.2.97.451

Table 1.2: Revision numbers of IPU 2022.2 PV release components included in SPS_EPO_04.01.04.804.0.zip package.

Subproject (component)	Location	Revision
Intel(R) SPS ME Firmware	/spsOperational.bin	SPS_EPO_04.01.04.804.0
Intel(R) SPS ME Recovery Boot Loader	/spsRecovery.bin	SPS_EPO_04.01.04.804.0
Intel(R) SPS ME Pure Recovery Boot Loader	/spsPureRecovery.bin	SPS_EPO_04.01.04.804.0
Intel Flash Image Tool for Server Platform Services only	/Tools/FlashImageTool	SPS_EPO_04.01.04.804.0
SPS ME SMBus Diagnostic Console	/Tools/MeDiagnosticConsole	SPS_Tools_4.2.61.89_epo

Table 1.3: Revision numbers visible in component properties, on the console, or over IPMI included in SPS_E5_04.01.04.804.0.zip package.

Console-Component	Revision
ME SPS Firmware Get Device Id response	50 01 04 14 02 21 57 01 00 0a 0b 04 80 40 01
ME SPS Recovery Boot Loader Get Device Id response	50 01 84 14 02 20 57 01 00 0a 0b 00 80 40 00
ME SPS Pure Recovery Boot Loader Get Device Id response	
HECI MKHI_GET_FW_VERSION response	04.01.04.804
spsFITc.exe	4.1.4.804
spsFPT.efi, spsFPTW64.exe	SPS_Tools_4.2.97.451
MESDC.exe	SPS_Tools_4.2.97.451
RemoteAgentLinux64, RemoteAgentWin64.exe	SPS_Tools_4.2.97.451
spsInfoWin64.exe, spsInfoLinux64, spsInfo.efi	SPS_Tools_4.2.97.451
spsManufWin64.exe, spsManuf.efi, spsManufLinux64	SPS_Tools_4.2.97.451

Table 1.3: Revision numbers visible in component properties, on the console, or over IPMI included in SPS_E5_04.01.04.804.0.zip package.

Console-Component	Revision
SPS NM PTU option ROM	0.6
SHA-256 hash to support UEFI Secure Boot	65 91 A3 70 2B A8 C6 A3 5C 3F F0 F5 77 DD C8 6A 4D F9 30 26 9E F9 08 61 F9 73 0B 8E 08 71 DB 39
Root Cert: Purley_clx_SpsNMPTU_root.cer	
File: Purley_clx_SpsNMPTU_signed.rom	
DB Cert: Purley_clx_SpsNMPTU_signer.cer	

Table 1.4: Revision numbers visible in component properties, on the console, or over IPMI included in SPS_EPO_04.01.04.804.0.zip package.

Console-Component	Revision
ME SPS Firmware Get Device Id response	50 01 04 14 02 21 57 01 00 0c 0b 00 80 40 01
ME SPS Recovery Boot Loader Get Device Id response	_____
ME SPS Pure Recovery Boot Loader Get Device Id response	
spsFITc.exe	4.1.4.804
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 IPU 2022.2 PV 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_04.01.04.804.0	<p>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_04.01.04.804.0 directory.</p> <p>SPSOperational - Uncompressed SPS firmware binary for Lewisburg stepping of silicon located in the main directory.</p> <p>SPSRecovery - Uncompressed SPS firmware binary for Lewisburg stepping of silicon located in the main directory.</p> <p>SPSPureRecovery - Uncompressed SPS firmware binary for Lewisburg stepping of silicon located in the main directory.</p> <p>Intel Flash Image Tool for Server Platform Services only - Microsoft 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.</p>

Table 2.1: Software package

No.	Package	Contents
4	SPS_EPO_04.01.04.804.0	<p>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_04.01.04.804.0 directory. The release package contains file "Tools User Guide EPO.pdf"</p> <p>SPSOperational - Uncompressed SPS firmware binary for Lewisburg stepping of silicon located in the main directory.</p> <p>SPSRecovery - Uncompressed SPS firmware binary for Lewisburg stepping of silicon located in the main directory.</p> <p>SPSPureRecovery - Uncompressed SPS firmware binary for Lewisburg stepping of silicon located in the main directory.</p> <p>Intel Flash Image Tool for Server Platform Services only - Microsoft 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.</p>

Table 2.1: Software package

No.	Package	Contents
5	SPS_Tools_4.2.97.451	<p>This is a release package with Intel SPS Tools. Tools from this package will work with -Refresh platform. The package will uncompress into Tools directory.</p> <p>Flash Programming Tool - Microsoft Windows* tool: Flash Programming Tool for PCH attached SPI Flash. This tool is unpacked into the /Tools/FlashProgrammingTool directory.</p> <p>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 /Tools/MeDiagnosticConsole directory.</p> <p>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 /Tools/MeDiagnosticConsoleAgent directory.</p> <p>SPS Info tool for checking basic ME health and supported features list in /Tools/SpsInfo directory.</p> <p>SPS Manuf tool for validation ME functionality on the manufacturing line in /Tools/SpsManuf directory.</p> <p>SiEn specific Sample Update Tool source code for online update over IPMI interface in /Tools/SampleUpdateTool directory.</p> <p>Null HECI driver - Windows setup provides null driver removing unknown device warning from Device manager in /Tools/NullHeciDriver directory.</p> <p>Compliance Tests IPMI Tool Scripts in /Tools/ComplianceTestsScripts directory.</p>
6	SPS_Tools_4.2.61.89_epo	<p>This is a release package with Intel SPS Tools. Tools from this package will work with -Refresh platform. The package will uncompress into Tools directory.</p> <p>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 /Tools/MeDiagnosticConsole directory.</p>

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_04.01.04.804.0 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 2016 R2*
- RHEL 7.22 x64*

This release was tested with the following versions:

- BIOS version: PLYXINT1.86B.0618.D09.2112130437
- 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

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.

A global reset is required when upgrading from version SPS_E5_04.00.04.405.0 or earlier.

Sending IPMI command 0x40 (Send Raw PECI) with Command Code 0xA1 (RdPktConfig) to read PCS 0x16 (Get DIMM Temperature Data) with Parameter 0x03 (Channel Number) while executing Cscript command "mc.dim-minfo(haltIfNeeded=False)" results in abnormal temperature readings (0xD5 = 213 [Celsius degrees]).

In this release SPS FW disables internal timeout for receiving DRAM Init Done HECI message from BIOS. This timeout could cause boot issues on platforms with large memory capacity or when Advanced Memory Tests are being run as part of MRC.

3.3. XML Changes

No changes since SPS_E5_04.01.04.505.0.

Table 3.1: XML changes.

Issue ID	Change title	Change description
----------	--------------	--------------------

3.4. Documentation Updates

Table 3.2: Current SPS Firmware Documentation.

Document Title	Revision	Ref.
SPS 4.0 External Product Specification	2.21	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	1.0.21	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
126603	NM erroneously and intermittently report latched throttle status for HW Protection policy
Description	When active policy is removed and NM Throttling Status sticky bits are cleared immediately after that, new throttling will be registered with Source value equal 0 and Duration under 1 second.
Root Cause	Incomplete implementation. When throttling source (policy) is removed, Node Manager releases the limit gradually in order to prevent sudden power spikes. This process takes under a second to complete, and during this time throttling will be reported which is not generated by any policy.
Status	Documented in External Interface Specification.
Workaround	After removing the policy, wait for at least 1 second before clearing the throttling sources sticky bits.
129260	Multiple UMA timeout SEL events when DCPMMs are mounted
Description	None
Root Cause	Unknown.
Status	Under Investigation.
129360	Neon City with DCPMM reboot endlessly when NMPTU is triggered
Description	None
Root Cause	Unknown.
Status	Under Investigation.
129485	Missing MCTP Endpoints with SPS_E5_04.01.02.224.0
Description	None

Table 4.2: Known Issues.

Issue Id	Description
Root Cause	Unknown.
Status	Under Investigation.
129671	CPU PCI Configuration Read (44h) returns ABh completion code
Description	PECI CPU Cfg Read unexpectedly returns ABh completion code
Root Cause	Unknown.
Status	Under Investigation.
Workaround	Using raw Peci command (40h)
1807135105	NUMA node 0 namespace turns raw after ww28 BKC update
Description	
Root Cause	Unknown
Status	Under Investigation
1807135076	CLST vs HW Protection Policy behavior in user scenarios
Description	When one nonredundant PSU is disconnected there are observed several SmaRT&CLST ramps before HW protection policy kicks in due to single PSU overload
Root Cause	Unknown
Status	Under Investigation
1807135107	Short pulse for NM_PROCHOT_N and NM_MEMHOT_N are observed during DC ON
Description	It is observed that the ME will drive the NM_PROCHOT_N and NM_MEMHOT_N for a short pulse during boot time.
Root Cause	Unknown
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
18012822127	During G3 cycling stress testing, system stopped at postcode "0.5"
Description	Intel has observed an intermittent failure resuming from G3 to S0 on the Neon City CRB when executing an AC cycling test. The system can be recovered by hitting the power button or cycling AC again. This is observed with any 2020.2 IPU SPS FW releases (Beta/PV)
Root Cause	Wrong order of switching PLL modes in platform boot-up.
Status	Fixed