# Intel® Server S2600WF, Intel® Server S2600BP, and Intel® Server S2600ST Board Families

## *Activation Procedures for Trusted Platform Module 2.0 and Intel® Trusted Execution Technology*

**Rev 2.0**

**January 2022**

Intel® Server Products and Solutions

<Blank page>

# *Document Revision History*

| Date | Revision | Changes |
|---|---|---|
| July 2019 | 1.0 | Initial release. |
| January 2022 | 2.0 | New Procedure added.<br>Minor updates throughout for clarity. |

# *Disclaimers*

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. Intel products are not intended for use in medical, life-saving, or life sustaining applications. Intel may make changes to specifications and product descriptions at any time, without notice.

A "Mission Critical Application" is any application in which failure of the Intel Product could result, directly or indirectly, in personal injury or death. SHOULD YOU PURCHASE OR USE INTEL'S PRODUCTS FOR ANY SUCH MISSION CRITICAL APPLICATION, YOU SHALL INDEMNIFY AND HOLD INTEL AND ITS SUBSIDIARIES, SUBCONTRACTORS AND AFFILIATES, AND THE DIRECTORS, OFFICERS, AND EMPLOYEES OF EACH, HARMLESS AGAINST ALL CLAIMS COSTS, DAMAGES, AND EXPENSES AND REASONABLE ATTORNEYS' FEES ARISING OUT OF, DIRECTLY OR INDIRECTLY, ANY CLAIM OF PRODUCT LIABILITY, PERSONAL INJURY, OR DEATH ARISING IN ANY WAY OUT OF SUCH MISSION CRITICAL APPLICATION, WHETHER OR NOT INTEL OR ITS SUBCONTRACTOR WAS NEGLIGENT IN THE DESIGN, MANUFACTURE, OR WARNING OF THE INTEL PRODUCT OR ANY OF ITS PARTS.

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 product 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 and the software described in it are furnished under license and may only be used or copied in accordance with the terms of the license. The information in this manual is furnished for informational use only, is subject to change without notice, and should not be construed as a commitment by Intel Corporation. Intel Corporation assumes no responsibility or liability for any errors or inaccuracies that may appear in this document or any software that may be provided in association with this document.

Except as permitted by such license, no part of this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means without the express written consent of Intel Corporation.

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/design/literature.htm.

Intel and Xeon are trademarks or registered trademarks of Intel Corporation.

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

# Table of Contents

# List of Figures

<This page intentionally left blank>

# 1. Trusted Platform Module 2.0 and Intel® Trusted Execution Technology Activation

The following sections contain the steps required to activate the Trusted Platform Module 2.0 (TPM) and Intel® Trusted Execution Technology (Intel® TXT) within the Intel® Server S2600 product family.

## 1.1 Tools preparation

Below tools are required when provisioning the Intel® Server System S2600 product family, and are obtained from Intel® via the following links:

- **Server Security Toolkit** (CBnTToolkit): https://cdrdv2.intel.com/v1/dl/getContent/630398
- **TPM provision tool** (TPMProvfilesCBnT): https://cdrdv2.intel.com/v1/dl/getContent/633967

**Note:** Login or creation of an account may be required to enter to the Resource & Design Center web page.

Once both libraries have been downloaded, unzip them, copy the content to a USB device and attach it to an available server USB port where Intel® TXT is being activated.

## 1.2 Setting the Administrator Password

The administrator password must be set in order to enable the TPM module within the Intel® Server System S2600 product family by accessing the **BIOS Security** menu as shown in Figure 1.


**Figure 2. BIOS Security menu**

This password may be between 1 to 14 characters long, and can both be case-sensitive and allow for special characters such as: **!@#$%^&*()-_+=?**.

**Note:** Disabling the administrator password disables all user passwords.

Once the password has been set, reboot the server in order to further configure the BIOS security and TPM settings.

## 1.3 Activating the TPM

Once the administrator password is set, the BIOS identifies the plugged chip in the system and enables relevant TPM options. Select the boxes in the PCR bank sub-menu in order to activate the chip's encryption algorithms and to store private keys within the PCR registries as shown in Figure 3.

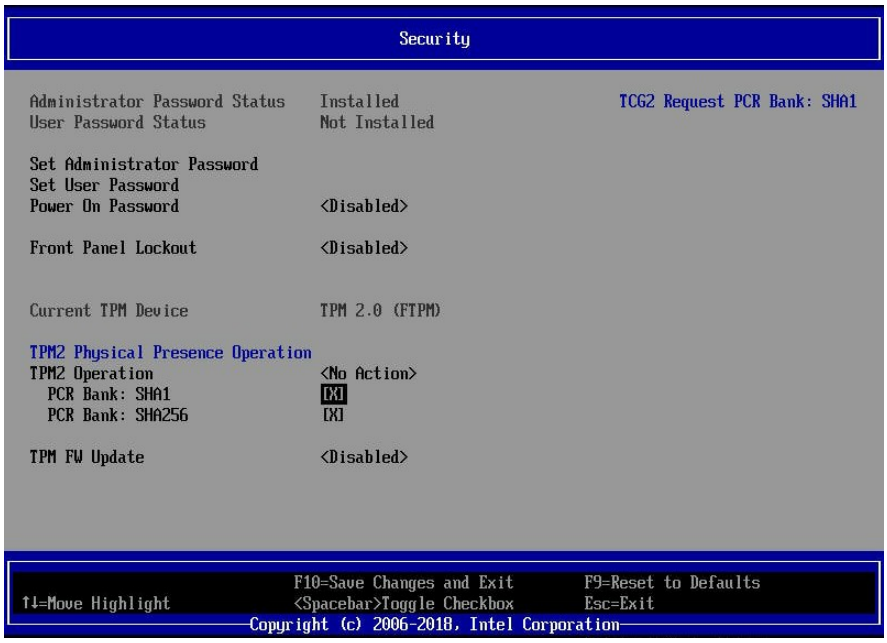


**Figure 4. Activating the PCR banks**

Launch an EFI shell from the previously created USB device. Navigate the following BIOS pathway to launch an EFI shell:

**Boot Manager --> Launch EFI Shell**


**Figure 5. Launching the EFI shell**

After launching the EFI shell, execute the following commands:

- **> fs0:**
- **FS0:\> cd "TPM2ProvfilesCBnT"**
- **FS0:\> ResetPlatformAuth.nsh SHA256 EXAMPLE**

```
FS0:\TPM2ProvfilesCBnT\> ResetPlatformAuth.nsh SHA256 EXAMPLE
FS0:\TPM2ProvfilesCBnT\> echo -OFF
**** Start Policy Session for PlatformPolicy
Attempting to satisfy PlatformPolicy and use it to change PlatformAuth
**** Policy OR (0, PhSecretSHA256)
**** PH HierarchyChangeAuth
**************************************************
**** Successfully set PlatformAuth to EMPTY ********
**************************************************
```

- **FS0:\> Tpm2TxtProv.nsh SHA256 EXAMPLE**

```
FS0:\TPM2ProvfilesCBnT\> Tpm2TxtProv.nsh SHA256 EXAMPLE
FS0:\TPM2ProvfilesCBnT\> echo -OFF
****** Provisioning NV Indexes ******
If PlatformAuth is not EMPTY, then first run ResetPlatformAuth.nsh SHA256 EXAMPLE
**** Start PW Session for PlatformAuth & Index Read Auth
************ Provisioning PS Index ********************
**** Checking if PS Index exists
PS Index does not exist
***** Creating PS Index *****
**** NV_DefineSpace for PS Index
***** Writing PS *****
**** Start Policy Session
**** Policy Branch 2
**** Writing NV Data
**** Checking AUX Index
**** Checking if AUX index exists
Aux Index does not exist
******** Creating Aux Index ********
**** AUX NV_DefineSpace
**************************************************
******* Provisioning Completed Successfully *******
**************************************************
FS0:\TPM2ProvfilesCBnT\> _
```

**Note:** If other boot media is connected on the platform, it may require fs1, fs2, fs3 etc. instead in order to enter the USB Flash Drive.
**Note:** The provision status must be undefined, otherwise running ResetPlatformAuth.nsh SHA256 EXAMPLE command will fail.

Reboot the server, launch the EFI shell, execute the following commands to check the TPM information logs:

- **fs0:**
- **FS0:\> cd "Server Security Toolkit VerX.XX" \"CBnTToolkit"**
- **FS0:\> TxtBtgInfo.efi -c TPM > "File Name".log**

Review the logs generated and verify the TPM Index information.

```
TPM 2.0 Index Information

************Reading NV Index PS LCP Definition**************
NvIndex:           0x01C10103
  NameAlg:           0x000B
  Attributes:        0x62040408
    0-PPWrite 0          1-OwnerWrite 0
    2-AuthWrite 0        3-PolicyWrite 1
    4-Counter 0          5-Bits  0
    6-Extend 0           7-reserved      0
    8-reserved 0         9-reserved      0
    10-PolicyDelete 1    11-WriteLocked 0
    12-WriteAll 0        13-WriteDefine 0
    14-WriteStClear 0    15-GlobalLock   0
    16-PPRead 0          17-OwnerRead 0
    18-AuthRead 1         19-PolicyRead  0
    20-reserved 0         21-reserved    0
    22-reserved 0         23-reserved    0
    24-reserved 0         25-NoDA 1
    26-Orderly 0                 27-ClearStClear 0
    28-ReadLocked        0      29-Written 1
    30-PlatformCreate    1  31-ReadStClear 0
  AuthPolicy Size:  0x0020
  AuthPolicy Digest:
9F 97 0E 88 34 0B 83 6B 76 8E 68 2D B1 BE 76 EC
3F 42 84 28 2F DD F6 4B 05 AC F8 FD 26 99 A7 1C
```

```
************Reading NV Index Aux Definition***************
NvIndex:           0x01C10102
  NameAlg:           0x000B
  Attributes:        0x42044408
    0-PPWrite 0          1-OwnerWrite 0
    2-AuthWrite 0        3-PolicyWrite 1
    4-Counter 0          5-Bits  0
    6-Extend 0           7-reserved      0
    8-reserved 0         9-reserved      0
    10-PolicyDelete 1    11-WriteLocked 0
    12-WriteAll 0        13-WriteDefine 0
    14-WriteStClear 1    15-GlobalLock   0
    16-PPRead 0          17-OwnerRead 0
    18-AuthRead 1         19-PolicyRead  0
    20-reserved 0         21-reserved    0
    22-reserved 0         23-reserved    0
    24-reserved 0         25-NoDA 1
    26-Orderly 0                 27-ClearStClear 0
    28-ReadLocked        0      29-Written 0
    30-PlatformCreate    1  31-ReadStClear 0
  AuthPolicy Size:  0x0020
  AuthPolicy Digest:
EF 9A 26 FC 22 D1 AE 8C EC FF 59 E9 48 1A C1 EC
53 3D BE 22 8B EC 6D 17 93 0F 4C B2 CC 5B 97 24
```

**Note:** If PS and AUX Index in the logs are defined the TPM has been provisioned

## 1.4 Activating Intel® TXT

Once you have verified both the technical specification criteria and the CPU model, proceed to the BIOS **Processor Configuration** menu to enable Intel® TXT and Intel® Virtualization Technology.

**Important Note:** An Intel® Xeon family processor containing Intel® TXT is required in order to activate Intel® TXT features.

The **Processor Configuration** menu is accessible via the following pathway:

**Main --> Advanced --> Processor Configuration**

In the **Processor Configuration** menu, set the following option to **Enabled:**

- Intel® Virtualization

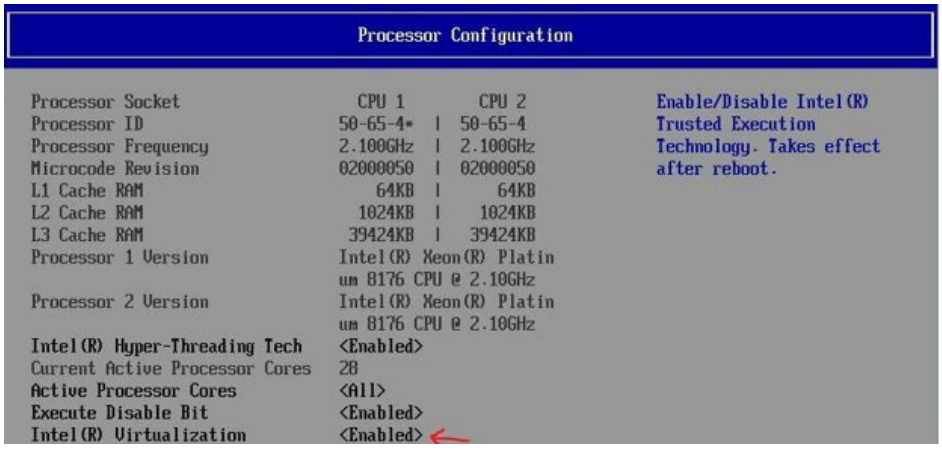


**Figure 6. Processor Configuration menu**

Once Intel® Virtualization is enabled navigate to the **Integrated IO Configuration** menu, which can be accessed via the following pathway:

**Main --> Advanced --> Integrated IO Configuration**

Set the following option to **Enabled**

- Intel® VT for Directed I/O

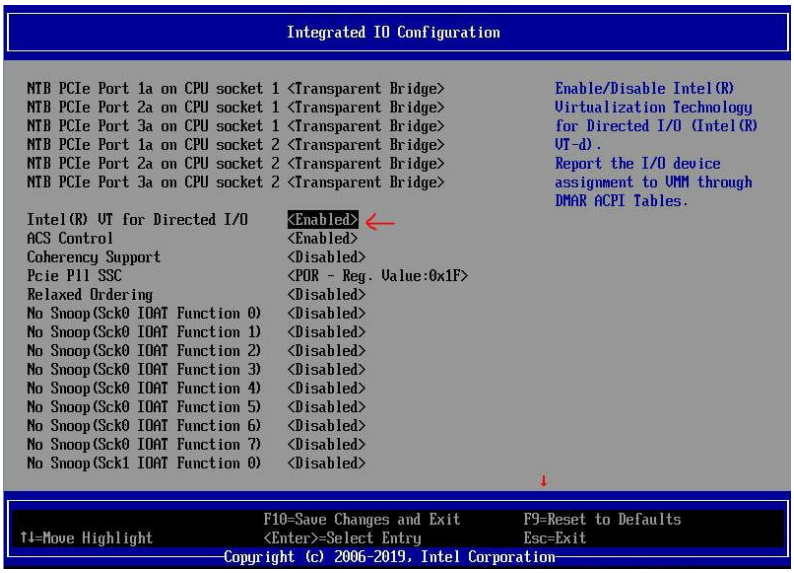


**Figure 7. Integrated IO Configuration menu**

Once both options are enabled, navigate back to the **Processor Configuration** menu, which can be accessed via the following pathway:

**Main --> Advanced --> Processor Configuration**

Set the following option to **Enabled**

- Intel® TXT

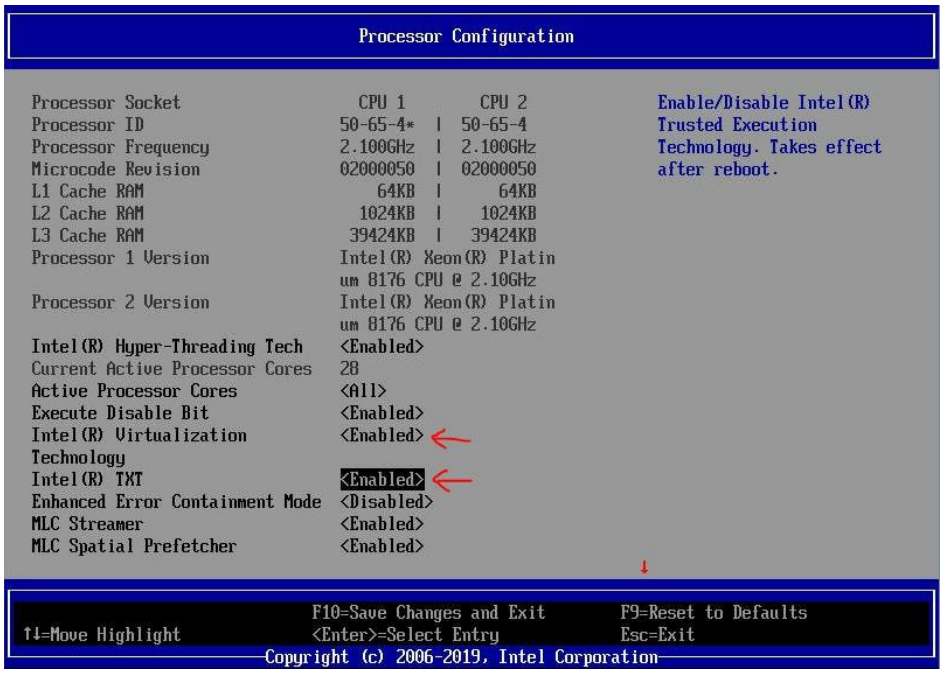


**Figure 8. Processor Configuration menu**

Press F10, save and reboot.

# *Appendix A. Glossary*

| Term | Definition |
|---|---|
| **BIOS** | Basic Input/Output System |
| **CPU** | Central Processing Unit |
| **EFI** | Extensible Firmware Interface |
| **PCR** | Platform Configuration Register |
| **SHA** | Secure Hash Algorithms |
| **TPM** | Trusted Platform Module |
| **Intel® TXT** | Intel® Trusted Execution Technology |
| **USB** | Universal Serial Bus |
| **VT** | Virtualized Technology |

# *Appendix B. Reference Documents*

- *Intel® Server System R2000WF Product Family. Technical Product Specification*
- *Intel® Server System R2000BP Product Family. Technical Product Specification*
- *Intel® Server System R2000ST Product Family. Technical Product Specification*
- *Client Content Library*
- *Enabling Intel® Trusted Execution Technology (Intel® TXT) on Purley Platforms*
- *One-Stop Intel® TXT Activation Guide*