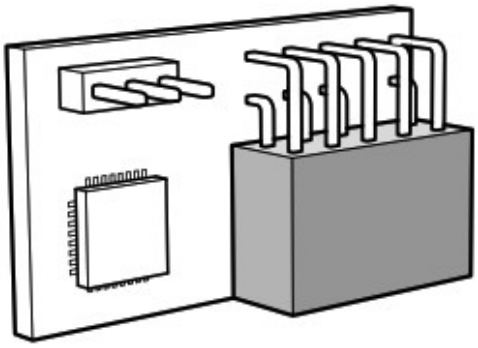
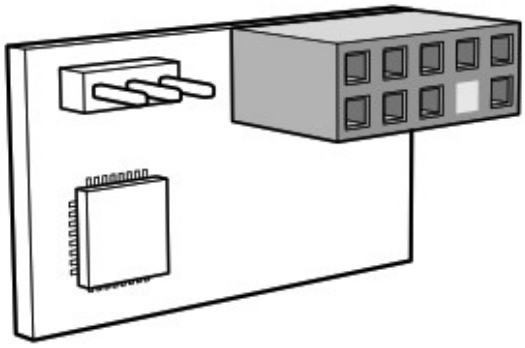
SUPERMICR AOM-TPM-9670V Trust Platform Module Vertical User Manual

TPM
AOM-TPM-9670V
AOM-TPM-9670H
AOM-TPM-9670V(H)-S





USER'S MANUAL
1.2

The information in this user's guide has been carefully reviewed and is believed to be accurate. The vendor assumes no responsibility for any inaccuracies that may be contained in this document and makes no commitment to update or to keep current the information in this manual, or to notify any person or organization of the updates. **Please Note: For the most up-to-date version of this manual, please see our website at www.supermicro.com**.

Super Micro Computer, Inc. (“Supermicro”) reserves the right to make changes to the product described in this manual at any time and without notice. This product, including software and documentation, is the property of Supermicro and/or its licensors, and is supplied only under a license. Any use or reproduction of this product is not allowed, except as expressly permitted by the terms of said license.
IN NO EVENT WILL SUPER MICRO COMPUTER, INC. BE LIABLE FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, SPECULATIVE OR CONSEQUENTIAL DAMAGES ARISING FROM THE USE OR INABILITY TO USE THIS PRODUCT OR DOCUMENTATION, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN PARTICULAR, SUPER MICRO COMPUTER, INC. SHALL NOT HAVE LIABILITY FOR ANY HARDWARE, SOFTWARE, OR DATA STORED OR USED WITH THE PRODUCT, INCLUDING THE COSTS OF REPAIRING, REPLACING, INTEGRATING, INSTALLING OR RECOVERING SUCH HARDWARE, SOFTWARE, OR DATA.
Any disputes arising between manufacturer and customer shall be governed by the laws of Santa Clara County in the State of California, USA. The State of California, County of Santa Clara shall be the exclusive venue for the resolution of any such disputes. Supermicro’s total liability for all claims will not exceed the price paid for the hardware product.
FCC Statement: Refer to Supermicro’s website for FCC Compliance Information.
California Best Management Practices Regulations for Perchlorate Materials: This Perchlorate warning applies only to products containing CR (Manganese Dioxide) Lithium coin cells. “Perchlorate Material-special handling may apply. See **www.dtsc.ca.gov/hazardouswaste/perchlorate**“.


WARNING: This product can expose you to chemicals including! lead, known to the State of California to cause cancer and birth defects or other reproductive harm. For more information, go to **www.P65Warnings.ca.gov**.

Manual Revision 1.2
Release Date: May 12, 2021,

Printed in the United States of America

Preface

About This User’s Guide

This user’s guide is written for system integrators, IT professionals, and knowledgeable end users who wish to add additional data security levels to their systems to protect highly sensitive applications. It provides detailed information on configuring, provisioning, and using the trusted platform module (TPM).

User’s Guide Organization

Chapter 1 provides an overview of the trusted platform module (TPM), including its features and uses.
Chapter 2 provides detailed instructions on installing, provisioning, and using the TPM.

Conventions Used in This User’s Guide

Pay special attention to the following symbols for proper TPM configuration.


Warning: Important information given to avoid TPM configuration errors.


Note: Additional information given to ensure correct TPM configuration setup.

Contents

Chapter 1: Introduction

Overview of the Trusted Platform Module (TPM)

The Trusted Platform Module (TPM9670) is a special add-on module that may be installed onto Supermicro X11 Dual Processor boards, and single Processor boards with socket 3647 only.

A. Types of TPMs

Note: TPM module must be provisioned in order to use Intel® TXT. Please contact Supermicro Technical Support to get more details about the Intel tool.
The TPM-9670 series uses TCG (Trusted Computing Group) version 2.0 firmware. The following SKUs are available:

- AOM-TPM-9670V, a vertical TPM module
- AOM-TPM-9670H, a horizontal TPM module

Horizontal vs. Vertical: Generally, whether you should use a TPM with a horizontal or vertical form factor depends on the physical space available. Horizontal TPMs are used in 1U chassis. Vertical TPMs are used in 2U or taller chassis heights; they are also designed with a smaller footprint to occupy less space on the motherboard.
Server vs. Client: To use the TXT function, each TPM has been provisioned as a server model or client model. Be sure to use the appropriate TPM for your needs. The server TPM is designed to run with Intel socket P (LGA 3647). The client TPM is designed to run on Intel with socket P (LGA 3647) as well.

Supermicro TPM Features

1. TCG 2.0 compliance
2. SPI interface
3. Microcontroller in 0.22/0.09-µm CMOS technology
4. Compliant embedded software
5. EEPROM for TCG firmware enhancements and for user data and keys
6. Hardware accelerator for SHA-1 and SHA-256 hash algorithm
7. True Random Number Generator (TRNG)
8. Tick counter with tamper detection
9. Protection against dictionary attack

10. Infineon's TPM 2.0 is Common Criteria certified at Evaluation Assurance Level (EAL) 4 Moderate
11. General-purpose I/O
12. Intel® Trusted Execution Technology (TXT) support
13. AMD® Secure Virtual Machine Architecture support
14. Full personalization with Endorsement Key (EK) and EK certificate
15. Power-saving sleep mode
16. 3.3V power supply
17. WHQL dual-mode 1.1b + 1.2 TPM Windows Kernel Mode Driver

Motherboards Supported for TPM

Please refer to the Supermicro website (**http://www.supermicro.com/**) for a complete and most up-to-date list of the motherboards that can support the TPM. As a general rule, these are most X9 motherboards, all X10 motherboards, and some AMD motherboards. Such motherboards will have a specially designated JTPM1 connector, which will be listed in the respective motherboard's manual.

Intel® TXT

The Intel TXT is a software tool that may be used in conjunction with the TPM to provide additional security for pre-launch firmware of clusters and clouds, including the BIOS, IPMI, SAS firmware, CMM firmware, and more. It is optional, but the TPM is required for it to be provisioned. It further increases system security by protecting firmware against malicious attacks to vulnerable areas.
It works by matching hypervisor measures with encryption keys upon system launch. If the hypervisor does not match the keys, then the hypervisor will be prevented from starting up.
To use the TXT, you need to enable TXT support after provisioning the TPM.

Note: TXT is only supported on Intel platforms that support TPM use.

A. How the TXT Works
The Intel TXT, when enabled, follows a step-by-step process to ensure security of pre-launch components.

1. Measures the hypervisor launch upon system startup
2. Checks for a match
3. If matched: The TXT signals "trusted," and the launch is allowed to proceed.
4. If mismatched: The TXT signals "untrusted," and the launch is blocked.

An Important Note to the User

The graphics shown in this user's guide were based on the latest information available at the time of publishing of this guide. The TPM screens shown on your computer may or may not look exactly like the screen shown in this user's guide.

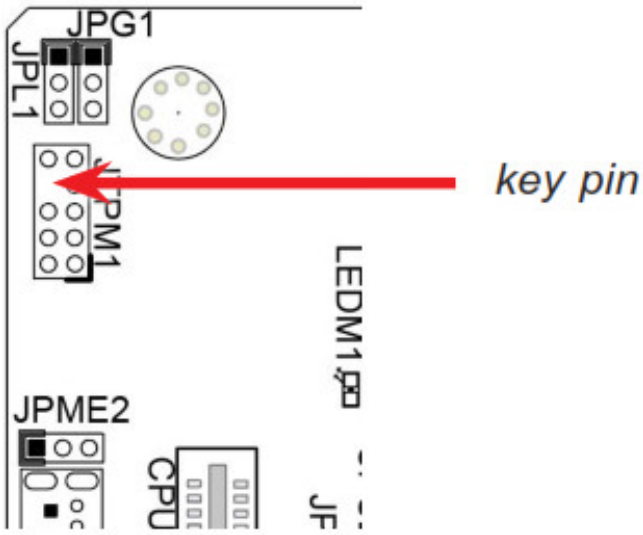
Chapter 2 Deploying and Using the TPM

Follow the instructions below to begin using the TPM.

Installing the TPM Onto the Motherboard

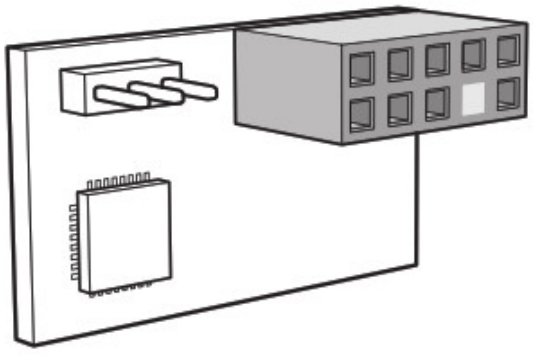
To install the Trusted Platform Module onto your motherboard, follow the steps below.

1. Find the 9-pin male JTPM1 connector on the motherboard. If you need help locating this connector, consult your motherboard manual. If the board does not have this feature, then it does not support the TPM.
2. Using the key pin as a reference, orient and align your TPM with the connector.

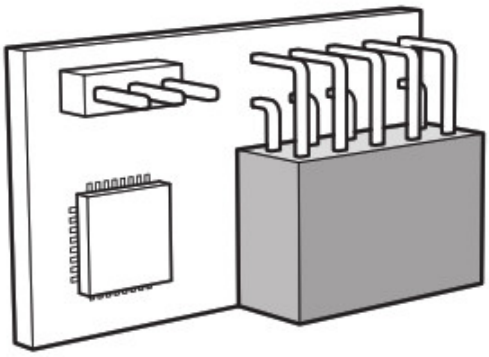


3. Carefully insert the TPM into the connector on the motherboard, taking care not to damage the pins.

Note: The orientation of the TPM to be installed depends on whether it has a horizontal or vertical form factor. The vertical TPM is intended to “stand” perpendicular to the motherboard, while the horizontal TPM lies flat (parallel) on the motherboard. See the below two images for the correct orientation.



Horizontal TPM



Vertical TPM

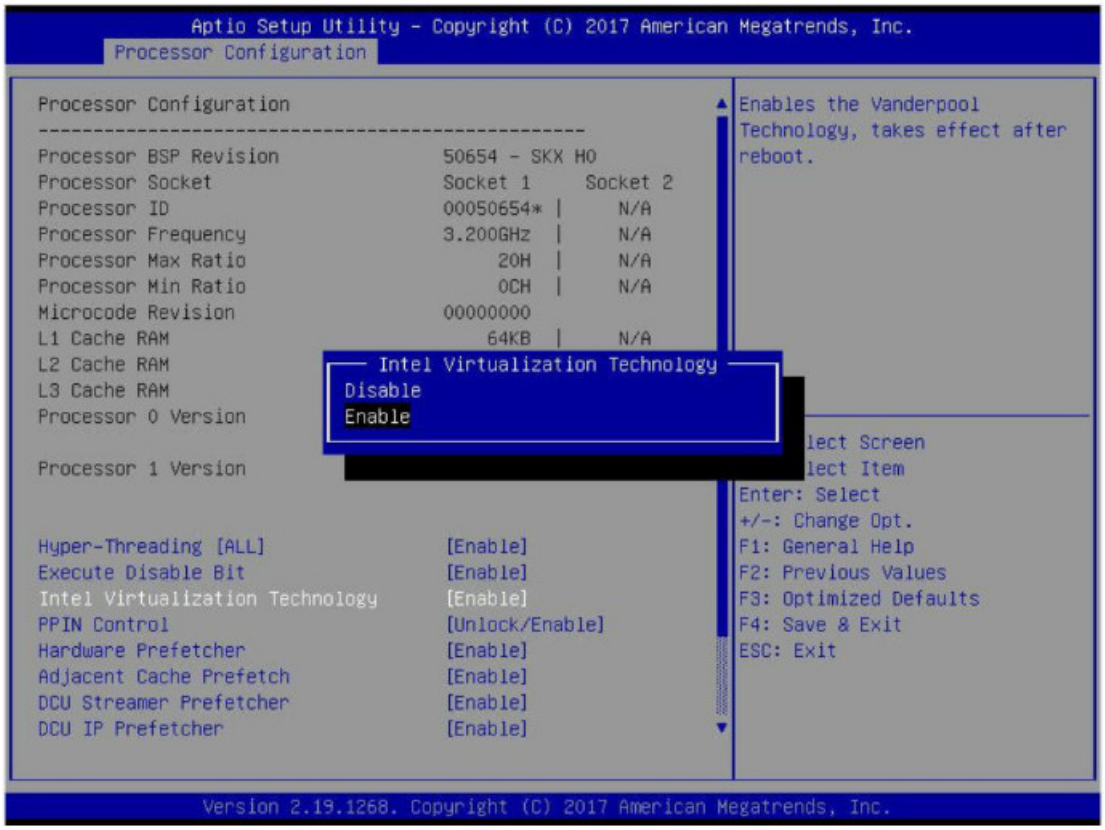
Enabling the TPM via the BIOS and Intel® Provision Utility

There are two components to the process of enabling the TPM. After you have installed the TPM onto the motherboard, you must first “verify” the TPM for the motherboard; this is done through the BIOS. (Also in the BIOS, you should enable TXT support.) After that, you then “lock” the TPM in the firmware. This is done through the provision utility provided by Intel.

A. Enabling the TPM in the BIOS

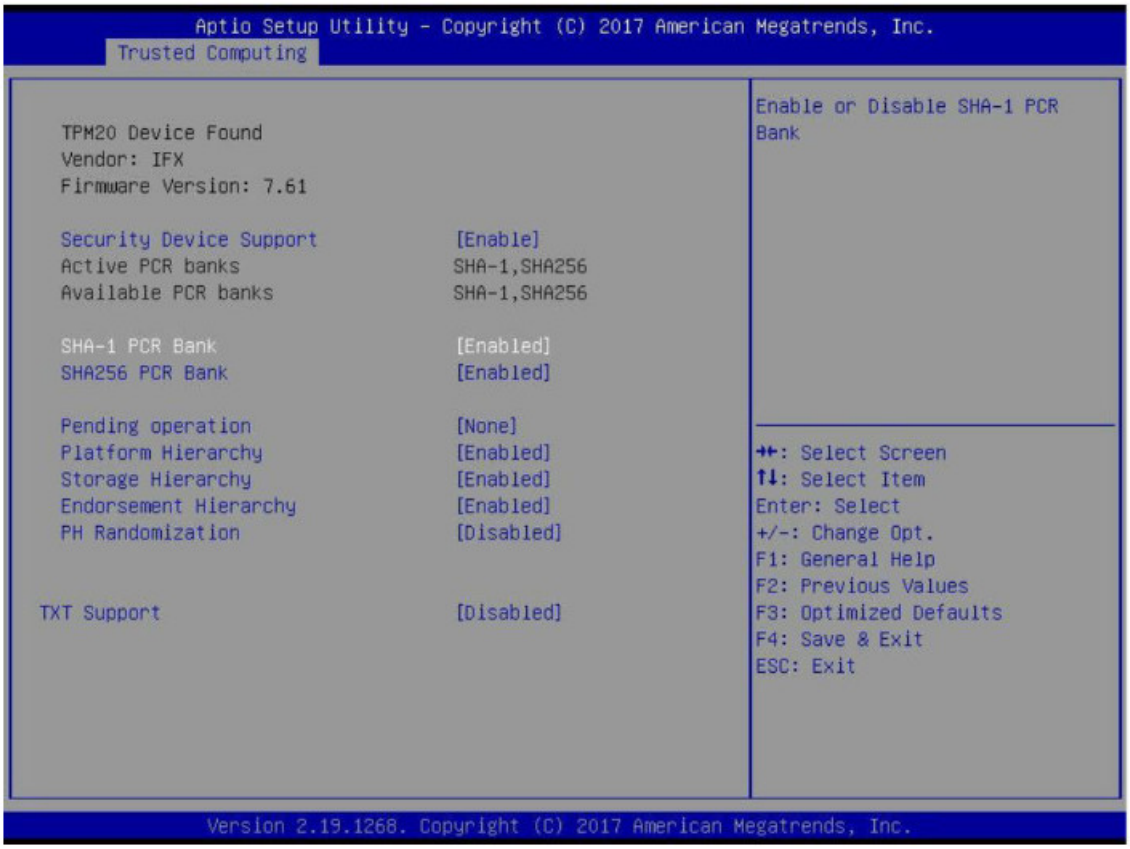
1. Enter the BIOS setup screen. You may do this either from the IPMI remote console or from the server directly using KVM. Reboot the system, and press the **<Del>** key as the system boots until you reach the BIOS screen.

2. You will be presented with the BIOS Setup main screen. Using your arrow keys, navigate to the “Advanced” tab. From there, navigate down and select the “CPU Configuration” option. Press **<Enter>**.
3. You will then be taken to the CPU Configuration page. Using your arrow keys, navigate down to the **“Intel Virtualization Technology”** option, as shown below, and press **<Enter>**. If this item is not already enabled, select **Enable** and press **<Enter>.**

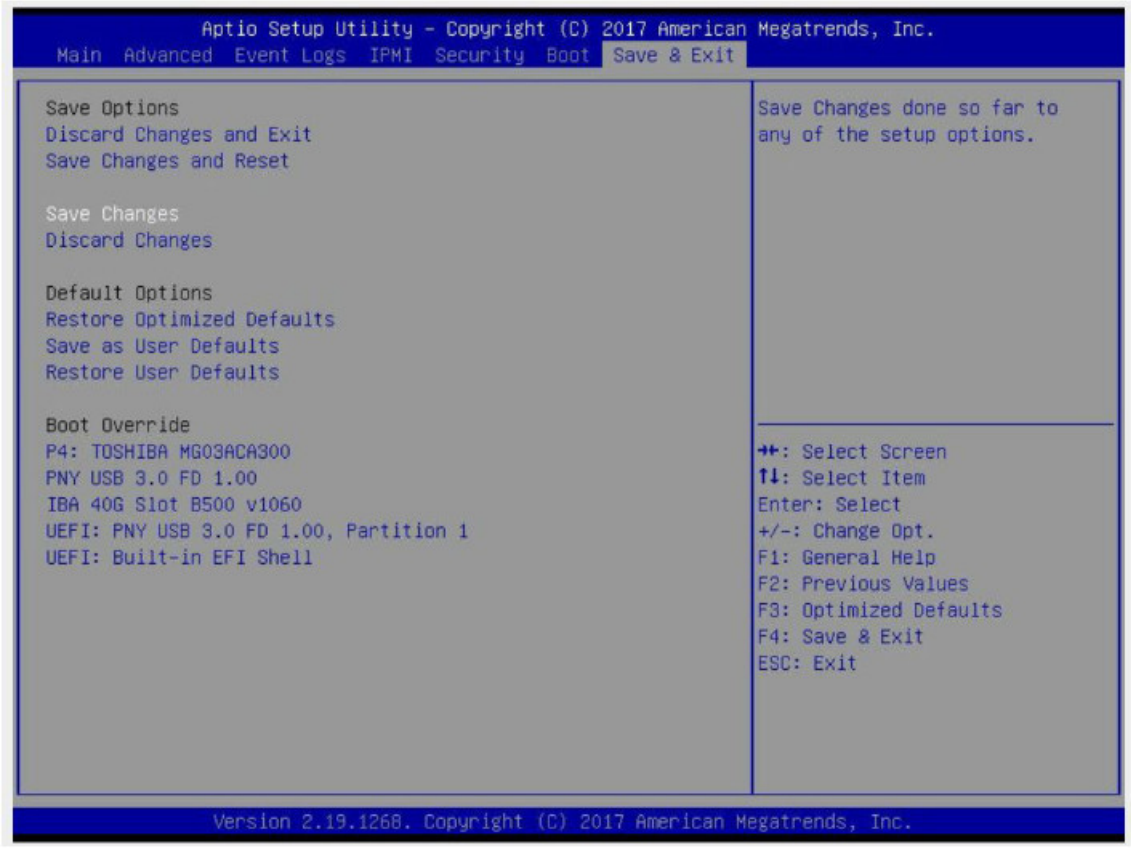


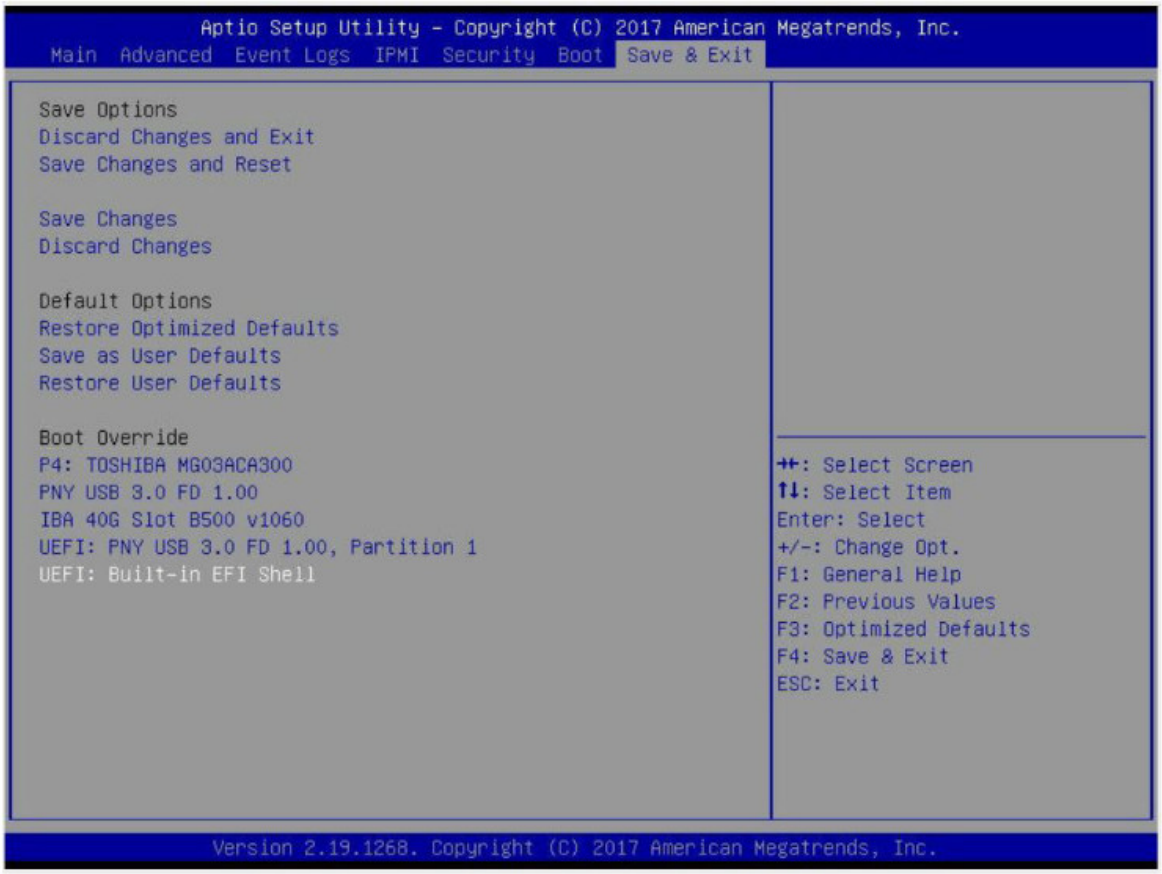
4. Once you have enabled virtualization support, press your **<Esc>** key until you are back to the “Advanced” tab. Navigate down to the “Trusted Computing” option and press **<Enter>.**
5. The Trusted Computing window will appear.

Note: “SHA-1 PCR Bank” and **“SHA-256 PCR Bank”** are Enabled.



6. Disable **"PH Randomization"** and **"TXT** Support" only. Using the arrow keys, select each option, press the **<Enter>** key to select Disabled, and press the **<Enter>** key again.
7. Press the **<Esc>** key to bring you back to the "Advanced" tab options. Use the arrow keys to toggle to the **"Save & Exit"** tab.
8. Use the arrow keys to select **"Save Changes".** Press the **<Enter>** key.
9. Use the arrow keys to select **"UEFI: Built-in EFI Shell"** and press the En- **ter>** key.





B. Provisioning Intel TXT (Server)

Note: If the TPM part number is AOM-TPM-9670V-S or AOM-TPM-9670HS, you do not need to get the Intel® Provisioning tool. Please go ahead and enable Intel TXT feature in the BIOS.

1. Next, you will need to provision Intel TXT in the UEFI shell. Once you have selected “UEFI: Built-in EFI Shell” in the BIOS, the system will boot into the Unified Extensible Firmware Interface (UEFI) with a list of available USB devices.
2. Each USB device has its own code. Type the code for the USB device that you want to use into the command line at the bottom of the screen, then press the <Enter> key.

   Note: The device used for the purposes of this user guide had a code of fs0. Replace this code with the code that corresponds to your device.
3. In the command line at the bottom of the screen, follow these steps below after typing “FS0:” 1. Go to directory “TPM2ProvTool” 2. Type the command “TPM2TxtProv.nsh sha 256 default”. The Provisioning process is now completed.

```
FS0:\TPM2ProvTool\TPM2 Prov Tool\> Tpm2TxtProv.nsh sha256 Default
FS0:\TPM2ProvTool\TPM2 Prov Tool\> echo -OFF
****** Provisioning NV Indexes *****
If PlatformAuth is not EMPTY, then first run ResetPlatformAuth.nsh sha256 Default
**** Start PW Session for PlatformAuth & Index Read Auth
********** Provisioning PS Index **********
**** Checking if PS Index exists
**** Comparing attributes against definition
**** Verifying if Data is correct
**** Checking AUX Index
**** Checking if AUX index exists
**** AUX already exists, check if provisioned correctly
Aux Index provisioned correctly
**************************************************
******* Provisioning Completed Successfully *******
**************************************************
FS0:\TPM2ProvTool\TPM2 Prov Tool\>
```

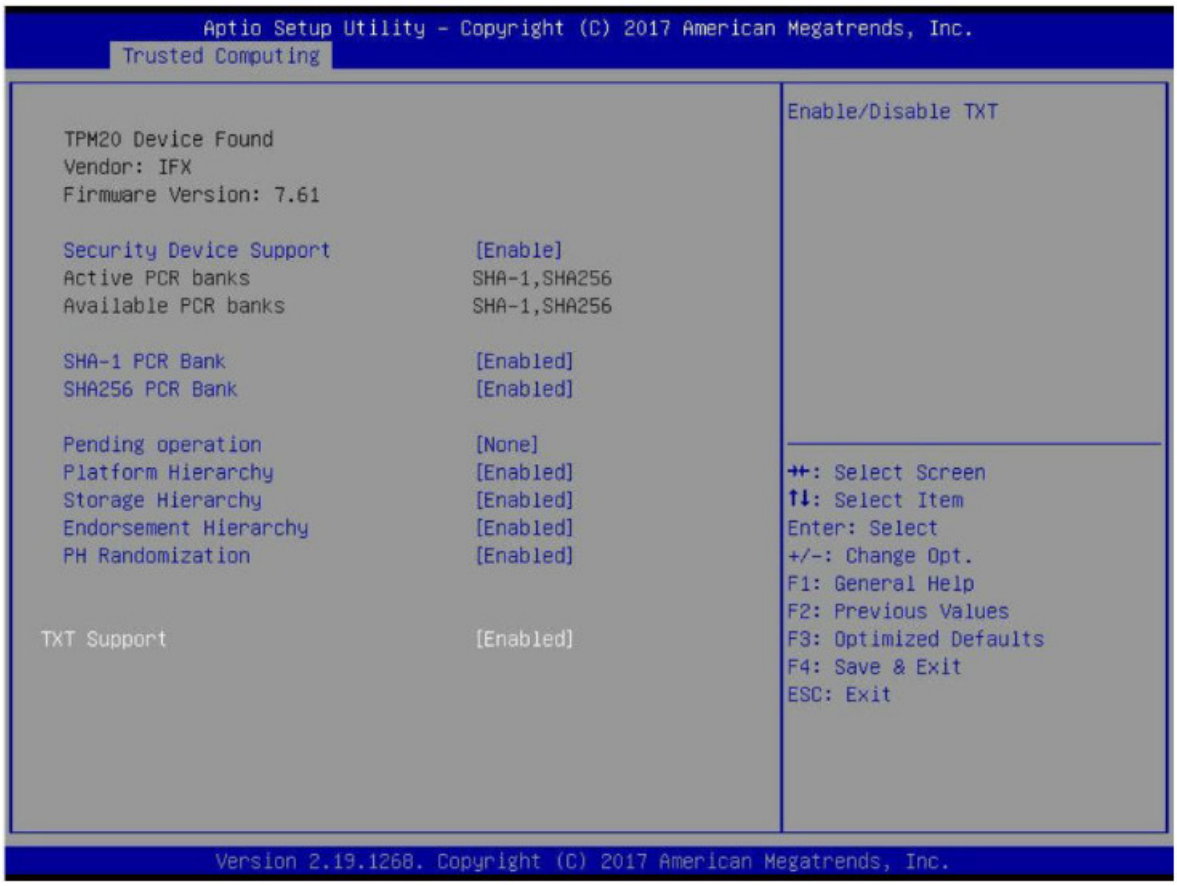
4. After the provisioning process has completed, you will need to go back into the BIOS and enable TXT Support. To do this, type **"exit"** in the command line at the bottom of the screen and press the **<Enter>** key.

```
FS0:\TPM2ProvTool\TPM2 Prov Tool\> Tpm2TxtProv.nsh sha256 Default
FS0:\TPM2ProvTool\TPM2 Prov Tool\> echo -OFF
****** Provisioning NV Indexes *****
If PlatformAuth is not EMPTY, then first run ResetPlatformAuth.nsh sha256 Default
**** Start PW Session for PlatformAuth & Index Read Auth
********** Provisioning PS Index **********
**** Checking if PS Index exists
**** Comparing attributes against definition
**** Verifying if Data is correct
**** Checking AUX Index
**** Checking if AUX index exists
**** AUX already exists, check if provisioned correctly
Aux Index provisioned correctly
**************************************************
******* Provisioning Completed Successfully *******
**************************************************
FS0:\TPM2ProvTool\TPM2 Prov Tool\> exit_
```

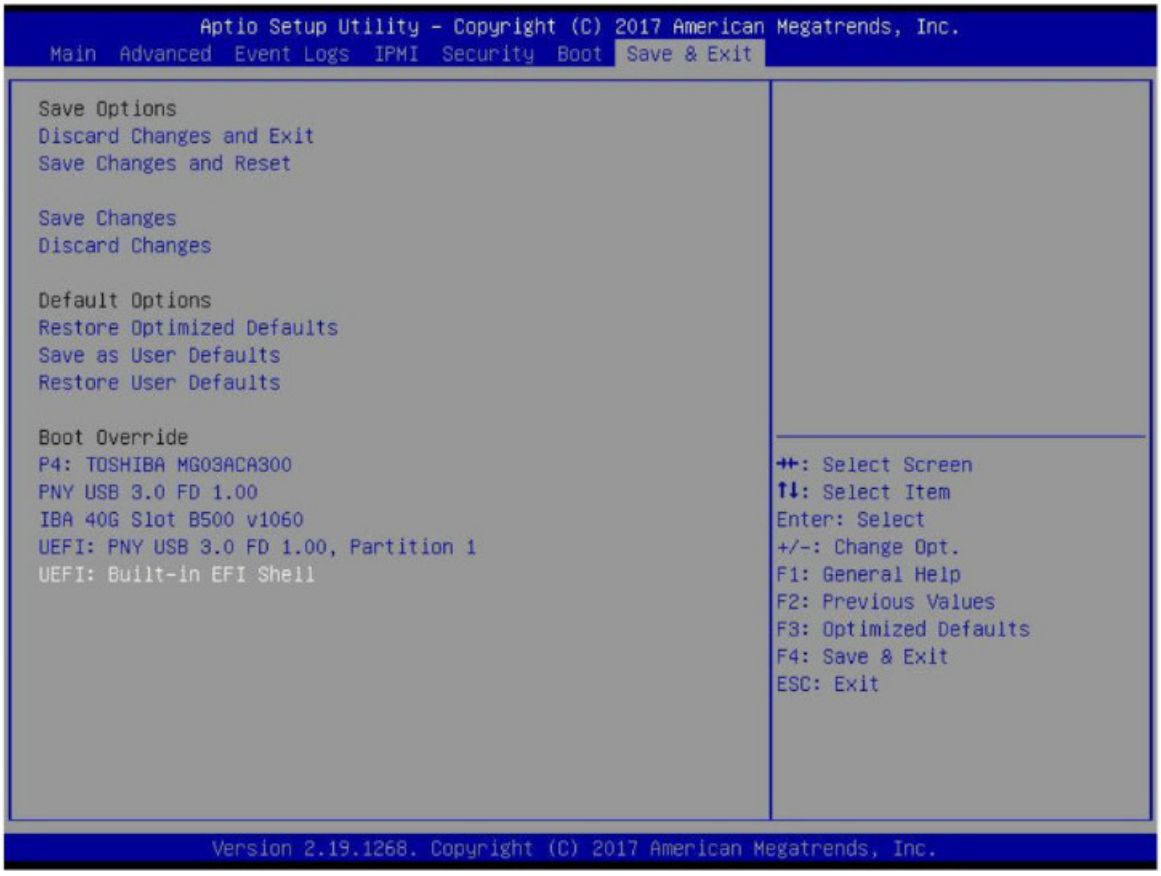
C. Enabling TXT Support

The last step is enabling TXT Support in the BIOS and UEFI shell.

1. Go back to the "Advanced" tab in the BIOS and enable Platform Hierarchy, Storage Hierarchy, Endorsement Hierarchy, PH Randomization, and TXT Support.



2. Go back to the “Save & Exit” tab and select “UEFI: Built-in EFI Shell” in the BIOS.



3. After enabling TXT Support in the BIOS, you will need to run TXT in the UEFI shell. In the command line at the bottom of the page, type **“getsec64. ef1 -l sen -a”** and press the<Enter> key. TXT support is now enabled..

```
 01/16/12  02:21a               1,712  Instructions.txt
 11/26/13  12:56a              21,468  sinit_error.txt
 04/01/14  01:14a              15,986  ver.txt
 05/23/11  06:10p             139,961  Bootable EFI disk Instructions.pdf
 01/16/12  02:33a             298,362  TTK-64.pdf
 03/11/14  01:02a              72,896  getsec64.efi
 06/05/12  11:29p              38,336  ServerSecrets.efi
 01/16/14  11:33p             295,584  ServerTXTINFO.efi
        14 File(s)   1,107,949 bytes
         3 Dir(s)


fs5:\Grantley_Refresh\TXT> getsec64.efi -l sen -a
**************************************************
GETSEC64 v1.3.4
Built: Mar 10 2014 13:11:58
Intel Corporation
Copyright (c) 2010-2014
**************************************************
GETSEC[SENTER] complete. System is now in TXT Environment.
```

4. To exit from the TXT environment, type **"getsec64.efi -l sexit"** in the command line at the bottom of the screen and press the **<Enter>** key.

```
06/08/2015  15:13 <DIR>        16,384  Source
09/21/2017  02:09 <DIR>        32,768  TPM2 Prov Tool
          0 File(s)          0 bytes
          5 Dir(s)
FS0:\TPM2ProvTool\> cd "TPM2 Prov Tool"
FS0:\TPM2ProvTool\TPM2 Prov Tool\> getsec64.efi -l sen -a
DEBUG: cmd_line_parse
**************************************************
GETSEC64 v1.3.15
Built: Nov 10 2015 09:53:18
Intel Corporation
Copyright (c) 2010-2015
**************************************************
DEBUG: Load ACM to TXT_SINIT.BASE
DEBUG: IsSecureEnvironment
DEBUG: do_getsec
BEBUG: RlpCnt 15
BEBUG: rlps_joined
GETSEC[SENTER] complete. System is now in TXT Environment.
FS0:\TPM2ProvTool\TPM2 Prov Tool\> getsec64.efi -l sexit
DEBUG: cmd_line_parse
**************************************************
GETSEC64 v1.3.15
Built: Nov 10 2015 09:53:18
Intel Corporation
Copyright (c) 2010-2015
**************************************************
DEBUG: Load ACM to TXT_SINIT.BASE
DEBUG: do_getsec
GETSEC[SEXIT] complete. System has exited TXT Environment.
FS0:\TPM2ProvTool\TPM2 Prov Tool\> _
```

(Disclaimer Continued)

The products sold by Supermicro are not intended for and will not be used in life support systems, medical equipment, nuclear facilities or systems, aircraft, aircraft devices, aircraft/emergency communication devices or other critical systems whose failure to perform be reasonably expected to result in significant injury or loss of life or catastrophic property damage. Accordingly, Supermicro disclaims any and all liability, and should buyer use or sell such products for use in such ultra-hazardous applications, it does so entirely at its own risk. Furthermore, buyer agrees to fully indemnify, defend and hold Supermicro harmless for and against any and all claims, demands, actions, litigation, and proceedings of any kind arising out of or related to such ultra-hazardous use or sale.

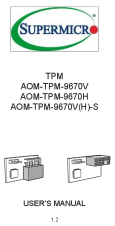
Contacting Supermicro

Headquarters
Address: Super Micro Computer, Inc. 980 Rock Ave. San Jose, CA 95131 U.S.A.
Tel: +1 (408) 503-8000
Fax: +1 (408) 503-8008
Email: marketing@supermicro.com (General Information) support@supermicro.com (Technical Support)
Website: www.supermicro.com

Europe
Address: Super Micro Computer B.V. Het Sterrenbeeld 28, 5215 ML ‘s-Hertogenbosch, The Netherlands
Tel: +31 (0) 73-6400390
Fax: +31 (0) 73-6416525
Email: sales@supermicro.nl (General Information) support@supermicro.nl (Technical Support)
rma@supermicro.nl (Customer Support)
Website: www.supermicro.nl

Asia-Pacific
Address: Super Micro Computer, Inc. 3F, No. 150, Jian 1st Rd. Zhonghe Dist., New Taipei City 235 Taiwan (R.O.C)
Tel: +886-(2) 8226-3990
Fax: +886-(2) 8226-3992
Email: support@supermicro.com.tw
Website: www.supermicro.com.tw

Documents / Resources

	SUPERMICR AOM-TPM-9670V Trust Platform Module Vertical [pdf] User Manual AOM-TPM-9670V, AOM-TPM-9670H, AOM-TPM-9670V H -S, Trust Platform Module Vertical