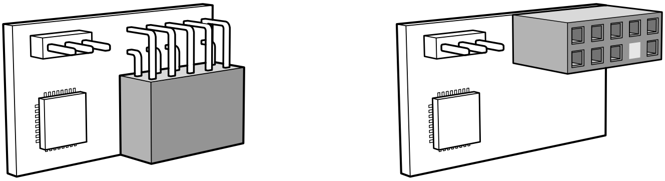
TPM
AOM-TPM-9670V
AOM-TPM-9670H
AOM-TPM-9670V-S-FIPS



USER'S MANUAL

Revision 1.0

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 web site 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 1.0

Release Date: July 19, 2022

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 mechanisms to their systems to protect highly sensitive applications. It provides detailed information on configuring, provisioning, and using the Trusted Platform Module (TPM) for X12 and H12 motherboards.

User's Guide Organization

Chapter 1 provides an overview of the 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 is given to avoid TPM configuration errors.

✏ **Note:** Additional information is given to ensure the correct and proper TPM configuration setup.

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)
Sales-USA@supermicro.com (Sales Inquiries)
Government_Sales-USA@supermicro.com (Gov. Sales Inquiries)
support@supermicro.com (Technical Support)
RMA@supermicro.com (RMA Support)
Webmaster@supermicro.com (Webmaster)

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_Europe@supermicro.com (Sales Inquiries)
Support_Europe@supermicro (Technical Support)
RMA_Europe@supermicro (RMA 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

Asia-Pacific

Email:	Sales-Asia@supermicro.com.tw (Sales Inquiries)
	Support@supermicro.com.tw (Technical Support)
	RMA@supermicro.com.tw (RMA Support)
Website:	www.supermicro.com.tw

Table of Contents

Chapter 1

Introduction

1.1 Overview of the Trusted Platform Module (TPM)

The Trusted Platform Module (TPM9670) is a special add-on module that may be installed onto Supermicro X12/H12 dual and single processor motherboards that support CPU Socket 3674 only.

Types of TPMs

Note: TPM modules must be provisioned in order to use Intel® Trusted Execution Technology (TXT). Please contact Supermicro Technical Support for more details about the Intel tool.

The TPM-9670 series add-on modules use 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 and 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. Both server TPM and client TPM are designed to support motherboards with Socket P (LGA3647) processors installed.

1.2 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 key support

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 (CC) 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

Note: On H12 motherboards, only H12SSG-AN6 and H12SSG-ANP6 support the SPI interface (10-pin header).

1.3 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. Such motherboards will have a specially designated JTPM1 connector, which will be listed in the respective motherboard's manual.

1.4 Intel® TXT

The Intel® Trusted Execution Technology (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 but not limited to the BIOS, IPMI, SAS firmware, and CMM firmware. It is optional, but the TPM is required for it to be provisioned. It further increases system security by protecting firmware against malicious attacks on vulnerable areas.

It works by matching hypervisor measures with encryption keys upon system launch. If the hypervisor does not match the keys, 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.

How the TXT Works

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

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

1.5 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 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

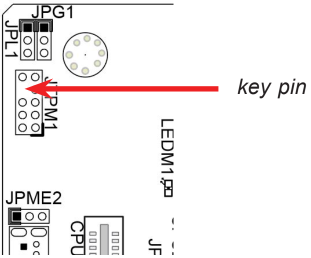
Follow the instructions below to begin using the TPM.

2.1 Installing the TPM Onto the Motherboard

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

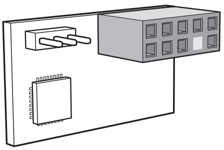
1. Find the 9-pin male JTPM1 connector on the motherboard. If you need help locating this connector, consult your motherboard manual. If the board does not have this feature, then it does not support the TPM.

2. Using the key pin as a reference, orient, and align your TPM with the connector.

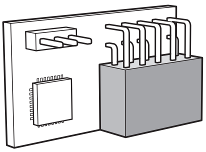


3. Carefully insert the TPM into the connector on the motherboard, making sure not to damage the pins.

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

2.2 Enabling the TPM via the BIOS and Intel® Provision Utility

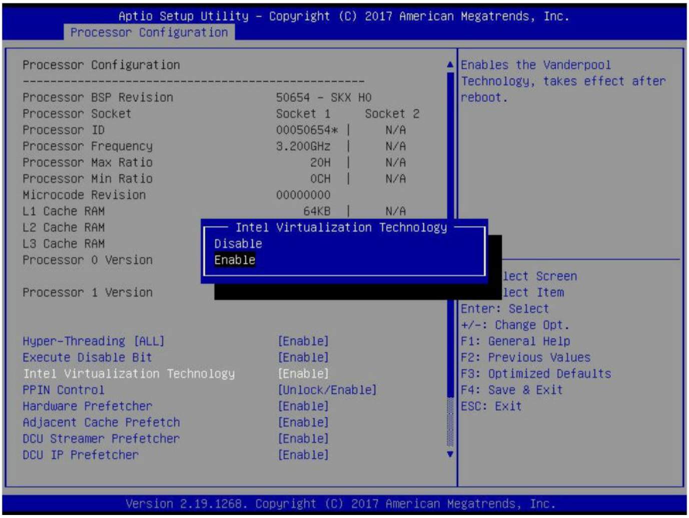
There are two components to the process of enabling the TPM. After you have installed the TPM onto the motherboard, you must first "verify" the TPM for the motherboard; this is done through the BIOS. (Also in the BIOS, you should enable TXT support.) After that, you then "lock" the TPM in the firmware. 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**>.

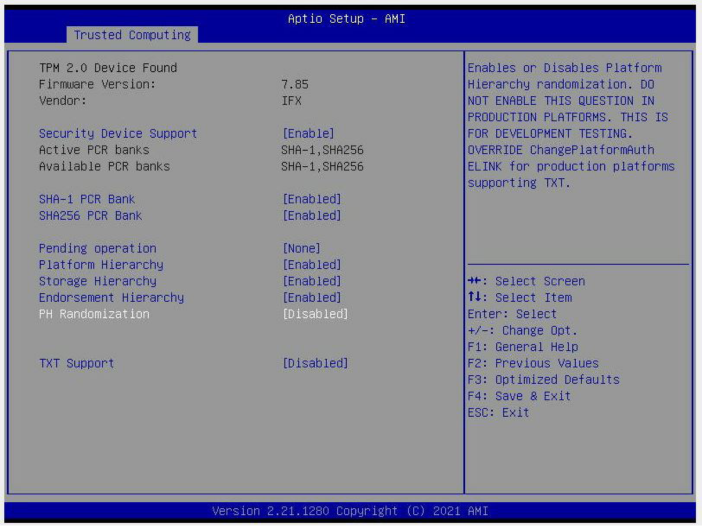


```
          Aptio Setup Utility - Copyright (C) 2017 American Megatrends, Inc.
     Processor Configuration

 Processor Configuration                                   Enables the Vanderpool
 --------------------------------------------------        Technology, takes effect after
 Processor BSP Revision              50654 - SKX H0        reboot.
 Processor Socket                    Socket 1     Socket 2
 Processor ID                        00050654* |     N/A
 Processor Frequency                 3.200GHz  |     N/A
 Processor Max Ratio                      20H  |     N/A
 Processor Min Ratio                      0CH  |     N/A
 Microcode Revision                  00000000
 L1 Cache RAM                            64KB  |     N/A
 L2 Cache RAM             ─ Intel Virtualization Technology ─
 L3 Cache RAM             Disable
 Processor 0 Version      Enable
                                                            lect Screen
 Processor 1 Version                                        lect Item
                                                           Enter: Select
                                                           +/-: Change Opt.
 Hyper-Threading [ALL]               [Enable]              F1: General Help
 Execute Disable Bit                 [Enable]              F2: Previous Values
 Intel Virtualization Technology     [Enable]              F3: Optimized Defaults
 PPIN Control                        [Unlock/Enable]       F4: Save & Exit
 Hardware Prefetcher                 [Enable]              ESC: Exit
 Adjacent Cache Prefetch             [Enable]
 DCU Streamer Prefetcher             [Enable]
 DCU IP Prefetcher                   [Enable]

            Version 2.19.1268. Copyright (C) 2017 American Megatrends, Inc.
```

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: By default, **"SHA-1 PCR Bank**" and "**SHA-256 PCR Bank**” are Enabled.



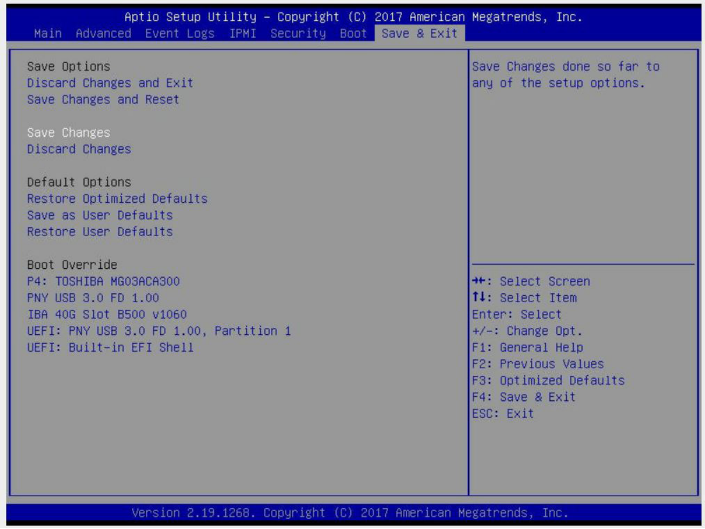
```
                              Aptio Setup - AMI
     Trusted Computing

    TPM 2.0 Device Found                                 Enables or Disables Platform
    Firmware Version:              7.85                  Hierarchy randomization. DO
    Vendor:                        IFX                   NOT ENABLE THIS QUESTION IN
                                                         PRODUCTION PLATFORMS. THIS IS
    Security Device Support        [Enable]              FOR DEVELOPMENT TESTING.
    Active PCR banks               SHA-1,SHA256          OVERRIDE ChangePlatformAuth
    Available PCR banks            SHA-1,SHA256          ELINK for production platforms
                                                         supporting TXT.
    SHA-1 PCR Bank                 [Enabled]
    SHA256 PCR Bank                [Enabled]

    Pending operation              [None]
    Platform Hierarchy             [Enabled]
    Storage Hierarchy              [Enabled]             →←: Select Screen
    Endorsement Hierarchy          [Enabled]             ↑↓: Select Item
    PH Randomization               [Disabled]            Enter: Select
                                                         +/-: Change Opt.
                                                         F1: General Help
    TXT Support                    [Disabled]            F2: Previous Values
                                                         F3: Optimized Defaults
                                                         F4: Save & Exit
                                                         ESC: Exit

                   Version 2.21.1280 Copyright (C) 2021 AMI
```

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.

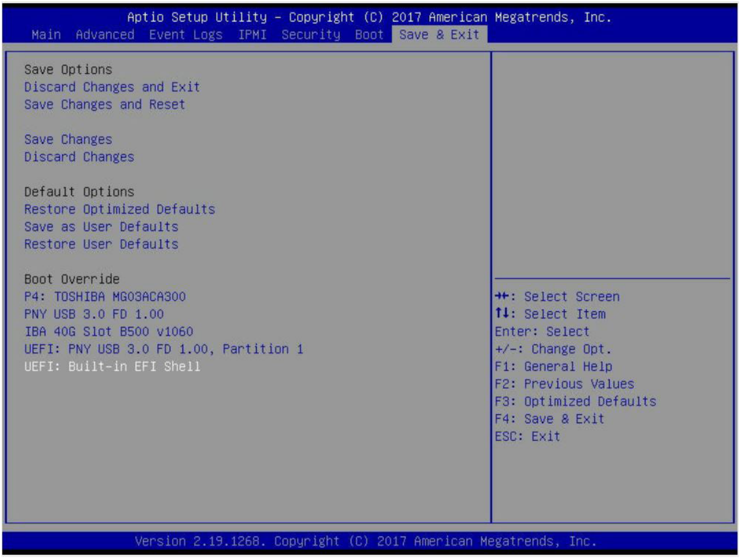
7. Press the <**Esc**> key to bring you back to the "**Advanced**" tab options. Use the arrow keys to toggle to the "**Save & Exit**" tab.

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 <**Enter**> key.



```
                Aptio Setup Utility - Copyright (C) 2017 American Megatrends, Inc.
     Main  Advanced  Event Logs  IPMI  Security  Boot  Save & Exit
  Save Options                                          Save Changes done so far to
  Discard Changes and Exit                              any of the setup options.
  Save Changes and Reset

  Save Changes
  Discard Changes

  Default Options
  Restore Optimized Defaults
  Save as User Defaults
  Restore User Defaults

  Boot Override
  P4: TOSHIBA MG03ACA300                                →←: Select Screen
  PNY USB 3.0 FD 1.00                                   ↑↓: Select Item
  IBA 40G Slot B500 v1060                               Enter: Select
  UEFI: PNY USB 3.0 FD 1.00, Partition 1                +/-: Change Opt.
  UEFI: Built-in EFI Shell                              F1: General Help
                                                        F2: Previous Values
                                                        F3: Optimized Defaults
                                                        F4: Save & Exit
                                                        ESC: Exit

                Version 2.19.1268. Copyright (C) 2017 American Megatrends, Inc.
```



```
                Aptio Setup Utility - Copyright (C) 2017 American Megatrends, Inc.
     Main  Advanced  Event Logs  IPMI  Security  Boot  Save & Exit
  Save Options
  Discard Changes and Exit
  Save Changes and Reset

  Save Changes
  Discard Changes

  Default Options
  Restore Optimized Defaults
  Save as User Defaults
  Restore User Defaults

  Boot Override
  P4: TOSHIBA MG03ACA300                                →←: Select Screen
  PNY USB 3.0 FD 1.00                                   ↑↓: Select Item
  IBA 40G Slot B500 v1060                               Enter: Select
  UEFI: PNY USB 3.0 FD 1.00, Partition 1                +/-: Change Opt.
  UEFI: Built-in EFI Shell                              F1: General Help
                                                        F2: Previous Values
                                                        F3: Optimized Defaults
                                                        F4: Save & Exit
                                                        ESC: Exit

                Version 2.19.1268. Copyright (C) 2017 American Megatrends, Inc.
```

B. Provisioning Intel TXT (Server)

Next, you will need to provision Intel® TXT in the UEFI shell.

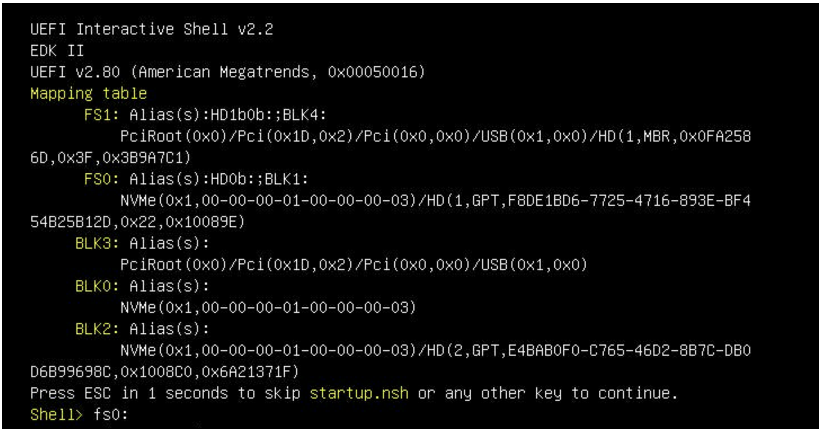
Note: If the TPM part number is AOM-TPM-9670V-S or AOM-TPM-9670H-S, you do not need to get the Intel® Provisioning tool. Please go ahead and enable the Intel TXT feature in the BIOS.

1. Select **"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 and press the **<Enter>** key.

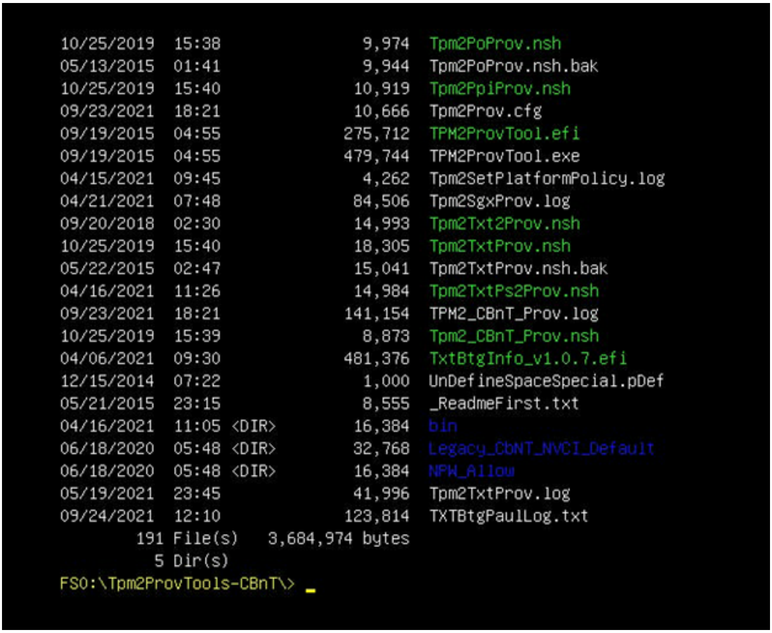
Note: The device used for the purposes of this user guide had a code of fs0. Replace this code with the code that corresponds to your device.

3. In the command line at the bottom of the screen, follow these steps below after typing **"FS0"**.



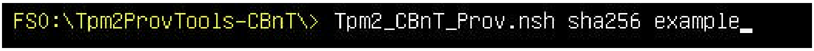
```
UEFI Interactive Shell v2.2
EDK II
UEFI v2.80 (American Megatrends, 0x00050016)
Mapping table
      FS1: Alias(s):HD1b0b:;BLK4:
          PciRoot(0x0)/Pci(0x1D,0x2)/Pci(0x0,0x0)/USB(0x1,0x0)/HD(1,MBR,0x0FA258
6D,0x3F,0x3B9A7C1)
      FS0: Alias(s):HD0b:;BLK1:
          NVMe(0x1,00-00-00-01-00-00-00-03)/HD(1,GPT,F8DE1BD6-7725-4716-893E-BF4
54B25B12D,0x22,0x10089E)
     BLK3: Alias(s):
          PciRoot(0x0)/Pci(0x1D,0x2)/Pci(0x0,0x0)/USB(0x1,0x0)
     BLK0: Alias(s):
          NVMe(0x1,00-00-00-01-00-00-00-03)
     BLK2: Alias(s):
          NVMe(0x1,00-00-00-01-00-00-00-03)/HD(2,GPT,E4BAB0F0-C765-46D2-8B7C-DB0
D6B99698C,0x1008C0,0x6A21371F)
Press ESC in 1 seconds to skip startup.nsh or any other key to continue.
Shell> fs0:
```

i. Go to the directory **"TPpm2ProvTools-CBnT"**.



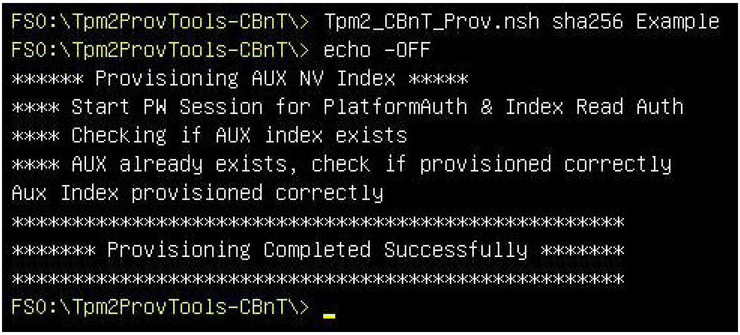
```
10/25/2019  15:38              9,974  Tpm2PoProv.nsh
05/13/2015  01:41              9,944  Tpm2PoProv.nsh.bak
10/25/2019  15:40             10,919  Tpm2PpiProv.nsh
09/23/2021  18:21             10,666  Tpm2Prov.cfg
09/19/2015  04:55            275,712  TPM2ProvTool.efi
09/19/2015  04:55            479,744  TPM2ProvTool.exe
04/15/2021  09:45              4,262  Tpm2SetPlatformPolicy.log
04/21/2021  07:48             84,506  Tpm2SgxProv.log
09/20/2018  02:30             14,993  Tpm2Txt2Prov.nsh
10/25/2019  15:40             18,305  Tpm2TxtProv.nsh
05/22/2015  02:47             15,041  Tpm2TxtProv.nsh.bak
04/16/2021  11:26             14,984  Tpm2TxtPs2Prov.nsh
09/23/2021  18:21            141,154  TPM2_CBnT_Prov.log
10/25/2019  15:39              8,873  Tpm2_CBnT_Prov.nsh
04/06/2021  09:30            481,376  TxtBtgInfo_v1.0.7.efi
12/15/2014  07:22              1,000  UnDefineSpaceSpecial.pDef
05/21/2015  23:15              8,555  _ReadmeFirst.txt
04/16/2021  11:05 <DIR>       16,384  bin
06/18/2020  05:48 <DIR>       32,768  Legacy_CbNT_NVCI_Default
06/18/2020  05:48 <DIR>       16,384  NPW_Allow
05/19/2021  23:45             41,996  Tpm2TxtProv.log
09/24/2021  12:10            123,814  TXTBtgPaulLog.txt
        191 File(s)   3,684,974 bytes
          5 Dir(s)
FS0:\Tpm2ProvTools-CBnT\> _
```

ii. Type the command **"Tpm2_CBnT_Prov.nsh sha256 example"**.



```
FS0:\Tpm2ProvTools-CBnT\> Tpm2_CBnT_Prov.nsh sha256 example_
```

iii. The provisioning process is now Completed.



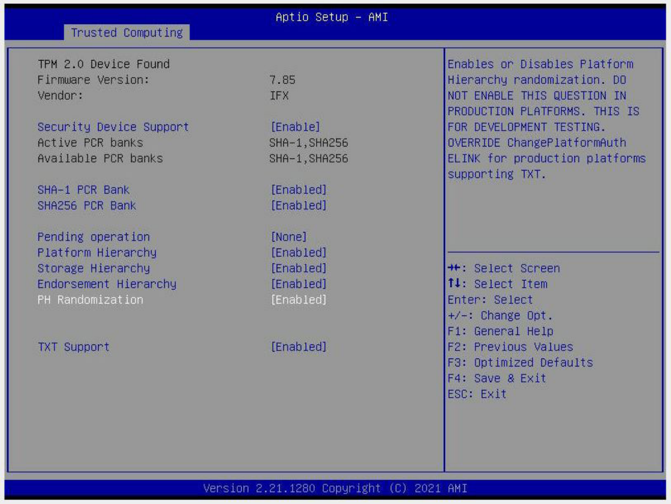
```
FS0:\Tpm2ProvTools-CBnT\> Tpm2_CBnT_Prov.nsh sha256 Example
FS0:\Tpm2ProvTools-CBnT\> echo -OFF
****** Provisioning AUX NV Index *****
**** Start PW Session for PlatformAuth & Index Read Auth
**** Checking if AUX index exists
**** AUX already exists, check if provisioned correctly
Aux Index provisioned correctly
***************************************************
******* Provisioning Completed Successfully *******
***************************************************
FS0:\Tpm2ProvTools-CBnT\> _
```

4. After the provisioning process has been 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.

C. Enabling TXT Support

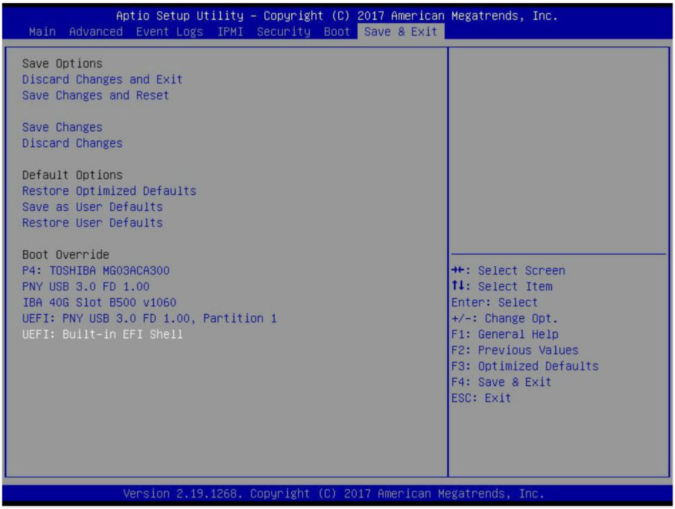
The last step is enabling TXT Support in the BIOS and UEFI shell.

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



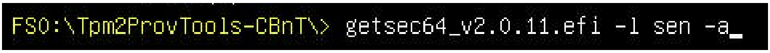
```
                                   Aptio Setup - AMI
          Trusted Computing

  TPM 2.0 Device Found                                   Enables or Disables Platform
  Firmware Version:                  7.85                Hierarchy randomization. DO
  Vendor:                            IFX                 NOT ENABLE THIS QUESTION IN
                                                         PRODUCTION PLATFORMS. THIS IS
  Security Device Support            [Enable]            FOR DEVELOPMENT TESTING.
  Active PCR banks                   SHA-1,SHA256        OVERRIDE ChangePlatformAuth
  Available PCR banks                SHA-1,SHA256        ELINK for production platforms
                                                         supporting TXT.
  SHA-1 PCR Bank                     [Enabled]
  SHA256 PCR Bank                    [Enabled]

  Pending operation                  [None]
  Platform Hierarchy                 [Enabled]
  Storage Hierarchy                  [Enabled]           →←: Select Screen
  Endorsement Hierarchy              [Enabled]           ↑↓: Select Item
  PH Randomization                   [Enabled]           Enter: Select
                                                         +/-: Change Opt.
                                                         F1: General Help
  TXT Support                        [Enabled]           F2: Previous Values
                                                         F3: Optimized Defaults
                                                         F4: Save & Exit
                                                         ESC: Exit

                    Version 2.21.1280 Copyright (C) 2021 AMI
```

2. Go back to the "Save & Exit" tab and select "UEFI: Built-in EFI Shell" in the BIOS. When the confirmation window appears, select <Yes>.



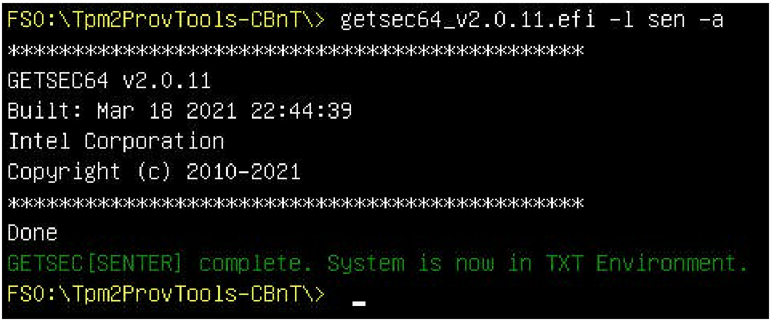
```
           Aptio Setup Utility - Copyright (C) 2017 American Megatrends, Inc.
    Main  Advanced  Event Logs  IPMI  Security  Boot  Save & Exit

  Save Options
  Discard Changes and Exit
  Save Changes and Reset

  Save Changes
  Discard Changes

  Default Options
  Restore Optimized Defaults
  Save as User Defaults
  Restore User Defaults

  Boot Override
  P4: TOSHIBA MG03ACA300                                 →←: Select Screen
  PNY USB 3.0 FD 1.00                                    ↑↓: Select Item
  IBA 40G Slot B500 v1060                                Enter: Select
  UEFI: PNY USB 3.0 FD 1.00, Partition 1                 +/-: Change Opt.
  UEFI: Built-in EFI Shell                               F1: General Help
                                                         F2: Previous Values
                                                         F3: Optimized Defaults
                                                         F4: Save & Exit
                                                         ESC: Exit

        Version 2.19.1268. Copyright (C) 2017 American Megatrends, Inc.
```

3. After Enabling TXT Support in BIOS, you will need to run TXT in the UEFI shell. In the Command line at the bottom of the page, type **"getsec64_v2.0.11.efi -l sen -a"** and press the <Enter> key. TXT support is now enabled.



```
FS0:\Tpm2ProvTools-CBnT\> getsec64_v2.0.11.efi -l sen -a_
```

4. To Exit from the TXT Environment, type **"getsec64_v2.0.11.efi -l sexit"** in the command line at the bottom of the screen and press the <Enter> key.



```
FS0:\Tpm2ProvTools-CBnT\> getsec64_v2.0.11.efi -l sen -a
*********************************************
GETSEC64 v2.0.11
Built: Mar 18 2021 22:44:39
Intel Corporation
Copyright (c) 2010-2021
*********************************************
Done
GETSEC[SENTER] complete. System is now in TXT Environment.
FS0:\Tpm2ProvTools-CBnT\>  _
```

(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.