



Trusted Platform Module (TPM) TCG 1.2 / 2.0

USER GUIDE

Revision 1.1c

The information in this User 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: This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the manufacturer's instruction manual, may cause harmful interference with radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case you will be required to correct the interference at your own expense.

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: Handling of lead solder materials used in this product may expose you to lead, a chemical known to the State of California to cause birth defects and other reproductive harm.

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.

Manual Revision 1.1c

Release Date: May 27, 2016

Unless you request and receive written permission from Super Micro Computer, Inc., you may not copy any part of this document. Information in this document is subject to change without notice. Other products and companies referred to herein are trademarks or registered trademarks of their respective companies or mark holders.

Copyright © 2016 by Super Micro Computer, Inc.
All rights reserved.

Printed in the United States of America

Preface

About This User Guide

This user 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 both TCG 1.2 and 2.0 for the trusted platform module (TPM).

Conventions Used in the User Guide

Special attention should be given to the following symbols for proper installation and to prevent damage done to the components or injury to yourself:



Warning: Important information given to avoid TPM configuration errors.



Note: Additional information given to differentiate various models or provides information for correct system setup.

Important Links

For your product to work properly, please follow the links below to download all necessary drivers/utilities and any pertinent user manuals/guides:

- Supermicro product manuals: <http://www.supermicro.com/support/manuals/>
- Product drivers and utilities: <ftp://ftp.supermicro.com>
- Product safety info: http://www.supermicro.com/about/policies/safety_information.cfm
- If you have any questions, please contact our support team at: support@supermicro.com

This user guide may be periodically updated without notice. Please check the Supermicro website for possible updates to the manual revision level.

An Important Note to the User

The graphics shown in this user 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.

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

Table of Contents

About This User Guide	3
Conventions Used in the User Guide	3
An Important Note to the User	3
Contacting Supermicro	4
Chapter 1 Introduction	
1.1 Overview of the Trusted Platform Module (TPM)	7
A. Types of TPMs for TPM 1.2	7
B. Types of TPMs for TPM 2.0	8
1.2 Supermicro TPM Features	9
1.3 Motherboards Supported for TPM.....	10
1.4 Intel® TXT	10
A. How the TXT Works	10
Chapter 2 Installation of the TPM 1.2	
2.1 Installing the TPM onto the Motherboard.....	11
2.2 Enabling the TPM 1.2 via the SUM	13
2.3 Enabling the TPM 1.2 via the BIOS and Intel ® Provision Utility.....	14
A. Enabling the TPM 1.2 in the BIOS.....	15
B. Provisioning via the Intel Provision Utility (Server)	18
C. Provisioning via the Intel Provision Utility (Client)	22
D. Enabling TXT Support.....	27
Chapter 3 Installation of the TPM 2.0	
3.1 Installing the TPM onto the Motherboard.....	28
3.2 Configuring the TPM 2.0 and Intel TXT for the Server.....	30
A. Enabling TPM 2.0 in the BIOS	30
B. Provisioning Intel TXT (Server)	34
C. Enabling TXT Support	37
3.3 Provisioning the TPM 2.0 and TXT Support for the Client.....	39
A. Clear the CMOS on the Motherboard	39
B. Provisioning Utility	39
C. Disabling PH Randomizations and TXT Support in the BIOS	40
D. Provisioning TXT Support in the UEFI Shell.....	44

E. Enabling PH Randomizations and TXT Support in the BIOS	47
F. Enabling TXT Support in the UEFI Shell	50

Chapter 1

Introduction

Congratulations on purchasing your TPM from an industry leader. Supermicro products are designed to provide you with the highest standards in quality and performance.

1.1 Overview of the Trusted Platform Module (TPM)

The Trusted Platform Module (TPM) is a special add-on module. It holds computer-generated encryption keys used to bind and authenticate input and output data passing through a system.

A. Types of TPMs for TPM 1.2



Note: Currently, all TPMs must be provisioned to use for TXT. Contact Supermicro technical support to get the Intel® Provisioning Utility.

The **TPM-9655 series** uses TCG 1.2 (Trusted Computing Group).

The following SKUs are available:

- AOM-TPM-9655V, a vertical TPM without provisioning
- AOM-TPM-9655H, a horizontal TPM without provisioning
- AOM-TPM-9655V-S, a vertical server TPM provisioned for TXT
- AOM-TPM-9655H-S, a horizontal server TPM provisioned for TXT
- AOM-TPM-9655V-C, a vertical client TPM provisioned for TXT
- AOM-TPM-9655H-C, a horizontal client TPM provisioned for TXT
- AOM-TPM-9665V-FS, a vertical server TPM provisioned for TXT, supports FIPs 140-2
- AOM-TPM-9665H-FS, a horizontal server TPM provisioned for TXT, supports FIPs 140-2

B. Types of TPMs for TPM 2.0

The **TPM-9665 series** uses TCG 2.0 (Trusted Computing Group).

The following SKUs are available:

- AOM-TPM-9665V, a vertical TPM without provisioning
- AOM-TPM-9665H, a horizontal TPM without provisioning
- AOM-TPM-9665V-S, a vertical server-side TPM
- AOM-TPM-9665H-S, a horizontal server-side TPM
- AOM-TPM-9665V-C, a vertical client-side TPM
- AOM-TPM-9665H-C, a horizontal client-side TPM

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 can be used in 1U chassis. Vertical TPMs can be 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 on Intel Xeon® E5 and E7, as well as Xeon-D processors. It has a 96-byte index memory. The client TPM is designed to run on Intel Core™ i5, Core i7, and Xeon E3 processors. It has a 48-byte index memory.

TPM Models and Supported AOMs	
TPM Version 1.2	TPM Version 2.0
AOM-TPM-9665V	AOM-TPM-9665V
AOM-TPM-9665H	AOM-TPM-9665H
AOM-TPM-9665V-S	AOM-TPM-9665V-S
AOM-TPM-9665H-S	AOM-TPM-9665H-S
AOM-TPM-9665V-C	AOM-TPM-9665V-C
AOM-TPM-9665H-C	AOM-TPM-9665H-C
AOM-TPM-9665V-FS	
AOM-TPM-9665H-FS	

1.2 Supermicro TPM Features

- TCG 1.2 compliance



Note: TPM 2.0 has TCG 2.0 compliance instead

- Microcontroller in 0.22/0.09- μ m CMOS technology
- Compliant embedded software
- EEPROM for TCG firmware enhancements and for user data and keys
- Hardware accelerator for SHA-1 and SHA-256 hash algorithm



Note: SHA-256 is recommended for TPM 2.0

- True Random Number Generator (TRNG)
- Tick counter with tamper detection
- Protection against dictionary attack
- Infineon's TPM 1.2 is Common Criteria certified at Evaluation Assurance Level (EAL) 4 Moderate



Note: The same is true of TPM 2.0

- General-purpose I/O
- Intel® Trusted Execution Technology (TXT) support
- AMD® Secure Virtual Machine Architecture support (**for TPM 1.2 only**)
- Full personalization with Endorsement Key (EK) and EK certificate
- Power-saving sleep mode
- 3.3V power supply
- WHQL dual-mode 1.1b + 1.2 TPM Windows Kernel Mode Driver (**For TPM 1.2 only**)



Note: At this time, TPM 2.0 supports Windows environments only

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 TXT is a software tool that may be used in conjunction with the TPM to provide additional security firmware (BIOS, IPMI, SAS, CMM, etc.) in virtualized environments such as cloud and cluster. 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.

Chapter 2

Installation of the TPM 1.2

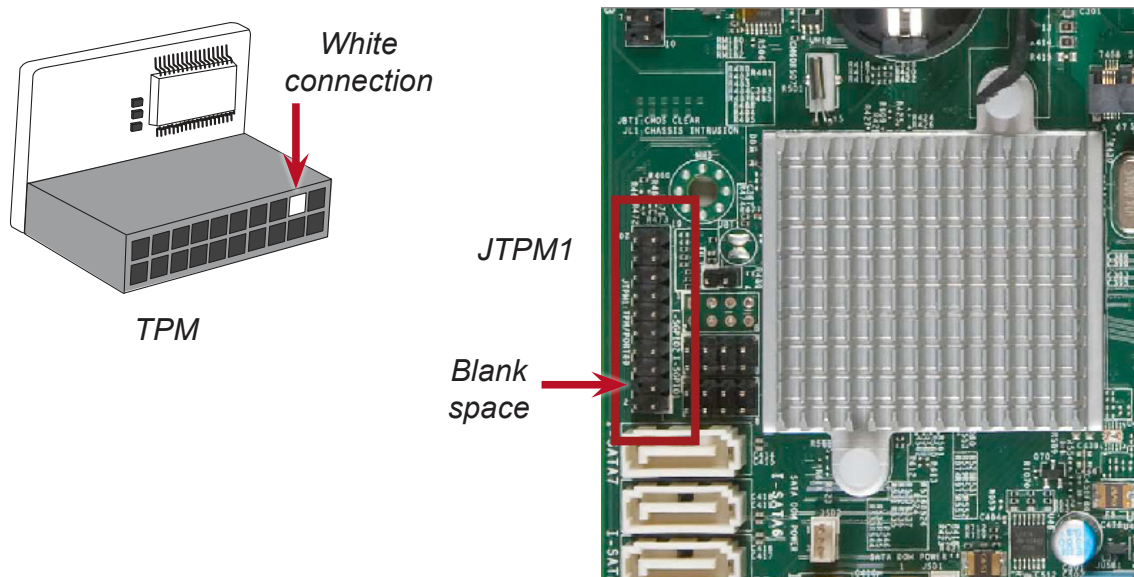
Follow the instructions below to begin using the TPM 1.2.

 **Note:** Please note that the module is not hot-swappable; you will have to power down your system prior to installation.

2.1 Installing the TPM onto the Motherboard

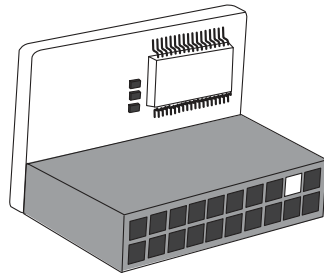
To install the Trusted Platform Module (TPM) onto your motherboard, follow the steps below.

1. Locate the 20-pin male JTPM1 connector on the motherboard (see the image below). If the board does not have this connector, then it does not support the TPM.
2. Using the white connection on the TPM and the blank space on JTPM1 as a reference, orient and align your TPM with the connector. Installing the TPM with the incorrect orientation may cause damage to the module and the motherboard.
3. Carefully insert the TPM into the connector on the motherboard, taking care not to damage the pins.

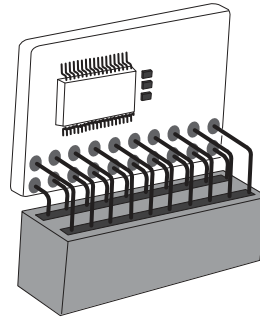


 **Note:** The above picture is an example of JTPM1. Your JTPM1 connector may be in a different location, or oriented differently. Please consult your motherboard user manual for more information.

 **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 two images below for the correct orientation.



Horizontal TPM



Vertical TPM

2.2 Enabling the TPM 1.2 via the SUM

The SUM (Supermicro Update Manager) is an optional tool that can be used to update and monitor Supermicro servers, as well as configure some firmware settings. Among these features is the ability to enable and provision the TPM 1.2. For the sake of efficiency and ease, it is highly recommended that you use the SUM. However, if you do not have the SUM available, you may also use the BIOS and Intel Provision Utility, as described in section 2.3.

 **Note:** If you don't have the SUM, you must request authorization to download it. For more information on the SUM and to request and download it, visit the Supermicro website at http://www.supermicro.com/products/nfo/SMS_SUM.cfm.

 **Note:** The commands below do not apply to X9 dual processor nor X10 single processor motherboards. If you have one of these motherboards, you must use the method described in section 2.3.

 **Note:** TPM 2.0 does not support the SUM.

1. You will need to obtain a license key to enable Out-of-Band (OOB). Once you have enabled OOB, you will be able to use the SUM.
2. Set up and activate the SUM if you have not done so. For instructions on how to do this, refer to the SUM user's guide.
3. Enter the following command:

```
sum -i <IP or host name> -u <username> -p <password> -c TpmProvision
--image_url <URL> --reboot [--id <id for URL> --pw <password for
URL>]
```

For example,

```
<SUM_HOME#> ./sum -i 192.168.34.56 -u ADMIN -p ADMIN -c
TpmProvision --image_url 'smb://192.168.35.1/MySharedPoint/
MyFolder/TPM.iso' --id smbuid --pw smbpasswd --reboot
```

4. The TPM 1.2 should now be ready for use.

2.3 Enabling the TPM 1.2 via the BIOS and Intel® Provision Utility

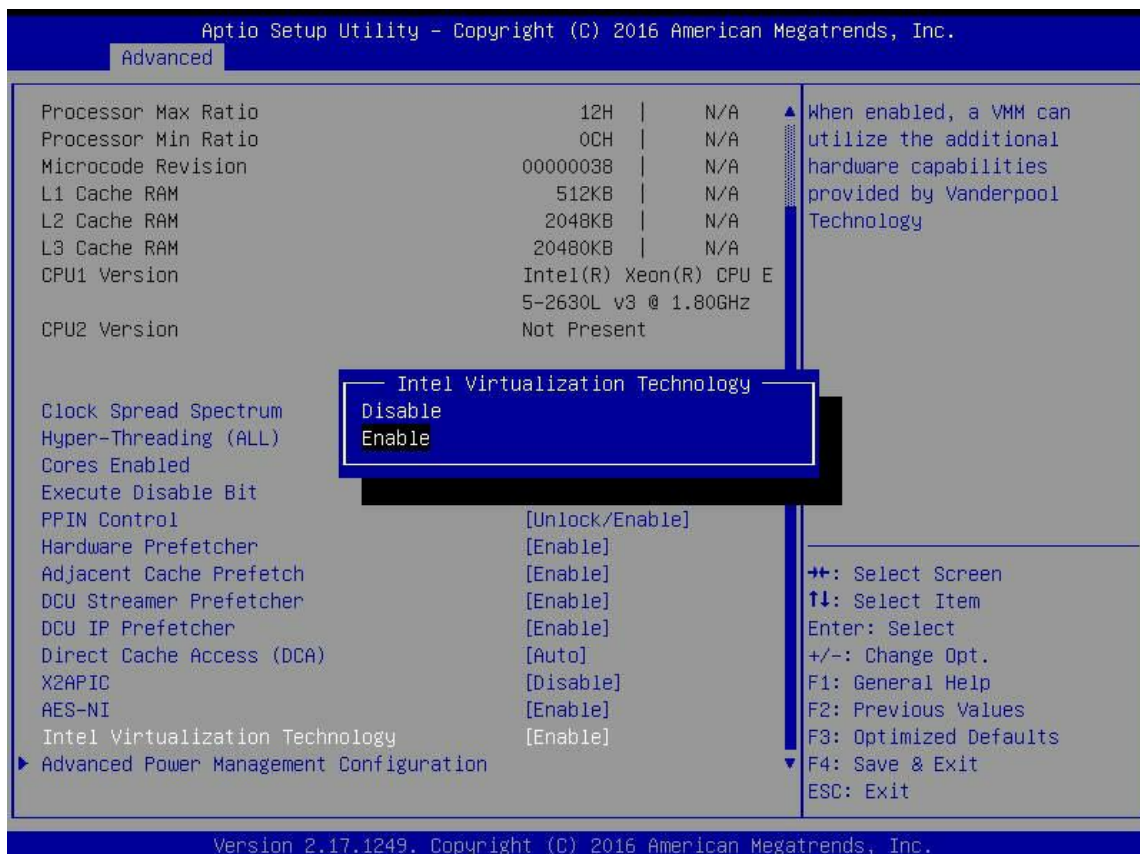
 **Note:** The steps described in the entirety of this section are for those who do not have the SUM, have motherboards incompatible with the SUM, or have experienced issues enabling the TPM 1.2 with the SUM. If you have already enabled the TPM 1.2 using the SUM as described in section 2.2, you do not need to complete the steps below.

 **Note:** As described in subsections C and D, you will need the Intel Provision Utility to successfully provision the TPM 1.2 for use. Please contact Supermicro to download this utility.

There are two components to the process of enabling the TPM 1.2. After you have installed the TPM 1.2 onto the motherboard, you must first "verify" the TPM 1.2 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 1.2 in the firmware. This is done through the provision utility provided by Intel.

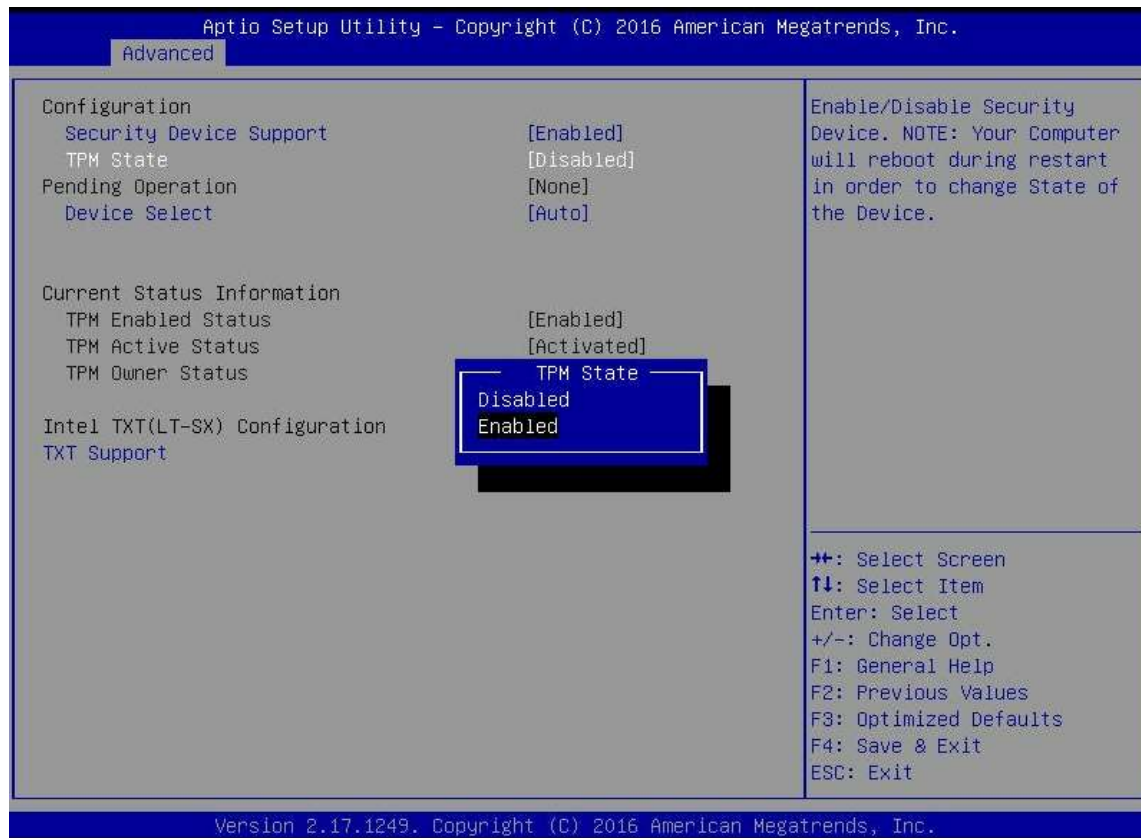
A. Enabling the TPM 1.2 in the BIOS

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 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, as shown below. Press <Enter>.
3. You will be taken to the CPU Configuration page. Using your arrow keys, navigate down to the "Intel Virtualization Technology" option, and press <Enter>. If this item is not already enabled, select "Enable" and press <Enter>.

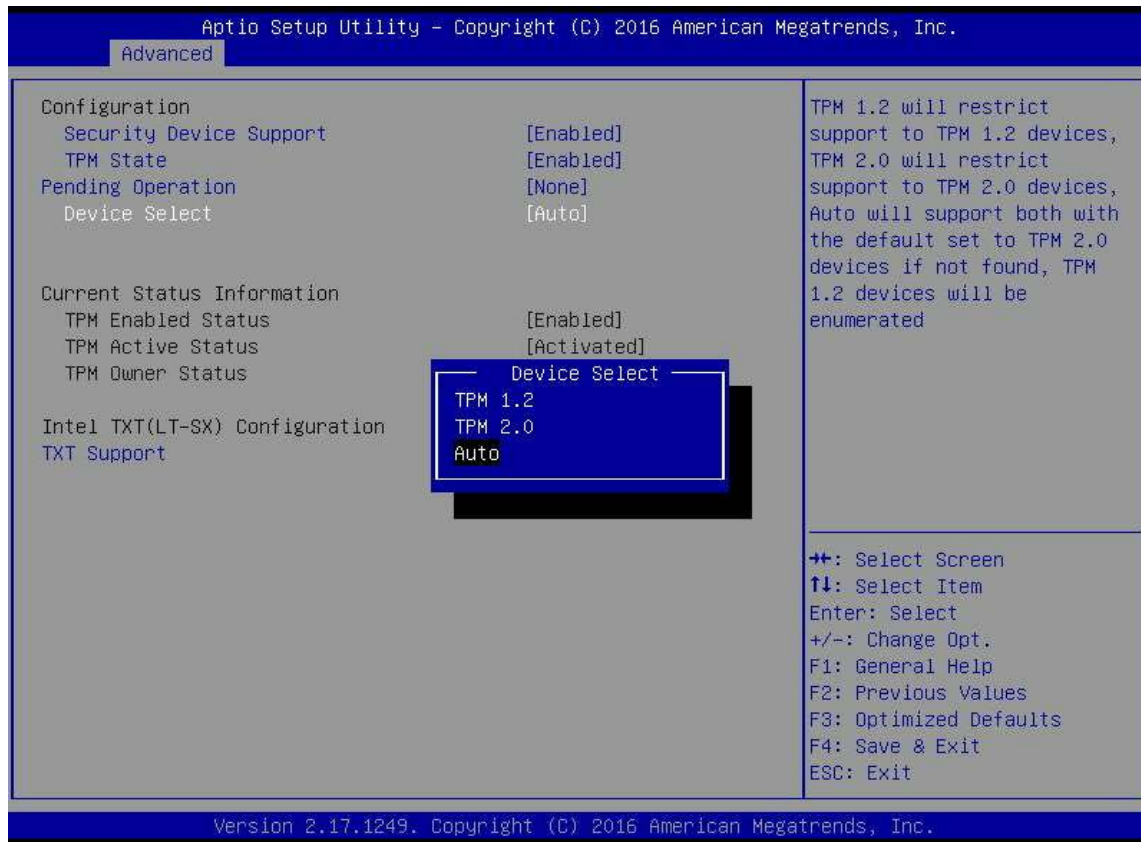


4. Once you have enabled virtualization support, press your <Esc> key until you are back to the *Advanced* tab. Navigate down to the "Trusted Computing" option and press <Enter>.
5. The Trusted Computing window will appear. Select "TPM State," and press <Enter>.

6. From the window that pops up, select "Enabled," as shown below, and press <Enter>.



7. Next, select "Device Select." Selecting the TPM 1.2/TPM 2.0 options will bypass any possible compatibility issues between the module and the motherboard. Selecting Auto will have the system auto-detect the model of TPM being used.

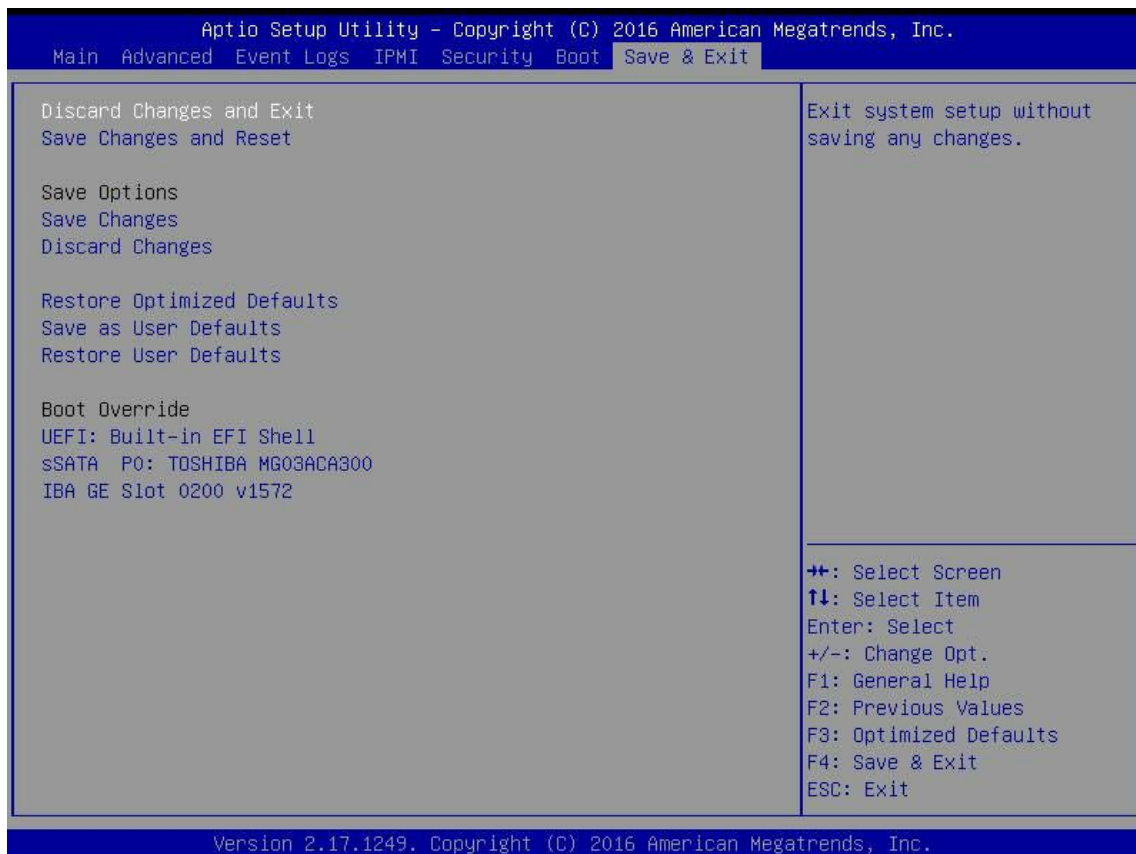


8. You must save your changes and reset for the changes to take effect. Press the <Esc> key to exit the Trusted Computing options and scroll to the Save & Exit tab. Select "Save Changes and Reset." The TPM is now enabled.

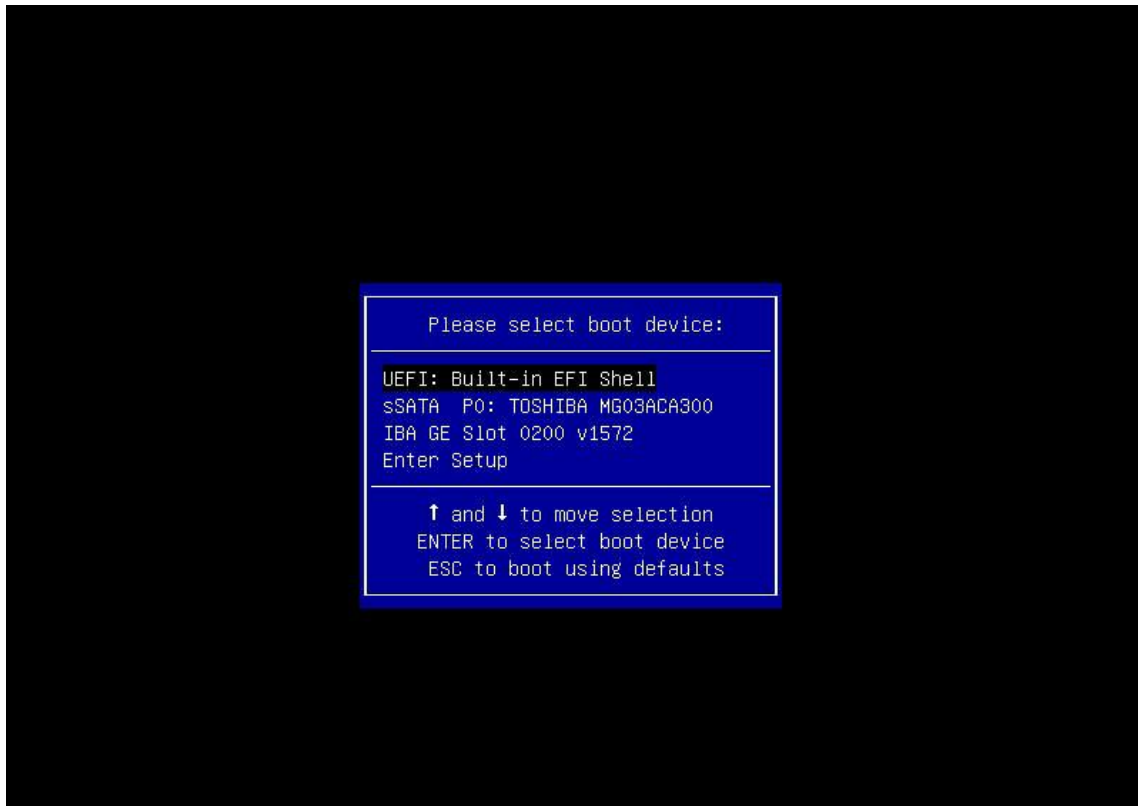
B. Provisioning via the Intel Provision Utility (Server)

After you enable the TPM 1.2 in the BIOS, you must provision it. Follow the steps below to do so on a server TPM platform. For provisioning on the client side, please refer to subsection D.

1. Save a copy of the utility to a USB flash drive, and plug the drive into your system. To download the utility, contact Supermicro support.
2. Boot into the UEFI shell. There are two ways you can do this, described below:
 - **Option 1:** From the BIOS, scroll to the *Save & Exit* tab. Select the option "UEFI: Built-in EFI Shell" under *Boot Override*, as shown in the screenshot on the next page. Press <Enter>. If a window pops up that prompts, "Save configuration and reset?" select "Yes" and press <Enter>.



- Option 2: Reboot the system. As the system boots up, press the <F11> key. The following list will appear. Using your arrow keys, select "UEFI: Built-in EFI Shell." Press <Enter>.



3. You are now in the EFI shell. If a line prompts you to press <Esc> to skip *startup.nsh*, do so.
4. (Optional) Type **map** to find out your USB ID. A list of devices connected to the motherboard will appear. Your USB flash drive should, by default, be fs0.

```

EFI Shell version 2.40 [5.11]
Current running mode 1.1.2
Device mapping table
fs0 :Removable HardDisk - Alias hd32a0c0b blk0
    PciRoot(0x0)/Pci(0x1A,0x0)/USB(0x0,0x0)/USB(0x2,0x0)/HD(1,MBR,0x0FA2586D,0x3F,0x3B9A7C1)
blk0 :Removable HardDisk - Alias hd32a0c0b fs0
    PciRoot(0x0)/Pci(0x1A,0x0)/USB(0x0,0x0)/USB(0x2,0x0)/HD(1,MBR,0x0FA2586D,0x3F,0x3B9A7C1)
blk1 :HardDisk - Alias (null)
    PciRoot(0x0)/Pci(0x11,0x4)/Sata(0x0,0xFFFF,0x0)/HD(1,MBR,0x6363CD45,0x800,0x32000)
blk2 :HardDisk - Alias (null)
    PciRoot(0x0)/Pci(0x11,0x4)/Sata(0x0,0xFFFF,0x0)/HD(2,MBR,0x6363CD45,0x32800,0xFFFFCD800)
blk3 :BlockDevice - Alias (null)
    PciRoot(0x0)/Pci(0x11,0x4)/Sata(0x0,0xFFFF,0x0)
blk4 :Removable BlockDevice - Alias (null)
    PciRoot(0x0)/Pci(0x1A,0x0)/USB(0x0,0x0)/USB(0x2,0x0)

Press ESC in 2 seconds to skip startup.nsh, any other key to continue.
Shell> _

```

5. In the command line at the bottom of the screen, type **fs0:** then press the <Enter> key.

```
Shell> fs0:
fs0:\> _
```

6. Type **cd serverTPMTool** and press the <Enter> key.

```
fs0:\> cd serverTPMTool
fs0:\ServerTPMTool> _
```

7. Type **cd Executable** and press the <Enter> key.

```
fs0:\ServerTPMTool> cd Executable
fs0:\ServerTPMTool\Executable> _
```

8. Type **DefaultTPMProvision-Locked.nsh** and press the <Enter> key.

```
fs0:\ServerTPMTool\Executable> DefaultTPMProvision-Locked.nsh_
```

9. To check that the TPM 1.2 has been successfully locked, type **ServerTPMTool.efi** and press the <Enter> key.

```
TPM read successful.
ERROR: 0x40000005 - Data file data size does not match the existing index data size.
DefaultTPMProvision-Locked.nsh> ServerTPMTool.efi PPI.nvi

Intel(R) TPM Tool x64 DEBUG. Major version:[1] Minor version:[.0] BUILD DATE:[Apr  9 2013].
Data File Read Complete.
TPM locked
TPM_Read_NV_Index_Info: Return Code - 0x02000000
ERROR: 0x40000008 - TPM read index info failed.
DefaultTPMProvision-Locked.nsh> ServerTPMTool.efi TPM_Lock.def

Intel(R) TPM Tool x64 DEBUG. Major version:[1] Minor version:[.0] BUILD DATE:[Apr  9 2013].
Definition File Read Complete.
TPM locked
```

10. From the menu that appears, press <1> ("Display TPM Status"), as shown above, and press the <Enter> key.

11. From the TPM Status Menu that appears, press <3>, and press the <Enter> key.

```
TPM Status Menu
1: Display TPM Interface Status
2: Display TPM Volatile flags
3: Display TPM Non-Volatile flags
Q: Previous Menu
> 3
```

12. You should receive an output log. The "nvLocked" item, indicated by the arrow below, should be set to 1. This shows that the TPM 1.2 has been successfully locked.

```
TPM Status Menu
1: Display TPM Interface Status
2: Display TPM Volatile flags
3: Display TPM Non-Volatile flags
Q: Previous Menu
> 3
```

```
TPM Permanent Flags value:
  disable           = 0
  ownership         = 1
  deactivated        = 0
  readPubek         = 0
  disableOwnerClear = 1
  allowMaintenance  = 0
  physicalPresenceLifetimeLock = 0
  physicalPresenceHwEnable = 0
  physicalPresenceCmdEnable = 1
  FIPS              = 0
  enableRevokeEK    = 0
  nvLocked           = 1
  tpmEstablished    = 0
```



13. If you come across any error messages along the way, or if the "nvLocked" item is still set to 0 despite your following the previous instructions, try the following troubleshooting tips:

- Make sure that the CPU you are using is compatible. It should be an Intel® Xeon® E3-1200 v2 or i3/i5/i7 model.

 **Note:** AOM-TPM-9655V-S and AOM-TPM-9655H-S are compatible with Xeon E5/E7 processors. AOM-TPM-9655V-C and AOM-TPM-9655H-C are compatible with Intel Core i5/i7 and Xeon E3 processors.

- If the problem persists, contact Supermicro's technical support.

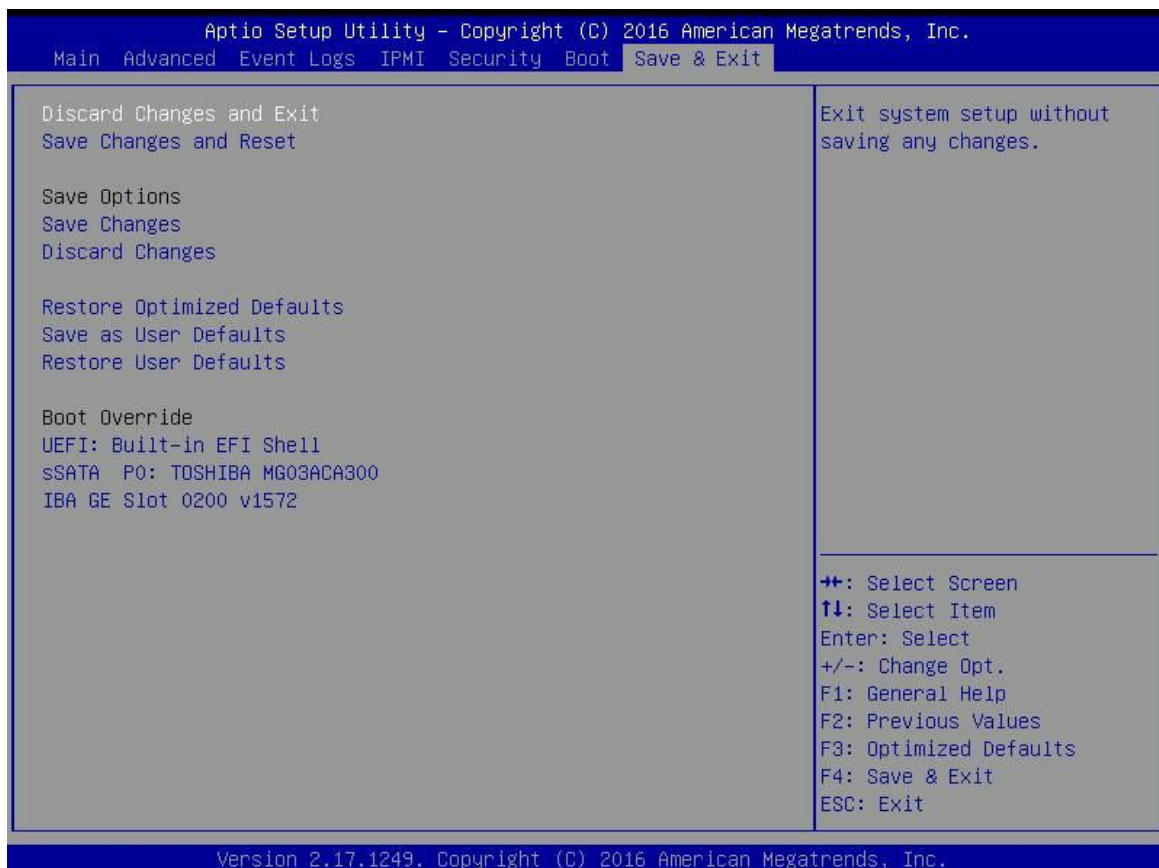
 **Note:** To exit the UEFI Shell, press <Q> and <Enter> until you reach the **fs0:** command line. Then either press <Ctrl><Alt> to reboot the system or type **exit**.

- If you entered the UEFI Shell from the BIOS, typing "exit" will send you back to the BIOS menu.
- If you entered the UEFI Shell from the F11 Boot Menu, typing "exit" will reboot the system.

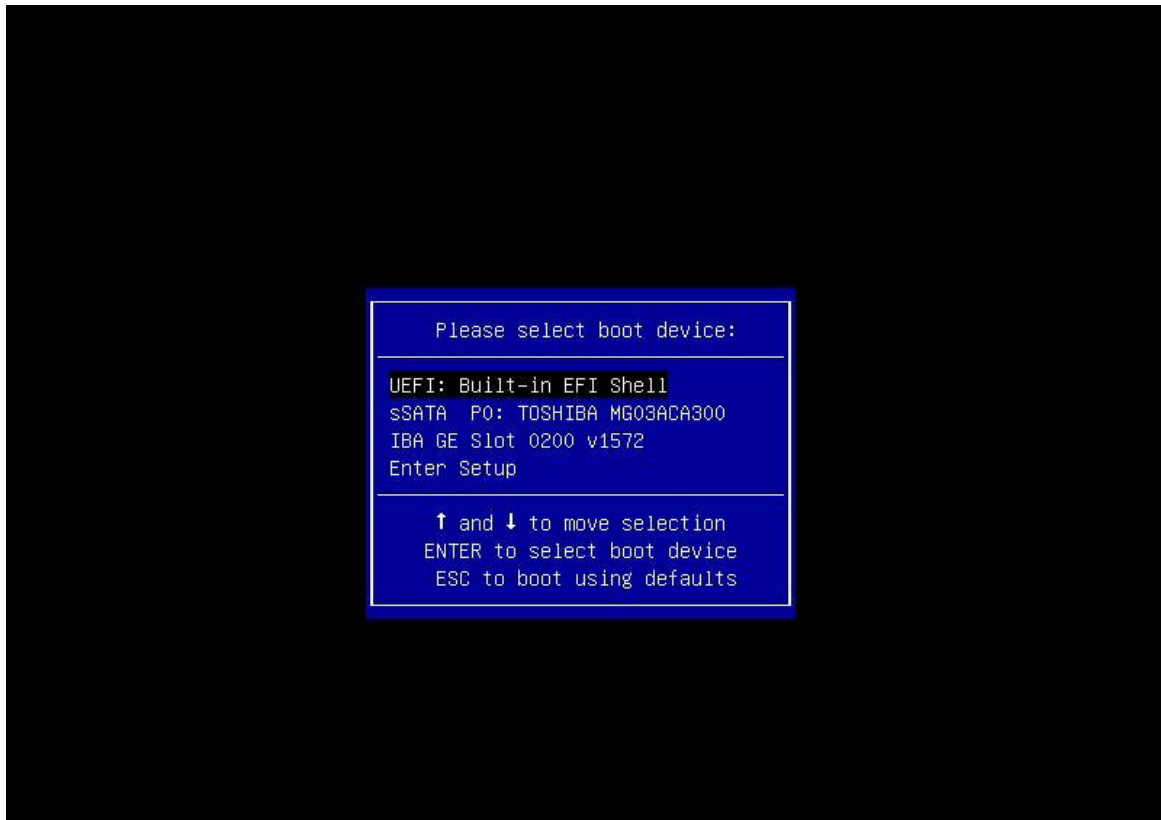
C. Provisioning via the Intel Provision Utility (Client)

After you enable the TPM 1.2 in the BIOS, you must provision it. Follow the steps below to do so on a client TPM platform.

1. Save a copy of the utility to a USB flash drive, and plug the drive into your system. To download the utility, contact Supermicro support.
2. Boot into the UEFI shell. There are two ways you can do this, described below:
 - **Option 1:** From the BIOS, scroll to the *Save & Exit* tab. Select the option "UEFI: Built-in EFI Shell" under *Boot Override*, as shown in the screenshot below. Press <Enter>. If a window pops up that prompts, "Save configuration and reset?" select "Yes" and press <Enter>.



- **Option 2:** Reboot the system. As the system boots up, press the <F11> key. The following list will appear. Using your arrow keys, select "UEFI: Built-in EFI Shell." Press <Enter>.



3. You are now in the EFI shell. If a line prompts you to press <Esc> to skip *startup.nsh*, do so.

```
EFI Shell version 2.40 [5.11]
Current running mode 1.1.2
Device mapping table
fs0 :Removable HardDisk - Alias hd32a0c0b blk0
      PciRoot(0x0)/Pci(0x1A,0x0)/USB(0x0,0x0)/USB(0x2,0x0)/HD(1,MBR,0x0FA2586D,0x3F,0x3B9A7C1)
blk0 :Removable HardDisk - Alias hd32a0c0b fs0
      PciRoot(0x0)/Pci(0x1A,0x0)/USB(0x0,0x0)/USB(0x2,0x0)/HD(1,MBR,0x0FA2586D,0x3F,0x3B9A7C1)
blk1 :HardDisk - Alias (null)
      PciRoot(0x0)/Pci(0x11,0x4)/Sata(0x0,0xFFFF,0x0)/HD(1,MBR,0x6363CD45,0x800,0x32000)
blk2 :HardDisk - Alias (null)
      PciRoot(0x0)/Pci(0x11,0x4)/Sata(0x0,0xFFFF,0x0)/HD(2,MBR,0x6363CD45,0x32800,0xFFFFCD800)
blk3 :BlockDevice - Alias (null)
      PciRoot(0x0)/Pci(0x11,0x4)/Sata(0x0,0xFFFF,0x0)
blk4 :Removable BlockDevice - Alias (null)
      PciRoot(0x0)/Pci(0x1A,0x0)/USB(0x0,0x0)/USB(0x2,0x0)

Press ESC in 2 seconds to skip startup.nsh, any other key to continue.
Shell> _
```

4. Type the following command to enter the flash drive directory: **fs0:**

```
Shell> fs0:
fs0:\> _
```

5. Type **TPMFactProv.efi -f defaultclienttpmprov-aux2.xml -l**

6. You should see the screen shown below indicating that the TPM 1.2 is now locked.

```
02/12/16 04:23p <DIR>          0 .
02/12/16 04:23p <DIR>          0 ..
09/09/14 07:20p              7,270 DefaultClientTpmProv-AUX2.xml
10/09/14 11:37a          325,888 ServerTPMTool.efi
10/24/14 06:46p              78 STARTUP.NSH
11/10/12 04:04p          268,032 TPMFactProv.efi
02/12/14 10:04a          215,872 txtinfo64_1.4.8.efi
      5 File(s)      817,140 bytes
      2 Dir(s)

fs0:\TPM Client Auto Script> TPMFactProv.efi -f DefaultClientTpmProv-AUX2.xml -l

DEBUG: main

Intel(R) TPM Factory Provisioning tool x64 DEBUG. Major version:[1] Minor version:[.0] BUILD DATE:[Oct 18 2012].

Parsing Intel(R) TPM Provisioning Tool Configuration File DefaultClientTpmProv-AUX2.xml.

PASSED - Intel(R) Factory Provisioning Tool. TPM provisioned properly. Return code = 0x0

fs0:\TPM Client Auto Script> _
```

7. To check that the TPM 1.2 has been successfully locked, type **ServerTPMTool.efi**

```
Parsing Intel(R) TPM Provisioning Tool Configuration File DefaultClientTpmProv-AUX2.xml.
PASSED - Intel(R) Factory Provisioning Tool. TPM provisioned properly. Return code = 0x0

fs0:\ServerTPMTool\Executable> ServerTPMTool.efi

Intel(R) TPM Tool x64 DEBUG. Major version:[1] Minor version:[.0] BUILD DATE:[Apr  9 2013].
1: Display TPM Status (Version, V-flags, P-flags, etc)
2: NV RAM Functions
3: Lock the TPM
4: Take Ownership
5: Clear Ownership
6: PCR Functions
7: TIS Functions
8: TPM Start Up
9: TPM Continue Self Test
Q: Quit
> 1
```

8. From the menu that appears, press <1> ("Display TPM Status"), and press <Enter>.
9. From the TPM Status Menu that appears, press <3>, and press <Enter>.
10. You should receive an output log. The "nvLocked" item, indicated by the arrow below, should be set to 1. This shows that the TPM 1.2 has been successfully locked.

```
TPM Status Menu
1: Display TPM Interface Status
2: Display TPM Volatile flags
3: Display TPM Non-Volatile flags
Q: Previous Menu
> 3
TPM Permanent Flags value:
  disable           = 0
  ownership         = 1
  deactivated       = 0
  readPubek        = 0
  disableOwnerClear = 1
  allowMaintenance = 0
  physicalPresenceLifetimeLock = 0
  physicalPresenceHwEnable = 0
  physicalPresenceCmdEnable = 1
  FIPS             = 0
  enableRevokeEK   = 0
  nvLocked          = 1
  tpmEstablished   = 0
```

11. If you come across any error messages along the way, or if the "nvLocked" item is still set to 0 despite your following the previous instructions, try the following troubleshooting tips:

- Make sure that the CPU you are using is compatible. It should be an Intel® Xeon® E3-1200 v2 or i3/i5/i7 model.



Note: AOM-TPM-9655V-S and AOM-TPM-9655H-S are compatible with Xeon D/E5/E7 processors. AOM-TPM-9655V-C and AOM-TPM-9655H-C are compatible with Intel Core i5/i7 and Xeon E3 processors.

- If the problem persists, contact Supermicro's technical support.



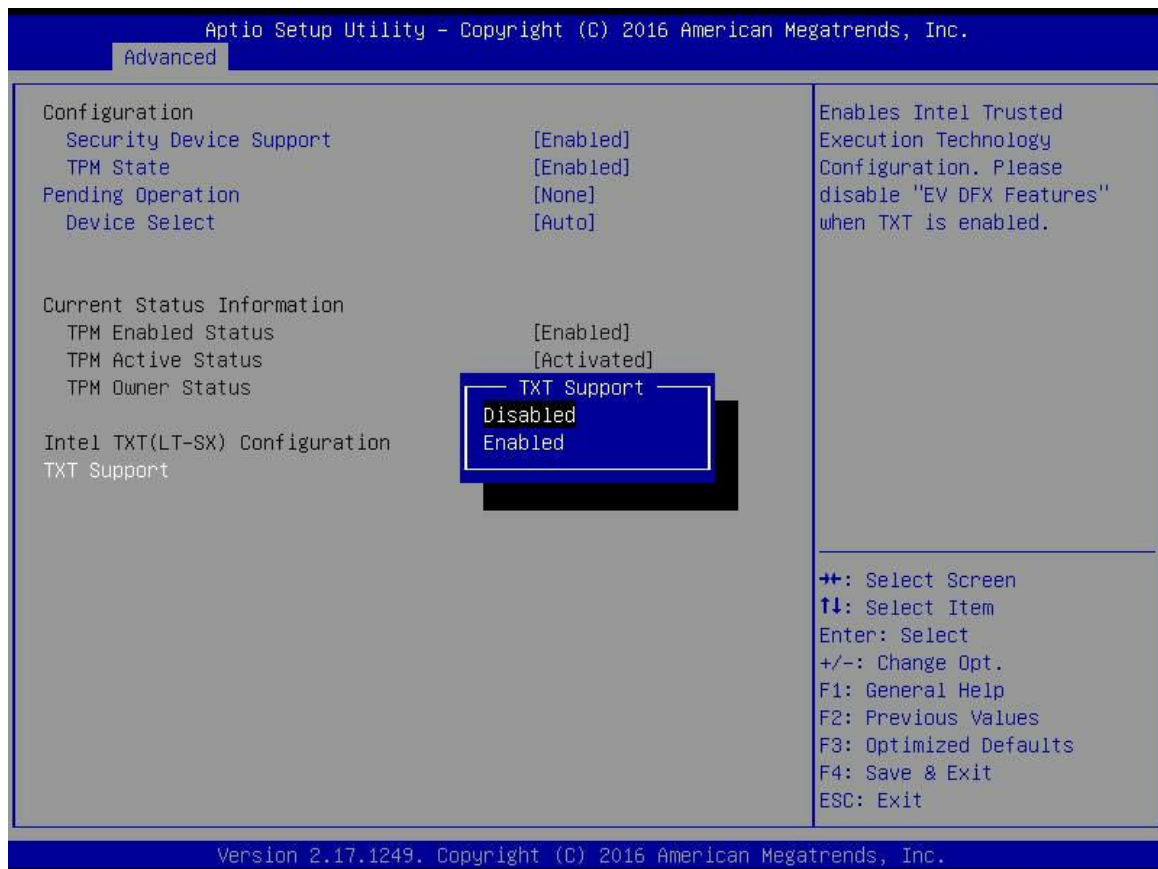
Note: To exit the UEFI Shell, press <Q> and <Enter> until you reach the **fs0:** command line. Then either press <Ctrl><Alt> to reboot the system or type **exit**.

- If you entered the UEFI Shell from the BIOS, typing "exit" will send you back to the BIOS menu.
- If you entered the UEFI Shell from the F11 Boot Menu, typing "exit" will reboot the system.

D. Enabling TXT Support

Follow the steps below to enable Intel TXT (Trusted Execution Technology). This is also done in the BIOS.

1. After provisioning the TPM 1.2 via the provisioning utility, restart the system and enter the BIOS setup screen.
2. Navigate to the Trusted Computing screen as described in subsection A, steps 2-4.
3. Select the "TXT Support" item. Press <Enter>. A "TXT Support" window will pop up as shown below.



4. Select "Enabled," and press <Enter>.
5. Save changes and reset to save your changes and allow them to take effect. The TXT is now enabled.
6. Use a third-party tool to test the hypervisor launch.

Chapter 3

Installation of the TPM 2.0

Follow the instructions below to begin using the TPM 2.0.

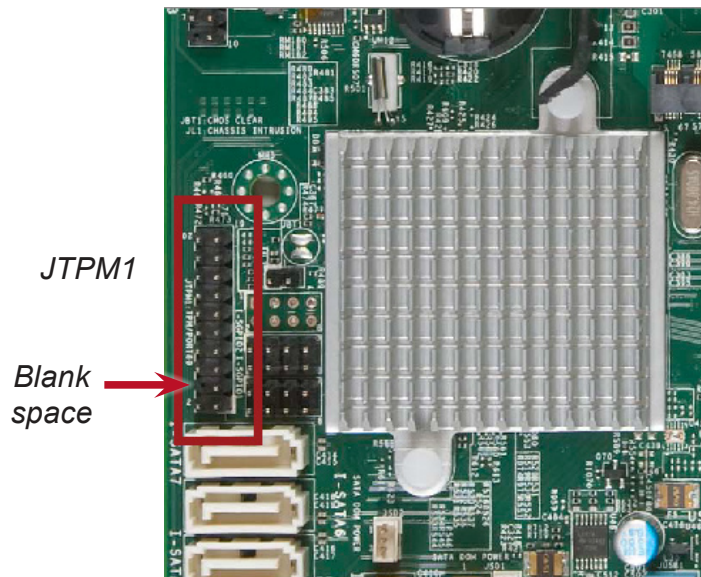
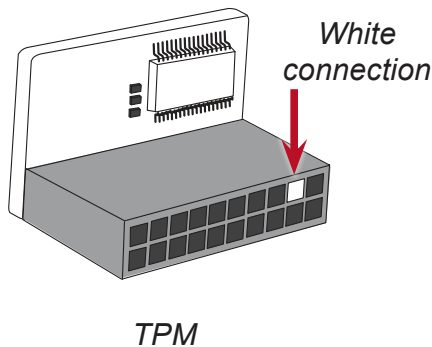


Note: Please note that the module is not hot-swappable; you will have to power down your system prior to installation.

3.1 Installing the TPM onto the Motherboard

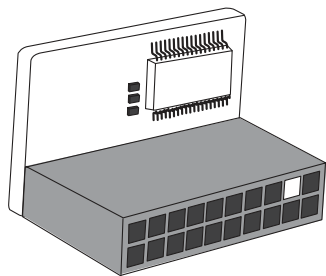
To install the Trusted Platform Module (TPM) onto your motherboard, follow the steps below.

1. Locate the 20-pin male JTPM1 connector on the motherboard (see the image below). If the board does not have this connector, then it does not support the TPM.
2. Using the white connection on the TPM and the blank space on JTPM1 as a reference, orient and align your TPM with the connector. Installing the TPM with the incorrect orientation may cause damage to the module and the motherboard.
3. Carefully insert the TPM into the connector on the motherboard, taking care not to damage the pins.

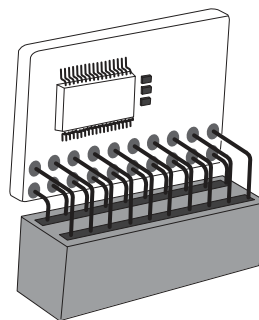


Note: The above picture is an example of JTPM1. Your JTPM1 connector may be in a different location, or oriented differently. Please consult your motherboard user manual for more information.

 **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 two images below for the correct orientation.



Horizontal TPM



Vertical TPM

4. After you have installed the TPM 2.0, you will need to obtain the Intel Provisioning Utility by contacting Supermicro technical support. Install the Intel Provisioning Utility onto a USB device and connect it to a compatible USB port on your motherboard.

3.2 Configuring the TPM 2.0 and Intel TXT for the Server

There are three steps involved in using the TPM 2.0. They are:

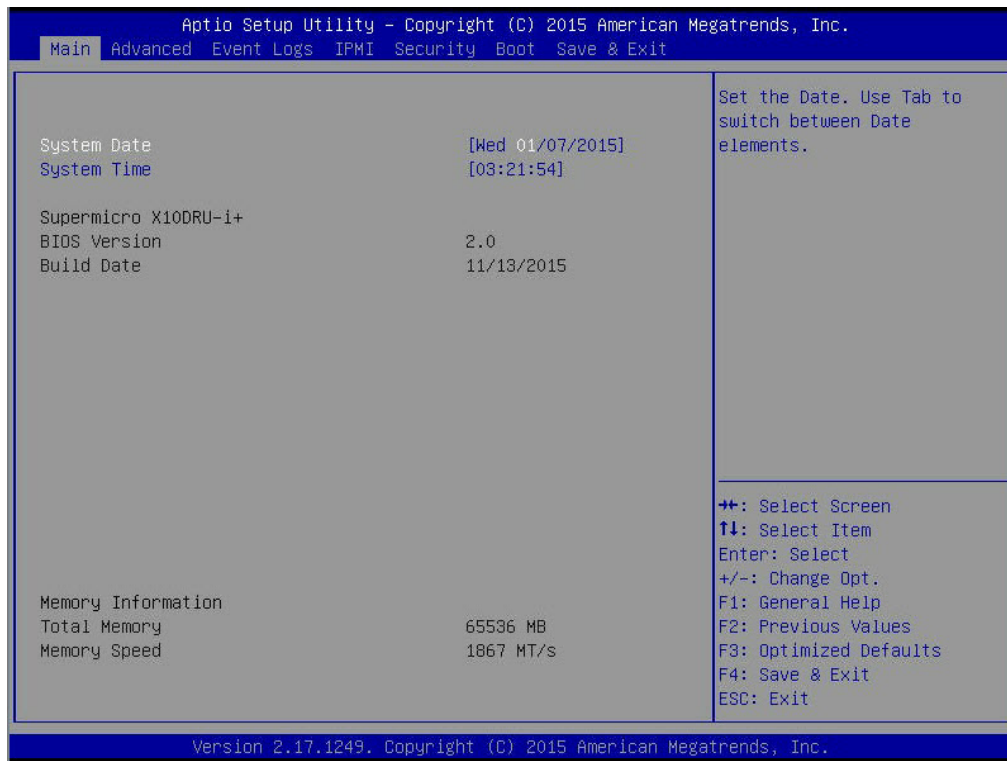
1. Enable TPM 2.0 in the BIOS
2. Provision Intel TXT in the UEFI shell
3. Enable TXT Support in the BIOS and UEFI shell

A. Enabling TPM 2.0 in the BIOS

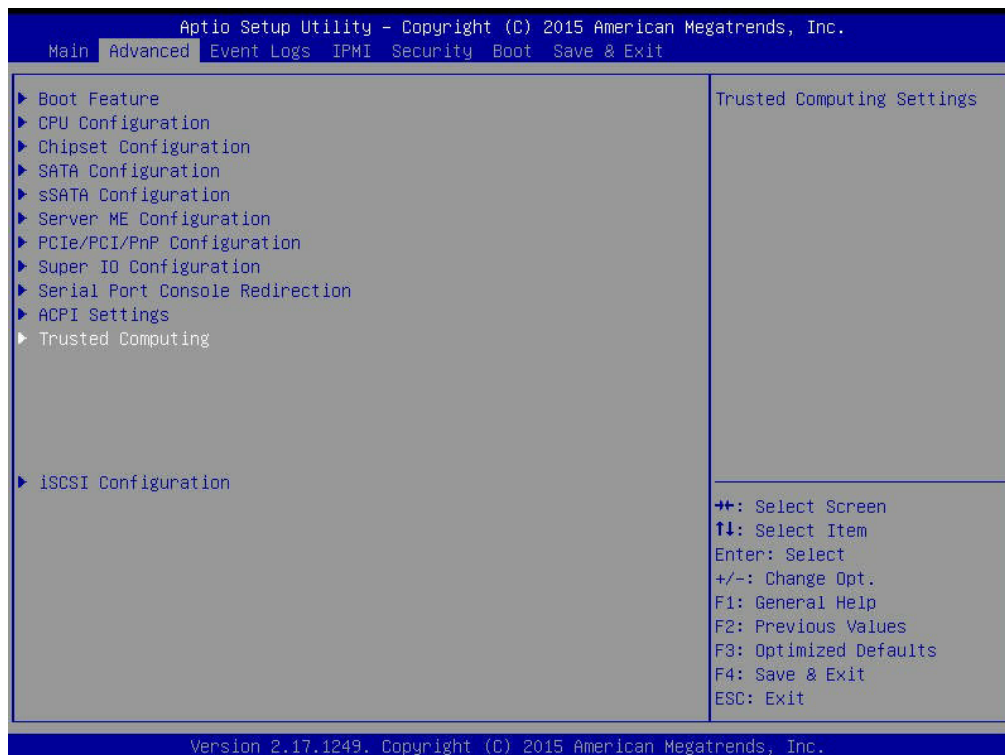
1. Start your computer. When it reaches the POST screen, press the <Delete> key continuously to reach the BIOS.



2. Your computer will boot into the BIOS (and you may stop pressing the Delete key).

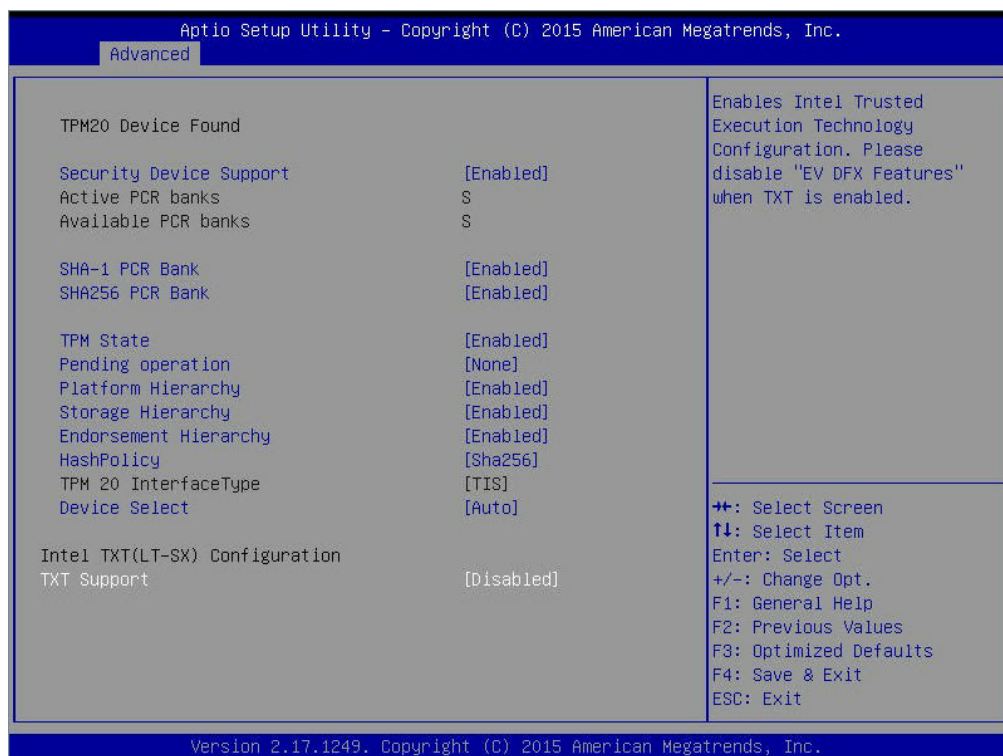
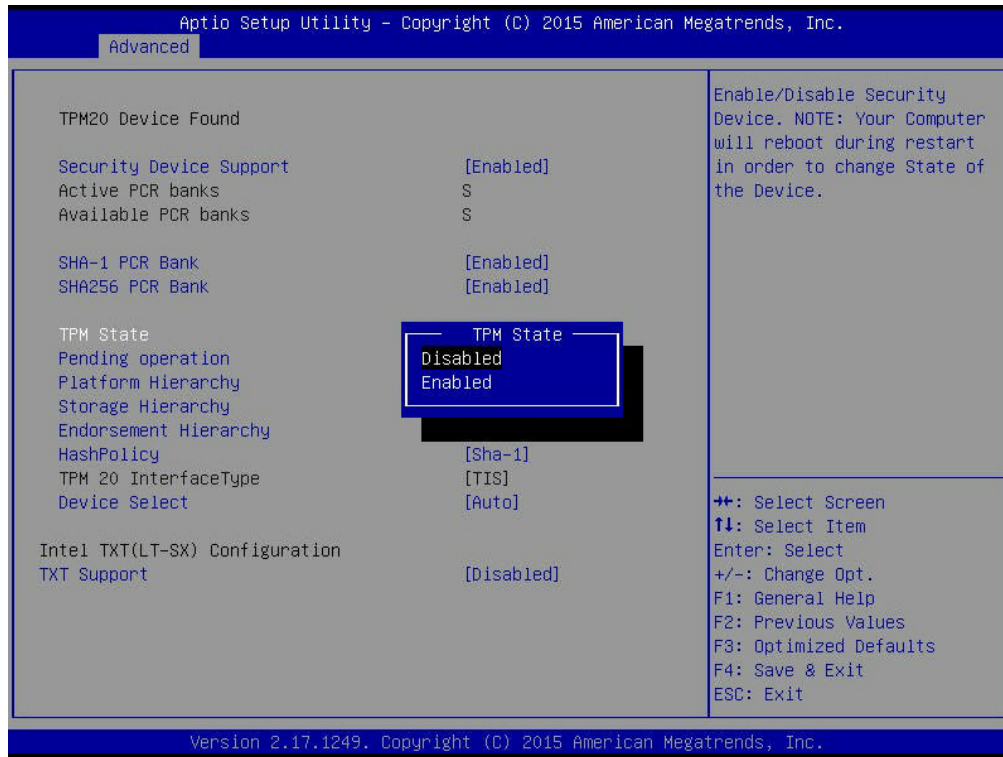


3. Using the arrow keys on your keyboard, toggle to the **Advanced** tab. Again using the arrow keys, select the **Trusted Computing** option. Press the <Enter> key.



- You will need to enable all **[Disabled]** options except for **TXT Support**. Using the arrow keys, select each option, press the <Enter> key, select **Enabled**, and press the <Enter> key again.

 **Note:** The Disabled options are TPM State, Platform Hierarchy, Storage Hierarchy, and Endorsement Hierarchy.





- Use the arrow keys to select **UEFI: Built-in EFI Shell** and press the **<Enter>** key.

B. Provisioning Intel TXT (Server)

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.
- Each USB device has its own code (circled in red in the picture below). Type the code for the USB device that you want to use into the command line at the bottom of the screen (outlined in green), then press the **<Enter>** key.



Note: The device used for the purposes of this user guide had a code of fs5. Replace this code with the code that corresponds to your device.

```

9,0x40,0x1FC0)
  blk1 :HardDisk - Alias hd30a65535a2 fs1
          PciRoot(0x0)/Pci(0x11,0x4)/Sata(0x0,0xFFFF,0x0)/HD(2,GPT,AF833ADD-8312-4D4B-B756-21719A9702B
3,0x6C2000,0x7FF800)
  blk2 :HardDisk - Alias hd30a65535a5 fs2
          PciRoot(0x0)/Pci(0x11,0x4)/Sata(0x0,0xFFFF,0x0)/HD(5,GPT,01A8DF67-DB2C-4EC2-970D-22FE8691EFE
2,0x2020,0x7CFE0)
  blk3 :HardDisk - Alias hd30a65535a6 fs3
          PciRoot(0x0)/Pci(0x11,0x4)/Sata(0x0,0xFFFF,0x0)/HD(6,GPT,84D9777E-9B77-4E74-A0AB-CB46285BBE0
3,0x7F020,0x7CFE0)
  blk4 :HardDisk - Alias hd30a65535a8 fs4
          PciRoot(0x0)/Pci(0x11,0x4)/Sata(0x0,0xFFFF,0x0)/HD(8,GPT,23A51B14-307B-496F-AE71-F07A924E0E3
9,0x133020,0x8EFE0)
  blk5 :Removable HardDisk - Alias hd36a0c0b fs5
          PciRoot(0x0)/Pci(0x1A,0x0)/USB(0x0,0x0)/USB(0x2,0x0)/HD(1,MBR,0x0051F21C,0x3F,0x3B9A7C1)
  blk6 :HardDisk - Alias (null)
          PciRoot(0x0)/Pci(0x11,0x4)/Sata(0x0,0xFFFF,0x0)/HD(3,GPT,4436988A-C55F-43D5-8275-A113B90259A
0,0xEC1800,0xE7F4708F)
  blk7 :HardDisk - Alias (null)
          PciRoot(0x0)/Pci(0x11,0x4)/Sata(0x0,0xFFFF,0x0)/HD(7,GPT,05BC07E5-C100-4614-9DD2-C033E0B9C7C
0,0xFC020,0x36FE0)
  blk8 :HardDisk - Alias (null)
          PciRoot(0x0)/Pci(0x11,0x4)/Sata(0x0,0xFFFF,0x0)/HD(9,GPT,965CDC9B-33ED-4411-92AC-A3852F3604F
B,0x1C2000,0x500000)
  blk9 :BlockDevice - Alias (null)
          PciRoot(0x0)/Pci(0x11,0x4)/Sata(0x0,0xFFFF,0x0)
  blkA :Removable BlockDevice - Alias (null)
          PciRoot(0x0)/Pci(0x1A,0x0)/USB(0x0,0x0)/USB(0x2,0x0)

Press ESC in 1 seconds to skip startup.nsh, any other key to continue.
Shell> _

```

3. The provisioning process is complete. In the command line at the bottom of the screen, type **tpm2txtprov.nsh sha256 example** and press the <Enter> key.

```

07/15/15 01:10p      273,088  TPM2ProvTool.efi
05/11/15 10:36a       8,473  Tpm2SgxiProv.nsh
09/01/15 12:07p      15,269  Tpm2TxtProv.nsh
05/21/15 12:47p      15,041  Tpm2TxtProv.nsh.bak
12/14/14 04:22p       1,000  UnDefineSpaceSpecial.pDef
09/01/15 12:00p      21,122  Tpm2PpiProv.log
01/07/15 02:20a      10,344  Tpm2Prov.cfg
09/01/15 12:00p      22,872  Tpm2SgxProv.log
01/07/15 02:20a      43,974  Tpm2TxtProv.log
    146 File(s)    1,297,891 bytes
     2 Dir(s)

fs5:\TPM2ProvTool\TPM2 Prov Tool> Tpm2TxtProv.nsh sha256 example
Tpm2TxtProv.nsh> 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
**** 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 *****
*****

fs5:\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.

```
07/15/15 01:10p      278,088  TPM2ProvTool.efi
05/11/15 10:36a       8,473  Tpm2SgxiProv.nsh
09/01/15 12:07p      15,269  Tpm2TxtProv.nsh
05/21/15 12:47p      15,041  Tpm2TxtProv.nsh.bak
12/14/14 04:22p       1,000  UnDefineSpaceSpecial.pDef
09/01/15 12:00p      21,122  Tpm2PpiProv.log
01/07/15 02:20a      10,344  Tpm2Prov.cfg
09/01/15 12:00p      22,872  Tpm2SgxProv.log
01/07/15 02:20a      48,974  Tpm2TxtProv.log
    146 File(s)    1,297,891 bytes
     2 Dir(s)

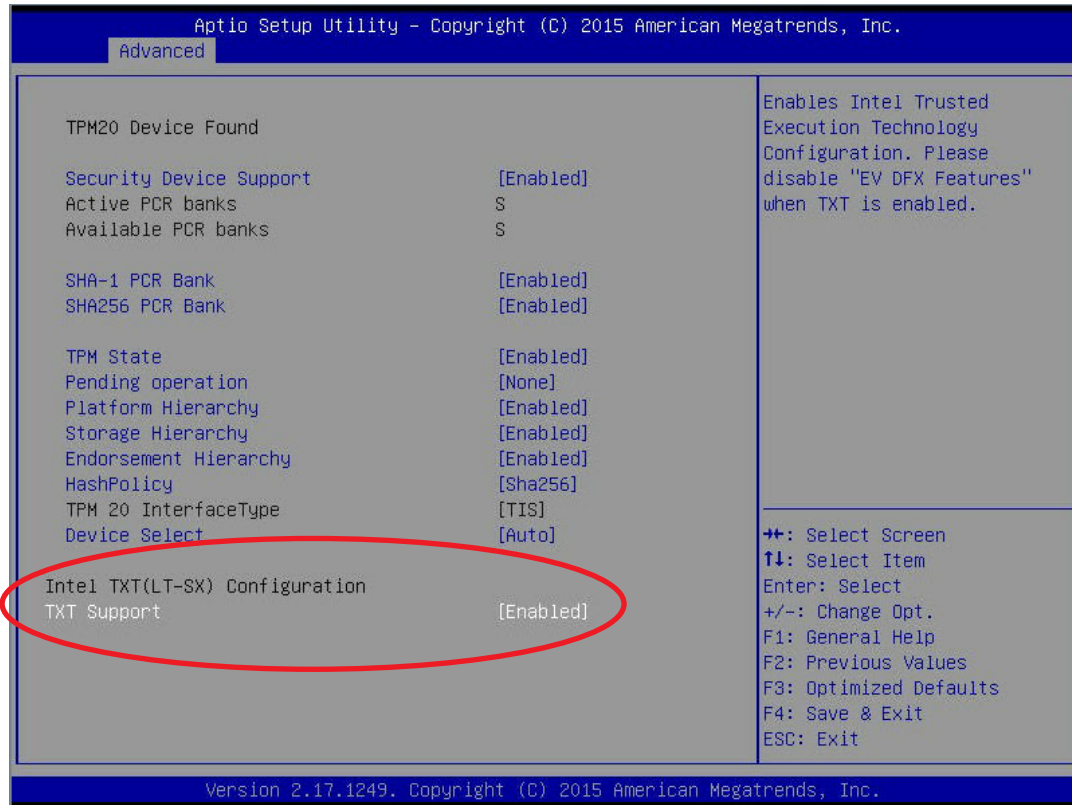
fs5:\TPM2ProvTool\TPM2 Prov Tool> Tpm2TxtProv.nsh sha256 example
Tpm2TxtProv.nsh> echo -OFF
***** Provisioning NV Indexes *****
If PlatformAuth is not EMPTY, then first run ResetPlatformAuth.nsh sha256 example
**** Start PW Session for PlatformAuth & Index Read Auth
***** Provisioning PS Index *****
**** Checking if PS Index exists
**** 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 *****
*****

fs5:\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 **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.efi -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[SENDER] 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.

```
fs5:\Grantley_Refresh\TXT> getsec64.efi -l sexit
*****
GETSEC64 v1.3.4
Built: Mar 10 2014 13:11:58
Intel Corporation
Copyright (c) 2010-2014
*****
GETSEC[SEXIT] complete. System has exited TXT Environment.

fs5:\Grantley_Refresh\TXT> _
```

3.3 Provisioning the TPM 2.0 and TXT Support for the Client

Follow the instructions below to provision the TPM 2.0 for the client. This procedure can currently only be done on Supermicro X11 uniprocessor motherboards.

There are six steps involved in provisioning the TPM 2.0 for the client side. They are:

1. Clear the CMOS on the motherboard
2. Obtain the provisioning utility and connect it to your system
3. Disable PH Randomizations and TXT Support in the BIOS
4. Provision TXT Support in the UEFI shell
5. Enable PH Randomizations and TXT Support in the BIOS
6. Enable TXT Support in the UEFI shell

A. Clear the CMOS on the Motherboard

Before performing the client provisioning process, you will need to clear the CMOS on your motherboard. Refer to the motherboard user manual for your particular motherboard for instructions on how to perform this process.

B. Provisioning Utility

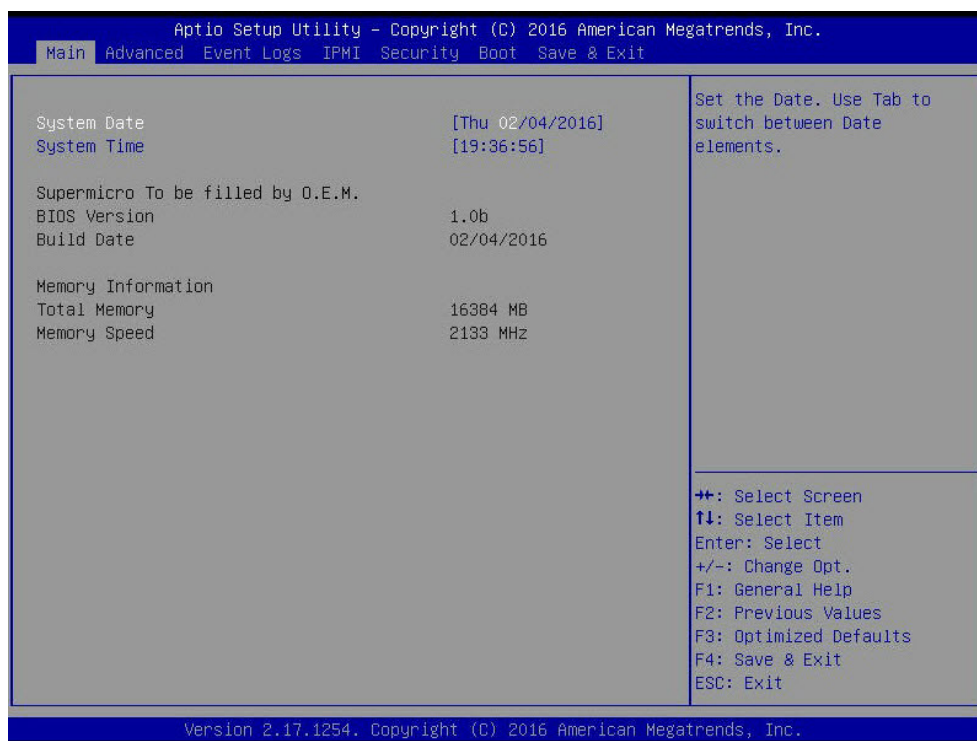
In order to perform the client provisioning, you will need to contact Supermicro support to obtain the provisioning utility. Upload it to a USB flash drive and connect the flash drive to the system you will be provisioning.

C. Disabling PH Randomizations and TXT Support in the BIOS

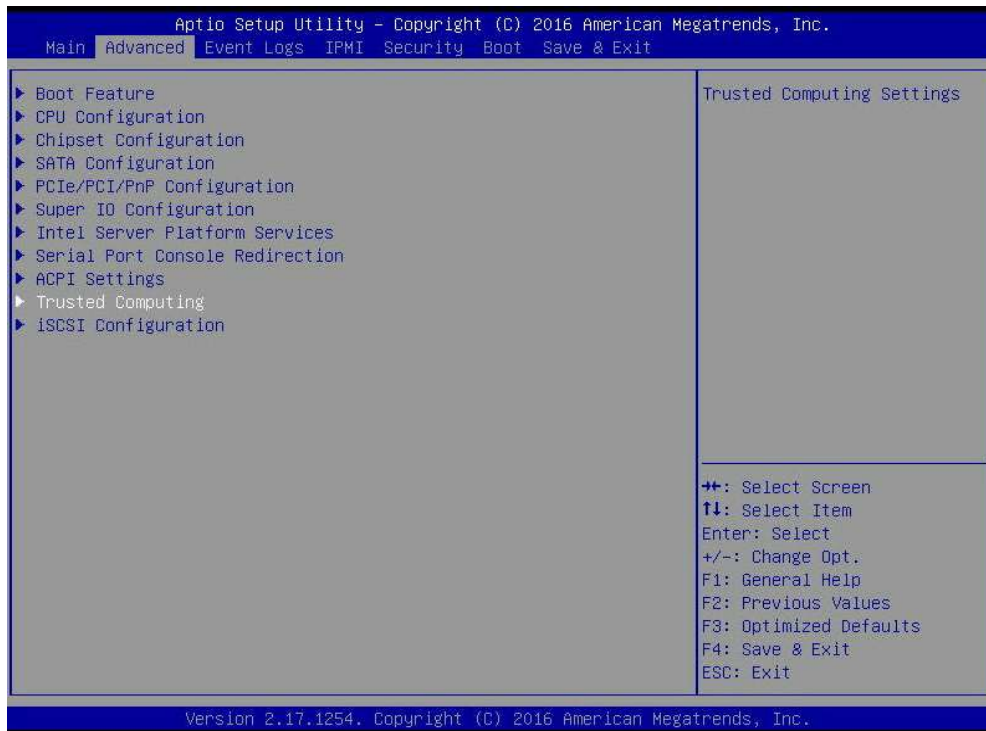
1. Start your system. When it reaches the POST screen, press the <Delete> key continuously to reach the BIOS.



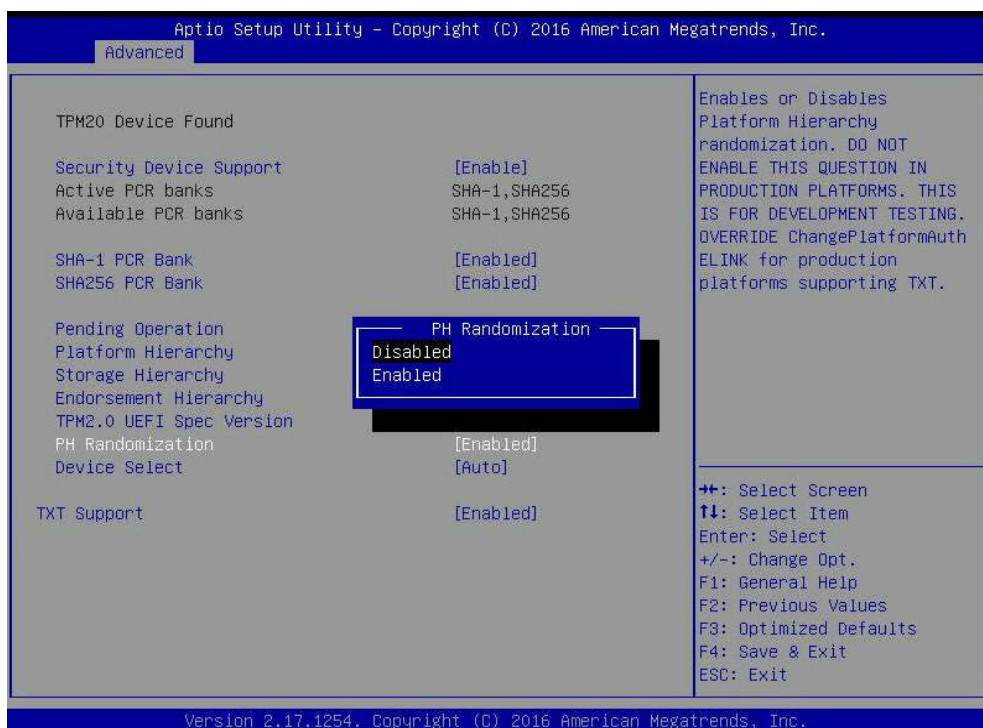
2. Your computer will boot into the BIOS (and you may stop pressing the Delete key)

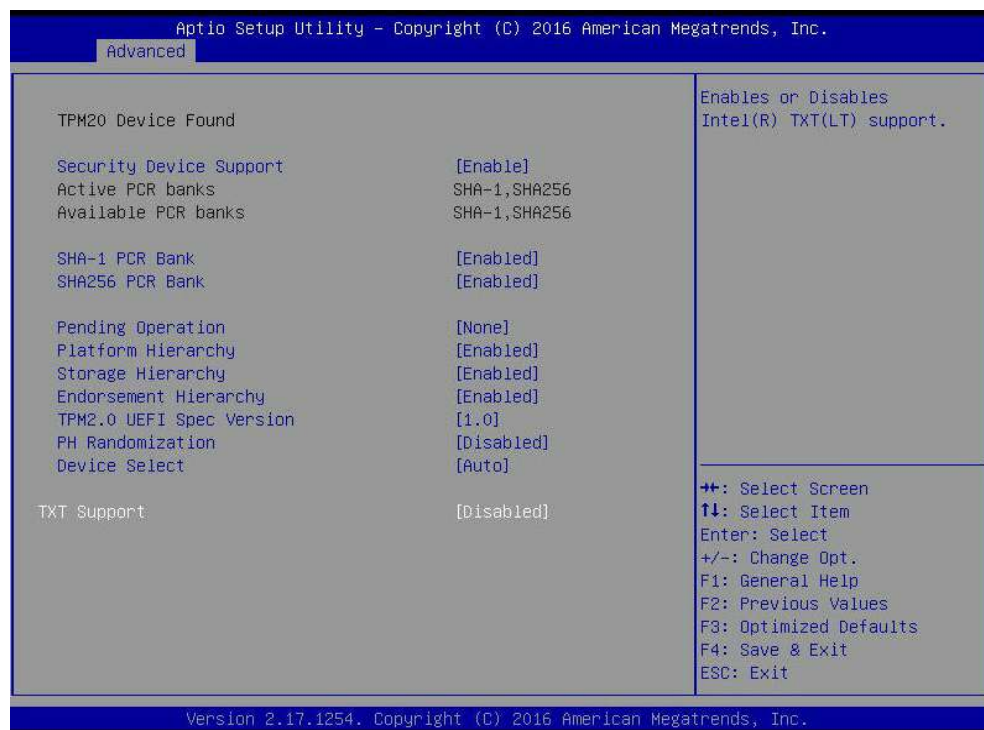


3. Using the arrow keys on your keyboard, toggle to the **Advanced** tab. Again using the arrow keys, select the **Trusted Computing** option. Press the <Enter> key.

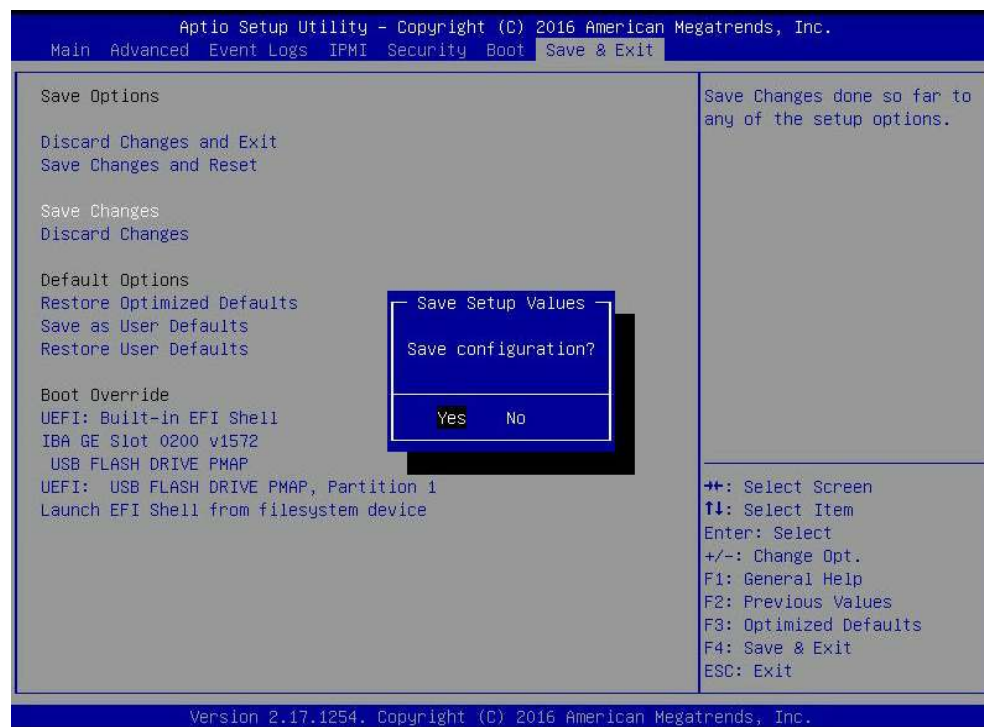


4. **PH Randomizations** and **TXT Support** are enabled. You will need to disable them. Using the arrow keys, select PH Randomizations, press the <Enter> key, use the arrow keys to select **Disabled**, and press the <Enter> key again. Do the same for TXT Support.

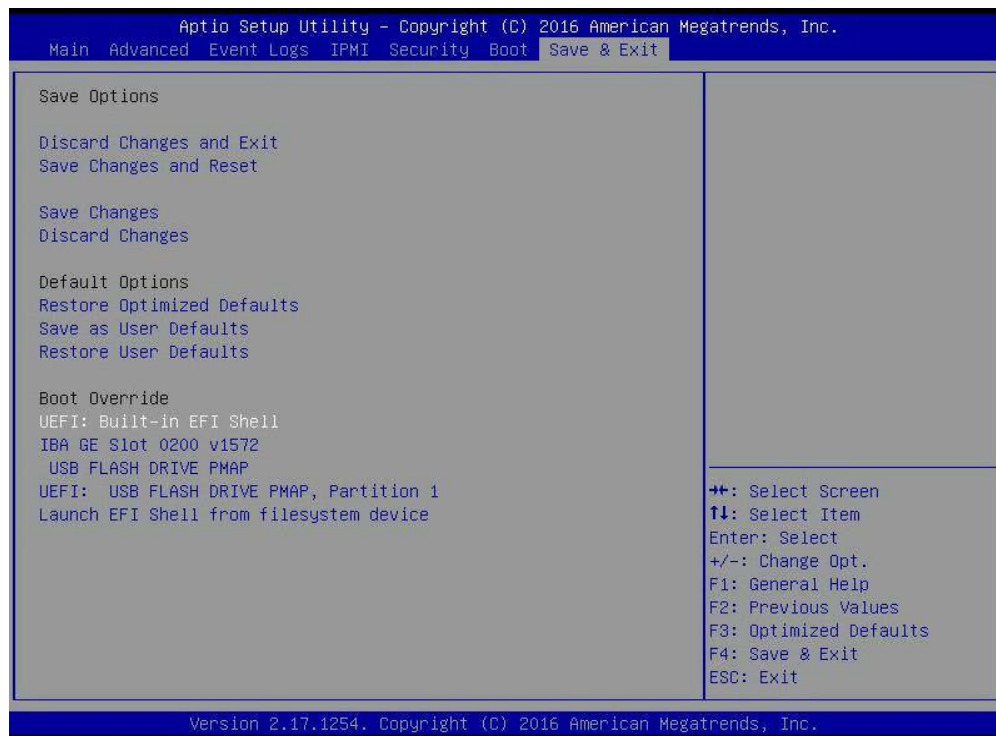




5. Press the <Esc> key to return to the main Advanced tab. Toggle to the **Save & Exit** tab. Select **Save Changes** and press the <Enter> key. You will be asked if you want to save the configuration. Select **Yes** and press the <Enter> key.



6. You will need to go into the UEFI shell and provision TXT Support. Select **UEFI: Built-in EFI Shell** and press the <Enter> key.



D. Provisioning TXT Support in the UEFI Shell

Once you have selected UEFI: Built-in EFI Shell in the BIOS, the system will boot into the **United Extensible Firmware Interface (UEFI)** with a list of available USB devices.

1. Each USB device has its own code (circled in red in the picture below). Type the code for the USB device that you want to use into the command line at the bottom of the screen (outlined in green), 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.

```
EFI Shell version 2.40 [5.11]
Current running mode 1.1.2
Device mapping table
fs0 :Removable HardDisk - Alias hd5e0b blk0
    PciRoot(0x0)/Pci(0x14,0x0)/USB(0x4,0x0)/HD(1,MBR,0x000C3DCA,0x3F,0x1EBFC1)
blk0 :Removable HardDisk - Alias hd5e0b fs0
    PciRoot(0x0)/Pci(0x14,0x0)/USB(0x4,0x0)/HD(1,MBR,0x000C3DCA,0x3F,0x1EBFC1)
blk1 :Removable BlockDevice - Alias (null)
    PciRoot(0x0)/Pci(0x14,0x0)/USB(0x4,0x0)

Press ESC in 1 seconds to skip startup.nsh, any other key to continue.
Shell> fs0: _
```

2. You will need to access the package that contains the provisioning utility. In the command line, type **CD** and the name of the utility. Press the <Enter> key. Then type **CD Provision_ALL_PS2**. Press the <Enter> key.



Note: The name of the utility may vary. For the purposes of this documentation, the utility used was named **TPM2_X11UP**.

```
EFI Shell version 2.40 [5.11]
Current running mode 1.1.2
Device mapping table
fs0 :Removable HardDisk - Alias hd5e0b blk0
    PciRoot(0x0)/Pci(0x14,0x0)/USB(0x4,0x0)/HD(1,MBR,0x000C3DCA,0x3F,0x1EBFC1)
blk0 :Removable HardDisk - Alias hd5e0b fs0
    PciRoot(0x0)/Pci(0x14,0x0)/USB(0x4,0x0)/HD(1,MBR,0x000C3DCA,0x3F,0x1EBFC1)
blk1 :Removable BlockDevice - Alias (null)
    PciRoot(0x0)/Pci(0x14,0x0)/USB(0x4,0x0)

Press ESC in 1 seconds to skip startup.nsh, any other key to continue.
Shell> fs0:

fs0:\> CD TPM2_X11UP

fs0:\TPM2_X11UP> CD Provision_ALL_PS2
```

3. Type **Define_AUX.nsh** and press the <Enter> key. Wait for the scripts to stop running and a line of yellow text to appear.

```
fs0:\TPM2_X11UP\Provision_ALL_PS2> Define_AUX.nsh
Define_AUX.nsh> echo -off
Reset Platform Auth
**** Start Policy Session for PlatformPolicy
Satisfy PlatformPolicy
**** Policy OR (0, PhSecretSHA256)
**** PH HierarchyChangeAuth
Did not satisfy PlatformPolicy
removing fs0:\TPM2_X11UP\Provision_ALL_PS2\Tpm2Prov.cfg
- [ok]
copying fs0:\TPM2_X11UP\Provision_ALL_PS2\Tpm2Prov_.cfg -> fs0:\TPM2_X11UP\Provision_ALL_PS2\Tpm2Prov.cfg
- [ok]
Creating Aux Index ...
Clearing AUXDeletionControl flag in PS Policy
Start Policy Session
Policy OR (Branch A, Branch B, Branch C)
Writing PS Policy to clear AUXDeletionControl flag
Flush Session 0
AUX Define
```

4. Type **Define_PS.nsh** and press the <Enter> key. Wait for the scripts to stop running and a line of yellow text to appear.

```
fs0:\TPM2_X11UP\Provision_ALL_PS2> Define_PS.nsh
Define_PS.nsh> echo -off
Reset Platform Auth
**** Start Policy Session for PlatformPolicy
Satisfy PlatformPolicy
**** Policy OR (0, PhSecretSHA256)
**** PH HierarchyChangeAuth
Did not satisfy PlatformPolicy
removing fs0:\TPM2_X11UP\Provision_ALL_PS2\Tpm2Prov.cfg
- [ok]
copying fs0:\TPM2_X11UP\Provision_ALL_PS2\Tpm2Prov_.cfg -> fs0:\TPM2_X11UP\Provision_ALL_PS2\Tpm2Prov.cfg
- [ok]
Start Policy Session
Policy Command Code (0, TPM_CC_NV_UndefineSpaceSpecial)
Policy OR (Branch A, Branch B, Branch C)
UndefineSpecial PS_Def.iDef
PS Define
Flush Session 0
Writing PS Policy
Start Policy Session
Policy OR (Branch A, Branch B, Branch C)
Writing NV Data
Flush Session 0
```

5. Type **Define_SGX.nsh** and press the <Enter> key. Wait for the scripts to stop running and a line of yellow text to appear.

```
fs0:\TPM2_X11UP\Provision_ALL_PS2> Define_SGX.nsh
Define_SGX.nsh> echo -off
Reset Platform Auth
**** Start Policy Session for PlatformPolicy
Satisfy PlatformPolicy
**** Policy OR (0, PhSecretSHA256)
**** PH HierarchyChangeAuth
Did not satisfy PlatformPolicy
removing fs0:\TPM2_X11UP\Provision_ALL_PS2\Tpm2Prov.cfg
- [ok]
copying fs0:\TPM2_X11UP\Provision_ALL_PS2\Tpm2Prov_.cfg -> fs0:\TPM2_X11UP\Provision_ALL_PS2\Tpm2Prov.cfg
- [ok]
Start Policy Session
Policy Command Code (0, TPM_CC_NV_UndefineSpaceSpecial)
Policy OR (Branch A, Branch B, Branch C)
UndefineSpecial SGX_Def.iDef
SGX Define
Writing NV Data
Flush Session 0
```



Note: This step may take a few minutes to process.

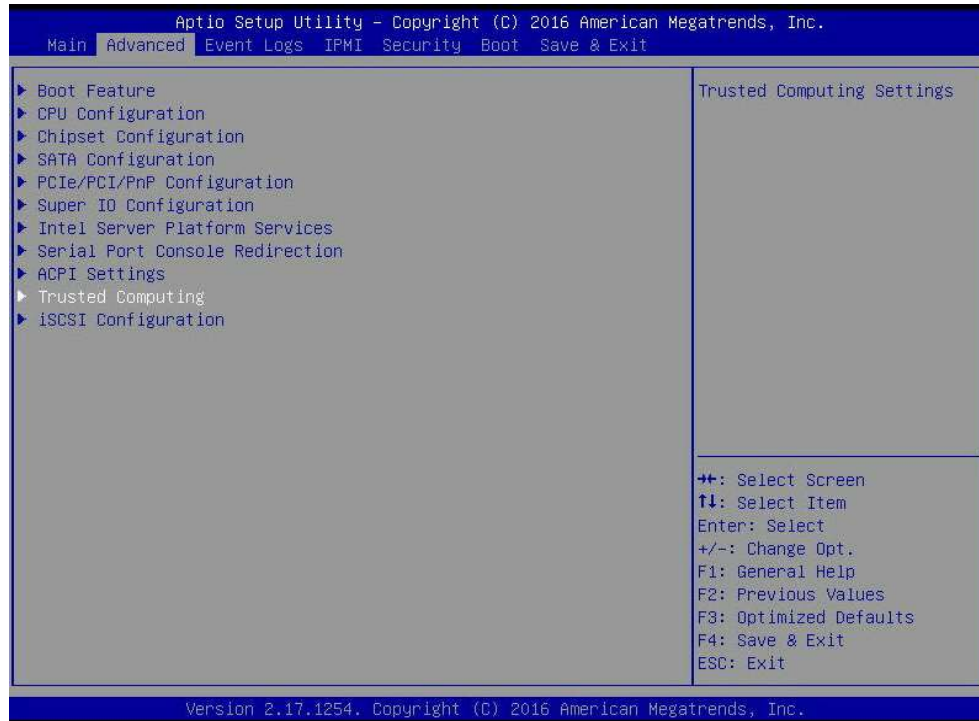
6. Type **Lock_PS2.nsh**. Press the <Enter> key. Wait for the scripts to stop running and a line of yellow text to appear.

```
fs0:\TPM2_X11UP\Provision_ALL_PS2> Lock_PS2.nsh
Lock_PS2.nsh> echo -off
Reset Platform Auth
**** Start Policy Session for PlatformPolicy
Satisfy PlatformPolicy
**** Policy OR (0, PhSecretSHA256)
**** PH HierarchyChangeAuth
Did not satisfy PlatformPolicy
removing fs0:\TPM2_X11UP\Provision_ALL_PS2\Tpm2Prov.cfg
- [ok]
copying fs0:\TPM2_X11UP\Provision_ALL_PS2\Tpm2Prov_.cfg -> fs0:\TPM2_X11UP\Provision_ALL_PS2\Tpm2Prov.cfg
- [ok]
Lock PS (for PS2 index only)
```

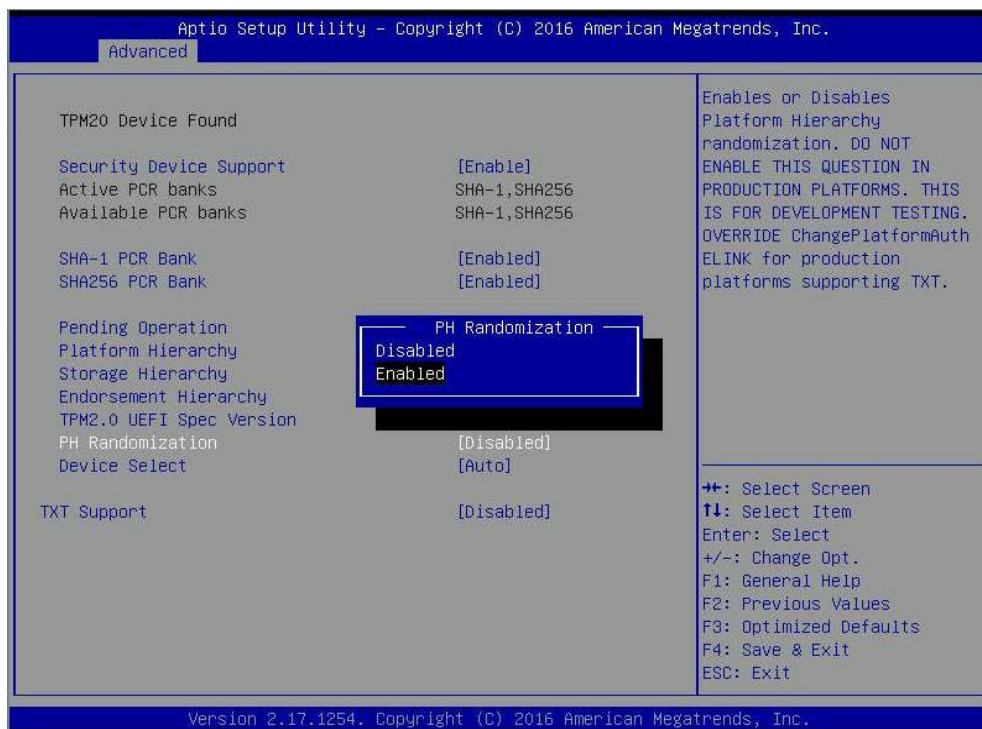
7. The provisioning process for TXT Support is complete. You will need to return to the BIOS and enable PH Randomizations and TXT Support. Type **exit** and press the <Enter> key. You will be brought back to the BIOS.

E. Enabling PH Randomizations and TXT Support in the BIOS

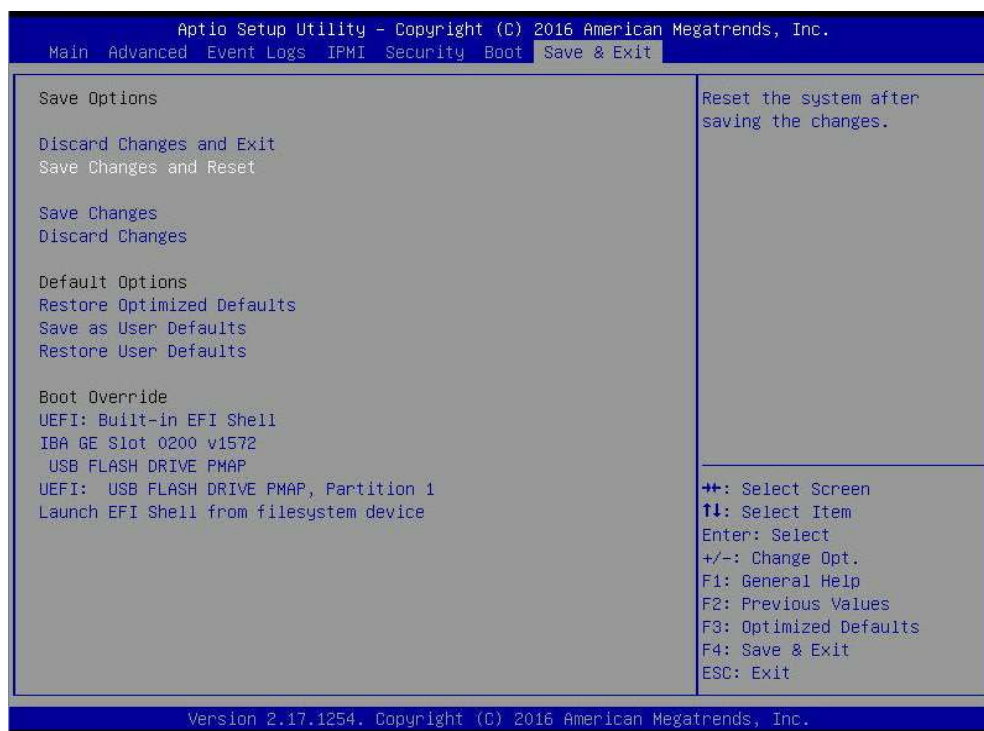
1. When you return to the BIOS after provisioning TXT Support in the UEFI shell, you will be brought back to the Save & Exit tab. Toggle to the Advanced tab and select Trusted Computing. Press the <Enter> key.



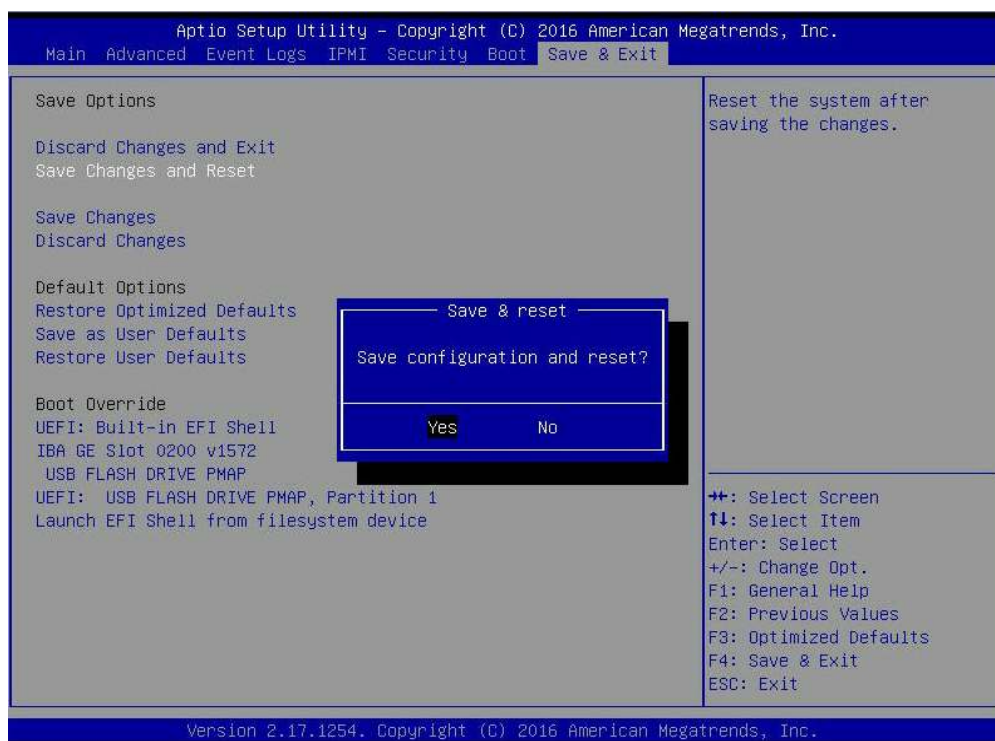
2. Select **PH Randomization**, press the <Enter> key, select **Enabled**, and press the <Enter> key again. Do the same for TXT Support.



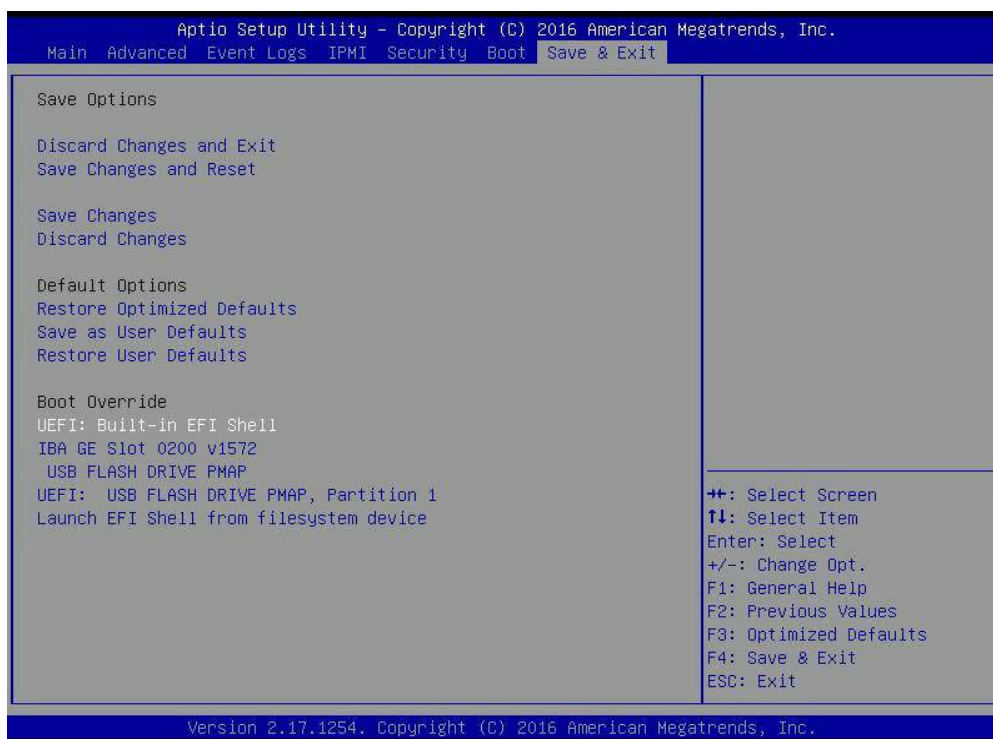
- Press the <Esc> key to return to the main Advanced tab. Toggle back to the Save & Exit tab.
- Select **Save Changes and Reset**. Press the <Enter> key.



- You will be asked if you want to save the configuration and reset. Select **Yes** and press the <Enter> key.



6. The BIOS portion of the provisioning process is complete. You will need to return to the UEFI shell and enable TXT Support. Select **UEFI: Built-in EFI Shell** and press the <Enter> key.



F. Enabling TXT Support in the UEFI Shell

1. When you return to the UEFI shell, you will need to go back and follow steps 1 through 3 of **Section 3.3 D: Provisioning TXT Support in the UEFI Shell**. Once you have done that, type **getsec64.efi -l sen** in the command line. Press the <Enter> key. The TPM 2.0 is now enabled for the client.

```
fs0:\TPM2_X11UP\Provision_ALL_PS2> getsec64.efi -l sen
*****
GETSEC64 v1.3.15
Built: Jan 27 2015 16:44:20
Intel Corporation
Copyright (c) 2010-2015
*****
GETSEC[SENDER] complete. System is now in TXT Environment.
```

2. Verify that there were no errors. If there were not, type **getsec64.efi -l SEXIT** in the command line. Press the <Enter> key to exit the UEFI shell.

```
fs0:\TPM2_X11UP\Provision_ALL_PS2> getsec64.efi -l sen
*****
GETSEC64 v1.3.15
Built: Jan 27 2015 16:44:20
Intel Corporation
Copyright (c) 2010-2015
*****
GETSEC[SENDER] complete. System is now in TXT Environment.

fs0:\TPM2_X11UP\Provision_ALL_PS2> getsec64.efi -l SEXIT
*****
GETSEC64 v1.3.15
Built: Jan 27 2015 16:44:20
Intel Corporation
Copyright (c) 2010-2015
*****
GETSEC[SEXIT] complete. System has exited TXT Environment.

fs0:\TPM2_X11UP\Provision_ALL_PS2> _
```