AOM-TPM-9672V
AOM-TPM-9672H
(TPM 2.0)

USER'S MANUAL

Revision 1.0

The information in this user's manual has been carefully reviewed and is believed to be accurate. The manufacturer 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 industrial 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: 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.

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 1.0

Release Date: August 11, 2025

Preface

About This Manual

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).

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.

An Important Note to the User

All graphic images and layout drawings shown in this user's guide are based upon the latest PCB revision available at the time of publishing this user's guide. The add-on card you have received may or may not look exactly the same as the graphics shown in this user's guide.

Returning Merchandise for Service

A receipt or copy of your invoice marked with the date of purchase is required before any warranty service will be rendered. You can obtain service by calling your vendor for a Returned Merchandise Authorization (RMA) number. When returning to the manufacturer, the RMA number should be prominently displayed on the outside of the shipping carton and mailed prepaid or hand-carried. Shipping and handling charges will be applied for all orders that must be mailed when service is complete. For faster service, RMA authorizations may be requested online (http://www.supermicro.com/support/rma/).

This warranty only covers normal consumer use and does not cover damages incurred in shipping or from failure due to the alteration, misuse, abuse, or improper maintenance of products.

During the warranty period, contact your distributor first for any product problems.

Conventions Used in the Manual

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

Warning! Indicates important information given to prevent equipment/property damage or personal injury.

Warning! Indicates high voltage may be encountered while performing a procedure.

Important: Important information given to ensure proper system installation or to relay safety precautions.

Note: Additional information given to differentiate various models or to provide information for proper system setup.

Important Links

For your system to work properly, follow the links to download all necessary drivers/utilities and the user's manual for your server.

- Supermicro product manuals: http://www.supermicro.com/support/manuals/
- Product drivers and utilities: https://www.supermicro.com/wdl/driver
- Product safety info: https://www.supermicro.com/en/about/policies/safety-information
- A secure data deletion tool designed to fully erase all data from storage devices can be found at our website: https://www.supermicro.com/about/policies/disclaimer.cfm?url=/wdl/utility/Lot9_Secure_Data_Deletion_Utility/
- If you have any questions, contact our support team at: support@supermicro.com
- Frequently Asked Questions: https://www.supermicro.com/FAQ/index.php
- If you have any feedback on Supermicro product manuals, contact our writing team at: Techwriterteam@supermicro.com

This manual may be periodically updated without notice. Check the Supermicro website for possible updates to the manual revision level.

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.com (Technical Support) RMA_Europe@supermicro.com (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
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 (TPM9672) is a special add-on module that may be installed onto Supermicro® X11, X12, X13, and X14 dual and single processor motherboards that only support CPU Socket 3674.

Note: TPM9672 can not be installed onto X14DBHM and X14SBHM.

Types of TPMs

Note: TPM module must be provisioned in order to support Intel® Trusted Execution Technology (TXT). Contact Supermicro Technical Support to get more details about the Intel tool.

The TPM-9672 series add-on modules use Trusted Computing Group (TCG) version 2.0 firmware.

The following SKUs are available:

- AOM-TPM-9672V, a vertical TPM module
- AOM-TPM-9672H, 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, which are 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 2.0 Features

The key features of this add-on card include the following.

- SP 800-90B compliance
- SPI interface
- Microcontroller in 0.22/0.09-µm CMOS technology
- Compliant embedded software
- EEPROM for TCG firmware enhancements as well as user data and key support
- Hardware accelerator for SHA-1 SHA-256, and SHA 384 hash algorithm
- True Random Number Generator (TRNG)
- Tick counter with tamper detection
- Protection against dictionary attack
- Infineon's TPM 2.0 is Common Criteria (CC) certified at Evaluation Assurance Level (EAL) 4 Moderate
- General-purpose I/O
- Intel Trusted Execution Technology (TXT) support
- AMD® Secure Virtual Machine Architecture support
- Full personalization with Endorsement Key (EK) and EK certificate
- Power-saving sleep mode
- +3.3 V power supply
- WHQL dual-mode 1.1b and 1.2 TPM Windows Kernel Mode Driver
- Proprietary fan headers
- Serial port headers
- SATADOM power connectors

1.3 Motherboards Supported for TPM

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. These motherboards will come with a specially designated JTPM1 connector on every board, 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, BMC firmware, SAS firmware, and CMM firmware. It is optional, but the TPM is required for it to be provisioned. It will further enhance system security by protecting firmware against malicious attacks on vulnerable areas.

It works by matching hypervisor measures with encryption keys upon system launch. If it 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: Note that this product is sold only as part of an integrated solution with Supermicro server systems.

How the TXT Works

When enabled, the Intel TXT 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 will signal "trusted," and the launch is allowed to proceed.
4. If mismatched: The TXT will signal "untrusted," and the launch is blocked.

Chapter 2

Deploying and Using the TPM 2.0

2.1 Add-On Module Layout

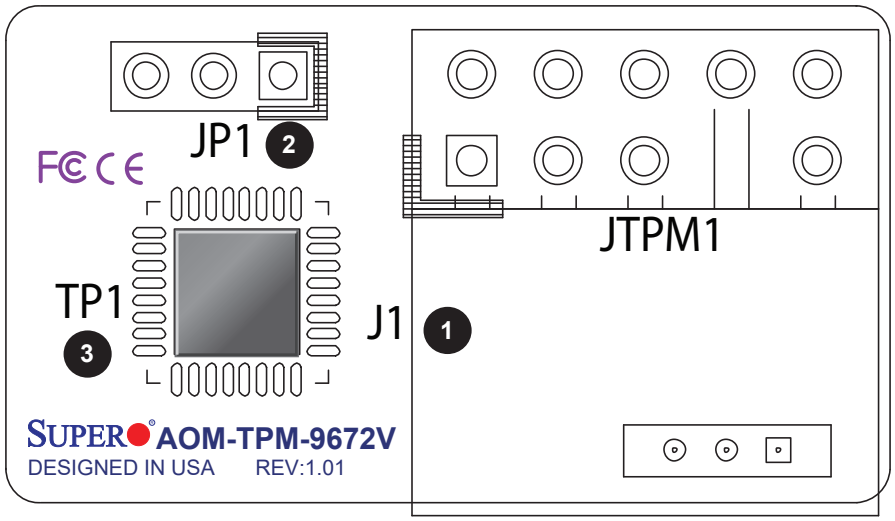

Figure 2-1: AOM-TPM-9672V Layout

2.2 Major Components

The following major components are installed on the AOM-TPM-9672V/H:

AOM-TPM-9672V/H Major Components		
No	**Component Name**	**Definition**
1	J1	LAN/BMC RJ45 Ports
2	JP1	1–2: SMBUS ARP Mode (Default)
		2–3: Static SMBUS Address Mode
3	JTPM1	Trusted Platform Module
4	TP1	Quad Small Form-Factor Pluggable 28 Port 2

2.3 Installing the TPM Onto the Motherboard

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

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.

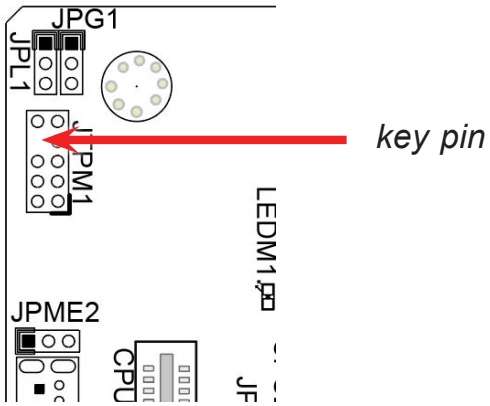

Figure 2-2: Key Pin Location

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 two images for the correct orientation.

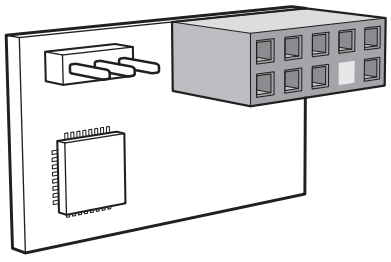

Figure 2-3: Horizontal TPM

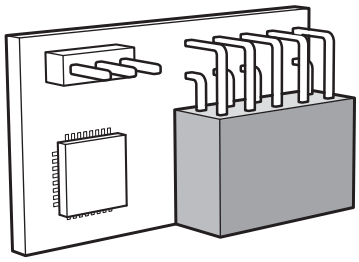

Figure 2-4: Vertical TPM

2.4 Enabling the TPM Through 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, which can also be used to enable TXT support. You will need to "lock" the TPM in the firmware. This is done through the provision utility provided by Intel. Use the arrow keys to highlight your chosen option, and press **<Enter>** to select.

Enabling the TPM in the BIOS

1. Enter the BIOS setup screen. You may do this either from the IPMI remote console or the server directly using KVM.
2. Reboot the system.
3. Press the **<Del>** key as the system boots until you reach the BIOS screen.
4. You will be presented with the BIOS Setup main screen.
5. Navigate to the **Advanced** tab.

6. Navigate down to select the **CPU Configuration**.

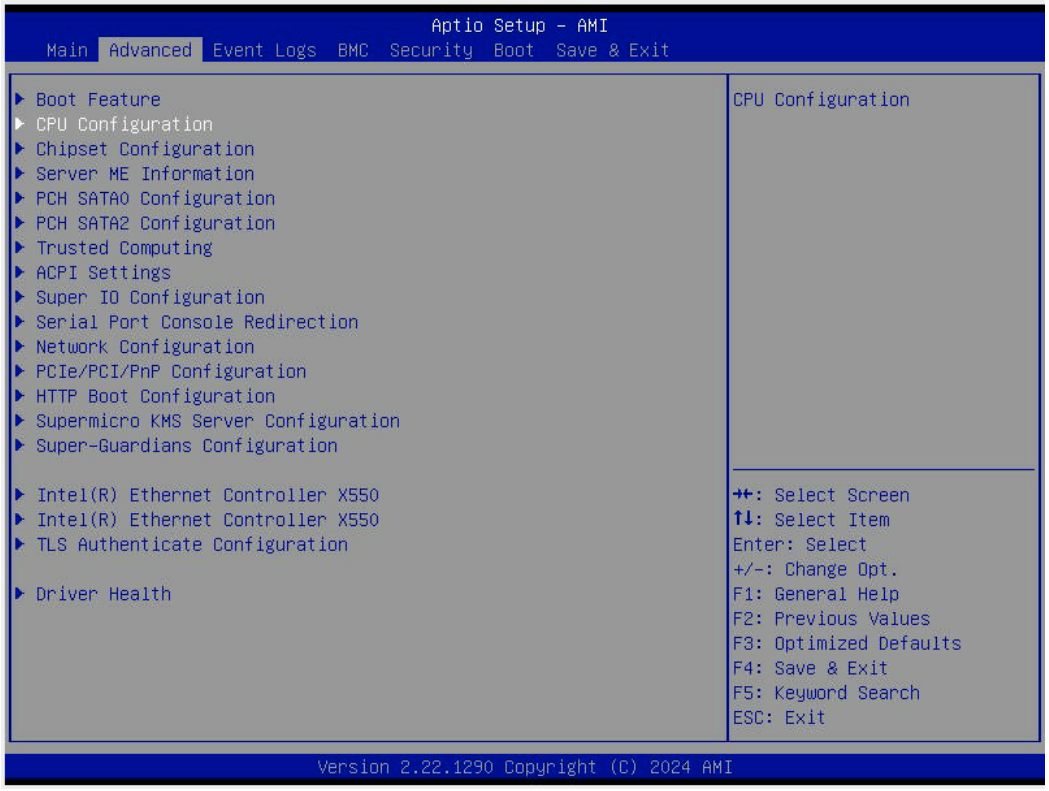

Figure 2-5: CPU Configuration Selected

7. You will then be taken to the CPU Configuration page. Navigate down to the **Intel Virtualization Technology**.

8. If this item is not already enabled, select **Enable**.

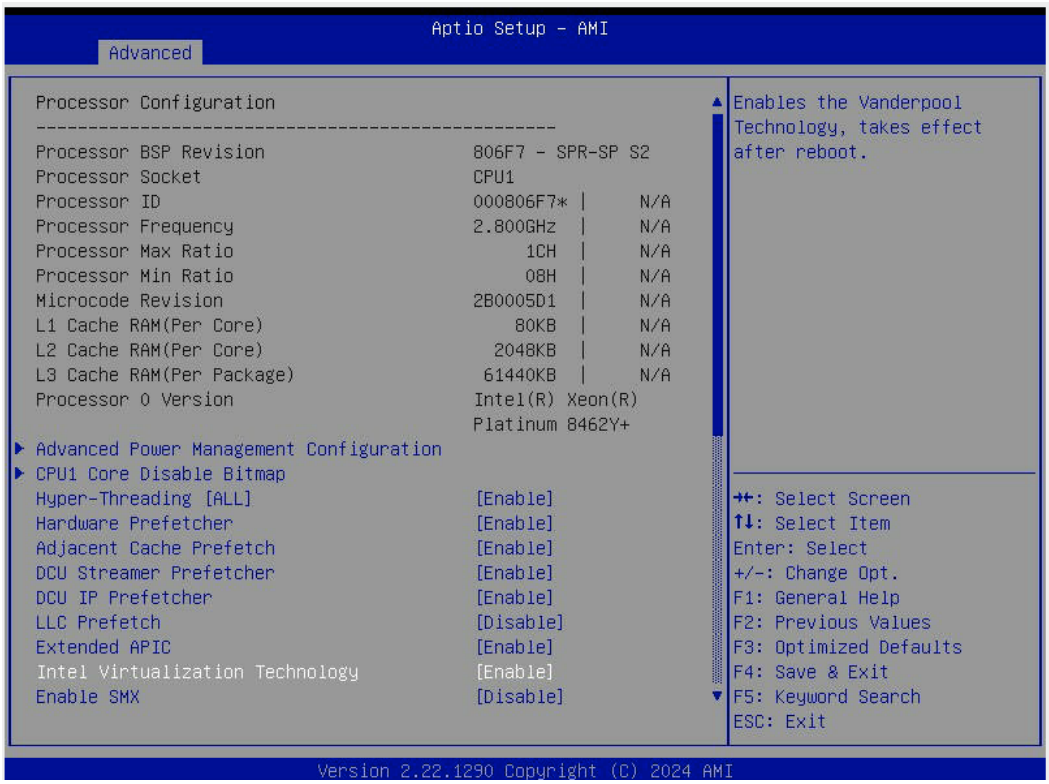

Figure 2-6: Enable Virtualization Technology

9. Once you have enabled virtualization support, press the **<Esc>** key until you are back to the **Advanced** tab.

10. Navigate down to select the **Trusted Computing**.
11. The Trusted Computing window will appear.

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

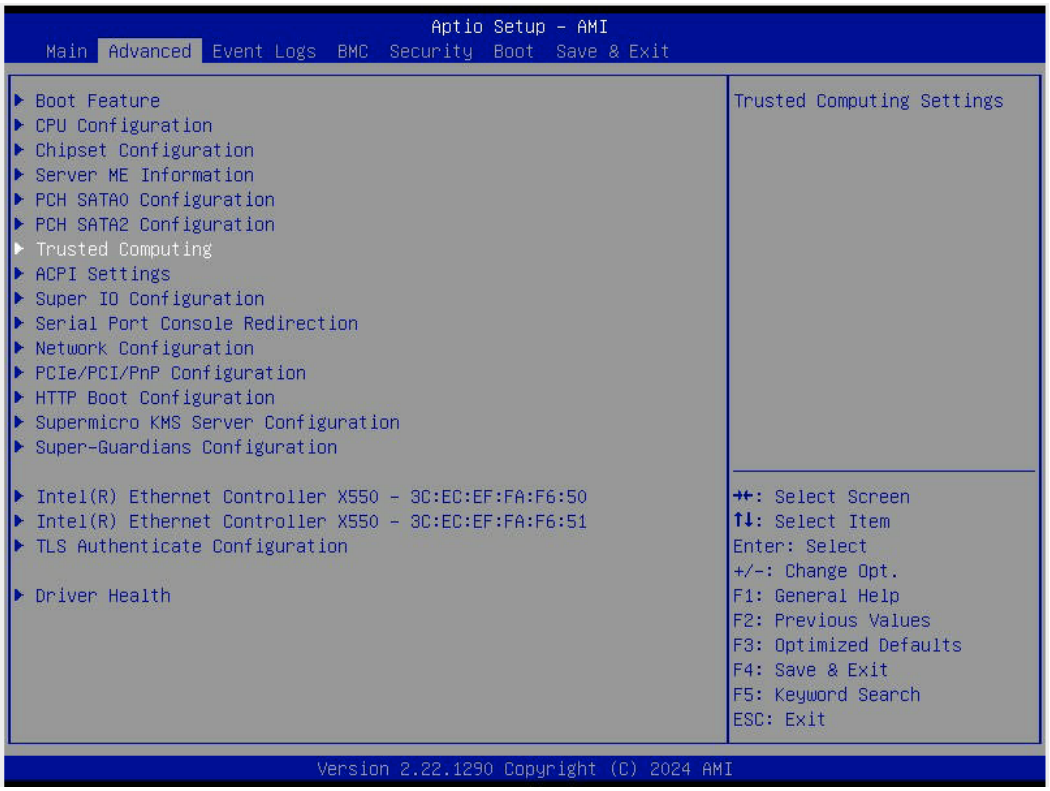

Figure 2-7: Trusted Computing Selected

12. Disable **PH Randomization** and **TXT Support** by selecting each option and selecting **Disabled** on each option menu.

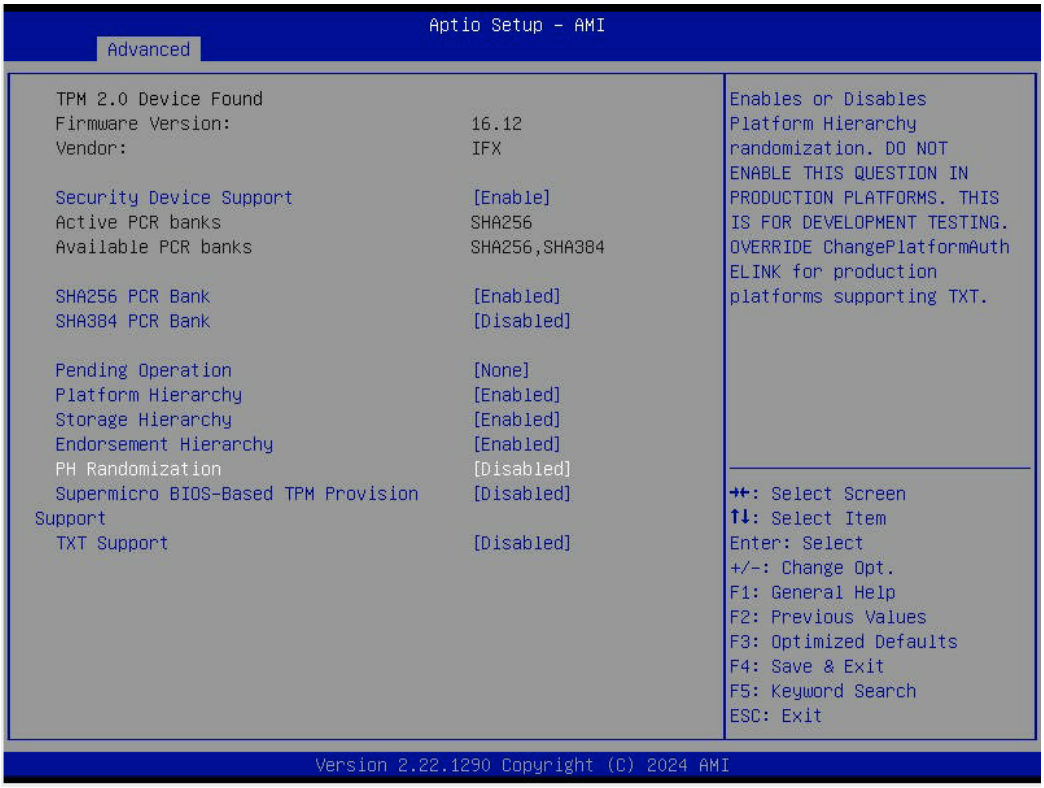

Figure 2-8: PH Randomization and TXT Support Disabled

13. Press the **<Esc>** key to return to the **Advanced** tab options.

14. Navigate to the **Save & Exit** tab.

15. Select **Save Changes**.

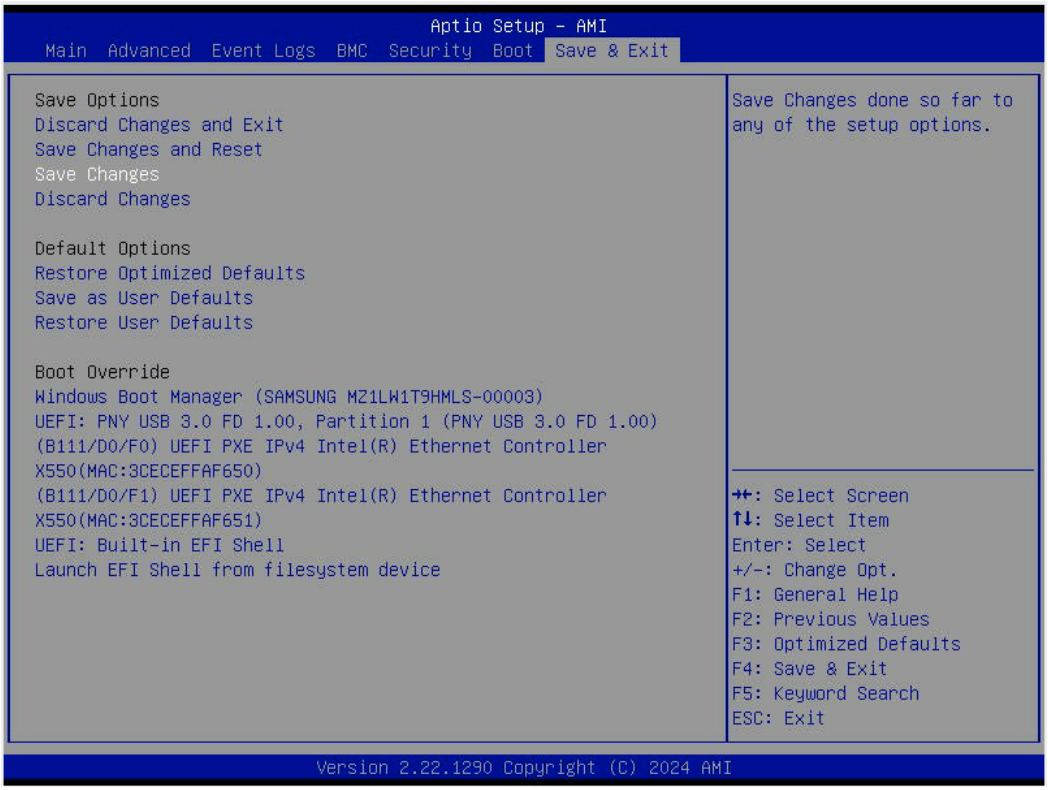

Figure 2-9: Save Changes Selected

16. Select **UEFI: Built-in EFI Shell**.

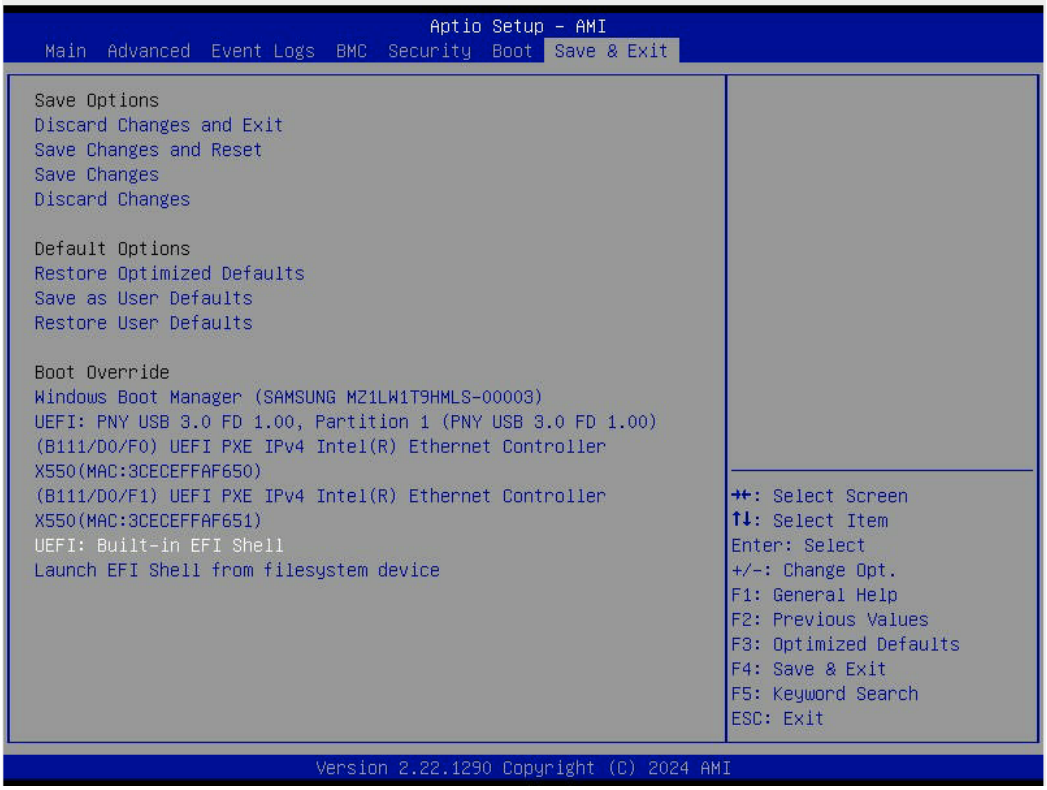

Figure 2-10: UEFI: Built-in EFI Shell Selected

Provisioning Intel TXT (Server)

To provision the Intel TXT server, take the following steps:

Note: If the TPM part number is AOM-TPM-9672H-S or AOM-TPM-9672V-S, you do not need to get the Intel Provisioning Tool. 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 after typing `FS0`:

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

   ii. Type the following command:

   ```
   Tpm2_CBnT_Prov.nsh sha256 example
   ```

   iii. The provisioning process is now completed.

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

Enabling TXT Support

Follow the steps to enable TXT Support in the BIOS and UEFI shell:

1. Once you boot to UEFI-Shell, go to the following directory:

   ```
   Tpm2ProvTools-CBnT
   ```

2. Go to:

   ```
   Fs0:
   ```

3. Run the following command:

   ```
   Ls
   ```

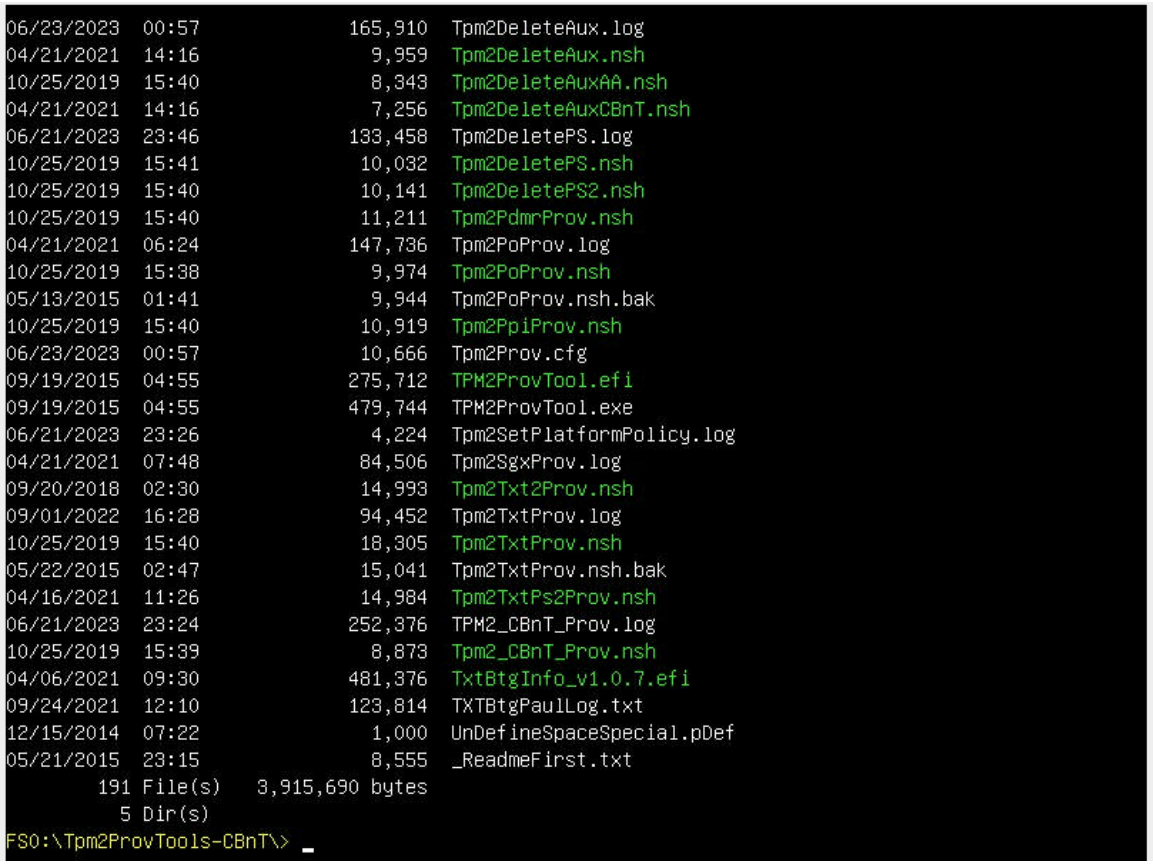

Figure 2-11: Tpm2ProvTools-CBnT Directory

4. Run the following command:

```
Tpm2_CBnT_Prov.nsh sha256 example
```

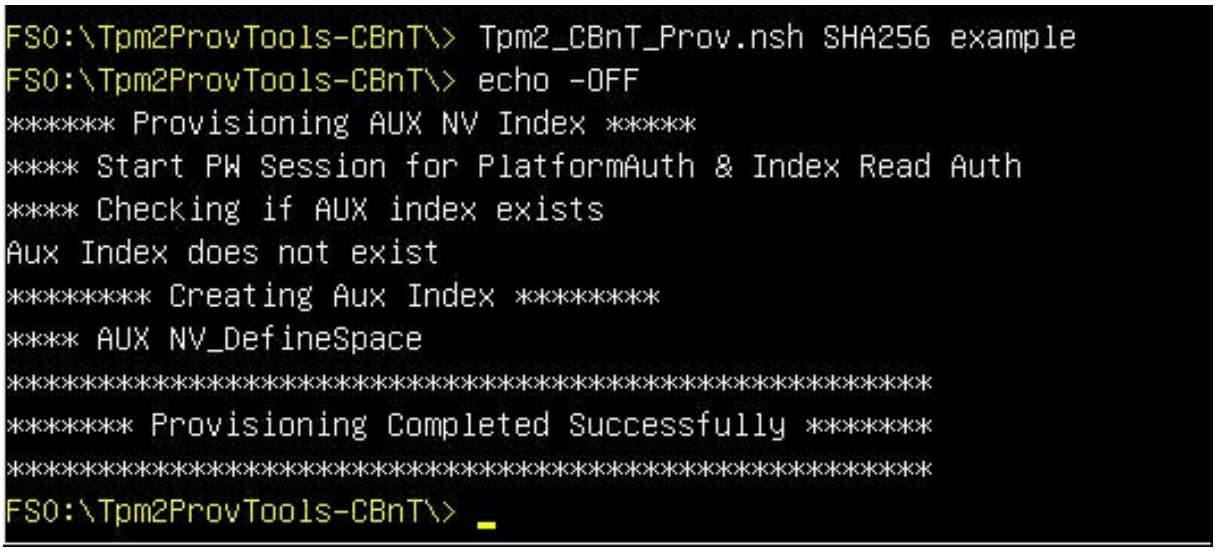

Figure 2-12: Provisioning Completed Sucessfully

5. Reset the system after the provisioning is complete.

Figure 2-13: Reset System Complete

6. Navigate back to the BIOS Main Menu.
7. Select **PH Randomization** and **TXT Support**.
8. Of the PH Randomization and TXT Support options, select **Enabled** for both.

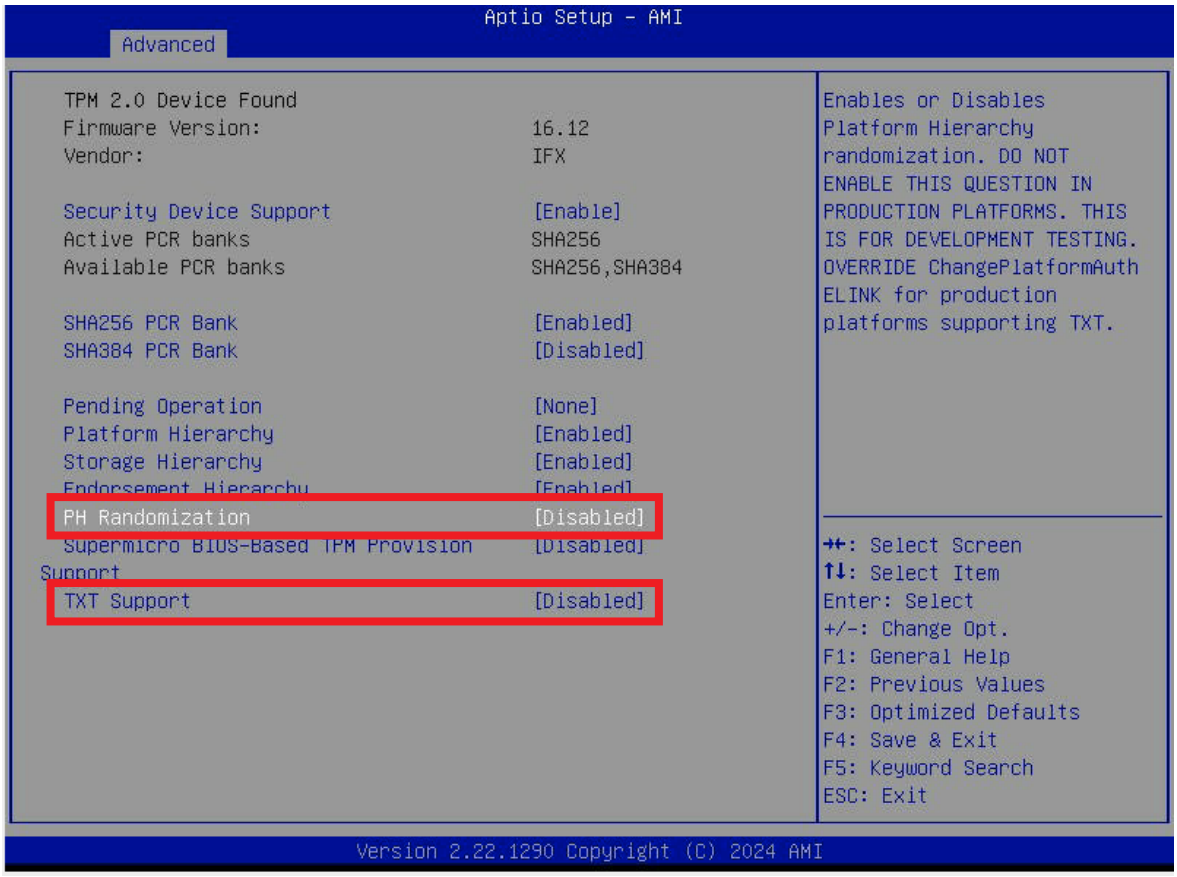

Figure 2-14: Reset System Successfully

9. Select **Save and Exit**.

10. Press **<F11>** to get to **UEFI-Shell: Built-in EFI Shell**.

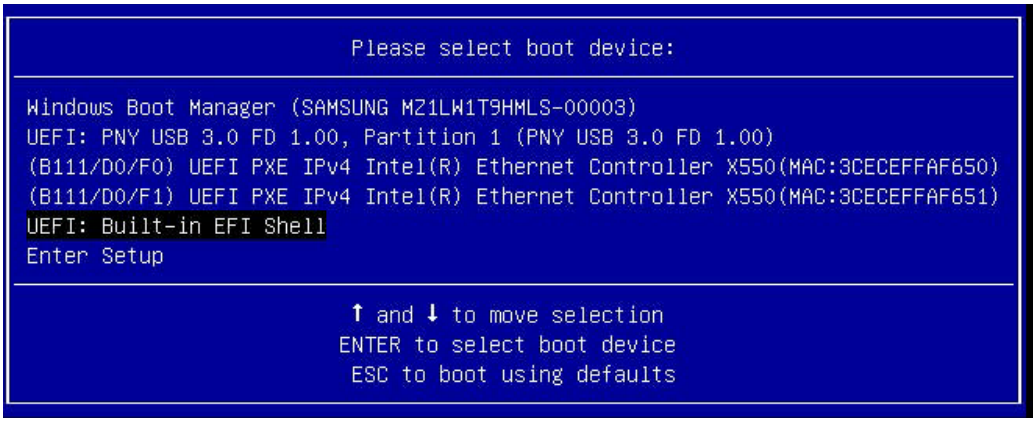

Figure 2-15: UEFI-Shell: Built-in EFI Shell Selected

11. After getting access to **Server Security ToolKit**, run the following command:

```
getsec64server_2.6.0.efi -1 sen -a
```

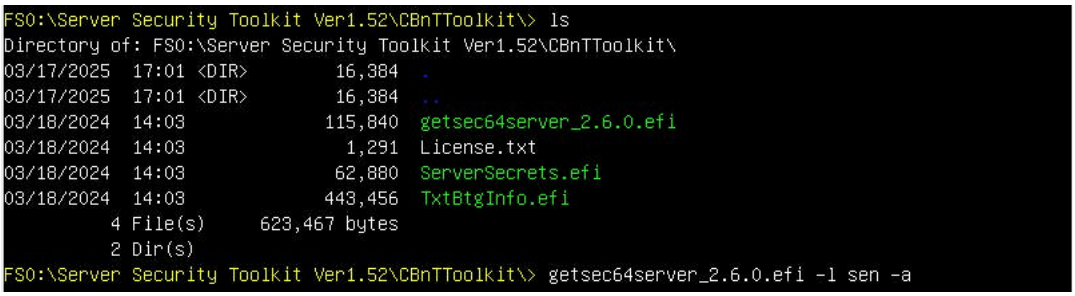

Figure 2-16: Server Security ToolKit

12. The system should be in TXT environment.

Figure 2-17: System Now In TXT Environment

(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.