One-Stop Intel TXT Activation Guide (intel®)

Supermicro® X9 and X10 Based Server Systems

Intel® Trusted Execution Technology (Intel® TXT) for Intel® Xeon processor-based servers is commonly used to enhance platform security by utilizing the underlying hardware based technology found in modern server platforms. Using a combination of the Intel Xeon processor-based and other industry leading platform technologies, such as Intel® Virtualization Technology (Intel VT), Trusted Platform Module (TPM), and appropriately configured BIOS with the Intel® SINIT ACM (authenticated code module); Intel TXT provides security against hypervisor, BIOS, firmware and other pre-launch software based attacks by establishing a 'root of trust' during the boot process. Enabling Intel TXT to protect your systems is a simple process and this will be showcased in this document.

Table of Contents

Assumptions & Guidance

- This document is intended to provide guidance for activating the TPM/Intel TXT in BIOS/uEFI console.

- As available, this document is intended to provide guidance for scale activation of TPM/Intel TXT.

- This document requires fundamental systems engineering knowledge and is intended for Systems Engineers and Systems Administrators.

- This document covers step by step instructions for two Supermicro X9 server platforms based on the Intel Xeon processor E5-2600 V2 family. Other Supermicro X9 and X10 based platforms with the optional TPM Module will have similar setup functionality.

- Microsoft Windows Server software does not support trusted-boot scenarios that are supported by Intel TXT; use cases are based around Linux based server platforms which also includes VMWare ESXi and variations of Openstack cloud-server software.

- Trusted Boot (tboot) is an open source, pre- kernel/VMM module that uses Intel Trusted Execution Technology (Intel TXT) to perform a measured and verified launch of an OS kernel/VMM. Project details: http://sourceforge.net/projects/tboot/

Supermicro Servers – X9DRD-iF and X9DRG-HF

Note: Both of these Supermicro Server boards have very similar BIOS and configuration. There may be some slight differences between each model, but in general the operations that are shown will work on all X9 based Supermicro boards with the Trusted Platform Module (TPM) Add-On-Module (AOM).

Supermicro provides two different TPM Add-on-Modules:
- Add-on-Module AOM-TPM-9655V (tall chassis/2U+ systems)
- Add-on-Module AOM-TPM-9655H (small chassis/1U systems)

Be sure to contact your Supermicro specialist as to which AOM is right for your X9 server system.

Platform Expectations
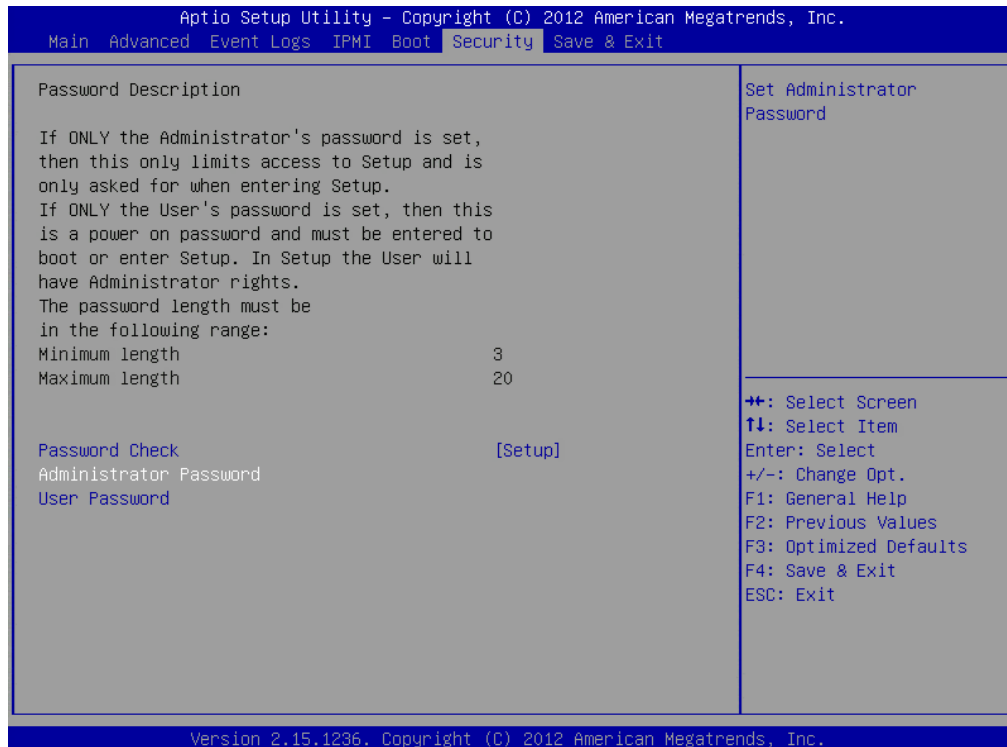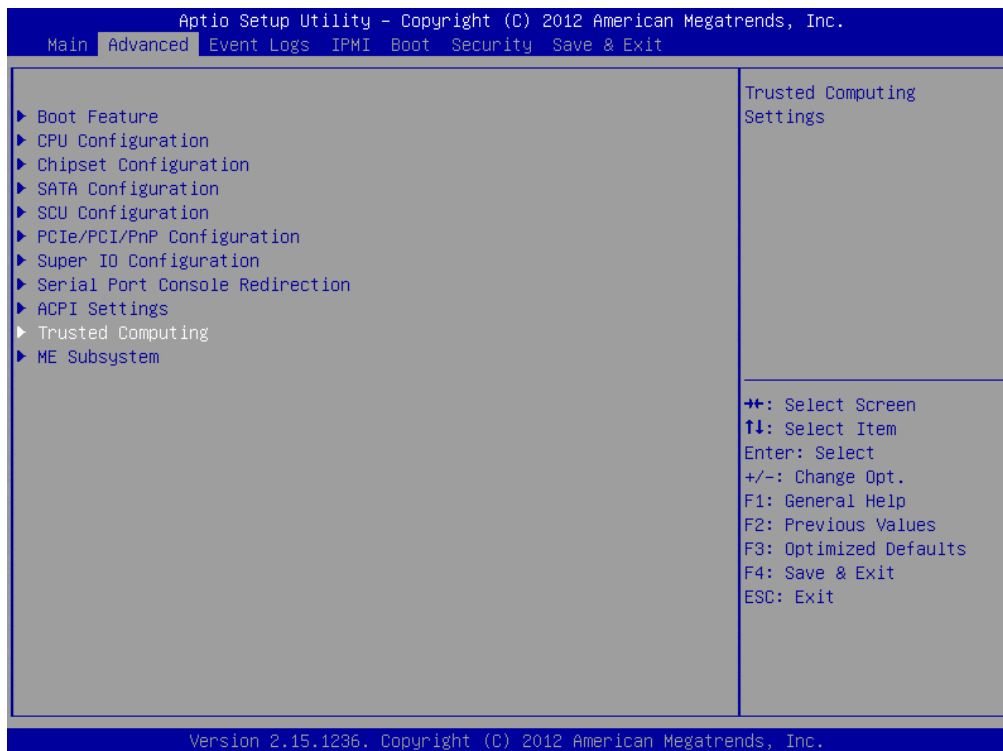- Supermicro ships the ACM as part of BIOS Firmware.
- Supermicro TPM Add-On-Module comes in 2 forms, be sure to validate with your Supermicro representative as to which module fits your server.
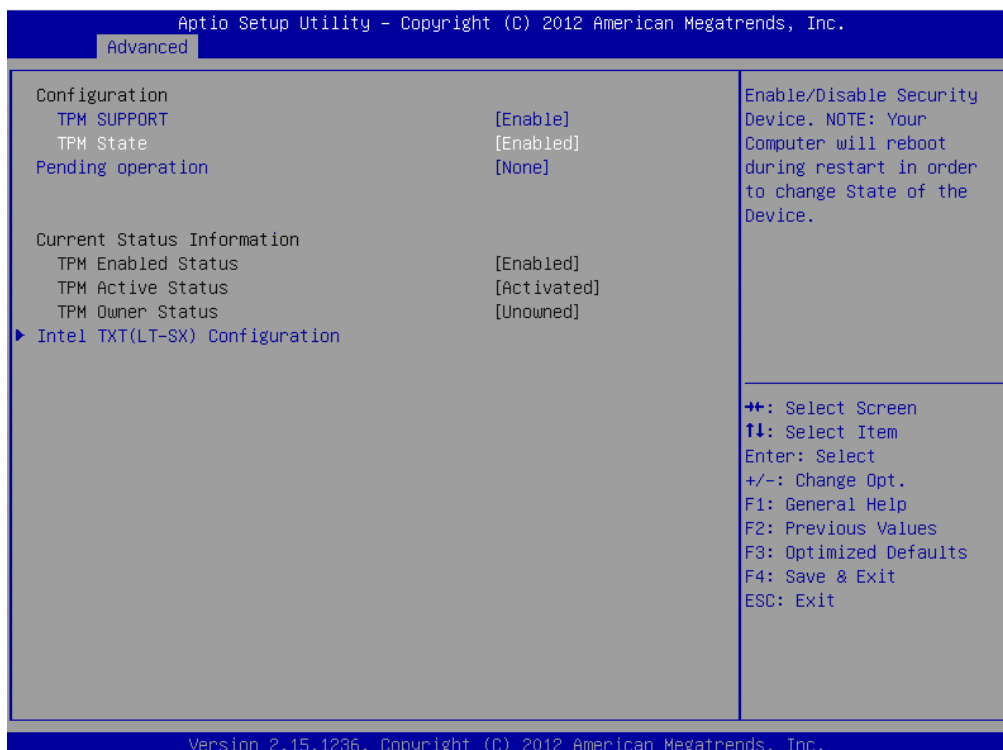
Out of the Box Configuration
- During system boot – Press *DEL key* to enter into the BIOS console
- Bios Console *> Security > Password Check < Setup Security > Administrator password >* Enter desired Password

```
             Aptio Setup Utility - Copyright (C) 2012 American Megatrends, Inc.
      Main   Advanced   Event Logs   IPMI   Boot   Security   Save & Exit

   Password Description                                        Set Administrator
                                                               Password
   If ONLY the Administrator's password is set,
   then this only limits access to Setup and is
   only asked for when entering Setup.
   If ONLY the User's password is set, then this
   is a power on password and must be entered to
   boot or enter Setup. In Setup the User will
   have Administrator rights.
   The password length must be
   in the following range:
   Minimum length                        3
   Maximum length                        20
                                                               ++: Select Screen
                                                               ↑↓: Select Item
   Password Check                        [Setup]               Enter: Select
   Administrator Password                                      +/-: Change Opt.
   User Password                                               F1: General Help
                                                               F2: Previous Values
                                                               F3: Optimized Defaults
                                                               F4: Save & Exit
                                                               ESC: Exit


             Version 2.15.1236. Copyright (C) 2012 American Megatrends, Inc.
```
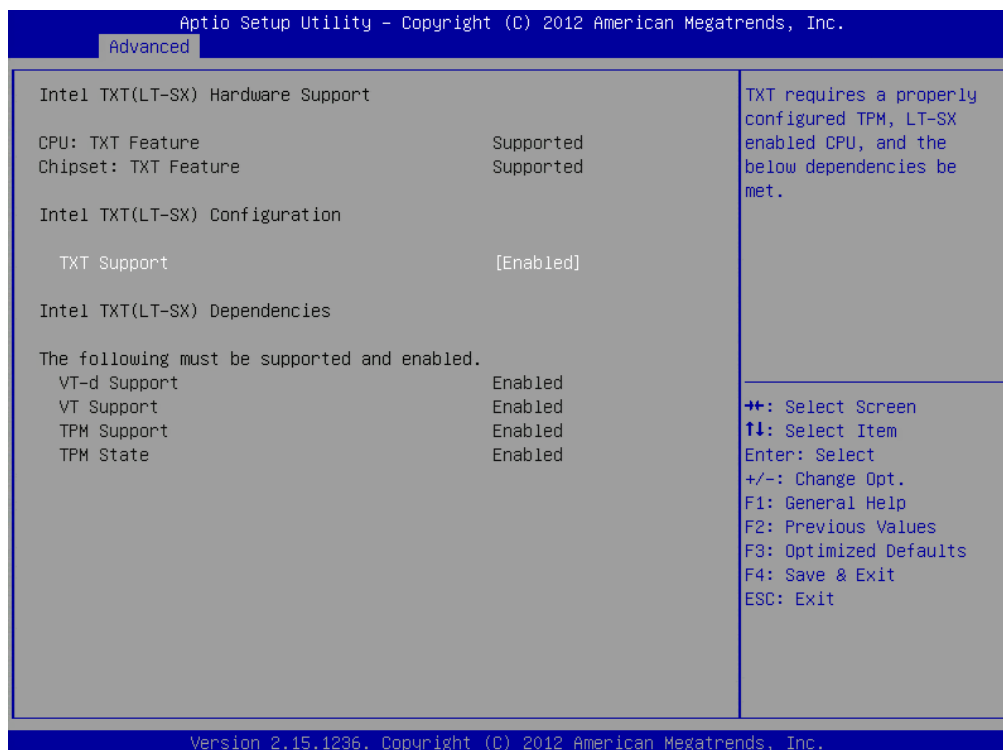
- Press *F4* and "*Yes*" to Reboot
- BIOS console > "*Enter the assigned Password*"
- *Advanced > Trusted computing > TPM Support > Enable*
- *Advanced > Trusted Computing > TPM State > Enable*


```
             Aptio Setup Utility - Copyright (C) 2012 American Megatrends, Inc.
      Main   Advanced   Event Logs   IPMI   Boot   Security   Save & Exit

   ▶ Boot Feature                                              Trusted Computing
   ▶ CPU Configuration                                         Settings
   ▶ Chipset Configuration
   ▶ SATA Configuration
   ▶ SCU Configuration
   ▶ PCIe/PCI/PnP Configuration
   ▶ Super IO Configuration
   ▶ Serial Port Console Redirection
   ▶ ACPI Settings
   ▶ Trusted Computing
   ▶ ME Subsystem
                                                               ++: Select Screen
                                                               ↑↓: Select Item
                                                               Enter: Select
                                                               +/-: Change Opt.
                                                               F1: General Help
                                                               F2: Previous Values
                                                               F3: Optimized Defaults
                                                               F4: Save & Exit
                                                               ESC: Exit


             Version 2.15.1236. Copyright (C) 2012 American Megatrends, Inc.
```

```
                Aptio Setup Utility - Copyright (C) 2012 American Megatrends, Inc.
        Advanced

    Configuration                                              Enable/Disable Security
        TPM SUPPORT                         [Enable]           Device. NOTE: Your
        TPM State                           [Enabled]          Computer will reboot
    Pending operation                       [None]             during restart in order
                                                               to change State of the
                                                               Device.
    Current Status Information
        TPM Enabled Status                  [Enabled]
        TPM Active Status                   [Activated]
        TPM Owner Status                    [Unowned]
    ▶ Intel TXT(LT-SX) Configuration
                                                               ↔: Select Screen
                                                               ↑↓: Select Item
                                                               Enter: Select
                                                               +/-: Change Opt.
                                                               F1: General Help
                                                               F2: Previous Values
                                                               F3: Optimized Defaults
                                                               F4: Save & Exit
                                                               ESC: Exit

                Version 2.15.1236. Copyright (C) 2012 American Megatrends, Inc.
```

- Press **F4** and *Yes* to Reboot
- Re-enter the BIOS console > *Advanced > Trusted computing > Intel TXT(LT-SX) Configuration > TXT support > Enabled*


```
                Aptio Setup Utility - Copyright (C) 2012 American Megatrends, Inc.
        Advanced

    Intel TXT(LT-SX) Hardware Support                          TXT requires a properly
                                                               configured TPM, LT-SX
    CPU: TXT Feature                        Supported          enabled CPU, and the
    Chipset: TXT Feature                    Supported          below dependencies be
                                                               met.
    Intel TXT(LT-SX) Configuration

      TXT Support                           [Enabled]

    Intel TXT(LT-SX) Dependencies

    The following must be supported and enabled.
        VT-d Support                        Enabled
        VT Support                          Enabled            ↔: Select Screen
        TPM Support                         Enabled            ↑↓: Select Item
        TPM State                           Enabled            Enter: Select
                                                               +/-: Change Opt.
                                                               F1: General Help
                                                               F2: Previous Values
                                                               F3: Optimized Defaults
                                                               F4: Save & Exit
                                                               ESC: Exit

                Version 2.15.1236. Copyright (C) 2012 American Megatrends, Inc.
```

- Press **F4** and "*yes*" to save and reboot

TPM Clear and Reactivate Intel TXT/TPM

TPM clear can be done either in BIOS console or from OS using Trousers DLL. One of the requirements for TPM clear is to transfer the TPM ownership. TPM clear action will deactivate the TPM... So reboot is required to activate the TPM/Intel TXT again in the server. Below are the steps to clear and reactivate the TPM/Intel TXT.
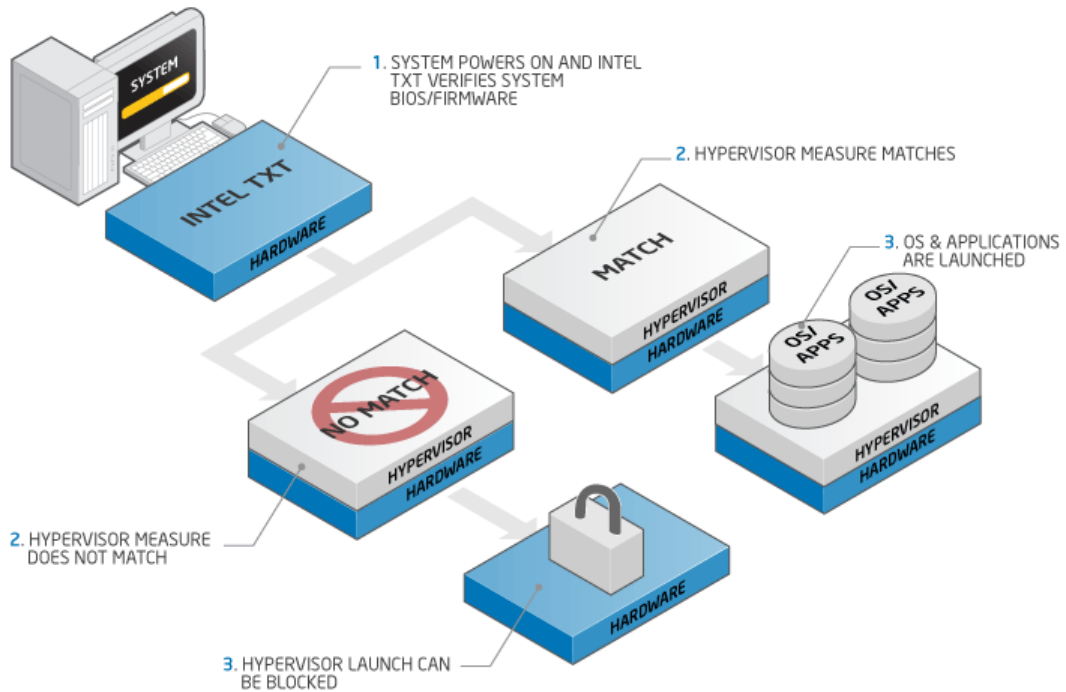
- Press *DEL* key to enter in to BIOS console
- *BIOS Console >"Enter the assigned Password"*
- *BIOS Console > Advanced > Trusted computing > TPM Support > Enable*
- *BIOS Console > Advanced > Trusted Computing > TPM State > Clear*
- Press *F4* and *Yes* to Reboot
- *BIOS Console > ""Enter the assigned Password" "*
- *BIOS Console > Advanced > Trusted computing > TPM Support > Enable*
- *BIOS Console > Advanced > Trusted Computing > TPM State > Enable*
- Press *DEL > Advanced > Trusted computing > Intel TXT(LT-SX) configuration > TXT support > Enabled*
- Press *F4* and "*yes*" to save and reboot

Scaling Activation of Intel TXT/TPM across Multiple Systems

Enabling Intel TXT/TPM on one system is great for testing and validating your platform. In real-world scenarios in the datacenter, customers generally have multiple systems that need enabling at the same time during setup and configuration. Fortunately many OEMs provide tools that lend themselves to assist the server administrator to perform this function.

Enabling Intel TXT across multiple systems allows for more use cases beyond the root-of-trust establishment on a single platform. Models such as Trusted Compute Pools can be developed where systems with Intel TXT can be placed on a 'whitelist' for access. This allows system administrators to place their highest security workloads on trusted platforms and reduce the threat to bare-metal attacks.

INTEL® TXT
INTEL TRUSTED EXECUTION TECHNOLOGY

1. SYSTEM POWERS ON AND INTEL TXT VERIFIES SYSTEM BIOS/FIRMWARE

2. HYPERVISOR MEASURE MATCHES

3. OS & APPLICATIONS ARE LAUNCHED

2. HYPERVISOR MEASURE DOES NOT MATCH

3. HYPERVISOR LAUNCH CAN BE BLOCKED

In order for Intel TXT to function properly the following dependencies need to be established:
- Intel Xeon processor-based server platform with Intel TXT enabled BIOS
- Intel Virtualization Technology (Intel VT) must be enabled
- Intel Virtualization Technology with Directed I/O (Intel VT-d) must be enabled
- A Trusted Platform Module (TPM) v1.2 must be enabled and activated
- The platform specific Intel SINIT ACM needs to be installed into the platform
- Finally, you need a hypervisor that supports trusted boot (t-boot)

Bare Metal Provisioning of Intel TXT

The process to take a bare-metal system with unknown settings to a fully functional Intel TXT enabled platform can take a few minutes per system. The process can be run in-band from the OS, or out-of-band (OOB) via PXE or other remote process. The schematic below shows the high-level process of how a system is updated.

1. The Server PXE boots and installs the OS as well as the OEM deployment tool.
2. The setup and configuration script issues the command that reads the current BIOS setting of the server.
3. The setup and configuration script modifies the TPM/Intel TXT and other inter-related settings to the desired states as prescribed by the administrator.
4. The setup and configuration script issues command that writes and updates the BIOS setting then reboots the server.
5. After several reboots (OEM specific), the TPM/Intel TXT setting will take effect.
6. At this point, the server is automatically configured for TPM/Intel TXT support without accessing the BIOS manually.

Intel TXT Scale Provisioning for Supermicro X9 and X10 Servers

The Supermicro Update Manager (SUM) remotely updates the BIOS and system settings of Supermicro X9 and X10 generation based machine through OOB (Out-Of-Band) communication channels, i.e., communication through the BMC/IPMI interface. Users can remotely edit system BIOS settings from a human-readable text file, and use this utility to update the target machine's system BIOS configuration. BIOS update and setting operations is independent of operating environment on target machine and can be executed before system OS/hypervisor is installed.

Supermicro Update Manager provides these key features:
- Updates BIOS ROM - Update/Preserve SMBIOS data, ME region, and NVRAM
- Gets/Sets BIOS settings - Current settings, and sets default settings
- Checks HW/FW support for OOB management
- Activates product keys to enable OOB BIOS management feature

To install SUM, follow these steps:
1. Extract the sum_x.x.x_Linux_x64_YYYYMMDD.tar.gz archive file.
2. Go to the extracted sum_x.x.x_Linux_x64 directory. Call this directory as "SUM_HOME".
3. Run SUM in the SUM_HOME directory.

```
<shell#> tar xzf sum_x.x.x_Linux_x64_YYYMMDD.tar.gz
<shell#> cd sum_x.x.x_Linux_x64
<SUM_HOME#> ./sum
```

Note: To fully utilize SUM to its full potential you need to license each platform to use the SUM tool. Acquiring multiple systems is a simple, one-time process which is described in the SUM Product Guide.

Here is an example of the configuration script that can be run in-band on the Supermicro X9 server platforms that will scan the BIOS, and change the appropriate settings that will set Intel TXT to be activated and ready for your hypervisor installation.

```
#!/bin/sh


./sum -c GetCurrentBiosCfgTextFile --file sample.txt --overwrite

cat sample.txt | sed -e "s/Intel Virtualization Technology=00/Intel Virtualization Technology=01/;s/Intel(R) VT-d=00/Intel(R) VT-
d=01/;s/TPM SUPPORT=00/TPM SUPPORT=01/;s/TPM State=00/TPM State=01/;s/Pending operation=00/Pending operation=08/;s/TXT
Support=00/TXT Support=01/" > sample1.txt

./sum -c ChangeBiosCfg --file sample1.txt --reboot
```

How to check the Intel TXT/TPM status

Linux Distributions

Assumption:

- Users have successfully activated Intel TXT in BIOS and OS by following the respective guides.
- To Activate the Intel TXT in Linux OS users are requested to follow the Intel TXT OS Setup Guide.
- TPM Status Can be read from linux OS through TPM Device Driver in Dom0.
- Issue below command to find the status of the TPM

  $ cat /sys/class/misc/tpm0/device/enabled
  # If it returns 0 then it is not enabled; if it returns 1 then it is enabled.

  $ cat /sys/class/misc/tpm0/device/active
  # If it returns o then it is not active; if it is returns 1 then it is active.

  $ cat /sys/class/misc/tpm0/device/owned
  # If it returns o then it is not owned; if it is returns 1 then it is owned.

  $ cat /sys/class/misc/tpm0/device/pcrs
  # Returns the PCR measurement values.

"**Txt-stat" Tool:**
- **txt-stat** is the Intel TXT status tool that is part of Tboot kernel to get the status of Intel TXT measurement.**txt-stat** tool collects the information from RAM and displays.
- Users can use this tool to check if the Intel TXT launch/boot was successful or not.
- Ensure to run the **tcsd daemon** before running this tool.

$ tcsd
$ txt-stat | more

VMware ESXi 5.x

1. Install ESXi on the Intel TXT/TPM activated host and add to the vCenter.
2. *Connect to the vCenter through IE browser* *http://<vCenter IP Address>/mob*
3. Click on the "**add exceptions**" in the next screen
4. Enter the **credentials** of the vCenter to connect to ESXi hosts.
5. Click on "**Content**"

6. In the following screen, search for "**Rootfolder**" and click on the value "**group-d1**"
7. In the following screen, search for "**Childentity**" and click on the value "**Datacenter-2**"
8. In the following screen, search for "**Hostfolder**" and click on the value "**group-h4**"
9. In the following screen, search for "**Childentity**" and click on the value "**Domain-C7**"
10. In the following screen, search for "*Host*" and click on the value "**host <ip address>**"

11. In next screen drag down to Methods table and click on "*QueryTpmAttestationReport*"
12. A separate window will open up - Click on "*Invoke method*"
13. In the Next screen user can see the Platform Configuration Register (PCR) values populated.

Note:
- If *ESXi* host is not Intel TXT provisioned then you will not see any PCR values in step 13.
- If users are sure that TPM is provisioned correctly but TPM value is unset in v-center then as a work around, disconnects the host and reconnects the host if the TPM value is unset.

Troubleshooting Guide

1. **How to determine if Intel TXT successfully launched?**

   In Linux Distributions:
   Use txt-stat tool to check if the Intel TXT launch is successful.

   ```
   root@ubuntu-tboot:~# txt-stat | grep measured
            TXT measured launch: TRUE
   TBOOT: measured launch succeeded
   ```

   In VMware ESXi:
   You can verify if TPM is enabled on your ESXi hosts with the following command:
   esxcli hardware trustedboot get

   ```
   ~ # esxcli hardware trustedboot get
      Drtm Enabled: true
      Tpm Present: true
   ```

   If users see TPM value is unset though it is provisioned correctly, as a work around disconnect and reconnect the host in vCenter will usually resolve the issue.

2. **How to validate the TPM:**

   There is tool called tpm-tools which is shipped with all Linux OS. This tools implements the TSS API and talks directly to the TPM

   $ tpm_selftest will show the current state of TPM
   $ tpm_version will show the tpm version

   ```
   root@mwtstubx01h:~# tpm_version
      TPM 1.2 Version Info:
      Chip Version:        1.2.8.8
      Spec Level:          2
      Errata Revision:     2
      TPM Vendor ID:       STM
      TPM Version:         01010000
      Manufacturer Info:   53544d20
   ```