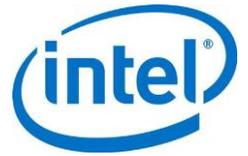


One-Stop Intel TXT Activation Guide



Intel® S2600GZ 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	3
Intel Servers Based on the S2600GZ Motherboard	4
Platform Expectations.....	4
Out of Box Configuration.....	4
TPM clear and Reactive Intel TXT/TPM.....	5
Scaling Activation of Intel TXT/TPM across Multiple Systems	6
Bare Metal Provisioning of Intel TXT.....	8
Intel TXT Scale Provisioning for Intel S2600 Family Servers	8
Installing Intel System Configuration Utility (syscfg).....	9
How to check the Intel TXT/TPM status	10
Linux Distributions	10
VMware ESXi 5.x.....	11
Troubleshooting Guide.....	12

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 Intel S2600GZ series server platforms based on the Intel Xeon processor E5-2600 V2 family. All Intel Server platforms supporting Intel TXT will have similar functionality as compared to this document.
- 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/>

Intel, the Intel logo, and Xeon, are trademarks of Intel Corporation in the U.S. and/or other countries. *Other names and brands may be claimed as the property of others. All information provided here is subject to change without notice. Contact your Intel representative to obtain the latest Intel product specifications and roadmaps. Statements in this document that refer to Intel's plans and expectations for the quarter, the year, and the future, are forward-looking statements that involve a number of risks and uncertainties. A detailed discussion of the factors that could affect Intel's results and plans is included in Intel's SEC filings, including the annual report on Form 10-K. Any forecasts of goods and services needed for Intel's operations are provided for discussion purposes only. Intel will have no liability to make any purchase in connection with forecasts published in this document. Copies of documents which have an order number and are referenced in this document may be obtained by calling 1-800-548-4725 or visit www.intel.com/design/literature.htm.

© 2014 Intel Corporation

Intel Servers Based on the S2600GZ Motherboard

```
Copyright (c) 2009 - 2013 Intel Corporation. All rights reserved.
Version 2.14.1219. Copyright (C) 2013 American Megatrends, Inc.
Bios Version: SE5C600.86B.02.03.0003.041920141333
BMC Firmware Version: 1.21.6038
SDR Version: SDR Package 1.13
ME Firmware Version: 2.1.7.328
Platform ID: S2600GZ
System memory detected: 131072 MB
Current memory speed: 1333 MT/s
Intel(R) Xeon(R) CPU E5-2697 v2 @ 2.70GHz
Number of physical processors identified: 2
*****
*****
AHCI Capable Controller enabling 2 ports of 6Gb/s SATA
SAS/SATA Capable Controller is disabled
*****
*****
USB Keyboard detected
USB Mouse detected

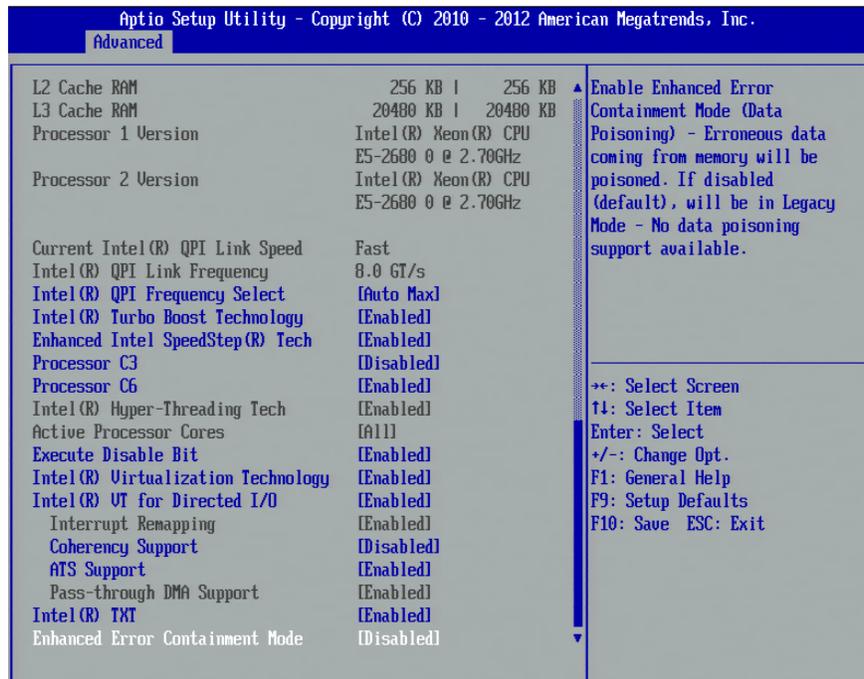
Press <F2> to enter setup, <F6> Boot Menu, <F12> Network Boot
```

Platform Expectations

- ACM is shipped as part of the BIOS firmware.

Out of Box Configuration

- Press **F2** to Enter in to BIOS Console
- Set password. Note: Password should be alphanumeric for EPSD servers.
- Press **F2** key > **Security** > Set Administrator Password > Press **F10** > save and reset > press "OK"
- Reboot the server
- Press **F2** > Enter the administrator Password > **Security** > **TPM Administrative control** > Turn On > Press **F10** > save and Reset > Press **OK** to reboot the server.
- Press **F2** > Enter the administrator Password > **Advanced** > **Intel VT** > **Enabled** ; **Intel VTd-IO** > **Enabled** ; **Intel TXT** > **enabled**

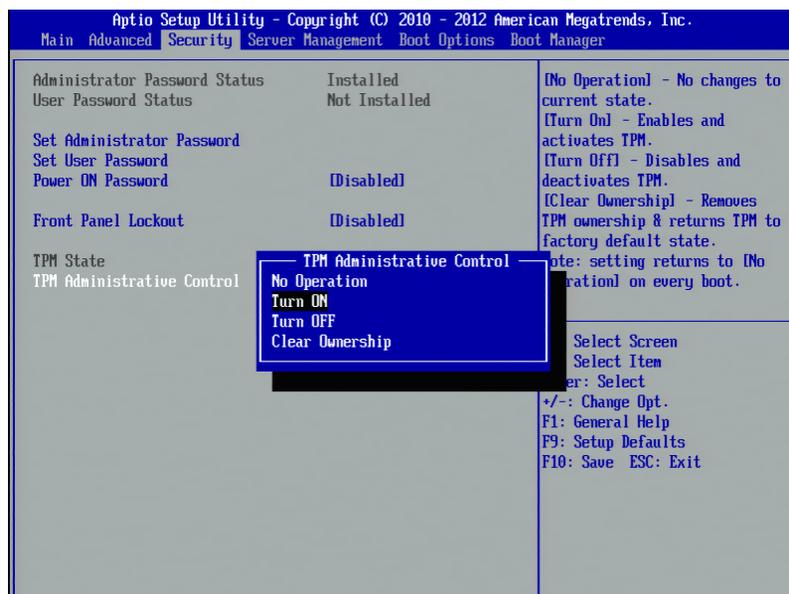


- Ensure TPM is ON and in Enabled state.
- Press **F2** > **Security** > **TPM State**

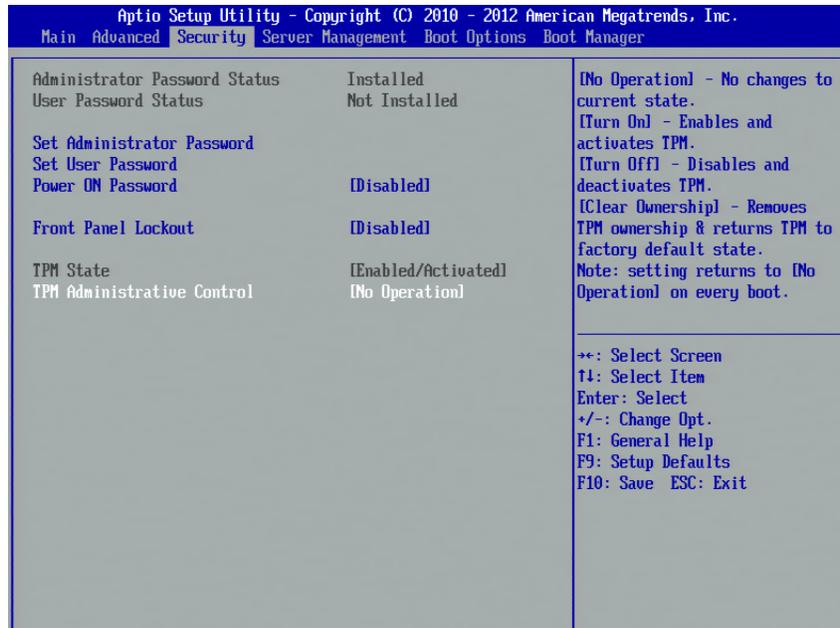
TPM clear and Reactive Intel TXT/TPM

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 **F2** > Enter password > **security** > **Trusted Platform Module** > **TPM Administrative control** > **Clear Ownership** > **F10** > save and Reset > press "OK"



- Press **F2** > Enter password > **security** > **Trusted Platform Module** > **TPM Administrative control** > **TPM ON** > **F10** > save and Reset > press "OK"
- To Ensure TPM Status, press **F2** > Enter password > **security** > **Trusted Platform Module** > **TPM state** > Enabled and activated.



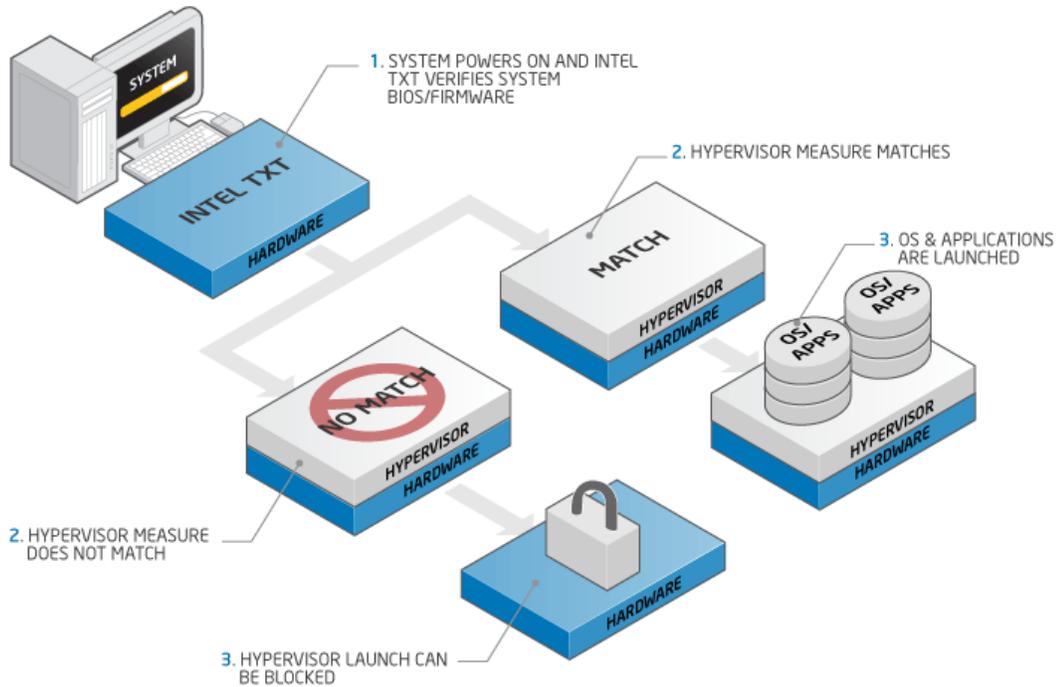
- Press F10 > Save and Reboot

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

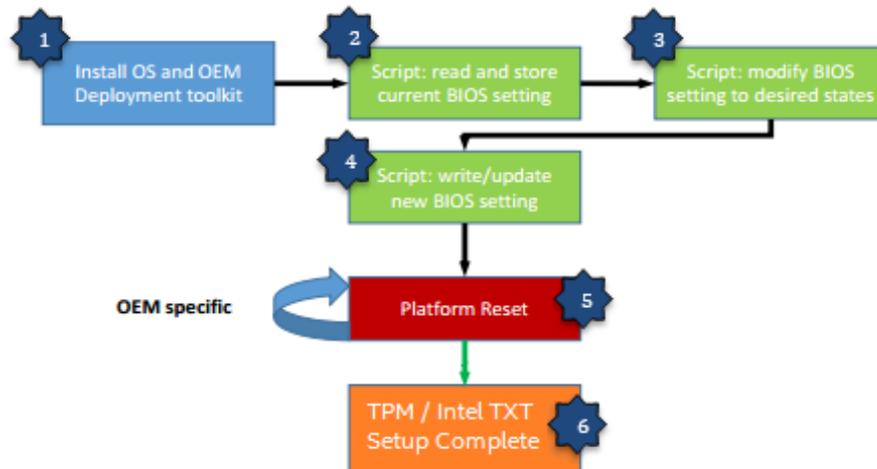


In order for Intel TXT to function properly the following dependencies need to be established:

- 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 Intel S2600 Family Servers

The [Intel System Configuration Utility](#) (syscfg) is a command-line utility that can be used to save and restore BIOS and firmware settings to a file or to set and display individual settings. The syscfg command may be used in a script to automate the process of configuring multiple servers. The utility can be run from EFI, Linux and Windows.

The Intel SCU tool provides these benefits:

- Saving and restoring Firmware and BIOS settings to a binary/INI file, and for configuring Firmware and BIOS settings via a command line interface.
- Modification of BIOS and configuration settings in Linux, uEFI, Windows, WinPE environments.
- Bulk modification across multiple platforms to set configurations using in-band or out of band access points. Intel Remote Management (RMM4) Module optional.

Installing Intel System Configuration Utility (syscfg)

The example below is for a linux installation. Refer to the syscfg instruction guide for other options for Windows, uEFI, or WinPE.

1. Regular Installation:

- a. Boot into Linux and unzip the syscfg utility zip file into a folder on your hard drive. After unzip, "RHEL" or "SLES" folder will be generated
The syscfg directory will have the following file.
 - Syscfg.zip
- b. Unzip to get the syscfg binaries and execute the syscfg commands.
- c. To uninstall remove the syscfg folder structure

2. RPM Installation:

- a. Boot into Linux and unzip the syscfg utility zip file into a folder on your hard drive copy syscfg rpm from Linux-RPM-package (for RHEL or SLES) to local folder.
- b. Install syscfg utility by using "rpm -ivh syscfg-Vxx.x-Bxx.ixxx.rpm". This will install the utility in "/usr/bin/syscfg/"
- c. On RHEL/SLES after installing the rpm close the terminal from which rpm was installed and then execute utility from a new terminal (example: "# syscfg -i").
 - d. To uninstall execute this command:
syscfg -e syscfg

Notes: In order to manipulate the TPM/Intel TXT on the Intel server, you must setup the administrator password first. You can manually setup the password or using the syscfg utility to do so.

Example: `syscfg /bap "" intel123 ;setup password from blank to intel123`

Due to the BIOS configuration, multiple reboots are required to setup TPM and Intel TXT on the Intel S2600GZ based server. The script below runs and performs validation checks upon each reboot to verify settings and will continue to push the required settings until verified and completed.

```
modprobe ipmi_devintf

if [ -f /root/Downloads/RHEL/t1 ]
then
    pushd /root/Downloads/RHEL/
    ./syscfg /bcs intel123 "Intel(R) TXT" 1
    sleep 5
    popd
    rm -f /root/Downloads/RHEL/t1
    cat /etc/rc.local | sed -e "s%/root/Downloads/RHEL/pcsdscript0616.sh%%" > /root/Downloads/RHEL/rctmp
    cat /root/Downloads/RHEL/rctmp > /etc/rc.local
    rm -f /root/Downloads/RHEL/rctmp
    init 6
else
    pushd /root/Downloads/RHEL/
    ./syscfg /bcs intel123 "Intel(R) Virtualization Technology" 1
    ./syscfg /bcs intel123 "Intel(R) VT for Directed I/O" 1
    ./syscfg /bcs intel123 "TPM Administrative Control" 6
    sleep 5
    touch t1
    popd
    cat /etc/rc.local | sed -e "s%^$/root/Downloads/RHEL/pcsdscript0616.sh%" > /root/Downloads/RHEL/rctmp
    cat /root/Downloads/RHEL/rctmp > /etc/rc.local
    init 6
fi
```

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 0 then it is not active; if it returns 1 then it is active.

\$ cat /sys/class/misc/tpm0/device/owned

If it returns 0 then it is not owned; if it returns 1 then it is owned.

\$ cat /sys/class/misc/tpm0/device/pcrs

Returns the PCR measurement values.

```
[root@XenTestbed ~]# cat /sys/class/misc/tpm0/device/pcrs
PCR-00: 83 DF FA 74 AB A6 23 9B E5 50 7C C7 8A 05 65 9F FE 6F 34 4D
PCR-01: 3A 3F 78 0F 11 A4 B4 99 69 FC AA 80 CD 6E 39 57 C3 3B 22 75
PCR-02: FE 87 F1 E2 23 F8 E7 36 6D 69 F4 03 35 AE B8 F4 74 00 07 F7
PCR-03: 3A 3F 78 0F 11 A4 B4 99 69 FC AA 80 CD 6E 39 57 C3 3B 22 75
PCR-04: C3 D9 B5 FE FD C2 35 89 45 ED E4 95 F8 D4 53 FF 7B 3C 1C 16
PCR-05: 70 58 97 12 22 AC D9 C2 40 76 D9 F1 3A 44 EF 6D 20 A9 87 07
PCR-06: 3A 3F 78 0F 11 A4 B4 99 69 FC AA 80 CD 6E 39 57 C3 3B 22 75
PCR-07: 3A 3F 78 0F 11 A4 B4 99 69 FC AA 80 CD 6E 39 57 C3 3B 22 75
PCR-08: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR-09: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR-10: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR-11: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR-12: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR-13: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR-14: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR-15: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR-16: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR-17: 01 49 36 FB 8E 27 3D 53 82 36 36 23 5B 16 26 AB 25 F1 C5 14
PCR-18: D4 C0 79 EC C5 5B 8E 11 1A C9 6C E4 C3 E0 49 F8 00 1B DA E2
PCR-19: 31 27 1D ED 60 3D 7F F5 4F 29 2C A0 E5 34 9E 3B 01 0C 3A 7E
PCR-20: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR-21: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR-22: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR-23: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
[root@XenTestbed ~]#
```

“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

```

Intel(r) TXT Configuration Registers:
STS: 0x00014081
  sender_done: TRUE
  sext_done: FALSE
  mem_config_lock: FALSE
  private_open: TRUE
  locality_1_open: FALSE
  locality_2_open: TRUE
ESTS: 0x00
  txt_reset: FALSE
E2STS: 0x0000000200000016
  secrets: TRUE
ERRORCODE: 0x00000000
DIDVID: 0x0000003fc0008086
  vendor_id: 0x8086
  device_id: 0xc000
  revision_id: 0x3f
FSBIF: 0x0000000000000000
QPIIF: 0x000000008c482000
SINIT.BASE: 0x8f700000
SINIT.SIZE: 131072B (0x20000)
HEAP.BASE: 0x8f720000
HEAP.SIZE: 917504B (0xe0000)
DPR: 0x00000008f800031
  lock: TRUE
  top: 0x8f900000
  size: 3MB (3145728B)
PUBLIC.KEY:
  08 77 7b 21 ec 4d 7f ce f7 68 2a 26 96 bc 5f 42
  a9 96 45 a4 21 81 10 7f 87 70 c2 24 37 fd e0 2c
.....
TXT measured launch: TRUE
secrets flag set: TRUE
.....

```

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**”

Home		
Managed Object Type: ManagedObjectReference:ServiceInstance		
Managed Object ID: ServiceInstance		
Properties		
NAME	TYPE	VALUE
capability	Capability	capability
content	ServiceContent	content
serverClock	dateTime	"2012-05-07T23:41:01.088527Z"
Methods		
RETURN TYPE	NAME	
dateTime	CurrentTime	
HostVMotionCompatibility[]	QueryVMotionCompatibility	
ServiceContent	RetrieveServiceContent	
ProductComponentInfo[]	RetrieveProductComponents	
Event[]	ValidateMigration	

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
```