One-Stop Intel TXT Activation Guide

DELL* PowerEdge 12G 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 DELL* PowerEdge* 12G server platforms based on the Intel Xeon processor E5-2600 V2 family, which is not fully conclusive of the product offerings available in the market today, but is provided to give a holistic review of many DELL server platforms.

- 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.

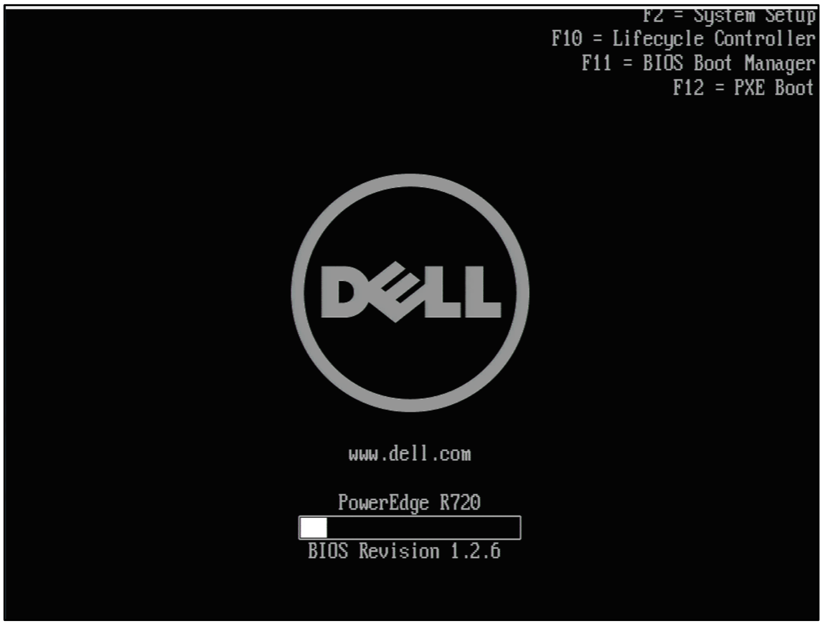
- Trusted Boot (tboot) is an open source, pre- kernel/VMM module that uses Intel Trusted Execution Technology (Intel TXT) to perform a measured and verified launch of an OS kernel/VMM. Project details: http://sourceforge.net/projects/tboot/

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

DELL PowerEdge Servers - R720, R620 & M620

Note: Each of these three DELL Server Platforms have very similar BIOS and configuration. There may be some slight differences between each model, but in general the operations that are shown for the R720 will work on the R620 and M620 (blade) models as well.



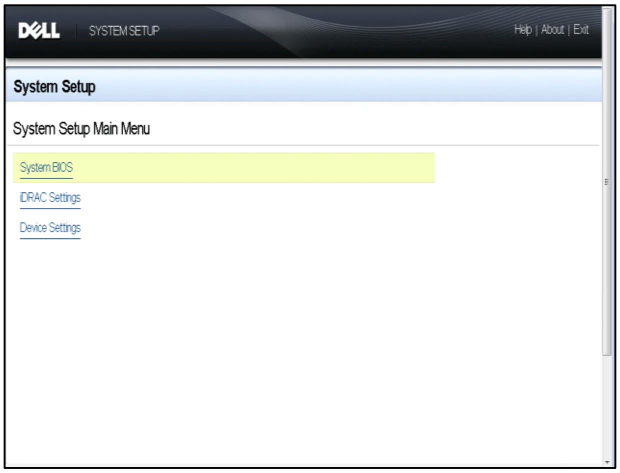
```
                                F2 = System Setup
                        F10 = Lifecycle Controller
                          F11 = BIOS Boot Manager
                                    F12 = PXE Boot

                 www.dell.com

                PowerEdge R720

              BIOS Revision 1.2.6
```

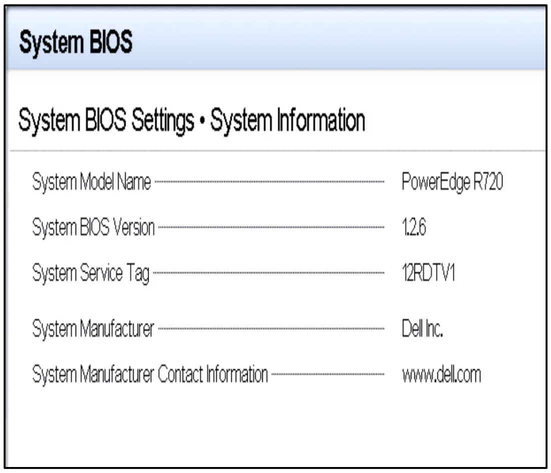
Platform Expectations

- DELL ships the server with both BIOS and uEFI mode
- DELL ships SINIT ACM as part of BIOS/uEFI
- Intel TXT launch was successful both in uEFI and BIOS mode.
- VMware ESXi supports Intel TXT launch in BIOS mode[legacy] only (not uEFI)

Out of the Box Configuration

1. Press ***F2*** to enter in to BIOS console





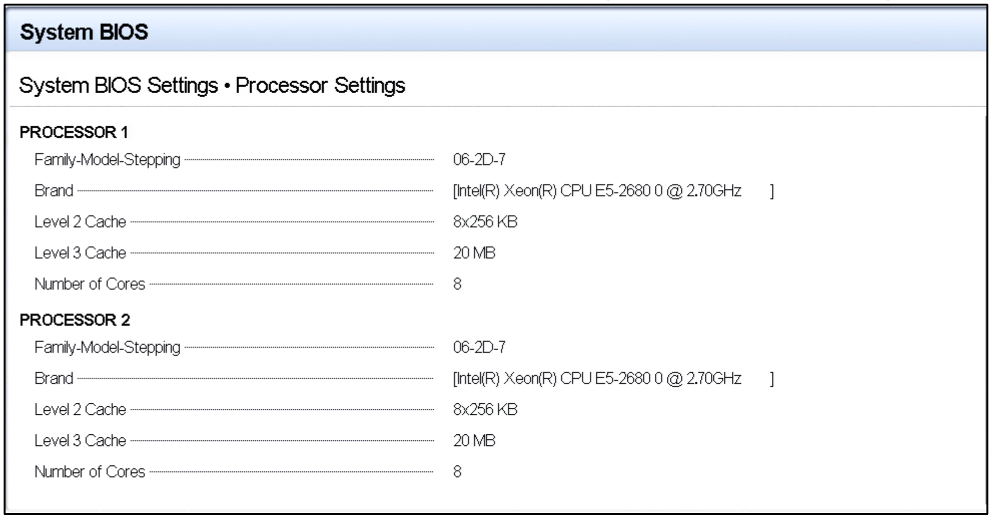
System BIOS

System BIOS Settings • System Information

System Model Name	PowerEdge R720
System BIOS Version	1.2.6
System Service Tag	12RDTV1
System Manufacturer	Dell Inc.
System Manufacturer Contact Information	www.dell.com

© Intel Corporation 2014

2. "Ensure to verify VT is enabled Click on ""***BIOS Settings""* > *Processor Settings* "**



System BIOS

System BIOS Settings • Processor Settings

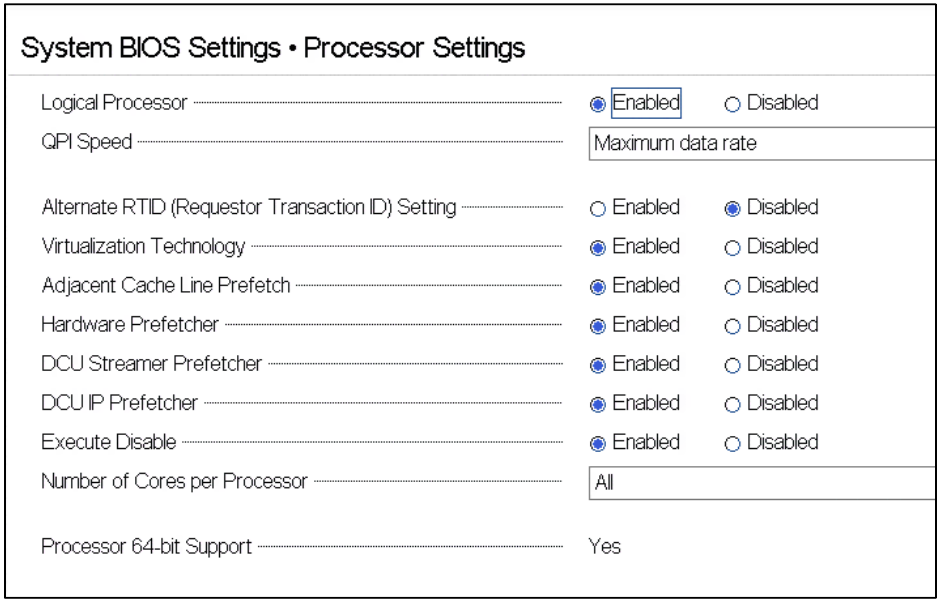
PROCESSOR 1

Family-Model-Stepping	06-2D-7
Brand	[Intel(R) Xeon(R) CPU E5-2680 0 @ 2.70GHz]
Level 2 Cache	8x256 KB
Level 3 Cache	20 MB
Number of Cores	8

PROCESSOR 2

Family-Model-Stepping	06-2D-7
Brand	[Intel(R) Xeon(R) CPU E5-2680 0 @ 2.70GHz]
Level 2 Cache	8x256 KB
Level 3 Cache	20 MB
Number of Cores	8

3. "Setup BIOS password: System BIOS Settings ***> System Security > Setup Password***

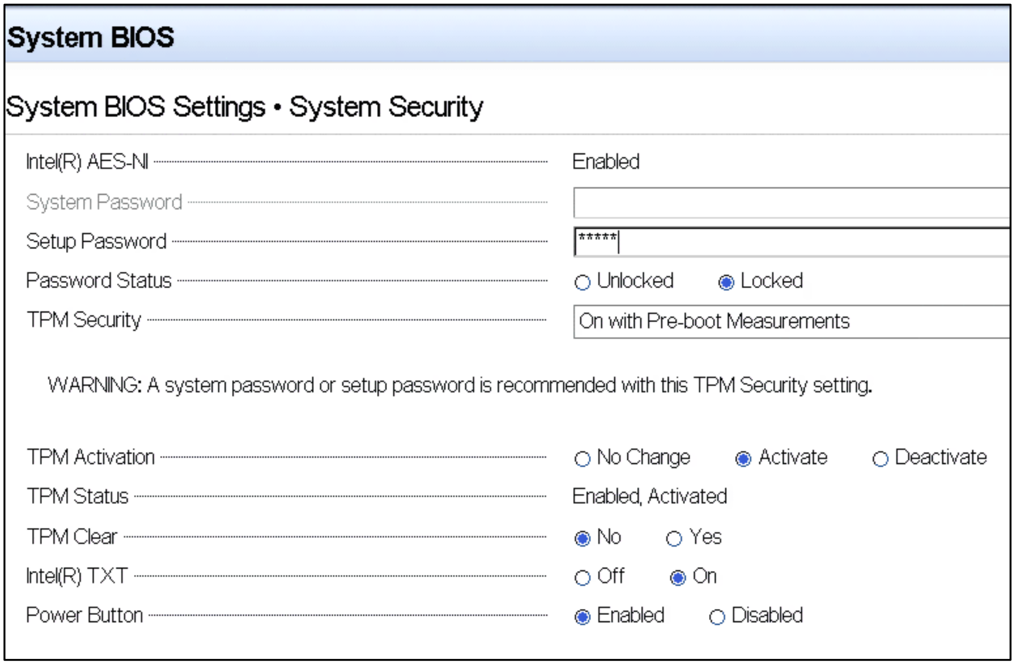


System BIOS Settings • Processor Settings

Logical Processor	● Enabled	○ Disabled
QPI Speed	Maximum data rate	
Alternate RTID (Requestor Transaction ID) Setting	○ Enabled	● Disabled
Virtualization Technology	● Enabled	○ Disabled
Adjacent Cache Line Prefetch	● Enabled	○ Disabled
Hardware Prefetcher	● Enabled	○ Disabled
DCU Streamer Prefetcher	● Enabled	○ Disabled
DCU IP Prefetcher	● Enabled	○ Disabled
Execute Disable	● Enabled	○ Disabled
Number of Cores per Processor	All	
Processor 64-bit Support	Yes	

© Intel Corporation 2014

4. System BIOS Settings > ***System Security > Password Status > Locked System BIOS Settings > System Security > On with Pre-boot Measurement System***



System BIOS

System BIOS Settings • System Security

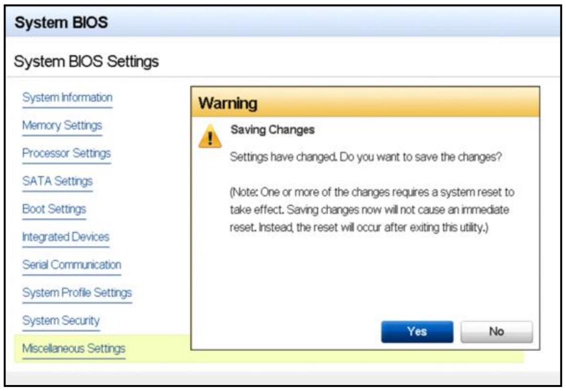
Intel(R) AES-NI: Enabled
System Password:
Setup Password: *****
Password Status: ○ Unlocked ● Locked
TPM Security: On with Pre-boot Measurements

WARNING: A system password or setup password is recommended with this TPM Security setting.

TPM Activation: ○ No Change ● Activate ○ Deactivate
TPM Status: Enabled, Activated
TPM Clear: ● No ○ Yes
Intel(R) TXT: ○ Off ● On
Power Button: ● Enabled ○ Disabled

5. BIOS Settings ***> System Security > TPM Activation > Activate System BIOS Settings > System Security > Intel TXT > On***

6. Press "**Esc**" key and click on "**yes**" to save the changes.



System BIOS

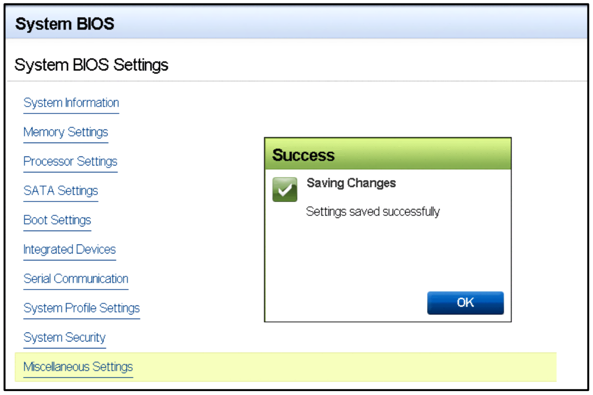
System BIOS Settings

Warning

Saving Changes

Settings have changed. Do you want to save the changes?

(Note: One or more of the changes requires a system reset to take effect. Saving changes now will not cause an immediate reset. Instead, the reset will occur after exiting this utility.)



System BIOS

System BIOS Settings

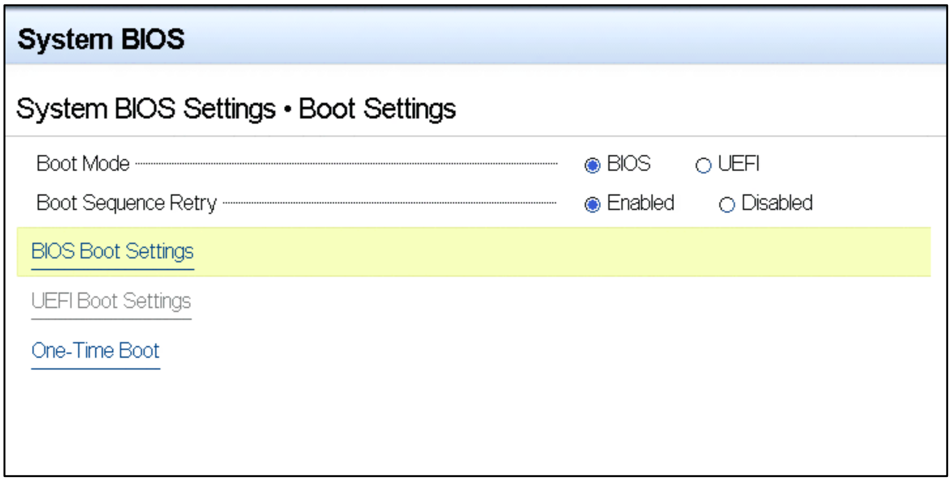
Success

Saving Changes

Settings saved successfully

7. System BIOS Settings > ***Boot Settings > Boot Mode > BIOS***

8. Esc > save settings > boot the server to BIOS mode if user wants to boot to VMware ESXi.



System BIOS

System BIOS Settings • Boot Settings

Boot Mode ● BIOS ○ UEFI

Boot Sequence Retry ● Enabled ○ Disabled

BIOS Boot Settings

UEFI Boot Settings

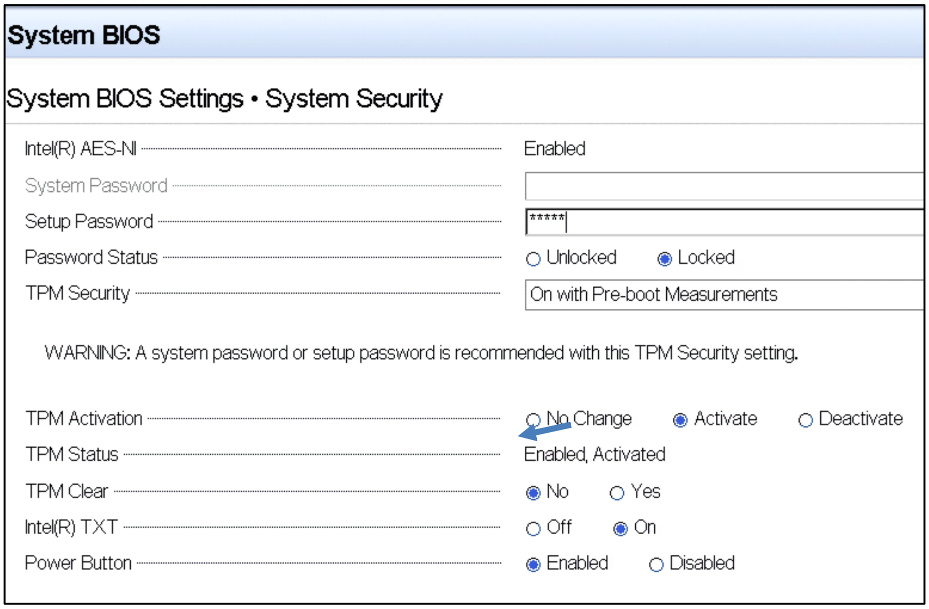
One-Time Boot

TPM Clear and Reactivate Intel TXT/TPM

TPM clear can be done either in BIOS/uEFI 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. A reboot is required to activate the TPM/Intel TXT again in the server

Below are the steps to clear the TPM in BIOS/uEFI console.

1. Press ***F2*** to enter in to BIOS console [it will prompt for BIOS password entry]
2. BIOS Settings > ***System Security > TPM Activation > Activate System BIOS Settings > System Security > TPM clear > On***



System BIOS

System BIOS Settings • System Security

Intel(R) AES-NI Enabled

System Password

Setup Password *****

Password Status ○ Unlocked ● Locked

TPM Security On with Pre-boot Measurements

WARNING: A system password or setup password is recommended with this TPM Security setting.

TPM Activation ○ No Change ● Activate ○ Deactivate

TPM Status Enabled, Activated

TPM Clear ● No ○ Yes

Intel(R) TXT ○ Off ● On

Power Button ● Enabled ○ Disabled

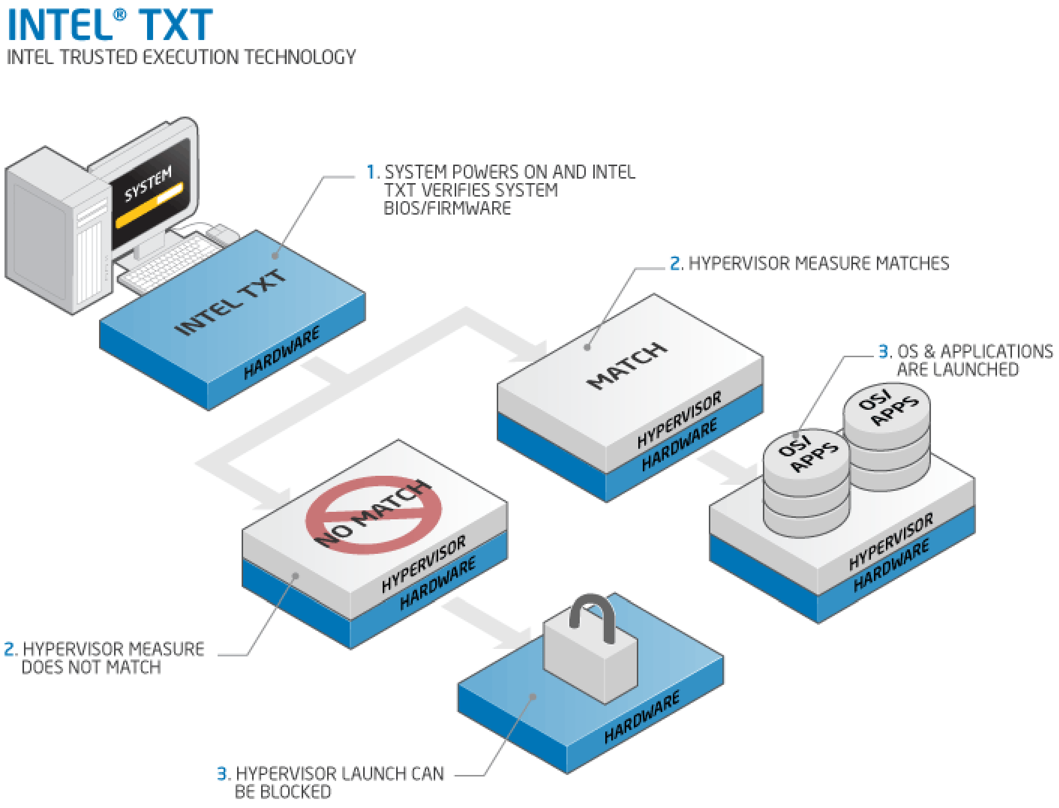
3. Press "***Esc***" key and click on "***yes***" to save the changes.
4. Press ***F2*** to enter in to BIOS console
5. "Ensure to verify VT is enabled Click on "***BIOS Settings" > Processor Settings***"

6. System BIOS Settings > **System Security > Password Status > Locked**
7. System BIOS Settings > **System Security > On with Pre-boot Measurements**
8. BIOS Settings > ***System Security > TPM Activation > Activate System BIOS Settings > System Security > Intel TXT > On"***
9. Press "***Esc***" key and click on "***yes***" to save the changes.
10. System BIOS Settings ***> Boot Settings > Boot Mode > BIOS***
11. Esc > save settings > boot the server

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.

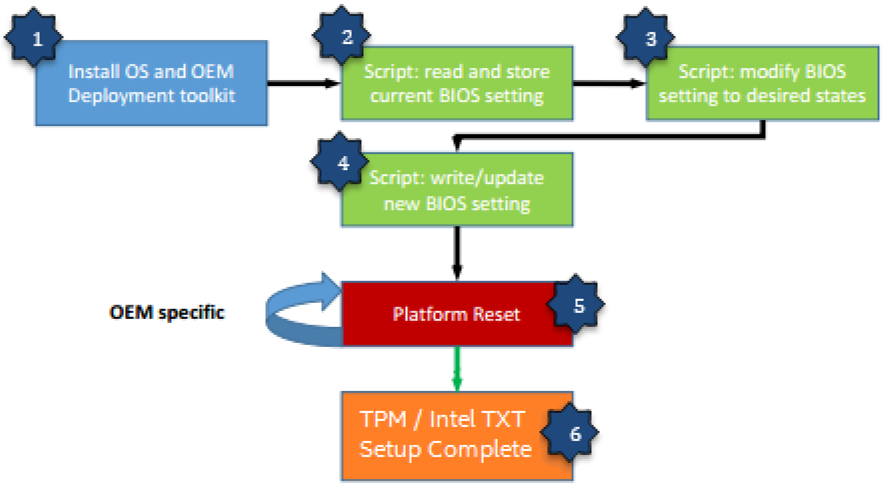

INTEL® TXT
INTEL TRUSTED EXECUTION TECHNOLOGY
SYSTEM
INTEL TXT
HARDWARE
1. SYSTEM POWERS ON AND INTEL TXT VERIFIES SYSTEM BIOS/FIRMWARE
2. HYPERVISOR MEASURE MATCHES
MATCH
HYPERVISOR
HARDWARE
3. OS & APPLICATIONS ARE LAUNCHED
OS/ APPS
OS/ APPS
HYPERVISOR
HARDWARE
NO MATCH
HYPERVISOR
HARDWARE
2. HYPERVISOR MEASURE DOES NOT MATCH
HARDWARE
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
Install OS and OEM Deployment toolkit
2
Script: read and store current BIOS setting
3
Script: modify BIOS setting to desired states
4
Script: write/update new BIOS setting
OEM specific
Platform Reset
5
TPM / Intel TXT Setup Complete
6

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 Corporation 2014

Intel TXT Scale Provisioning for DELL PowerEdge 12G Servers

The Dell OpenManage Deployment Toolkit (DTK) is a bare metal automation toolkit that allows you to collect BIOS settings, then script the BIOS changes needed to enable the Intel TXT components.

The DELL OpenManage DTK provides these benefits:

- Provides the tools necessary to automate the pre-operating system configuration tasks and the unattended operating system installation tasks when deploying PowerEdge systems.
- Scales to support from one to many system deployment efforts.
- Facilitates consistent system configurations across multiple systems.
- Provides diverse and useful deployment tools that can be utilized in many different ways.

Dell OpenManage DTK RPM Installation

If you have already downloaded the OpenManage DTK, here is a quick RPM installation – some content may be different depending on versions that you have downloaded:

Authenticate to the DELL iDRAC

- Enter username and password
- Open a terminal
- Mount the DTK through virtual media or DVD
- Navigate to directory in the media
- Change directory to RPMs and find the appropriate OS (example cd /RPMs/rhel6/x86_64/)
- Install the dependent libsmbios RPM
  - rpm -ivh libsmbios-2.2.27-4.9.1.el6x86_64.rpm
- Install the dependent smbios RPM
  - rpm -ivh smbio-utils-bin *******.rpm
- Install all the dependent RPMs using srvadmin*
  - rpm -ivh srvadmin*
- Install syscfg RPM for BIOS
  - rpm -ivh syscfg*********.rpm
- Install dtk scripts RPM
  - rpm -ivh dtk-scripts******.rpm
- Start all the srvadmin services
  - /opt/dell/srvadmin/sbin/srvadmin-services.sh start
- Export all the PATHs (they're included them in the script below)
- Test out run any syscfg command
  - syscfg -o test.ini
- Use an editor (vi or nano) to modify if needed

© Intel Corporation 2014

Here is an example of the configuration script that can be run on the DELL PowerEdge 12G 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
export PATH=$PATH:/opt/dell/toolkit/bin/
export LD_Library_PATH=/opt/dell/toolkit/bin/
export PATH=$PATH:/opt/dell/srvadmin/sbin/

./syscap.sh sample.ini
cat sample.ini | sed -e
“s/ProcVirtualization=disable/ProcVirtualization=enable/;s/TpmSecurity=off/TpmSecurity=onpbm/;s/TpmActivation=nochange/TpmActivation=activate/;s/IntelTxt=off/IntelTxt=on/;s/;TpmActivation/TpmActivation/;s/;IntelTxt/IntelTxt/" > sample1.ini
./sysrep.sh sample1.ini
init 6
```

Note: setup passwords and system passwords cannot be cleared using the DTK on DELL systems prior to 12G systems.

How to check the Intel TXT/TPM status

Linux Distributions

Assumption:

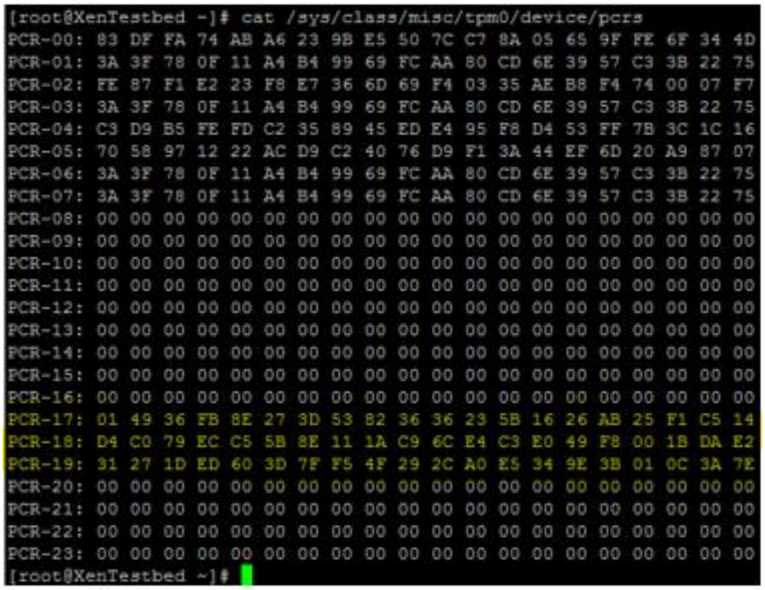
- Users have successfully activated Intel TXT in BIOS and OS by following the respective guides.
- To Activate the Intel TXT in Linux OS users are requested to follow the Intel TXT OS Setup Guide.
- TPM Status Can be read from linux OS through TPM Device Driver in Dom0.
- Issue below command to find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

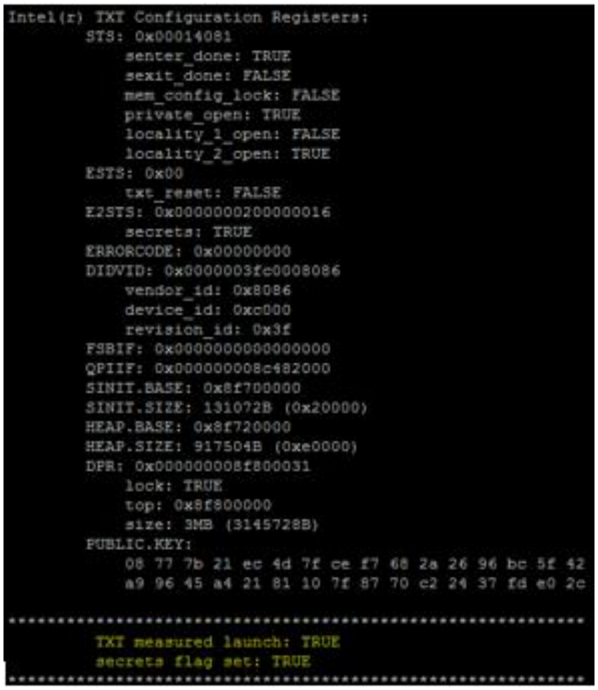


```
[root@XenTestbed ~]# cat /sys/class/misc/tpm0/device/pcrs
PCR-00: 83 DF FA 74 AB A6 23 9B E5 50 7C C7 8A 05 65 9F FE 6F 34 4D
PCR-01: 3A 3F 78 0F 11 A4 B4 99 69 FC AA 80 CD 6E 39 57 C3 3B 22 75
PCR-02: FE 87 F1 E2 23 F8 E7 36 6D 69 F4 03 35 AE B8 F4 74 00 07 F7
PCR-03: 3A 3F 78 0F 11 A4 B4 99 69 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 00
PCR-09: 00 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 00
PCR-11: 00 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 00
PCR-13: 00 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 00
PCR-15: 00 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 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 00
PCR-21: 00 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 00
PCR-23: 00 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.

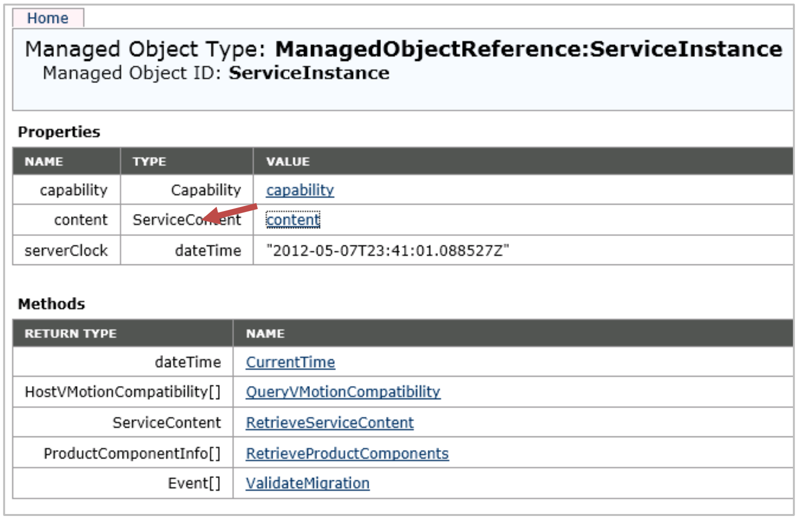
$ tcsd
$ txt-stat | more



```
Intel(r) TXT Configuration Registers:
        STS: 0x00014081
            senter_done: TRUE
            sexit_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: 0x000000008f800031
            lock: TRUE
            top: 0x8f800000
            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:

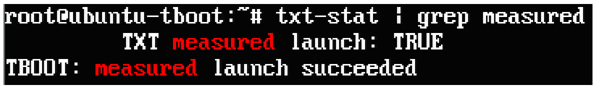
- If *ESXi* host is not Intel TXT provisioned then you will not see any PCR values in step 13.
- If users are sure that TPM is provisioned correctly but TPM value is unset in v-center then as a work around, disconnects the host and reconnects the host if the TPM value is unset.

Troubleshooting Guide

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

In Linux Distributions:

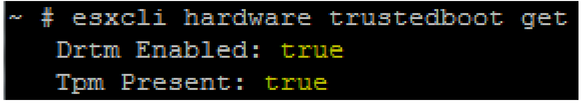
Use txt-stat tool to check if the Intel TXT launch is successful.



```
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



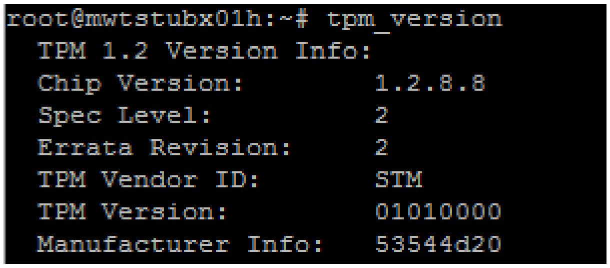
```
~ # esxcli hardware trustedboot get
   Drtm Enabled: true
   Tpm Present: true
```

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
```

© Intel Corporation 2014