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  
Cisco Rack Servers – C220M3 ...................................................... 4  
  Platform Expectations ............................................................ 4  
  Out of the Box Configuration .................................................. 4  
  TPM Clear and Reactivate Intel TXT/TPM .................................... 8  
Cisco Blade Server – B200M3 ....................................................... 9  
  Platform Expectations ............................................................ 9  
  Out of the Box Configuration .................................................. 9  
  TPM Clear and Reactivate Intel TXT/TPM .................................... 9  
Scaling Activation of Intel TXT/TPM across Multiple Systems ............... 10  
  Bare Metal Provisioning of Intel TXT ........................................... 11  
    Intel TXT Scale Provisioning for Cisco Rack and Blade Servers .......... 11  
How to check the Intel TXT/TPM status ....................................... 12  
  Linux Distributions .................................................................. 12  
  VMware ESXi 5.x ....................................................................... 13  
Troubleshooting Guide ............................................................... 14
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 Cisco* UCS server platforms based on the Intel Xeon processor E5-2600 V2 family. The examples given will work for the M3-generation servers: B200, B22, B420 blades and C220, C240, C22 and C24 rack based platforms – some screens may differ from what is shown.

- 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 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
Cisco Rack Servers - C220M3

Platform Expectations

- Cisco ships the server only in legacy BIOS mode
- Cisco ships SINIT ACM as part of BIOS
- After TPM clear Actions, two reboots are required to get the proper Intel TXT measurements
- Configuration should be similar for the C240, C22 and C24 rack based platforms as well.

Out of the Box Configuration

1. Press F2 to Enter in to BIOS console
2. Ensure the Intel VT/Intel VT-d are enabled under Advanced > Processor Configuration
3. BIOS console > Security > *set Administrator Password* save settings and reboot the server

4. Press **F2** and enter the Password to enter to BIOS console

5. Enable the TPM support [BIOS setting > Advanced > TPM support > Enabled and reboot]
6. Activate Intel TXT BIOS setting > Trusted Computing > TXT Support > Enabled
7. Press F10 to save the settings and reboot the server **Ctl+Alt+Del**
8. Press F2 and enter the Password to enter to BIOS console
9. Ensure TPM state is enabled **BIOS setting > Advanced > TPM state > enabled**

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.

1. Press **F2** key to enter to BIOS console
2. BIOS console > **Advanced > Security > Set Administrator Password** > “enter password twice”
3. BIOS console > **Advanced > TPM State > Disabled**
4. Save Settings and Reboot the Server **Ctl+Alt+Del**
5. Press **F2** key again to enter to BIOS console
6. BIOS console > **Advanced > Security > Set Administrator Password** > “enter password twice”
7. BIOS console > **Advanced > TPM Support > Enabled**
8. Save Settings and Reboot **Ctl+Alt+Del**
9. Press **F2 > BIOS Setting > Advanced > TPM State > Enabled**
10. Esc key twice
11. Bios Settings > **Advanced > Trusted Computing > TXT support > Enabled**
12. Save Settings and Reboot **Ctl+Alt+Del**

Note: Ensure the current Status Information under BIOS settings > Advanced > Current Status Info
Cisco Blade Server – B200M3

Platform Expectations
- Cisco ships the server only in legacy BIOS mode
- Cisco ships SINIT ACM as part of BIOS
- After TPM clear Actions, two reboots are required to get the proper Intel TXT measurements
- Configuration should be similar for the B22 and B420 blade based platforms as well.

Out of the Box Configuration
1. Press **F2** key to enter to BIOS console
2. BIOS console > **Advanced** > **TPM Support** > **Enabled**
3. Save Settings and Reboot **Ctl+Alt+Del**
4. **F2** > BIOS Console > **Advanced** > **TPM State** > **Enabled**
5. Esc key twice
6. Advanced > **Trusted Computing** > **TXT support** > **Enabled**
7. Save Settings and Reboot **Ctl+Alt+Del**

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. Reboot is required to activate the TPM/Intel TXT again.
1. Press **F2** key to enter to BIOS console
2. BIOS console > **Advanced** > **Security** > **Set Administrator Password** > "enter password twice"
3. BIOS console > **Advanced** > **TPM State** > **Disabled**
4. Save Settings and Reboot the Server **Ctl+Alt+Del**
5. Press **F2** key again to enter to BIOS console
6. BIOS console > **Advanced** > **Security** > **Set Administrator Password** > "enter password twice"
7. BIOS console > **Advanced** > **TPM Support** > **Enabled**
8. Save Settings and Reboot **Ctl+Alt+Del**
9. Press **F2** > **BIOS Setting** > **Advanced** > **TPM State** > **Enabled**
10. Esc key twice
11. Bios Settings > Advanced > Trusted Computing > TXT support > Enabled
12. Save Settings and Reboot Ctrl+Alt+Del

Note: Ensure the current Status Information under BIOS settings > Advanced > Current Status Info

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.

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 Cisco Rack and Blade Servers**

Cisco UCS provides the Server Configuration Utility, which is a bootable image that can perform BIOS modifications, install operating systems, and diagnostics of Cisco UCS servers. As of the publication date, the Cisco UCS Server Configuration Utility does not have a scale enabling tool available for Intel TXT activation. Please check with your Cisco representative for potential plans to optimize this solution.
How to check the Intel TXT/TPM status

Linux Distributions

Assumptions:
- Users have successfully activated Intel TXT in BIOS and OS by following the respective guides.
- To Activate 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.

“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 vCenter 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 IntelTXT launch is successful.

   In VMware ESXi:
   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@mwtsnbx01h:~# tpm_version
TPM 1.2 Version Info:
Chip Version: 1.2.8.8
Spec Level: 2
Errata Revision: 2
TPM Vendor ID: 5TM
TPM Version: 01010000
Manufacturer Info: 53544d20
```