Installing and Configuring the TPM module

To integrate the TPM module, hardware-wise, follow these steps:

- **1.** Turn off the power to the system, all drives, enclosures, and system components. Remove the power cord(s).
- 2. Remove the server cover. For instructions, see your server system documentation.
- **3.** Insert the standoff into the hole in the server/workstation board and insert the TPM module connector into the connector in the board. To locate the TPM module connector and the hole on your server/workstation board, see your server/workstation board documentation.
- **4.** Press down gently but firmly to ensure that the module is properly seated in the connectors, and then tighten the tamper resistant screw.

To configure the TPM module, follow these guidelines:

- 1. Restart the system into the BIOS.
- 2. Enable UEFI mode; this is under BIOS / Boot maintenance Manager / Advance Boot options / Boot Mode

	Advanced Boot Options	3
System Boot Timeout Boot Mode Boot Option Retry USB Boot Priority Static Boot Order Reset Static Boot Order	[0] <legacy> <disabled> <enabled> <disabled> <no UEFT Legacy</no </disabled></enabled></disabled></legacy>	When Boot Mode is Legacy, the BIOS only loads modules required for booting Legacy Operating Systems. When Boot Mode is UEFI, the BIOS only loads modules required for booting UEFI-aware Operating Systems.
t↓=Move Highlight <0 Copuright	Enter>=Complete Entry (c) 2010-2016, Intel C	Esc=Exit Entry Corporation

- 3. Press: F10 / Press: Y / System reboots / Go to BIOS again
- 4. Once back into the BIOS, go into the Security tab, and set the Administrator Password.

6. Once back into the BIOS, go back to Security tab, and hit Enter on "TPM2 Operation", and on "Clear TPM2 ClearControl (NO) + Clear"

	Security	
Administrator Password Status User Password Status	Installed Not Installed	Select one of the supported operation to change TPM2 state.
Set Administrator Password Set User Password Power On Password Front Panel Lockout	rd Action 2 ClearControl(NO) + Clear	
Current TPM Device	TPM 2.0 (DTPM)	
TPM2 Physical Presence Op TPM2 Operation	<mark>veration</mark> KNo Action>	
↑↓=Move Highlight <f Copyright</f 	Cnter>=Complete Entry Es (c) 2010-2016, Intel Corpo	c=Exit Entry ration

- 7. Press: F10 / Press: Y / System reboots
- **8.** Press F12 and then, enter the BIOS, again.



9. Once back into the BIOS, go into the Advance/ Integrated IO configuration menu and activate "Intel (R) VT for Directed I/O".

Integrated IO Configuration		
NTB PCIe Port on CPU socket 1 Relaxed Ordering Intel(R) UT for Directed I/O Snooped Response Wait Time for Posted Prefetch ► IOU Non-Posted Prefetch C	<transparent bridge=""> <enable> <disable> <enabled <enabled="" disabled="" ontr<="" th=""><th>Enable/Disable Intel (R) Uirtualization Technology for Directed I/O (Intel (R) UT-d). Report the I/O device assignment to UMM through DMAR ACPI Tables.</th></enabled></disable></enable></transparent>	Enable/Disable Intel (R) Uirtualization Technology for Directed I/O (Intel (R) UT-d). Report the I/O device assignment to UMM through DMAR ACPI Tables.
t↓=Move Highlight <e Copyright</e 	nter>=Complete Entry E: (c) 2010-2016, Intel Corp	sc=Exit Entry pration

10. Go into the Advance/Processor Configuration and enable both, the "Intel (R) Virtualization Technology and "Intel (R) TXT" options:

Processor Configuration		
Processor 2 Version	-2667 v3 @ 3.20GHz Not Present	† Scroll Up Intel (R) Uirtualization Technology allows a platform to run
Intel(R) Hyper-Threading Tech Active Processor Cores Execute Disable Bit Intel(R) Virtualization	<enabled> <a disabled<="" enabled="" td=""><td>multiple operating systems and applications in independent partitions.</td></enabled>	multiple operating systems and applications in independent partitions.
Intel(R) IXT Enhanced Error Containment Mode	<disabled> <disabled></disabled></disabled>	Note: A change to this option requires the system to be
MLC Streamer MLC Spatial Prefetcher	<enabled> <enabled></enabled></enabled>	powered off and then Hore (D/d) ↓ Scroll Down
1∔=Move Highlight <e Copyright</e 	nter>=Complete Entry (c) 2010-2016, Intel Co	Esc=Exit Entry rporation
		Configuration changed

Note: If "Intel (R) TXT" field appears gray and cannot be modified (as shown in previous picture), you need to save the changes (Pressing F10 and then Y), reboot and enter BIOS, again, to finally enable the "Intel (R) TXT" option as shown below:

Processor Configuration		
L3 Cache RAM	20480KB I N/A	† Scroll Up Enable/Disable
Processor 1 Version	Intel(R) Xeon(R) CPU E5 -2667 v3 @ 3,206Hz	Intel(R) Trusted Execution Technology.
Processor 2 Version	Not Present	Takes effect after reboot.
Intel (R) Hyper-Threading Tech Active Processor Cores Execute Disable Bit Intel (R) Virtualization Technology Intel (R) TAT Enhanced Error Containment Mode	CE Enabled Disabled (function of the state o	
		4 Scroll Down
1∔=Move Highlight <e Copyright</e 	inter≻=Complete Entry Es (c) 2010-2016, Intel Corpo	c=Exit Entry ration

11. Save the changes, exit the BIOS, and reboot the system into the Operating System. Thus, in order to see the TPM 2.0 device as enable/usable, go into the Device Manager, under Security Devices, as shown below:



Alternatively, go into the Windows Trusted Platform Module Management (cmd command: > tpm.msc); under the Status section, you will see that the TPM is ready to be utilized, as shown below.

		^
Windows computers containing the eatures for applications. This sna configure the device. It also allow	he Trusted Platform Module (TPM) security hardware provide enhanced security ap-in displays information about the computer's TPM and allows administrators to vs administrators to view and manage commands understood by the Sevice.	
Status		•
The TPM is ready for use.		
TPM Management		•
Change TPM owner passw	rord. 🧔	
Clear the TPM to remove o	wnership and reset the TPM to factory defaults.	