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.

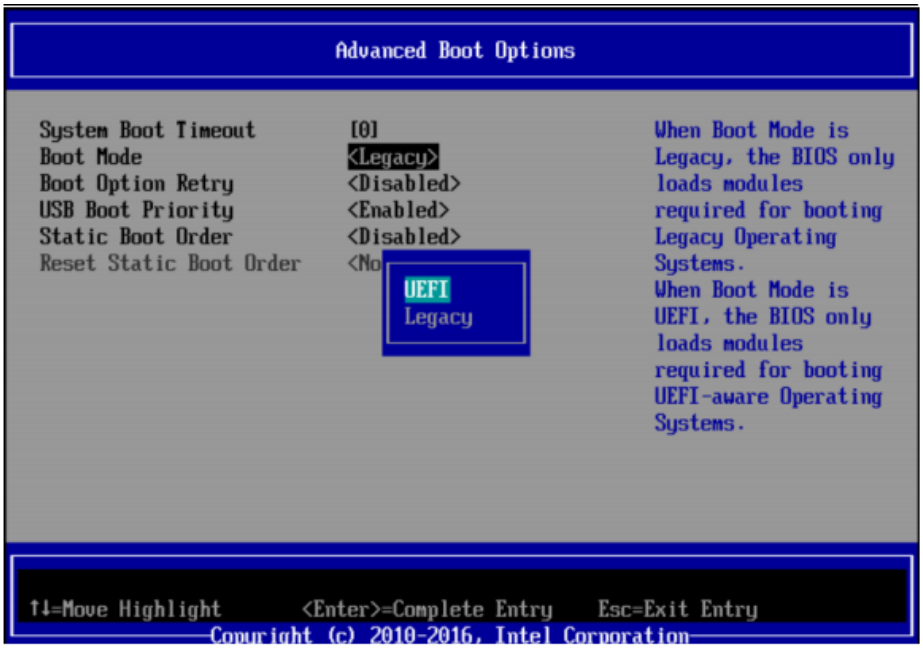
3. Insert the standoff into the hole in the server/workstation board and insert the TPM module connector into the connector in the board. To locate the TPM module connector and the hole on your server/workstation board, see your server/workstation board documentation.

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.

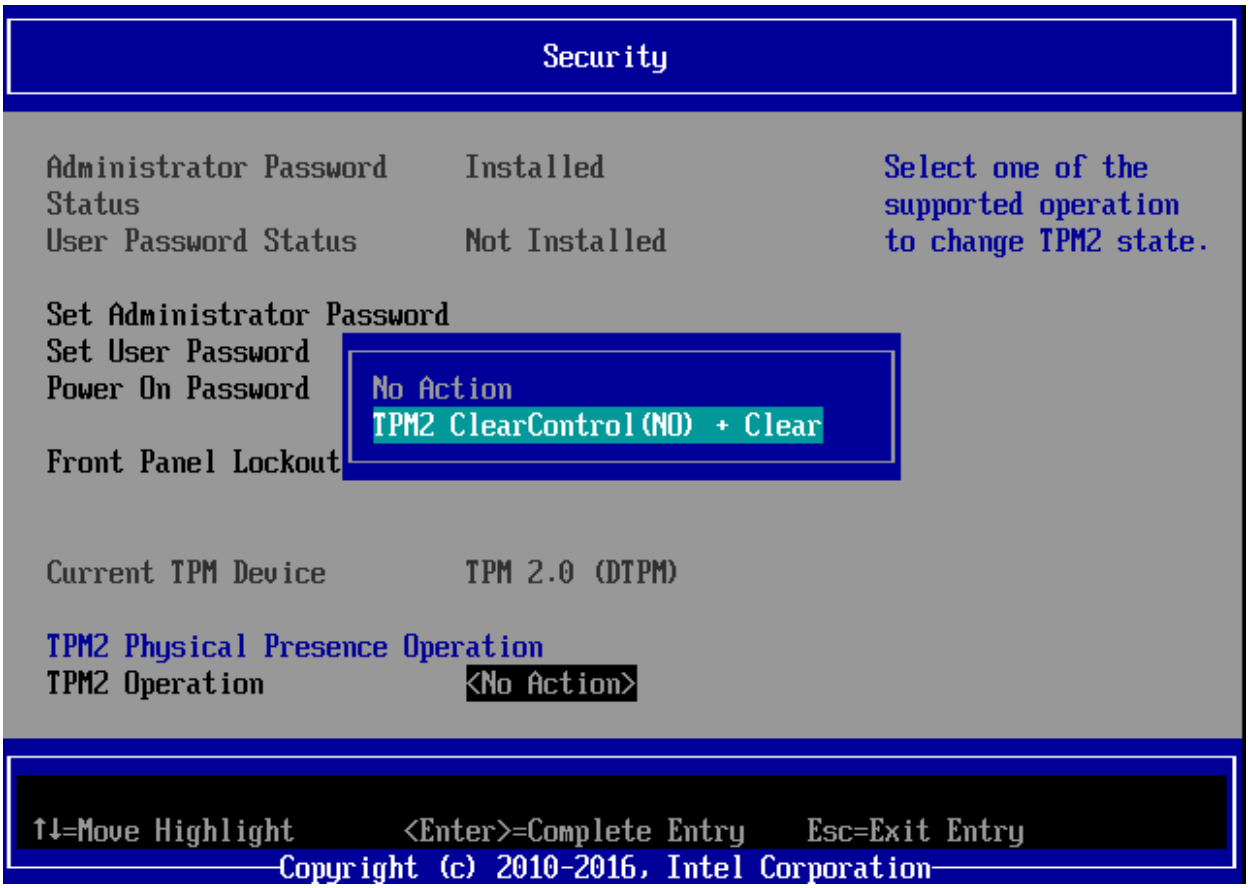
2. Enable UEFI mode; this is under BIOS / Boot maintenance Manager / Advance Boot options / Boot Mode



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.

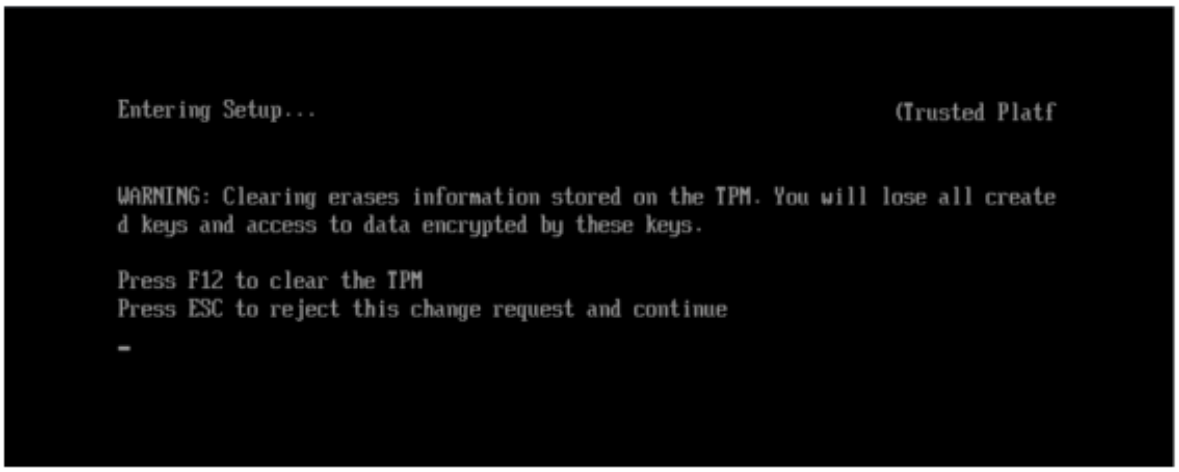
5. Press: F10 / Press: Y / System reboots / Go to BIOS again

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

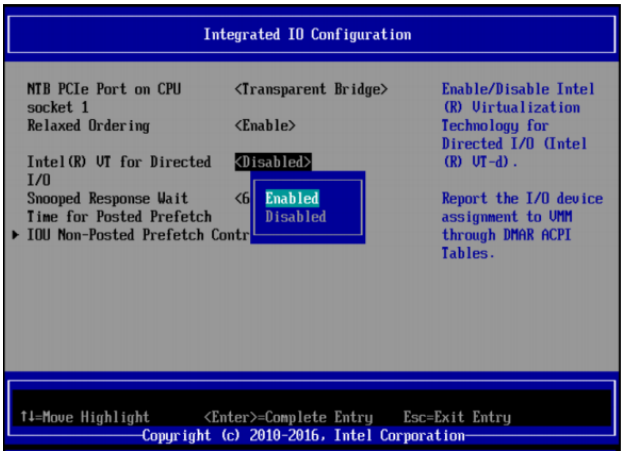


7. Press: F10 / Press: Y / System reboots

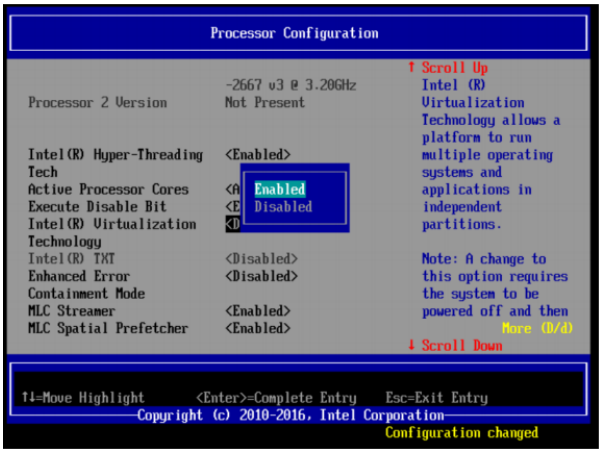
8. Press F12 and then, enter the BIOS, again.



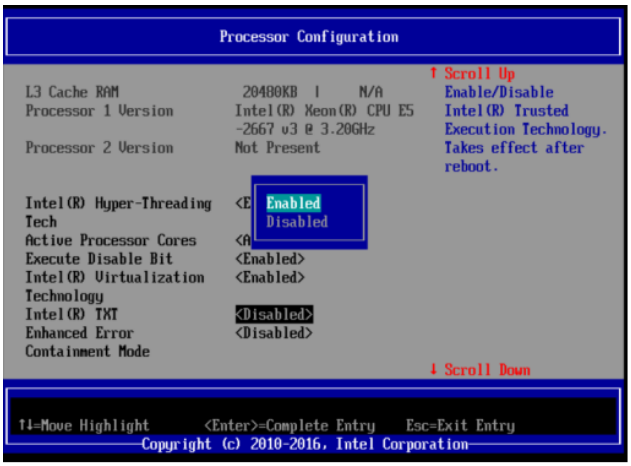
9. Once back into the BIOS, go into the Advance/ Integrated IO configuration menu and activate “Intel (R) VT for Directed I/O”.



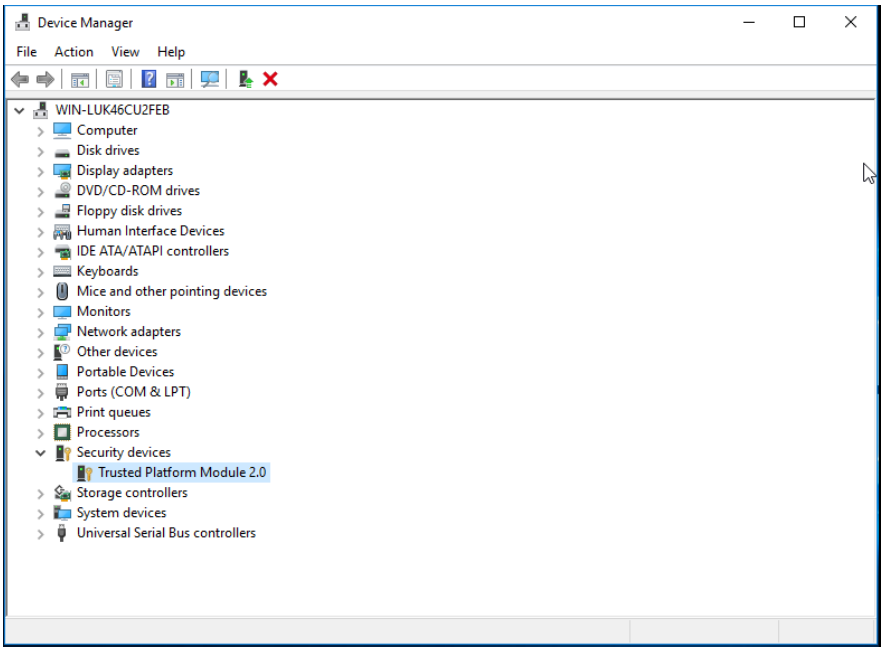
10. Go into the Advance/Processor Configuration and enable both, the “Intel (R) Virtualization Technology and “Intel (R) TXT” options:



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:



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.