msi

Infineon TPM Module
MS-4136
Firmware Update

EXCLUSIVE msi WORLD'S FIRST msi
NEXT GAMING DIMENSION

MGA

SOME ARE PC, WE ARE GAMING TRUE GAMING

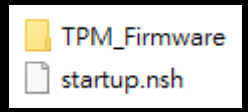
Download files

Download TPMFWupdate.zip

https://www.dropbox.com/s/ri3syiozx1icbia/TPMFWupdate.zip?dl=0

Extract TPMFWupdate.zip

Copy TPM_Firmware and startup.nsh to root folder of USB flash drive



How to setup?

Remove all storage devices from your motherboard

Only insert USB flash drive to your motherboard

How to setup?

- Intel 100, 200, 300, X299 series motherboards

SETTINGS \ Security \ Trusted Computing \

Security Device Support = [Disabled]

TPM Device Selection = [dTPM]

GAMING Series

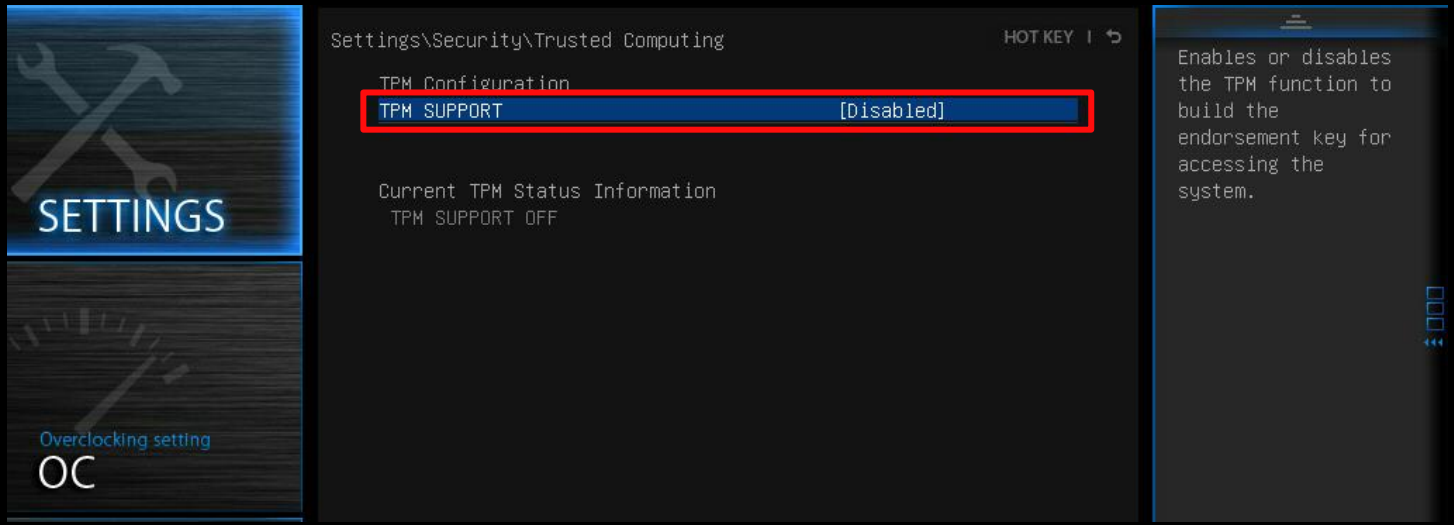
PRO Series

How to setup?

- Intel 8, 9 series motherboards

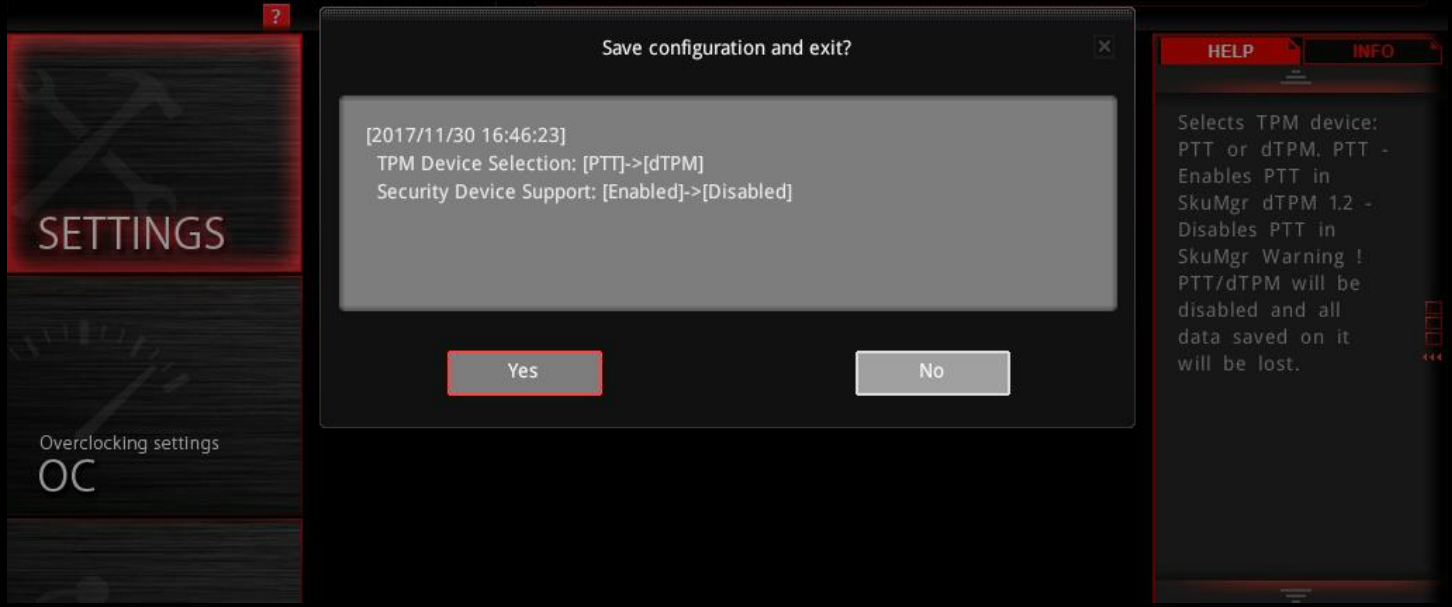
SETTINGS \ Security \ Trusted Computing \

TPM Support = [Disabled]



How to setup?

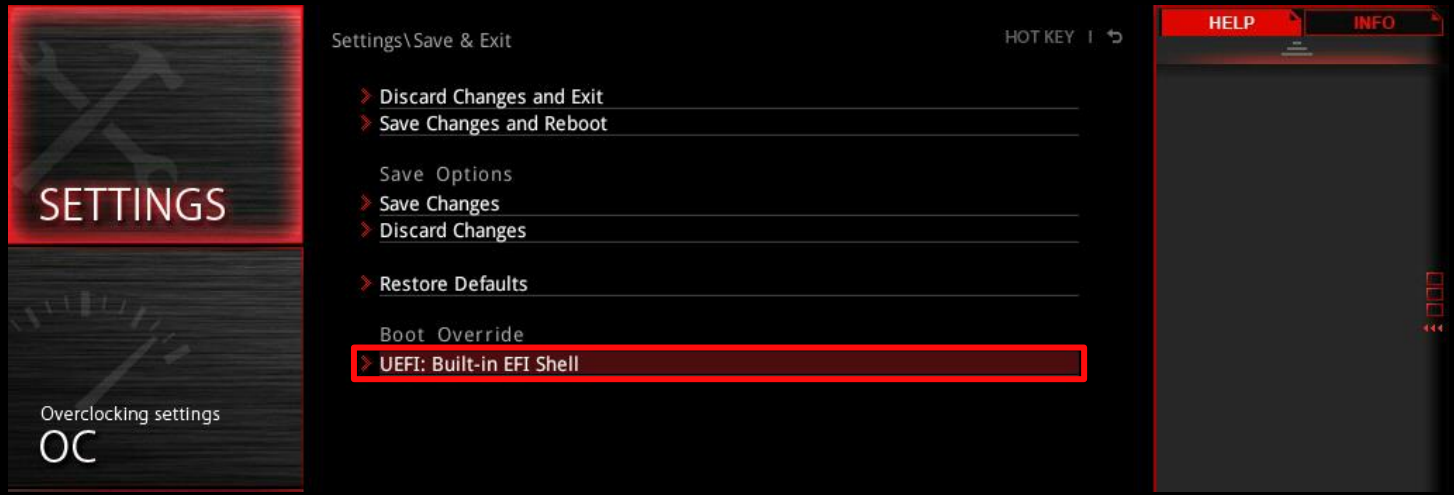
Press F10 to save settings and boot into BIOS again



How to setup?

Boot into EFI Shell

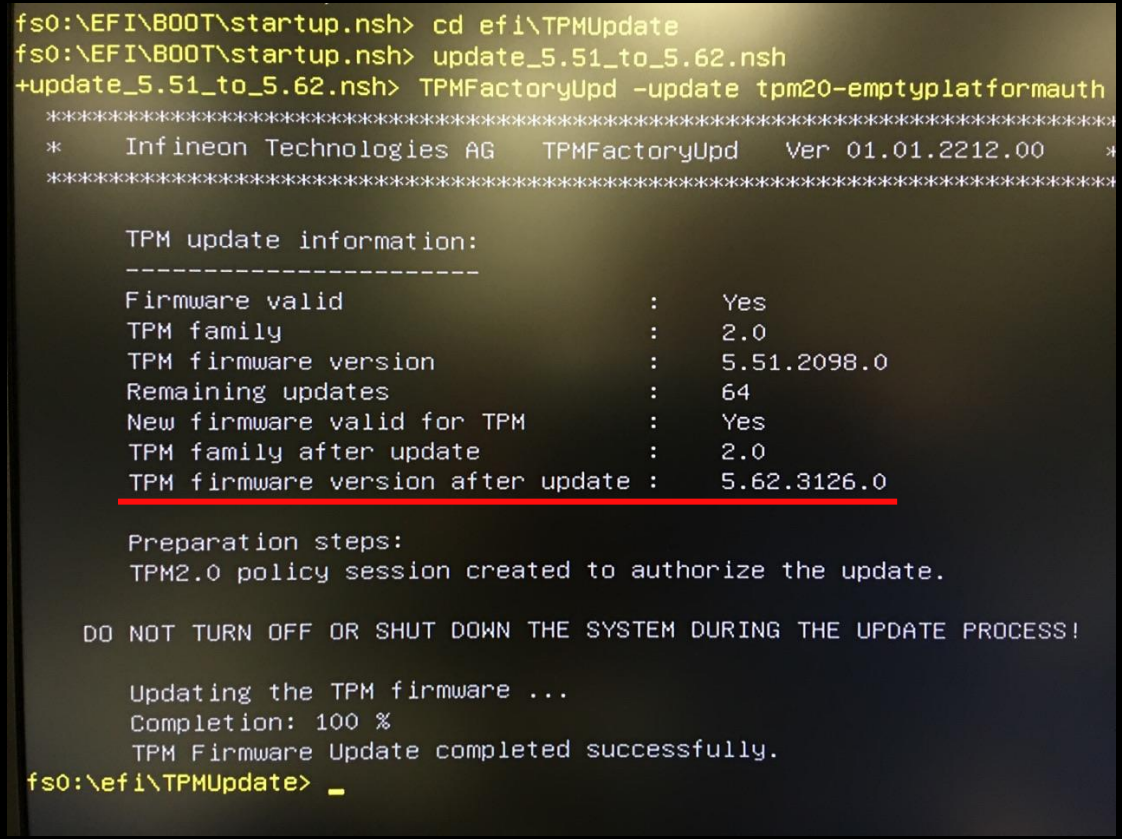
SETTINGS \ Save & Exit \ UEFI: Built-in EFI Shell



FW Update

System boots into EFI Shell and updates firmware Automatically

New version 5.62.3126.0




msi
TRUE GAMING
SOME ARE PC, WE ARE GAMING