



msi

Infineon TPM Module
MS-4136
Firmware Update



SOME ARE PC, WE ARE GAMING TRUE  GAMING

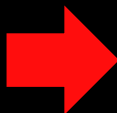
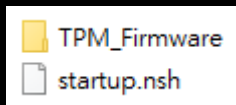
Download files

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]



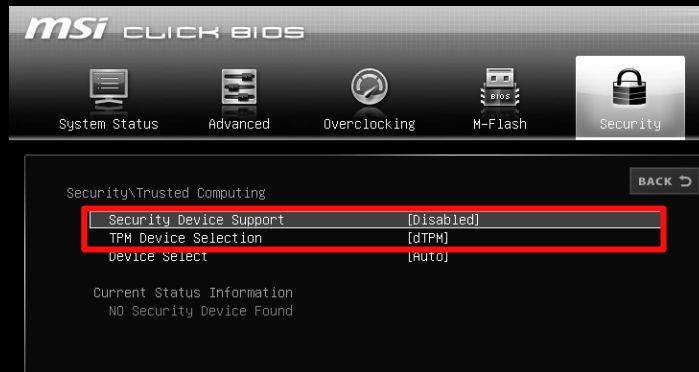
Settings\Security\Trusted Computing

HOT KEY | ↵

Security Device Support	[Disabled]
TPM Device Selection	[dTPM]
Device Select	[Auto]

Current Status Information
NO Security Device Found

GAMING Series



msi CLICK BIOS

System Status Advanced Overclocking M-Flash Security

Security\Trusted Computing

BACK ↵

Security Device Support	[Disabled]
TPM Device Selection	[dTPM]
Device Select	[Auto]

Current Status Information
NO Security Device Found

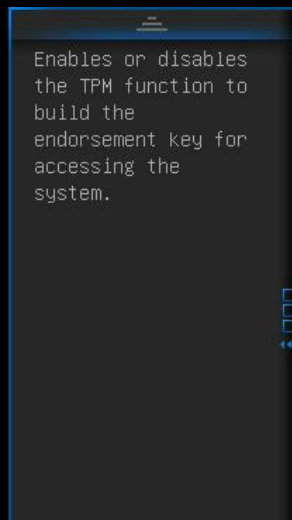
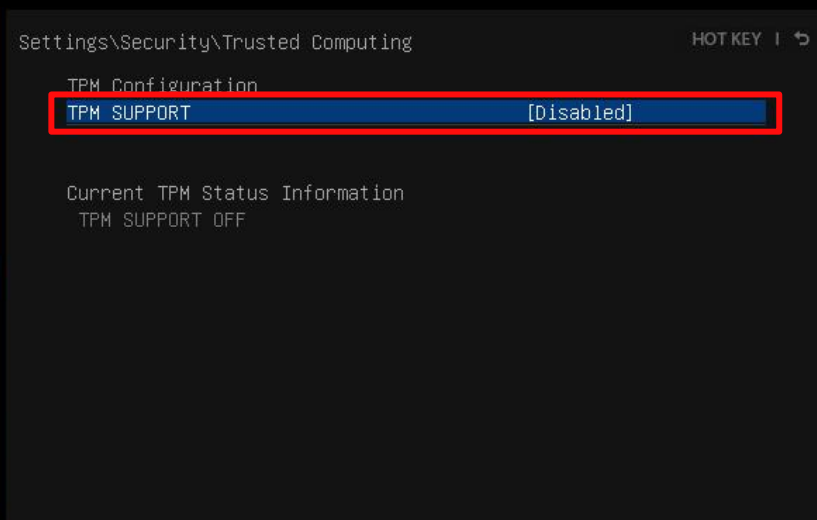
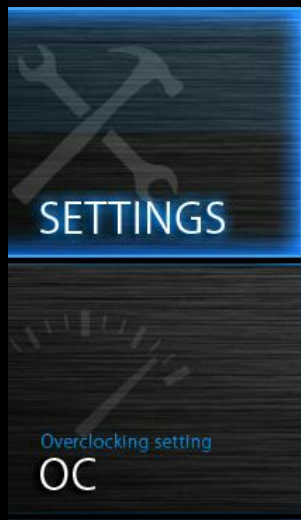
PRO Series

How to setup?

➡ Intel 8, 9 series motherboards

SETTINGS \ Security \ Trusted Computing \

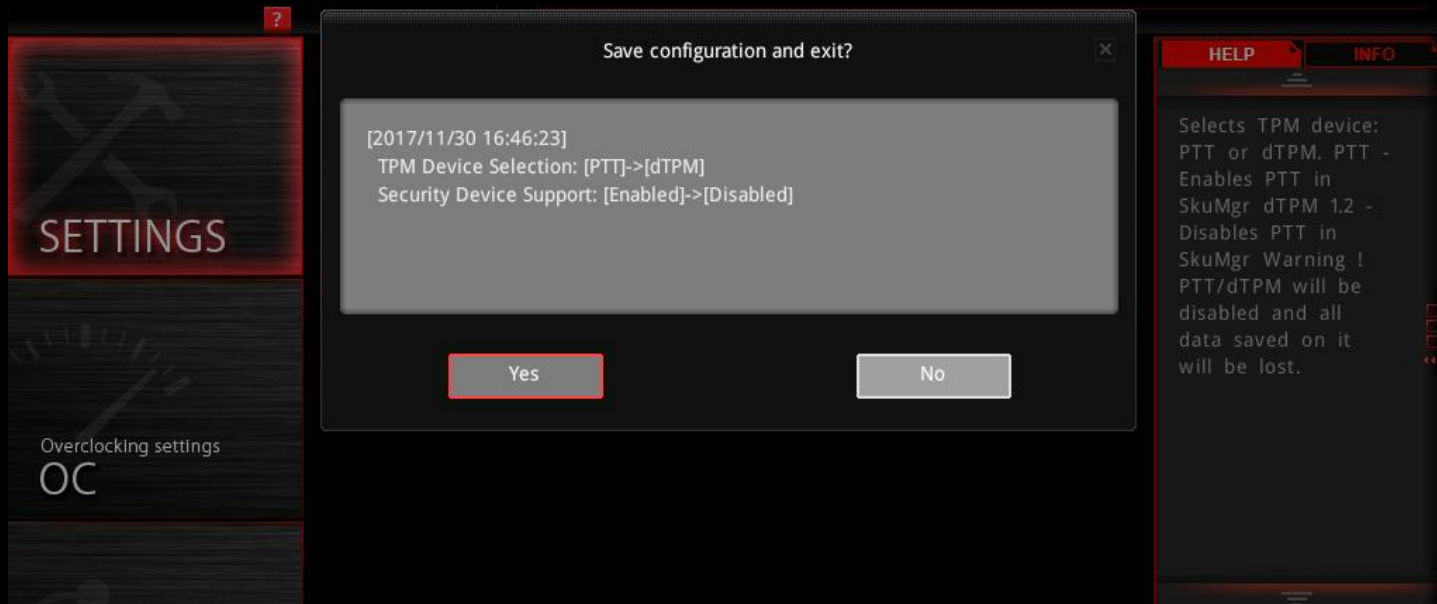
TPM Support = [Disabled]



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



Settings\Save & Exit

HOT KEY | ↩

- > Discard Changes and Exit
- > Save Changes and Reboot

Save Options

- > Save Changes
- > Discard Changes

- > Restore Defaults

Boot Override

- > UEFI: Built-in EFI Shell



FW Update

System boots into
EFI Shell and
updates firmware
Automatically

New version
5.62.3126.0

```
fs0:\EFI\BOOT\startup.nsh> cd efi\TPMUpdate
fs0:\EFI\BOOT\startup.nsh> update_5.51_to_5.62.nsh
+update_5.51_to_5.62.nsh> TPMFactoryUpd -update tpm20-emptyplatformauth
*****
* Infineon Technologies AG TPMFactoryUpd Ver 01.01.2212.00 *
*****

TPM update information:
-----
Firmware valid                : Yes
TPM family                    : 2.0
TPM firmware version          : 5.51.2098.0
Remaining updates             : 64
New firmware valid for TPM    : Yes
TPM family after update       : 2.0
TPM firmware version after update : 5.62.3126.0

Preparation steps:
TPM2.0 policy session created to authorize the update.

DO NOT TURN OFF OR SHUT DOWN THE SYSTEM DURING THE UPDATE PROCESS!

Updating the TPM firmware ...
Completion: 100 %
TPM Firmware Update completed successfully.
fs0:\efi\TPMUpdate> _
```




msi®

TRUE **G**AMING
SOME ARE PC, WE ARE GAMING