msi TPM 2.0 Trusted Platform Module User Guide

Contents

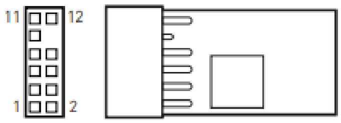
msi

msi TPM 2.0 Trusted Platform Module

About Trusted Platform Module (TPM)

Trusted Platform Module (TPM) is a security technology that uses cryptography to store essential and critical information on PCs. TPM can protect your important data from malware or malicious attack by generating and validating the encryption keys.

Overview of TPM 2.0 card



Specifications

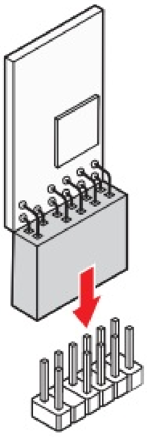
Chipset	SLB 9672 VU 2.0 FW 15.22
Interface	SPI
Form Factor	0.5079 in. x 0.8469 in. (12.90 x 21.51 mm)
OS	*Supports Windows® 11, Windows® 10

Supported motherboards

Intel®	AMD
Intel® 400 series	AMD X570 series (SPI)
Intel® 500 series	AMD B550 series
Intel® 600 series	AMD A520 series
Intel® 700 series	AMD X670 series
Intel® W790 series	AMD B650 series

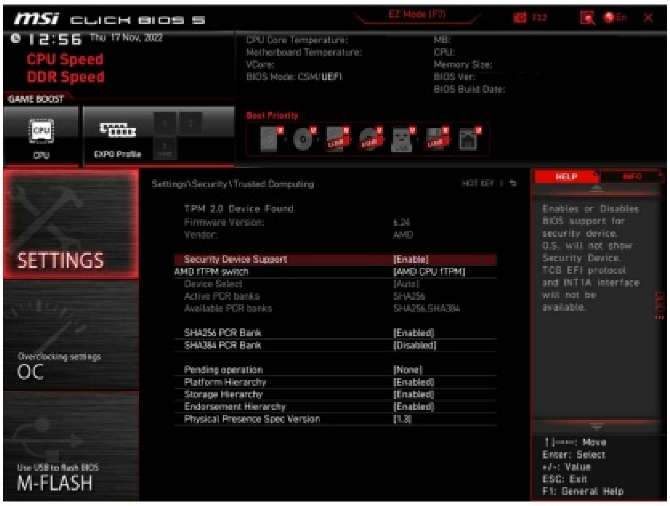
Installing TPM 2.0 card onto the Motherboard
Insert TPM 2.0 card to the TPM pin header on your motherboard.

Pin	Signal Name	Pin	Signal Name
1	SPI Power	2	SPI Chip Select
3	Master In Slave Out (SPI Data)	4	Master Out Slave In (SPI Data)
5	Reserved	6	SPI Clock
7	Ground	8	SPI Reset
9	Reserved	10	No Pin
11	Reserved	12	Interrupt Request



Enabling the TPM via the BIOS For AMD platforms

- Press to enter the BIOS Setup program at the system startup.
- Press to enter the Advanced Mode.
- Go to Settings > Security > Trusted Computing.
- Set Security Device Support to [Enable].

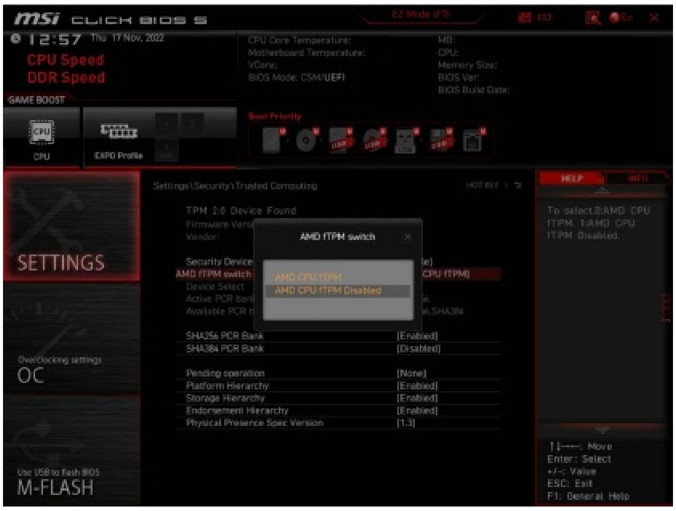


```
12:56 Thu 17 Nov, 2022
CPU Speed
DDR Speed
CPU Core Temperature:                 MB:
Motherboard Temperature:              CPU:
VCore:                                Memory Size:
BIOS Mode: CSM/UEFI                   BIOS Ver:
                                      BIOS Build Date:

Settings\Security\Trusted Computing                HOT KEY

  TPM 2.0 Device Found
  Firmware Version:                   6.24
  Vendor:                             AMD

  Security Device Support             [Enable]
AMD fTPM switch                       [AMD CPU fTPM]
  Device Select                       [Auto]
  Active PCR banks                    SHA256
  Available PCR banks                 SHA256,SHA384

  SHA256 PCR Bank                     [Enabled]
  SHA384 PCR Bank                     [Disabled]

  Pending operation                   [None]
  Platform Hierarchy                  [Enabled]
  Storage Hierarchy                   [Enabled]
  Endorsement Hierarchy               [Enabled]
  Physical Presence Spec Version      [1.3]
```

Enables or Disables BIOS support for security device. O.S. will not show Security Device. TCG EFI protocol and INT1A interface will not be available.

```
↑↓←→: Move
Enter: Select
+/-: Value
ESC: Exit
F1: General Help
```

- Set AMD fTPM switch to [AMD CPU fTPM Disabled]

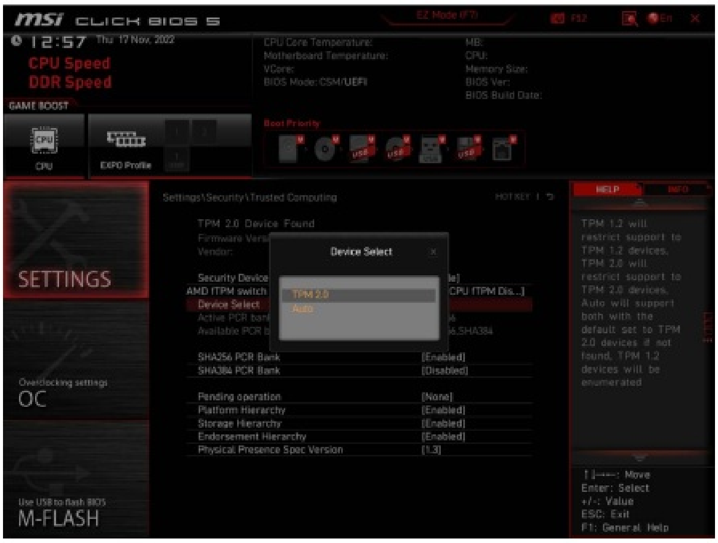


```
12:57 Thu 17 Nov, 2022
CPU Speed
DDR Speed
CPU Core Temperature:                 MB:
Motherboard Temperature:              CPU:
VCore:                                Memory Size:
BIOS Mode: CSM/UEFI                   BIOS Ver:
                                      BIOS Build Date:

Settings\Security\Trusted Computing                HOT KEY

  TPM 2.0 Device Found
  Firmware Versi
  Vendor:

  Security Device                     le]
AMD fTPM switch                       CPU fTPM]
  Device Select
  Active PCR ban                      6
  Available PCR b                     6,SHA384

  SHA256 PCR Bank                     [Enabled]
  SHA384 PCR Bank                     [Disabled]

  Pending operation                   [None]
  Platform Hierarchy                  [Enabled]
  Storage Hierarchy                   [Enabled]
  Endorsement Hierarchy               [Enabled]
  Physical Presence Spec Version      [1.3]

        AMD fTPM switch
        AMD CPU fTPM
        AMD CPU fTPM Disabled
```

To select 0:AMD CPU fTPM, 1:AMD CPU fTPM Disabled.

```
↑↓←→: Move
Enter: Select
+/-: Value
ESC: Exit
F1: General Help
```

- Set Device Select to [TPM 2.0]



```
12:57 Thu 17 Nov, 2022
CPU Speed
DDR Speed
CPU Core Temperature:                 MB:
Motherboard Temperature:              CPU:
VCore:                                Memory Size:
BIOS Mode: CSM/UEFI                   BIOS Ver:
                                      BIOS Build Date:

Settings\Security\Trusted Computing                HOTKEY

  TPM 2.0 Device Found
  Firmware Versi
  Vendor:

  Security Device                     le]
AMD fTPM switch                       CPU fTPM Dis...]
  Device Select
  Active PCR ban                      6
  Available PCR b                     6,SHA384

  SHA256 PCR Bank                     [Enabled]
  SHA384 PCR Bank                     [Disabled]

  Pending operation                   [None]
  Platform Hierarchy                  [Enabled]
  Storage Hierarchy                   [Enabled]
  Endorsement Hierarchy               [Enabled]
  Physical Presence Spec Version      [1.3]

        Device Select
        TPM 2.0
        Auto
```

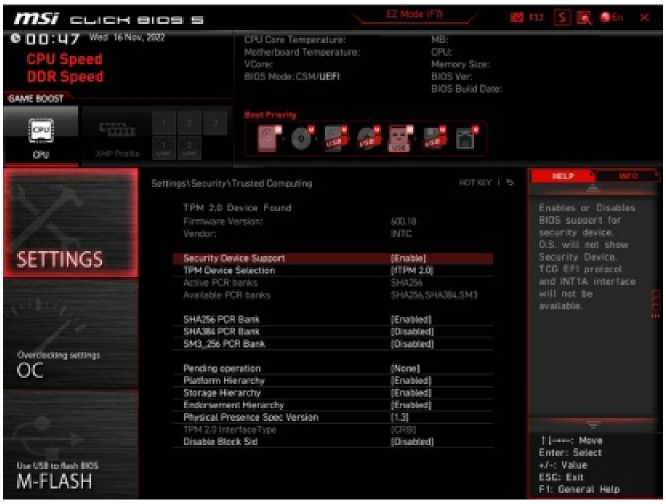
TPM 1.2 will restrict support to TPM 1.2 devices, TPM 2.0 will restrict support to TPM 2.0 devices, Auto will support both with the default set to TPM 2.0 devices if not found, TPM 1.2 devices will be enumerated

```
↑↓←→: Move
Enter: Select
+/-: Value
ESC: Exit
F1: General Help
```

For Intel® platforms

- Press to enter the BIOS Setup program at the system startup.
- Press to enter the Advanced Mode.
- Go to Settings > Security > Trusted Computing.

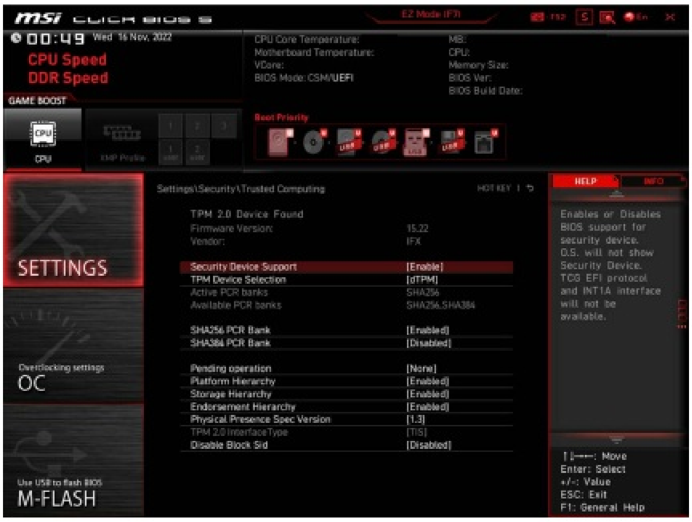
- Set Security Device Support to [Enable].



```
Settings\Security\Trusted Computing

TPM 2.0 Device Found
Firmware Version:                 600.18
Vendor:                           INTC

Security Device Support           [Enable]
TPM Device Selection              [fTPM 2.0]
Active PCR banks                  SHA256
Available PCR banks               SHA256,SHA384,SM3

SHA256 PCR Bank                   [Enabled]
SHA384 PCR Bank                   [Disabled]
SM3_256 PCR Bank                  [Disabled]

Pending operation                 [None]
Platform Hierarchy                [Enabled]
Storage Hierarchy                 [Enabled]
Endorsement Hierarchy             [Enabled]
Physical Presence Spec Version    [1.3]
TPM 2.0 InterfaceType             [CRB]
Disable Block Sid                 [Disabled]
```

Enables or Disables BIOS support for security device. O.S. will not show Security Device. TCG EFI protocol and INT1A interface will not be available.

- Set TPM Device Selection to [dTPM].

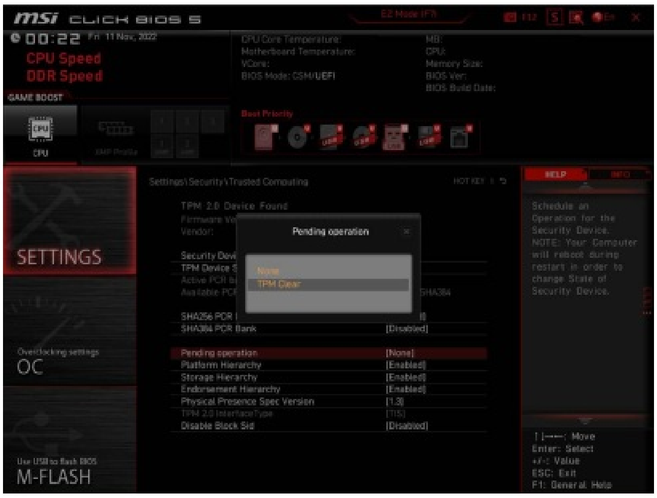


```
Settings\Security\Trusted Computing

TPM 2.0 Device Found
Firmware Version:                 15.22
Vendor:                           IFX

Security Device Support           [Enable]
TPM Device Selection              [dTPM]
Active PCR banks                  SHA256
Available PCR banks               SHA256,SHA384

SHA256 PCR Bank                   [Enabled]
SHA384 PCR Bank                   [Disabled]

Pending operation                 [None]
Platform Hierarchy                [Enabled]
Storage Hierarchy                 [Enabled]
Endorsement Hierarchy             [Enabled]
Physical Presence Spec Version    [1.3]
TPM 2.0 InterfaceType             [TIS]
Disable Block Sid                 [Disabled]
```

Enables or Disables BIOS support for security device. O.S. will not show Security Device. TCG EFI protocol and INT1A interface will not be available.

Clearing TPM from the BIOS

- Press to enter the BIOS Setup program at the system startup.
- Press to enter the Advanced Mode.
- Go to Settings > Security > Trusted Computing.
- Set Pending operation to [TPM Clear].



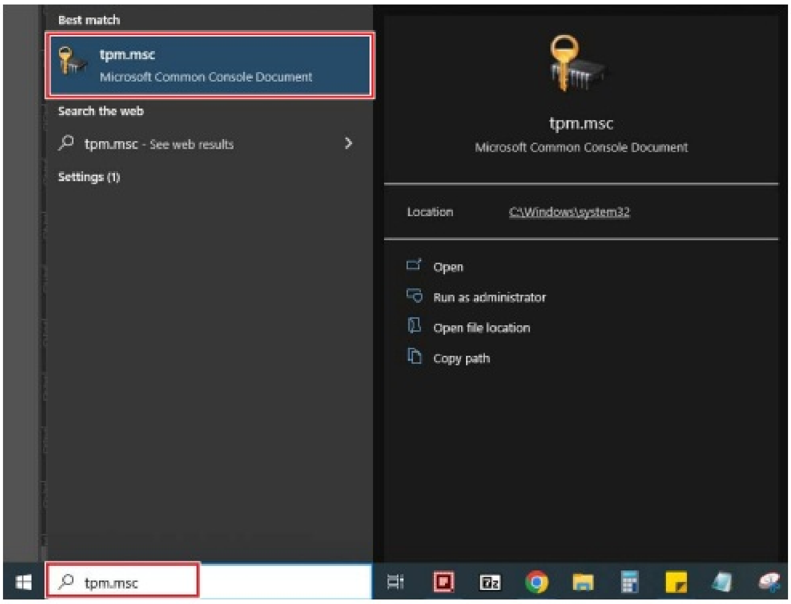
```
Settings\Security\Trusted Computing

TPM 2.0 Device Found

SHA384 PCR Bank                   [Disabled]

Pending operation                 [None]
Platform Hierarchy                [Enabled]
Storage Hierarchy                 [Enabled]
Endorsement Hierarchy             [Enabled]
Physical Presence Spec Version    [1.3]
TPM 2.0 InterfaceType             [TIS]
Disable Block Sid                 [Disabled]
```

Pending operation
None
TPM Clear

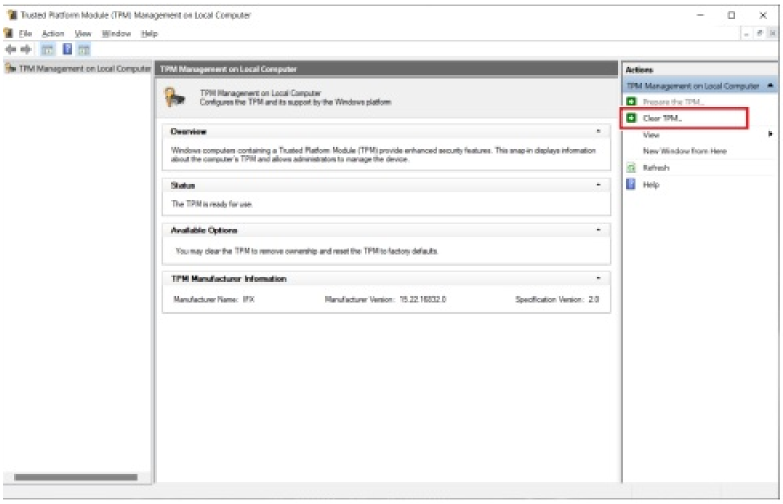
Schedule an Operation for the Security Device. NOTE: Your Computer will reboot during restart in order to change State of Security Device.

Clearing TPM from OS

- Type tpm.msc in the search box next to the Start icon .
- Click tpm.msc to enter TPM management.



- Click Clear TPM… under Actions


Trusted Platform Module (TPM) Management on Local Computer
File
Action
View
Window
Help
TPM Management on Local Computer
TPM Management on Local Computer
Actions
TPM Management on Local Computer
Prepare the TPM...
Clear TPM...
View
New Window from Here
Refresh
Help

TPM Management on Local Computer
Configures the TPM and its support by the Windows platform

Overview

Windows computers containing a Trusted Platform Module (TPM) provide enhanced security features. This snap-in displays information about the computer's TPM and allows administrators to manage the device.

Status

The TPM is ready for use.

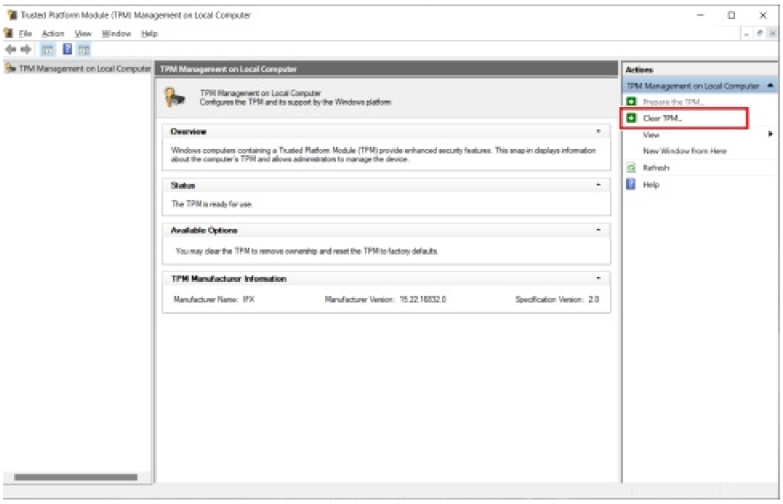
Available Options

You may clear the TPM to remove ownership and reset the TPM to factory defaults.

TPM Manufacturer Information

Manufacturer Name: IFX   Manufacturer Version: 15.22.16832.0   Specification Version: 2.0

- Click Restart when a window pops up


Trusted Platform Module (TPM) Management on Local Computer
File
Action
View
Window
Help
TPM Management on Local Computer
TPM Management on Local Computer
Actions
TPM Management on Local Computer
Prepare the TPM...
Clear TPM...
View
New Window from Here
Refresh
Help

TPM Management on Local Computer
Configures the TPM and its support by the Windows platform

Overview

Windows computers containing a Trusted Platform Module (TPM) provide enhanced security features. This snap-in displays information about the computer's TPM and allows administrators to manage the device.

Status

The TPM is ready for use.

Available Options

You may clear the TPM to remove ownership and reset the TPM to factory defaults.

TPM Manufacturer Information

Manufacturer Name: IFX   Manufacturer Version: 15.22.16832.0   Specification Version: 2.0

Documents / Resources

msi TPM 2.0 (9672) User Guide	msi TPM 2.0 Trusted Platform Module [pdf] User Guide TPM 2.0 Trusted Platform Module, TPM 2.0, Trusted Platform Module, Platform Module, Module

Manuals+,