TPM 2.0 (9672)

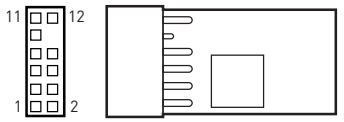
User Guide

Contents

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

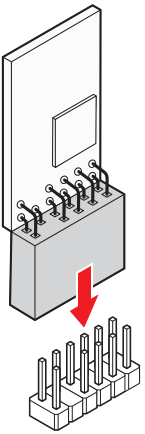
* Starting 21H1, the time window that certified TPMs can be used will be extended from 2 to 3 years.
This means that SLB 9672 FW 15.22 will be usable until April 1st of 2024 w/o any re-certification.
SLB 9672 FW 15.22 is targeted to be re-certified for 22H1 and 23/H1 in order to be usable until April 1st 2026.

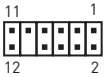
Supported motherboards

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.





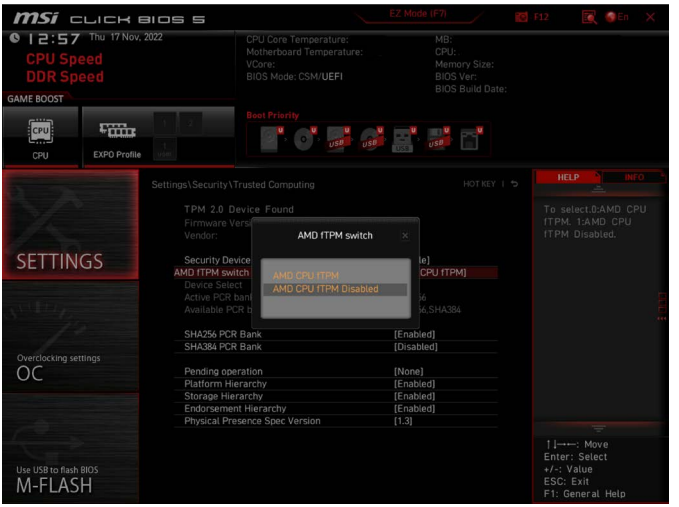
Pin	Signal Name	Pin	Signal Name
1	SPI Power	2	SPI Chip Select
3	Master In Slave Out (SPI Data)	4	Master Out Slave In (SPI Data)
5	Reserved	6	SPI Clock
7	Ground	8	SPI Reset
9	Reserved	10	No Pin
11	Reserved	12	Interrupt Request

Enabling the TPM via the BIOS

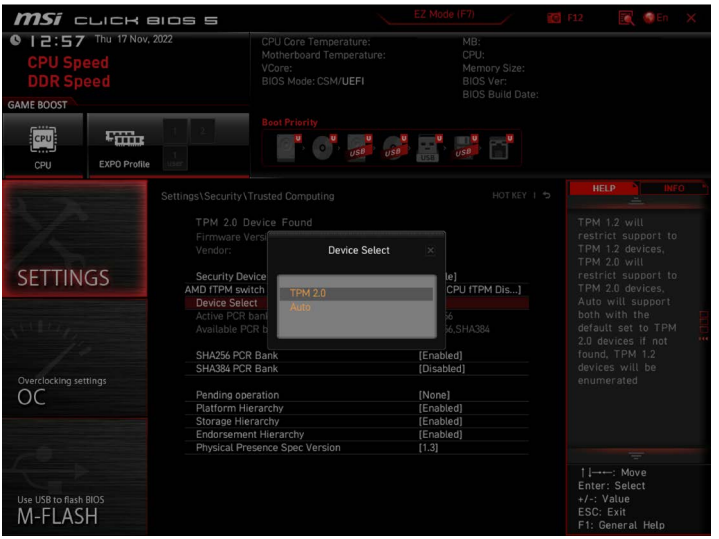
For AMD platforms

1. Press **<Delete>** to enter the BIOS Setup program at the system startup.
2. Press **<F7>** to enter the Advanced Mode.
3. Go to **Settings > Security > Trusted Computing**.
4. Set **Security Device Support** to **[Enable]**.

5. Set **AMD fTPM switch** to **[AMD CPU fTPM Disabled]**.



6. Set **Device Select** to **[TPM 2.0]**.



7. Press **<F10>** to save the changes. Exit the BIOS Setup program and boot into the OS.

For Intel® platforms

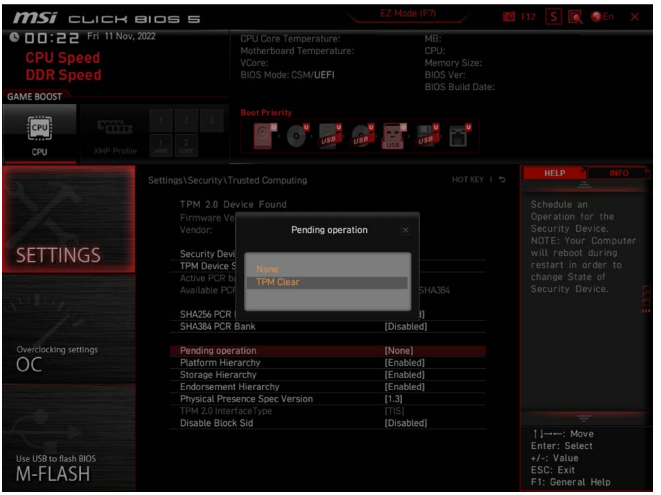
1. Press **<Delete>** to enter the BIOS Setup program at the system startup.
2. Press **<F7>** to enter the Advanced Mode.
3. Go to **Settings > Security > Trusted Computing**.
4. Set **Security Device Support** to **[Enable]**.

5. Set **TPM Device Selection** to **[dTPM]**.

6. Press **<F10>** to save the changes. Exit the BIOS Setup program and boot into the OS.

Clearing TPM from the BIOS

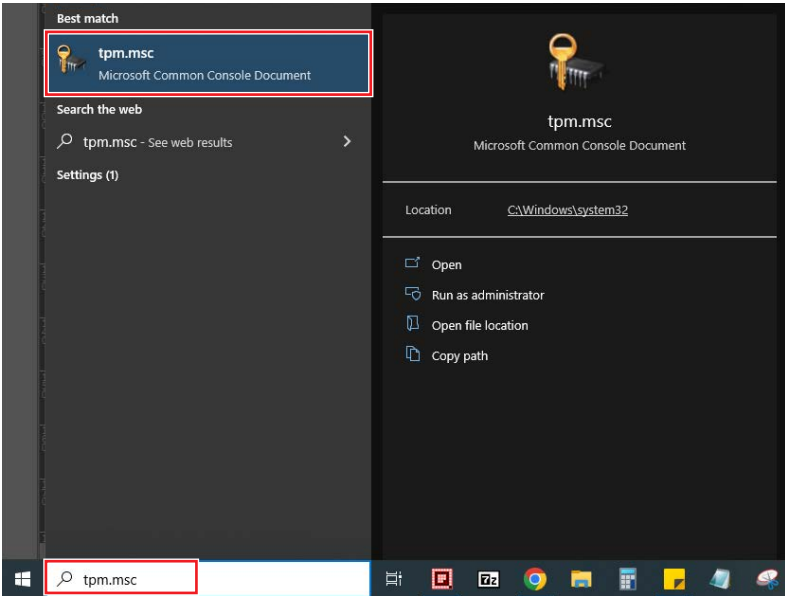
1. Press **<Delete>** to enter the BIOS Setup program at the system startup.
2. Press **<F7>** to enter the Advanced Mode.
3. Go to **Settings > Security > Trusted Computing**.
4. Set **Pending operation** to **[TPM Clear]**.



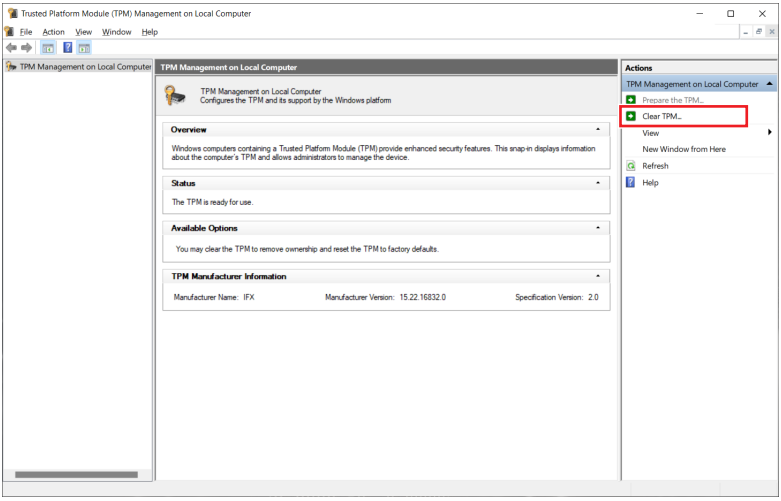
5. Press **<F10>** to save the changes and exit the BIOS Setup program.

Clearing TPM from OS

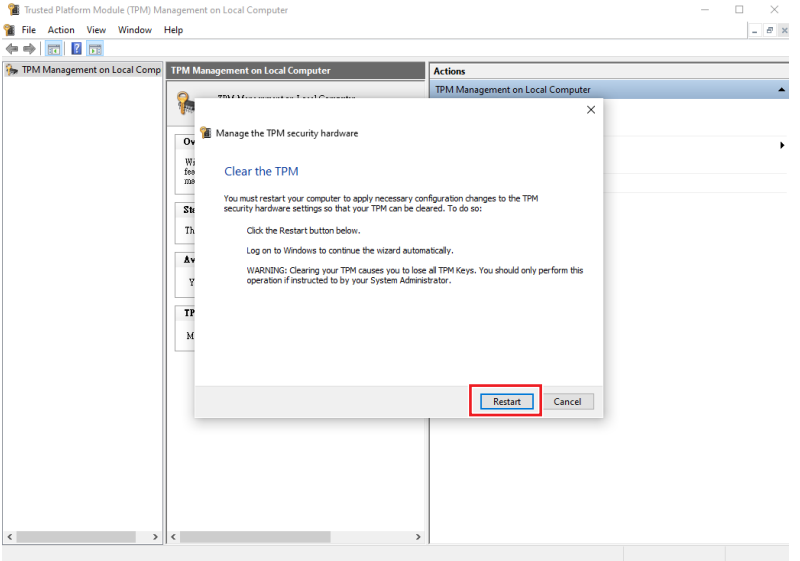
1. Type **tpm.msc** in the search box next to the Start icon .
2. Click **tpm.msc** to enter TPM management.



3. Click **Clear TPM...** under Actions.



4. Click **Restart** when a window pops up.



5. If the DOS Prompt appears, press **<F12>** to clear the TPM.
6. Wait until your computer boots up.