

TPM 2.0 (9672) User Guide



Contents

About Trusted Platform Module (TPM)	. 3
Overview of TPM 2.0 card	. 3
Installing TPM 2.0 card onto the Motherboard	. 4
Enabling the TPM via the BIOS	. 5
Clearing TPM from the BIOS	. 8
Clearing TPM from OS	. 9

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)
05	*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.



	12	2	
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].

MSI CLICK	alos 5		EZ Mode (F7)	🌠 F12 🔣 🎯 En 🗙
CPU Speed DDR Speed	2022	CPU Core Temperature: Motherboard Temperature: VCore: BIOS Mode: CSM/ UEFI		
CPU EXPO Profile	1 2 Luser	Boot Priority		
52		usted Computing rice Found		
SETTINGS	Vendor: Security Devic AMD fTPM switch Device Select Active PCR bar Available PCR	Device Select	Le] CPU fTPM Dis] 56 36,SHA384	
Overclocking settings	SHA256 PCR B SHA384 PCR B	Bank Bank	[Enabled] [Disabled]	
	Pending opera Platform Hiera Storage Hiera Endorsement Physical Prese	nton archy rchy Hierarchy arce Spec Version	[None] [Enabled] [Enabled] [Enabled] [1 3]	
1 Contraction of the second		nice Spec version		
Use USB to flash BIOS M-FLASH				Filter: Move Enter: Select +/-: Value ESC: Exit F1: General Help

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].

MSÍ CLICH E	alos 5		EZ Mode (F7)	10 - F	12 🗴 💽 🚳 En	×
© 0 0 : U 9 Wed 16 Nov, 2022		CPU Core Temperature: Motherboard Temperature:	MB: CPU:			
DDR Speed		BIOS Mode: CSM/UEFI	BIOS Ver:			
CALLE DOOGT						
GAME BOOST						
CPU XMP Profile						
STREET, STREET, ST	Settings\Security\T				HELP INFO	
	TPM 2.0 De Firmware Ve Vendor:	evice Found ersion:	15.22 IFX		Enables or Disables BIOS support for security device.	
SETTINGS	Security Dev	ice Support	[Enable]		Security Device.	
	TPM Device :	Selection	[dTPM]		TCG EFI protocol	
Station of the second se	Active PCR b	anks	SHA256		and INITA Interface	-
1 X # 1 / 1	Available PC	R banks	SHA256, SHA384		available	đ
State 11	SHA254 DCD	Bank	[Enabled]			
	SHA384 PCR	Bank	[Disabled]			
Overclocking settings	Pending oper	ration	[None]			
OC	Platform Hie	rarchy	[Enabled]			
	Storage Hier	arcny t Hierarchy	[Enabled]			
	Physical Pro	sence Spec Version	[1 3]			
	TPM 2.0 Inter	rfaceType	[TIS]			
10	Disable Bloc	k Sid	[Disabled]			
Use USB to flash BIOS M-FLASH					†↓→→-: Move Enter: Select +/-: Value ESC: Exit F1: General Help	

 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].

<i>MSÍ</i> CLICK BIOS S		EZ Mode (F7)	🛿 F12 🚺 💽 🚳 En 🛛 🗙
CPU Speed DDR Speed GAME BOOST	CPU Core Temperature: Motherboard Temperature: VCore: BIOS Mode: CSM/ UEFI		
CPU XMP Profile user addr	Boot Priority		
Settings\Securit TPM 2. Firmwar Vendor:	y\Trusted Computing Device Found e Ve Pending operation		
SETTINGS Security TPM Dev Active P Avitable SHA2561	Devi Ce S None PCF PCF CE I	SHA384	
Overclocking settings OC Platform Storage Endorse Physical TPM 2.0	PCR Bank operation Hierarchy Hierarchy Presence Spec Version InterfaceType	[Disabled] [Enabled] [Enabled] [Enabled] [Labled] [1.3] [TIS]	
Use USB to flash BIOS M-FLASH	3lock Sid	[Disabled]	1 I→→: Nove Enter: Select +/-: Value ESC: Exit F1: General Help

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 **E**.
- 2. Click tpm.msc to enter TPM management.

Best match	
tpm.msc Microsoft Common Console Document	
Search the web	tpm.msc Microsoft Common Console Document
	Location <u>C:\Windows\system32</u>
	 □ Open □ Run as administrator □ Open file location □ Copy path
	H 🗉 🖸 🌖 🖬 🖥 🗾 🥥

3. Click Clear TPM... under Actions.

Trusted Platform Module (TPM) Manag	tement on Local Computer		- 0	×
File Action View Window Help				- 8 ×
🗢 🔿 🔟 🔟				
🐎 TPM Management on Local Computer	TPM Management on Local Computer	A	tions	
	D TPM Management on Local Computer	TF	M Management on Local Co	mputer 🔺
	Configures the TPM and its support by the Windows platform	E	Prepare the TPM_	_
			Clear TPM_	
	Overview	10	View	•
	Windows computers containing a Trusted Platform Module (TPM) provide enhanced security features. This snap-in displays information whose the computer's TPM and allows administrators to manage the device.		New Window from Here	
			Refresh	
	Status	2	Help	
	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			

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.