

TPM-M R2.0 (14-1) TPM-L R2.0 (20-1) Quick Start Guide

Using the TPM-M R2.0 / TPM-L R2.0 card

The TPM-M R2.0 / TPM-L R2.0 card securely store keys, digital certificates, passwords, and data. It helps enhance the network security, protects digital identities, and ensures platform integrity.

The TPM-M R2.0 / TPM-L R2.0 card only supports the following OS:

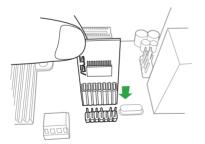
64-bit Windows[®] 7, UEFI OS, with KB2920188 Windows hotfix installed

NOTE: You have to set the Launch CSM item in the BIOS to Enabled, the OS Type item to Other OS. Refer to the user guide of your motherboard on how to change the BIOS settings.

- 64-bit Windows® 8.1, UEFI OS
- 64-bit Windows® 10, UEFI OS

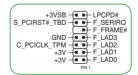
To use the TPM-M R2.0 / TPM-L R2.0 card:

1. Insert the TPM-M R2.0 card to the TPM connector on your motherboard.

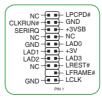


Pin definition:

• TPM-M R2.0 (14-1)



• TPM-L R2.0 (20-1)



- 2. Press < Delete > or < F2 > to enter the BIOS Setup program at the system startup.
- 3. From the BIOS Setup EZ Mode screen, press <**F7**> to enter the Advanced Mode.
- 4. From the Advanced Mode screen, click **Advanced** > **Trusted Computing**.

UEFI BIOS Utility - Advanced Mode	
12/10/2015 16:16 🗢 🖶 English 🖆 MyFavorite(F3) 🗞 Qfan Control(F6) 통 Quick Note(F9) 🕐 Hot Keys	
My Favorites Main Ai Tweaker <u>Advanced</u> Monitor Boot Tool Exit	Hardware Monitor
➤ Trusted Computing	
➤ CPU Configuration	Frequency Temperature 2700 MHz 32°C
 Platform Misc Configuration 	
➤ System Agent (SA) Configuration	100.0 MHz 1.008 V
> PCH Configuration	Ratio 27x
➤ PCH Storage Configuration	
> USB Configuration	Memory
Onboard Devices Configuration	Frequency Voltage 1600 MHz 1.485 V
► APM Configuration	
Network Stack Configuration	8192 MB
► HDD/SSD SMART Information	Voltage
	+12V +5V 12.096 V 4.960 V
Trusted Computing Settings	+3.3V 3.408 V
Last Modified EXMode version 2.17.1246. Copyright () 2015 American Megatrends, Inc.	e(F7) - Search on FAQ

5. Set the Security Device Support and TPM State items to [Enabled].

UEFI BIOS Utility - Adv	anced Mode			θ	
12/10/2015 16:16 to English	🗐 MyFavorite(F3) 🕹 Qfan Control(F	6) 🐺 Quick Note(F9)	? Hot Keys		
	weaker <u>Advanced</u> Monit	or Boot Tool	Exit	[] Hardwa	are Monitor
← Advanced\Trusted Computing					
				Frequency 2700 MHz	Temperature 32°C
Security Device Support		Enable	·		
TPM State		Enabled	·	100.0 MHz	1.008 V
Pending operation		None	•	Ratio 27x	
				Memory	
				Frequency 1600 MHz	Voltage 1,485 V
				Capacity 8192 MB	1,465 ¥
				Voltage	
				+12V 12.096 V	+SV 4.960 V
(i)				+3.3V 3.408 V	
M			st Modified EzMode	(F7) -3] :	Search on FAQ
	Version 2.17.1246. Copyright (C) 20	15 American Megatrend	ls, Inc.		- / 7

 Press <F10> to save the changes, exit the BIOS Setup program and boot into the OS. Now you can start using the TPM-M R2.0 / TPM-L R2.0 card with Windows[®] BitLocker.

Clearing the TPM security hardware

You can clear the TPM security hardware either from the BIOS or the OS.

Clearing from the BIOS

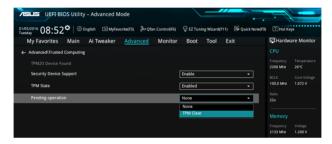
To clear from the BIOS:

NOTE: You can only use this method on Windows® 7 64-bit.

1. Launch the Trusted Computing BIOS screen.

NOTE: For details, refer to steps 2-4 of the section Using the TPM-M R2.0 / TPM-L R2.0 card.

2. Set the Pending operation item to [TPM Clear].



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

Clearing from the OS

To clear from the OS:

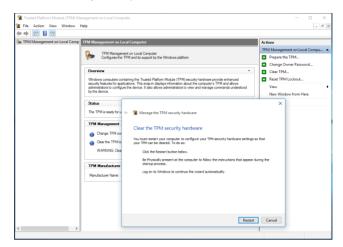
NOTE: This method is only supported on Windows® 8.1 64-bit and Windows® 10 64-bit.

 Click the Windows Start button, and enter tpm.msc in the search box. The TPM Management screen appears.

Trusted Platform Module (TPM) Management on Local Computer	– 🗆 ×
1 File Action View Window Help	- <i>0</i> ×
See TPM Management on Local Comp TPM Management on Local Computer	Actions
	TPM Management on Local Compu
TPM Management on Local Computer Configures the TPM and its support by the Windows platform	Prepare the TPM
	Change Owner Password
Overview -	Clear TPM
Windows computers containing the Trusted Platform Module (TPM) security hardware provide enhanced	Reset TPM Lockout
security features for applications. This snap-in displays information about the computer's TPM and allows administrators to configure the device. It also allows administrators to view and manage commands understood	View
by the device.	New Window from Here
Status	Refresh
The TPM is ready for use, with reduced functionality.	🛛 Help
TPM Management	
Change TPM owner password. Ja	
Cear the TPM to remove ownership and reset the TPM to factory defaults.	
WARNING: Clearing the TPM causes you to lose all TPM keys and data protected by those keys.	
the remain second way in the cause you to be all the keys and data protected by more keys.	
TPM Manufacturer Information *	
Manufacturer Name: IFX Manufacturer Version: 5.51 Specification Version: 2.0	

2. Under Actions, click Clear TPM...

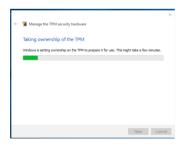
3. Click Restart to restart your computer.



4. When the DOS prompt appears, press <F12> to clear the TPM.



5. Wait until your computer boots up and the OS completes its TPM initialization.



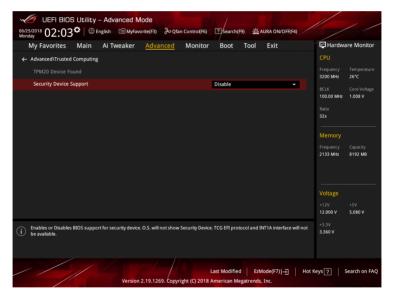
Updating the firmware

WARNING: Before updating your firmware, ensure that you have decrypted your encrypted data first. Your data cannot be decrypted after the firmware update.

To update your firmware:

NOTE: As an example, here we list down detailed steps of updating from version FW5.61.2785 to FW5.63.3144 for your reference.

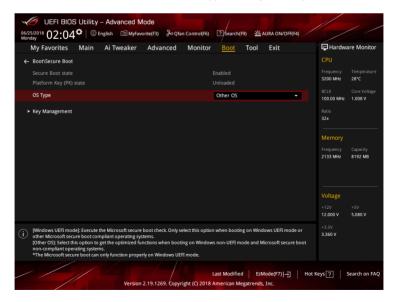
- Download the latest firmware update package for your TPM-M R2.0 / TPM-L R2.0 card from the ASUS support website at <u>https://www.asus.com/support/</u>. Extract the content of the zip package onto a USB flash drive.
- Restart your computer and enter the Advanced Mode of the BIOS setup program. Go to Advanced > Trusted Computing, and set the Security Device Support item to [Disable].



 Go to Boot > CSM(Compatibility Support Module), and set the Launch CSM item to [Disabled].



4. Go to Boot > Secure Boot, and set the OS Type item to [Other OS].



 Press <F10> to save your changes, exit the BIOS Setup program, and reboot your system. The EFI Shell prompt screen displays.



6. Key in fs0: to access the USB drive where the update files are located.

Navigate to the directory (TPM_FU_5.63\Tools\UEFI\Bin\x64) where the update files are located, key in **dir** and press <**Enter**> to display the content.

EFI Shell version 2.60 [5.13]				
Current running mode 1.1.2				
Device mapping table				
fs0	:Removable HardDisk - Alias hd6c0b blk0			
	PciRoot(0X0)/Pci(0x14,0x0)/USB(0x2,0x0)/HD(1, MBR, 0x25474627,0x3F, 0x777			
FC1)				
blk0	:Removable HardDisk - Alias hd6c0b fs0			
	PciRoot(0x0)/Pci(0x14,0x0)/USB(0x2,0x0)/HD(1, MBR, 0x25474627,0x3F. 0x777			
FC1)				
blkl	:Removable BlockDevice - Alias (null)			
	PciRoot(0x0)/Pci(0x14,0X0)/USB(0X2,0x0)			
Press ESC	C in 1 seconds to skip startup.nsh, any other key to continue.			
Shell> fs0:				
fs0:\TPM_FU_5.63\Tools\UEFI\Bin\x64> DIR				

7. Find and execute **TPMFactoryUpd -update tpm20-emptyplatformauth -firmware PM20_5.61.2785.0_to_TPM20_5.63.3144.0.BIN** to update your firmware.

fs0:\TPM_FU_5.63\Tools\UEFI\Bin\x64> DIR Directory of: fs0:\TPM_FU_5.63\Tools\UEFI\Bin\x64				
02/13/18 05:53p 02/13/18 05:53p 12/05/17 02:54a 12/05/17 03:17a 12/05/17 02:54a	o <dir> 4,09 1 316,54 371,25</dir>			
3 File(s) 2 Dir(s) fs0:\TPM FU 5.6		TPMFactoryUpd -update tom20-emptyplatformauth		
02/13/18 05:53p 12/05/17 02:54a 12/05/17 03:17a 12/05/17 02:54a 3 File(s) 2 Dir(s) fs0:\TPM_FU_5.63	 O <dir> 4,09</dir> 316,54 371,25 438,22 1,126,027 bytes 	6 4 IFXTPMUpdate.efi 9 TPM20_5.61.2785.0_to_TPM20_5.63.3144.0.BIN 4 TPMFactoryUpd.efi TPMFactoryUpd -update tpm20-emptyplatformauth		

