

TPM-SPI (14-1 pin) Quick Start Guide

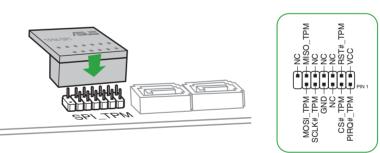
Using the TPM-SPI card

The TPM-SPI card securely stores keys, digital certificates, passwords, and data. It helps enhance the network security, protects digital identities, and ensures platform integrity.

The TPM-SPI card supports 64-bit Windows® 10 UEFI OS only.

To use the TPM-SPI card:

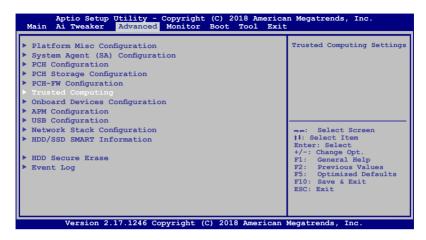
1. Insert the TPM-SPI card to the SPI_TPM connector on your motherboard.



NOTE: The TPM module and BIOS share the same pin layout. The NC signal is used for the TPM-SPI, while the BIOS signal is used for the motherboard.

Pin definition:

- 2. Press < Delete > or <F2 > to enter the BIOS Setup program at the system startup.
- 3. From the Advanced menu, click Trusted Computing.



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

Aptio Setup Utility - Copyrigh Main Ai Tweaker Advanced Monitor	nt (C) 2018 America E Boot Tool Exit			
TFM20 Device Found Security Device Support Active FCR banks Available FCR banks	[Enable] SHA-1,SHA256 SHA-1,SHA256	Enables or Disables BIOS support for security device. 0.S. will not show Security Device. TCG EFI protocol and INTLA interface will not be available.		
SHA-1 PCR Bank SHA256 PCR Bank	[Enabled] [Enabled]			
Pending operation Platform Hierarchy Storage Hierarchy Endorsement Hierarchy TPM2.0 UEFI Spec Version Physical Presence Spec Version	[None] [Enabled] [Enabled] [TCG_2] [1.3]	: Select Screen H: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F5: Optimized Defaults F10: Save & Exit ESC: Exit		
Version 2.17.1246 Copyright (C) 2018 American Megatrends, Inc.				

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

Clearing the TPM security hardware

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

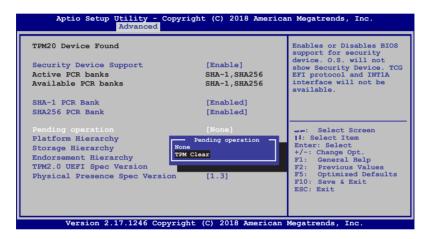
Clearing from the BIOS

To clear from the BIOS:

1. Launch the Trusted Computing BIOS screen.

NOTE: For details, refer to steps 2-3 of the section Using the TPM-SPI 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:

1. In the Windows[®] Search box, key in **tpm.msc** and press <Enter>. The TPM Management screen appears.

Trusted Platform Module (TPM) M	anagement on Local Computer	- 🗆 ×
🖀 File Action View Window	Help	- 0 ×
(+ +) 🔃 🖬 📷		
	TM Management on Local Computer TM Management on Local Computer TM Management on Local Computer Concer Concer Concer Concer Concer Concer Concer Concer Concer Concer Concer Concer Concer Concer Con	Actions TPM Management on Local Comput. Propers the TPM Chang Cover Passed Chang Cover Passed Beat TPM Locked Yew Work Window from Here Reference Reference Reference
	TPM Manufacturer Information Manufacturer Version: 5.51 Specification Version: 2.0	

- 2. Under Actions, click Clear TPM...
- 3. Click **Restart** to restart your computer.

1 Trusted Platform Module (TPM) M	anagement on Local Computer	- 🗆 🗙
👔 File Action View Window	Help	- 8 ×
(+ +) 🖂 🖬 📷		
1 TPM Management on Local Comp	TPM Management on Local Computer	Actions
		TPM Management on Loca A
	TPM Management on Local Computer Configures the TPM and its support by the Windows platform	Prepare the TPM
		Clear TPM
	Overview -	View >
Windows computers containing a Trusted Platform Module (TPM) provide enhanced security features. This snap-in		New Window from Here
	displays information about the computer's TPM and allows administrators to manage the device.	Q Refresh
	Status	🖉 Help
	The TPM is ready for use.	
	×	
	As Manage the TPM security hardware	
	manage the remised only nationale	
	Clear the TPM	
	n Clear the IPM	
	You must restart your computer to apply necessary configuration changes to the TPM security hardware settings so that your TPM can be cleared. To do so:	
	Cick the Restart button below.	
	Log on to Windows to continue the wizard automatically.	
	WARNING: Clearing your TPM causes you to lose all TPM Keys. You should only perform this operation if instructed to by your System Administrator.	
< >		
	Restart Cancel	