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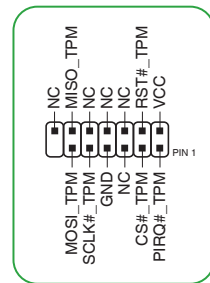
The TPM-SPI card supports 64-bit Windows® 10 UEFI OS only.

To use the TPM-SPI card:

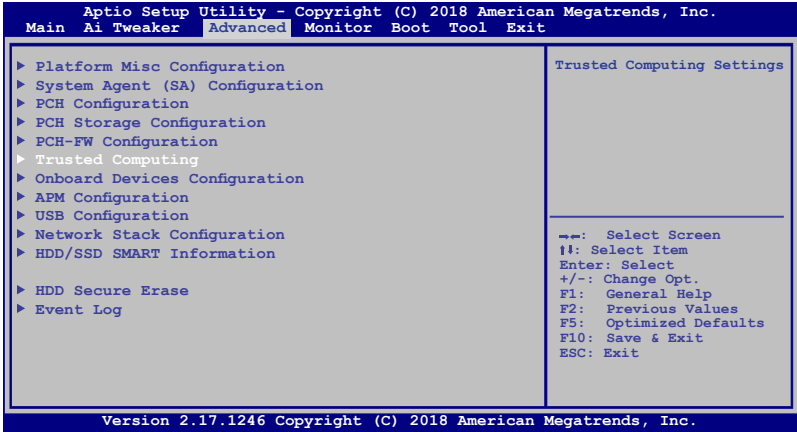1. Insert the TPM-SPI card to the SPI_TPM connector on your motherboard.
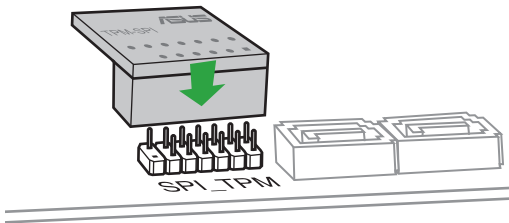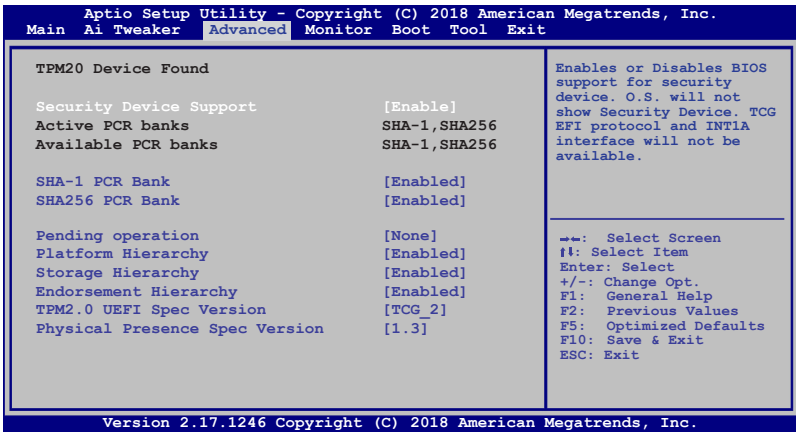
Pin definition:

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.

2. Press <**Delete**> or <**F2**> to enter the BIOS Setup program at the system startup.

3. From the Advanced menu, click **Trusted Computing**.

```
          Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.
    Main  Ai Tweaker  Advanced  Monitor  Boot  Tool  Exit

  ▶ Platform Misc Configuration              Trusted Computing Settings
  ▶ System Agent (SA) Configuration
  ▶ PCH Configuration
  ▶ PCH Storage Configuration
  ▶ PCH-FW Configuration
  ▶ Trusted Computing
  ▶ Onboard Devices Configuration
  ▶ APM Configuration
  ▶ USB Configuration
  ▶ Network Stack Configuration              ➡←:  Select Screen
  ▶ HDD/SSD SMART Information                 ↑↓: Select Item
                                             Enter: Select
  ▶ HDD Secure Erase                         +/-: Change Opt.
  ▶ Event Log                                F1:  General Help
                                             F2:  Previous Values
                                             F5:  Optimized Defaults
                                             F10: Save & Exit
                                             ESC: Exit


          Version 2.17.1246 Copyright (C) 2018 American Megatrends, Inc.
```

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

```
          Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.
    Main  Ai Tweaker  Advanced  Monitor  Boot  Tool  Exit

    TPM20 Device Found                       Enables or Disables BIOS
                                             support for security
    Security Device Support    [Enable]      device. O.S. will not
    Active PCR banks           SHA-1,SHA256  show Security Device. TCG
    Available PCR banks        SHA-1,SHA256  EFI protocol and INT1A
                                             interface will not be
    SHA-1 PCR Bank             [Enabled]     available.
    SHA256 PCR Bank            [Enabled]

    Pending operation          [None]        ➡←:  Select Screen
    Platform Hierarchy         [Enabled]     ↑↓: Select Item
    Storage Hierarchy          [Enabled]     Enter: Select
    Endorsement Hierarchy      [Enabled]     +/-: Change Opt.
    TPM2.0 UEFI Spec Version   [TCG_2]       F1:  General Help
    Physical Presence Spec Version [1.3]     F2:  Previous Values
                                             F5:  Optimized Defaults
                                             F10: Save & Exit
                                             ESC: Exit


          Version 2.17.1246 Copyright (C) 2018 American Megatrends, Inc.
```

5. 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

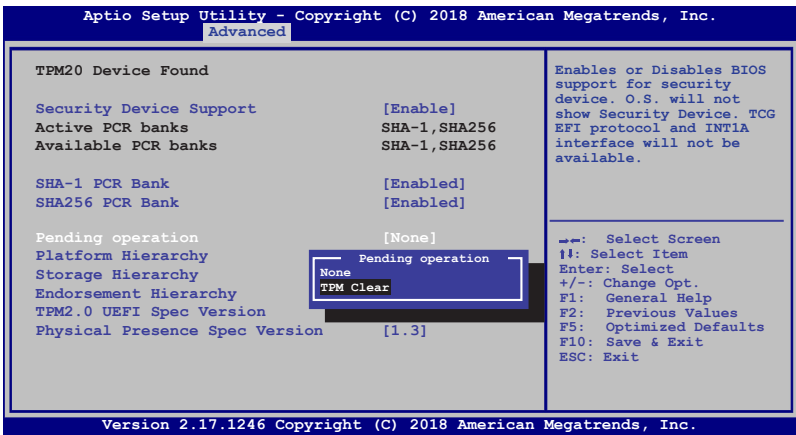You can clear the TPM security hardware either from the BIOS or the OS.

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**].

```
         Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.
                    Advanced

        TPM20 Device Found                                    Enables or Disables BIOS
                                                              support for security
        Security Device Support          [Enable]             device. O.S. will not
        Active PCR banks                 SHA-1,SHA256          show Security Device. TCG
        Available PCR banks              SHA-1,SHA256          EFI protocol and INT1A
                                                              interface will not be
        SHA-1 PCR Bank                   [Enabled]             available.
        SHA256 PCR Bank                  [Enabled]

        Pending operation                [None]               →←:  Select Screen
        Platform Hierarchy          ┌──── Pending operation ────┐  ↑↓: Select Item
        Storage Hierarchy           │ None                      │  Enter: Select
        Endorsement Hierarchy       │ TPM Clear                 │  +/-: Change Opt.
        TPM2.0 UEFI Spec Version    └───────────────────────────┘  F1:  General Help
        Physical Presence Spec Version   [1.3]                 F2:  Previous Values
                                                              F5:  Optimized Defaults
                                                              F10: Save & Exit
                                                              ESC: Exit

              Version 2.17.1246 Copyright (C) 2018 American Megatrends, Inc.
```
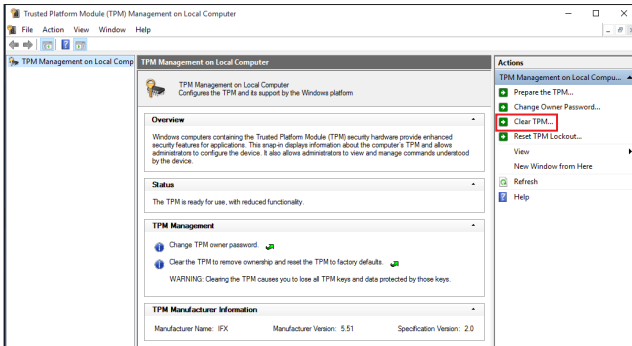
3. Press <**F10**> to save the changes and exit the BIOS Setup program.

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.

2.   Under **Actions**, click **Clear TPM...**

3.   Click **Restart** to restart your computer.