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:

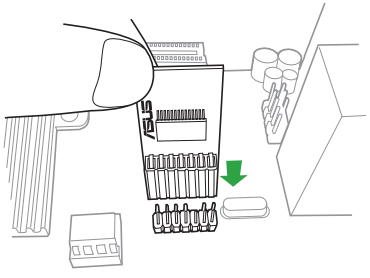
- 64-bit Windows® 7, UEFI OS, with KB2920188 Windows hotfix installed

  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

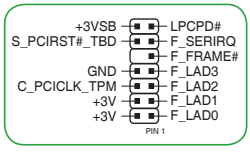
To use the TPM-M R2.0 / TPM-L R2.0 card:

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

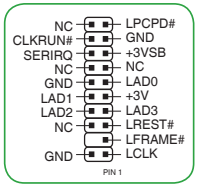


Pin definition:

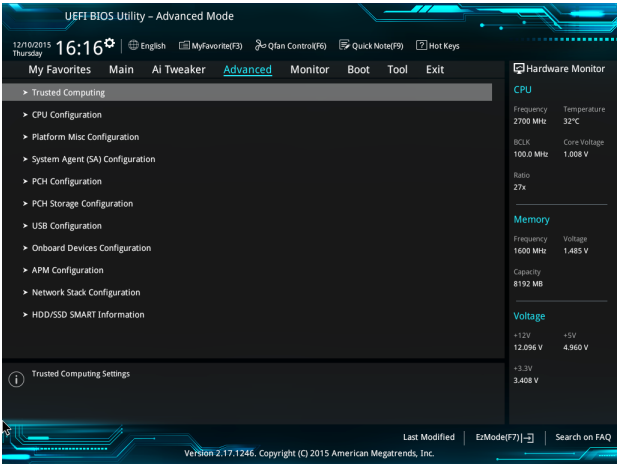
- **TPM-M R2.0 (14-1)**



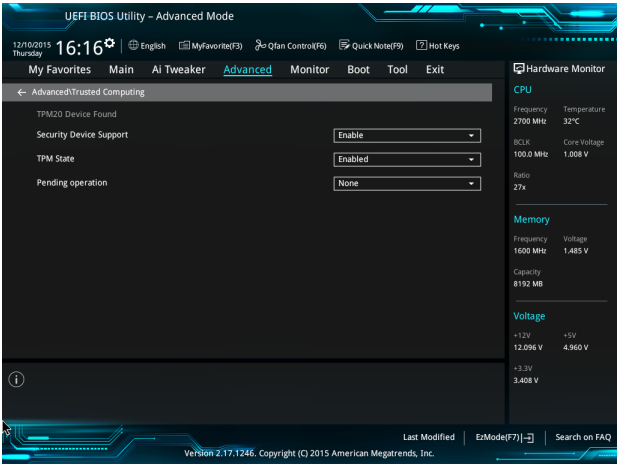
- **TPM-L R2.0 (20-1)**



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**.



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



6. 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

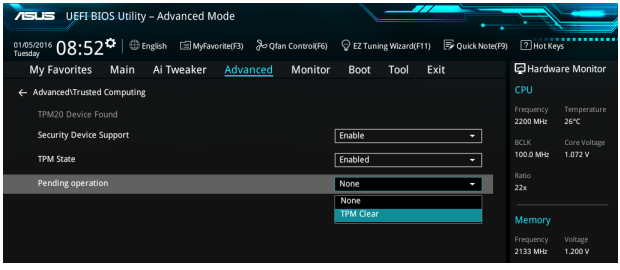
To clear from the BIOS:

> **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**].



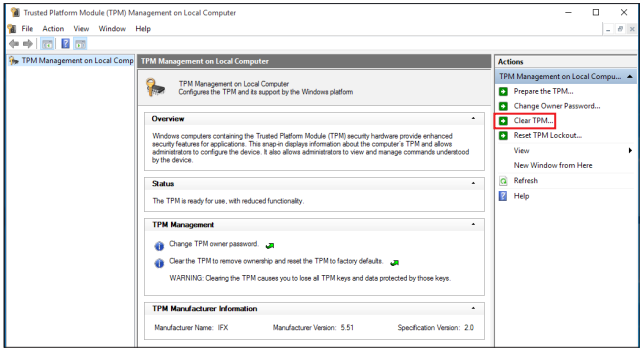
3. Press <**F10**> to save the changes and exit the BIOS Setup program.

Clearing from the OS

To clear from the OS:

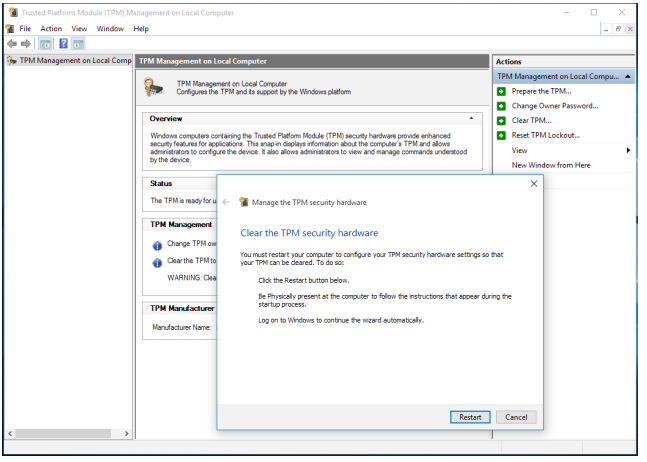
> **NOTE**: This method is only supported on Windows® 8.1 64-bit and Windows® 10 64-bit.

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

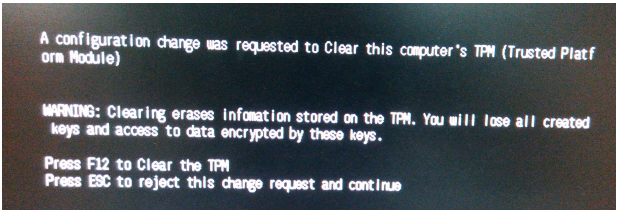


2. Under **Actions**, click **Clear TPM...**

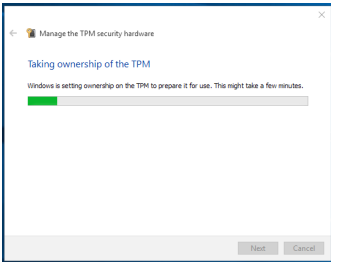
3. Click **Restart** to restart your computer.



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.



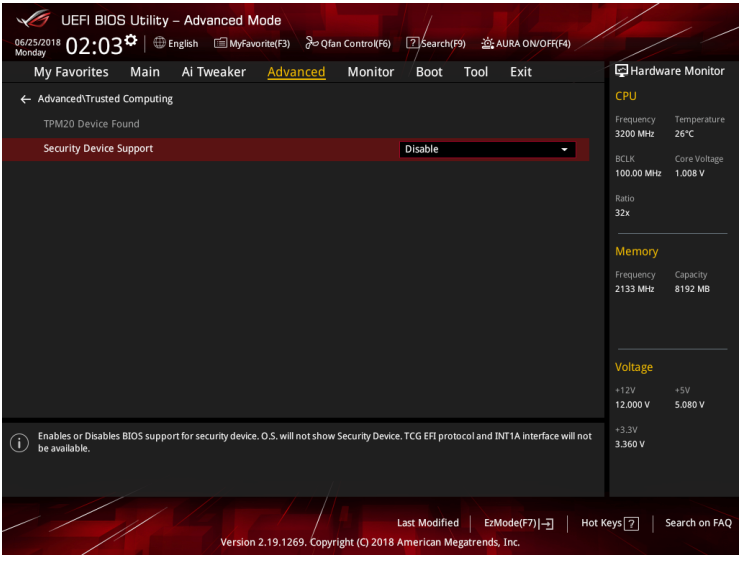
Updating the firmware

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

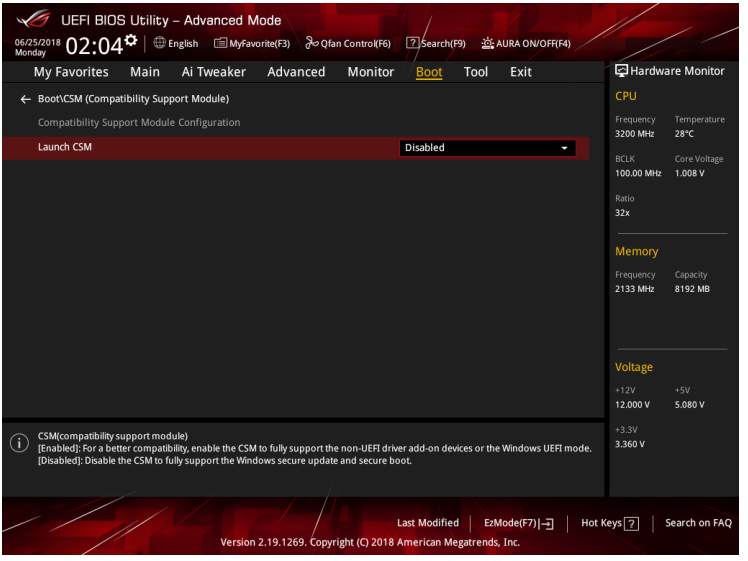
To update your firmware:

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

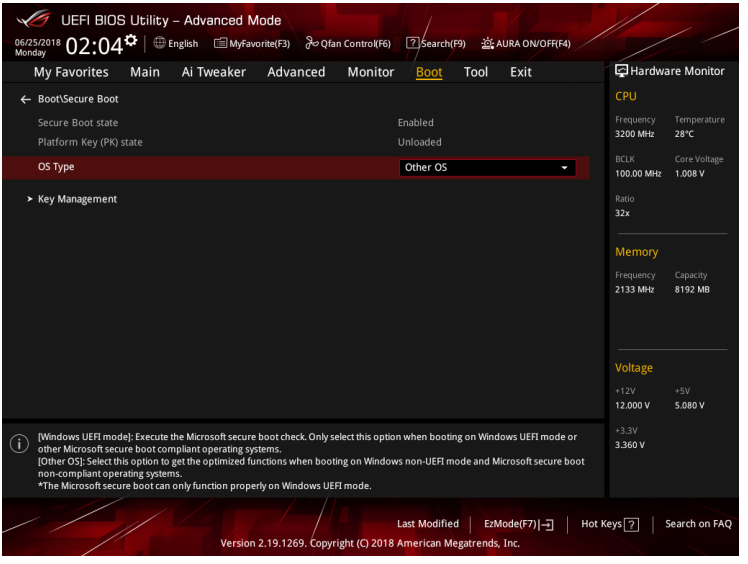
1. Download the latest firmware update package for your TPM-M R2.0 / TPM-L R2.0 card from the ASUS support website at https://www.asus.com/support/. Extract the content of the zip package onto a USB flash drive.
2. Restart your computer and enter the Advanced Mode of the BIOS setup program. Go to **Advanced**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



3. 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].



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

```
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 in 1 seconds to skip startup.nsh, any other key to continue.
Shell>
```

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 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  <DIR>              4,096  .
   02/13/18   05:53p  <DIR>              4,096  ..
   12/05/17   02:54a                   316,544  IFXTPMUpdate.efi
   12/05/17   03:17a                   371,259  TPM20_5.61.2785.0_to_TPM20_5.63.3144.0.BIN
   12/05/17   02:54a                   438,224  TPMFactoryUpd.efi
              3 File(s)        1,126,027 bytes
              2 Dir(s)

   fs0:\TPM_FU_5.63\Tools\UEFI\Bin\x64> TPMFactoryUpd -update tpm20-emptyplatformauth
   -firmware TPM20_5.61.2785.0_to_TPM20_5.63.3144.0.BIN
```

15060-75800100