GC-TPM2.0 SPI V2

User's Manual

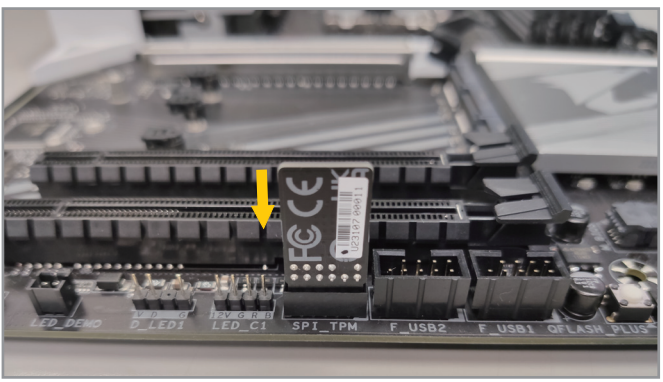
Rev. 1002

GC-TPM2.0 SPI V2 is an SPI interface TPM module card designed to provide TPM 2.0 function on GIGABYTE's motherboards. Before enabling GC-TPM2.0 SPI V2, first complete the steps below:

1. Installing the GC-TPM2.0 SPI V2 card
2. Configuring BIOS settings

Step 1: Installing the GC-TPM2.0 SPI V2 Card

Install the GC-TPM2.0 SPI V2 card in the SPI_TPM header (Trusted Platform Module header) on your GIGABYTE motherboard. (If your processor has built-in TPM support, follow the steps on the next page to disable the built-in TPM feature first.)

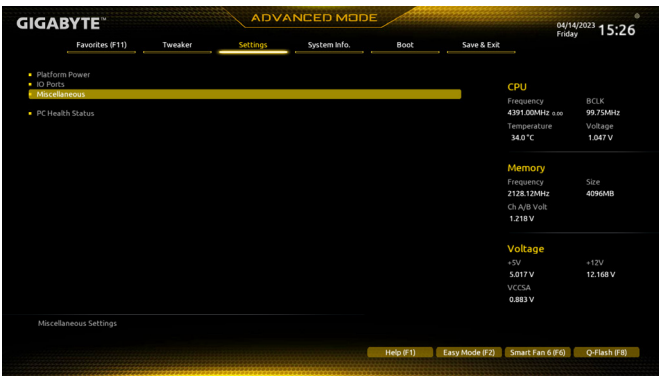


Step 2: Configuring BIOS Settings

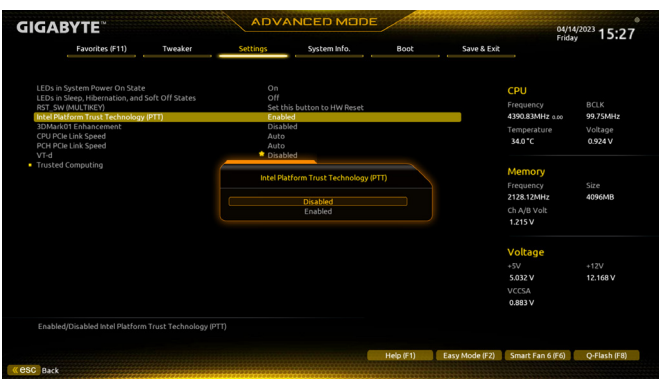
Refer to the following BIOS settings based on your motherboard chipset.

A. Intel platform

Turn on your computer and press <Delete> to enter BIOS Setup during the POST (Power-On Self-Test). Go to the **Settings\Miscellaneous** menu.



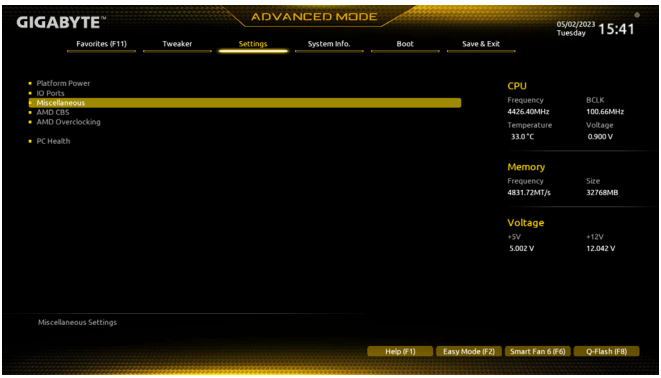
Set **Intel Platform Trust Technology (PTT)** to **Disabled**. Then save the changes and exit BIOS Setup.



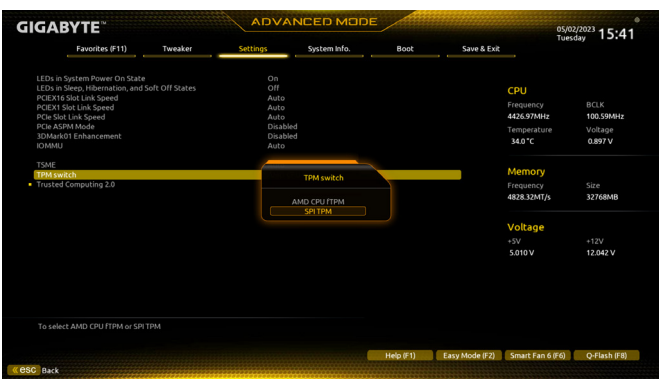
The BIOS Setup menus and options described may differ from the exact settings for your motherboard. The actual BIOS Setup menu options are dependent on the motherboard you have and the BIOS version.

B. AMD platform

Turn on your computer and press <Delete> to enter BIOS Setup during the POST (Power-On Self-Test). Go to the **Settings\Miscellaneous** menu.



Set **TPM switch** to **SPI TPM**. Then save the changes and exit BIOS Setup.



The BIOS Setup menus and options described may differ from the exact settings for your motherboard. The actual BIOS Setup menu options are dependent on the motherboard you have and the BIOS version.

Checking TPM status

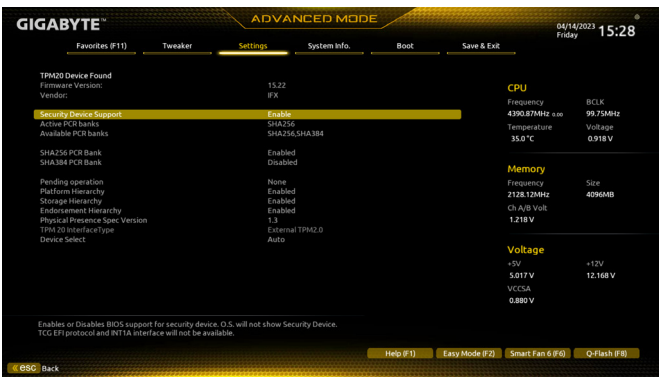
You can check whether the TPM 2.0 function is enabled and look up related information.

A. Intel Platform

Path: Settings\Miscellaneous\Trusted Computing

☞ **Security Device Support**

Enables or disables Trusted Platform Module (TPM).



B. AMD Platform

Path: Settings\Miscellaneous\Trusted Computing 2.0

☞ **Security Device Support**

Enables or disables Trusted Platform Module (TPM).