Enable TPM 2.0 on your PC – Microsoft Support

Windows 10 · https://cleversupport.ca/docs/windows-10/enable-tpm-2-0-on-your-pc-microsoft-support/

Published August 2021

This article is intended for users who are not able to upgrade to Windows 11 because their PC is not currently enabled with TPM 2.0 or their PC is capable of running TPM 2.0 but is not set up to do so. If you are unfamiliar with this level of technical detail, we recommend that you consult your PC manufacturer's support information for more instructions specific to your device.

Most PCs that have shipped in the last 5 years are capable of running Trusted Platform Module version 2.0 (TPM 2.0). TPM 2.0 is required to run Windows 11, as an important building block for security-related features. TPM 2.0 is used in Windows 11 for a number of features, including Windows Hello for identity protection and BitLocker for data protection.

In some cases, PCs that are capable of running TPM 2.0 are not set up to do so. If you are considering upgrading to Windows 11, check to ensure TPM 2.0 is enabled on your device. Most retail PC motherboards used by people building their own PC, for example, ship with TPM turned off by default even though it is almost always available to be enabled.

Option 1: Use the Windows Security app

1. Run **Settings** > **Update & Security** > **Windows Security** > **Device Security**
    a. If you do not see a **Security processor** section on this screen your PC may have a TPM that is disabled. see How to enable TPM for more information or check your PC manufacturer's support information for instructions. to enable the TPM. If you are able to enable a TPM, complete the next step to verify that it is a TPM 2.0.
    b. If you see an option for **Security processor details** under **Security processor**, select that and verify that your **Specification version** is 2.0. If it is less than 2.0, your device does not meet the Windows 11 requirements.

Option 2: Use the Microsoft Management Console

1. Press [**Windows Key**] + **R** or select **Start** > **Run**.
2. Type “tpm.msc” (do not use quotation marks) and choose **OK**.
   a. If you see a message saying a “Compatible TPM cannot be found,” your PC may have a TPM that is disabled. See How to enable TPM for more information or check your PC manufacturer’s support information for instructions to enable the TPM. If you are able to enable the TPM, complete the next step to verify that it is a TPM 2.0.
   b. If you see a message confirming TPM is ready to use, check **Specification Version** under **TPM Manufacturer Information** to verify it is 2.0. If it is less than 2.0 your device does not meet the Windows 11 requirement.

How to enable TPM

If you need to enable TPM, these settings are managed via the UEFI BIOS (PC firmware) and vary based on your device. You can access these settings by choosing: **Settings** > **Update & Security** > **Recovery** > **Restart now**.

From the next screen, choose **Troubleshoot** > **Advanced options** > **UEFI Firmware Settings** > **Restart** to make the changes. These settings are sometimes contained in a sub-menu in the UEFI BIOS labeled **Advanced**, **Security**, or **Trusted Computing**. The option to enable the TPM may be labeled **Security Device**, **Security Device Support**, **TPM State**, **AMD fTPM switch**, **AMD PSP fTPM**, **Intel PTT**,or **Intel Platform Trust Technology**.

If you are unsure how to make any needed changes to the TPM settings, we recommend that you check your PC manufacturer’s support information or contact their support organization. Below are links to information from some PC manufacturers to help you get started:

Asus

Dell

HP

Lenovo

Microsoft Surface