Device protection in Windows Security

*Windows 10 Security*

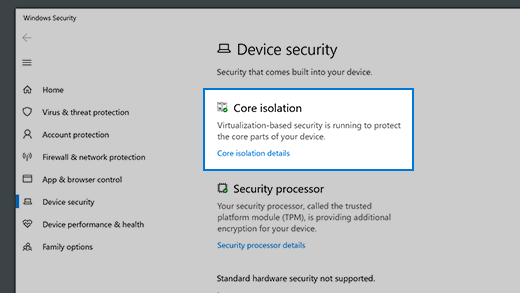
Windows Security provides the following built-in security options to help protect your device from malicious software attacks.

To access the features described below, in the search box on the taskbar, type **windows security**, select it from the results, and then select **Device security**.

**Notes:**What you actually see on the **Device security** page may vary depending upon what your hardware supports.

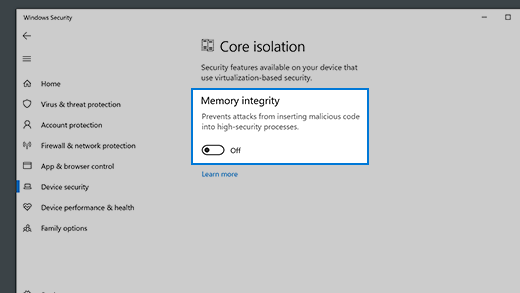
* For more info about Windows Security, see [Stay protected with Windows Security](https://support.microsoft.com/en-us/windows/stay-protected-with-windows-security-2ae0363d-0ada-c064-8b56-6a39afb6a963).
* For more info about Windows Defender Firewall, see [Turn Windows Defender Firewall on or off](https://support.microsoft.com/en-us/windows/turn-microsoft-defender-firewall-on-or-off-ec0844f7-aebd-0583-67fe-601ecf5d774f).
* For help with your password, see [Change or reset your Windows password](https://support.microsoft.com/en-us/windows/change-or-reset-your-windows-password-8271d17c-9f9e-443f-835a-8318c8f68b9c).

Core isolation

Core isolation provides added protection against malware and other attacks by isolating computer processes from your operating system and device. Select **Core isolation details** to enable, disable, and change the settings for core isolation features.  
  


Memory integrity

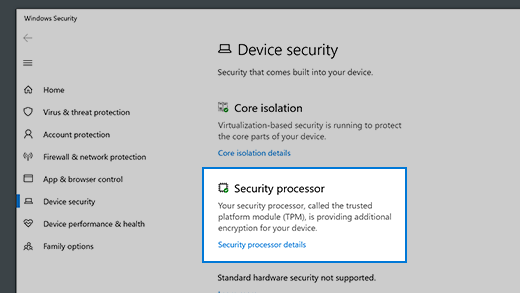
Memory integrity is a feature of core isolation. By turning on the **Memory integrity** setting, you can help prevent malicious code from accessing high-security processes in the event of an attack.



Security processor

Your security processor provides additional encryption for your device.

Security processor details



This is where you’ll find info about the security processor manufacturer and version numbers, as well as about the security processor’s status. Select **Security processor details**, and then on the details page, select **Security processor troubleshooting** for additional info and options.

**Note:** If you don't see a Security processor entry on this screen then it's likely that your device doesn't have the TPM hardware necessary for this feature.

Security processor troubleshooting

The following are advanced options for troubleshooting your security processor.

**Error messages**

This is where you'll see any relevant error messages about your security processor. Here's a list of the error messages that might appear:

* A firmware update is needed for your security processor (TPM).
* TPM is disabled and requires attention.
* TPM storage is not available. Please clear your TPM.
* Device health attestation isn't available. Please clear your TPM.
* Device health attestation isn't supported on this device.
* Your TPM isn't compatible with your firmware, and may not be working properly.
* TPM measured boot log is missing. Try restarting your device.
* There is a problem with your TPM. Try restarting your device.

If you still encounter problems after addressing an error message, contact your device manufacturer for assistance.

**Clear TPM**

Select **Clear TPM** to reset your security processor to its default settings. Make sure to back up your data before you clear the TPM.

**Send Feedback**

Select **Send Feedback**(in older versions of Windows 10 it says **Collect Logs**) to gather more information that might help you understand issues with your security processor and submit that feedback through the Windows Feedback Hub. The logs will be saved to a folder on your desktop.

Secure boot

Secure boot prevents a sophisticated and dangerous type of malware—a *rootkit*—from loading when you start your device. Rootkits use the same permissions as the operating system and start before it, which means they can completely hide themselves. Rootkits are often part of an entire suite of malware that can bypass local logins, record passwords and keystrokes, transfer private files, and capture cryptographic data.

You may have to disable secure boot to run some PC graphics cards, hardware, or operating systems such as Linux or earlier versions of Windows. For more info, see [How to disable and re-enable secure boot](https://docs.microsoft.com/windows-hardware/manufacture/desktop/disabling-secure-boot).

Hardware security capability

At the bottom of the Device security screen, one of the following messages appears, indicating the security capability of your device.

Your device meets the requirements for standard hardware security

This means your device supports memory integrity and core isolation and also has:

* TPM 2.0 (also referred to as your security processor)
* Secure boot enabled
* DEP
* UEFI MAT

Your device meets the requirements for enhanced hardware security

This means that in addition to meeting all the requirements of standard hardware security, your device also has memory integrity turned on.

Your device exceeds the requirements for enhanced hardware security (*Note: In Windows 20H2 this message will say "Your device has all Secured-core PC features enabled")*

This means that in addition to meeting all the requirements of enhanced hardware security, your device also has System Management Mode (SMM) protection turned on.

Standard hardware security not supported

This means that your device does not meet at least one of the requirements of standard hardware security.

**Improving hardware security**

If the security capability of your device isn't what you'd like it to be, you might need to turn on certain hardware features (such as secure boot, if supported) or change the settings in your system's BIOS. Contact your hardware manufacturer to see what features are supported by your hardware and how to activate them.

More info and troubleshooting resources

More info about antivirus and firewall protection in Windows Security

Windows Security is the built-in security app that comes with Windows 10. It includes Microsoft Defender Antivirus protection and Windows Defender Firewall.

* [Stay protected with Windows Security](https://support.microsoft.com/en-us/windows/stay-protected-with-windows-security-2ae0363d-0ada-c064-8b56-6a39afb6a963)
* [Turn Windows Defender Firewall on or off](https://support.microsoft.com/en-us/windows/turn-microsoft-defender-firewall-on-or-off-ec0844f7-aebd-0583-67fe-601ecf5d774f)
* [Help protect my PC with Microsoft Defender Offline](https://support.microsoft.com/en-us/windows/help-protect-my-pc-with-microsoft-defender-offline-9306d528-64bf-4668-5b80-ff533f183d6c)

Troubleshooting resources

* One of the first things to try in troubleshooting is to ensure that you have the latest updates installed. Go to **Start** > **Settings** > **Update and security** and **Check for updates**.
* If Windows Security is displayed in the wrong language, follow the guidance in [Windows Language Packs](https://support.microsoft.com/en-us/windows/language-packs-for-windows-a5094319-a92d-18de-5b53-1cfc697cfca8) to get it to display in the language of your choice. Generally, Windows Security uses the language that Windows 10 is set to at **Start** > **Settings** > **Time & Language**.
* If Windows Security blocks printer installation, you can temporarily disable Windows Defender Firewall while you install the printer on your PC**.**To do this, see [Turn Windows Defender Firewall on or off](https://support.microsoft.com/en-us/windows/turn-microsoft-defender-firewall-on-or-off-ec0844f7-aebd-0583-67fe-601ecf5d774f). After you've installed the printer, make sure you turn the firewall back on.  
    
  If you have a wireless printer on a network that you can't access after you've enabled Windows Security, you may need to configure your Windows Defender Firewall settings to allow access. For help with this process, contact your printer manufacturer.
* If you experience a kernel security check failure when you run a Windows Security feature, this may be a corrupted or outdated driver issue. To investigate and fix this situation, see [Update drivers in Windows 10](https://support.microsoft.com/en-us/windows/update-drivers-in-windows-10-ec62f46c-ff14-c91d-eead-d7126dc1f7b6).