5 - Device Security



Even though you'll probably never change any of these settings, for completion's sake, it will be covered briefly.

□ Device security

Security that comes built into your device.

Core isolation

Virtualization-based security is running to protect the core parts of your

Core isolation details

Standard hardware security not supported.

Learn more

Core isolation

. Memory Integrity - Prevents attacks from inserting malicious code into high-security processes.

Core isolation

Security features available on your device that use virtualization-based

Memory integrity

Prevents attacks from inserting malicious code into high-security processes.



Warning: Unless you are 100% confident in what you are doing, it is recommended that you leave the default settings.

The below images are from another machine to show another security feature that should be available in a personal Windows 10 device.

Security processor

Security processor

Your security processor, called the trusted platform module (TPM), is providing additional encryption for your device.

Below are the Security processor details.

Below are the Security processor details.

Security processor details

Information about the trusted platform module (TPM).

Specifications

Manufacturer Intel (INTC) Manufacturer version Specification version 303.12.0.0 2.0

PPI specification version 1.2
TPM specification sub-version 1.16 (9/21/2016)
PC client spec version 1.00

Status

Attestation Ready Ready Storage

Security processor troubleshooting

Learn more

What is the Trusted Platform Module (TPM)?

Per Microsoft, "Trusted Platform Module (TPM) technology is designed to provide hardware-based, security-related functions. A TPM chip is a secure crypto-processor that is designed to carry out cryptographic operations. The chip includes multiple physical security mechanisms to make it tamper-resistant, and malicious software is unable to tamper with the security functions of the TPM".