

# Windows Fundamentals Part 3

---

Learned:

- Windows Defender Firewall helps protect the system by blocking unsafe applications and websites by reducing the risk of malware and preventing unauthorized access.
- You can run a scan in the Virus & Threat Protection section to detect and remove files or programs that may contain malware.
- You can choose between a quick scan, full scan, or custom scan to quickly detect surface-level threats or thoroughly check the system for hidden malware.
- Tools like Bit Locker or Volume Shadow Copy Service help in keeping the device secure by backing up data or ensuring that when offline everything stay's protected.

## Windows Updates

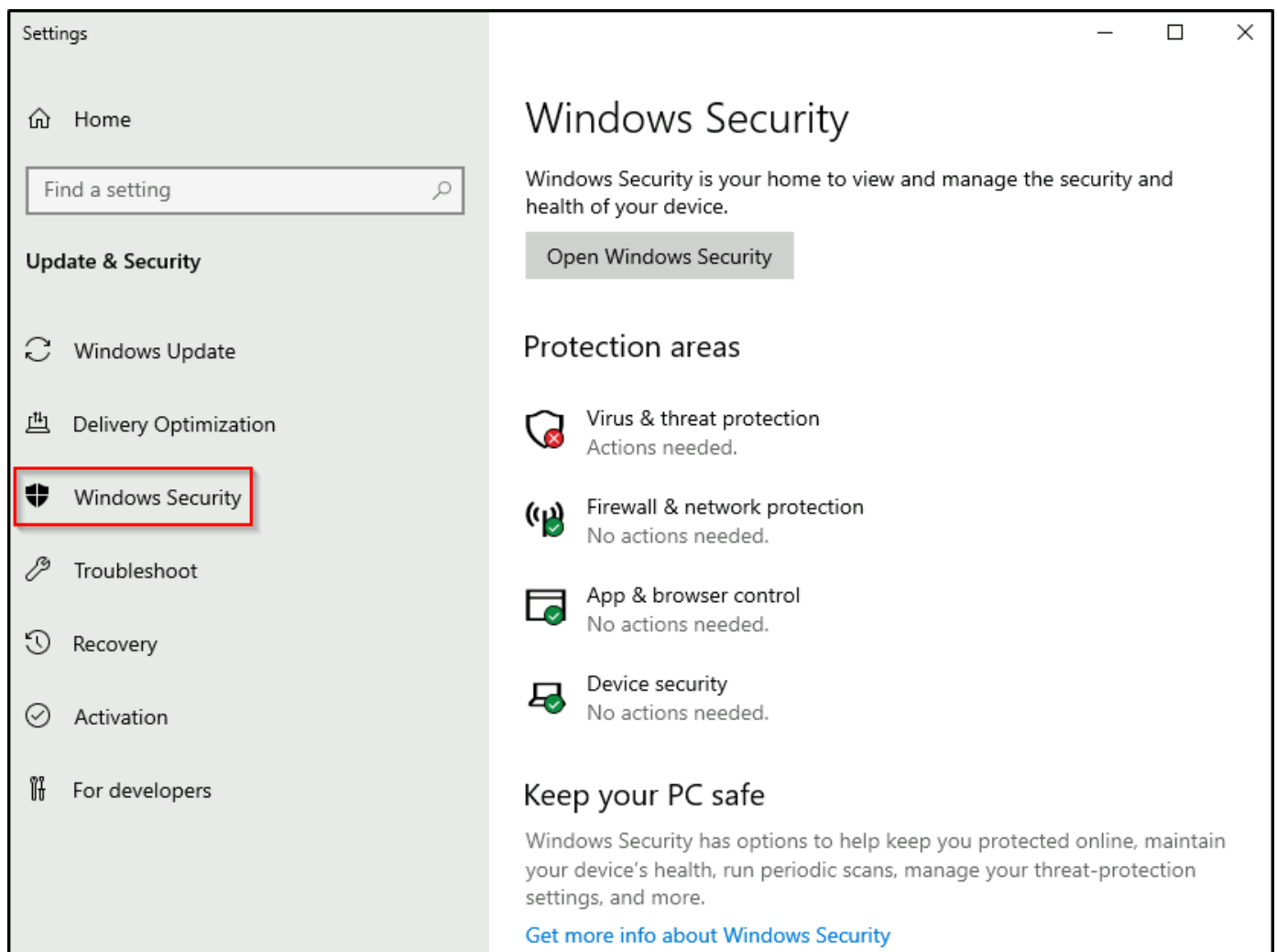
Windows Update is a service provided by Microsoft to provide security updates, feature enhancements, and patches for the Windows operating system and other Microsoft products, such as Microsoft Defender.

Updates are typically released on the 2nd Tuesday of each month. This day is called **Patch Tuesday**.

## Windows Security

---

**Windows Security** is also available in **Settings**.



## Virus & Threat Protection

Virus & threat protection is divided into two parts:

- **Current threats**
- **Virus & threat protection settings**

The image below only focuses on **Current threats**.

# Virus & threat protection

Protection for your device against threats.

## Current threats

No current threats.

Last scan: 6/10/2021 2:00 AM (quick scan)

0 threats found.

Scan lasted 26 seconds

34572 files scanned.

Quick scan

[Scan options](#)

[Threat history](#)

## Current threats

## Scan options

- **Quick scan** - Checks folders in your system where threats are commonly found.
- **Full scan** - Checks all files and running programs on your hard disk. This scan could take longer than one hour.
- **Custom scan** - Choose which files and locations you want to check.

## Threat history

- **Last scan** - Windows Defender Antivirus automatically scans your device for viruses and other threats to help keep it safe.
- **Quarantined threats** - Quarantined threats have been isolated and prevented from running on your device. They will be periodically removed.
- **Allowed threats** - Allowed threats are items identified as threats, which you allowed to run on your device.

## Virus & threat protection settings

## Manage settings

- **Real-time protection** - Locates and stops malware from installing or running on your device.

- **Cloud-delivered protection** - Provides increased and faster protection with access to the latest protection data in the cloud.
- **Automatic sample submission** - Send sample files to Microsoft to help protect you and others from potential threats.
- **Controlled folder access** - Protect files, folders, and memory areas on your device from unauthorized changes by unfriendly applications.
- **Exclusions** - Windows Defender Antivirus won't scan items that you've excluded.
- **Notifications** - Windows Defender Antivirus will send notifications with critical information about the health and security of your device.

## Ransomware protection

- **Controlled folder access** - Ransomware protection requires this feature to be enabled, which in turn requires Real-time protection to be enabled.

## Firewall & Network Protection

---

What is a **firewall**?

Per Microsoft, "*Traffic flows into and out of devices via what we call ports. A firewall is what controls what is - and more importantly isn't - allowed to pass through those ports. You can think of it like a security guard standing at the door, checking the ID of everything that tries to enter or exit*".

The below image will reflect what you will see when you navigate to **Firewall & network protection**.

# 🔒 Firewall & network protection

Who and what can access your networks.

## Domain network

Firewall is on.

## Private network (active)

Firewall is on.

## Public network

Firewall is on.

[Allow an app through firewall](#)

[Network and Internet troubleshooter](#)

[Firewall notification settings](#)

[Advanced settings](#)

[Restore firewalls to default](#)

### Domain, Private, and Public

- **Domain** - The domain profile applies to networks where the host system can authenticate to a domain controller.
- **Private** - The private profile is a user-assigned profile and is used to designate private or home networks.
- **Public** - The default profile is the public profile, used to designate public networks such as Wi-Fi hotspots at coffee shops, airports, and other locations.

If you click on any firewall profile, another screen will appear with two options: **turn the firewall on/off** and **block all incoming connections**.

## Private network

Networks at home or work, where you know and trust the people and devices on the network, and where your device is set as discoverable.

### Active private networks

 Network 3

### Windows Defender Firewall

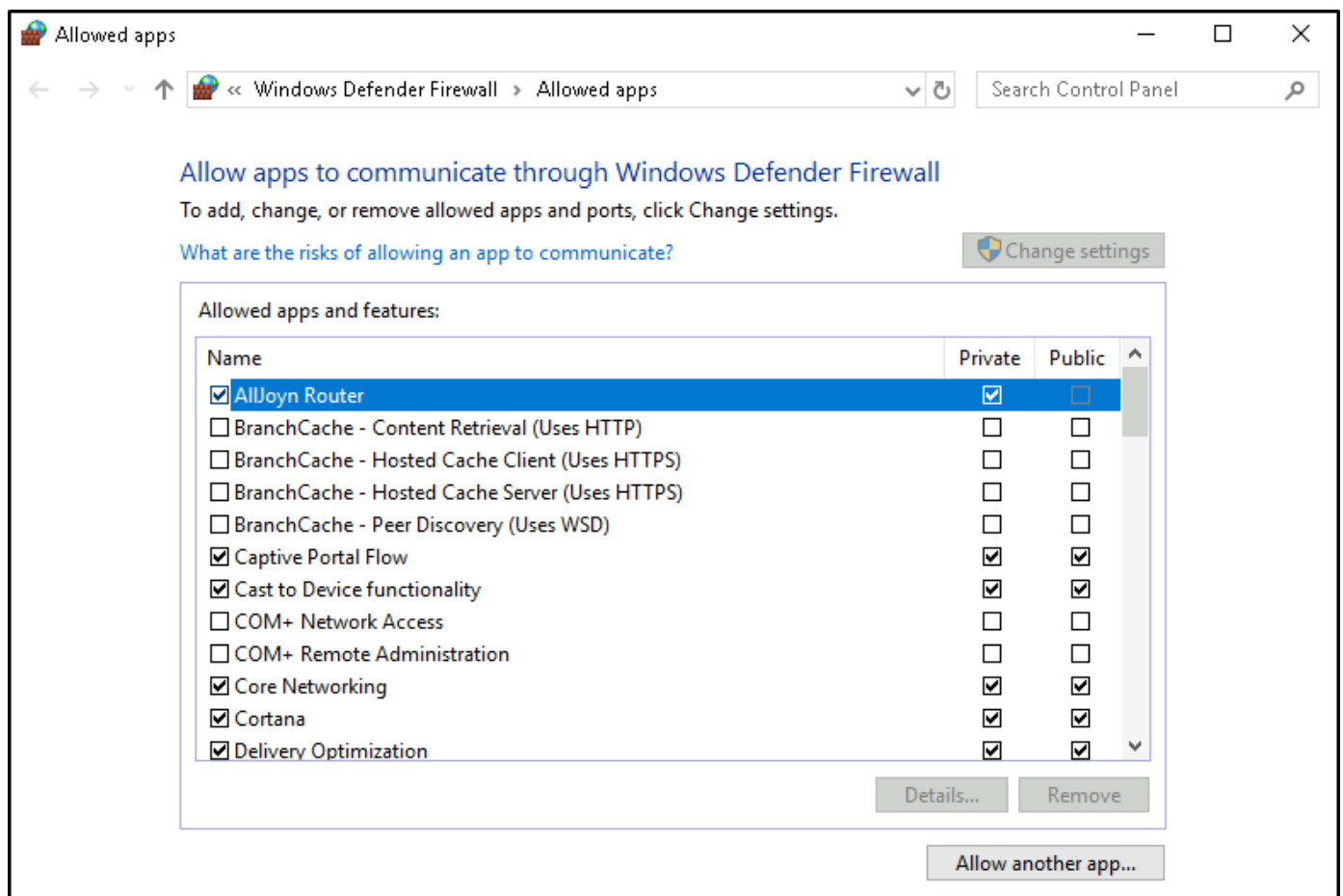
Helps protect your device while on a private network.

 On

### Incoming connections

Prevents incoming connections when on a private network.

☐ Blocks all incoming connections, including those in the list of allowed apps.



In the above image, several apps have access in the Private and/or Public firewall profile. Some of the apps will provide additional information if it's available via the [Details](#) button.

## App & Browser Control

***"Microsoft Defender SmartScreen protects against phishing or malware websites and applications, and the downloading of potentially malicious files".***

## App & browser control

App protection and online security.

### Check apps and files

Windows Defender SmartScreen helps protect your device by checking for unrecognized apps and files from the web.

☐ Block

☒ Warn

☐ Off

[Privacy Statement](#)

### Exploit protection

Exploit protection is built into Windows 10 to help protect your device against attacks. Out of the box, your device is already set up with the protection settings that work best for most people.

[Exploit protection settings](#)

[Privacy Statement](#)

[Learn more](#)

### Check apps and files

- **Windows Defender SmartScreen** helps protect your device by checking for unrecognized apps and files from the web.

## Windows protected your PC

Windows Defender SmartScreen prevented an unrecognized app from starting. Running this app might put your PC at risk.

[More info](#)

Don't run

### Exploit protection



- Exploit protection is built into Windows 10 to help protect your device against attacks.

## Exploit protection

See the Exploit protection settings for your system and programs. You can customize the settings you want.

### System settings   Program settings


#### Control flow guard (CFG)

Ensures control flow integrity for indirect calls.

Use default (On) 

#### Data Execution Prevention (DEP)

Prevents code from being run from data-only memory pages.

Use default (On) 

#### Force randomization for images (Mandatory ASLR)

Force relocation of images not compiled with /DYNAMICBASE

Use default (Off) 

#### Randomize memory allocations (Bottom-up ASLR)

Randomize locations for virtual memory allocations.

## Device Security

---

## Device security

Security that comes built into your device.

### Core isolation

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

[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 security.

### Memory integrity

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

 Off

### Security processor

## Security processor

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

[Security processor details](#)



## Security processor details

Information about the trusted platform module (TPM).

### Specifications

Manufacturer	Intel (INTC)
Manufacturer version	303.12.0.0
Specification version	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
Storage	Ready

[Security processor troubleshooting](#)

[Learn more](#)

## Trusted Platform Module (TPM)

*"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".*

## Bit Locker

---

*"BitLocker Drive Encryption is a data protection feature that integrates with the operating system and addresses the threats of data theft or exposure from lost, stolen, or inappropriately decommissioned computers".*

On devices with TPM installed, BitLocker offers the best protection.

*The TPM is a hardware component installed in many newer computers by the computer manufacturers. It works with BitLocker to help protect user data and to ensure that a computer has not been tampered with while the system was offline".*

## Volume Shadow Copy Service

---

Volume Shadow Copy Service (VSS) creates a consistent shadow copy (also known as a snapshot or a point-in-time copy) of the data that is to be backed up.

Volume Shadow Copies are stored on the System Volume Information folder on each drive that has protection enabled.

If VSS is enabled you can perform the following tasks within **advanced system settings**.

- **Create a restore point**
- **Perform system restore**
- **Configure restore settings**
- **Delete restore points**

Malware writers know of this Windows feature and write code in their malware to look for these files and delete them. Doing so makes it impossible to recover from a ransomware attack unless you have an offline/off-site backup.