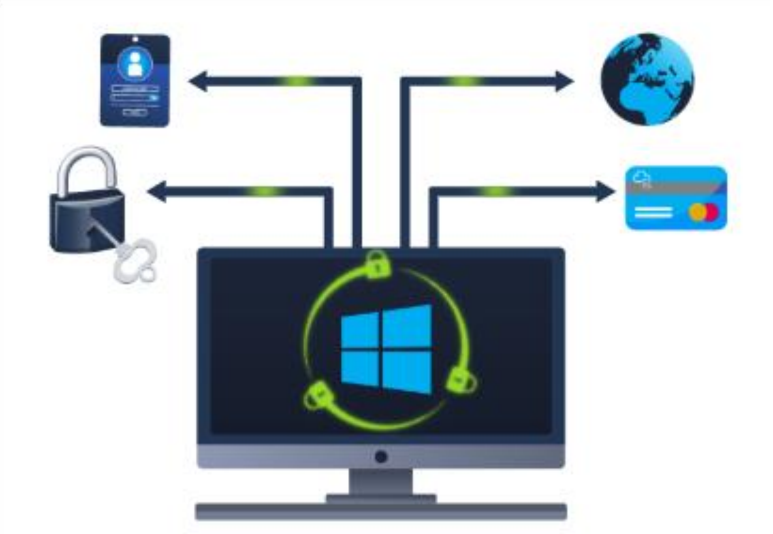
Module 3 Windows Fundamentals 3

Task 1- Introduction



We will continue our journey exploring the Windows operating system.

To summarize the previous two rooms:

- In Windows Fundamentals 1, we covered the desktop, the file system, user account control, the control panel, settings, and the task manager.
- In Windows Fundamentals 2, we covered various utilities, such as System Configuration, Computer Management, Resource Monitor, etc.

This module will attempt to provide an overview of the security features within the Windows operating system.

Press the **Start Machine** button below to launch the attached virtual machine.

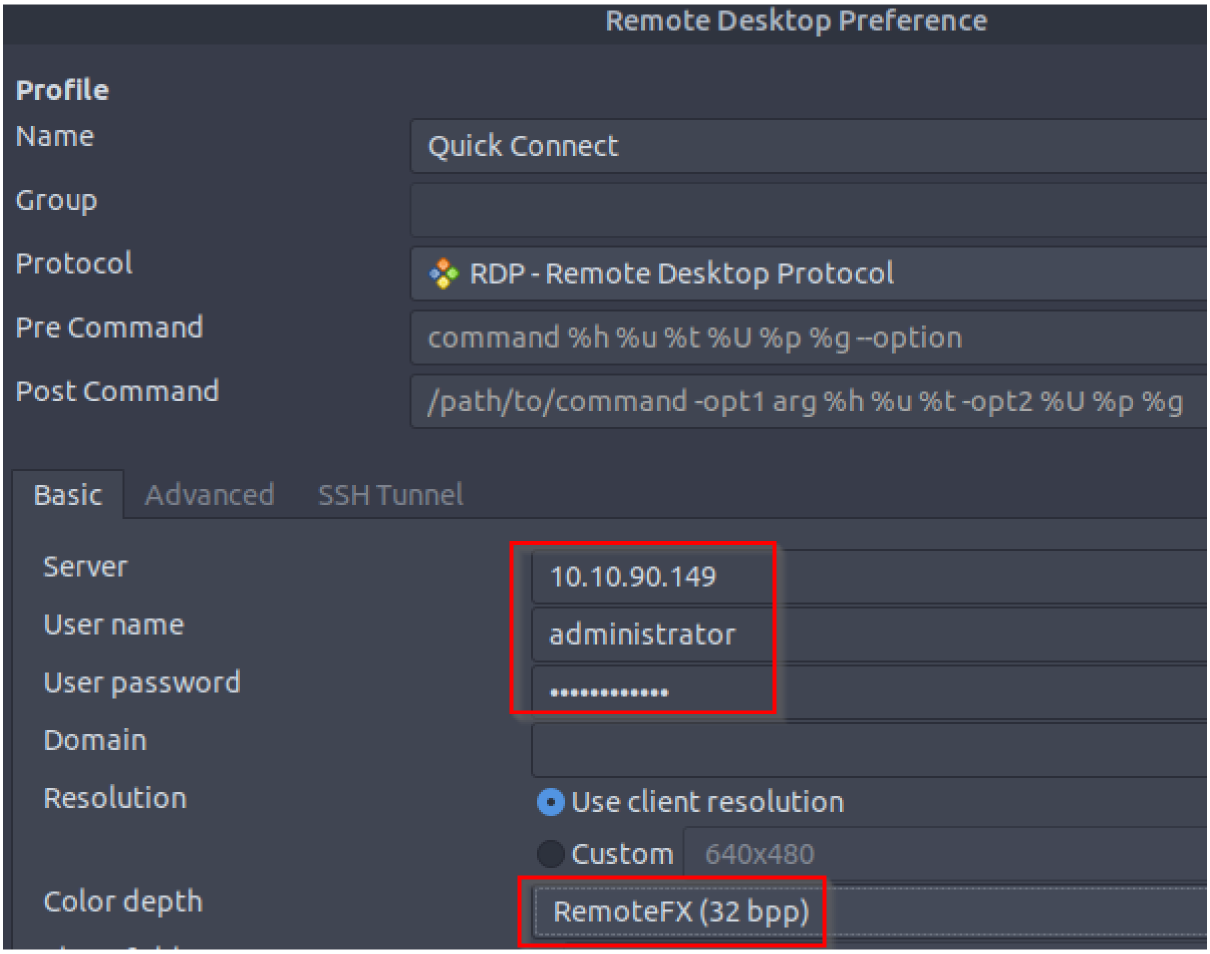
Start Machine

If you wish to access the virtual machine via Remote Desktop, use the credentials below.

Machine IP: MACHINE_IP

User: administrator

Password: letmein123!



Remote Desktop Preference

Profile

Name: Quick Connect

Group:

Protocol: RDP - Remote Desktop Protocol

Pre Command: command %h %u %t %U %p %g --option

Post Command: /path/to/command -opt1 arg %h %u %t -opt2 %U %p %g

Server: 10.10.90.149

User name: administrator

User password: ••••••••••••

Domain:

Resolution: ● Use client resolution ○ Custom 640x480

Color depth: RemoteFX (32 bpp)

Accept the Certificate when prompted, and you should be logged into the remote system now.

Note: The virtual machine may take up to 3 minutes to load.

Answer the questions below

Read the above and start the virtual machine.

Task 2- Windows Updates

Let's start things off with **Windows Update**.

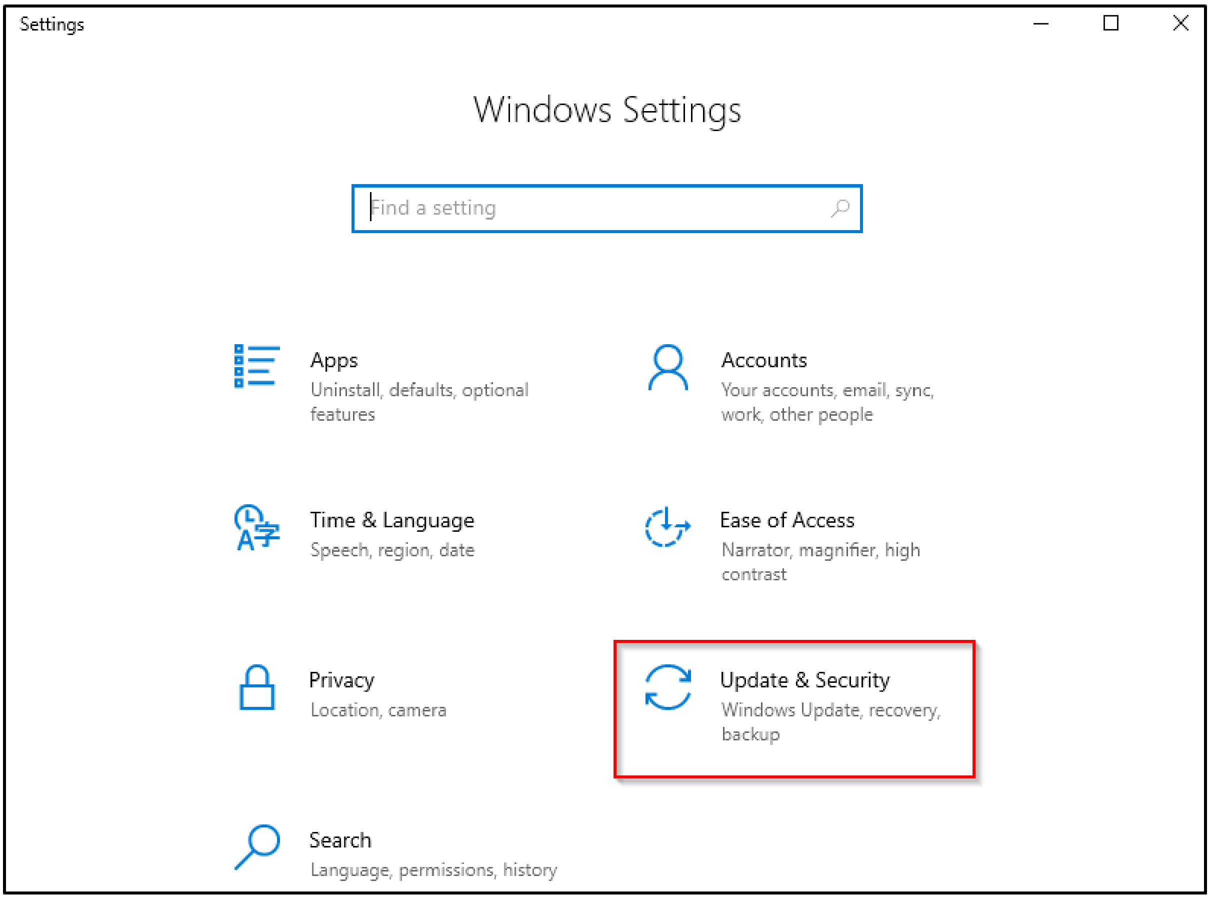
Windows Update is a service provided by Microsoft to provide security updates, feature enhancements, and patches for the Windows operating system and other Microsoft products, such as Microsoft Defender.

Updates are typically released on the 2nd Tuesday of each month. This day is called **Patch Tuesday**. That doesn't necessarily mean that a critical update/patch has to wait for the next Patch Tuesday to be released. If the update is urgent, then Microsoft will push the update via the Windows Update service to the Windows devices.

Refer to the following link to see the **Microsoft Security Update Guide** here**.**

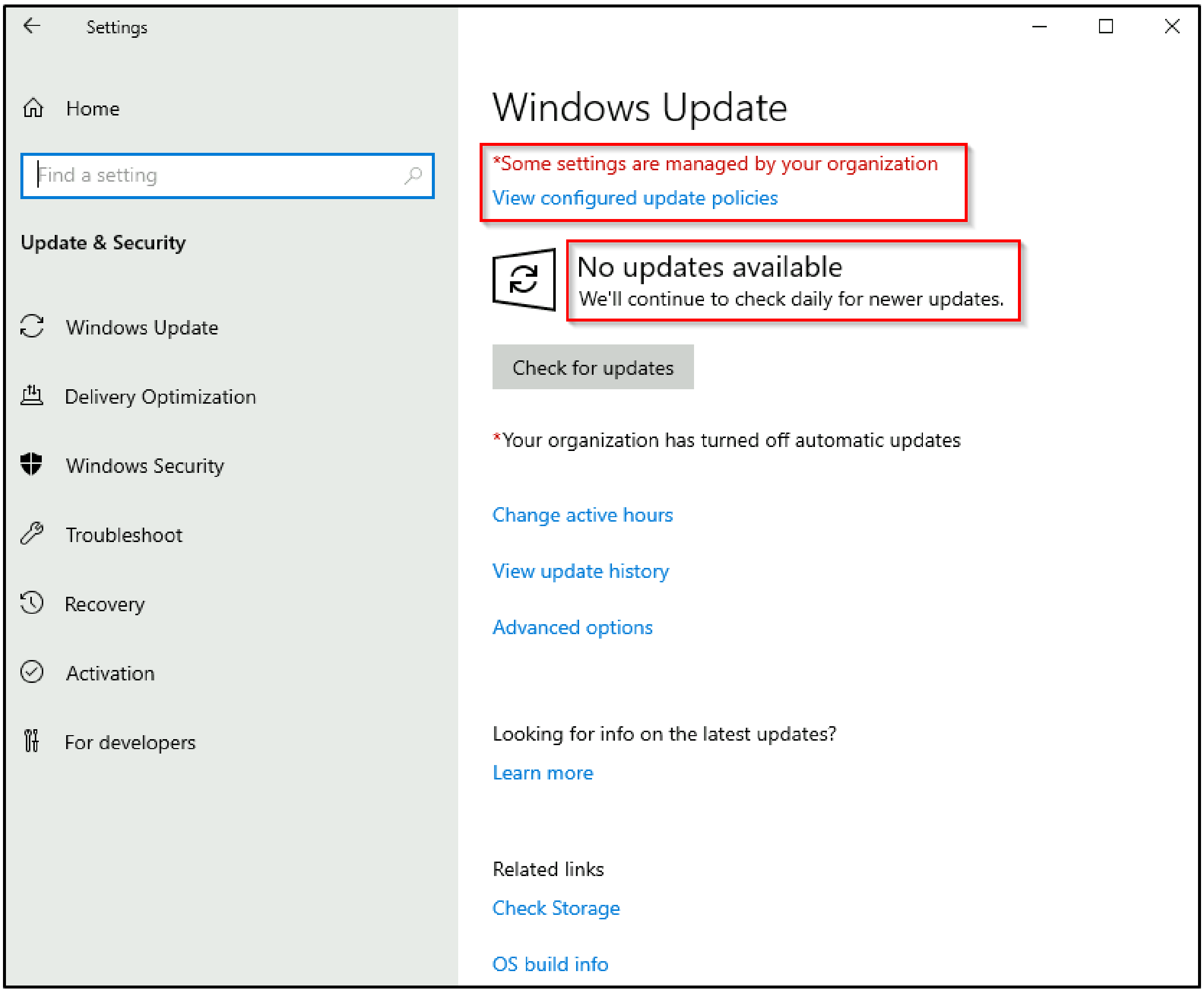
Windows Update is located in Settings. See below.

Tip: Another way to access Windows Update is from the Run dialog box, or CMD, by running the command control /name Microsoft.WindowsUpdate.


Settings
Windows Settings
Find a setting
Apps
Uninstall, defaults, optional features
Accounts
Your accounts, email, sync, work, other people
Time & Language
Speech, region, date
Ease of Access
Narrator, magnifier, high contrast
Privacy
Location, camera
Update & Security
Windows Update, recovery, backup
Search
Language, permissions, history

In the attached VM, there are a few things to highlight.

1. The Windows Update settings are 'managed'. (Typically, home users will not see this type of message)
2. There are no available updates available for the virtual machine. (The attached virtual machine does not have Internet access to communicate with Microsoft to obtain new updates)



Settings

Home

Find a setting

Update & Security

Windows Update

Delivery Optimization

Windows Security

Troubleshoot

Recovery

Activation

For developers

Windows Update

*Some settings are managed by your organization

View configured update policies

No updates available

We'll continue to check daily for newer updates.

Check for updates

*Your organization has turned off automatic updates

Change active hours

View update history

Advanced options

Looking for info on the latest updates?

Learn more

Related links

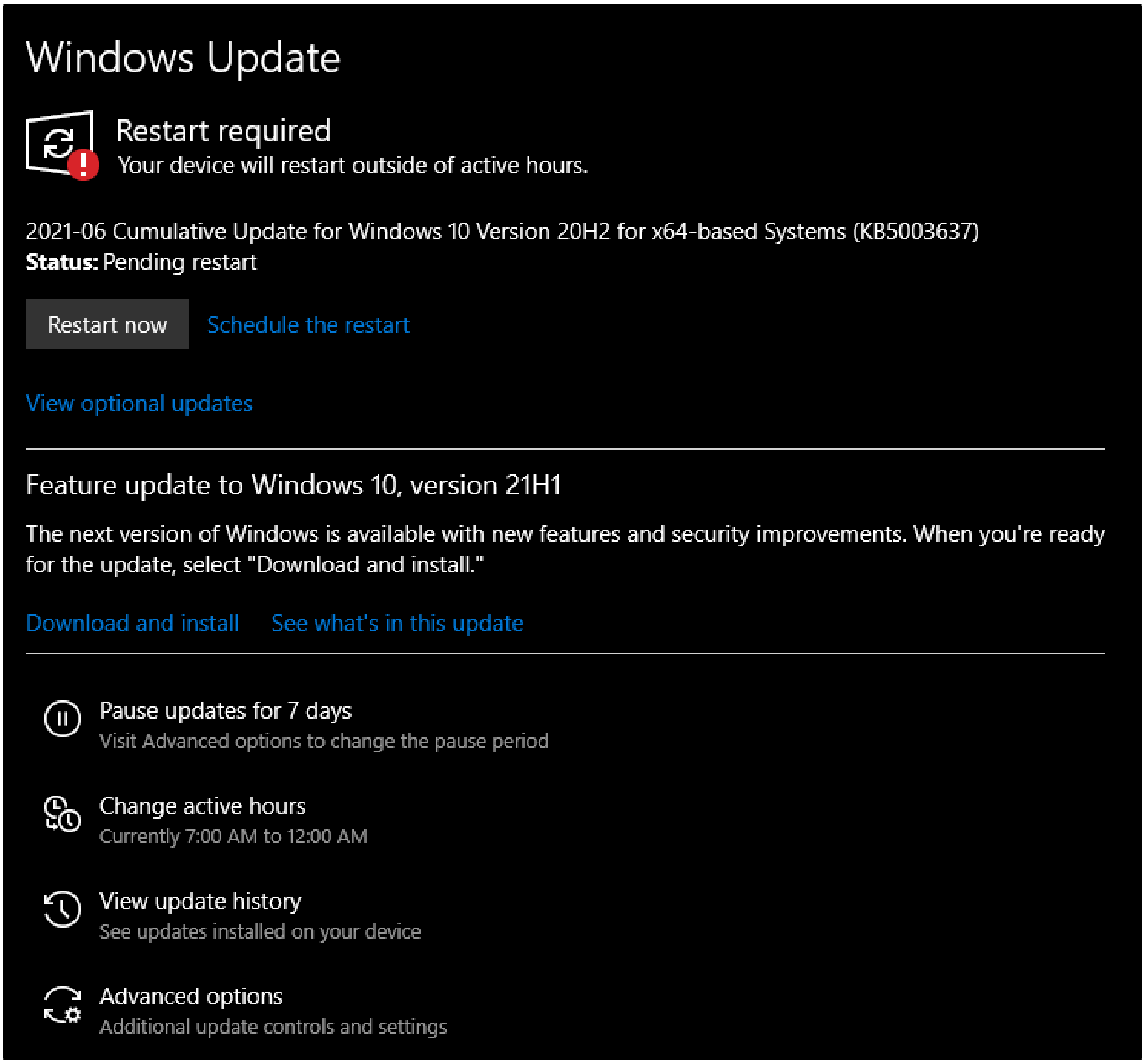
Check Storage

OS build info

Throughout the years, Windows users have grown accustomed to pushing Windows Updates off to a later date or not installing the updates at all. Various reasons caused this action, one being the fact that a reboot is typically required after a Windows update.

Microsoft notably addressed this issue with Windows 10. The updates can no longer be ignored or pushed to the side until forgotten. Windows updates can only be postponed, but eventually, the update will happen, and your computer will reboot. Microsoft provides these updates to keep the device safe and secure.

Below is an image showing how a **Restart required** looks and the several options available regarding scheduling the restart.



Windows Update

Restart required

Your device will restart outside of active hours.

2021-06 Cumulative Update for Windows 10 Version 20H2 for x64-based Systems (KB5003637)

Status: Pending restart

Feature update to Windows 10, version 21H1

The next version of Windows is available with new features and security improvements. When you're ready for the update, select "Download and install."

Download and install
See what's in this update
Pause updates for 7 days
Visit Advanced options to change the pause period
Change active hours

Currently 7:00 AM to 12:00 AM

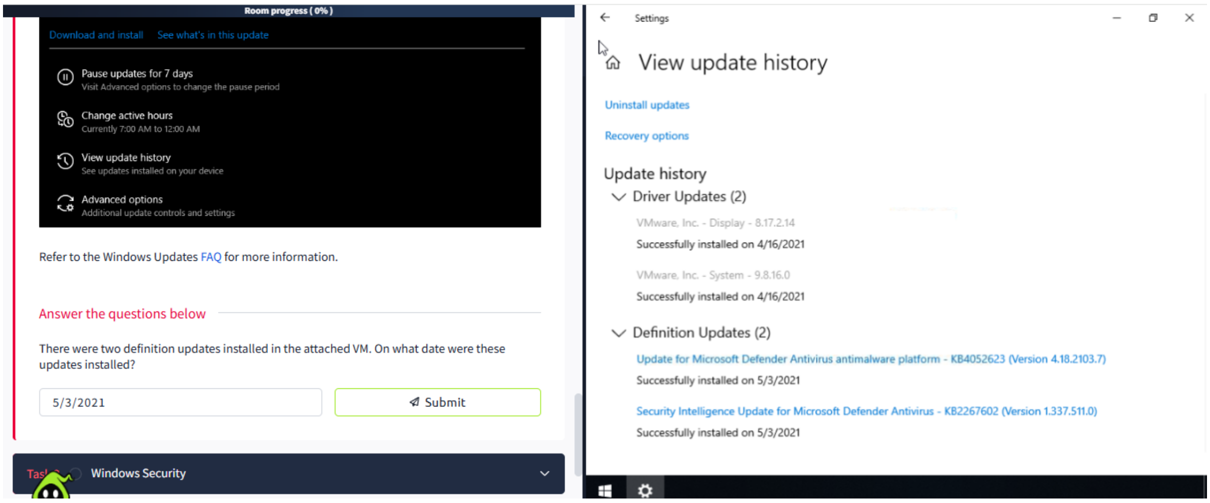
View update history
See updates installed on your device
Advanced options
Additional update controls and settings

Refer to the Windows Updates FAQ for more information.

Answer the questions below

There were two definition updates installed in the attached VM. On what date were these updates installed?

5/3/2021



Pause updates for 7 days
Visit Advanced options to change the pause period

Change active hours
Currently 7:00 AM to 12:00 AM

View update history
See updates installed on your device

Advanced options
Additional update controls and settings

Refer to the Windows Updates FAQ for more information.

Answer the questions below

There were two definition updates installed in the attached VM. On what date were these updates installed?

5/3/2021

View update history

Update history

Driver Updates (2)

VMware, Inc. - Display - 8.17.2.14
Successfully installed on 4/16/2021

VMware, Inc. - System - 9.8.16.0
Successfully installed on 4/16/2021

Definition Updates (2)

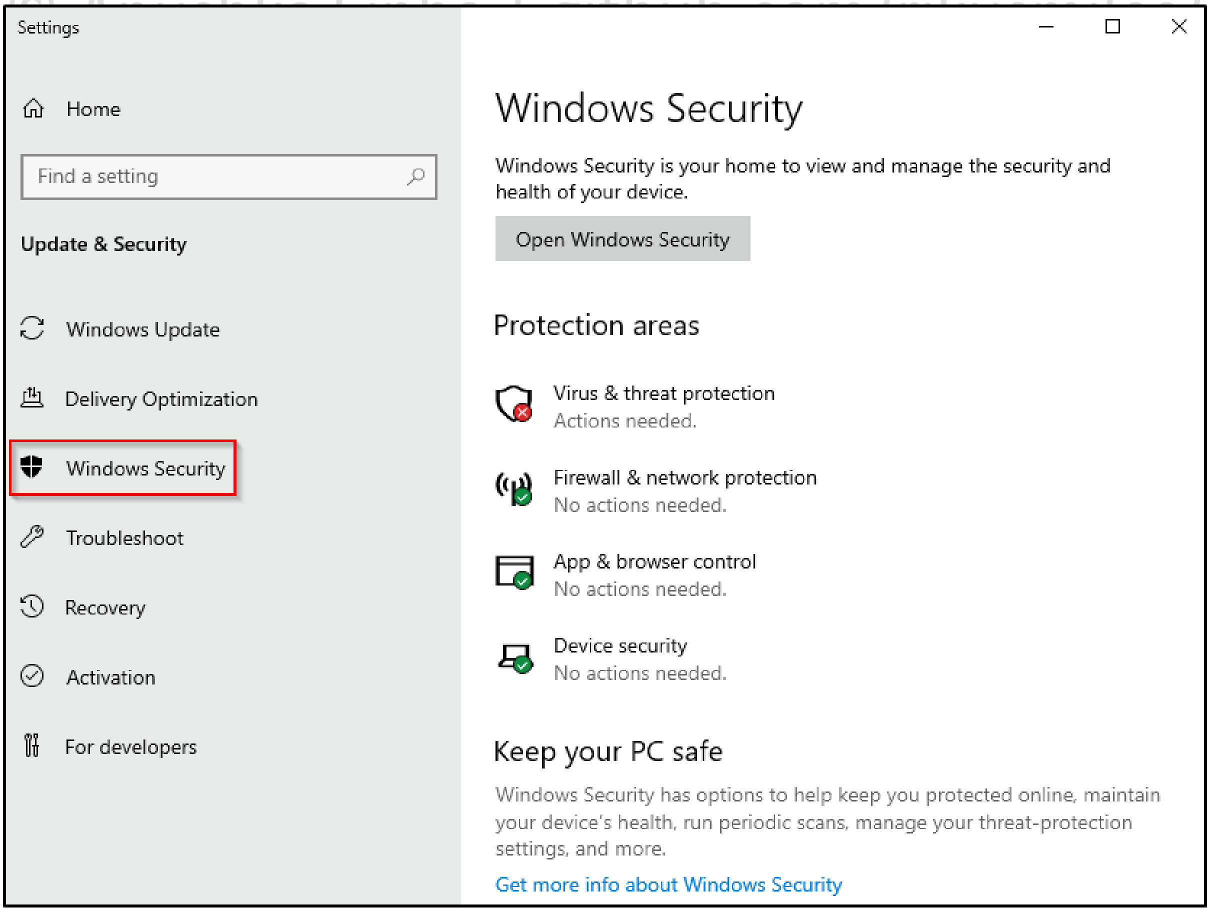
Update for Microsoft Defender Antivirus antimalware platform - KB4052623 (Version 4.18.2103.7)
Successfully installed on 5/3/2021

Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.337.511.0)
Successfully installed on 5/3/2021

Task 3- Windows Security

Per Microsoft, "***Windows Security** is your home to manage the tools that protect your device and your data*".

In case you missed it, **Windows Security** is also available in **Settings**.



Windows Security

Windows Security is your home to view and manage the security and health of your device.

Protection areas

Virus & threat protection
Actions needed.

Firewall & network protection
No actions needed.

App & browser control
No actions needed.

Device security
No actions needed.

Keep your PC safe

Windows Security has options to help keep you protected online, maintain your device's health, run periodic scans, manage your threat-protection settings, and more.

In the above image, focus your attention on **Protection areas**.

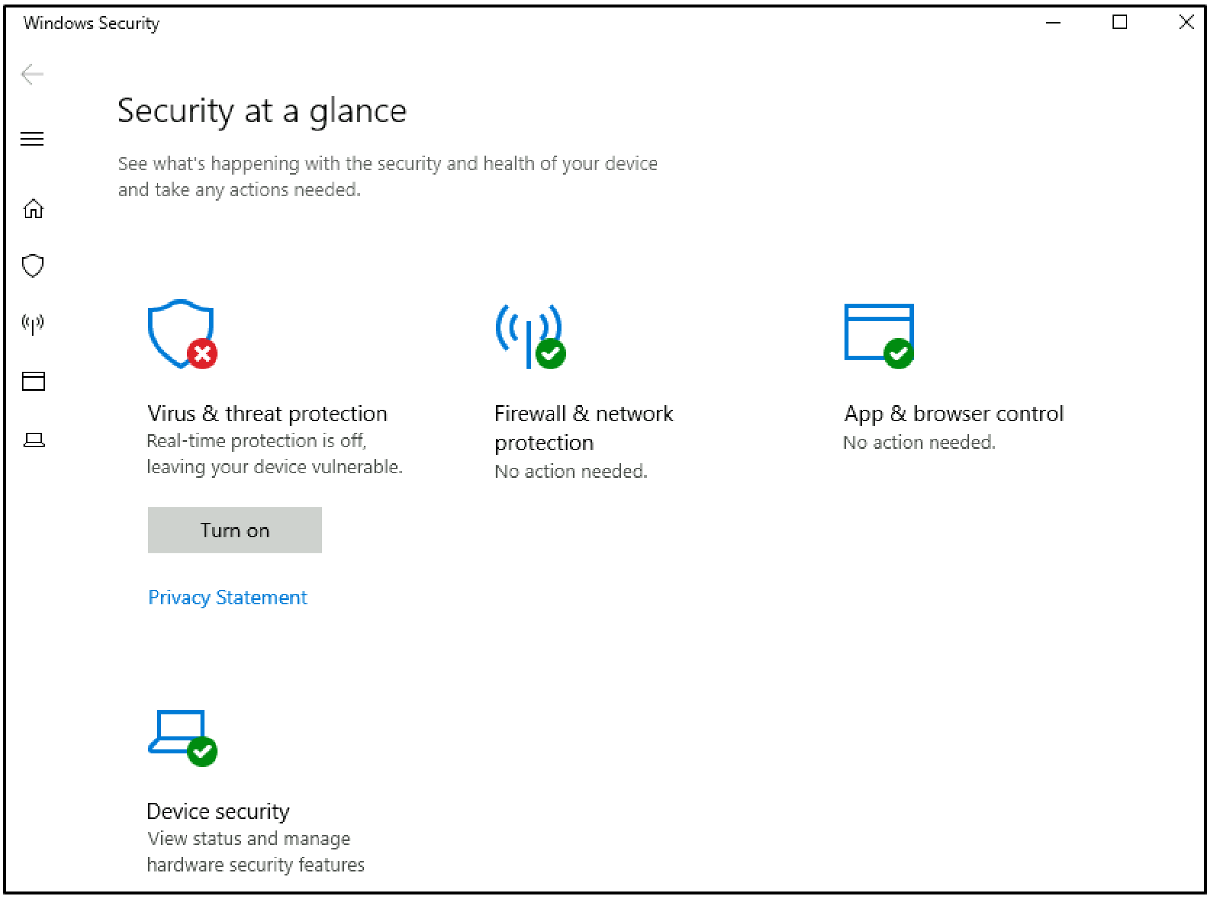
- **Virus & threat protection**
- **Firewall & network protection**
- **App & browser control**
- **Device security**

Each following task will briefly touch on these areas.

Before proceeding, let's provide a quick comment on the status icons.

- **Green** means your device is sufficiently protected, and there aren't any recommended actions.
- **Yellow** means there is a safety recommendation for you to review.
- **Red** is a warning that something needs your immediate attention.

Click on Open Windows Security.



Windows Security

Security at a glance

See what's happening with the security and health of your device and take any actions needed.

Virus & threat protection
Real-time protection is off, leaving your device vulnerable.

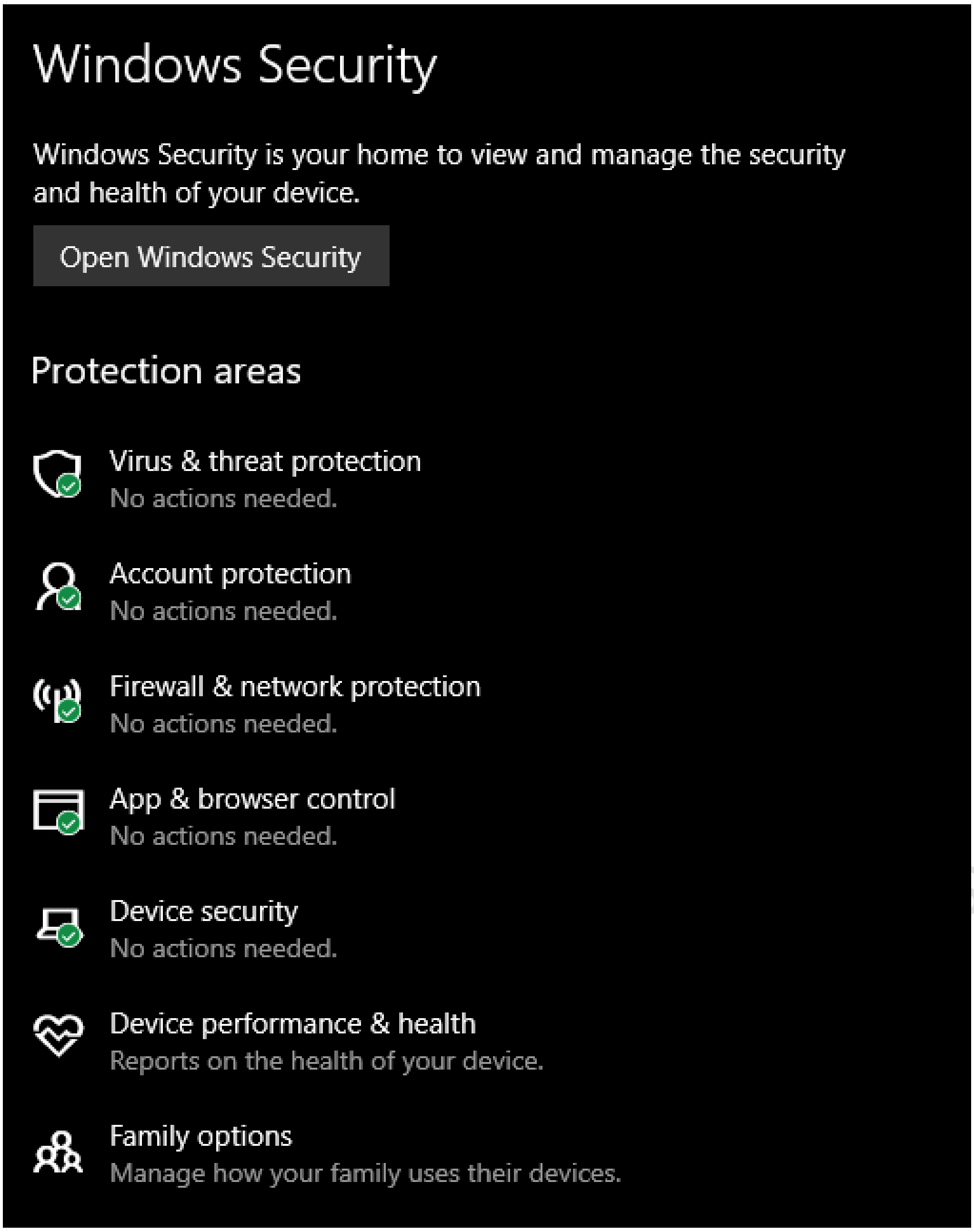
Firewall & network protection
No action needed.

App & browser control
No action needed.

Device security
View status and manage hardware security features

Note: Since the attached VM is a **Windows Server 2019** edition, it looks different from a **Windows 10 Home** or **Professional** edition.

The below image is from a Windows 10 device.



Windows Security

Windows Security is your home to view and manage the security and health of your device.

Protection areas

Virus & threat protection
No actions needed.

Account protection
No actions needed.

Firewall & network protection
No actions needed.

App & browser control
No actions needed.

Device security
No actions needed.

Device performance & health
Reports on the health of your device.

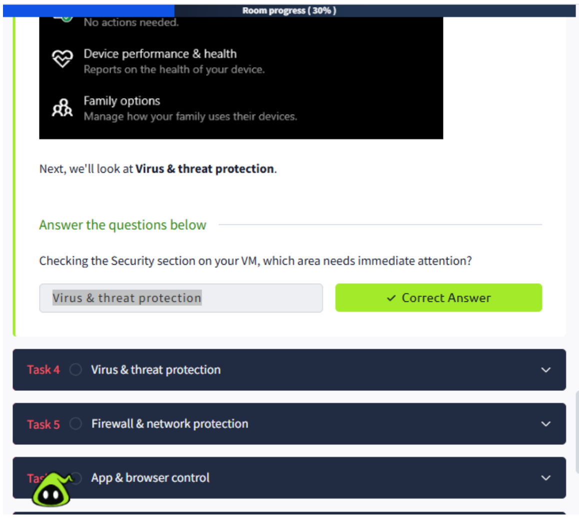
Family options
Manage how your family uses their devices.

Next, we'll look at **Virus & threat protection**.

Answer the questions below

Checking the Security section on your VM, which area needs immediate attention?

Virus & threat protection



Room progress (30%)

No actions needed.

Device performance & health
Reports on the health of your device.

Family options
Manage how your family uses their devices.

Next, we'll look at **Virus & threat protection**.

Answer the questions below

Checking the Security section on your VM, which area needs immediate attention?

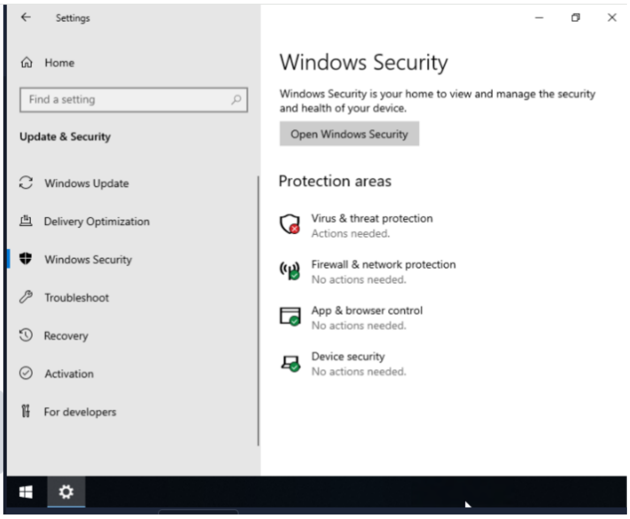
Virus & threat protection

✓ Correct Answer

Task 4 ○ Virus & threat protection

Task 5 ○ Firewall & network protection

Ta ○ App & browser control



Settings

Home

Find a setting

Update & Security

Windows Update

Delivery Optimization

Windows Security

Troubleshoot

Recovery

Activation

For developers

Windows Security

Windows Security is your home to view and manage the security and health of your device.

Open Windows Security

Protection areas

Virus & threat protection
Actions needed.

Firewall & network protection
No actions needed.

App & browser control
No actions needed.

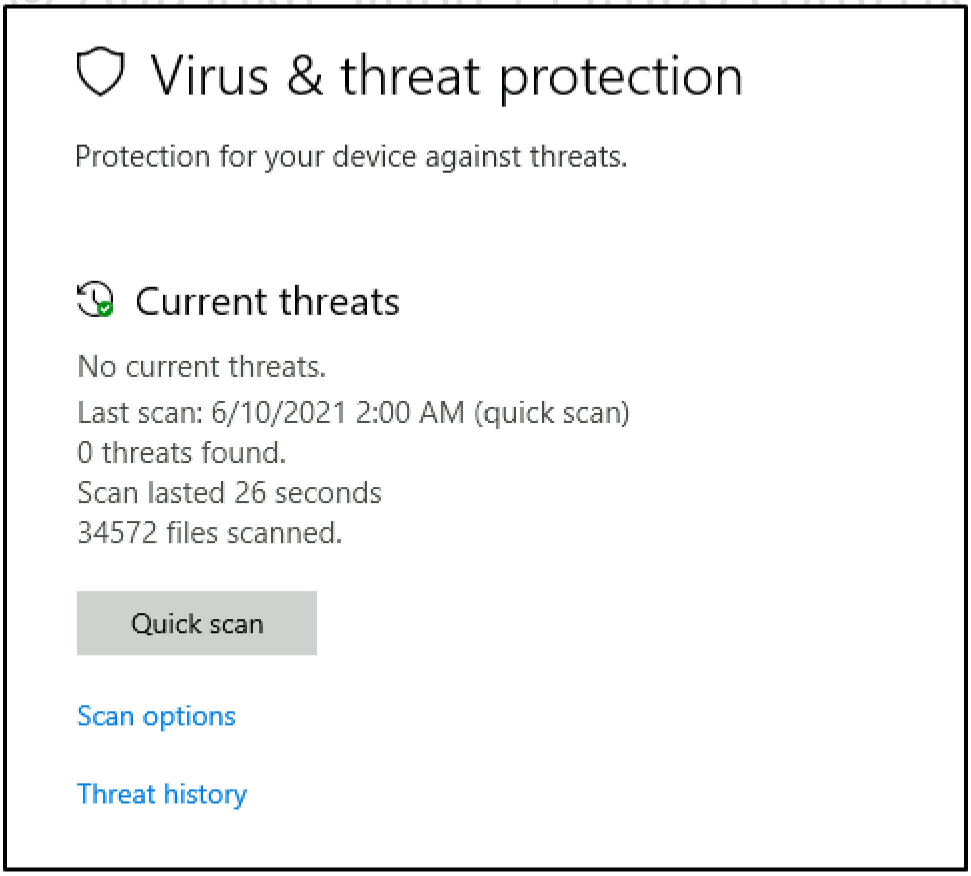
Device security
No actions needed.

Task 4- 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

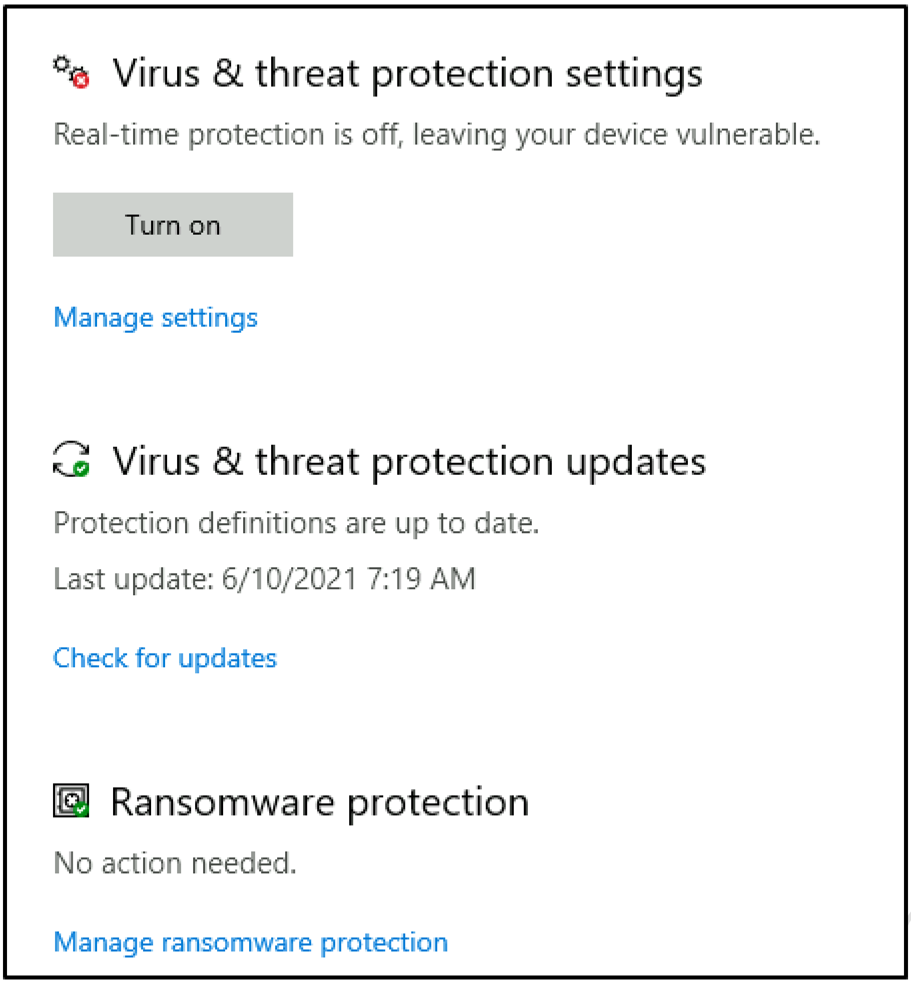
- **Quick scan** - Checks folders in your system where threats are commonly found.
- **Full scan** - Checks all files and running programs on your hard disk. This scan could take longer than one hour.
- **Custom scan** - Choose which files and locations you want to check.

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.

Warning: Allow an item to run that has been identified as a threat only if you are **100%** sure of what you are doing.

Next is **Virus & threat protection settings**.



Virus & threat protection settings

Real-time protection is off, leaving your device vulnerable.

Manage settings

Virus & threat protection updates

Protection definitions are up to date.

Last update: 6/10/2021 7:19 AM

Check for updates

Ransomware protection

No action needed.

Manage ransomware protection

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.

Warning: Excluded items could contain threats that make your device vulnerable. Only use this option if you are **100%** sure of what you are doing.

Virus & threat protection updates

- **Check for updates** - Manually check for updates to update Windows Defender Antivirus definitions.

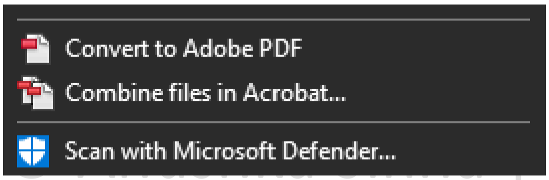
Ransomware protection

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

Note: Real-time protection is turned off in the attached VM to decrease the chances of performance issues. Since the VM can't reach the Internet and there aren't any threats in the VM, this is safe to do. Real-time protection should definitely be enabled in your personal Windows devices unless you have a 3rd party product that provides the same protection. Ensure it's always up-to-date and enabled.

Tip: You can perform on-demand scans on any file/folder by right-clicking the item and selecting 'Scan with Microsoft Defender'.

The below image was taken from another Windows device to show this feature.



Answer the questions below

Specifically, what is turned off that Windows is notifying you to turn on?

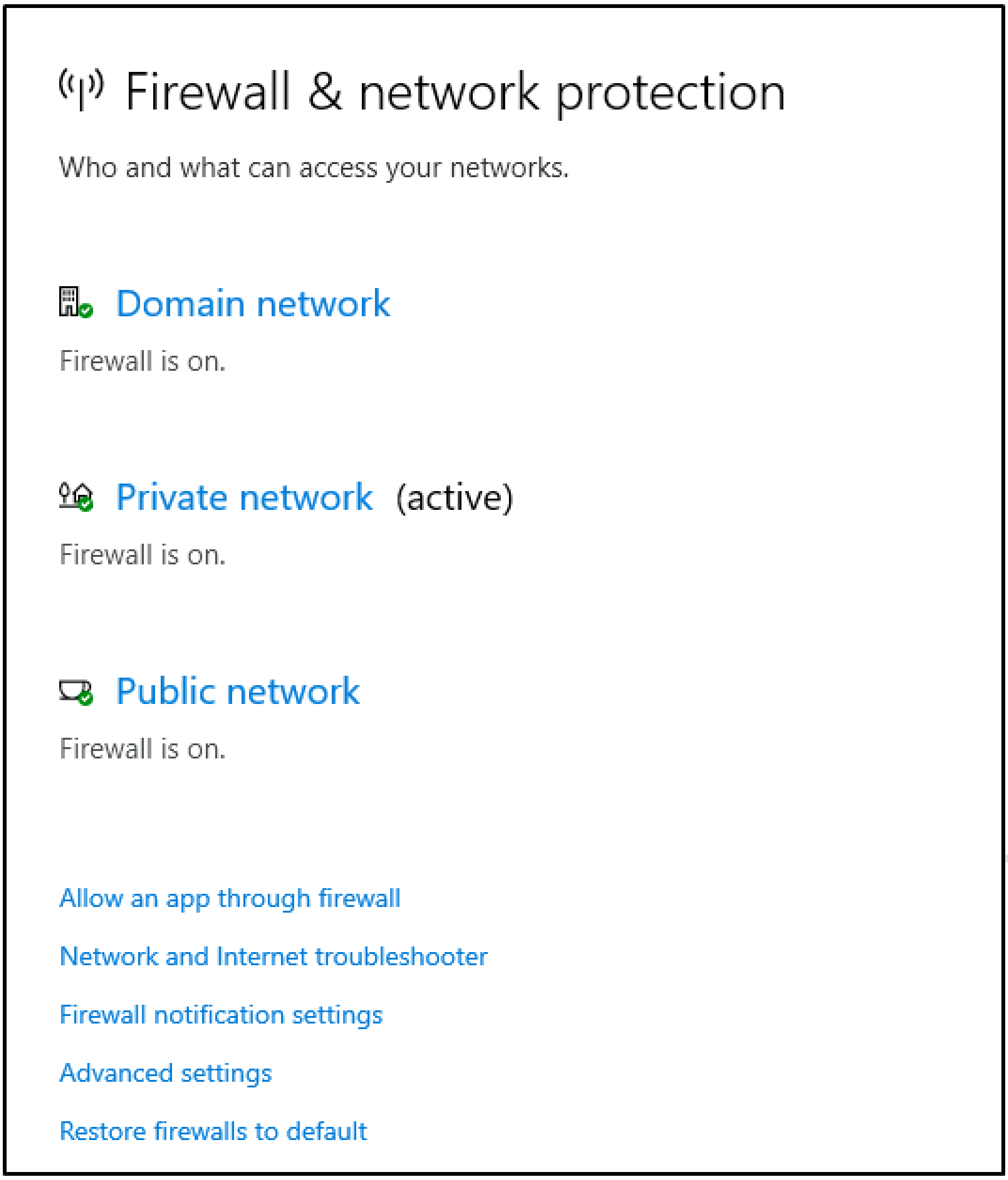
Real-time protection

Task 5- 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

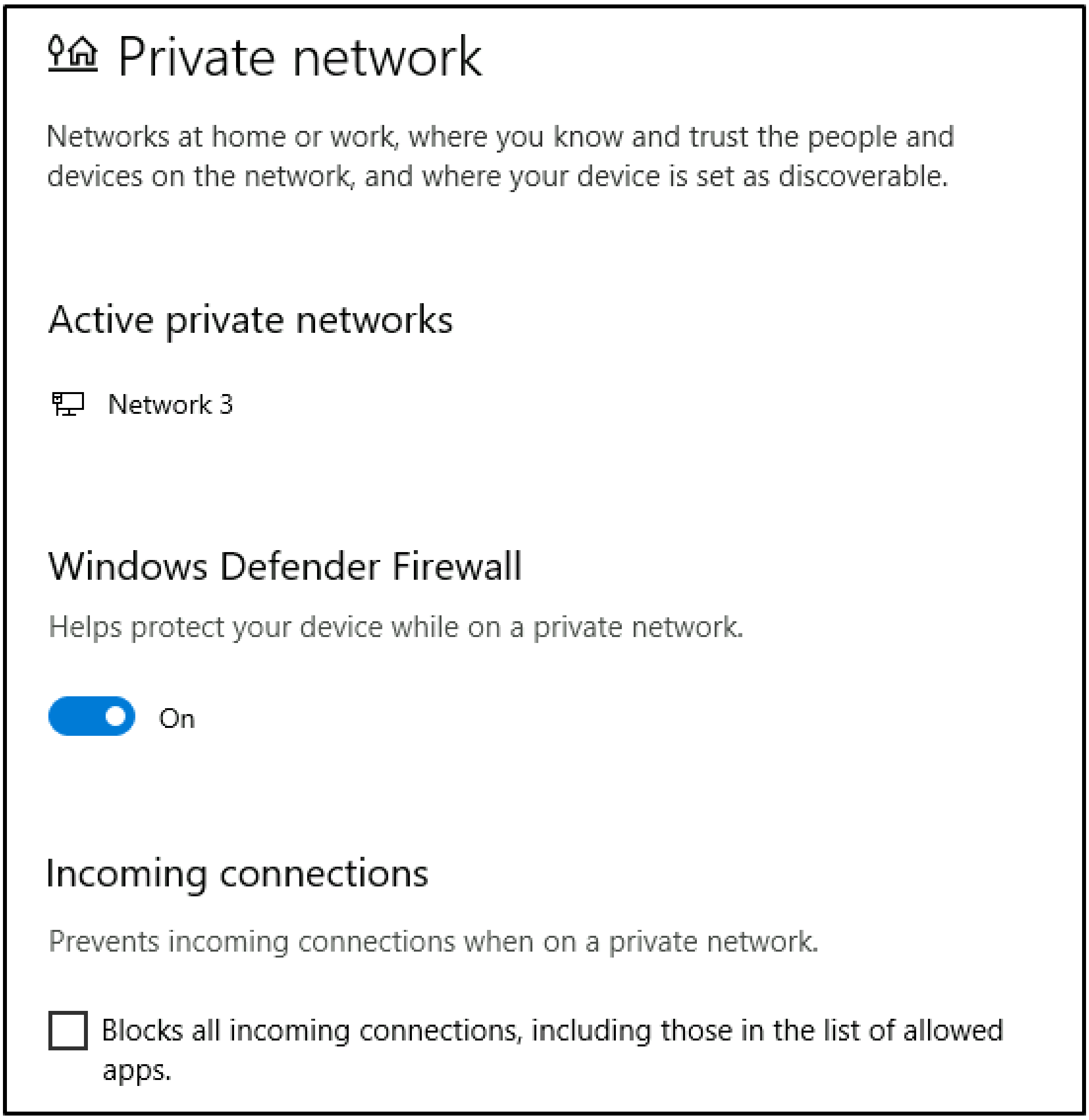
Note: Each network may have different status icons for you.

What is the difference between the 3 (**Domain**, **Private**, and **Public**)?

Per Microsoft, "*Windows Firewall offers three firewall profiles: 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

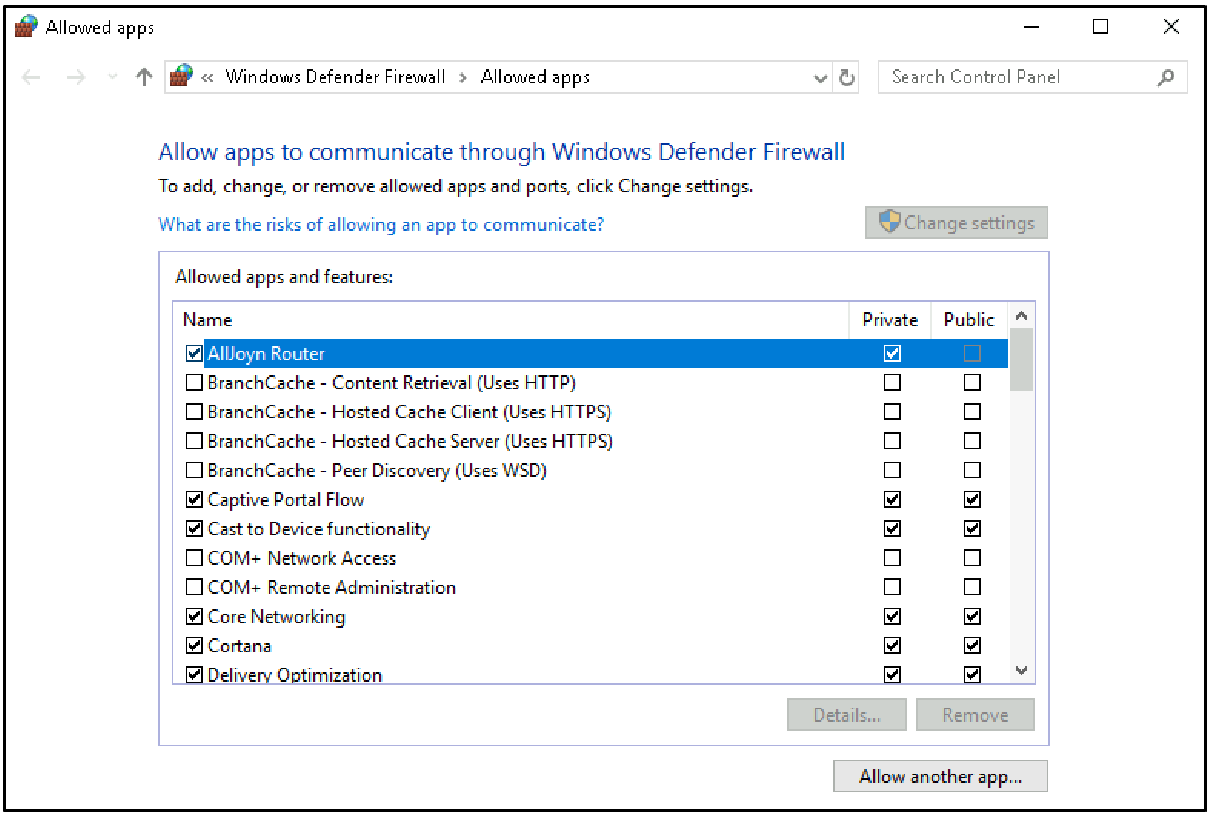
Incoming connections

Prevents incoming connections when on a private network.

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

Warning: Unless you are **100%** confident in what you are doing, it is recommended that you leave your Windows Defender Firewall enabled.

Allow an app through firewall



Allow apps to communicate through Windows Defender Firewall

To add, change, or remove allowed apps and ports, click Change settings.

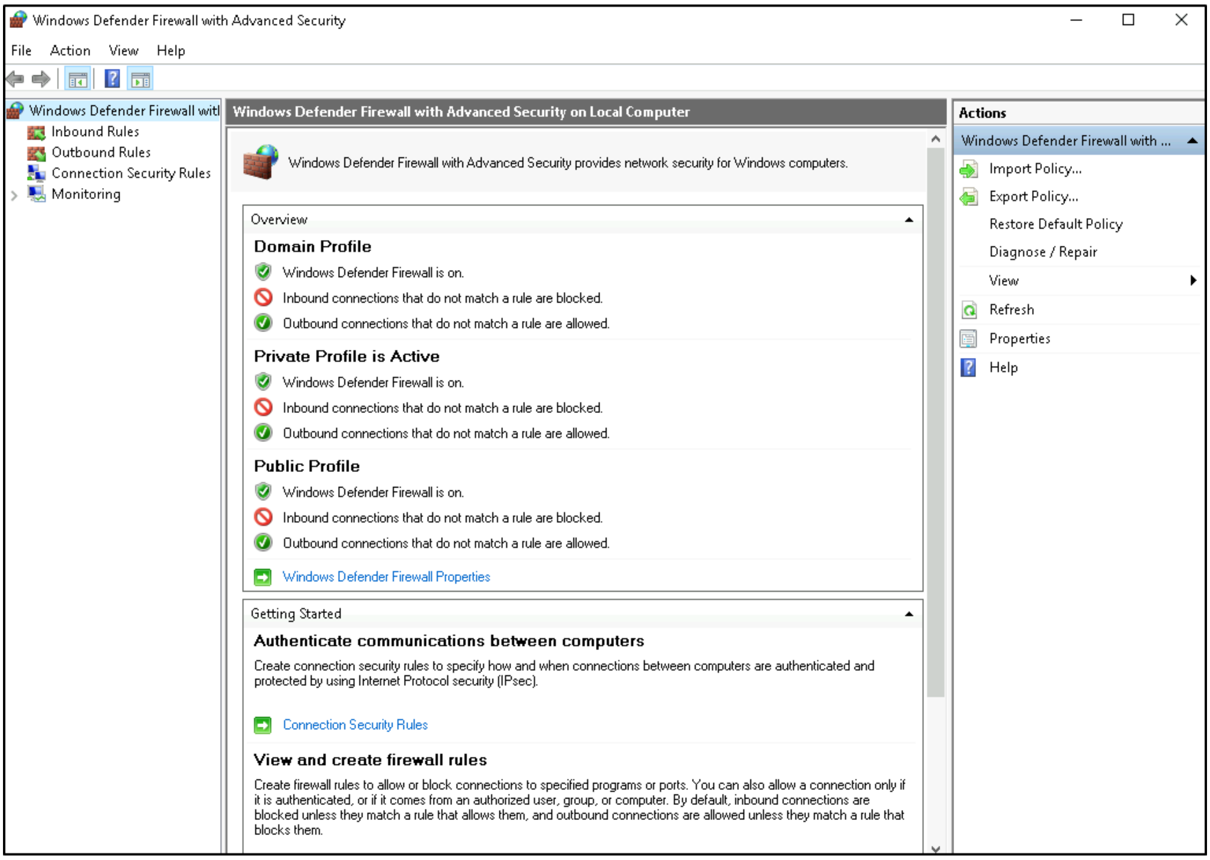
What are the risks of allowing an app to communicate?

Allowed apps and features:

Name	Private	Public
☑ AllJoyn Router	☑	□
□ BranchCache - Content Retrieval (Uses HTTP)	□	□
□ BranchCache - Hosted Cache Client (Uses HTTPS)	□	□
□ BranchCache - Hosted Cache Server (Uses HTTPS)	□	□
□ BranchCache - Peer Discovery (Uses WSD)	□	□
☑ Captive Portal Flow	☑	☑
☑ Cast to Device functionality	☑	☑
□ COM+ Network Access	□	□
□ COM+ Remote Administration	□	□
☑ Core Networking	☑	☑
☑ Cortana	☑	☑
☑ Delivery Optimization	☑	☑

You can view what the current settings for any firewall profile are. 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.

Advanced Settings



Windows Defender Firewall with Advanced Security on Local Computer

Windows Defender Firewall with Advanced Security provides network security for Windows computers.

Overview

Domain Profile

- ✓ Windows Defender Firewall is on.
- ⊘ Inbound connections that do not match a rule are blocked.
- ✓ Outbound connections that do not match a rule are allowed.

Private Profile is Active

- ✓ Windows Defender Firewall is on.
- ⊘ Inbound connections that do not match a rule are blocked.
- ✓ Outbound connections that do not match a rule are allowed.

Public Profile

- ✓ Windows Defender Firewall is on.
- ⊘ Inbound connections that do not match a rule are blocked.
- ✓ Outbound connections that do not match a rule are allowed.

Windows Defender Firewall Properties

Getting Started

Authenticate communications between computers

Create connection security rules to specify how and when connections between computers are authenticated and protected by using Internet Protocol security (IPsec).

Connection Security Rules

View and create firewall rules

Create firewall rules to allow or block connections to specified programs or ports. You can also allow a connection only if it is authenticated, or if it comes from an authorized user, group, or computer. By default, inbound connections are blocked unless they match a rule that allows them, and outbound connections are allowed unless they match a rule that blocks them.

Configuring the **Windows Defender Firewall** is for advanced Windows users. Refer to the following Microsoft documentation on best practices here.

Tip: Command to open the Windows Defender Firewall is WF.msc.

Answer the questions below

If you were connected to airport Wi-Fi, what most likely will be the active firewall profile?

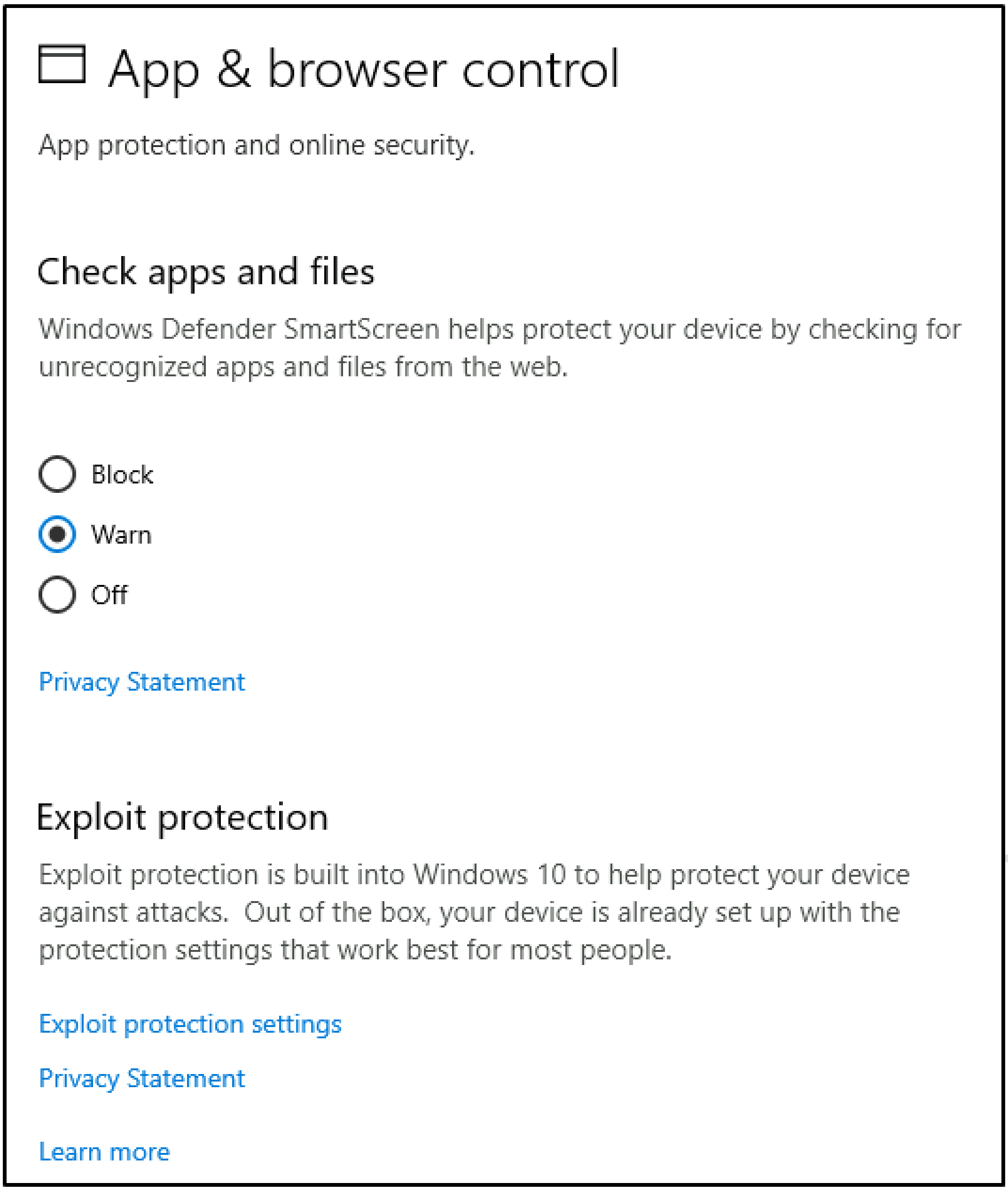
Public network

Task 6- App & browser control

In this section, you can change the settings for the **Microsoft Defender SmartScreen**.

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

Refer to the official Microsoft document for more information on Microsoft Defender SmartScreen here.



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.

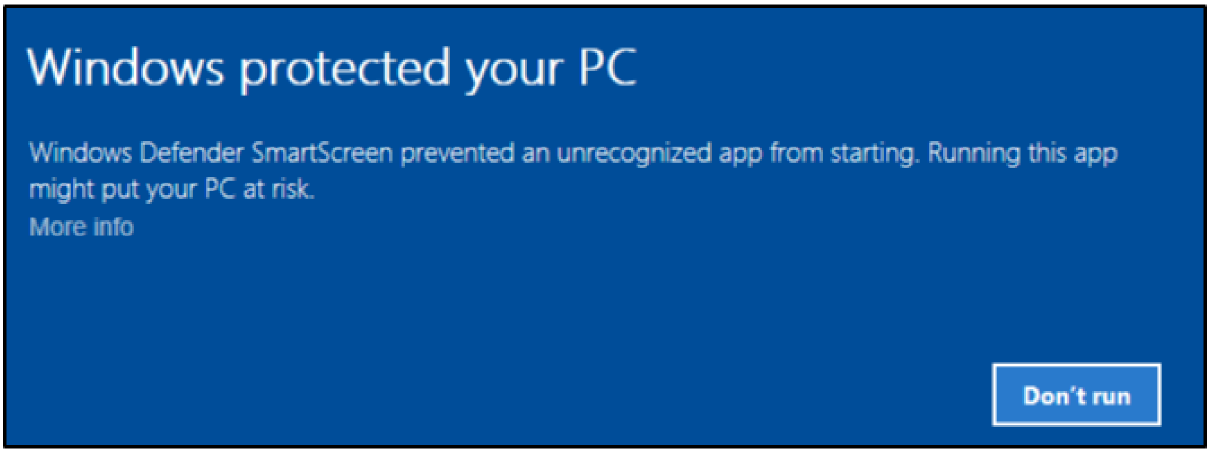
Exploit protection settings

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.

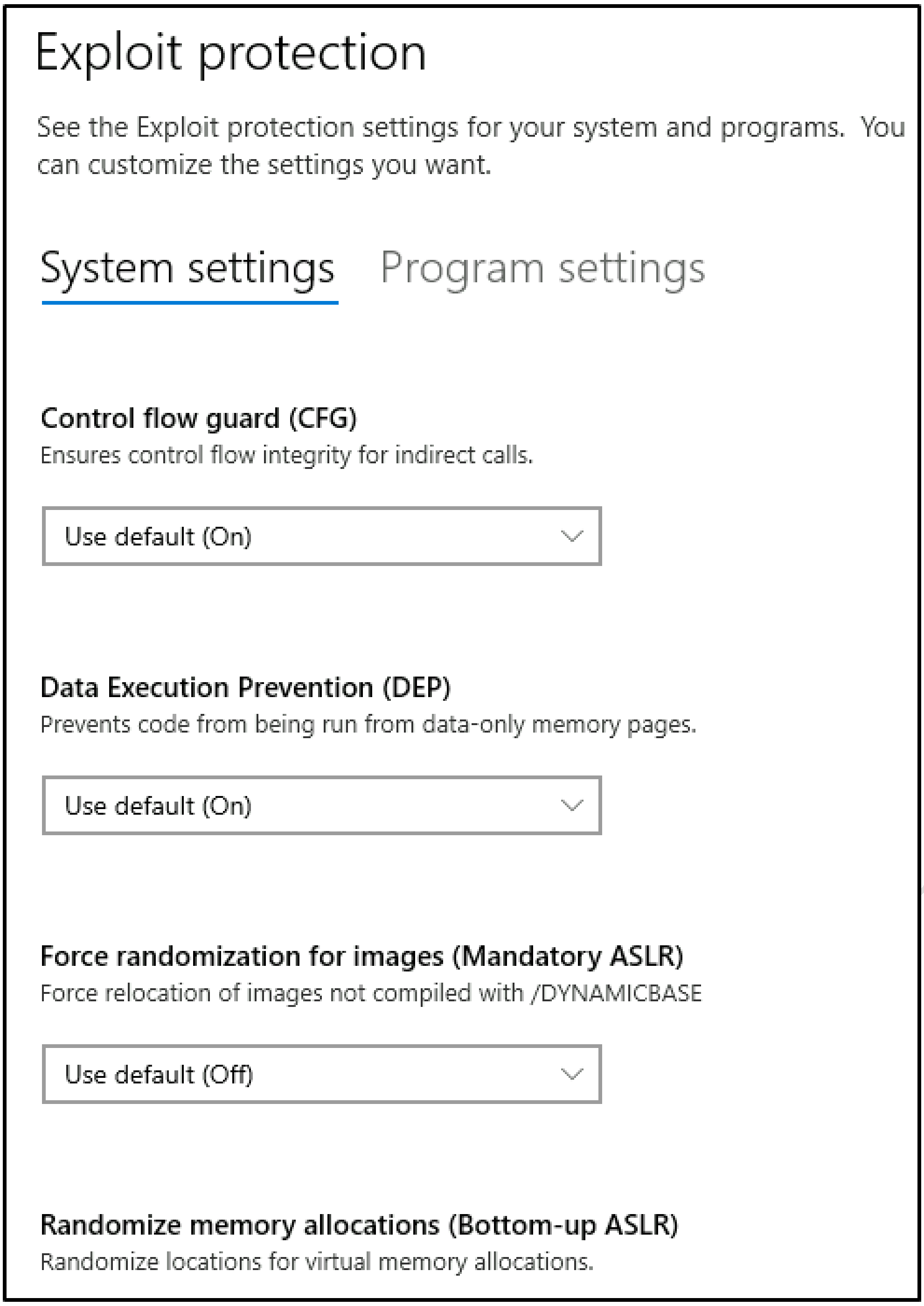


Windows protected your PC

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

Exploit protection

- Exploit protection is built into Windows 10 (and, in our case, Windows Server 2019to 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.

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.

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

Task 8- BitLocker

What is **BitLocker**?

Per Microsoft, "*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.

Per Microsoft, "*BitLocker provides the most protection when used with a Trusted Platform Module (TPM) version 1.2 or later. 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*".

Refer to the official Microsoft documentation to learn more about BitLocker here.

Note: The BitLocker feature is not included in the attached VM.

Answer the questions below

We should use a removable drive on systems **without** a TPM version 1.2 or later. What does this removable drive contain?

Startup key

Task 9- Volume Shadow Copy Service

Per Microsoft, the **Volume Shadow Copy Service** (VSS) coordinates the required actions to create a consistent shadow copy (also known as a snapshot or a point-in-time copy) of the data that is to be backed up.

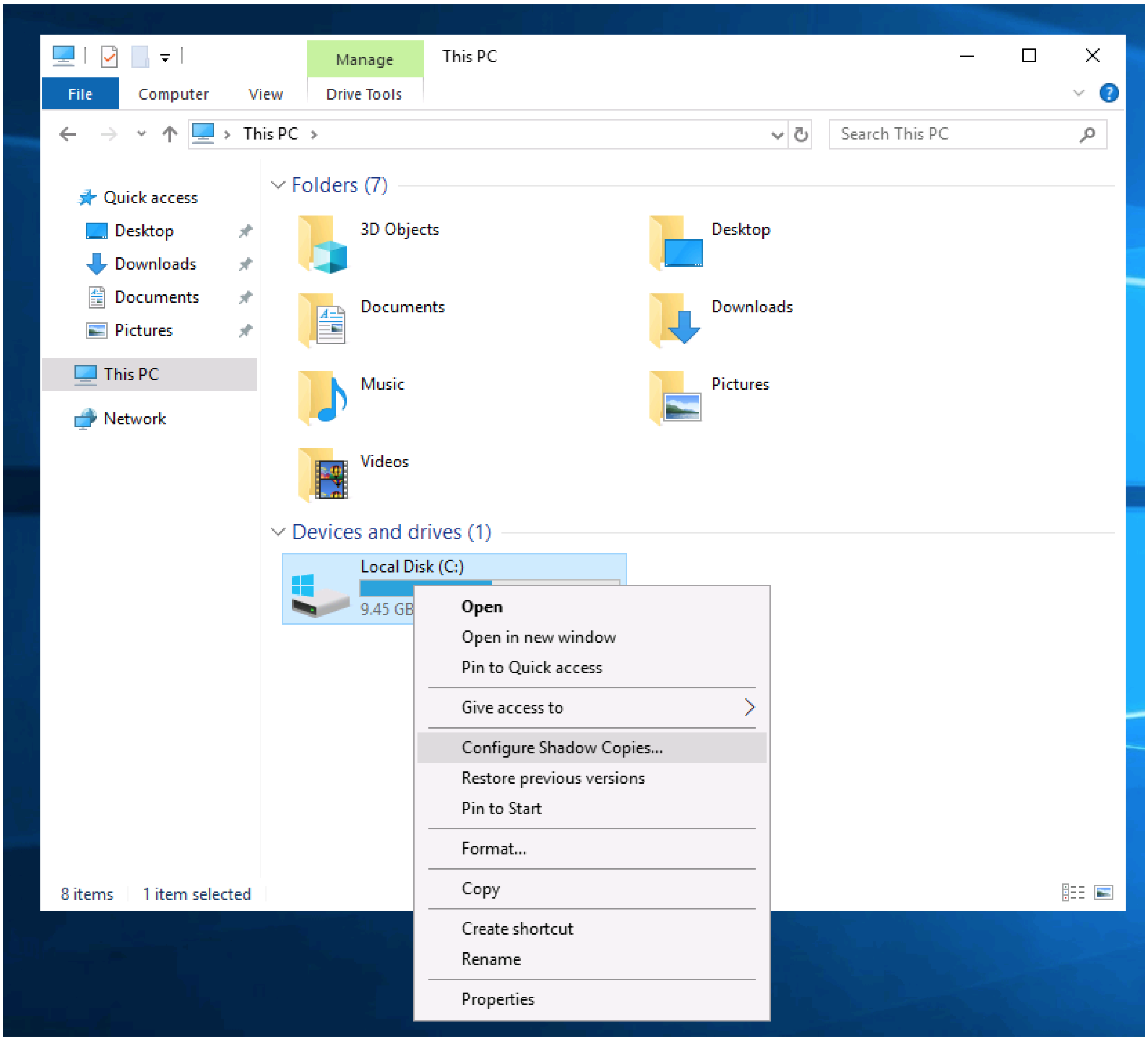
Volume Shadow Copies are stored on the System Volume Information folder on each drive that has protection enabled.

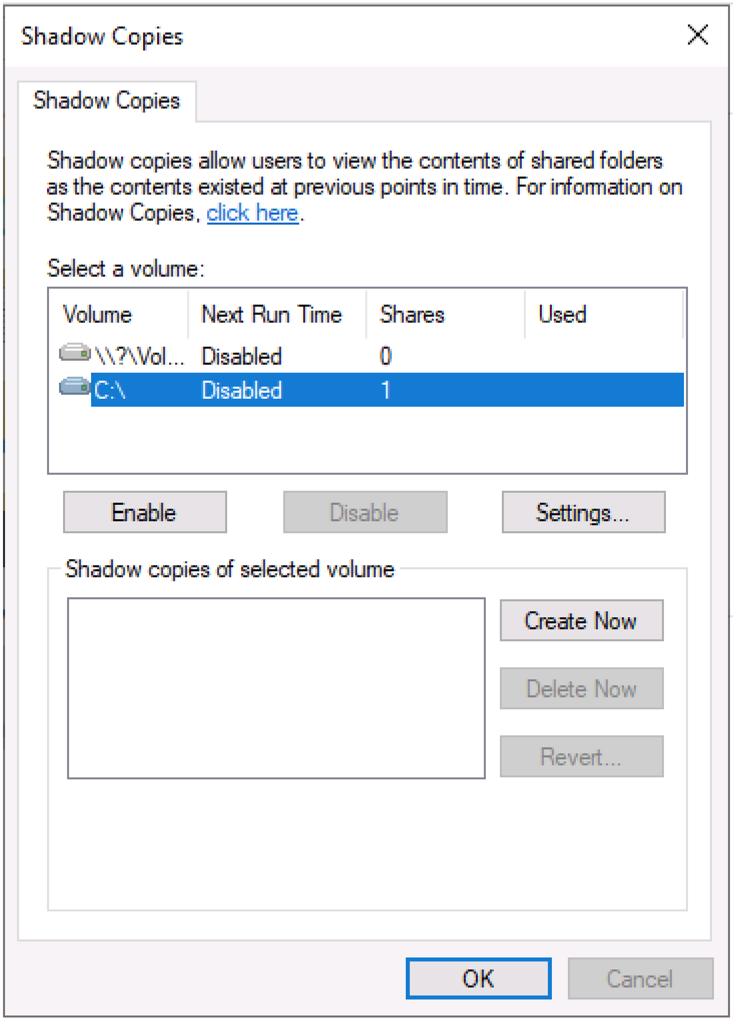
If VSS is enabled (**System Protection** turned on), you can perform the following tasks from within **advanced system settings**.

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

From a security perspective, 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.

If you wish to configure Shadow Copies within the attached VM, see below.





Shadow Copies

Shadow copies allow users to view the contents of shared folders as the contents existed at previous points in time. For information on Shadow Copies, click here.

Select a volume:

Volume	Next Run Time	Shares	Used
\\?\Vol...	Disabled	0	
C:\	Disabled	1	

Shadow copies of selected volume

Bonus: If you wish to interact hands-on with VSS, I suggest exploring Day 23 of Advent of Cyber 2.

Answer the questions below

What is VSS?

Volume Shadow Copy Service.

Task 10- Conclusion

In this room, we covered several built-in Windows security tools that ship with the Windows OS to help keep the device protected.

There is still so much to explain and cover regarding the Windows OS. As mentioned in the Windows Fundamentals 1 room, "*The content is aimed at those who wish to understand and use the Windows OS on a more comfortable level* ."

To learn more about the Windows OS, you'll need to continue the journey on your own.

Further reading material:

- Antimalware Scan Interface
- Credential Guard
- Windows 10 Hello
- CSO Online - The best new Windows 10 security features

Note: Attackers use built-in Windows tools and utilities in an attempt to go undetected within the victim environment. This tactic is known as Living Off The Land. Refer to the following resource here to learn more about this.

References:

TryHackMe Labs