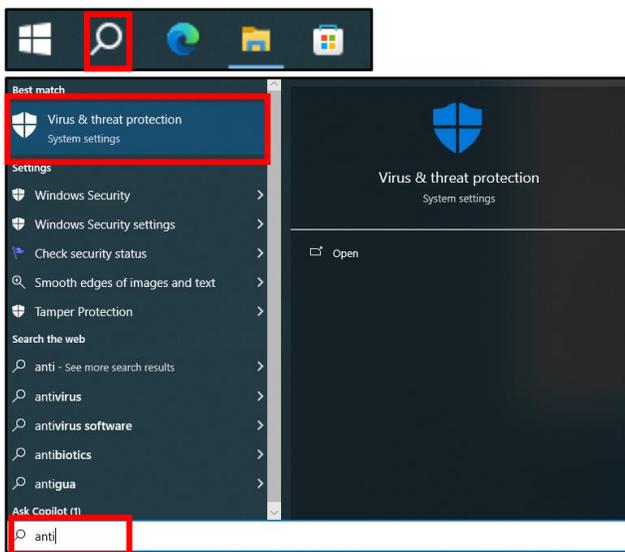


ANTI-VIRUS

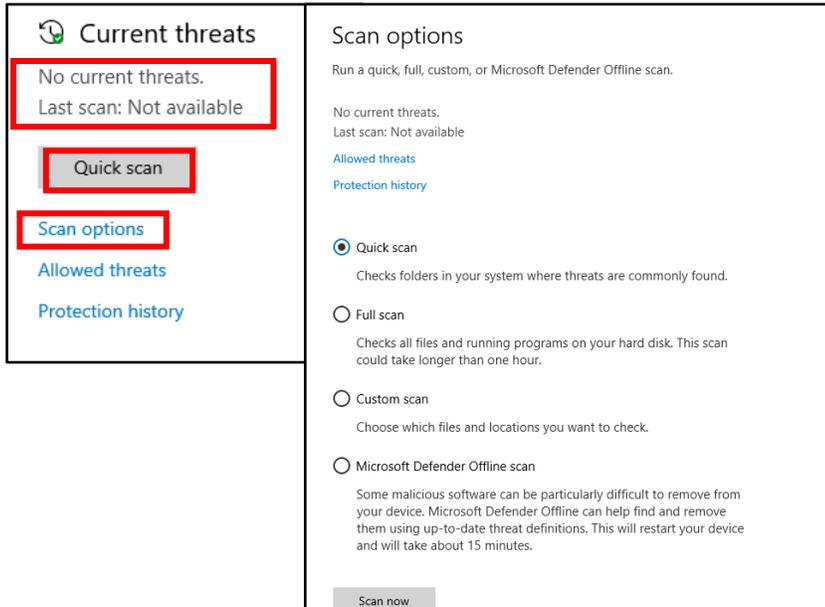
Windows Security

Start by going to the search tab at the bottom left near the windows button. Once here you can type in “anti” and it will pull up the “Virus & threat protection” screen. Once here, you can start going through the Windows built in anti-virus software. **Note:** If you have a separate anti-virus software installed, it will appear here as highlighted below, and will conflict with windows anti-virus software. It is **recommended** that you just use Windows built in anti-virus, it is just shown in this card for training purposes.



Current threats

If you continue to scroll down you will reach the “Current threats” portion. Here it will display if there are any current threats detected and when your last scan was. It is recommended you do a “quick scan” every week. You can also go into the “scan options” and choose what type of scan you want to perform.



This card is based off of Windows OS. MacOS has its own anti-virus system called XProtect. There is no way to access XProtect through Mac settings. You can always download additional anti-virus software's to your MAC, but it is recommended that you just use XProtect as they can conflict with each other.

ANTI-VIRUS

Virus & threat protection

Next is the “Virus & threat protection” settings. Here it will display if the anti-virus has detected any viruses or threats that need to be dealt with. You can also go into “Manage settings” to ensure certain ones are enabled. It is recommended that you keep all the options enabled. As shown below, if you have other anti-virus software installed, some options will be turned off.

Virus & threat protection settings
No action needed.
[Manage settings](#)

Virus & threat protection updates
Security intelligence is up to date.
Last update: 8/27/2024 5:23 PM
[Check for updates](#)

Virus & threat protection settings
View and update Virus & threat protection settings for Microsoft Defender Antivirus.
You're using other antivirus providers.
Real-time protection
Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.
 Off
Cloud-delivered protection
Provides increased and faster protection with access to the latest protection data in the cloud. Works best with Automatic sample submission turned on.
 On
Automatic sample submission
Send sample files to Microsoft to help protect you and others from potential threats. We'll prompt you if the file we need is likely to contain personal information.
 On
[Submit a sample manually](#)

Tamper Protection
Prevents others from tampering with important security features.
 Off
[Learn more](#)
Controlled folder access requires turning on Real-time protection.
Controlled folder access
Protect files, folders, and memory areas on your device from unauthorized changes by unfriendly applications.
[Manage Controlled folder access](#)

Exclusions
Microsoft Defender Antivirus won't scan items that you've excluded. Excluded items could contain threats that make your device vulnerable.
[Add or remove exclusions](#)

Notifications
Microsoft Defender Antivirus will send notifications with critical information about the health and security of your device. You can specify which non-critical notifications you would like.
[Change notification settings](#)

Ransomware protection

Last is the “Ransomware protection” portion. It will display if your anti-virus has detected any ransomware. You can also go into “manage ransomware protection” to view its settings. Note: For the ransomware data recovery to work, you must have it connected to your “OneDrive.” If you happen to have an anti-virus you use and like, it is recommended you go down to “Microsoft Defender Antivirus options” and have it enabled.

Ransomware protection
No action needed.
[Manage ransomware protection](#)

Microsoft Defender Antivirus options
You can keep using your current provider, and have Microsoft Defender Antivirus periodically check for threats.
Periodic scanning
 On

Ransomware protection
Protect your files against threats like ransomware, and see how to restore files in case of an attack.
Controlled folder access requires turning on Real-time protection.
Controlled folder access
Protect files, folders, and memory areas on your device from unauthorized changes by unfriendly applications.
 Off
Ransomware data recovery
You may be able to recover files in these accounts in case of a ransomware attack.
OneDrive - Personal
Free account with individual file recovery.
[View files](#)