How to Add Antivirus Exclusions to your Antivirus Software

Joseph - 2022-06-14 - AV Exceptions

Antivirus protection software may sometimes interfere with the processes our VPN application requires to run correctly. To resolve this, please add the following exceptions below to your antivirus program:

Please be aware that these steps may not line up with your specific version of antivirus software; if this is the case, you may need to search online for steps that are a better match to your version.

File Exclusions:
Windows:

- C:\Program Files\Private Internet Access

- C:\Program Files\Private Internet Access\tap\win10

- C:\Program Files\Private Internet Access\tap\win7

- C:\Program Files\Private Internet Access\pia-client.exe

- C:\Program Files\Private Internet Access\pia-openvpn.exe

- C:\Program Files\Private Internet Access\pia-service.exe

- C:\Program Files\Private Internet Access\pia-support-tool.exe

- C:\Program Files\Private Internet Access\pia-wgservice.exe

- C:\Program Files\Private Internet Access\pia-unbound.exe

Mac:

- /Applications/Private Internet Access/

- /Applications/Private Internet Access.app/Contents/MacOS/pia-wireguard-go

- /Applications/Private Internet Access.app/Contents/MacOS/pia-unbound

Linux:

- /opt/piavpn

- /opt/piavpn/bin/pia-wireguard-go

- /opt/piavpn/bin/pia-unbound

AVAST:

1. Open Avast Antivirus user interface and go to Menu > Settings

2. Ensure the General tab is selected, then select Exceptions

3. Click The Add Exception button

4. Add an exception in one of the following ways:

    1. Type the file path, folder path or URL into the Text box and then click Add Exception.

        1. On Windows: C:\Program Files\Private Internet Access

        2. On macOS: /Applications/Private Internet Access.app

        3. On Linux: /opt/piavpn

    2. Click Browse, select the box next to the file or folder you want to add to the exceptions list and then select OK

AVG:

1. Open AVG Internet Security user interface and go to Menu > Settings

2. Ensure the General tab is selected, then click Exceptions

3. Click the Add Exception button

4. Add an exception in one of the following ways:

    1. Type the file path, folder path or URL into the Text box and then click Add Exception.

        1. On Windows: C:\Program Files\Private Internet Access

        2. On macOS: /Applications/Private Internet Access.app

        3. On Linux: /opt/piavpn

    2. Click Browse, select the box next to the file or folder you want to add to the exceptions list and then select OK

BitDefender:

1. Open the Bitdefender user interface, and go to the Protection window

2. In the ANTIVIRUS section select Settings

3. Select on the Exclusions tab

4. Select List of files and folders excluded from scanning menu

5. Select Add

6. Select Browse and select the folder that you want to be excluded from scanning:

    1. Exclude the PIA files and application from both On-demand scanning and On-access scanning

        1. On Windows: C:\Program Files\Private Internet Access

        2. On macOS: /Applications/Private Internet Access.app

        3. On Linux: /opt/piavpn

7. Select Add to save the changes you have made

Comodo Firewall:

1. Open Comodo user interface, and go to Security Settings

2. Select Antivirus and then select the Exclusions tab

3. The Exception panel has two tabs:

    1. Excluded Paths- This will display a list of paths/ folders/ files on your computer which are excluded from both Real-time and on-demand antivirus scans

    2. Excluded Applications - This will display a list of applications which are excluded from real-time antivirus scans. Items can be excluded by clicking 'Ignore' in the virus Scan Results.

4. To exclude a drive partition, folder, sub-folder or a file from both the real-time and on-demand scheduled times will need to be done by adding them to the Excluded Paths tab.

5. Click the handle from the bottom center and click on 'Add' from the options.

6. Choose 'Files' from the 'Add' drop-down.

7. Add files or locations to exclude by entering or browsing for the file path.

8. Select OK

ESET:

1. Open ESET user interface and go to Advanced setup.

2. Select Detection engine.

3. Then Exclusions

4. Click Files and folders to be excluded from scanning

5. Lastly, click Add if adding new exceptions, Edit if you need to change a path, or Delete to remove an exception.

McAfee:

1. Open your McAfee security software.

2. Click PC Security (on Windows) or Mac Security (on macOS).

3. Click Real-Time Scanning.

4. Click Excluded Files.

5. Click Add file.

6. Browse to, and select, the file that you want to exclude from scans.

7. Repeat the process as needed to exclude multiple files from being scanned.

The Real-Time Scanner does not scan your chosen files after you complete these steps

Norton:

1. Open the Norton user interface, and go Settings

2. Click on the "Antivirus and SONAR Exclusions"

3. Select the "Configure" link next to "Items to Exclude from scans".

4. Select Add

5. Select Browse and select the folder or file that you want to exclude from scans and click OK twice

6. Click Apply and then OK to apply and save the new settings

7. Reselect the Configure link next to "Items to Exclude from Auto-Protect, SONAR and Download Intelligence Detection."

8. Use the same method to add a file or folder to the Auto-protect, SONAR and Download Intelligence Detection Exclusions list

9. Click OK to return to the main window.

Webroot:

1. Open the Webroot user interface and click the gear icon next to PC Security.

2. Select Block/Allow Files

3. Click Add File or drag and drop files

4. Once the files are added, select Allow

ZoneAlarm:

1. Launch the Zone alarm Firewall user interface, Right click the ZoneAlarm icon and select "Show ZoneAlarm Control Center"

2. Select the "Program Control" from the main navigation bar on the left side of the window

3. Select Add

4. Browse the list starting from "My Computer" to the following folder:

    1. On Windows: C:\Program Files\Private Internet Access

    2. On macOS: /Applications/Private Internet Access.app

    3. On Linux: /opt/piavpn

5. Select the Private Internet Access folder and press "Open".

6. On the Program Control Screen click each question mark the Private Internet Access rows and select the green checkmark that says Allow

Once you've added the above exclusions to your antivirus software, be sure to Click "OK" to save. Then a, reboot and reinstallation are required to establish these security changes. Please see our guides section for instructions on how to reinstall the VPN software here.