Antivirus Exclusions

32 TDO KB August 21, 2025 Setup, Troubleshooting 96.30K

Overview

Below lists tested Anti-virus programs that will work with TDO as long as they are configured correctly with listed exclusions. TDO should run fine with most other anti-virus programs as long as they allow settings for exclusions. Only a few anti-virus programs are not recommended as listed below.

****TDO does not provide technical support specific to the antivirus programs. If you are having technical issues with your antivirus, please contact your IT/Vendor for support. ****

Tested and Working with TDO Anti-virus Solutions with exclusions set:

- CYLANCE Antivirus - Scroll to the bottom of the page and enter your info.
- ESET Antivirus
- Microsoft Windows Defender/Security Essentials (Free) (NOTE: exclusions may need to be set in group policy to exclude blocking child processes. https://kb.tdo4endo.com/article.php?id=960)
- AVG Free (Free)
- Managed Antivirus (Exclusions need to be set on all workstations)

Tested and NOT Working with TDO Anti-Virus Solutions:

- Symantec Endpoint
- Norton Products (360, 2013, Anti-virus)
- Avast
- Trend Micro (Even with Antivirus exclusions created, Trend Micro can cause Main Timer errors while using the program)
- Cybereason (Even with Antivirus exclusions created, Cybereason can cause the usernames and device configuration options in TDO not to show. Can cause the TDO auto fix not to work)

Anti-virus with known issues without proper exclusions:

- Threatlocker: As of 8/20/25 TDO has noticed Threatlocker causing issues with TDO Cloud service. We recommend ensuring all Typical TDO Exclusions are set in Threatlocker.

Typical TDO Exclusions:

Server Exclusions:

- C:\Program Files (x86)\TDOffice
- TDO folder in data share for TDO (Including TDOfficeData and TDOBuilds folder)

Path Exclusions: 32bit Workstations:

- C:\Program Files\TDOffice
- C:\Program Files\Microsoft Access Runtime
- C:\Program Files\Microsoft Office
- TDO Netdrive Share (S:\TDOfficedata)

If using RVG Kodak Integration:

- C:\TW
- C:\Program Files\Common Files\Trophy
- C:\Program Data\TW
- C:\Program Files\Carestream

64bit Workstations

- C:\Program Files (x86)\TDOffice
- C:\Program Files (x86)\Microsoft Access Runtime
- C:\Program Files (x86)\Microsoft Office
- TDO Netdrive Share (S:\TDOfficedata)

If using RVG Kodak Integration:

- C:\TW
- C:\Program Files (x86)\Common Files\Trophy
- C:\Program Data\TW
- C:\Program files (x86)\Carestream

Workstation Firewall ports:

- Port exclusions: UDP/TCP - 4150

Server Ports:

- UDP/TCP 4150 for all traffic in Windows Firewall for all "firewall profiles"
- Exclusions for SqlServr.exe and SQLBrowser.exe for all "firewall profiles" (to find the path to these files, find the processes in Task Manager, right-click, open file location)
- Servers with GentleWave machines, add Port: TCP/UDP - 8739

If using Sophos:

- Exploit Mitigation must be turned off. After turning this setting off, the workstation does require a reboot. This setting protects the computer from malicious code that may be embedded in office documents, however it can cause TDO to not launch properly when turned on. When this is off, please be careful opening office documents from unknown or untrusted sources.

Software Firewalls:

TDO Requires that the following ports be open in all software firewalls (i.e. Windows Firewall) for inbound and outbound traffic.

TCP/UDP 4150

Online URL: https://kb.tdo4endo.com/article.php?id=32