Teramind Antivirus & EDR Configuration Guide

Ver 5.5 (24 July 2026)

TERAMIND

Table of Contents

Overview **2**

Essential Exclusions **2**

Must Add for Both Cloud and On-Premises Deployments: 2

Add This If You Are Using the Revealed/Visible Agent: 2

Termporary Exclusions **2**

Add for Both Cloud and On-Premises Deployments: 2

Add for On-Premises Deployments Only: 3

Checking Server IP Addresses and Ports **3**

Avast Business Antivirus **4**

File Shield Exceptions 4

Behavior Shield Exceptions 5

If Agent Binaries Were Already Quarantined 6

Additional Recommendations 6

BitDefender Total Security **7**

CrowdStrike Endpoint Security/Falcon **11**

ESET Endpoint Security **13**

ESET Cloud Protect **15**

ESET LiveGuard **16**

Kaspersky Endpoint Security **17**

McAfee Endpoint Security **21**

Sophos Endpoint Protection **24**

Sophos Home **26**

Windows Defender **27**

Solving Issues with Older Virus Definitions 28

Restoring a Quarantined Agent 30

Instructions for Other Antivirus Software **31**

macOS Exclusions **32**

Other Endpoint Detection and Response (EDR) Solutions **33**

Overview

Generally, your antivirus/EDR program will recognize Teramind software without issues. However, if your antivirus blocks the Teramind Agent installation or updates, this guide helps you fix that.

If you still encounter any issues after following this guide, please contact us at support@termind.co and a support engineer will help you troubleshoot the problem.

Essential Exclusions

Must Add for Both Cloud and On-Premises Deployments:

- `c:\programdata\{4cec2908-5ce4-48f0-a717-8fc833d8017a}`
- `c:\windows\system32\drivers\tmfsdrv2.sys`
- `c:\windows\system32\drivers\tm_filter.sys`

For some AV software, you might need to add this:

- `c:\windows\SystemTemp\tmtemp\*\*\bundle.exe`

Add This If You Are Using the Revealed/Visible Agent:

- `c:\ProgramData\Teramind Agent`

> If your security solution uses SSL inspection, DNS filtering, or proxy-based traffic controls (e.g., Zscaler, Cisco Umbrella, etc.), you need to exclude Teramind domains and traffic. Failing to do so could lead to connection issues or prevent certain features from working properly.

Termporary Exclusions

Add for Both Cloud and On-Premises Deployments:

- `c:\windows\system32\drivers\set*.tmp`
- `c:\windows\temp\*.tmp`
- `c:\windows\installer\*.*`
- `c:\windows\SystemTemp\tmtemp\**\*.*`
  Or
- `c:\windows\SystemTemp\tmtemp`
  (with subfolders)

> You can usually remove these after installing the Agent. However, for Cloud setups with automatic updates, it's best to keep these exceptions to prevent the antivirus from blocking updates.

Add for On-Premises Deployments Only:

You will need to add the following temporary additional exceptions when installing the Agent remotely (On-Premise) via the Teramind Dashboard:

- `%windir%\*.exe`

Remove these after the Agent installation/update.

If Teramind Agent is already installed, remove it, add the exceptions, and then reinstall it.

- Instructions on how to remove the Agent
- Instruction on how to install the Agent

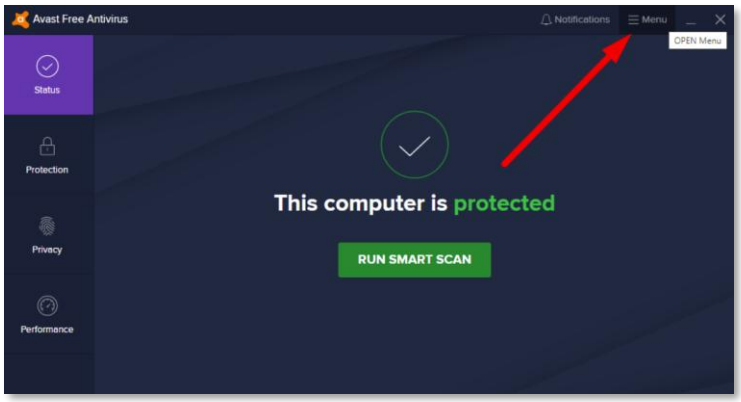
Checking Server IP Addresses and Ports

To make sure Teramind works smoothly, some antivirus/firewall settings need to be checked. Check out this Knowledge Base article to verify the necessary IPs/ports are reachable.

Avast Business Antivirus

Avast Business Antivirus maintains two separate exclusion lists: one for File Shield (file/folder scanning) and one for Behavior Shield (runtime behavioral/HIPS detection). Both must be configured.

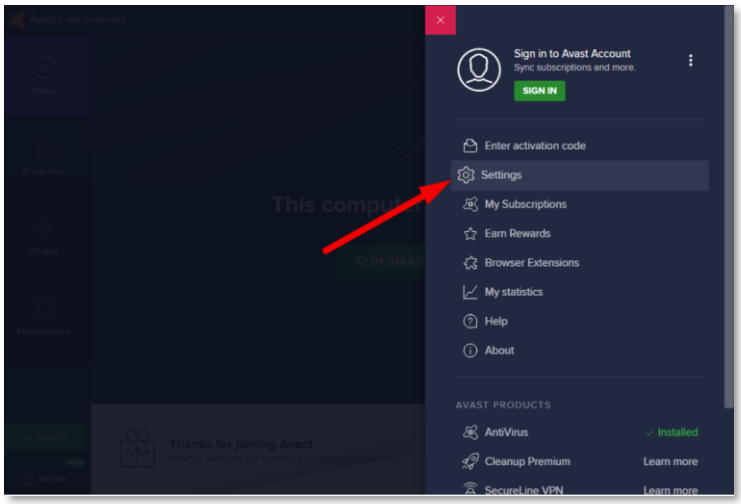
File Shield Exceptions



Step 1:

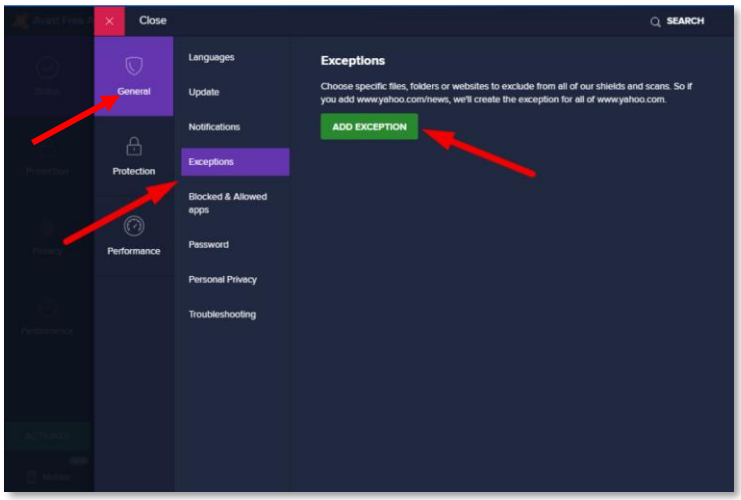
Open *Avast Business Antivirus*.

Click the **Menu** at the top right.



Step 2:

Select **Settings.**

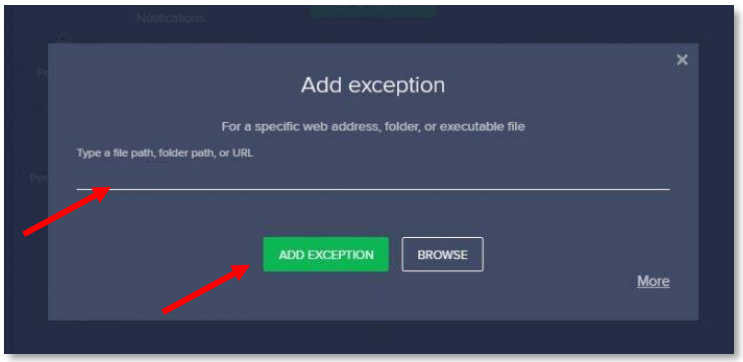


Step 3:

Select the **General** tab.

Select **Exceptions**.

Click the **ADD EXCEPTION** button.



Step 4:

Enter the following file and folder paths one at a time, and click **Add Exception**:

- `c:\programdata\{4cec2908-5ce4-48f0-a717-8fc833d8017a}\`
- `c:\windows\system32\drivers\tmfsdrv2.sys`
- `c:\windows\system32\drivers\tm_filter.sys`

Repeat *Step 3-4* until all the exceptions are added.

Behavior Shield Exceptions

Behavior Shield performs runtime behavioral analysis independently of File Shield. It can flag the Agent's user-session process (`dwm.exe`) under the *IDP.Generic* heuristic because of the Agent's legitimate monitoring activity (screen capture, keystroke interception, process injection).

If the Agent directory is not also excluded in Behavior Shield, Avast may quarantine these binaries as *IDP.Generic*. This creates a silent failure: the core Agent service (`tsvchst`) keeps running and pinging the server normally, so the device still shows as online in the dashboard, while user-session monitoring is silently disabled. The only visible symptom is a stale "last activity" date, easily mistaken for a machine that's been turned off.

Configure the following exclusions to prevent this:

> **Note:** Exact menu paths may vary slightly between Avast Business Hub (cloud-managed) and a locally installed Avast Business Antivirus client.

Step 1: Open **Avast Business Hub** (cloud-managed) or the local **Avast Business Antivirus** client.

Step 2: Navigate to **Protection > Behavior Shield > Settings** (or **Exceptions**).

Step 3: Add the full Agent installation directory as an exclusion:

- `c:\programdata\{4cec2908-5ce4-48f0-a717-8fc833d8017a}\`

Step 4: If the interface supports process-level exclusions, also add the following executables:

- `dwm.exe`
- `mtm.exe`
- `mtm64.exe`
- `svc.exe`
- `nsxpsrenderer.exe`

Step 5: Apply and save. If the deployment is centrally managed, push the exclusions via **Avast Business Hub** policy rather than configuring each endpoint individually.

> **Note:** Exact menu paths may vary slightly between Avast Business Hub (cloud-managed) and a locally installed Avast Business Antivirus client.

If Agent Binaries Were Already Quarantined

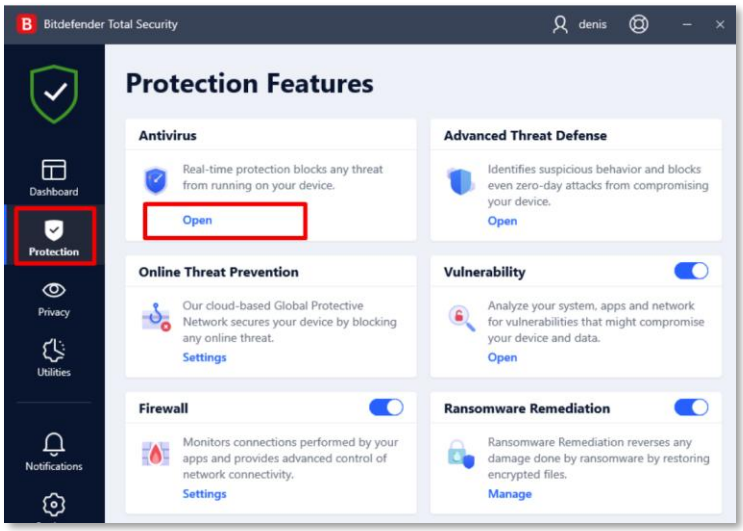
If the endpoint is showing the symptoms above (stale last activity, no user sessions, Agent stuck on an old version), check whether Avast has already quarantined Agent files:

- Open the **Avast client** > **Protection** > **Virus Chest** (or **Avast Business Hub** > **Reports** > **Threats**) and look for `IDP.Generic` detections against `dwm.exe` and/or `rundll32.exe` under the Agent's `\updates\` directory.
- If `dwm.exe` was quarantined, restoring the file from quarantine alone will not reliably restore the Agent to a functional state - a full Agent reinstall is required.
- Add both the File Shield and Behavior Shield exclusions above first, then reinstall using the latest Agent MSI:
  ```
  msiexec /i "teramind_agent.msi" TMUPDATE=1 /qn
  ```
- If the updater binary was also quarantined, the Agent may be stranded on an old version even with auto-update enabled - reinstalling with the exclusions in place prevents this from recurring.
- After reinstalling, confirm all three services are running by using the following commands:
  ```
  sc query tsvchst
  sc query tmfsdrv2
  sc query tm_filter
  ```
  Then confirm the device shows active user sessions in the dashboard.

Additional Recommendations

- **Use publisher-based *allow rules* where possible.** As of March 26, 2026, all Agent binaries are signed with a DigiCert certificate under the publisher name Teramind. Where your Avast policy supports it, create *allow rules* by publisher name rather than by file path or certificate hash - this avoids recurrence when certificates rotate or Agent versions change.
- **Deploy exclusions fleet-wide via Avast Business Hub.** For multi-endpoint environments, push both File Shield and Behavior Shield exclusions as a centrally managed policy rather than relying on per-endpoint configuration.
- **AVG Business is similarly affected.** AVG Business uses the same scanning engine and behavioral detection framework as Avast Business. Apply the same Behavior Shield exclusion steps described above.

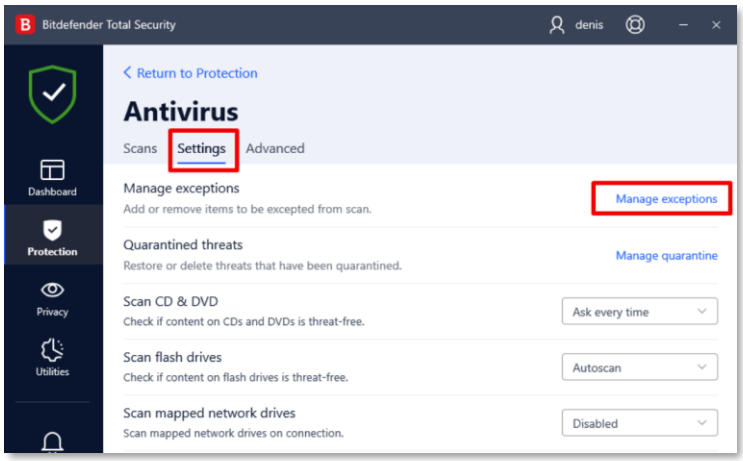
BitDefender Total Security



Step 1:

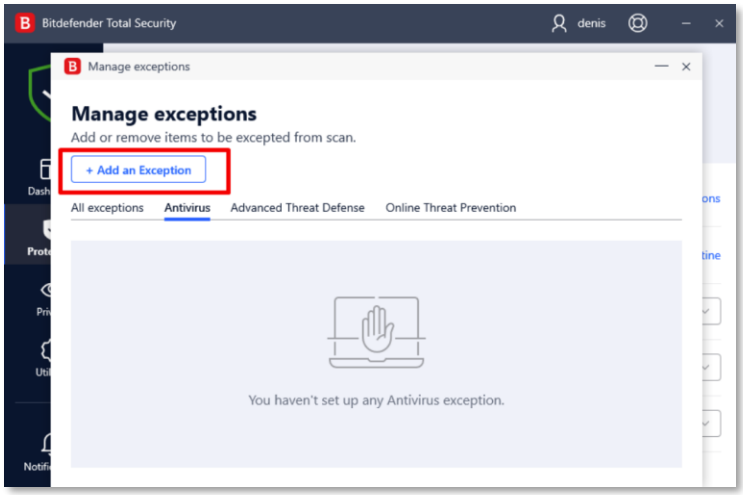
Open *BitDefender Total Security*.

Go to the **Protection** tab and click **Open** under the *Antivirus* tile.



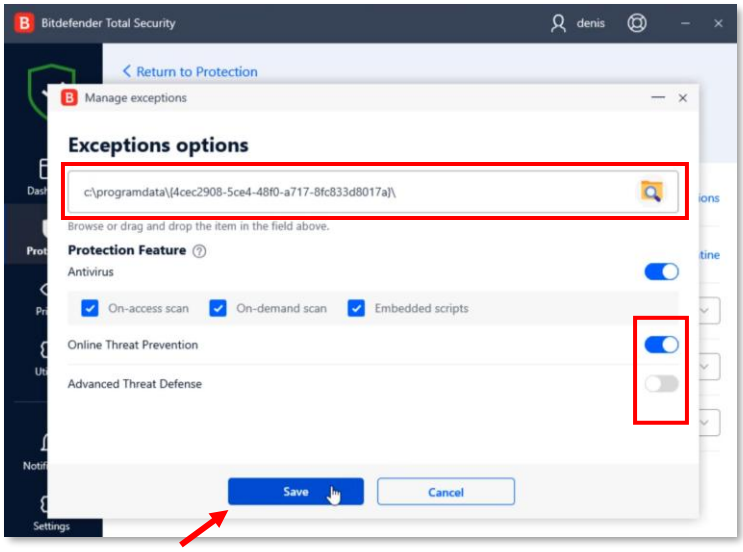
Step 2:

Click the **Settings** tab, then **Manage exceptions**.



Step 3:

In the *Manage exceptions* window, click **+ Add an Exception**.



Step 4:

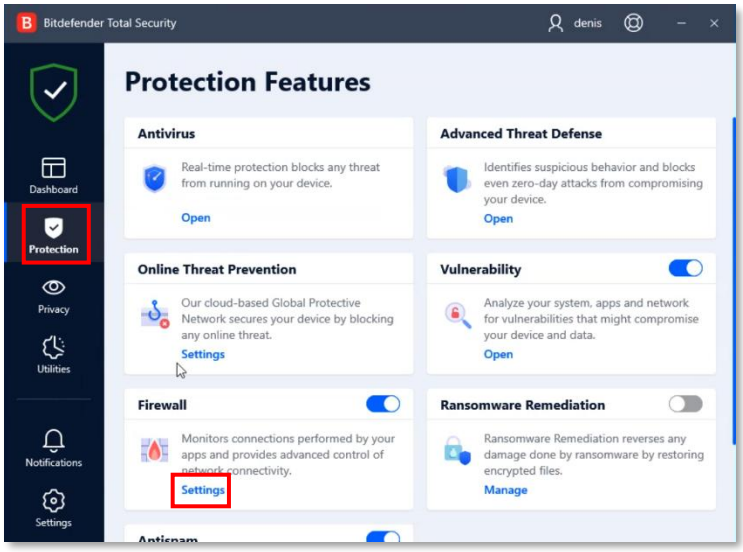
Enter each of the following paths and ensure **Antivirus** and **Online Threat Prevention** are turned on, then click **Save**:

- `c:\programdata\{4cec2908-5ce4-48f0-a717-8fc833d8017a}\`
- `c:\windows\system32\drivers\tmfsdrv2.sys`
- `c:\windows\system32\drivers\tm_filter.sys`

Repeat *Step 3-4* until all the exceptions are added.

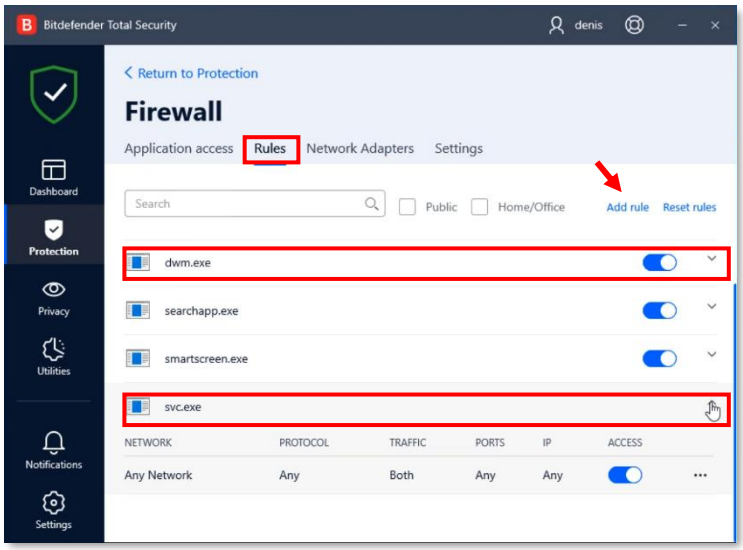
Close the *Manage exceptions* window.

The above exceptins should be enough for the Teramind Revealed Agent to work properly. However, if you have a Stealth Agent installed, please follow the additional steps below.



Step 5 (Stealth Agent Only)

Go back to the **Protection** tab and click **Settings** under the *Firewall* tile.

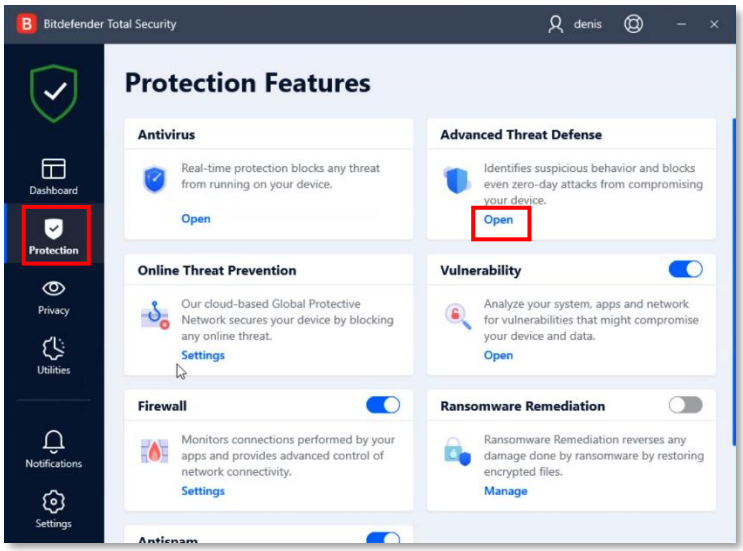


Step 6:

Click the **Rules** tab.

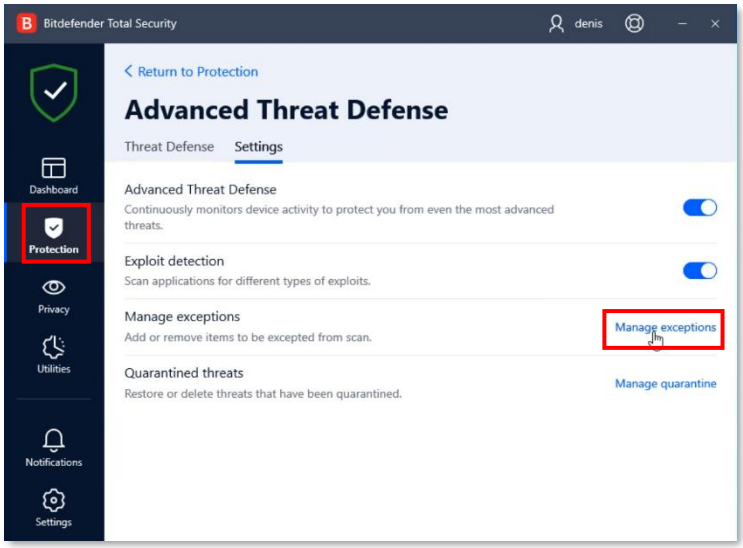
Make sure the **ACCESS** option for `dwm.exe` and `svc.exe` rules are enabled for *Any Network* (you can click a rule to expand/collapse it).

If not present, click the **Add rule** link to add them.



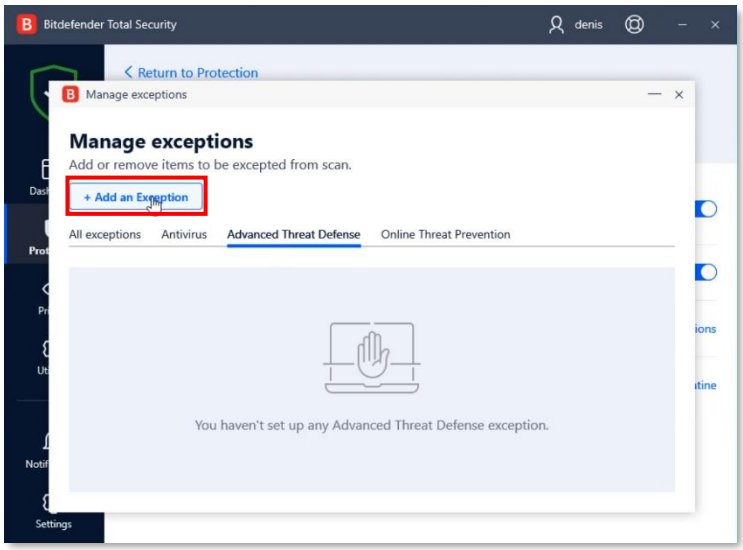
Step 7:

Go back to the **Protection** tab and click **Open** under the *Advanced Threat Defense* tile.



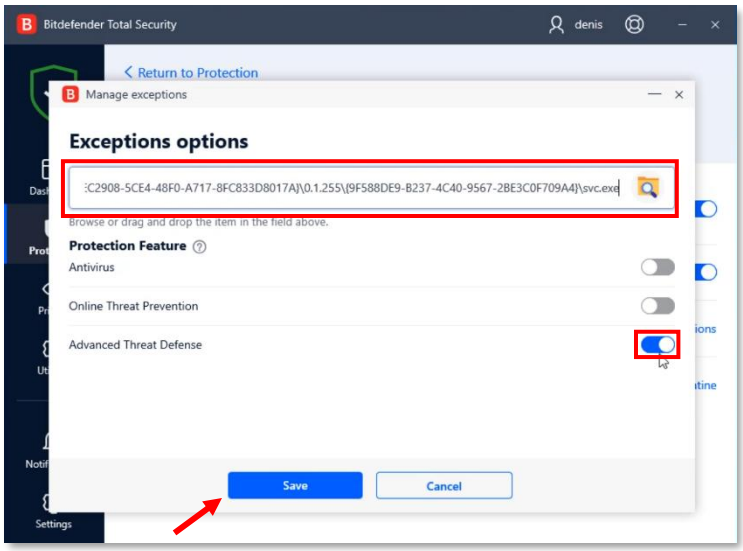
Step 8:

Click the **Settings** tab and then **Manage exceptions**.



Step 9:

In the *Manage exceptions* window, click the + **Add an Exception** button.



Step 10:

Enter the first exception from the list below:

- `c:\programdata\{4cec2908-5ce4-48f0-a717-8fc833d8017a}\<agent ver>\{04287722-eb08-4929-bef0-cc1a76cbff1b}\svc.exe`
- `c:\programdata\{4cec2908-5ce4-48f0-a717-8fc833d8017a}\<agent ver>\{04287722-eb08-4929-bef0-cc1a76cbff1b}\dwm.exe`

*Replace **<agent ver>** with your own Agent version. For example, **0.1.255**. You can check for the Agent version from your Teramind Dashboard. Select the COMPUTERS menu then click a computer's name.*

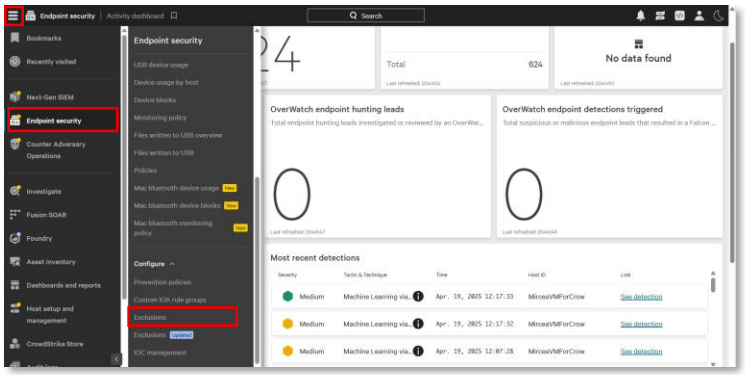
Make sure **Advanced Threat Defense** (and all its sub options) is turned on.

Click the **Save** button.

Repeat *Step 9-10* until all the exceptions are added.

CrowdStrike Endpoint Security/Falcon

For CrowdStrike Falcon EDR, you will need to add two exclusions. Follow the steps below to add them.

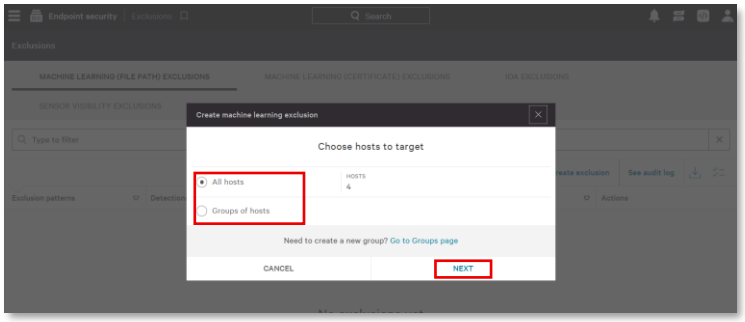


Step 1:

Log into your *Flacon Endpoint Security* console (for example: `https://falcon.crowdstrike.com/`).

Open the main menu by clicking the **Hamburger** icon at the top-left corner.

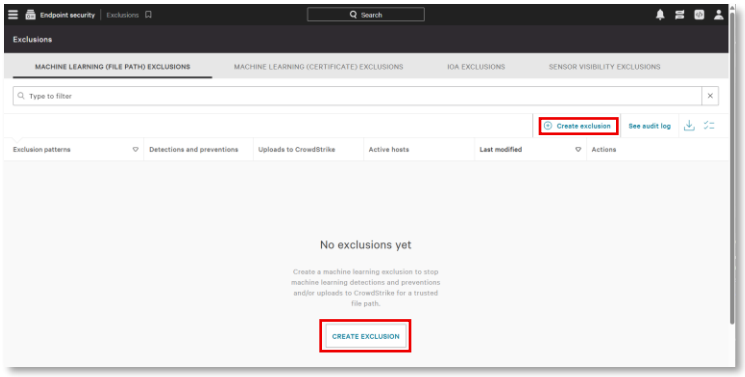
Select **Endpoint security** > **Exclusions**.



Step 2:

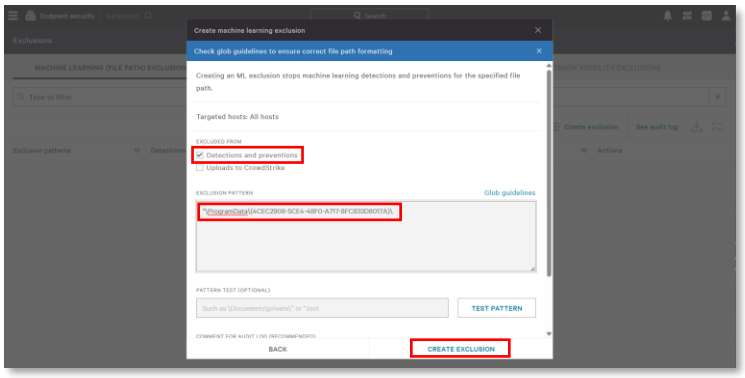
Choose an option for the hosts. You can either select **All hosts** or **Group of hosts**.

Click the **NEXT** button.



Step 3:

In the *Exclusions* screen, click any of the **Create exclusion** buttons.



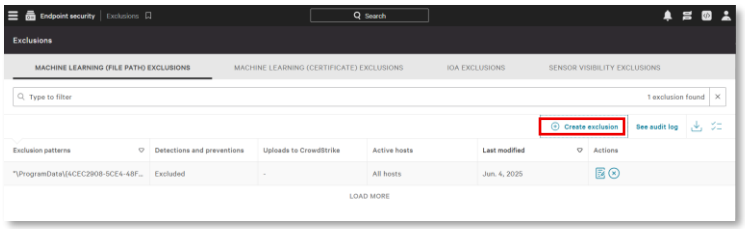
Step 4:

Under *EXCLUDED FROM*, turn on the **Detections and preventions** option.

In the **EXCLUSION PATTERN** field, enter the following exclusion:

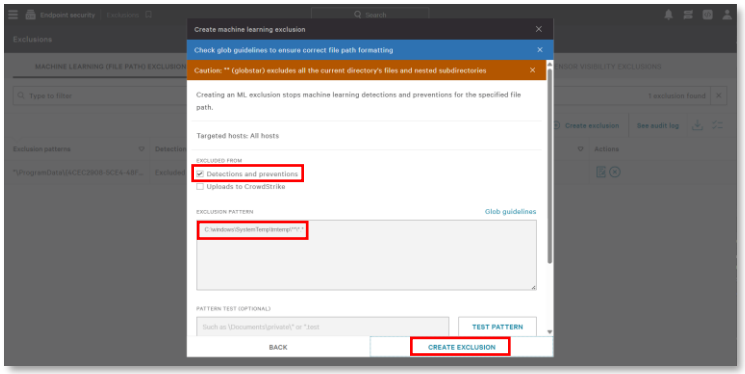
```
*\ProgramData\{4CEC2908-5CE4-48F0-A717-8FC833D8017A}\
```

Then, click the **CREATE EXCLUSION** button. The exclusion will be added and you will be taken back to the *Exclusion* screen.



Step 5:

In the *Exclusions* screen, click the **Create exclusion** button again.



Step 6:

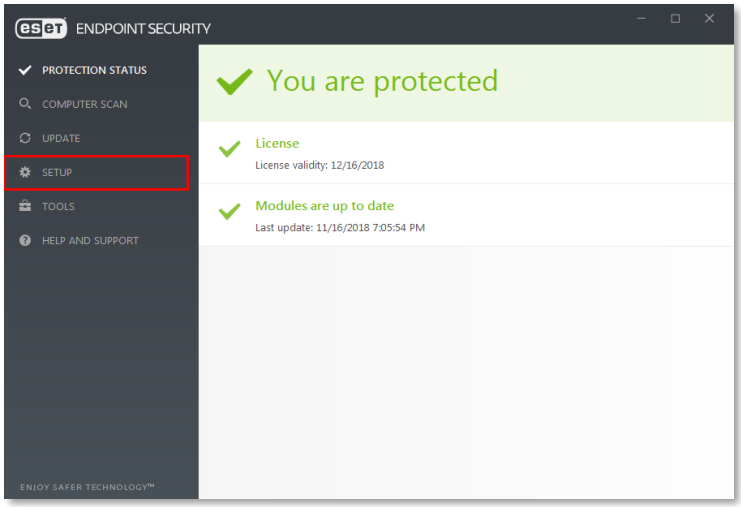
Under *EXCLUDED FROM*, turn on the **Detections and preventions** option.

In the **EXCLUSION PATTERN** field, enter the following exclusion:

```
c:\windows\SystemTemp\tmtemp\**\*.*
```

Then, click the **CREATE EXCLUSION** button.

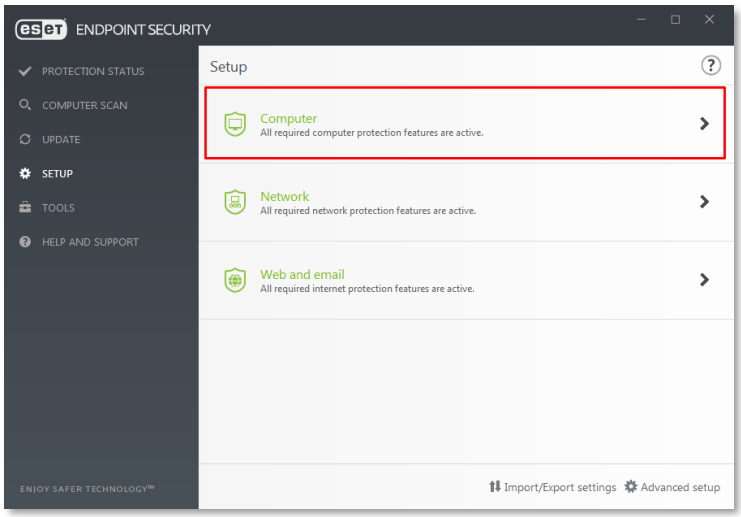
ESET Endpoint Security



Step 1:

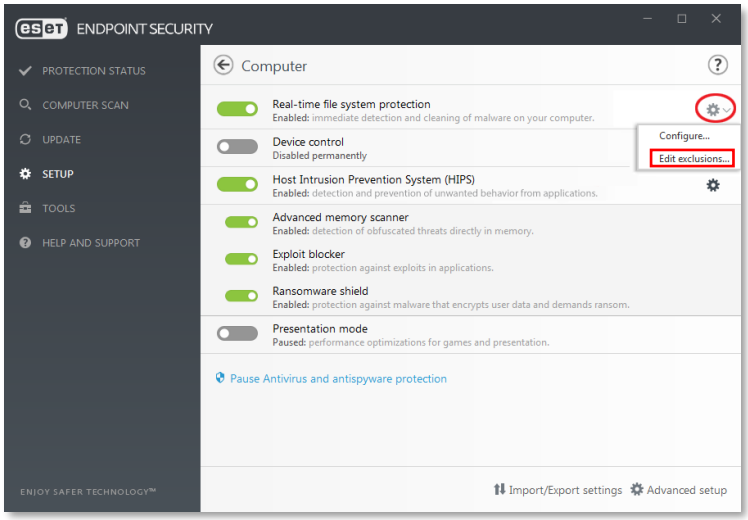
Open *ESET Endpoint Security*.

From the ESET Endpoint Security's main window, select the **SETUP** menu to go the *Setup* screen.



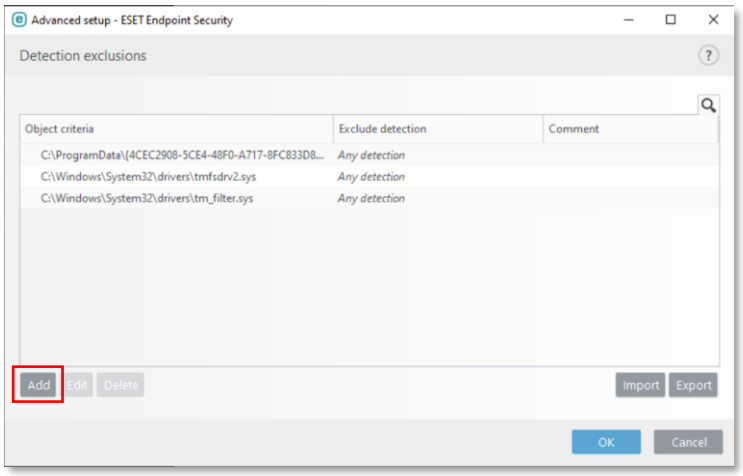
Step 2:

Select **Computer** from the *Setup* screen.



Step 3:

Click the **Cog Wheel** ⚙ next to *Real-time file system protection* and select **Edit exclusions…** from the pull-down menu.



Step 4:

Click the **Add** button to add the following paths to the *Detection exclusions* list:

- `c:\programdata\{4cec2908-5ce4-48f0-a717-8fc833d8017a}\`
- `c:\windows\system32\drivers\tmfsdrv2.sys`
- `c:\windows\system32\drivers\tm_filter.sys`
- `c:\documents and settings\All Users\{4CEC2908-5CE4-48F0-A717-8FC833D8017A}\*`
- `c:\Users\All Users\{4CEC2908-5CE4-48F0-A717-8FC833D8017A}\*`
- `c:\documents and settings\All Users\{4CEC2908-5CE4-48F0-A717-8FC833D8017A}\*\*\*.dll`
- `c:\Users\All Users\{4CEC2908-5CE4-48F0-A717-8FC833D8017A}\*\*\*.dll`
- `c:\ProgramData\{4CEC2908-5CE4-48F0-A717-8FC833D8017A}\*\*\*.dll`

Click the **Save** button when done.

ESET Cloud Protect

Setting up Teramind with ESET Cloud Protect is straightforward if you add a few simple exceptions. This will help make sure Teramind and ESET Cloud Protect work together without any conflicts.

Here are the necessary exceptions:

- `c:\programdata\{4cec2908-5ce4-48f0-a717-8fc833d8017a}`
- `c:\windows\system32\drivers\tmfsdrv2.sys`
- `c:\windows\system32\drivers\tm_filter.sys`
- `c:\ProgramData\{4CEC2908-5CE4-48F0-A717-8FC833D8017A}\*\*\*.dll`

For detailed instructions on adding these exceptions, please refer to ESET's own help guide. You can find it here: ESET's documentation.

You will also need to create an exclusion based on the Detection Name. To learn how to create this kind of exclusion, check out this section of the ESET documentation.

ESET LiveGuard

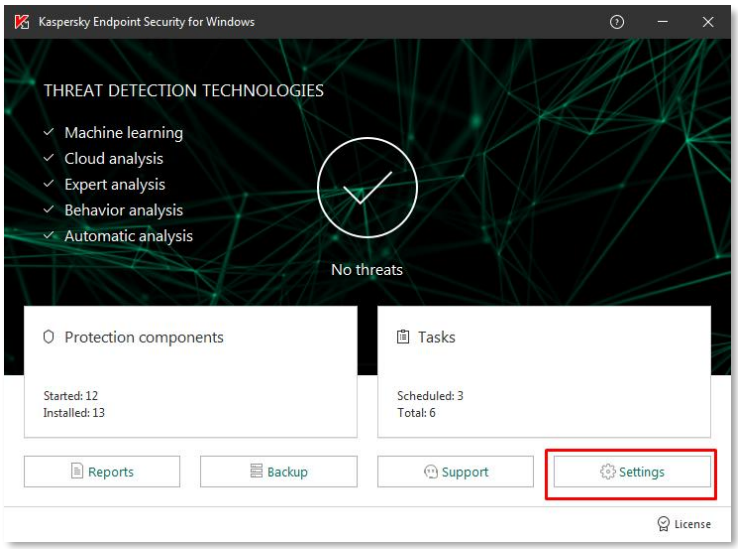
If you're using ESET LiveGuard, you'll want to add these same exceptions to ensure Teramind runs smoothly:

- `c:\programdata\{4cec2908-5ce4-48f0-a717-8fc833d8017a}`
- `c:\windows\system32\drivers\tmfsdrv2.sys`
- `c:\windows\system32\drivers\tm_filter.sys`
- `c:\ProgramData\{4CEC2908-5CE4-48F0-A717-8FC833D8017A}\*\*\*.dll`

For specific instructions on adding exclusions in ESET LiveGuard, please check out ESET's documentation here: ESET's documentation.

Kaspersky Endpoint Security

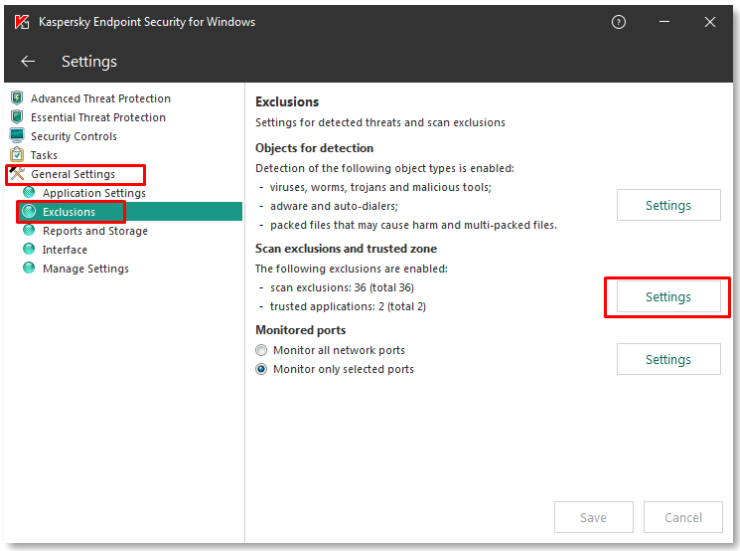
Teramind is already on Kaspersky's approved list, so you probably won't need to make any changes. But, if you run into any problems, here's what you can do:



Step 1:

Open *Kaspersky Endpoint Security*.

Click the **Settings**.



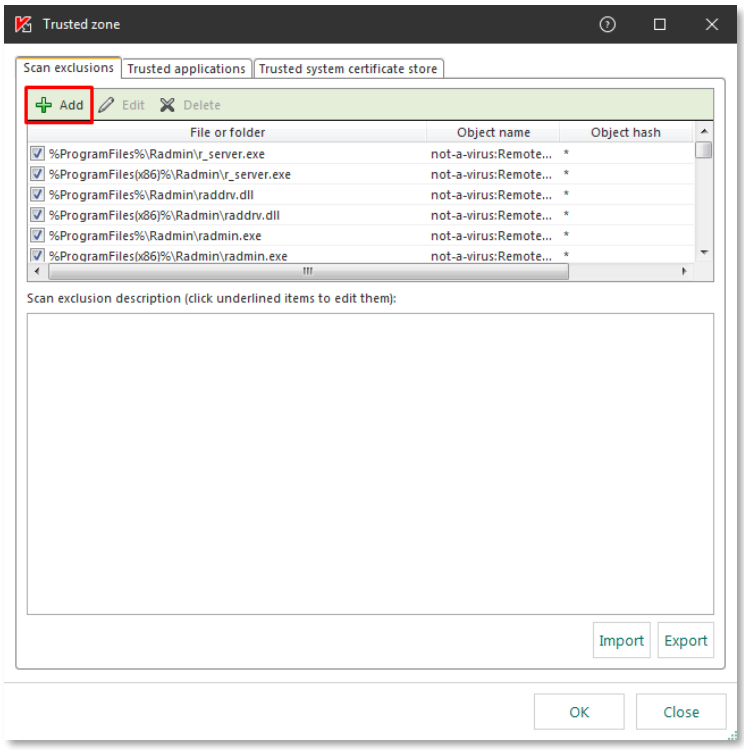
Step 2:

In the *Setting* screen, choose **General Settings** from the list on the left side.

Select **Exclusions** under it.

Click the **Settings** button on the right side of the *Scan exclusions and trusted zone* section.

This will take you to the *Trusted zone* screen.

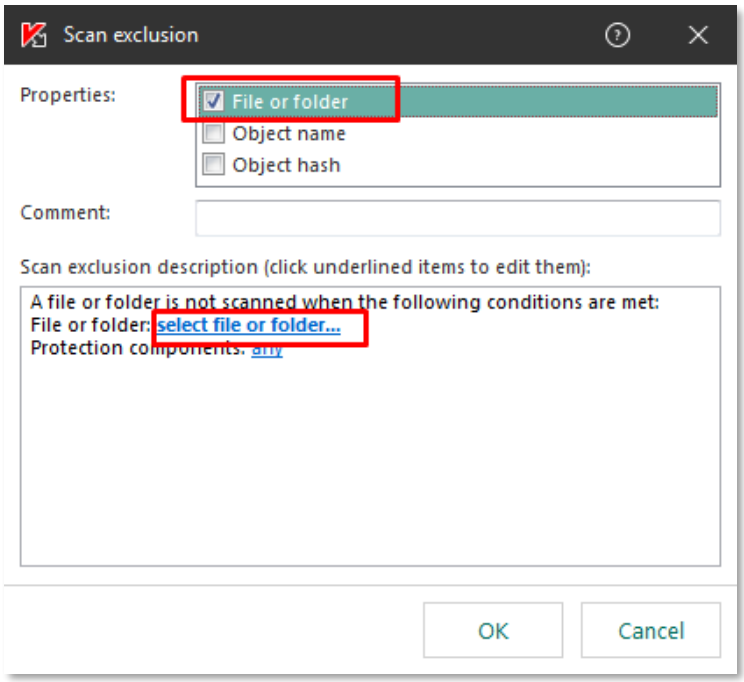


Step 3:

In the *Trusted zone* screen, select the **Scan exclusions** tab.

Click the **Add** button.

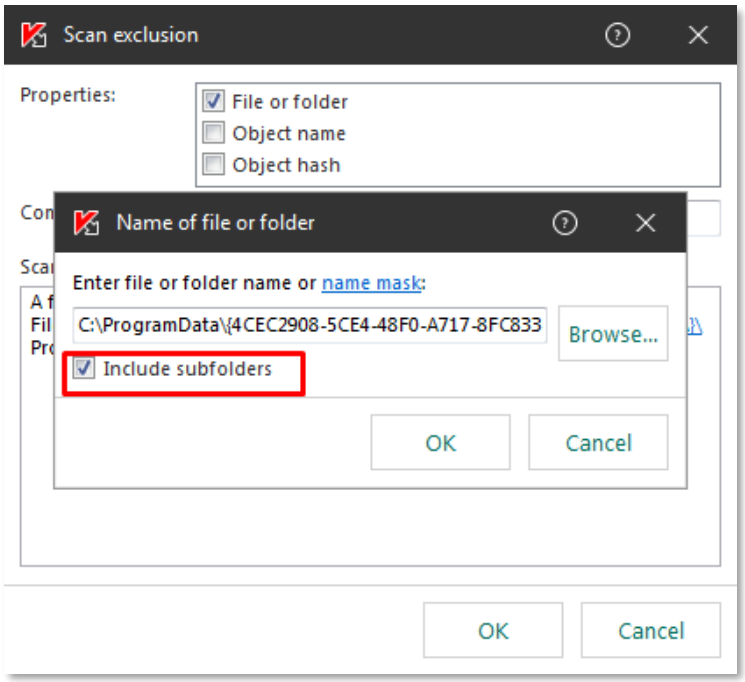
This will open the *Scan exclusion* window.



Step 4:

In the *Scan exclusion* pop-up window, turn on **File or folder** in the *Properties* section.

Under the *Scan exclusion description* section, click the **select file or folder…** link.



Step 5:

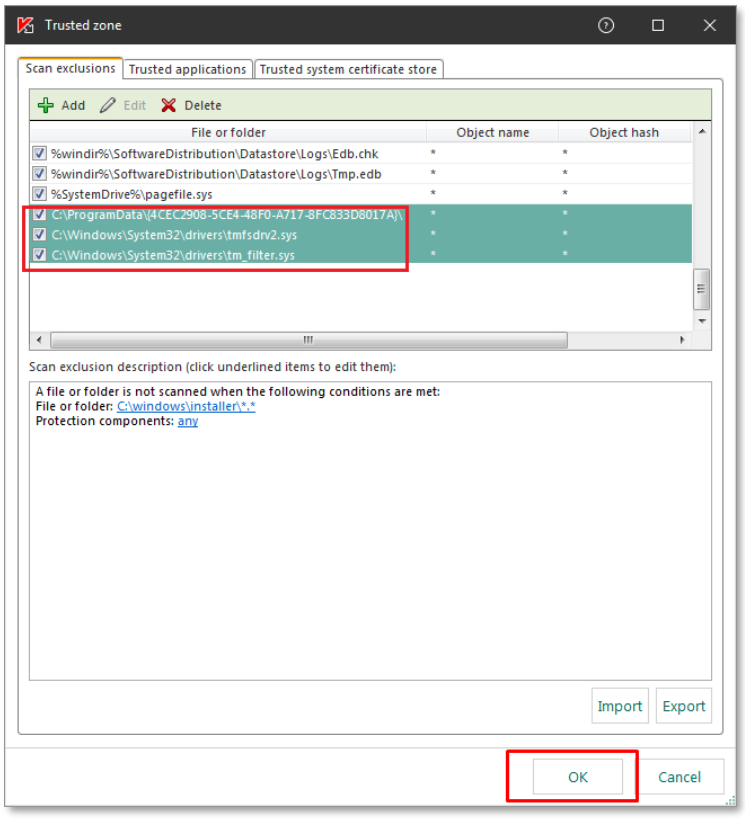
Enter the following exclusion:

- `c:\programdata\{4cec2908-5ce4-48f0-a717-8fc833d8017a}\`

Turn on the **Include subfolders** option.

Click **OK** to add the item.

Click **OK** again to close the *Scan exclusion* window and return to the *Trusted zone* screen.

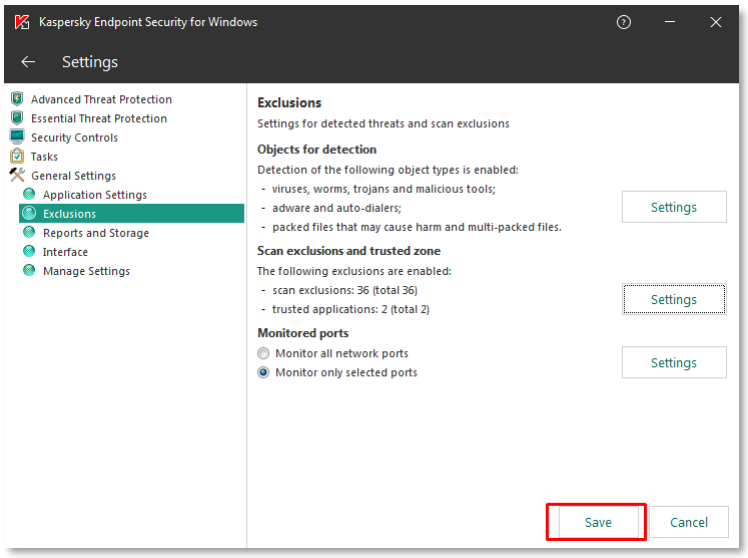


Step 6:

Repeat *Step 3-5* above to add the rest of the exclusions from the list below:

- `c:\programdata\{4cec2908-5ce4-48f0-a717-8fc833d8017a}\`
- `c:\windows\system32\drivers\tmfsdrv2.sys`
- `c:\windows\system32\drivers\tm_filter.sys`

Click **OK** to return to the *Settings* window.

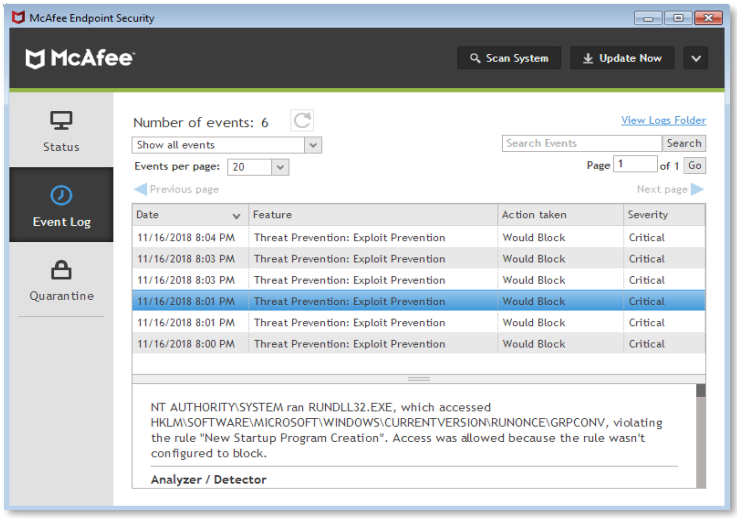


Step 7:

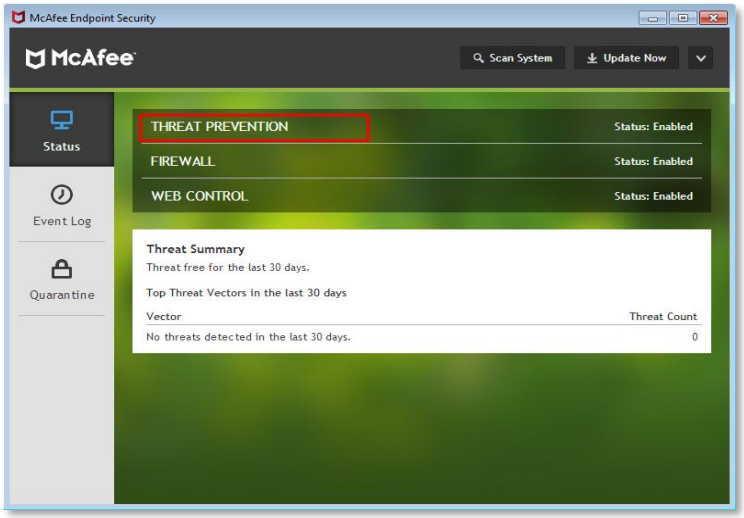
Click the **Save** button to save your changes.

McAfee Endpoint Security

Teramind is on McAfee's approved list, so you usually won't need to make any changes. But, if you still run into any issues, give this a try:



McAfee Endpoint Security usually works well when you install the Teramind Agent. However, when updating the Agent, you might see an event exception. The following instructions will help you fix that issue.



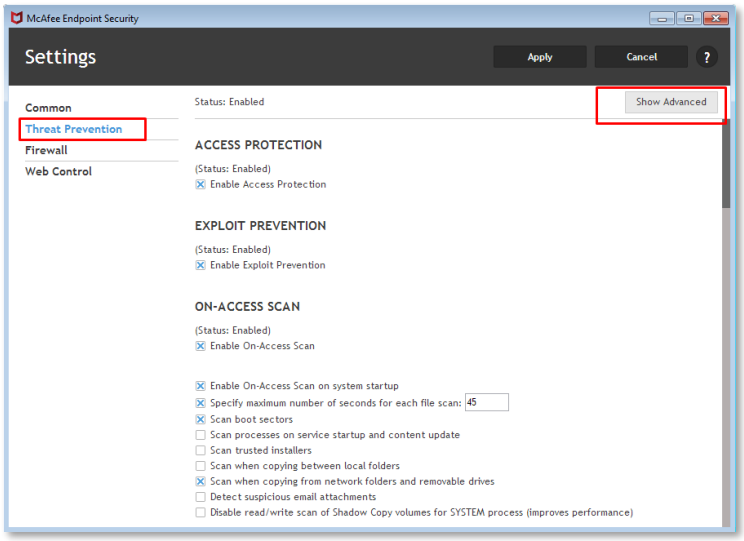
Step 1:

Open *McAfee Endpoint Security*.

From the main window, click the **Status** tab.

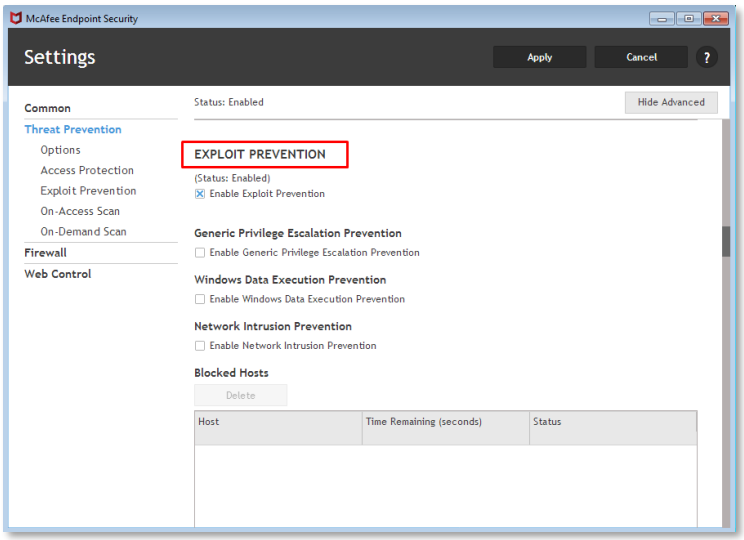
Select the **THREAT PREVENTION** option.

This will take you to the *Settings* panel.



Step 2:

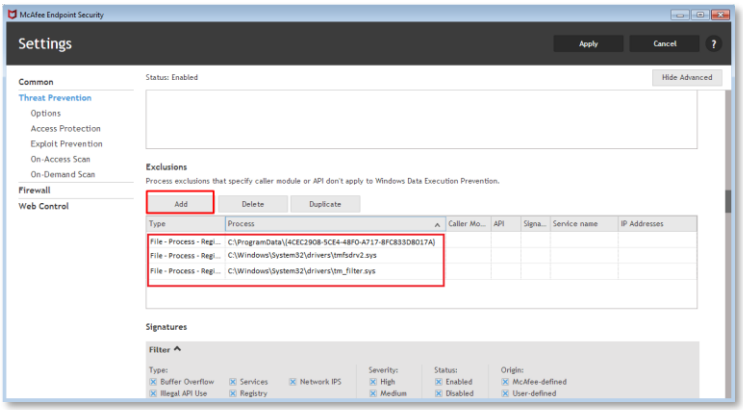
Click the **Show Advanced** button near the top-right corner.



Step 3:

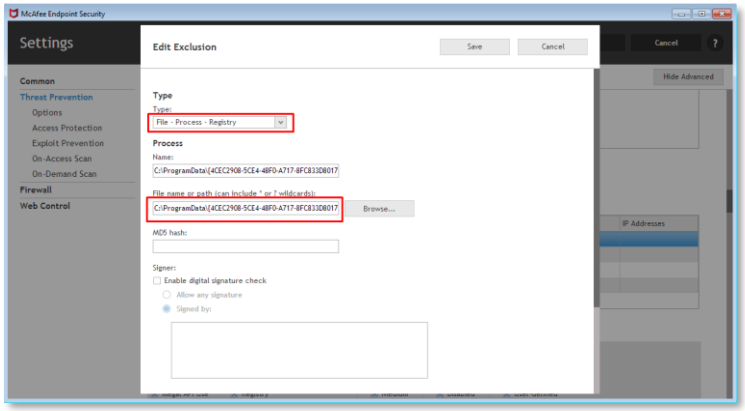
Scroll down until you find the *EXPLOIT PREVENTION* option.

Click the **EXPLOIT PREVENTION** option.



Step 4:

Click the **Add** button under *Exclusions*. The *Edit Exclusion* window will pop-up.



Step 5:

Under *Type*, select **File – Process – Registry**.

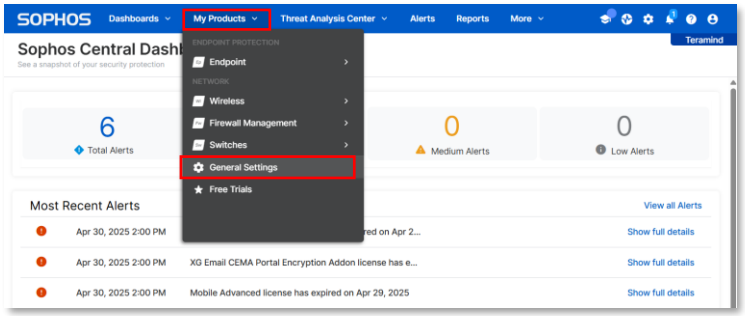
Add the following in the **File name or path**… field:

- `c:\programdata\{4cec2908-5ce4-48f0-a717-8fc833d8017a}\`

Repeat *Step 4-5* to add the rest of the exceptions:

- `c:\windows\system32\drivers\tmfsdrv2.sys`
- `c:\windows\system32\drivers\tm_filter.sys`

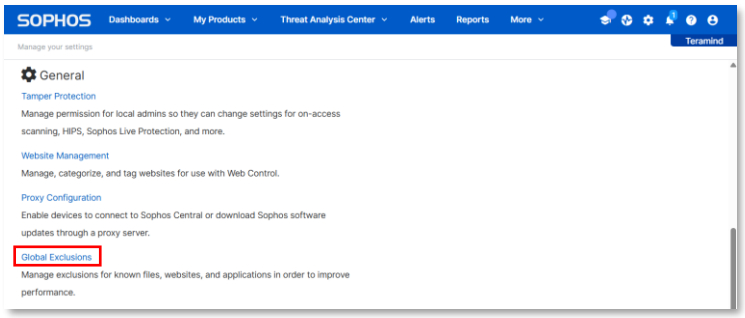
Sophos Endpoint Protection



Step 1:

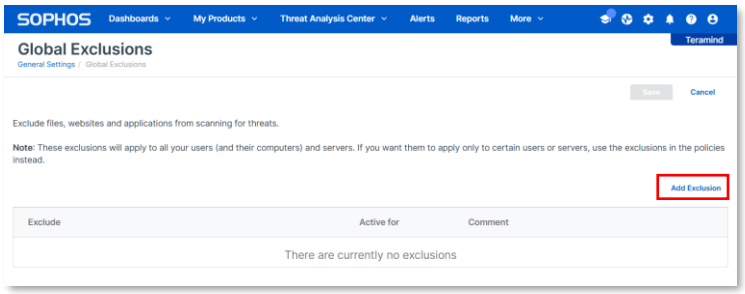
Log into your *Sophos Central* portal (e.g., `https://central.sophos.com/`).

Select **My Products** > **General Settings**.



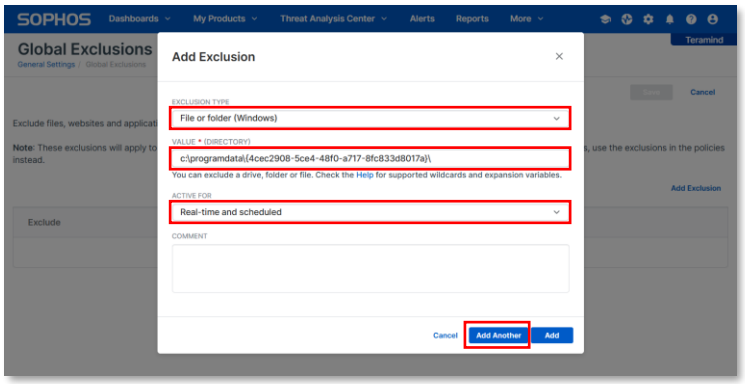
Step 2:

Under the *General* section, click the **Global Exclusions** link.



Step 3:

Click the **Add Exclusion** button in the *Global Exclusions* screen.



Step 4:

In the *Add Exclusion* pop-up window, select **File or folder (Windows)** from the *EXCLUSION TYPE* pull-down menu.

Enter the following exclusion in the **VALUE** field:

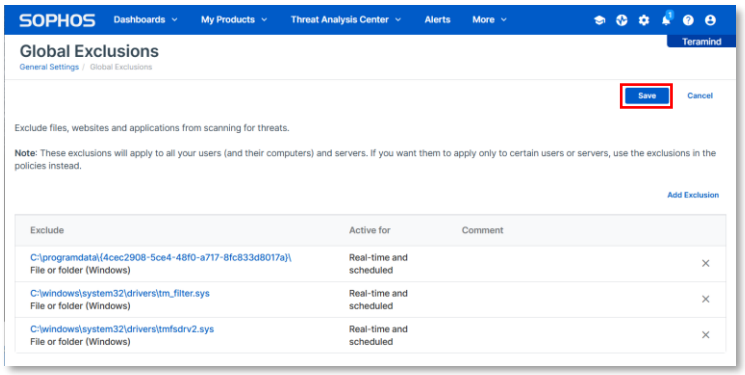
`c:\programdata\{4cec2908-5ce4-48f0-a717-8fc833d8017a}\`

Select **Real-time and scheduled** from the *ACTIVE FOR* pull-down menu.

Click the **Add Another** button and add the following two exclusions one by one:

- `c:\windows\system32\drivers\tmfsdrv2.sys`

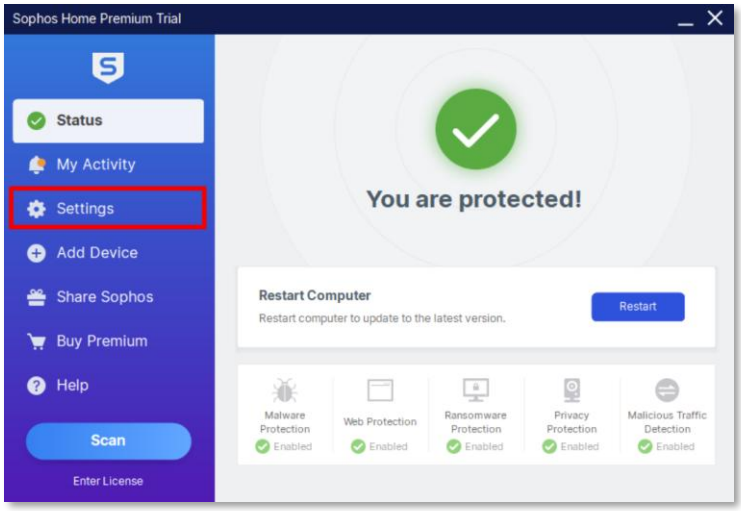
- `c:\windows\system32\drivers\tm_filter.sys`



Step 5:

Click the **Save** button to save the exclusions.

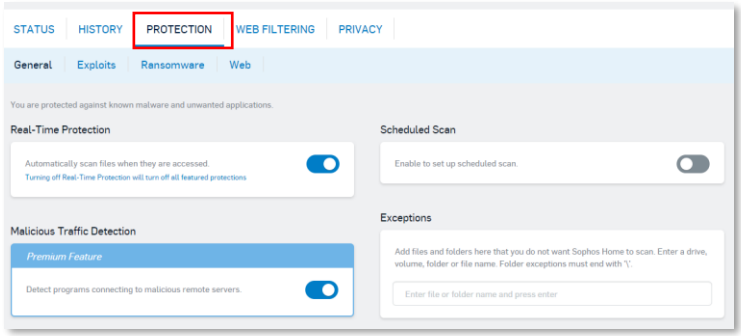
Sophos Home



Step 1:

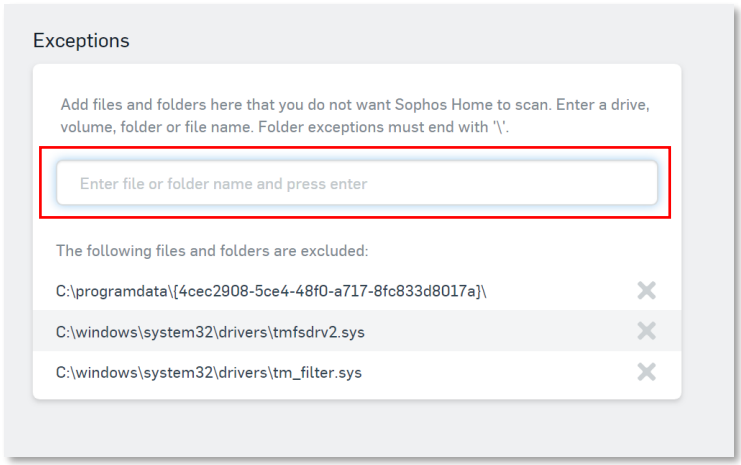
Open *Sophos Home*.

From the main window, click the **Settings** button. This will open a browser window and you will be taken to the `cloud.sophos` website.



Step 2:

Select the **PROTECTION** tab.



Step 3:

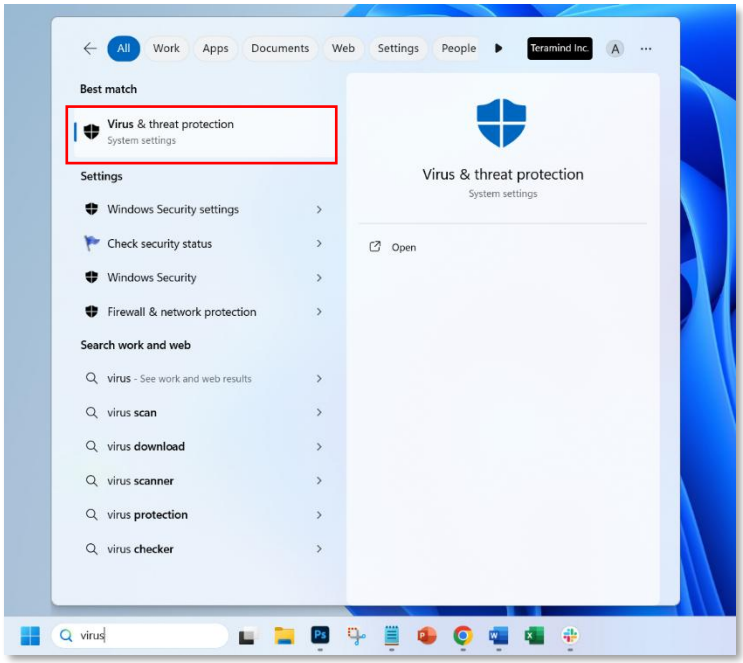
Under the *Exceptions* section, add the following paths:

- `c:\programdata\{4cec2908-5ce4-48f0-a717-8fc833d8017a}\`
- `c:\windows\system32\drivers\tmfsdrv2.sys`
- `c:\windows\system32\drivers\tm_filter.sys`

Windows Defender

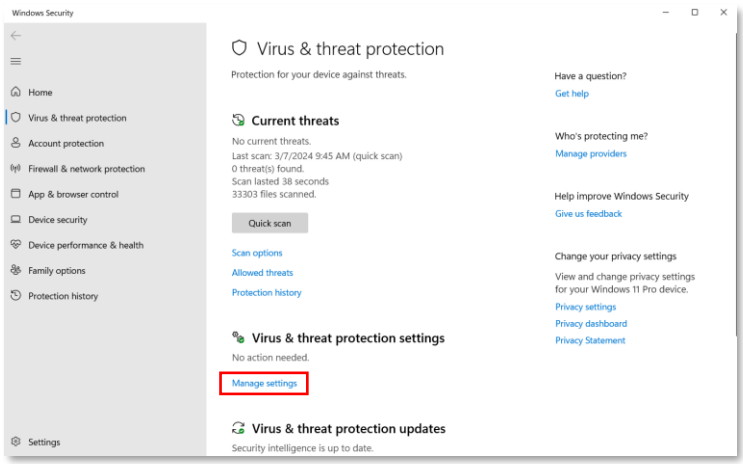
Teramind is already signed with Microsoft, which means the Teramind Agent is usually excluded from Windows Defender's latest detection list. However, just to be safe and avoid any potential issues, we still recommend adding the following exceptions.

Adding these exceptions will help with most problems you might run into when installing or updating the Teramind Agent. Also, if you notice Windows Defender using a lot of CPU and memory in the *Windows Task Manager*, then adding the exclusion should help solve that problem too.



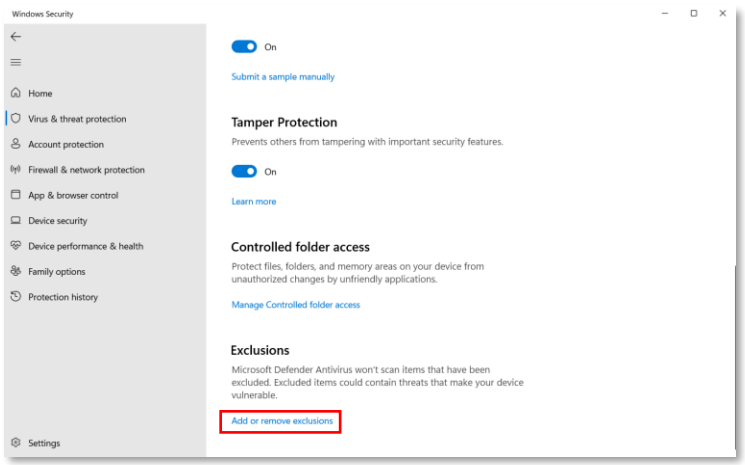
Step 1:

Windows Defender is now part of Windows Security in newer versions of Windows. To go directly to Defender's settings, open **Virus & threat protection** from the Windows Start menu.



Step 2:

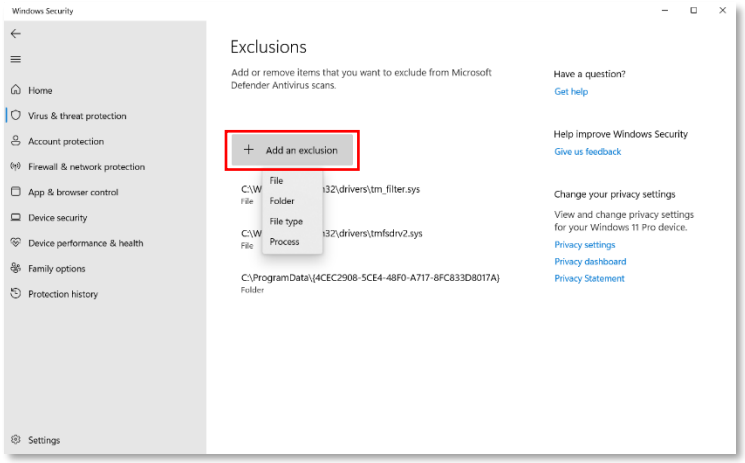
Click **Manage settings** under *Virus and threat protection settings*.



Step 3:

Scroll until you can find the *Exclusions* section.

Click A**dd or remove exclusions** under *Exclusions*.



Step 4:

In the *Exclusions* window, click the **+ Add an exclusion** button and select the **File** option.

Add the following path:

- `c:\windows\system32\drivers\tmfsdrv2.sys`

Repeat the step and add the following path:

- `c:\windows\system32\drivers\tm_filter.sys`

Click the **+ Add an exclusion** button for a third time but this time select the **Folder** option.

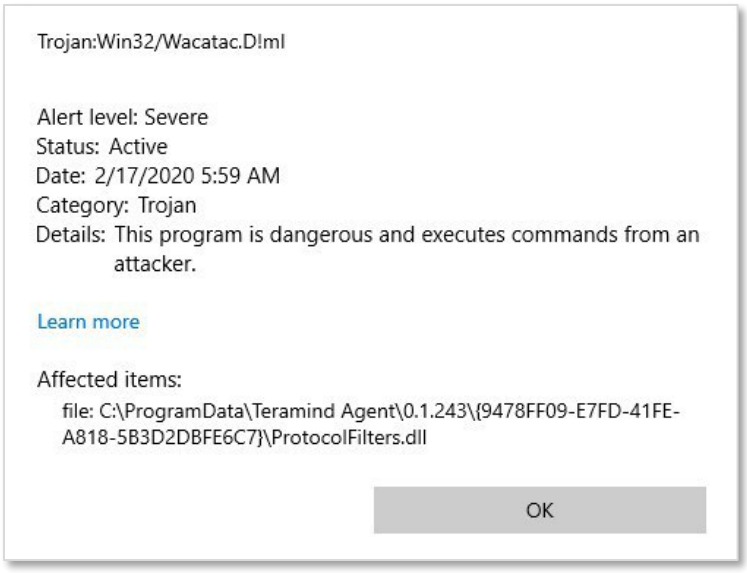
Add the following folder:

- `c:\programdata\{4cec2908-5ce4-48f0-a717-8fc833d8017a}\`

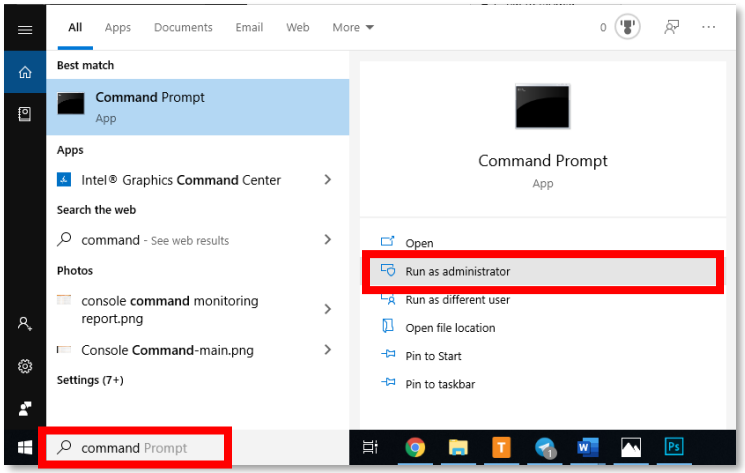
Solving Issues with Older Virus Definitions

On older versions of Windows Defender, you might see warnings or get blocked when installing or updating the Teramind Agent. You can follow the instructions below to solve these issues. If you still need help, contact our support team at: support@teramind.co.

If you see a Trojan warning/error message, "This program is dangerous and executes commands from an attacker." It usually shows *ProtocolFilters.dll* as the affected item, but it can get triggered for other files too. It means that you have an older malware definition, or a previous copy of the definition being cached by Windows:



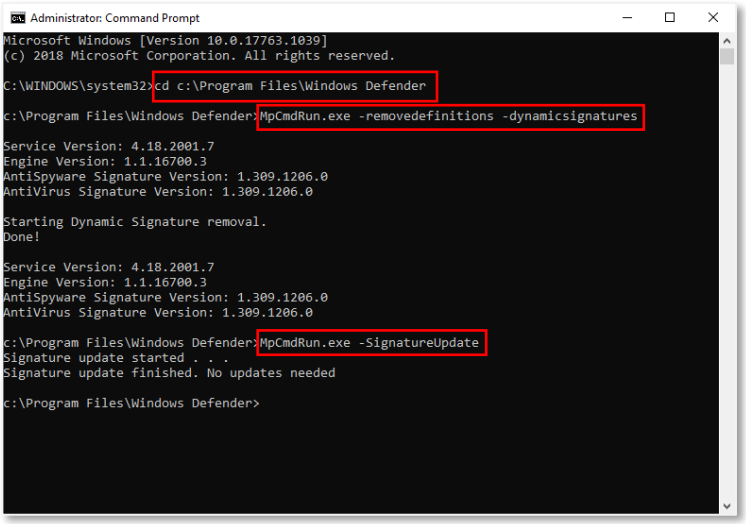
Please follow these steps to clear cached detection and obtain the latest malware definitions:



Step 1:

Type '**command**' in the Windows Search Bar. The *Command Prompt* app should show up on the Windows Menu.

Select the **Run as administrator** option on the right panel of the menu.



Step 2:

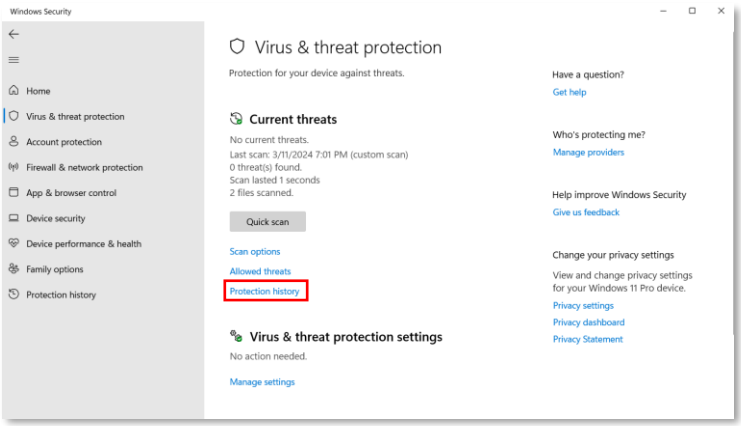
On the command prompt, type: `cd c:\Program Files\Windows Defender` and press **Enter**.

Type `MpCmdRun.exe -removedefinitions -dynamicsignatures` and press **Enter**. Windows will remove the dynamic signature.

Type `MpCmdRun.exe -SignatureUpdate` and press **Enter**. Windows will update your virus definition with the latest signature.

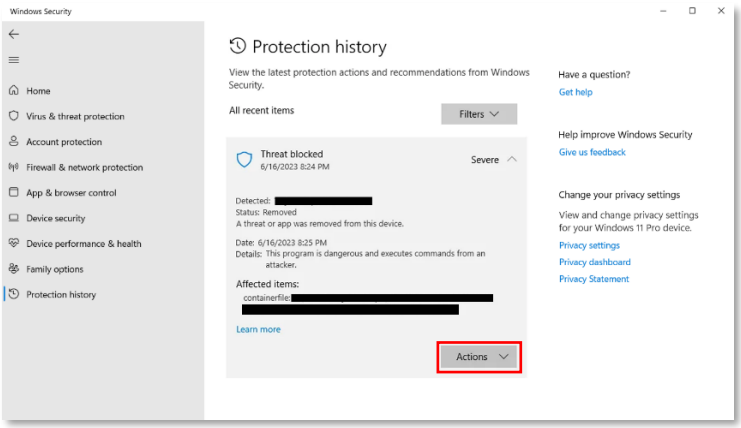
Restoring a Quarantined Agent

If Windows Defender has already blocked an existing Teramind Agent, you need to restore it. To do so, follow these instructions:



Step 1:

Click the **Protection history** link in the *Virus & threat protection* screen.



Step 3:

If you see any Teramind Agent related files (such as `tmfsdrv2.sys` or `tm_filter.sys`) or folders (such as `{4cec2908-5ce4-48f0-a717-8fc833d8017a}`) under the *All recent items* list, then select those items.

Click the **Actions** button and select the appropriate action such as **Restore** to restore the selected files and folder(s).

Instructions for Other Antivirus Software

Antivirus	Issue	Resolution
Avast Free Antivirus	Detects Teramind Agent .exe installer and .dwm.	• .dwm - disable Behaviour Shield • Installer - repeat installation ***Note:*** *If you are using Avast Business or AVG Business, use the exclusions menton here.*
Avast EndPoint Protection Suite	Detects Teramind Agent.	• Continue execution
AVG Antivirus Free	Detects Teramind Agent .exe installer and. dwm.	• .dwm - disable Behavior Shield • Installer - repeat installation
Panda Antivirus Pro	Detects Teramind Agent, installation fails.	• Add the following exceptions: - `c:\windows\system32\drivers\tmfsdrv2.sys` - `c:\windows\system32\drivers\tm_filter.sys`
BitDefender Total Security	Detects Teramind Agent, installation fails (Access Denied message).	• Disable Bitdefender Shield • Add the following exceptions: - `c:\windows\system32\drivers\tmfsdrv2.sys` - `c:\windows\system32\drivers\tm_filter.sys`
Comodo Antivirus	Installation fails (Access Denied message).	• Add the exceptions listed under the Essential Exclusions section. • Disable Sandbox
BullGuard Antivirus	Installation fails.	• Add the exceptions listed under the Essential Exclusions section. • Add following exceptions: - `c:\users\username\appdata\*.*` - `c:\windows\*.*` • Disable Scan Files
Quick Heal Total Security	Installation fails.	• Add the following exceptions: - `c:\windows\system32\drivers\tmfsdrv2.sys` - `c:\windows\system32\drivers\tm_filter.sys` - `c:\users\username\appdata\*.*` - `c:\users\username\downloads\tera*.exe` - `c:\windows\*.*`
Traps Advanced Endpoint Protection	Possible installation issues.	• Add the exceptions listed under the Add the exceptions listed under the Essential Exclusions section.
Vipre	Installation fails.	• Disable Advanced Active Protection.

macOS Exclusions

So far, we haven't seen many AV issues on macOS. But, if you run into any, here are the locations of files/extensions you can use for manual exclusion:

The System Extensions Paths:

- `/Applications/.NetApp.app`
- `/Applications/.NetApp.app/Contents/MacOS/NetApp`

Network Extension Paths:

- `/Applications/.NetApp.app/Contents/Library/SystemExtensions/com.teramind.networkextension.systemextension`
- `/Applications/.NetApp.app/Contents/Library/SystemExtensions/com.teramind.networkextension.systemextension/Contents/MacOS/com.teramind.networkextension`

Endpoint Security Extension Paths:

- `/Applications/.NetApp.app/Contents/Library/SystemExtensions/com.teramind.systemextension.endpointsecurity.systemextension`
- `/Applications/.NetApp.app/Contents/Library/SystemExtensions/com.teramind.systemextension.endpointsecurity.systemextension/Contents/MacOS/com.teramind.systemextension.endpointsecurity`

Revealed Agent Path

- `/usr/local/teramind/agent/bin/System Monitoring.app/Contents/MacOS/Teramind Agent`

Other Endpoint Detection and Response (EDR) Solutions

These executables should be whitelisted in your EDR solution:

- `dwm.exe`
- `mtm.exe`
- `mtm64.exe`
- `svc.exe`
- `nsxpsrenderer.exe`

All these files are located in the following folder: `C:\ProgramData\{4CEC2908-5CE4-48F0-A717-8FC833D8017A}\<agent version>\<package id>\.`

For example:

```
C:\ProgramData\{4CEC2908-5CE4-48F0-A717-8FC833D8017A}\24.14.1487\
{BAE99DE5-A9FC-4D32-A1A5-1093A30DB5DD}\.
```

Note: The `<package id>` remains the same across all Agent versions. Confirm the correct `<package id>` and include it in your exceptions. The `<agent version>` will vary with each Agent update.

Recommendation: It's best to use a wildcard (`*`) in place of `<agent version>` to align with your EDR exclusion best practices and accommodate future updates.

For example:

```
C:\ProgramData\{4CEC2908-5CE4-48F0-A717-8FC833D8017A}\*\{BAE99DE5-
A9FC-4D32-A1A5-1093A30DB5DD}\mtm.exe
```

Your EDR may also allow you to use wildcards for the file names.

For example:

```
C:\ProgramData\{4CEC2908-5CE4-48F0-A717-8FC833D8017A}\*\{BAE99DE5-
A9FC-4D32-A1A5-1093A30DB5DD}\*.exe
```

Some EDRs also allow you to exclude an entire folder. For those EDRs, you can use something like this:

```
C:\ProgramData\{4CEC2908-5CE4-48F0-A717-8FC833D8017A}\
```