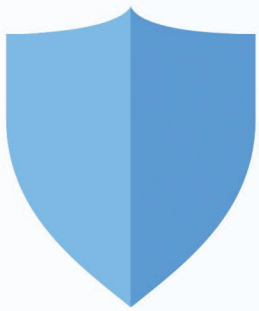


# Antivirus Configuration Guide for EmpMonitor Agent

Version 2.0

EmpMonitor

# Table of Contents



# Antivirus and EmpMonitor Agent

We make every effort possible to be antivirus-friendly. EmpMonitor has been whitelisted from many of the leading antivirus packages. We also sign all of our software with an extended validation certificate. In most cases, your antivirus software will recognize EmpMonitor as legitimate software and not interfere.

However, there might be situations where your antivirus can block you from installing the EmpMonitor Agent or generate false positives. We have provided a step by step guide for configuring some of the most common antivirus software. Please follow the instructions in this guide to add exceptions and unblock the required ports.

# Instructions To Configure Most Commonly Used Antivirus Software

To make it easier to configure the exception settings, we have included step by step instructions for the most commonly used antivirus software in the next few pages.

# Windows Defender Antivirus Configuration for EMP Monitor

On **Windows 10**, the **Windows Defender Antivirus** is your default anti-malware engine to protect your device and data from viruses, rootkits, ransomware, and other security threats.

Although for the most part the built-in Windows 10 antivirus does a pretty good job, it may flag a file or folder that you trust as malicious. If you want to prevent this type of behavior from happening, **Windows Defender Antivirus** includes an option to exclude files and folders, as well as file types and processes from getting scanned and blocked.

In this **Windows 10 guide**, we walk you through the **steps to exclude specific items and locations from Windows Defender Antivirus scans**.

## How to prevent Windows Defender from scanning specific files?

If you have certain files, folders, file types, and processes that you want to exclude from **Windows Defender Antivirus scans**, use the following steps:

**Step 1:** Open **Windows Defender Security Center.**

**Step 2:** Click on **Virus & threat protection.**

**Step 3:** Under "**Exclusions**," click the Add or remove exclusions option.

**Step 4:** Click the **Add an exclusion** button.

**Step 5:** Select the content you want to exclude from Windows Defender Antivirus, such as:

- **File** — Excludes only one file per exclusion.
- **Folder** — Excludes a folder and its content, including sub-folders.
- **File type** — Instead of excluding files and folder locations, you can configure the antivirus to ignore files with a specific extension no matter their location.
- **Process** — Excludes background processes by name.

**Step 6:** Continue with the on-screen directions to add the new exclusion depending on your selection. (For example, if you select File, you simply need to browse and select the file you want to exclude. Or if you select the File type option, you only need to enter the extension of the file format to skip during scans.)

Once you complete the above-mentioned steps, you may need to repeat the instructions to exclude other items you don't want the antivirus to scan to avoid false positives.

At any time, you can remove an exclusion using the same instructions, but on step No. 4, make sure to select the item and click the **Remove** button.

# Mcafee Antivirus Configuration for EMP Monitor

## Steps to exclude Files & Folder in McAfee

Add all EmpMonitor files in the McAfee.

**Step 1:** Go to “**Setting**” >> “**Real-Time Scanning**”.

**Step 2:** Click on **Excluded Files** >> ‘’**Add File**’’ and select this path

- Only select the **.exe** file.

  i.e., C:\Users\HP CROMA\AppData\Local\Programs\BizAnalystDesktop\BizAnalystDesktop.exe

# Bitdefender Antivirus Configuration for EMP Monitor

In **Bitdefender 2018**, the **Advanced Threat Defense and Antivirus** feature allow you to configure exclusions for trusted applications, which means that these apps will not be scanned and are not going to get automatically blocked if they perform malware-like actions.

At the same time, the Safe Files gives you the possibility to choose which applications may change or delete your protected files.

## Adding Antivirus Exclusions

**Bitdefender** allows the exclusion of specific files, folders, or file extensions from scanning.
To add any of them to the Exclusions list, follow the steps explained below:

**Step 1:** Open the **Bitdefender** program and go to the **Protection** windows.

**Step 2:** Click the **VIEW FEATURES** link.

**Step 3:** Select the **Settings** icon in the upper-right corner of the **ANTIVIRUS** module.

**Step 4:** Select the **Exclusions** tab.

**Step 5:** Click on the **List of files and folders excluded from scanning** as per the menu.

**Step 6:** Click the **Add** button.

**Step 7:** Click **Browse** and select the folder that you want to be excluded from scanning.

Make sure it’s excluded from **Both on-demand scanning** and **on-access scanning**.

**Step 8:** Click **Add** to save the changes and close the window.

**Bitdefender 2018** also allows you to exclude file extensions from scanning. When excluded, files with those extensions will no longer be scanned by Bitdefender.
To exclude file extensions from scanning:

**Step 1:** Click the **List of extensions excluded from the scanning** accordion menu.

**Step 2:** Click the **Add** button.

**Step 3:** Enter the extensions that you want to be excluded from scanning, separating them with semicolons (;). Here is an example: **txt**;**avi**;**jpg**. Again, make sure the extensions are excluded from **Both on-demand scanning** and **on-access scanning**.

Adding a process to the Advanced Threat Defense exclusions list.
You can configure exclusion rules for trusted applications so that **Advanced Threat Defense** does not block them if they perform malware-like actions.

**NOTE:** Advanced Threat Defense will continue to monitor excluded applications.

If an excluded application is detected to perform suspicious activities, the event will simply be logged and reported to Bitdefender Cloud as a detection error. To start adding processes to the Advanced Threat Defense exclusions list, you must:

**Step 1:** Open the main Bitdefender interface.

**Step 2:** Go to the **Protection** window.

**Step 3:** Click the **VIEW FEATURES** link.

**Step 4:** Click the ⚙ icon in the lower-right corner of the **ADVANCED THREAT DEFENSE** module.

**Step 5:** In the **WHITELIST** window, click **Add applications to the whitelist**.

**Step 6:** Find and select the application you want to be excluded, select its **.exe** file, then click **OK**.

**Step 7:** To remove an entry from the list, click the **Remove** button next to it.

# Norton Antivirus Configuration for EMP Monitor

## How to Exclude Files and Folders From Norton Antivirus Software Scans?

There are dozens of **Norton Security Antivirus programs** on the market, but the process for excluding files is essentially the same. For example, to exclude specific files and folders from a Norton Security scan in Windows 10:

**Step 1:** Open the **Norton Antivirus Software** and select **Settings**.

**Step 2:** Select **Antivirus**.

**Step 3:** Select the **Scans and Risks** tab.

**Step 4:** Scroll down to the **Exclusions/ Low Risks** section and select **Configure [+]** next to **Items to Exclude From Scans**.

**Step 5:** Select **Clear Files IDs Excluded During Scans** to reset your exclusion settings.

**Step 6:** Select **Add Folders** or **Add Files** and choose the file/ folder you want to exclude. When you are finished, select **OK** to save the changes.

**Step 7:** At this point, you can exit any open windows and close the Norton software.

# Kaspersky Antivirus Configuration for EMP Monitor

## How to add an application to exclusions in Kaspersky Internet Security?

**Step 1:** Open the settings **Kaspersky Internet Security** and choose **Additional** –> **Threats and Exclusions.**

**Step 2:** Select **Manage exclusions** or **Specify trusted applications**.

Select the file or application to exclude from the scan scope in Kaspersky Internet Security.

Optionally, specify the protection component that should not scan the application. You can learn more about setting up exclusions in Kaspersky Internet Security in the Knowledge Base.

## How to exclude a link from the scan scope in Kaspersky Internet Security?

**Step 1:** Open the **settings** in **Kaspersky Internet Security** and choose **Protection** –> **Web Anti-Virus**.

**Step 2:** In the Web Anti-Virus settings window, select **Advanced Settings**.

**Step 3:** Click Configure trusted URLs and specify the link or links you want Kaspersky Internet Security not to check.

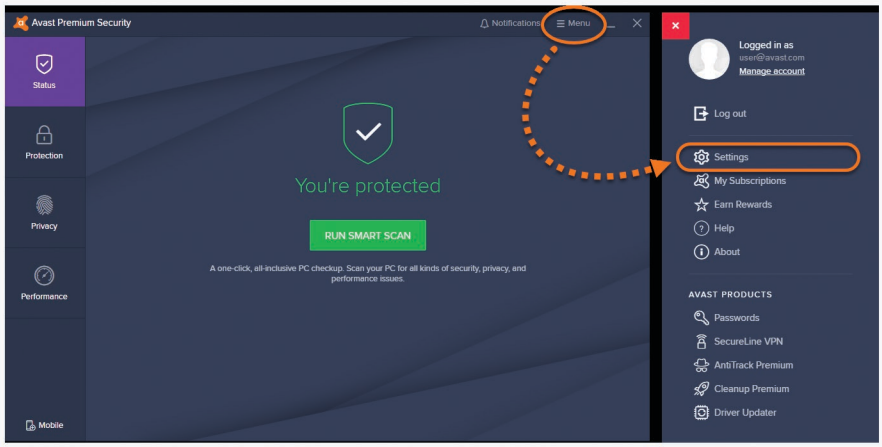
For more information, see the detailed article in our Knowledge Base devoted to checking Web pages for threats in Kaspersky Internet Security.

# Avast Antivirus Configuration for EMP Monitor Avast

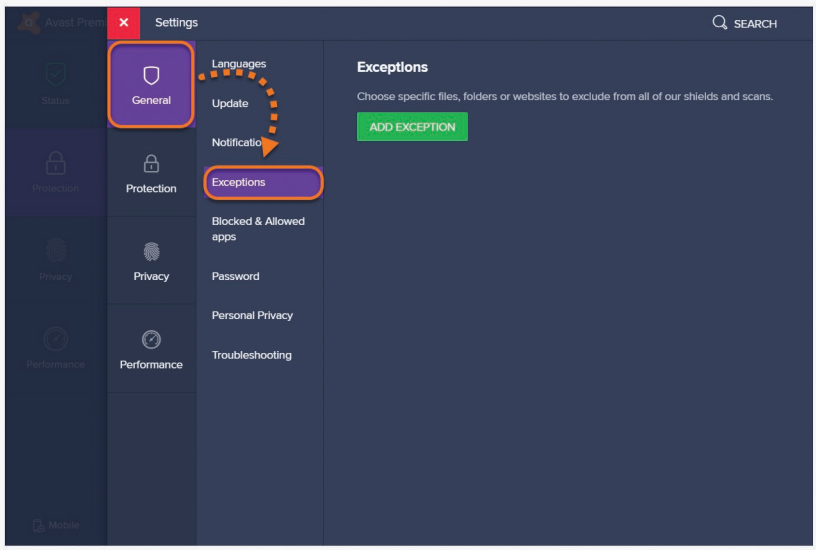
## Add an Exception

Setting global exceptions excludes individual files, entire folders, and websites from all scans and shields at once. Scans and Shields analyze all file, application, and web activity in real-time.
To define an exception for all scans and shields:

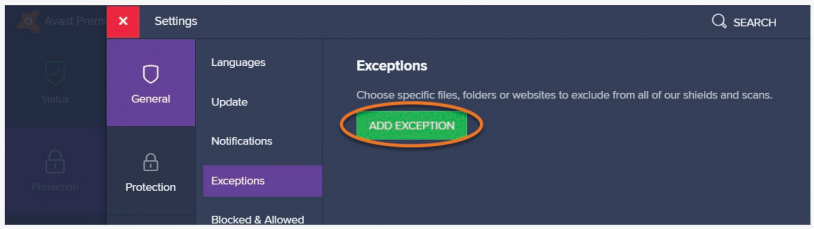
**Step 1:** Open the Avast Antivirus user interface and select **Menu ▸ Settings**.



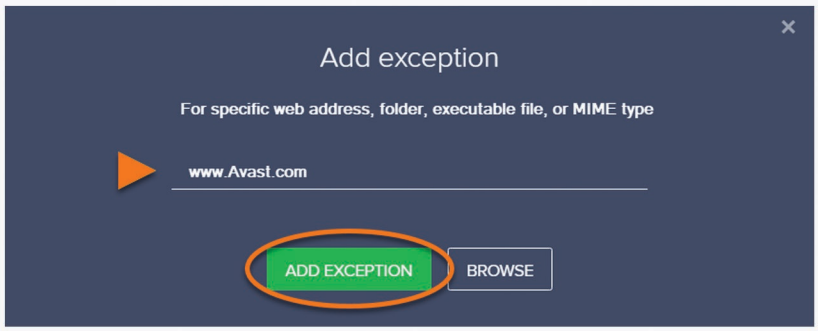

**Step 2:** Ensure the **General** tab is selected, then click **Exceptions**.



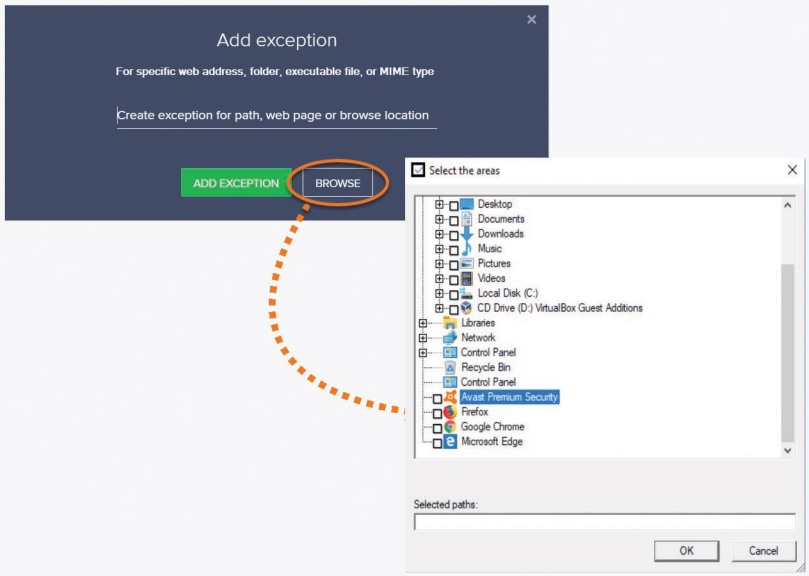
**Step 3:** Click the Add Exception button.




**Step 4:** Add an exception in one of the following ways:
Type the file path, folder path, or URL into the **text box**, then click **Add Exception**.




**Step 5:** Click **Browse**, tick the box next to the file or folder you want to add to the exceptions list, then click **OK**.

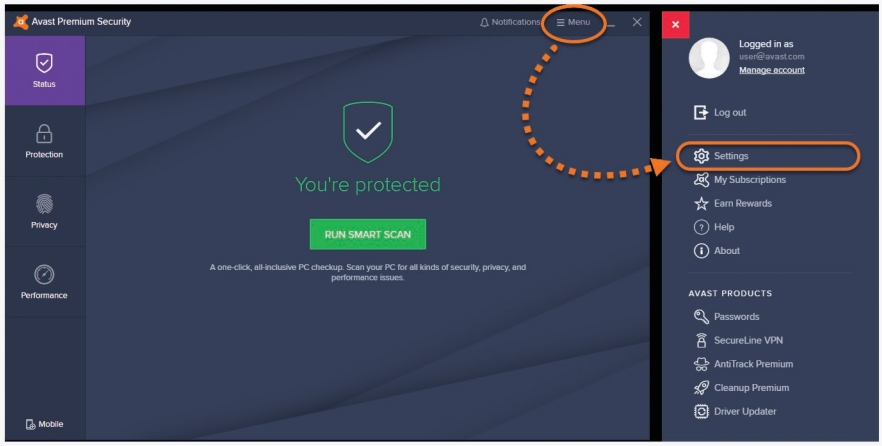



Your selected file, folder, or URL is added to the exceptions list.

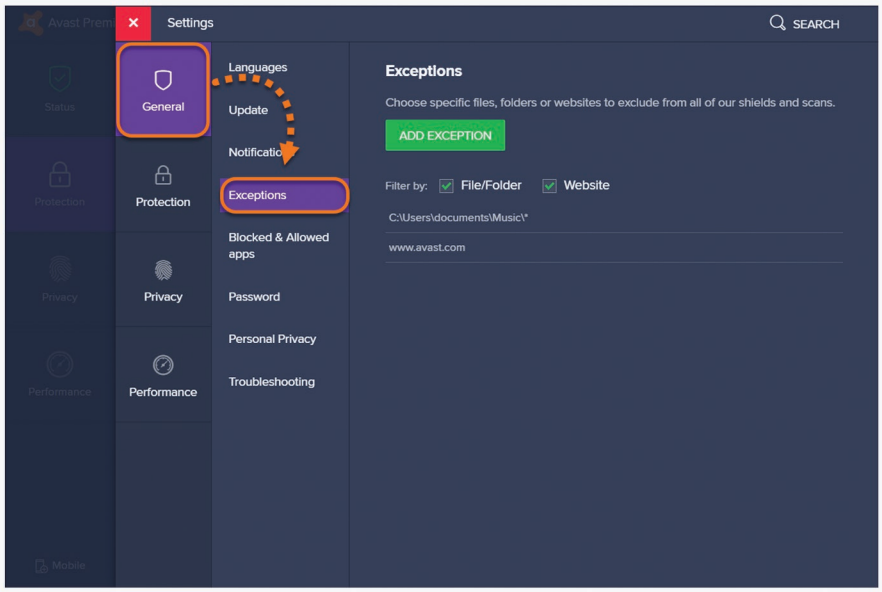
## View the Exceptions List

After you specify a file, folder, or website to exclude from Avast Antivirus scans and shields, you can view and remove any item from the list individually:

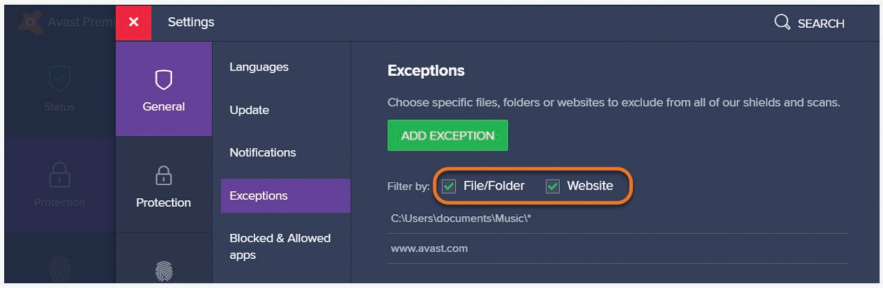
**Step 1:** From the main **Avast Antivirus** user interface, go to Menu >>>>>>>>> Settings.



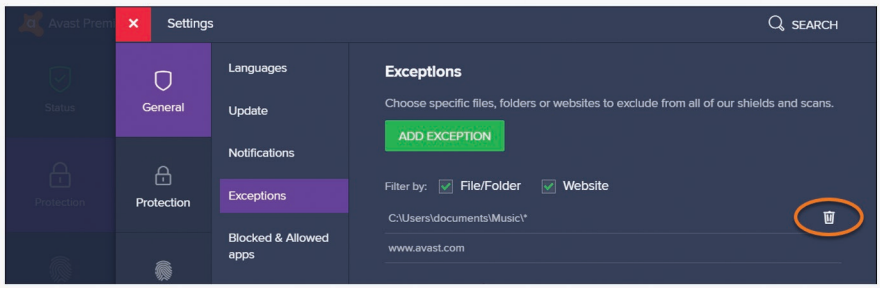

**Step 2:** Ensure the **General** tab is selected, then click **Exceptions**.



**Step 3:** Ensure the boxes next to **File/Folder** and **Website** are ticked to see all exceptions in the list. The Exceptions list is visible below these filters.

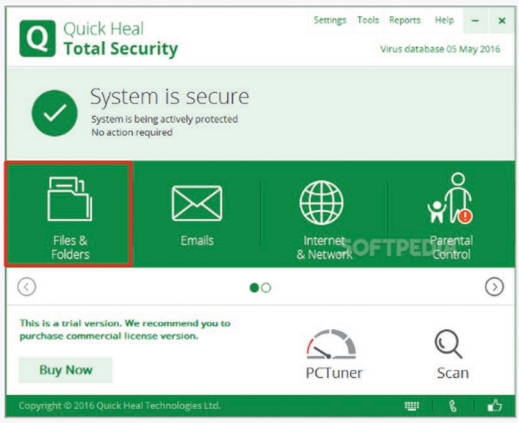



**Step 4:** To delete an item from the list, hover the cursor over the panel for the exception you want to delete, then click the trash icon. The list will update automatically.

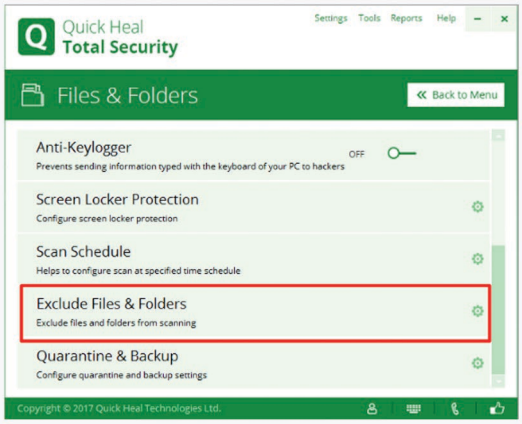


# QuickHeal Antivirus Configuration for EMP Monitor

**Step 1:** Open **Quick Heal** and Click on **Files and Folders**.

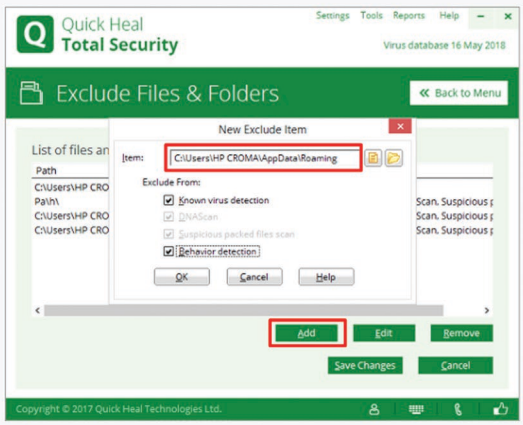



**Step 2:** Go to **Exclude files and folders**.



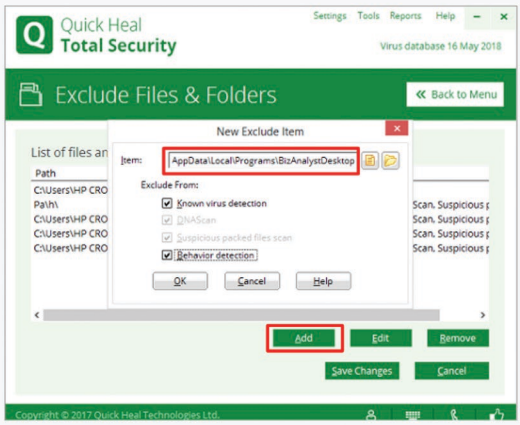

**Step 3:** Do the following steps to Exclude file

- Click on **ADD** Button
- Go to the Log file path copy it i.e, **C:\Program Files (x86)\ Microsoft Corp\EmpMonitor**
- Paste it in the ITEM box, And Exclude it from **Known virus detection and Behavior detection >> OK**




**Step 4:** Go to the following path

- Again repeat the steps Click on **Add** button.
- Open Path **C:\Program Files (x86)\Microsoft Corp\EmpMonitor.**
- Paste it in the ITEM box, And Exclude it from **Known virus detection and Behavior detection >> OK**

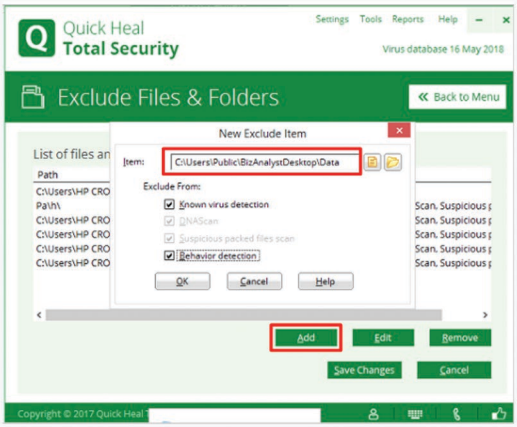


**Step 5:** Go to the following path

- i.e., **C:\Program Files (x86)\Microsoft Corp\EmpMonitor.**
- **Paste it in the ITEM box, And Exclude it from Known virus detection and Behavior detection >> OK.**

**Step 6:** Again repeat the steps

- Open path **C:\Program Files (x86)\Microsoft Corp\EmpMonitor**
- Paste it in the ITEM box, And Exclude it from **Known virus detection and Behavior detection >> OK**




# Net Protector Antivirus Configuration for EMP Monitor

## Steps to exclude files & Folder in Net Protector.

There are dozens of **Norton Security Antivirus programs** on the market, but the process for excluding files is essentially the same. For example, to exclude specific files and folders from a Norton Security scan in Windows 10:

**Step 1:** Go to the **Protection** tab.

**Step 2:** Click on **Online Protection**.

**Uncheck** all the **checkbox >> Apply**.

**Step 3:** Go to Web Security Tab.

Click on **Parental Control** and turn it **Off**.

**Step 4:** **In the same Web Security Tab**.

Click on **Firewall** and turn it **Off.**

**Step 5:** Open **Run Dialogue Box**, Type **services.msc**

**Step 6:** Search for **Net Protector Firewall Properties & Net Protector Web Protection**

**Step 7:** Click on each one

**Stop** the process >> Select **Disabled** from the dropdown list >> **Ok**

# ESET Antivirus Configuration for EMP Monitor

Exclusions enable you to exclude files and folders from scanning. To ensure that all objects are scanned for threats, we recommend only creating exclusions when it is absolutely necessary.

However, there are situations where you may need to exclude an object, for example large database entries that would slow your computer during a scan or software that conflicts with the scan.

You can add **files and folders** to be **excluded from scanning** into the list of exclusions via **Advanced setup (F5) > Detection engine > Exclusions > Files and folders to be excluded from scanning > Edit.**

To exclude an object (path, threat or hash) from scanning, click **Add** and enter the path to an object or select it in the tree structure. You can also **Edit** or **Delete** selected entries.

## Types of exclusions

**Path** – Path to excluded files and folders.

**Detection** (or **Threat**) – If there is a name of a detection / threat next to an excluded file, it means that the file is only excluded for the given threat, not completely. If that file becomes infected later with other malware, it will be detected by the antivirus module.

This type of exclusion can only be used for certain types of infiltration and it can be created either in the threat alert window reporting the infiltration (click **Show advanced options** and then select **Exclude from detection**), or by clicking **Tools > Quarantine** and then right-clicking the quarantined file and selecting **Restore and exclude from scanning** from the context menu.

**Hash** – Excludes a file based on specified hash (SHA1), regardless of the file type, location, name or its extension.

# Malwarebytes Antivirus Configuration for EMP Monitor

## Exclude detections in Malwarebytes for Windows

**Malwarebytes for Windows** can block items, including websites, applications, and files, that are not inherently malicious. The most common non-malicious detections are Potentially Unwanted Programs (PUPs) and Potentially Unwanted Modifications (PUMs).

There may be occasions when **Malwarebytes** for Windows flags an item you trust as malicious. Add the item to your exclusions to stop **Malwarebytes** for Windows from blocking an item **you know and trust.**

Note that when you add a detected item to **Malwarebytes Exclusions**, it is omitted from future scans and protection events.

In Malwarebytes for Windows, there are four types of exclusions you can add:

- Exclude a File or Folder
- Exclude a Website
- Exclude an Application that Connects to the Internet
- Exclude a Previously Detected Exploit

Malwarebytes for Windows exclusions

**Step 1:** Open **Malwarebytes for Windows**.

**Step 2:** Click **Settings**, then click the **Exclusions** tab.

**Step 3:** To add an item to the exclusion list, click **Add Exclusion**.

**Step 4:** Select the type of exclusion you want to add.

**Step 5:** Click **Next**, then follow the next prompt to add your exclusion and confirm your changes.