

Discover ∨ Product documentation ∨ Development languages ∨ Topics ∨

Sign in

Microsoft Defender

Microsoft Defender products & services V Security resources V

📆 Filter by title

Companionity with other security products

Find malware detection names for Microsoft Defender for Endpoint

- > Microsoft Defender Antivirus security intelligence and product updates
- > Manage Microsoft Defender Antivirus for your organization
- > Deploy and report on Microsoft Defender **Antivirus**
- > Scans and remediation
- Microsoft Defender Antivirus exclusions

Configure custom exclusions

Exclusions based on file extension and folder location

### Exclusions for files opened by processes

Contextual file and folder exclusions **Exclusions for Windows Server** Common mistakes to avoid

- > Troubleshooting mode for Defender for Endpoint
- > Diagnostics and performance for Microsoft Defender Antivirus
- > Troubleshooting Microsoft Defender **Antivirus**
- > Behavioral blocking and containment **UEFI** scanning in Defender for Endpoint Run Microsoft Defender Antivirus in a sandbox

Early Launch Antimalware (ELAM) and Microsoft Defender Antivirus

Hardware acceleration and Microsoft Defender Antivirus

Address false positives/negatives in Microsoft Defender for Endpoint

- > Manage device configuration
- > Investigate and respond to threats
- > Reference
- > Microsoft Defender XDR docs

Download PDF

··· / Microsoft Defender / Microsoft Defender for Endpoint /



## Configure exclusions for files opened by processes

Article • 04/24/2024 • 3 contributors

Feedback

#### In this article

Examples of process exclusions

Configure the list of exclusions for files opened by specified processes

Use Windows Management Instruction (WMI) to exclude files that have been opened by specified processes from scans

Use the Windows Security app to exclude files that have been opened by specified processes from scans

Show 2 more

### Applies to:

- Microsoft Defender for Endpoint Plan 1
- Microsoft Defender for Endpoint Plan 2
- Microsoft Defender Antivirus

#### **Platforms**

Windows

You can exclude files that are opened by specific processes from Microsoft Defender Antivirus scans. Note that these types of exclusions are for files that are opened by processes and not the processes themselves. To exclude a process, add a file exclusion (see Configure and validate exclusions based on file extension and folder location).

See Important points about exclusions and review the information in Manage exclusions for Microsoft Defender for Endpoint and Microsoft Defender Antivirus before defining your exclusion lists.

This article describes how to configure exclusion lists.

## **Examples of process exclusions**

Expand table

Exclusion	Example
Any file on the machine that is opened by any process with a specific file name	Specifying test.exe would exclude files opened by:
	<pre>c:\sample\test.exe</pre>
	<pre>d:\internal\files\test.exe</pre>
Any file on the machine that is opened by any process under a specific folder	Specifying c:\test\sample\* would exclude files opened by:
	<pre>c:\test\sample\test.exe</pre>
	<pre>c:\test\sample\test2.exe</pre>
	<pre>c:\test\sample\utility.exe</pre>

Any file on the machine that is opened by a specific process in a specific folder

Specifying c:\test\process.exe would exclude files only opened by c:\test\process.exe

When you add a process to the process exclusion list, Microsoft Defender Antivirus won't scan files opened by that process, no matter where the files are located. The process itself, however, will be scanned unless it has also been added to the file exclusion list.

The exclusions only apply to always-on real-time protection and monitoring. They don't apply to scheduled or on-demand scans.

Changes made with Group Policy to the exclusion lists **will show** in the lists in the Windows Security app. However, changes made in the Windows Security app **will not show** in the Group Policy lists.

You can add, remove, and review the lists for exclusions in Group Policy, Microsoft Configuration Manager, Microsoft Intune, and with the Windows Security app, and you can use wildcards to further customize the lists.

You can also use PowerShell cmdlets and WMI to configure the exclusion lists, including reviewing your lists.

By default, local changes made to the lists (by users with administrator privileges; changes made with PowerShell and WMI) are merged with the lists as defined (and deployed) by Group Policy, Configuration Manager, or Intune. The Group Policy lists take precedence if there are conflicts.

You can configure how locally and globally defined exclusions lists are merged to allow local changes to override managed deployment settings.

#### ! Note

**Network Protection** and **Attack surface reduction rules** are directly impacted by process exclusions on all platforms, meaning that a process exclusion on any OS (Windows, MacOS, Linux) will result in Network Protection or ASR being unable to inspect traffic or enforce rules for that specific process.

## Image name vs full path for process exclusions

Two different types of process exclusions may be set. A process may be excluded by image name, or by full path. The image name is simply the file name of the process, without the path.

For example, given the process MyProcess.exe running from C:\MyFolder\ the full path to this process would be C:\MyFolder\MyProcess.exe and the image name is MyProcess.exe.

Image name exclusions are much more broad - an exclusion on MyProcess.exe will exclude any processes with this image name, regardless of the path they are run from. So for example, if the process MyProcess.exe is excluded by image name, it will also be excluded if it is run from C:\MyOtherFolder, from removable media, et cetera. As such it is recommended that whenever possible, the full path is used.

## Use wildcards in the process exclusion list

The use of wildcards in the process exclusion list is different from their use in other exclusion lists. When the process exclusion is defined as an image name only, wildcard usage is not allowed. However when a full path is used, wildcards are supported and the wildcard behavior behaves as described in File and Folder Exclusions

The use of environment variables (such as %ALLUSERSPROFILE%) as wildcards when defining items in the process exclusion list is also supported. Details and a full list of supported environment variables are described in File and Folder Exclusions.

The following table describes how the wildcards can be used in the process exclusion list, when a path is supplied:

Expand table

Wildcard	Example use	Example matches
* (asterisk)	C:\MyFolder\*	Any file opened by C:\MyFolder\MyProce
Replaces any number of characters.		or C:\MyFolder\AnotherProcess.exe
	C:\*\*\MyProcess.exe	Any file opened by
		C:\MyFolder1\MyFolder2\MyProcess.exe
		C:\MyFolder3\MyFolder4\MyProcess.exe
	<pre>C:\*\MyFolder\My*.exe</pre>	Any file opened by
		C:\MyOtherFolder\MyFolder\MyProcess
		C:\AnotherFolder\MyFolder\MyOtherPro
'?' (question	<pre>C:\MyFolder\MyProcess??.exe</pre>	Any file opened by C:\MyFolder\MyProce
mark)		Or C:\MyFolder\MyProcessAA.exe Or
Replaces one character.		C:\MyFolder\MyProcessF5.exe
Environment	%ALLUSERSPROFILE%\MyFolder\MyProcess.exe	Any file opened by
Variables		C:\ProgramData\MyFolder\MyProcess.ex

## **Contextual Process Exclusions**

Note that a process exclusion may also be defined via a Contextual exclusion allowing for example a specific file to be excluded only if it is opened by a specific process.

## Configure the list of exclusions for files opened by specified processes

## Use Microsoft Intune to exclude files that have been opened by specified processes from scans

For more information, see Configure device restriction settings in Microsoft Intune and Microsoft Defender Antivirus device restriction settings for Windows 10 in Intune.

# Use Microsoft Configuration Manager to exclude files that have been opened by specified processes from scans

See How to create and deploy antimalware policies: Exclusion settings for details on configuring Microsoft Configuration Manager (current branch).

## Use Group Policy to exclude files that have been opened by specified processes from scans

- 1. On your Group Policy management computer, open the Group Policy Management Console, right-click the Group Policy Object you want to configure and click **Edit**.
- 2. In the **Group Policy Management Editor**, go to **Computer configuration** and click **Administrative templates**.

- 3. Expand the tree to Windows components > Microsoft Defender Antivirus > Exclusions.
- 4. Double-click Process Exclusions and add the exclusions:
  - a. Set the option to **Enabled**.
  - b. Under the Options section, click Show....
  - c. Enter each process on its own line under the **Value name** column. See the example table for the different types of process exclusions. Enter **0** in the **Value** column for all processes.
- 5. Click OK.

## Use PowerShell cmdlets to exclude files that have been opened by specified processes from scans

Using PowerShell to add or remove exclusions for files that have been opened by processes requires using a combination of three cmdlets with the -ExclusionProcess parameter. The cmdlets are all in the Defender module.

The format for the cmdlets is:



The following are allowed as the <cmdlet>:

**Expand table** 

Configuration action	PowerShell cmdlet
Create or overwrite the list	Set-MpPreference
Add to the list	Add-MpPreference
Remove items from the list	Remove-MpPreference

### (i) Important

If you have created a list, either with <u>Set-MpPreference</u> or <u>Add-MpPreference</u>, using the <u>Set-MpPreference</u> cmdlet again will overwrite the existing list.

For example, the following code snippet would cause Microsoft Defender Antivirus scans to exclude any file that is opened by the specified process:



For more information on how to use PowerShell with Microsoft Defender Antivirus, see Manage antivirus with PowerShell cmdlets and Microsoft Defender Antivirus cmdlets.

# Use Windows Management Instruction (WMI) to exclude files that have been opened by specified processes from scans

Use the **Set**, **Add**, and **Remove** methods of the **MSFT\_MpPreference** class for the following properties:



The use of **Set**, **Add**, and **Remove** is analogous to their counterparts in PowerShell: Set-MpPreference, Add-MpPreference, and Remove-MpPreference.

For more information and allowed parameters, see Windows Defender WMIv2 APIs.

# Use the Windows Security app to exclude files that have been opened by specified processes from scans

Follow the instructions in Add exclusions in the Windows Security app.

## Review the list of exclusions

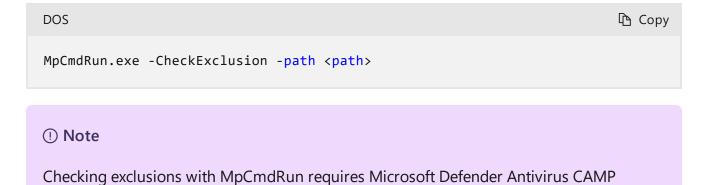
You can retrieve the items in the exclusion list with MpCmdRun, PowerShell, Microsoft Configuration Manager, Intune, or the Windows Security app.

If you use PowerShell, you can retrieve the list in two ways:

- Retrieve the status of all Microsoft Defender Antivirus preferences. Each of the lists are displayed on separate lines, but the items within each list are combined into the same line.
- Write the status of all preferences to a variable, and use that variable to only call the specific list you're interested in. Each use of Add-MpPreference is written to a new line.

## Validate the exclusion list by using MpCmdRun

To check exclusions with the dedicated command-line tool mpcmdrun.exe, use the following command:



version 4.18.1812.3 (released in December 2018) or later.

## Review the list of exclusions alongside all other Microsoft Defender Antivirus preferences by using PowerShell

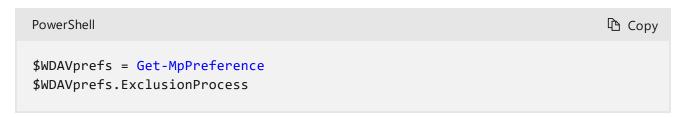
Use the following cmdlet:



For more information on how to use PowerShell with Microsoft Defender Antivirus, see Use PowerShell cmdlets to configure and run Microsoft Defender Antivirus and Microsoft Defender Antivirus cmdlets .

## Retrieve a specific exclusions list by using PowerShell

Use the following code snippet (enter each line as a separate command); replace **WDAVprefs** with whatever label you want to name the variable:



For more information on how to use PowerShell with Microsoft Defender Antivirus, see Use PowerShell cmdlets to configure and run Microsoft Defender Antivirus and Microsoft Defender Antivirus cmdlets.



If you're looking for Antivirus related information for other platforms, see:

- <u>Set preferences for Microsoft Defender for Endpoint on macOS</u>
- Microsoft Defender for Endpoint on Mac
- macOS Antivirus policy settings for Microsoft Defender Antivirus for Intune
- Set preferences for Microsoft Defender for Endpoint on Linux
- Microsoft Defender for Endpoint on Linux
- <u>Configure Defender for Endpoint on Android features</u>
- Configure Microsoft Defender for Endpoint on iOS features

## Related articles

- Configure and validate exclusions in Microsoft Defender Antivirus scans
- Configure and validate exclusions based on file name, extension, and folder location
- Configure Microsoft Defender Antivirus exclusions on Windows Server
- Common mistakes to avoid when defining exclusions
- Customize, initiate, and review the results of Microsoft Defender Antivirus scans and remediation
- Microsoft Defender Antivirus in Windows 10



Do you want to learn more? Engage with the Microsoft Security community in our Tech Community: Microsoft Defender for Endpoint Tech Community ☑.

## **Feedback**

Provide product feedback ☑

## Additional resources

**M** Training

Module

MD-102 2-Manage Microsoft Defender for Endpoint - Training

This module explores using Microsoft Defender for Endpoint to provide additional protection and monitor devices against threats.

Certification

#### Microsoft 365 Certified: Endpoint Administrator Associate - Certifications

Plan and execute an endpoint deployment strategy, using essential elements of modern management, comanagement approaches, and Microsoft Intune integration.