Contextual file and folder exclusions - Microsoft Defender for Endpoint

By chrisda

Archived: 2026-04-05 20:06:04 UTC

This article/section describes the contextual file and folder exclusions capability for Microsoft Defender Antivirus on Windows. This capability allows you to be more specific when you define under which context Microsoft Defender Antivirus shouldn't scan a file or folder, by applying restrictions.

Overview

Exclusions are primarily intended to mitigate affects on performance. They come at the penalty of reduced protection value. These restrictions allow you to limit this protection reduction by specifying circumstances under which the exclusion should apply. Contextual exclusions aren't suitable for addressing false positives in a reliable way. If you encounter a false positive, you can submit files for analysis through the Microsoft Defender portal (subscription required) or through the Microsoft Security Intelligence website. For a temporary suppression method, consider creating a custom *allow* indicator in Microsoft Defender for Endpoint.

There are four restrictions you can apply to limit the applicability of an exclusion:

- **File/folder path type restriction**. You can restrict exclusions to only apply if the target is a file, or a folder by making the intent specific. If the target is a file but the exclusion is specified to be a folder, the exclusion doesn't apply. Conversely, if the target is folder but the exclusion is specified to be a file, the exclusion applies.
- **Scan type restriction**. Enables you to define the required scan type for an exclusion to apply. For example, you only want to exclude a certain folder from Full scans but not from a "resource" scan (targeted scan).
- **Scan trigger type restriction**. You can use this restriction to specify that the exclusion should only apply when the scan is initiated by a specific event, such as:
    - on demand;
    - on access; or
    - originating from behavioral monitoring.
- **Process restriction**. Enables you to define that an exclusion should only apply when a file or folder is being accessed by a specific process.

Configuring restrictions

Restrictions are typically applied by adding the restriction type to the file or folder exclusion path.

Restriction	TypeName	value
File/folder	`PathType`	`file` `folder`
Scan type	`ScanType`	`quick` `full`

Scan trigger	`ScanTrigger`	`OnDemand`
		`OnAccess`
		`BM` (Behavior monitoring)

Process	`Process`	`<path>`

Important

TypeName and value keywords are case sensitive.

Requirements

This capability requires Microsoft Defender Antivirus.

- Platform version: **4.18.2205.7** or later
- Engine version: **1.1.19300.2** or later

See Microsoft Defender Antivirus security intelligence and product updates.

Syntax

As a starting point, you might already have exclusions in place that you wish to make more specific. To form the exclusion string, first define the path to the file or folder to be excluded, then add the type name and associated value, as shown in the following example.

```
<PATH>\:{TypeName:value,TypeName:value}
```

Keep in mind that *all* **types** and **values** are case sensitive.

Note

Conditions inside `{}` MUST be true for the restriction to match. For example, if you specify two scan triggers this cannot be true, and the exclusion will not apply. To specify two restrictions of the same type, create two separate exclusions.

Examples

The following string excludes `c:\documents\design.doc` only if it's a file and only in on-access scans:

```
c:\documents\design.doc\:{PathType:file,ScanTrigger:OnAccess}
```

The following string excludes `c:\documents\design.doc` only if it's scanned (on-access), due to it being accessed by a process having the image name `winword.exe` :

```
c:\documents\design.doc\:{Process:"winword.exe"}
```

File and folder paths can contain wildcards, as in the following example:

```
c:\*\*.doc\:{PathType:file,ScanTrigger:OnDemand}
```

The process image path can contain wildcards, as in the following example:

```
c:\documents\design.doc\:{Process:"C:\Program Files*\Microsoft Office\root\Office??\winword.exe"}
```

File/folder restriction

You can restrict exclusions to only apply if the target is a file or a folder by making the intent specific. If the target is a file but the exclusion is specified to be a folder, the exclusion doesn't apply. Conversely, if the target is folder but the exclusion is specified to be a file, the exclusion applies.

File/folder exclusions default behavior

If you don't specify any other options, the file/folder is excluded from all types of scans, *and* the exclusion applies regardless of whether the target is a file or a folder. For more information about customizing exclusions to only apply to a specific scan type, see Scan type restriction.

Note

Wildcards are supported in file/folder exclusions.

Folders

To ensure an exclusion only applies if the target is a folder, not a file you can use the **PathType:folder** restriction. For example:

```
C:\documents\*\:{PathType:folder}
```

Files

To make sure an exclusion only applies if the target is a file, not a folder you can use the PathType: file restriction. For example:

```
C:\documents\*.mdb\:{PathType:file}
```

Scan type restriction

By default, exclusions apply to all scan types:

- **resource**: a single file or folder is scanned in a targeted way (for example, right-click, Scan)

- **quick**: common startup locations utilized by malware, memory, and certain registry keys
- **full**: includes quick scan locations and complete file system (all files and folders)

To mitigate performance issues, you can exclude a folder or a set of files from being scanned by a specific scan type. You can also define the required scan type for an exclusion to apply.

To exclude a folder from being scanned only during a full scan, specify a restriction type together with the file or folder exclusion, as in the following example:

```
C:\documents\:{ScanType:full}
```

To exclude a folder from being scanned only during a quick scan, specify a restriction type together with the file or folder exclusion, as in the following example:

```
C:\program.exe\:{ScanType:quick}
```

If you want to make sure this exclusion only applies to a specific file and not a folder (c:\foo.exe could be a folder), also apply the `PathType` restriction, as in the following example:

```
C:\program.exe\:{ScanType:quick,PathType:file}
```

Scan trigger restriction

By default, basic exclusions apply to all scan triggers. ScanTrigger restriction enables you to specify that the exclusion should only apply when the scan was initiated by a specific event; on demand (including quick, full, and targeted scans), on access or originating from behavioral monitoring (including memory scans).

- **OnDemand**: a scan that's triggered by a command or admin action. Remember that scheduled quick and full scans also fall under this category.
- **OnAccess**: a file or folder is opened/written/read/modified (typically considered real-time protection)
- **BM**: a behavioral trigger causes the behavioral monitoring to scan a specific file

To exclude a file or folder and its contents from being scanned only when the file is being scanned after being accessed, define a scan trigger restriction such as the following example:

```
c:\documents\:{ScanTrigger:OnAccess}
```

Process restriction

This restriction allows you to define that an exclusion should only apply when a file or folder is being accessed by a specific process. A common scenario is when you want to avoid excluding the process as that avoidance would cause Defender Antivirus to ignore other operations by that process. Wildcards are supported in the process name/path.

Note

Using a large amount of process exclusion restrictions on a machine can adversely affect performance. In addition, if an exclusion is restricted to a certain process or processes, other active processes (such as indexing, backup,

updates) can still trigger file scans.

To exclude a file or folder only when accessed by a specific process, create a normal file or folder exclusion and add the process to restrict the exclusion to. For example:

```
c:\documents\design.doc\:{Process:"winword.exe", Process:"msaccess.exe", Process:"C:\Program Files*\Microsoft Office\root\Office??\winword.exe"}
```

How to configure

After constructing your desired contextual exclusions, you can use your existing management tool to configure file and folder exclusions using the string you created.

See Configure and validate exclusions for Microsoft Defender Antivirus scans.

See also

- Exclusions overview
- Common mistakes to avoid when defining exclusions
