Microsoft

Windows Defender Antivirus & Windows Defender Exploit Guard

Protection evaluation guide

Evaluate Windows Defender Antivirus and Windows Defender Exploit Guard in Windows 10

In Windows 10 you can use next-generation protection features offered by Windows Defender Antivirus (Windows Defender AV) and Windows Defender Exploit Guard (Windows Defender EG).

This topic explains how to enable and test the key protection features in Windows Defender AV and Windows Defender EG, and provides you with guidance and links to more information.

We recommend you use this evaluation PowerShell script to configure these features, but you can individually enable each feature with the cmdlets described in the rest of this document.

See the following product documentation libraries for more information about our EPP products:

- Windows Defender Antivirus
- Windows Defender Exploit Guard

This topic describes configuration options in Windows 10, version 1803. Some options may also be available in earlier versions of Windows 10, and may have slightly different names or titles.

If you have any questions about a detection that Windows Defender AV makes, or you discover a missed detection, you can submit a file to us at our sample submission help site.

Use PowerShell to enable the features

This guide provides the Windows Defender cmdlets that configure the features you should use to evaluate our protection.

To use these cmdlets:

1. Open an elevated instance of PowerShell (choose to **Run as administrator**).
2. Enter the command listed in this guide and press **Enter**.

You can check the status of all settings before you begin, or during your evaluation, by using the Get-MpPreference PowerShell cmdlet.

Windows Defender AV will indicate a detection through standard Windows notifications. You can also review detections in the Windows Defender AV app.

The Windows event log also records detection and engine events. See the Windows Defender Antivirus events topic for a list of event IDs and their corresponding actions.

Cloud protection features

Standard definition updates can take hours to prepare and deliver; our cloud-delievered protection service can deliver this protection in seconds.

More details are available in Use next-gen technologies in Windows Defender Antivirus through cloud-delivered protection.

Enable the Windows Defender Cloud for near-instant protection and increased protection:

```
Set-MpPreference -MAPSReporting Advanced
```

Automatically submit samples to increase group protection:

```
Set-MpPreference -SubmitSamplesConsent Always
```

Use the cloud to block new malware within seconds

```
Set-MpPreference -DisableBlockAtFirstSeen 0
```

Scan all downloaded files and attachments[1]

```
Set-MpPreference -DisableIOAVProtection 0
```

Set cloud block level to 'High'

```
Set-MpPreference -CloudBlockLevel High
```

Set cloud block timeout to 1 minute

```
Set-MpPreference -CloudExtendedTimeout 50
```

Always-on protection (real-time scanning)

Windows Defender AV scans files as soon as they are seen by Windows, and will monitor running processes for known or suspected malicious behaviors. If the antivirus engine discovers malicious modification, it will immediately block the process or file from running.

See Configure behavioral, heuristic, and real-time protection for more details on these options.

Constantly monitor files and processes for known malware modifications

```
Set-MpPreference -DisableRealtimeMonitoring 0
```

[1] Note, this setting is not honored in Mozilla Firefox

Constantly monitor for known malware behaviors – even in 'clean' files and running programs

```
Set-MpPreference -DisableBehaviorMonitoring 0
```

Scan scripts as soon as they are seen or run

```
Set-MpPreference -DisableScriptScanning 0
```

Scan removable drives as soon as they are inserted or mounted

```
Set-MpPreference -DisableRemovableDriveScanning 0
```

Potentially Unwanted Application protection

Potentially unwanted applications are files and apps that are not traditionally classified as malicious. These include third-party installers for common software, ad-injection and certain types of toolbars in your browser.

Prevent grayware, adware, and other potentially unwanted apps from installing

```
Set-MpPreference -PUAProtection Enabled
```

Email and archive scanning

You can set Windows Defender Antivirus to automatically scan certain types of email files and archive files (such as .zip files) when they are seen by Windows. More information about this feature can be found under the Manage email scans in Windows Defender topic.

Scan email files and archives

```
Set-MpPreference -DisableArchiveScanning 0
Set-MpPreference -DisableEmailScanning 0
```

Manage product and protection updates

Typically, you receive Windows Defender AV updates from Windows update once per day. However, you can increase the frequency of those updates by setting the following options, and ensuring that your updates are managed either in System Center Configuration Manager, with Group Policy, or in Intune.

Update signatures every day

```
Set-MpPreference -SignatureUpdateInterval 8
```

Check to update signatures before running a scheduled scan

```
Set-MpPreference -CheckForSignaturesBeforeRunningScan 1
```

Advanced threat and exploit mitigation and prevention Controlled folder access

Windows Defender Exploit Guard provides features that help protect devices from known malicious behaviors and attacks on vulnerable technologies.

Prevent malicious and suspicious apps (such as ransomware) from making changes to protected folders with Controlled folder access

```
Set-MpPreference -EnableControlledFolderAccess Enabled
```

Block connections to known bad IP addresses and other network connections with Network protection

```
Set-MpPreference -EnableNetworkProtection Enabled
```

Apply a standard set of mitigations with Exploit protection

```
Invoke-WebRequest
https://demo.wd.microsoft.com/Content/ProcessMitigation.xml -OutFile
ProcessMitigation.xml
Set-ProcessMitigation -PolicyFilePath ProcessMitigation.xml
```

Block known malicious attack vectors with Attack surface reduction

```
Add-MpPreference -AttackSurfaceReductionRules_Ids 75668C1F-73B5-4CF0-BB93-
3ECF5CB7CC84 -AttackSurfaceReductionRules_Actions Enabled
Add-MpPreference -AttackSurfaceReductionRules_Ids 3B576869-A4EC-4529-8536-
B80A7769E899 -AttackSurfaceReductionRules_Actions Enabled
Add-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB-401B-4EfC-AADC-
AD5F3C50688A -AttackSurfaceReductionRules_Actions Enabled
Add-MpPreference -AttackSurfaceReductionRules_Ids D3E037E1-3EB8-44C8-A917-
57927947596D -AttackSurfaceReductionRules_Actions Enabled
Add-MpPreference -AttackSurfaceReductionRules_Ids 5BEB7EFE-FD9A-4556801D-
275E5FFC04CC -AttackSurfaceReductionRules_Actions Enabled
Add-MpPreference -AttackSurfaceReductionRules_Ids BE9BA2D9-53EA-4CDC-84E5-
9B1EEEE46550 -AttackSurfaceReductionRules_Actions Enabled
Add-MpPreference -AttackSurfaceReductionRules_Ids 92E97FA1-2EDF-4476-BDD6-
9DD0B4DDDC7B -AttackSurfaceReductionRules_Actions Enabled
Add-MpPreference -AttackSurfaceReductionRules_Ids D1E49AAC-8F56-4280-B9BA-
993A6D77406C -AttackSurfaceReductionRules_Actions Enabled
Add-MpPreference -AttackSurfaceReductionRules_Ids B2B3F03D-6A65-4F7B-A9C7-
1C7EF74A9BA4 -AttackSurfaceReductionRules_Actions Enabled
Add-MpPreference -AttackSurfaceReductionRules_Ids C1DB55AB-C21A-4637-BB3F-
A12568109D35 -AttackSurfaceReductionRules_Actions Enabled
Add-MpPreference -AttackSurfaceReductionRules_Ids 01443614-CD74-433A-B99E-
2ECDC07BFC25 -AttackSurfaceReductionRules_Actions Enabled
```

Some rules may block behavior you find acceptable in your organization. In these cases, change the rule from **Enabled** to **Audit** to prevent unwanted blocks. For more information about audit mode, see Use audit mode to evaluate Windows Defender Exploit Guard features.

One-click Windows Defender Offline

Windows Defender Offline is a specialized tool that comes with Windows 10, and allows you to boot a machine into a dedicated environment outside of the normal operating system. It's especially useful for potent malware, such as rootkits.

See Windows Defender Offline in Windows 10 for more information on how this feature works.

Ensure notifications allow you to boot the PC into a specialized malware removal environment

```
Set-MpPreference -UILockdown 0
```

Resources

This section lists a number of resources that can assist you with evaluating Windows Defender Antivirus.

- Windows Defender in Windows 10 library
- Windows Defender for Windows Server 2016 library
- Windows 10 security library
- Windows 10 security overview
- Microsoft Malware Protection Center website – threat research and response
- Microsoft Malware Protection Center blog – threat research
- Ransomware protection in Windows 10 – whitepaper (PDF download)
- Microsoft Secure website
- Microsoft Secure blog