Attack surface reduction rules reference

Article • 05/02/2024

Applies to:

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

Platforms:

- Windows

This article provides information about Microsoft Defender for Endpoint attack surface reduction rules (ASR rules):

- ASR rules supported operating system versions
- ASR rules supported configuration management systems
- Per ASR rule alert and notification details
- ASR rule to GUID matrix
- ASR rule modes
- Per-rule-descriptions

> **Important**
>
> Some information in this article relates to a prereleased product which may be substantially modified before it's commercially released. Microsoft makes no warranties, expressed or implied, with respect to the information provided here.

> **Tip**
>
> As a companion to this article, see our **Microsoft Defender for Endpoint setup guide** to review best practices and learn about essential tools such as attack surface reduction and next-generation protection. For a customized experience based on your environment, you can access the Defender for **Endpoint automated setup guide** in the Microsoft 365 admin center.

Attack surface reduction rules by type

Attack surface reduction rules are categorized as one of two types:

- **Standard protection rules**: Are the minimum set of rules which Microsoft recommends you always enable, while you're evaluating the effect and configuration needs of the other ASR rules. These rules typically have minimal-to-no noticeable impact on the end user.
- **Other rules**: Rules that require some measure of following the documented deployment steps [Plan > Test (audit) > Enable (block/warn modes)], as documented in the Attack surface reduction rules deployment guide

For the easiest method to enable the standard protection rules, see: Simplified standard protection option.

Expand table

ASR rule name:	Standard protection rule?	Other rule?
Block abuse of exploited vulnerable signed drivers	Yes	
Block Adobe Reader from creating child processes		Yes
Block all Office applications from creating child processes		Yes

ASR rule name:	Standard protection rule?	Other rule?
Block credential stealing from the Windows local security authority subsystem (lsass.exe)	Yes	
Block executable content from email client and webmail		Yes
Block executable files from running unless they meet a prevalence, age, or trusted list criterion		Yes
Block execution of potentially obfuscated scripts		Yes
Block JavaScript or VBScript from launching downloaded executable content		Yes
Block Office applications from creating executable content		Yes
Block Office applications from injecting code into other processes		Yes
Block Office communication application from creating child processes		Yes
Block persistence through WMI event subscription	Yes	
Block process creations originating from PSExec and WMI commands		Yes
Block rebooting machine in Safe Mode (preview)		Yes
Block untrusted and unsigned processes that run from USB		Yes
Block use of copied or impersonated system tools (preview)		Yes
Block Webshell creation for Servers		Yes
Block Win32 API calls from Office macros		Yes
Use advanced protection against ransomware		Yes

Microsoft Defender Antivirus exclusions and ASR rules

Microsoft Defender Antivirus exclusions apply to some Microsoft Defender for Endpoint capabilities, such as some of the attack surface reduction rules.

The following ASR rules DO NOT honor Microsoft Defender Antivirus exclusions:

Expand table

ASR rules name:
Block Adobe Reader from creating child processes
Block process creations originating from PSExec and WMI commands
Block credential stealing from the Windows local security authority subsystem (lsass.exe)
Block Office applications from creating executable content
Block Office applications from injecting code into other processes
Block Office communication application from creating child processes

> **Note**
>
> For information about configuring per-rule exclusions, see the section titled **Configure ASR rules per-rule exclusions** in the topic Test attack surface reduction rules.

ASR rules and Defender for Endpoint Indicators of Compromise (IOC)

The following ASR rules DO NOT honor Microsoft Defender for Endpoint Indicators of Compromise (IOC):

Expand table

ASR rule name	Description
Block credential stealing from the Windows local security authority subsystem (lsass.exe)	Doesn't honor indicators of compromise for files or certificates.
Block Office applications from injecting code into other processes	Doesn't honor indicators of compromise for files or certificates.
Block Win32 API calls from Office macros	Doesn't honor indicators of compromise for certificates.

ASR rules supported operating systems

The following table lists the supported operating systems for rules that are currently released to general availability. The rules are listed alphabetical order in this table.

> **Note**
>
> Unless otherwise indicated, the minimum Windows 10 build is version 1709 (RS3, build 16299) or later; the minimum Windows Server build is version 1809 or later.

Attack surface reduction rules in Windows Server 2012 R2 and Windows Server 2016 are available for devices onboarded using the modern unified solution package. For more information, see New Windows Server 2012 R2 and 2016 functionality in the modern unified solution.

Expand table

Rule name	Windows 11 and Windows 10	Windows Server 2022 and Windows Server 2019	Windows Server	Windows Server 2016 [1, 2]	Windows Server 2012 R2 [1, 2]
Block abuse of exploited vulnerable signed drivers	Y	Y	Y version 1803 (Semi-Annual Enterprise Channel) or later	Y	Y
Block Adobe Reader from creating child processes	Y version 1809 or later [3]	Y	Y	Y	Y
Block all Office applications from creating child processes	Y	Y	Y	Y	Y
Block credential stealing from the Windows local security authority subsystem (lsass.exe)	Y version 1803 or later [3]	Y	Y	Y	Y
Block executable content from email client and webmail	Y	Y	Y	Y	Y
Block executable files from running unless they meet a prevalence, age, or	Y version 1803 or	Y	Y	Y	Y

Rule name	Windows 11 and Windows 10	Windows Server 2022 and Windows Server 2019	Windows Server	Windows Server 2016 [1, 2]	Windows Server 2012 R2 [1, 2]
trusted list criterion	later [3]				
Block execution of potentially obfuscated scripts	Y	Y	Y	Y	Y
Block JavaScript or VBScript from launching downloaded executable content	Y	Y	Y	N	N
Block Office applications from creating executable content	Y	Y	Y	Y	Y
Block Office applications from injecting code into other processes	Y	Y	Y	Y	Y
Block Office communication application from creating child processes	Y	Y	Y	Y	Y
Block persistence through Windows Management Instrumentation (WMI) event subscription	Y version 1903 (build 18362) or later [3]	Y	Y version 1903 (build 18362) or later	N	N
Block process creations originating from PSExec and WMI commands	Y version 1803 or later [3]	Y	Y	Y	Y
Block rebooting machine in Safe Mode (preview)	Y	Y	Y	Y	Y

Rule name	Windows 11 and Windows 10	Windows Server 2022 and Windows Server 2019	Windows Server	Windows Server 2016 [1, 2]	Windows Server 2012 R2 [1, 2]
Block untrusted and unsigned processes that run from USB	Y	Y	Y	Y	Y
Block use of copied or impersonated system tools (preview)	Y	Y	Y	Y	Y
Block Webshell creation for Servers	N	Y Exchange Role Only	Y Exchange Role Only	Y Exchange Role Only	Y Exchange Role Only
Block Win32 API calls from Office macros	Y	N	N	N	N
Use advanced protection against ransomware	Y version 1803 or later [3]	Y	Y	Y	Y

(1) Refers to the modern unified solution for Windows Server 2012 and 2016. For more information, see Onboard Windows Servers to the Defender for Endpoint service.

(2) For Windows Server 2016 and Windows Server 2012 R2, the minimum required version of Microsoft Endpoint Configuration Manager is version 2111.

(3) Version and build number apply only to Windows 10.

ASR rules supported configuration management systems

Links to information about configuration management system versions referenced in this table are listed below this table.

Expand table

Rule name	Microsoft Intune	Microsoft Endpoint Configuration Manager	Group Policy[1]	PowerShell[1]
Block abuse of exploited vulnerable signed drivers	Y		Y	Y
Block Adobe Reader from creating child processes	Y		Y	Y
Block all Office applications from creating child processes	Y	Y CB 1710	Y	Y
Block credential stealing from the Windows local security authority subsystem (lsass.exe)	Y	Y CB 1802	Y	Y
Block executable content from email client and webmail	Y	Y CB 1710	Y	Y
Block executable files from running unless they meet a prevalence, age, or trusted list criterion	Y	Y CB 1802	Y	Y
Block execution of potentially obfuscated scripts	Y	Y CB 1710	Y	Y
Block JavaScript or VBScript from launching downloaded executable content	Y	Y CB 1710	Y	Y

Rule name	Microsoft Intune	Microsoft Endpoint Configuration Manager	Group Policy[1]	PowerShell[1]
Block Office applications from creating executable content	Y	Y CB 1710	Y	Y
Block Office applications from injecting code into other processes	Y	Y CB 1710	Y	Y
Block Office communication application from creating child processes	Y	Y CB 1710	Y	Y
Block persistence through WMI event subscription	Y		Y	Y
Block process creations originating from PSExec and WMI commands	Y		Y	Y
Block rebooting machine in Safe Mode (preview)	Y		Y	Y
Block untrusted and unsigned processes that run from USB	Y	Y CB 1802	Y	Y
Block use of copied or impersonated system tools (preview)	Y		Y	Y
Block Webshell creation for Servers	Y		Y	Y
Block Win32 API calls from Office macros	Y	Y CB 1710	Y	Y

Rule name	Microsoft Intune	Microsoft Endpoint Configuration Manager	Group Policy[1]	PowerShell[1]
Use advanced protection against ransomware	Y	Y CB 1802	Y	Y

(1) You can configure attack surface reduction rules on a per-rule basis by using any rule's GUID.

- Configuration Manager CB 1710
- Configuration Manager CB 1802
- Microsoft Configuration Manager CB 1710
- System Center Configuration Manager (SCCM) CB 1710
  SCCM is now Microsoft Configuration Manager.

Per ASR rule alert and notification details

Toast notifications are generated for all rules in Block mode. Rules in any other mode don't generate toast notifications.

For rules with the "Rule State" specified:

- ASR rules with <ASR Rule, Rule State> combinations are used to surface alerts (toast notifications) on Microsoft Defender for Endpoint only for devices at cloud block level **High**. Devices not at High cloud block level won't generate alerts for any <ASR Rule, Rule State> combinations
- EDR alerts are generated for ASR rules in the specified states, for devices at cloud block level **High+**

Expand table

Rule name:	Rule state:	Generates alerts in EDR? (Yes | No)	Generates toast notifications? (Yes | No)
		*Only for devices at cloud block level **High**+*	*In Block mode only* and *only for devices at cloud block level **High***
Block abuse of exploited vulnerable signed drivers		N	Y
Block Adobe Reader from creating child processes	Block	Y	Y
Block all Office applications from creating child processes		N	Y
Block credential stealing from the Windows local security authority subsystem (lsass.exe)		N	Y
Block executable content from email client and webmail		Y	Y
Block executable files from running unless they meet a prevalence, age, or trusted list criterion		N	Y
Block execution of potentially obfuscated scripts	Audit | Block	Y | Y	N | Y
Block JavaScript or VBScript from launching downloaded executable content	Block	Y	Y
Block Office applications from creating executable content		N	Y
Block Office applications from injecting code into other processes		N	Y
Block Office communication application from creating child processes		N	Y
Block persistence through WMI event subscription	Audit |	Y | Y	N | Y

Rule name:	Rule state:	Generates alerts in EDR? (Yes | No)	Generates toast notifications? (Yes | No)
	Block		
Block process creations originating from PSExec and WMI commands		N	Y
Block rebooting machine in Safe Mode (preview)		N	N
Block untrusted and unsigned processes that run from USB	Audit | Block	Y | Y	N | Y
Block use of copied or impersonated system tools (preview)		N	N
Block Webshell creation for Servers		N	N
Block Win32 API calls from Office macros		N	Y
Use advanced protection against ransomware	Audit | Block	Y | Y	N | Y

ASR rule to GUID matrix

Expand table

Rule Name	Rule GUID
Block abuse of exploited vulnerable signed drivers	56a863a9-875e-4185-98a7-b882c64b5ce5
Block Adobe Reader from creating child processes	7674ba52-37eb-4a4f-a9a1-f0f9a1619a2c
Block all Office applications from creating child processes	d4f940ab-401b-4efc-aadc-ad5f3c50688a

Rule Name	Rule GUID
Block credential stealing from the Windows local security authority subsystem (lsass.exe)	9e6c4e1f-7d60-472f-ba1a-a39ef669e4b2
Block executable content from email client and webmail	be9ba2d9-53ea-4cdc-84e5-9b1eeee46550
Block executable files from running unless they meet a prevalence, age, or trusted list criterion	01443614-cd74-433a-b99e-2ecdc07bfc25
Block execution of potentially obfuscated scripts	5beb7efe-fd9a-4556-801d-275e5ffc04cc
Block JavaScript or VBScript from launching downloaded executable content	d3e037e1-3eb8-44c8-a917-57927947596d
Block Office applications from creating executable content	3b576869-a4ec-4529-8536-b80a7769e899
Block Office applications from injecting code into other processes	75668c1f-73b5-4cf0-bb93-3ecf5cb7cc84
Block Office communication application from creating child processes	26190899-1602-49e8-8b27-eb1d0a1ce869
Block persistence through WMI event subscription * File and folder exclusions not supported.	e6db77e5-3df2-4cf1-b95a-636979351e5b
Block process creations originating from PSExec and WMI commands	d1e49aac-8f56-4280-b9ba-993a6d77406c
Block rebooting machine in Safe Mode (preview)	33ddedf1-c6e0-47cb-833e-de6133960387
Block untrusted and unsigned processes that run from USB	b2b3f03d-6a65-4f7b-a9c7-1c7ef74a9ba4
Block use of copied or impersonated system tools (preview)	c0033c00-d16d-4114-a5a0-dc9b3a7d2ceb
Block Webshell creation for Servers	a8f5898e-1dc8-49a9-9878-85004b8a61e6
Block Win32 API calls from Office macros	92e97fa1-2edf-4476-bdd6-9dd0b4dddc7b
Use advanced protection against ransomware	c1db55ab-c21a-4637-bb3f-a12568109d35

ASR rule modes

- **Not configured** or **Disable**: The state in which the ASR rule isn't enabled or is disabled. The code for this state = 0.
- **Block**: The state in which the ASR rule is enabled. The code for this state is 1.
- **Audit**: The state in which the ASR rule is evaluated for the effect it would have on the organization or environment if enabled (set to block or warn). The code for this state is 2.
- **Warn** The state in which the ASR rule is enabled and presents a notification to the end-user, but permits the end-user to bypass the block. The code for this state is 6.

Warn mode is a block-mode type that alerts users about potentially risky actions. Users can choose to bypass the block warning message and allow the underlying action. Users can select **OK** to enforce the block, or select the bypass option - **Unblock** - through the end-user pop-up toast notification that is generated at the time of the block. After the warning is unblocked, the operation is allowed until the next time the warning message occurs, at which time the end-user will need to reperform the action.

When the allow button is clicked, the block is suppressed for 24 hours. After 24 hours, the end-user will need to allow the block again. The warn mode for ASR rules is only supported for RS5+ (1809+) devices. If bypass is assigned to ASR rules on devices with older versions, the rule will be in blocked mode.

You can also set a rule in warn mode via PowerShell by specifying the AttackSurfaceReductionRules_Actions as "Warn". For example:

PowerShell

```
Add-MpPreference -AttackSurfaceReductionRules_Ids 56a863a9-875e-4185-98a7-b882c64b5ce5 -
AttackSurfaceReductionRules_Actions Warn
```

Per rule descriptions

Block abuse of exploited vulnerable signed drivers

This rule prevents an application from writing a vulnerable signed driver to disk. In-the-wild, vulnerable signed drivers can be exploited by local applications - *that have sufficient privileges* - to gain access to the kernel. Vulnerable signed drivers enable attackers to disable or circumvent security solutions, eventually leading to system compromise.

The **Block abuse of exploited vulnerable signed drivers** rule doesn't block a driver already existing on the system from being loaded.

> **Note**
>
> You can configure this rule using Intune OMA-URI. See **Intune OMA-URI** for configuring custom rules.
>
> You can also configure this rule using **PowerShell**.
>
> To have a driver examined, use this Web site to **Submit a driver for analysis**.

Intune Name: `Block abuse of exploited vulnerable signed drivers`

Configuration Manager name: Not yet available

GUID: `56a863a9-875e-4185-98a7-b882c64b5ce5`

Advanced hunting action type:

- `AsrVulnerableSignedDriverAudited`
- `AsrVulnerableSignedDriverBlocked`

Block Adobe Reader from creating child processes

This rule prevents attacks by blocking Adobe Reader from creating processes.

Malware can download and launch payloads and break out of Adobe Reader through social engineering or exploits. By blocking child processes from being generated by Adobe Reader, malware attempting to use Adobe Reader as an attack vector are prevented from spreading.

Intune name: `Process creation from Adobe Reader (beta)`

Configuration Manager name: Not yet available

GUID: `7674ba52-37eb-4a4f-a9a1-f0f9a1619a2c`

Advanced hunting action type:

- `AsrAdobeReaderChildProcessAudited`
- `AsrAdobeReaderChildProcessBlocked`

Dependencies: Microsoft Defender Antivirus

Block all Office applications from creating child processes

This rule blocks Office apps from creating child processes. Office apps include Word, Excel, PowerPoint, OneNote, and Access.

Creating malicious child processes is a common malware strategy. Malware that abuses Office as a vector often runs VBA macros and exploit code to download and attempt to run more payloads. However, some legitimate line-of-business applications might also generate child processes for benign purposes; such as spawning a command prompt or using PowerShell to configure registry settings.

Intune name: `Office apps launching child processes`

Configuration Manager name: `Block Office application from creating child processes`

GUID: `d4f940ab-401b-4efc-aadc-ad5f3c50688a`

Advanced hunting action type:

- `AsrOfficeChildProcessAudited`
- `AsrOfficeChildProcessBlocked`

Dependencies: Microsoft Defender Antivirus

Block credential stealing from the Windows local security authority subsystem

This rule helps prevent credential stealing by locking down Local Security Authority Subsystem Service (LSASS).

LSASS authenticates users who sign in on a Windows computer. Microsoft Defender Credential Guard in Windows normally prevents attempts to extract credentials from LSASS. Some organizations can't enable Credential Guard on all of their computers because of compatibility issues with custom smartcard drivers or other programs that load into the Local Security Authority (LSA). In these cases, attackers can use tools like Mimikatz to scrape cleartext passwords and NTLM hashes from LSASS.

By default the state of this rule is set to block. In most cases, many processes make calls to LSASS for access rights that are not needed. For example, such as when the initial block from the ASR rule results in a subsequent call for a lesser privilege which subsequently succeeds. For information about the types of rights that are typically requested in process calls to LSASS, see: Process Security and Access Rights.

Enabling this rule doesn't provide additional protection if you have LSA protection enabled since the ASR rule and LSA protection work similarly. However, when LSA protection cannot be enabled, this rule can be configured to provide equivalent protection against malware that target `lsass.exe`.

> ⓘ **Note**

In this scenario, the ASR rule is classified as "not applicable" in Defender for Endpoint settings in the Microsoft Defender portal.

The *Block credential stealing from the Windows local security authority subsystem* ASR rule doesn't support WARN mode.

In some apps, the code enumerates all running processes and attempts to open them with exhaustive permissions. This rule denies the app's process open action and logs the details to the security event log. This rule can generate a lot of noise. If you have an app that simply enumerates LSASS, but has no real impact in functionality, there is no need to add it to the exclusion list. By itself, this event log entry doesn't necessarily indicate a malicious threat.

Intune name: `Flag credential stealing from the Windows local security authority subsystem`

Configuration Manager name: `Block credential stealing from the Windows local security authority subsystem`

GUID: `9e6c4e1f-7d60-472f-ba1a-a39ef669e4b2`

Advanced hunting action type:

- `AsrLsassCredentialTheftAudited`
- `AsrLsassCredentialTheftBlocked`

Dependencies: Microsoft Defender Antivirus

Block executable content from email client and webmail

This rule blocks email opened within the Microsoft Outlook application, or Outlook.com and other popular webmail providers from propagating the following file types:

- Executable files (such as .exe, .dll, or .scr)
- Script files (such as a PowerShell .ps1, Visual Basic .vbs, or JavaScript .js file)

Intune name: `Execution of executable content (exe, dll, ps, js, vbs, etc.) dropped from email (webmail/mail client) (no exceptions)`

Microsoft Configuration Manager name: `Block executable content from email client and webmail`

GUID: `be9ba2d9-53ea-4cdc-84e5-9b1eeee46550`

Advanced hunting action type:

- `AsrExecutableEmailContentAudited`
- `AsrExecutableEmailContentBlocked`

Dependencies: Microsoft Defender Antivirus

> **Note**
>
> The rule **Block executable content from email client and webmail** has the following alternative descriptions, depending on which application you use:
>
> - Intune (Configuration Profiles): Execution of executable content (exe, dll, ps, js, vbs, etc.) dropped from email (webmail/mail client) (no exceptions).
> - Configuration Manager: Block executable content download from email and webmail clients.
> - Group Policy: Block executable content from email client and webmail.

Block executable files from running unless they meet a prevalence, age, or trusted list criterion

This rule blocks executable files, such as .exe, .dll, or .scr, from launching. Thus, launching untrusted or unknown executable files can be risky, as it might not be initially clear if the files are malicious.

> **ⓘ Important**
>
> You must enable cloud-delivered protection to use this rule.
>
> The rule **Block executable files from running unless they meet a prevalence, age, or trusted list criterion** with GUID `01443614-cd74-433a-b99e-2ecdc07bfc25` is owned by Microsoft and is not specified by admins. This rule uses cloud-delivered protection to update its trusted list regularly.
>
> You can specify individual files or folders (using folder paths or fully qualified resource names) but you can't specify which rules or exclusions apply to.

Intune name: `Executables that don't meet a prevalence, age, or trusted list criteria`

Configuration Manager name: `Block executable files from running unless they meet a prevalence, age, or trusted list criteria`

GUID: `01443614-cd74-433a-b99e-2ecdc07bfc25`

Advanced hunting action type:

- `AsrUntrustedExecutableAudited`
- `AsrUntrustedExecutableBlocked`

Dependencies: Microsoft Defender Antivirus, Cloud Protection

Block execution of potentially obfuscated scripts

This rule detects suspicious properties within an obfuscated script.

> **Important**
>
> PowerShell scripts are now supported for the "Block execution of potentially obfuscated scripts" rule.

Script obfuscation is a common technique that both malware authors and legitimate applications use to hide intellectual property or decrease script loading times. Malware authors also use obfuscation to make malicious code harder to read, which hampers close scrutiny by humans and security software.

Intune name: `Obfuscated js/vbs/ps/macro code`

Configuration Manager name: `Block execution of potentially obfuscated scripts`

GUID: `5beb7efe-fd9a-4556-801d-275e5ffc04cc`

Advanced hunting action type:

- `AsrObfuscatedScriptAudited`
- `AsrObfuscatedScriptBlocked`

Dependencies: Microsoft Defender Antivirus, AntiMalware Scan Interface (AMSI)

Block JavaScript or VBScript from launching downloaded executable content

This rule prevents scripts from launching potentially malicious downloaded content. Malware written in JavaScript or VBScript often acts as a downloader to fetch and launch other malware from the Internet.

Although not common, line-of-business applications sometimes use scripts to download and launch installers.

Intune name: `js/vbs executing payload downloaded from Internet (no exceptions)`

Configuration Manager name: `Block JavaScript or VBScript from launching downloaded executable content`

GUID: `d3e037e1-3eb8-44c8-a917-57927947596d`

Advanced hunting action type:

- `AsrScriptExecutableDownloadAudited`
- `AsrScriptExecutableDownloadBlocked`

Dependencies: Microsoft Defender Antivirus, AMSI

Block Office applications from creating executable content

This rule prevents Office apps, including Word, Excel, and PowerPoint, from creating potentially malicious executable content, by blocking malicious code from being written to disk.

Malware that abuses Office as a vector might attempt to break out of Office and save malicious components to disk. These malicious components would survive a computer reboot and persist on the system. Therefore, this rule defends against a common persistence technique. This rule also blocks execution of untrusted files that may have been saved by Office macros that are allowed to run in Office files.

Intune name: `Office apps/macros creating executable content`

Configuration Manager name: `Block Office applications from creating executable content`

GUID: `3b576869-a4ec-4529-8536-b80a7769e899`

Advanced hunting action type:

- `AsrExecutableOfficeContentAudited`
- `AsrExecutableOfficeContentBlocked`

Dependencies: Microsoft Defender Antivirus, RPC

Block Office applications from injecting code into other processes

This rule blocks code injection attempts from Office apps into other processes.

> **Note**
>
> The Block applications from injecting code into other processes ASR rule does not support WARN mode.

> **Important**
>
> This rule requires restarting Microsoft 365 Apps (Office applications) for the configuration changes to take effect.

Attackers might attempt to use Office apps to migrate malicious code into other processes through code injection, so the code can masquerade as a clean process.

There are no known legitimate business purposes for using code injection.

This rule applies to Word, Excel, OneNote, and PowerPoint.

Intune name: `Office apps injecting code into other processes (no exceptions)`

Configuration Manager name: `Block Office applications from injecting code into other processes`

GUID: `75668c1f-73b5-4cf0-bb93-3ecf5cb7cc84`

Advanced hunting action type:

- `AsrOfficeProcessInjectionAudited`
- `AsrOfficeProcessInjectionBlocked`

Dependencies: Microsoft Defender Antivirus

Block Office communication application from creating child processes

This rule prevents Outlook from creating child processes, while still allowing legitimate Outlook functions.

This rule protects against social engineering attacks and prevents exploiting code from abusing vulnerabilities in Outlook. It also protects against Outlook rules and forms exploits that attackers can use when a user's credentials are compromised.

> **Note**
>
> This rule blocks DLP policy tips and ToolTips in Outlook. This rule applies to Outlook and Outlook.com only.

Intune name: `Process creation from Office communication products (beta)`

Configuration Manager name: Not available

GUID: `26190899-1602-49e8-8b27-eb1d0a1ce869`

Advanced hunting action type:

- `AsrOfficeCommAppChildProcessAudited`
- `AsrOfficeCommAppChildProcessBlocked`

Dependencies: Microsoft Defender Antivirus

Block persistence through WMI event subscription

This rule prevents malware from abusing WMI to attain persistence on a device.

> **Important**
>
> File and folder exclusions don't apply to this attack surface reduction rule.

Fileless threats employ various tactics to stay hidden, to avoid being seen in the file system, and to gain periodic execution control. Some threats can abuse the WMI repository and event model to stay hidden.

> **Note**
>
> If `CcmExec.exe` (SCCM Agent) is detected on the device, the ASR rule is classified as "not applicable" in Defender for Endpoint settings in the Microsoft Defender portal.

Intune name: `Persistence through WMI event subscription`

Configuration Manager name: Not available

GUID: `e6db77e5-3df2-4cf1-b95a-636979351e5b`

Advanced hunting action type:

- `AsrPersistenceThroughWmiAudited`
- `AsrPersistenceThroughWmiBlocked`

Dependencies: Microsoft Defender Antivirus, RPC

Block process creations originating from PSExec and WMI commands

This rule blocks processes created through PsExec and WMI from running. Both PsExec and WMI can remotely execute code. There's a risk of malware abusing functionality of PsExec and WMI for command and control purposes, or to spread an infection throughout an organization's network.

> ⚠ **Warning**
>
> Only use this rule if you're managing your devices with **Intune** or another MDM solution. This rule is incompatible with management through **Microsoft Endpoint Configuration Manager** because this rule blocks WMI commands the Configuration Manager client uses to function correctly.

Intune name: `Process creation from PSExec and WMI commands`

Configuration Manager name: Not applicable

GUID: `d1e49aac-8f56-4280-b9ba-993a6d77406c`

Advanced hunting action type:

- `AsrPsexecWmiChildProcessAudited`
- `AsrPsexecWmiChildProcessBlocked`

Dependencies: Microsoft Defender Antivirus

Block rebooting machine in Safe Mode (preview)

This rule prevents the execution of commands to restart machines in Safe Mode.

Safe Mode is a diagnostic mode that only loads the essential files and drivers needed for Windows to run. However, in Safe Mode, many security products are either disabled or operate in a limited capacity, which allows attackers to further launch tampering commands, or simply execute and encrypt all files on the machine. This rule blocks such attacks by preventing processes from restarting machines in Safe Mode.

> ⓘ **Note**
>
> This capability is currently in preview. Additional upgrades to improve efficacy are under development.

Intune Name: `[PREVIEW] Block rebooting machine in Safe Mode`

Configuration Manager name: Not yet available

GUID: `33ddedf1-c6e0-47cb-833e-de6133960387`

Dependencies: Microsoft Defender Antivirus

Block untrusted and unsigned processes that run from USB

With this rule, admins can prevent unsigned or untrusted executable files from running from USB removable drives, including SD cards. Blocked file types include executable files (such as .exe, .dll, or .scr)

> ⓘ **Important**

Files copied from the USB to the disk drive will be blocked by this rule if and when it's about to be executed on the disk drive.

Intune name: `Untrusted and unsigned processes that run from USB`

Configuration Manager name: `Block untrusted and unsigned processes that run from USB`

GUID: `b2b3f03d-6a65-4f7b-a9c7-1c7ef74a9ba4`

Advanced hunting action type:

- `AsrUntrustedUsbProcessAudited`
- `AsrUntrustedUsbProcessBlocked`

Dependencies: Microsoft Defender Antivirus

Block use of copied or impersonated system tools (preview)

This rule blocks the use of executable files that are identified as copies of Windows system tools. These files are either duplicates or impostors of the original system tools.

Some malicious programs may try to copy or impersonate Windows system tools to avoid detection or gain privileges. Allowing such executable files can lead to potential attacks. This rule prevents propagation and execution of such duplicates and impostors of the system tools on Windows machines.

> **Note**
>
> This capability is currently in preview. Additional upgrades to improve efficacy are under development.

Intune Name: `[PREVIEW] Block use of copied or impersonated system tools`

Configuration Manager name: Not yet available

GUID: `c0033c00-d16d-4114-a5a0-dc9b3a7d2ceb`

Dependencies: Microsoft Defender Antivirus

Block Webshell creation for Servers

This rule blocks web shell script creation on Microsoft Server, Exchange Role.

A web shell script is a specifically crafted script that allows an attacker to control the compromised server. A web shell may include functionalities such as receiving and executing malicious commands, downloading and executing malicious files, stealing and exfiltrating credentials and sensitive information, identifying potential targets etc.

Intune name: `Block Webshell creation for Servers`

GUID: `a8f5898e-1dc8-49a9-9878-85004b8a61e6`

Dependencies: Microsoft Defender Antivirus

Block Win32 API calls from Office macros

This rule prevents VBA macros from calling Win32 APIs.

Office VBA enables Win32 API calls. Malware can abuse this capability, such as calling Win32 APIs to launch malicious shellcode without writing anything directly to disk. Most organizations don't rely on the ability to call Win32 APIs in their day-to-day functioning, even if they use macros in other ways.

Intune name: `Win32 imports from Office macro code`

Configuration Manager name: `Block Win32 API calls from Office macros`

GUID: `92e97fa1-2edf-4476-bdd6-9dd0b4dddc7b`

Advanced hunting action type:

- `AsrOfficeMacroWin32ApiCallsAudited`
- `AsrOfficeMacroWin32ApiCallsBlocked`

Dependencies: Microsoft Defender Antivirus, AMSI

Use advanced protection against ransomware

This rule provides an extra layer of protection against ransomware. It uses both client and cloud heuristics to determine whether a file resembles ransomware. This rule doesn't block files that have one or more of the following characteristics:

- The file has already been found to be unharmful in the Microsoft cloud.
- The file is a valid signed file.
- The file is prevalent enough to not be considered as ransomware.

The rule tends to err on the side of caution to prevent ransomware.

> ⓘ **Note**
>
> You must enable cloud-delivered protection to use this rule.

Intune name: `Advanced ransomware protection`

Configuration Manager name: `Use advanced protection against ransomware`

GUID: `c1db55ab-c21a-4637-bb3f-a12568109d35`

Advanced hunting action type:

- `AsrRansomwareAudited`
- `AsrRansomwareBlocked`

Dependencies: Microsoft Defender Antivirus, Cloud Protection

See also

- Attack surface reduction rules deployment overview
- Plan attack surface reduction rules deployment
- Test attack surface reduction rules
- Enable attack surface reduction rules
- Operationalize attack surface reduction rules
- Attack surface reduction rules report
- Attack surface reduction rules reference
- Exclusions for Microsoft Defender for Endpoint and Microsoft Defender Antivirus

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

Feedback