Attack surface reduction rules reference - Microsoft Defender for Endpoint

By limwainstein

Archived: 2026-04-05 17:14:58 UTC

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.

Prerequisites

Supported operating systems

- Windows

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 effect 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.

ASR rule name	Standard protection rule?	Other rule?
Block abuse of exploited vulnerable signed drivers	Yes	
Block Adobe Reader from creating child processes[1]		Yes
Block all Office applications from creating child processes		Yes
Block credential stealing from the Windows local security authority subsystem (lsass.exe)[1] [2]	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[3]		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[1]		Yes
Block Office applications from injecting code into other processes[1] [2]		Yes
Block Office communication application from creating child processes[1]		Yes
Block persistence through WMI event subscription	Yes	
Block process creations originating from PSExec and WMI commands[1]		Yes
Block rebooting machine in Safe Mode		Yes
Block untrusted and unsigned processes that run from USB		Yes
Block use of copied or impersonated system tools		Yes
Block Webshell creation for Servers		Yes
Block Win32 API calls from Office macros[4]		Yes
Use advanced protection against ransomware		Yes

[1] This ASR rule doesn't honor Microsoft Defender Antivirus exclusions. For information about configuring ASR per-rule exclusions, see Configure attack surface reduction per-rule exclusions.

[2] This ASR rule doesn't honor Microsoft Defender for Endpoint Indicators of Compromise (IOC) for files or certificates.

[3] Currently, this ASR rule might not be available in the Intune Attack Surface Reduction policy configuration due to a known backend issue. But, the rule still exists and is available through other methods. For example, Microsoft Defender for Endpoint security settings management, Configuration Service Provider (CSP), Add-MpPreference, or existing Intune ASR policy configuration in rules created before the issue.

[4] This ASR rule doesn't honor Microsoft Defender for Endpoint Indicators of Compromise (IOC) 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.

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

Rule name	Windows 10 and 11	Windows Server version 1803, 2019, and later	Windows Server 2016 and 2012 R2
Block executable files from running unless they meet a prevalence, age, or trusted list criterion*	Y Windows 10 version 1803 or later	Y	Y
Block execution of potentially obfuscated scripts	Y	Y	Y
Block JavaScript or VBScript from launching downloaded executable content	Y	Y	N
Block Office applications from creating executable content	Y	Y	Y
Block Office applications from injecting code into other processes	Y	Y	Y
Block Office communication application from creating child processes	Y	Y	Y
Block persistence through Windows Management Instrumentation (WMI) event subscription	Y Windows 10 version 1903 (build 18362) or later	Y Windows 10 version 1903 (build 18362) or later	N
Block process creations originating from PSExec and WMI commands	Y Windows 10 version 1803 or later	Y	Y
Block rebooting machine in Safe Mode	Y	Y	Y
Block untrusted and unsigned processes that run from USB	Y	Y	Y
Block use of copied or impersonated system tools	Y	Y	Y

Rule name	Windows 10 and 11	Windows Server version 1803, 2019, and later	Windows Server 2016 and 2012 R2
Block Webshell creation for Servers	N	Y Exchange role only	Y on Windows Server 2016 Exchange role only N on Windows Server 2012 R2
Block Win32 API calls from Office macros	Y	N	N
Use advanced protection against ransomware	Y Windows 10 version 1803 or later	Y	Y

* Currently, this ASR rule might not be available in the Intune Attack Surface Reduction policy configuration due to a known backend issue. But, the rule still exists and is available through other methods. For example, Microsoft Defender for Endpoint security settings management, Configuration Service Provider (CSP), Add-MpPreference, or existing Intune ASR policy configuration in rules created before the issue).

Note

- For Windows Server 2012 R2 and Windows Server 2016, see Onboard Windows Server 2016 and Windows Server 2012 R2.
- If you're using Configuration Manager, the minimum required version of Microsoft Configuration Manager is version 2111 (December 2021).

ASR rules supported configuration management systems

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

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

* Currently, this ASR rule might not be available in the Intune Attack Surface Reduction policy configuration due to a known backend issue. But, the rule still exists and is available through other methods. For example, Microsoft Defender for Endpoint security settings management, Configuration Service Provider (CSP), Add-MpPreference, or existing Intune ASR policy configuration in rules created before the issue).

- 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 set at the cloud block level `High`.
- Devices that aren't set at the cloud block level `High` don't generate alerts for any `ASR Rule, Rule State` combinations.
- Endpoint Detection and Response (EDR) alerts are generated for ASR rules in the specified states, for devices set at the cloud block level `High+`.
- Toast notifications occur in block mode only and for devices set at the cloud block level `High`.

* Currently, this ASR rule might not be available in the Intune Attack Surface Reduction policy configuration due to a known backend issue. But, the rule still exists and is available through other methods. For example, Microsoft Defender for Endpoint security settings management, Configuration Service Provider (CSP), Add-MpPreference, or existing Intune ASR policy configuration in rules created before the issue).

ASR rule to GUID matrix

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
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

Rule Name	Rule GUID
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	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	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

* Currently, this ASR rule might not be available in the Intune Attack Surface Reduction policy configuration due to a known backend issue. But, the rule still exists and is available through other methods. For example, Microsoft Defender for Endpoint security settings management, Configuration Service Provider (CSP), Add-MpPreference, or existing Intune ASR policy configuration in rules created before the issue).

ASR rule modes

Rule mode	Code	Description
Not configured or **Disabled**	0	The ASR rule isn't enabled or is disabled.
Block	1	The ASR rule is enabled in block mode.
Audit	2	The ASR rule is evaluated for the effect on the environment if enabled in Block or Warn mode.
Warn	6	The ASR rule is enabled and presents a notification to the user, but the user can bypass the block.

Warn is a type of block that alerts users to potentially risky actions via a warning pop-up. Users can select **OK** to enforce the block, or select **Unblock** to bypass the block for the next 24 hours. After 24 hours, the user needs to allow the block again.

Warn mode for ASR rules is supported only in Windows 10 version 1809 or later. Older versions of Windows 10 with a Warn mode rule assigned are effectively in Block mode.

In PowerShell, you can create an ASR rule in warn mode by specifying the *AttackSurfaceReductionRules_Actions* parameter with the value `Warn`. For example:

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

Per rule descriptions

Block abuse of exploited vulnerable signed drivers

Note

To protect your environment from vulnerable drivers, you should first implement these methods:

- For Windows 10 or later, Windows Server 2016 or later using Microsoft App Control for Business, you should block all drivers by default and only allow drivers that you deem necessary and aren't known to be vulnerable.
- For Windows 8.1 or older, Windows Server 2012 R2 or older, using Microsoft AppLocker, you should block all drivers by default and only allow drivers that you deem necessary and aren't known to be vulnerable.
- For Windows 11 or later, and Windows Server core 1809 or later, or Windows Server 2019 or later, you should also enable Microsoft Windows vulnerable driver block list. Then, as another layer of defense, you should enable this attack surface reduction rule.

This rule prevents an application from writing a vulnerable signed driver to disk. In-the-wild, local applications *with sufficient privileges* can exploit vulnerable signed drivers 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.

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 Adobe Reader from generating child processes, 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. For example, 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

Note

If you have LSA protection enabled, this attack surface reduction rule isn't required. For a more secure posture, we also recommend enabling Credential Guard with the LSA protection.

If the LSA protection is enabled, the ASR rule is classified as *not applicable* in Defender for Endpoint management settings in the Microsoft Defender portal.

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. 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 *not configured* (disabled). In most cases, many processes make calls to LSASS for access rights that aren't needed. For example, when the initial block from the ASR rule results in a subsequent call for a lesser privilege that 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 extra protection if you have LSA protection enabled since the ASR rule and LSA protection work similarly. However, if you can't enable LSA protection, you can configure this rule to provide equivalent protection against malware that targets `lsass.exe`.

Tip

- ASR audit events don't generate toast notifications. The LSASS ASR rule produces large volume of audit events, almost all of which are safe to ignore when the rule is enabled in block mode. You can choose to skip the audit mode evaluation and proceed to block mode deployment. We recommend starting with a small set of devices and gradually expanding to cover the rest.
- The rule is designed to suppress block reports/toasts for friendly processes. It's also designed to drop reports for duplicate blocks. As such, the rule is well suited to be enabled in block mode, irrespective of whether toast notifications are enabled or disabled.
- ASR in warn mode is designed to present users with a block toast notification that includes an "Unblock" button. Due to the "safe to ignore" nature of LSASS ASR blocks and their large volume, WARN mode isn't

advisable for this rule (irrespective of whether toast notifications are enabled or disabled).
- This rule is designed to block the processes from accessing LSASS.EXE process memory. It doesn't block them from running. If you see processes like svchost.exe being blocked, it's only blocking from accessing LSASS process memory. Thus, svchost.exe and other processes can be safely ignored. The one exception is in the following known issues.

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 numerous noise. If you have an app that simply enumerates LSASS, but has no real effect in functionality, there's 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

Known issues: These applications and "Block credential stealing from the Windows local security authority subsystem" rule, are incompatible:

For technical support, contact the software publisher.

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)
- Archive files (such as .zip and others)

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

Tip

* Currently, this ASR rule might not be available in the Intune Attack Surface Reduction policy configuration due to a known backend issue. But, the rule still exists and is available through other methods. For example, Microsoft Defender for Endpoint security settings management, Configuration Service Provider (CSP), Add-MpPreference, or existing Intune ASR policy configuration in rules created before the issue).

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. This rule uses cloud-delivered protection to update its trusted list regularly. You can specify individual files or folders by using folder paths or fully qualified resource names. It also supports the **ASROnlyPerRuleExclusions** setting.

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.

Note

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

Important

You must enable cloud-delivered protection to use this 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, Anti-malware Scan Interface (AMSI), Cloud Protection

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 being used as a vector to persist malicious code on disk. Malware that abuses Office as a vector might attempt to save malicious components to disk that would survive a computer reboot and persist on the system. This rule defends against this persistence technique by blocking access (open/execute) to the code written to disk. This rule also blocks execution of untrusted files that might 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 don't 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

Known issues: These applications and "Block Office applications from injecting code into other processes" rule, are incompatible:

For technical support, contact the software publisher.

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.

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.

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 you're utilizing Configuration Manager (CM, previously known as MEMCM or SCCM) with `CcmExec.exe` (SCCM Agent), we recommend running it in audit mode for at least 60 days. Once you're prepared to switch to block mode, ensure you deploy the appropriate ASR rules, considering any necessary rule exclusions.

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 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

This rule prevents the execution of certain commands to restart machines in Safe Mode. In Safe Mode, many security products are either disabled or operate in a limited capacity. This effect allows attackers to further launch tampering commands, or execute and encrypt all files on the machine. This rule blocks abuse of Safe Mode by preventing commonly abused commands like `bcdedit` and `bootcfg` from restarting machines in Safe Mode. Safe Mode is still accessible manually from the Windows Recovery Environment.

Intune Name: `Block rebooting machine in Safe Mode`

Configuration Manager name: Not yet available

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

Advanced hunting action type:

- `AsrSafeModeRebootedAudited`
- `AsrSafeModeRebootBlocked`
- `AsrSafeModeRebootWarnBypassed`

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

This rule blocks files copied from the USB to the disk drive 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

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 might 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.

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

Configuration Manager name: Not yet available

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

Advanced hunting action type:

- `AsrAbusedSystemToolAudited`
- `AsrAbusedSystemToolBlocked`

- `AsrAbusedSystemToolWarnBypassed`

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 crafted script that allows an attacker to control the compromised server.

A web shell might include functionalities such as receiving and executing malicious commands, downloading and executing malicious files, stealing and exfiltrating credentials and sensitive information, and identifying potential targets.

Intune name: `Block Webshell creation for Servers`

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

Dependencies: Microsoft Defender Antivirus

Note

When you manage ASR rules using Microsoft Defender for Endpoint security settings management, you need to configure the **Block Webshell creation for Servers** setting as `Not Configured` in Group Policy or other local settings. If this rule is set to any other value (such as `Enabled` or `Disabled`), it could cause conflicts and prevent the policy from applying correctly through security settings management.

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 is 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.

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
- Troubleshoot attack surface reduction rules

Source: https://learn.microsoft.com/microsoft-365/security/defender-endpoint/attack-surface-reduction-rules-reference#block-execution-of-potentially-obfuscated-scripts