Enable attack surface reduction rules - Microsoft Defender for Endpoint

By limwainstein

Archived: 2026-04-05 23:51:26 UTC

Attack surface reduction rules help prevent actions that malware often abuses to compromise devices and networks. This article describes how to enable and configure attack surface reduction rules via:

- Microsoft Intune
- Mobile Device Management (MDM)
- Microsoft Configuration Manager
- Group policy (GP)
- PowerShell

To use the entire feature-set of attack surface reduction rules, the following requirements must be met:

- Microsoft Defender Antivirus must be set as the primary antivirus. It must not be running in passive mode or be disabled.
- Real-time protection must be on.
- Cloud-Delivery Protection must be on (some rules require Cloud Protection).
- You must have Cloud Protection network connectivity
- Recommended: Microsoft 365 E5

  Although attack surface reduction rules don't require a Microsoft 365 E5 license, it is recommended to use attack surface reduction rules with a Microsoft 365 E5 license (or similar licensing SKU) to take advantage of advanced management capabilities, including monitoring, analytics, and workflows available in Defender for Endpoint, as well as reporting and configuration capabilities in the Microsoft Defender XDR portal. While these advanced capabilities aren't available with an E3 license, with an E3 license you can still use Event Viewer to review attack surface reduction rule events.

  If you have another license, such as Windows Professional or Microsoft 365 E3 that doesn't include advanced monitoring and reporting capabilities, you can develop your own monitoring and reporting tools on top of the events that are generated at each endpoint when attack surface reduction rules are triggered (for example, Event Forwarding).

  To learn more about Windows licensing, see Windows 10 Licensing and get the Volume Licensing guide for Windows 10.

You can set attack surface reduction rules for devices that are running any of the following editions and versions of Windows:

- Windows 11 Pro
- Windows 11 Enterprise
- Windows 10 Pro, version 1709 or later
- Windows 10 Enterprise, version 1709 or later
- Windows Server, version 1803 (Semi-Annual Channel) or later
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022
- Windows Server 2025
- Azure Stack HCI OS, version 23H2 and later

Note

Some attack surface reduction rules are only enforced if Office executables are installed under the system-defined %ProgramFiles% or %ProgramFiles(x86)% directories (on most systems, %ProgramFiles% points to C:\Program Files). If Office is installed in a custom path outside one of these system-defined directories, these rules won't apply. The affected rules are:

- Block Office communication applications from creating child processes (26190899-1602-49e8-8b27-eb1d0a1ce869)
- Block all Office applications from creating child processes (D4F940AB-401B-4EFC-AADC-AD5F3C50688A)
- Block Office applications from injecting code into other processes (75668C1F-73B5-4CF0-BB93-3ECF5CB7CC84)

Each attack surface reduction rule contains one of four settings:

- **Not configured** or **Disabled**: Disable the attack surface reduction rule
- **Block**: Enable the attack surface reduction rule
- **Audit**: Evaluate how the attack surface reduction rule would impact your organization if enabled
- **Warn**: Enable the attack surface reduction rule but allow the end user to bypass the block

You can enable attack surface reduction rules by using any of the following methods:

- Microsoft Intune
- Mobile Device Management (MDM)
- Microsoft Configuration Manager
- Group policy (GP)
- PowerShell

Enterprise-level management such as Intune or Microsoft Configuration Manager is recommended. Enterprise-level management overwrites any conflicting group policy or PowerShell settings on startup.

You can exclude files and folders from being evaluated by most attack surface reduction rules. This means that even if an attack surface reduction rule determines the file or folder contains malicious behavior, it doesn't block the file from running.

Important

Excluding files or folders can severely reduce the protection provided by attack surface reduction rules. Excluded files are allowed to run, and no report or event are recorded. If attack surface reduction rules are detecting files that you believe shouldn't be detected, you should use audit mode first to test the rule. An exclusion is applied only when the excluded application or service starts. For example, if you add an exclusion for an update service that is already running, the update service continues to trigger events until the service is stopped and restarted.

When adding exclusions, keep these points in mind:

- Exclusions are typically based on individual files or folders (using folder paths or the full path of the file to be excluded).
- Exclusion paths can use environment variables and wildcards. See Use wildcards in the file name and folder path or extension exclusion lists
- When deployed through group policy, PowerShell, or Intune, you can configure exclusions for specific attack surface reduction rules. For Intune instructions, see Configure attack surface reduction rules per-rule exclusions.
- Exclusions can be added based on certificate and file hashes, by allowing specified Defender for Endpoint file and certificate indicators. See Overview of indicators.

If a conflicting policy is applied via MDM and GP, the setting applied from Group Policy takes precedence.

Attack surface reduction rules for managed devices support behavior for merging settings from different policies to create a policy superset for each device. Only the settings that aren't in conflict are merged, whereas policy conflicts aren't added to the superset of rules. Previously, if two policies included conflicts for a single setting, both policies were flagged as being in conflict, and no settings from either profile were deployed.

Attack surface reduction rule merge behavior works as follows:

- Attack surface reduction rules from the following profiles are evaluated for each device to which the rules apply:
    - **Devices** > **Configuration profiles** > **Endpoint protection profile** > **Microsoft Defender Exploit Guard** > **Attack Surface Reduction**. (See Attack Surface Reduction.)
    - **Endpoint security** > **Attack surface reduction policy** > **Attack surface reduction rules**. (See Attack surface reduction rules.)
    - **Endpoint security** > **Security baselines** > **Microsoft Defender ATP Baseline** > **Attack Surface Reduction Rules**. (See Microsoft Defender for Endpoint security baseline settings reference for Microsoft Intune.)
- Settings that don't have conflicts are added to a superset of policy for the device.

- When two or more policies have conflicting settings, the conflicting settings aren't added to the combined policy, while settings that don't conflict are added to the superset policy that applies to a device.
- Only the configurations for conflicting settings are held back.

This section provides configuration details for the following configuration methods:

- Intune
- Custom profile in Intune
- MDM
- Microsoft Configuration Manager
- Group policy
- PowerShell

The following procedures for enabling attack surface reduction rules include instructions for how to exclude files and folders.

1. Select **Endpoint Security** > **Attack surface reduction**. Choose an existing attack surface reduction rule or create a new one. To create a new one, select **Create Policy** and enter information for this profile. For **Profile type**, select **Attack surface reduction rules**. If you've chosen an existing profile, select **Properties** and then select **Settings**.
2. In the **Configuration settings** pane, select **Attack Surface Reduction** and then select the desired setting for each attack surface reduction rule.
3. Under **List of additional folders that need to be protected**, **List of apps that have access to protected folders**, and **Exclude files and paths from attack surface reduction rules**, enter individual files and folders.

   You can also select **Import** to import a CSV file that contains files and folders to exclude from attack surface reduction rules. Each line in the CSV file should be formatted as follows:

   `C:\folder`, `%ProgramFiles%\folder\file`, `C:\path`
4. Select **Next** on the three configuration panes, then select **Create** if you're creating a new policy or **Save** if you're editing an existing policy.

Note

In the latest Intune interface, **Configuration profiles** is located under **Devices > Configuration profiles**.
Earlier versions of Intune showed this under **Device configuration > Profiles**.
If you don't see "Configuration Profile" as written in older instructions, look for **Configuration profiles** under the Devices menu.

1. Select **Device configuration** > **Profiles**. Choose an existing endpoint protection profile or create a new one. To create a new one, select **Create profile** and enter information for this profile. For **Profile type**,

select **Endpoint protection**. If you've chosen an existing profile, select **Properties** and then select **Settings**.

2. In the **Endpoint protection** pane, select **Windows Defender Exploit Guard**, and then select **Attack Surface Reduction**. Select the desired setting for each attack surface reduction rule.

3. Under **Attack Surface Reduction exceptions**, enter individual files and folders. You can also select **Import** to import a CSV file that contains files and folders to exclude from attack surface reduction rules. Each line in the CSV file should be formatted as follows:

   `C:\folder`, `%ProgramFiles%\folder\file`, `C:\path`

4. Select **OK** on the three configuration panes. Then select **Create** if you're creating a new endpoint protection file or **Save** if you're editing an existing one.

You can use Microsoft Intune OMA-URI to configure custom attack surface reduction rules. The following procedure uses the rule Block abuse of exploited vulnerable signed drivers for the example.

1. In the Microsoft Intune admin center at https://intune.microsoft.com, select **Devices** > **Manage devices** > **Configuration**. Or, to go directly to the **Devices | Configuration** page, use https://intune.microsoft.com/#view/Microsoft_Intune_DeviceSettings/DevicesMenu/~/configuration.

2. On the **Policies** tab of the **Devices | Configuration** page, select **Create** > **New policy**.

   Screenshot of the Policies tab of the Devices - Configuration page in the Microsoft Intune admin center with Create selected.

3. In the **Create a profile** flyout that opens, configure the following settings:

   - **Platform**: Select **Windows 10 and later**.
   - **Profile type**: Select one of the following values:

     - **Templates**

       In the **Template name** section that appears, select **Custom**.

       or

     - If attack surface reduction rules are already set through Endpoint security, select **Settings Catalog**.

   When you're finished on the **Create a profile** flyout, select **Create**.

   The rule profile attributes in the Microsoft Intune admin center portal.

4. The Custom template tool opens to step **1 Basics**. In **1 Basics**, in **Name**, type a name for your template, and in **Description** you can type a description (optional).
   The basic attributes in the Microsoft Intune admin center portal

5. Click **Next**. Step **2 Configuration settings** opens. For OMA-URI Settings, click **Add**. Two options now appear: **Add** and **Export**.

   
   Screenshot showing the configuration settings in the Microsoft Intune admin center portal.

6. Click **Add** again. The **Add Row OMA-URI Settings** opens. In **Add Row**, fill in the following information:

   1. In **Name**, type a name for the rule.
   2. In **Description**, type a brief description.
   3. In **OMA-URI**, type or paste the specific OMA-URI link for the rule that you're adding. Refer to the MDM section in this article for the OMA-URI to use for this example rule. For attack surface reduction rule GUIDS, see Per rule descriptions.
   4. In **Value**, type or paste the GUID value, the `\=` sign and the State value with no spaces (`GUID=StateValue`):

      - `0` : Disable (Disable the attack surface reduction rule)
      - `1` : Block (Enable the attack surface reduction rule)
      - `2` : Audit (Evaluate how the attack surface reduction rule would impact your organization if enabled)
      - `6` : Warn (Enable the attack surface reduction rule but allow the end-user to bypass the block)

      
      The OMA URI configuration in the Microsoft Intune admin center portal.

7. Select **Save**. **Add Row** closes. In **Custom**, select **Next**. In step **3 Scope tags**, scope tags are optional. Do one of the following:

   - Select **Select Scope tags**, select the scope tag (optional) and then select **Next**.
   - Or select **Next**

8. In step **4 Assignments**, in **Included Groups**, for the groups that you want this rule to apply, select from the following options:

   - **Add groups**
   - **Add all users**
   - **Add all devices**

   
   The assignments in the Microsoft Intune admin center portal

9. In **Excluded groups**, select any groups that you want to exclude from this rule, and then select **Next**.

10. In step **5 Applicability Rules** for the following settings, do the following:

    1. In **Rule**, select either **Assign profile if**, or **Don't assign profile if**.

2. In **Property**, select the property to which you want this rule to apply.
3. In **Value**, enter the applicable value or value range.


The applicability rules in the Microsoft Intune admin center portal.

11. Select **Next**. In step **6 Review + create**, review the settings and information you've selected and entered, and then select **Create**.


Screenshot showing the Review and create option in the Microsoft Intune admin center portal.

Rules are active and live within minutes.

Note

Regarding conflict handling, if you assign a device two different attack surface reduction policies, potential policy conflicts can occur, depending on whether rules are assigned different states, whether conflict management is in place, and whether the result is an error.

Nonconflicting rules don't result in an error, and such rules are applied correctly. The first rule is applied, and subsequent nonconflicting rules are merged into the policy.

Use the ./Vendor/MSFT/Policy/Config/Defender/AttackSurfaceReductionRules configuration service provider (CSP) to individually enable and set the mode for each rule.

The following is a sample for reference, using GUID values for Attack surface reduction rules reference.

```
OMA-URI path: ./Vendor/MSFT/Policy/Config/Defender/AttackSurfaceReductionRules
```

```
Value: 75668c1f-73b5-4cf0-bb93-3ecf5cb7cc84=2|3b576869-a4ec-4529-8536-b80a7769e899=1|d4f940ab-401b-4efc-aadc-ad5f3c50688a=2|d3e037e1-3eb8-44c8-a917-57927947596d=1|5beb7efe-fd9a-4556-801d-275e5ffc04cc=0|be9ba2d9-53ea-4cdc-84e5-9b1eeee46550=1
```

The values to enable (Block), disable, warn, or enable in audit mode are:

- 0: Disable (Disable the attack surface reduction rule)
- 1: Block (Enable the attack surface reduction rule)
- 2: Audit (Evaluate how the attack surface reduction rule would impact your organization if enabled)
- 6: Warn (Enable the attack surface reduction rule but allow the end-user to bypass the block). Warn mode is available for most of the attack surface reduction rules.

Use the ./Vendor/MSFT/Policy/Config/Defender/AttackSurfaceReductionOnlyExclusions configuration service provider (CSP) to add exclusions.

Example:

```
OMA-URI path: ./Vendor/MSFT/Policy/Config/Defender/AttackSurfaceReductionOnlyExclusions
```

```
Value: c:\path|e:\path|c:\Exclusions.exe
```

Note

Be sure to enter OMA-URI values without spaces.

1. In Microsoft Configuration Manager, go to **Assets and Compliance** > **Endpoint Protection** > **Windows Defender Exploit Guard**.
2. Select **Home** > **Create Exploit Guard Policy**.
3. Enter a name and a description, select **Attack Surface Reduction**, and select **Next**.
4. Choose which rules will block or audit actions and select **Next**.
5. Review the settings and select **Next** to create the policy.
6. After the policy is created, select **Close**.

Warning

There's a known issue with the applicability of attack surface reduction on Server OS versions which is marked as compliant without any actual enforcement. Currently, there's no defined release date for when this will be fixed.

Important

If you're using "Disable admin merge" set to `true` on devices, and you're using any of the following tools/methods, adding ASR rules per-rule exclusions or local ASR rule exclusions don't apply:

- Defender for Endpoint Security Settings Management (Disable Local Admin Merge)
- Intune (Disable Local Admin Merge)
- The Defender CSP (**DisableLocalAdminMerge**)
- Group Policy (Configure local administrator merge behavior for lists) To modify this behavior, you need to change "Disable admin merge" to `false`.

Warning

If you manage your computers and devices with Intune, Configuration Manager, or other enterprise-level management platform, the management software overwrites any conflicting group policy settings on startup.

1. Open the Group Policy Management Console (GPMC) on your Group Policy management computer.
2. In the GPMC console tree, expand Group Policy Objects in the forest and domain containing the GPO that you want to edit.
3. Right-click on the GPO, and then select **Edit**.
4. In the **Group Policy Management Editor**, go to **Computer configuration** > **Administrative templates** > **Windows components** > **Microsoft Defender Antivirus** > **Microsoft Defender Exploit Guard** > **Attack Surface Reduction**.

5. In the details pane of **Attack Surface Reduction**, the available settings are:

    - Configure Attack Surface Reduction rules
    - Exclude files and paths from Attack surface reduction rules
    - Apply a list of exclusions to specific attack surface reduction (ASR) rules

    To open and configure an ASR rule setting, use any of the following methods:

    - Double-click on the setting.
    - Right-click on the setting, and then select **Edit**
    - Select the setting, and then select **Action** > **Edit**.

The available settings are described in the following subsections.

Important

Quotation marks aren't supported in any of the group policy values.

Don't use leading or trailing spaces in ASR rule IDs.

Microsoft renamed Windows Defender Antivirus to Microsoft Defender Antivirus beginning with Windows 10 version 2004 (May 2020). Group Policy paths on earlier versions of Windows might still reference Windows Defender Antivirus, while newer builds show Microsoft Defender Antivirus. Both names refer to the same policy location.

1. In the details pane of **Attack Surface Reduction**, open the **Configure Attack Surface Reduction rules** setting.

2. In the setting window that opens, configure the following options:

    1. Select **Enabled**.
    2. **Set the state for each ASR rule**: Select **Show...**.

3. In the **Set the state for each ASR rule** dialog that opens, configure the following settings:

    - **Value name**: Enter the GUID value of the ASR rule.
    - **Value**: Enter one of the following values:
        - 0: Off
        - 1: Block
        - 2: Audit
        - 5: Not configured
        - 6: Warn

    Screenshot of Configure Attack Surface Reduction rules in Group Policy.

    For more information, see ASR rule modes.

    Repeat this step as many times as necessary. When you're finished, select **OK**.

1. In the details pane of **Attack Surface Reduction**, open the **Exclude files and paths from Attack surface reduction rules** setting.

2. In the setting window that opens, configure the following options:

    1. Select **Enabled**.
    2. **Exclusions from ASR rules**: Select **Show...**.

3. In the **Exclusions from ASR rules** dialog that opens, configure the following settings:

    - **Value name**: Enter the GUID value of the ASR rule.
    - **Value**: Enter one of the following types of values:
        - To exclude all files in a folder, enter the full folder path. For example, `C:\Data\Test`.
        - To exclude a specific file in a specify folder (recommended), enter the path and filename. For example, `C:\Data\Test\test.exe`.

    Repeat this step as many times as necessary. When you're finished, select **OK**.

Note

If the **Apply a list of exclusions to specific attack surface reduction (ASR) rules** setting isn't available in your GPMC, you need version 24H2 or later of the Administrative Templates files in your Central Store.

1. In the details pane of **Attack Surface Reduction**, open the **Apply a list of exclusions to specific attack surface reduction (ASR) rules** setting.

2. In the setting window that opens, configure the following options:

    1. Select **Enabled**.
    2. **Exclusions for each ASR rule**: Select **Show...**.

3. In the **Exclusions for each ASR rule** dialog that opens, configure the following settings:

    - **Value name**: Enter the GUID value of the ASR rule.
    - **Value**: Enter one or more exclusions for the ASR rule. Use the syntax `Path1\ProcessName1>Path2ProcessName2>...PathNProcessNameN`. For example, `C:\Windows\Notepad.exe>c:\Windows\regedit.exe>C:\SomeFolder\test.exe`.

    Repeat this step as many times as necessary. When you're finished, select **OK**.

Warning

If you manage your computers and devices with Intune, Configuration Manager, or another enterprise-level management platform, the management software overwrites any conflicting PowerShell settings on startup.

1. Type **powershell** in the Start menu, right-click **Windows PowerShell** and select **Run as administrator**.

2. Type one of the following cmdlets. For more information, such as rule ID, refer to Attack surface reduction rules reference.

Task	PowerShell cmdlet
Enable attack surface reduction rules	`Set-MpPreference -AttackSurfaceReductionRules_Ids <rule ID> -AttackSurfaceReductionRules_Actions Enabled`
Enable attack surface reduction rules in audit mode	`Add-MpPreference -AttackSurfaceReductionRules_Ids <rule ID> -AttackSurfaceReductionRules_Actions AuditMode`
Enable attack surface reduction rules in warn mode	`Add-MpPreference -AttackSurfaceReductionRules_Ids <rule ID> -AttackSurfaceReductionRules_Actions Warn`
Enable attack surface reduction Block abuse of exploited vulnerable signed drivers	`Add-MpPreference -AttackSurfaceReductionRules_Ids 56a863a9-875e-4185-98a7-b882c64b5ce5 -AttackSurfaceReductionRules_Actions Enabled`
Turn off attack surface reduction rules	`Add-MpPreference -AttackSurfaceReductionRules_Ids <rule ID> -AttackSurfaceReductionRules_Actions Disabled`

Important

You must specify the state individually for each rule, but you can combine rules and states in a comma-separated list.

In the following example, the first two rules are enabled, the third rule is disabled, and the fourth rule is enabled in audit mode: `Set-MpPreference -AttackSurfaceReductionRules_Ids <rule ID 1>,<rule ID 2>,<rule ID 3>,<rule ID 4> -AttackSurfaceReductionRules_Actions Enabled, Enabled, Disabled, AuditMode`

You can also use the `Add-MpPreference` PowerShell verb to add new rules to the existing list.

Warning

`Set-MpPreference` overwrites the existing set of rules. If you want to add to the existing set, use `Add-MpPreference` instead. You can obtain a list of rules and their current state by using `Get-MpPreference`.

3. To exclude files and folders from attack surface reduction rules, use the following cmdlet:

```
Add-MpPreference -AttackSurfaceReductionOnlyExclusions "<fully qualified path or resource>"
```

Continue to use `Add-MpPreference -AttackSurfaceReductionOnlyExclusions` to add more files and folders to the list.

Important

Use `Add-MpPreference` to append or add apps to the list. Using the `Set-MpPreference` cmdlet will overwrite the existing list.

- Attack surface reduction rules reference
- Evaluate attack surface reduction
- Attack surface reduction FAQ
