CIS Microsoft Defender Antivirus Benchmark

v1.0.0 - 02-20-2026

Terms of Use

Please see the below link for our current terms of use:

https://www.cisecurity.org/cis-securesuite/cis-securesuite-membership-terms-of-use/

For information on referencing and/or citing CIS Benchmarks in 3rd party documentation (including using portions of Benchmark Recommendations) please contact CIS Legal (legalnotices@cisecurity.org) and request guidance on copyright usage.

NOTE: It is ***NEVER*** acceptable to host a CIS Benchmark in ***ANY*** format (PDF, etc.) on a 3rd party (non-CIS owned) site.

Table of Contents

Overview

All CIS Benchmarks™ (Benchmarks) focus on technical configuration settings used to maintain and/or increase the security of the addressed technology, and they should be used in **conjunction** with other essential cyber hygiene tasks like:

- Monitoring the base operating system and applications for vulnerabilities and quickly updating with the latest security patches.
- End-point protection (Antivirus software, Endpoint Detection and Response (EDR), etc.).
- Logging and monitoring user and system activity.

In the end, the Benchmarks are designed to be a key **component** of a comprehensive cybersecurity program.

Important Usage Information

All Benchmarks are available free for non-commercial use from the CIS Website. They can be used to manually assess and remediate systems and applications. In lieu of manual assessment and remediation, there are several tools available to assist with assessment:

- CIS Configuration Assessment Tool (CIS-CAT® Pro Assessor)
- CIS Benchmarks™ Certified 3rd Party Tooling

These tools make the hardening process much more scalable for large numbers of systems and applications.

NOTE: Some tooling focuses only on the Benchmark Recommendations that can be fully automated (skipping ones marked **Manual**). It is important that ***ALL*** Recommendations (**Automated** and **Manual**) be addressed since all are important for properly securing systems and are typically in scope for audits.

Key Stakeholders

Cybersecurity is a collaborative effort, and cross functional cooperation is imperative within an organization to discuss, test, and deploy Benchmarks in an effective and efficient way. The Benchmarks are developed to be best practice configuration guidelines applicable to a wide range of use cases. In some organizations, exceptions to specific Recommendations will be needed, and this team should work to prioritize the problematic Recommendations based on several factors like risk, time, cost, and labor. These exceptions should be properly categorized and documented for auditing purposes.

Apply the Correct Version of a Benchmark

Benchmarks are developed and tested for a specific set of products and versions and applying an incorrect Benchmark to a system can cause the resulting pass/fail score to be incorrect. This is due to the assessment of settings that do not apply to the target systems. To assure the correct Benchmark is being assessed:

- **Deploy the Benchmark applicable to the way settings are managed in the environment:** An example of this is the Microsoft Windows family of Benchmarks, which have separate Benchmarks for Group Policy, Intune, and Stand-alone systems based upon how system management is deployed. Applying the wrong Benchmark in this case will give invalid results.

- **Use the most recent version of a Benchmark**: This is true for all Benchmarks, but especially true for cloud technologies. Cloud technologies change frequently and using an older version of a Benchmark may have invalid methods for auditing and remediation.

Exceptions

The guidance items in the Benchmarks are called recommendations and not requirements, and exceptions to some of them are expected and acceptable. The Benchmarks strive to be a secure baseline, or starting point, for a specific technology, with known issues identified during Benchmark development are documented in the Impact section of each Recommendation. In addition, organizational, system specific requirements, or local site policy may require changes as well, or an exception to a Recommendation or group of Recommendations (e.g. A Benchmark could Recommend that a Web server not be installed on the system, but if a system's primary purpose is to function as a Webserver, there should be a documented exception to this Recommendation for that specific server).

In the end, exceptions to some Benchmark Recommendations are common and acceptable, and should be handled as follows:

- The reasons for the exception should be reviewed cross-functionally and be well documented for audit purposes.
- A plan should be developed for mitigating, or eliminating, the exception in the future, if applicable.
- If the organization decides to accept the risk of this exception (not work toward mitigation or elimination), this should be documented for audit purposes.

It is the responsibility of the organization to determine their overall security policy, and which settings are applicable to their unique needs based on the overall risk profile for the organization.

Remediation

CIS has developed Build Kits for many technologies to assist in the automation of hardening systems. Build Kits are designed to correspond to Benchmark's "Remediation" section, which provides the manual remediation steps necessary to make that Recommendation compliant to the Benchmark.

When remediating systems (changing configuration settings on deployed systems as per the Benchmark's Recommendations), please approach this with caution and test thoroughly.

The following is a reasonable remediation approach to follow:

- CIS Build Kits, or internally developed remediation methods should never be applied to production systems without proper testing.
- Proper testing consists of the following:
  - Understand the configuration (including installed applications) of the targeted systems. Various parts of the organization may need different configurations (e.g., software developers vs standard office workers).
  - Read the Impact section of the given Recommendation to help determine if there might be an issue with the targeted systems.
  - Test the configuration changes with representative lab system(s). If issues arise during testing, they can be resolved prior to deploying to any production systems.
  - When testing is complete, initially deploy to a small sub-set of production systems and monitor closely for issues. If there are issues, they can be resolved prior to deploying more broadly.
  - When the initial deployment above is completed successfully, iteratively deploy to additional systems and monitor closely for issues. Repeat this process until the full deployment is complete.

Summary

Using the Benchmarks Certified tools, working as a team with key stakeholders, being selective with exceptions, and being careful with remediation deployment, it is possible to harden large numbers of deployed systems in a cost effective, efficient, and safe manner.

NOTE: As previously stated, the PDF versions of the CIS Benchmarks™ are available for free, non-commercial use on the CIS Website. All other formats of the CIS Benchmarks™ (MS Word, Excel, and Build Kits) are available for CIS SecureSuite® members.

CIS-CAT® Pro is also available to CIS SecureSuite® members.

Target Technology Details

This document provides prescriptive guidance for establishing a secure configuration posture for **Microsoft Defender Antivirus**.

This secure configuration guide is based on **Microsoft Defender Antivirus** and is intended for all releases of the Microsoft Windows Operating Systems. This secure configuration guide was tested against **Microsoft Windows 11 Release 25H2 Enterprise** and **Microsoft Windows Server 2025 Enterprise** edition.

Ensure that the latest version of this benchmark is downloaded, as it contains new and updated group policy objects (GPO) released by Microsoft. To be certain that all new and updated GPOs are installed on the system, please download the latest version of the `ADMX/ADML` templates for **Microsoft Windows 11**. The newest version of the templates can be downloaded from Microsoft here: Download Administrative Templates (.admx) for Windows 11 2025 Update (25H2) from Official Microsoft Download Center.

Please note that all versions of the Windows OS, including Server, need the newest Windows 11 `ADMX/ADML` templates, as these templates contain all required GPOs for Benchmark compliance.

To obtain the latest version of this secure configuration guide, please visit the CIS Website or visit the CIS WorkBench Community. If you have questions, comments, or have identified ways to improve this guide, please write to us at feedback@cisecurity.org.

Intended Audience

The Microsoft Windows Benchmarks are written for **Active Directory domain-joined** systems using **Active Directory's Group Policy Manager** only. This benchmark is not intended for use on standalone or workgroup systems, systems joined to a cloud offering, such as Entra ID, or systems created, maintained, or used in the Cloud. This benchmark covers supported endpoint states for **Active Directory** and **Entra Hybrid joined** systems that receive policies from **Active Directory Group Policy Manager** only.

The Microsoft Defender Antivirus Benchmark includes settings available across the following Microsoft Defender Antivirus plans. If a recommendation falls outside the **Microsoft Defender Antivirus (Built-in, baseline protection)** plan, this will be noted within the recommendation.

- Microsoft Defender Antivirus (Built-in, baseline protection)
- Microsoft Defender for Endpoint Plan 1, (Foundational enterprise endpoint protection)
- Microsoft Defender for Business, (SMB-focused EDR, simplified)
- Microsoft Defender for Endpoint Plan 2, (Full enterprise EDR + XDR tier)

Consensus Guidance

This CIS Benchmark™ was created using a consensus review process comprised of a global community of subject matter experts. The process combines real world experience with data-based information to create technology specific guidance to assist users to secure their environments. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

Each CIS Benchmark undergoes two phases of consensus review. The first phase occurs during initial Benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the Benchmark. This discussion occurs until consensus has been reached on Benchmark recommendations. The second phase begins after the Benchmark has been published. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in the Benchmark. If you are interested in participating in the consensus process, please visit https://workbench.cisecurity.org/.

Typographical Conventions

The following typographical conventions are used throughout this guide:

Convention	Meaning
`Stylized Monospace font`	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
`Monospace font`	Used for inline code, commands, UI/Menu selections or examples. Text should be interpreted exactly as presented.
`<Monospace font in brackets>`	Text set in angle brackets denote a variable requiring substitution for a real value.
Italic font	Used to reference other relevant settings, CIS Benchmarks and/or Benchmark Communities. Also, used to denote the title of a book, article, or other publication.
Bold font	Additional information or caveats things like **Notes**, **Warnings**, or **Cautions** (usually just the word itself and the rest of the text normal).

Recommendation Definitions

The following defines the various components included in a CIS recommendation as applicable. If any of the components are not applicable it will be noted, or the component will not be included in the recommendation.

Title

Concise description for the recommendation's intended configuration.

Assessment Status

An assessment status is included for every recommendation. The assessment status indicates whether the given recommendation can be automated or requires manual steps to implement. Both statuses are equally important and are determined and supported as defined below:

Automated

Represents recommendations for which assessment of a technical control can be fully automated and validated to a pass/fail state. Recommendations will include the necessary information to implement automation.

Manual

Represents recommendations for which assessment of a technical control cannot be fully automated and requires all or some manual steps to validate that the configured state is set as expected. The expected state can vary depending on the environment.

Profile

A collection of recommendations for securing a technology or a supporting platform. Most benchmarks include at least a Level 1 and Level 2 Profile. Level 2 extends Level 1 recommendations and is not a standalone profile. The Profile Definitions section in the benchmark provides the definitions as they pertain to the recommendations included for the technology.

Description

Detailed information pertaining to the setting with which the recommendation is concerned. In some cases, the description will include the recommended value.

Rationale Statement

Detailed reasoning for the recommendation to provide the user a clear and concise understanding on the importance of the recommendation.

Impact Statement

Any security, functionality, or operational consequences that can result from following the recommendation.

Audit Procedure

Systematic instructions for determining if the target system complies with the recommendation.

Remediation Procedure

Systematic instructions for applying recommendations to the target system to bring it into compliance according to the recommendation.

Default Value

Default value for the given setting in this recommendation, if known. If not known, either not configured or not defined will be applied.

References

Additional documentation relative to the recommendation.

CIS Critical Security Controls® (CIS Controls®)

The mapping between a recommendation and the CIS Controls is organized by CIS Controls version, Safeguard, and Implementation Group (IG). The Benchmark in its entirety addresses the CIS Controls safeguards of (v7) “5.1 - Establish Secure Configurations” and (v8) '4.1 - Establish and Maintain a Secure Configuration Process” so individual recommendations will not be mapped to these safeguards.

Additional Information

Supplementary information that does not correspond to any other field but may be useful to the user.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1 - Workstation**

  This profile is for Corporate/Enterprise Environments and is considered general use.

  Items in this profile intend to:

  - be the starting baseline for most organizations;
  - be practical and prudent;
  - provide a clear security benefit; and
  - not inhibit the utility of the technology beyond acceptable means.

- **Level 2 - Workstation**

  This profile extends the Level 1 (L1) profile and is intended for High Security/Sensitive Data Environment with limited functionality.

  Items in this profile exhibit one or more of the following characteristics:

  - are intended for environments or use cases where security is more critical than manageability and usability;
  - may negatively inhibit the utility or performance of the technology; and
  - limit the ability of remote management/access.

  Note: Implementation of Level 2 requires that both Level 1 and Level 2 settings are applied.

- **Level 1 - Server**

  Items in this profile apply to Member Servers and Domain Controller and are intended to:

  - be practical and prudent;
  - provide a clear security benefit; and
  - not inhibit the utility of the technology beyond acceptable means.

- **Level 2 - Server**

  This profile extends the "Level 1 - Server" profile and are intended for Member Servers and Domain Controllers. Items in this profile exhibit one or more of the following characteristics:

  - are intended for environments or use cases where security is paramount
  - acts as defense in depth measure
  - may negatively inhibit the utility or performance of the technology

  Note: Implementation of Level 2 requires that both Level 1 and Level 2 settings are applied.

Acknowledgements

This Benchmark exemplifies the great things a community of users, vendors, and subject matter experts can accomplish through consensus collaboration. The CIS community thanks the entire consensus team with special recognition to the following individuals who contributed greatly to the creation of this guide:

The Center for Internet Security extends special recognition and thanks to Rick Munck, Hung Nguyen, and Carlos Mayol Berral from Microsoft for assisting in developing the configuration recommendations contained in this document.

Editor
Haemish Edgerton
Jennifer Jarose

Contributor
Matthias Dominick
Caleb Eifert
Martin Himken
Johannes Kristjansson
Aaron Margosis
James Robinson
Phil White
Matthew Woods
Justin Young
Kevin Zhang

Recommendations

1 Microsoft Defender Antivirus

This section contains recommendations related to Microsoft Defender Antivirus.

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Warning:

If using Group Policy to manage Microsoft Defender Antivirus settings, any changes made to tamper-protected settings are ignored. If changes must be made and those changes are blocked by tamper protection, use troubleshooting mode to temporarily disable tamper protection on the device.

After troubleshooting mode ends, any changes made to tamper-protected settings are reverted to their configured state. To change the values on tamper-protected settings permanently, disable tamper protection temporarily before turning it back on after the settings have changed. This method can pose security risks, and doesn't work on devices that are offline when tamper protection was temporarily disabled.

When tamper protection is turned on, the following tamper-protected settings can't be changed.

- Virus and threat protection remains enabled.
- Real-time protection remains turned on.
- Behavior monitoring remains turned on.
- Antivirus protection, including IOfficeAntivirus (IOAV) remains enabled.
- Cloud protection remains enabled.
- Security intelligence updates occur.
- Automatic actions are taken on detected threats.
- Notifications are visible in the Windows Security app on Windows devices.
- Archived files are scanned.
- Exclusions can't be modified or added

1.1 Client Interface

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

1.2 Device Control

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 11 Release 21H2 Administrative Templates (or newer).

1.3 Exclusions

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

1.4 Features

This section contains recommendations related to Features.

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 11 Release 22H2 Administrative Templates v1.0 (or newer).

1.4.1 Ensure 'Enable EDR in block mode' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Workstation
- Level 1 - Server

Description:

This policy setting controls whether Microsoft Defender Antivirus Endpoint Detection and Response (EDR) is enabled in block mode (passive remediation).

The recommended state for this setting is: `Enabled`.

Note: This setting is available with Microsoft Defender Antivirus platform release v4.18.2202.X and newer.

Rationale:

When Microsoft Defender Antivirus is not the primary antivirus product and is running in passive mode, EDR in block mode provides added protection against malicious artifacts.

Impact:

If Microsoft Defender Antivirus is running EDR will be enabled in block mode. If the system does not have Microsoft Defender Antivirus installed and running, then this setting will have no effect.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Features:PassiveRemediation
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Microsoft Defender Antivirus\Features\Enable EDR in block mode
```

Note: This Group Policy path is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 11 Release 24H2 Administrative Templates (or newer).

Default Value:

Disabled. (EDR will not run in block mode.)

References:

1. GRID: MS-00000598
2. https://learn.microsoft.com/en-us/defender-endpoint/edr-in-block-mode

Additional Information:

- Microsoft Defender Antivirus (Built-in, baseline protection)
- Microsoft Defender for Endpoint Plan 2, (Full enterprise EDR + XDR tier)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.1 Deploy and Maintain Anti-Malware Software Deploy and maintain anti-malware software on all enterprise assets.	●	●	●
v7	8.1 Utilize Centrally Managed Anti-malware Software Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.		●	●

1.5 MAPS

This section contains recommendations related to Microsoft Active Protection Service (MAPS).

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

1.5.1 Ensure 'Configure local setting override for reporting to Microsoft MAPS' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

This policy setting configures a local override for the configuration to join Microsoft Active Protection Service (MAPS), which Microsoft renamed to *Windows Defender Antivirus Cloud Protection Service* and then *Microsoft Defender Antivirus Cloud Protection Service*.

The recommended state for this setting is: `Disabled`.

Rationale:

The decision on whether to participate in Microsoft MAPS / Microsoft Defender Antivirus Cloud Protection Service for malicious software reporting should be made centrally in an enterprise managed environment, so that all computers within it behave consistently in that regard. Configuring this setting to Disabled ensures that the decision remains centrally managed.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows
Defender\Spynet:LocalSettingOverrideSpynetReporting
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Microsoft Defender Antivirus\MAPS\Configure local setting override
for reporting to Microsoft MAPS
```

Note: This Group Policy path is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Default Value:

Disabled. (Group Policy will take priority over the local preference setting.)

References:

1. https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/enable-cloud-protection-microsoft-defender-antivirus?view=o365-worldwide
2. GRID: MS-00000464

Additional Information:

- Microsoft Defender Antivirus (Built-in, baseline protection)
- Microsoft Defender for Endpoint Plan 1, (Foundational enterprise endpoint protection)
- Microsoft Defender for Endpoint Plan 2, (Full enterprise EDR + XDR tier)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

1.5.2 Ensure 'Configure the 'Block at First Sight' feature' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

This policy setting configures whether the device checks (in real time) with the Microsoft Active Protection Service (MAPS) before allowing certain content to be run or accessed.

The block at first sight feature works when Microsoft Defender Antivirus encounters a suspicious but undetected file. It then queries the Microsoft cloud protection backend and applies heuristics, machine learning, and automated analysis of the file to determine whether the files are malicious.

The recommended state for this setting is: `Enabled`.

Warning: This setting requires at least *Microsoft Defender for Endpoint Plan 1 (Foundational enterprise endpoint protection)* to function. If *Plan 1* is not in use, an exception to this recommendation is required.

Rationale:

Enabling the Block at First Sight feature enhances threat protection by using next-generation protection to detect new malware and block it within seconds.

Impact:

The block at first sight can block nonportable executable files (such as JS, VBS, or macros) and executable files, running the latest Defender antimalware platform on Windows or Windows Server.

Note: The block at first sight feature requires the following Group Policy settings to be configured to function.

- *Join Microsoft MAPS* must be `enabled`.
- *Send file samples when further analysis is required* should be set to `1 (Send safe samples)` or `3 (Send all samples)`
- *Scan all downloaded files* and attachments must be `enabled`.
- *Turn off real-time protection* must **NOT** be `enabled`.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows
Defender\Spynet:DisableBlockAtFirstSeen
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Microsoft Defender Antivirus\MAPS\Configure the 'Block at First
Sight' feature
```

Note: This Group Policy path is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

References:

1. https://learn.microsoft.com/en-us/defender-endpoint/configure-block-at-first-sight-microsoft-defender-antivirus
2. GRID: MS-00000639

Additional Information:

- Microsoft Defender for Endpoint Plan 1, (Foundational enterprise endpoint protection)
- Microsoft Defender for Endpoint Plan 2, (Full enterprise EDR + XDR tier)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.1 Deploy and Maintain Anti-Malware Software Deploy and maintain anti-malware software on all enterprise assets.	●	●	●
v7	8.1 Utilize Centrally Managed Anti-malware Software Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.		●	●

1.5.3 Ensure 'Join Microsoft MAPS' is set to 'Enabled: Advanced' (Automated)

Profile Applicability:

- Level 1 - Workstation
- Level 1 - Server

Description:

This policy setting configures Microsoft Active Protection Service (MAPS). Microsoft MAPS is designed to help Microsoft continually update and improve definitions of malware, spyware and other potentially unwanted software and to help Microsoft improve Windows Defender and related technologies.

The recommended state for this setting is: `Enabled: Advanced`.

Note: In Windows 10 and above, Basic membership is no longer available, so setting the value to `1` Basic, or `2` Advanced, enrolls the device into Advanced membership. For more information, please visit: Turn on cloud protection in Microsoft Defender Antivirus - Microsoft Defender for Endpoint | Microsoft Learn.

Rationale:

Cloud protection works with Microsoft Defender Antivirus to provide intelligent, real-time threat detection. Microsoft strongly recommends enabling cloud protection, as several advanced security features in Microsoft Defender for Endpoint rely on it to function properly. To fully take advantage of these protections, including several ASR rules, this setting must be enabled to allow for MAPS reporting.

Impact:

MAPS will send detailed information about malware and potentially unwanted software, including the full path to the software, and detailed information about how the software has affected the device.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `2`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Spynet:SpynetReporting
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: Advanced`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Microsoft Defender Antivirus\MAPS\Join Microsoft MAPS
```

Note: This Group Policy path is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Default Value:

Disabled. (Microsoft MAPS / Microsoft Defender Antivirus Cloud Protection Service will not be joined.)

References:

1. https://learn.microsoft.com/en-us/defender-endpoint/enable-cloud-protection-microsoft-defender-antivirus#use-group-policy-to-turn-on-cloud-protection
2. GRID: MS-00000465
3. https://learn.microsoft.com/en-us/defender-endpoint/enable-cloud-protection-microsoft-defender-antivirus

Additional Information:

- Microsoft Defender Antivirus (Built-in, baseline protection)
- Microsoft Defender for Endpoint Plan 1, (Foundational enterprise endpoint protection)
- Microsoft Defender for Endpoint Plan 2, (Full enterprise EDR + XDR tier)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

1.5.4 Ensure 'Send file samples when further analysis is required' is set to 'Enabled: Send safe samples automatically' or higher (Automated)

Profile Applicability:

- Level 1 - Workstation
- Level 1 - Server

Description:

This policy setting configures the behavior of samples sent to Microsoft for submission when opt-in for MAPS telemetry is set.

The recommended state for this setting is: `Enabled: Send safe samples` or `Enabled: Send all samples`.

Rationale:

For the *Block at First Sight* feature to function properly, the *Send file samples when further analysis is required* setting must be configured as prescribed.

Impact:

Submitting samples carries a small risk that sensitive information may be inadvertently included.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1` or `3`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Spynet:SubmitSamplesConsent
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: Send safe samples` or `Enabled: Send all samples`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Microsoft Defender Antivirus\MAPS\Send file samples when further
analysis is required
```

Note: This Group Policy path is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Default Value:

Not configured.

References:

1. GRID: MS-00000640

Additional Information:

- Microsoft Defender Antivirus (Built-in, baseline protection)
- Microsoft Defender for Endpoint Plan 1, (Foundational enterprise endpoint protection)
- Microsoft Defender for Endpoint Plan 2, (Full enterprise EDR + XDR tier)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.1 Deploy and Maintain Anti-Malware Software Deploy and maintain anti-malware software on all enterprise assets.	●	●	●
v7	8.1 Utilize Centrally Managed Anti-malware Software Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.		●	●

1.6 Microsoft Defender Exploit Guard

This section contains Microsoft Defender Exploit Guard settings.

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

Note: This section was originally named *Windows Defender Exploit Guard* but was renamed by Microsoft to *Microsoft Defender Exploit Guard* starting with the Microsoft Windows 10 Release 2004 Administrative Templates.

1.6.1 Attack Surface Reduction

This section contains Attack Surface Reduction settings.

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

1.6.1.1 Ensure 'Configure Attack Surface Reduction rules' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Workstation
- Level 1 - Server

Description:

This policy setting controls the state for the Attack Surface Reduction (ASR) rules.

The recommended state for this setting is: `Enabled`.

Rationale:

Attack surface reduction helps prevent actions and apps that are typically used by exploit-seeking malware to infect machines.

Impact:

When a rule is triggered, a notification will be displayed from the Action Center.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit
Guard\ASR:ExploitGuard_ASR_Rules
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Microsoft Defender Antivirus\Microsoft Defender Exploit
Guard\Attack Surface Reduction\Configure Attack Surface Reduction rules
```

Note: This Group Policy path is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

Default Value:

Disabled. (No ASR rules will be configured.)

References:

1. https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/enable-attack-surface-reduction?view=o365-worldwide
2. https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/attack-surface-reduction?view=o365-worldwide
3. GRID: MS-00000466

Additional Information:

- Microsoft Defender Antivirus (Built-in, baseline protection)
- Microsoft Defender for Endpoint Plan 1, (Foundational enterprise endpoint protection)
- Microsoft Defender for Endpoint Plan 2, (Full enterprise EDR + XDR tier)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 Enable Anti-Exploitation Features Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●
v7	8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		●	●

1.6.1.2 Ensure 'Configure Attack Surface Reduction rules: Set the state for each ASR rule' is set to '56a863a9-875e-4185-98a7-b882c64b5ce5:1' (Automated)

Profile Applicability:

- Level 1 - Workstation
- Level 1 - Server

Description:

This rule prevents an application from writing a vulnerable signed driver to disk.

Rule ID and name:

- `56a863a9-875e-4185-98a7-b882c64b5ce5` (Block abuse of exploited vulnerable signed drivers)

The recommended state for this setting is: `56a863a9-875e-4185-98a7-b882c64b5ce5:1` (Block).

Note: More information on ASR rules can be found at the following link: Use Attack surface reduction rules to prevent malware infection | Microsoft Docs

Note #2: The *Block abuse of exploited vulnerable signed drivers* setting does not block a driver that already exists on the system from being loaded.

Rationale:

Attack surface reduction helps prevent actions and apps that are typically used by exploit-seeking malware to infect systems.

Vulnerable signed drivers can be exploited by local applications that have sufficient privileges to gain access to the kernel. This enables threat actors to disable or circumvent security solutions, eventually leading to system compromise.

Impact:

When a rule is triggered, a notification will be displayed from the Action Center.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_SZ` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit
Guard\ASR\Rules:56a863a9-875e-4185-98a7-b882c64b5ce5
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `56a863a9-875e-4185-98a7-b882c64b5ce5` with a value of `1`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Microsoft Defender Antivirus\Microsoft Defender Exploit
Guard\Attack Surface Reduction\Configure Attack Surface Reduction rules: Set
the state for each ASR rule
```

Note: This Group Policy path is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

Default Value:

Disabled. (No ASR rules will be configured.)

References:

1. https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/enable-attack-surface-reduction?view=o365-worldwide
2. https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/attack-surface-reduction?view=o365-worldwide
3. GRID: MS-00000641

Additional Information:

- Microsoft Defender Antivirus (Built-in, baseline protection)
- Microsoft Defender for Endpoint Plan 1, (Foundational enterprise endpoint protection)
- Microsoft Defender for Endpoint Plan 2, (Full enterprise EDR + XDR tier)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 Enable Anti-Exploitation Features Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●
v7	8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		●	●

1.6.1.3 Ensure 'Configure Attack Surface Reduction rules: Set the state for each ASR rule' is set to '7674ba52-37eb-4a4f-a9a1-f0f9a1619a2c:1' (Automated)

Profile Applicability:

- Level 1 - Workstation
- Level 1 - Server

Description:

This rule blocks Adobe Reader from creating processes.

Rule ID and name:

- `7674ba52-37eb-4a4f-a9a1-f0f9a1619a2c` (Block Adobe Reader from creating child processes)

The recommended state for this setting is: `7674ba52-37eb-4a4f-a9a1-f0f9a1619a2c:1` (Block).

Note: More information on ASR rules can be found at the following link: Use Attack surface reduction rules to prevent malware infection | Microsoft Docs

Rationale:

Attack surface reduction helps prevent actions and apps that are typically used by exploit-seeking malware to infect machines.

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.

Impact:

When a rule is triggered, a notification will be displayed from the Action Center.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_SZ` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules:7674ba52-37eb-4a4f-a9a1-f0f9a1619a2c
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `7674ba52-37eb-4a4f-a9a1-f0f9a1619a2c` with a value of `1`:

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Microsoft Defender Exploit Guard\Attack Surface Reduction\Configure Attack Surface Reduction rules: Set the state for each ASR rule
```

Note: This Group Policy path is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

Default Value:

Disabled. (No ASR rules will be configured.)

References:

1. https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/enable-attack-surface-reduction?view=o365-worldwide
2. https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/attack-surface-reduction?view=o365-worldwide
3. GRID: MS-00000642

Additional Information:

- Microsoft Defender Antivirus (Built-in, baseline protection)
- Microsoft Defender for Endpoint Plan 1, (Foundational enterprise endpoint protection)
- Microsoft Defender for Endpoint Plan 2, (Full enterprise EDR + XDR tier)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 Enable Anti-Exploitation Features Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●
v7	8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		●	●

1.6.1.4 Ensure 'Configure Attack Surface Reduction rules: Set the state for each ASR rule' is set to 'd4f940ab-401b-4efc-aadc-ad5f3c50688a:2' or higher (Automated)

Profile Applicability:

- Level 1 - Workstation
- Level 1 - Server

Description:

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

Rule ID and name:

- `d4f940ab-401b-4efc-aadc-ad5f3c50688a` (Block all Office applications from creating child processes)

The recommended state for this setting is: `d4f940ab-401b-4efc-aadc-ad5f3c50688a:2` (Audit) or higher. Configuring this setting to `d4f940ab-401b-4efc-aadc-ad5f3c50688a:1` (Block) also conforms to the benchmark.

Note: More information on ASR rules can be found at the following link: Use Attack surface reduction rules to prevent malware infection | Microsoft Docs

Rationale:

Attack surface reduction helps prevent actions and apps that are typically used by exploit-seeking malware to infect machines.

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.

Impact:

When a rule is triggered, a notification will be displayed from the Action Center.

Warning: Prior to configuring this rule in `Block` mode, it should be enabled in `Audit` mode to verify that it does not introduce issues, especially for Microsoft Outlook.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_SZ` value of `2` or `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules:d4f940ab-401b-4efc-aadc-ad5f3c50688a
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `d4f940ab-401b-4efc-aadc-ad5f3c50688a` with a value of `2` or `1`:

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Microsoft Defender Exploit Guard\Attack Surface Reduction\Configure Attack Surface Reduction rules: Set the state for each ASR rule
```

Note: This Group Policy path is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

Default Value:

Disabled. (No ASR rules will be configured.)

References:

1. https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/enable-attack-surface-reduction?view=o365-worldwide
2. https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/attack-surface-reduction?view=o365-worldwide
3. GRID: MS-00000643

Additional Information:

- Microsoft Defender Antivirus (Built-in, baseline protection)
- Microsoft Defender for Endpoint Plan 1, (Foundational enterprise endpoint protection)
- Microsoft Defender for Endpoint Plan 2, (Full enterprise EDR + XDR tier)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 Enable Anti-Exploitation Features Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●
v7	8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		●	●

1.6.1.5 Ensure 'Configure Attack Surface Reduction rules: Set the state for each ASR rule' is set to '9e6c4e1f-7d60-472f-ba1a-a39ef669e4b2:1' (Automated)

Profile Applicability:

- Level 1 - Workstation
- Level 1 - Server

Description:

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

Rule ID and name:

- `9e6c4e1f-7d60-472f-ba1a-a39ef669e4b2` (Block credential stealing from the Windows local security authority subsystem (lsass.exe))

The recommended state for this setting is: `9e6c4e1f-7d60-472f-ba1a-a39ef669e4b2:1` (Block).

Note: More information on ASR rules can be found at the following link: Use Attack surface reduction rules to prevent malware infection | Microsoft Docs

Rationale:

Attack surface reduction helps prevent actions and apps that are typically used by exploit-seeking malware to infect machines.

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.

Impact:

When a rule is triggered, a notification will be displayed from the Action Center.

Note: Enabling this rule doesn't provide additional protection if LSA protection is 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`.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_SZ` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules:9e6c4e1f-7d60-472f-ba1a-a39ef669e4b2
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `9e6c4e1f-7d60-472f-ba1a-a39ef669e4b2` with a value of `1`:

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Microsoft Defender Exploit Guard\Attack Surface Reduction\Configure Attack Surface Reduction rules: Set the state for each ASR rule
```

Note: This Group Policy path is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

Default Value:

Disabled. (No ASR rules will be configured.)

References:

1. https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/enable-attack-surface-reduction?view=o365-worldwide
2. https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/attack-surface-reduction?view=o365-worldwide
3. GRID: MS-00000644

Additional Information:

- Microsoft Defender Antivirus (Built-in, baseline protection)
- Microsoft Defender for Endpoint Plan 1, (Foundational enterprise endpoint protection)
- Microsoft Defender for Endpoint Plan 2, (Full enterprise EDR + XDR tier)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 Enable Anti-Exploitation Features Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●
v7	8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		●	●

1.6.1.6 Ensure 'Configure Attack Surface Reduction rules: Set the state for each ASR rule' is set to 'be9ba2d9-53ea-4cdc-84e5-9b1eeee46550:1' (Automated)

Profile Applicability:

- Level 1 - Workstation
- Level 1 - Server

Description:

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)

Rule ID and name:

- `be9ba2d9-53ea-4cdc-84e5-9b1eeee46550` (Block executable content from email client and webmail)

The recommended state for this setting is: `be9ba2d9-53ea-4cdc-84e5-9b1eeee46550:1` (Block).

Note: More information on ASR rules can be found at the following link: Use Attack surface reduction rules to prevent malware infection | Microsoft Docs

Rationale:

Attack surface reduction helps prevent actions and apps that are typically used by exploit-seeking malware to infect machines.

Impact:

When a rule is triggered, a notification will be displayed from the Action Center.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_SZ` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules:be9ba2d9-53ea-4cdc-84e5-9b1eeee46550
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `be9ba2d9-53ea-4cdc-84e5-9b1eeee46550` with a value of `1`:

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Microsoft Defender Exploit Guard\Attack Surface Reduction\Configure Attack Surface Reduction rules: Set the state for each ASR rule
```

Note: This Group Policy path is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

Default Value:

Disabled. (No ASR rules will be configured.)

References:

1. https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/enable-attack-surface-reduction?view=o365-worldwide
2. https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/attack-surface-reduction?view=o365-worldwide
3. GRID: MS-00000645

Additional Information:

- Microsoft Defender Antivirus (Built-in, baseline protection)
- Microsoft Defender for Endpoint Plan 1, (Foundational enterprise endpoint protection)
- Microsoft Defender for Endpoint Plan 2, (Full enterprise EDR + XDR tier)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 Enable Anti-Exploitation Features Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●
v7	8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		●	●

1.6.1.7 Ensure 'Configure Attack Surface Reduction rules: Set the state for each ASR rule' is set to '01443614-cd74-433a-b99e-2ecdc07bfc25:2' or higher (Automated)

Profile Applicability:

- Level 1 - Workstation
- Level 1 - Server

Description:

This rule blocks executable files, such as .exe, .dll, or .scr, from launching.

Rule ID and name:

- `01443614-cd74-433a-b99e-2ecdc07bfc25` (Block executable files from running unless they meet a prevalence, age, or trusted list criterion)

The recommended state for this setting is: `01443614-cd74-433a-b99e-2ecdc07bfc25:2` (Audit) or higher. Configuring this setting to `01443614-cd74-433a-b99e-2ecdc07bfc25:1` (Block) also conforms to the benchmark.

Note: More information on ASR rules can be found at the following link: Use Attack surface reduction rules to prevent malware infection | Microsoft Docs

Note #2: Cloud-delivered protection must be enabled to use this rule.

Rationale:

Attack surface reduction helps prevent actions and apps that are typically used by exploit-seeking malware to infect machines.

Launching untrusted or unknown executable files can be risky, as it might not be initially clear if the files are malicious.

Organizations may find implementing `Block` to be too strict, however in `Audit` mode there is still valuable information that can be logged for threat hunters to sift through and analyze.

Impact:

When a rule is triggered, a notification will be displayed from the Action Center. To parse audit logs effectively an organization may need to implement a SIEM solution.

Warning: Prior to configuring this rule in `Block` mode, it should be enabled in `Audit` mode to verify that it does not introduce issues, especially for Microsoft Outlook. This rule **will** block legitimate programs.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_SZ` value of `2` or `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules:01443614-cd74-433a-b99e-2ecdc07bfc25
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `01443614-cd74-433a-b99e-2ecdc07bfc25` with a value of `2` or `1`:

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Microsoft Defender Exploit Guard\Attack Surface Reduction\Configure Attack Surface Reduction rules: Set the state for each ASR rule
```

Note: This Group Policy path is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

Default Value:

Disabled. (No ASR rules will be configured.)

References:

1. https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/enable-attack-surface-reduction?view=o365-worldwide
2. https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/attack-surface-reduction?view=o365-worldwide
3. GRID: MS-00000646

Additional Information:

- Microsoft Defender Antivirus (Built-in, baseline protection)
- Microsoft Defender for Endpoint Plan 1, (Foundational enterprise endpoint protection)
- Microsoft Defender for Endpoint Plan 2, (Full enterprise EDR + XDR tier)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 Enable Anti-Exploitation Features Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●
v7	8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		●	●

1.6.1.8 Ensure 'Configure Attack Surface Reduction rules: Set the state for each ASR rule' is set to '5beb7efe-fd9a-4556-801d-275e5ffc04cc:2' or higher (Automated)

Profile Applicability:

- Level 1 - Workstation
- Level 1 - Server

Description:

This rule detects suspicious properties within an obfuscated script.

Rule ID and name:

- `5beb7efe-fd9a-4556-801d-275e5ffc04cc` (Block execution of potentially obfuscated scripts)

The recommended state for this setting is: `5beb7efe-fd9a-4556-801d-275e5ffc04cc:2` (Audit). Configuring this setting to `5beb7efe-fd9a-4556-801d-275e5ffc04cc:1` (Block) also conforms to the benchmark.

Note: More information on ASR rules can be found at the following link: Use Attack surface reduction rules to prevent malware infection | Microsoft Docs

Rationale:

Attack surface reduction helps prevent actions and apps that are typically used by exploit-seeking malware to infect machines.

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.

Impact:

When a rule is triggered, a notification will be displayed from the Action Center.

Note: Cloud-delivered protection must be enabled to use this rule.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_SZ` value of `2` or `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules:5beb7efe-fd9a-4556-801d-275e5ffc04cc
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `5beb7efe-fd9a-4556-801d-275e5ffc04cc` with a value of `2` or `1`:

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Microsoft Defender Exploit Guard\Attack Surface Reduction\Configure Attack Surface Reduction rules: Set the state for each ASR rule
```

Note: This Group Policy path is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

Default Value:

Disabled. (No ASR rules will be configured.)

References:

1. https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/enable-attack-surface-reduction?view=o365-worldwide
2. https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/attack-surface-reduction?view=o365-worldwide
3. GRID: MS-00000647

Additional Information:

- Microsoft Defender Antivirus (Built-in, baseline protection)
- Microsoft Defender for Endpoint Plan 1, (Foundational enterprise endpoint protection)
- Microsoft Defender for Endpoint Plan 2, (Full enterprise EDR + XDR tier)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 Enable Anti-Exploitation Features Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●
v7	8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		●	●

1.6.1.9 Ensure 'Configure Attack Surface Reduction rules: Set the state for each ASR rule' is set to 'd3e037e1-3eb8-44c8-a917-57927947596d:1' (Automated)

Profile Applicability:

- Level 1 - Workstation
- Level 1 - Server

Description:

This rule prevents scripts from launching potentially malicious downloaded content.

Rule ID and name:

- `d3e037e1-3eb8-44c8-a917-57927947596d` (Block JavaScript or VBScript from launching downloaded executable content)

The recommended state for this setting is: `d3e037e1-3eb8-44c8-a917-57927947596d:1` (Block).

Note: More information on ASR rules can be found at the following link: Use Attack surface reduction rules to prevent malware infection | Microsoft Docs

Rationale:

Attack surface reduction helps prevent actions and apps that are typically used by exploit-seeking malware to infect machines.

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.

Impact:

When a rule is triggered, a notification will be displayed from the Action Center.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_SZ` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules:d3e037e1-3eb8-44c8-a917-57927947596d
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `d3e037e1-3eb8-44c8-a917-57927947596d` with a value of `1`:

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Microsoft Defender Exploit Guard\Attack Surface Reduction\Configure Attack Surface Reduction rules: Set the state for each ASR rule
```

Note: This Group Policy path is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

Default Value:

Disabled. (No ASR rules will be configured.)

References:

1. https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/enable-attack-surface-reduction?view=o365-worldwide
2. https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/attack-surface-reduction?view=o365-worldwide
3. GRID: MS-00000648

Additional Information:

- Microsoft Defender Antivirus (Built-in, baseline protection)
- Microsoft Defender for Endpoint Plan 1, (Foundational enterprise endpoint protection)
- Microsoft Defender for Endpoint Plan 2, (Full enterprise EDR + XDR tier)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 Enable Anti-Exploitation Features Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●
v7	8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		●	●

1.6.1.10 Ensure 'Configure Attack Surface Reduction rules: Set the state for each ASR rule' is set to '3b576869-a4ec-4529-8536-b80a7769e899:1' (Automated)

Profile Applicability:

- Level 1 - Workstation
- Level 1 - Server

Description:

This rule prevents Office apps, including Word, Excel, and PowerPoint, from being used as a vector to persist malicious code on disk.

Rule ID and name:

- `3b576869-a4ec-4529-8536-b80a7769e899` (Block Office applications from creating executable content)

The recommended state for this setting is: `3b576869-a4ec-4529-8536-b80a7769e899:1` (Block).

Note: More information on ASR rules can be found at the following link: Use Attack surface reduction rules to prevent malware infection | Microsoft Docs

Rationale:

Attack surface reduction helps prevent actions and apps that are typically used by exploit-seeking malware to infect machines.

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.

Impact:

When a rule is triggered, a notification will be displayed from the Action Center.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_SZ` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules:3b576869-a4ec-4529-8536-b80a7769e899
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `3b576869-a4ec-4529-8536-b80a7769e899` with a value of `1`:

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Microsoft Defender Exploit Guard\Attack Surface Reduction\Configure Attack Surface Reduction rules: Set the state for each ASR rule
```

Note: This Group Policy path is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

Default Value:

Disabled. (No ASR rules will be configured.)

References:

1. https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/enable-attack-surface-reduction?view=o365-worldwide
2. https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/attack-surface-reduction?view=o365-worldwide
3. GRID: MS-00000649

Additional Information:

- Microsoft Defender Antivirus (Built-in, baseline protection)
- Microsoft Defender for Endpoint Plan 1, (Foundational enterprise endpoint protection)
- Microsoft Defender for Endpoint Plan 2, (Full enterprise EDR + XDR tier)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 Enable Anti-Exploitation Features Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●
v7	8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		●	●

1.6.1.11 Ensure 'Configure Attack Surface Reduction rules: Set the state for each ASR rule' is set to '75668c1f-73b5-4cf0-bb93-3ecf5cb7cc84:1' (Automated)

Profile Applicability:

- Level 1 - Workstation
- Level 1 - Server

Description:

This rule blocks Office apps from injecting code into other processes. Office apps included in this setting are Word, Excel, PowerPoint, and OneNote.

Rule ID and name:

- `75668c1f-73b5-4cf0-bb93-3ecf5cb7cc84` (Block Office applications from injecting code into other processes)

The recommended state for this setting is: `75668c1f-73b5-4cf0-bb93-3ecf5cb7cc84:1` (Block).

Note: More information on ASR rules can be found at the following link: Use Attack surface reduction rules to prevent malware infection | Microsoft Docs

Rationale:

Attack surface reduction helps prevent actions and apps that are typically used by exploit-seeking malware to infect machines.

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.

Impact:

When a rule is triggered, a notification will be displayed from the Action Center.

Note: While Microsoft states that "there are no known legitimate business purposes for using code injection", this ASR will trigger on legitimate processes, so it is recommended to start in `Audit` mode before creating a list of exceptions and moving finally to `Block`.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_SZ` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules:75668c1f-73b5-4cf0-bb93-3ecf5cb7cc84
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `75668c1f-73b5-4cf0-bb93-3ecf5cb7cc84` with a value of `1`:

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Microsoft Defender Exploit Guard\Attack Surface Reduction\Configure Attack Surface Reduction rules: Set the state for each ASR rule
```

Note: This Group Policy path is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

Default Value:

Disabled. (No ASR rules will be configured.)

References:

1. https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/enable-attack-surface-reduction?view=o365-worldwide
2. https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/attack-surface-reduction?view=o365-worldwide
3. GRID: MS-00000650

Additional Information:

- Microsoft Defender Antivirus (Built-in, baseline protection)
- Microsoft Defender for Endpoint Plan 1, (Foundational enterprise endpoint protection)
- Microsoft Defender for Endpoint Plan 2, (Full enterprise EDR + XDR tier)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 Enable Anti-Exploitation Features Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●
v7	8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		●	●

1.6.1.12 Ensure 'Configure Attack Surface Reduction rules: Set the state for each ASR rule' is set to '26190899-1602-49e8-8b27-eb1d0a1ce869:2' or higher (Automated)

Profile Applicability:

- Level 1 - Workstation
- Level 1 - Server

Description:

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

Rule ID and name:

- `26190899-1602-49e8-8b27-eb1d0a1ce869` (Block Office communication application from creating child processes)

The recommended state for this setting is: `26190899-1602-49e8-8b27-eb1d0a1ce869:2` (Audit). Configuring this setting to `26190899-1602-49e8-8b27-eb1d0a1ce869:1` (Block) also conforms to the benchmark.

Note: More information on ASR rules can be found at the following link: Use Attack surface reduction rules to prevent malware infection | Microsoft Docs

Rationale:

This ASR 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.

Impact:

This rule will block DLP policy tips and ToolTips in Outlook and applies to Outlook and Outlook.com only.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_SZ` value of `2` or `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules:26190899-1602-49e8-8b27-eb1d0a1ce869
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `26190899-1602-49e8-8b27-eb1d0a1ce869` with a value of `2` or `1`:

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Microsoft Defender Exploit Guard\Attack Surface Reduction\Configure Attack Surface Reduction rules: Set the state for each ASR rule
```

Note: This Group Policy path is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

Default Value:

Disabled. (No ASR rules will be configured.)

References:

1. https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/enable-attack-surface-reduction?view=o365-worldwide
2. https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/attack-surface-reduction?view=o365-worldwide
3. GRID: MS-00000651

Additional Information:

- Microsoft Defender Antivirus (Built-in, baseline protection)
- Microsoft Defender for Endpoint Plan 1, (Foundational enterprise endpoint protection)
- Microsoft Defender for Endpoint Plan 2, (Full enterprise EDR + XDR tier)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 Enable Anti-Exploitation Features Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●
v7	8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		●	●

1.6.1.13 Ensure 'Configure Attack Surface Reduction rules: Set the state for each ASR rule' is set to 'e6db77e5-3df2-4cf1-b95a-636979351e5b:1' (Automated)

Profile Applicability:

- Level 1 - Workstation
- Level 1 - Server

Description:

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

Rule ID and name:

- `e6db77e5-3df2-4cf1-b95a-636979351e5b` (Block persistence through WMI event subscription)

The recommended state for this setting is: `e6db77e5-3df2-4cf1-b95a-636979351e5b:1` (Block).

Note: More information on ASR rules can be found at the following link: Use Attack surface reduction rules to prevent malware infection | Microsoft Docs

Note #2: 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.

Rationale:

Attack surface reduction helps prevent actions and apps that are typically used by exploit-seeking malware to infect machines.

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.

Impact:

When a rule is triggered, a notification will be displayed from the Action Center.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_SZ` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules:e6db77e5-3df2-4cf1-b95a-636979351e5b
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `e6db77e5-3df2-4cf1-b95a-636979351e5b` with a value of `1`:

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Microsoft Defender Exploit Guard\Attack Surface Reduction\Configure Attack Surface Reduction rules: Set the state for each ASR rule
```

Note: This Group Policy path is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

Default Value:

Disabled. (No ASR rules will be configured.)

References:

1. https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/enable-attack-surface-reduction?view=o365-worldwide
2. https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/attack-surface-reduction?view=o365-worldwide
3. GRID: MS-00000652

Additional Information:

- Microsoft Defender Antivirus (Built-in, baseline protection)
- Microsoft Defender for Endpoint Plan 1, (Foundational enterprise endpoint protection)
- Microsoft Defender for Endpoint Plan 2, (Full enterprise EDR + XDR tier)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 Enable Anti-Exploitation Features Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●
v7	8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		●	●

1.6.1.14 Ensure 'Configure Attack Surface Reduction rules: Set the state for each ASR rule' is set to '33ddedf1-c6e0-47cb-833e-de6133960387:1' (Automated)

Profile Applicability:

- Level 1 - Workstation
- Level 1 - Server

Description:

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

Rule ID and name:

- `33ddedf1-c6e0-47cb-833e-de6133960387` (Block rebooting machine in Safe Mode)

The recommended state for this setting is: `33ddedf1-c6e0-47cb-833e-de6133960387:1` (Block).

Note: More information on ASR rules can be found at the following link: Use Attack surface reduction rules to prevent malware infection | Microsoft Docs

Note #2: Safe Mode is still accessible manually from the Windows Recovery Environment.

Rationale:

Attack surface reduction helps prevent actions and apps that are typically used by exploit-seeking malware to infect machines.

When a system is in Safe Mode, many security controls are disabled or operate with reduced functionality, which can allow attackers to execute tampering commands or encrypt files. This rule mitigates that risk by blocking commonly abused commands, such as 'bcdedit' and 'bootcfg', that are used to restart systems into Safe Mode.

Impact:

The system will not start in Safe Mode when using commands such as 'bcdedit' and 'bootcfg'.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_SZ` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules:33ddedf1-c6e0-47cb-833e-de6133960387
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `33ddedf1-c6e0-47cb-833e-de6133960387` with a value of `1`:

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Microsoft Defender Exploit Guard\Attack Surface Reduction\Configure Attack Surface Reduction rules: Set the state for each ASR rule
```

Note: This Group Policy path is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

Default Value:

Disabled. (No ASR rules will be configured.)

References:

1. https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/enable-attack-surface-reduction?view=o365-worldwide
2. https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/attack-surface-reduction?view=o365-worldwide
3. GRID: MS-00000653

Additional Information:

- Microsoft Defender Antivirus (Built-in, baseline protection)
- Microsoft Defender for Endpoint Plan 1, (Foundational enterprise endpoint protection)
- Microsoft Defender for Endpoint Plan 2, (Full enterprise EDR + XDR tier)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 Enable Anti-Exploitation Features Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●
v7	8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		●	●

1.6.1.15 Ensure 'Configure Attack Surface Reduction rules: Set the state for each ASR rule' is set to 'b2b3f03d-6a65-4f7b-a9c7-1c7ef74a9ba4:1' (Automated)

Profile Applicability:

- Level 1 - Workstation
- Level 1 - Server

Description:

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).

Rule ID and name:

- `b2b3f03d-6a65-4f7b-a9c7-1c7ef74a9ba4` (Block untrusted and unsigned processes that run from USB)

The recommended state for this setting is: `b2b3f03d-6a65-4f7b-a9c7-1c7ef74a9ba4:1` (Block).

Note: More information on ASR rules can be found at the following link: Use Attack surface reduction rules to prevent malware infection | Microsoft Docs

Rationale:

Attack surface reduction helps prevent actions and apps that are typically used by exploit-seeking malware to infect machines.

Impact:

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_SZ` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules:b2b3f03d-6a65-4f7b-a9c7-1c7ef74a9ba4
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `b2b3f03d-6a65-4f7b-a9c7-1c7ef74a9ba4` with a value of `1`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Microsoft Defender Antivirus\Microsoft Defender Exploit
Guard\Attack Surface Reduction\Configure Attack Surface Reduction rules: Set
the state for each ASR rule
```

Note: This Group Policy path is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

Default Value:

Disabled. (No ASR rules will be configured.)

References:

1. https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/enable-attack-surface-reduction?view=o365-worldwide
2. https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/attack-surface-reduction?view=o365-worldwide
3. GRID: MS-00000654

Additional Information:

- Microsoft Defender Antivirus (Built-in, baseline protection)
- Microsoft Defender for Endpoint Plan 1, (Foundational enterprise endpoint protection)
- Microsoft Defender for Endpoint Plan 2, (Full enterprise EDR + XDR tier)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 Enable Anti-Exploitation Features Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●
v7	8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		●	●

1.6.1.16 Ensure 'Configure Attack Surface Reduction rules: Set the state for each ASR rule' is set to '92e97fa1-2edf-4476-bdd6-9dd0b4dddc7b:1' (Automated)

Profile Applicability:

- Level 1 - Workstation

Description:

This rule prevents VBA macros from calling Win32 APIs. Office VBA enables Win32 API calls.

Rule ID and name:

- `92e97fa1-2edf-4476-bdd6-9dd0b4dddc7b` (Block Win32 API calls from Office macros)

The recommended state for this setting is: `92e97fa1-2edf-4476-bdd6-9dd0b4dddc7b:1` (Block).

Note: More information on ASR rules can be found at the following link: Use Attack surface reduction rules to prevent malware infection | Microsoft Docs

Rationale:

Attack surface reduction helps prevent actions and apps that are typically used by exploit-seeking malware to infect machines.

Malware can abuse VBA macro calls with various methods, 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.

Impact:

Files copied from the USB to the disk drive can be blocked by this setting.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_SZ` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules:92e97fa1-2edf-4476-bdd6-9dd0b4dddc7b
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `92e97fa1-2edf-4476-bdd6-9dd0b4dddc7b` with a value of `1`:

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Microsoft Defender Exploit Guard\Attack Surface Reduction\Configure Attack Surface Reduction rules: Set the state for each ASR rule
```

Note: This Group Policy path is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

Default Value:

Disabled. (No ASR rules will be configured.)

References:

1. https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/enable-attack-surface-reduction?view=o365-worldwide
2. https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/attack-surface-reduction?view=o365-worldwide
3. GRID: MS-00000655

Additional Information:

- Microsoft Defender Antivirus (Built-in, baseline protection)
- Microsoft Defender for Endpoint Plan 1, (Foundational enterprise endpoint protection)
- Microsoft Defender for Endpoint Plan 2, (Full enterprise EDR + XDR tier)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 Enable Anti-Exploitation Features Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●
v7	8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		●	●

1.6.1.17 Ensure 'Configure Attack Surface Reduction rules: Set the state for each ASR rule' is set to 'c1db55ab-c21a-4637-bb3f-a12568109d35:2' or higher (Automated)

Profile Applicability:

- Level 1 - Workstation
- Level 1 - Server

Description:

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.

Rule ID and name:

- `c1db55ab-c21a-4637-bb3f-a12568109d35` (Use advanced protection against ransomware)

The recommended state for this setting is: `c1db55ab-c21a-4637-bb3f-a12568109d35:2` (Audit) or higher. Configuring this setting to `c1db55ab-c21a-4637-bb3f-a12568109d35:1` (Block) also conforms to the benchmark.

Note: More information on ASR rules can be found at the following link: Use Attack surface reduction rules to prevent malware infection | Microsoft Docs

Rationale:

This ASR rule can help an organization enhance its protection against ransomware by using both cloud and local heuristics.

Impact:

When a rule is triggered, a notification will be displayed from the Action Center. To parse audit logs effectively an organization may need to implement a SIEM solution.

Implementing this recommendation could impact certain workflows, making it unsuitable for universal enforcement across the organization without first adding exceptions.

Note: Cloud-delivered protection must be enabled to use this rule.

Warning: Prior to configuring this rule in `Block` mode, it should be enabled in `Audit` mode to verify that it does not introduce issues, especially for Microsoft Outlook. This rule **will** block legitimate programs.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_SZ` value of `2` or `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules:c1db55ab-c21a-4637-bb3f-a12568109d35
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `c1db55ab-c21a-4637-bb3f-a12568109d35` with a value of `2` or `1`:

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Microsoft Defender Exploit Guard\Attack Surface Reduction\Configure Attack Surface Reduction rules: Set the state for each ASR rule
```

Note: This Group Policy path is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

Default Value:

Disabled. (No ASR rules will be configured.)

References:

1. https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/enable-attack-surface-reduction?view=o365-worldwide
2. https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/attack-surface-reduction?view=o365-worldwide
3. GRID: MS-00000656

Additional Information:

- Microsoft Defender Antivirus (Built-in, baseline protection)
- Microsoft Defender for Endpoint Plan 1, (Foundational enterprise endpoint protection)
- Microsoft Defender for Endpoint Plan 2, (Full enterprise EDR + XDR tier)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 Enable Anti-Exploitation Features Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●
v7	8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		●	●

1.6.2 Controlled Folder Access

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

1.6.3 Network Protection

This section contains Windows Network Protection settings.

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

1.6.3.1 Ensure 'Prevent users and apps from accessing dangerous websites' is set to 'Enabled: Block' (Automated)

Profile Applicability:

- Level 1 - Workstation

Description:

This policy setting controls Microsoft Defender Exploit Guard network protection.

The recommended state for this setting is: `Enabled: Block`.

Rationale:

This setting can help prevent employees from using any application to access dangerous domains that may host phishing scams, exploit-hosting sites, and other malicious content on the Internet.

Impact:

Users and applications will not be able to access dangerous domains.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\windows Defender\Windows Defender Exploit
Guard\Network Protection:EnableNetworkProtection
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: Block`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Windows Defender Antivirus\Windows Defender Exploit Guard\Network
Protection\Prevent users and apps from accessing dangerous websites
```

Note: This Group Policy path is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

Default Value:

Disabled. (Users and applications will not be blocked from connecting to dangerous domains.)

References:

1. https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/network-protection?view=o365-worldwide
2. GRID: MS-00000468

Additional Information:

- Microsoft Defender Antivirus (Built-in, baseline protection)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.3 Maintain and Enforce Network-Based URL Filters Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.		●	●
v8	10.5 Enable Anti-Exploitation Features Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●
v7	7.4 Maintain and Enforce Network-Based URL Filters Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.		●	●
v7	8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		●	●

1.7 MpEngine

This section contains recommendations for MpEngine.

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 10 Release 1703 Administrative Templates (or newer).

1.7.1 Ensure 'Enable file hash computation feature' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Workstation
- Level 1 - Server

Description:

This setting determines whether hash values are computed for files scanned by Microsoft Defender.

The recommended state for this setting is: `Enabled`.

Rationale:

When running an antivirus solution such as Microsoft Defender Antivirus, it is important to ensure that it is configured to monitor for suspicious and known malicious activity. File hashes are a reliable way of detecting changes to files, and can speed up the scan process by skipping files that have not changed since they were last scanned and determined to be safe. A changed file hash can also be cause for additional scrutiny.

Impact:

This setting could cause performance degradation during initial deployment and for users where new executable content is frequently being created (such as software developers), or where applications are frequently installed or updated.

For more information on this setting, please visit Security baseline (FINAL): Windows 10 and Windows Server, version 2004 - Microsoft Tech Community - 1543631.

Note: The impact of this setting should be monitored closely during deployment to ensure user and system performance impact is within acceptable limits.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\MpEngine:EnableFileHashComputation
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirus\MpEngine\Enable file hash computation feature
```

Note: This Group Policy path is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

Default Value:

Disabled. (File hash values are not computed during scans.)

References:

1. GRID: MS-00000469

Additional Information:

- Microsoft Defender Antivirus (Built-in, baseline protection)
- Microsoft Defender for Endpoint Plan 1, (Foundational enterprise endpoint protection)
- Microsoft Defender for Endpoint Plan 2, (Full enterprise EDR + XDR tier)
- Microsoft Defender for Business, (SMB-focused EDR, simplified)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.1 Deploy and Maintain Anti-Malware Software Deploy and maintain anti-malware software on all enterprise assets.	●	●	●
v7	8.1 Utilize Centrally Managed Anti-malware Software Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.		●	●

1.7.2 Ensure 'Select cloud protection level' is set to Enabled: Moderate blocking level' or higher (Automated)

Profile Applicability:

- Level 1 - Workstation
- Level 1 - Server

Description:

This policy setting determines how aggressive Microsoft Defender Antivirus will be in blocking and scanning suspicious files. Threat data from this feature is analyzed in real time using, machine learning models, and behavioral analysis.

Options for blocking levels are:

- `Default blocking level` provides strong detection without increasing the risk of detecting legitimate files.
- `Moderate blocking level` provides moderate only for high confidence detections
- `High blocking level` applies a strong level of detection while optimizing client performance (but can also give a greater chance of false positives).
- `High + blocking level` applies extra protection measures (might affect client performance and increase the chance of false positives).
- `Zero tolerance blocking level` blocks all unknown executables.

The recommended state for this setting is: `Enabled: Moderate blocking level`. Configuring this setting to `High blocking level`, `High+ blocking level`, or `Zero tolerance blocking level` also conforms to the benchmark.

Rationale:

Attackers routinely deploy new malware variants that can change faster than signature updates. Enabling cloud protection can close this gap with its ability to detect and block new, unknown, and fast-moving threats.

Impact:

Although higher protection levels can increase detection of new threats, it can also raise the potential for false positives.

Note: The select cloud protection level feature requires the following Group Policy setting to be configured to function.

- *Join Microsoft MAPS* must be `enabled`.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`, `2`, `4`, or `6`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\MpEngine:MpCloudBlockLevel
```

Note: If a Resultant Set of Policy with Group Policy (RSOP) is run on the system, and `Default blocking level` is selected, it can produce misleading results. A setting with a `0` value is read as disabled by RSOP.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: Moderate blocking level`, `High blocking level`, `High+ blocking level`, or `Zero tolerance blocking level`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Microsoft Defender Antivirus\MpEngine\Select cloud protection
level
```

Note: This Group Policy path is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 11 Release 24H2 Administrative Templates (or newer).

Default Value:

Enabled: Default blocking level. (Provides strong detection without increasing the risk of detecting legitimate files.)

References:

1. GRID: MS-00000657

Additional Information:

- Microsoft Defender Antivirus (Built-in, baseline protection)
- Microsoft Defender for Endpoint Plan 1, (Foundational enterprise endpoint protection)
- Microsoft Defender for Endpoint Plan 2, (Full enterprise EDR + XDR tier)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.1 Deploy and Maintain Anti-Malware Software Deploy and maintain anti-malware software on all enterprise assets.	●	●	●
v7	8.1 Utilize Centrally Managed Anti-malware Software Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.		●	●

1.8 Network Inspection System

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

1.8.1 Ensure 'Convert warn verdict to block' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 - Workstation
- Level 2 - Server

Description:

This policy setting controls whether Microsoft Defender Antivirus network protection will display a warning, or block network traffic.

The recommended state for this setting is: `Enabled`.

Rationale:

Potentially suspicious network traffic should be blocked until it has been reviewed, and an exception has been granted.

Impact:

Legitimate network traffic could be blocked by Microsoft Defender Antivirus network protection.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\NIS:EnableConvertWarnToBlock
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Network Inspection System\Convert warn verdict to block
```

Note: This Group Policy path is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 11 Release 24H2 Administrative Templates (or newer).

Default Value:

Disabled. (Network protection will display a warning for warn verdicts.)

References:

1. GRID: MS-00000599
2. https://learn.microsoft.com/en-us/defender-endpoint/network-protection

Additional Information:

- Microsoft Defender Antivirus (Built-in, baseline protection)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.1 Deploy and Maintain Anti-Malware Software Deploy and maintain anti-malware software on all enterprise assets.	●	●	●
v7	8.1 Utilize Centrally Managed Anti-malware Software Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.		●	●

1.9 Quarantine

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

1.10 Real-time Protection

This section contains settings related to Real-time Protection.

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

1.10.1 Ensure 'Configure monitoring for incoming and outgoing file and program activity' is set to 'Enabled: bi-directional (full on access)' (Automated)

Profile Applicability:

- Level 1 - Workstation
- Level 1 - Server

Description:

This policy setting configures monitoring for incoming and outgoing files, without having to turn off monitoring entirely. This setting only applies to NTFS volumes. For any other file system types, full monitoring of file and program activity will be present on those volumes.

The recommended state for this setting is: `Enabled: bi-directional (full on access)`.

Warning: When configured as recommended, the Group Policy Object (GPO) will automatically appear as `Disabled` after saving. This behavior is expected and indicates the setting was applied correctly.

Rationale:

When running an antivirus solution such as Microsoft Defender Antivirus, it is important to ensure that it is configured to monitor in real-time for suspicious activity.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time
Protection:RealtimeScanDirection
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: bi-directional (full on access)`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Microsoft Defender Antivirus\Real-Time Protection\Configure
monitoring for incoming and outgoing file and program activity
```

Note: This Group Policy path is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 11 Release 24H2 Administrative Templates (or newer).

Default Value:

Disabled. (Monitoring for incoming and outgoing files will be enabled.)

References:

1. GRID: MS-00000658

Additional Information:

- Microsoft Defender Antivirus (Built-in, baseline protection)
- Microsoft Defender for Endpoint Plan 1, (Foundational enterprise endpoint protection)
- Microsoft Defender for Endpoint Plan 2, (Full enterprise EDR + XDR tier)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.1 Deploy and Maintain Anti-Malware Software Deploy and maintain anti-malware software on all enterprise assets.	●	●	●
v7	8.1 Utilize Centrally Managed Anti-malware Software Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.		●	●

1.10.2 Ensure 'Configure real-time protection and Security Intelligence Updates during OOBE' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Workstation
- Level 1 - Server

Description:

This policy setting configures whether Real-time Protection and Security Intelligence Updates are enabled during the Out of Box experience (OOBE).

The recommended state for this setting is: `Enabled`.

Rationale:

Critical Windows zero-day patch updates should be applied during OOBE to help mitigate against malicious attacks.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time
Protection:OobeEnableRtpAndSigUpdate
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Microsoft Defender Antivirus\Real-Time Protection\Configure real-
time protection and Security Intelligence Updates during OOBE
```

Note: This Group Policy path is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 11 Release 24H2 Administrative Templates (or newer).

Default Value:

Enabled. (Real-time Protection and Security Intelligence will be updated during OOBE.)

References:

1. GRID: MS-00000600
2. https://learn.microsoft.com/en-us/windows-hardware/customize/desktop/windows-updates-during-oobe-in-windows-11
3. https://techcommunity.microsoft.com/blog/microsoft-security-baselines/windows-11-version-24h2-security-baseline/4252801

Additional Information:

- Microsoft Defender Antivirus (Built-in, baseline protection)
- Microsoft Defender for Endpoint Plan 1, (Foundational enterprise endpoint protection)
- Microsoft Defender for Endpoint Plan 2, (Full enterprise EDR + XDR tier)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.1 Deploy and Maintain Anti-Malware Software Deploy and maintain anti-malware software on all enterprise assets.	●	●	●
v7	8.1 Utilize Centrally Managed Anti-malware Software Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.		●	●

1.10.3 Ensure 'Monitor file and program activity on your computer' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Workstation
- Level 1 - Server

Description:

This policy setting configures monitoring for file and program activity.

The recommended state for this setting is: `Enabled`.

Rationale:

Attackers routinely deploy new malware variants that can change faster than signature updates. Enabling this setting ensures that file and program activity are continually monitored.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time
Protection:DisableOnAccessProtection
```

Note: A value of `0`, enables this setting although this value is typically used to disable a setting. This has to do with how the registry value `DisableOnAccessProtection` interacts with the system.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Microsoft Defender Antivirus\Real-Time Protection\Monitor file and
program activity on your computer
```

Note: This Group Policy path is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Default Value:

Enabled.

References:

1. GRID: MS-00000659

Additional Information:

- Microsoft Defender Antivirus (Built-in, baseline protection)
- Microsoft Defender for Endpoint Plan 1, (Foundational enterprise endpoint protection)
- Microsoft Defender for Endpoint Plan 2, (Full enterprise EDR + XDR tier)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.1 Deploy and Maintain Anti-Malware Software Deploy and maintain anti-malware software on all enterprise assets.	●	●	●
v7	8.1 Utilize Centrally Managed Anti-malware Software Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.		●	●

1.10.4 Ensure 'Scan all downloaded files and attachments' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Workstation
- Level 1 - Server

Description:

This policy setting configures scanning for all downloaded files and attachments.

The recommended state for this setting is: `Enabled`.

Rationale:

When running an antivirus solution such as Microsoft Defender Antivirus, it is important to ensure that it is configured to heuristically monitor in real-time for suspicious and known malicious activity.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time
Protection:DisableIOAVProtection
```

Note: A value of `0`, enables this setting although this value is typically used to disable a setting. This has to do with how the registry value `DisableIOAVProtection` interacts with the system.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Microsoft Defender Antivirus\Real-Time Protection\Scan all
downloaded files and attachments
```

Note: This Group Policy path is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Default Value:

Enabled. (All downloaded files and attachments will be scanned.)

References:

1. https://learn.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-antivirus/configure-real-time-protection-microsoft-defender-antivirus
2. GRID: MS-00000470

Additional Information:

- Microsoft Defender Antivirus (Built-in, baseline protection)
- Microsoft Defender for Endpoint Plan 1, (Foundational enterprise endpoint protection)
- Microsoft Defender for Endpoint Plan 2, (Full enterprise EDR + XDR tier)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.1 Deploy and Maintain Anti-Malware Software Deploy and maintain anti-malware software on all enterprise assets.	●	●	●
v7	8.1 Utilize Centrally Managed Anti-malware Software Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.		●	●

1.10.5 Ensure 'Turn off real-time protection' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Workstation
- Level 1 - Server

Description:

This policy setting configures real-time protection prompts for known malware detection. Microsoft Defender Antivirus alerts when malware or potentially unwanted software attempts to install itself or run on the system.

The recommended state for this setting is: `Disabled`.

Rationale:

When running an antivirus solution such as Microsoft Defender Antivirus, it is important to ensure that it is configured to heuristically monitor in real-time for suspicious and known malicious activity.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time
Protection:DisableRealtimeMonitoring
```

Note: A value of `0`, enables this setting although this value is typically used to disable a setting. This has to do with how the registry value `DisableRealtimeMonitoring` interacts with the system.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Microsoft Defender Antivirus\Real-Time Protection\Turn off real-
time protection
```

Note: This Group Policy path is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Default Value:

Disabled. (Microsoft Defender Antivirus will prompt users to take actions on malware detections.)

References:

1. https://learn.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-antivirus/configure-real-time-protection-microsoft-defender-antivirus
2. https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-protection-features-microsoft-defender-antivirus?view=o365-worldwide
3. GRID: MS-00000471

Additional Information:

- Microsoft Defender Antivirus (Built-in, baseline protection)
- Microsoft Defender for Endpoint Plan 1, (Foundational enterprise endpoint protection)
- Microsoft Defender for Endpoint Plan 2, (Full enterprise EDR + XDR tier)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.1 Deploy and Maintain Anti-Malware Software Deploy and maintain anti-malware software on all enterprise assets.	●	●	●
v7	8.1 Utilize Centrally Managed Anti-malware Software Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.		●	●

1.10.6 Ensure 'Turn on behavior monitoring' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Workstation
- Level 1 - Server

Description:

This policy setting allows you to configure behavior monitoring for Microsoft Defender Antivirus.

The recommended state for this setting is: `Enabled`.

Rationale:

When running an antivirus solution such as Microsoft Defender Antivirus, it is important to ensure that it is configured to heuristically monitor in real-time for suspicious and known malicious activity.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time
Protection:DisableBehaviorMonitoring
```

Note: A value of `0`, enables this setting although this value is typically used to disable a setting. This has to do with how the registry value `DisableBehaviorMonitoring` interacts with the system.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Microsoft Defender Antivirus\Real-Time Protection\Turn on behavior
monitoring
```

Note: This Group Policy path is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Default Value:

Enabled. (Behavior monitoring will be enabled.)

References:

1. https://learn.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-antivirus/configure-real-time-protection-microsoft-defender-antivirus
2. GRID: MS-00000472

Additional Information:

- Microsoft Defender Antivirus (Built-in, baseline protection)
- Microsoft Defender for Endpoint Plan 1, (Foundational enterprise endpoint protection)
- Microsoft Defender for Endpoint Plan 2, (Full enterprise EDR + XDR tier)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.7 Use Behavior-Based Anti-Malware Software Use behavior-based anti-malware software.		●	●
v7	8.1 Utilize Centrally Managed Anti-malware Software Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.		●	●

1.10.7 Ensure 'Turn on process scanning whenever real-time protection is enabled' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Workstation
- Level 1 - Server

Description:

This policy setting configures process scanning when real-time protection is turned on. This helps to catch malware which could start when real-time protection is turned off.

The recommended state for this setting is: `Enabled`.

Rationale:

When running an antivirus solution such as Microsoft Defender Antivirus, it is important to ensure that it is configured to heuristically monitor in real-time for suspicious and known malicious activity.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time
Protection:DisableScanOnRealtimeEnable
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Microsoft Defender Antivirus\Real-Time Protection\Turn on process
scanning whenever real-time protection is enabled
```

Note: This Group Policy path is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 11 Release 24H2 Administrative Templates (or newer).

Default Value:

Enabled.

References:

1. GRID: MS-00000660

Additional Information:

- Microsoft Defender Antivirus (Built-in, baseline protection)
- Microsoft Defender for Endpoint Plan 1, (Foundational enterprise endpoint protection)
- Microsoft Defender for Endpoint Plan 2, (Full enterprise EDR + XDR tier)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.1 Deploy and Maintain Anti-Malware Software Deploy and maintain anti-malware software on all enterprise assets.	●	●	●
v7	8.1 Utilize Centrally Managed Anti-malware Software Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.		●	●

1.10.8 Ensure 'Turn on script scanning' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Workstation
- Level 1 - Server

Description:

This policy setting allows script scanning to be turned on/off. Script scanning intercepts scripts then scans them before they are executed on the system.

The recommended state for this setting is: `Enabled`.

Rationale:

When running an antivirus solution such as Microsoft Defender Antivirus, it is important to ensure that it is configured to heuristically monitor in real-time for suspicious and known malicious activity.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time
Protection:DisableScriptScanning
```

Note: A value of `0`, enables this setting although this value is typically used to disable a setting. This has to do with how the registry value `DisableScriptScanning` interacts with the system.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Microsoft Defender Antivirus\Real-Time Protection\Turn on script
scanning
```

Note: This Group Policy path is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 11 Release 21H2 Administrative Templates (or newer).

Default Value:

Enabled. (Script scanning will be enabled.)

References:

1. https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-advanced-scan-types-microsoft-defender-antivirus?view=o365-worldwide
2. GRID: MS-00000473

Additional Information:

- Microsoft Defender Antivirus (Built-in, baseline protection)
- Microsoft Defender for Endpoint Plan 1, (Foundational enterprise endpoint protection)
- Microsoft Defender for Endpoint Plan 2, (Full enterprise EDR + XDR tier)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.7 Use Behavior-Based Anti-Malware Software Use behavior-based anti-malware software.		●	●
v7	8.1 Utilize Centrally Managed Anti-malware Software Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.		●	●

1.11 Remediation

This section contains settings related to Remediation.

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

1.11.1 Behavioral Network Blocks

This section contains settings related to Behavioral Network Blocks.

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 11 Release 24H2 Administrative Templates (or newer).

1.11.1.1 Brute-Force Protection

This section contains settings related to Brute-Force Protection.

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 11 Release 24H2 Administrative Templates (or newer).

1.11.1.1.1 Ensure 'Configure Brute-Force Protection aggressiveness' is set to 'Enabled: Medium' or higher (Automated)

Profile Applicability:

- Level 2 - Workstation
- Level 2 - Server

Description:

This policy setting configures whether Brute-Force Protection in Microsoft Defender Antivirus is enabled. Brute-force protection can detect and block attempts to forcibly sign in to a system.

The recommended state for this setting is: `Enabled: Medium`. Configuring this setting to `Enabled: High` also conforms to the benchmark.

Rationale:

This feature can help reduce the likelihood of a successful brute force attack.

Impact:

Some legitimate authentication attempts may be detected or blocked depending on the configuration of this feature.

When set to `Medium`, detections or blocks will occur when the confidence level is above 99%.

When set to `High`, detections or blocks will occur when the confidence level is above 90%.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1` or `2`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Remediation\Behavioral
Network Blocks\Brute Force Protection:BruteForceProtectionAggressiveness
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: Medium` or `Enabled: High`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Microsoft Defender Antivirus\Remediation\Behavioral Network
Blocks\Brute-Force Protection\Configure Brute-Force Protection aggressiveness
```

Note: This Group Policy path is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 11 Release 24H2 Administrative Templates (or newer).

Default Value:

Low. (Block only when confidence level is 100%.)

References:

1. GRID: MS-00000601

Additional Information:

- Microsoft Defender Antivirus (Built-in, baseline protection)
- Microsoft Defender for Endpoint Plan 1, (Foundational enterprise endpoint protection)
- Microsoft Defender for Endpoint Plan 2, (Full enterprise EDR + XDR tier)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.1 Deploy and Maintain Anti-Malware Software Deploy and maintain anti-malware software on all enterprise assets.	●	●	●
v7	8.1 Utilize Centrally Managed Anti-malware Software Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.		●	●

1.11.1.1.2 Ensure 'Configure Remote Encryption Protection Mode' is set to 'Enabled: Audit' or higher (Automated)

Profile Applicability:

- Level 1 - Workstation
- Level 1 - Server

Description:

This policy setting configures the Brute-Force Protection feature in Microsoft Defender Antivirus. Brute-Force Protection can detect and block attempts to forcibly initiate sign-ins and sessions.

The recommended state for this setting is: `Enabled: Audit`. Configuring this setting to `Enabled: Block` also conforms to the benchmark.

Note: Configuring the value to either `Default` or `Off` does **not** conform to this benchmark.

Note #2: This setting's name is duplicated in the *Remote Encryption Protection* section, but they configure two different behaviors.

Rationale:

This feature assists with mitigating brute force attempts by detecting and blocking unauthorized sign-ins and sessions.

Impact:

Legitimate sign-ins and sessions could be detected or blocked by this feature if too many failed attempts are detected.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `2` or `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Remediation\Behavioral
Network Blocks\Brute Force Protection:BruteForceProtectionConfiguredState
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: Audit` or `Enabled: Block`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Microsoft Defender Antivirus\Remediation\Behavioral Network
Blocks\Brute-Force Protection\Configure Remote Encryption Protection Mode
```

Note: This Group Policy path is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 11 Release 24H2 Administrative Templates (or newer).

Default Value:

Not configured. (Apply defaults, which can vary depending on the antivirus engine version and the platform.)

References:

1. GRID: MS-00000602

Additional Information:

- Microsoft Defender Antivirus (Built-in, baseline protection)
- Microsoft Defender for Endpoint Plan 1, (Foundational enterprise endpoint protection)
- Microsoft Defender for Endpoint Plan 2, (Full enterprise EDR + XDR tier)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.1 Deploy and Maintain Anti-Malware Software Deploy and maintain anti-malware software on all enterprise assets.	●	●	●
v7	8.1 Utilize Centrally Managed Anti-malware Software Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.		●	●

1.11.1.2 Remote Encryption Protection

This section contains settings related to Remote Encryption Protection.

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 11 Release 24H2 Administrative Templates (or newer).

1.11.1.2.1 Ensure 'Configure how aggressively Remote Encryption Protection blocks threats' is set to 'Enabled: Medium' or higher (Automated)

Profile Applicability:

- Level 2 - Workstation
- Level 2 - Server

Description:

This policy setting configures how aggressively Remote Encryption Prevention Protection blocks malicious IP addresses.

The recommended state for this setting is: `Enabled: Medium` or higher. Configuring this setting to `Enabled: High` also conforms to the benchmark.

Rationale:

This feature can help reduce the likelihood of users visiting malicious websites.

Impact:

Legitimate websites could be detected or blocked by Remote Encryption Prevention Protection depending on the configuration of this feature.

When set to `Medium`, detections or blocks will occur when the confidence level is above 99%.

When set to `High`, detections or blocks will occur when the confidence level is above 90%.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1` or `2`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Remediation\Behavioral
Network Blocks\Remote Encryption
Protection:RemoteEncryptionProtectionAggressiveness
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: Medium` or `Enabled: High`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Microsoft Defender Antivirus\Remediation\Behavioral Network
Blocks\Remote Encryption Protection\Configure how aggressively Remote
Encryption Protection blocks threats
```

Note: This Group Policy path is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 11 Release 24H2 Administrative Templates (or newer).

Default Value:

Low. (Block only when confidence level is 100%.)

References:

1. GRID: MS-00000603

Additional Information:

- Microsoft Defender Antivirus (Built-in, baseline protection)
- Microsoft Defender for Endpoint Plan 1, (Foundational enterprise endpoint protection)
- Microsoft Defender for Endpoint Plan 2, (Full enterprise EDR + XDR tier)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.1 Deploy and Maintain Anti-Malware Software Deploy and maintain anti-malware software on all enterprise assets.	●	●	●
v7	8.1 Utilize Centrally Managed Anti-malware Software Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.		●	●

1.11.1.2.2 Ensure 'Configure Remote Encryption Protection Mode' is set to 'Enabled: Audit' or higher (Automated)

Profile Applicability:

- Level 1 - Workstation
- Level 1 - Server

Description:

This policy setting sets the mode for Remote Encryption Protection in Microsoft Defender Antivirus, which can detect and block attempts to replace local files with encrypted versions from another device.

The recommended state for this setting is: `Enabled: Audit`. Configuring this setting to `Enabled: Block` also conforms to the benchmark.

Note: Configuring the value to either `Default` or `Off` does **not** conform to this benchmark.

Note #2: This setting's name is duplicated in the *Brute-Force Protection* section, but they configure two different behaviors.

Rationale:

This feature assists with detecting and blocks malicious remote encryption behavior, such as when a threat actor attempts to remotely encrypt files on a victim machine using compromised credentials, network channels, or lateral movement techniques.

Impact:

False positives blocking legitimate remote operations could be detected or blocked by this feature.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `2` or `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Remediation\Behavioral
Network Blocks\Remote Encryption
Protection:RemoteEncryptionProtectionConfiguredState
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: Audit` or `Enabled: Block`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Microsoft Defender Antivirus\Remediation\Behavioral Network
Blocks\Remote Encryption Protection\Configure Remote Encryption Protection
Mode
```

Note: This Group Policy path is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 11 Release 24H2 Administrative Templates (or newer).

Default Value:

Not configured. (Apply defaults, which can vary depending on the antivirus engine version and the platform.)

References:

1. GRID: MS-00000602

Additional Information:

- Microsoft Defender Antivirus (Built-in, baseline protection)
- Microsoft Defender for Endpoint Plan 1, (Foundational enterprise endpoint protection)
- Microsoft Defender for Endpoint Plan 2, (Full enterprise EDR + XDR tier)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.1 Deploy and Maintain Anti-Malware Software Deploy and maintain anti-malware software on all enterprise assets.	●	●	●
v7	8.1 Utilize Centrally Managed Anti-malware Software Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.		●	●

1.12 Reporting

This section contains settings related to Microsoft Defender Reporting.

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

1.12.1 Ensure 'Configure Watson events' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 - Workstation
- Level 2 - Server

Description:

This policy setting determines whether Watson events are sent to Microsoft. Watson events are the reports that get sent to Microsoft when a program or service crashes or fails, including the possibility of automatic submission.

The recommended state for this setting is: `Disabled`.

Rationale:

In high-security environments, data must never be shared with third-parties without explicit consent, as it may contain sensitive information.

Impact:

Watson events will not be sent to Microsoft automatically when a program or service crashes or fails.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows
Defender\Reporting:DisableGenericRePorts
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Microsoft Defender Antivirus\Reporting\Configure Watson events
```

Note: This Group Policy path is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Default Value:

Enabled. (Watson events *will* be sent to Microsoft automatically when a program or service crashes or fails.)

References:

1. GRID: MS-00000474

Additional Information:

- Microsoft Defender Antivirus (Built-in, baseline protection)
- Microsoft Defender for Endpoint Plan 1, (Foundational enterprise endpoint protection)
- Microsoft Defender for Endpoint Plan 2, (Full enterprise EDR + XDR tier)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	13.3 Monitor and Block Unauthorized Network Traffic Deploy an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting information security professionals.			●

1.12.2 Ensure 'Configure whether to report Dynamic Signature dropped events' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Workstation
- Level 1 - Server

Description:

This policy setting configures whether to report Dynamic Signature dropped events. Dynamic Signature events are Microsoft Defender Antivirus log events that relate to cloud-delivered, on-demand threat signatures that Microsoft pushes to endpoints outside of the normal scheduled signature update cycle.

The recommended state for this setting is: `Enabled`.

Rationale:

Microsoft Defender Antivirus logs Dynamic Signature dropped events when it blocks or removes a file using a dynamically delivered signature, but the signature is not fully processed or applied and is subsequently discarded. This may indicate an issue with signature updates or with the system’s ability to properly receive or handle dynamic signatures.

Impact:

Enabling dynamic signature dropped events will generate additional events when this feature is enabled.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows
Defender\Reporting:EnableDynamicSignatureDroppedEventReporting
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Microsoft Defender Antivirus\Reporting\Configure whether to report
Dynamic Signature dropped events
```

Note: This Group Policy path is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Default Value:

Disabled.

References:

1. https://learn.microsoft.com/en-us/defender-endpoint/configure-notifications-microsoft-defender-antivirus
2. GRID: MS-00000661

Additional Information:

- Microsoft Defender Antivirus (Built-in, baseline protection)
- Microsoft Defender for Endpoint Plan 1, (Foundational enterprise endpoint protection)
- Microsoft Defender for Endpoint Plan 2, (Full enterprise EDR + XDR tier)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

1.13 Scan

This section contains settings related to Microsoft Defender scanning.

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

1.13.1 Ensure 'Check for the latest virus and spyware security intelligence before running a scheduled scan' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Workstation
- Level 1 - Server

Description:

This policy setting controls whether to check for new virus and spyware security intelligence before running a scan.

The recommended state for this setting is: `Enabled`.

Note: This setting applies to scheduled scans and has no effect on scans that are initiated manually from the user interface or to the ones that have been started from the command line using `mpcmdrun -Scan`.

Rationale:

A malware scan is only as effective as the threat definitions it uses. Running a scan with outdated intelligence significantly reduces detection accuracy and can create a false sense of security.

Impact:

Checking for updated security intelligence can add a small amount of overhead before a scan begins.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows
Defender\Scan:CheckForSignaturesBeforeRunningScan
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Microsoft Defender Antivirus\Scan\Check for the latest virus and
spyware security intelligence before running a scheduled scan
```

Note: This Group Policy path is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 11 Release 24H2 Administrative Templates (or newer).

Default Value:

Disabled. (The scan will start using the existing security intelligence.)

References:

1. GRID: MS-00000662

Additional Information:

- Microsoft Defender Antivirus (Built-in, baseline protection)
- Microsoft Defender for Endpoint Plan 1, (Foundational enterprise endpoint protection)
- Microsoft Defender for Endpoint Plan 2, (Full enterprise EDR + XDR tier)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.1 Deploy and Maintain Anti-Malware Software Deploy and maintain anti-malware software on all enterprise assets.	●	●	●
v7	8.1 Utilize Centrally Managed Anti-malware Software Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.		●	●

1.13.2 Ensure 'Scan archive files' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Workstation
- Level 1 - Server

Description:

This policy setting configures whether Microsoft Defender Antivirus scans for malicious software and unwanted software in archive files such as `.ZIP` or `.CAB` files.

The recommended state for this setting is: `Enabled`.

Rationale:

Archive files such as `.zip`, `.rar`, `.7z`, and `.iso` are a common and effective way threat actors hide malware, bypass basic defenses, and to delay detection.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Scan:DisableArchiveScanning
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Microsoft Defender Antivirus\Scan\Scan archive files
```

Note: This Group Policy path is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 11 Release 24H2 Administrative Templates (or newer).

Default Value:

Enabled.

References:

1. GRID: MS-00000663

Additional Information:

- Microsoft Defender Antivirus (Built-in, baseline protection)
- Microsoft Defender for Endpoint Plan 1, (Foundational enterprise endpoint protection)
- Microsoft Defender for Endpoint Plan 2, (Full enterprise EDR + XDR tier)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.1 Deploy and Maintain Anti-Malware Software Deploy and maintain anti-malware software on all enterprise assets.	●	●	●
v7	8.1 Utilize Centrally Managed Anti-malware Software Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.		●	●

1.13.3 Ensure 'Scan excluded files and directories during quick scans' is set to 'Enabled: 1' (Automated)

Profile Applicability:

- Level 1 - Workstation
- Level 1 - Server

Description:

This policy setting manages whether Microsoft Defender Antivirus scans excluded files and directories when running a Quick Scan.

The recommended state for this setting is: `Enabled: 1`.

Rationale:

The Real-time Protection feature excludes some files and directories for contextual reasons. This setting ensures that these are scanned during a Quick Scan.

Impact:

A Quick Scan could take longer when including the contextually excluded files and directories.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows
Defender\Scan:QuickScanIncludeExclusions
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: 1`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Microsoft Defender Antivirus\Scan\Scan excluded files and
directories during quick scans
```

Note: This Group Policy path is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 11 Release 24H2 Administrative Templates (or newer).

Default Value:

Disabled. (Contextual exclusions are not scanned during Quick Scans.)

References:

1. GRID: MS-00000604
2. https://learn.microsoft.com/en-us/defender-endpoint/schedule-antivirus-scans

Additional Information:

- Microsoft Defender Antivirus (Built-in, baseline protection)
- Microsoft Defender for Endpoint Plan 1, (Foundational enterprise endpoint protection)
- Microsoft Defender for Endpoint Plan 2, (Full enterprise EDR + XDR tier)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.1 Deploy and Maintain Anti-Malware Software Deploy and maintain anti-malware software on all enterprise assets.	●	●	●
v7	8.1 Utilize Centrally Managed Anti-malware Software Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.		●	●

1.13.4 Ensure 'Scan packed executables' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Workstation
- Level 1 - Server

Description:

This policy setting manages whether Microsoft Defender Antivirus scans packed executables. Packed executables are executable files that contain compressed code.

The recommended state for this setting is: `Enabled`.

Rationale:

Packing executables is a way to compress and create smaller files and can make it difficult to access and analyze the code associated with the executable. This is a common method to obfuscate malicious executables by bad actors.

Impact:

None - This is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows
Defender\Scan:DisablePackedExeScanning
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Microsoft Defender Antivirus\Scan\Scan packed executables
```

Note: This Group Policy path is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 and Server 2012 R2 Administrative Templates (or newer).

Default Value:

Enabled. (Packed executables will be scanned.)

References:

1. https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-advanced-scan-types-microsoft-defender-antivirus?view=o365-worldwide#settings-and-locations
2. GRID: MS-00000475

Additional Information:

- Microsoft Defender Antivirus (Built-in, baseline protection)
- Microsoft Defender for Endpoint Plan 1, (Foundational enterprise endpoint protection)
- Microsoft Defender for Endpoint Plan 2, (Full enterprise EDR + XDR tier)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.4 Configure Automatic Anti-Malware Scanning of Removable Media Configure anti-malware software to automatically scan removable media.		●	●
v7	8.4 Configure Anti-Malware Scanning of Removable Devices Configure devices so that they automatically conduct an anti-malware scan of removable media when inserted or connected.	●	●	●

1.13.5 Ensure 'Scan removable drives' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Workstation
- Level 1 - Server

Description:

This policy setting manages whether to scan for malicious and unwanted software in the contents of removable drives, such as USB flash drives, when running a full scan.

The recommended state for this setting is: `Enabled`.

Rationale:

It is important to ensure that any present removable drives are always included in any type of scan, as removable drives are more likely to contain malicious software brought into the managed environment from an external, unmanaged computer.

Impact:

Removable drives will be scanned during any type of scan by Microsoft Defender Antivirus.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows
Defender\Scan:DisableRemovableDriveScanning
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Microsoft Defender Antivirus\Scan\Scan removable drives
```

Note: This Group Policy path is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Default Value:

Disabled. (Removable drives will not be scanned during a full scan. Removable drives may still be scanned during quick scan and custom scan.)

References:

1. https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-advanced-scan-types-microsoft-defender-antivirus?view=o365-worldwide#settings-and-locations
2. GRID: MS-00000476

Additional Information:

- Microsoft Defender Antivirus (Built-in, baseline protection)
- Microsoft Defender for Endpoint Plan 1, (Foundational enterprise endpoint protection)
- Microsoft Defender for Endpoint Plan 2, (Full enterprise EDR + XDR tier)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.4 Configure Automatic Anti-Malware Scanning of Removable Media Configure anti-malware software to automatically scan removable media.		●	●
v7	8.4 Configure Anti-Malware Scanning of Removable Devices Configure devices so that they automatically conduct an anti-malware scan of removable media when inserted or connected.	●	●	●

1.13.6 Ensure 'Specify the day of the week to run a scheduled scan' is set to 'Enabled: 0' or higher, but not '8' (Automated)

Profile Applicability:

- Level 1 - Workstation
- Level 1 - Server

Description:

This policy setting configures the day of the week to perform a scheduled scan.

The recommended state for this setting is: `Enabled: 0` or higher, but not `8`.

This setting can be configured with the following values:

- (0x0) Every Day
- (0x1) Sunday
- (0x2) Monday
- (0x3) Tuesday
- (0x4) Wednesday
- (0x5) Thursday
- (0x6) Friday
- (0x7) Saturday
- (0x8) Never (default)

Rationale:

Performing a scheduled scan at least once a week is a consistent way to verify that critical parts of the system remain clean.

Impact:

If `Quick Scans` are used for the scheduled scan type, this setting is not expected to negatively affect system performance, as these scans are intentionally designed to be lightweight.

If `Full Scans` are used for the scheduled scan type, this may impact system performance as a full scan comprehensively scans every file, folder, running process, and system area on the device.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`, `1`, `2`, `3`, `4`, `5`, `6`, or `7`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Scan:ScheduleDay
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: 0` or higher, but not `8`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Microsoft Defender Antivirus\Scan\Specify the day of the week to
run a scheduled scan
```

Note: This Group Policy path is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 and Server 2012 R2 Administrative Templates (or newer).

References:

1. GRID: MS-00000664

Additional Information:

- Microsoft Defender Antivirus (Built-in, baseline protection)
- Microsoft Defender for Endpoint Plan 1, (Foundational enterprise endpoint protection)
- Microsoft Defender for Endpoint Plan 2, (Full enterprise EDR + XDR tier)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.1 Deploy and Maintain Anti-Malware Software Deploy and maintain anti-malware software on all enterprise assets.	●	●	●
v7	8.1 Utilize Centrally Managed Anti-malware Software Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.		●	●

1.13.7 Ensure 'Specify the scan type to use for a scheduled scan' is set to 'Enabled: Quick Scan (default)' or higher (Automated)

Profile Applicability:

- Level 1 - Workstation
- Level 1 - Server

Description:

This policy setting configures the scan type to use during a scheduled scan.

The recommended state for this setting is: `Enabled: Quick Scan (default)`. Configuring this setting to `Full Scan` also conforms to the benchmark.

Rationale:

Preforming antivirus scans helps protect systems, data, and users from a wide range of security threats.

Impact:

If `Quick Scan` is configured, this setting is not expected to negatively impact system performance, as quick scans are designed to be lightweight.

If `Full Scan` is configured, it might negatively impact the system, as a full scan comprehensively scans every file, folder, running process, and system area on the device.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1` or `2`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Scan:ScanParameters
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: 1`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Microsoft Defender Antivirus\Scan\Specify the scan type to use for
a scheduled scan
```

Note: This Group Policy path is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (The default scan type will be used.)

References:

1. GRID: MS-00000665

Additional Information:

- Microsoft Defender Antivirus (Built-in, baseline protection)
- Microsoft Defender for Endpoint Plan 1, (Foundational enterprise endpoint protection)
- Microsoft Defender for Endpoint Plan 2, (Full enterprise EDR + XDR tier)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.1 Deploy and Maintain Anti-Malware Software Deploy and maintain anti-malware software on all enterprise assets.	●	●	●
v7	8.1 Utilize Centrally Managed Anti-malware Software Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.		●	●

1.13.8 Ensure 'Specify the time for a daily quick scan' is set to 'Enabled: 1' or higher (Automated)

Profile Applicability:

- Level 1 - Workstation
- Level 1 - Server

Description:

This policy setting configures the time of day at which to perform a daily quick scan.

The recommended state for this setting is: `Enabled: 1` or higher.

Note: The time value is represented as the number of minutes past midnight (00:00). For example, 120 (0x78) is equivalent to 02:00 AM. By default, this setting is set to a time value of 2:00 AM. The schedule is based on local time on the computer where the scan is executing.

Rationale:

Preforming a daily quick scan is a consistent, low-impact way to verify that critical parts of the system remain clean.

Impact:

This setting is not expected to negatively impact system performance, as quick scans are designed to be lightweight.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1` or higher.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Scan:ScheduleQuickScanTime
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: 1` or higher:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Microsoft Defender Antivirus\Scan\Specify the time for a daily
quick scan
```

Note: This Group Policy path is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 and Server 2012 R2 Administrative Templates (or newer).

Default Value:

Disabled.

References:

1. GRID: MS-00000666

Additional Information:

- Microsoft Defender Antivirus (Built-in, baseline protection)
- Microsoft Defender for Endpoint Plan 1, (Foundational enterprise endpoint protection)
- Microsoft Defender for Endpoint Plan 2, (Full enterprise EDR + XDR tier)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.1 Deploy and Maintain Anti-Malware Software Deploy and maintain anti-malware software on all enterprise assets.	●	●	●
v7	8.1 Utilize Centrally Managed Anti-malware Software Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.		●	●

1.13.9 Ensure 'Specify the time of day to run a scheduled scan' is set to 'Enabled: 1' or higher (Automated)

Profile Applicability:

- Level 1 - Workstation
- Level 1 - Server

Description:

This policy setting configures the time of day at which to perform a scheduled scan.

The recommended state for this setting is: `Enabled: 1` or higher.

Note: The time value is represented as the number of minutes past midnight (00:00). For example, 120 (0x78) is equivalent to 02:00 AM. By default, this setting is set to a time value of 2:00 AM. The schedule is based on local time on the computer where the scan is executing.

Rationale:

Preforming a daily quick scan is a consistent, low-impact way to verify that critical parts of the system remain clean.

Impact:

This setting is not expected to negatively impact system performance, as quick scans are designed to be lightweight.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1` or higher.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Scan:ScheduleTime
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: 1` or higher:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Microsoft Defender Antivirus\Scan\Specify the time of day to run a
scheduled scan
```

Note: This Group Policy path is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 and Server 2012 R2 Administrative Templates (or newer).

Default Value:

Disabled. (A scheduled scan will run at a default time.)

References:

1. GRID: MS-00000667

Additional Information:

- Microsoft Defender Antivirus (Built-in, baseline protection)
- Microsoft Defender for Endpoint Plan 1, (Foundational enterprise endpoint protection)
- Microsoft Defender for Endpoint Plan 2, (Full enterprise EDR + XDR tier)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.1 Deploy and Maintain Anti-Malware Software Deploy and maintain anti-malware software on all enterprise assets.	●	●	●
v7	8.1 Utilize Centrally Managed Anti-malware Software Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.		●	●

1.13.10 Ensure 'Trigger a quick scan after X days without any scans' is set to 'Enabled: 7' (Automated)

Profile Applicability:

- Level 1 - Workstation
- Level 1 - Server

Description:

This policy setting configures the number of days after the last scan (of any type) before an aggressive Quick Scan is automatically triggered.

The recommended state for this setting is: `Enabled: 7` days.

Rationale:

Antivirus scans should be performed on a regular basis so that malicious software can be detected and remediated before malicious activity occurs.

Impact:

This setting should have no adverse effect on the system.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `7`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows
Defender\Scan:DaysUntilAggressiveCatchupQuickScan
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: 7` days:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Microsoft Defender Antivirus\Scan\Trigger a quick scan after X
days without any scans
```

Note: This Group Policy path is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 11 Release 24H2 Administrative Templates (or newer).

Default Value:

Disabled. (Aggressive Quick Scans are disabled.)

References:

1. GRID: MS-00000605

Additional Information:

- Microsoft Defender Antivirus (Built-in, baseline protection)
- Microsoft Defender for Endpoint Plan 1, (Foundational enterprise endpoint protection)
- Microsoft Defender for Endpoint Plan 2, (Full enterprise EDR + XDR tier)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.1 Deploy and Maintain Anti-Malware Software Deploy and maintain anti-malware software on all enterprise assets.	●	●	●
v7	8.1 Utilize Centrally Managed Anti-malware Software Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.		●	●

1.13.11 Ensure 'Turn on e-mail scanning' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Workstation
- Level 1 - Server

Description:

This policy setting configures e-mail scanning. When e-mail scanning is enabled, the engine will parse the mailbox and mail files, according to their specific format, to analyze the mail bodies and attachments. Several e-mail formats are currently supported, for example: pst (Outlook), dbx, mbx, mime (Outlook Express), binhex (Mac).

The recommended state for this setting is: `Enabled`.

Rationale:

All emails should be scanned by an antivirus solution such as Microsoft Defender Antivirus, as email attachments are a commonly used attack vector to infiltrate computers with malicious software.

Impact:

E-mail scanning by Microsoft Defender Antivirus will be enabled.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Scan:DisableEmailScanning
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Microsoft Defender Antivirus\Scan\Turn on e-mail scanning
```

Note: This Group Policy path is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Default Value:

Disabled. (E-mail scanning by Microsoft Defender Antivirus will be disabled.)

References:

1. https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-advanced-scan-types-microsoft-defender-antivirus?view=o365-worldwide#settings-and-locations
2. GRID: MS-00000477

Additional Information:

- Microsoft Defender Antivirus (Built-in, baseline protection)
- Microsoft Defender for Endpoint Plan 1, (Foundational enterprise endpoint protection)
- Microsoft Defender for Endpoint Plan 2, (Full enterprise EDR + XDR tier)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.1 Deploy and Maintain Anti-Malware Software Deploy and maintain anti-malware software on all enterprise assets.	●	●	●
v7	8.1 Utilize Centrally Managed Anti-malware Software Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.		●	●

1.14 Security Intelligence Updates

This section contains settings related to Security Intelligence Updates.

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Note: This section was initially named *Signature Updates* but was renamed by Microsoft to *Security Intelligence Updates* starting with the Microsoft Windows 10 Release 1903 Administrative Templates.

1.14.1 Ensure 'Specify the interval to check for security intelligence updates' is set to 'Enabled: 4' or fewer, but not '0' (Automated)

Profile Applicability:

- Level 1 - Workstation
- Level 1 - Server

Description:

This policy setting configures an interval at which to check for security intelligence updates. Security intelligence updates are the continuously updated packages that Microsoft Defender Antivirus uses to recognize, classify, and block the latest malware, spyware, unwanted software, and potentially harmful behaviors.

The recommended state for this setting is: `Enabled: 4` or fewer, but not `0`.

Note: The time value is represented as the number of hours between update checks. Valid values range from 1 (every hour) to 24 (once per day).

Rationale:

A malware scan is only as effective as the threat definitions it uses. Running a scan with outdated intelligence significantly reduces detection accuracy and can create a false sense of security.

Impact:

Checking for updated security intelligence can add a small amount of overhead to system.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `4`, `3`, `2`, or `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Signature
Updates:SignatureUpdateInterval
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: 4` or fewer, but not `0`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Microsoft Defender Antivirus\Security Intelligence Updates\Specify
the interval to check for security intelligence updates
```

Note: This Group Policy path is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 and Server 2012 R2 Administrative Templates (or newer).

Default Value:

Disabled. (Checks for security intelligence updates will occur at the default interval.)

References:

1. GRID: MS-00000668

Additional Information:

- Microsoft Defender Antivirus (Built-in, baseline protection)
- Microsoft Defender for Endpoint Plan 1, (Foundational enterprise endpoint protection)
- Microsoft Defender for Endpoint Plan 2, (Full enterprise EDR + XDR tier)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.1 Deploy and Maintain Anti-Malware Software Deploy and maintain anti-malware software on all enterprise assets.	●	●	●
v7	8.1 Utilize Centrally Managed Anti-malware Software Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.		●	●

1.15 Threats

This section contains settings related to Threats.

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

1.15.1 Ensure 'Specify threat alert levels at which default action should not be taken when detected' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Workstation
- Level 1 - Server

Description:

This policy setting configures which automatic remediation action Microsoft Defender Antivirus will take for each threat alert level detection.

The recommended state for this setting is: `Enabled`.

Rationale:

By default, Defender uses the action embedded in each threat's malware signature (clean, quarantine, remove, etc.). Configuring this setting ensures the same action is always taken, regardless of how Microsoft classifies a specific threat.

Impact:

If tamper protection is enabled in the environment, this setting is ignored because tamper protection enforces its own default action.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows
Defender\Threats:Threats_ThreatSeverityDefaultAction
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Microsoft Defender Antivirus\Threats\Specify threat alert levels
at which default action should not be taken when detected
```

Note: This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Not Configured.

References:

1. GRID: MS-00000669

Additional Information:

- Microsoft Defender Antivirus (Built-in, baseline protection)
- Microsoft Defender for Endpoint Plan 1, (Foundational enterprise endpoint protection)
- Microsoft Defender for Endpoint Plan 2, (Full enterprise EDR + XDR tier)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.1 Deploy and Maintain Anti-Malware Software Deploy and maintain anti-malware software on all enterprise assets.	●	●	●
v7	8.1 Utilize Centrally Managed Anti-malware Software Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.		●	●

1.15.2 Ensure 'Specify threat alert levels at which default action should not be taken when detected' is set to 'Enabled: Medium: 2 or 3' (Automated)

Profile Applicability:

- Level 1 - Workstation
- Level 1 - Server

Description:

This policy setting configures which automatic remediation action Microsoft Defender Antivirus will take for each threat alert level detection.

Valid threat alert levels are:

- 1 = Low
- 2 = Medium
- 4 = High
- 5 = Severe

Valid remediation action values are:

- 2 = Quarantine
- 3 = Remove
- 6 = Ignore

Threat alert levels are added under "options" for this setting. Each entry must be listed as a name value pair. The name defines a threat alert level, and the value contains the action ID for the remediation action that should be taken.

The recommended state for this setting is: `Enabled` with (value name) `2` and (value) `2`. Configuring this setting to `Enabled` with (value name) `2` and (value) `3` also conforms to the benchmark.

Rationale:

By default, Defender uses the action embedded in each threat's malware signature (clean, quarantine, remove, etc.). Configuring this setting ensures the same action is always taken, regardless of how Microsoft classifies a specific threat.

Impact:

If tamper protection is enabled in the environment, this setting is ignored because tamper protection enforces its own default action. In this case an exception to this recommendation will be needed.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_SZ` value of `2` or `3`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows
Defender\Threats\ThreatSeverityDefaultAction:2
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled` with (value name) `2` and (value) `2` or `Enabled` with (value name) `2` and (value) `3`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Microsoft Defender Antivirus\Threats\Specify threat alert levels
at which default action should not be taken when detected
```

Note: This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Not Configured.

References:

1. GRID: MS-00000669

Additional Information:

- Microsoft Defender Antivirus (Built-in, baseline protection)
- Microsoft Defender for Endpoint Plan 1, (Foundational enterprise endpoint protection)
- Microsoft Defender for Endpoint Plan 2, (Full enterprise EDR + XDR tier)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.1 Deploy and Maintain Anti-Malware Software Deploy and maintain anti-malware software on all enterprise assets.	●	●	●
v7	8.1 Utilize Centrally Managed Anti-malware Software Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.		●	●

1.15.3 Ensure 'Specify threat alert levels at which default action should not be taken when detected' is set to 'Enabled: High: 2 or 3' (Automated)

Profile Applicability:

- Level 1 - Workstation
- Level 1 - Server

Description:

This policy setting configures which automatic remediation action Microsoft Defender Antivirus will take for each threat alert level detection.

Valid threat alert levels are:

- 1 = Low
- 2 = Medium
- 4 = High
- 5 = Severe

Valid remediation action values are:

- 2 = Quarantine
- 3 = Remove
- 6 = Ignore

Threat alert levels are added under "options" for this setting. Each entry must be listed as a name value pair. The name defines a threat alert level, and the value contains the action ID for the remediation action that should be taken.

The recommended state for this setting is: `Enabled` with (value name) `4` and (value) `2`. Configuring this setting to `Enabled` with (value name) `4` and (value) `3` also conforms to the benchmark.

Rationale:

By default, Defender uses the action embedded in each threat's malware signature (clean, quarantine, remove, etc.). Configuring this setting ensures the same action is always taken, regardless of how Microsoft classifies a specific threat.

Impact:

If tamper protection is enabled in the environment, this setting is ignored because tamper protection enforces its own default action. In this case an exception to this recommendation will be needed.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_SZ` value of `2` or `3`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows
Defender\Threats\ThreatSeverityDefaultAction:4
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled` with (value name) `4` and (value) `2` or `Enabled` with (value name) `4` and (value) `3`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Microsoft Defender Antivirus\Threats\Specify threat alert levels
at which default action should not be taken when detected
```

Note: This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Not Configured.

References:

1. GRID: MS-00000669

Additional Information:

- Microsoft Defender Antivirus (Built-in, baseline protection)
- Microsoft Defender for Endpoint Plan 1, (Foundational enterprise endpoint protection)
- Microsoft Defender for Endpoint Plan 2, (Full enterprise EDR + XDR tier)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.1 Deploy and Maintain Anti-Malware Software Deploy and maintain anti-malware software on all enterprise assets.	●	●	●
v7	8.1 Utilize Centrally Managed Anti-malware Software Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.		●	●

1.15.4 Ensure 'Specify threat alert levels at which default action should not be taken when detected' is set to 'Enabled: Severe: 2 or 3' (Automated)

Profile Applicability:

- Level 1 - Workstation
- Level 1 - Server

Description:

This policy setting configures which automatic remediation action Microsoft Defender Antivirus will take for each threat alert level detection.

Valid threat alert levels are:

- 1 = Low
- 2 = Medium
- 4 = High
- 5 = Severe

Valid remediation action values are:

- 2 = Quarantine
- 3 = Remove
- 6 = Ignore

Threat alert levels are added under "options" for this setting. Each entry must be listed as a name value pair. The name defines a threat alert level, and the value contains the action ID for the remediation action that should be taken.

The recommended state for this setting is: `Enabled` with (value name) `5` and (value) `2`. Configuring this setting to `Enabled` with (value name) `5` and (value) `3` also conforms to the benchmark.

Rationale:

By default, Defender uses the action embedded in each threat's malware signature (clean, quarantine, remove, etc.). Configuring this setting ensures the same action is always taken, regardless of how Microsoft classifies a specific threat.

Impact:

If tamper protection is enabled in the environment, this setting is ignored because tamper protection enforces its own default action. In this case an exception to this recommendation will be needed.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_SZ` value of `2` or `3`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows
Defender\Threats\ThreatSeverityDefaultAction:5
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled` with (value name) `5` and (value) `2` or `Enabled` with (value name) `5` and (value) `3`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Microsoft Defender Antivirus\Threats\Specify threat alert levels
at which default action should not be taken when detected
```

Note: This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Not Configured.

References:

1. GRID: MS-00000669

Additional Information:

- Microsoft Defender Antivirus (Built-in, baseline protection)
- Microsoft Defender for Endpoint Plan 1, (Foundational enterprise endpoint protection)
- Microsoft Defender for Endpoint Plan 2, (Full enterprise EDR + XDR tier)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.1 Deploy and Maintain Anti-Malware Software Deploy and maintain anti-malware software on all enterprise assets.	●	●	●
v7	8.1 Utilize Centrally Managed Anti-malware Software Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.		●	●

1.16 Ensure 'Configure detection for potentially unwanted applications' is set to 'Enabled: Block' (Automated)

Profile Applicability:

- Level 1 - Workstation
- Level 1 - Server

Description:

This policy setting controls detection and action for Potentially Unwanted Applications (PUA), which are sneaky unwanted application bundlers or their bundled applications, that can deliver adware or malware.

The recommended state for this setting is: `Enabled: Block`.

For more information, see this link: Block potentially unwanted applications with Microsoft Defender Antivirus | Microsoft Docs

Rationale:

Potentially unwanted applications can increase the risk of your network being infected with malware, cause malware infections to be harder to identify, and can waste IT resources in cleaning up the applications. They should be blocked from installation.

Impact:

Applications that are identified by Microsoft as PUA will be blocked at download and install time.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender:PUAProtection
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: Block`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Microsoft Defender Antivirus\Configure detection for potentially
unwanted applications
```

Note: This Group Policy path is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 10 Release 1809 & Server 2019 Administrative Templates (or newer).

Default Value:

Disabled. (Applications that are identified by Microsoft as PUA will not be blocked.)

References:

1. https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/detect-block-potentially-unwanted-apps-microsoft-defender-antivirus?view=o365-worldwide
2. GRID: MS-00000462
3. https://learn.microsoft.com/en-us/defender-endpoint/detect-block-potentially-unwanted-apps-microsoft-defender-antivirus

Additional Information:

- Microsoft Defender Antivirus (Built-in, baseline protection)
- Microsoft Defender for Endpoint Plan 1, (Foundational enterprise endpoint protection)
- Microsoft Defender for Endpoint Plan 2, (Full enterprise EDR + XDR tier)
- Microsoft Defender for Business, (SMB-focused EDR, simplified)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.1 Deploy and Maintain Anti-Malware Software Deploy and maintain anti-malware software on all enterprise assets.	●	●	●
v7	2.7 Utilize Application Whitelisting Utilize application whitelisting technology on all assets to ensure that only authorized software executes and all unauthorized software is blocked from executing on assets.			●
v7	8.1 Utilize Centrally Managed Anti-malware Software Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.		●	●

1.17 Ensure 'Control whether exclusions are visible to local users' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Workstation
- Level 1 - Server

Description:

This policy setting controls whether Microsoft Defender Antivirus exclusions are visible to local users on the system.

The recommended state for this setting is: `Enabled`.

Warning: This setting requires at least *Microsoft Defender for Endpoint Plan 1 (Foundational enterprise endpoint protection)* to function. If *Plan 1* is not in use, an exception to this recommendation is required.

Rationale:

Only administrators should be able to view and manage Microsoft Defender Antivirus exclusions.

Impact:

Local users will not be able to view Microsoft Defender Antivirus exclusions.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows
Defender:HideExclusionsFromLocalUsers
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Microsoft Defender Antivirus\Control whether exclusions are
visible to local users
```

Note: This Group Policy path is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 11 Release 24H2 Administrative Templates (or newer).

Default Value:

Disabled. (Local users are able to view Microsoft Defender Antivirus exclusions.)

References:

1. GRID: MS-00000597
2. https://learn.microsoft.com/en-us/defender-endpoint/configure-exclusions-microsoft-defender-antivirus

Additional Information:

- Microsoft Defender for Endpoint Plan 1, (Foundational enterprise endpoint protection)
- Microsoft Defender for Endpoint Plan 2, (Full enterprise EDR + XDR tier)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.1 Deploy and Maintain Anti-Malware Software Deploy and maintain anti-malware software on all enterprise assets.	●	●	●
v7	8.1 Utilize Centrally Managed Anti-malware Software Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.		●	●

1.18 Ensure 'Turn off routine remediation' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Workstation
- Level 1 - Server

Description:

This policy setting configures whether Microsoft Defender Antivirus automatically takes action on all detected threats. The action to be taken on a particular threat is determined by the combination of the policy-defined action, user-defined action, and the signature-defined action.

The recommended state for this setting is: `Disabled`.

Rationale:

If this setting is enabled, Microsoft Defender prompts the user to take action on detected threats. Allowing users to choose threat remediation actions is not considered a best practice, as it can lead to inconsistent or unsafe responses.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows
Defender:DisableRoutinelyTakingAction
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Microsoft Defender Antivirus\Turn off routine remediation
```

Note: This Group Policy path is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (Microsoft Defender Antivirus automatically takes action on all detected threats after a nonconfigurable delay of approximately five seconds.)

References:

1. https://learn.microsoft.com/en-us/defender-endpoint/configure-remediation-microsoft-defender-antivirus
2. GRID: MS-00000670

Additional Information:

- Microsoft Defender Antivirus (Built-in, baseline protection)
- Microsoft Defender for Endpoint Plan 1, (Foundational enterprise endpoint protection)
- Microsoft Defender for Endpoint Plan 2, (Full enterprise EDR + XDR tier)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.1 Deploy and Maintain Anti-Malware Software Deploy and maintain anti-malware software on all enterprise assets.	●	●	●
v7	8.1 Utilize Centrally Managed Anti-malware Software Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.		●	●

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	**Microsoft Defender Antivirus**		
1.1	**Client Interface**		
1.2	**Device Control**		
1.3	**Exclusions**		
1.4	**Features**		
1.4.1	Ensure 'Enable EDR in block mode' is set to 'Enabled' (Automated)	☐	☐
1.5	**MAPS**		
1.5.1	Ensure 'Configure local setting override for reporting to Microsoft MAPS' is set to 'Disabled' (Automated)	☐	☐
1.5.2	Ensure 'Configure the 'Block at First Sight' feature' is set to 'Enabled' (Automated)	☐	☐
1.5.3	Ensure 'Join Microsoft MAPS' is set to 'Enabled: Advanced' (Automated)	☐	☐
1.5.4	Ensure 'Send file samples when further analysis is required' is set to 'Enabled: Send safe samples automatically' or higher (Automated)	☐	☐
1.6	**Microsoft Defender Exploit Guard**		
1.6.1	**Attack Surface Reduction**		
1.6.1.1	Ensure 'Configure Attack Surface Reduction rules' is set to 'Enabled' (Automated)	☐	☐
1.6.1.2	Ensure 'Configure Attack Surface Reduction rules: Set the state for each ASR rule' is set to '56a863a9-875e-4185-98a7-b882c64b5ce5:1' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.6.1.3	Ensure 'Configure Attack Surface Reduction rules: Set the state for each ASR rule' is set to '7674ba52-37eb-4a4f-a9a1-f0f9a1619a2c:1' (Automated)	☐	☐
1.6.1.4	Ensure 'Configure Attack Surface Reduction rules: Set the state for each ASR rule' is set to 'd4f940ab-401b-4efc-aadc-ad5f3c50688a:2' or higher (Automated)	☐	☐
1.6.1.5	Ensure 'Configure Attack Surface Reduction rules: Set the state for each ASR rule' is set to '9e6c4e1f-7d60-472f-ba1a-a39ef669e4b2:1' (Automated)	☐	☐
1.6.1.6	Ensure 'Configure Attack Surface Reduction rules: Set the state for each ASR rule' is set to 'be9ba2d9-53ea-4cdc-84e5-9b1eeee46550:1' (Automated)	☐	☐
1.6.1.7	Ensure 'Configure Attack Surface Reduction rules: Set the state for each ASR rule' is set to '01443614-cd74-433a-b99e-2ecdc07bfc25:2' or higher (Automated)	☐	☐
1.6.1.8	Ensure 'Configure Attack Surface Reduction rules: Set the state for each ASR rule' is set to '5beb7efe-fd9a-4556-801d-275e5ffc04cc:2' or higher (Automated)	☐	☐
1.6.1.9	Ensure 'Configure Attack Surface Reduction rules: Set the state for each ASR rule' is set to 'd3e037e1-3eb8-44c8-a917-57927947596d:1' (Automated)	☐	☐
1.6.1.10	Ensure 'Configure Attack Surface Reduction rules: Set the state for each ASR rule' is set to '3b576869-a4ec-4529-8536-b80a7769e899:1' (Automated)	☐	☐
1.6.1.11	Ensure 'Configure Attack Surface Reduction rules: Set the state for each ASR rule' is set to '75668c1f-73b5-4cf0-bb93-3ecf5cb7cc84:1' (Automated)	☐	☐
1.6.1.12	Ensure 'Configure Attack Surface Reduction rules: Set the state for each ASR rule' is set to '26190899-1602-49e8-8b27-eb1d0a1ce869:2' or higher (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.6.1.13	Ensure 'Configure Attack Surface Reduction rules: Set the state for each ASR rule' is set to 'e6db77e5-3df2-4cf1-b95a-636979351e5b:1' (Automated)	☐	☐
1.6.1.14	Ensure 'Configure Attack Surface Reduction rules: Set the state for each ASR rule' is set to '33ddedf1-c6e0-47cb-833e-de6133960387:1' (Automated)	☐	☐
1.6.1.15	Ensure 'Configure Attack Surface Reduction rules: Set the state for each ASR rule' is set to 'b2b3f03d-6a65-4f7b-a9c7-1c7ef74a9ba4:1' (Automated)	☐	☐
1.6.1.16	Ensure 'Configure Attack Surface Reduction rules: Set the state for each ASR rule' is set to '92e97fa1-2edf-4476-bdd6-9dd0b4dddc7b:1' (Automated)	☐	☐
1.6.1.17	Ensure 'Configure Attack Surface Reduction rules: Set the state for each ASR rule' is set to 'c1db55ab-c21a-4637-bb3f-a12568109d35:2' or higher (Automated)	☐	☐
1.6.2	**Controlled Folder Access**		
1.6.3	**Network Protection**		
1.6.3.1	Ensure 'Prevent users and apps from accessing dangerous websites' is set to 'Enabled: Block' (Automated)	☐	☐
1.7	**MpEngine**		
1.7.1	Ensure 'Enable file hash computation feature' is set to 'Enabled' (Automated)	☐	☐
1.7.2	Ensure 'Select cloud protection level' is set to Enabled: Moderate blocking level' or higher (Automated)	☐	☐
1.8	**Network Inspection System**		
1.8.1	Ensure 'Convert warn verdict to block' is set to 'Enabled' (Automated)	☐	☐
1.9	**Quarantine**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.10	**Real-time Protection**		
1.10.1	Ensure 'Configure monitoring for incoming and outgoing file and program activity' is set to 'Enabled: bi-directional (full on access)' (Automated)	☐	☐
1.10.2	Ensure 'Configure real-time protection and Security Intelligence Updates during OOBE' is set to 'Enabled' (Automated)	☐	☐
1.10.3	Ensure 'Monitor file and program activity on your computer' is set to 'Enabled' (Automated)	☐	☐
1.10.4	Ensure 'Scan all downloaded files and attachments' is set to 'Enabled' (Automated)	☐	☐
1.10.5	Ensure 'Turn off real-time protection' is set to 'Disabled' (Automated)	☐	☐
1.10.6	Ensure 'Turn on behavior monitoring' is set to 'Enabled' (Automated)	☐	☐
1.10.7	Ensure 'Turn on process scanning whenever real-time protection is enabled' is set to 'Enabled' (Automated)	☐	☐
1.10.8	Ensure 'Turn on script scanning' is set to 'Enabled' (Automated)	☐	☐
1.11	**Remediation**		
1.11.1	**Behavioral Network Blocks**		
1.11.1.1	**Brute-Force Protection**		
1.11.1.1.1	Ensure 'Configure Brute-Force Protection aggressiveness' is set to 'Enabled: Medium' or higher (Automated)	☐	☐
1.11.1.1.2	Ensure 'Configure Remote Encryption Protection Mode' is set to 'Enabled: Audit' or higher (Automated)	☐	☐
1.11.1.2	**Remote Encryption Protection**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.11.1.2.1	Ensure 'Configure how aggressively Remote Encryption Protection blocks threats' is set to 'Enabled: Medium' or higher (Automated)	☐	☐
1.11.1.2.2	Ensure 'Configure Remote Encryption Protection Mode' is set to 'Enabled: Audit' or higher (Automated)	☐	☐
1.12	**Reporting**		
1.12.1	Ensure 'Configure Watson events' is set to 'Disabled' (Automated)	☐	☐
1.12.2	Ensure 'Configure whether to report Dynamic Signature dropped events' is set to 'Enabled' (Automated)	☐	☐
1.13	**Scan**		
1.13.1	Ensure 'Check for the latest virus and spyware security intelligence before running a scheduled scan' is set to 'Enabled' (Automated)	☐	☐
1.13.2	Ensure 'Scan archive files' is set to 'Enabled' (Automated)	☐	☐
1.13.3	Ensure 'Scan excluded files and directories during quick scans' is set to 'Enabled: 1' (Automated)	☐	☐
1.13.4	Ensure 'Scan packed executables' is set to 'Enabled' (Automated)	☐	☐
1.13.5	Ensure 'Scan removable drives' is set to 'Enabled' (Automated)	☐	☐
1.13.6	Ensure 'Specify the day of the week to run a scheduled scan' is set to 'Enabled: 0' or higher, but not '8' (Automated)	☐	☐
1.13.7	Ensure 'Specify the scan type to use for a scheduled scan' is set to 'Enabled: Quick Scan (default)' or higher (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.13.8	Ensure 'Specify the time for a daily quick scan' is set to 'Enabled: 1' or higher (Automated)	☐	☐
1.13.9	Ensure 'Specify the time of day to run a scheduled scan' is set to 'Enabled: 1' or higher (Automated)	☐	☐
1.13.10	Ensure 'Trigger a quick scan after X days without any scans' is set to 'Enabled: 7' (Automated)	☐	☐
1.13.11	Ensure 'Turn on e-mail scanning' is set to 'Enabled' (Automated)	☐	☐
1.14	**Security Intelligence Updates**		
1.14.1	Ensure 'Specify the interval to check for security intelligence updates' is set to 'Enabled: 4' or fewer, but not '0' (Automated)	☐	☐
1.15	**Threats**		
1.15.1	Ensure 'Specify threat alert levels at which default action should not be taken when detected' is set to 'Enabled' (Automated)	☐	☐
1.15.2	Ensure 'Specify threat alert levels at which default action should not be taken when detected' is set to 'Enabled: Medium: 2 or 3' (Automated)	☐	☐
1.15.3	Ensure 'Specify threat alert levels at which default action should not be taken when detected' is set to 'Enabled: High: 2 or 3' (Automated)	☐	☐
1.15.4	Ensure 'Specify threat alert levels at which default action should not be taken when detected' is set to 'Enabled: Severe: 2 or 3' (Automated)	☐	☐
1.16	Ensure 'Configure detection for potentially unwanted applications' is set to 'Enabled: Block' (Automated)	☐	☐
1.17	Ensure 'Control whether exclusions are visible to local users' is set to 'Enabled' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.18	Ensure 'Turn off routine remediation' is set to 'Disabled' (Automated)	☐	☐

Appendix: Change History

Date: 02/20/2026 Version: 1.0.0
Initial Public Release