CIS Benchmarks

CIS Microsoft Edge Benchmark

v1.0.1 - 05-18-2022

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/

Table of Contents

Overview

This document provides prescriptive guidance for establishing a secure configuration posture for the Microsoft Edge Browser, also known as Microsoft Edge for Business. This guide was tested against Microsoft Edge v85 on the Windows 10 Release 2004 operating system. To obtain the latest version of this guide, please visit http://benchmarks.cisecurity.org. If you have questions, comments, or have identified ways to improve this guide, please write us at feedback@cisecurity.org.

Intended Audience

The CIS Microsoft Edge Benchmarks are written for Microsoft Windows Active Directory domain-joined systems using Group Policy, not standalone/workgroup systems. Adjustments/tailoring to some recommendations will be needed to maintain functionality if attempting to implement CIS hardening on standalone systems.

Consensus Guidance

This benchmark was created using a consensus review process comprised of subject matter experts. 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, or examples. Text should be interpreted exactly as presented.
<italic font in brackets>	Italic texts set in angle brackets denote a variable requiring substitution for a real value.
Italic font	Used to denote the title of a book, article, or other publication.
Note	Additional information or caveats

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 Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1 (L1) - Corporate/Enterprise Environment (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 (L2) - High Security/Sensitive Data Environment (limited functionality)**

  This profile extends the "Level 1 (L1)" profile. 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.

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:

Contributor
Brian Engleman
William Ferguson
Johannes Goerlich
Daniel Jasiak

Editor
Jennifer Jarose
Clifford Moten

Recommendations

1 Microsoft Edge

This section contains recommendations for Microsoft Edge.

This Group Policy section is provided by the Group Policy template `MSEdge.admx/adml` that is included with the Microsoft Edge v85 Administrative Templates (or newer).

1.1 Microsoft Edge

This section contains recommendations for Microsoft Edge settings.

This Group Policy section is provided by the Group Policy template `MSEdge.admx/adml` that is included with the Microsoft Edge v85 Administrative Templates (or newer).

1.1.1 (L1) Ensure 'Ads setting for sites with intrusive ads' is set to 'Enabled: Block ads on sites with intrusive ads' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This setting controls whether ads are blocked on sites with intrusive ads.

The recommended state for this setting is: `Enabled: Block ads on sites with intrusive ads`.

Rationale:

Intrusive ads are ads found on websites that are invasive or unwelcome. These ads can contain malicious files or can fool an unknowing user into giving away their username and/or password.

Impact:

Ads that may be non-intrusive can be blocked.

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 which should be set to `2`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:AdsSettingForIntrusiveAds
Sites
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: Block ads on sites with intrusive ads`

```
Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Ads
setting for sites with intrusive ads
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from: Download Microsoft Edge for Business - Microsoft.

Default Value:

Enabled: Block ads on sites with intrusive ads (Default value).

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.2 (L1) Ensure 'Allow download restrictions' is set to 'Enabled: Block potentially dangerous downloads' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy controls whether Microsoft Edge blocks certain types of downloads, and prevents users from bypassing security warnings, depending on the classification of Safe Browsing.

If this policy is not configured the default state of 'No special restrictions' will be used and the downloads will go through the usual security restrictions based on Microsoft Defender SmartScreen analysis results if it is used.

Note: These restrictions only apply to downloads from web page content, as well as the 'download link...' context menu option. These restrictions don't apply to saving or downloading the currently displayed page, nor do they apply to the Save as PDF option from the printing options. For more information on Microsoft Defender SmartScreen, please visit Microsoft Defender SmartScreen Frequently Asked Questions.

Note #2: Microsoft Edge relies on the Internet Explorer zones (Local Machine, Local Intranet, Trusted, Internet, Restricted) to determine which sites may bypass this policy setting. Please see Security Zones in Edge – text/plain for more information.

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

Rationale:

Downloads can contain malware that has the potential to exfiltrate sensitive data or encrypt critical systems for ransom.

Impact:

Users will be prevented from downloading certain types of files, and will not be able to bypass security warnings.

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 which should be set to `2`:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:DownloadRestrictions
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Allow
download restrictions
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from: Download Microsoft Edge for Business - Microsoft.

Default Value:

Enabled: No special restrictions. With the default value, the downloads will go through the usual security restrictions based on Microsoft Defender SmartScreen analysis results.

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.3 (L2) Ensure 'Allow file selection dialog' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This policy setting allows access to local files by allowing file selection dialogs in Microsoft Edge.

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

Rationale:

Allowing users to import favorites, uploading files, and savings links could pose potential security risks by allowing data to be uploaded to external sites or by downloading malicious files. By not allowing the file selection dialog the end-user will not be prompted for uploads/downloads preventing data exfiltration and possible system infection by malware.

Impact:

If you disable this setting users will no longer be prompted when performing actions which would trigger a file selection dialog. Instead, the file selection dialog box assumes the user clicked "Cancel". Being as this is not the default behavior, impact to the user will be noticeable, and the user will not be able to upload and download files.

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 which should be set to `0`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:AllowFileSelectionDialogs
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Allow
file selection dialogs
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from: Download Microsoft Edge for Business - Microsoft.

Default Value:

Enabled.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#allowfileselectiondialogs

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.4 (L1) Ensure 'Allow Google Cast to connect to Cast devices on all IP addresses' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether Google Cast is able to connect to all IP Addresses or only private IP Addresses as defined in RFC1918 (IPv4) and RFC4193 (IPv6). Note that if the `EnabledMediaRouter` policy is set to `Disabled` there is no positive or negative effect for this setting.

The recommended state for this setting is `Disabled`.

Rationale:

Allowing Google Cast to connect to public IP addresses could allow media and other potentially sensitive data to be exposed to the public. Disabling this setting will ensure that Google Cast is only able to connect to private (ie: internal) IP addresses.

Impact:

If this setting is set to `Disabled` there will be no effect to the user, as the default behavior of `Not Configured` has the same behavior as disabling the 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 which should be set to `0`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:MediaRouterCastAllowAllIP
s
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Allow
Google Cast to connect to Cast devices on all IP addresses
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from: Download Microsoft Edge for Business - Microsoft.

Default Value:

Disabled.

Google Cast connects to Cast devices on RFC1918/RFC4193 private addresses only, unless you enable the CastAllowAllIPs feature.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#mediaroutercastallowallips

CIS Controls:

Version 7

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.

1.1.5 (L1) Ensure 'Allow importing of autofill form data' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether users are allow to import autofill data from other browsers into Microsoft Edge.

The recommended state for this setting is `Disabled`.

Rationale:

Allowing autofill data to be imported could potentially allow sensitive data such as personally identifiable information (PII) from a non-secured source into Microsoft Edge. Considering that storage of sensitive data should be handled with care disabling this setting is recommended.

Impact:

If you set this setting to `Disabled` users will be unable to perform an import of autofill data during Microsoft Edge first run. This will also prevent users from importing data after Microsoft Edge has been setup.

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 which should be set to `0`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:ImportAutofillFormData
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Allow
importing of autofill form data
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from: Download Microsoft Edge for Business - Microsoft.

Default Value:

Autofill data is imported at first run, and users can choose whether to import this data manually during later browsing sessions.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#importautofillformdata

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.6 (L1) Ensure 'Allow importing of browser settings' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether users are able to import settings from another browser into Microsoft Edge.

The recommended state for this setting is `Disabled`.

Rationale:

Having settings automatically imported or allowing users to import settings from another browser into Microsoft Edge could potentially allow for non-recommended settings to be applied temporarily creating a potential security risk.

Impact:

Users will be unable to perform an import of other browser settings into Microsoft Edge.

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 which should be set to `0`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:ImportBrowserSettings
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Allow
importing of browser settings
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from: Download Microsoft Edge for Business - Microsoft.

Default Value:

Browser settings are imported at first run, and users can choose whether to import them manually during later browsing sessions.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#importbrowsersettings

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.7 (L1) Ensure 'Allow importing of home page settings' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether users are able to import homepage settings from another browser into Microsoft Edge as well as whether homepage settings are imported on first use.

The recommended state for this setting is `Disabled`.

Rationale:

Having the homepage setting automatically imported or allowing users to import this setting from another browser into Microsoft Edge allows for the potential of compromised settings being imported into Microsoft Edge.

Impact:

If you set this setting to `Disabled` users will be unable to perform an import homepage settings from other browsers into Microsoft Edge.

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 which should be set to `0`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:ImportHomepage
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Allow
importing of home page settings
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from: [Download Microsoft Edge for Business - Microsoft](#).

Default Value:

The home page setting is imported at first run, and users can choose whether to import this data manually during later browsing sessions.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#importhomepage

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.8 (L1) Ensure 'Allow importing of payment info' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether users are able to import payment information from another browser into Microsoft Edge as well as whether payment information is imported on first use.

The recommended state for this setting is `Disabled`.

Rationale:

Having payment information automatically imported or allowing users to import payment data from another browser into Microsoft Edge could allow for sensitive data to be imported into Edge.

Impact:

Users will be unable to perform a payment information import from other browsers into Microsoft Edge.

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 which should be set to `0`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:ImportPaymentInfo
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Allow
importing of payment info
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Payment info is imported at first run, and users can choose whether to import it manually during later browsing sessions.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#importpaymentinfo

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.9 (L1) Ensure 'Allow importing of saved passwords' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether users are able to import saved passwords from another browser into Microsoft Edge as well as whether passwords are imported on first use.

The recommended state for this setting is `Disabled`.

Rationale:

Having saved passwords automatically imported or allowing users to import password data from another browser into Microsoft Edge allows for sensitive data to be imported into Edge.

Impact:

If you set this setting to `Disabled` users will be unable to perform a saved passwords import from other browsers into Microsoft Edge.

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 which should be set to `0`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:ImportSavedPasswords
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Allow
importing saved passwords
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Passwords are imported at first run, and users can choose whether to import them manually during later browsing sessions.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#importsavedpasswords

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.10 (L1) Ensure 'Allow importing of search engine settings' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether users are able to import search engine settings from another browser into Microsoft Edge as well as whether said setting is imported on first use.

The recommended state for this setting is `Disabled`.

Rationale:

Having search engine settings automatically imported or allowing users to import the settings from another browser into Microsoft Edge could allow for a malicious search engine to be set.

Impact:

If you set this setting to `Disabled` users will be unable to perform an import of their search engine settings from other browsers into Microsoft Edge.

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 which should be set to `0`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:ImportSearchEngine
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Allow
importing search engine settings
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Search engine settings are imported at first run, and users can choose whether to import this data manually during later browsing sessions.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#importsearchengine

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.11 (L1) Ensure 'Allow managed extensions to use the Enterprise Hardware Platform API' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting allows extensions installed by enterprise policies to be allowed to use the Enterprise Hardware Platform API.

The recommended state for this setting is `Disabled`.

Rationale:

It is recommended that this setting is disabled unless otherwise directed by Enterprise policies.

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 which should be set to `0`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:EnterpriseHardwarePlatfor
mAPIEnabled
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Allow
managed extensions to use the Enterprise Hardware Platform API
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Disabled.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#enterprisehardwareplatformapienabled

CIS Controls:

Version 7

7.2 Disable Unnecessary or Unauthorized Browser or Email Client Plugins
Uninstall or disable any unauthorized browser or email client plugins or add-on applications.

1.1.12 (L2) Ensure 'Allow or block audio capture' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This policy setting allows you to set whether the end-user is prompted for access to audio capture devices. This may be Enabled (Default) or Disabled, in which case audio capture will only work for URLs configured in the *AudioCaptureAllowedUrls* setting.

Note: The *AudioCaptureAllowedUrls* setting will also need to be configured along with this setting.

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

Rationale:

With the end-user having the ability to allow or deny audio capture for websites in Microsoft Edge, could open an organization up to a malicious site that may capture proprietary information through the browser. By limiting or disallowing this setting, it removes the end-user's discretion leaving it up to the organization as to the sites allowed to use this ability.

Impact:

If this setting is disabled users will not be prompted for audio devices when using websites which may need this access, for example a web-based conferencing system. If there are sites which access will be allowed, this will need to be configured in the *AudioCaptureAllowedUrls* 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 which should be set to `0`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:AudioCaptureAllowed
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Allow
or block audio capture
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Enabled.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#audiocaptureallowed

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.13 (L2) Ensure 'Allow or block video capture' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This policy setting allows you to set whether the end-user is prompted for access to audio capture devices. This may be enabled (Default), or Disabled in which case audio capture will only work for URLs configured in the *VideoCaptureAllowedUrls* setting.

Note: The *VideoCaptureAllowedUrls* setting will also need to be configured along with this setting.

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

Rationale:

With the end-user having the ability to allow or deny video capture for websites in Microsoft Edge, could open an organization up to a malicious site that may capture proprietary information through the browser. By limiting or disallowing video capture it removes the end-user's discretion leaving it up to the organization as to the sites allowed to use this ability.

Impact:

If you disable this setting users will not be prompted for audio devices when using websites which may need this access, for example a web-based conferencing system. If there are sites which access will be allowed, configuration of the *VideoCaptureAllowedUrls* setting will be necessary.

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 which should be set to `0`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:VideoCaptureAllowed
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Allow
or block video capture
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Enabled.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#videocaptureallowed

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.14 (L2) Ensure 'Allow or deny screen capture' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This policy setting controls whether Microsoft Edge can use screen-share APIs including web-based online meetings, video, or screen sharing.

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

Rationale:

Allowing screen-share APIs within Microsoft Edge could potentially allow for sensitive data to be shared via screen captures.

Impact:

Users will be unable to utilize APIs which support web-based meetings, video, and screen capture. This could potentially have disruption to users whom may have utilized these abilities in the past.

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 which should be set to `0`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:ScreenCaptureAllowed
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Allow
or deny screen capture
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Enabled.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#screencaptureallowed

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.15 (L1) Ensure 'Allow personalization of ads search and news by sending browsing history to Microsoft' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether Microsoft is able to collect a user's browsing history and searches in Microsoft Edge for the purpose of personalizing searches, news, and other Microsoft services.

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

Rationale:

Sharing a user's browsing and search history could inadvertently expose data which should be protected.

Impact:

User's data will not be shared with Microsoft.

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 which should be set to `0`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:PersonalizationReportingE
nabled
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Allow
personalization of ads search and news by sending browsing history to
Microsoft
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Enabled.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#personalizationreportingenabled

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.16 (L1) Ensure 'Allow queries to a Browser Network Time service' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether Microsoft Edge can send queries to a network time service for accurate timestamps. This check helps in validation of certificates.

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

Rationale:

Microsoft Edge uses a network time service to randomly track times from a trusted external service. This allows Microsoft Edge the ability for verification of a certificate's validity and is important for certificate validation.

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 which should be set to `1`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:BrowserNetworkTimeQueries
Enabled
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Allow
queries to a Browser Network Time service
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Enabled.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#browsernetworktimequeriesenabled
2. https://docs.microsoft.com/en-us/microsoft-edge/privacy-whitepaper

CIS Controls:

Version 7

6.1 Utilize Three Synchronized Time Sources
Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.

1.1.17 (L2) Ensure 'Allow suggestions from local providers' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This policy setting determines whether suggestions from providers on a local device are able to be utilized for Microsoft Edge.

Note: Some features may not be available if a policy to disable this feature has been applied. For example, Browsing History suggestions will not be available if the *SavingBrowserHistoryDisabled* setting is enabled.

The recommended state for this setting is: `Disabled`

Rationale:

Data should not be shared with 3rd party vendors in an enterprise managed environment. Allowing this could unintentionally share data with local providers that are not managed by the organization.

Impact:

Some features may not be available to users such as browsing and search suggestions that would be based on the collected data.

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 which should be set to `0`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:LocalProvidersEnabled
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Allow
suggestions from local providers
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Not Configured - Suggestions from local providers are allowed but the user can change the setting using the settings toggle.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#localprovidersenabled

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.18 (L1) Ensure 'Allow the audio sandbox to run' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether audio processes in Microsoft Edge run in a sandbox.

Note: Security software setups within your environment might interfere with the sandbox.

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

Rationale:

Having audio processes run in a sandbox ensures that if a website misuses audio processes that data may not be manipulated or exfiltrated from 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 which should be set to `1`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:AudioSandboxEnabled
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Allow
the audio sandbox to run
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Not Configured - The default configuration for the audio sandbox will be used, which might differ based on the platform.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#audiosandboxenabled

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.19 (L1) Ensure 'Allow user feedback' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether users are able to utilize the Edge Feedback feature to send feedback, suggestions and surveys to Microsoft as well as issue reports.

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

Rationale:

Data should not be shared with 3rd party vendors in an enterprise managed environment.

Impact:

Users will not be able to send feedback to Microsoft.

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 which should be set to `0`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:UserFeedbackAllowed
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Allow
user feedback
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Enabled.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#userfeedbackallowed

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.20 (L2) Ensure 'Allow users to open files using the ClickOnce protocol' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This policy setting allows users to use the ClickOnce protocol for opening files via applications inside of Microsoft Edge instead of downloading them to their device. The ClickOnce protocol allows websites to request that the browser open files from a specific URL using the ClickOnce file handler on the user's computer or device.

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

Rationale:

Allowing users to configure ClickOnce could potentially allow malicious files to be automatically opened within Microsoft Edge. By not allowing this, the end-user will need to download file allowing it to be scanned before opening.

Impact:

Users will have to download files to their system and will be unable to open them directly in Microsoft Edge. Disabling ClickOnce will also prevent ClickOnce applications (.application files) from working properly.

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 which should be set to `0`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:ClickOnceEnabled
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Allow
users top open files using the ClickOnce protocol
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Disabled - Users will have the option to enable the use of the ClickOnce protocol with the edge://flags/ page.

References:

1. https://docs.microsoft.com/en-us/visualstudio/deployment/clickonce-security-and-deployment?view=vs-2019
2. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#clickonceenabled

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.21 (L2) Ensure 'Allow users to open files using the DirectInvoke protocol' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This policy setting allows users to utilize the DirectInvoke protocol for opening files via applications inside of Microsoft Edge instead of downloading them to their device.

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

Rationale:

Allowing users to configure DirectInvoke could potentially allow malicious files to be automatically opened within Microsoft Edge. By not allowing this the end-user will need to download files allowing for the file to be scanned before opening.

Impact:

Users will have to download files to their device and will be unable to open them directly in Microsoft Edge. Disabling DirectInvoke could also prevent some SharePoint functions from working properly.

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 which should be set to `0`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:DirectInvokeEnabled
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Allow
users to open files using the DirectInvoke protocol
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Enabled.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#directinvokeenabled
2. https://go.microsoft.com/fwlink/?linkid=2103872
3. https://go.microsoft.com/fwlink/?linkid=2099871

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.22 (L2) Ensure 'Allow users to proceed from the HTTPS warning page' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This policy setting controls whether a user is able to proceed to a webpage when an invalid SSL certificate warning has occurred.

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

Rationale:

Sites protected by SSL should always be recognized as valid in the web browser. Allowing a user to make the decision as to whether what appears to be an invalid certificate could open an organization up to users visiting a site that is otherwise not secure and or malicious in nature.

Impact:

Users will not be able to click past the invalid certificate error to view the website.

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 which should be set to `0`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:SSLErrorOverrideAllowed
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Allow
users to proceed from the HTTPS warning page
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Enabled.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#sslerroroverrideallowed

CIS Controls:

Version 7

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.

1.1.23 (L1) Ensure 'Allow websites to query for available payment methods' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting allows you to set whether a website can check to see if the user has payment methods saved.

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

Rationale:

Saving payment information in Microsoft Edge could lead to the sensitive data being leaked and used for non-legitimate purposes.

Impact:

Websites will be unable to query whether payment information within Microsoft Edge is available.

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 which should be set to `0`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:PaymentMethodQueryEnabled
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Allow
websites to query for available payment methods
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Enabled.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#paymentmethodqueryenabled

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.24 (L1) Ensure 'Allows a page to show popups during its unloading' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether popups show during page unloading in Microsoft Edge.

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

Rationale:

Allowing popups during page unloading can allow a page with a vulnerability to exhaust system resources through popups or introduce malware onto the system if clicked.

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 which should be set to `0`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:AllowPopupsDuringPageUnlo
ad
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Microsoft
Edge\Allows a page to show popups during its unloading
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Disabled.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#allowpopupsduringpageunload

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.25 (L2) Ensure 'Ask where to save downloaded files' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This policy setting controls whether a user is presented with a prompt asking where downloaded files should be saved, rather than files being downloaded to the default download directory.

The recommended state for this setting is `Disabled`.

Rationale:

Ensuring files from external sources are saved in a location known to be protected will help ensure mitigations for malicious files are not circumvented.

Impact:

Users will not be prompted when downloading files, all files will be downloaded to the default download directory.

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 which should be set to `0`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:PromptForDownloadLocation
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Ask
where to save downloaded files
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Not Configured - If this policy is not configured, the user will be able to change this setting.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#promptfordownloadlocation

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.26 (L1) Ensure 'Automatically import another browser's data and settings at first run' is set to 'Enabled: Disables automatic import, and the import section of the first-run experience is skipped' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether settings are imported from another browser into Microsoft Edge.

Note: The browser data from Microsoft Edge Legacy will always be silently migrated at the first run, irrespective of the value of this policy.

The recommended state for this setting is: `Enabled: Disables automatic import, and the import section of the first-run experience is skipped`.

Rationale:

Having settings automatically imported from another browser into Microsoft Edge could potentially allow for non-recommended settings to be applied temporarily creating a potential security risk.

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 which should be set to `4`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:AutoImportAtFirstRun
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`: `Disables automatic import, and the import section of the first-run experience is skipped`

```
Computer Configuration\Policies\Administrative Templates\Microsoft
Edge\Automatically import another browser's data and settings at first run
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Enabled - Automatically imports all supported datatypes and settings from the default browser

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#autoimportatfirstrun

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.27 (L2) Ensure 'Block third party cookies' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This policy controls whether web page elements from a domain other than that in the address bar is able to set cookies.

The recommended state for this setting is `Enabled`.

Rationale:

Allowing third-party cookies could potentially allow tracking of your web activities by third-party entities which may expose information that could be used for an attack on the end-user.

Impact:

Disabling third-party cookies could cause some websites to not function as expected (e.g., Microsoft 365 or Salesforce).

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 which should be set to `1`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:BlockThirdPartyCookies
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Block
third party cookies
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Enabled - Users can change this setting.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#blockthirdpartycookies

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.28 (L1) Ensure 'Block tracking of users' web-browsing activity' is set to 'Enabled: Balanced (Blocks harmful trackers and trackers from sites user has not visited; content and ads will be less personalized)' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether websites may track user's web-browsing activity.

The recommended state for this setting is: `Enabled: Balanced (Blocks harmful trackers and trackers from sites user has not visited; content and ads will be less personalized`.

Rationale:

Allowing websites to track user web-browsing activity allows for sites to gather information which could be potentially harmful and used to target users and businesses.

Impact:

Content and ads will have minimal personalization and website may not function properly.

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 which should be set to `2`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:TrackingPrevention
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: Balanced (Blocks harmful trackers and trackers from sites user has not visited; content and ads will be less personalized)`

```
Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Block
tracking of users' web-browsing activity
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Not Configured.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#trackingprevention

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.29 (L2) Ensure 'Browser sign-in settings' is set to 'Enabled: Disable browser sign-in' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This policy setting controls whether a user can sign into Microsoft Edge with an account to use services such as sync and single sign on.

Note: To control the availability of sync, use the *SyncDisabled* (Disable synchronization of data using Microsoft sync services) policy.

The recommended state for this setting is: `Disabled: Disable browser sign-in`.

Rationale:

Users will not be able to sign in to Microsoft Edge with an account. Signing in to Edge does not automaticaly sync users data, to control the availability of sync, use the *SyncDisabled* (Disable synchronization of data using Microsoft sync services) policy.

Impact:

Users will not be able to sign into the Microsoft Edge browser.

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 which should be set to `0`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:BrowserSignin
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`: `Disable browser sign-in`

```
Computer Configuration\Policies\Administrative Templates\Microsoft
Edge\Browser sign-in settings
```

Note: This setting works in conjunction with the *NonRemovableProfileEnabled* setting which will need to be set to `Disabled` because the setting *NonRemovableProfileEnabled* disables the creation of an automatically signed in browser profile.
Note #2: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Not Configured - Users can decide if they want to enable the browser sign-in option and use it as they see fit.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#browsersignin

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.30 (L1) Ensure 'Clear browsing data when Microsoft Edge closes' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy controls whether web browser data, such as forms, passwords and visited sites is deleted each time Microsoft Edge is closed.

Note: If this policy is enabled, do not enable the *AllowDeletingBrowserHistory* policy, because it will take precedence over the *ClearBrowsingDataOnExit* policy and all data will be deleted when Microsoft Edge closes, regardless of how *AllowDeletingBrowserHistory* is configured.

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

Rationale:

Deleting browser data on close will delete information that may be important for a computer investigation and investigators such as Computer Forensics Analysts may not be able to retrieve pertinent information to the investigation.

Impact:

Browsing data will not be deleted on closing and the user will not be able to change this setting.

Note: This setting will preserve browsing history that could contain a users personal browsing history. Please make sure that this setting is in compliance with organizational policies.

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 which should be set to `0`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:ClearBrowsingDataOnExit
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Clear
browsing data when Microsoft Edge closes
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Disabled - But users can configure the Clear browsing data option in Settings.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#clearbrowsingdataonexit

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.31 (L1) Ensure 'Clear cached images and files when Microsoft Edge closes' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy controls whether cached images and files are deleted each time Microsoft Edge closes.

Note: If this policy is disabled, do not enable the *ClearBrowsingDataOnExit* policy, because it will take precedence over the *ClearCachedImagesAndFilesOnExit* policy and will delete all browsing data when Microsoft Edge closes, regardless of how the *ClearCachedImagesAndFilesOnExit* policy is configured.

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

Rationale:

Deleting browser data on close will delete information that may be important for a computer investigation and investigators such as Computer Forensics Analysts may not be able to retrieve pertinent information to the investigation.

Impact:

Cached images and files will not be deleted on closing and the user will be unable to change 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 which should be set to `0`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:ClearCachedImagesAndFiles
OnExit
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Clear
cached images and files when Microsoft Edge closes
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Not Configured - But users can choose whether cached images and files are cleared on exit.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#clearcachedimagesandfilesonexit

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.32 (L1) Ensure 'Configure InPrivate mode availability' is set to 'Enabled: InPrivate mode disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether Edge InPrivate mode is available or even forced for the user.

The recommended state for this setting is: `Enabled: InPrivate mode disabled`.

Rationale:

Disabling InPrivate mode for Microsoft Edge will ensure that browsing data is logged on the system which may be important for forensics.

Impact:

Users will not be able to initiate the InPrivate browsing mode for Microsoft Edge.

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 which should be set to `1`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:InPrivateModeAvailability
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Microsoft
Edge\Configure InPrivate mode availability
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Enabled: InPrivate mode available.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#inprivatemodeavailability

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.33 (L2) Ensure 'Configure Online Text To Speech' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This policy setting determines whether Online Text to Speech voice fonts which is part of Azure Cognitive Services, are available to users. These voice fonts are higher quality than the pre-installed system voice fonts.

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

Rationale:

Enabling Online Text to Speech could allow data to be transmitted to a third-party, which could lead to sensitive data being exposed.

Impact:

Users will be unable to utilize Online Text to Speech.

Note: This setting will prevent the Online Text to Speech feature which can be used by users with with visual or learning disabilities to read the text of documents out loud. Please make sure this feature is not needed within the environment before disabling 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 which should be set to `0`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:ConfigureOnlineTextToSpee
ch
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Microsoft
Edge\Configure Online Text To Speech
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Enabled.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#configureonlinetexttospeech
2. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#configureonlinetexttospeech
3. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#configureonlinetexttospeech

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.34 (L1) Ensure 'Configure the list of names that will bypass the HSTS policy check' is set to 'Disabled' (Manual)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting allows a list of names to be specified that will be exempt from HTTP Strict Transport Security (HSTS) policy checks then potentially upgraded from http:// to https://.

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

Rationale:

Allowing hostnames to be exempt from HSTS policy checks could allow for *protocol downgrade attacks* and *cookie hijackings*.

Impact:

There should be no adverse affect to users.

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 which should be **absent** or does not have a **registry value** defined.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:HSTSPolicyBypassList
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Microsoft
Edge\Configure the list of names that will bypass the HSTS policy check
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Not Configured.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#hstspolicybypasslist

CIS Controls:

Version 7

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.

1.1.35 (L1) Ensure 'Configure the list of types that are excluded from synchronization' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting allows you to specify data types that will be limited/excluded from uploading data to the Microsoft Edge synchronization service.

The recommended state for this setting is: `Enabled` with the following CASE SENSITIVE datatype `passwords`.

Note: In a High Security/Sensitive Data Environment (L2), this setting should also include the following options: `settings`, `favorites`, `addressesAndMore`, `extensions` and `collections`.

Rationale:

Storing and sharing information could potentially expose sensitive information including but not limited to user passwords and login information. Allowing this synchronization could also potentially allow an end user to pull corporate data that was synchronized into the cloud to a personal machine.

Impact:

Password data will not be synchronized with the Azure AD Tenant.

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 which should be set to `passwords`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge\SyncTypesListDisabled:1
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled` with the following CASE SENSITIVE datatype `passwords`.

```
Computer Configuration\Policies\Administrative Templates\Microsoft
Edge\Configure the list of types that are excluded from synchronization
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Not Configured.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#synctypeslistdisabled

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.36 (L1) Ensure 'Configure the Share experience' is set to 'Enabled: Don't allow using the Share experience' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting allows users to be able to access the Share experience from the *Settings and More* menu in Microsoft Edge, which can allow information to be shared with other apps on the system.

The recommended state for this setting is: `Enabled: Don't allow using the Share experience`.

Rationale:

Having this setting enabled could allow malicious content from Microsoft Edge to be exposed to other parts of the operating system.

Impact:

Users will not be able to view or use the Share button in the toolbar as it will be hidden.

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 which should be set to `1`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:ConfigureShare
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: Don't allow using the Share experience`

```
Computer Configuration\Policies\Administrative Templates\Microsoft
Edge\Configure the Share experience
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Enabled: Allow using the Share experience

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#configureshare

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.37 (L1) Ensure 'Continue running background apps after Microsoft Edge closes' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting determines whether processes from Microsoft Edge may start at Operating System sign-in and continue running once an Edge browser window is closed. This allows background apps and the current browsing session to remain active, including any session cookies. An open background process displays an icon in the system tray and can always be closed from there.

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

Rationale:

Allowing processes from the browser to run in the background could allow a malicious script or code to continue running even once the browser windows has been closed.

Impact:

The browser will close its processes and will not continue running as a background process.

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 which should be set to `0`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:BackgroundModeEnabled
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Microsoft
Edge\Continue running background apps after Microsoft Edge closes
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Disabled - But the user can configure its behavior in edge://settings/system.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#backgroundmodeenabled

CIS Controls:

Version 7

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.

1.1.38 (L1) Ensure 'Control communication with the Experimentation and Configuration Service' is set to 'Enabled: Disable communication with the Experimentation and Configuration Service' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether Microsoft Edge uses the Experimentation and Configuration Service to deploy the Experimentation and Configuration payload which consists of a list of early in development features that Microsoft is enabling for testing and feedback.

The recommended state for this setting is: `Enabled: Disable communication with the Experimentation and Configuration Service`.

Rationale:

This setting allows feedback (data) to be sent back to a third-party for testing of development features for Microsoft Edge, and can also deliver a payload that contains a list of actions to take on certain domains for compatibility reasons.

Impact:

Data will not be sent back to a third-party and payloads will not be delivered.

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 which should be set to `0`.

```
SOFTWARE\Policies\Microsoft\Edge:ExperimentationAndConfigurationServiceContro
l
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: Disable communication with the Experimentation and Configuration Service`

```
Computer Configuration\Policies\Administrative Templates\Microsoft
Edge\Control communication with the Experimentation and Configuration Service
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Enabled: Retrieve configurations only.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#experimentationandconfigurationservicecontrol

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.39 (L1) Ensure 'Delete old browser data on migration' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy controls whether web browser data is deleted after migration to Microsoft Edge, this data includes forms, passwords, and visited sites.

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

Rationale:

Deleting browser data will delete information that may be important for a computer investigation and investigators such as Computer Forensics Analysts may not be able to retrieve pertinent information to the investigation.

Impact:

Browsing data will not be deleted during migration.

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 which should be set to `0`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:DeleteDataOnMigration
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Microsoft
Edge\Delete old browser data on migration
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Disabled.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#deletedataonmigration

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.40 (L1) Ensure 'Disable saving browser history' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy controls whether browser history is saved and prevents users from changing the policy.

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

Rationale:

Deleting browser data will delete information that may be important for a computer investigation and investigators such as Computer Forensics Analysts may not be able to retrieve pertinent information to the investigation.

Impact:

None - this is the default behavior.

Note: This setting will preserve browsing history that could contain a users personal browsing history. Please make sure that this setting is in compliance with organizational policies.

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 which should be set to `0`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:SavingBrowserHistoryDisab
led
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Microsoft
Edge\Disable saving browser history
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Disabled.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#savingbrowserhistorydisabled

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.41 (L1) Ensure 'Disable synchronization of data using Microsoft sync services' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether data synchronization with Microsoft sync services is allowed as well as whether the sync consent prompt appears to users. Examples of synced data include, but are not limited to, history and favorites.

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

Rationale:

Data should not be shared with third party vendors in an enterprise managed environment.

Impact:

User will be unable to sync data with Microsoft, the prompt for sync consent will also be hidden from the user.

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 which should be set to `1`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:SyncDisabled
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Microsoft
Edge\Disable synchronization of data using Microsoft sync services
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Not Configured - Users will be able to turn sync on or off.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#syncdisabled

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.42 (L1) Ensure 'DNS interception checks enabled' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting determines whether a local switch is configured for DNS interception checks. These checks attempt to discover if the browser is behind a proxy that redirects unknown host names.

Note: This detection might not be necessary in an enterprise environment where the network configuration is known. It can be disabled to avoid additional DNS and HTTP traffic on start-up and each DNS configuration change.

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

Rationale:

Disabling these checks could potentially allow DNS hijacking and poisoning.

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 which should be set to `1`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:DNSInterceptionChecksEnab
led
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Microsoft Edge\DNS
interception checks enabled
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Enabled.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#dnsinterceptionchecksenabled

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.43 (L1) Ensure 'Enable AutoFill for addresses' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy controls whether the AutoFill feature of Microsoft Edge is enabled for the auto-complete feature for addresses and other information in web forms.

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

Rationale:

Allowing autofill data to be saved in Microsoft Edge could potentially allow storage of sensitive data such as personally identifiable information (PII). Considering that storage of sensitive data should be handled with care disabling this setting is recommended.

Impact:

Users will be unable to store autofill address information in Microsoft Edge and they will also not be prompted to use such information on webforms. Disabling this setting also stops any past activity of autofill.

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 which should be set to `0`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:AutofillAddressEnabled
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Microsoft
Edge\Enable AutoFill for addresses
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Enabled - Users can control AutoFill for addresses in the user interface.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#autofilladdressenabled

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.44 (L1) Ensure 'Enable AutoFill for credit cards' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether users are able to utilize payment information stored in Microsoft Edge as well as whether they are prompted to save credit card information.

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

Rationale:

Having payment information automatically filled in and saved in Microsoft Edge could allow for an attacker to gain access to this sensitive data.

Impact:

Users will be unable to use and store AutoFill data for credit card information in Microsoft Edge.

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 which should be set to `0`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:AutofillCreditCardEnabled
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Microsoft
Edge\Enable AutoFill for credit cards
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Enabled - Users can control AutoFill for credit cards.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#autofillcreditcardenabled

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.45 (L1) Ensure 'Enable component updates in Microsoft Edge' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy determines whether updates for Microsoft Edge components are enabled in Microsoft Edge.

Note: Updates that are deemed "critical for security" are still applied even if you disable this policy as well as any component that doesn't contain executable code, that doesn't significantly alter the behavior of the browser.

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

Rationale:

Component updates should always be up to date to ensure the latest security patches and capabilities are applied.

Impact:

Updates will be automatically downloaded.

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 which should be set to `1`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:ComponentUpdatesEnabled
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Microsoft
Edge\Enable component updates in Microsoft Edge
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Enabled.

References:

1. Not Configured Behavior: An icon is shown in the browser informing the user to restart Microsoft Edge.

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.46 (L1) Ensure 'Enable deleting browser and download history' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy controls whether users are able to delete browser and download history for Microsoft Edge.

Note: Even when this policy disabled, the browsing and download history aren't guaranteed to be retained. Users can edit or delete the history database files directly, and the browser itself may remove (based on expiration period) or archive any or all history items at any time.

The recommended state for this setting is `Disabled`.

Rationale:

Deleting browser data will delete information that may be important for a computer investigation and investigators such as Computer Forensics Analysts may not be able to retrieve pertinent information to the investigation.

Impact:

Browser data deletion by users will be prohibited.

Note: This setting will preserve browsing history that could contain a users personal browsing history. Please make sure that this setting is in compliance with organizational policies.

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 which should be set to `0`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:AllowDeletingBrowserHisto
ry
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Microsoft
Edge\Enable deleting browser and download history
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Enabled.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#allowdeletingbrowserhistory

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.47 (L1) Ensure 'Enable globally scoped HTTP auth cache' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether HTTP auth credentials may be automatically used in the context of another web site visited in Microsoft Edge.

Note: This policy is intended to give enterprises depending on the legacy behavior a chance to update their login procedures and will be removed in the future.

The recommended state for this setting is `Disabled`.

Rationale:

Allowing HTTP auth credentials to be shared without the users consent could lead to a user sharing sensitive information without their knowledge. Enabling this setting could also lead to some types of cross-site attacks, that would allow users to be tracked across sites without the use of cookies.

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 which should be set to `0`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:GloballyScopeHTTPAuthCach
eEnabled
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Microsoft
Edge\Enable globally scoped HTTP auth cache
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Disabled.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#globallyscopehttpauthcacheenabled

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.48 (L2) Ensure 'Enable guest mode' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This policy setting controls whether a user may utilized guest profiles in Microsoft Edge.

The recommended state for this setting is `Disabled`.

Rationale:

In a guest profile, the browser doesn't import browsing data from existing profiles, and it deletes browsing data when all guest profiles are closed.

Deleting browser data will delete information that may be important for a computer investigation and investigators such as Computer Forensics Analysts may not be able to retrieve pertinent information to the investigation.

Impact:

Users will not be able to initiate Guest mode for Microsoft Edge.

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 which should be set to `0`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:BrowserGuestModeEnabled
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Microsoft
Edge\Enable guest mode
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Enabled.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#browserguestmodeenabled

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.49 (L1) Ensure 'Enable network prediction' is set to 'Enabled: Don't predict network actions on any network connection' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls the network prediction feature which controls DNS prefetching, TCP and SSL pre-connection and pre-rendering of web pages.

The recommended state for this setting is `Enabled: Don't predict network actions on any network connection`.

Rationale:

Opening connections to resources that may not be used could allow un-needed connections increasing attack surface and in some cases could lead to opening connections to resources which the user did not intend to utilize.

Impact:

None - this is the default behavior, with the exception of users being able to change the default.

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 which should be set to `2`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:NetworkPredictionOptions
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: Don't predict network actions on any network connection`

```
Computer Configuration\Policies\Administrative Templates\Microsoft
Edge\Enable network prediction
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Enabled - But the user can change the policy.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#networkpredictionoptions

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.50 (L2) Ensure 'Enable online OCSP/CRL checks' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This policy setting controls whether online OCSP/CRL revocation checks will be required.

The recommended state for this setting is `Enabled`.

Rationale:

Allowing certificates that have not been validated opens an organization up for an attack in which illegitimate sites are could potentially be presented as trusted.

Impact:

Certificates that are not publicly verified will not be trusted and the user will be warned that the certificate is not trusted.

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 which should be set to `1`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:EnableOnlineRevocationChe
cks
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Microsoft
Edge\Enable online OCSP/CRL checks
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Disabled.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#enableonlinerevocationchecks

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.51 (L1) Ensure 'Enable Proactive Authentication' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether Proactive Authentication is turned on or off. If enabled Microsoft Edge will try to authenticate a signed-in user with Microsoft services at regular intervals.

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

Rationale:

Allowing Microsoft Edge to try and sign-in the user to services with their account could allow sign the user into a service/site which they may not want to be signed in for many reasons including security and protection of files on the system. There is an increased risk with authentication credentials being sent at intervals in an attempt to sign into different services.

Impact:

Users may be asked to sign in to Microsoft services individually as they visit Microsoft sites.

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 which should be set to `0`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:ProactiveAuthEnabled
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Microsoft
Edge\Enable Proactive Authentication
```

Note: This setting works in conjunction with the *NonRemovableProfileEnabled* setting which will need to be set to `Disabled` because the setting *NonRemovableProfileEnabled* disables the creation of an automatically signed in browser profile.
Note #2: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Enabled.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#proactiveauthenabled

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.52 (L1) Ensure 'Enable profile creation from the Identity flyout menu or the Settings page' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether user profiles are able to create new profiles in Microsoft Edge.

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

Rationale:

Allowing users to create new profiles could allow for such profiles to be removed or switched which may end up in a situation that hides or even removes data which may be important for computer investigation and investigators such as Computer Forensics Analysts may not be able to retrieve pertinent information to the investigation.

Impact:

Users will be unable to utilize the `Add profile` option in Microsoft Edge.

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 which should be set to `0`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:BrowserAddProfileEnabled
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Microsoft
Edge\Enable profile creation from the Identity flyout menu or the Settings
page
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Enabled

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#browseraddprofileenabled

CIS Controls:

Version 7

16.6 Maintain an Inventory of Accounts
Maintain an inventory of all accounts organized by authentication system.

1.1.53 (L1) Ensure 'Enable renderer code integrity' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether unknown and potentially hostile code will be allowed to load inside of Microsoft Edge.

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

Rationale:

Disabling this setting could have a detrimental effect on Microsoft Edge's security and stability as unknown, hostile, and/or unstable code will be able to load within the browser's renderer processes.

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 which should be set to `1`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:RendererCodeIntegrityEnab
led
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Microsoft
Edge\Enable renderer code integrity
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Enabled.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#renderercodeintegrityenabled

CIS Controls:

Version 7

7.3 Limit Use of Scripting Languages in Web Browsers and Email Clients
Ensure that only authorized scripting languages are able to run in all web browsers and email clients.

1.1.54 (L1) Ensure 'Enable resolution of navigation errors using a web service' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether Microsoft Edge can issue a dataless connection to a web service to probe networks, (ex: Hotel and Airport Wi-Fi) for connectivity issues.

Note: Except on Windows 8 and later versions of Windows, Microsoft Edge *always* uses native APIs to resolve connectivity issues.

The recommended state for this setting is `Disabled`.

Rationale:

This setting could potentially allow information about the user's network to be disclosed.

Impact:

Microsoft Edge will use native APIs for potential resolution of network connectivity and navigation issues.

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 which should be set to `0`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:ResolveNavigationErrorsUs
eWebService
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Microsoft
Edge\Enable resolution of navigation errors using a web service
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Not Configured.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#resolvenavigationerrorsusewebservice

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.55 (L2) Ensure 'Enable Search suggestions' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This policy setting determines whether web search suggestions are used in Microsoft Edge Address bar and Auto-Suggest lists.

The recommended state for this setting is `Disabled`.

Rationale:

Characters that are typed by the user are sent to a search engine before the Enter key is pressed therefore, it is possible for unintended data to be sent.

Impact:

Users will not get customized web suggestions for search results, they will still receive local suggestions.

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 which should be set to `0`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:SearchSuggestEnabled
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Microsoft
Edge\Enable search suggestions
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Enabled - But users can change the setting.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#searchsuggestenabled

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.56 (L1) Ensure 'Enable security warnings for command-line flags' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting prevents Microsoft Edge from showing security warnings that potentially dangerous command-line flags are in use at its' launch.

The recommended state of this setting is 'Enabled'.

Rationale:

If Microsoft Edge is being launched with potentially dangerous flags this information should be exposed to the user as a warning, if not the user may be unintentionally using non-secure settings and be exposed to security flaws.

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 which should be set to `1`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:CommandLineFlagSecurityWa
rningsEnabled
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Microsoft
Edge\Enable security warnings for command-line flags
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Enabled.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#commandlineflagsecuritywarningsenabled

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.57 (L1) Ensure 'Enable site isolation for every site' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting ensures that each website runs in its own process so that a site will not be able to utilize or take data from another running site.

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

Rationale:

Enabling site isolation can help stop sites from inadvertently sharing data with other running sites. This will help protect data from un-trusted sources.

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 which should be set to `1`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:SitePerProcess
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Microsoft
Edge\Enable site isolation for every site
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Enabled.

Note: If this policy is disabled or not configured, a user can opt out of site isolation. (For example, by using "Disable site isolation" entry in edge://flags.) **Disabling the policy or not configuring the policy doesn't turn off Site Isolation.**

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#siteperprocess

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.58 (L2) Ensure 'Enable Translate' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This policy setting enables Microsoft translation services on Microsoft Edge. Microsoft Edge offers translation functionality to the user by showing an integrated translate flyout when appropriate, and a translate option on the right-click context menu.

The recommended setting is `Disabled`.

Rationale:

Data should not be shared with 3rd party vendors in an enterprise managed environment. Enabling this service could potentially allow sensitive information to be sent to a 3rd party for translation.

Impact:

The translate feature will not be available for users.

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 which should be set to `0`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:TranslateEnabled
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Microsoft
Edge\Enable Translate
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Not Configured.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#translateenabled

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.59 (L1) Ensure 'Enable usage and crash-related data reporting' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

The policy setting allows the reporting of usage and crash-related data to Microsoft.

Note: This policy is deprecated. It is currently supported but will become obsolete in Microsoft Edge v89. This policy will be replaced by the policy: *DiagnosticDatafor* on Windows 7, Windows 8, and macOS.

This policy will be replaced by *Allow Telemetry* on Windows 10.

For more information please visit Configure Windows diagnostic data in your organization (Windows 10) - Windows Privacy | Microsoft Docs.

The recommended state for this setting is `Disabled`.

Rationale:

Usage data and crash-related data could potentially contain sensitive information from the system's memory. Data should be protected and not shared with third-party vendors.

Impact:

Usage and crash-related data will not be sent to Microsoft.

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 which should be set to `0`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:MetricsReportingEnabled
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Microsoft
Edge\Enable usage and crash-related data reporting
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Not Configured.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#metricsreportingenabled

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.60 (L1) Ensure 'Enable use of ephemeral profiles' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether user profiles are switched to ephemeral mode. In ephemeral mode, profile data is saved on disk for the length of the session and then the data is deleted after the session is over. Therefore, no data is saved to the device.

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

Rationale:

Allowing use of ephemeral profiles allows a user to use Microsoft Edge with no data being logged to the system. Deleting browser data will delete information that may be important for a computer investigation and investigators such as Computer Forensics Analysts may not be able to retrieve pertinent information to the investigation.

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 which should be set to `0`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:ForceEphemeralProfiles
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Microsoft
Edge\Enable use of ephemeral profiles
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Disabled.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#forceephemeralprofiles

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.61 (L2) Ensure 'Enforce Bing SafeSearch' is set to 'Enabled: Configure moderate search restrictions in Bing' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This policy setting ensures that web search results with Bing are presented with the SafeSearch settings that can be specified in this setting.

The recommended state for this setting is `Enabled: Configure moderate search restrictions in Bing`.

Rationale:

Allowing search results to present sites that may have malicious content should be prohibited to help ensure users do not accidentally visit sites that are prone to malicious content including spyware, adware, and viruses.

Impact:

Users search results will be filtered and content such as adult text, videos and images will not be shown.

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 which should be set to `1`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:ForceBingSafeSearch
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: Configure moderate search restrictions in Bing`

```
Computer Configuration\Policies\Administrative Templates\Microsoft
Edge\Enforce Bing SafeSearch
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Disabled - But users can configure this policy.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#forcebingsafesearch

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.62 (L2) Ensure 'Enforce Google SafeSearch' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This policy setting ensures that web search results with Google are performed with SafeSearch set to active.

The recommended state for this setting is `Disabled`.

Rationale:

Allowing search results to present sites that may have malicious content should be prohibited to help ensure users do not accidentally visit sites that are more prone to malicious content including spyware, adware, and viruses.

Impact:

Users search results will be filtered and content such as adult text, videos and images will not be shown.

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 which should be set to `0`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:ForceGoogleSafeSearch
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Microsoft
Edge\Enforce Google SafeSearch
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Disabled - But users can set the value.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#forcegooglesafesearch

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.63 (L2) Ensure 'Extend Adobe Flash content setting to all content' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This policy setting allows Adobe Flash content embedded in websites to run.

The recommended state for this setting is `Disabled`.

Rationale:

Allowing flash plugins or 'hidden' Flash content could open up a user to malicious content and activity. In addition, Adobe Flash will no longer be supported by the manufacturer as of December 31, 2020.

Impact:

Adobe Flash content may be blocked from the end user.

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 which should be set to `0`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:RunAllFlashInAllowMode
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Microsoft
Edge\Extend Adobe Flash content setting to all content
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Disabled.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#runallflashinallowmode

CIS Controls:

Version 7

2.2 Ensure Software is Supported by Vendor
Ensure that only software applications or operating systems currently supported by the software's vendor are added to the organization's authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system.

1.1.64 (L1) Ensure 'Hide the First-run experience and splash screen' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether the First-run experience and splash screen is presented to the user the first time Microsoft Edge is opened. Some of the options presented to the user include the ability to import data from other web browsers on the system.

The recommended state for this setting is `Enabled`.

Rationale:

Allowing the First-run experience and configuration options could potentially allow the user to perform actions that are prohibited such as importing autofill, credit card, and other sensitive data.

Impact:

Users will not be prompted with the First-run experience screens.

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 which should be set to `1`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:HideFirstRunExperience
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Hide
the First-run experience and splash screen
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Disabled.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#hidefirstrunexperience

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.65 (L1) Ensure 'Manage exposure of local IP addresses by WebRTC' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting specifies a list of URLs or patterns which local IP address will be exposed by WebRTC.

Note: If this policy is enabled, disabled, or not configured, and *edge://flags/#enable-webrtc-hide-local-ips-with-mdns* is Disabled, WebRTC will expose local IP addresses.

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

Rationale:

Enabling this setting and allowing exposure of IP addresses can allow an attacker to gather information about the internal network that could potentially be utilized to breach and traverse a network.

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 will have **no registry** value if it is set to `Disabled`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge\WebRtcLocalIpsAllowedUrls
:Default
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Microsoft
Edge\Manage exposure of local IP addressess by WebRTC
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Disabled.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#webrtclocalipsallowedurls

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.66 (L1) Ensure 'Notify a user that a browser restart is recommended or required for pending updates' is set to 'Enabled: Required - Show a recurring prompt to the user indicating that a restart is required' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This setting determines whether the a notification to restart Microsoft Edge due to an update is recommended or required.

Note: If this setting is set to `Enabled: Required - Show a recurring prompt to the user indicating that a restart is required` the browser will be automatically restarted based on the *RelaunchNotificationPeriod* setting which is recommended to be 24 hours.

The recommended state for this setting is: `Enabled: Required - Show a recurring prompt to the user indicating that a restart is required`.

Rationale:

The end-user will receive a notification informing them that an update has been applied and that the browser must be restarted in order for the update to be completed. Once updates have been pushed by the organization it is pertinent that the update is applied as soon as possible. Enabling this notification will ensure that users restart their browser in a timely fashion.

Impact:

When updates are applied by an organization the end-user will receive a notification after 24 hours that they must restart the browser for updates to complete, after 24 hours the browser will be automatically restarted.

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 which should be set to `2`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:RelaunchNotification
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: Required - Show a recurring prompt to the user indicating that a restart is required`

```
Computer Configuration\Policies\Administrative Templates\Microsoft
Edge\Notify a user that a browser restart is recommended or required for
pending updates
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Not Configured - An icon is shown in the browser informing the user to restart Microsoft Edge.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#relaunchnotification

CIS Controls:

Version 7

3.5 Deploy Automated Software Patch Management Tools
Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.

1.1.67 (L1) Ensure 'Restrict exposure of local IP address by WebRTC' is set to 'Enabled: Allow public interface over http default route. This doesn't expose the local IP address' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting specifies whether the local IP address will be exposed by WebRTC.

The recommended state for this setting is `Enabled: Allow public interface over http default route. This doesn't expose the local IP address`.

Rationale:

Allowing the exposure of IP addresses allows attacker to gather information on the internal network that could potentially be utilized to breach and traverse the network.

Impact:

The local IP address will not be exposed.

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 which should be set to `default_public_interface_only`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:WebRtcLocalhostIpHandling
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: Allow public interface over http default route. This doesn't expose the local IP address`

```
Computer Configuration\Policies\Administrative Templates\Microsoft
Edge\Restrict exposure of local IP address by WebRTC
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Disabled - WebRTC exposes the local IP address.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#webrtclocalhostiphandling

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.68 (L1) Ensure 'Send site information to improve Microsoft services' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether information about visited websites in Microsoft Edge is sent to Microsoft.

The recommended state for this setting is `Disabled`.

Rationale:

Data should not be shared with 3rd party vendors in an enterprise managed environment.

Impact:

Information about visited sites as well as diagnostic data (Default - Required diagnostic data (formally known as Basic)), such as device, battery, networking, processor and memory, virtualization, operating system, and Windows storage attributes.

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 which should be set to `0`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:SendSiteInfoToImproveServ
ices
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Send
site information to improve Microsoft services
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Enabled - Required diagnostic data (formally known as Basic).

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#sendsiteinfotoimproveservices

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.69 (L1) Ensure 'Set disk cache size, in bytes' is set to 'Enabled: 250609664' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This setting controls the size of the cache, in bytes, used to store files on the disk.

The recommended state for this setting is: `Enabled: 250609664`

Note: The value specified in this policy isn't a hard boundary but rather a suggestion to the caching system; any value below a few megabytes is too small and will be rounded up to a reasonable minimum.

Note #2: The recommended disk size for cache is 50 - 250MB, according to Microsoft.

Rationale:

Having enough disk space for browser cache is important for a computer investigation and investigators such as Computer Forensics Analysts to be able to retrieve pertinent information to the investigation.

Impact:

Browser cache will take up to 250MB in disk space.

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 which should be set to `ef00000`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:DiskCacheSize
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: 250609664`

```
Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Set
disk cache size, in bytes
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Enabled - Default size is used.

References:

1. https://docs.microsoft.com/en-us/deployedge/microsoft-edge-policies#diskcachesize

CIS Controls:

Version 7

6.4 Ensure adequate storage for logs
Ensure that all systems that store logs have adequate storage space for the logs generated.

1.1.70 (L1) Ensure 'Set the time period for update notifications' is set to 'Enabled: 86400000' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This setting does not determine if updates are applied, the policy setting allows setting a time period in which users are notified that Microsoft Edge has been updated and must be closed and re-opened.

The recommended state for this setting is: `Enabled: 86400000`.

Rationale:

This setting is a notification for the end-user informing them that an update has been applied and that the browser must be restarted in order for the update to be completed. Once updates have been pushed by the organization it is pertinent that said update takes affect as soon as possible. Enabling this notification will ensure users restart the browser in a timely fashion.

Impact:

When updates are applied by an organization the end-user will receive a notification after 24 hours that they must restart the browser for updates to complete.

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 which should be set to `5265c00`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:RelaunchNotificationPerio
d
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: 86400000`

```
Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Set
the time period for update notifications
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Enabled - One week.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#relaunchnotificationperiod

CIS Controls:

Version 7

3.5 Deploy Automated Software Patch Management Tools
Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.

1.1.71 (L2) Ensure 'Show an "Always open" checkbox in external protocol dialog' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This policy setting controls if the user is prompted with an "Always open" check box when an external protocol prompt is show.

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

Rationale:

Allowing a protocol to automatically always open for webpages could allow a malicious website to open programs on a device leaving it open to attacks.

Impact:

The end user will be prompted each time they click a link that opens an external protocol, even if they have utilized it before.

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 which should be set to `0`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:ExternalProtocolDialogSho
wAlwaysOpenCheckbox
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Show
an "Always open" checkbox in external protocol dialog
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Enabled. (v84 or greater)

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#externalprotocoldialogshowalwaysopencheckbox

CIS Controls:

Version 7

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.

1.1.72 (L2) Ensure 'Specify if online OCSP/CRL checks are required for local trust anchors' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This policy setting controls whether online certificate revocation checks (OCSP/CRL) are required and if a check online is not possible the certificate will be treated as though it is revoked.

The recommended state for this is `Enabled`.

Rationale:

Certificates should always be validated, not doing so could potentially allow a revoked certificate being used to give a false sense of a secure connection.

Impact:

If Microsoft Edge is not able to obtain a revocation status, the certificate will be treated as though it is revoked, therefore the website will not be loaded.

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 which should be set to `1`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:RequireOnlineRevocationCh
ecksForLocalAnchors
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Microsoft
Edge\Specify if online OCSP/CRL checks are required for local trust anchors
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Disabled

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#requireonlinerevocationchecksforlocalanchors

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.73 (L1) Ensure 'Suggest similar pages when a webpage can’t be found' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether Microsoft Edge may connect to a web service to generate URLs and search suggestions for website connectivity issues. If disabled standard errors will be issued, if enabled errors will be customized with URL suggestions.

The recommended state for this setting is `Disabled`.

Rationale:

This setting could potentially lead to a leak of information regarding the types of websites being visited, it may also open users up to redirection to a malicious site in the event that the service generating information becomes compromised.

Impact:

Users will still be presented an error in the event that a website cannot be reached however, the message may be more generic than the user would get in the instance of this service being 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 which should be set to `0`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:AlternateErrorPagesEnable
d
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Microsoft
Edge\Suggest similar pages when a webpage can’t be found
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Not Configured - Users will have the option to enable this setting with the edge://settings/privacy page.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#alternateerrorpagesenabled

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.2 Cast

This section contains recommendations for Microsoft Edge Cast settings.

This Group Policy section is provided by the Group Policy template `MSEdge.admx/adml` that is included with the Microsoft Edge v85 Administrative Templates (or newer).

1.2.1 (L1) Ensure 'Enable Google Cast' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting determines whether users may utilize Google Cast. Note that when this setting is set to `Disabled` the *Show the cast icon in the toolbar* setting is ignored as the icon is removed.

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

Rationale:

The use of Google Cast could allow users to show potentially sensitive information to non-trusted devices. These devices could be in public areas.

Impact:

Users will not be able to utilize Google Cast and the Google Cast icon will not be displayed in Microsoft Edge.

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 which should be set to `0`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:EnableMediaRouter
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Microsoft
Edge\Cast\Enable Google Cast
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Enabled.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#enablemediarouter

CIS Controls:

Version 7

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.

1.3 Content Settings

This section contains recommendations for Microsoft Edge Content settings.

This Group Policy section is provided by the Group Policy template `MSEdge.admx/adml` that is included with the Microsoft Edge v85 Administrative Templates (or newer).

1.3.1 (L2) Ensure 'Control use of the Web Bluetooth API' is set to 'Enabled: Do not allow any site to request access to Bluetooth' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This policy setting controls whether websites can access connected Bluetooth devices.

The recommended state for this setting is: `Enabled: Do not allow any site to request access to Bluetooth devices via the Web Bluetooth API`.

Rationale:

Web Bluetooth could potentially be used for attacks that may bypass other controls regarding connected Bluetooth hardware including microphones, cameras, and other devices which information could be gathered from or inappropriately utilzed.

Impact:

Websites will be unable to utilize connected Bluetooth devices via the API, this includes web cameras, microphones, and other USB devices.

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 which should be set to `2`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:DefaultWebBluetoothGuardS
etting
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`: `Do not allow any site to request access to Bluetooth devices via the Web Bluetooth API`

```
Computer Configuration\Policies\Administrative Templates\Microsoft
Edge\Content settings\Control use of the Web Bluetooth API
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Enabled - Users will be asked whether websites can access any Bluetooth device. Users may change this setting.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#defaultwebbluetoothguardsetting

CIS Controls:

Version 7

15.9 Disable Wireless Peripheral Access of Devices
Disable wireless peripheral access of devices (such as Bluetooth and NFC), unless such access is required for a business purpose.

1.3.2 (L2) Ensure 'Control use of the WebUSB API' is set to 'Enabled: Do not allow any site to request access to USB' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This policy setting controls whether websites can access connected USB devices.

The recommended state for this setting is `Enabled: Do not allow any site to request access to USB devices via the WebUSB API`.

Rationale:

WebUSB could potentially be used for attacks that may bypass other controls regarding connected USB hardware including hardware authentication devices.

Impact:

Websites will be unable to utilize connected USB devices via the API, this includes web cameras, microphones, and other USB devices.

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 which should be set to `2`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:DefaultWebUsbGuardSetting
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: Don't allow any site to request access to USB devices via the WebUSB API`

```
Computer Configuration\Policies\Administrative Templates\Microsoft
Edge\Content settings\Control use of the WebUSB API
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Enabled - Users will be asked whether websites can access USB devices. Users may change this setting.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#defaultwebusbguardsetting

CIS Controls:

Version 7

13.7 Manage USB Devices
If USB storage devices are required, enterprise software should be used that can configure systems to allow the use of specific devices. An inventory of such devices should be maintained.

1.3.3 (L2) Ensure 'Default Adobe Flash setting' is set to 'Enabled: Block the Adobe Flash plug-in' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This policy setting determines whether the use of Adobe Flash will be allowed for websites visited inside of Microsoft Edge.

The recommended setting is `Enabled: Block the Adobe Flash plug-in`

Rationale:

Adobe Flash has many known vulnerabilities which can expose a users machine to several attacks, furthermore Adobe Flash will be discontinued in the future.

Impact:

Websites using Adobe Flash will not operate as expected.

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 which should be set to `2`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:DefaultPluginsSetting
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Microsoft
Edge\Content settings\Default Adobe Flash setting
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Not Configured - But the user can change this setting.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#defaultpluginssetting

CIS Controls:

Version 7

7.2 Disable Unnecessary or Unauthorized Browser or Email Client Plugins
Uninstall or disable any unauthorized browser or email client plugins or add-on applications.

1.3.4 (L1) Ensure 'Default geolocation setting' is set to 'Enabled: Don't allow any site to track users physical location' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether a users' physical location can be tracked by websites.

The recommended state for this setting is: `Enabled: Don't allow any site to track users' physical location`.

Rationale:

Geolocation should not be shared with websites to ensure protection of the users privacy regarding location. Additionally location information could lead to clues regarding the users network infrastructure surrounding the device they are utilizing.

Impact:

Location information will not be shared with websites in Microsoft Edge. This could have an affect on websites that utilize this information for customized content.

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 which should be set to `2`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:DefaultGeolocationSetting
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: Don't allow any site to track users' physical location`

```
Computer Configuration\Policies\Administrative Templates\Microsoft
Edge\Content settings\Default geolocation setting
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Enabled: Ask whenever a site wants to track users' physical location.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#defaultgeolocationsetting

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.4 Default search provider

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

This Group Policy section is provided by the Group Policy template `MSEdge.admx/adml` that is included with the Microsoft Edge v85 Administrative Templates (or newer).

1.5 Extensions

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

This Group Policy section is provided by the Group Policy template `MSEdge.admx/adml` that is included with the Microsoft Edge v85 Administrative Templates (or newer).

1.6 HTTP authentication

This section contains recommendations for Microsoft Edge HTTP authentication settings.

This Group Policy section is provided by the Group Policy template `MSEdge.admx/adml` that is included with the Microsoft Edge v85 Administrative Templates (or newer).

1.6.1 (L1) Ensure 'Allow cross-origin HTTP Basic Auth prompts' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether third-party sub-content can open a HTTP Basic Auth dialog and is typically disabled.

The recommended state for this setting is `Disabled`.

Rationale:

This setting is typically disabled to help combat phishing attempts.

Impact:

Disabling this setting should have minimal impact to the user as it is typically disabled by default and third-party sub-content can't open a HTTP Basic Auth dialog box.

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 which should be set to `0`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:AllowCrossOriginAuthPromp
t
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Microsoft Edge\HTTP
authentication\Allow cross-origin HTTP Basic Auth prompts
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Disabled.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#allowcrossoriginauthprompt

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.6.2 (L2) Ensure 'Supported authentication schemes' is set to 'Enabled: digest, ntlm, negotiate' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This setting specifies what HTTP authentication methods are supported.

The recommended setting is `Enabled: digest, ntlm, negotiate`.

Rationale:

Basic authentication is the least secure method of authenticating as it sends username and password information in un-encrypted form which should never be done for security reasons.

Impact:

Any sites that utilizes Basic Authentication will be impacted. Sites will need to be reconfigured to support a more secure form of authentication.

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 which should be set to `digest, ntlm, negotiate`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:AuthSchemes
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Microsoft Edge\HTTP
authentication\Supported authentication schemes
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Enabled - The following schemes will be used: basic, digest, ntlm, and negotiate.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#authschemes
2. https://www.chromium.org/developers/design-documents/http-authentication

CIS Controls:

Version 7

16.5 Encrypt Transmittal of Username and Authentication Credentials
Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.

1.7 Native Messaging

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

This Group Policy section is provided by the Group Policy template `MSEdge.admx/adml` that is included with the Microsoft Edge v85 Administrative Templates (or newer).

1.8 Password manager and protection

This section contains recommendations for Microsoft Edge Password manager and protection settings.

This Group Policy section is provided by the Group Policy template `MSEdge.admx/adml` that is included with the Microsoft Edge v85 Administrative Templates (or newer).

1.8.1 (L1) Ensure 'Enable saving passwords to the password manager' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting enables or disables the ability for users to save their passwords in Microsoft Edge.

The recommended state for this setting is `Disabled`.

Rationale:

Saving passwords in Edge could lead to a users web passwords being breached if an attacker were to gain access to their web browser especially in the case of an unattended and unlocked workstation.

Impact:

Users will be unable to utilize the Microsoft Edge built-in password manager.

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 which should be set to `0`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:PasswordManagerEnabled
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Microsoft
Edge\Password manager and protection\Enable saving passwords to the password
manager
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Enabled - But the user can change this setting.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#passwordmanagerenabled

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.9 Printing

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

This Group Policy section is provided by the Group Policy template `MSEdge.admx/adml` that is included with the Microsoft Edge v85 Administrative Templates (or newer).

1.10 Proxy server

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

This Group Policy section is provided by the Group Policy template `MSEdge.admx/adml` that is included with the Microsoft Edge v85 Administrative Templates (or newer).

1.11 SmartScreen settings

This section contains recommendations for Microsoft Edge SmartScreen settings.

This Group Policy section is provided by the Group Policy template `MSEdge.admx/adml` that is included with the Microsoft Edge v85 Administrative Templates (or newer).

1.11.1 (L1) Ensure 'Configure Microsoft Defender SmartScreen' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting allows configuration of Microsoft Defender SmartScreen. Microsoft Defender SmartScreen helps to identify phishing and malware websites and to make informed decisions about downloads.

The recommended state for this setting is `Enabled`.

Rationale:

Windows Defender SmartScreen can provide messages and warnings to users to help thwart phishing attempts and malicious software.

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 which should be set to `1`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:SmartScreenEnabled
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Microsoft
Edge\SmartScreen settings\Configure Microsoft Defender SmartScreen
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Not Configured - But the user can change this setting.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#smartscreenenabled

CIS Controls:

Version 7

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.

1.11.2 (L1) Ensure 'Configure Microsoft Defender SmartScreen to block potentially unwanted apps' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting allows configuration of Microsoft Defender SmartScreen and whether potentially unwanted apps are blocked.

The recommended state for this setting is `Enabled`.

Rationale:

Windows Defender SmartScreen can block unwanted apps that will help inform and protect users from vulnerabilities related to adware and low-reputation apps.

Impact:

Microsoft Defender SmartScreen will block potentially dangerous apps. This could stop the user from installing an app that could be potentially harmful to 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 which should be set to `1`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:SmartScreenPuaEnabled
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Microsoft
Edge\SmartScreen settings\Configure Microsoft Defender SmartScreen to block
potentially unwanted apps
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Not Configured - But the user can change this setting.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#smartscreenpuaenabled

CIS Controls:

Version 7

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.

1.11.3 (L1) Ensure 'Force Microsoft Defender SmartScreen checks on downloads from trusted sources' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether Microsoft Defender SmartScreen can check if downloads have been retrieved from a trusted source.

The recommended state for this setting is `Enabled`.

Rationale:

Windows Defender SmartScreen can verify that downloads are from a trusted source will can greatly reduce the chances of a user downloading an infected package to their machine.

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 which should be set to `1`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:SmartScreenForTrustedDown
loadsEnabled
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Force
Microsoft Defender SmartScreen checks on downloads from trusted sources
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Enabled - But the user can change this setting.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#smartscreenfortrusteddownloadsenabled

CIS Controls:

Version 7

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.

1.11.4 (L1) Ensure 'Prevent bypassing Microsoft Defender SmartScreen prompts for sites' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether users may bypass the SmartScreen warning if a site is deemed unsafe.

The recommended state for this setting is `Enabled`.

Rationale:

Windows Defender SmartScreen can provide messages and warnings to users to help thwart phishing and malicious software however, by default, users may bypass these warnings.

Impact:

SmartScreen will not allow a user to bypass the warning message.

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 which should be set to `1`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:PreventSmartScreenPromptO
verride
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Microsoft
Edge\SmartScreen settings\Prevent bypassing Microsoft Defender SmartScreen
prompts for sites
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Disabled.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#preventsmartscreenpromptoverride

CIS Controls:

Version 7

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.

1.11.5 (L1) Ensure 'Prevent bypassing of Microsoft Defender SmartScreen warnings about downloads' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether users may override Microsoft Defender SmartScreen warnings regarding downloads that are unverified.

The recommended state for this setting is `Enabled`.

Rationale:

Smartscreen checks downloads and verifies whether they are deemed safe or not. Only allowing verified downloads greatly reduces risk of a download containing a virus, spyware, or other unwanted software.

Impact:

User will not be able to download software that has not been verified by SmartScreen.

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 which should be set to `1`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge:PreventSmartScreenPromptO
verrideForFiles
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Microsoft
Edge\SmartScreen settings\Prevent bypassing of Microsoft Defender SmartScreen
warnings about downloads
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSEdge.admx/adml` that can be downloaded from Microsoft here.

Default Value:

Disabled.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#preventsmartscreenpromptoverrideforfiles

CIS Controls:

Version 7

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 Startup, home page and new tab page

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

This Group Policy section is provided by the Group Policy template `MSEdge.admx/adml` that is included with the Microsoft Edge v85 Administrative Templates (or newer).

2 Microsoft Edge - Default Settings (users can override)

This section is intentionally blank and exists to ensure the structure of Microsoft Edge benchmark is consistent.

These policy settings may be overridden by the user therefor no policy configurations are recommended for this section.

This Group Policy section is provided by the Group Policy template `MSEdge.admx/adml` that is included with the Microsoft Edge v85 Administrative Templates (or newer).

3 Microsoft Edge Update

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

This Group Policy section is provided by the Group Policy template `MSEdge.admx/adml` that is included with the Microsoft Edge v85 Administrative Templates (or newer).

Appendix: Summary Table

Control		Set Correctly	
		Yes	No
1	**Microsoft Edge**		
1.1	**Microsoft Edge**		
1.1.1	(L1) Ensure 'Ads setting for sites with intrusive ads' is set to 'Enabled: Block ads on sites with intrusive ads' (Automated)	□	□
1.1.2	(L1) Ensure 'Allow download restrictions' is set to 'Enabled: Block potentially dangerous downloads' (Automated)	□	□
1.1.3	(L2) Ensure 'Allow file selection dialog' is set to 'Disabled' (Automated)	□	□
1.1.4	(L1) Ensure 'Allow Google Cast to connect to Cast devices on all IP addresses' is set to 'Disabled' (Automated)	□	□
1.1.5	(L1) Ensure 'Allow importing of autofill form data' is set to 'Disabled' (Automated)	□	□
1.1.6	(L1) Ensure 'Allow importing of browser settings' is set to 'Disabled' (Automated)	□	□
1.1.7	(L1) Ensure 'Allow importing of home page settings' is set to 'Disabled' (Automated)	□	□
1.1.8	(L1) Ensure 'Allow importing of payment info' is set to 'Disabled' (Automated)	□	□
1.1.9	(L1) Ensure 'Allow importing of saved passwords' is set to 'Disabled' (Automated)	□	□
1.1.10	(L1) Ensure 'Allow importing of search engine settings' is set to 'Disabled' (Automated)	□	□
1.1.11	(L1) Ensure 'Allow managed extensions to use the Enterprise Hardware Platform API' is set to 'Disabled' (Automated)	□	□
1.1.12	(L2) Ensure 'Allow or block audio capture' is set to 'Disabled' (Automated)	□	□
1.1.13	(L2) Ensure 'Allow or block video capture' is set to 'Disabled' (Automated)	□	□
1.1.14	(L2) Ensure 'Allow or deny screen capture' is set to 'Disabled' (Automated)	□	□
1.1.15	(L1) Ensure 'Allow personalization of ads search and news by sending browsing history to Microsoft' is set to 'Disabled' (Automated)	□	□
1.1.16	(L1) Ensure 'Allow queries to a Browser Network Time service' is set to 'Enabled' (Automated)	□	□
1.1.17	(L2) Ensure 'Allow suggestions from local providers' is set to 'Disabled' (Automated)	□	□

1.1.18	(L1) Ensure 'Allow the audio sandbox to run' is set to 'Enabled' (Automated)	□	□
1.1.19	(L1) Ensure 'Allow user feedback' is set to 'Disabled' (Automated)	□	□
1.1.20	(L2) Ensure 'Allow users to open files using the ClickOnce protocol' is set to 'Disabled' (Automated)	□	□
1.1.21	(L2) Ensure 'Allow users to open files using the DirectInvoke protocol' is set to 'Disabled' (Automated)	□	□
1.1.22	(L2) Ensure 'Allow users to proceed from the HTTPS warning page' is set to 'Disabled' (Automated)	□	□
1.1.23	(L1) Ensure 'Allow websites to query for available payment methods' is set to 'Disabled' (Automated)	□	□
1.1.24	(L1) Ensure 'Allows a page to show popups during its unloading' is set to 'Disabled' (Automated)	□	□
1.1.25	(L2) Ensure 'Ask where to save downloaded files' is set to 'Disabled' (Automated)	□	□
1.1.26	(L1) Ensure 'Automatically import another browser's data and settings at first run' is set to 'Enabled: Disables automatic import, and the import section of the first-run experience is skipped' (Automated)	□	□
1.1.27	(L2) Ensure 'Block third party cookies' is set to 'Enabled' (Automated)	□	□
1.1.28	(L1) Ensure 'Block tracking of users' web-browsing activity' is set to 'Enabled: Balanced (Blocks harmful trackers and trackers from sites user has not visited; content and ads will be less personalized)' (Automated)	□	□
1.1.29	(L2) Ensure 'Browser sign-in settings' is set to 'Enabled: Disable browser sign-in' (Automated)	□	□
1.1.30	(L1) Ensure 'Clear browsing data when Microsoft Edge closes' is set to 'Disabled' (Automated)	□	□
1.1.31	(L1) Ensure 'Clear cached images and files when Microsoft Edge closes' is set to 'Disabled' (Automated)	□	□
1.1.32	(L1) Ensure 'Configure InPrivate mode availability' is set to 'Enabled: InPrivate mode disabled' (Automated)	□	□
1.1.33	(L2) Ensure 'Configure Online Text To Speech' is set to 'Disabled' (Automated)	□	□
1.1.34	(L1) Ensure 'Configure the list of names that will bypass the HSTS policy check' is set to 'Disabled' (Manual)	□	□
1.1.35	(L1) Ensure 'Configure the list of types that are excluded from synchronization' is set to 'Enabled' (Automated)	□	□
1.1.36	(L1) Ensure 'Configure the Share experience' is set to 'Enabled: Don't allow using the Share experience' (Automated)	□	□

1.1.37	(L1) Ensure 'Continue running background apps after Microsoft Edge closes' is set to 'Disabled' (Automated)	□	□
1.1.38	(L1) Ensure 'Control communication with the Experimentation and Configuration Service' is set to 'Enabled: Disable communication with the Experimentation and Configuration Service' (Automated)	□	□
1.1.39	(L1) Ensure 'Delete old browser data on migration' is set to 'Disabled' (Automated)	□	□
1.1.40	(L1) Ensure 'Disable saving browser history' is set to 'Disabled' (Automated)	□	□
1.1.41	(L1) Ensure 'Disable synchronization of data using Microsoft sync services' is set to 'Enabled' (Automated)	□	□
1.1.42	(L1) Ensure 'DNS interception checks enabled' is set to 'Enabled' (Automated)	□	□
1.1.43	(L1) Ensure 'Enable AutoFill for addresses' is set to 'Disabled' (Automated)	□	□
1.1.44	(L1) Ensure 'Enable AutoFill for credit cards' is set to 'Disabled' (Automated)	□	□
1.1.45	(L1) Ensure 'Enable component updates in Microsoft Edge' is set to 'Enabled' (Automated)	□	□
1.1.46	(L1) Ensure 'Enable deleting browser and download history' is set to 'Disabled' (Automated)	□	□
1.1.47	(L1) Ensure 'Enable globally scoped HTTP auth cache' is set to 'Disabled' (Automated)	□	□
1.1.48	(L2) Ensure 'Enable guest mode' is set to 'Disabled' (Automated)	□	□
1.1.49	(L1) Ensure 'Enable network prediction' is set to 'Enabled: Don't predict network actions on any network connection' (Automated)	□	□
1.1.50	(L2) Ensure 'Enable online OCSP/CRL checks' is set to 'Enabled' (Automated)	□	□
1.1.51	(L1) Ensure 'Enable Proactive Authentication' is set to 'Disabled' (Automated)	□	□
1.1.52	(L1) Ensure 'Enable profile creation from the Identity flyout menu or the Settings page' is set to 'Disabled' (Automated)	□	□
1.1.53	(L1) Ensure 'Enable renderer code integrity' is set to 'Enabled' (Automated)	□	□
1.1.54	(L1) Ensure 'Enable resolution of navigation errors using a web service' is set to 'Disabled' (Automated)	□	□
1.1.55	(L2) Ensure 'Enable Search suggestions' is set to 'Disabled' (Automated)	□	□
1.1.56	(L1) Ensure 'Enable security warnings for command-line flags' is set to 'Enabled' (Automated)	□	□

1.1.57	(L1) Ensure 'Enable site isolation for every site' is set to 'Enabled' (Automated)	□	□
1.1.58	(L2) Ensure 'Enable Translate' is set to 'Disabled' (Automated)	□	□
1.1.59	(L1) Ensure 'Enable usage and crash-related data reporting' is set to 'Disabled' (Automated)	□	□
1.1.60	(L1) Ensure 'Enable use of ephemeral profiles' is set to 'Disabled' (Automated)	□	□
1.1.61	(L2) Ensure 'Enforce Bing SafeSearch' is set to 'Enabled: Configure moderate search restrictions in Bing' (Automated)	□	□
1.1.62	(L2) Ensure 'Enforce Google SafeSearch' is set to 'Disabled' (Automated)	□	□
1.1.63	(L2) Ensure 'Extend Adobe Flash content setting to all content' is set to 'Disabled' (Automated)	□	□
1.1.64	(L1) Ensure 'Hide the First-run experience and splash screen' is set to 'Enabled' (Automated)	□	□
1.1.65	(L1) Ensure 'Manage exposure of local IP addresses by WebRTC' is set to 'Disabled' (Automated)	□	□
1.1.66	(L1) Ensure 'Notify a user that a browser restart is recommended or required for pending updates' is set to 'Enabled: Required - Show a recurring prompt to the user indicating that a restart is required' (Automated)	□	□
1.1.67	(L1) Ensure 'Restrict exposure of local IP address by WebRTC' is set to 'Enabled: Allow public interface over http default route. This doesn't expose the local IP address' (Automated)	□	□
1.1.68	(L1) Ensure 'Send site information to improve Microsoft services' is set to 'Disabled' (Automated)	□	□
1.1.69	(L1) Ensure 'Set disk cache size, in bytes' is set to 'Enabled: 250609664' (Automated)	□	□
1.1.70	(L1) Ensure 'Set the time period for update notifications' is set to 'Enabled: 86400000' (Automated)	□	□
1.1.71	(L2) Ensure 'Show an "Always open" checkbox in external protocol dialog' is set to 'Disabled' (Automated)	□	□
1.1.72	(L2) Ensure 'Specify if online OCSP/CRL checks are required for local trust anchors' is set to 'Enabled' (Automated)	□	□
1.1.73	(L1) Ensure 'Suggest similar pages when a webpage can’t be found' is set to 'Disabled' (Automated)	□	□
1.2	**Cast**		
1.2.1	(L1) Ensure 'Enable Google Cast' is set to 'Disabled' (Automated)	□	□
1.3	**Content Settings**		

1.3.1	(L2) Ensure 'Control use of the Web Bluetooth API' is set to 'Enabled: Do not allow any site to request access to Bluetooth' (Automated)	□	□
1.3.2	(L2) Ensure 'Control use of the WebUSB API' is set to 'Enabled: Do not allow any site to request access to USB' (Automated)	□	□
1.3.3	(L2) Ensure 'Default Adobe Flash setting' is set to 'Enabled: Block the Adobe Flash plug-in' (Automated)	□	□
1.3.4	(L1) Ensure 'Default geolocation setting' is set to 'Enabled: Don't allow any site to track users physical location' (Automated)	□	□
1.4	**Default search provider**		
1.5	**Extensions**		
1.6	**HTTP authentication**		
1.6.1	(L1) Ensure 'Allow cross-origin HTTP Basic Auth prompts' is set to 'Disabled' (Automated)	□	□
1.6.2	(L2) Ensure 'Supported authentication schemes' is set to 'Enabled: digest, ntlm, negotiate' (Automated)	□	□
1.7	**Native Messaging**		
1.8	**Password manager and protection**		
1.8.1	(L1) Ensure 'Enable saving passwords to the password manager' is set to 'Disabled' (Automated)	□	□
1.9	**Printing**		
1.10	**Proxy server**		
1.11	**SmartScreen settings**		
1.11.1	(L1) Ensure 'Configure Microsoft Defender SmartScreen' is set to 'Enabled' (Automated)	□	□
1.11.2	(L1) Ensure 'Configure Microsoft Defender SmartScreen to block potentially unwanted apps' is set to 'Enabled' (Automated)	□	□
1.11.3	(L1) Ensure 'Force Microsoft Defender SmartScreen checks on downloads from trusted sources' is set to 'Enabled' (Automated)	□	□
1.11.4	(L1) Ensure 'Prevent bypassing Microsoft Defender SmartScreen prompts for sites' is set to 'Enabled' (Automated)	□	□
1.11.5	(L1) Ensure 'Prevent bypassing of Microsoft Defender SmartScreen warnings about downloads' is set to 'Enabled' (Automated)	□	□
1.12	**Startup, home page and new tab page**		
2	**Microsoft Edge - Default Settings (users can override)**		
3	**Microsoft Edge Update**		

Appendix: Change History

Date	Version	Changes for this version
10-27-2020	1.0.0	Initial Release
05-18-2022	1.0.1	UPDATE - 1.1 (L1) Ensure 'Manage exposure of local IP addresses by WebRTC' is set to 'Disabled' Ticket# 15471