CIS Microsoft Intune for Edge Benchmark

v1.0.0 - 01-28-2026

Terms of Use

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

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

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

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

Table of Contents

Terms of Use *1*

Table of Contents *2*

Overview *8*

Important Usage Information **8**

Key Stakeholders **8**

Apply the Correct Version of a Benchmark **9**

Exceptions **9**

Remediation **10**

Summary **10**

Target Technology Details **11**

Intended Audience **11**

Consensus Guidance **12**

Typographical Conventions **13**

Recommendation Definitions *14*

Title **14**

Assessment Status **14**

Automated **14**

Manual **14**

Profile **14**

Description **14**

Rationale Statement **14**

Impact Statement **15**

Audit Procedure **15**

Remediation Procedure **15**

Default Value **15**

References **15**

CIS Critical Security Controls® (CIS Controls®) **15**

Additional Information **15**

Profile Definitions **16**

Acknowledgements **17**

Recommendations *18*

1 Microsoft Edge **18**

1.1 Application Guard settings **18**

1.2 Cast **19**

1.2.1 (L1) Ensure 'Enable Google Cast' is set to 'Disabled' (Automated) 20

1.3 Certificate management settings **22**

1.3.1 (L1) Ensure 'Allow users to manage installed CA certificates' is set to 'Enabled: Disallow users from managing certificates' (Automated) 23
1.4 Content Settings 25
1.4.1 (L2) Ensure 'Allow read access via the File System API on these sites' is set to 'Disabled' (Automated) 26
1.4.2 (L2) Ensure 'Choose whether users can receive customized background images and text, suggestions, notifications, and tips for Microsoft services' is set to 'Disabled' (Automated) 28
1.4.3 (L1) Ensure 'Control use of insecure content exceptions' is set to 'Enabled: Do not allow any site to load blockable mixed content' (Automated) 30
1.4.4 (L2) Ensure 'Control use of JavaScript JIT' is set to 'Enabled: Do not allow any site to run JavaScript JIT' (Automated) 32
1.4.5 (L2) Ensure 'Control use of the File System API for reading' is set to 'Enabled: Don't allow any site to request read access to files and directories via the File System API' (Automated) 34
1.4.6 (L1) Ensure 'Control use of the File System API for writing' is set to 'Enabled: Don't allow any site to request write access to files and directories' (Automated) 36
1.4.7 (L2) Ensure 'Control use of the Web Bluetooth API' is set to 'Enabled: Do not allow any site to request access to Bluetooth devices via the Web Bluetooth API' (Automated) 38
1.4.8 (L2) Ensure 'Control use of the WebHID API' is set to 'Enabled: Do not allow any site to request access to HID devices via the WebHID API' (Automated) 40
1.4.9 (L1) Ensure 'Default automatic downloads setting' is set to 'Enabled: Don´t allow any website to perform automatic downloads' (Automated) 42
1.4.10 (L1) Ensure 'Default geolocation setting' is set to 'Enabled: Don't allow any site to track users' physical location' (Automated) 44
1.4.11 (L2) Ensure 'Default setting for third-party storage partitioning' is set to 'Enabled: Block third-party storage partitioning from being enabled.' (Automated) 46
1.5 Default search provider 48
1.6 Downloads 49
1.6.1 (L1) Ensure 'Enable insecure download warnings' is set to 'Enabled' (Automated) 50
1.7 Edge Website Typo Protection settings 52
1.7.1 (L1) Ensure 'Configure Edge Website Typo Protection' is set to 'Enabled' (Automated) 53
1.8 Edge Workspaces settings 55
1.9 Experimentation 56
1.9.1 (L1) Ensure 'Configure users ability to override feature flags' is set to 'Enabled: Prevent users from overriding feature flags' (Automated) 57
1.10 Extensions 59
1.10.1 (L1) Ensure 'Blocks external extensions from being installed' is set to 'Enabled' (Automated) 60
1.10.2 (L2) Ensure 'Configure extension management settings' is set to 'Enabled: { "*": {"installation_mode": "blocked" }}' (Automated) 62
1.11 Games settings 64
1.11.1 (L1) Ensure 'Enable Gamer Mode' is set to 'Disabled' (Automated) 65
1.12 Generative AI 67
1.13 HTTP authentication 68
1.13.1 (L1) Ensure 'Allow Basic authentication for HTTP' is set to 'Disabled' (Automated) 69
1.13.2 (L1) Ensure 'Allow cross-origin HTTP Authentication prompts' is set to 'Disabled' (Automated) 71
1.13.3 (L2) Ensure 'Supported authentication schemes' is set to 'Enabled: ntlm, negotiate' (Automated) 73
1.14 Identity and sign-in 75
1.14.1 (L1) Ensure 'Guided Switch Enabled' is set to 'Disabled' (Automated) 76
1.15 Idle Browser Actions 78
1.16 Immersive Reader settings 78
1.17 Kiosk Mode settings 78
1.18 Manageability 78

1.19 Native Messaging **78**
1.20 Network settings **79**
1.20.1 (L1) Ensure 'Specifies whether to block requests from public websites to devices on a user's local network' is set to 'Enabled' (Automated) 80
1.21 Password manager and protection **82**
1.21.1 (L1) Ensure 'Enable saving passwords to the password manager' is set to 'Disabled' (Automated) 83
1.22 PDF Reader **85**
1.23 Permit or deny screen capture **85**
1.24 Performance **86**
1.24.1 (L1) Ensure 'Enable startup boost' is set to 'Disabled' (Automated) 87
1.25 Printing **89**
1.26 Private Network Request Settings **89**
1.27 Proxy server **89**
1.28 Related Website Sets Settings **89**
1.29 Scareware Blocker settings **89**
1.30 Sleeping tabs settings **89**
1.31 SmartScreen settings **90**
1.31.1 (L1) Ensure 'Configure Microsoft Defender SmartScreen' is set to 'Enabled' (Automated) 91
1.31.2 (L1) Ensure 'Configure Microsoft Defender SmartScreen to block potentially unwanted apps' is set to 'Enabled' (Automated) 93
1.31.3 (L1) Ensure 'Enable Microsoft Defender SmartScreen DNS requests' is set to 'Enabled' (Automated) 95
1.31.4 (L1) Ensure 'Force Microsoft Defender SmartScreen checks on downloads from trusted sources' is set to 'Enabled' (Automated) 97
1.31.5 (L1) Ensure 'Prevent bypassing Microsoft Defender SmartScreen prompts for sites' is set to 'Enabled' (Automated) 99
1.31.6 (L1) Ensure 'Prevent bypassing of Microsoft Defender SmartScreen warnings about downloads' is set to 'Enabled' (Automated) 101
1.32 Startup, home page and new tab page **103**
1.32.1 (L1) Ensure 'Disable Bing chat entry-points on Microsoft Edge Enterprise new tab page' is set to 'Disabled' (Automated) 104
1.33 (L1) Ensure 'Ads setting for sites with intrusive ads' is set to 'Enabled: Block ads on sites with intrusive ads.' (Automated) 106
1.34 (L1) Ensure 'Allow download restrictions' is set to 'Enabled: Block malicious downloads' (Automated) 108
1.35 (L2) Ensure 'Allow features to download assets from the Asset Delivery Service' is set to 'Disabled' (Automated) 110
1.36 (L2) Ensure 'Allow file selection dialogs' is set to 'Disabled' (Automated) 112
1.37 (L1) Ensure 'Allow Google Cast to connect to Cast devices on all IP addresses' is set to 'Disabled' (Automated) 114
1.38 (L1) Ensure 'Allow import of data from other browsers on each Microsoft Edge launch' is set to 'Disabled' (Automated) 116
1.39 (L1) Ensure 'Allow importing of autofill form data' is set to 'Disabled' (Automated) 118
1.40 (L1) Ensure 'Allow importing of browser settings' is set to 'Disabled' (Automated) 120
1.41 (L1) Ensure 'Allow importing of home page settings' is set to 'Disabled' (Automated) 122
1.42 (L1) Ensure 'Allow importing of payment info' is set to 'Disabled' (Automated) 124
1.43 (L1) Ensure 'Allow importing of saved passwords' is set to 'Disabled' (Automated) 126
1.44 (L1) Ensure 'Allow importing of search engine settings' is set to 'Disabled' (Automated) 128
1.45 (L1) Ensure 'Allow managed extensions to use the Enterprise Hardware Platform API' is set to 'Disabled' (Automated) 130
1.46 (L2) Ensure 'Allow or block audio capture' is set to 'Disabled' (Automated) 132
1.47 (L2) Ensure 'Allow or block video capture' is set to 'Disabled' (Automated) 134
1.48 (L2) Ensure 'Allow or deny screen capture' is set to 'Disabled' (Automated) 136

1.49 (L1) Ensure 'Allow personalization of ads, search and news by sending browsing history to Microsoft' is set to 'Disabled' (Automated) 138
1.50 (L1) Ensure 'Allow queries to a Browser Network Time service' is set to 'Enabled' (Automated) 140
1.51 (L1) Ensure 'Allow remote debugging' is set to 'Disabled' (Automated) 142
1.52 (L1) Ensure 'Allow the audio sandbox to run' is set to 'Enabled' (Automated) 144
1.53 (L2) Ensure 'Allow unconfigured sites to be reloaded in Internet Explorer mode' is set to 'Disabled' (Automated) 146
1.54 (L1) Ensure 'Allow user feedback' is set to 'Disabled' (Automated) 148
1.55 (L2) Ensure 'Allow users to open files using the ClickOnce protocol' is set to 'Disabled' (Automated) 150
1.56 (L2) Ensure 'Allow users to open files using the DirectInvoke protocol' is set to 'Disabled' (Automated) 152
1.57 (L2) Ensure 'Allow users to proceed from the HTTPS warning page' is set to 'Disabled' (Automated) 154
1.58 (L1) Ensure 'Allow Web Authentication requests on sites with broken TLS certificates' is set to 'Disabled' (Automated) 156
1.59 (L1) Ensure 'Allow websites to query for available payment methods' is set to 'Disabled' (Automated) 158
1.60 (L2) Ensure 'AutoLaunch Protocols Component Enabled' is set to 'Disabled' (Automated) 160
1.61 (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) 162
1.62 (L1) Ensure 'Automatically open downloaded MHT or MHTML files from the web in Internet Explorer mode' is set to 'Disabled' (Automated) 164
1.63 (L2) Ensure 'Block third party cookies' is set to 'Enabled' (Automated) 166
1.64 (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)' or higher (Automated) 168
1.65 (L2) Ensure 'Browser sign-in settings' is set to 'Enabled: Disable browser sign-in' (Automated) 170
1.66 (L1) Ensure 'Clear browsing data when Microsoft Edge closes' is set to 'Disabled' (Automated) 172
1.67 (L1) Ensure 'Clear cached images and files when Microsoft Edge closes' is set to 'Disabled' (Automated) 174
1.68 (L1) Ensure 'Clear history for IE and IE mode every time you exit' is set to 'Disabled' (Automated) 176
1.69 (L1) Ensure 'Configure browser process code integrity guard setting' is set to 'Enabled: Enable code integrity guard enforcement in the browser process.' (Automated) 178
1.70 (L1) Ensure 'Configure InPrivate mode availability' is set to 'Enabled: InPrivate mode disabled' (Automated) 180
1.71 (L2) Ensure 'Configure Online Text To Speech' is set to 'Disabled' (Automated) 182
1.72 (L2) Ensure 'Configure Speech Recognition' is set to 'Disabled' (Automated) 184
1.73 (L1) Ensure 'Configure the list of names that will bypass the HSTS policy check' is set to 'Disabled' (Automated) 186
1.74 (L1) Ensure 'Configure the list of types that are excluded from synchronization' is set to 'Enabled' (Automated) 188
1.75 (L1) Ensure 'Configure the Share experience' is set to 'Enabled: Don't allow using the Share experience' (Automated) 190
1.76 (L1) Ensure 'Continue running background apps after Microsoft Edge closes' is set to 'Disabled' (Automated) 192
1.77 (L1) Ensure 'Control communication with the Experimentation and Configuration Service' is set to 'Enabled: Disable communication with the Experimentation and Configuration Service' (Automated) 194
1.78 (L2) Ensure 'Control use of the Headless Mode' is set to 'Disabled' (Automated) 196

1.79 (L2) Ensure 'Control use of the Serial API' is set to 'Enable: Do not allow any site to request access to serial ports via the Serial API' (Automated) 198
1.80 (L1) Ensure 'Control where security restrictions on insecure origins apply' is set to 'Disabled' (Automated) 200
1.81 (L2) Ensure 'Default sensors setting' is set to 'Enabled: Do not allow any site to access sensors' (Automated) 202
1.82 (L1) Ensure 'Delete old browser data on migration' is set to 'Disabled' (Automated) 204
1.83 (L1) Ensure 'Disable saving browser history' is set to 'Disabled' (Automated) 206
1.84 (L1) Ensure 'Disable synchronization of data using Microsoft sync services' is set to 'Enabled' (Automated) 208
1.85 (L1) Ensure 'DNS interception checks enabled' is set to 'Enabled' (Automated) 210
1.86 (L1) Ensure 'Dynamic Code Settings' is set to 'Enabled: Prevent the browser process from creating dynamic code' (Automated) 212
1.87 (L1) Ensure 'Edge 3P SERP Telemetry Enabled' is set to 'Disabled' (Automated) 214
1.88 (L1) Ensure 'Edge Wallet E-Tree Enabled' is set to 'Disabled' (Automated) 216
1.89 (L1) Ensure 'Enable Application Bound Encryption' is set to 'Enabled' (Automated) 218
1.90 (L1) Ensure 'Enable AutoFill for addresses' is set to 'Disabled' (Automated) 220
1.91 (L1) Ensure 'Enable AutoFill for payment instruments' is set to 'Disabled' (Automated) 222
1.92 (L1) Ensure 'Enable browser legacy extension point blocking' is set to 'Enabled' (Automated) 224
1.93 (L1) Ensure 'Enable component updates in Microsoft Edge' is set to 'Enabled' (Automated) 226
1.94 (L1) Ensure 'Enable deleting browser and download history' is set to 'Disabled' (Automated) 228
1.95 (L2) Ensure 'Enable Drop feature in Microsoft Edge' is set to 'Disabled' (Automated) .. 230
1.96 (L1) Ensure 'Enable globally scoped HTTP auth cache' is set to 'Disabled' (Automated) 232
1.97 (L2) Ensure 'Enable guest mode' is set to 'Disabled' (Automated) 234
1.98 (L1) Ensure 'Enable network prediction' is set to 'Enabled: Don't predict network actions on any network connection' (Automated) 236
1.99 (L1) Ensure 'Enable profile creation from the Identity flyout menu or the Settings page' is set to 'Disabled' (Automated) 238
1.100 (L1) Ensure 'Enable resolution of navigation errors using a web service' is set to 'Disabled' (Automated) 240
1.101 (L2) Ensure 'Enable search suggestions' is set to 'Disabled' (Automated) 242
1.102 (L1) Ensure 'Enable security warnings for command-line flags' is set to 'Enabled' (Automated) 244
1.103 (L1) Ensure 'Enable site isolation for every site' is set to 'Enabled' (Automated) 246
1.104 (L1) Ensure 'Enable the Search bar' is set to 'Disabled' (Automated) 248
1.105 (L1) Ensure 'Enable tab organization suggestions' is set to 'Disabled' (Automated) ... 250
1.106 (L2) Ensure 'Enable Translate' is set to 'Disabled' (Automated) 252
1.107 (L1) Ensure 'Enable upload files from mobile in Microsoft Edge desktop' is set to 'Disabled' (Automated) 254
1.108 (L1) Ensure 'Enable use of ephemeral profiles' is set to 'Disabled' (Automated) 256
1.109 (L1) Ensure 'Enable warnings for insecure forms' is set to 'Enabled' (Automated) 258
1.110 (L2) Ensure 'Enable QR Code Generator' is set to 'Disabled' (Automated) 260
1.111 (L1) Ensure 'Enables DALL-E themes generation' is set to 'Disabled' (Automated) 262
1.112 (L2) Ensure 'Enforce Bing SafeSearch' is set to 'Enabled: Configure moderate search restrictions in Bing' (Automated) 264
1.113 (L2) Ensure 'Enforce Google SafeSearch' is set to 'Enabled' (Automated) 266
1.114 (L1) Ensure 'Enhance the security state in Microsoft Edge' is set to 'Enabled: Balanced mode' or higher (Automated) 268
1.115 (L2) Ensure 'Enhanced Security Mode configuration for Intranet zone sites' is set to 'Disabled' (Automated) 270
1.116 (L1) Ensure 'Hide the First-run experience and splash screen' is set to 'Enabled' (Automated) 272

1.117 (L1) Ensure 'In-app support Enabled' is set to 'Disabled' (Automated) 274
1.118 (L2) Ensure 'Live captions allowed' is set to 'Disabled' (Automated) 276
1.119 (L1) Ensure 'Manage exposure of local IP addressess by WebRTC' is set to 'Disabled' (Automated) 278
1.120 (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) 280
1.121 (L1) Ensure 'Set disk cache size, in bytes' is set to 'Enabled: 250609664' (Automated) 282
1.122 (L1) Ensure 'Set the time period for update notifications' is set to 'Enabled: 86400000' (Automated) 284
1.123 (L1) Ensure 'Shopping in Microsoft Edge Enabled' is set to 'Disabled' (Automated) 286
1.124 (L2) Ensure 'Show an "Always open" checkbox in external protocol dialog' is set to 'Disabled' (Automated) 288
1.125 (L1) Ensure 'Show Microsoft Rewards experiences' is set to 'Disabled' (Automated) 290
1.126 (L1) Ensure 'Show the Reload in Internet Explorer mode button in the toolbar' is set to 'Disabled' (Automated) 292
1.127 (L1) Ensure 'Specifies whether SharedArrayBuffers can be used in a non cross-origin-isolated context' is set to 'Disabled' (Automated) 294
1.128 (L2) Ensure 'Specify if online OCSP/CRL checks are required for local trust anchors' is set to 'Enabled' (Automated) 296
1.129 (L2) Ensure 'Spell checking provided by Microsoft Editor' is set to 'Disabled' (Automated) 298
1.130 (L1) Ensure 'Standalone Sidebar Enabled' is set to 'Disabled' (Automated) 300
1.131 (L1) Ensure 'Suggest similar pages when a webpage can’t be found' is set to 'Disabled' (Automated) 302
1.132 (L1) Ensure 'Suppress the unsupported OS warning' is set to 'Disabled' (Automated) 304
1.133 (L2) Ensure 'Text prediction enabled by default' is set to 'Disabled' (Automated) 306
1.134 (L1) Ensure 'Wait for Internet Explorer mode tabs to completely unload before ending the browser session' is set to 'Disabled' (Automated) 308
1.135 (L1) Ensure 'Wallet Donation Enabled' is set to 'Disabled' (Automated) 310

2 Microsoft Edge - Default Settings (users can override) 312

3 Microsoft Edge Update 312
3.1 Applications 313
3.1.1 (L1) Ensure 'Update policy override default' is set to 'Enabled: Automatic silent updates only' or Higher (Automated) 314
3.2 Microsoft Edge WebView2 Runtime 316
3.3 Preferences 317
3.3.1 (L1) Ensure 'Auto-update check period override' is set to any value except '0' (Automated) 318

4 Microsoft Edge WebView2 320
4.1 Network settings 320

Appendix: Summary Table 321

Appendix: Change History 335

Overview

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

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

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

Important Usage Information

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

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

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

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

Key Stakeholders

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

Apply the Correct Version of a Benchmark

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

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

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

Exceptions

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

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

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

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

Remediation

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

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

The following is a reasonable remediation approach to follow:

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

Summary

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

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

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

Target Technology Details

This document provides prescriptive guidance for establishing a secure configuration posture for the Microsoft Edge Browser, also known as Microsoft Edge for Business. This guide was tested against Microsoft Edge v138 on Microsoft Windows 11 (Release 25H2) 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 Microsoft Edge Intune Benchmarks are written for **MDM-joined** systems using Microsoft Intune device configuration profiles only. This benchmark is **not** intended for use on standalone or workgroup systems, systems joined to and receive policies from Active Directory, or systems created, maintained, or used in other Cloud offerings. This benchmark covers supported endpoint states for **Entra Hybrid Joined** and **Entra Joined** systems that receive policies from **Microsoft Intune** using **Configuration Profiles** only.

Consensus Guidance

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

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

Typographical Conventions

The following typographical conventions are used throughout this guide:

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

Recommendation Definitions

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

Title

Concise description for the recommendation's intended configuration.

Assessment Status

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

Automated

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

Manual

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

Profile

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

Description

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

Rationale Statement

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

Impact Statement

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

Audit Procedure

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

Remediation Procedure

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

Default Value

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

References

Additional documentation relative to the recommendation.

CIS Critical Security Controls® (CIS Controls®)

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

Additional Information

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

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1 (L1) - General Use**

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

  Items in this profile intend to:

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

- **Level 2 (L2) - Limited Functionality**

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

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

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

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

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:

Editor

Jennifer Jarose
Caleb Eifert
Matt Woods

Contributor

Daniel Jasiak
William Ferguson
Uzoma Ifeakanwa
Haemish Edgerton
Krishna Rayavaram
Aaron Margosis

Recommendations

1 Microsoft Edge

This section contains recommendations for Microsoft Edge.

1.1 Application Guard settings

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

1.2 Cast

This section contains recommendations for Microsoft Edge Cast settings.

1.2.1 (L1) Ensure 'Enable Google Cast' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - General Use

Description:

This policy setting determines whether Google Cast is available to users.

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

Note: When this setting is set to `Disabled` the *Show the cast icon in the toolbar* setting is ignored as the icon is removed.

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 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 setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:EnableMediaRouter
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`.

```
Microsoft Edge\Cast\Enable Google Cast
```

Default Value:

Enabled.

References:

1. https://learn.microsoft.com/en-us/DeployEdge/microsoft-edge-browser-policies/enablemediarouter
2. GRID: BR-00000108

CIS Controls:

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

1.3 Certificate management settings

This section contains recommendations for Certificate management settings

1.3.1 (L1) Ensure 'Allow users to manage installed CA certificates' is set to 'Enabled: Disallow users from managing certificates' (Automated)

Profile Applicability:

- Level 1 (L1) - General Use

Description:

This policy configures the level of access users have when managing CA certificates in Microsoft Edge.

The recommended state for this setting is: `Enabled`: `Disallow users from managing certificates`.

Rationale:

Configuring this policy to the recommended state prevents users from unknowingly installing certificates that grant excessive trust, such as root CAs from unverified sources. It also prevents system-trusted certificates from being tampered with by users.

Impact:

Users will not be able to manage certificates.

Audit:

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

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:CACertificatemanagementAllowed
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Enabled`: `Disallow users from managing certificates`:

```
Microsoft Edge\Certificate management settings\Allow users to manage
installed CA certificates
```

Default Value:

Enabled: UserOnly (Users can only manage certificates they have personally added)

References:

1. https://learn.microsoft.com/en-us/deployedge/microsoft-edge-browser-policies/cacertificatemanagementallowed
2. GRID: BR-00000139

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

1.4 Content Settings

This section contains recommendations for Microsoft Edge Content settings.

1.4.1 (L2) Ensure 'Allow read access via the File System API on these sites' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - Limited Functionality

Description:

This policy setting allows organizations to list the URL patterns that specify which sites can ask users to grant them read access to files or directories in the host operating system´s file system via the File System API.

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

Note: Leaving this policy not configured allows the *DefaultFileSystemReadGuardSetting* (Control use of the File System API for reading) to apply for all sites. This setting is configured in the Level 2 profile: *Ensure 'Control use of the File System API for reading' is set to 'Enabled: Don't allow any site to request read access to files and directories'*.

Note #2: URL patterns can´t conflict with *FileSystemReadBlockedForUrls* (Block read access via the File System API on these sites). Neither policy takes precedence if a URL matches with both.

Rationale:

This API allows web apps to read or save changes directly to files and folders on user devices. It also allows for the reading and writing files and the File System Access API provides the ability to open a directory and enumerate its contents.

Allowing web apps the ability to enumerate the contents of a directory by reading or saving changes directly to files and folders opens the organization to the possibility of malicious content being saved directly to user devices.

Impact:

Users with creative roles that require read access to files and directories via the File System API may need additional permissions granted for said roles.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is in effect when the following registry value `does not exist`.

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:FileSystemReadAskForUrls
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\Content settings\Allow read access via the File System API on these sites
```

Default Value:

Not configured. (*DefaultFileSystemReadGuardSetting* (Control use of the File System API for reading) applies for all sites, if it´s set. If not, users´ personal settings apply.)

References:

1. https://docs.microsoft.com/en-us/deployedge/microsoft-edge-policies#filesystemreadaskforurls
2. https://web.dev/file-system-access/
3. GRID: BR-00000109

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.4 Restrict Unnecessary or Unauthorized Browser and Email Client Extensions Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.		●	●
v7	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.		●	●

1.4.2 (L2) Ensure 'Choose whether users can receive customized background images and text, suggestions, notifications, and tips for Microsoft services' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - Limited Functionality

Description:

This policy setting configures whether users can receive customized background images and text, suggestions, and tips for Microsoft services.

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

Rationale:

Disabling this feature helps prevent unintentional data sharing with Microsoft and third-parties.

Impact:

Users will not be able to receive customized background images and text, notifications, or tips for Microsoft services.

Audit:

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

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:SpotlightExperiencesAndRecommendationsEnabled
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\Content settings\Choose whether users can receive customized background images and text, suggestions, notifications, and tips for Microsoft services
```

Default Value:

Enabled. (Spotlight experiences and recommendations are turned on.)

References:

1. https://learn.microsoft.com/en-us/deployedge/microsoft-edge-browser-policies/spotlightexperiencesandrecommendationsenabled
2. GRID: BR-00000119

CIS Controls:

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

1.4.3 (L1) Ensure 'Control use of insecure content exceptions' is set to 'Enabled: Do not allow any site to load blockable mixed content' (Automated)

Profile Applicability:

- Level 1 (L1) - General Use

Description:

This policy setting allows for the configuration for users to add exceptions to allow mixed content for specific sites.

The recommended state for this setting is: `Enabled: Do not allow any site to load mixed content`

Note: This policy can be overridden for specific URL patterns using the *insecurecontentAllowedForUrls) (Allow insecure content on specified sites)* and *insecurecontentBlockedForUrls* (Block insecure content on specified sites) policies.

Rationale:

Allowing mixed (secure / insecure) content from a site can lead to malicious content being loaded. Mixed content occurs if the initial request is secure over HTTPS, but HTTPS and HTTP content is subsequently loaded to display the web page. HTTPS content is secure. HTTP content is insecure.

Impact:

Users will not be able to add exceptions for mix content webpages.

Audit:

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

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:DefaultinsecurecontentSetting
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Enabled: Do not allow any site to load blockable mixed content`:

```
Microsoft Edge\Content Settings\Control use of insecure content exceptions
```

Default Value:

Enabled. (Users will be allowed to add exceptions to allow blockable mixed content and disable autoupgrades for optionally blockable mixed content.)

References:

1. https://learn.microsoft.com/en-us/deployedge/microsoft-edge-browser-policies/defaultinsecurecontentsetting
2. GRID: BR-00000110

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.3 Maintain and Enforce Network-Based URL Filters Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.		●	●
v7	7.5 Subscribe to URL-Categorization service Subscribe to URL categorization services to ensure that they are up-to-date with the most recent website category definitions available. Uncategorized sites shall be blocked by default.		●	●

1.4.4 (L2) Ensure 'Control use of JavaScript JIT' is set to 'Enabled: Do not allow any site to run JavaScript JIT' (Automated)

Profile Applicability:

- Level 2 (L2) - Limited Functionality

Description:

This policy setting specifies whether Microsoft Edge will run the v8 JavaScript engine with JIT (Just In Time) compiler. JIT is a complex pipeline of processes used to optimize JavaScript code for performance.

Note: This policy can be overridden for specific URL patterns using the *JavaScriptJitAllowedForSites* (Allow JavaScript to use JIT on these sites)_ and *JavaScriptJitBlockedForSites* (Block JavaScript from using JIT on these sites) policies.

The recommended state for this setting is: `Enabled: Do not allow any site to run JavaScript JIT`.

Rationale:

Microsoft's research has revealed that attackers usually target the JavaScript engine called “Just-In-Time (JIT) compilation” to hack web browsers. Disabling the JavaScript just-in-time (JIT) compiler prevents attackers from hacking into systems that Microsoft Edge uses.

Impact:

Disabling the JavaScript JIT will mean that Microsoft Edge may render web content more slowly, and may also disable parts of JavaScript including WebAssembly. Users may experience slower rendering of web content.

Audit:

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

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:DefaultJavaScriptJitSetting
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Enabled: Do not allow any site to run JavaScript JIT`:

```
Microsoft Edge\Content Settings\Control use of JavaScript JIT
```

Default Value:

Enabled.

References:

1. https://www.onmsft.com/news/microsoft-edges-super-duper-secure-mode-addresses-javascript-vulnerabilities-in-a-brand-new-way
2. GRID: BR-00000111

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.4 Restrict Unnecessary or Unauthorized Browser and Email Client Extensions Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.		●	●
v7	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.		●	●

1.4.5 (L2) Ensure 'Control use of the File System API for reading' is set to 'Enabled: Don't allow any site to request read access to files and directories via the File System API' (Automated)

Profile Applicability:

- Level 2 (L2) - Limited Functionality

Description:

This policy setting determines whether websites can ask for read access to the host operating system´s file system using the File System API.

The recommended state for this setting is: `Enabled: Don't allow any site to request read access to files and directories via the File System API`.

Rationale:

There is a large category of attack vectors that are opened by allowing web applications access to files. By setting this policy to `Enabled: Don't allow any site to request read access to files and directories` implements additional protections to safeguard against accidental sharing of sensitive information contained in local files.

Impact:

Users with creative roles that require the File System API access permission to read files for photo, video, and text editors or for creating integrated development environments will need additional permissions granted based on their role.

Audit:

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

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:DefaultFileSystemReadGuardSetting
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Enabled: Don't allow any site to request read access to files and directories via the File System API`:

```
Microsoft Edge\Content settings\Control use of the File System API for reading
```

Default Value:

AskFileSystemRead (3) = Allow sites to ask the user to grant read access to files and directories via the File System API. (Websites can ask for access. Users can change this setting.)

References:

1. https://docs.microsoft.com/en-us/microsoft-edge/progressive-web-apps-chromium/how-to/handle-files
2. GRID: BR-00000112

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.4 Restrict Unnecessary or Unauthorized Browser and Email Client Extensions Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.		●	●
v7	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.		●	●

1.4.6 (L1) Ensure 'Control use of the File System API for writing' is set to 'Enabled: Don't allow any site to request write access to files and directories' (Automated)

Profile Applicability:

- Level 1 (L1) - General Use

Description:

This policy setting specifies whether websites can ask for write access to the host operating system´s filesystem using the File System API. By default, websites can ask for access. Users can change this setting. By setting this policy to (2), access is denied.

The recommended state for this setting is: `Enabled: Don't allow any site to request write access to files and directories`.

Rationale:

There is a large category of attack vectors that are opened by allowing web applications access to files. By setting this policy to `Enabled: Don't allow any site to request write access to files and directories` implements additional protection to safeguard against accidental sharing of sensitive information contained in local files.

Impact:

Users with creative roles that require the File System API access permission to write files for photo, video, and text editors or for creating integrated development environments will need additional permissions granted based on their role.

Audit:

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

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:DefaultFileSystemWriteGuardSetting
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Enabled: Don't allow any site to request write access to files and directories`:

```
Microsoft Edge\Content settings\Control use of the File System API for writing
```

Default Value:

AskFileSystemWrite (3) = Allow sites to ask the user to grant write access to files and directories

References:

1. https://docs.microsoft.com/en-us/microsoft-edge/progressive-web-apps-chromium/how-to/handle-files
2. GRID: BR-00000113

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.4 Restrict Unnecessary or Unauthorized Browser and Email Client Extensions Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.		●	●
v7	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.		●	●

1.4.7 (L2) Ensure 'Control use of the Web Bluetooth API' is set to 'Enabled: Do not allow any site to request access to Bluetooth devices via the Web Bluetooth API' (Automated)

Profile Applicability:

- Level 2 (L2) - 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 utilized.

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 setting is backed by the following registry location with a `REG_DWORD` value of `2`.

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:DefaultWebBluetoothGuardSetting
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Enabled: Do not allow any site to request access to Bluetooth devices via the Web Bluetooth API`:

```
Microsoft Edge\Content settings\Control use of the Web Bluetooth API
```

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
2. GRID: BR-00000114

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.4 Restrict Unnecessary or Unauthorized Browser and Email Client Extensions Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.		●	●
v7	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.		●	●

1.4.8 (L2) Ensure 'Control use of the WebHID API' is set to 'Enabled: Do not allow any site to request access to HID devices via the WebHID API' (Automated)

Profile Applicability:

- Level 2 (L2) - Limited Functionality

Description:

This policy setting determines whether a website can ask for access to use the WebHID API. The WebHID API allows websites to access alternative auxiliary keyboards and exotic gamepads.

The recommended state for this setting is: `Enabled: Do not allow any site to request access to HID devices via the WebHID API`.

Rationale:

Disabling the WebHID API prevents HID peripherals from exposing powerful functionality that should not be made accessible to the page without explicit consent. For instance, a HID peripheral may have sensors that allow it to collect information about its surroundings; a device may store private information that should not be revealed or overwritten. Operating systems typically do not restrict access to HID devices from applications, and this access can occasionally be abused to damage the device or corrupt the data stored on it.

Impact:

WebHID describes a wide array of devices that could be supported through HID, including virtual reality controls, flight simulators, medical equipment, and more. Disabling WebHID would require additional drivers or modification to enable support for approved devices.

Audit:

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

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:DefaultWebHidGuardSetting
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Enabled: Do not allow any site to request access to HID devices via the WebHID API`:

```
Microsoft Edge\Content settings\Control use of the WebHID API
```

Default Value:

Allow site to ask the user to grant access to a HID device.

References:

1. https://docs.microsoft.com/en-us/deployedge/microsoft-edge-policies#defaultwebhidguardsetting
2. GRID: BR-00000115

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.4 Restrict Unnecessary or Unauthorized Browser and Email Client Extensions Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.		●	●
v7	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.		●	●

1.4.9 (L1) Ensure 'Default automatic downloads setting' is set to 'Enabled: Don´t allow any website to perform automatic downloads' (Automated)

Profile Applicability:

- Level 1 (L1) - General Use

Description:

This policy setting controls whether websites can perform multiple downloads successively without user interaction.

The recommended state for this setting is: `Enabled: Don´t allow any website to perform automatic downloads`.

Rationale:

Unintentional malicious content could be downloaded without user interaction if websites are allowed to perform automatic downloads.

Impact:

Websites will not be able to perform automatic downloads.

Audit:

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

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:DefaultAutomaticDownloadsSetting
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Enabled: Don´t allow any website to perform automatic downloads`:

```
Microsoft Edge\Content settings\Default automatic downloads setting
```

Default Value:

Enabled. (Multiple automatic downloads can be performed in all sites, and the user can change this setting.)

References:

1. https://learn.microsoft.com/en-us/DeployEdge/microsoft-edge-policies#defaultautomaticDownloadsSetting
2. GRID: BR-00000116

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

1.4.10 (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) - General Use

Description:

This policy setting controls whether a user's 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 user's privacy regarding location. Additionally, location information could lead to clues regarding the user's network infrastructure surrounding the device they are utilizing.

Impact:

Location information will not be shared with websites in Microsoft Edge. This could impact 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 setting is backed by the following registry location with a `REG_DWORD` value of `2`.

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:DefaultGeolocationSetting
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Enabled: Don't allow any site to track users' physical location`:

```
Microsoft Edge\Content settings\Default geolocation setting
```

Default Value:

Enabled. (Ask whenever a site wants to track users physical location.)

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#defaultgeolocationsetting
2. GRID: BR-00000117

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

1.4.11 (L2) Ensure 'Default setting for third-party storage partitioning' is set to 'Enabled: Block third-party storage partitioning from being enabled.' (Automated)

Profile Applicability:

- Level 2 (L2) - Limited Functionality

Description:

This policy setting configures the use of third-party storage partitioning. When using storage partitioning, a site cannot join data across different sites to track the user across the web.

The recommended state for this setting is: `Enabled: Block third-party storage partitioning from being enabled.`.

Rationale:

Third-party storage partitioning can prevent certain types of side-channel cross-site tracking.

Impact:

This setting may cause users to experience issues with sites they regularly visit that already grant access to third-parties.

Audit:

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

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:DefaultThirdPartyStoragePartitioningSetting
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Enabled: Block third-party storage partitioning from being enabled.`:

```
Microsoft Edge\Cast\Default setting for third-party storage partitioning
```

Default Value:

Enabled: Allow. (Third-party storage partitioning is on by default for some users starting with Microsoft Edge version 115.)

References:

1. https://learn.microsoft.com/en-us/DeployEdge/microsoft-edge-policies#defaultthirdpartystoragepartitioningsetting
2. GRID: BR-00000118

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

1.5 Default search provider

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

1.6 Downloads

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

1.6.1 (L1) Ensure 'Enable insecure download warnings' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - General Use

Description:

This policy setting configures whether warnings are enabled when potentially dangerous content is downloaded over HTTP.

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

Rationale:

Downloading files over HTTP is not secure, and is vulnerable to interception and modification. Enabling this policy setting helps users avoid potentially harmful content by flagging executables and archives from insecure sources.

Impact:

When a user tries to download potentially dangerous content from an HTTP site, the user will receive a UI warning, such as "Insecure download blocked." The user will still have an option to proceed and download the item.

Audit:

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

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:ShowDownloadsInsecureWarningsEnabled
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Enabled`:

```
Microsoft Edge\Downloads\Enable insecure download warnings
```

Default Value:

Enabled.

References:

1. https://learn.microsoft.com/en-us/deployedge/microsoft-edge-browser-policies/showdownloadsinsecurewarningsenabled

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

1.7 Edge Website Typo Protection settings

This section contains recommendations for Edge Website Typo Protection settings.

1.7.1 (L1) Ensure 'Configure Edge Website Typo Protection' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - General Use

Description:

This policy setting configures whether to turn on Edge TyposquattingChecker. The Edge TyposquattingChecker provides warning messages to help protect users from potential typo squatting sites. Typo squatting is a type of social engineering attack which targets internet users who incorrectly type a URL into their web browser rather than using a search engine. Typically, it involves tricking users into visiting malicious websites with URLs that are common misspellings of legitimate websites.

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

Rationale:

The Edge TyposquattingChecker will provide a warning message and can help protect users from potential typo squatting by alerting the user to the potential of accessing a malicious site.

Impact:

Users will see a warning message when attempting to access a site identified by Microsoft as a potential typosquatting site. Occasionally, legitimate sites may be mistakenly flagged as typosquatting.

Audit:

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

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:TyposquattingCheckerEnabled
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Enabled`:

```
Microsoft Edge\Typosquatting Checker settings\Configure Edge Website Typo
Protection
```

Default Value:

Enabled. (Users can choose whether to use Edge TyposquattingChecker.)

References:

1. https://docs.microsoft.com/en-us/DeployEdge/microsoft-edge-policies#typosquattingcheckerenabled
2. GRID: BR-00000120

CIS Controls:

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

1.8 Edge Workspaces settings

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

1.9 Experimentation

This section contains recommendations for Microsoft Edge Experimentation settings.

1.9.1 (L1) Ensure 'Configure users ability to override feature flags' is set to 'Enabled: Prevent users from overriding feature flags' (Automated)

Profile Applicability:

- Level 1 (L1) - General Use

Description:

This policy setting configures users' ability to override state of feature flags. Feature flags are settings a team can define that indicate whether a given set of features is visible in the user experience and/or invoked within the functionality.

The recommended state for this setting is: `Enabled: Prevent users from overriding feature flags`.

Rationale:

The ability to enter commands and override programs should be limited at the CLI to prevent unintentional system configuration alterations. Additionally, feature flags are not necessary for users, as they are typically used by Development teams.

Impact:

It can be risky for experimental features to be allowed in an enterprise managed environment because this can introduce bugs and security holes into systems, making it easier for an attacker to gain access. It is generally preferred to only use production-ready features.

Audit:

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

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:FeatureFlagoverridesControl
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Enabled: Prevent users from overriding feature flags`:

```
Microsoft Edge\Experimentation\Configure users ability to override feature flags
```

Default Value:

Enabled: Allow users to override feature flags.

References:

1. https://docs.microsoft.com/en-us/devops/operate/progressive-experimentation-feature-flags
2. GRID: BR-00000121

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.4 Restrict Unnecessary or Unauthorized Browser and Email Client Extensions Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.		●	●
v7	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.		●	●

1.10 Extensions

This section contains recommendations for Microsoft Edge Extensions settings.

1.10.1 (L1) Ensure 'Blocks external extensions from being installed' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - General Use

Description:

This policy setting determines whether external extensions (an extension that is not installed from the Chrome Web Store) can be installed.

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

Rationale:

Allowing users to install extensions from locations other than the Chrome Web Store can lead to unknown or malicious extensions being installed.

Impact:

Users will not be able to install extensions that do not originate form the Chrome web store.

Audit:

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

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:BlockExternalExtensions
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Enabled`:

```
Microsoft Edge\Extensions\Blocks external extensions from being installed
```

Default Value:

Disabled. (Users can change the setting.)

References:

1. https://learn.microsoft.com/en-us/DeployEdge/microsoft-edge-policies#blockexternalextensions
2. GRID: BR-00000122

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.3 Address Unauthorized Software Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.	●	●	●
v7	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.		●	●

1.10.2 (L2) Ensure 'Configure extension management settings' is set to 'Enabled: { "": {"installation_mode": "blocked" }}' (Automated)*

Profile Applicability:

- Level 2 (L2) - Limited Functionality

Description:

This policy setting controls extension management settings for Microsoft Edge, including any controlled by existing extension-related policies. This policy supersedes any legacy policies that might be set.

The recommended state for this setting is: `Enabled: { "*": {"installation_mode": "blocked" }}`.

NOTE: This policy maps an extension ID or an update URL to its specific setting only. A default configuration can be set for the special ID "*", which applies to all extensions without a custom configuration in this policy. With an update URL, configuration applies to extensions with the exact update URL stated in the extension manifest. If the *override_update_url* flag is set to true, the extension is installed and updated using the update URL specified in the *ExtensionInstallForcelist (Control which extensions are installed silently)* policy or in *update_url* field in this policy. The flag *override_update_url* is ignored if the *update_url* is the Edge Add-ons website update URL.

Note #2: For more granular control the *ExtensionInstallForcelist* and *ExtensionInstallAllowlist (Allow specific extensions to be installed)* to allow or force install of specific extensions even if the store is blocked using the JSON in the example. {"update_url:https://clients2.google.com/service/update2/crx":{"installation_mode":"blocked"}}

For more details, check out the detailed guide to *ExtensionSettings* policy available from Microsoft at Detailed guide to the ExtensionSettings policy | Microsoft Learn.

Rationale:

Blocking extensions that could potentially allow remote control of the system through the browser is good security practice. If extensions are needed for securing the browser, or for enterprise use, these can be enabled by configuring the setting *Allow specific extensions to be installed*.

Impact:

Any installed extension will be removed unless it is specified on the extension allowlist, if an organization is using any approved password managers ensure that the extension is added to the allowlist.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a `REG_SZ` value of `{ "*": {"installation_mode": "blocked" }}`.

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:ExtensionSettings
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Enabled: { "*": {"installation_mode": "blocked" }}`:

```
Microsoft Edge\Extensions\Configure extension management settings
```

Default Value:

Not configured.

References:

1. https://go.microsoft.com/fwlink/?linkid=2161555
2. GRID: BR-00000123

Additional Information:

Note: For Windows instances not joined to a Microsoft Active Directory domain and macOS instances not managed via MDM or joined to a domain via MCX, forced installation is limited to apps and extensions listed in the Microsoft Edge Add-ons website.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.4 Restrict Unnecessary or Unauthorized Browser and Email Client Extensions Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.		●	●
v7	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.		●	●

1.11 Games settings

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

1.11.1 (L1) Ensure 'Enable Gamer Mode' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - General Use

Description:

Microsoft Edge Gamer Mode allows the personalization of browsers with gaming themes and gives the option of enabling Efficiency Mode for PC gaming, the Gaming feed on new tabs, sidebar apps for gamers, and more.

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

Rationale:

Allowing users the ability to use the gamer mode feature in Microsoft Edge could lead to data leakage or intellectual property being exposed.

Impact:

The gamer mode feature in Microsoft Edge will not function.

Audit:

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

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:GamerModeEnabled
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\Games settings\Enable gamer mode
```

Default Value:

Enabled. (Users can use the gamer mode feature in Microsoft Edge.)

References:

1. https://learn.microsoft.com/en-us/DeployEdge/microsoft-edge-policies#gamermodeenabled
2. GRID: BR-00000124

CIS Controls:

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

1.12 Generative AI

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

1.13 HTTP authentication

This section contains recommendations for Microsoft Edge HTTP authentication settings.

1.13.1 (L1) Ensure 'Allow Basic authentication for HTTP' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - General Use

Description:

This policy setting determines if Basic authentication receives challenges over non-secure HTTP. Basic authentication is a non-secure authentication method that relies on sending the username and password to the server in plaintext.

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

Note: This policy setting is ignored (and Basic is always forbidden) if the *AuthSchemes (Supported authentication schemes)* policy is set and does not include Basic.

Rationale:

Basic authentication is less robust than other authentication methods available because credentials including passwords are transmitted in plain text. An attacker who can capture these credentials in plain text can gain access to the system.

Impact:

Non-secure HTTP requests from the Basic authentication scheme are blocked, and only secure HTTPS is allowed.

Audit:

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

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:BasicAuthOverHttpEnabled
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\HTTP authentication\Allow Basic authentication for HTTP
```

Default Value:

Enabled. (Basic authentication challenges received over non-secure HTTP will be allowed.)

References:

1. https://techcommunity.microsoft.com/t5/microsoft-security-baselines/security-baseline-for-microsoft-edge-version-88/ba-p/2094443#:~:text=A%20new%20Microsoft%20Edge%20security,from%20the%20Security%20Compliance%20Toolkit.&text=HTTP%20Basic%20Authentication%20is%20a,server%20in%20plaintext%20(base64).
2. GRID: BR-00000125

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	14.4 Encrypt All Sensitive Information in Transit Encrypt all sensitive information in transit.		●	●

1.13.2 (L1) Ensure 'Allow cross-origin HTTP Authentication prompts' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - 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 setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:AllowCrossOriginAuthPrompt
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\HTTP authentication\Allow cross-origin HTTP Authentication prompts
```

Default Value:

Disabled.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#allowcrossoriginauthprompt
2. GRID: BR-00000126

CIS Controls:

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

1.13.3 (L2) Ensure 'Supported authentication schemes' is set to 'Enabled: ntlm, negotiate' (Automated)

Profile Applicability:

- Level 2 (L2) - Limited Functionality

Description:

This setting specifies what HTTP authentication methods are supported by Microsoft Edge.

The recommended setting is: `Enabled: ntlm, negotiate`.

Rationale:

Basic and Digest authentication do not provide sufficient security and can lead to submission of user's password in plaintext or minimal protection (Integrated Authentication is supported for negotiate and ntlm challenges only).

Impact:

Any sites that utilize Basic or Digest 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 setting is backed by the following registry location with a `REG_SZ` value of `ntlm, negotiate`.

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:AuthSchemes
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Enabled: ntlm, negotiate`:

```
Microsoft Edge\HTTP authentication\Supported authentication schemes
```

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
3. GRID: BR-00000127

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	14.4 Encrypt All Sensitive Information in Transit Encrypt all sensitive information in transit.		●	●

1.14 Identity and sign-in

This section contains recommendations for Microsoft Edge Identity and sign-in Settings.

1.14.1 (L1) Ensure 'Guided Switch Enabled' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - General Use

Description:

This policy setting allows Microsoft Edge to prompt the user to switch to the appropriate profile when Microsoft Edge detects that a link is a personal or work link.

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

Rationale:

Linking personal Microsoft Accounts to a company device could inadvertently lead to data being transferred from the environment to a personal device.

Impact:

Users won't be prompted to switch to another account when there´s a profile and link mismatch.

Audit:

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

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:GuidedSwitchEnabled
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\Identity and sign-in\Guided Switch Enabled
```

Default Value:

Enabled. (Guided switch is turned on by default. A user can override this value in the browser settings.)

References:

1. https://learn.microsoft.com/en-us/DeployEdge/microsoft-edge-policies#guidedswitchEnabled
2. GRID: BR-00000128

CIS Controls:

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

1.15 Idle Browser Actions

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

1.16 Immersive Reader settings

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

1.17 Kiosk Mode settings

This section contains recommendations for Microsoft Edge Kiosk Mode settings.

1.18 Manageability

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

1.19 Native Messaging

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

1.20 Network settings

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

1.20.1 (L1) Ensure 'Specifies whether to block requests from public websites to devices on a user's local network' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - General Use

Description:

This policy setting configures whether Microsoft Edge will prevent websites from making requests to local network devices without explicit user permission.

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

Rationale:

If you disable or don't configure this policy, Microsoft Edge handles these requests using the default behavior, which may include showing warnings in DevTools and allowing the request to proceed depending on the context. Blocking websites from making requests to local network devices without explicit user permission can prevent malicious websites from sending unauthorized commands to devices like routers, printers, or IoT gadgets on your network. Enabling this policy setting will also protect your local network from being probed by sites using such requests.

Note: This feature improves local network security by deprecating direct access to private IP addresses from public websites unless explicitly granted by the user. For more information about Local Network Access, see https://wicg.github.io/local-network-access/.

Impact:

Microsoft Edge will prevent websites from making requests to local network devices without explicit user permission. Web apps that rely on automatic access to local devices (e.g., for configuration or diagnostics) may stop working unless permission is explicitly granted.

Audit:

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

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:localnetworkaccessRestrictionsEnabled
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Enabled`:

```
Microsoft Edge\Network settings\Specifies whether to block requests from
public websites to devices on a user's local network
```

Default Value:

Disabled.

References:

1. https://learn.microsoft.com/en-us/deployedge/microsoft-edge-browser-policies/localnetworkaccessrestrictionsenabled

Additional Information:

Note: `LocalNetworkAccessAllowedForUrls` = "Allow sites to make requests to local network endpoints."

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.3 Maintain and Enforce Network-Based URL Filters Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.		●	●
v7	7.5 Subscribe to URL-Categorization service Subscribe to URL categorization services to ensure that they are up-to-date with the most recent website category definitions available. Uncategorized sites shall be blocked by default.		●	●

1.21 Password manager and protection

This section contains recommendations for Microsoft Edge Password manager and protection settings.

1.21.1 (L1) Ensure 'Enable saving passwords to the password manager' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - General Use

Description:

This policy setting controls 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 user's 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 setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:PasswordManagerEnabled
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\Password manager and protection\Enable saving passwords to the password manager
```

Default Value:

Enabled. (The user can change this setting.)

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#passwordmanagerenabled
2. GRID: BR-00000129

CIS Controls:

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

1.22 PDF Reader

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

1.23 Permit or deny screen capture

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

1.24 Performance

This section contains recommendations for Microsoft Edge Performance Settings.

1.24.1 (L1) Ensure 'Enable startup boost' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - General Use

Description:

This policy setting allows Microsoft Edge processes to start at OS sign-in and restart in background after the last browser window is closed.

If Microsoft Edge is running in background mode, the browser might not close when the last window is closed, and the browser won´t be restarted in background when the window closes. See the *BackgroundModeEnabled (Continue running background apps after Microsoft Edge closes)* policy for information about what happens after configuring Microsoft Edge background mode behavior.

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

Note: The startup boost policy may initially be configured off or on by the user; the user can configure its behavior in edge://settings/system.

Rationale:

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

Impact:

Users will experience normal browser start-up times which may seem slow in comparison to Startup boost.

Audit:

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

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:StartupBoostEnabled
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\Performance\Enable startup boost
```

Default Value:

Not configured. (Start boost may initially be off or on.)

References:

1. https://support.microsoft.com/en-us/topic/get-help-with-startup-boost-ebef73ed-5c72-462f-8726-512782c5e442
2. https://docs.microsoft.com/en-us/deployedge/microsoft-edge-policies#startupboostenabled
3. GRID: BR-00000130

CIS Controls:

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

1.25 Printing

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

1.26 Private Network Request Settings

This section contains recommendations for Microsoft Edge Private Network Request Settings.

1.27 Proxy server

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

1.28 Related Website Sets Settings

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

1.29 Scareware Blocker settings

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

1.30 Sleeping tabs settings

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

1.31 SmartScreen settings

This section contains recommendations for Microsoft Edge SmartScreen settings.

1.31.1 (L1) Ensure 'Configure Microsoft Defender SmartScreen' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - 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 setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:SmartScreenEnabled
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Enabled`:

```
Microsoft Edge\SmartScreen settings\Configure Microsoft Defender SmartScreen
```

Default Value:

Enabled. (The user can change this setting.)

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#smartscreenenabled
2. GRID: BR-00000132

CIS Controls:

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

1.31.2 (L1) Ensure 'Configure Microsoft Defender SmartScreen to block potentially unwanted apps' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - 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 setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:SmartScreenPuaEnabled
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Enabled`:

```
Microsoft Edge\SmartScreen settings\Configure Microsoft Defender SmartScreen
to block potentially unwanted apps
```

Default Value:

Not Configured. (The user can change this setting.)

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#smartscreenpuaenabled
2. GRID: BR-00000133

CIS Controls:

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

1.31.3 (L1) Ensure 'Enable Microsoft Defender SmartScreen DNS requests' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - General Use

Description:

This policy setting configures DNS requests made by Microsoft Defender SmartScreen.

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

Note: This policy is available only on Windows instances that are joined to a Microsoft Active Directory domain, Windows 10 Pro or Enterprise instances that are enrolled for device management, or macOS instances that are that are managed via MDM or joined to a domain via MCX.

Rationale:

Whenever SmartScreen is enabled for Edge browser, SmartScreen tries to check if the website is a phishing/malicious URL and does a local DNS query. If the DNS server fails to resolve the website, Web Isolation will not be used to isolate those websites.

Impact:

DNS server might not resolve queries sent to external websites or the website may have no information stored on its local server or cache.

Warning: Disabling DNS requests will prevent Microsoft Defender SmartScreen from getting IP addresses, and potentially impact the IP-based protections provided.

Audit:

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

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:SmartScreenDnsRequestsEnabled
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Enabled`:

```
Microsoft Edge\SmartScreen settings\Enable Microsoft Defender SmartScreen DNS
requests
```

Default Value:

Enabled. (Microsoft Defender SmartScreen will make DNS requests.)

References:

1. https://docs.microsoft.com/en-us/deployedge/microsoft-edge-policies#smartscreendnsrequestsenabled
2. GRID: BR-00000134

CIS Controls:

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

1.31.4 (L1) Ensure 'Force Microsoft Defender SmartScreen checks on downloads from trusted sources' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - 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 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 setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:SmartScreenForTrustedDownloadsEnabled
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Enabled`:

```
Microsoft Edge\SmartScreen settings\Force Microsoft Defender SmartScreen
checks on downloads from trusted sources
```

Default Value:

Enabled. (The user can change this setting.)

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#smartscreenfortrusteddownloadsenabled
2. GRID: BR-00000135

CIS Controls:

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

1.31.5 (L1) Ensure 'Prevent bypassing Microsoft Defender SmartScreen prompts for sites' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - 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 setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:PreventSmartScreenPromptOverride
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Enabled`:

```
Microsoft Edge\SmartScreen settings\Prevent bypassing Microsoft Defender
SmartScreen prompts for sites
```

Default Value:

Disabled.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#preventsmartscreenpromptoverride
2. GRID: BR-00000136

CIS Controls:

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

1.31.6 (L1) Ensure 'Prevent bypassing of Microsoft Defender SmartScreen warnings about downloads' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - 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:

Users 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 setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:PreventSmartScreenPromptOverrideForFiles
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Enabled`:

```
Microsoft Edge\SmartScreen settings\Prevent bypassing of Microsoft Defender SmartScreen warnings about downloads
```

Default Value:

Disabled.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#preventsmartscreenpromptoverrideforfiles
2. GRID: BR-00000137

CIS Controls:

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

1.32 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.

1.32.1 (L1) Ensure 'Disable Bing chat entry-points on Microsoft Edge Enterprise new tab page' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - General Use

Description:

By default, there are two Bing Chat entry-points on the new tab page. One is inside the new tab page search box, and one is in the Bing Autosuggest drawer on-click.

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

Rationale:

Allowing the use of the Bing chat entry-points feature in Microsoft Edge could lead to sensitive data being exposed.

Impact:

The Bing chat entry-points will not appear on the new tab page.

Audit:

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

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:NewTabPageBingChatEnabled
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\Startup, home page and new tab page\Disable Bing chat entry-
points on Microsoft Edge Enterprise new tab page
```

Default Value:

Enabled. (There is no change on the Microsoft Edge Enterprise new tab page and the Bing chat entry-points are there for users in Microsoft Edge.)

References:

1. https://learn.microsoft.com/en-us/DeployEdge/microsoft-edge-policies#newtabpagebingchatenabled
2. GRID: BR-00000138

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●

1.33 (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) - General Use

Description:

This setting controls whether ads are blocked on sites with intrusive ads. Intrusive ads are typically ads that push invasive, unwelcomed, and irrelevant ads in front of consumers. These ads can pop up unexpectedly, block the host page, open new pages and windows, or play video and audio at inopportune times.

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 could be blocked.

Audit:

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

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:AdsSettingForIntrusiveAdsSites
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Enabled: Block ads on sites with intrusive ads.`:

```
Microsoft Edge\Ads setting for sites with intrusive ads
```

Default Value:

Enabled. (Block ads on sites with intrusive ads.)

References:

1. GRID: BR-00000001

CIS Controls:

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

1.34 (L1) Ensure 'Allow download restrictions' is set to 'Enabled: Block malicious downloads' (Automated)

Profile Applicability:

- Level 1 (L1) - General Use

Description:

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

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

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, or 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 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.

Rationale:

Downloads could 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 setting is backed by the following registry location with a `REG_DWORD` value of `4`.

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

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Enabled: Block malicious downloads`:

```
Microsoft Edge\Allow download restrictions
```

Note: The setting `Allow download restrictions` can appear twice in the settings picker. Be sure to choose the one that includes the setting value in the dropdown box as indicated above.

Default Value:

Enabled. (No special restrictions. The downloads will go through the usual security restrictions based on Microsoft Defender SmartScreen analysis results.)

References:

1. GRID: BR-00000002

CIS Controls:

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

1.35 (L2) Ensure 'Allow features to download assets from the Asset Delivery Service' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - Limited Functionality

Description:

This policy setting configures the Microsoft Edge Asset Delivery Service. The Edge Asset Delivery Service is a general pipeline used to deliver assets to Microsoft Edge Clients. These assets can be configuration files or Machine Learning models that power the features that use this service.

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

Rationale:

To reduce the attack surface of the system, downloads such as those described in this recommendation should not be allowed to automatically download without the approval of an Administrator.

Impact:

Microsoft Edge features will not be able to download assets needed for them to run correctly.

Audit:

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

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:EdgeAssetDeliveryServiceEnabled
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\Allow features to download assets from the Asset Delivery
Service
```

Default Value:

Enabled. (Features can download assets from the Asset Delivery Service.)

References:

1. https://docs.microsoft.com/en-us/deployedge/microsoft-edge-policies#edgeassetdeliveryserviceenabled
2. GRID: BR-00000003

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.5 Allowlist Authorized Software Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.		●	●
v7	2.7 Utilize Application Whitelisting Utilize application whitelisting technology on all assets to ensure that only authorized software executes and all unauthorized software is blocked from executing on assets.			●

1.36 (L2) Ensure 'Allow file selection dialogs' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - 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:

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 setting is backed by the following registry location with a `REG_DWORD` value of `0`.

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

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\Allow file selection dialogs
```

Default Value:

Enabled.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#allowfileselectiondialogs
2. GRID: BR-00000004

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	2.7 Utilize Application Whitelisting Utilize application whitelisting technology on all assets to ensure that only authorized software executes and all unauthorized software is blocked from executing on assets.			●

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

Profile Applicability:

- Level 1 (L1) - General Use

Description:

This policy setting controls whether Google Cast can connect to all IP Addresses or only private IP Addresses as defined in RFC1918 (IPv4) and RFC4193 (IPv6).

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

Note: If the *EnabledMediaRouter* policy is set to `Disabled` there is no positive or negative effect for this setting.

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:

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 setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:MediaRouterCastAllowAllIPs
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\Allow Google Cast to connect to Cast devices on all IP
addresses
```

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
2. GRID: BR-00000005

CIS Controls:

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

1.38 (L1) Ensure 'Allow import of data from other browsers on each Microsoft Edge launch' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - General Use

Description:

This policy setting controls if users will get a prompt following each Microsoft Edge launch to import their data from other browsers. Microsoft Edge will import data such as passwords, bookmarks, cookies, browsing history, and payment information depending on which browser this data is being imported from. At this time, Microsoft Edge can only import data from Google Chrome, Mozilla Firefox, Internet Explorer, and some third-party Password Managers.

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

Rationale:

Allowing users to import data from another browser into Microsoft Edge could allow for sensitive data to be imported into Edge.

Impact:

Users will not get a prompt to import their data from other browsers after each Microsoft Edge launch.

Audit:

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

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:ImportOnEachLaunch
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\Allow import of data from other browsers on each Microsoft
Edge launch
```

Default Value:

Users can activate this feature from a Microsoft Edge prompt or from the Settings page.

References:

1. https://support.microsoft.com/en-us/microsoft-edge/what-s-imported-to-microsoft-edge-ab7d9fa1-4586-23ce-8116-e46f44987ac2#:~:text=to%20Microsoft%20Edge.-,In%20Microsoft%20Edge%2C%20go%20to%20Settings%20and%20more%20%3E%20Settings%20%3E,Select%20Import.
2. https://learn.microsoft.com/en-us/DeployEdge/microsoft-edge-policies#importoneachlaunch
3. GRID: BR-00000006

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

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

Profile Applicability:

- Level 1 (L1) - General Use

Description:

This policy setting controls the user's ability 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. Storage of sensitive data should be handled with care.

Impact:

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 set up.

Audit:

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

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

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\Allow importing of autofill form data
```

Default Value:

Enabled. (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
2. GRID: BR-00000007

CIS Controls:

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

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

Profile Applicability:

- Level 1 (L1) - 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 setting is backed by the following registry location with a `REG_DWORD` value of `0`.

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

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\Allow importing of browser settings
```

Default Value:

Enabled. (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
2. GRID: BR-00000008

CIS Controls:

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

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

Profile Applicability:

- Level 1 (L1) - General Use

Description:

This policy setting controls whether users can 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 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 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 setting is backed by the following registry location with a `REG_DWORD` value of `0`.

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

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\Allow importing of home page settings
```

Default Value:

Enabled. (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
2. GRID: BR-00000009

CIS Controls:

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

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

Profile Applicability:

- Level 1 (L1) - General Use

Description:

This policy setting controls whether users can 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 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 setting is backed by the following registry location with a `REG_DWORD` value of `0`.

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

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\Allow importing of payment info
```

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
2. GRID: BR-00000010

CIS Controls:

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

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

Profile Applicability:

- Level 1 (L1) - General Use

Description:

This policy setting controls whether users can 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:

Saved passwords that are 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:

Users will be unable to import saved passwords 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 setting is backed by the following registry location with a `REG_DWORD` value of `0`.

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

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\Allow importing of saved passwords
```

Default Value:

Enabled. (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
2. GRID: BR-00000011

CIS Controls:

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

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

Profile Applicability:

- Level 1 (L1) - General Use

Description:

This policy setting controls whether users can 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:

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 setting is backed by the following registry location with a `REG_DWORD` value of `0`.

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

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\Allow importing of search engine settings
```

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
2. GRID: BR-00000012

CIS Controls:

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

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

Profile Applicability:

- Level 1 (L1) - General Use

Description:

This policy setting allows extensions installed by enterprise policies to be allowed to use the Enterprise Hardware Platform API. This API handles requests from extensions for the manufacturer and model of the hardware platform where the browser is running.

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

Rationale:

Allowing extensions to access the Enterprise Hardware Platform API could lead to the system being compromised. 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 setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:EnterpriseHardwarePlatformAPIEnabled
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`

```
Microsoft Edge\Allow managed extensions to use the Enterprise Hardware
Platform API
```

Default Value:

Disabled.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#enterprisehardwareplatformapienabled
2. GRID: BR-00000013

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.4 Restrict Unnecessary or Unauthorized Browser and Email Client Extensions Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.		●	●
v7	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.		●	●

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

Profile Applicability:

- Level 2 (L2) - Limited Functionality

Description:

This policy setting configures whether the end-user is prompted for access to audio capture devices.

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

Note: The *AudioCaptureAllowedUrls* setting will need to be configured along with this setting if this feature is needed for specific websites.

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:

Users will not be prompted by 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 setting is backed by the following registry location with a `REG_DWORD` value of `0`.

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

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`

```
Microsoft Edge\Allow or block audio capture
```

Default Value:

Enabled. (Users are prompted for audio capture access except from the URLs in the *AudioCaptureAllowedUrls* list. These listed URLs are granted access without prompting.)

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#audiocaptureallowed
2. GRID: BR-00000014

CIS Controls:

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

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

Profile Applicability:

- Level 2 (L2) - Limited Functionality

Description:

This policy setting allows you to set whether the end-user is prompted for access to audio capture devices.

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

Note: The *VideoCaptureAllowedUrls* setting will need to be configured along with this setting if this feature is needed for specific websites.

Rationale:

End-user having the ability to allow or deny video capture for websites in Microsoft Edge, could open an organization up to malicious sites that 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 video capturing permissions 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 setting is backed by the following registry location with a `REG_DWORD` value of `0`.

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

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\Allow or block video capture
```

Default Value:

Enabled. (Users are prompted for video capturing permissions except from the URLs in the *VideoCaptureAllowedUrls* list. These listed URLs are granted access without prompting.)

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#videocaptureallowed
2. GRID: BR-00000015

CIS Controls:

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

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

Profile Applicability:

- Level 2 (L2) - 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 not be able to utilize APIs which support web-based meetings, video, and screen capture. This could potentially disrupt users who 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 setting is backed by the following registry location with a `REG_DWORD` value of `0`.

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

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\Allow or deny screen capture
```

Default Value:

Enabled.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#screencaptureallowed
2. GRID: BR-00000016

CIS Controls:

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

1.49 (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) - 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 could be sensitive.

Impact:

Users' data will not be shared with Microsoft and the personalization of searches, news, etc. will not be available.

Audit:

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

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:PersonalizationReportingEnabled
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\Allow personalization of ads, search and news by sending
browsing history to Microsoft
```

Default Value:

Enabled.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#personalizationreportingenabled
2. GRID: BR-00000017

CIS Controls:

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

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

Profile Applicability:

- Level 1 (L1) - 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 setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:BrowserNetworkTimeQueriesEnabled
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Enabled`:

```
Microsoft Edge\Allow queries to a Browser Network Time service
```

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
3. GRID: BR-00000018

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.4 Standardize Time Synchronization Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.		●	●
v7	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.		●	●

1.51 (L1) Ensure 'Allow remote debugging' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - General Use

Description:

This policy setting controls whether users may use remote debugging. This feature allows remote debugging of live content on a Windows 10 or later device from a Windows or macOS computer.

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

Rationale:

Disabling remote debugging enhances security and protects applications from unauthorized access. Some attack tools can exploit this feature to extract information, or to insert malicious code.

Impact:

Users will not be able access the remote debugging feature in Microsoft Edge.

Audit:

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

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:RemoteDebuggingAllowed
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\Allow remote debugging
```

Default Value:

Enabled. (Users may use remote debugging by specifying --remote-debug-port and --remote-debugging-pipe command line switches.)

References:

1. https://learn.microsoft.com/en-us/DeployEdge/microsoft-edge-browser-policies/remotedebuggingallowed
2. GRID: BR-00000019

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.4 Restrict Unnecessary or Unauthorized Browser and Email Client Extensions Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.		●	●
v7	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.		●	●

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

Profile Applicability:

- Level 1 (L1) - General Use

Description:

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

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

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

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.

Impact:

The audio process will not run in the sandbox and the WebRTC audio-processing module will run in the renderer process.

Audit:

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

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

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Enabled`:

```
Microsoft Edge\Allow the audio sandbox to run
```

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
2. GRID: BR-00000020

CIS Controls:

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

1.53 (L2) Ensure 'Allow unconfigured sites to be reloaded in Internet Explorer mode' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - Limited Functionality

Description:

This policy setting allows users to reload unconfigured sites (that are not configured in the Enterprise mode Site List) in Internet Explorer mode when browsing in Microsoft Edge for a site that requires Internet Explorer for compatibility.

After a site has been reloaded in Internet Explorer mode, "in-page" navigations will stay in Internet Explorer mode (for example, a link, script, or form on the page, or a server-side redirect from another "in-page" navigation). Users can choose to exit from Internet Explorer mode, or Microsoft Edge will automatically exit from Internet Explorer mode when a navigation that isn´t "in-page" occurs (for example, using the address bar, the back button, or a favorite link). Users can also optionally tell Microsoft Edge to use Internet Explorer mode for the site in the future.

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

Note: Enabling this setting takes precedence over how the *InternetExplorerIntegrationTestingAllowed (Allow internet Explorer mode testing)* policy is configured, and that policy will be disabled.

Rationale:

Internet Explorer is officially retired and unsupported. Allowing browsers to reconfigure into Internet Explorer mode could open an organization up to a malicious site due to its lack of support for modern security features.

Impact:

If this setting is `Disabled` users will not be able to reload unconfigured sites in Internet Explorer mode for compatibility. When users try to launch shortcuts or file associations that use Internet Explorer, they will be redirected to open the same file/URL in Microsoft Edge. When users try to launch Internet Explorer by directly invoking the `iexplore.exe` binary, Microsoft Edge will launch instead.

Audit:

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

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:InternetExplorerIntegrationReloadInIEModeAllowed
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\Allow unconfigured sites to be reloaded in Internet Explorer mode
```

Default Value:

Not Configured.

References:

1. https://docs.microsoft.com/en-us/deployedge/edge-ie-mode-local-site-list
2. GRID: BR-00000021

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.3 Maintain and Enforce Network-Based URL Filters Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.		●	●
v7	7.1 Ensure Use of Only Fully Supported Browsers and Email Clients Ensure that only fully supported web browsers and email clients are allowed to execute in the organization, ideally only using the latest version of the browsers and email clients provided by the vendor.	●	●	●
v7	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.		●	●

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

Profile Applicability:

- Level 1 (L1) - 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 third-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 setting is backed by the following registry location with a `REG_DWORD` value of `0`.

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

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\Allow user feedback
```

Default Value:

Enabled.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#userfeedbackallowed
2. GRID: BR-00000022

CIS Controls:

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

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

Profile Applicability:

- Level 2 (L2) - 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 setting is backed by the following registry location with a `REG_DWORD` value of `0`.

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

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\Allow users to open files using the ClickOnce protocol
```

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
3. GRID: BR-00000023

CIS Controls:

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

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

Profile Applicability:

- Level 2 (L2) - 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 setting is backed by the following registry location with a `REG_DWORD` value of `0`.

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

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\Allow users to open files using the DirectInvoke protocol
```

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
4. GRID: BR-00000024

CIS Controls:

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

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

Profile Applicability:

- Level 2 (L2) - Limited Functionality

Description:

This policy setting controls whether a user can 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 setting is backed by the following registry location with a `REG_DWORD` value of `0`.

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

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\Allow users to proceed from the HTTPS warning page
```

Default Value:

Enabled.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#sslerroroverrideallowed
2. GRID: BR-00000025

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

1.58 (L1) Ensure 'Allow Web Authentication requests on sites with broken TLS certificates' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - General Use

Description:

This policy setting configures whether Microsoft Edge will allow web authentication requests on websites that have TLS certificates with errors (i.e. Websites considered not secure).

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

Rationale:

A "broken" TLS certificate cannot be validated by the browser or application due to it being misconfigured, expired, or invalid in some other way. This prevents a secure connection from being made. Allowing Web Authentication requests on sites with broken TLS certificates may lead to sensitive information being exposed.

Impact:

Web authentication requests on Websites that are considered not secure will be blocked.

Audit:

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

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:AllowWebAuthnWithBrokenTlsCerts
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\Allow Web Authentication requests on sites with broken TLS
certificates
```

Default Value:

Disabled.

References:

1. https://learn.microsoft.com/en-us/deployedge/microsoft-edge-browser-policies/allowwebauthnwithbrokentlscerts
2. GRID: BR-00000105

CIS Controls:

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

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

Profile Applicability:

- Level 1 (L1) - 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 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 setting is backed by the following registry location with a `REG_DWORD` value of `0`.

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

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\Allow websites to query for available payment methods
```

Default Value:

Enabled.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#paymentmethodqueryenabled
2. GRID: BR-00000026

CIS Controls:

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

1.60 (L2) Ensure 'AutoLaunch Protocols Component Enabled' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - Limited Functionality

Description:

This policy setting controls the AutoLaunch Protocols Component. This component allows Microsoft to provide a list similar to the *AutoLaunchProtocolsFromOrigins* (Define a list of Protocols that can launch an external application from listed origins without prompting the user) policy, which allows certain external Protocols to launch without prompt or blocking certain Protocols (on specified origins).

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

Rationale:

Allowing applications to AutoLaunch without prompting users for websites in Microsoft Edge could open an organization up to malicious sites that may capture proprietary information through the browser app.

Impact:

Disabling this setting will prompt users whether to allow or deny Microsoft Edge to open certain links in their associated application, no protocols can launch without prompt.

Audit:

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

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:AutoLaunchProtocolsComponentEnabled
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\AutoLaunch Protocols Component Enabled
```

Default Value:

Enabled. (The AutoLaunch Protocols component is enabled.)

References:

1. https://docs.microsoft.com/en-us/deployedge/microsoft-edge-policies#autolaunchprotocolscomponentenabled
2. GRID: BR-00000027

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.4 Restrict Unnecessary or Unauthorized Browser and Email Client Extensions Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.		●	●
v7	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.		●	●

1.61 (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) - General Use

Description:

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

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

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

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 setting is backed by the following registry location with a `REG_DWORD` value of `4`.

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

Remediation:

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

```
Microsoft Edge\Automatically import another browser's data and settings at first run
```

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
2. GRID: BR-00000028

CIS Controls:

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

1.62 (L1) Ensure 'Automatically open downloaded MHT or MHTML files from the web in Internet Explorer mode' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - General Use

Description:

This policy setting controls whether MHT or MHTML files that are downloaded from the web are automatically opened in Internet Explorer mode. MHTML files are archives of HTML code and companion files such as images and audio.

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

Rationale:

Internet Explorer is officially retired and unsupported. Opening files in an unsupported browser that does not have modern protections in place could lead to an attack that exploits a vulnerability in the legacy software.

Impact:

MHT or MHTML files will not open in Internet Explorer mode.

Audit:

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

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:InternetExplorerIntegrationZoneIdentifierMhtFileAllowed
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\Automatically open downloaded MHT or MHTML files from the web in Internet Explorer mode
```

Default Value:

Disabled. (MHT or MHTML files that are downloaded from the web won´t automatically open in Internet Explorer mode)

References:

1. GRID: BR-00000029

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	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.		●	●

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

Profile Applicability:

- Level 2 (L2) - Limited Functionality

Description:

This policy controls whether web page elements from a domain other than that in the address bar can 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 setting is backed by the following registry location with a `REG_DWORD` value of `1`.

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

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Enabled`:

```
Microsoft Edge\Block third party cookies
```

Default Value:

Enabled. (Users can change this setting.)

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#blockthirdpartycookies
2. GRID: BR-00000030

CIS Controls:

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

1.64 (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)' or higher (Automated)

Profile Applicability:

- Level 1 (L1) - 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)`.

Configuring this setting to `Enabled: Strict (blocks harmful trackers and majority of trackers from all sites; content and ads will have minimal personalization. Some parts of sites might not work)` also conforms to the benchmark.

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 the website may not function properly.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a `REG_DWORD` value of `2` or `3`.

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

Remediation:

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

```
Microsoft Edge\Block tracking of users' web-browsing activity
```

Default Value:

Disabled. (Users can set their own level of tracking prevention.)

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#trackingprevention
2. GRID: BR-00000031

CIS Controls:

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

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

Profile Applicability:

- Level 2 (L2) - 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.

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

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

Note #2: 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.

Rationale:

Users will not be able to sign into Microsoft Edge with an account. Signing into Edge does not automatically 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 setting is backed by the following registry location with a `REG_DWORD` value of `0`.

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

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Enabled: Disable browser sign-in`:

```
Microsoft Edge\Browser sign-in settings
```

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
2. GRID: BR-00000032

CIS Controls:

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

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

Profile Applicability:

- Level 1 (L1) - 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.

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

Note: If this policy is enabled, the *AllowDeletingBrowserHistory* policy will take precedence over the *ClearBrowsingDataOnExit* policy and all data will be deleted when Microsoft Edge closes, regardless of how *AllowDeletingBrowserHistory* is configured. The *AllowDeletingBrowserHistory* policy is set to `Disabled` as a safeguard incase this policy is changed.

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 user's personal browsing history. Ensure 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 setting is backed by the following registry location with a `REG_DWORD` value of `0`.

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

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\Clear browsing data when Microsoft Edge closes
```

Default Value:

Disabled. (Users can configure the Clear browsing data option in Settings.)

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#clearbrowsingdataonexit
2. GRID: BR-00000033

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

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

Profile Applicability:

- Level 1 (L1) - General Use

Description:

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

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

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.

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 setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:ClearCachedImagesAndFilesOnExit
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\Clear cached images and files when Microsoft Edge closes
```

Default Value:

Not Configured. (Users can choose whether cached images and files are cleared on exit.)

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#clearcachedimagesandfilesonexit
2. GRID: BR-00000034

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

1.68 (L1) Ensure 'Clear history for IE and IE mode every time you exit' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - General Use

Description:

This policy setting controls whether history will be cleared for Internet Explorer (IE) and IE mode every time a user exits the browser.

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

Rationale:

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

Impact:

History will not be cleared for IE and IE mode every time a user exits the browser.

Audit:

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

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:InternetExplorerModeclearDataOnExitEnab
led
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\Clear history for IE and IE mode every time you exit
```

Default Value:

Disabled. (Internet Explorer browsing history will not be cleared on browser exit.)

References:

1. https://learn.microsoft.com/en-us/DeployEdge/microsoft-edge-policies#InternetExplorerModeclearDataOnExitEnabled
2. GRID: BR-00000035

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

1.69 (L1) Ensure 'Configure browser process code integrity guard setting' is set to 'Enabled: Enable code integrity guard enforcement in the browser process.' (Automated)

Profile Applicability:

- Level 1 (L1) - General Use

Description:

This policy setting controls the use of code integrity guard in the browser process, which only allows Microsoft signed binaries to load.

The recommended state for this setting is: `Enabled: Enable code integrity guard enforcement in the browser process.`.

Rationale:

Code Integrity Guard ensures Microsoft's digital signature is present when loading binaries into a process. Binaries without Microsoft's digital signature are blocked to protect the system from unknown binaries and prevent the injection of untrustworthy binaries into a process.

Impact:

Binaries without Microsoft's digital signature are blocked from being loaded into a process.

Audit:

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

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:browserCodeIntegritySetting
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Enabled: Enable code integrity guard enforcement in the browser process.`:

```
Microsoft Edge\Configure browser process code integrity guard setting
```

Default Value:

Disabled. (Prevents the browser from enabling code integrity guard in the browser process.)

References:

1. https://learn.microsoft.com/en-us/DeployEdge/microsoft-edge-policies#browserCodeIntegritySetting
2. https://www.cloudficient.com/blog/why-microsoft-edge-is-more-secure-now-than-ever
3. GRID: BR-00000037

CIS Controls:

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

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

Profile Applicability:

- Level 1 (L1) - 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 recorded 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 setting is backed by the following registry location with a `REG_DWORD` value of `1`.

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

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Enabled: InPrivate mode disabled`:

```
Microsoft Edge\Configure InPrivate mode availability
```

Default Value:

Enabled. (InPrivate mode available.)

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#inprivatemodeavailability
2. GRID: BR-00000038

CIS Controls:

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

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

Profile Applicability:

- Level 2 (L2) - Limited Functionality

Description:

This policy setting determines whether Online Text to Speech voice fonts which is part of Azure Cognitive Services, are available. 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.

Warning: Disabling this setting will turn off the Online Text to Speech feature, which helps individuals with visual or learning disabilities by reading document text aloud. Before disabling, make sure this feature is not required for accessibility purposes.

Audit:

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

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:ConfigureOnlineTextToSpeech
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\Configure Online Text To Speech
```

Default Value:

Enabled.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#configureonlinetexttospeech
2. GRID: BR-00000039

CIS Controls:

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

1.72 (L2) Ensure 'Configure Speech Recognition' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - Limited Functionality

Description:

This policy setting specifies whether websites can use the W3C Web speech API to recognize speech from the user. The Microsoft Edge implementation of the Web speech API uses Azure Cognitive Services, so voice data will leave the machine.

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

Rationale:

Allowing speech recognition to use the Web speech API in Azure Cognitive permits voice data to leave the machine, potentially allowing sensitive data to be collected from a non-secured third-party source.

Impact:

Users will be unable to use speech recognition for voice typing. Users that use speech recognition for accessibility will need other tools implemented for voice typing.

Warning: Disabling this setting will turn off the Speech Recognition feature. Before disabling, make sure this feature is not required for accessibility purposes.

Audit:

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

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:SpeechRecognitionEnabled
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\Configure Speech Recognition
```

Default Value:

Enabled. (Web-based applications that use the Web speech API can use speech recognition.)

References:

1. https://blogs.windows.com/msedgedev/2016/06/01/introducing-speech-synthesis-api/
2. GRID: BR-00000041

CIS Controls:

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

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

Profile Applicability:

- Level 1 (L1) - 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 effect when disabling this policy setting.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is in effect when the following registry value `does not exist`.

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

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`.

```
Microsoft Edge\Configure the list of names that will bypass the HSTS policy check
```

Default Value:

Not Configured.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#hstspolicybypasslist
2. GRID: BR-00000042

CIS Controls:

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

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

Profile Applicability:

- Level 1 (L1) - 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 setting is backed by the following registry location with a `REG_SZ` value of `passwords`.

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

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Enabled` with the following CASE SENSITIVE datatype `passwords`:

```
Microsoft Edge\Configure the list of types that are excluded from
synchronization
```

- Add the word `passwords` to the dialog box, in all lower case.

Default Value:

Not Configured.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#synctypeslistdisabled
2. GRID: BR-00000043

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

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

Profile Applicability:

- Level 1 (L1) - 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 setting is backed by the following registry location with a `REG_DWORD` value of `1`.

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

Remediation:

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

```
Microsoft Edge\Configure the Share experience
```

Default Value:

Enabled. (Allow using the Share experiences.)

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#configureshare
2. GRID: BR-00000044

CIS Controls:

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

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

Profile Applicability:

- Level 1 (L1) - 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 once the browser 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 setting is backed by the following registry location with a `REG_DWORD` value of `0`.

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

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\Continue running background apps after Microsoft Edge closes
```

Default Value:

Disabled. (The user can configure its behavior in edge://settings/system.)

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#backgroundmodeenabled
2. GRID: BR-00000046

CIS Controls:

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

1.77 (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) - 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 setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:ExperimentationAndConfigurationServiceControl
```

Remediation:

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

```
Microsoft Edge\Control communication with the Experimentation and
Configuration Service
```

Default Value:

Enabled. (Retrieve configurations only.)

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#experimentationandconfigurationservicecontrol
2. GRID: BR-00000047

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.5 Allowlist Authorized Software Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.		●	●
v7	2.7 Utilize Application Whitelisting Utilize application whitelisting technology on all assets to ensure that only authorized software executes and all unauthorized software is blocked from executing on assets.			●

1.78 (L2) Ensure 'Control use of the Headless Mode' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - Limited Functionality

Description:

This policy setting controls whether users can launch Microsoft Edge in headless mode. A headless browser is a browser that is not configured with a Graphical User Interface (GUI) and is executed via command-line or using network communication.

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

Rationale:

Although this feature can be very useful to developers, an attacker could programmatically scrape website content and install malicious scripts on devices running the browser's headless interface.

Impact:

Users will not be able to access headless mode in Microsoft Edge.

Audit:

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

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:HeadlessModeEnabled
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\Control use of the Headless Mode
```

Default Value:

Enabled. (Microsoft Edge allows use of the headless mode.)

References:

1. https://docs.microsoft.com/en-us/deployedge/microsoft-edge-policies#headlessmodeenabled
2. GRID: BR-00000048

CIS Controls:

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

1.79 (L2) Ensure 'Control use of the Serial API' is set to 'Enable: Do not allow any site to request access to serial ports via the Serial API' (Automated)

Profile Applicability:

- Level 2 (L2) - Limited Functionality

Description:

This policy setting configures whether websites can access the systems serial ports.

The recommended state for this setting is: `Enable: Do not allow any site to request access to serial ports via the Serial API`.

Note: If more granular control is needed (per website) then this setting can be used in combination with the *SerialAllowAllPortsForUrls* (Allow the Serial API on specific sites), *SerialAskForUrls* and *SerialBlockedForUrls* (Block the Serial API on specific sites) settings. For example, SerialAllowAllPortsForUrls can be used to allow serial port access to specific sites. Please see the References Section for more information.

Rationale:

Preventing access to system serial ports may prevent malicious sites from using these ports and accessing attached devices.

Impact:

Legitimate websites that need access to the Serial API will be denied access.

Audit:

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

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:DefaultSerialGuardSetting
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Enable: Do not allow any site to request access to serial ports via the Serial API`:

```
Microsoft Edge\Control use of the Serial API
```

Default Value:

Enabled. (`AskSerial (3)` = Allow sites to ask for user permission to access a serial port (Websites can ask users whether they can access a serial port, and users can change this setting.))

References:

1. https://docs.microsoft.com/en-us/deployedge/microsoft-edge-policies#control-use-of-the-serial-api
2. GRID: BR-00000049

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.4 Restrict Unnecessary or Unauthorized Browser and Email Client Extensions Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.		●	●
v7	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.		●	●

1.80 (L1) Ensure 'Control where security restrictions on insecure origins apply' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - General Use

Description:

This policy setting allows for a specified list of origins (URLs) or hostname patterns (like "*.contoso.com") for which security restrictions on insecure origins don´t apply.

Allowed origins for legacy applications that can´t deploy TLS or set up a staging server for internal web development so that developers can test features requiring secure contexts without having to deploy TLS on the staging server. This policy also prevents the origin from being labeled *Not Secure* in the omnibox.

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

Rationale:

Insecure contexts should always be labeled as insecure.

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 setting is in effect when the following registry value `does not exist`.

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:OverrideSecurityRestrictionsOnInsecureOrigin
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\Control where security restrictions on insecure origins apply
```

Default Value:

Enabled.

References:

1. https://chromeenterprise.google/policies/#OverrideSecurityRestrictionsOnInsecureOrigin
2. GRID: BR-00000050

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

1.81 (L2) Ensure 'Default sensors setting' is set to 'Enabled: Do not allow any site to access sensors' (Automated)

Profile Applicability:

- Level 2 (L2) - Limited Functionality

Description:

This policy setting configures whether websites can access and use sensors such as motion and light.

The recommended state for this setting is: `Enabled: Do not allow any site to access sensors`.

Rationale:

Sensor APIs may expose data to sites and services and may even give sites control over functionality. Due to privacy concerns, sensors should never be accessed by websites or third-party vendors.

Impact:

Access to sensors, such as motion and light, will not be accessible by websites.

Audit:

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

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:DefaultSensorsSetting
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Enabled: Do not allow any site to access sensors`:

```
Microsoft Edge\Default sensors setting
```

Default Value:

Enabled. (Allow sites to access sensors.)

References:

1. GRID: BR-00000051

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

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

Profile Applicability:

- Level 1 (L1) - 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 setting is backed by the following registry location with a `REG_DWORD` value of `0`.

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

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\Delete old browser data on migration
```

Default Value:

Disabled.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#deletedataonmigration
2. GRID: BR-00000052

CIS Controls:

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

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

Profile Applicability:

- Level 1 (L1) - 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 user's personal browsing history. Ensure 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 setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:SavingBrowserHistoryDisabled
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\Disable saving browser history
```

Default Value:

Disabled.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#savingbrowserhistorydisabled
2. GRID: BR-00000053

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

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

Profile Applicability:

- Level 1 (L1) - 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:

Users 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 setting is backed by the following registry location with a `REG_DWORD` value of `1`.

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

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Enabled`:

```
Microsoft Edge\Disable synchronization of data using Microsoft sync services
```

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
2. GRID: BR-00000054

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

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

Profile Applicability:

- Level 1 (L1) - 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.

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

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.

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 setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:DNSInterceptionChecksEnabled
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Enabled`:

```
Microsoft Edge\DNS interception checks enabled
```

Default Value:

Enabled. (DNS interception checks are performed.)

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#dnsinterceptionchecksenabled
2. GRID: BR-00000055

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.2 Use DNS Filtering Services Use DNS filtering services on all enterprise assets to block access to known malicious domains.	●	●	●
v7	7.7 Use of DNS Filtering Services Use DNS filtering services to help block access to known malicious domains.	●	●	●

1.86 (L1) Ensure 'Dynamic Code Settings' is set to 'Enabled: Prevent the browser process from creating dynamic code' (Automated)

Profile Applicability:

- Level 1 (L1) - General Use

Description:

This policy setting controls the Dynamic Code Settings for Microsoft Edge.

The recommended state for this setting is: `Enabled: Prevent the browser process from creating dynamic code`.

Rationale:

Leaving this policy in its default state decreases the security of Microsoft Edge by allowing potentially hostile Dynamic Code and third-party code to make changes to Microsoft Edge's behavior.

Impact:

Compatibility issues may arise with third-party software (e.g. certain printer drivers) that must run in the browser process.

Audit:

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

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:DynamicCodeSettings
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Enabled: Prevent the browser process from creating dynamic code`:

```
Microsoft Edge\Dynamic Code Settings
```

Default Value:

Default (0) (Microsoft Edge browser process is allowed to create dynamic code).

References:

1. https://learn.microsoft.com/en-us/deployedge/microsoft-edge-browser-policies/dynamiccodesettings
2. GRID: BR-00000106

CIS Controls:

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

1.87 (L1) Ensure 'Edge 3P SERP Telemetry Enabled' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - General Use

Description:

This policy setting controls Edge3P Telemetry in Microsoft Edge. Edge3P Telemetry captures the searches a user does on third-party search providers without identifying the person or the device.

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

Rationale:

Enabling this feature sends data to a third-party service, which could lead to sensitive data being exposed.

Impact:

Data will not be sent to a third-party.

Audit:

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

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:Edge3PSerpTelemetryEnabled
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\Edge 3P SERP Telemetry Enabled
```

Default Value:

Disabled. (Edge 3P SERP Telemetry feature will be enabled.)

References:

1. GRID: BR-00000056

CIS Controls:

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

1.88 (L1) Ensure 'Edge Wallet E-Tree Enabled' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - General Use

Description:

This policy settings configures the use of the Wallet E-Tree feature in Microsoft Edge.

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

Rationale:

Allowing a third-party to track users while browsing the internet in Microsoft Edge, Weather from Microsoft Start, or Microsoft Wallet can lead to privacy and possible data loss issues.

Impact:

The Edge Wallet E-Tree feature will not be available to users.

Audit:

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

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:EdgeWalletEtreeEnabled
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\Edge Wallet E-Tree Enabled
```

Default Value:

Enabled. (Users can use the Edge Wallet E-Tree feature.)

References:

1. https://support.microsoft.com/en-us/topic/faq-for-e-tree-on-microsoft-edge-microsoft-weather-and-microsoft-wallet-d6fde56e-b61d-4990-bd69-7a503ed64895#:~:text=Want%20to%20do%20what%20you,be%20planted%20on%20your%20behalf.
2. GRID: BR-00000057

CIS Controls:

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

1.89 (L1) Ensure 'Enable Application Bound Encryption' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - General Use

Description:

This policy setting configures whether encryption keys used for local data storage are bound to Microsoft Edge whenever possible.

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

Rationale:

When this policy setting is disabled, it has a detrimental effect on Microsoft Edge´s security by allowing unknown and potentially hostile apps the possibility to retrieve the encryption keys used to secure data.

Impact:

Compatibility issues may arise, such as scenarios where other applications need legitimate access to Microsoft Edge data.

Audit:

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

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:ApplicationBoundEncryptionEnabled
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Enabled`:

```
Microsoft Edge\Enable Application Bound Encryption
```

Default Value:

Enabled.

References:

1. https://learn.microsoft.com/en-us/deployedge/microsoft-edge-browser-policies/applicationboundencryptionenabled
2. GRID: BR-00000107

CIS Controls:

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

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

Profile Applicability:

- Level 1 (L1) - 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 setting is backed by the following registry location with a `REG_DWORD` value of `0`.

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

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\Enable AutoFill for addresses
```

Default Value:

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

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#autofilladdressenabled
2. GRID: BR-00000058

CIS Controls:

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

1.91 (L1) Ensure 'Enable AutoFill for payment instruments' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - General Use

Description:

This policy setting controls whether users can utilize payment information, such as credit or debit cards in web forms using previously stored information.

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

Rationale:

Having payment information stored and auto filled 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 and debit card information in Microsoft Edge.

Audit:

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

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

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\Enable AutoFill for payment instruments
```

Default Value:

Enabled. (Users can control AutoFill for payment instruments.)

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#autofillcreditcardenabled
2. GRID: BR-00000059

CIS Controls:

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

1.92 (L1) Ensure 'Enable browser legacy extension point blocking' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - General Use

Description:

This policy setting sets the *ProcessExtensionPointDisablePolicy* on Microsoft Edge´s browser process to block code injection from legacy third party applications.

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

Note: Per Microsoft, only turn off the policy if there are compatibility issues with third-party software that must run inside Microsoft Edge´s browser process.

Rationale:

If this policy is set to `Disabled`, it may have a detrimental effect on Microsoft Edge´s security and stability as unknown and potentially hostile code can load inside Microsoft Edge´s browser process.

Impact:

Compatibility issues with third-party software can occur.

Audit:

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

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:BrowserLegacyExtensionPointsBlockingEnabled
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Enabled`:

```
Microsoft Edge\Enable browser legacy extension point blocking
```

Default Value:

Enabled. (*ProcessExtensionPointDisablePolicy* is applied to block legacy extension points in the browser process.)

References:

1. GRID: BR-00000060

CIS Controls:

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

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

Profile Applicability:

- Level 1 (L1) - General Use

Description:

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

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

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.

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 setting is backed by the following registry location with a `REG_DWORD` value of `1`.

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

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Enabled`:

```
Microsoft Edge\Enable component updates in Microsoft Edge
```

Default Value:

Enabled.

References:

1. GRID: BR-00000061

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.4 Perform Automated Application Patch Management Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	●	●	●
v7	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.	●	●	●

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

Profile Applicability:

- Level 1 (L1) - General Use

Description:

This policy controls whether users can delete browser and download history for Microsoft Edge.

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

Note: Even when this policy is `Disabled`, the browsing and download history isn'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.

Rationale:

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

Impact:

Browser data deletion by users will be prohibited.

Note: This setting will preserve browsing history that could contain a user's personal browsing history. Ensure 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 setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:AllowDeletingBrowserHistory
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\Enable deleting browser and download history
```

Default Value:

Enabled. (Users can delete the browsing and download history.)

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#allowdeletingbrowserhistory
2. GRID: BR-00000062

CIS Controls:

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

1.95 (L2) Ensure 'Enable Drop feature in Microsoft Edge' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - Limited Functionality

Description:

This policy setting configures the drop feature in Microsoft Edge. The drop feature lets users send messages or files to themselves.

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

Rationale:

Enabling the Microsoft Edge Drop feature could allow sensitive data to be transmitted to a device that is not authorized or a third-party, which could lead to that data being exposed.

Impact:

Users can't use the drop feature in Microsoft Edge to share files and messages between phones and desktop devices.

Audit:

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

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:EdgeEdropenabled
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\Enable Drop feature in Microsoft Edge
```

Default Value:

Enabled. (Users can use the Drop feature in Microsoft Edge.)

References:

1. https://learn.microsoft.com/en-us/DeployEdge/microsoft-edge-policies#EdgeEdropenabled
2. https://www.microsoft.com/en-us/edge/features/drop?form=MT00D8
3. GRID: BR-00000063

CIS Controls:

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

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

Profile Applicability:

- Level 1 (L1) - 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.

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

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

Rationale:

Allowing HTTP auth credentials to be shared without the user's 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 setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:GloballyScopeHTTPAuthCacheEnabled
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\Enable globally scoped HTTP auth cache
```

Default Value:

Disabled.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#globallyscopehttpauthcacheenabled
2. GRID: BR-00000064

CIS Controls:

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

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

Profile Applicability:

- Level 2 (L2) - Limited Functionality

Description:

This policy setting controls whether a user may utilize 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 setting is backed by the following registry location with a `REG_DWORD` value of `0`.

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

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\Enable guest mode
```

Default Value:

Enabled. (Microsoft Edge lets users browse in guest profiles.)

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#browserguestmodeenabled
2. GRID: BR-00000060

CIS Controls:

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

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

Profile Applicability:

- Level 1 (L1) - 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 increase attack surface and, in some cases, lead to opening connections to resources which the user did not intend to utilize.

Impact:

None - this is the default behavior, apart from 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 setting is backed by the following registry location with a `REG_DWORD` value of `2`.

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

Remediation:

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

```
Microsoft Edge\Enable network prediction
```

Default Value:

Enabled. (The user can change the policy.)

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#networkpredictionoptions
2. GRID: BR-00000066

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

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

Profile Applicability:

- Level 1 (L1) - General Use

Description:

This policy setting controls whether users can 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 setting is backed by the following registry location with a `REG_DWORD` value of `0`.

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

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\Enable profile creation from the Identity flyout menu or the
Settings page
```

Default Value:

Enabled. (Microsoft Edge allows users to use **Add profile** on the Identity flyout menu or the Settings page to create new profiles.)

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#browseraddprofileenabled
2. GRID: BR-00000067

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.1 Establish and Maintain an Inventory of Accounts Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.	●	●	●
v7	16.6 Maintain an Inventory of Accounts Maintain an inventory of all accounts organized by authentication system.		●	●

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

Profile Applicability:

- Level 1 (L1) - General Use

Description:

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

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

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

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 setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:ResolveNavigationErrorsUseWebService
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\Enable resolution of navigation errors using a web service
```

Default Value:

Not Configured. (Microsoft Edge respects the user preference that´s set under Services at edge://settings/privacy.)

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#resolvenavigationerrorsusewebservice
2. GRID: BR-00000068

CIS Controls:

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

1.101 (L2) Ensure 'Enable search suggestions' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - 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, instead 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 setting is backed by the following registry location with a `REG_DWORD` value of `0`.

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

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\Enable search suggestions
```

Default Value:

Enabled. (Users can change the setting.)

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#searchsuggestenabled
2. GRID: BR-00000069

CIS Controls:

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

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

Profile Applicability:

- Level 1 (L1) - 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 unintentionally be 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 setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:CommandLineFlagSecurityWarningsEnabled
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Enabled`:

```
Microsoft Edge\Enable security warnings for command-line flags
```

Default Value:

Enabled.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#commandlineflagsecuritywarningsenabled
2. GRID: BR-00000070

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

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

Profile Applicability:

- Level 1 (L1) - 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 untrusted sources.

Impact:

None - this is the default behavior.

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.

Audit:

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

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

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Enabled`:

```
Microsoft Edge\Enable site isolation for every site
```

Default Value:

Enabled.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#siteperprocess
2. GRID: BR-00000071

CIS Controls:

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

1.104 (L1) Ensure 'Enable the Search bar' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - General Use

Description:

This policy setting configures the use of the search bar. The search bar is used to search the web from a user's desktop or from an application. The search bar provides a search box, powered by Edge default search engine, that shows web suggestions and opens all web searches in Microsoft Edge.

The search bar can be launched from the "More tools" menu or jump list in Microsoft Edge.

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

Note: The option to enable the search bar at startup will be toggled on if the ´SearchbarIsEnabledOnStartup´ (Allow the Search bar at Windows startup) policy is `Enabled`. If the ´SearchbarIsEnabledOnStartup´ is `Disabled` or `not configured`, the option to enable the search bar at startup will be toggled off.

Rationale:

Allowing users to have the ability to search from their desktop or an application could lead to the user unintentionally pasting sensitive information in the search bar.

Impact:

Users will not be able to use the search featured powered by Edge default search engine from a desktop or an application.

Audit:

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

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:SearchbarAllowed
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\Enable the Search bar
```

Default Value:

Enabled. (The search bar will be automatically enabled for all profiles.)

References:

1. GRID: BR-00000073

CIS Controls:

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

1.105 (L1) Ensure 'Enable tab organization suggestions' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - General Use

Description:

This policy setting controls whether Microsoft Edge can use its tab organization service to help name or suggest tab groups.

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

Rationale:

Sending Microsoft Edge tab data (URLs, page titles, and existing group information) to the tab organization service could led to privacy concerns or sensitive data being exposed to a third-party.

Impact:

Suggestions for tab groups will not be available to users.

Audit:

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

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:TabServicesEnabled
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\Enable tab organization suggestions
```

Default Value:

Enabled. (When a user creates a tab group or activates certain "Group Similar Tabs" features Microsoft Edge sends tab data to its tab organization service.)

References:

1. https://learn.microsoft.com/en-us/deployedge/microsoft-edge-browser-policies/tabservicesenabled
2. GRID: BR-00000072

CIS Controls:

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

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

Profile Applicability:

- Level 2 (L2) - 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 third-party vendors in an enterprise managed environment. Enabling this service could potentially allow sensitive information to be sent to a third-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 setting is backed by the following registry location with a `REG_DWORD` value of `0`.

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

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\Enable Translate
```

Default Value:

Not Configured. (Users can choose whether to use the translation functionality or not.)

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#translateenabled
2. GRID: BR-00000074

CIS Controls:

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

1.107 (L1) Ensure 'Enable upload files from mobile in Microsoft Edge desktop' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - General Use

Description:

This policy settings allows the configuration of the Edge "Upload from mobile" feature. The "Upload from mobile" feature allows users to select file(s) from a mobile device and upload to a via a webpage in Microsoft Edge.

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

Rationale:

Allowing users the ability to use the file upload from mobile feature in Microsoft Edge could lead to data leakage or intellectual property being exposed.

Impact:

The file upload from mobile feature in Microsoft Edge will not function.

Audit:

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

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:UploadFromPhoneEnabled
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\Enable upload files from mobile in Microsoft Edge desktop
```

Default Value:

Enabled. (Users can upload files via the upload from mobile feature in Microsoft Edge.)

References:

1. GRID: BR-00000075

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.4 Restrict Unnecessary or Unauthorized Browser and Email Client Extensions Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.		●	●
v7	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.		●	●

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

Profile Applicability:

- Level 1 (L1) - 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:

The use of ephemeral profiles will not be allowed, and user browser data will be saved to the system.

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 setting is backed by the following registry location with a `REG_DWORD` value of `0`.

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

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\Enable use of ephemeral profiles
```

Default Value:

Disabled.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#forceephemeralprofiles
2. GRID: BR-00000076

CIS Controls:

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

1.109 (L1) Ensure 'Enable warnings for insecure forms' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - General Use

Description:

This policy setting controls the handling of insecure forms (forms submitted over HTTP) embedded in secure (HTTPS) sites in the browser.

When enabled, a full-page warning will be shown, and autofill will be disabled for those forms. When disabled, warnings will not be shown for insecure forms, and autofill will work normally.

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

Rationale:

The default setting of enabled warnings for insecure forms enforces secure connections when domains are capable of HTTPS and prevents auto-filling of data imported from a non-secure source.

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 setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:InsecureFormsWarningsEnabled
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Enabled`:

```
Microsoft Edge\Enable warnings for insecure forms
```

Default Value:

Enabled. (A full-page warning will be shown when an insecure form is submitted. Additionally, a warning bubble will be shown next to the form fields when they are focused, and autofill will be disabled for those forms.)

References:

1. https://docs.microsoft.com/en-us/deployedge/microsoft-edge-policies#insecureformswarningsenabled
2. GRID: BR-00000077

CIS Controls:

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

1.110 (L2) Ensure 'Enable QR Code Generator' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - Limited Functionality

Description:

The QR Code Generator feature in Microsoft Edge allows users the ability to generate QR codes to internal and external sites.

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

Rationale:

Allowing users the ability to generate QR codes in Microsoft Edge could lead to sensitive data being exposed.

Impact:

The QR code generator feature in Microsoft Edge will not function.

Audit:

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

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:QRCodeGeneratorEnabled
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\Enable QR Code Generator
```

Default Value:

Enabled. (Users can use the QR code generator feature in Microsoft Edge.)

References:

1. https://learn.microsoft.com/en-us/deployedge/microsoft-edge-policies#qrcodegeneratorenabled
2. GRID: BR-00000104

CIS Controls:

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

1.111 (L1) Ensure 'Enables DALL-E themes generation' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - General Use

Description:

This policy setting configures the use of generated browser themes using DALL-E and apply them to Microsoft Edge. DALL-E is an open Artificial Intelligence (AI) system that creates realistic images and art from text descriptions (prompts).

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

Rationale:

The rush to bring GenAI to market has brought to light concerns about the training data rapidly ingested by these large language models (LLMs). Content creators have complained copyright infringement on the content generated by these products. This has resulted in lawsuits against major corporations, the results of which may shape future laws and regulations about the use of certain products and/or the content created by them.

Due to this, there is an unknown element of risk involved in utilizing content generated by DALL-E in an enterprise environment and it is therefore recommended to disable this setting to mitigate that future risk around intellectual property.

Impact:

Users will not be able to generate browser themes using DALL-E.

Audit:

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

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:AIGenThemesEnabled
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\Enables DALL-E themes generation
```

Default Value:

Enabled. (Users can generate AI themes.)

References:

1. GRID: BR-00000078

CIS Controls:

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

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

Profile Applicability:

- Level 2 (L2) - 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 setting is backed by the following registry location with a `REG_DWORD` value of `1`.

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

Remediation:

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

```
Microsoft Edge\Enforce Bing SafeSearch
```

Default Value:

Disabled. (Users can configure this policy.)

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#forcebingsafesearch
2. GRID: BR-00000079

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

1.113 (L2) Ensure 'Enforce Google SafeSearch' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 (L2) - 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: `Enabled`.

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 setting is backed by the following registry location with a `REG_DWORD` value of `1`.

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

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Enabled`:

```
Microsoft Edge\Enforce Google SafeSearch
```

Default Value:

Disabled. (Users can set the value.)

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#forcegooglesafesearch
2. GRID: BR-00000080

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

1.114 (L1) Ensure 'Enhance the security state in Microsoft Edge' is set to 'Enabled: Balanced mode' or higher (Automated)

Profile Applicability:

- Level 1 (L1) - General Use

Description:

This policy setting configures "enhance the security state" in Microsoft Edge. Enhanced security in Microsoft Edge helps safeguard against memory-related vulnerabilities by disabling just-in-time (JIT) JavaScript compilation and enabling additional operating system protections for the browser. These protections include Hardware-enforced Stack Protection and Arbitrary Code Guard (ACG).

Enhanced security provides two levels of browsing security: Balanced and Strict. Balanced mode is an adaptive mode that builds on a user's behavior on a particular device. Strict mode applies added security protections for all the sites a user visits. Users may report some challenges accomplishing their usual tasks when in strict mode.

The recommended state for this setting is: `Enabled: Balanced mode`. Configuring this setting to `Enabled: Strict mode` also conforms to the benchmark.

Rationale:

Balance mode will help reduce the risk of an attack by automatically applying stricter security settings on unfamiliar sites while adapting to browsing habits over time.

Impact:

Users will no longer be able to bypass protection for previously visited unfamiliar sites.

Edge will apply added security protections to sites that are not visited often or are unknown. Websites that are browsed frequently will be left out.

Note: Most sites will work as expected.

Audit:

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

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:EnhanceSecurityMode
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Enabled: Balanced mode` or `Enabled: Strict mode`:

```
Microsoft Edge\Enhance the security state in Microsoft Edge
```

Default Value:

Disabled.

References:

1. https://support.microsoft.com/en-us/microsoft-edge/enhance-your-security-on-the-web-with-microsoft-edge-b8199f13-b21b-4a08-a806-daed31a1929d
2. GRID: BR-00000081

CIS Controls:

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

1.115 (L2) Ensure 'Enhanced Security Mode configuration for Intranet zone sites' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - Limited Functionality

Description:

This policy setting controls whether Microsoft Edge will apply enhanced security mode on Intranet zone sites. Enhanced security mode in Microsoft Edge mitigates memory-related vulnerabilities by disabling just-in-time (JIT) JavaScript compilation and enabling additional operating system protections for the browser.

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

Rationale:

Enhanced security mode provides 'defense-in-depth' protection that makes it more difficult for a malicious site to use an unpatched vulnerability to write to executable memory.

Impact:

Disabling this setting could lead to Intranet zone sites acting in an unexpected manner.

Audit:

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

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:EnhanceSecurityModeBypassIntranet
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\Enhanced Security Mode configuration for Intranet zone sites
```

Default Value:

Disabled. (Microsoft Edge will apply enhanced Security Mode on Intranet zone sites.)

References:

1. https://learn.microsoft.com/en-us/DeployEdge/microsoft-edge-policies#EnhanceSecurityModeBypassIntranet
2. https://learn.microsoft.com/en-us/deployedge/microsoft-edge-security-browse-safer#defense-in-depth
3. GRID: BR-00000082

CIS Controls:

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

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

Profile Applicability:

- Level 1 (L1) - 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 setting is backed by the following registry location with a `REG_DWORD` value of `1`.

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

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Enabled`:

```
Microsoft Edge\Hide the First-run experience and splash screen
```

Default Value:

Disabled.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#hidefirstrunexperience
2. GRID: BR-00000083

CIS Controls:

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

1.117 (L1) Ensure 'In-app support Enabled' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - General Use

Description:

This policy setting allows users to contact in-app Microsoft support agents directly from the Microsoft Edge browser.

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

Rationale:

In-app support shares a user's browsing and search history, which could inadvertently expose and share sensitive data with Microsoft.

Impact:

Users will not be able to use or turn on the in-app support feature in the Microsoft Edge browser.

Audit:

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

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:InAppSupportEnabled
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\In-app support Enabled
```

Default Value:

Enabled. (Users can invoke in-app support.)

References:

1. GRID: BR-00000084

CIS Controls:

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

1.118 (L2) Ensure 'Live captions allowed' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - Limited Functionality

Description:

This policy setting allows users to turn live captions on or off. Live captions are an accessibility feature that converts speech from the audio that plays in Microsoft Edge to text and shows this text in a separate window.

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

Rationale:

Enabling live captions could allow data to be transmitted to a third-party, which could lead to sensitive data being exposed.

Impact:

Users won't be able to turn live captions on. In addition, if speech recognition files have been downloaded previously, they will be deleted from the device in 30 days.

Note: An exception to this recommendation might be needed as this is an accessibility feature that is legitimately needed by some users. Take this into consideration when applying this setting.

Audit:

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

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:LiveCaptionsAllowed
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\Live captions allowed
```

Default Value:

Enabled. (Users can turn this feature on or off.)

References:

1. https://learn.microsoft.com/en-us/DeployEdge/microsoft-edge-policies#liveCaptionsAllowed
2. GRID: BR-00000085

CIS Controls:

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

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

Profile Applicability:

- Level 1 (L1) - General Use

Description:

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

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

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.

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 setting is in effect when the following registry value `does not exist`.

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

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\Manage exposure of local IP addressess by WebRTC
```

Default Value:

Disabled.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#webrtclocalipsallowedurls
2. GRID: BR-00000086

CIS Controls:

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

1.120 (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) - General Use

Description:

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

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

Note: If this setting is set as prescribed, the browser will automatically restart based on the *RelaunchNotificationPeriod* setting which is recommended to be 24 hours.

Rationale:

The end-user will receive a notification informing them that an update has been applied and that the browser must be restarted 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 setting is backed by the following registry location with a `REG_DWORD` value of `2`.

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

Remediation:

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

```
Microsoft Edge\Notify a user that a browser restart is recommended or
required for pending updates
```

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
2. GRID: BR-00000087

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.4 Perform Automated Application Patch Management Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	●	●	●
v7	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.	●	●	●

1.121 (L1) Ensure 'Set disk cache size, in bytes' is set to 'Enabled: 250609664' (Automated)

Profile Applicability:

- Level 1 (L1) - 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 setting is backed by the following registry location with a `REG_DWORD` value of `250609664`.

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:DiskCacheSize
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Enabled: 250609664`:

```
Microsoft Edge\Set disk cache size, in bytes
```

Default Value:

Enabled. (Default size is used.)

References:

1. https://docs.microsoft.com/en-us/deployedge/microsoft-edge-policies#diskcachesize
2. GRID: BR-00000088

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.3 Ensure Adequate Audit Log Storage Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.	●	●	●
v7	6.4 Ensure adequate storage for logs Ensure that all systems that store logs have adequate storage space for the logs generated.		●	●

1.122 (L1) Ensure 'Set the time period for update notifications' is set to 'Enabled: 86400000' (Automated)

Profile Applicability:

- Level 1 (L1) - 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 for the update to be completed. Once updates have been pushed by the organization it is pertinent that said update takes effect 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 setting is backed by the following registry location with a `REG_DWORD` value of `86400000`.

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:RelaunchNotificationPeriod
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Enabled: 86400000`:

```
Microsoft Edge\Set the time period for update notifications
```

Default Value:

Enabled. (One week.)

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#relaunchnotificationperiod
2. GRID: BR-00000089

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.4 Perform Automated Application Patch Management Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	●	●	●
v7	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.	●	●	●

1.123 (L1) Ensure 'Shopping in Microsoft Edge Enabled' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - General Use

Description:

This policy setting allows users to compare the prices of products, get coupons or rebates from the website, auto-apply coupons, and check out faster using autofill data. Coupons for the current retailer and prices from other retailers will be fetched from a server.

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

Note: Starting in Microsoft Edge version 90.0.818.56, the behavior of the messaging letting users know that there is a coupon, rebate, price comparison or price history available on shopping domains is also done through a horizontal banner below the address bar.

Rationale:

Shopping in Microsoft Edge shares a user's browsing and search history to provide price comparison and coupons, which could inadvertently expose and share sensitive data with a third-party.

Impact:

Users with roles that require this feature will have to perform price comparisons on their own unless they are exempted from this setting.

Audit:

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

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:EdgeShoppingAssistantEnabled
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\Shopping in Microsoft Edge Enabled
```

Default Value:

Enabled. (Shopping features such as price comparison, coupons, rebates and express checkout will be automatically applied for retail domains. Coupons for the current retailer and prices from other retailers will be fetched from a server.)

References:

1. https://docs.microsoft.com/en-us/deployedge/microsoft-edge-policies#edgeshoppingassistantenabled
2. GRID: BR-00000090

CIS Controls:

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

1.124 (L2) Ensure 'Show an "Always open" checkbox in external protocol dialog' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - Limited Functionality

Description:

This policy setting controls if the user is prompted with an "Always open" check box when an external protocol prompt is shown.

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 setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:ExternalProtocolDialogShowAlwaysOpenCheckbox
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\Show an "Always open" checkbox in external protocol dialog
```

Default Value:

Enabled. (v84 or greater)

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#externalprotocoldialogshowalwaysopencheckbox
2. GRID: BR-00000091

CIS Controls:

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

1.125 (L1) Ensure 'Show Microsoft Rewards experiences' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - General Use

Description:

This policy setting controls whether the Microsoft Reward experience is available to users and if notifications are received. The Microsoft Rewards experience is a free program that allows the user to earn points when searching on Bing.com. With these points, the users can buy merchandise from the Microsoft Store online and in Windows 10.

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

Note: The Bing Rewards experience was merged with the Microsoft Reward experience in 2016.

Rationale:

Due to privacy concerns, data should never be sent to or tracked by any third-party since this data could contain sensitive information.

Impact:

The Microsoft Rewards experience will not be shown in the Microsoft Edge user profile.

Audit:

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

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:ShowMicrosoftRewards
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\Show Microsoft Rewards experiences
```

Default Value:

Enabled. (In the search and earn markets users will see the Microsoft Rewards experience in their Microsoft Edge user profile.)

References:

1. GRID: BR-00000092

CIS Controls:

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

1.126 (L1) Ensure 'Show the Reload in Internet Explorer mode button in the toolbar' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - General Use

Description:

This policy setting shows the Reload in Internet Explorer mode button in the toolbar. IE Mode in Microsoft Edge allows organizations that still need Internet Explorer 11, (which is not supported) for backward compatibility with existing websites.

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

Note: The button will only be shown on the toolbar when the *Allow unconfigured sites to be reloaded in Internet Explorer mode* policy is Enabled (which is set to `Disabled` in the benchmark).

Rationale:

Internet Explorer is officially retired and unsupported. Allowing browsers to reconfigure into Internet Explorer mode could open an organization up to malicious sites due to its lack of support for modern security features.

Impact:

Users will not be able to see or use the Internet Explorer Mode toolbar.

Audit:

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

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:InternetExplorerModeToolbarButtonEnabled
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\Show the Reload in Internet Explorer mode button in the toolbar
```

Default Value:

Enabled. (Reload in Internet mode button is pinned to the toolbar.)

References:

1. https://docs.microsoft.com/en-us/deployedge/edge-ie-mode
2. GRID: BR-00000093

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.1 Ensure Use of Only Fully Supported Browsers and Email Clients Ensure only fully supported browsers and email clients are allowed to execute in the enterprise, only using the latest version of browsers and email clients provided through the vendor.	●	●	●
v8	9.4 Restrict Unnecessary or Unauthorized Browser and Email Client Extensions Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.		●	●
v7	7.1 Ensure Use of Only Fully Supported Browsers and Email Clients Ensure that only fully supported web browsers and email clients are allowed to execute in the organization, ideally only using the latest version of the browsers and email clients provided by the vendor.	●	●	●
v7	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.		●	●

1.127 (L1) Ensure 'Specifies whether SharedArrayBuffers can be used in a non cross-origin-isolated context' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - General Use

Description:

This policy setting specifies whether SharedArrayBuffers can be used in a non-cross-origin-isolated context. A SharedArrayBuffer is a binary data buffer that can be used to create views on shared memory. SharedArrayBuffers have a memory access vulnerability in several popular CPUs.

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

Rationale:

Disabling this policy prevents attackers from being able to exploit memory access vulnerabilities found in popular CPUs.

Impact:

Users may experience slightly slower loading of webpages.

Audit:

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

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:SharedArrayBufferUnrestrictedAccessAllowed
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\Specifies whether SharedArrayBuffers can be used in a non cross-origin-isolated context
```

Default Value:

Enabled. (Sites are allowed to use SharedArrayBuffers.)

References:

1. https://blogs.windows.com/msedgedev/2018/01/03/speculative-execution-mitigations-microsoft-edge-internet-explorer/
2. https://docs.microsoft.com/en-us/DeployEdge/microsoft-edge-policies#sharedarraybufferunrestrictedaccessallowed
3. GRID: BR-00000094

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

1.128 (L2) Ensure 'Specify if online OCSP/CRL checks are required for local trust anchors' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 (L2) - 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 to be used to give a false sense of a secure connection.

Impact:

If Microsoft Edge cannot 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 setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:RequireOnlineRevocationChecksForLocalAnchors
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Enabled`:

```
Microsoft Edge\Specify if online OCSP/CRL checks are required for local trust anchors
```

Default Value:

Disabled.

References:

1. https://docs.microsoft.com/DeployEdge/microsoft-edge-policies#requireonlinerevocationchecksforlocalanchors
2. GRID: BR-00000095

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

1.129 (L2) Ensure 'Spell checking provided by Microsoft Editor' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - Limited Functionality

Description:

This policy setting controls whether the Microsoft Editor service provides enhanced spell and grammar checking for eligible text fields.

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

Rationale:

Microsoft Editor is an AI-powered service that that sends data to a third-party cloud service. Sending this data to the cloud could lead to sensitive data being exposed.

Impact:

Spell check can only be provided by local engines that use platform or Hunspell services. The results from these engines might be less informative than the results Microsoft Editor can provide.

Note: If the `spellcheckEnabled` (Enable spellcheck) policy is set to `Disabled`, or the user disables spell checking in the settings page, this policy will have no effect.

Audit:

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

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:MicrosoftEditorProofingEnabled
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\Spell checking provided by Microsoft Editor
```

Default Value:

Enabled. (Microsoft Editor spell check can be used for eligible text fields.)

References:

1. https://learn.microsoft.com/en-us/DeployEdge/microsoft-edge-policies#MicrosoftEditorProofingEnabled
2. GRID: BR-00000096

CIS Controls:

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

1.130 (L1) Ensure 'Standalone Sidebar Enabled' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - General Use

Description:

This policy setting controls whether users will have the ability to activate the standalone sidebar. The standalone sidebar is an optional mode for the sidebar in Microsoft Edge and uses Bing AI. When this mode is activated by a user, the sidebar appears in a fixed position on the Microsoft Windows desktop and is hidden from the browser application frame.

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

Rationale:

Microsoft Edge determines what data to send to Bing AI based on the user's query and their consent to share data with Microsoft. This could allow data to be transmitted to a third-party cloud service. This could lead to sensitive data being exposed.

Bing AI offers various features, such as summarizing financial reports, comparing financials of different companies, and aiding users in creating and editing content which could also lead to sensitive data being exposed.

Impact:

Users will not be able to access the *HubsSidebarEnabled* (Show Hubs Sidebar) and it will also prevent them from accessing standalone sidebar and using the Bing AI feature.

Audit:

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

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:StandaloneHubsSidebarEnabled
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\Standalone Sidebar Enabled
```

Default Value:

Enabled. (Users will have the ability to activate the standalone sidebar.)

References:

1. https://learn.microsoft.com/en-us/DeployEdge/microsoft-edge-policies#standaloneHubsSidebarEnabled
2. https://learn.microsoft.com/en-us/microsoft-edge/privacy-whitepaper/#bing-chat-in-microsoft-edge-sidebar
3. GRID: BR-00000097

CIS Controls:

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

1.131 (L1) Ensure 'Suggest similar pages when a webpage can’t be found' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - 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 with an error if 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 setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:AlternateErrorPagesEnabled
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\Suggest similar pages when a webpage can’t be found
```

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
2. GRID: BR-00000098

CIS Controls:

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

1.132 (L1) Ensure 'Suppress the unsupported OS warning' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - General Use

Description:

This policy setting suppresses the warning that appears when Microsoft Edge is running on a computer or operating system that is no longer supported. If this policy is disabled or unset, the warnings will appear on such unsupported computers or operating systems.

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

Rationale:

Users will be notified if the Operating System software is no longer supported.

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 setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:SuppressUnsupportedOSWarning
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\Suppress the unsupported OS warning
```

Default Value:

Disabled. (Warnings will appear on such unsupported computers or operating systems.)

References:

1. GRID: BR-00000099

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.2 Ensure Authorized Software is Currently Supported Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently.	●	●	●
v7	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.	●	●	●

1.133 (L2) Ensure 'Text prediction enabled by default' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - Limited Functionality

Description:

This policy setting controls whether text predictions will be provided for eligible text fields. The Microsoft Turing service uses natural language processing to generate predictions for long-form editable text fields on web pages.

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

Rationale:

Enabling text predictions could allow data to be transmitted to a third-party cloud service, which could lead to sensitive data being exposed.

Impact:

Text predictions will not be provided in eligible text fields. Sites may still provide their own text predictions.

Audit:

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

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:TextPredictionEnabled
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\Text prediction enabled by default
```

Default Value:

Enabled. (Text predictions will be provided for eligible text fields.)

References:

1. https://learn.microsoft.com/en-us/DeployEdge/microsoft-edge-policies#textpredictionEnabled
2. GRID: BR-00000101

CIS Controls:

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

1.134 (L1) Ensure 'Wait for Internet Explorer mode tabs to completely unload before ending the browser session' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - General Use

Description:

This policy setting causes Microsoft Edge to continue running until all Internet Explorer tabs have completely finished unloading. This allows Internet Explorer plugins like ActiveX controls to perform additional critical work even after the browser has been closed.

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

Rationale:

Enabling this policy can cause stability and performance issues, and Microsoft Edge processes may remain active in the background with no visible windows if the webpage or plugin prevents Internet Explorer from unloading. This policy should only be used if your organization depends on a plugin that requires this behavior.

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 setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:InternetExplorerIntegrationAlwayswaitFo
rUnload
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\Wait for Internet Explorer mode tabs to completely unload
before ending the browser session
```

Default Value:

Disabled. (Microsoft Edge will not always wait for Internet Explorer mode tabs to fully unload before ending the browser session.)

References:

1. https://learn.microsoft.com/en-us/DeployEdge/microsoft-edge-policies#InternetExplorerIntegrationAlwayswaitForUnload
2. GRID: BR-00000102

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

1.135 (L1) Ensure 'Wallet Donation Enabled' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - General Use

Description:

The Wallet Donation feature in Microsoft Edge allows users to view their donation summary, explore Nonprofit organizations (NPOs), donate to an NPO, manage their monthly donations, and view their donation history.

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

Rationale:

Allowing users the ability to use the wallet donation feature in Microsoft Edge could lead to sensitive data being exposed.

Impact:

The wallet donation feature in Microsoft Edge will not function.

Audit:

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

```
HKLM\SOFTWARE\Policies\Microsoft\Edge:WalletDonationEnabled
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Edge\Wallet Donation Enabled
```

Default Value:

Enabled. (Users can use the wallet donation feature in Microsoft Edge.)

References:

1. https://learn.microsoft.com/en-us/DeployEdge/microsoft-edge-policies#walletdonationenabled
2. GRID: BR-00000103

CIS Controls:

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

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 therefore no policy configurations are recommended for this section.

3 Microsoft Edge Update

This section contains recommendations for Microsoft Edge Update.

3.1 Applications

This section contains recommendations for Applications.

3.1.1 (L1) Ensure 'Update policy override default' is set to 'Enabled: Automatic silent updates only' or Higher (Automated)

Profile Applicability:

- Level 1 (L1) - General Use

Description:

This policy settings sets the default behavior for all channels concerning the way Microsoft Edge Update handles available updates for Microsoft Edge.

The recommended state for this setting is: `Enabled: Always allow updates (recommended)` or `Enabled: Automatic silent updates only`.

Note: This setting can be overridden for individual channels by specifying the *Update policy override* policy for those specific channels.

Note #2: This policy is available only on Windows instances that are joined to a Microsoft® Active Directory® domain.

Rationale:

Applying software updates as soon as they become available can ensure that systems will always have the most recent critical updates installed.

Impact:

The latest Microsoft Edge updates are automatically installed. Enterprises that use other means of patching systems will need to exclude this recommendation from the benchmark.

Audit:

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

```
HKLM\SOFTWARE\Policies\Microsoft\EdgeUpdate:UpdateDefault
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Enabled: Always allow updates (recommended)` or `Enabled: Automatic silent updates only`:

```
Microsoft Edge Update\Applications\Update policy override default
```

Default Value:

Microsoft Edge Update handles available updates as specified by the *Update policy override* policy.

References:

1. GRID: BR-00000140

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.4 Perform Automated Application Patch Management Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	●	●	●
v7	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.	●	●	●

3.2 Microsoft Edge WebView2 Runtime

This section contains recommendations for Microsoft Edge Microsoft Edge WebView2 Runtime.

3.3 Preferences

This section contains recommendations for Microsoft Edge Microsoft Edge Preferences.

3.3.1 (L1) Ensure 'Auto-update check period override' is set to any value except '0' (Automated)

Profile Applicability:

- Level 1 (L1) - General Use

Description:

This policy setting configures the minimum number of minutes between automatic update checks.

The recommended state for this setting is: any value **except** `0`.

Rationale:

Automatic updates can help ensure that the computers in the environment will always have the most recent critical updates and can decrease the amount of time the system will remain vulnerable between updates and patches.

Impact:

If using a third-party for patching, an exception to this recommendation will be needed.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location which should be set to any `REG_DWORD` value **except** `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\EdgeUpdate:AutoUpdateCheckPeriodMinutes
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to any value **except** `0`:

```
Microsoft Edge Update\Preferences\Auto-update check period override
```

Default Value:

1400 (10 hours)

References:

1. GRID: BR-00000141

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.4 Perform Automated Application Patch Management Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	●	●	●
v7	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.	●	●	●

4 Microsoft Edge WebView2

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

4.1 Network settings

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

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	**Microsoft Edge**		
1.1	**Application Guard settings**		
1.2	**Cast**		
1.2.1	(L1) Ensure 'Enable Google Cast' is set to 'Disabled' (Automated)	☐	☐
1.3	**Certificate management settings**		
1.3.1	(L1) Ensure 'Allow users to manage installed CA certificates' is set to 'Enabled: Disallow users from managing certificates' (Automated)	☐	☐
1.4	**Content Settings**		
1.4.1	(L2) Ensure 'Allow read access via the File System API on these sites' is set to 'Disabled' (Automated)	☐	☐
1.4.2	(L2) Ensure 'Choose whether users can receive customized background images and text, suggestions, notifications, and tips for Microsoft services' is set to 'Disabled' (Automated)	☐	☐
1.4.3	(L1) Ensure 'Control use of insecure content exceptions' is set to 'Enabled: Do not allow any site to load blockable mixed content' (Automated)	☐	☐
1.4.4	(L2) Ensure 'Control use of JavaScript JIT' is set to 'Enabled: Do not allow any site to run JavaScript JIT' (Automated)	☐	☐
1.4.5	(L2) Ensure 'Control use of the File System API for reading' is set to 'Enabled: Don't allow any site to request read access to files and directories via the File System API' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.4.6	(L1) Ensure 'Control use of the File System API for writing' is set to 'Enabled: Don't allow any site to request write access to files and directories' (Automated)	☐	☐
1.4.7	(L2) Ensure 'Control use of the Web Bluetooth API' is set to 'Enabled: Do not allow any site to request access to Bluetooth devices via the Web Bluetooth API' (Automated)	☐	☐
1.4.8	(L2) Ensure 'Control use of the WebHID API' is set to 'Enabled: Do not allow any site to request access to HID devices via the WebHID API' (Automated)	☐	☐
1.4.9	(L1) Ensure 'Default automatic downloads setting' is set to 'Enabled: Don´t allow any website to perform automatic downloads' (Automated)	☐	☐
1.4.10	(L1) Ensure 'Default geolocation setting' is set to 'Enabled: Don't allow any site to track users' physical location' (Automated)	☐	☐
1.4.11	(L2) Ensure 'Default setting for third-party storage partitioning' is set to 'Enabled: Block third-party storage partitioning from being enabled.' (Automated)	☐	☐
1.5	**Default search provider**		
1.6	**Downloads**		
1.6.1	(L1) Ensure 'Enable insecure download warnings' is set to 'Enabled' (Automated)	☐	☐
1.7	**Edge Website Typo Protection settings**		
1.7.1	(L1) Ensure 'Configure Edge Website Typo Protection' is set to 'Enabled' (Automated)	☐	☐
1.8	**Edge Workspaces settings**		
1.9	**Experimentation**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.9.1	(L1) Ensure 'Configure users ability to override feature flags' is set to 'Enabled: Prevent users from overriding feature flags' (Automated)	☐	☐
1.10	**Extensions**		
1.10.1	(L1) Ensure 'Blocks external extensions from being installed' is set to 'Enabled' (Automated)	☐	☐
1.10.2	(L2) Ensure 'Configure extension management settings' is set to 'Enabled: { "*": {"installation_mode": "blocked" }}' (Automated)	☐	☐
1.11	**Games settings**		
1.11.1	(L1) Ensure 'Enable Gamer Mode' is set to 'Disabled' (Automated)	☐	☐
1.12	**Generative AI**		
1.13	**HTTP authentication**		
1.13.1	(L1) Ensure 'Allow Basic authentication for HTTP' is set to 'Disabled' (Automated)	☐	☐
1.13.2	(L1) Ensure 'Allow cross-origin HTTP Authentication prompts' is set to 'Disabled' (Automated)	☐	☐
1.13.3	(L2) Ensure 'Supported authentication schemes' is set to 'Enabled: ntlm, negotiate' (Automated)	☐	☐
1.14	**Identity and sign-in**		
1.14.1	(L1) Ensure 'Guided Switch Enabled' is set to 'Disabled' (Automated)	☐	☐
1.15	**Idle Browser Actions**		
1.16	**Immersive Reader settings**		
1.17	**Kiosk Mode settings**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.18	**Manageability**		
1.19	**Native Messaging**		
1.20	**Network settings**		
1.20.1	(L1) Ensure 'Specifies whether to block requests from public websites to devices on a user's local network' is set to 'Enabled' (Automated)	☐	☐
1.21	**Password manager and protection**		
1.21.1	(L1) Ensure 'Enable saving passwords to the password manager' is set to 'Disabled' (Automated)	☐	☐
1.22	**PDF Reader**		
1.23	**Permit or deny screen capture**		
1.24	**Performance**		
1.24.1	(L1) Ensure 'Enable startup boost' is set to 'Disabled' (Automated)	☐	☐
1.25	**Printing**		
1.26	**Private Network Request Settings**		
1.27	**Proxy server**		
1.28	**Related Website Sets Settings**		
1.29	**Scareware Blocker settings**		
1.30	**Sleeping tabs settings**		
1.31	**SmartScreen settings**		
1.31.1	(L1) Ensure 'Configure Microsoft Defender SmartScreen' is set to 'Enabled' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.31.2	(L1) Ensure 'Configure Microsoft Defender SmartScreen to block potentially unwanted apps' is set to 'Enabled' (Automated)	☐	☐
1.31.3	(L1) Ensure 'Enable Microsoft Defender SmartScreen DNS requests' is set to 'Enabled' (Automated)	☐	☐
1.31.4	(L1) Ensure 'Force Microsoft Defender SmartScreen checks on downloads from trusted sources' is set to 'Enabled' (Automated)	☐	☐
1.31.5	(L1) Ensure 'Prevent bypassing Microsoft Defender SmartScreen prompts for sites' is set to 'Enabled' (Automated)	☐	☐
1.31.6	(L1) Ensure 'Prevent bypassing of Microsoft Defender SmartScreen warnings about downloads' is set to 'Enabled' (Automated)	☐	☐
1.32	**Startup, home page and new tab page**		
1.32.1	(L1) Ensure 'Disable Bing chat entry-points on Microsoft Edge Enterprise new tab page' is set to 'Disabled' (Automated)	☐	☐
1.33	(L1) Ensure 'Ads setting for sites with intrusive ads' is set to 'Enabled: Block ads on sites with intrusive ads.' (Automated)	☐	☐
1.34	(L1) Ensure 'Allow download restrictions' is set to 'Enabled: Block malicious downloads' (Automated)	☐	☐
1.35	(L2) Ensure 'Allow features to download assets from the Asset Delivery Service' is set to 'Disabled' (Automated)	☐	☐
1.36	(L2) Ensure 'Allow file selection dialogs' is set to 'Disabled' (Automated)	☐	☐
1.37	(L1) Ensure 'Allow Google Cast to connect to Cast devices on all IP addresses' is set to 'Disabled' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.38	(L1) Ensure 'Allow import of data from other browsers on each Microsoft Edge launch' is set to 'Disabled' (Automated)	☐	☐
1.39	(L1) Ensure 'Allow importing of autofill form data' is set to 'Disabled' (Automated)	☐	☐
1.40	(L1) Ensure 'Allow importing of browser settings' is set to 'Disabled' (Automated)	☐	☐
1.41	(L1) Ensure 'Allow importing of home page settings' is set to 'Disabled' (Automated)	☐	☐
1.42	(L1) Ensure 'Allow importing of payment info' is set to 'Disabled' (Automated)	☐	☐
1.43	(L1) Ensure 'Allow importing of saved passwords' is set to 'Disabled' (Automated)	☐	☐
1.44	(L1) Ensure 'Allow importing of search engine settings' is set to 'Disabled' (Automated)	☐	☐
1.45	(L1) Ensure 'Allow managed extensions to use the Enterprise Hardware Platform API' is set to 'Disabled' (Automated)	☐	☐
1.46	(L2) Ensure 'Allow or block audio capture' is set to 'Disabled' (Automated)	☐	☐
1.47	(L2) Ensure 'Allow or block video capture' is set to 'Disabled' (Automated)	☐	☐
1.48	(L2) Ensure 'Allow or deny screen capture' is set to 'Disabled' (Automated)	☐	☐
1.49	(L1) Ensure 'Allow personalization of ads, search and news by sending browsing history to Microsoft' is set to 'Disabled' (Automated)	☐	☐
1.50	(L1) Ensure 'Allow queries to a Browser Network Time service' is set to 'Enabled' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.51	(L1) Ensure 'Allow remote debugging' is set to 'Disabled' (Automated)	☐	☐
1.52	(L1) Ensure 'Allow the audio sandbox to run' is set to 'Enabled' (Automated)	☐	☐
1.53	(L2) Ensure 'Allow unconfigured sites to be reloaded in Internet Explorer mode' is set to 'Disabled' (Automated)	☐	☐
1.54	(L1) Ensure 'Allow user feedback' is set to 'Disabled' (Automated)	☐	☐
1.55	(L2) Ensure 'Allow users to open files using the ClickOnce protocol' is set to 'Disabled' (Automated)	☐	☐
1.56	(L2) Ensure 'Allow users to open files using the DirectInvoke protocol' is set to 'Disabled' (Automated)	☐	☐
1.57	(L2) Ensure 'Allow users to proceed from the HTTPS warning page' is set to 'Disabled' (Automated)	☐	☐
1.58	(L1) Ensure 'Allow Web Authentication requests on sites with broken TLS certificates' is set to 'Disabled' (Automated)	☐	☐
1.59	(L1) Ensure 'Allow websites to query for available payment methods' is set to 'Disabled' (Automated)	☐	☐
1.60	(L2) Ensure 'AutoLaunch Protocols Component Enabled' is set to 'Disabled' (Automated)	☐	☐
1.61	(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)	☐	☐
1.62	(L1) Ensure 'Automatically open downloaded MHT or MHTML files from the web in Internet Explorer mode' is set to 'Disabled' (Automated)	☐	☐
1.63	(L2) Ensure 'Block third party cookies' is set to 'Enabled' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.64	(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)' or higher (Automated)	☐	☐
1.65	(L2) Ensure 'Browser sign-in settings' is set to 'Enabled: Disable browser sign-in' (Automated)	☐	☐
1.66	(L1) Ensure 'Clear browsing data when Microsoft Edge closes' is set to 'Disabled' (Automated)	☐	☐
1.67	(L1) Ensure 'Clear cached images and files when Microsoft Edge closes' is set to 'Disabled' (Automated)	☐	☐
1.68	(L1) Ensure 'Clear history for IE and IE mode every time you exit' is set to 'Disabled' (Automated)	☐	☐
1.69	(L1) Ensure 'Configure browser process code integrity guard setting' is set to 'Enabled: Enable code integrity guard enforcement in the browser process.' (Automated)	☐	☐
1.70	(L1) Ensure 'Configure InPrivate mode availability' is set to 'Enabled: InPrivate mode disabled' (Automated)	☐	☐
1.71	(L2) Ensure 'Configure Online Text To Speech' is set to 'Disabled' (Automated)	☐	☐
1.72	(L2) Ensure 'Configure Speech Recognition' is set to 'Disabled' (Automated)	☐	☐
1.73	(L1) Ensure 'Configure the list of names that will bypass the HSTS policy check' is set to 'Disabled' (Automated)	☐	☐
1.74	(L1) Ensure 'Configure the list of types that are excluded from synchronization' is set to 'Enabled' (Automated)	☐	☐
1.75	(L1) Ensure 'Configure the Share experience' is set to 'Enabled: Don't allow using the Share experience' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.76	(L1) Ensure 'Continue running background apps after Microsoft Edge closes' is set to 'Disabled' (Automated)	☐	☐
1.77	(L1) Ensure 'Control communication with the Experimentation and Configuration Service' is set to 'Enabled: Disable communication with the Experimentation and Configuration Service' (Automated)	☐	☐
1.78	(L2) Ensure 'Control use of the Headless Mode' is set to 'Disabled' (Automated)	☐	☐
1.79	(L2) Ensure 'Control use of the Serial API' is set to 'Enable: Do not allow any site to request access to serial ports via the Serial API' (Automated)	☐	☐
1.80	(L1) Ensure 'Control where security restrictions on insecure origins apply' is set to 'Disabled' (Automated)	☐	☐
1.81	(L2) Ensure 'Default sensors setting' is set to 'Enabled: Do not allow any site to access sensors' (Automated)	☐	☐
1.82	(L1) Ensure 'Delete old browser data on migration' is set to 'Disabled' (Automated)	☐	☐
1.83	(L1) Ensure 'Disable saving browser history' is set to 'Disabled' (Automated)	☐	☐
1.84	(L1) Ensure 'Disable synchronization of data using Microsoft sync services' is set to 'Enabled' (Automated)	☐	☐
1.85	(L1) Ensure 'DNS interception checks enabled' is set to 'Enabled' (Automated)	☐	☐
1.86	(L1) Ensure 'Dynamic Code Settings' is set to 'Enabled: Prevent the browser process from creating dynamic code' (Automated)	☐	☐
1.87	(L1) Ensure 'Edge 3P SERP Telemetry Enabled' is set to 'Disabled' (Automated)	☐	☐
1.88	(L1) Ensure 'Edge Wallet E-Tree Enabled' is set to 'Disabled' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.89	(L1) Ensure 'Enable Application Bound Encryption' is set to 'Enabled' (Automated)	☐	☐
1.90	(L1) Ensure 'Enable AutoFill for addresses' is set to 'Disabled' (Automated)	☐	☐
1.91	(L1) Ensure 'Enable AutoFill for payment instruments' is set to 'Disabled' (Automated)	☐	☐
1.92	(L1) Ensure 'Enable browser legacy extension point blocking' is set to 'Enabled' (Automated)	☐	☐
1.93	(L1) Ensure 'Enable component updates in Microsoft Edge' is set to 'Enabled' (Automated)	☐	☐
1.94	(L1) Ensure 'Enable deleting browser and download history' is set to 'Disabled' (Automated)	☐	☐
1.95	(L2) Ensure 'Enable Drop feature in Microsoft Edge' is set to 'Disabled' (Automated)	☐	☐
1.96	(L1) Ensure 'Enable globally scoped HTTP auth cache' is set to 'Disabled' (Automated)	☐	☐
1.97	(L2) Ensure 'Enable guest mode' is set to 'Disabled' (Automated)	☐	☐
1.98	(L1) Ensure 'Enable network prediction' is set to 'Enabled: Don't predict network actions on any network connection' (Automated)	☐	☐
1.99	(L1) Ensure 'Enable profile creation from the Identity flyout menu or the Settings page' is set to 'Disabled' (Automated)	☐	☐
1.100	(L1) Ensure 'Enable resolution of navigation errors using a web service' is set to 'Disabled' (Automated)	☐	☐
1.101	(L2) Ensure 'Enable search suggestions' is set to 'Disabled' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.102	(L1) Ensure 'Enable security warnings for command-line flags' is set to 'Enabled' (Automated)	☐	☐
1.103	(L1) Ensure 'Enable site isolation for every site' is set to 'Enabled' (Automated)	☐	☐
1.104	(L1) Ensure 'Enable the Search bar' is set to 'Disabled' (Automated)	☐	☐
1.105	(L1) Ensure 'Enable tab organization suggestions' is set to 'Disabled' (Automated)	☐	☐
1.106	(L2) Ensure 'Enable Translate' is set to 'Disabled' (Automated)	☐	☐
1.107	(L1) Ensure 'Enable upload files from mobile in Microsoft Edge desktop' is set to 'Disabled' (Automated)	☐	☐
1.108	(L1) Ensure 'Enable use of ephemeral profiles' is set to 'Disabled' (Automated)	☐	☐
1.109	(L1) Ensure 'Enable warnings for insecure forms' is set to 'Enabled' (Automated)	☐	☐
1.110	(L2) Ensure 'Enable QR Code Generator' is set to 'Disabled' (Automated)	☐	☐
1.111	(L1) Ensure 'Enables DALL-E themes generation' is set to 'Disabled' (Automated)	☐	☐
1.112	(L2) Ensure 'Enforce Bing SafeSearch' is set to 'Enabled: Configure moderate search restrictions in Bing' (Automated)	☐	☐
1.113	(L2) Ensure 'Enforce Google SafeSearch' is set to 'Enabled' (Automated)	☐	☐
1.114	(L1) Ensure 'Enhance the security state in Microsoft Edge' is set to 'Enabled: Balanced mode' or higher (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.115	(L2) Ensure 'Enhanced Security Mode configuration for Intranet zone sites' is set to 'Disabled' (Automated)	☐	☐
1.116	(L1) Ensure 'Hide the First-run experience and splash screen' is set to 'Enabled' (Automated)	☐	☐
1.117	(L1) Ensure 'In-app support Enabled' is set to 'Disabled' (Automated)	☐	☐
1.118	(L2) Ensure 'Live captions allowed' is set to 'Disabled' (Automated)	☐	☐
1.119	(L1) Ensure 'Manage exposure of local IP addressess by WebRTC' is set to 'Disabled' (Automated)	☐	☐
1.120	(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)	☐	☐
1.121	(L1) Ensure 'Set disk cache size, in bytes' is set to 'Enabled: 250609664' (Automated)	☐	☐
1.122	(L1) Ensure 'Set the time period for update notifications' is set to 'Enabled: 86400000' (Automated)	☐	☐
1.123	(L1) Ensure 'Shopping in Microsoft Edge Enabled' is set to 'Disabled' (Automated)	☐	☐
1.124	(L2) Ensure 'Show an "Always open" checkbox in external protocol dialog' is set to 'Disabled' (Automated)	☐	☐
1.125	(L1) Ensure 'Show Microsoft Rewards experiences' is set to 'Disabled' (Automated)	☐	☐
1.126	(L1) Ensure 'Show the Reload in Internet Explorer mode button in the toolbar' is set to 'Disabled' (Automated)	☐	☐
1.127	(L1) Ensure 'Specifies whether SharedArrayBuffers can be used in a non cross-origin-isolated context' is set to 'Disabled' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.128	(L2) Ensure 'Specify if online OCSP/CRL checks are required for local trust anchors' is set to 'Enabled' (Automated)	☐	☐
1.129	(L2) Ensure 'Spell checking provided by Microsoft Editor' is set to 'Disabled' (Automated)	☐	☐
1.130	(L1) Ensure 'Standalone Sidebar Enabled' is set to 'Disabled' (Automated)	☐	☐
1.131	(L1) Ensure 'Suggest similar pages when a webpage can’t be found' is set to 'Disabled' (Automated)	☐	☐
1.132	(L1) Ensure 'Suppress the unsupported OS warning' is set to 'Disabled' (Automated)	☐	☐
1.133	(L2) Ensure 'Text prediction enabled by default' is set to 'Disabled' (Automated)	☐	☐
1.134	(L1) Ensure 'Wait for Internet Explorer mode tabs to completely unload before ending the browser session' is set to 'Disabled' (Automated)	☐	☐
1.135	(L1) Ensure 'Wallet Donation Enabled' is set to 'Disabled' (Automated)	☐	☐
2	**Microsoft Edge - Default Settings (users can override)**		
3	**Microsoft Edge Update**		
3.1	**Applications**		
3.1.1	(L1) Ensure 'Update policy override default' is set to 'Enabled: Automatic silent updates only' or Higher (Automated)	☐	☐
3.2	**Microsoft Edge WebView2 Runtime**		
3.3	**Preferences**		
3.3.1	(L1) Ensure 'Auto-update check period override' is set to any value except '0' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
4	**Microsoft Edge WebView2**		
4.1	**Network settings**		

Appendix: Change History

Date: 1/28/2026 Version: 1.0.0