

CIS Google Chrome Enterprise Core Browser Benchmark

v1.0.0 - 06-30-2025

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 Introduction.....	18
Recommendation Order.....	18
Enforced Defaults.....	18
Viewing the Resulting "Policies" in Chrome.....	18
2 Settings.....	19

2.1 Sign-in Settings	20
2.1.1 (L2) Ensure 'Browser sign in settings' is set to 'Disabled browser sign-in' (Automated)	21
2.1.2 (L1) Ensure 'Azure Cloud Authentication' Is Set to 'Enable Azure cloud authentication' (Manual)	23
2.2 Apps and Extensions	25
2.2.1 (L2) Ensure 'Manifest v2 extension availability' Is Set to 'Enable force-installed manifest v2 extensions on the sign-in screen' (Automated)	26
2.3 Site Isolation	28
2.3.1 (L1) Ensure 'Site isolation' is set to 'Require Site Isolation for all websites, as well as any origins below' (Automated)	29
2.4 Security	31
2.4.1 (L1) Ensure 'Password manager' is Explicitly Configured (Manual)	32
2.4.2 (L1) Ensure 'Web Authentication requests on sites with broken TLS certificates' Is Set to 'Do not allow WebAuthn API requests on sites with broken TLS certificates' (Automated)	34
2.4.3 (L1) Ensure 'Post-quantum TLS' Is Set to 'Allow post-quantum key agreement in TLS connections' (Automated)	36
2.4.4 (L1) Ensure 'Incognito mode' is set to 'Disallow incognito mode' (Automated)	38
2.4.5 (L1) Ensure 'Browser history' is set to 'Always save browser history' (Automated)	40
2.4.6 (L1) Ensure 'Clear browser history' Is Set to 'Do not allow clearing history in settings menu' (Automated)	42
2.4.7 (L1) Ensure 'Force ephemeral mode' is set to 'Do not erase local user data' (Automated)	44
2.4.8 (L1) Ensure 'Online revocation checks' is set to 'Perform online OCSP/CRL checks' (Automated)	46
2.4.9 (L1) Ensure 'Geolocation' is set to 'Do not allow sites to detect users' geolocation' (Automated)	48
2.4.10 (L1) Ensure 'Allowed certificate transparency URLs' is Not Set (Automated)	50
2.4.11 (L1) Ensure 'Certificate transparency CA allowlist' is Not Set (Automated)	52
2.4.12 (L1) Ensure 'Renderer App Container' Is Set to 'Enable the Renderer App Container sandbox' (Automated)	54
2.4.13 (L1) Ensure 'Enable leak detection for entered credentials' Is Set to 'Enable Leak detection for entered credentials' (Manual)	56
2.4.14 (L1) Ensure 'Audio sandbox' is set to 'Always sandbox the audio process' (Automated)	58
2.4.15 (L1) Ensure 'Unsupported system warning' is set to 'Allow Chrome to display warnings when running on an unsupported system' (Automated)	60
2.4.16 (L2) Ensure 'Advanced Protection program' Is Set to 'Users enrolled in the Advanced Protection program will receive extra protections' (Manual)	62
2.4.17 (L1) Ensure 'Override insecure origin restrictions' is Not Set (Automated)	64
2.4.18 (L1) Ensure 'Command-line flags' is set to 'Show security warnings when potentially dangerous command-line flags are used' (Automated)	66
2.4.19 (L1) Ensure 'Allow remote debugging' is set to 'Do not allow use of the remote debugging' (Automated)	68
2.4.20 (L1) Ensure 'TLS encrypted ClientHello' Is 'Enable the TLS Encrypted ClientHello experiment' (Automated)	70
2.4.21 (L1) Ensure 'Strict MIME type checking for worker scripts' Is Set to 'Require a JavaScript MIME type for worker scripts' (Automated)	72
2.4.22 (L2) Ensure 'Enforce local anchor constraints' Is 'Enforce constraints in locally added trust anchors' (Automated)	74
2.4.23 (L1) Ensure 'File/directory picker without user gesture' Is Not Set (Automated)	76
2.4.24 (L1) Ensure 'Media picker without user gesture' Is Not Configured (Automated)	78
2.5 Remote access (Chrome Remote Desktop)	80
2.5.1 (L1) Ensure 'Remote access hosts' is set with a domain defined in 'Remote access host domain' (Manual)	81
2.5.2 (L1) Ensure 'Firewall traversal' is set to 'Disable firewall traversal' (Automated)	83
2.5.3 (L1) Ensure 'Firewall traversal' is set to 'Disable the use of relay servers' (Automated)	85

2.5.4 (L1) Ensure 'Remote support connections' is set to 'Prevent remote support connections' (Manual).....	87
2.6 Network.....	89
2.6.1 (L1) Ensure 'Proxy mode' is Not Set to 'Always auto detect the proxy' (Automated)	90
2.6.2 (L2) Ensure 'Supported authentication schemes' is set to 'NTLM' and 'Negotiate' (Automated)	92
2.6.3 (L2) Ensure 'SSL error override' is set to 'Block users from clicking through SSL warnings' (Automated).....	94
2.6.4 (L1) Ensure 'WebRTC ICE candidate URLs for local IPs' Is Not Set (Automated).....	96
2.6.5 (L2) Ensure 'DNS over HTTPS' is set to 'Enable DNS-over-HTTPS without insecure fallback' (Automated)	98
2.6.6 (L1) Ensure 'Cross-origin authentication' is set to 'Block cross-origin authentication' (Automated)	101
2.6.7 (L1) Ensure 'Enable globally scoped HTTP authentication cache' is set to 'Disabled' (Automated)	103
2.6.8 (L1) Ensure 'HSTS policy bypass list' is Not Set (Automated).....	105
2.6.9 (L1) Ensure 'DNS interception checks enabled' is set to 'Perform DNS interception checks ' (Automated)	107
2.6.10 (L1) Ensure 'Network service sandbox' Is Set to 'Enable the network sandbox' (Automated).....	109
2.6.11 (L1) Ensure 'Http Allowlist' Is Properly Configured (Manual)	111
2.6.12 (L1) Ensure 'Automatic HTTPS upgrades' Is Set to 'Allow HTTPS upgrades' (Automated)	113
2.7 Import Settings	115
2.7.1 (L1) Ensure 'Import autofill data' is set to 'Disable imports of autofill data' (Automated)	116
2.7.2 (L1) Ensure 'Import homepage' is set to 'Disable imports of homepage' (Automated) ..	118
2.7.3 (L1) Ensure 'Import saved passwords' is set to 'Disable imports of saved passwords' (Automated)	120
2.7.4 (L1) Ensure 'Import search engines' is set to 'Disable imports of search engines' (Automated)	122
2.8 Content	124
2.8.1 (L2) Ensure 'Screen video capture' is set to 'Do not allow sites to prompt the user to share a video stream of their screen' (Automated)	125
2.8.2 (L1) Ensure 'Cast' is set to 'Do not allow users to cast' (Automated)	127
2.8.3 (L1) Ensure 'Clipboard' Is Set to 'Do not allow any site to use the clipboard site permission' (Automated).....	129
2.8.4 (L1) Ensure 'Enable URL-keyed anonymized data collection' is set to 'Data collection is never active' (Automated).....	132
2.8.5 (L1) Ensure 'Third-party cookie blocking' is set to 'Disallow third-party cookies' (Automated)	134
2.8.6 (L1) Ensure 'Cast' is set to 'Do not allow users to Cast' (Automated).....	136
2.8.7 (L2) Ensure 'Cookies' is set to 'Session Only' (Automated)	138
2.8.8 (L2) Ensure 'SafeSearch and Restricted Mode' is set to 'Always use Safe Search for Google Web Search queries' (Automated).....	140
2.8.9 (L1) Ensure 'First-Party Sets' Is Set to 'Disable First-Party Sets for all affected users' (Manual).....	142
2.8.10 (L1) Ensure 'Allow local file access to file:// URLs on these sites in the PDF Viewer' Is Not Set (Automated).....	144
2.8.11 (L2) Ensure 'Notifications' is set to 'Do not allow any site to show desktop notifications' (Automated)	146
2.8.12 (L2) Ensure 'WebUSB API' is set to 'Do not allow any site to request access to USB devices via the WebUSB API' (Automated)	148
2.8.13 (L1) Ensure 'Allow third-party partitioning to be enabled' in 'Third-party storage partitioning' Is Configured (Manual).....	150

2.8.14 (L2) Ensure 'Third-party storage partitioning' Is Set to 'Block third-party storage partitioning from being enabled' (Automated)	152
2.8.15 (L2) Ensure 'Web Bluetooth API' is set to 'Do not allow any site to request access to Bluetooth devices via the Web Bluetooth API' (Automated)	154
2.8.16 (L1) Ensure 'Control use of insecure content exceptions' is set to 'Do not allow any site to load mixed content' (Automated)	156
2.9 User Experience.....	158
2.9.1 (L1) Ensure 'Download location prompt' is set to 'Ask the user where to save the file before downloading' (Automated).....	159
2.9.2 (L2) Ensure 'Browser guest mode' is set to 'Prevent guest browser logins' (Automated)	161
2.9.3 (L1) Ensure 'Credit card form Autofill' is set to 'Never Autofill credit card forms' (Automated)	163
2.9.4 (L2) Ensure 'Address form Autofill' is set to 'Never Autofill address forms' (Automated)	165
2.9.5 (L1) Ensure 'Allow user feedback' is set to 'Do not allow user feedback' (Automated) ..	167
2.9.6 (L2) Ensure 'File selection dialogs' is set to 'Block file selection dialogs' (Automated) ..	169
2.9.7 (L2) Ensure 'Google Translate' is set to 'Never offer translation' (Automated)	171
2.9.8 (L1) Ensure 'Spell check service' is set to 'Disable the spell checking web service' (Automated)	173
2.9.9 (L1) Ensure 'Network prediction' Is Set to 'Do not predict network actions' (Automated)	175
2.9.10 (L1) Ensure 'Alternate error pages' is set to 'Never use alternate error pages' (Automated)	177
2.9.11 (L1) Ensure 'Payment methods' is set to 'Always tell websites that no payment methods are saved' (Automated)	179
2.10 Omnibox Search Provider	181
2.10.1 (L2) Ensure 'Search suggest' is set to 'Never allow users to use Search Suggest' (Automated)	182
2.10.2 (L1) Ensure 'Side Panel search' Is Set to 'Disable Side Panel search on all web pages' (Automated)	184
2.11 Hardware	186
2.11.1 (L1) Ensure 'Enterprise Hardware Platform API' is set to 'Do not allow managed extensions to use the Enterprise Hardware Platform API' (Automated)	187
2.11.2 (L2) Ensure 'Video input (camera)' is set to 'Disable camera input for websites and apps' (Automated)	189
2.11.3 (L2) Ensure 'Audio input (microphone)' is set to 'Disable audio input' (Automated)	191
2.11.4 (L2) Ensure 'Sensors' is set to 'Do not allow any site to access sensors' (Automated)	193
2.11.5 (L2) Ensure 'Web Serial API' is set to 'Do not allow any site to request access to serial ports via the Web Serial API' (Automated)	195
2.12 Chrome Safe Browsing	197
2.12.1 (L1) Ensure no URLs Are Configured in 'Safe Browsing allowed domains' (Automated)	198
2.12.2 (L1) Ensure 'Safe Browsing for trusted sources' is set to 'Perform Safe Browsing checks on all downloaded files' (Automated)	200
2.12.3 (L1) Ensure 'Disable bypassing Safe Browsing warnings' is set to 'Do not allow user to bypass Safe Browsing warning' (Automated)	202
2.12.4 (L1) Ensure 'Download restrictions' is set to 'Block malicious downloads' (Automated)	204
2.12.5 (L1) Ensure 'Suppress lookalike domain warnings on domains' is Not Set (Automated)	206
2.12.6 (L2) Ensure 'SafeSites URL filter' is set to 'Filter top level sites (but not embedded iframes) for adult content' (Automated)	209
2.12.7 (L1) Ensure 'Safe Browsing protection' is set to 'Safe Browsing is active in the standard mode' and 'Allow higher-protection proxied lookups' (Manual)	211

2.13 Generative AI	214
2.13.1 Ensure 'Generative AI policy defaults' Is Set to 'Allow GenAI features without improving AI models' (Automated)	215
2.13.2 Ensure 'Help me write' Is Set to 'Use the value specified in the Generative AI policy defaults setting' (Automated)	217
2.13.3 Ensure 'DevTools AI features' Is Set to 'Use the value specified in the Generative AI policy defaults setting' (Automated)	219
2.13.4 Ensure 'History search settings' Is Set to 'Use the value specified in the Generative AI policy defaults setting' (Automated)	221
2.13.5 Ensure 'Tab compare' Is Set to 'Use the value specified in the Generative AI policy defaults setting' (Automated)	223
2.13.6 Ensure 'Help me read' Is Set to 'Use the value specified in the Generative AI policy defaults setting' (Manual)	225
2.14 Chrome Updates	226
2.14.1 (L1) Ensure 'Component updates' is set to 'Enable updates for all components' (Automated)	227
2.14.2 (L1) Ensure 'Relaunch notification' sets 'Time Period (hours)' to '168 or less' and 'Initial quiet period (hours)' to less than 'Time Period (hours)' (Automated)	230
2.14.3 (L1) Ensure 'Relaunch notification' is set to 'Show notification recommending relaunch' (Automated)	232
2.15 Chrome Variations	234
2.15.1 (L1) Ensure 'Variations' is set to 'Enable Chrome variations' (Manual)	235
2.16 Other Settings	238
2.16.1 (L1) Ensure 'Google time service' is set to 'Allow queries to a Google server to retrieve an accurate timestamp' (Automated)	239
2.16.2 (L1) Ensure 'Disk cache size in bytes' in 'Disk cache size' is set to '250609664' (Automated)	242
2.16.3 (L1) Ensure 'Chrome Sync (ChromeOS)' is set to 'Allow Chrome Sync' and Exclude 'Passwords' (Automated)	244
2.16.4 (L1) Ensure 'Metrics reporting' is set to 'Do not send anonymous reports of usage and crash-related data to Google' (Automated)	246
2.16.5 (L1) Ensure 'Chrome Sync and Roaming Profiles (Chrome Browser - Cloud Managed)' is set to 'Disallow Sync' (Automated)	248
2.16.6 (L1) Ensure 'Allow reporting of domain reliability related data' Is 'Never send domain reliability data to Google' (Automated)	250
2.16.7 (L2) Ensure 'Prohibited Native Messaging hosts' in 'Native Messaging blocked hosts' is set to '*' (Automated)	252
2.16.8 (L1) Ensure 'Background mode' is set to 'Disable background mode' (Automated)	254
3 Apps & Extensions	256
3.1 Extensions	257
3.1.1 (L1) Ensure 'External extensions' is set to 'Block external extensions from being installed' (Automated)	258
3.1.2 (L1) Ensure 'Allowed types of apps and extensions' is set to 'Extension', 'Hosted App', 'Chrome Packaged App', and 'Theme' (Automated)	260
3.1.3 (L1) Ensure 'App and extension install sources' Is Not Set (Automated)	262
3.1.4 (L1) Ensure 'Chrome Web Store unpublished extensions' Is Set to 'Disable unpublished extensions' (Automated)	264
Appendix: Summary Table	266
Appendix: CIS Controls v7 IG 1 Mapped Recommendations	276
Appendix: CIS Controls v7 IG 2 Mapped Recommendations	278
Appendix: CIS Controls v7 IG 3 Mapped Recommendations	284
Appendix: CIS Controls v7 Unmapped Recommendations	290

<i>Appendix: CIS Controls v8 IG 1 Mapped Recommendations</i>	<i>291</i>
<i>Appendix: CIS Controls v8 IG 2 Mapped Recommendations</i>	<i>295</i>
<i>Appendix: CIS Controls v8 IG 3 Mapped Recommendations</i>	<i>301</i>
<i>Appendix: CIS Controls v8 Unmapped Recommendations.....</i>	<i>307</i>
<i>Appendix: Change History</i>	<i>308</i>

Overview

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

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

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

Important Usage Information

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

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

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

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

Key Stakeholders

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

Apply the Correct Version of a Benchmark

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

- **Deploy the Benchmark applicable to the way settings are managed in the environment:** An example of this is the Microsoft Windows family of Benchmarks, which have separate Benchmarks for Group Policy, Intune, and Stand-alone systems based upon how system management is deployed. Applying the wrong Benchmark in this case will give invalid results.
- **Use the most recent version of a Benchmark:** This is true for all Benchmarks, but especially true for cloud technologies. Cloud technologies change frequently and using an older version of a Benchmark may have invalid methods for auditing and remediation.

Exceptions

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

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

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

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

Remediation

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

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

The following is a reasonable remediation approach to follow:

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

Summary

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

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

CIS-CAT® Pro is also available to CIS [SecureSuite](#)® members.

Target Technology Details

This document provides prescriptive guidance for establishing a secure configuration posture for Google Chrome browser. This guide was tested against Google Chrome v138. 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 Google Chrome CIS Benchmarks are written for Google Chrome managed using Google Workspace, not standalone/workgroup systems. Adjustments/tailoring to some recommendations will be needed to maintain functionality if attempting to implement CIS hardening on standalone systems.

Consensus Guidance

This 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
<code>Stylized Monospace font</code>	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
<code>Monospace font</code>	Used for inline code, commands, UI/Menu selections or examples. Text should be interpreted exactly as presented.
<code><Monospace font in brackets></code>	Text set in angle brackets denote a variable requiring substitution for a real value.
<i>Italic font</i>	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) - Corporate/Enterprise Environment (general use)**

Items in this profile intend to:

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

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

This profile extends the "Level 1 (L1)" profile. Items in this profile exhibit one or more of the following characteristics:

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

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

Acknowledgements

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

Contributor

Edward Byrd , Center for Internet Security, New York
Jordan Rakoske
Brian Howson
Johannes Goerlich , Siemens AG
Fletcher Oliver
Adrian Clark
Joe Goerlich , Siemens AG
Patrick Stoeckle , Siemens AG
John Mahlman
Joseph Musso
Loren Hudziak
Daniel Christopher
Kari Byrd

Editor

Phil White , Center for Internet Security, New York
Edward Byrd , Center for Internet Security, New York
Josh Franklin

Recommendations

1 Introduction

This Benchmark assumes that Google Chrome is managed via Google Workspace.

Recommendation Order

This Benchmark has high-level sections based on various security related concerns (Enforced Defaults, Privacy, etc.). The recommendations are in order of the order in Google Workspace.

Enforced Defaults

Many of the settings specified in this Benchmark are also the default settings for the browser. These are specified for the following reasons:

1. The default (Unset) setting may have the same effect as what is prescribed, but they allow the user to change these settings at any time. Actually configuring the browser setting to the prescribed value will prevent the user from changing it.
2. Many organizations want the ability to scan systems for Benchmark compliance and configuration drift using CIS (CIS-CAT) or CIS certified third party tools ([CIS Vendor Partners](#)). Having these settings specified in the Benchmark allows for this.

Viewing the Resulting "Policies" in Chrome

These "Policy" settings can be viewed in Google Chrome directly by typing <chrome://policy/> directly into the Google Chrome address box, or through Google Workspace, <https://admin.google.com>.

For more information on Google Chrome Enterprise Core Browser management, visit <https://chromeenterprise.google/products/cloud-management/>

2 Settings

Settings is a high level configuration option in the Google admin console for managing user and organization settings for the Google Chrome Browser.

2.1 Sign-in Settings

The Google Chrome Admin Sign-in settings are the configuration options for managing user access and data synchronization on Chrome browsers within an organization within the Google Admin console. Administrators can control how users sign in to the Chrome browser on managed devices, including whether they can sign in at all, which accounts they can use, and whether they can sync their browser data to their Google account.

2.1.1 (L2) Ensure 'Browser sign in settings' is set to 'Disabled browser sign-in' (Automated)

Profile Applicability:

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

Description:

Google Chrome offers to sign in with your Google account and use account-related services like Chrome sync. It is possible to sign in to Google Chrome with a Google account to use services like synchronization, and can also be used for configuration and management of the browser.

- **Disable browser sign-in** (0)
- **Enable browser sign-in** (1)
- **Force users to sign-in to use the browser** (2)

The recommended state for this setting is: **Enabled** with a value of **Disable browser sign-in** (0)

NOTE: If an organization is a Google Workspace Enterprise customer, they will want to leave this setting enabled so that users can sign in with Google accounts.

Rationale:

Since external accounts are unmanaged and potentially used to access several private computer systems and many different websites, connecting accounts via sign-in poses a security risk for the company. It interferes with the corporate management mechanisms, as well as permits an unwanted leak of corporate information and possible mixture with private, non-company data.

Impact:

If this setting is configured, the user cannot sign in to the browser and use Google account-based services like Chrome sync.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Browser sign in settings**
6. Ensure **Configuration** is set to **Disabled browser sign-in**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Browser sign in settings**
6. Set **Configuration** to **Disabled browser sign-in**
7. Select **Save**

Default Value:

Unset (Same as Enabled: Enable browser sign-in, but user can change)

References:

1. <https://chromeenterprise.google/policies/#BrowserSignin>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.2 <u>Use DNS Filtering Services</u> Use DNS filtering services on all enterprise assets to block access to known malicious domains.			
v7	4.8 <u>Log and Alert on Changes to Administrative Group Membership</u> Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.			

2.1.2 (L1) Ensure 'Azure Cloud Authentication' Is Set to 'Enable Azure cloud authentication' (Manual)

Profile Applicability:

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

Description:

This policy setting allows accounts backed by a Microsoft® cloud identity provider (i.e., Microsoft Azure Active Directory or the consumer Microsoft account identity provider) to be signed into web properties using that identity automatically. It can be configured to either:

- Disabled (0): **Disable Microsoft® cloud authentication**
- Enabled (1): **Enable Microsoft® cloud authentication**

If the value for **CloudAPAuthEnabled** is not changed from the default, it will behave as if it is disabled.

Rationale:

Enabling this policy setting allows users to use Microsoft Cloud Authentication for any site that requires CA (Cloud Authentication) and does not require an extension.

Impact:

There should be no impact to the user.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **<https://admin.google.com>** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Azure Cloud Authentication**
6. Ensure **Configuration** is set to **Enable Azure cloud authentication**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Azure Cloud Authentication**
6. Set **Configuration** to **Enable Azure cloud authentication**
7. Select **Save**

Default Value:

Unset (Disabled)

References:

1. <https://chromeenterprise.google/policies/#CloudAPAuthEnabled>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.2 <u>Use DNS Filtering Services</u> Use DNS filtering services on all enterprise assets to block access to known malicious domains.			
v7	4.8 <u>Log and Alert on Changes to Administrative Group Membership</u> Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.			

2.2 Apps and Extensions

Apps and extensions settings are configuration options in the Google admin console for control which applications and browser extensions users can install and use on their Chrome browsers within an organization.

Administrators can block unwanted apps, force-install necessary ones, and manage access to specific features by setting policies for each app or extension within the organization.

2.2.1 (L2) Ensure 'Manifest v2 extension availability' Is Set to 'Enable force-installed manifest v2 extensions on the sign-in screen' (Automated)

Profile Applicability:

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

Description:

This policy setting controls extension management settings for Google Chrome, specifically v2 extensions. This policy setting is being sunsetted as Google develops the Manifest v3, but that rollout is currently postponed.

The policy can be configured to:

- Default (0): Default browser behavior
- Disabled (1): Manifest v2 is disabled
- Enabled (2): Manifest v2 is enabled
- Forced Only (3): Manifest v2 is enabled for forced extensions only

Rationale:

Setting this to Forced Only will not allow users to install any additional v2 extensions, and all existing, non-forced, v2 extensions will be disabled.

Impact:

Users that use extensions regularly will have a set of them blocked, which will change their user experience.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Manifest v2 extension availability**
6. Ensure **Configuration** is set to **Enable force-installed manifest v2 extensions on the sign-in screen**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Manifest v2 extension availability**
6. Set **Configuration** to **Enable force-installed manifest v2 extensions on the sign-in screen**
7. Select **Save**

References:

1. <https://chromeenterprise.google/policies/#ExtensionManifestV2Availability>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.2 <u>Establish and Maintain a Remediation Process</u> Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.			
v7	9.4 <u>Apply Host-based Firewalls or Port Filtering</u> Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			

2.3 Site Isolation

Site isolation settings are configuration options in the Google admin console for isolating all sites, or only specific origins, on Chrome browsers within an organization.

Administrators can control whether different websites load in separate processes within the browser, effectively isolating them from each other to enhance security by preventing malicious sites from accessing sensitive data from other websites, essentially acting as a critical security feature to protect against cross-site attacks like Spectre and Meltdown.

2.3.1 (L1) Ensure 'Site isolation' is set to 'Require Site Isolation for all websites, as well as any origins below' (Automated)

Profile Applicability:

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

Description:

This setting controls if every website will load into its own process.

Disabled (0): Doesn't turn off site isolation, but it lets users opt out.

The recommended state for this setting is: **Enabled** (1)

Rationale:

Chrome will load each website in its own process. Even if a site bypasses the same-origin policy, the extra security will help stop the site from stealing your data from another website.

Impact:

If the policy is enabled, each site will run in its own process which will cause the system to use more memory. You might want to look at the **Enable Site Isolation for specified origins** policy setting to get the best of both worlds – isolation and limited impact for users – by using **Enable Site Isolation for specified origins** with a list of the sites you want to isolate.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Site isolation**
6. Ensure **Configuration** is set to **Require Site Isolation for all websites, as well as any origins below**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Site isolation**
6. Set **Configuration** to **Require Site Isolation for all websites, as well as any origins below**
7. Select **Save**

Default Value:

Unset (Same as Disabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#SitePerProcess>
2. <https://www.chromium.org/Home/chromium-security/site-isolation>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.3 <u>Ensure Adequate Audit Log Storage</u> Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.			
v7	10.5 <u>Ensure Backups Have At least One Non-Continuously Addressable Destination</u> Ensure that all backups have at least one backup destination that is not continuously addressable through operating system calls.			

2.4 Security

Security settings are configuration options in the Google admin console for managing various security aspects of Chrome browsers within an organization.

Administrators can control features like blocking specific websites, managing extensions, enforcing password policies, controlling site permissions, and setting Safe Browsing protection levels, all aimed at enhancing user security and preventing potential threats.

2.4.1 (L1) Ensure 'Password manager' is Explicitly Configured (Manual)

Profile Applicability:

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

Description:

Google Chrome has a built-in password manager to store passwords for users. Chrome will use local authentication to allow users to gain access to these passwords.

The recommended state for this setting is: Explicitly set to **Enabled** (1) or **Disabled** (0) based on the organization's needs.

NOTE: If you choose to Enable this setting, please review **Disable synchronization of data with Google** and ensure this setting is configured to meet organizational requirements.

Rationale:

The Google Chrome password manager is **Enabled** by default and each organization should review and determine if they want to allow users to store passwords in the Browser. If another solution is used instead of the built-in Chrome option then an organization should configure the setting to **Disabled**.

Impact:

Organizationally dependent.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **<https://admin.google.com>** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Password manager**
6. Ensure **Configuration** is set to **Always allow use of password manager** or **Never allow use of password manager**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Password manager**
6. Set **Configuration** to **Always allow use of password manager** or **Never allow use of password manager**
7. Select **Save**

Default Value:

Unset (Same as Enabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#PasswordManagerEnabled>
2. <https://www.ncsc.gov.uk/blog-post/what-does-ncsc-think-password-managers>
3. <https://pages.nist.gov/800-63-3/sp800-63b.html>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.2 <u>Use DNS Filtering Services</u> Use DNS filtering services on all enterprise assets to block access to known malicious domains.			
v7	4.8 <u>Log and Alert on Changes to Administrative Group Membership</u> Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.			

2.4.2 (L1) Ensure 'Web Authentication requests on sites with broken TLS certificates' Is Set to 'Do not allow WebAuthn API requests on sites with broken TLS certificates' (Automated)

Profile Applicability:

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

Description:

This policy setting controls the WebAuthn API and its interaction with sites that have a broken TLS certificate. It can be configured to either:

- Disabled (0): Do not allow WebAuthn API requests on sites with broken TLS certificates.
- Enabled (1): Allow WebAuthn API requests on sites with broken TLS certificates.

If the value for `AllowWebAuthnWithBrokenTlsCerts` is not changed from the default, it will behave as it is disabled.xempt.

Rationale:

Setting this policy will block the ability to authenticate to any website that does not have a valid TLS certificate since the identity of the site cannot be verified.

Impact:

There should be no user impact.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Devices`
3. Select `Chrome`
4. Select `Settings`
5. Under `User & browser settings`, select `Web Authentication requests on sites with broken TLS certificates`
6. Ensure `Configuration` is set to `Do not allow WebAuthn API requests on sites with broken TLS certificates`

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Web Authentication requests on sites with broken TLS certificates**
6. Set **Configuration** to **Do not allow WebAuthn API requests on sites with broken TLS certificates**
7. Select **Save**

Default Value:

Unset (Disabled)

References:

1. <https://chromeenterprise.google/policies/#AllowWebAuthnWithBrokenTlsCerts>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v8	14.4 <u>Train Workforce on Data Handling Best Practices</u> Train workforce members on how to identify and properly store, transfer, archive, and destroy sensitive data. This also includes training workforce members on clear screen and desk best practices, such as locking their screen when they step away from their enterprise asset, erasing physical and virtual whiteboards at the end of meetings, and storing data and assets securely.			

2.4.3 (L1) Ensure 'Post-quantum TLS' Is Set to 'Allow post-quantum key agreement in TLS connections' (Automated)

Profile Applicability:

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

Description:

This configures whether Google Chrome will offer a post-quantum key agreement algorithm in TLS, using the ML-KEM NIST standard, and will protect user traffic from quantum computers when communicating with compatible servers. Enabling a post-quantum key agreement is backwards compatible, so there will be no issue with existing TLS servers.

Rationale:

This will protect user traffic from quantum computer decrypting.

Impact:

There should be no impact on the user

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **Security**, select **Post-quantum TLS**
6. Ensure **Configuration** is set to **Allow post-quantum key agreement in TLS connections**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **Security**, select **Post-quantum TLS**
6. Set **Configuration** to **Allow post-quantum key agreement in TLS connections**
7. Select **Save**

References:

1. <https://chromeenterprise.google/policies/#PostQuantumKeyAgreementEnabled>

CIS Controls:

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

2.4.4 (L1) Ensure 'Incognito mode' is set to 'Disallow incognito mode' (Automated)

Profile Applicability:

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

Description:

Specifies whether the user may open pages in Incognito mode in Google Chrome. The possible values are:

- Incognito mode available (0 - Same as Disabled))
- Incognito mode disabled (1)
- Incognito mode forced (2)

The recommended state for this setting is: Enabled: Incognito mode disabled (1)

Rationale:

Incognito mode in Chrome gives you the choice to browse the internet without your activity being saved to your browser or device.

Allowing users to use the browser without any information being saved can hide evidence of malicious behaviors. This information 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 Incognito mode for Google Chrome.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select Devices
3. Select Chrome
4. Select Settings
5. Under User & browser settings, select Incognito mode
6. Ensure Configuration is set to Disallow incognito mode

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Incognito mode**
6. Set **Configuration** to **Disallow incognito mode**
7. Select **Save**

Default Value:

Unset (Same as Enabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#IncognitoModeAvailability>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.4.5 (L1) Ensure 'Browser history' is set to 'Always save browser history' (Automated)

Profile Applicability:

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

Description:

Google Chrome is configured to save the browser history.

The recommended state for this setting is: **Always save browser history**

NOTE: This setting will preserve browsing history that could contain a user's personal browsing history. Please make sure that this setting is in compliance with organizational policies.

Rationale:

Browser history shall be saved as it may contain indicators of compromise.

Impact:

None - This is the default behavior.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Browser history**
6. Ensure **Configuration** is set to **Always save browser history**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Browser history**
6. Set **Configuration** to **Always save browser history**
7. Select **Save**

Default Value:

Unset (Same as Disabled, but user can change).

References:

1. <https://chromeenterprise.google/policies/#SavingBrowserHistoryDisabled>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	3.5 <u>Deploy Automated Software Patch Management Tools</u> 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.			

2.4.6 (L1) Ensure 'Clear browser history' Is Set to 'Do not allow clearing history in settings menu' (Automated)

Profile Applicability:

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

Description:

Google Chrome can delete the browser and download history using the clear browsing data menu.

The recommended state for this setting is: **Disabled** (0)

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

Rationale:

If users can delete websites they have visited or files they have downloaded it will be easier for them to hide evidence that they have visited unauthorized or malicious sites.

Impact:

If this setting is disabled, browsing and download history cannot be deleted by using the clear browsing data menu.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Clear browser history**
6. Ensure **Configuration** is set to **Do not allow clearing history in settings menu**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Clear browser history**
6. Set **Configuration** to **Do not allow clearing history in settings menu**
7. Select **Save**

Default Value:

Unset (Same as Enabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#AllowDeletingBrowserHistory>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.2 <u>Use DNS Filtering Services</u> Use DNS filtering services on all enterprise assets to block access to known malicious domains.			
v7	4.8 <u>Log and Alert on Changes to Administrative Group Membership</u> Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.			

2.4.7 (L1) Ensure 'Force ephemeral mode' is set to 'Do not erase local user data' (Automated)

Profile Applicability:

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

Description:

This 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: **Do not erase local user data**

Rationale:

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

Impact:

None - This is the default behavior.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **<https://admin.google.com>** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Force ephemeral mode**
6. Ensure **Erase local data when the browser is closed** is set to **Do not erase local user data**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Force ephemeral mode**
6. Set **Erase local data when the browser is closed** to **Do not erase local user data**
7. Select **Save**

Default Value:

Unset (Same as Disabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#ForceEphemeralProfiles>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.2 <u>Use DNS Filtering Services</u> Use DNS filtering services on all enterprise assets to block access to known malicious domains.			
v7	4.8 <u>Log and Alert on Changes to Administrative Group Membership</u> Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.			

2.4.8 (L1) Ensure 'Online revocation checks' is set to 'Perform online OCSP/CRL checks' (Automated)

Profile Applicability:

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

Description:

Google Chrome performs revocation checking for server certificates that successfully validate and are signed by locally-installed CA certificates. If Google Chrome is unable to obtain revocation status information, such certificates will be treated as revoked ('hard-fail').

Disabled: Google Chrome uses existing online revocation-checking settings.

The recommended state for this setting is: **Enabled** (1)

Rationale:

Certificates shall always be validated.

Impact:

A revocation check will be performed for server certificates that successfully validate and are signed by locally-installed CA certificates. if the OCSP server goes down, then this will hard-fail and prevent browsing to those sites.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Online revocation checks**
6. Ensure **Configuration** is set to **Perform online OCSP/CRL checks**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Online revocation checks**
6. Set **Configuration** to **Perform online OCSP/CRL checks**
7. Select **Save**

Default Value:

Unset (Same as Disabled, and users can change)

References:

1. <https://chromeenterprise.google/policies/#RequireOnlineRevocationChecksForLocalAnchors>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.4.9 (L1) Ensure 'Geolocation' is set to 'Do not allow sites to detect users' geolocation' (Automated)

Profile Applicability:

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

Description:

Google Chrome supports tracking a user's physical location using GPS, data about nearby Wi-Fi access points or cellular signal sites/towers (even if you're not using them), and your computer's IP.

- **Disabled** (0, same as 3)
- **Allow sites to track the users' physical location** (1)
- **Do not allow any site to track the users' physical location** (2)
- **Ask whenever a site wants to track the users' physical location** (3)

The recommended state for this setting is: **Enabled** with a value **Do not allow any site to track the users' physical location** (2)

Rationale:

From a privacy point of view it is not desirable to submit indicators regarding the location of the device, since the processing of this information cannot be determined. Furthermore, this may leak information about the network infrastructure around the device.

Impact:

If this setting is disabled, chrome will no longer send data about nearby Wi-Fi access points or cellular signal sites/towers (even if you're not using them), and your computer's IP address to Google.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **<https://admin.google.com>** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Geolocation**
6. Ensure **Configuration** is set to **Do not allow sites to detect users' geolocation**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Geolocation**
6. Set **Configuration** to **Do not allow sites to detect users' geolocation**
7. Select **Save**

Default Value:

Unset (Same as Disabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#DefaultGeolocationSetting>
2. <https://www.w3.org/2010/api-privacy-ws/papers/privacy-ws-24.pdf>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	4.8 <u>Log and Alert on Changes to Administrative Group Membership</u> Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.			

2.4.10 (L1) Ensure 'Allowed certificate transparency URLs' is Not Set (Automated)

Profile Applicability:

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

Description:

Google Chrome can specify URLs/hostnames for which Certificate Transparency will not be enforced. If this setting is disabled, no URLs are excluded from Certificate Transparency requirements.

The recommended state for this setting is: **Disabled** (0)

Rationale:

Certificates that are required to be disclosed via Certificate Transparency shall be treated for all URLs as untrusted if they are not disclosed according to the Certificate Transparency policy.

Impact:

None - This is the default behavior.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Allowed certificate transparency URLs**
6. Ensure **Allowed certificate transparency URLs** is empty

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Allowed certificate transparency URLs**
6. Remove all URLs from **Allowed certificate transparency URLs**
7. Select **Save**

Default Value:

Unset (Same as Disabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#CertificateTransparencyEnforcementDisabledForUrls>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.4.11 (L1) Ensure 'Certificate transparency CA allowlist' is Not Set (Automated)

Profile Applicability:

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

Description:

Google Chrome can exclude certificates by their subjectPublicKeyInfo hashes from enforcing Certificate Transparency requirements. If this setting is disabled, no certificates are excluded from Certificate Transparency requirements.

The recommended state for this setting is: **Disabled** (0)

Rationale:

Certificate Transparency requirements shall be enforced for all certificates.

Impact:

None - This is the default behavior.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Certificate transparency CA allowlist**
6. Ensure **Certificate transparency CA allowlist** is empty

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Certificate transparency CA allowlist**
6. Remove all CAs from **Certificate transparency CA allowlist**
7. Select **Save**

Default Value:

Unset (Same as Disabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#CertificateTransparencyEnforcementDisabledForCas>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.4.12 (L1) Ensure 'Renderer App Container' Is Set to 'Enable the Renderer App Container sandbox' (Automated)

Profile Applicability:

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

Description:

This setting controls the ability for Google Chrome to allow the Render App Container sandbox to be used while navigating to certain sites. It can be configured to either:

- Disabled (0): **Disable the Renderer App Container sandbox**
- Enabled (1): **Enable the Renderer App Container sandbox**

If the value for **RendererAppContainerEnabled** is not changed from the default, it will behave as if it is enabled.

Rationale:

Disabling this policy would weaken the sandbox that Google Chrome uses for the renderer process, and will have a detrimental effect on the security and stability of the browser. This policy needs to be enabled to maintain security and stability.

Impact:

This would only impact users if there is third-party software that must run inside renderer processes.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **<https://admin.google.com>** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Renderer App Container**
6. Ensure **Configuration** is set to **Enable the Renderer App Container sandbox**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Renderer App Container**
6. Set **Configuration** to **Enable the Renderer App Container sandbox**
7. Select **Save**

Default Value:

Unset (Enabled)

References:

1. <https://chromeenterprise.google/policies/#RendererAppContainerEnabled>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.2 <u>Use DNS Filtering Services</u> Use DNS filtering services on all enterprise assets to block access to known malicious domains.			
v7	4.8 <u>Log and Alert on Changes to Administrative Group Membership</u> Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.			

2.4.13 (L1) Ensure 'Enable leak detection for entered credentials' Is Set to 'Enable Leak detection for entered credentials' (Manual)

Profile Applicability:

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

Description:

This policy controls the ability for Google Chrome to verify if any entered credentials were part of a leak. If a user's credentials are compromised, the user will be alerted. The password is not stored on Google's servers, unless Password Sync is enabled, and is encrypted with a secret key known only to your device. To find out more on how Google protects your password, see their support article [How Chrome protects your passwords](#).

Note: This setting has no effect if **Safe Browsing** is not enabled.

Rationale:

Users should be aware if any of their credentials have been compromised or leaked.

Impact:

There should be no impact on the user.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **Security**, select **Enable leak detection for entered credentials**
6. Ensure **Configuration** is set to **Users enrolled in the Advanced Protection program will receive extra protections**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **Security**, select **Enable leak detection for entered credentials**
6. Set **Configuration** to **Users enrolled in the Advanced Protection program will receive extra protections**
7. Select **Save**

Default Value:

Unset (Allow the user to decide)

References:

1. <https://chromeenterprise.google/policies/#PasswordLeakDetectionEnabled>
2. <https://support.google.com/chrome/a/answer/13597868?hl=en>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.2 <u>Use DNS Filtering Services</u> Use DNS filtering services on all enterprise assets to block access to known malicious domains.			
v7	4.8 <u>Log and Alert on Changes to Administrative Group Membership</u> Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.			

2.4.14 (L1) Ensure 'Audio sandbox' is set to 'Always sandbox the audio process' (Automated)

Profile Applicability:

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

Description:

This setting controls whether audio processes in Google Chrome run in a sandbox.

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

The recommended state for this setting is: **Enabled** (1)

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:

None - This is the default behavior.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Audio sandbox**
6. Ensure **Configuration** is set to **Always sandbox the audio process**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Audio sandbox**
6. Set **Configuration** to **Always sandbox the audio process**
7. Select **Save**

Default Value:

Unset (Same as Enabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#AudioSandboxEnabled>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.3 <u>Ensure Adequate Audit Log Storage</u> Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.			
v7	10.5 <u>Ensure Backups Have At least One Non-Continuously Addressable Destination</u> Ensure that all backups have at least one backup destination that is not continuously addressable through operating system calls.			

2.4.15 (L1) Ensure 'Unsupported system warning' is set to 'Allow Chrome to display warnings when running on an unsupported system' (Automated)

Profile Applicability:

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

Description:

Google Chrome will show a warning that appears when Google Chrome is running on a computer or operating system that is no longer supported.

The recommended state for this setting is: **Disabled** (0)

Rationale:

The user shall be informed if the used software is no longer supported.

Impact:

None - This is the default behavior.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Unsupported system warning**
6. Ensure **Configuration** is set to **Allow Chrome to display warnings when running on an unsupported system**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Unsupported system warning**
6. Set **Configuration** to **Allow Chrome to display warnings when running on an unsupported system**
7. Select **Save**

Default Value:

Unset (Same as Disabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#SuppressUnsupportedOSWarning>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.2 <u>Ensure Authorized Software is Currently Supported</u> 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 <u>Ensure Software is Supported by Vendor</u> 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.			

2.4.16 (L2) Ensure 'Advanced Protection program' Is Set to 'Users enrolled in the Advanced Protection program will receive extra protections' (Manual)

Profile Applicability:

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

Description:

The Advanced Protection Program is a service offered by Google for users whose accounts contain particularly valuable files or sensitive information. This service requires at least one passkey or FIDO compliant security key. Since this is an additional service, and requires the purchase of additional hardware, this is not a scored recommendation but is recommended for anyone who is already signed up for the Advanced Protection Program service.

Note: At the time this benchmark was published the Advanced Protection Program was available at no charge but to use the program your organization may need to purchase security keys.

Rationale:

If a user (or organization) has already enabled the Advanced Protection Program, those user(s) should use the features offered.

Impact:

There should be no impact on the user.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **Security**, select **Advanced Protection program**
6. Ensure **Configuration** is set to **Users enrolled in the Advanced Protection program will receive extra protections**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **Security**, select **Advanced Protection program**
6. Set **Configuration** to **Users enrolled in the Advanced Protection program will receive extra protections**
7. Select **Save**

Default Value:

'Users enrolled in the Advanced Protection program will receive extra protections'

References:

1. <https://chromeenterprise.google/policies/#AdvancedProtectionAllowed>
2. https://landing.google.com/intl/en_in/advancedprotection/
3. <https://support.google.com/accounts/answer/7539956?hl=en#zippy=%2Chow-much-does-advanced-protection-cost>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.4.17 (L1) Ensure 'Override insecure origin restrictions' is Not Set (Automated)

Profile Applicability:

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

Description:

Google Chrome can use a list of origins (URLs) or hostname patterns (such as "*.example.com") for which security restrictions on insecure origins will not apply and are prevented from being labeled as "Not Secure" in the omnibox.

The recommended state for this setting is: **Disabled** (0)

Rationale:

Insecure contexts shall always be labeled as insecure.

Impact:

None - This is the default behavior.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Override insecure origin restrictions**
6. Ensure **Origin or hostname patterns to ignore insecure origins security restrictions** is empty

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Override insecure origin restrictions**
6. Remove all hostnames from **Origin or hostname patterns to ignore insecure origins security restrictions**
7. Select **Save**

Default Value:

Unset (Same as Disabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#OverrideSecurityRestrictionsOnInsecureOrigin>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.4.18 (L1) Ensure 'Command-line flags' is set to 'Show security warnings when potentially dangerous command-line flags are used' (Automated)

Profile Applicability:

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

Description:

This setting prevents Google Chrome from showing security warnings that potentially dangerous command-line flags are in use at its launch.

The recommended state of this setting is: **Enabled** (0)

Rationale:

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

Impact:

None - This is the default behavior.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Command-line flags**
6. Ensure **Configuration** is set to **Show security warnings when potentially dangerous command-line flags are used**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Command-line flags**
6. Set **Configuration** to **Show security warnings when potentially dangerous command-line flags are used**
7. Select **Save**

Default Value:

Unset (Same as Enabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#CommandLineFlagSecurityWarningsEnabled>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.3 <u>Ensure Adequate Audit Log Storage</u> Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.			
v7	7.2 <u>Disable Unnecessary or Unauthorized Browser or Email Client Plugins</u> Uninstall or disable any unauthorized browser or email client plugins or add-on applications.			

2.4.19 (L1) Ensure 'Allow remote debugging' is set to 'Do not allow use of the remote debugging' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (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 Google Chrome.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Allow remote debugging**
6. Ensure **Configuration** is set to **Do not allow use of the remote debugging**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Allow remote debugging**
6. Set **Configuration** to **Do not allow use of the remote debugging**
7. Select **Save**

Default Value:

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

Additional Information:

I copied/adjusted this rule from [MS Edge, rule 1.41](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.2 Establish and Maintain a Remediation Process Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.			
v8	13.5 Manage Access Control for Remote Assets Manage access control for assets remotely connecting to enterprise resources. Determine amount of access to enterprise resources based on: up-to-date anti-malware software installed, configuration compliance with the enterprise's secure configuration process, and ensuring the operating system and applications are up-to-date.			

2.4.20 (L1) Ensure 'TLS encrypted ClientHello' Is 'Enable the TLS Encrypted ClientHello experiment' (Automated)

Profile Applicability:

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

Description:

This setting controls the defaults for using Encrypted ClientHello (ECH). ECH is an extension to TLS and encrypts the initial handshake with a website that can only be decrypted by that website. Google Chrome may, or may not, use ECH based on 3 factors: sever support, HTTPS DNS record availability, or rollout status. It can be configured to either:

- Disabled (0): **Disable the TLS Encrypted ClientHello experiment**
- Enabled (1): **Enable the TLS Encrypted ClientHello experiment**

If the value for **EncryptedClientHelloEnabled** is not changed from the default, it will behave as it is enabled.

Rationale:

Previously all handshakes were in the open and could expose sensitive information like the name of the website that you are connecting to. Setting this policy will allow Google Chrome to use an encrypted hello, or handshake, with a website where it is supported, thus not exposing sensitive information.

Impact:

There should be no impact on the user.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **<https://admin.google.com>** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **TLS encrypted ClientHello**
6. Ensure **Configuration** is set to **Enable the TLS Encrypted ClientHello experiment**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **TLS encrypted ClientHello**
6. Set **Configuration** to **Enable the TLS Encrypted ClientHello experiment**
7. Select **Save**

Default Value:

Unset (Enabled)

References:

1. <https://chromeenterprise.google/policies/#EncryptedClientHelloEnabled>

CIS Controls:

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

2.4.21 (L1) Ensure 'Strict MIME type checking for worker scripts' Is Set to 'Require a JavaScript MIME type for worker scripts' (Automated)

Profile Applicability:

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

Description:

This setting controls the ability for Google Chrome to upgrade to HTTPS from HTTP while navigating to certain sites. It can be configured to either:

- Disabled (0): Scripts for workers (Web Workers, Service Workers, etc.) use lax MIME type checking. Worker scripts with legacy MIME types, like text/ascii, will work.
- Enabled (1): Scripts for workers (Web Workers, Service Workers, etc.) require a JavaScript MIME type, like text/javascript. Worker scripts with legacy MIME types, like text/ascii, will be rejected.

If the value for `StrictMimetypeCheckForWorkerScriptsEnabled` is not changed from the default, it will behave as if it is enabled.

Rationale:

Setting this policy will require worker scripts to use more secure and strict JavaScript MIME types and ones with legacy MIME Types will be rejected.

Impact:

This should have no impact on users.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Strict MIME type checking for worker scripts**
6. Ensure **Configuration** is set to **Require a JavaScript MIME type for worker scripts**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Strict MIME type checking for worker scripts**
6. Set **Configuration** to **Require a JavaScript MIME type for worker scripts**
7. Select **Save**

Default Value:

Unset (Enabled)

References:

1. <https://chromeenterprise.google/policies/#StrictMimetypeCheckForWorkerScriptsEnabled>

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.			

2.4.22 (L2) Ensure 'Enforce local anchor constraints' Is 'Enforce constraints in locally added trust anchors' (Automated)

Profile Applicability:

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

Description:

This setting controls constraints encoded into trust anchors loaded from the platform trust store. It can be configured to either:

- Disabled (0): Do not enforce constraints in locally added trust anchors
- Enabled (1): Enforce constraints in locally added trust anchors

If the value for `EnforceLocalAnchorConstraintsEnabled` is not changed from the default, it will behave as if it is enabled.

Rationale:

Setting this policy will not allow access to any sites that do not enforce constraints.

Impact:

Enabling this might cause certain internal sites to not properly load until they are updated.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Enforce local anchor constraints**
6. Ensure **Configuration** is set to **Enforce constraints in locally added trust anchors**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Enforce local anchor constraints**
6. Set **Configuration** to **Enforce constraints in locally added trust anchors**
7. Select **Save**

Default Value:

Unset (Enabled)

References:

1. <https://chromeenterprise.google/policies/#EnforceLocalAnchorConstraintsEnabled>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.4.23 (L1) Ensure 'File/directory picker without user gesture' Is Not Set (Automated)

Profile Applicability:

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

Description:

This setting controls the ability for `showOpenFilePicker()`, `showSaveFilePicker()`, and `showDirectoryPicker()` web APIs to be called without user interaction.

If the value for `FileOrDirectoryPickerWithoutGestureAllowedForOrigins` is not changed from the default, it will behave as if it is disabled.

Rationale:

Setting this policy would allow the URLs selected to call the `showOpenFilePicker()`, `showSaveFilePicker()`, and `showDirectoryPicker()` web APIs without any user gesture/interaction. This policy does not need to be set for this reason.

Impact:

Disabling this policy should have no impact on the user.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **File/directory picker without user gesture**
6. Ensure **Allow file or directory picker APIs to be called without prior user gesture** is empty

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **File/directory picker without user gesture**
6. Remove all URLs from **Allow file or directory picker APIs to be called without prior user gesture**
7. Select **Save**

Default Value:

Unset (Disabled)

References:

1. <https://chromeenterprise.google/policies/#FileOrDirectoryPickerWithoutGestureAllowedForOrigins>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.2 Establish and Maintain a Remediation Process Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.			
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			

2.4.24 (L1) Ensure 'Media picker without user gesture' Is Not Configured (Automated)

Profile Applicability:

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

Description:

This setting controls the ability for `getDisplayMedia()` web API to be called without user interaction based on sites that are configured in this policy. By default, no site can call the `getDisplayMedia()` API for screen capture without a prior user gesture.

Rationale:

Setting this policy would allow the URLs selected to call the `getDisplayMedia()` web APIs without any user gesture/interaction. This policy does not need to be set for this reason.

Impact:

Disabling this policy should have no impact on the user.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **Security**, select **Media picker without user gesture**
6. Ensure **Allow screen capture without prior user gesture** is empty

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **Security**, select **Media picker without user gesture**
6. Remove all URLs from **Allow screen capture without prior user gesture**
7. Select **Save**

Default Value:

Unset (disabled)

References:

1. <https://chromeenterprise.google/policies/#ScreenCaptureWithoutGestureAllowedForOrigins>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.5 Remote access (Chrome Remote Desktop)

This section has recommendations specifically for configuring Chrome Remote Desktop.

2.5.1 (L1) Ensure 'Remote access hosts' is set with a domain defined in 'Remote access host domain' (Manual)

Profile Applicability:

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

Description:

Chrome allows the configuration of a list of domains that are allowed to access the user's system. When enabled, remote systems can only connect if they are one of the specified domains listed.

Setting this to an empty list (Disabled) allows remote systems from any domain to connect to this user's system.

The recommended state for this setting is: **Enabled** (1) and at least one domain set

NOTE: The list of domains is organization specific.

Rationale:

Remote assistance connections shall be restricted.

Impact:

If this setting is enabled, only systems from the specified domains can connect to the user's system.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Remote access hosts**
6. Ensure **Remote access host domain** is set to your organization's required domain

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Remote access hosts**
6. Set **Remote access host domain** to your organization's required domain
7. Select **Save**

Default Value:

Unset (Same as Disabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#RemoteAccessHostClientDomainList>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	13.5 <u>Manage Access Control for Remote Assets</u> Manage access control for assets remotely connecting to enterprise resources. Determine amount of access to enterprise resources based on: up-to-date anti-malware software installed, configuration compliance with the enterprise's secure configuration process, and ensuring the operating system and applications are up-to-date.			
v7	12.12 <u>Manage All Devices Remotely Logging into Internal Network</u> Scan all enterprise devices remotely logging into the organization's network prior to accessing the network to ensure that each of the organization's security policies has been enforced in the same manner as local network devices.			

2.5.2 (L1) Ensure 'Firewall traversal' is set to 'Disable firewall traversal' (Automated)

Profile Applicability:

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

Description:

Chrome enables the usage of STUN servers which allows remote clients to discover and connect to a machine even if they are separated by a firewall. By disabling this feature, in conjunction with filtering outgoing UDP connections, the machine will only allow connections from machines within the local network.

The recommended state for this setting is: **Disabled** (0)

Rationale:

If this setting is enabled, remote clients can discover and connect to these machines even if they are separated by a firewall.

Impact:

If this setting is disabled and outgoing UDP connections are filtered by the firewall, this machine will only allow connections from client machines within the local network.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Firewall traversal**
6. Ensure **Configuration** is set to **Disable firewall traversal**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Firewall traversal**
6. Set **Configuration** to **Disable firewall traversal**
7. Select **Save**

Default Value:

Unset (Same as Enabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#RemoteAccessHostFirewallTraversal>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	13.5 Manage Access Control for Remote Assets Manage access control for assets remotely connecting to enterprise resources. Determine amount of access to enterprise resources based on: up-to-date anti-malware software installed, configuration compliance with the enterprise's secure configuration process, and ensuring the operating system and applications are up-to-date.			
v7	12.12 Manage All Devices Remotely Logging into Internal Network Scan all enterprise devices remotely logging into the organization's network prior to accessing the network to ensure that each of the organization's security policies has been enforced in the same manner as local network devices.			

2.5.3 (L1) Ensure 'Firewall traversal' is set to 'Disable the use of relay servers' (Automated)

Profile Applicability:

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

Description:

Google Chrome allows the use of relay servers when clients are trying to connect to this machine and a direct connection is not available.

- **Disable** (0): The use of relay servers by the remote access host is not allowed
- **Enabled** (1): The use of relay servers by the remote access host is allowed

The recommended state for this setting is: **Disabled** (0)

Rationale:

Relay servers shall not be used to circumvent firewall restrictions.

Impact:

If this setting is disabled, remote clients can not use relay servers to connect to this machine.

NOTE: Setting this to Disabled doesn't turn remote access off, but only allows connections from the same network (not NAT traversal or relay).

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Firewall traversal**
6. Ensure **Configuration** is set to **Disable the use of relay servers**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Firewall traversal**
6. Set **Configuration** to **Disable the use of relay servers**
7. Select **Save**

Default Value:

Unset (Same as Enabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#RemoteAccessHostAllowRelayedConnection>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	13.5 Manage Access Control for Remote Assets Manage access control for assets remotely connecting to enterprise resources. Determine amount of access to enterprise resources based on: up-to-date anti-malware software installed, configuration compliance with the enterprise's secure configuration process, and ensuring the operating system and applications are up-to-date.			
v7	12.12 Manage All Devices Remotely Logging into Internal Network Scan all enterprise devices remotely logging into the organization's network prior to accessing the network to ensure that each of the organization's security policies has been enforced in the same manner as local network devices.			

2.5.4 (L1) Ensure 'Remote support connections' is set to 'Prevent remote support connections' (Manual)

Profile Applicability:

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

Description:

This is a setting for Chrome Remote desktop. If this setting is Disabled, the remote access host service cannot be started or configured to accept incoming connections.

- **Disabled** (0): Prevent remote access connections to this machine
- **Enabled** (1): Allow remote access connections to this machine

The recommended state for this setting is: **Disabled** (0)

Rationale:

Only approved remote access systems should be used.

NOTE: If Chrome Remote Desktop is approved and required for use, then this setting can be ignored.

Impact:

This setting will disable Chrome Remote Desktop. In general, Chrome Remote Desktop is not used by most businesses, so disabling it should have no impact.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Remote support connections**
6. Ensure **Configuration** is set to **Prevent remote support connections**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Remote support connections**
6. Set **Configuration** to **Prevent remote support connections**
7. Select **Save**

Default Value:

Unset (Same as Enabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#RemoteAccessHostAllowRemoteAccessConnections>
2. <https://remotedesktop.google.com/?pli=1>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	13.5 <u>Manage Access Control for Remote Assets</u> Manage access control for assets remotely connecting to enterprise resources. Determine amount of access to enterprise resources based on: up-to-date anti-malware software installed, configuration compliance with the enterprise's secure configuration process, and ensuring the operating system and applications are up-to-date.			
v7	12.12 <u>Manage All Devices Remotely Logging into Internal Network</u> Scan all enterprise devices remotely logging into the organization's network prior to accessing the network to ensure that each of the organization's security policies has been enforced in the same manner as local network devices.			

2.6 Network

Network settings are configuration options in the Google admin console for controlling and configuring network access settings of Chrome browsers within an organization.

Administrators can control network policies for the Chrome browser such as proxy settings, DNS clients, VPN configurations, and defining access restrictions.

2.6.1 (L1) Ensure 'Proxy mode' is Not Set to 'Always auto detect the proxy' (Automated)

Profile Applicability:

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

Description:

Google Chrome offers the functionality to configure the proxy settings by automatic discovery using WPAD (Web Proxy Auto-Discovery Protocol). Setting this configures the proxy settings for Chrome and ARC-apps, which ignore all proxy-related options specified from the command line.

Disabled (0): Lets users choose their proxy settings.

The recommended state for this setting is: **Enabled** and the value of **ProxyMode** is not set to **auto_detect**

Rationale:

Attackers may abuse the WPAD auto-config functionality to supply computers with a PAC file that specifies a rogue web proxy under their control.

Impact:

If the policy is enabled, the proxy configuration will no longer be discovered using WPAD.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Proxy mode**
6. Ensure **Configuration** is not set to **Always auto detect the proxy**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Proxy mode**
6. Set **Configuration** to a setting other than **Always auto detect the proxy**
7. Select **Save**

Default Value:

Unset (Same as Disabled, and users can change)

References:

1. <https://chromeenterprise.google/policies/#ProxySettings>
2. http://www.ptsecurity.com/download/wpad_weakness_en.pdf
3. <https://www.blackhat.com/us-16/briefings.html#crippling-https-with-unholy-pac>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	13.10 Perform Application Layer Filtering Perform application layer filtering. Example implementations include a filtering proxy, application layer firewall, or gateway.			●
v7	12.9 Deploy Application Layer Filtering Proxy Server Ensure that all network traffic to or from the Internet passes through an authenticated application layer proxy that is configured to filter unauthorized connections.			●

2.6.2 (L2) Ensure 'Supported authentication schemes' is set to 'NTLM' and 'Negotiate' (Automated)

Profile Applicability:

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

Description:

Specifies which HTTP authentication schemes are supported by Google Chrome.

Disabled (0): Allows all supported authentication schemes.

The recommended state for this setting is: **Enabled** with the value of **ntlm, negotiate**

Rationale:

Possible values are 'basic', 'digest', 'ntlm' and 'negotiate'. Basic and Digest authentication do not provide sufficient security and can lead to submission of user passwords in plaintext or minimal protection (Integrated Authentication is supported for negotiate and ntlm challenges only).

Impact:

If some legacy application(s) or website(s) required insecure authentication mechanisms they will not work correctly.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Supported authentication schemes**
6. Ensure **Configuration** is set to **NTLM** and **Negotiate**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Supported authentication schemes**
6. Set **Configuration** to **NTLM** and **Negotiate**
7. Select **Save**

Default Value:

Unset (Same as Disabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#AuthSchemes>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v7	16.5 <u>Encrypt Transmittal of Username and Authentication Credentials</u> Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.			

2.6.3 (L2) Ensure 'SSL error override' is set to 'Block users from clicking through SSL warnings' (Automated)

Profile Applicability:

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

Description:

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

The recommended state for this setting is: **Disabled** (0)

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 there 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:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **SSL error override**
6. Ensure **Configuration** is set to **Block users from clicking through SSL warnings**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **SSL error override**
6. Set **Configuration** to **Block users from clicking through SSL warnings**
7. Select **Save**

Default Value:

Unset (Same as Enabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#SSLErrorOverrideAllowed>

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	7.4 Maintain and Enforce Network-Based URL Filters Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.			

2.6.4 (L1) Ensure 'WebRTC ICE candidate URLs for local IPs' Is Not Set (Automated)

Profile Applicability:

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

Description:

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

The recommended state for this setting is: **Disabled** (0)

NOTE: This setting, if Enabled, weakens the protection of local IPs if needed by administrators.

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:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **WebRTC ICE candidate URLs for local IPs**
6. Ensure **URLs for which local IPs are exposed in WebRTC ICE candidates** is empty

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **WebRTC ICE candidate URLs for local IPs**
6. Remove all URLs from **URLs for which local IPs are exposed in WebRTC ICE candidates**
7. Select **Save**

Default Value:

Unset (Same as Disabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#WebRtcLocalIpsAllowedUrls>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.2 <u>Use DNS Filtering Services</u> Use DNS filtering services on all enterprise assets to block access to known malicious domains.			
v7	4.8 <u>Log and Alert on Changes to Administrative Group Membership</u> Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.			

2.6.5 (L2) Ensure 'DNS over HTTPS' is set to 'Enable DNS-over-HTTPS without insecure fallback' (Automated)

Profile Applicability:

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

Description:

This controls the mode of the DNS-over-HTTPS resolver. Please note that this setting will only set the default mode for each query. The mode may be overridden for special types of queries, such as requests to resolve a DNS-over-HTTPS server hostname.

- **Disable DNS-over-HTTPS** (off)
- **Enable DNS-over-HTTPS with insecure fallback** (automatic) - Enable DNS-over-HTTPS queries first if a DNS-over-HTTPS server is available and may fallback to sending insecure queries on error.
- **Enable DNS-over-HTTPS without insecure fallback** (secure) - Only send DNS-over-HTTPS queries and will fail to resolve on error.

The recommended state for this setting is: **Enabled** with a value of **Enable DNS-over-HTTPS without insecure fallback** (secure)

Note: When enabling this policy, it is recommended to also configure the **DnsOverHttpsTemplates** policy so that the URI templates are set. You can find out more information on the [DnsOverHttpsTemplates enterprise policy site](#).

Rationale:

DNS over HTTPS (DOH) has a couple primary benefits:

1. Encrypting DNS name resolution traffic helps to hide your online activities, since DoH hides the name resolution requests from the ISP and from anyone listening on intermediary networks.
2. DoH also helps to prevent DNS spoofing and man-in-the-middle (MitM) attacks.

Impact:

Not all DNS providers support DOH, so choice is limited. Also, Enterprises sometimes monitor DNS requests to block access to malicious or inappropriate sites. DNS monitoring can also sometimes be used to detect malware attempting to "phone home." Because DoH encrypts name resolution requests, it can create a security monitoring blind spot.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **DNS over HTTPS**
6. Ensure **Configuration** is set to **Enable DNS-over-HTTPS without insecure fallback**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **DNS over HTTPS**
6. Set **Configuration** to **Enable DNS-over-HTTPS without insecure fallback**
7. Select **Save**

Default Value:

Unset (Same as Enable DNS-over-HTTPS with insecure fallback (automatic). If any policy is set, either through being domain-joined or active policy with cloud management (or profile lists), then it sometimes reverts to Disable DNS-over-HTTPS and users can't change it.

References:

1. <https://chromeenterprise.google/policies/#DnsOverHttpsMode>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v8	14.4 <u>Train Workforce on Data Handling Best Practices</u> Train workforce members on how to identify and properly store, transfer, archive, and destroy sensitive data. This also includes training workforce members on clear screen and desk best practices, such as locking their screen when they step away from their enterprise asset, erasing physical and virtual whiteboards at the end of meetings, and storing data and assets securely.			

2.6.6 (L1) Ensure 'Cross-origin authentication' is set to 'Block cross-origin authentication' (Automated)

Profile Applicability:

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

Description:

This 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: **Block cross-origin authentication**

Rationale:

This setting is typically disabled to help combat phishing attempts.

Impact:

None - This is the default behavior.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Cross-origin authentication**
6. Ensure **Specify whether third-party sub-content on a page is allowed to pop-up an HTTP basic authentication dialog box.** is set to **Block cross-origin authentication**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Cross-origin authentication**
6. Set **Specify whether third-party sub-content on a page is allowed to pop-up an HTTP basic authentication dialog box.** to **Block cross-origin authentication**
7. Select **Save**

Default Value:

Unset (Same as Disabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#AllowCrossOriginAuthPrompt>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.6.7 (L1) Ensure 'Enable globally scoped HTTP authentication cache' is set to 'Disabled' (Automated)

Profile Applicability:

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

Description:

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

The recommended state for this setting is: **Disabled** (0)

NOTE: This setting is intended to give enterprises depending on the legacy behavior 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:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Globally scoped HTTP authentication cache**
6. Ensure **Configuration** is set to **Block cross-origin authentication**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Globally scoped HTTP authentication cache**
6. Set **Configuration** to **HTTP authentication credentials are scoped to top-level sites**
7. Select **Save**

Default Value:

Unset (Same as Disabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#GloballyScopeHTTPAuthCacheEnabled>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.6.8 (L1) Ensure 'HSTS policy bypass list' is Not Set (Automated)

Profile Applicability:

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

Description:

This 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** (0)

Rationale:

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

Impact:

None - This is the default behavior.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **HSTS policy bypass list**
6. Ensure **List of hostnames that will bypass the HSTS policy check** is empty

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **HSTS policy bypass list**
6. Remove all hostnames from **List of hostnames that will bypass the HSTS policy check**
7. Select **Save**

Default Value:

Unset (Same as Disabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#HSTSPolicyBypassList>

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	7.4 Maintain and Enforce Network-Based URL Filters Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.			

2.6.9 (L1) Ensure 'DNS interception checks enabled' is set to 'Perform DNS interception checks ' (Automated)

Profile Applicability:

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

Description:

This 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** (1)

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 startup and each DNS configuration change.

Rationale:

Disabling these checks could potentially allow DNS hijacking and poisoning.

Impact:

None - This is the default behavior.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **DNS interception checks enabled**
6. Ensure **Configuration** is set to **Perform DNS interception checks**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **DNS interception checks enabled**
6. Set **Configuration** to **Perform DNS interception checks**
7. Select **Save**

Default Value:

Unset (Same as Enabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#DNSInterceptionChecksEnabled>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.7 Remediate Detected Vulnerabilities Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.		●	●
v7	4.9 Log and Alert on Unsuccessful Administrative Account Login Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.		●	●

2.6.10 (L1) Ensure 'Network service sandbox' Is Set to 'Enable the network sandbox' (Automated)

Profile Applicability:

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

Description:

This policy dictates whether network service processes can run sandboxed. The default configuration is this policy is enabled.

Rationale:

Running network service processes unsandboxed leaves users open to additional security risks.

Impact:

There should be no impact on the user.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **Network**, select **Network service sandbox**
6. Ensure **Configuration** is set to **Enable the network sandbox**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **Network**, select **Network service sandbox**
6. Set **Configuration** to **Enable the network sandbox**
7. Select **Save**

Default Value:

Unset (same as enabled)

References:

1. <https://chromeenterprise.google/policies/#NetworkServiceSandboxEnabled>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.			

2.6.11 (L1) Ensure 'Http Allowlist' Is Properly Configured (Manual)

Profile Applicability:

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

Description:

This setting allows administrators to list specific sites that will not be upgraded to HTTPS and will not show an error interstitial if **HTTPS-First Mode** is enabled.

Note: Wildcards (*, [*], etc.) are not allowed in the URL listings.

Rationale:

Setting this policy allows organizations to maintain access to servers that do not support HTTPS without having to disable HTTPS-First mode or HTTPS Upgrades.

Impact:

This should not have an impact on the user.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **HTTP Allowlist**
6. Ensure **Allowed HTTP URLs** is set to your organization's requirements

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **HTTP Allowlist**
6. Set **Allowed HTTP URLs** to your organization's requirements
7. Select **Save**

References:

1. <https://chromeenterprise.google/policies/#HttpAllowlist>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.7 Allowlist Authorized Scripts Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.			●
v7	2.5 Integrate Software and Hardware Asset Inventories The software inventory system should be tied into the hardware asset inventory so all devices and associated software are tracked from a single location.			●

2.6.12 (L1) Ensure 'Automatic HTTPS upgrades' Is Set to 'Allow HTTPS upgrades' (Automated)

Profile Applicability:

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

Description:

This setting controls the ability for Google Chrome to upgrade to HTTPS from HTTP while navigating to certain sites. It can be configured to either:

- Disabled (0): **Disable HTTPS Upgrades**
- Enabled (1): **HTTPS Upgrades may be applied depending on feature launch status**

If the value for **HttpsUpgradesEnabled** is not changed from the default, it will behave as if it is enabled.

Rationale:

Enabling this setting will upgrade the connection to a site from HTTP to HTTPS where available, verifying the identity of the site visited.

Impact:

This should have no impact on the user.

Note: If there are internal sites/servers that use HTTP only, set those in the policy **HttpAllowlist**

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Automatic HTTPS upgrades**
6. Ensure **Configuration** is set to **Allow HTTPS upgrades**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Automatic HTTPS upgrades**
6. Set **Configuration** to **Allow HTTPS upgrades**
7. Select **Save**

Default Value:

Unset (Enabled)

References:

1. <https://chromeenterprise.google/policies/#HttpsUpgradesEnabled>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.5 <u>Securely Dispose of Data</u> Securely dispose of data as outlined in the enterprise's data management process. Ensure the disposal process and method are commensurate with the data sensitivity.			
v7	7.4 <u>Maintain and Enforce Network-Based URL Filters</u> Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.			

2.7 Import Settings

Import settings are configuration options in the Google admin console for managing users importing existing data into the Chrome browser profiles within an organization.

Administrators can control whether users are allowed to import autofill data, bookmarks, browsing history, saved passwords, or search engines from previous browser usage.

2.7.1 (L1) Ensure 'Import autofill data' is set to 'Disable imports of autofill data' (Automated)

Profile Applicability:

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

Description:

This setting controls whether users are allowed to import autofill data from other browsers into Google Chrome.

If you set this setting to **Disable imports of autofill data**, users will be unable to perform an import of autofill data during Google Chrome run. This will also prevent users from importing data after Google Chrome has been set up.

The recommended state for this setting is **Disable imports of autofill data**.

Rationale:

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

Impact:

None - This is the default behavior.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **<https://admin.google.com>** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Import autofill data**
6. Ensure **Configuration** is set to **Disable imports of autofill data**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Import autofill data**
6. Set **Configuration** to **Disable imports of autofill data**
7. Select **Save**

Default Value:

Unset (Same as Disabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#ImportAutofillFormData>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.2 <u>Use DNS Filtering Services</u> Use DNS filtering services on all enterprise assets to block access to known malicious domains.			
v7	4.8 <u>Log and Alert on Changes to Administrative Group Membership</u> Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.			

2.7.2 (L1) Ensure 'Import homepage' is set to 'Disable imports of homepage' (Automated)

Profile Applicability:

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

Description:

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

If you set this setting to **Disabled** users will be unable to perform an import homepage settings from other browsers into Google Chrome.

The recommended state for this setting is: **Disabled** (0)

Rationale:

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

Impact:

None - This is the default behavior.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Import homepage**
6. Ensure **Configuration** is set to **Disable imports of homepage**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Import homepage**
6. Set **Configuration** to **Disable imports of homepage**
7. Select **Save**

Default Value:

Unset (Same as Disabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#ImportHomepage>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.2 <u>Use DNS Filtering Services</u> Use DNS filtering services on all enterprise assets to block access to known malicious domains.			
v7	4.8 <u>Log and Alert on Changes to Administrative Group Membership</u> Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.			

2.7.3 (L1) Ensure 'Import saved passwords' is set to 'Disable imports of saved passwords' (Automated)

Profile Applicability:

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

Description:

This setting controls if saved passwords from the default browser can be imported (on first run and later manually).

The recommended state for this setting is: **Disabled** (0)

Rationale:

In Chrome, passwords can be stored in plain-text and revealed by clicking the “show” button next to the password field by going to `chrome://settings/passwords/`.

Impact:

If this setting is disabled, saved passwords from other browsers are not imported.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Import saved passwords**
6. Ensure **Configuration** is set to **Disable imports of saved passwords**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Import saved passwords**
6. Set **Configuration** to **Disable imports of saved passwords**
7. Select **Save**

Default Value:

Unset (Same as Enabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#ImportSavedPasswords>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.2 <u>Use DNS Filtering Services</u> Use DNS filtering services on all enterprise assets to block access to known malicious domains.			
v7	4.8 <u>Log and Alert on Changes to Administrative Group Membership</u> Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.			

2.7.4 (L1) Ensure 'Import search engines' is set to 'Disable imports of search engines' (Automated)

Profile Applicability:

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

Description:

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

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

The recommended state for this setting is: **Disabled** (0)

Rationale:

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

Impact:

None - This is the default behavior.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **<https://admin.google.com>** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Import search engines**
6. Ensure **Configuration** is set to **Disable imports of search engines**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Import search engines**
6. Set **Configuration** to **Disable imports of search engines**
7. Select **Save**

Default Value:

Unset (Same as Disabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#ImportSearchEngine>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.2 <u>Use DNS Filtering Services</u> Use DNS filtering services on all enterprise assets to block access to known malicious domains.			
v7	4.8 <u>Log and Alert on Changes to Administrative Group Membership</u> Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.			

2.8 Content

Content settings are configuration options in the Google admin console for managing what types of content websites can access on a user's Chrome browser within an organization.

Administrators can control how users interact with content Chrome browser on managed devices, including cookies, JavaScript, pop-ups, or images, and can set restrictions on a site-by-site basis to manage privacy and security within an organization.

2.8.1 (L2) Ensure 'Screen video capture' is set to 'Do not allow sites to prompt the user to share a video stream of their screen' (Automated)

Profile Applicability:

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

Description:

If enabled or not configured (default), a Web page can use screen-share APIs (e.g., `getDisplayMedia()` or the Desktop Capture extension API) to prompt the user to select a tab, window, or desktop to capture.

Rationale:

The end-user having the ability to allow or deny screen capture for websites in Google Chrome could open an organization up to a malicious site that may capture proprietary information through the browser. By limiting or disallowing screen capture, it removes the end-user's discretion, leaving it up to the organization which sites are allowed to use this ability.

Impact:

When this policy is disabled, any calls to screen-share APIs will fail with an error. This policy is not considered (and a site will be allowed to use screen-share APIs) if the site matches an origin pattern in any of the following policies:

ScreenCaptureAllowedByOrigins, WindowCaptureAllowedByOrigins, TabCaptureAllowedByOrigins, SameOriginTabCaptureAllowedByOrigins.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Screen video capture**
6. Ensure **Configuration** is set to **Do not allow sites to prompt the user to share a video stream of their screen**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Screen video capture**
6. Set **Configuration** to **Do not allow sites to prompt the user to share a video stream of their screen**
7. Select **Save**

Default Value:

Unset (Same as Enabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#ScreenCaptureAllowed>
2. <https://chromeenterprise.google/policies/#SameOriginTabCaptureAllowedByOrigins>
3. <https://chromeenterprise.google/policies/#ScreenCaptureAllowedByOrigins>
4. <https://chromeenterprise.google/policies/#TabCaptureAllowedByOrigins>
5. <https://chromeenterprise.google/policies/#WindowCaptureAllowedByOrigins>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.8.2 (L1) Ensure 'Cast' is set to 'Do not allow users to cast' (Automated)

Profile Applicability:

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

Description:

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

The recommended state for this setting is: **Disabled** (0)

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:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Cast**
6. Ensure **Allow users to Cast from Chrome** is set to **Do not allow users to cast**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Cast**
6. Set **Allow users to Cast from Chrome** to **Do not allow users to cast**
7. Select **Save**

Default Value:

Unset (Same as Disabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#MediaRouterCastAllowAllIPs>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> 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 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

2.8.3 (L1) Ensure 'Clipboard' Is Set to 'Do not allow any site to use the clipboard site permission' (Automated)

Profile Applicability:

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

Description:

This setting controls the defaults for clipboard permission access from sites. It can be configured to either:

- Disabled (2): Does not allow access to the clipboard site permission by any site
- Enabled (3): Sites ask the user to allow access to the clipboard site permission

If the value for `DefaultClipboardSetting` is not changed from the default, it will behave as if it is enabled. `ClipboardAllowedForUrls` or `ClipboardBlockedForUrls` will override this setting for any site that matches the configured URL patterns.

With the setting disabled, organizations will need to set `ClipboardAllowedForUrls` for any URLs they want to make exempt.

Rationale:

The clipboard stores data, text, and images that are shared between all applications. An organization would disable clipboard access to restrict sites from reading the contents of the clipboard when visiting.

Impact:

Not allowing sites to have access to the clipboard permission can cause issues with formatting or access to needed images on the clipboard.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Devices`
3. Select `Chrome`
4. Select `Settings`
5. Under `User & browser settings`, select `Clipboard`
6. Ensure `Configuration` is set to `Do not allow any site to use the clipboard site permission`

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Clipboard**
6. Set **Configuration** to **Do not allow any site to use the clipboard site permission**
7. Select **Save**

Default Value:

Allow clipboard permission access

References:

1. <https://chromeenterprise.google/policies/#DefaultClipboardSetting>

Additional Information:

If your organization requires a set of sites permitted to access the clipboard, configure them via this setting in the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Clipboard**
6. Set URLs required by your organization in **Allow these sites to access the clipboard**
7. Select **Save**

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.2 <u>Use DNS Filtering Services</u> Use DNS filtering services on all enterprise assets to block access to known malicious domains.			
v7	4.8 <u>Log and Alert on Changes to Administrative Group Membership</u> Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.			

2.8.4 (L1) Ensure 'Enable URL-keyed anonymized data collection' is set to 'Data collection is never active' (Automated)

Profile Applicability:

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

Description:

Google Chrome offers the feature URL-keyed anonymized data collection. This sends URLs of pages the user visits to Google to optimize its services.

The recommended state for this setting is: **Disabled** (0)

Rationale:

Anonymized data collection shall be disabled, since it is unclear which information exactly is sent to Google.

Impact:

Anonymized data will not be sent to Google to help optimize its services

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Enable URL-keyed anonymized data collection**
6. Ensure **Configuration** is set to **Data collection is never active**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Enable URL-keyed anonymized data collection**
6. Set **Configuration** to **Data collection is never active**
7. Select **Save**

Default Value:

Unset (Same as Enabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#UrlKeyedAnonymizedDataCollectionEnabled>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	3.5 <u>Deploy Automated Software Patch Management Tools</u> 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.			

2.8.5 (L1) Ensure 'Third-party cookie blocking' is set to 'Disallow third-party cookies' (Automated)

Profile Applicability:

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

Description:

Chrome allows cookies to be set by web page elements that are not from the domain in the user's address bar. Enabling this feature prevents third party cookies from being set.

The recommended state for this setting is: **Enabled** (1)

Rationale:

Blocking third-party cookies can help protect a user's privacy by eliminating a number of website tracking cookies.

Impact:

Enabling this setting prevents cookies from being set by web page elements that are not from the domain that is in the browser's address bar.

NOTE: Third Party Cookies and Tracking Protection are required for many business critical websites, including Microsoft 365 web apps (Office 365), Salesforce, and SAP Analytics Cloud. If these, or similar services, are needed by the organization, then this setting can be Disabled.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Third-party cookie blocking**
6. Ensure **Configuration** is set to **Disallow third-party cookies**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Third-party cookie blocking**
6. Set **Configuration** to **Disallow third-party cookies**
7. Select **Save**

Default Value:

Unset (Same as Disabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#BlockThirdPartyCookies>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.2 <u>Use DNS Filtering Services</u> Use DNS filtering services on all enterprise assets to block access to known malicious domains.			
v7	4.8 <u>Log and Alert on Changes to Administrative Group Membership</u> Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.			

2.8.6 (L1) Ensure 'Cast' is set to 'Do not allow users to Cast' (Automated)

Profile Applicability:

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

Description:

Google Cast can send the contents of tabs, sites, or the desktop from the browser to a remote display and sound system.

The recommended state for this setting is: **Disabled** (0)

Rationale:

Google Cast may send the contents of tabs, sites, or the desktop from the browser to non-trusted devices on the local network segment.

Impact:

If this is disabled, Google Cast is not activated and the toolbar icon is not shown.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Cast**
6. Ensure **Configuration** is set to **Do not allow users to Cast**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Cast**
6. Set **Configuration** to **Do not allow users to Cast**
7. Select **Save**

Default Value:

Unset (Same as Enabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#EnableMediaRouter>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> 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 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

2.8.7 (L2) Ensure 'Cookies' is set to 'Session Only' (Automated)

Profile Applicability:

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

Description:

When leaving the setting `_RestoreOnStartup` unset results in the use of `_DefaultCookiesSetting` for all sites, if it's set. If `_DefaultCookiesSetting` is not set, the user's personal setting applies.

- **Disabled** (0, user's personal setting applies)
- **Allow all sites to set local data** (1)
- **Do not allow any site to set local data** (2)
- **Keep cookies for the duration of the session** (4)

The recommended state for this setting is: **Enabled** with a value of **Keep cookies for the duration of the session** (4)

NOTE: If the *RestoreOnStartup* setting is set to restore URLs from previous sessions this setting will not be respected and cookies will be stored permanently for those sites. An example of those URLs are SSO or intranet sites.

Rationale:

Permanently stored cookies may be used for malicious intent.

Impact:

If this setting is enabled, cookies will be cleared when the session closes.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Cookies**
6. Ensure **Configuration** is set to **Session Only**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Cookies**
6. Set **Configuration** to **Session Only**
7. Select **Save**

Default Value:

Unset (Same as Disabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#DefaultCookiesSetting>
2. <https://chromeenterprise.google/policies/#RestoreOnStartup>
3. <https://chromeenterprise.google/policies/#CookiesSessionOnlyForUrls>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.8.8 (L2) Ensure 'SafeSearch and Restricted Mode' is set to 'Always use Safe Search for Google Web Search queries' (Automated)

Profile Applicability:

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

Description:

This setting ensures that web search results with Google are performed with SafeSearch set to always active. Disabled means SafeSearch in Google Search is not enforced.

The recommended state for this setting is: **Enabled** (1)

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:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **<https://admin.google.com>** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **SafeSearch and Restricted Mode**
6. Ensure **Configuration** is set to **Always use Safe Search for Google Web Search queries**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **SafeSearch and Restricted Mode**
6. Set **Configuration** to **Always use Safe Search for Google Web Search queries**
7. Select **Save**

Default Value:

Unset (Same as Disabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#ForceGoogleSafeSearch>

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	7.4 Maintain and Enforce Network-Based URL Filters Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.			

2.8.9 (L1) Ensure 'First-Party Sets' Is Set to 'Disable First-Party Sets for all affected users' (Manual)

Profile Applicability:

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

Description:

This policy controls access to the First-Party Sets. First-party Sets are a way for sites to declare relationships with each other and enable limited cross-site cookie access for specific, user-facing purposes. It can be configured to either:

- Disabled (0): Disable First-Party Sets for all affected users
- Enabled (1): Enable First-Party Sets for all affected users

Rationale:

Setting this policy will not allow sites to declare the relationships that allow them to access the cross-site cookies.

Impact:

This may cause unexpected behavior as a user moves between affiliated sites.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **First-Party Sets**
6. Ensure **Configuration** is set to **Disable First-Party Sets for all affected users**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **First-Party Sets**
6. Set **Configuration** to **Disable First-Party Sets for all affected users**
7. Select **Save**

Default Value:

Enabled

References:

1. <https://chromeenterprise.google/policies/#FirstPartySetsEnabled>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.3 <u>Ensure Adequate Audit Log Storage</u> Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.8.10 (L1) Ensure 'Allow local file access to file:// URLs on these sites in the PDF Viewer' Is Not Set (Automated)

Profile Applicability:

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

Description:

This setting will allow specified URLs to access `file://` URLs in the PDF Viewer. By default all domains are blocked from accessing `file://` URLs in the PDF Viewer

Rationale:

Blocking all domains, or a restricted list of domains, from opening a downloaded PDF file blocks the possibility of a malicious file being masked as a PDF. It could also block unknown or malicious code contained within the PDF that would run on the immediate opening within a browser tab.

Impact:

Users will be required to open PDF files manually in the PDF Viewer or in the organization's PDF viewing application.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Allow local file access to file:// URLs on these sites in the PDF Viewer**
6. Ensure **Allowed URLs** is empty

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Allow local file access to file:// URLs on these sites in the PDF Viewer**
6. Remove all URLs from **Allowed URLs**
7. Select **Save**

References:

1. <https://chromeenterprise.google/policies/#PdfLocalFileAccessAllowedForDomainS>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	14.6 <u>Train Workforce Members on Recognizing and Reporting Security Incidents</u> Train workforce members to be able to recognize a potential incident and be able to report such an incident.			
v7	3.3 <u>Protect Dedicated Assessment Accounts</u> Use a dedicated account for authenticated vulnerability scans, which should not be used for any other administrative activities and should be tied to specific machines at specific IP addresses.			

2.8.11 (L2) Ensure 'Notifications' is set to 'Do not allow any site to show desktop notifications' (Automated)

Profile Applicability:

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

Description:

Google Chrome offers websites the ability to display desktop notifications. These are push messages which are sent from the website operator through Google infrastructure to Chrome.

- Allow sites to show desktop notifications (1)
- Do not allow any site to show desktop notifications (2)
- Ask every time a site wants to show desktop notifications (3)

The recommended state for this setting is: Enabled with a value of Do not allow any site to show desktop notifications (2)

Rationale:

If the website operator decides to send messages unencrypted, Google's servers may process it as plain text. Furthermore, potentially compromised or faked notifications might trick users into clicking on a malicious link.

Impact:

If this setting is enabled and set to Do not allow any site to show desktop notifications, notifications will not be displayed for any sites and the user will not be asked.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select Devices
3. Select Chrome
4. Select Settings
5. Under User & browser settings, select Notifications
6. Ensure Configuration is set to Do not allow any site to show desktop notifications

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Notifications**
6. Set **Configuration** to **Do not allow any site to show desktop notifications**
7. Select **Save**

Default Value:

Unset (Same as Enabled, with 'Ask every time a site wants to show desktop notifications')

References:

1. <https://chromeenterprise.google/policies/#DefaultNotificationsSetting>
2. <https://www.google.com/chrome/privacy/whitepaper.html#notifications>
3. <https://medium.com/@BackmaskSWE/push-messages-isnt-secure-enough-69121c683cc6>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.8.12 (L2) Ensure 'WebUSB API' is set to 'Do not allow any site to request access to USB devices via the WebUSB API' (Automated)

Profile Applicability:

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

Description:

Google Chrome has an API which allows access to connected USB devices from the browser

- Do not allow any site to request access to USB devices via the WebUSB API (2)
- Allow sites to ask the user to grant access to a connected USB device (3)

The recommended state for this setting is: Enabled with a value of Do not allow any site to request access to USB devices via the WebUSB API (2)

Rationale:

WebUSB is opening the doors for sophisticated phishing attacks that could bypass hardware-based two-factor authentication devices (e.g. Yubikey devices).

Impact:

If this setting is configured, websites can no longer access connected USB devices via the API (this includes web cameras, headphones, and other USB devices) which could also prevent some two factor authentication (2FA) USB devices from working properly.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select Devices
3. Select Chrome
4. Select Settings
5. Under User & browser settings, select WebUSB API
6. Ensure Configuration is set to Do not allow any site to request access to USB devices via the WebUSB API

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **WebUSB API**
6. Set **Configuration** to **Do not allow any site to request access to USB devices via the WebUSB API**
7. Select **Save**

Default Value:

Unset (Same as Enabled: Allow sites to ask the user to grant access to a connected USB device, but user can change)

References:

1. <https://chromeenterprise.google/policies/#DefaultWebUsbGuardSetting>
2. <https://www.wired.com/story/chrome-yubikey-phishing-webusb/>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	13.7 <u>Manage USB Devices</u> If USB storage devices are required, enterprise software should be used that can configure systems to allow the use of specific devices. An inventory of such devices should be maintained.			

2.8.13 (L1) Ensure 'Allow third-party partitioning to be enabled' in 'Third-party storage partitioning' Is Configured (Manual)

Profile Applicability:

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

Description:

This setting will block specific sites your organization selects from accessing the storage session from any other site. This will allow an organization to block third party trackers that are embedded on multiple sites from tracking a user across the sites they visit. It will also allow blocking third party access to the user agent and to infer data about the user from the data from another site.

Setting the Level 2 recommendation **Block third-party storage partitioning from being enabled** will remove any sites listed in **Allow third-party partitioning to be enabled** and block all sites.

Rationale:

If your organization does not want to block all third-party sites from accessing the user agent, you can configure a curated list of sites to block.

Impact:

This might cause the user experience to vary from allowed sites to blocked sites.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **<https://admin.google.com>** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Third-party storage partitioning**
6. Ensure **Third-party storage partitioning** is set to your organization's requirements

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Third-party storage partitioning**
6. Set **Third-party storage partitioning** to to your organization's requirements
7. Select **Save**

References:

1. <https://chromeenterprise.google/policies/#ThirdPartyStoragePartitioningBlockedForOrigins>
2. <https://groups.google.com/a/chromium.org/g/blink-dev/c/24hK6DKJnqY?pli=1>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.2 <u>Use DNS Filtering Services</u> Use DNS filtering services on all enterprise assets to block access to known malicious domains.			
v7	4.8 <u>Log and Alert on Changes to Administrative Group Membership</u> Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.			

2.8.14 (L2) Ensure 'Third-party storage partitioning' Is Set to 'Block third-party storage partitioning from being enabled' (Automated)

Profile Applicability:

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

Description:

This setting will block any site from accessing the storage session from any other site. This will block third party trackers that are embedded on multiple sites from tracking a user across the sites they visit. Blocking third party access to the user agent will not allow sites to infer data about the user from the data from another site.

It can be configured to either:

- Enabled (1): Allow third-party storage partitioning to be enabled.
- Disabled (2): Block third-party storage partitioning from being enabled.

Rationale:

Setting this requires that user agent state needs to be keyed by more than a single origin or site. It can also defend against timing attacks on web privacy.

Impact:

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

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Third-party storage partitioning**
6. Ensure **Configuration** is set to **Block third-party storage partitioning from being enabled**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Third-party storage partitioning**
6. Set **Configuration** to **Block third-party storage partitioning from being enabled**
7. Select **Save**

Default Value:

Not Configured

References:

1. <https://chromeenterprise.google/policies/#DefaultThirdPartyStoragePartitioningSetting>
2. <https://privacycg.github.io/storage-partitioning/>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	14.6 <u>Train Workforce Members on Recognizing and Reporting Security Incidents</u> Train workforce members to be able to recognize a potential incident and be able to report such an incident.	●	●	●
v7	3.3 <u>Protect Dedicated Assessment Accounts</u> Use a dedicated account for authenticated vulnerability scans, which should not be used for any other administrative activities and should be tied to specific machines at specific IP addresses.		●	●

2.8.15 (L2) Ensure 'Web Bluetooth API' is set to 'Do not allow any site to request access to Bluetooth devices via the Web Bluetooth API' (Automated)

Profile Applicability:

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

Description:

Google Chrome has an API which allows the access to nearby Bluetooth devices from the browser with users consent.

- Do not allow any site to request access to Bluetooth devices via the Web Bluetooth API (2)
- Allow sites to ask the user to grant access to a nearby Bluetooth device (3)

The recommended state for this setting is: Enabled with a value of Do not allow any site to request access to Bluetooth devices via the Web Bluetooth API (2)

Rationale:

A malicious website could exploit a vulnerable Bluetooth device.

Impact:

If this setting is configured, websites can no longer access nearby Bluetooth devices via the API (this includes web cameras, headphones, and other Bluetooth devices) and the user will never be asked.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select Devices
3. Select Chrome
4. Select Settings
5. Under User & browser settings, select Web Bluetooth API
6. Ensure Configuration is set to Do not allow any site to request access to Bluetooth devices via the Web Bluetooth API

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Web Bluetooth API**
6. Set **Configuration** to **Do not allow any site to request access to Bluetooth devices via the Web Bluetooth API**
7. Select **Save**

Default Value:

Unset (Same as Enabled: Allow sites to ask the user to grant access to a nearby Bluetooth device, but user can change)

References:

1. <https://chromeenterprise.google/policies/#DefaultWebBluetoothGuardSetting>
2. https://webbluetoothcg.github.io/web-bluetooth/use-cases.html#security_privacy

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	15.9 <u>Disable Wireless Peripheral Access of Devices</u> Disable wireless peripheral access of devices (such as Bluetooth and NFC), unless such access is required for a business purpose.			

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

Profile Applicability:

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

Description:

Setting controls whether users can add exceptions to allow mixed content for specific sites.

- Do not allow any site to load mixed content (2)
- Allow users to add exceptions to allow mixed content (3)

The recommended state for this setting is: **Enabled** with the value of **Do not allow any site to load mixed content** (2)

NOTE: This policy can be overridden for specific URL patterns using the *InsecureContentAllowedForUrls* and *InsecureContentBlockedForUrls* 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 mix content.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Control use of insecure content exceptions**
6. Ensure **Configuration** is set to **Do not allow any site to load mixed content**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Control use of insecure content exceptions**
6. Set **Configuration** to **Do not allow any site to load mixed content**
7. Select **Save**

Default Value:

Unset (Same as Enabled: Allow users to add exceptions to allow mixed content, but user can change)

References:

1. <https://chromeenterprise.google/policies/#DefaultInsecureContentSetting>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.3 <u>Maintain and Enforce Network-Based URL Filters</u> 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 <u>Subscribe to URL-Categorization service</u> 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.			

2.9 User Experience

Sign-in settings are configuration options in the Google admin console for managing various aspects of how users interact with the Chrome browser within an organization.

Administrators can control how users interact with the Chrome browser on managed devices, including features like the new tab page, search settings, extensions, and even the visual appearance, to tailor the browsing experience for their organization's specific needs and security policies.

2.9.1 (L1) Ensure 'Download location prompt' is set to 'Ask the user where to save the file before downloading' (Automated)

Profile Applicability:

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

Description:

Google Chrome offers to download files automatically to the default download directory without prompting.

If this setting is enabled, users are always asked where to save each file before downloading.

The recommended state for this setting is: **Enabled** (1)

Rationale:

Users shall be prevented from the drive-by-downloads threat.

Impact:

None - This is the default behavior.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Download location prompt**
6. Ensure **Configuration** is set to **Ask the user where to save the file before downloading**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Download location prompt**
6. Set **Configuration** to **Ask the user where to save the file before downloading**
7. Select **Save**

Default Value:

Unset (Same as Enabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#PromptForDownloadLocation>
2. <https://www.ghacks.net/2017/05/18/you-should-disable-automatic-downloads-in-chrome-right-now/>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.9.2 (L2) Ensure 'Browser guest mode' is set to 'Prevent guest browser logins' (Automated)

Profile Applicability:

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

Description:

This setting controls whether a user may utilize guest profiles in Google Chrome.

The recommended state for this setting is: **Disabled** (0)

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 Google Chrome.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Browser guest mode**
6. Ensure **Configuration** is set to **Prevent guest browser logins**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Browser guest mode**
6. Set **Configuration** to **Prevent guest browser logins**
7. Select **Save**

Default Value:

Unset (Same as Enabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#BrowserGuestModeEnabled>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.2 <u>Use DNS Filtering Services</u> Use DNS filtering services on all enterprise assets to block access to known malicious domains.			
v7	4.8 <u>Log and Alert on Changes to Administrative Group Membership</u> Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.			

2.9.3 (L1) Ensure 'Credit card form Autofill' is set to 'Never Autofill credit card forms' (Automated)

Profile Applicability:

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

Description:

Chrome allows users to auto-complete web forms with saved credit card information. Disabling this feature will prompt a user to enter all information manually.

The recommended state for this setting is: **Disabled** (0)

Rationale:

If an attacker gains access to a user's machine where the user has stored credit card AutoFill data, information could be harvested.

Impact:

If this setting is disabled, credit card AutoFill will be inaccessible to users.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Credit card form Autofill**
6. Ensure **Configuration** is set to **Never Autofill credit card forms**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Credit card form Autofill**
6. Set **Configuration** to **Never Autofill credit card forms**
7. Select **Save**

Default Value:

Unset (Same as Enabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#AutofillCreditCardEnabled>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.2 <u>Use DNS Filtering Services</u> Use DNS filtering services on all enterprise assets to block access to known malicious domains.			
v7	4.8 <u>Log and Alert on Changes to Administrative Group Membership</u> Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.			

2.9.4 (L2) Ensure 'Address form Autofill' is set to 'Never Autofill address forms' (Automated)

Profile Applicability:

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

Description:

Chrome allows users to auto-complete web forms with saved information such as address or phone number. Disabling this feature will prompt a user to enter all information manually.

The recommended state for this setting is: **Disabled** (0)

Rationale:

If an attacker gains access to a user's machine where the user has stored address AutoFill data, information could be harvested.

Impact:

If this setting is disabled, AutoFill will be inaccessible to users.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Address form Autofill**
6. Ensure **Configuration** is set to **Never Autofill address forms**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Address form Autofill**
6. Set **Configuration** to **Never Autofill address forms**
7. Select **Save**

Default Value:

Unset (Same as Enabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#AutofillAddressEnabled>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.2 <u>Use DNS Filtering Services</u> Use DNS filtering services on all enterprise assets to block access to known malicious domains.			
v7	4.8 <u>Log and Alert on Changes to Administrative Group Membership</u> Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.			

2.9.5 (L1) Ensure 'Allow user feedback' is set to 'Do not allow user feedback' (Automated)

Profile Applicability:

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

Description:

This setting controls whether users are able to utilize the Chrome feedback feature to send feedback, suggestions, and surveys to Google, as well as issue reports.

The recommended state for this setting is: **Disabled** (0)

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 Google.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **<https://admin.google.com>** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Allow user feedback**
6. Ensure **Configuration** is set to **Do not allow user feedback**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to **<https://admin.google.com>** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Allow user feedback**
6. Set **Configuration** to **Do not allow user feedback**
7. Select **Save**

Default Value:

Unset (Same as Enabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#UserFeedbackAllowed>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.2 <u>Use DNS Filtering Services</u> Use DNS filtering services on all enterprise assets to block access to known malicious domains.			
v7	4.8 <u>Log and Alert on Changes to Administrative Group Membership</u> Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.			

2.9.6 (L2) Ensure 'File selection dialogs' is set to 'Block file selection dialogs' (Automated)

Profile Applicability:

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

Description:

This setting allows access to local files by allowing file selection dialogs in Google Chrome.

The recommended state for this setting is: **Disabled** (0)

Rationale:

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

Impact:

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

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **File selection dialogs**
6. Ensure **Configuration** is set to **Block file selection dialogs**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **File selection dialogs**
6. Set **Configuration** to **Block file selection dialogs**
7. Select **Save**

Default Value:

Unset (Same as Enabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#AllowFileSelectionDialogs>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.7 Allowlist Authorized Scripts Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.			●
v7	2.5 Integrate Software and Hardware Asset Inventories The software inventory system should be tied into the hardware asset inventory so all devices and associated software are tracked from a single location.			●

2.9.7 (L2) Ensure 'Google Translate' is set to 'Never offer translation' (Automated)

Profile Applicability:

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

Description:

This setting enables Google translation services on Google Chrome.

The recommended state for this setting is: **Disabled** (0)

Rationale:

Content of internal web pages may be leaked to Google's translation service.

Impact:

After disabling this feature, the contents of a web page are no longer sent to Google for translation.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Google Translate**
6. Ensure **Configuration** is set to **Never offer translation**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Google Translate**
6. Set **Configuration** to **Never offer translation**
7. Select **Save**

Default Value:

Unset (Same as Enabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#TranslateEnabled>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.2 <u>Use DNS Filtering Services</u> Use DNS filtering services on all enterprise assets to block access to known malicious domains.			
v7	4.8 <u>Log and Alert on Changes to Administrative Group Membership</u> Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.			

2.9.8 (L1) Ensure 'Spell check service' is set to 'Disable the spell checking web service' (Automated)

Profile Applicability:

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

Description:

Google Chrome can use Google web service to help resolve spelling errors.

The recommended state for this setting is: **Disabled** (0)

Rationale:

Information typed in may be leaked to Google's spellcheck web service.

Impact:

After disabling this feature, Chrome no longer sends the entire contents of text fields to Google as you type them. Spell checking can still be performed using a downloaded dictionary. This setting only controls the usage of the online service.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Spell check service**
6. Ensure **Configuration** is set to **Disable the spell checking web service**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Spell check service**
6. Set **Configuration** to **Disable the spell checking web service**
7. Select **Save**

Default Value:

Unset (Same as Enabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#SpellCheckServiceEnabled>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.2 <u>Use DNS Filtering Services</u> Use DNS filtering services on all enterprise assets to block access to known malicious domains.			
v7	4.8 <u>Log and Alert on Changes to Administrative Group Membership</u> Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.			

2.9.9 (L1) Ensure 'Network prediction' Is Set to 'Do not predict network actions' (Automated)

Profile Applicability:

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

Description:

Google Chrome comes with the network prediction feature which provides DNS prefetching, TCP and SSL preconnection, and prerendering of web pages.

- Predict network actions on any network connection (0) or (1)
- Do not predict network actions on any network connection (2)

The recommended state for this setting is: Enabled with a value of Do not predict network actions on any network connection (2)

Rationale:

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

Impact:

Users will not be presented with web page predictions.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select Devices
3. Select Chrome
4. Select Settings
5. Under User & browser settings, select Network prediction
6. Ensure Configuration is set to Do not predict network actions

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Network prediction**
6. Set **Configuration** to **Do not predict network actions**
7. Select **Save**

Default Value:

Unset (Same as Enabled with a value of Predict network actions on any network connection)

References:

1. <https://chromeenterprise.google/policies/#NetworkPredictionOptions>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.9.10 (L1) Ensure 'Alternate error pages' is set to 'Never use alternate error pages' (Automated)

Profile Applicability:

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

Description:

Google Chrome offers to show suggestions for the page you were trying to reach when it is unable to connect to a web address such as 'Page Not Found'.

The recommended state for this setting is: **Disabled** (0)

Rationale:

Using navigation suggestions may leak information about the web site intended to be visited.

Impact:

If this setting is disabled, Chrome will no longer use a web service to help resolve navigation errors.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Alternate error pages**
6. Ensure **Configuration** is set to **Never use alternate error pages**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Alternate error pages**
6. Set **Configuration** to **Never use alternate error pages**
7. Select **Save**

Default Value:

Unset (Same as Enabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#AlternateErrorPagesEnabled>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.2 <u>Use DNS Filtering Services</u> Use DNS filtering services on all enterprise assets to block access to known malicious domains.			
v7	4.8 <u>Log and Alert on Changes to Administrative Group Membership</u> Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.			

2.9.11 (L1) Ensure 'Payment methods' is set to 'Always tell websites that no payment methods are saved' (Automated)

Profile Applicability:

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

Description:

This 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** (0)

Rationale:

Saving payment information in Google Chrome could lead to sensitive data being leaked and used for non-legitimate purposes.

Impact:

Websites will be unable to query whether payment information within Google Chrome is available.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Payment methods**
6. Ensure **Configuration** is set to **Always tell websites that no payment methods are saved**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Payment methods**
6. Set **Configuration** to **Always tell websites that no payment methods are saved**
7. Select **Save**

Default Value:

Unset (Same as Enabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#PaymentMethodQueryEnabled>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.2 <u>Use DNS Filtering Services</u> Use DNS filtering services on all enterprise assets to block access to known malicious domains.			
v7	4.8 <u>Log and Alert on Changes to Administrative Group Membership</u> Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.			

2.10 Omnibox Search Provider

Omnibox search provider settings are configuration options in the Google admin console for managing search options in Chrome browsers within an organization.

Administrators can control how user's interact with the omnibox in the Chrome browser on managed devices, including search suggestions, side panel configurations, history searches, and even what default search provider the browser will use.

2.10.1 (L2) Ensure 'Search suggest' is set to 'Never allow users to use Search Suggest' (Automated)

Profile Applicability:

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

Description:

Google Chrome offers suggestions in Google Chrome's omnibox while a user is typing.

The recommended state for this setting is: **Disabled** (0)

Rationale:

Using search suggestions may leak information as soon as it is typed/pasted into the omnibox, e.g. passwords, internal webservices, folder structures, etc.

Impact:

The user has to send the search request actively by using the search button or hitting "Enter".

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Search suggest**
6. Ensure **Configuration** is set to **Never allow users to use Search Suggest**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Search suggest**
6. Set **Configuration** to **Never allow users to use Search Suggest**
7. Select **Save**

Default Value:

Unset (Same as Enabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#SearchSuggestEnabled>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.2 <u>Use DNS Filtering Services</u> Use DNS filtering services on all enterprise assets to block access to known malicious domains.			
v7	4.8 <u>Log and Alert on Changes to Administrative Group Membership</u> Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.			

2.10.2 (L1) Ensure 'Side Panel search' Is Set to 'Disable Side Panel search on all web pages' (Automated)

Profile Applicability:

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

Description:

This setting controls the Google Search Side Panel. It can be configured to either:

- Disabled (0): **Disable Google Search Side Panel on all web pages**
- Enabled (1): **Enable Google Search Side Panel on all web pages**

Rationale:

Setting this policy will not allow the Google Search Side Panel on any webpages.

Impact:

This should have no user impact.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **<https://admin.google.com>** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Side Panel search**
6. Ensure **Configuration** is set to **Disable Side Panel search on all web pages**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to **<https://admin.google.com>** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Side Panel search**
6. Set **Configuration** to **Disable Side Panel search on all web pages**
7. Select **Save**

References:

1. <https://chromeenterprise.google/policies/#GoogleSearchSidePanelEnabled>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.2 <u>Use DNS Filtering Services</u> Use DNS filtering services on all enterprise assets to block access to known malicious domains.			
v7	4.8 <u>Log and Alert on Changes to Administrative Group Membership</u> Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.			

2.11 Hardware

Hardware settings are configuration options in the Google admin console for restricting or allowing specific hardware functions of Chrome browsers within an organization.

Administrators can control how hardware is accessed in Chrome browser on managed devices, including USB access, camera usage, and file system access.

2.11.1 (L1) Ensure 'Enterprise Hardware Platform API' is set to 'Do not allow managed extensions to use the Enterprise Hardware Platform API' (Automated)

Profile Applicability:

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

Description:

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

The recommended state for this setting is: **Disabled** (0)

Rationale:

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

Impact:

None - This is the default behavior.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Enterprise Hardware Platform API**
6. Ensure **Configuration** is set to **Do not allow managed extensions to use the Enterprise Hardware Platform API**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Enterprise Hardware Platform API**
6. Set **Configuration** to **Do not allow managed extensions to use the Enterprise Hardware Platform API**
7. Select **Save**

Default Value:

Unset (Same as Disabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#EnterpriseHardwarePlatformAPIEnabled>

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.			

2.11.2 (L2) Ensure 'Video input (camera)' is set to 'Disable camera input for websites and apps' (Automated)

Profile Applicability:

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

Description:

This setting allows administrators to set whether the end-user is prompted for access to video capture devices.

- **Disabled** (0): Turns off prompts and video capture will only work for URLs configured in the *VideoCaptureAllowedUrls* list.
- **Enabled** (1): With the exception of URLs set in the *VideoCaptureAllowedUrls* list, users get prompted for video capture access.

NOTE: The setting affects all video input (not just the built-in camera).

The recommended state for this setting is: **Disabled** (0)

Rationale:

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

Impact:

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

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Video input (camera)**
6. Ensure **Configuration** is set to **Disable camera input for websites and apps**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Video input (camera)**
6. Set **Configuration** to **Disable camera input for websites and apps**
7. Select **Save**

Default Value:

Unset (Same as Enabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#VideoCaptureAllowed>
2. <https://chromeenterprise.google/policies/#VideoCaptureAllowedUrls>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.2 <u>Use DNS Filtering Services</u> Use DNS filtering services on all enterprise assets to block access to known malicious domains.			
v7	4.8 <u>Log and Alert on Changes to Administrative Group Membership</u> Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.			

2.11.3 (L2) Ensure 'Audio input (microphone)' is set to 'Disable audio input' (Automated)

Profile Applicability:

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

Description:

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

- **Disabled** (0): Turns off prompts and audio capture will only work for URLs configured in the *AudioCaptureAllowedUrls* list.
- **Enabled** (1): With the exception of URLs set in the *AudioCaptureAllowedUrls* list, users get prompted for audio capture access.

NOTE: The setting affects all audio input (not just the built-in microphone).

The recommended state for this setting is: **Disabled**

Rationale:

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

Impact:

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

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Audio input (microphone)**
6. Ensure **Configuration** is set to **Disable audio input**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Audio input (microphone)**
6. Set **Configuration** to **Disable audio input**
7. Select **Save**

Default Value:

Unset (Same as Enabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#AudioCaptureAllowed>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.2 <u>Use DNS Filtering Services</u> Use DNS filtering services on all enterprise assets to block access to known malicious domains.			
v7	4.8 <u>Log and Alert on Changes to Administrative Group Membership</u> Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.			

2.11.4 (L2) Ensure 'Sensors' is set to 'Do not allow any site to access sensors' (Automated)

Profile Applicability:

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

Description:

This setting controls website access and use of system sensors such as motion and light.

- Allow sites to access sensors (1)
- Do not allow any site to access sensors (2)

The recommended state for this setting is: Do not allow any site to access sensors (2)

The recommended state for this setting is: Enabled with a value of Do not allow any site to access sensors

NOTE: If more granular control is needed (per website) then this setting can be used in combination with the *SensorsAllowedForUrls* and *SensorsBlockedForUrls* settings. For example, *SensorsAllowedForUrls* can be used to allow sensor access to specific sites. Please see the references below for more information.

Rationale:

Preventing access to system sensors may prevent malicious sites from using these sensors for user profiling (OpSec).

Impact:

This setting would also prevent legitimate sites from accessing it as well.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select Devices
3. Select Chrome
4. Select Settings
5. Under User & browser settings, select Sensors
6. Ensure Configuration is set to Do not allow any site to access sensors

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Sensors**
6. Set **Configuration** to **Do not allow any site to access sensors**
7. Select **Save**

Default Value:

Unset (Same as Enabled with a value of Allow sites to access sensors, but user can change)

References:

1. <https://chromeenterprise.google/policies/#DefaultSensorsSetting>
2. <https://chromeenterprise.google/policies/#SensorsAllowedForUrls>
3. <https://chromeenterprise.google/policies/#SensorsBlockedForUrls>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> 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 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

2.11.5 (L2) Ensure 'Web Serial API' is set to 'Do not allow any site to request access to serial ports via the Web Serial API' (Automated)

Profile Applicability:

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

Description:

This setting controls website access and use of the system serial port.

- Do not allow any site to request access to serial ports via the Serial API (2)
- Allow sites to ask the user to grant access to a serial port (3)

The recommended state for this setting is: Do not allow any site to request access to serial ports via the Serial API (2)

NOTE: If more granular control is needed (per website) then this setting can be used in combination with the *SerialAllowAllPortsForUrls*, *SerialAskForUrls* and *SerialBlockedForUrls* settings. For example, *SerialAllowAllPortsForUrls* can be used to allow serial port access to specific sites. Please see the references below for more information.

Rationale:

Preventing access to system serial ports may prevent malicious sites from using these ports and accessing the devices attached.

Impact:

This setting would also prevent legitimate sites from accessing it as well.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Web Serial API**
6. Ensure **Configuration** is set to **Do not allow any site to request access to serial ports via the Web Serial API**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Web Serial API**
6. Set **Configuration** to **Do not allow any site to request access to serial ports via the Web Serial API**
7. Select **Save**

Default Value:

Unset (Same as Enabled with Allow sites to ask the user to grant access to a serial port, but user can change)

References:

1. <https://chromeenterprise.google/policies/#DefaultSerialGuardSetting>
2. <https://chromeenterprise.google/policies/#SerialAskForUrls>
3. <https://chromeenterprise.google/policies/#SerialBlockedForUrls>
4. <https://chromeenterprise.google/policies/#SerialAllowAllPortsForUrls>

CIS Controls:

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

2.12 Chrome Safe Browsing

Chrome safe browsing settings are configuration options in the Google admin console for managing the level of protection users receive from potentially harmful websites, downloads, and extensions by enabling or disabling Google's Safe Browsing feature on Chrome browsers within an organization.

Administrators can control how users interact with safe browsing in the Chrome browser on managed devices, including:

- **Standard protection** - basic security against known threats
- **Enhanced protection** - provides more robust security by detecting potential new dangers but requires sharing more browsing data with Google

These features act as a safeguard against malware, phishing attempts, and other malicious online content by warning users before they access unsafe sites.

2.12.1 (L1) Ensure no URLs Are Configured in 'Safe Browsing allowed domains' (Automated)

Profile Applicability:

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

Description:

The setting determines the functionality of Safe Browsing.

- **Disabled** (0): Safe Browsing protection applies to all resources
- **Enabled** (1), with a list of 1 or more sites: Means Safe Browsing will trust the domains you designate. It won't check them for dangerous resources such as phishing, malware, or unwanted software.

The recommended state for this setting is: **Disabled** (0)

NOTE: Safe Browsing's download protection service won't check downloads hosted on these domains, and its password protection service won't check for password reuse.

Rationale:

Google Safe Browsing will help protect users from a variety of malicious and fraudulent sites, or from downloading dangerous files.

Impact:

None - This is the default behavior.

NOTE: The only real impact is possible user annoyance if they are going to a legitimate site that is falsely considered fraudulent (a rare occurrence). This can be handled by adding the site to the allowlist and/or notifying Google of the false finding.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Safe Browsing allowed domains**
6. Ensure **Allow Domains** is empty

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Safe Browsing allowed domains**
6. Remove any URLs from **Allowed Domains**
7. Select **Save**

Default Value:

Unset (Same as Disabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#SafeBrowsingAllowlistDomains>
2. <https://safebrowsing.google.com/>

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	7.4 Maintain and Enforce Network-Based URL Filters Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.			

2.12.2 (L1) Ensure 'Safe Browsing for trusted sources' is set to 'Perform Safe Browsing checks on all downloaded files' (Automated)

Profile Applicability:

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

Description:

Google Chrome can be adjusted to allow downloads without Safe Browsing checks when the requested file is from a trusted source. Trusted sources can be defined using recommendation 'Configure the list of domains on which Safe Browsing will not trigger warnings'.

The recommended state for this setting is: **Disabled** (0)

NOTE: On Microsoft® Windows®, this functionality is only available on instances that are joined to a Microsoft® Active Directory® domain, running on Windows 10 Pro, or enrolled in Chrome Browser Cloud Management.

Rationale:

Information requested from trusted sources shall not be sent to Google's safe browsing servers.

Impact:

If this setting is disabled, files downloaded from intranet resources will not be checked by Google Services.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Safe Browsing for trusted sources**
6. Ensure **Configuration** is set to **Perform Safe Browsing checks on all downloaded files**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Safe Browsing for trusted sources**
6. Set **Configuration** to **Perform Safe Browsing checks on all downloaded files**
7. Select **Save**

Default Value:

Unset (Same as Enabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#SafeBrowsingForTrustedSourcesEnabled>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.2 <u>Use DNS Filtering Services</u> Use DNS filtering services on all enterprise assets to block access to known malicious domains.			
v7	4.8 <u>Log and Alert on Changes to Administrative Group Membership</u> Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.			

2.12.3 (L1) Ensure 'Disable bypassing Safe Browsing warnings' is set to 'Do not allow user to bypass Safe Browsing warning' (Automated)

Profile Applicability:

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

Description:

Google provides the Safe Browsing service. It shows a warning page when users navigate to sites that are flagged as potentially malicious.

Disabled (0): Users can choose to proceed to the flagged site after the warning appears.

The recommended state for this setting is: **Enabled** (1)

Rationale:

Malicious web pages are widely spread on the internet and pose the most significant threat to the user today. Users shall be prevented from navigating to potentially malicious web content.

Impact:

Enabling this setting prevents users from proceeding anyway from the warning page to the malicious site. In some cases legitimate sites could be blocked and users would be prevented from accessing.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Disable bypassing Safe Browsing warnings**
6. Ensure **Configuration** is set to **Do not allow user to bypass Safe Browsing warning**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Disable bypassing Safe Browsing warnings**
6. Set **Configuration** to **Do not allow user to bypass Safe Browsing warning**
7. Select **Save**

Default Value:

Unset (Same as Disabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#DisableSafeBrowsingProceedAnyway>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.3 <u>Maintain and Enforce Network-Based URL Filters</u> 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	7.4 <u>Maintain and Enforce Network-Based URL Filters</u> Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.			

2.12.4 (L1) Ensure 'Download restrictions' is set to 'Block malicious downloads' (Automated)

Profile Applicability:

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

Description:

Google Chrome can block certain types of downloads, and won't let users bypass the security warnings, depending on the classification of Safe Browsing.

- No special restrictions. Default. (0, Disabled) (Default)
- Block malicious downloads and dangerous file types. (1)
- Block malicious downloads, uncommon or unwanted downloads and dangerous file types. (2)
- Block all downloads. (3)
- Block malicious downloads. Recommended. (4)

The recommended state for this setting is: **Enabled** with a value of **Block malicious downloads. Recommended.** (4)

NOTE: These restrictions apply to downloads triggered from webpage content, as well as the Download link... menu option. They don't apply to the download of the currently displayed page or to saving as PDF from the printing options.

Rationale:

Users shall be prevented from downloading malicious file types, and shall not be able to bypass security warnings.

Impact:

If this setting is enabled, all downloads are allowed, except for those that carry Safe Browsing warnings. These are downloads that have been identified as risky or from a risky source by the [Google Safe Browsing Global intelligence engine](#).

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Download restrictions**
6. Ensure **Configuration** is set to **Block malicious downloads**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Download restrictions**
6. Set **Configuration** to **Block malicious downloads**
7. Select **Save**

Default Value:

Unset (Same as Disabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#DownloadRestrictions>
2. <https://developers.google.com/safe-browsing>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.3 <u>Ensure Adequate Audit Log Storage</u> Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.			
v7	10.5 <u>Ensure Backups Have At least One Non-Continuously Addressable Destination</u> Ensure that all backups have at least one backup destination that is not continuously addressable through operating system calls.			

2.12.5 (L1) Ensure 'Suppress lookalike domain warnings on domains' is Not Set (Automated)

Profile Applicability:

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

Description:

This setting prevents the display of lookalike URL warnings on the sites listed. These warnings are typically shown on sites that Google Chrome believes might be trying to spoof another site with which the user is familiar.

- **Disabled** (0) or set to an empty list: Warnings may appear on any site the user visits.
- **Enabled** (1) and set to one or more domains: No lookalike warnings pages will be shown when the user visits pages on that domain.

The recommended state for this setting is: **Disabled** (0)

Rationale:

Look-alike domains are intentionally misleading to give users the false impression that they're interacting with trusted brands, leading to significant reputation damage, financial losses, and data compromise for established enterprises.

In addition, this technique is commonly used to host phishing sites, and often leads to account takeover attacks. Users are prompted to enter their credentials on a fake website, and scammers take control of their online accounts with little effort to engage in fraudulent activity.

Impact:

None - This is the default behavior.

NOTE: The only real impact is possible user annoyance if they are going to a legitimate site that is falsely considered fraudulent (a rare occurrence). This can be handled by adding the site to the allowlist and/or notifying Google of the false finding.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Suppress lookalike domain warnings on domains**
6. Ensure **Allowlisted Domains** is empty

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Suppress lookalike domain warnings on domains**
6. Remove all URLs from **Allowlisted Domains**
7. Select **Save**

Default Value:

Unset (Same as Disabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#LookalikeWarningAllowlistDomains>
2. <https://safebrowsing.google.com/>
3. <https://bugs.chromium.org/p/chromium/issues/entry?template=Safety+Tips+Appeals>
4. <https://krebsonsecurity.com/2018/03/look-alike-domains-and-visual-confusion/>
5. <https://www.phishlabs.com/blog/the-anatomy-of-a-look-alike-domain-attack/>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.3 <u>Maintain and Enforce Network-Based URL Filters</u> 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	7.4 <u>Maintain and Enforce Network-Based URL Filters</u> Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.			

2.12.6 (L2) Ensure 'SafeSites URL filter' is set to 'Filter top level sites (but not embedded iframes) for adult content' (Automated)

Profile Applicability:

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

Description:

Google Chrome can use the Google Safe Search API to classify URLs as pornographic or not.

The recommended state for this setting is: **Filter top level sites (but not embedded iframes) for adult content**

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.

NOTE: Using Google's Safe Search API may leak information which is typed/pasted by mistake into the omnibox, e.g. passwords, internal webservices, folder structures, etc.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **SafeSites URL filter**
6. Ensure **Configuration** is set to **Filter top level sites (but not embedded iframes) for adult content**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **SafeSites URL filter**
6. Set **Configuration** to **Filter top level sites (but not embedded iframes)** for adult content
7. Select **Save**

Default Value:

Unset (Same as Enabled with "Do not filter sites for adult content", but user can change)

References:

1. <https://chromeenterprise.google/policies/#SafeSitesFilterBehavior>

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	7.4 Maintain and Enforce Network-Based URL Filters Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.			

2.12.7 (L1) Ensure 'Safe Browsing protection' is set to 'Safe Browsing is active in the standard mode' and 'Allow higher-protection proxied lookups' (Manual)

Profile Applicability:

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

Description:

Control whether Google Chrome's Safe Browsing feature is enabled and the mode in which it operates. If you set this setting as mandatory, users cannot change or override the Safe Browsing setting in Google Chrome.

If this setting is left not set, Safe Browsing will operate in Standard Protection mode but users can change this setting.

- **No Protection** (0): Safe Browsing is never active.
- **Standard Protection** (1): Safe Browsing is active in the standard mode.
- **Enhanced Protection** (2): Safe Browsing is active in the enhanced mode. This mode provides better security, but requires sharing more browsing information with Google.

The recommended state for this setting is: **Safe Browsing is active in the standard mode.** (1) or higher

Rationale:

Google Safe Browsing will help protect users from a variety of malicious and fraudulent sites, or from downloading dangerous files.

NOTE: Google recommends using Enhanced Safe Browsing Mode (2). Turning on Enhanced Safe Browsing will substantially increase protection from dangerous websites and downloads, but will share more data with Google.

For more details, please refer to the items in the References section below.

Impact:

None - This is the default behavior (Standard Protection).

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Safe Browsing protection**
6. Ensure **Safe Browsing Protection Level** is set to **Safe Browsing is active in the standard mode**
7. Ensure **Allow Safe Browsing's standard protection mode to send partial hashes of URLs to Google** is set to **Allow higher-protection proxied lookups**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Safe Browsing protection**
6. Ensure **Safe Browsing Protection Level** is set to **Safe Browsing is active in the standard mode**
7. Ensure **Allow Safe Browsing's standard protection mode to send partial hashes of URLs to Google** is set to **Allow higher-protection proxied lookups**
8. Select **Save**

Default Value:

Unset (Same as Standard Protection, but user can change)

References:

1. <https://chromeenterprise.google/policies/#SafeBrowsingProtectionLevel>
2. <https://security.googleblog.com/2020/05/enhanced-safe-browsing-protection-now.html>
3. <https://security.googleblog.com/2021/06/new-protections-for-enhanced-safe.html>
4. https://developers.google.com/safe-browsing?_ga=2.65351149.274800631.1631808382-2031399475.1630502681

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.3 <u>Maintain and Enforce Network-Based URL Filters</u> 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	7.4 <u>Maintain and Enforce Network-Based URL Filters</u> Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.			

2.13 Generative AI

Generative AI settings are configuration options in the Google admin console for managing various aspects of how users interact with AI features in the Chrome browser within an organization. This includes features like text generation, search enhancements, and comparison tools, enabling customization of the browsing experience to meet specific organizational needs and security policies.

The security recommendations provided are based on the assumption that an organization utilizes AI-powered products. A trust relationship with the technology vendor is essential, as sensitive data may be stored on their servers, similar to email and cloud storage. However, some features of the AI model also require the level of trust between customers of the AI model. If your data is used to train the AI model, then the other customers of the AI model can receive guidance that could be based on your organization's data. Enabling any AI feature(s) should be driven by organizational requirements.

Note: For compliance, adherence to security recommendations is achieved by either implementing the recommended settings or disabling the feature(s) based on organizational needs.

Note: Ensure proprietary data is not used for AI model training to prevent data leaks.

2.13.1 Ensure 'Generative AI policy defaults' Is Set to 'Allow GenAI features without improving AI models' (Automated)

Profile Applicability:

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

Description:

The **Generative AI policy defaults** sets the default options for all policies in the **Generative AI** feature set if those setting are unset. This policy will be overridden for any settings that are set individually.

The **Generative AI policy defaults** can only be set in the Google Admin Console and cannot be set locally.

Note: For compliance, adherence to security recommendations is achieved by either implementing the recommended setting or disabling the feature(s) based on organizational needs.

Rationale:

Setting a default baseline for all the settings in the **Generative AI** section and will also encompass any new settings as they are added to the Google Admin Console. To find what features are currently available and set through the **Generative AI policy defaults** you can visit the [Chrome—Generative AI features and policies](#)

Impact:

This should have no impact on the user.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **Generative AI**, select **Generative AI policy defaults**
6. Ensure **Configuration** is set to **Allow GenAI features without improving AI models**

Note:* For compliance, adherence to security recommendations is also achieved by ensuring **Configuration** is set to **Do not allow GenAI features**.

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **Generative AI**, select **Generative AI policy defaults**
6. Set **Configuration** to **Allow GenAI features without improving AI models**
7. Select **Save**

*Note:** For compliance, adherence to security recommendations is also achieved by setting **Configuration** to **Do not allow GenAI features**.

Default Value:

Allow GenAI features without improving AI models is the default for Enterprise users managed by Google Admin console and for Education accounts managed by Google Workspace.

References:

1. <https://chromeenterprise.google/policies/#GenAiDefaultSettings>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v8	15.3 <u>Classify Service Providers</u> Classify service providers. Classification consideration may include one or more characteristics, such as data sensitivity, data volume, availability requirements, applicable regulations, inherent risk, and mitigated risk. Update and review classifications annually, or when significant enterprise changes occur that could impact this Safeguard.		●	●
v7	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

2.13.2 Ensure 'Help me write' Is Set to 'Use the value specified in the Generative AI policy defaults setting' (Automated)

Profile Applicability:

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

Description:

Help me write is an AI-based assistant that helps a user write web content, and is based on prompts entered by the user and the contents of the web page.

Note: For compliance, adherence to security recommendations is achieved by either implementing the recommended setting or disabling the feature(s) based on organizational needs.

Rationale:

Not allowing the **Help me write** feature to improve the AI model's content can stop possible leakage of your organization's propriety information if it is used in the prompts to create the content.

Impact:

This should have no impact on the user.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **Generative AI**, select **Help me write**
6. Ensure **Configuration** is set to **Allow help me write without improving AI models** (or **Use the value specified in the Generative AI policy defaults setting**)

Note: For compliance, adherence to security recommendations is also achieved by setting **Configuration** to **Do not allow help me write**.

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **Generative AI**, select **Help me write**
6. Set **Configuration** to **Allow help me write without improving AI models** (or **Use the value specified in the Generative AI policy defaults setting**)
7. Select **Save**

Note: For compliance, adherence to security recommendations is also achieved by setting **Configuration** to **Do not allow help me write**.

Default Value:

Unset (will follow the policy set in **GenAiDefaultSettings**)

References:

1. <https://chromeenterprise.google/policies/#HelpMeWriteSettings>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v8	15.3 <u>Classify Service Providers</u> Classify service providers. Classification consideration may include one or more characteristics, such as data sensitivity, data volume, availability requirements, applicable regulations, inherent risk, and mitigated risk. Update and review classifications annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

2.13.3 Ensure 'DevTools AI features' Is Set to 'Use the value specified in the Generative AI policy defaults setting' (Automated)

Profile Applicability:

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

Description:

DevTools AI features is an AI-based assistant that provides additional debugging information. It requires the sending of error messages, stack traces, code snippets, network requests, and/or any other data collected for debugging purposes to Google to train the generative AI model. That data could include prompts, inputs, outputs, source materials, and written feedback, depending on the feature, and may also be reviewed by humans to improve AI models.

Note: Response body or authentication and cookie headers in network requests are not included in the data sent to the server.

Note: For compliance, adherence to security recommendations is achieved by either implementing the recommended setting or disabling the feature(s) based on organizational needs.

Rationale:

Not allowing the **DevTools AI features** feature to improve the AI model's content can stop possible leakage of your organization's propriety information of internal webs in the collected data.

Impact:

This should have no impact on the user.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **Generative AI**, select **DevTools AI features**
6. Ensure **Configuration** is set to **Allow DevTools Generative AI Features without improving AI models** (or **Use the value specified in the Generative AI policy defaults setting**)

Note: For compliance, adherence to security recommendations is also achieved by setting **Configuration** to **Do not allow DevTools Generative AI Features**.

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **Generative AI**, select **DevTools AI features**
6. Set **Configuration** to **Allow DevTools Generative AI Features without improving AI models** (or Use the value specified in the **Generative AI policy defaults setting**)
7. Select **Save**

Note: For compliance, adherence to security recommendations is also achieved by setting **Configuration** to **Do not allow DevTools Generative AI Features**.

Default Value:

Unset (will follow the policy set in **GenAiDefaultSettings**)

References:

1. <https://chromeenterprise.google/policies/#DevToolsGenAiSettings>

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.		●	●
v8	15.3 Classify Service Providers Classify service providers. Classification consideration may include one or more characteristics, such as data sensitivity, data volume, availability requirements, applicable regulations, inherent risk, and mitigated risk. Update and review classifications annually, or when significant enterprise changes occur that could impact this Safeguard.		●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

2.13.4 Ensure 'History search settings' Is Set to 'Use the value specified in the Generative AI policy defaults setting' (Automated)

Profile Applicability:

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

Description:

History search settings is an AI-based assistant that helps search their browsing history and can receive generated answers based on page contents in addition to just page title and URL.

Note: For compliance, adherence to security recommendations is achieved by either implementing the recommended setting or disabling the feature(s) based on organizational needs.

Rationale:

Not allowing the **History search settings** feature to improve the AI model's content can stop possible leakage of both your organization's propriety information through visited sites as well as any PPI from sites visited.

Impact:

This should have no impact on the user.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **Generative AI**, select **History search settings**
6. Ensure **Configuration** is set to **Allow AI history search without improving AI models** (or **Use the value specified in the Generative AI policy defaults setting**)

Note: For compliance, adherence to security recommendations is also achieved by setting **Configuration** to **Do not allow AI history search**.

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **Generative AI**, select **History search settings**
6. Set **Configuration** to **Allow AI history search without improving AI models** (or **Use the value specified in the Generative AI policy defaults setting**)
7. Select **Save**

Note: For compliance, adherence to security recommendations is also achieved by setting **Configuration** to **Do not allow AI history search**.

Default Value:

Unset (will follow the policy set in **GenAiDefaultSettings**)

References:

1. <https://chromeenterprise.google/policies/#HistorySearchSettings>

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.		●	●
v8	15.3 Classify Service Providers Classify service providers. Classification consideration may include one or more characteristics, such as data sensitivity, data volume, availability requirements, applicable regulations, inherent risk, and mitigated risk. Update and review classifications annually, or when significant enterprise changes occur that could impact this Safeguard.		●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

2.13.5 Ensure 'Tab compare' Is Set to 'Use the value specified in the Generative AI policy defaults setting' (Automated)

Profile Applicability:

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

Description:

Tab compare is an AI-based tool for comparing product information across a user's tabs. This feature can be offered to the user when multiple tabs with products in a similar category are open.

Note: For compliance, adherence to security recommendations is achieved by either implementing the recommended setting or disabling the feature(s) based on organizational needs.

Rationale:

Not allowing the **Tab compare** feature to improve the AI model's content can stop possible leakage of your organization's propriety information, or PII, if it is used.

Impact:

This should have no impact on the user.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **Generative AI**, select **Tab compare**
6. Ensure **Configuration** is set to **Allow tab compare without improving AI models** (or **Use the value specified in the Generative AI policy defaults setting**)

Note: For compliance, adherence to security recommendations is also achieved by setting **Configuration** to **Do not allow tab compare**.

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **Generative AI**, select **Tab compare**
6. Set **Configuration** to **Allow tab compare without improving AI models** (or **Use the value specified in the Generative AI policy defaults setting**)
7. Select **Save**

Note: For compliance, adherence to security recommendations is also achieved by setting **Configuration** to **Do not allow tab compare**.

Default Value:

Unset (will follow the policy set in **GenAiDefaultSettings**)

References:

1. <https://chromeenterprise.google/policies/#TabCompareSettings>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v8	15.3 <u>Classify Service Providers</u> Classify service providers. Classification consideration may include one or more characteristics, such as data sensitivity, data volume, availability requirements, applicable regulations, inherent risk, and mitigated risk. Update and review classifications annually, or when significant enterprise changes occur that could impact this Safeguard.		●	●
v7	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

2.13.6 Ensure 'Help me read' Is Set to 'Use the value specified in the Generative AI policy defaults setting' (Manual)

Profile Applicability:

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

Description:

Rationale:

Audit:

Remediation:

References:

1. https://admin.google.com/u/1/ac/chrome/settings/user/details/help_me_read_settings_setting_group?ac_ouid=03ph8a2z4j7oqvq&rapt=AEjHL4NFISArXbekf4eV1jk0pYWliEuKs3T-mhnlWy6a13UObuTB6NziLuytTb0Qhkyfcz6x1p2T5ifA0xqwN1WzsdbhUc4wzJO2lOWboSs5-6gRIXP56CA

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v8	15.3 <u>Classify Service Providers</u> Classify service providers. Classification consideration may include one or more characteristics, such as data sensitivity, data volume, availability requirements, applicable regulations, inherent risk, and mitigated risk. Update and review classifications annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

2.14 Chrome Updates

Chrome update settings are configuration options in the Google admin console for managing full control of the update process for on Chrome browsers within an organization.

Administrators can control how and when Google Chrome browsers on managed devices receive updates, including specifying which update channel (Stable, Beta, Dev) to use, setting target versions, and determining whether updates are automatically applied or require manual intervention.

2.14.1 (L1) Ensure 'Component updates' is set to 'Enable updates for all components' (Automated)

Profile Applicability:

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

Description:

Google Chrome's Component Updater updates several components of Google Chrome on a regular basis (applies only to Chrome browser components).

The recommended state for this setting is: **Enabled** (1)

NOTE: Updates to any component that does not contain executable code, does not significantly alter the behavior of the browser, or is critical for its security will not be disabled (E.g. certificate revocation lists and Safe Browsing data is updated regardless of this setting). FYI <chrome://components> lists all components, but not if they are affected by this setting.

NOTE: Google provided the following list of **some of the components** controlled by this setting:

- Recovery component
- Pnacl
- Floc
- Optimization hints
- SSL error assistant
- CRL set
- Origin trials
- SW reporter
- PKI metadata

Rationale:

Google Chrome Updater shall be used to keep the components bundled to Chrome up to date.

Impact:

None - This is the default behavior.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Component updates**
6. Ensure **Configuration** is set to **Enable updates for all components**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Component updates**
6. Set **Configuration** to **Enable updates for all components**
7. Select **Save**

Default Value:

Unset (Same as Enabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#ComponentUpdatesEnabled>

Additional Information:

To check the current components versions, navigate to <chrome://components>.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.4 <u>Perform Automated Application Patch Management</u> Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.			
v7	3.5 <u>Deploy Automated Software Patch Management Tools</u> 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.			

2.14.2 (L1) Ensure 'Relaunch notification' sets 'Time Period (hours)' to '168 or less' and 'Initial quiet period (hours)' to less than 'Time Period (hours)' (Automated)

Profile Applicability:

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

Description:

Google Chrome allows to set the time period, in milliseconds, over which users are notified that it must be relaunched to apply a pending update.

If not set, or **Disabled**, the default period of 604800000 milliseconds (7 days) is used.

The recommended state for this setting is: **Enabled** with value **86400000** (1 day)

Rationale:

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

Impact:

After this time period, the user will be repeatedly informed of the need for an update until a Browser restart is completed.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **<https://admin.google.com>** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Relaunch notification**
6. Ensure **Time Period (hours)** is set to a value **≤168**
7. Ensure **Initial quiet period (hours)** is set to a value **<** the value of **Time Period (hours)**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Relaunch notification**
6. Set **Time Period (hours)** to a value ≤ 168
7. Set **Initial quiet period (hours)** to a value $<$ the value of **Time Period (hours)**
8. Select **Save**

Default Value:

Unset (Same as Disabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#RelaunchNotificationPeriod>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.4 <u>Perform Automated Application Patch Management</u> Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.			
v7	3.5 <u>Deploy Automated Software Patch Management Tools</u> 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.			

2.14.3 (L1) Ensure 'Relaunch notification' is set to 'Show notification recommending relaunch' (Automated)

Profile Applicability:

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

Description:

Google Chrome can notify users that it must be restarted to apply a pending update. This setting controls how users are notified to relaunch Chrome browser or restart their ChromeOS device to get the latest update.

The control can be set to one of three options:

- No relaunch notification: Activates a minimal default level of notifications. Chrome browser indicates to users that a relaunch is needed via subtle changes to its menu. In ChromeOS, a notification in the system tray prompts the user to relaunch.
- Show notification recommending relaunch: Users see a recurring message that they should relaunch Chrome browser or restart their ChromeOS device. Users can close the notification and keep using the old version of Chrome browser or ChromeOS until they choose to relaunch Chrome browser or restart their ChromeOS device.
- Force relaunch after a period: Users can close the notification but will see a recurring message that they need to relaunch Chrome browser or restart their ChromeOS device within a certain amount of time.

The recommended state for this setting is: **Enabled** with a value of **Show a recurring prompt to the user indicating that a relaunch is required** (2)

Rationale:

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

Impact:

A recurring warning will be shown to the user indicating that a browser relaunch will be forced once the notification period passes. The user's session is restored after the relaunch of Google Chrome.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Relaunch notification**
6. Ensure **Configuration** is set to **Show notification recommending relaunch**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Relaunch notification**
6. Set **Configuration** to **Show notification recommending relaunch**
7. Select **Save**

Default Value:

Unset (Same as Disabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#RelaunchNotification>

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.			

2.15 Chrome Variations

Chrome variation settings are configuration options in the Google admin console for managing the rollout process to ensure stability and quality control on Chrome browsers within an organization.

Administrators can control how experimental features or updates are rolled out to users for Chrome browser on managed devices, enabling them to test new Chrome functionalities on a subset of users before a full release.

2.15.1 (L1) Ensure 'Variations' is set to 'Enable Chrome variations' (Manual)

Profile Applicability:

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

Description:

Configuring this setting allows specifying which variations are allowed to be applied in Google Chrome. Variations provide a means for Google to offer modifications to Google Chrome without shipping a new version of the browser by selectively enabling or disabling already existing features.

- **Enable all variations** (0): Allows all variations to be applied to the browser (Default value).
- **Enable variations concerning critical fixes only** (1): Allows only variations considered critical security or stability fixes to be applied to Google Chrome.
- **Disable all variations** (2): Prevent all variations from being applied to the browser. Please note that this mode can potentially prevent the Google Chrome developers from providing critical security fixes in a timely manner and is thus not recommended.

The recommended state for this setting is: **Enable all variations** (0)

NOTE: Google strongly believes there is no added security benefit for turning this to critical fixes, as leaving it on increases the stability of the browser. Disabling variations can also prevent getting critical security updates in a timely manner.

Rationale:

Google strongly recommends leaving this setting at the default (0 = Enable all variations), so fixes are gradually enabled (or if necessary, rapidly disabled) via the Chrome Variations framework.

Impact:

None - This is the default behavior.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Variations**
6. Ensure **Configuration** is set to **Enable Chrome variations**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Variations**
6. Set **Configuration** to **Enable Chrome variations**
7. Select **Save**

Default Value:

Unset (Same as Disabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#ChromeVariations>
2. https://support.google.com/chrome/a/answer/9805991?p=Manage_the_Chrome_variations_framework&_ga=2.161804159.274800631.1631808382-2031399475.1630502681&visit_id=637674174853642930-2644817764&rd=1

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.4 <u>Perform Automated Application Patch Management</u> Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.			
v7	3.5 <u>Deploy Automated Software Patch Management Tools</u> 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.			
v7	7.4 <u>Maintain and Enforce Network-Based URL Filters</u> Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.			

2.16 Other Settings

Chrome variation settings are configuration options in the Google admin console for managing miscellaneous options that don't neatly fit into other categories on Chrome browsers within an organization.

Administrators can control various aspects of the Chrome browser experience not covered by standard settings like extensions, security, or user profiles, potentially including things like startup pages, search engine defaults, or specific feature toggles depending on the organization's needs.

2.16.1 (L1) Ensure 'Google time service' is set to 'Allow queries to a Google server to retrieve an accurate timestamp' (Automated)

Profile Applicability:

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

Description:

This setting controls whether Google Chrome can send queries to a Google time service for accurate timestamps. This check helps in validation of certificates.

The recommended state for this setting is: **Enabled**(1)

Rationale:

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

Impact:

None - This is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location which should be set to **1**:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:BrowserNetworkTimeQueriesEnabled
```

To verify this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Google time service**
6. Ensure **Configuration** is set to **Allow queries to a Google server to retrieve an accurate timestamp**

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\Google\Google  
Chrome\Allow queries to a Google time service
```

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Google time service**
6. Set **Configuration** to **Allow queries to a Google server to retrieve an accurate timestamp**
7. Select **Save**

Default Value:

Unset (Same as Enabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#BrowserNetworkTimeQueriesEnabled>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.4 <u>Standardize Time Synchronization</u> Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.		●	●
v7	6.1 <u>Utilize Three Synchronized Time Sources</u> 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.		●	●

2.16.2 (L1) Ensure 'Disk cache size in bytes' in 'Disk cache size' is set to '250609664' (Automated)

Profile Applicability:

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

Description:

This setting controls the size of the cache, in bytes, used to store files on the disk.

The recommended state for this setting is: **Enabled: 250609664** or greater

NOTE The value specified in this setting 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.

Rationale:

Having enough disk space for browser cache is important for a computer investigation and for 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:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Disk cache size**
6. Ensure **Disk cache size in bytes** is set to **250609664**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Disk cache size**
6. Set **Disk cache size in bytes** to **250609664**
7. Select **Save**

Default Value:

Unset (Same as Enabled with a system managed smaller default size, but the user can change)

References:

1. <https://chromeenterprise.google/policies/#DiskCacheSize>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.5 <u>Securely Dispose of Data</u> Securely dispose of data as outlined in the enterprise's data management process. Ensure the disposal process and method are commensurate with the data sensitivity.			
v7	7.4 <u>Maintain and Enforce Network-Based URL Filters</u> Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.			

2.16.3 (L1) Ensure 'Chrome Sync (ChromeOS)' is set to 'Allow Chrome Sync' and Exclude 'Passwords' (Automated)

Profile Applicability:

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

Description:

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

The recommended state for this setting is: **Enabled** with the following text value **passwords** (Case Sensitive)

NOTE: Other settings in addition to **passwords** can be included based on organizational needs.

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 Google Chrome synchronization service.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **<https://admin.google.com>** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Chrome Sync (ChromeOS)**
6. Ensure **Configuration** is set to **Allow Chrome Sync**
7. Ensure **List of types that should be excluded from synchronization** is set to **Passwords**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Chrome Sync (ChromeOS)**
6. Set **Configuration** to **Allow Chrome Sync**
7. Set **List of types that should be excluded from synchronization** to **Passwords**
8. Select **Save**

Default Value:

Unset (Same as Disabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#SyncTypesListDisabled>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.16.4 (L1) Ensure 'Metrics reporting' is set to 'Do not send anonymous reports of usage and crash-related data to Google' (Automated)

Profile Applicability:

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

Description:

This setting controls anonymous reporting of usage and crash-related data about Google Chrome to Google.

The recommended state for this setting is: **Disabled** (0)

NOTE: This setting is not available on Windows instances that are not joined to a Microsoft® Active Directory® domain.

Rationale:

Anonymous crash/usage data can be used to identify people, companies and information, which can be considered data ex-filtration from company systems.

Impact:

If this setting is disabled, this information is not sent to Google.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Metrics reporting**
6. Ensure **Configuration** is set to **Do not send anonymous reports of usage and crash-related data to Google**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Metrics reporting**
6. Set **Configuration** to **Do not send anonymous reports of usage and crash-related data to Google**
7. Select **Save**

Default Value:

Unset (Same as Enabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#MetricsReportingEnabled>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.2 <u>Use DNS Filtering Services</u> Use DNS filtering services on all enterprise assets to block access to known malicious domains.			
v7	4.8 <u>Log and Alert on Changes to Administrative Group Membership</u> Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.			

2.16.5 (L1) Ensure 'Chrome Sync and Roaming Profiles (Chrome Browser - Cloud Managed)' is set to 'Disallow Sync' (Automated)

Profile Applicability:

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

Description:

Google Chrome can synchronize browser data using Google-hosted synchronization services. Examples of synced data include, but are not limited to, history and favorites.

The recommended state for this setting is: **Enabled** (1)

NOTE: if your organization allows synchronization of data with Google, then disabling this setting will synchronize saved passwords with Google.

Rationale:

Browser data shall not be synchronized into the Google Cloud.

Impact:

If this setting is enabled, browser data will no longer sync with Google across devices/platforms, allowing users to pick up where they left off.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Chrome Sync and Roaming Profiles (Chrome Browser - Cloud Managed)**
6. Ensure **Configuration** is set to **Disallow Sync**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Chrome Sync and Roaming Profiles (Chrome Browser - Cloud Managed)**
6. Set **Configuration** to **Disallow Sync**
7. Select **Save**

Default Value:

Unset (Same as Disabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#SyncDisabled>

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	4.8 Log and Alert on Changes to Administrative Group Membership Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.			

2.16.6 (L1) Ensure 'Allow reporting of domain reliability related data' Is 'Never send domain reliability data to Google' (Automated)

Profile Applicability:

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

Description:

This setting controls the defaults for clipboard permission access from sites. It can be configured to either:

- Disabled (0): **Never send domain reliability data to Google**
- Enabled (1): **Domain Reliability data may be sent to Google depending on Chrome User Metrics (UMA) policy**

If the value for **DomainReliabilityAllowed** is not changed from the default, it will behave as it is enabled.

Rationale:

Setting this policy to disabled can stop any accidental data leakage.

Impact:

There should be no impact on the user.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **<https://admin.google.com>** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Allow reporting of domain reliability related data**
6. Ensure **Configuration** is set to **Never send domain reliability data to Google**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Allow reporting of domain reliability related data**
6. Set **Configuration** to **Never send domain reliability data to Google**
7. Select **Save**

Default Value:

Unset (Enabled)

References:

1. <https://chromeenterprise.google/policies/#DomainReliabilityAllowed>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.2 <u>Use DNS Filtering Services</u> Use DNS filtering services on all enterprise assets to block access to known malicious domains.			
v7	4.1 <u>Maintain Inventory of Administrative Accounts</u> Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.			

2.16.7 (L2) Ensure 'Prohibited Native Messaging hosts' in 'Native Messaging blocked hosts' is set to '*' (Automated)

Profile Applicability:

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

Description:

Allows you to specify which native messaging hosts should not be loaded.

Disabled (0): Google Chrome will load all installed native messaging hosts.

The recommended state for this setting is: **Enabled** with a value of *

NOTE: This needs to be handled carefully. If an extension is enabled, yet can't communicate with its backend code, it could behave in strange ways which results in helpdesk tickets + support load.

Rationale:

For consistency with Plugin and Extension policies, native messaging should be blocklisted by default, requiring explicit administrative approval of applications for allowlisting. An example of an application that uses native messaging is the 1Password password manager.

Impact:

A blocklist value of '*' means all native messaging hosts are blocklisted unless they are explicitly listed in the allowlist.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Native Messaging blocked hosts**
6. Ensure **Prohibited Native Messaging hosts** is set to *

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Native Messaging blocked hosts**
6. Set **Prohibited Native Messaging hosts** to *
7. Select **Save**

Default Value:

Unset (Same as Disabled, and users can change)

References:

1. <https://chromeenterprise.google/policies/#NativeMessagingBlocklist>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.4 <u>Restrict Unnecessary or Unauthorized Browser and Email Client Extensions</u> Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.			
v7	7.2 <u>Disable Unnecessary or Unauthorized Browser or Email Client Plugins</u> Uninstall or disable any unauthorized browser or email client plugins or add-on applications.			

2.16.8 (L1) Ensure 'Background mode' is set to 'Disable background mode' (Automated)

Profile Applicability:

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

Description:

Chrome allows for processes started while the browser is open to remain running once the browser has been closed. It also allows for background apps and the current browsing session to remain active after the browser has been closed.

With this setting Disabled, the browser will close its processes and will stop running background apps.

The recommended state for this setting is: **Disabled** (0)

Rationale:

If this setting is enabled, vulnerable or malicious plugins, apps and processes can continue running even after Chrome has closed.

Impact:

None - This is the default behavior.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Background mode**
6. Ensure **Configuration** is set to **Disable background mode**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Background mode**
6. Set **Configuration** to **Disable background mode**
7. Select **Save**

Default Value:

Unset (Same as Disabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#BackgroundModeEnabled>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> 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 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

3 Apps & Extensions

Apps & extensions is a high level configuration option in the Google admin console for more fine-tuned control for applications and extensions for the Google Chrome browsers within an organization.

3.1 Extensions

3.1.1 (L1) Ensure 'External extensions' is set to 'Block external extensions from being installed' (Automated)

Profile Applicability:

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

Description:

Enabling this setting blocks external extensions (an extension that is not installed from the Chrome Web Store) from being installed.

The recommended state for this setting is: **Enabled** (1)

Rationale:

Allowing users to install extensions from other locations (not the Chrome Web Store) can lead to malicious extensions being installed.

Impact:

User will only be allowed to install extension for the Chrome web store.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Apps & extensions**
5. Under **User & browser settings**, select **Additional Settings**
6. Ensure **External extensions** is set to **Block external extensions from being installed**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Apps & extensions**
5. Under **User & browser settings**, select **Additional Settings**
6. Set **External extensions** to **Block external extensions from being installed**
7. Select **Save**

Default Value:

Unset (Same as Disabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#BlockExternalExtensions>
2. https://developer.chrome.com/docs/extensions/mv2/external_extensions/

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.4 <u>Restrict Unnecessary or Unauthorized Browser and Email Client Extensions</u> Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.			
v7	7.2 <u>Disable Unnecessary or Unauthorized Browser or Email Client Plugins</u> Uninstall or disable any unauthorized browser or email client plugins or add-on applications.			

3.1.2 (L1) Ensure 'Allowed types of apps and extensions' is set to 'Extension', 'Hosted App', 'Chrome Packaged App', and 'Theme' (Automated)

Profile Applicability:

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

Description:

Enabling this setting allows you to specify which app/extension types are allowed.

Disabled (0): Results in no restrictions on the acceptable extension and app types.

The recommended state for this setting is: **Enabled** with the values of **extension**, **hosted_app**, **platform_app**, **theme**.

Rationale:

App or extension types that could be misused or are deprecated shall no longer be installed.

NOTE: Google has removed support for Chrome Apps which includes the types **hosted_app** and **platform_app**. The blog post indicates that these types will require a setting to be enabled for continued use through June 2022.

Impact:

Extensions already installed will be removed if its type is denylisted and the extension itself is not allowlisted.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **<https://admin.google.com>** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Apps & extensions**
5. Under **User & browser settings**, select **Additional Settings**
6. Ensure **Allowed types of apps and extensions** is set to **Extension**, **Hosted App**, **Chrome Packaged App**, and **Theme**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Apps & extensions**
5. Under **User & browser settings**, select **Additional Settings**
6. Set **Allowed types of apps and extensions** to **Extension**, **Hosted App**, **Chrome Packaged App**, and **Theme**
7. Select **Save**

Default Value:

Unset (Same as Disabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#ExtensionAllowedTypes>
2. <https://blog.chromium.org/2020/08/changes-to-chrome-app-support-timeline.html>
3. https://chromium.googlesource.com/chromium/src/+HEAD/extensions/docs/extension_and_app_types.md

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>9.4 Restrict Unnecessary or Unauthorized Browser and Email Client Extensions</u> Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.		●	●
v7	<u>7.2 Disable Unnecessary or Unauthorized Browser or Email Client Plugins</u> Uninstall or disable any unauthorized browser or email client plugins or add-on applications.		●	●

3.1.3 (L1) Ensure 'App and extension install sources' Is Not Set (Automated)

Profile Applicability:

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

Description:

Enabling this setting allows you to specify which extensions the users can NOT install. Extensions already installed will be removed if blocklisted.

Disabled (0): then the user can install any extension in Google Chrome.

The recommended state for this setting is: **Enabled** with a value of *

NOTE: Chrome does offer a more granular permission-based configuration called **Extension management settings** if blocklisting all extensions is too aggressive, which allows an organization to drill down to the exact permissions that they want to lock down. The extensions management settings require more coordination and effort to understand what the security requirements are to block site and device permissions globally as well as more IT management to deploy. The benefit would be allowing access to more extensions to their end-users. See link in reference section

NOTE: If Chrome Cleanup is Disabled, users may want to configure the extension blocklist instead of using the Extension Management option. Chrome Cleanup can help protect against malicious extensions when paired with the Extension Management setting.

Rationale:

This can be used to block extensions that could potentially allow remote control of the system through the browser. If there are extensions needed for securing the browser or for enterprise use, these can be enabled by configuring either the setting **Configure extension installation allowlist** or the setting **Extension management settings**.

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:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Apps & extensions**
5. Under **User & browser settings**, select **Additional Settings**
6. Ensure **App and extension install sources** is empty

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Apps & extensions**
5. Under **User & browser settings**, select **Additional Settings**
6. Remove all URLs from **App and extension install sources**
7. Select **Save**

Default Value:

Unset (Same as Disabled, and users can change)

References:

1. <https://chromeenterprise.google/policies/#ExtensionInstallBlocklist>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>9.4 Restrict Unnecessary or Unauthorized Browser and Email Client Extensions</u> Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.		●	●
v7	<u>7.2 Disable Unnecessary or Unauthorized Browser or Email Client Plugins</u> Uninstall or disable any unauthorized browser or email client plugins or add-on applications.		●	●

3.1.4 (L1) Ensure 'Chrome Web Store unpublished extensions' Is Set to 'Disable unpublished extensions' (Automated)

Profile Applicability:

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

Description:

This policy disables any extensions in Google Chrome that were downloaded from the Chrome Web Store and are now unpublished. The policy can be configured to either:

- Enabled (0): **Allow unpublished extensions**
- Disabled (1): **Disable unpublished extensions**

If the value for **ExtensionUnpublishedAvailability** is not changed from the default, it will behave as it is enabled.

Note: Off-store extensions such as unpacked extensions installed using developer mode and extensions installed using the command-line switch are ignored. Force-installed extensions that are self-hosted are ignored. All version-pinned extensions are also ignored.

Rationale:

Disabling unpublished extensions will remove the ability to run any extensions that are no longer being updated or patched.

Impact:

This may disable extensions commonly used by users in your organization.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **<https://admin.google.com>** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Apps & extensions**
5. Under **User & browser settings**, select **Additional Settings**
6. Ensure **Chrome Web Store unpublished extensions** is set to **Disable unpublished extensions**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Apps & extensions**
5. Under **User & browser settings**, select **Additional Settings**
6. Set **Chrome Web Store unpublished extensions** to **Disable unpublished extensions**
7. Select **Save**

Default Value:

Allow unpublished extensions

References:

1. <https://chromeenterprise.google/policies/#ExtensionUnpublishedAvailability>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.2 Establish and Maintain a Remediation Process Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.			
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	Introduction		
2	Settings		
2.1	Sign-in Settings		
2.1.1	(L2) Ensure 'Browser sign in settings' is set to 'Disabled browser sign-in' (Automated)	☐	☐
2.1.2	(L1) Ensure 'Azure Cloud Authentication' Is Set to 'Enable Azure cloud authentication' (Manual)	☐	☐
2.2	Apps and Extensions		
2.2.1	(L2) Ensure 'Manifest v2 extension availability' Is Set to 'Enable force-installed manifest v2 extensions on the sign-in screen' (Automated)	☐	☐
2.3	Site Isolation		
2.3.1	(L1) Ensure 'Site isolation' is set to 'Require Site Isolation for all websites, as well as any origins below' (Automated)	☐	☐
2.4	Security		
2.4.1	(L1) Ensure 'Password manager' is Explicitly Configured (Manual)	☐	☐
2.4.2	(L1) Ensure 'Web Authentication requests on sites with broken TLS certificates' Is Set to 'Do not allow WebAuthn API requests on sites with broken TLS certificates' (Automated)	☐	☐
2.4.3	(L1) Ensure 'Post-quantum TLS' Is Set to 'Allow post-quantum key agreement in TLS connections' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.4.4	(L1) Ensure 'Incognito mode' is set to 'Disallow incognito mode' (Automated)	☐	☐
2.4.5	(L1) Ensure 'Browser history' is set to 'Always save browser history' (Automated)	☐	☐
2.4.6	(L1) Ensure 'Clear browser history' Is Set to 'Do not allow clearing history in settings menu' (Automated)	☐	☐
2.4.7	(L1) Ensure 'Force ephemeral mode' is set to 'Do not erase local user data' (Automated)	☐	☐
2.4.8	(L1) Ensure 'Online revocation checks' is set to 'Perform online OCSP/CRL checks' (Automated)	☐	☐
2.4.9	(L1) Ensure 'Geolocation' is set to 'Do not allow sites to detect users' geolocation' (Automated)	☐	☐
2.4.10	(L1) Ensure 'Allowed certificate transparency URLs' is Not Set (Automated)	☐	☐
2.4.11	(L1) Ensure 'Certificate transparency CA allowlist' is Not Set (Automated)	☐	☐
2.4.12	(L1) Ensure 'Renderer App Container' Is Set to 'Enable the Renderer App Container sandbox' (Automated)	☐	☐
2.4.13	(L1) Ensure 'Enable leak detection for entered credentials' Is Set to 'Enable Leak detection for entered credentials' (Manual)	☐	☐
2.4.14	(L1) Ensure 'Audio sandbox' is set to 'Always sandbox the audio process' (Automated)	☐	☐
2.4.15	(L1) Ensure 'Unsupported system warning' is set to 'Allow Chrome to display warnings when running on an unsupported system' (Automated)	☐	☐
2.4.16	(L2) Ensure 'Advanced Protection program' Is Set to 'Users enrolled in the Advanced Protection program will receive extra protections' (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.4.17	(L1) Ensure 'Override insecure origin restrictions' is Not Set (Automated)	☐	☐
2.4.18	(L1) Ensure 'Command-line flags' is set to 'Show security warnings when potentially dangerous command-line flags are used' (Automated)	☐	☐
2.4.19	(L1) Ensure 'Allow remote debugging' is set to 'Do not allow use of the remote debugging' (Automated)	☐	☐
2.4.20	(L1) Ensure 'TLS encrypted ClientHello' Is 'Enable the TLS Encrypted ClientHello experiment' (Automated)	☐	☐
2.4.21	(L1) Ensure 'Strict MIME type checking for worker scripts' Is Set to 'Require a JavaScript MIME type for worker scripts' (Automated)	☐	☐
2.4.22	(L2) Ensure 'Enforce local anchor constraints' Is 'Enforce constraints in locally added trust anchors' (Automated)	☐	☐
2.4.23	(L1) Ensure 'File/directory picker without user gesture' Is Not Set (Automated)	☐	☐
2.4.24	(L1) Ensure 'Media picker without user gesture' Is Not Configured (Automated)	☐	☐
2.5	Remote access (Chrome Remote Desktop)		
2.5.1	(L1) Ensure 'Remote access hosts' is set with a domain defined in 'Remote access host domain' (Manual)	☐	☐
2.5.2	(L1) Ensure 'Firewall traversal' is set to 'Disable firewall traversal' (Automated)	☐	☐
2.5.3	(L1) Ensure 'Firewall traversal' is set to 'Disable the use of relay servers' (Automated)	☐	☐
2.5.4	(L1) Ensure 'Remote support connections' is set to 'Prevent remote support connections' (Manual)	☐	☐
2.6	Network		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.6.1	(L1) Ensure 'Proxy mode' is Not Set to 'Always auto detect the proxy' (Automated)	☐	☐
2.6.2	(L2) Ensure 'Supported authentication schemes' is set to 'NTLM' and 'Negotiate' (Automated)	☐	☐
2.6.3	(L2) Ensure 'SSL error override' is set to 'Block users from clicking through SSL warnings' (Automated)	☐	☐
2.6.4	(L1) Ensure 'WebRTC ICE candidate URLs for local IPs' Is Not Set (Automated)	☐	☐
2.6.5	(L2) Ensure 'DNS over HTTPS' is set to 'Enable DNS-over-HTTPS without insecure fallback' (Automated)	☐	☐
2.6.6	(L1) Ensure 'Cross-origin authentication' is set to 'Block cross-origin authentication' (Automated)	☐	☐
2.6.7	(L1) Ensure 'Enable globally scoped HTTP authentication cache' is set to 'Disabled' (Automated)	☐	☐
2.6.8	(L1) Ensure 'HSTS policy bypass list' is Not Set (Automated)	☐	☐
2.6.9	(L1) Ensure 'DNS interception checks enabled' is set to 'Perform DNS interception checks ' (Automated)	☐	☐
2.6.10	(L1) Ensure 'Network service sandbox' Is Set to 'Enable the network sandbox' (Automated)	☐	☐
2.6.11	(L1) Ensure 'Http Allowlist' Is Properly Configured (Manual)	☐	☐
2.6.12	(L1) Ensure 'Automatic HTTPS upgrades' Is Set to 'Allow HTTPS upgrades' (Automated)	☐	☐
2.7	Import Settings		
2.7.1	(L1) Ensure 'Import autofill data' is set to 'Disable imports of autofill data' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.7.2	(L1) Ensure 'Import homepage' is set to 'Disable imports of homepage' (Automated)	☐	☐
2.7.3	(L1) Ensure 'Import saved passwords' is set to 'Disable imports of saved passwords' (Automated)	☐	☐
2.7.4	(L1) Ensure 'Import search engines' is set to 'Disable imports of search engines' (Automated)	☐	☐
2.8	Content		
2.8.1	(L2) Ensure 'Screen video capture' is set to 'Do not allow sites to prompt the user to share a video stream of their screen' (Automated)	☐	☐
2.8.2	(L1) Ensure 'Cast' is set to 'Do not allow users to cast' (Automated)	☐	☐
2.8.3	(L1) Ensure 'Clipboard' Is Set to 'Do not allow any site to use the clipboard site permission' (Automated)	☐	☐
2.8.4	(L1) Ensure 'Enable URL-keyed anonymized data collection' is set to 'Data collection is never active' (Automated)	☐	☐
2.8.5	(L1) Ensure 'Third-party cookie blocking' is set to 'Disallow third-party cookies' (Automated)	☐	☐
2.8.6	(L1) Ensure 'Cast' is set to 'Do not allow users to Cast' (Automated)	☐	☐
2.8.7	(L2) Ensure 'Cookies' is set to 'Session Only' (Automated)	☐	☐
2.8.8	(L2) Ensure 'SafeSearch and Restricted Mode' is set to 'Always use Safe Search for Google Web Search queries' (Automated)	☐	☐
2.8.9	(L1) Ensure 'First-Party Sets' Is Set to 'Disable First-Party Sets for all affected users' (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.8.10	(L1) Ensure 'Allow local file access to file:// URLs on these sites in the PDF Viewer' Is Not Set (Automated)	☐	☐
2.8.11	(L2) Ensure 'Notifications' is set to 'Do not allow any site to show desktop notifications' (Automated)	☐	☐
2.8.12	(L2) Ensure 'WebUSB API' is set to 'Do not allow any site to request access to USB devices via the WebUSB API' (Automated)	☐	☐
2.8.13	(L1) Ensure 'Allow third-party partitioning to be enabled' in 'Third-party storage partitioning' Is Configured (Manual)	☐	☐
2.8.14	(L2) Ensure 'Third-party storage partitioning' Is Set to 'Block third-party storage partitioning from being enabled' (Automated)	☐	☐
2.8.15	(L2) Ensure 'Web Bluetooth API' is set to 'Do not allow any site to request access to Bluetooth devices via the Web Bluetooth API' (Automated)	☐	☐
2.8.16	(L1) Ensure 'Control use of insecure content exceptions' is set to 'Do not allow any site to load mixed content' (Automated)	☐	☐
2.9	User Experience		
2.9.1	(L1) Ensure 'Download location prompt' is set to 'Ask the user where to save the file before downloading' (Automated)	☐	☐
2.9.2	(L2) Ensure 'Browser guest mode' is set to 'Prevent guest browser logins' (Automated)	☐	☐
2.9.3	(L1) Ensure 'Credit card form Autofill' is set to 'Never Autofill credit card forms' (Automated)	☐	☐
2.9.4	(L2) Ensure 'Address form Autofill' is set to 'Never Autofill address forms' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.9.5	(L1) Ensure 'Allow user feedback' is set to 'Do not allow user feedback' (Automated)	☐	☐
2.9.6	(L2) Ensure 'File selection dialogs' is set to 'Block file selection dialogs' (Automated)	☐	☐
2.9.7	(L2) Ensure 'Google Translate' is set to 'Never offer translation' (Automated)	☐	☐
2.9.8	(L1) Ensure 'Spell check service' is set to 'Disable the spell checking web service' (Automated)	☐	☐
2.9.9	(L1) Ensure 'Network prediction' Is Set to 'Do not predict network actions' (Automated)	☐	☐
2.9.10	(L1) Ensure 'Alternate error pages' is set to 'Never use alternate error pages' (Automated)	☐	☐
2.9.11	(L1) Ensure 'Payment methods' is set to 'Always tell websites that no payment methods are saved' (Automated)	☐	☐
2.10	Omnibox Search Provider		
2.10.1	(L2) Ensure 'Search suggest' is set to 'Never allow users to use Search Suggest' (Automated)	☐	☐
2.10.2	(L1) Ensure 'Side Panel search' Is Set to 'Disable Side Panel search on all web pages' (Automated)	☐	☐
2.11	Hardware		
2.11.1	(L1) Ensure 'Enterprise Hardware Platform API' is set to 'Do not allow managed extensions to use the Enterprise Hardware Platform API' (Automated)	☐	☐
2.11.2	(L2) Ensure 'Video input (camera)' is set to 'Disable camera input for websites and apps' (Automated)	☐	☐
2.11.3	(L2) Ensure 'Audio input (microphone)' is set to 'Disable audio input' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.11.4	(L2) Ensure 'Sensors' is set to 'Do not allow any site to access sensors' (Automated)	☐	☐
2.11.5	(L2) Ensure 'Web Serial API' is set to 'Do not allow any site to request access to serial ports via the Web Serial API' (Automated)	☐	☐
2.12	Chrome Safe Browsing		
2.12.1	(L1) Ensure no URLs Are Configured in 'Safe Browsing allowed domains' (Automated)	☐	☐
2.12.2	(L1) Ensure 'Safe Browsing for trusted sources' is set to 'Perform Safe Browsing checks on all downloaded files' (Automated)	☐	☐
2.12.3	(L1) Ensure 'Disable bypassing Safe Browsing warnings' is set to 'Do not allow user to bypass Safe Browsing warning' (Automated)	☐	☐
2.12.4	(L1) Ensure 'Download restrictions' is set to 'Block malicious downloads' (Automated)	☐	☐
2.12.5	(L1) Ensure 'Suppress lookalike domain warnings on domains' is Not Set (Automated)	☐	☐
2.12.6	(L2) Ensure 'SafeSites URL filter' is set to 'Filter top level sites (but not embedded iframes) for adult content' (Automated)	☐	☐
2.12.7	(L1) Ensure 'Safe Browsing protection' is set to 'Safe Browsing is active in the standard mode' and 'Allow higher-protection proxied lookups' (Manual)	☐	☐
2.13	Generative AI		
2.13.1	Ensure 'Generative AI policy defaults' Is Set to 'Allow GenAI features without improving AI models' (Automated)	☐	☐
2.13.2	Ensure 'Help me write' Is Set to 'Use the value specified in the Generative AI policy defaults setting' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.13.3	Ensure 'DevTools AI features' Is Set to 'Use the value specified in the Generative AI policy defaults setting' (Automated)	☐	☐
2.13.4	Ensure 'History search settings' Is Set to 'Use the value specified in the Generative AI policy defaults setting' (Automated)	☐	☐
2.13.5	Ensure 'Tab compare' Is Set to 'Use the value specified in the Generative AI policy defaults setting' (Automated)	☐	☐
2.13.6	Ensure 'Help me read' Is Set to 'Use the value specified in the Generative AI policy defaults setting' (Manual)	☐	☐
2.14	Chrome Updates		
2.14.1	(L1) Ensure 'Component updates' is set to 'Enable updates for all components' (Automated)	☐	☐
2.14.2	(L1) Ensure 'Relaunch notification' sets 'Time Period (hours)' to '168 or less' and 'Initial quiet period (hours)' to less than 'Time Period (hours)' (Automated)	☐	☐
2.14.3	(L1) Ensure 'Relaunch notification' is set to 'Show notification recommending relaunch' (Automated)	☐	☐
2.15	Chrome Variations		
2.15.1	(L1) Ensure 'Variations' is set to 'Enable Chrome variations' (Manual)	☐	☐
2.16	Other Settings		
2.16.1	(L1) Ensure 'Google time service' is set to 'Allow queries to a Google server to retrieve an accurate timestamp' (Automated)	☐	☐
2.16.2	(L1) Ensure 'Disk cache size in bytes' in 'Disk cache size' is set to `250609664` (Automated)	☐	☐
2.16.3	(L1) Ensure 'Chrome Sync (ChromeOS)' is set to 'Allow Chrome Sync' and Exclude 'Passwords' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.16.4	(L1) Ensure 'Metrics reporting' is set to 'Do not send anonymous reports of usage and crash-related data to Google' (Automated)	☐	☐
2.16.5	(L1) Ensure 'Chrome Sync and Roaming Profiles (Chrome Browser - Cloud Managed)' is set to 'Disallow Sync' (Automated)	☐	☐
2.16.6	(L1) Ensure 'Allow reporting of domain reliability related data' Is 'Never send domain reliability data to Google' (Automated)	☐	☐
2.16.7	(L2) Ensure 'Prohibited Native Messaging hosts' in 'Native Messaging blocked hosts' is set to '*' (Automated)	☐	☐
2.16.8	(L1) Ensure 'Background mode' is set to 'Disable background mode' (Automated)	☐	☐
3	Apps & Extensions		
3.1	Extensions		
3.1.1	(L1) Ensure 'External extensions' is set to 'Block external extensions from being installed' (Automated)	☐	☐
3.1.2	(L1) Ensure 'Allowed types of apps and extensions' is set to 'Extension', 'Hosted App', 'Chrome Packaged App', and 'Theme' (Automated)	☐	☐
3.1.3	(L1) Ensure 'App and extension install sources' Is Not Set (Automated)	☐	☐
3.1.4	(L1) Ensure 'Chrome Web Store unpublished extensions' Is Set to 'Disable unpublished extensions' (Automated)	☐	☐

Appendix: CIS Controls v7 IG 1 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
2.2.1	(L2) Ensure 'Manifest v2 extension availability' Is Set to 'Enable force-installed manifest v2 extensions on the sign-in screen'	☐	☐
2.3.1	(L1) Ensure 'Site isolation' is set to 'Require Site Isolation for all websites, as well as any origins below'	☐	☐
2.4.5	(L1) Ensure 'Browser history' is set to 'Always save browser history'	☐	☐
2.4.14	(L1) Ensure 'Audio sandbox' is set to 'Always sandbox the audio process'	☐	☐
2.4.15	(L1) Ensure 'Unsupported system warning' is set to 'Allow Chrome to display warnings when running on an unsupported system'	☐	☐
2.4.23	(L1) Ensure 'File/directory picker without user gesture' Is Not Set	☐	☐
2.6.10	(L1) Ensure 'Network service sandbox' Is Set to 'Enable the network sandbox'	☐	☐
2.8.4	(L1) Ensure 'Enable URL-keyed anonymized data collection' is set to 'Data collection is never active'	☐	☐
2.12.4	(L1) Ensure 'Download restrictions' is set to 'Block malicious downloads'	☐	☐
2.13.1	Ensure 'Generative AI policy defaults' Is Set to 'Allow GenAI features without improving AI models'	☐	☐
2.13.2	Ensure 'Help me write' Is Set to 'Use the value specified in the Generative AI policy defaults setting'	☐	☐
2.13.3	Ensure 'DevTools AI features' Is Set to 'Use the value specified in the Generative AI policy defaults setting'	☐	☐
2.13.4	Ensure 'History search settings' Is Set to 'Use the value specified in the Generative AI policy defaults setting'	☐	☐
2.13.5	Ensure 'Tab compare' Is Set to 'Use the value specified in the Generative AI policy defaults setting'	☐	☐

Recommendation		Set Correctly	
		Yes	No
2.13.6	Ensure 'Help me read' Is Set to 'Use the value specified in the Generative AI policy defaults setting'	☐	☐
2.14.1	(L1) Ensure 'Component updates' is set to 'Enable updates for all components'	☐	☐
2.14.2	(L1) Ensure 'Relaunch notification' sets 'Time Period (hours)' to '168 or less' and 'Initial quiet period (hours)' to less than 'Time Period (hours)'	☐	☐
2.14.3	(L1) Ensure 'Relaunch notification' is set to 'Show notification recommending relaunch'	☐	☐
2.15.1	(L1) Ensure 'Variations' is set to 'Enable Chrome variations'	☐	☐
3.1.4	(L1) Ensure 'Chrome Web Store unpublished extensions' Is Set to 'Disable unpublished extensions'	☐	☐

Appendix: CIS Controls v7 IG 2 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
2.1.1	(L2) Ensure 'Browser sign in settings' is set to 'Disabled browser sign-in'	☐	☐
2.1.2	(L1) Ensure 'Azure Cloud Authentication' Is Set to 'Enable Azure cloud authentication'	☐	☐
2.2.1	(L2) Ensure 'Manifest v2 extension availability' Is Set to 'Enable force-installed manifest v2 extensions on the sign-in screen'	☐	☐
2.3.1	(L1) Ensure 'Site isolation' is set to 'Require Site Isolation for all websites, as well as any origins below'	☐	☐
2.4.1	(L1) Ensure 'Password manager' is Explicitly Configured	☐	☐
2.4.3	(L1) Ensure 'Post-quantum TLS' Is Set to 'Allow post-quantum key agreement in TLS connections'	☐	☐
2.4.5	(L1) Ensure 'Browser history' is set to 'Always save browser history'	☐	☐
2.4.6	(L1) Ensure 'Clear browser history' Is Set to 'Do not allow clearing history in settings menu'	☐	☐
2.4.7	(L1) Ensure 'Force ephemeral mode' is set to 'Do not erase local user data'	☐	☐
2.4.9	(L1) Ensure 'Geolocation' is set to 'Do not allow sites to detect users' geolocation'	☐	☐
2.4.12	(L1) Ensure 'Renderer App Container' Is Set to 'Enable the Renderer App Container sandbox'	☐	☐
2.4.13	(L1) Ensure 'Enable leak detection for entered credentials' Is Set to 'Enable Leak detection for entered credentials'	☐	☐
2.4.14	(L1) Ensure 'Audio sandbox' is set to 'Always sandbox the audio process'	☐	☐
2.4.15	(L1) Ensure 'Unsupported system warning' is set to 'Allow Chrome to display warnings when running on an unsupported system'	☐	☐

Recommendation		Set Correctly	
		Yes	No
2.4.18	(L1) Ensure 'Command-line flags' is set to 'Show security warnings when potentially dangerous command-line flags are used'	☐	☐
2.4.20	(L1) Ensure 'TLS encrypted ClientHello' Is 'Enable the TLS Encrypted ClientHello experiment'	☐	☐
2.4.21	(L1) Ensure 'Strict MIME type checking for worker scripts' Is Set to 'Require a JavaScript MIME type for worker scripts'	☐	☐
2.4.23	(L1) Ensure 'File/directory picker without user gesture' Is Not Set	☐	☐
2.6.2	(L2) Ensure 'Supported authentication schemes' is set to 'NTLM' and 'Negotiate'	☐	☐
2.6.3	(L2) Ensure 'SSL error override' is set to 'Block users from clicking through SSL warnings'	☐	☐
2.6.4	(L1) Ensure 'WebRTC ICE candidate URLs for local IPs' Is Not Set	☐	☐
2.6.8	(L1) Ensure 'HSTS policy bypass list' is Not Set	☐	☐
2.6.9	(L1) Ensure 'DNS interception checks enabled' is set to 'Perform DNS interception checks '	☐	☐
2.6.10	(L1) Ensure 'Network service sandbox' Is Set to 'Enable the network sandbox'	☐	☐
2.6.12	(L1) Ensure 'Automatic HTTPS upgrades' Is Set to 'Allow HTTPS upgrades'	☐	☐
2.7.1	(L1) Ensure 'Import autofill data' is set to 'Disable imports of autofill data'	☐	☐
2.7.2	(L1) Ensure 'Import homepage' is set to 'Disable imports of homepage'	☐	☐
2.7.3	(L1) Ensure 'Import saved passwords' is set to 'Disable imports of saved passwords'	☐	☐
2.7.4	(L1) Ensure 'Import search engines' is set to 'Disable imports of search engines'	☐	☐
2.8.2	(L1) Ensure 'Cast' is set to 'Do not allow users to cast'	☐	☐
2.8.3	(L1) Ensure 'Clipboard' Is Set to 'Do not allow any site to use the clipboard site permission'	☐	☐
2.8.4	(L1) Ensure 'Enable URL-keyed anonymized data collection' is set to 'Data collection is never active'	☐	☐

Recommendation		Set Correctly	
		Yes	No
2.8.5	(L1) Ensure 'Third-party cookie blocking' is set to 'Disallow third-party cookies'	☐	☐
2.8.6	(L1) Ensure 'Cast' is set to 'Do not allow users to Cast'	☐	☐
2.8.8	(L2) Ensure 'SafeSearch and Restricted Mode' is set to 'Always use Safe Search for Google Web Search queries'	☐	☐
2.8.10	(L1) Ensure 'Allow local file access to file:// URLs on these sites in the PDF Viewer' Is Not Set	☐	☐
2.8.12	(L2) Ensure 'WebUSB API' is set to 'Do not allow any site to request access to USB devices via the WebUSB API'	☐	☐
2.8.13	(L1) Ensure 'Allow third-party partitioning to be enabled' in 'Third-party storage partitioning' Is Configured	☐	☐
2.8.14	(L2) Ensure 'Third-party storage partitioning' Is Set to 'Block third-party storage partitioning from being enabled'	☐	☐
2.8.15	(L2) Ensure 'Web Bluetooth API' is set to 'Do not allow any site to request access to Bluetooth devices via the Web Bluetooth API'	☐	☐
2.8.16	(L1) Ensure 'Control use of insecure content exceptions' is set to 'Do not allow any site to load mixed content'	☐	☐
2.9.2	(L2) Ensure 'Browser guest mode' is set to 'Prevent guest browser logins'	☐	☐
2.9.3	(L1) Ensure 'Credit card form Autofill' is set to 'Never Autofill credit card forms'	☐	☐
2.9.4	(L2) Ensure 'Address form Autofill' is set to 'Never Autofill address forms'	☐	☐
2.9.5	(L1) Ensure 'Allow user feedback' is set to 'Do not allow user feedback'	☐	☐
2.9.7	(L2) Ensure 'Google Translate' is set to 'Never offer translation'	☐	☐
2.9.8	(L1) Ensure 'Spell check service' is set to 'Disable the spell checking web service'	☐	☐
2.9.10	(L1) Ensure 'Alternate error pages' is set to 'Never use alternate error pages'	☐	☐
2.9.11	(L1) Ensure 'Payment methods' is set to 'Always tell websites that no payment methods are saved'	☐	☐

Recommendation		Set Correctly	
		Yes	No
2.10.1	(L2) Ensure 'Search suggest' is set to 'Never allow users to use Search Suggest'	☐	☐
2.10.2	(L1) Ensure 'Side Panel search' Is Set to 'Disable Side Panel search on all web pages'	☐	☐
2.11.1	(L1) Ensure 'Enterprise Hardware Platform API' is set to 'Do not allow managed extensions to use the Enterprise Hardware Platform API'	☐	☐
2.11.2	(L2) Ensure 'Video input (camera)' is set to 'Disable camera input for websites and apps'	☐	☐
2.11.3	(L2) Ensure 'Audio input (microphone)' is set to 'Disable audio input'	☐	☐
2.11.4	(L2) Ensure 'Sensors' is set to 'Do not allow any site to access sensors'	☐	☐
2.11.5	(L2) Ensure 'Web Serial API' is set to 'Do not allow any site to request access to serial ports via the Web Serial API'	☐	☐
2.12.1	(L1) Ensure no URLs Are Configured in 'Safe Browsing allowed domains'	☐	☐
2.12.2	(L1) Ensure 'Safe Browsing for trusted sources' is set to 'Perform Safe Browsing checks on all downloaded files'	☐	☐
2.12.3	(L1) Ensure 'Disable bypassing Safe Browsing warnings' is set to 'Do not allow user to bypass Safe Browsing warning'	☐	☐
2.12.4	(L1) Ensure 'Download restrictions' is set to 'Block malicious downloads'	☐	☐
2.12.5	(L1) Ensure 'Suppress lookalike domain warnings on domains' is Not Set	☐	☐
2.12.6	(L2) Ensure 'SafeSites URL filter' is set to 'Filter top level sites (but not embedded iframes) for adult content'	☐	☐
2.12.7	(L1) Ensure 'Safe Browsing protection' is set to 'Safe Browsing is active in the standard mode' and 'Allow higher-protection proxied lookups'	☐	☐
2.13.1	Ensure 'Generative AI policy defaults' Is Set to 'Allow GenAI features without improving AI models'	☐	☐
2.13.2	Ensure 'Help me write' Is Set to 'Use the value specified in the Generative AI policy defaults setting'	☐	☐

Recommendation		Set Correctly	
		Yes	No
2.13.3	Ensure 'DevTools AI features' Is Set to 'Use the value specified in the Generative AI policy defaults setting'	☐	☐
2.13.4	Ensure 'History search settings' Is Set to 'Use the value specified in the Generative AI policy defaults setting'	☐	☐
2.13.5	Ensure 'Tab compare' Is Set to 'Use the value specified in the Generative AI policy defaults setting'	☐	☐
2.13.6	Ensure 'Help me read' Is Set to 'Use the value specified in the Generative AI policy defaults setting'	☐	☐
2.14.1	(L1) Ensure 'Component updates' is set to 'Enable updates for all components'	☐	☐
2.14.2	(L1) Ensure 'Relaunch notification' sets 'Time Period (hours)' to '168 or less' and 'Initial quiet period (hours)' to less than 'Time Period (hours)'	☐	☐
2.14.3	(L1) Ensure 'Relaunch notification' is set to 'Show notification recommending relaunch'	☐	☐
2.15.1	(L1) Ensure 'Variations' is set to 'Enable Chrome variations'	☐	☐
2.16.1	(L1) Ensure 'Google time service' is set to 'Allow queries to a Google server to retrieve an accurate timestamp'	☐	☐
2.16.2	(L1) Ensure 'Disk cache size in bytes' in 'Disk cache size' is set to `250609664`	☐	☐
2.16.4	(L1) Ensure 'Metrics reporting' is set to 'Do not send anonymous reports of usage and crash-related data to Google'	☐	☐
2.16.5	(L1) Ensure 'Chrome Sync and Roaming Profiles (Chrome Browser - Cloud Managed)' is set to 'Disallow Sync'	☐	☐
2.16.6	(L1) Ensure 'Allow reporting of domain reliability related data' Is 'Never send domain reliability data to Google'	☐	☐
2.16.7	(L2) Ensure 'Prohibited Native Messaging hosts' in 'Native Messaging blocked hosts' is set to '*'	☐	☐
2.16.8	(L1) Ensure 'Background mode' is set to 'Disable background mode'	☐	☐
3.1.1	(L1) Ensure 'External extensions' is set to 'Block external extensions from being installed'	☐	☐

Recommendation		Set Correctly	
		Yes	No
3.1.2	(L1) Ensure 'Allowed types of apps and extensions' is set to 'Extension', 'Hosted App', 'Chrome Packaged App', and 'Theme'	☐	☐
3.1.3	(L1) Ensure 'App and extension install sources' Is Not Set	☐	☐
3.1.4	(L1) Ensure 'Chrome Web Store unpublished extensions' Is Set to 'Disable unpublished extensions'	☐	☐

Appendix: CIS Controls v7 IG 3 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
2.1.1	(L2) Ensure 'Browser sign in settings' is set to 'Disabled browser sign-in'	☐	☐
2.1.2	(L1) Ensure 'Azure Cloud Authentication' Is Set to 'Enable Azure cloud authentication'	☐	☐
2.2.1	(L2) Ensure 'Manifest v2 extension availability' Is Set to 'Enable force-installed manifest v2 extensions on the sign-in screen'	☐	☐
2.3.1	(L1) Ensure 'Site isolation' is set to 'Require Site Isolation for all websites, as well as any origins below'	☐	☐
2.4.1	(L1) Ensure 'Password manager' is Explicitly Configured	☐	☐
2.4.3	(L1) Ensure 'Post-quantum TLS' Is Set to 'Allow post-quantum key agreement in TLS connections'	☐	☐
2.4.5	(L1) Ensure 'Browser history' is set to 'Always save browser history'	☐	☐
2.4.6	(L1) Ensure 'Clear browser history' Is Set to 'Do not allow clearing history in settings menu'	☐	☐
2.4.7	(L1) Ensure 'Force ephemeral mode' is set to 'Do not erase local user data'	☐	☐
2.4.9	(L1) Ensure 'Geolocation' is set to 'Do not allow sites to detect users' geolocation'	☐	☐
2.4.12	(L1) Ensure 'Renderer App Container' Is Set to 'Enable the Renderer App Container sandbox'	☐	☐
2.4.13	(L1) Ensure 'Enable leak detection for entered credentials' Is Set to 'Enable Leak detection for entered credentials'	☐	☐
2.4.14	(L1) Ensure 'Audio sandbox' is set to 'Always sandbox the audio process'	☐	☐
2.4.15	(L1) Ensure 'Unsupported system warning' is set to 'Allow Chrome to display warnings when running on an unsupported system'	☐	☐

Recommendation		Set Correctly	
		Yes	No
2.4.18	(L1) Ensure 'Command-line flags' is set to 'Show security warnings when potentially dangerous command-line flags are used'	☐	☐
2.4.20	(L1) Ensure 'TLS encrypted ClientHello' Is 'Enable the TLS Encrypted ClientHello experiment'	☐	☐
2.4.21	(L1) Ensure 'Strict MIME type checking for worker scripts' Is Set to 'Require a JavaScript MIME type for worker scripts'	☐	☐
2.4.23	(L1) Ensure 'File/directory picker without user gesture' Is Not Set	☐	☐
2.5.1	(L1) Ensure 'Remote access hosts' is set with a domain defined in 'Remote access host domain'	☐	☐
2.5.2	(L1) Ensure 'Firewall traversal' is set to 'Disable firewall traversal'	☐	☐
2.5.3	(L1) Ensure 'Firewall traversal' is set to 'Disable the use of relay servers'	☐	☐
2.5.4	(L1) Ensure 'Remote support connections' is set to 'Prevent remote support connections'	☐	☐
2.6.1	(L1) Ensure 'Proxy mode' is Not Set to 'Always auto detect the proxy'	☐	☐
2.6.2	(L2) Ensure 'Supported authentication schemes' is set to 'NTLM' and 'Negotiate'	☐	☐
2.6.3	(L2) Ensure 'SSL error override' is set to 'Block users from clicking through SSL warnings'	☐	☐
2.6.4	(L1) Ensure 'WebRTC ICE candidate URLs for local IPs' Is Not Set	☐	☐
2.6.8	(L1) Ensure 'HSTS policy bypass list' is Not Set	☐	☐
2.6.9	(L1) Ensure 'DNS interception checks enabled' is set to 'Perform DNS interception checks '	☐	☐
2.6.10	(L1) Ensure 'Network service sandbox' Is Set to 'Enable the network sandbox'	☐	☐
2.6.11	(L1) Ensure 'Http Allowlist' Is Properly Configured	☐	☐
2.6.12	(L1) Ensure 'Automatic HTTPS upgrades' Is Set to 'Allow HTTPS upgrades'	☐	☐
2.7.1	(L1) Ensure 'Import autofill data' is set to 'Disable imports of autofill data'	☐	☐

Recommendation		Set Correctly	
		Yes	No
2.7.2	(L1) Ensure 'Import homepage' is set to 'Disable imports of homepage'	☐	☐
2.7.3	(L1) Ensure 'Import saved passwords' is set to 'Disable imports of saved passwords'	☐	☐
2.7.4	(L1) Ensure 'Import search engines' is set to 'Disable imports of search engines'	☐	☐
2.8.2	(L1) Ensure 'Cast' is set to 'Do not allow users to cast'	☐	☐
2.8.3	(L1) Ensure 'Clipboard' Is Set to 'Do not allow any site to use the clipboard site permission'	☐	☐
2.8.4	(L1) Ensure 'Enable URL-keyed anonymized data collection' is set to 'Data collection is never active'	☐	☐
2.8.5	(L1) Ensure 'Third-party cookie blocking' is set to 'Disallow third-party cookies'	☐	☐
2.8.6	(L1) Ensure 'Cast' is set to 'Do not allow users to Cast'	☐	☐
2.8.8	(L2) Ensure 'SafeSearch and Restricted Mode' is set to 'Always use Safe Search for Google Web Search queries'	☐	☐
2.8.10	(L1) Ensure 'Allow local file access to file:// URLs on these sites in the PDF Viewer' Is Not Set	☐	☐
2.8.12	(L2) Ensure 'WebUSB API' is set to 'Do not allow any site to request access to USB devices via the WebUSB API'	☐	☐
2.8.13	(L1) Ensure 'Allow third-party partitioning to be enabled' in 'Third-party storage partitioning' Is Configured	☐	☐
2.8.14	(L2) Ensure 'Third-party storage partitioning' Is Set to 'Block third-party storage partitioning from being enabled'	☐	☐
2.8.15	(L2) Ensure 'Web Bluetooth API' is set to 'Do not allow any site to request access to Bluetooth devices via the Web Bluetooth API'	☐	☐
2.8.16	(L1) Ensure 'Control use of insecure content exceptions' is set to 'Do not allow any site to load mixed content'	☐	☐
2.9.2	(L2) Ensure 'Browser guest mode' is set to 'Prevent guest browser logins'	☐	☐
2.9.3	(L1) Ensure 'Credit card form Autofill' is set to 'Never Autofill credit card forms'	☐	☐
2.9.4	(L2) Ensure 'Address form Autofill' is set to 'Never Autofill address forms'	☐	☐

Recommendation		Set Correctly	
		Yes	No
2.9.5	(L1) Ensure 'Allow user feedback' is set to 'Do not allow user feedback'	☐	☐
2.9.6	(L2) Ensure 'File selection dialogs' is set to 'Block file selection dialogs'	☐	☐
2.9.7	(L2) Ensure 'Google Translate' is set to 'Never offer translation'	☐	☐
2.9.8	(L1) Ensure 'Spell check service' is set to 'Disable the spell checking web service'	☐	☐
2.9.10	(L1) Ensure 'Alternate error pages' is set to 'Never use alternate error pages'	☐	☐
2.9.11	(L1) Ensure 'Payment methods' is set to 'Always tell websites that no payment methods are saved'	☐	☐
2.10.1	(L2) Ensure 'Search suggest' is set to 'Never allow users to use Search Suggest'	☐	☐
2.10.2	(L1) Ensure 'Side Panel search' Is Set to 'Disable Side Panel search on all web pages'	☐	☐
2.11.1	(L1) Ensure 'Enterprise Hardware Platform API' is set to 'Do not allow managed extensions to use the Enterprise Hardware Platform API'	☐	☐
2.11.2	(L2) Ensure 'Video input (camera)' is set to 'Disable camera input for websites and apps'	☐	☐
2.11.3	(L2) Ensure 'Audio input (microphone)' is set to 'Disable audio input'	☐	☐
2.11.4	(L2) Ensure 'Sensors' is set to 'Do not allow any site to access sensors'	☐	☐
2.11.5	(L2) Ensure 'Web Serial API' is set to 'Do not allow any site to request access to serial ports via the Web Serial API'	☐	☐
2.12.1	(L1) Ensure no URLs Are Configured in 'Safe Browsing allowed domains'	☐	☐
2.12.2	(L1) Ensure 'Safe Browsing for trusted sources' is set to 'Perform Safe Browsing checks on all downloaded files'	☐	☐
2.12.3	(L1) Ensure 'Disable bypassing Safe Browsing warnings' is set to 'Do not allow user to bypass Safe Browsing warning'	☐	☐
2.12.4	(L1) Ensure 'Download restrictions' is set to 'Block malicious downloads'	☐	☐

Recommendation		Set Correctly	
		Yes	No
2.12.5	(L1) Ensure 'Suppress lookalike domain warnings on domains' is Not Set	☐	☐
2.12.6	(L2) Ensure 'SafeSites URL filter' is set to 'Filter top level sites (but not embedded iframes) for adult content'	☐	☐
2.12.7	(L1) Ensure 'Safe Browsing protection' is set to 'Safe Browsing is active in the standard mode' and 'Allow higher-protection proxied lookups'	☐	☐
2.13.1	Ensure 'Generative AI policy defaults' Is Set to 'Allow GenAI features without improving AI models'	☐	☐
2.13.2	Ensure 'Help me write' Is Set to 'Use the value specified in the Generative AI policy defaults setting'	☐	☐
2.13.3	Ensure 'DevTools AI features' Is Set to 'Use the value specified in the Generative AI policy defaults setting'	☐	☐
2.13.4	Ensure 'History search settings' Is Set to 'Use the value specified in the Generative AI policy defaults setting'	☐	☐
2.13.5	Ensure 'Tab compare' Is Set to 'Use the value specified in the Generative AI policy defaults setting'	☐	☐
2.13.6	Ensure 'Help me read' Is Set to 'Use the value specified in the Generative AI policy defaults setting'	☐	☐
2.14.1	(L1) Ensure 'Component updates' is set to 'Enable updates for all components'	☐	☐
2.14.2	(L1) Ensure 'Relaunch notification' sets 'Time Period (hours)' to '168 or less' and 'Initial quiet period (hours)' to less than 'Time Period (hours)'	☐	☐
2.14.3	(L1) Ensure 'Relaunch notification' is set to 'Show notification recommending relaunch'	☐	☐
2.15.1	(L1) Ensure 'Variations' is set to 'Enable Chrome variations'	☐	☐
2.16.1	(L1) Ensure 'Google time service' is set to 'Allow queries to a Google server to retrieve an accurate timestamp'	☐	☐
2.16.2	(L1) Ensure 'Disk cache size in bytes' in 'Disk cache size' is set to '250609664'	☐	☐
2.16.4	(L1) Ensure 'Metrics reporting' is set to 'Do not send anonymous reports of usage and crash-related data to Google'	☐	☐

Recommendation		Set Correctly	
		Yes	No
2.16.5	(L1) Ensure 'Chrome Sync and Roaming Profiles (Chrome Browser - Cloud Managed)' is set to 'Disallow Sync'	☐	☐
2.16.6	(L1) Ensure 'Allow reporting of domain reliability related data' Is 'Never send domain reliability data to Google'	☐	☐
2.16.7	(L2) Ensure 'Prohibited Native Messaging hosts' in 'Native Messaging blocked hosts' is set to '*'	☐	☐
2.16.8	(L1) Ensure 'Background mode' is set to 'Disable background mode'	☐	☐
3.1.1	(L1) Ensure 'External extensions' is set to 'Block external extensions from being installed'	☐	☐
3.1.2	(L1) Ensure 'Allowed types of apps and extensions' is set to 'Extension', 'Hosted App', 'Chrome Packaged App', and 'Theme'	☐	☐
3.1.3	(L1) Ensure 'App and extension install sources' Is Not Set	☐	☐
3.1.4	(L1) Ensure 'Chrome Web Store unpublished extensions' Is Set to 'Disable unpublished extensions'	☐	☐

Appendix: CIS Controls v7 Unmapped Recommendations

Recommendation		Set Correctly	
		Yes	No
2.4.2	(L1) Ensure 'Web Authentication requests on sites with broken TLS certificates' Is Set to 'Do not allow WebAuthn API requests on sites with broken TLS certificates'	☐	☐
2.4.19	(L1) Ensure 'Allow remote debugging' is set to 'Do not allow use of the remote debugging'	☐	☐
2.6.5	(L2) Ensure 'DNS over HTTPS' is set to 'Enable DNS-over-HTTPS without insecure fallback'	☐	☐

Appendix: CIS Controls v8 IG 1 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
2.1.1	(L2) Ensure 'Browser sign in settings' is set to 'Disabled browser sign-in'	☐	☐
2.1.2	(L1) Ensure 'Azure Cloud Authentication' Is Set to 'Enable Azure cloud authentication'	☐	☐
2.2.1	(L2) Ensure 'Manifest v2 extension availability' Is Set to 'Enable force-installed manifest v2 extensions on the sign-in screen'	☐	☐
2.3.1	(L1) Ensure 'Site isolation' is set to 'Require Site Isolation for all websites, as well as any origins below'	☐	☐
2.4.1	(L1) Ensure 'Password manager' is Explicitly Configured	☐	☐
2.4.2	(L1) Ensure 'Web Authentication requests on sites with broken TLS certificates' Is Set to 'Do not allow WebAuthn API requests on sites with broken TLS certificates'	☐	☐
2.4.6	(L1) Ensure 'Clear browser history' Is Set to 'Do not allow clearing history in settings menu'	☐	☐
2.4.7	(L1) Ensure 'Force ephemeral mode' is set to 'Do not erase local user data'	☐	☐
2.4.12	(L1) Ensure 'Renderer App Container' Is Set to 'Enable the Renderer App Container sandbox'	☐	☐
2.4.13	(L1) Ensure 'Enable leak detection for entered credentials' Is Set to 'Enable Leak detection for entered credentials'	☐	☐
2.4.14	(L1) Ensure 'Audio sandbox' is set to 'Always sandbox the audio process'	☐	☐
2.4.15	(L1) Ensure 'Unsupported system warning' is set to 'Allow Chrome to display warnings when running on an unsupported system'	☐	☐
2.4.18	(L1) Ensure 'Command-line flags' is set to 'Show security warnings when potentially dangerous command-line flags are used'	☐	☐
2.4.19	(L1) Ensure 'Allow remote debugging' is set to 'Do not allow use of the remote debugging'	☐	☐

Recommendation		Set Correctly	
		Yes	No
2.4.23	(L1) Ensure 'File/directory picker without user gesture' Is Not Set	☐	☐
2.6.4	(L1) Ensure 'WebRTC ICE candidate URLs for local IPs' Is Not Set	☐	☐
2.6.5	(L2) Ensure 'DNS over HTTPS' is set to 'Enable DNS-over-HTTPS without insecure fallback'	☐	☐
2.6.10	(L1) Ensure 'Network service sandbox' Is Set to 'Enable the network sandbox'	☐	☐
2.6.12	(L1) Ensure 'Automatic HTTPS upgrades' Is Set to 'Allow HTTPS upgrades'	☐	☐
2.7.1	(L1) Ensure 'Import autofill data' is set to 'Disable imports of autofill data'	☐	☐
2.7.2	(L1) Ensure 'Import homepage' is set to 'Disable imports of homepage'	☐	☐
2.7.3	(L1) Ensure 'Import saved passwords' is set to 'Disable imports of saved passwords'	☐	☐
2.7.4	(L1) Ensure 'Import search engines' is set to 'Disable imports of search engines'	☐	☐
2.8.3	(L1) Ensure 'Clipboard' Is Set to 'Do not allow any site to use the clipboard site permission'	☐	☐
2.8.5	(L1) Ensure 'Third-party cookie blocking' is set to 'Disallow third-party cookies'	☐	☐
2.8.9	(L1) Ensure 'First-Party Sets' Is Set to 'Disable First-Party Sets for all affected users'	☐	☐
2.8.10	(L1) Ensure 'Allow local file access to file:// URLs on these sites in the PDF Viewer' Is Not Set	☐	☐
2.8.13	(L1) Ensure 'Allow third-party partitioning to be enabled' in 'Third-party storage partitioning' Is Configured	☐	☐
2.8.14	(L2) Ensure 'Third-party storage partitioning' Is Set to 'Block third-party storage partitioning from being enabled'	☐	☐
2.9.2	(L2) Ensure 'Browser guest mode' is set to 'Prevent guest browser logins'	☐	☐
2.9.3	(L1) Ensure 'Credit card form Autofill' is set to 'Never Autofill credit card forms'	☐	☐
2.9.4	(L2) Ensure 'Address form Autofill' is set to 'Never Autofill address forms'	☐	☐

Recommendation		Set Correctly	
		Yes	No
2.9.5	(L1) Ensure 'Allow user feedback' is set to 'Do not allow user feedback'	☐	☐
2.9.7	(L2) Ensure 'Google Translate' is set to 'Never offer translation'	☐	☐
2.9.8	(L1) Ensure 'Spell check service' is set to 'Disable the spell checking web service'	☐	☐
2.9.10	(L1) Ensure 'Alternate error pages' is set to 'Never use alternate error pages'	☐	☐
2.9.11	(L1) Ensure 'Payment methods' is set to 'Always tell websites that no payment methods are saved'	☐	☐
2.10.1	(L2) Ensure 'Search suggest' is set to 'Never allow users to use Search Suggest'	☐	☐
2.10.2	(L1) Ensure 'Side Panel search' Is Set to 'Disable Side Panel search on all web pages'	☐	☐
2.11.2	(L2) Ensure 'Video input (camera)' is set to 'Disable camera input for websites and apps'	☐	☐
2.11.3	(L2) Ensure 'Audio input (microphone)' is set to 'Disable audio input'	☐	☐
2.12.2	(L1) Ensure 'Safe Browsing for trusted sources' is set to 'Perform Safe Browsing checks on all downloaded files'	☐	☐
2.12.4	(L1) Ensure 'Download restrictions' is set to 'Block malicious downloads'	☐	☐
2.14.1	(L1) Ensure 'Component updates' is set to 'Enable updates for all components'	☐	☐
2.14.2	(L1) Ensure 'Relaunch notification' sets 'Time Period (hours)' to '168 or less' and 'Initial quiet period (hours)' to less than 'Time Period (hours)'	☐	☐
2.14.3	(L1) Ensure 'Relaunch notification' is set to 'Show notification recommending relaunch'	☐	☐
2.15.1	(L1) Ensure 'Variations' is set to 'Enable Chrome variations'	☐	☐
2.16.2	(L1) Ensure 'Disk cache size in bytes' in 'Disk cache size' is set to `250609664`	☐	☐
2.16.4	(L1) Ensure 'Metrics reporting' is set to 'Do not send anonymous reports of usage and crash-related data to Google'	☐	☐

Recommendation		Set Correctly	
		Yes	No
2.16.5	(L1) Ensure 'Chrome Sync and Roaming Profiles (Chrome Browser - Cloud Managed)' is set to 'Disallow Sync'	☐	☐
2.16.6	(L1) Ensure 'Allow reporting of domain reliability related data' Is 'Never send domain reliability data to Google'	☐	☐
3.1.4	(L1) Ensure 'Chrome Web Store unpublished extensions' Is Set to 'Disable unpublished extensions'	☐	☐

Appendix: CIS Controls v8 IG 2 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
2.1.1	(L2) Ensure 'Browser sign in settings' is set to 'Disabled browser sign-in'	☐	☐
2.1.2	(L1) Ensure 'Azure Cloud Authentication' Is Set to 'Enable Azure cloud authentication'	☐	☐
2.2.1	(L2) Ensure 'Manifest v2 extension availability' Is Set to 'Enable force-installed manifest v2 extensions on the sign-in screen'	☐	☐
2.3.1	(L1) Ensure 'Site isolation' is set to 'Require Site Isolation for all websites, as well as any origins below'	☐	☐
2.4.1	(L1) Ensure 'Password manager' is Explicitly Configured	☐	☐
2.4.2	(L1) Ensure 'Web Authentication requests on sites with broken TLS certificates' Is Set to 'Do not allow WebAuthn API requests on sites with broken TLS certificates'	☐	☐
2.4.3	(L1) Ensure 'Post-quantum TLS' Is Set to 'Allow post-quantum key agreement in TLS connections'	☐	☐
2.4.6	(L1) Ensure 'Clear browser history' Is Set to 'Do not allow clearing history in settings menu'	☐	☐
2.4.7	(L1) Ensure 'Force ephemeral mode' is set to 'Do not erase local user data'	☐	☐
2.4.12	(L1) Ensure 'Renderer App Container' Is Set to 'Enable the Renderer App Container sandbox'	☐	☐
2.4.13	(L1) Ensure 'Enable leak detection for entered credentials' Is Set to 'Enable Leak detection for entered credentials'	☐	☐
2.4.14	(L1) Ensure 'Audio sandbox' is set to 'Always sandbox the audio process'	☐	☐
2.4.15	(L1) Ensure 'Unsupported system warning' is set to 'Allow Chrome to display warnings when running on an unsupported system'	☐	☐
2.4.18	(L1) Ensure 'Command-line flags' is set to 'Show security warnings when potentially dangerous command-line flags are used'	☐	☐

Recommendation		Set Correctly	
		Yes	No
2.4.19	(L1) Ensure 'Allow remote debugging' is set to 'Do not allow use of the remote debugging'	☐	☐
2.4.20	(L1) Ensure 'TLS encrypted ClientHello' Is 'Enable the TLS Encrypted ClientHello experiment'	☐	☐
2.4.21	(L1) Ensure 'Strict MIME type checking for worker scripts' Is Set to 'Require a JavaScript MIME type for worker scripts'	☐	☐
2.4.23	(L1) Ensure 'File/directory picker without user gesture' Is Not Set	☐	☐
2.5.1	(L1) Ensure 'Remote access hosts' is set with a domain defined in 'Remote access host domain'	☐	☐
2.5.2	(L1) Ensure 'Firewall traversal' is set to 'Disable firewall traversal'	☐	☐
2.5.3	(L1) Ensure 'Firewall traversal' is set to 'Disable the use of relay servers'	☐	☐
2.5.4	(L1) Ensure 'Remote support connections' is set to 'Prevent remote support connections'	☐	☐
2.6.2	(L2) Ensure 'Supported authentication schemes' is set to 'NTLM' and 'Negotiate'	☐	☐
2.6.3	(L2) Ensure 'SSL error override' is set to 'Block users from clicking through SSL warnings'	☐	☐
2.6.4	(L1) Ensure 'WebRTC ICE candidate URLs for local IPs' Is Not Set	☐	☐
2.6.5	(L2) Ensure 'DNS over HTTPS' is set to 'Enable DNS-over-HTTPS without insecure fallback'	☐	☐
2.6.8	(L1) Ensure 'HSTS policy bypass list' is Not Set	☐	☐
2.6.9	(L1) Ensure 'DNS interception checks enabled' is set to 'Perform DNS interception checks '	☐	☐
2.6.10	(L1) Ensure 'Network service sandbox' Is Set to 'Enable the network sandbox'	☐	☐
2.6.12	(L1) Ensure 'Automatic HTTPS upgrades' Is Set to 'Allow HTTPS upgrades'	☐	☐
2.7.1	(L1) Ensure 'Import autofill data' is set to 'Disable imports of autofill data'	☐	☐
2.7.2	(L1) Ensure 'Import homepage' is set to 'Disable imports of homepage'	☐	☐

Recommendation		Set Correctly	
		Yes	No
2.7.3	(L1) Ensure 'Import saved passwords' is set to 'Disable imports of saved passwords'	☐	☐
2.7.4	(L1) Ensure 'Import search engines' is set to 'Disable imports of search engines'	☐	☐
2.8.2	(L1) Ensure 'Cast' is set to 'Do not allow users to cast'	☐	☐
2.8.3	(L1) Ensure 'Clipboard' Is Set to 'Do not allow any site to use the clipboard site permission'	☐	☐
2.8.5	(L1) Ensure 'Third-party cookie blocking' is set to 'Disallow third-party cookies'	☐	☐
2.8.6	(L1) Ensure 'Cast' is set to 'Do not allow users to Cast'	☐	☐
2.8.8	(L2) Ensure 'SafeSearch and Restricted Mode' is set to 'Always use Safe Search for Google Web Search queries'	☐	☐
2.8.9	(L1) Ensure 'First-Party Sets' Is Set to 'Disable First-Party Sets for all affected users'	☐	☐
2.8.10	(L1) Ensure 'Allow local file access to file:// URLs on these sites in the PDF Viewer' Is Not Set	☐	☐
2.8.12	(L2) Ensure 'WebUSB API' is set to 'Do not allow any site to request access to USB devices via the WebUSB API'	☐	☐
2.8.13	(L1) Ensure 'Allow third-party partitioning to be enabled' in 'Third-party storage partitioning' Is Configured	☐	☐
2.8.14	(L2) Ensure 'Third-party storage partitioning' Is Set to 'Block third-party storage partitioning from being enabled'	☐	☐
2.8.15	(L2) Ensure 'Web Bluetooth API' is set to 'Do not allow any site to request access to Bluetooth devices via the Web Bluetooth API'	☐	☐
2.8.16	(L1) Ensure 'Control use of insecure content exceptions' is set to 'Do not allow any site to load mixed content'	☐	☐
2.9.2	(L2) Ensure 'Browser guest mode' is set to 'Prevent guest browser logins'	☐	☐
2.9.3	(L1) Ensure 'Credit card form Autofill' is set to 'Never Autofill credit card forms'	☐	☐
2.9.4	(L2) Ensure 'Address form Autofill' is set to 'Never Autofill address forms'	☐	☐
2.9.5	(L1) Ensure 'Allow user feedback' is set to 'Do not allow user feedback'	☐	☐

Recommendation		Set Correctly	
		Yes	No
2.9.7	(L2) Ensure 'Google Translate' is set to 'Never offer translation'	☐	☐
2.9.8	(L1) Ensure 'Spell check service' is set to 'Disable the spell checking web service'	☐	☐
2.9.10	(L1) Ensure 'Alternate error pages' is set to 'Never use alternate error pages'	☐	☐
2.9.11	(L1) Ensure 'Payment methods' is set to 'Always tell websites that no payment methods are saved'	☐	☐
2.10.1	(L2) Ensure 'Search suggest' is set to 'Never allow users to use Search Suggest'	☐	☐
2.10.2	(L1) Ensure 'Side Panel search' Is Set to 'Disable Side Panel search on all web pages'	☐	☐
2.11.1	(L1) Ensure 'Enterprise Hardware Platform API' is set to 'Do not allow managed extensions to use the Enterprise Hardware Platform API'	☐	☐
2.11.2	(L2) Ensure 'Video input (camera)' is set to 'Disable camera input for websites and apps'	☐	☐
2.11.3	(L2) Ensure 'Audio input (microphone)' is set to 'Disable audio input'	☐	☐
2.11.4	(L2) Ensure 'Sensors' is set to 'Do not allow any site to access sensors'	☐	☐
2.11.5	(L2) Ensure 'Web Serial API' is set to 'Do not allow any site to request access to serial ports via the Web Serial API'	☐	☐
2.12.1	(L1) Ensure no URLs Are Configured in 'Safe Browsing allowed domains'	☐	☐
2.12.2	(L1) Ensure 'Safe Browsing for trusted sources' is set to 'Perform Safe Browsing checks on all downloaded files'	☐	☐
2.12.3	(L1) Ensure 'Disable bypassing Safe Browsing warnings' is set to 'Do not allow user to bypass Safe Browsing warning'	☐	☐
2.12.4	(L1) Ensure 'Download restrictions' is set to 'Block malicious downloads'	☐	☐
2.12.5	(L1) Ensure 'Suppress lookalike domain warnings on domains' is Not Set	☐	☐
2.12.6	(L2) Ensure 'SafeSites URL filter' is set to 'Filter top level sites (but not embedded iframes) for adult content'	☐	☐

Recommendation		Set Correctly	
		Yes	No
2.12.7	(L1) Ensure 'Safe Browsing protection' is set to 'Safe Browsing is active in the standard mode' and 'Allow higher-protection proxied lookups'	☐	☐
2.13.1	Ensure 'Generative AI policy defaults' Is Set to 'Allow GenAI features without improving AI models'	☐	☐
2.13.2	Ensure 'Help me write' Is Set to 'Use the value specified in the Generative AI policy defaults setting'	☐	☐
2.13.3	Ensure 'DevTools AI features' Is Set to 'Use the value specified in the Generative AI policy defaults setting'	☐	☐
2.13.4	Ensure 'History search settings' Is Set to 'Use the value specified in the Generative AI policy defaults setting'	☐	☐
2.13.5	Ensure 'Tab compare' Is Set to 'Use the value specified in the Generative AI policy defaults setting'	☐	☐
2.13.6	Ensure 'Help me read' Is Set to 'Use the value specified in the Generative AI policy defaults setting'	☐	☐
2.14.1	(L1) Ensure 'Component updates' is set to 'Enable updates for all components'	☐	☐
2.14.2	(L1) Ensure 'Relaunch notification' sets 'Time Period (hours)' to '168 or less' and 'Initial quiet period (hours)' to less than 'Time Period (hours)'	☐	☐
2.14.3	(L1) Ensure 'Relaunch notification' is set to 'Show notification recommending relaunch'	☐	☐
2.15.1	(L1) Ensure 'Variations' is set to 'Enable Chrome variations'	☐	☐
2.16.1	(L1) Ensure 'Google time service' is set to 'Allow queries to a Google server to retrieve an accurate timestamp'	☐	☐
2.16.2	(L1) Ensure 'Disk cache size in bytes' in 'Disk cache size' is set to `250609664'	☐	☐
2.16.4	(L1) Ensure 'Metrics reporting' is set to 'Do not send anonymous reports of usage and crash-related data to Google'	☐	☐
2.16.5	(L1) Ensure 'Chrome Sync and Roaming Profiles (Chrome Browser - Cloud Managed)' is set to 'Disallow Sync'	☐	☐
2.16.6	(L1) Ensure 'Allow reporting of domain reliability related data' Is 'Never send domain reliability data to Google'	☐	☐

Recommendation		Set Correctly	
		Yes	No
2.16.7	(L2) Ensure 'Prohibited Native Messaging hosts' in 'Native Messaging blocked hosts' is set to '*'	☐	☐
2.16.8	(L1) Ensure 'Background mode' is set to 'Disable background mode'	☐	☐
3.1.1	(L1) Ensure 'External extensions' is set to 'Block external extensions from being installed'	☐	☐
3.1.2	(L1) Ensure 'Allowed types of apps and extensions' is set to 'Extension', 'Hosted App', 'Chrome Packaged App', and 'Theme'	☐	☐
3.1.3	(L1) Ensure 'App and extension install sources' Is Not Set	☐	☐
3.1.4	(L1) Ensure 'Chrome Web Store unpublished extensions' Is Set to 'Disable unpublished extensions'	☐	☐

Appendix: CIS Controls v8 IG 3 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
2.1.1	(L2) Ensure 'Browser sign in settings' is set to 'Disabled browser sign-in'	☐	☐
2.1.2	(L1) Ensure 'Azure Cloud Authentication' Is Set to 'Enable Azure cloud authentication'	☐	☐
2.2.1	(L2) Ensure 'Manifest v2 extension availability' Is Set to 'Enable force-installed manifest v2 extensions on the sign-in screen'	☐	☐
2.3.1	(L1) Ensure 'Site isolation' is set to 'Require Site Isolation for all websites, as well as any origins below'	☐	☐
2.4.1	(L1) Ensure 'Password manager' is Explicitly Configured	☐	☐
2.4.2	(L1) Ensure 'Web Authentication requests on sites with broken TLS certificates' Is Set to 'Do not allow WebAuthn API requests on sites with broken TLS certificates'	☐	☐
2.4.3	(L1) Ensure 'Post-quantum TLS' Is Set to 'Allow post-quantum key agreement in TLS connections'	☐	☐
2.4.6	(L1) Ensure 'Clear browser history' Is Set to 'Do not allow clearing history in settings menu'	☐	☐
2.4.7	(L1) Ensure 'Force ephemeral mode' is set to 'Do not erase local user data'	☐	☐
2.4.12	(L1) Ensure 'Renderer App Container' Is Set to 'Enable the Renderer App Container sandbox'	☐	☐
2.4.13	(L1) Ensure 'Enable leak detection for entered credentials' Is Set to 'Enable Leak detection for entered credentials'	☐	☐
2.4.14	(L1) Ensure 'Audio sandbox' is set to 'Always sandbox the audio process'	☐	☐
2.4.15	(L1) Ensure 'Unsupported system warning' is set to 'Allow Chrome to display warnings when running on an unsupported system'	☐	☐
2.4.18	(L1) Ensure 'Command-line flags' is set to 'Show security warnings when potentially dangerous command-line flags are used'	☐	☐

Recommendation		Set Correctly	
		Yes	No
2.4.19	(L1) Ensure 'Allow remote debugging' is set to 'Do not allow use of the remote debugging'	☐	☐
2.4.20	(L1) Ensure 'TLS encrypted ClientHello' Is 'Enable the TLS Encrypted ClientHello experiment'	☐	☐
2.4.21	(L1) Ensure 'Strict MIME type checking for worker scripts' Is Set to 'Require a JavaScript MIME type for worker scripts'	☐	☐
2.4.23	(L1) Ensure 'File/directory picker without user gesture' Is Not Set	☐	☐
2.5.1	(L1) Ensure 'Remote access hosts' is set with a domain defined in 'Remote access host domain'	☐	☐
2.5.2	(L1) Ensure 'Firewall traversal' is set to 'Disable firewall traversal'	☐	☐
2.5.3	(L1) Ensure 'Firewall traversal' is set to 'Disable the use of relay servers'	☐	☐
2.5.4	(L1) Ensure 'Remote support connections' is set to 'Prevent remote support connections'	☐	☐
2.6.1	(L1) Ensure 'Proxy mode' is Not Set to 'Always auto detect the proxy'	☐	☐
2.6.2	(L2) Ensure 'Supported authentication schemes' is set to 'NTLM' and 'Negotiate'	☐	☐
2.6.3	(L2) Ensure 'SSL error override' is set to 'Block users from clicking through SSL warnings'	☐	☐
2.6.4	(L1) Ensure 'WebRTC ICE candidate URLs for local IPs' Is Not Set	☐	☐
2.6.5	(L2) Ensure 'DNS over HTTPS' is set to 'Enable DNS-over-HTTPS without insecure fallback'	☐	☐
2.6.8	(L1) Ensure 'HSTS policy bypass list' is Not Set	☐	☐
2.6.9	(L1) Ensure 'DNS interception checks enabled' is set to 'Perform DNS interception checks '	☐	☐
2.6.10	(L1) Ensure 'Network service sandbox' Is Set to 'Enable the network sandbox'	☐	☐
2.6.11	(L1) Ensure 'Http Allowlist' Is Properly Configured	☐	☐
2.6.12	(L1) Ensure 'Automatic HTTPS upgrades' Is Set to 'Allow HTTPS upgrades'	☐	☐

Recommendation		Set Correctly	
		Yes	No
2.7.1	(L1) Ensure 'Import autofill data' is set to 'Disable imports of autofill data'	☐	☐
2.7.2	(L1) Ensure 'Import homepage' is set to 'Disable imports of homepage'	☐	☐
2.7.3	(L1) Ensure 'Import saved passwords' is set to 'Disable imports of saved passwords'	☐	☐
2.7.4	(L1) Ensure 'Import search engines' is set to 'Disable imports of search engines'	☐	☐
2.8.2	(L1) Ensure 'Cast' is set to 'Do not allow users to cast'	☐	☐
2.8.3	(L1) Ensure 'Clipboard' Is Set to 'Do not allow any site to use the clipboard site permission'	☐	☐
2.8.5	(L1) Ensure 'Third-party cookie blocking' is set to 'Disallow third-party cookies'	☐	☐
2.8.6	(L1) Ensure 'Cast' is set to 'Do not allow users to Cast'	☐	☐
2.8.8	(L2) Ensure 'SafeSearch and Restricted Mode' is set to 'Always use Safe Search for Google Web Search queries'	☐	☐
2.8.9	(L1) Ensure 'First-Party Sets' Is Set to 'Disable First-Party Sets for all affected users'	☐	☐
2.8.10	(L1) Ensure 'Allow local file access to file:// URLs on these sites in the PDF Viewer' Is Not Set	☐	☐
2.8.12	(L2) Ensure 'WebUSB API' is set to 'Do not allow any site to request access to USB devices via the WebUSB API'	☐	☐
2.8.13	(L1) Ensure 'Allow third-party partitioning to be enabled' in 'Third-party storage partitioning' Is Configured	☐	☐
2.8.14	(L2) Ensure 'Third-party storage partitioning' Is Set to 'Block third-party storage partitioning from being enabled'	☐	☐
2.8.15	(L2) Ensure 'Web Bluetooth API' is set to 'Do not allow any site to request access to Bluetooth devices via the Web Bluetooth API'	☐	☐
2.8.16	(L1) Ensure 'Control use of insecure content exceptions' is set to 'Do not allow any site to load mixed content'	☐	☐
2.9.2	(L2) Ensure 'Browser guest mode' is set to 'Prevent guest browser logins'	☐	☐
2.9.3	(L1) Ensure 'Credit card form Autofill' is set to 'Never Autofill credit card forms'	☐	☐

Recommendation		Set Correctly	
		Yes	No
2.9.4	(L2) Ensure 'Address form Autofill' is set to 'Never Autofill address forms'	☐	☐
2.9.5	(L1) Ensure 'Allow user feedback' is set to 'Do not allow user feedback'	☐	☐
2.9.6	(L2) Ensure 'File selection dialogs' is set to 'Block file selection dialogs'	☐	☐
2.9.7	(L2) Ensure 'Google Translate' is set to 'Never offer translation'	☐	☐
2.9.8	(L1) Ensure 'Spell check service' is set to 'Disable the spell checking web service'	☐	☐
2.9.10	(L1) Ensure 'Alternate error pages' is set to 'Never use alternate error pages'	☐	☐
2.9.11	(L1) Ensure 'Payment methods' is set to 'Always tell websites that no payment methods are saved'	☐	☐
2.10.1	(L2) Ensure 'Search suggest' is set to 'Never allow users to use Search Suggest'	☐	☐
2.10.2	(L1) Ensure 'Side Panel search' Is Set to 'Disable Side Panel search on all web pages'	☐	☐
2.11.1	(L1) Ensure 'Enterprise Hardware Platform API' is set to 'Do not allow managed extensions to use the Enterprise Hardware Platform API'	☐	☐
2.11.2	(L2) Ensure 'Video input (camera)' is set to 'Disable camera input for websites and apps'	☐	☐
2.11.3	(L2) Ensure 'Audio input (microphone)' is set to 'Disable audio input'	☐	☐
2.11.4	(L2) Ensure 'Sensors' is set to 'Do not allow any site to access sensors'	☐	☐
2.11.5	(L2) Ensure 'Web Serial API' is set to 'Do not allow any site to request access to serial ports via the Web Serial API'	☐	☐
2.12.1	(L1) Ensure no URLs Are Configured in 'Safe Browsing allowed domains'	☐	☐
2.12.2	(L1) Ensure 'Safe Browsing for trusted sources' is set to 'Perform Safe Browsing checks on all downloaded files'	☐	☐
2.12.3	(L1) Ensure 'Disable bypassing Safe Browsing warnings' is set to 'Do not allow user to bypass Safe Browsing warning'	☐	☐

Recommendation		Set Correctly	
		Yes	No
2.12.4	(L1) Ensure 'Download restrictions' is set to 'Block malicious downloads'	☐	☐
2.12.5	(L1) Ensure 'Suppress lookalike domain warnings on domains' is Not Set	☐	☐
2.12.6	(L2) Ensure 'SafeSites URL filter' is set to 'Filter top level sites (but not embedded iframes) for adult content'	☐	☐
2.12.7	(L1) Ensure 'Safe Browsing protection' is set to 'Safe Browsing is active in the standard mode' and 'Allow higher-protection proxied lookups'	☐	☐
2.13.1	Ensure 'Generative AI policy defaults' Is Set to 'Allow GenAI features without improving AI models'	☐	☐
2.13.2	Ensure 'Help me write' Is Set to 'Use the value specified in the Generative AI policy defaults setting'	☐	☐
2.13.3	Ensure 'DevTools AI features' Is Set to 'Use the value specified in the Generative AI policy defaults setting'	☐	☐
2.13.4	Ensure 'History search settings' Is Set to 'Use the value specified in the Generative AI policy defaults setting'	☐	☐
2.13.5	Ensure 'Tab compare' Is Set to 'Use the value specified in the Generative AI policy defaults setting'	☐	☐
2.13.6	Ensure 'Help me read' Is Set to 'Use the value specified in the Generative AI policy defaults setting'	☐	☐
2.14.1	(L1) Ensure 'Component updates' is set to 'Enable updates for all components'	☐	☐
2.14.2	(L1) Ensure 'Relaunch notification' sets 'Time Period (hours)' to '168 or less' and 'Initial quiet period (hours)' to less than 'Time Period (hours)'	☐	☐
2.14.3	(L1) Ensure 'Relaunch notification' is set to 'Show notification recommending relaunch'	☐	☐
2.15.1	(L1) Ensure 'Variations' is set to 'Enable Chrome variations'	☐	☐
2.16.1	(L1) Ensure 'Google time service' is set to 'Allow queries to a Google server to retrieve an accurate timestamp'	☐	☐
2.16.2	(L1) Ensure 'Disk cache size in bytes' in 'Disk cache size' is set to `250609664'	☐	☐
2.16.4	(L1) Ensure 'Metrics reporting' is set to 'Do not send anonymous reports of usage and crash-related data to Google'	☐	☐

Recommendation		Set Correctly	
		Yes	No
2.16.5	(L1) Ensure 'Chrome Sync and Roaming Profiles (Chrome Browser - Cloud Managed)' is set to 'Disallow Sync'	☐	☐
2.16.6	(L1) Ensure 'Allow reporting of domain reliability related data' Is 'Never send domain reliability data to Google'	☐	☐
2.16.7	(L2) Ensure 'Prohibited Native Messaging hosts' in 'Native Messaging blocked hosts' is set to '*'	☐	☐
2.16.8	(L1) Ensure 'Background mode' is set to 'Disable background mode'	☐	☐
3.1.1	(L1) Ensure 'External extensions' is set to 'Block external extensions from being installed'	☐	☐
3.1.2	(L1) Ensure 'Allowed types of apps and extensions' is set to 'Extension', 'Hosted App', 'Chrome Packaged App', and 'Theme'	☐	☐
3.1.3	(L1) Ensure 'App and extension install sources' Is Not Set	☐	☐
3.1.4	(L1) Ensure 'Chrome Web Store unpublished extensions' Is Set to 'Disable unpublished extensions'	☐	☐

Appendix: CIS Controls v8 Unmapped Recommendations

Recommendation		Set Correctly	
		Yes	No
	No unmapped recommendations to CIS Controls v8	☐	☐

Appendix: Change History

Date	Version	Changes for this version
June 16, 2025	1.0.0	Initial Draft Release
June 30, 2025	1.0.0	Initial Published Release – This version replaces the previous Google Chrome Cloud Management v1.0.0 Benchmark but is a completely new benchmark organized using the Google Workspace GUI.