

CIS Google Chrome Benchmark

v2.1.0 - 12-21-2021

Terms of Use

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

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

Table of Contents

Terms of Use	1
Overview	9
1.1 --- USAGE NOTES ---	9
1.2 Recommendation Order	9
1.3 Enforced Defaults	9
1.4 Viewing the Resulting "Policies" in Chrome	10
Intended Audience	10
Consensus Guidance	10
Typographical Conventions	11
Assessment Status	11
Profile Definitions	12
Acknowledgements	13
Recommendations	14
1 Enforced Defaults	14
1.1 HTTP authentication	15
1.1.1 (L1) Ensure 'Cross-origin HTTP Authentication prompts' is set to 'Disabled' (Automated)	15
1.2 Safe Browsing settings	17
1.2.1 (L1) Ensure 'Configure the list of domains on which Safe Browsing will not trigger warnings' is set to 'Disabled' (Automated)	17
1.2.2 (L1) Ensure 'Safe Browsing Protection Level' is set to 'Enabled: Standard Protection' or higher (Manual)	19
1.3 (L1) Ensure 'Allow Google Cast to connect to Cast devices on all IP addresses' is set to 'Disabled' (Automated)	21
1.4 (L1) Ensure 'Allow queries to a Google time service' is set to 'Enabled' (Automated)	23
1.5 (L1) Ensure 'Allow the audio sandbox to run' is set to 'Enabled' (Automated)	25
1.6 (L1) Ensure 'Ask where to save each file before downloading' is set to 'Enabled' (Automated)	27

1.7 (L1) Ensure 'Continue running background apps when Google Chrome is closed' is set to 'Disabled' (Automated)	29
1.8 (L2) Ensure 'Control SafeSites adult content filtering' is set to 'Enabled: Filter top level sites (but not embedded iframes) for adult content' specified (Automated)	31
1.9 (L1) Ensure 'Determine the availability of variations' is set to 'Disabled' (Manual)	33
1.10 (L1) Ensure 'Disable Certificate Transparency enforcement for a list of Legacy Certificate Authorities' is set to 'Disabled' (Automated)	35
1.11 (L1) Ensure 'Disable Certificate Transparency enforcement for a list of subjectPublicKeyInfo hashes' is set to 'Disabled' (Automated)	37
1.12 (L1) Ensure 'Disable Certificate Transparency enforcement for a list of URLs' is set to 'Disabled' (Automated)	39
1.13 (L1) Ensure 'Disable saving browser history' is set to 'Disabled' (Automated)	41
1.14 (L1) Ensure 'DNS interception checks enabled' is set to 'Enabled' (Automated)	43
1.15 (L1) Ensure 'Enable component updates in Google Chrome' is set to 'Enabled' (Automated)	45
1.16 (L1) Ensure 'Enable globally scoped HTTP auth cache' is set to 'Disabled' (Automated)	47
1.17 (L1) Ensure 'Enable online OCSP/CRL checks' is set to 'Disabled' (Automated)	49
1.18 (L1) Ensure 'Enable Renderer Code Integrity' is set to 'Enabled' (Automated)	51
1.19 (L1) Ensure 'Enable security warnings for command-line flags' is set to 'Enabled' (Automated)	53
1.20 (L1) Ensure 'Enable third party software injection blocking' is set to 'Enabled' (Automated)	55
1.21 (L1) Ensure 'Enables managed extensions to use the Enterprise Hardware Platform API' is set to 'Disabled' (Automated)	56
1.22 (L1) Ensure 'Ephemeral profile' is set to 'Disabled' (Automated)	58
1.23 (L1) Ensure 'Import autofill form data from default browser on first run' is set to 'Disabled' (Automated)	60

1.24 (L1) Ensure 'Import of homepage from default browser on first run' is set to 'Disabled' (Automated).....	62
1.25 (L1) Ensure 'Import search engines from default browser on first run' is set to 'Disabled' (Automated)	64
1.26 (L1) Ensure 'List of names that will bypass the HSTS policy check' is set to 'Disabled' (Manual)	66
1.27 (L1) Ensure 'Origins or hostname patterns for which restrictions on insecure origins should not apply' is set to 'Disabled' (Automated).....	68
1.28 (L1) Ensure 'Suppress lookalike domain warnings on domains' is set to 'Disabled' (Manual)	70
1.29 (L1) Ensure 'Suppress the unsupported OS warning' is set to 'Disabled' (Automated).....	72
1.30 (L1) Ensure 'URLs for which local IPs are exposed in WebRTC ICE candidates' is set to 'Disabled' (Automated).....	74
2 Attack Surface Reduction	76
2.1 Update settings (Google section of GPO)	77
2.1.1 (L1) Ensure 'Update policy override' is set to 'Enabled' with 'Always allow updates (recommended)' or 'Automatic silent updates' specified (Automated) ..	77
2.2 Content settings	79
2.2.1 (L1) Ensure 'Control use of insecure content exceptions' is set to 'Enabled: Do not allow any site to load mixed content' (Automated).....	79
2.2.2 (L2) Ensure 'Control use of the Web Bluetooth API' is set to 'Enabled: Do not allow any site to request access to Bluetooth devices via the Web Bluetooth API' (Automated).....	81
2.2.3 (L2) Ensure 'Control use of the WebUSB API' is set to 'Enabled: Do not allow any site to request access to USB devices via the WebUSB API' (Automated).....	83
2.2.4 (L2) Ensure 'Default notification setting' is set to 'Enabled: Do not allow any site to show desktop notifications' (Automated)	85
2.3 Extensions.....	87
2.3.1 (L1) Ensure 'Blocks external extensions from being installed' is set to 'Enabled' (Automated).....	87
2.3.2 (L1) Ensure 'Configure allowed app/extension types' is set to 'Enabled: extension, hosted_app, platform_app, theme' (Automated)	89

2.3.3 (L1) Ensure 'Configure extension installation blocklist' is set to 'Enabled: *' (Automated).....	91
2.4 HTTP authentication.....	93
2.4.1 (L1) Ensure 'Supported authentication schemes' is set to 'Enabled: ntlm, negotiate' (Automated)	93
2.5 Native Messaging.....	95
2.5.1 (L2) Ensure 'Configure native messaging blocklist' is set to 'Enabled: *' (Automated).....	95
2.6 Password manager	97
2.6.1 (L1) Ensure 'Enable saving passwords to the password manager' is Explicitly Configured (Manual)	97
2.7 Printing.....	99
2.7.1 (L1) Ensure 'Enable Google Cloud Print Proxy' is set to 'Disabled' (Automated).....	99
2.8 Remote access (Chrome Remote Desktop)	101
2.8.1 Ensure 'Allow remote access connections to this machine' is set to 'Disabled' (Manual)	101
2.8.2 (L1) Ensure 'Allow remote users to interact with elevated windows in remote assistance sessions' is set to 'Disabled' (Automated)	103
2.8.3 (L1) Ensure 'Configure the required domain names for remote access clients' is set to 'Enabled' with a domain defined (Manual).....	105
2.8.4 (L1) Ensure 'Enable curtaining of remote access hosts' is set to 'Disabled' (Automated).....	107
2.8.5 (L1) Ensure 'Enable firewall traversal from remote access host' is set to 'Disabled' (Automated).....	109
2.8.6 (L1) Ensure 'Enable or disable PIN-less authentication for remote access hosts' is set to 'Disabled' (Automated)	111
2.8.7 (L1) Ensure 'Enable the use of relay servers by the remote access host' is set to 'Disabled'. (Automated).....	113
2.9 (L1) Ensure 'Allow download restrictions' is set to 'Enabled: Block dangerous downloads' (Automated)	115
2.10 (L2) Ensure 'Allow proceeding from the SSL warning page' is set to 'Disabled' (Automated).....	117

2.11 (L1) Ensure 'Disable proceeding from the Safe Browsing warning page' is set to 'Enabled' (Automated).....	119
2.12 (L1) Ensure 'Enable Chrome Cleanup on Windows' is Configured (Manual)	121
2.13 (L1) Ensure 'Enable Site Isolation for every site' is set to 'Enabled' (Automated).....	123
2.14 (L2) Ensure 'Force Google SafeSearch' is set to 'Enabled' (Automated)	125
2.15 (L1) Ensure 'Notify a user that a browser relaunch or device restart is recommended or required' is set to 'Enabled: Show a recurring prompt to the user indication that a relaunch is required' specified (Automated)	127
2.16 (L1) Ensure 'Proxy settings' is set to 'Enabled' and does not contain "ProxyMode": "auto_detect" (Automated)	129
2.17 (L2) Ensure 'Require online OCSP/CRL checks for local trust anchors' is set to 'Enabled' (Automated).....	131
2.18 (L1) Ensure 'Set the time period for update notifications' is set to 'Enabled: 86400000' (Automated)	133
3 Privacy	135
3.1 Content settings	136
3.1.1 (L2) Ensure 'Default cookies setting' is set to 'Enabled: Keep cookies for the duration of the session' (Automated)	136
3.1.2 (L1) Ensure 'Default geolocation setting' is set to 'Enabled: Do not allow any site to track the users' physical location' (Automated)	138
3.2 Google Cast	140
3.2.1 (L1) Ensure 'Enable Google Cast' is set to 'Disabled' (Automated).....	140
3.3 (L1) Ensure 'Allow websites to query for available payment methods' is set to 'Disabled' (Automated).....	142
3.4 (L1) Ensure 'Block third party cookies' is set to 'Enabled' (Automated)	144
3.5 (L2) Ensure 'Browser sign in settings' is set to 'Enabled: Disabled browser sign-in' (Automated).....	146
3.6 (L1) Ensure 'Control how Chrome Cleanup reports data to Google' is set to 'Disabled' (Automated).....	148
3.7 (L1) Ensure 'Disable synchronization of data with Google' is set to 'Enabled' (Automated).....	150
3.8 (L1) Ensure 'Enable alternate error pages' is set to 'Disabled' (Automated)	152

3.9 (L1) Ensure 'Enable deleting browser and download history' is set to 'Disabled' (Automated).....	154
3.10 (L1) Ensure 'Enable network prediction' is set to 'Enabled: Do not predict actions on any network connection' (Automated)	156
3.11 (L1) Ensure 'Enable or disable spell checking web service' is set to 'Disabled' (Automated).....	158
3.12 (L1) Ensure 'Enable reporting of usage and crash-related data' is set to 'Disabled' (Automated).....	160
3.13 (L1) Ensure 'Enable Safe Browsing for trusted sources' is set to 'Disabled' (Automated).....	162
3.14 (L2) Ensure 'Enable search suggestions' is set to 'Disabled' (Automated) ..	164
3.15 (L2) Ensure 'Enable Translate' is set to 'Disabled' (Automated)	166
3.16 (L1) Ensure 'Enable URL-keyed anonymized data collection' is set to 'Disabled' (Automated).....	167
4 Data Loss Prevention	169
4.1 Allow or deny screen capture.....	170
4.1.1 (L2) Ensure 'Allow or deny screen capture' is set to 'Disabled' (Automated)	170
4.2 Content settings	172
4.2.1 (L2) Ensure 'Control use of the Serial API' is set to 'Enable: Do not allow any site to request access to serial ports via the Serial API' (Automated)	172
4.2.2 (L2) Ensure 'Default Sensors Setting' is set to 'Enabled: Do not allow any site to access sensors' (Automated).....	174
4.3 Printing.....	176
4.3.1 (L1) Ensure 'Enable submission of documents to Google Cloud print' is set to 'Disabled' (Automated).....	176
4.4 (L2) Ensure 'Allow invocation of file selection dialogs' is set to 'Disabled' (Automated).....	178
4.5 (L2) Ensure 'Allow or deny audio capture' is set to 'Disabled' (Automated).	180
4.6 (L2) Ensure 'Allow or deny video capture' is set to 'Disabled' (Automated).	182
4.7 (L1) Ensure 'Allow user feedback' is set to 'Disabled' (Automated)	184
4.8 (L2) Ensure 'Controls the mode of DNS-over-HTTPS' is set to 'Enabled: secure' (Automated).....	185

4.9 (L1) Ensure 'Enable AutoFill for addresses' is set to 'Disabled' (Automated)	187
4.10 (L1) Ensure 'Enable AutoFill for credit cards' is set to 'Disabled' (Automated)	189
4.11 (L1) Ensure 'Import saved passwords from default browser on first run' is set to 'Disabled' (Automated)	191
4.12 (L1) Ensure 'List of types that should be excluded from synchronization' is set to 'Enabled: passwords' (Automated)	193
5 Forensics (Post Incident)	195
5.1 (L2) Ensure 'Enable guest mode in browser' is set to 'Disabled' (Automated)	195
5.2 (L2) Ensure 'Incognito mode availability ' is set to 'Enabled: Incognito mode disabled' (Automated)	197
5.3 (L1) Ensure 'Set disk cache size, in bytes' is set to 'Enabled: 250609664' (Automated)	199
Appendix: Recommendation Summary Table	201
Appendix: CIS Controls v7 IG 1 Mapped Recommendations	207
Appendix: CIS Controls v7 IG 2 Mapped Recommendations	208
Appendix: CIS Controls v7 IG 3 Mapped Recommendations	210
Appendix: CIS Controls v8 IG 1 Mapped Recommendations	213
Appendix: CIS Controls v8 IG 2 Mapped Recommendations	214
Appendix: CIS Controls v8 IG 3 Mapped Recommendations	217
Appendix: Change History	220

Overview

This document provides prescriptive guidance for establishing a secure configuration posture for Google Chrome browser. This guide was tested against Google Chrome v96. 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.

IMPORTANT NOTE: This Benchmark assumes the installation of the Google Chrome and Google Update ADMX/ADML templates into the Active Directory policy store for the domain(s) of interest. These can be obtained at the following web locations:

- [Chrome](#)
- [Google Update](#)

1.1 --- USAGE NOTES ---

Some helpful guidance on using this Benchmark.

1.2 Recommendation Order

This Benchmark has high-level sections based on various security related concerns (Enforced Defaults, Privacy, etc.). Within each of these major sections the recommendations are ordered alphabetically, and are grouped in the relevant sub-section where the setting is located in the Google Chrome GPO as shown in the Microsoft Group Policy Management Editor when the GPO is sorted alphabetically by setting (Clicking the **Setting** column in the Microsoft Group Policy Management Editor right pane view).

1.3 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.

1.4 Viewing the Resulting "Policies" in Chrome

This benchmark is designed to use Windows Group Policy on a domain joined system to set the appropriate Windows registry values that pertain to Google Chrome. In the end, these settings change the internal "policy" configuration of Google Chrome. These "Policy" settings can be viewed in Google Chrome directly by typing `chrome://policy/` directly into the Google Chrome address box.

Intended Audience

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

Consensus Guidance

This benchmark was created using a consensus review process comprised of subject matter experts. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

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

Typographical Conventions

The following typographical conventions are used throughout this guide:

Convention	Meaning
<code>Stylized Monospace font</code>	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
Monospace font	Used for inline code, commands, or examples. Text should be interpreted exactly as presented.
<i><italic font in brackets></i>	Italic texts set in angle brackets denote a variable requiring substitution for a real value.
<i>Italic font</i>	Used to denote the title of a book, article, or other publication.
Note	Additional information or caveats

Assessment Status

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

Automated

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

Manual

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

Profile Definitions

The following configuration profiles are defined by this Benchmark:

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

Items in this profile intend to:

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

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

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

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

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

Acknowledgements

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

Contributor

Fletcher Oliver, Google

Johannes Goerlich , Siemens AG

Jordan Rakoske GSEC, GCWN, Center for Internet Security

Brian Howson

Adrian Clark

Editor

Phil White, Center for Internet Security

Recommendations

1 Enforced Defaults

This section contains recommendations that are configured by default when you install Google Chrome. Enforcing these settings at an enterprise level can prevent these settings from changing to a less secure option.

1.1 HTTP authentication

1.1.1 (L1) Ensure 'Cross-origin HTTP Authentication prompts' is set to 'Disabled' (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: `Disabled (0)`

Rationale:

This setting is typically disabled to help combat phishing attempts.

Impact:

None - This is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location which should be set to 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:AllowCrossOriginAuthPrompt
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Google\Google  
Chrome\HTTP authentication\Cross-origin HTTP Authentication prompts
```

Default Value:

Unset (Same as Disabled, but user can change)

References:

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

1.2 Safe Browsing settings

1.2.1 (L1) Ensure 'Configure the list of domains on which Safe Browsing will not trigger warnings' is set to 'Disabled' (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 download 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:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting will have **no registry** value (the key will not exist) if it is set to `Disabled`:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:SafeBrowsingAllowlistDomains

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to Disabled:

```
Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Safe Browsing settings\Configure the list of domains on which Safe Browsing will not trigger warnings
```





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 <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.			

1.2.2 (L1) Ensure 'Safe Browsing Protection Level' is set to 'Enabled: Standard Protection' or higher (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 it operates in. 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

The recommended state for this setting is: Standard Protection (1) or higher

Rationale:

Google Safe Browsing will help protect users from a variety of malicious and fraudulent sites, or download dangerous files.

NOTE: Google recommend 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:

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:SafeBrowsingProtectionLevel
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to Enabled: Standard Protection:

```
Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Safe Browser settings\Safe Browsing Protection Level
```





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 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.			

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

Profile Applicability:

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

Description:

This 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:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location which should be set to 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:MediaRouterCastAllowAllIPs
```

Remediation:

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

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





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.			

1.4 (L1) Ensure 'Allow queries to a Google time service' is set to 'Enabled' (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
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Allow queries to a Google time service
```





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.			

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

Profile Applicability:

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

Description:

This 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:

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:AudioSandboxEnabled
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Google\Google  
Chrome\Allow the audio sandbox to run
```

Default Value:

Unset (Same as Enabled, but user can change)

References:

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

1.6 (L1) Ensure 'Ask where to save each file before downloading' is set to 'Enabled' (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:

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:PromptForDownloadLocation
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Ask where to save each file before downloading
```

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/>

1.7 (L1) Ensure 'Continue running background apps when Google Chrome is closed' is set to 'Disabled' (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:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location which should be set to 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:BackgroundModeEnabled
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to Disabled:

```
Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Continue running background apps when Google Chrome is closed
```





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.			

1.8 (L2) Ensure 'Control SafeSites adult content filtering' is set to 'Enabled: Filter top level sites (but not embedded iframes) for adult content' specified (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: Enabled with a value of Filter top level sites (but not embedded iframes) for adult content (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.

NOTE: Using Googles Safe Search API may leak information which is typed/pasted by mistake into the omnibox, e.g. passwords, internal webservices, folder structures, etc.

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:SafeSitesFilterBehavior
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to Enabled: Do not filter sites for adult content:

```
Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Control SafeSites adult content filtering.
```






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 <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.			

1.9 (L1) Ensure 'Determine the availability of variations' is set to 'Disabled' (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.

- `Disabled (0)`: Allows all variations to be applied to the browser (also referred to as `VariationsEnabled`).
- `CriticalFixesOnly (1)`: Allows only variations considered critical security or stability fixes to be applied to Google Chrome.
- `VariationsDisabled (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: `Disabled (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.

Rationale:

Google strongly recommends to leave 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:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location which should be set to 0:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:ChromeVariations

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to Disabled (same as VariationsEnabled):

Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Determine the availability of variations









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](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 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.			
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.			

1.10 (L1) Ensure 'Disable Certificate Transparency enforcement for a list of Legacy Certificate Authorities' is set to 'Disabled' (Automated)

Profile Applicability:

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

Description:

Google Chrome can disable the enforcing of Certificate Transparency requirements for a list of Legacy Certificate Authorities.

If this setting is disabled, certificates not properly publicly disclosed as required by Certificate Transparency are untrusted.

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

Rationale:

Legacy Certificate Authorities shall follow the Certificate Transparency policy.

Impact:

None - This is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting will have **no registry** value (the key will not exist) if it is set to `Disabled`:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:CertificateTransparencyEnforcementDisabledForLegacyCas
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Disable Certificate Transparency enforcement for a list of Legacy Certificate Authorities
```

Default Value:

Unset (Same as Disabled, but user can change)

References:

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

1.11 (L1) Ensure 'Disable Certificate Transparency enforcement for a list of subjectPublicKeyInfo hashes' is set to 'Disabled' (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:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting will have **no registry** value (the key will not exist) if it is set to Disabled:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:CertificateTransparencyEnforcementDisabledForCas
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to Disabled:

```
Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Disable Certificate Transparency enforcement for a list of subjectPublicKeyInfo hashes
```

Default Value:

Unset (Same as Disabled, but user can change)

References:

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

1.12 (L1) Ensure 'Disable Certificate Transparency enforcement for a list of URLs' is set to 'Disabled' (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:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting will have **no registry** value (the key will not exist) if it is set to `Disabled`:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:CertificateTransparencyEnforcementDisabledForUrls
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Disable Certificate Transparency enforcement for a list of URLs
```

Default Value:

Unset (Same as Disabled, but user can change)

References:

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

1.13 (L1) Ensure 'Disable saving browser history' is set to 'Disabled' (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: Disabled (0)

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

Rationale:

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

Impact:

None - This is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location which should be set to 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:SavingBrowserHistoryDisabled
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to Disabled:

```
Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Disable saving browser history
```

Default Value:

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

References:

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

1.14 (L1) Ensure 'DNS interception checks enabled' is set to 'Enabled' (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 start-up and each DNS configuration change.

Rationale:

Disabling these checks could potentially allow DNS hijacking and poisoning.

Impact:

None - This is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location which should be set to 1:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:DNSInterceptionChecksEnabled
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\DNS interception checks enabled
```

Default Value:

Unset (Same as Enabled, but user can change)

References:

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

1.15 (L1) Ensure 'Enable component updates in Google Chrome' is set to 'Enabled' (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 settings.

NOTE: Google provided the following list of "**some of the components**" controlled by this settings:

- 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:

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\ComponentUpdatesEnabled

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to Enabled:

Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Enable component updates in Google Chrome

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 Perform Automated Application Patch Management Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.			
v7	3.5 Deploy Automated Software Patch Management Tools Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.			

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

Profile Applicability:

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

Description:

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

Impact:

None - This is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location which should be set to 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:GloballyScopeHTTPAuthCacheEnabled
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Enable globally scoped HTTP auth cache
```


Default Value:

Unset (Same as Disabled, but user can change)

References:

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

1.17 (L1) Ensure 'Enable online OCSP/CRL checks' is set to 'Disabled' (Automated)

Profile Applicability:

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

Description:

Google Chrome can reactivate soft-fail, online revocation checks although they provide no effective security benefit.

If this setting is disabled, unsecure online OCSP/CRL checks are no longer performed.

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

Rationale:

CRLSets are primarily a means by which Chrome can quickly block certificates in emergency situations. As a secondary function they can also contain some number of non-emergency revocations. These latter revocations are obtained by crawling CRLs published by CAs.

Online (i.e. OCSP and CRL) checks are not, by default, performed by Chrome. The underlying system certificate library always performs these checks no matter what Chrome does, so enabling it here is redundant.

An attacker may block OCSP traffic and cause revocation checks to pass in order to cause usage of soft-fail behavior. Furthermore, the browser may leak what website is being accessed and who accesses it to CA servers.

Impact:

None - This is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location which should be set to 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:EnableOnlineRevocationChecks
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to Disabled:

```
Computer Configuration\Policies\Administrative Templates\Google\Google  
Chrome\Enable online OCSP/CRL checks
```

Default Value:

Unset (Same as Disabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#EnableOnlineRevocationChecks>
2. <https://medium.com/@alexeysamoshkin/how-ssl-certificate-revocation-is-broken-in-practice-af3b63b9cb3>
3. <https://dev.chromium.org/Home/chromium-security/crlsets>

1.18 (L1) Ensure 'Enable Renderer Code Integrity' is set to 'Enabled' (Automated)

Profile Applicability:

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

Description:

This setting controls whether unknown and potentially hostile code will be allowed to load inside of Google Chrome.

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

Rationale:

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

Impact:

None - This is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location which should be set to 1:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:RendererCodeIntegrityEnabled
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Enable Renderer Code Integrity
```

Default Value:

Unset (Same as Enabled, but user can change)

References:

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

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

Profile Applicability:

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

Description:

This 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:

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\CommandLineFlagSecurityWarningsEnabled
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Enable security warnings for command-line flags
```

Default Value:

Unset (Same as Enabled, but user can change)

References:

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

1.20 (L1) Ensure 'Enable third party software injection blocking' is set to 'Enabled' (Automated)

Profile Applicability:

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

Description:

Google Chrome can prevent third party software from injecting executable code into Chrome's processes.

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

Rationale:

Third party software shall not be able to inject executable code into Chrome's processes.

Impact:

None - This is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location which should be set to 1:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:ThirdPartyBlockingEnabled
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Enable third party software injection blocking
```

Default Value:

Unset (Same as Enabled, but user can change)

References:

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

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

Profile Applicability:

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

Description:

This 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:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location which should be set to 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:EnterpriseHardwarePlatformAPIEnabled
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Enables managed extensions to use the Enterprise Hardware Platform API
```





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	<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.			

1.22 (L1) Ensure 'Ephemeral profile' is set to 'Disabled' (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: `Disabled (0)`

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:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location which should be set to 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:ForceEphemeralProfiles
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Google\Google  
Chrome\Ephemeral profile
```

Default Value:

Unset (Same as Disabled, but user can change)

References:

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

1.23 (L1) Ensure 'Import autofill form data from default browser on first run' is set to 'Disabled' (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 `Disabled` 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 setup.

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

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:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location which should be set to 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:ImportAutofillFormData
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Google\Google  
Chrome\Import autofill form data from default browser on first run
```

Default Value:

Unset (Same as Disabled, but user can change)

References:

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

1.24 (L1) Ensure 'Import of homepage from default browser on first run' is set to 'Disabled' (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:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location which should be set to 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:ImportHomepage
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Google\Google  
Chrome\Import of homepage from default browser on first run
```

Default Value:

Unset (Same as Disabled, but user can change)

References:

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

1.25 (L1) Ensure 'Import search engines from default browser on first run' is set to 'Disabled' (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:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location which should be set to 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:ImportSearchEngine
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Import search engines from default browser on first run
```

Default Value:

Unset (Same as Disabled, but user can change)

References:

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

1.26 (L1) Ensure 'List of names that will bypass the HSTS policy check' is set to 'Disabled' (Manual)

Profile Applicability:

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

Description:

This 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:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location which should be **absent** or does not have a **registry value** defined:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:HSTSPolicyBypassList
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Google\Google  
Chrome\List of names that will bypass the HSTS policy check
```





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 <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.			

1.27 (L1) Ensure 'Origins or hostname patterns for which restrictions on insecure origins should not apply' is set to 'Disabled' (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:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location which should be set to 0:

```
HKKEY_LOCAL_MACHINE\SOFTWARE\Policies\Chrome:OverrideSecurityRestrictionsOnInsecureOrigin
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to Disabled:

```
Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Origins or hostname patterns for which restrictions on insecure origins should not apply
```

Default Value:

Unset (Same as Disabled, but user can change)

References:

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

1.28 (L1) Ensure 'Suppress lookalike domain warnings on domains' is set to 'Disabled' (Manual)

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 the user is familiar with.

- `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 use to host phishing sites, and often lead 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 the are going to a legitimate site that is falsely considered fraudulent (a rare occurrence). This an be handled by adding the site to the allowlist and/of notifying Google of the false finding.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location which should be set to 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:LookalikeWarningAllowlistDomains
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to Disabled:

```
Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Suppress lookalike domain warnings on domains
```





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 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.			

1.29 (L1) Ensure 'Suppress the unsupported OS warning' is set to 'Disabled' (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:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location which should be set to 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:SuppressUnsupportedOSWarning
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to Disabled:

```
Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Suppress the unsupported OS warning
```







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	<p><u>2.2 Ensure Authorized Software is Currently Supported</u></p> <p>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.</p>			
v7	<p><u>2.2 Ensure Software is Supported by Vendor</u></p> <p>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.</p>			

1.30 (L1) Ensure 'URLs for which local IPs are exposed in WebRTC ICE candidates' is set to 'Disabled' (Automated)

Profile Applicability:

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

Description:

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

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

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting will have **no registry** value (the key will not exist) if it is set to `Disabled`:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\WebRtcLocalIpsAllowedUrls
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\URLs for which local IPs are exposed in WebRTC ICE candidates
```

Default Value:

Unset (Same as Disabled, but user can change)

References:

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

2 Attack Surface Reduction

This section contains recommendations that help reduce the overall attack surface. Organizations should review these settings and any potential impacts to ensure they make sense within the environment since they restrict some browser functionality.

2.1 Update settings (Google section of GPO)

These settings are not in the normal \Google\Google Chrome\ section of the GPO.

2.1.1 (L1) Ensure 'Update policy override' is set to 'Enabled' with 'Always allow updates (recommended)' or 'Automatic silent updates' specified (Automated)

Profile Applicability:

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

Description:

Google Update manages installation of available Google Chrome updates from Google. This setting allows to define whether updates are to be applied automatically. Depending on the business scenario updates shall be applied periodically or also if the user seeks for updates.

- Updates disabled: Never apply updates (0)
- Always allow updates: Updates are always applied when found, either by periodic update check or by a manual update check (1)
- Manual updates only: Updates are only applied when the user does a manual update check (2)
- Automatic silent updates only: Updates are only applied when they are found via the periodic update check (3)

Disabled (0): Google Update handles available updates as specified by "Update policy override default".

The recommended state for this setting is: Enabled with a value of Always allow updates (1) or Automatic silent updates (3)

NOTE: This policy is available only on Windows instances that are joined to a Microsoft® Active Directory® domain.

Rationale:

Software updates shall be applied as soon as they are available since they may include latest security patches.

Impact:

Latest updates are automatically applied at least periodically.

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 or 3:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Update:Update{8A69D345-D564-463C-AFF1-A69D9E530F96}
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to Enabled: Always allow updates (recommended) **OR** Enabled: Automatic silent updates only:

```
Computer Configuration\Policies\Administrative Templates\Google\Google Update\Applications\Google Chrome\Update policy override
```







Default Value:

Inherit the value from 'Update policy override default'.

References:

1. https://admx.help/?Category=GoogleUpdate&Policy=Google.Policies.Update::Pol_UpdatePolicyGoogleChrome
2. https://admx.help/?Category=ChromeEnterprise&Policy=Google.Policies.Update::Pol_DefaultUpdatePolicy

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.			

2.2 Content settings

2.2.1 (L1) Ensure 'Control use of insecure content exceptions' is set to 'Enabled: 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:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location which should be set to 2:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:DefaultInsecureContentSetting
```


Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to

Enabled: Do not allow any site to load mixed content:

```
Computer Configuration\Policies\Administrative Templates\Google\Google  
Chrome\Content Settings\Do not allow any site to load mixed content
```





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.			

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

Profile Applicability:

- Level 2 (L2) - 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 no longer can access nearby Bluetooth device via the API (this includes web cameras, headphones, and other Bluetooth devices) and the user will never be asked.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location which should be set to 2:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:DefaultWebBluetoothGuardSetting
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to Enabled: Do not allow any site to request access to Bluetooth devices via the Web Bluetooth API:

```
Computer Configuration\Policies\Administrative Templates\Google\Google  
Chrome\Content Settings\Control use of the Web Bluetooth API
```





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	<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>15.9 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.			

2.2.3 (L2) Ensure 'Control use of the WebUSB API' is set to 'Enabled: 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 the 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:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location which should be set to 2:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:DefaultWebUsbGuardSetting
--

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to Enabled: Do not allow any site to request access to USB devices via the WebUSB API:

Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Content Settings\Control use of the WebUSB API





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	<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>13.7 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.			

2.2.4 (L2) Ensure 'Default notification setting' is set to 'Enabled: 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 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 (0)
- Do not allow any site to show desktop notifications (1)
- Ask every time a site wants to show desktop notifications (2)

The recommended state for this setting is: Enabled with a value of Do not allow any site to show desktop notifications (1)

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:

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:DefaultNotificationsSetting
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to Enabled: Do not allow any site to show desktop notifications selected from the drop down:

Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Content Settings\Default notification setting

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>

2.3 Extensions

2.3.1 (L1) Ensure 'Blocks external extensions from being installed' is set to 'Enabled' (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:

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\BlockExternalExtensions
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Google\Google  
Chrome\Extensions\Blocks external extensions from being installed
```





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	<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.			

2.3.2 (L1) Ensure 'Configure allowed app/extension types' is set to 'Enabled: extension, hosted_app, platform_app, theme' (Automated)

Profile Applicability:

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

Description:

Enabling this setting allows you to specify which app/extensions 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 it's type is denylisted and the extension itself is not allowlisted.

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 extension, hosted_app, platform_app, theme:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\ExtensionAllowedTypes
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to Enabled: extension, hosted_app, platform_app, theme:

```
Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Extensions\Configure allowed app/extension types
```





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](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	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.			

2.3.3 (L1) Ensure 'Configure extension installation blocklist' is set to 'Enabled: *' (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 requires 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 allow 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:

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 *:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\ExtensionInstallBlocklist
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to Enabled: *:

```
Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Extensions\Configure extension installation blocklist
```





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	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.			

2.4 HTTP authentication

2.4.1 (L1) Ensure 'Supported authentication schemes' is set to 'Enabled: ntlm, negotiate' (Automated)

Profile Applicability:

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

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 users password 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:

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 ntlm, negotiate:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:AuthSchemes
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to Enabled: ntlm, negotiate:

```
Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\HTTP Authentication\Supported authentication schemes
```





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.			

2.5 Native Messaging

2.5.1 (L2) Ensure 'Configure native messaging blocklist' is set to 'Enabled: *' (Automated)

Profile Applicability:

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

Description:

Allows you to specify which native messaging hosts that 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. Examples of applications that use 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:

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 `*`:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:NativeMessagingBlocklist
```


Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to Enabled: * specified.

Computer Configuration\Policies\Administrative Templates\Google Chrome\Native Messaging\Configure native messaging blocklist





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.			

2.6 Password manager

2.6.1 (L1) Ensure 'Enable saving passwords to the 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:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location which should be set to 0 or 1 (Organization dependent):

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:PasswordManagerEnabled
```

Remediation:

To establish the recommended configuration via Group Policy, configure the following setting to meet organizational requirements:

Computer Configuration\Policies\Administrative Templates\Google\Google Chrome>Password manager\Enable the password manager
--

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>

2.7 Printing

2.7.1 (L1) Ensure 'Enable Google Cloud Print Proxy' is set to 'Disabled' (Automated)

Profile Applicability:

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

Description:

This setting enables Google Chrome to act as a proxy between Google Cloud Print and legacy printers connected to the machine.

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

Rationale:

Disabling this option will prevent users from printing documents from unmanaged devices to an organization's printer.

Impact:

If this setting is disabled, users cannot enable the proxy, and the machine will not be allowed to share its local printers with Google Cloud Print.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location which should be set to 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:CloudPrintProxyEnabled
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to Disabled:

```
Computer Configuration\Policies\Administrative Templates\Google\Google  
Chrome\Printing\Enable Google Cloud Print Proxy
```





Default Value:

Unset (Same as Enabled, but user can change)

References:

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

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 Remote access (Chrome Remote Desktop)

This section has recommendation specifically for configuring Chrome Remote Desktop.

2.8.1 Ensure 'Allow remote access connections to this machine' is set to 'Disabled' (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:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location which should be set to 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:RemoteAccessHostAllowRemoteAccessConnections`
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to Disabled:

```
Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Remote Access\Allow remote access connections to this machine
```




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.			

2.8.2 (L1) Ensure 'Allow remote users to interact with elevated windows in remote assistance sessions' is set to 'Disabled' (Automated)

Profile Applicability:

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

Description:

Google Chrome can be set to run the remote assistance host in a process with uiAccess permissions. This allows remote users to interact with elevated windows on the local user's desktop.

If this setting is disabled, the remote assistance host will run in the user's context. Furthermore, remote users cannot interact with elevated windows on the desktop.

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

Rationale:

Remote users shall not be able to escalate privileges.

Impact:

None - This is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location which should be set to 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:RemoteAccessHostAllowUiAccessForRemoteAssistance
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to Disabled:

```
Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Remote access\Allow remote users to interact with elevated windows in remote assistance sessions
```





Default Value:

Unset (Same as Disabled, but user can change)

References:

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

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.			

2.8.3 (L1) Ensure 'Configure the required domain names for remote access clients' is set to 'Enabled' with a domain defined (Manual)

Profile Applicability:

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

Description:

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

Setting this to an empty list (Disabled) allows remote systems from any domain to connect to this users 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:

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 or more organizationally specific domain(s):

<code>HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:RemoteAccessHostClientDomainList</code>
--

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to Enabled and enter an organizational specific domain(s) (e.g. nodomain.local):

```
Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Remote access\Configure the required domain names for remote access clients
```




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.			

2.8.4 (L1) Ensure 'Enable curtaining of remote access hosts' is set to 'Disabled' (Automated)

Profile Applicability:

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

Description:

Allow someone physically present at the host machine to see what a user is doing while a remote connection is in progress.

If this setting is disabled, host's physical input and output devices are enabled while a remote connection is in progress.

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

Rationale:

If a remote session is in progress the user physically present at the host machine shall be able to see what a remote user is doing.

Impact:

None - This is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location which should be set to 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:RemoteAccessHostRequireCurtain
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to Disabled:

```
Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Remote access\Enable curtaining of remote access hosts
```




Default Value:

Unset (Same as Disabled, but user can change)

References:

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

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.			

2.8.5 (L1) Ensure 'Enable firewall traversal from remote access host' is set to 'Disabled' (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 this 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:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location which should be set to 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:RemoteAccessHostFirewallTraversal
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to Disabled:

```
Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Remote access\Enable firewall traversal from remote access host
```




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 <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.			

2.8.6 (L1) Ensure 'Enable or disable PIN-less authentication for remote access hosts' is set to 'Disabled' (Automated)

Profile Applicability:

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

Description:

Chrome allows a user to opt-out of using user-specified PIN authentication and instead pair clients and hosts during connection time.

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

Rationale:

If this setting is enabled, users can opt to pair clients and hosts at connection time, eliminating the need to enter a PIN every time.

Impact:

If this setting is disabled, users will be required to enter PIN every time.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location which should be set to 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:RemoteAccessHostAllowClientPairing
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to Disabled:

```
Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Remote access\Enable or disable PIN-less authentication
```




Default Value:

Unset (Same as Enabled, but user can change)

References:

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

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.			

2.8.7 (L1) Ensure 'Enable the use of relay servers by the remote access host' is set to 'Disabled'. (Automated)

Profile Applicability:

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

Description:

Google Chrome allows the use 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:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location which should be set to 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:RemoteAccessHostAllowRelayedConnection
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to Disabled:

```
Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Remote access\Enable the use of relay servers by the remote access host
```




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 <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.			

2.9 (L1) Ensure 'Allow download restrictions' is set to 'Enabled: Block dangerous 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 (0, Disabled)
- Block dangerous downloads (1)
- Block potentially dangerous downloads (2)
- Block all downloads (3)
- Block malicious downloads (4)

The recommended state for this setting is: Enabled with a value of Block dangerous downloads (1)

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 certain types of files, 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:

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:DownloadRestrictions

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to

Enabled: Block dangerous downloads:

```
Computer Configuration\Policies\Administrative Templates\Google\Google  
Chrome\Allow download restrictions
```

Default Value:

Unset (Same as Disabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#DownloadRestrictions>
2. <https://developers.google.com/safe-browsing>

2.10 (L2) Ensure 'Allow proceeding from the SSL warning page' is set to 'Disabled' (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 what appears to be an invalid certificate could open an organization up to users visiting a site that is otherwise not secure and or malicious in nature.

Impact:

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

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location which should be set to 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:SSLErrorOverrideAllowed
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Google\Google  
Chrome\Allow proceeding from the SSL warning page
```





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 <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.			

2.11 (L1) Ensure 'Disable proceeding from the Safe Browsing warning page' is set to 'Enabled' (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 in 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:

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:DisableSafeBrowsingProceedAnyway
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to Enabled:

```
Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Disable proceeding from the Safe Browsing warning page
```






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 (L1) Ensure 'Enable Chrome Cleanup on Windows' is Configured (Manual)

Profile Applicability:

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

Description:

Chrome provides a Cleanup-feature to detect unwanted software. This feature periodically scans the system for unwanted software and will ask the user if they wish to remove it, if any has been found.

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

Rationale:

The Google Chrome Cleanup is `Enabled` by default and each organization should review and determine if they want to use this solutions for malware detection. If another solution is used instead of the built in Chrome option then an organization should configure the setting to `Disabled`.

Impact:

Organizational Specific.

NOTE: If `Disabled`, Chrome Cleanup will no longer be able to scan the system. If users do not have a centrally managed anti-malware solution then leaving this setting `Enabled` can help protect a system.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location which should be set to 0 or 1 (Organization dependent):

HKKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:ChromeCleanupEnabled
--

Remediation:

To establish the recommended configuration via Group Policy, configure the following setting to meet organizational requirements:

Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Enable Chrome Cleanup on Windows





Default Value:

Unset (Same as Enabled, and users can change)

References:

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

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.6 Centrally Manage Anti-Malware Software Centrally manage anti-malware software.			
v7	8.1 Utilize Centrally Managed Anti-malware Software Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.			

2.13 (L1) Ensure 'Enable Site Isolation for every site' is set to 'Enabled' (Automated)

Profile Applicability:

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

Description:

This 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. So, 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:

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:SitePerProcess
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to Enabled:

```
Computer Configuration\Policies\Administrative Templates\Google\Google  
Chrome\Enable Site Isolation for every site
```

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>

2.14 (L2) Ensure 'Force Google SafeSearch' is set to 'Enabled' (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:

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:ForceGoogleSafeSearch
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Google\Google  
Chrome\Force Google SafeSearch
```





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 <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.			

2.15 (L1) Ensure 'Notify a user that a browser relaunch or device restart is recommended or required' is set to 'Enabled: Show a recurring prompt to the user indication that a relaunch is required' specified (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 once the notification period defined by the recommendation *Set the time period for update notifications* is passed.

- Show a recurring prompt to the user indicating that a relaunch is recommended (1)
- Show a recurring prompt to the user indicating that a relaunch is required (2)

Disabled: Google Chrome indicates to the user that a relaunch is needed via subtle changes to its menu.

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:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location which should be set to 2:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:RelaunchNotification
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to Enabled: Show a recurring prompt to the user indication that a relaunch is required:

```
Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Notify a user that a browser relaunch or device restart is recommended or required
```







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.			

2.16 (L1) Ensure 'Proxy settings' is set to 'Enabled' and does not contain "ProxyMode": "auto_detect" (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:

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 **NOT** be set to auto_detect:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:ProxyMode
```

Remediation:

To establish the recommended configuration via Group Policy, make sure the following UI path is set to 'Enabled' and the value of ProxyMode is not set to auto_detect:

```
Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Proxy settings
```

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.			●

2.17 (L2) Ensure 'Require online OCSP/CRL checks for local trust anchors' is set to 'Enabled' (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:

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:RequireOnlineRevocationChecksForLocalAnchors
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Require online OCSP/CRL checks for local trust anchors
```

Default Value:

Unset (Same as Disabled, and users can change)

References:

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

2.18 (L1) Ensure 'Set the time period for update notifications' is set to 'Enabled: 86400000' (Automated)

Profile Applicability:

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

Description:

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 affect 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:

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 86400000.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:RelaunchNotificationPeriod
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to Enabled: 5265C00 (86400000 in Hexidecimal):

```
Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Set the time period for update notifications
```







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	<u>7.4 Perform Automated Application Patch Management</u> Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.			
v7	<u>3.5 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.			

3 Privacy

This section contains recommendations that help improve user privacy. Organizations should review these settings and any potential impacts to ensure they make sense within the environment since they restrict some browser functionality.

3.1 Content settings

3.1.1 (L2) Ensure 'Default cookies setting' is set to 'Enabled: Keep cookies for the duration of the session' (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.

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:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location which should be set to 4:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:DefaultCookiesSetting
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to Enabled **with** Keep cookies for the duration of the session:

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Content  
Settings\Default cookies setting
```

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>

3.1.2 (L1) Ensure 'Default geolocation setting' is set to 'Enabled: Do not allow any site to track the users' physical location' (Automated)

Profile Applicability:

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

Description:

Google Chrome supports tracking the users' 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 (3)

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:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location which should be set to 2:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:DefaultGeolocationSetting
--

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to

Enabled: Do not allow any site to track the users' physical location:

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Content  
Settings\Default geolocation setting
```

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>

3.2 Google Cast

3.2.1 (L1) Ensure 'Enable Google Cast' is set to 'Disabled' (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:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location which should be set to 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:EnableMediaRouter
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to Disabled:

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Google Cast\Enable Google Cast
```





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.			

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

Profile Applicability:

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

Description:

This 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 the 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:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location which should be set to 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:PaymentMethodQueryEnabled
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Google\Google  
Chrome\Allow websites to query for available payment methods
```

Default Value:

Unset (Same as Enabled, but user can change)

References:

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

3.4 (L1) Ensure 'Block third party cookies' is set to 'Enabled' (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:

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\BlockThirdPartyCookies
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to Enabled:

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Block third party cookies
```

Default Value:

Unset (Same as Disabled, but user can change)

References:

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

3.5 (L2) Ensure 'Browser sign in settings' is set to 'Enabled: 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 can not sign in to the browser and use google account based services like Chrome sync.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location which should be set to 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:BrowserSignin
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to Enabled: Disable browser sign-in

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Browser  
sign in settings
```

Default Value:

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

References:

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

3.6 (L1) Ensure 'Control how Chrome Cleanup reports data to Google' is set to 'Disabled' (Automated)

Profile Applicability:

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

Description:

Chrome provides a Cleanup-feature to detect unwanted software. If this setting is `Enabled`, the results of the cleanup may be shared with Google (based on the setting of `SafeBrowsingExtendedReportingEnabled`) to assist with future unwanted software detection. These results will contain file metadata, automatically installed extensions and registry keys.

If the setting is `Disabled`, the results of the cleanup will not be shared with Google regardless of the value of `SafeBrowsingExtendedReportingEnabled`.

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:

Chrome Cleanup detected unwanted software, will no longer report metadata about the scan to Google.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location which should be set to 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:ChromeCleanupReportingEnabled
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to Disabled:

Computer Configuration\Administrative Templates\Google\Google Chrome\Control how Chrome Cleanup reports data to Google
--

Default Value:

Unset (Same as Enabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#MetricsReportingEnabled>
2. <https://www.google.com/chrome/privacy/whitepaper.html>
3. <https://chromeenterprise.google/policies/#SafeBrowsingExtendedReportingEnabled>

3.7 (L1) Ensure 'Disable synchronization of data with Google' is set to 'Enabled' (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:

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:SyncDisabled
```

Remediation:

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

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Disable synchronization of data with Google
```

Default Value:

Unset (Same as Disabled, but user can change)

References:

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

3.8 (L1) Ensure 'Enable alternate error pages' is set to 'Disabled' (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 does no longer use a web service to help resolve navigation errors.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location which should be set to 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:AlternateErrorPagesEnabled
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to Disabled:

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Enable alternate error pages
```

Default Value:

Unset (Same as Enabled, but user can change)

References:

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

3.9 (L1) Ensure 'Enable deleting browser and download history' is set to 'Disabled' (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:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location which should be set to 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:AllowDeletingBrowserHistory
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to Disabled:

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Enable deleting browser and download history
```

Default Value:

Unset (Same as Enabled, but user can change)

References:

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

3.10 (L1) Ensure 'Enable network prediction' is set to 'Enabled: Do not predict actions on any network connection' (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 un-needed connections increasing attack surface and in some cases could lead to opening connections to resources which the user did not intend to utilize.

Impact:

Users will not be presented with web page predictions.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location which should be set to 2:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:NetworkPredictionOptions
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to Enabled: Do not predict actions on any network connection:

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Enable network prediction
```

Default Value:

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

References:

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

3.11 (L1) Ensure 'Enable or disable spell checking web service' is set to 'Disabled' (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 as you type in them to Google. Spell checking can still be performed using a downloaded dictionary; this setting only controls the usage of the online service.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location which should be set to 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:SpellCheckServiceEnabled
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to Disabled:

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Enable or disable spell checking web service
```

Default Value:

Unset (Same as Enabled, but user can change)

References:

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

3.12 (L1) Ensure 'Enable reporting of usage and crash-related data' is set to 'Disabled' (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:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location which should be set to 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:MetricsReportingEnabled
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to Disabled:

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Enable reporting of usage and crash-related data
```

Default Value:

Unset (Same as Enabled, but user can change)

References:

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

3.13 (L1) Ensure 'Enable Safe Browsing for trusted sources' is set to 'Disabled' (Automated)

Profile Applicability:

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

Description:

Google Chrome can be adjusted to allow download without Safe Browsing checks when the requested files 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:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location which should be set to 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:SafeBrowsingForTrustedSourcesEnabled
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to Disabled:

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Enable  
Safe Browsing for trusted sources
```

Default Value:

Unset (Same as Enabled, but user can change)

References:

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

3.14 (L2) Ensure 'Enable search suggestions' is set to 'Disabled' (Automated)

Profile Applicability:

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

Description:

Google Chrome offers suggestions in Google Chrome's omnibox while 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:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location which should be set to 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:SearchSuggestEnabled
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to Disabled:

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Enable search suggestions
```

Default Value:

Unset (Same as Enabled, but user can change)

References:

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

3.15 (L2) Ensure 'Enable Translate' is set to 'Disabled' (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 Chrome contents of a web page are no longer sent to Google for translation.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location which should be set to 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:TranslateEnabled
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to Disabled:

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Enable Translate
```

Default Value:

Unset (Same as Enabled, but user can change)

References:

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

3.16 (L1) Ensure 'Enable URL-keyed anonymized data collection' is set to 'Disabled' (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:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location which should be set to 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\UrlKeyedAnonymizedDataCollectionEnabled
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to Disabled:

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Enable URL-keyed anonymized data collection
```

Default Value:

Unset (Same as Enabled, but user can change)

References:

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

4 Data Loss Prevention

This section contains recommendations to help prevent and protect against unwanted loss of data. Organizations should review these settings and any potential impacts to ensure they makes sense within the environment since they so restrict some browser functionality.

4.1 Allow or deny screen capture

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

Profile Applicability:

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

Description:

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

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

NOTE: This setting 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 other settings:

ScreenCaptureAllowedByOrigins, WindowCaptureAllowedByOrigins, TabCaptureAllowedByOrigins, SameOriginTabCaptureAllowedByOrigins.

Rationale:

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

Impact:

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

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location which should be set to 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:ScreenCaptureAllowed
```

Remediation:

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

Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Allow or deny screen capture\Allow or deny screen capture
--

Default Value:

Unset (Same as Enabled, but user can change)

References:

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

4.2 Content settings

4.2.1 (L2) Ensure 'Control use of the Serial API' is set to 'Enable: Do not allow any site to request access to serial ports via the Serial API' (Automated)

Profile Applicability:

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

Description:

This setting controls website access and use of 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 port and accessing the devices attached.

Impact:

This setting would also prevent legitimate sites from accessing it as well.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location which should be set to 2:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:DefaultSerialGuardSetting
--

Remediation:

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

Do not allow any site to request access to serial ports via the Serial API:

Computer Configuration\Administrative Templates\Google\Google Chrome\Content settings\Control use of the Serial API





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	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.			

4.2.2 (L2) Ensure 'Default Sensors Setting' is set to 'Enabled: 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 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:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location which should be set to 2:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:DefaultSensorsSetting
--

Remediation:

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

Do not allow any site to access sensors:

Computer Configuration\Administrative Templates\Google\Google Chrome\Content settings\Default sensors setting




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.			

4.3 Printing

4.3.1 (L1) Ensure 'Enable submission of documents to Google Cloud print' is set to 'Disabled' (Automated)

Profile Applicability:

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

Description:

This setting enables Google Chrome to submit documents to Google Cloud Print for printing.

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

NOTE: This only affects Google Cloud Print support in Google Chrome. It does not prevent users from submitting print jobs on web sites.

Rationale:

Disabling this option will prevent users from printing possible confidential enterprise documents through the cloud.

Impact:

If this setting is disabled, users cannot print to Google Cloud Print from the Chrome print dialog

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location which should be set to 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:CloudPrintSubmitEnabled
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to Disabled:

```
Computer Configuration\Administrative Templates\Google\Google  
Chrome\Printing\Enable submission of documents to Google Cloud print
```





Default Value:

Unset (Same as Enabled, but user can change)

References:

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

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.			

4.4 (L2) Ensure 'Allow invocation of file selection dialogs' is set to 'Disabled' (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, uploading files, and savings links could pose potential security risks by allowing data to be uploaded to external sites or by downloading malicious files. By not allowing the file selection dialog the end-user will not be prompted for uploads/downloads preventing data exfiltration and possible system infection by malware.

Impact:

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

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location which should be set to 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:AllowFileSelectionDialogs
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Google\Google  
Chrome\Allow invocation of file selection dialogs
```

Default Value:

Unset (Same as Enabled, but user can change)

References:

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

4.5 (L2) Ensure 'Allow or deny audio capture' is set to 'Disabled' (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:

With 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 as to the sites allowed to use this ability for specific approved sites.

Impact:

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

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location which should be set to 0:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:AudioCaptureAllowed
--

Remediation:

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

Computer Configuration\Administrative Templates\Google\Google Chrome\Allow or deny audio capture
--

Default Value:

Unset (Same as Enabled, but user can change)

References:

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

4.6 (L2) Ensure 'Allow or deny video capture' is set to 'Disabled' (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:

With 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 as to the sites allowed to use this ability for specific approved sites.

Impact:

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

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location which should be set to 0:

HKKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:VideoCaptureAllowed

Remediation:

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

Computer Configuration\Administrative Templates\Google\Google Chrome\Allow or deny video capture
--

Default Value:

Unset (Same as Enabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#VideoCaptureAllowed>
2. <https://chromeenterprise.google/policies/#VideoCaptureAllowedUrls>

4.7 (L1) Ensure 'Allow user feedback' is set to 'Disabled' (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 3rd party vendors in an enterprise managed environment.

Impact:

Users will not be able to send feedback to Google.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location which should be set to 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\UserFeedbackAllowed
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Google\Google  
Chrome\Allow user feedback
```

Default Value:

Unset (Same as Enabled, but user can change)

References:

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

4.8 (L2) Ensure 'Controls the mode of DNS-over-HTTPS' is set to 'Enabled: secure' (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)`

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 that is attempting to "phone home." Because DoH encrypts name resolution requests, it can create a security monitoring blind spot.

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 `secure` (text string):

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:DnsOverHttpsMode
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to Enabled: DNS-over-HTTPS without insecure fallback:

```
Computer Configuration\Policies\Administrative Templates\Google\Google  
Chrome\Controls the mode of DNS-over-HTTPS
```

Default Value:

Unset (Same as Enable DNS-over-HTTPS with insecure fallback (automatic), but user can change)

References:

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

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

Profile Applicability:

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

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:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location which should be set to 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:AutofillAddressEnabled
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to Disabled:

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Enable  
AutoFill for addresses
```

Default Value:

Unset (Same as Enabled, but user can change)

References:

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

4.10 (L1) Ensure 'Enable AutoFill for credit cards' is set to 'Disabled' (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:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location which should be set to 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:AutofillCreditCardEnabled
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to Disabled:

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Enable  
AutoFill for credit cards
```

Default Value:

Unset (Same as Enabled, but user can change)

References:

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

4.11 (L1) Ensure 'Import saved passwords from default browser on first run' is set to 'Disabled' (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:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location which should be set to `0`:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:ImportSavedPasswords
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to Disabled:

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Import saved passwords from default browser on first run
```

Default Value:

Unset (Same as Enabled, but user can change)

References:

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

4.12 (L1) Ensure 'List of types that should be excluded from synchronization' is set to 'Enabled: 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 Azure AD Tenant.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location which should be set to `passwords`:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:SyncTypesListDisabled
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: passwords` (Case Sensitive):

```
Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\List of types that should be excluded from synchronization
```

Default Value:

Unset (Same as Disabled, but user can change)

References:

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

5 Forensics (Post Incident)

This section contains recommendations to help in post incident forensics and analysis. Organizations should review these settings and any potential impacts to ensure they makes sense within the environment.

5.1 (L2) Ensure 'Enable guest mode in browser' is set to 'Disabled' (Automated)

Profile Applicability:

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

Description:

This setting controls whether a user may utilized 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:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location which should be set to 0:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:BrowserGuestModeEnabled
--

Remediation:

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

Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Enable guest mode in browser
--

Default Value:

Unset (Same as Enabled, but user can change)

References:

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

5.2 (L2) Ensure 'Incognito mode availability ' is set to 'Enabled: Incognito mode disabled' (Automated)

Profile Applicability:

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

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:

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:IncognitoModeAvailability
```

Remediation:

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

Incognito mode disabled:

```
Computer Configuration\Policies\Administrative Templates\Google\Google  
Chrome\Incognito mode availability
```

Default Value:

Unset (Same as Enabled, but user can change)

References:

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

5.3 (L1) Ensure 'Set disk cache size, in bytes' is set to 'Enabled: 250609664' (Automated)

Profile Applicability:

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

Description:

This setting controls the size of the cache, in bytes, used to store files on the disk.

The recommended state for this setting is: Enabled: 250609664 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 investigators such as Computer Forensics Analysts to be able to retrieve pertinent information to the investigation.

Impact:

Browser cache will take up to 250MB in disk space.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location which should be set to ef00000 (250609664 in hexadecimal format):

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:DiskCacheSize
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to Enabled: 250609664:

```
Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Set disk cache size in bytes
```


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>

Appendix: Recommendation Summary Table

Control		Set Correctly	
		Yes	No
1	Enforced Defaults		
1.1	HTTP authentication		
1.1.1	(L1) Ensure 'Cross-origin HTTP Authentication prompts' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.2	Safe Browsing settings		
1.2.1	(L1) Ensure 'Configure the list of domains on which Safe Browsing will not trigger warnings' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.2.2	(L1) Ensure 'Safe Browsing Protection Level' is set to 'Enabled: Standard Protection' or higher (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.3	(L1) Ensure 'Allow Google Cast to connect to Cast devices on all IP addresses' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.4	(L1) Ensure 'Allow queries to a Google time service' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.5	(L1) Ensure 'Allow the audio sandbox to run' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.6	(L1) Ensure 'Ask where to save each file before downloading' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.7	(L1) Ensure 'Continue running background apps when Google Chrome is closed' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.8	(L2) Ensure 'Control SafeSites adult content filtering' is set to 'Enabled: Filter top level sites (but not embedded iframes) for adult content' specified (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.9	(L1) Ensure 'Determine the availability of variations' is set to 'Disabled' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.10	(L1) Ensure 'Disable Certificate Transparency enforcement for a list of Legacy Certificate Authorities' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.11	(L1) Ensure 'Disable Certificate Transparency enforcement for a list of subjectPublicKeyInfo hashes' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.12	(L1) Ensure 'Disable Certificate Transparency enforcement for a list of URLs' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.13	(L1) Ensure 'Disable saving browser history' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

Control		Set Correctly	
		Yes	No
1.14	(L1) Ensure 'DNS interception checks enabled' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.15	(L1) Ensure 'Enable component updates in Google Chrome' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.16	(L1) Ensure 'Enable globally scoped HTTP auth cache' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.17	(L1) Ensure 'Enable online OCSP/CRL checks' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.18	(L1) Ensure 'Enable Renderer Code Integrity' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.19	(L1) Ensure 'Enable security warnings for command-line flags' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.20	(L1) Ensure 'Enable third party software injection blocking' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.21	(L1) Ensure 'Enables managed extensions to use the Enterprise Hardware Platform API' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.22	(L1) Ensure 'Ephemeral profile' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.23	(L1) Ensure 'Import autofill form data from default browser on first run' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.24	(L1) Ensure 'Import of homepage from default browser on first run' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.25	(L1) Ensure 'Import search engines from default browser on first run' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.26	(L1) Ensure 'List of names that will bypass the HSTS policy check' is set to 'Disabled' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.27	(L1) Ensure 'Origins or hostname patterns for which restrictions on insecure origins should not apply' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.28	(L1) Ensure 'Suppress lookalike domain warnings on domains' is set to 'Disabled' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.29	(L1) Ensure 'Suppress the unsupported OS warning' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.30	(L1) Ensure 'URLs for which local IPs are exposed in WebRTC ICE candidates' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2	Attack Surface Reduction		
2.1	Update settings (Google section of GPO)		
2.1.1	(L1) Ensure 'Update policy override' is set to 'Enabled' with 'Always allow updates (recommended)' or 'Automatic silent updates' specified (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

Control		Set Correctly	
		Yes	No
2.2	Content settings		
2.2.1	(L1) Ensure 'Control use of insecure content exceptions' is set to 'Enabled: Do not allow any site to load mixed content' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.2	(L2) Ensure 'Control use of the Web Bluetooth API' is set to 'Enabled: Do not allow any site to request access to Bluetooth devices via the Web Bluetooth API' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.3	(L2) Ensure 'Control use of the WebUSB API' is set to 'Enabled: Do not allow any site to request access to USB devices via the WebUSB API' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.4	(L2) Ensure 'Default notification setting' is set to 'Enabled: Do not allow any site to show desktop notifications' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3	Extensions		
2.3.1	(L1) Ensure 'Blocks external extensions from being installed' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2	(L1) Ensure 'Configure allowed app/extension types' is set to 'Enabled: extension, hosted_app, platform_app, theme' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3	(L1) Ensure 'Configure extension installation blocklist' is set to 'Enabled: *' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.4	HTTP authentication		
2.4.1	(L1) Ensure 'Supported authentication schemes' is set to 'Enabled: ntlm, negotiate' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.5	Native Messaging		
2.5.1	(L2) Ensure 'Configure native messaging blocklist' is set to 'Enabled: *' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.6	Password manager		
2.6.1	(L1) Ensure 'Enable saving passwords to the password manager' is Explicitly Configured (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.7	Printing		
2.7.1	(L1) Ensure 'Enable Google Cloud Print Proxy' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.8	Remote access (Chrome Remote Desktop)		
2.8.1	Ensure 'Allow remote access connections to this machine' is set to 'Disabled' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.8.2	(L1) Ensure 'Allow remote users to interact with elevated windows in remote assistance sessions' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

Control		Set Correctly	
		Yes	No
2.8.3	(L1) Ensure 'Configure the required domain names for remote access clients' is set to 'Enabled' with a domain defined (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.8.4	(L1) Ensure 'Enable curtaining of remote access hosts' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.8.5	(L1) Ensure 'Enable firewall traversal from remote access host' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.8.6	(L1) Ensure 'Enable or disable PIN-less authentication for remote access hosts' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.8.7	(L1) Ensure 'Enable the use of relay servers by the remote access host' is set to 'Disabled'. (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.9	(L1) Ensure 'Allow download restrictions' is set to 'Enabled: Block dangerous downloads' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.10	(L2) Ensure 'Allow proceeding from the SSL warning page' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.11	(L1) Ensure 'Disable proceeding from the Safe Browsing warning page' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.12	(L1) Ensure 'Enable Chrome Cleanup on Windows' is Configured (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.13	(L1) Ensure 'Enable Site Isolation for every site' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.14	(L2) Ensure 'Force Google SafeSearch' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.15	(L1) Ensure 'Notify a user that a browser relaunch or device restart is recommended or required' is set to 'Enabled: Show a recurring prompt to the user indication that a relaunch is required' specified (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.16	(L1) Ensure 'Proxy settings' is set to 'Enabled' and does not contain "ProxyMode": "auto_detect" (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.17	(L2) Ensure 'Require online OCSP/CRL checks for local trust anchors' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.18	(L1) Ensure 'Set the time period for update notifications' is set to 'Enabled: 86400000' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3	Privacy		
3.1	Content settings		
3.1.1	(L2) Ensure 'Default cookies setting' is set to 'Enabled: Keep cookies for the duration of the session' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.1.2	(L1) Ensure 'Default geolocation setting' is set to 'Enabled: Do not allow any site to track the users' physical location' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.2	Google Cast		

Control		Set Correctly	
		Yes	No
3.2.1	(L1) Ensure 'Enable Google Cast' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3	(L1) Ensure 'Allow websites to query for available payment methods' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.4	(L1) Ensure 'Block third party cookies' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.5	(L2) Ensure 'Browser sign in settings' is set to 'Enabled: Disabled browser sign-in' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6	(L1) Ensure 'Control how Chrome Cleanup reports data to Google' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.7	(L1) Ensure 'Disable synchronization of data with Google' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.8	(L1) Ensure 'Enable alternate error pages' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.9	(L1) Ensure 'Enable deleting browser and download history' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.10	(L1) Ensure 'Enable network prediction' is set to 'Enabled: Do not predict actions on any network connection' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.11	(L1) Ensure 'Enable or disable spell checking web service' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.12	(L1) Ensure 'Enable reporting of usage and crash-related data' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.13	(L1) Ensure 'Enable Safe Browsing for trusted sources' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.14	(L2) Ensure 'Enable search suggestions' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.15	(L2) Ensure 'Enable Translate' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.16	(L1) Ensure 'Enable URL-keyed anonymized data collection' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4	Data Loss Prevention		
4.1	Allow or deny screen capture		
4.1.1	(L2) Ensure 'Allow or deny screen capture' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2	Content settings		
4.2.1	(L2) Ensure 'Control use of the Serial API' is set to 'Enabled: Do not allow any site to request access to serial ports via the Serial API' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.2	(L2) Ensure 'Default Sensors Setting' is set to 'Enabled: Do not allow any site to access sensors' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

Control		Set Correctly	
		Yes	No
4.3	Printing		
4.3.1	(L1) Ensure 'Enable submission of documents to Google Cloud print' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.4	(L2) Ensure 'Allow invocation of file selection dialogs' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.5	(L2) Ensure 'Allow or deny audio capture' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.6	(L2) Ensure 'Allow or deny video capture' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.7	(L1) Ensure 'Allow user feedback' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.8	(L2) Ensure 'Controls the mode of DNS-over-HTTPS' is set to 'Enabled: secure' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.9	(L1) Ensure 'Enable AutoFill for addresses' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.10	(L1) Ensure 'Enable AutoFill for credit cards' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.11	(L1) Ensure 'Import saved passwords from default browser on first run' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.12	(L1) Ensure 'List of types that should be excluded from synchronization' is set to 'Enabled: passwords' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5	Forensics (Post Incident)		
5.1	(L2) Ensure 'Enable guest mode in browser' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2	(L2) Ensure 'Incognito mode availability ' is set to 'Enabled: Incognito mode disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.3	(L1) Ensure 'Set disk cache size, in bytes' is set to 'Enabled: 250609664' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v7 IG 1 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.9	(L1) Ensure 'Determine the availability of variations' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
1.15	(L1) Ensure 'Enable component updates in Google Chrome' is set to 'Enabled'	<input type="checkbox"/>	<input type="checkbox"/>
1.29	(L1) Ensure 'Suppress the unsupported OS warning' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.1.1	(L1) Ensure 'Update policy override' is set to 'Enabled' with 'Always allow updates (recommended)' or 'Automatic silent updates' specified	<input type="checkbox"/>	<input type="checkbox"/>
2.15	(L1) Ensure 'Notify a user that a browser relaunch or device restart is recommended or required' is set to 'Enabled: Show a recurring prompt to the user indication that a relaunch is required' specified	<input type="checkbox"/>	<input type="checkbox"/>
2.18	(L1) Ensure 'Set the time period for update notifications' is set to 'Enabled: 86400000'	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v7 IG 2 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.2.1	(L1) Ensure 'Configure the list of domains on which Safe Browsing will not trigger warnings' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
1.2.2	(L1) Ensure 'Safe Browsing Protection Level' is set to 'Enabled: Standard Protection' or higher	<input type="checkbox"/>	<input type="checkbox"/>
1.3	(L1) Ensure 'Allow Google Cast to connect to Cast devices on all IP addresses' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
1.4	(L1) Ensure 'Allow queries to a Google time service' is set to 'Enabled'	<input type="checkbox"/>	<input type="checkbox"/>
1.7	(L1) Ensure 'Continue running background apps when Google Chrome is closed' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
1.8	(L2) Ensure 'Control SafeSites adult content filtering' is set to 'Enabled: Filter top level sites (but not embedded iframes) for adult content' specified	<input type="checkbox"/>	<input type="checkbox"/>
1.9	(L1) Ensure 'Determine the availability of variations' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
1.15	(L1) Ensure 'Enable component updates in Google Chrome' is set to 'Enabled'	<input type="checkbox"/>	<input type="checkbox"/>
1.21	(L1) Ensure 'Enables managed extensions to use the Enterprise Hardware Platform API' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
1.26	(L1) Ensure 'List of names that will bypass the HSTS policy check' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
1.28	(L1) Ensure 'Suppress lookalike domain warnings on domains' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
1.29	(L1) Ensure 'Suppress the unsupported OS warning' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.1.1	(L1) Ensure 'Update policy override' is set to 'Enabled' with 'Always allow updates (recommended)' or 'Automatic silent updates' specified	<input type="checkbox"/>	<input type="checkbox"/>
2.2.1	(L1) Ensure 'Control use of insecure content exceptions' is set to 'Enabled: Do not allow any site to load mixed content'	<input type="checkbox"/>	<input type="checkbox"/>
2.2.2	(L2) Ensure 'Control use of the Web Bluetooth API' is set to 'Enabled: Do not allow any site to request access to Bluetooth devices via the Web Bluetooth API'	<input type="checkbox"/>	<input type="checkbox"/>
2.2.3	(L2) Ensure 'Control use of the WebUSB API' is set to 'Enabled: Do not allow any site to request access to USB devices via the WebUSB API'	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
2.3.1	(L1) Ensure 'Blocks external extensions from being installed' is set to 'Enabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2	(L1) Ensure 'Configure allowed app/extension types' is set to 'Enabled: extension, hosted_app, platform_app, theme'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3	(L1) Ensure 'Configure extension installation blocklist' is set to 'Enabled: *'	<input type="checkbox"/>	<input type="checkbox"/>
2.4.1	(L1) Ensure 'Supported authentication schemes' is set to 'Enabled: ntlm, negotiate'	<input type="checkbox"/>	<input type="checkbox"/>
2.5.1	(L2) Ensure 'Configure native messaging blocklist' is set to 'Enabled: *'	<input type="checkbox"/>	<input type="checkbox"/>
2.7.1	(L1) Ensure 'Enable Google Cloud Print Proxy' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.10	(L2) Ensure 'Allow proceeding from the SSL warning page' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.11	(L1) Ensure 'Disable proceeding from the Safe Browsing warning page' is set to 'Enabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.12	(L1) Ensure 'Enable Chrome Cleanup on Windows' is Configured	<input type="checkbox"/>	<input type="checkbox"/>
2.14	(L2) Ensure 'Force Google SafeSearch' is set to 'Enabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.15	(L1) Ensure 'Notify a user that a browser relaunch or device restart is recommended or required' is set to 'Enabled: Show a recurring prompt to the user indication that a relaunch is required' specified	<input type="checkbox"/>	<input type="checkbox"/>
2.18	(L1) Ensure 'Set the time period for update notifications' is set to 'Enabled: 86400000'	<input type="checkbox"/>	<input type="checkbox"/>
3.2.1	(L1) Ensure 'Enable Google Cast' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
4.2.1	(L2) Ensure 'Control use of the Serial API' is set to 'Enable: Do not allow any site to request access to serial ports via the Serial API'	<input type="checkbox"/>	<input type="checkbox"/>
4.2.2	(L2) Ensure 'Default Sensors Setting' is set to 'Enabled: Do not allow any site to access sensors'	<input type="checkbox"/>	<input type="checkbox"/>
4.3.1	(L1) Ensure 'Enable submission of documents to Google Cloud print' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v7 IG 3 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.2.1	(L1) Ensure 'Configure the list of domains on which Safe Browsing will not trigger warnings' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
1.2.2	(L1) Ensure 'Safe Browsing Protection Level' is set to 'Enabled: Standard Protection' or higher	<input type="checkbox"/>	<input type="checkbox"/>
1.3	(L1) Ensure 'Allow Google Cast to connect to Cast devices on all IP addresses' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
1.4	(L1) Ensure 'Allow queries to a Google time service' is set to 'Enabled'	<input type="checkbox"/>	<input type="checkbox"/>
1.7	(L1) Ensure 'Continue running background apps when Google Chrome is closed' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
1.8	(L2) Ensure 'Control SafeSites adult content filtering' is set to 'Enabled: Filter top level sites (but not embedded iframes) for adult content' specified	<input type="checkbox"/>	<input type="checkbox"/>
1.9	(L1) Ensure 'Determine the availability of variations' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
1.15	(L1) Ensure 'Enable component updates in Google Chrome' is set to 'Enabled'	<input type="checkbox"/>	<input type="checkbox"/>
1.21	(L1) Ensure 'Enables managed extensions to use the Enterprise Hardware Platform API' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
1.26	(L1) Ensure 'List of names that will bypass the HSTS policy check' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
1.28	(L1) Ensure 'Suppress lookalike domain warnings on domains' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
1.29	(L1) Ensure 'Suppress the unsupported OS warning' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.1.1	(L1) Ensure 'Update policy override' is set to 'Enabled' with 'Always allow updates (recommended)' or 'Automatic silent updates' specified	<input type="checkbox"/>	<input type="checkbox"/>
2.2.1	(L1) Ensure 'Control use of insecure content exceptions' is set to 'Enabled: Do not allow any site to load mixed content'	<input type="checkbox"/>	<input type="checkbox"/>
2.2.2	(L2) Ensure 'Control use of the Web Bluetooth API' is set to 'Enabled: Do not allow any site to request access to Bluetooth devices via the Web Bluetooth API'	<input type="checkbox"/>	<input type="checkbox"/>
2.2.3	(L2) Ensure 'Control use of the WebUSB API' is set to 'Enabled: Do not allow any site to request access to USB devices via the WebUSB API'	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
2.3.1	(L1) Ensure 'Blocks external extensions from being installed' is set to 'Enabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2	(L1) Ensure 'Configure allowed app/extension types' is set to 'Enabled: extension, hosted_app, platform_app, theme'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3	(L1) Ensure 'Configure extension installation blocklist' is set to 'Enabled: *'	<input type="checkbox"/>	<input type="checkbox"/>
2.4.1	(L1) Ensure 'Supported authentication schemes' is set to 'Enabled: ntlm, negotiate'	<input type="checkbox"/>	<input type="checkbox"/>
2.5.1	(L2) Ensure 'Configure native messaging blocklist' is set to 'Enabled: *'	<input type="checkbox"/>	<input type="checkbox"/>
2.7.1	(L1) Ensure 'Enable Google Cloud Print Proxy' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.8.1	Ensure 'Allow remote access connections to this machine' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.8.2	(L1) Ensure 'Allow remote users to interact with elevated windows in remote assistance sessions' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.8.3	(L1) Ensure 'Configure the required domain names for remote access clients' is set to 'Enabled' with a domain defined	<input type="checkbox"/>	<input type="checkbox"/>
2.8.4	(L1) Ensure 'Enable curtaining of remote access hosts' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.8.5	(L1) Ensure 'Enable firewall traversal from remote access host' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.8.6	(L1) Ensure 'Enable or disable PIN-less authentication for remote access hosts' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.8.7	(L1) Ensure 'Enable the use of relay servers by the remote access host' is set to 'Disabled'.	<input type="checkbox"/>	<input type="checkbox"/>
2.10	(L2) Ensure 'Allow proceeding from the SSL warning page' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.11	(L1) Ensure 'Disable proceeding from the Safe Browsing warning page' is set to 'Enabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.12	(L1) Ensure 'Enable Chrome Cleanup on Windows' is Configured	<input type="checkbox"/>	<input type="checkbox"/>
2.14	(L2) Ensure 'Force Google SafeSearch' is set to 'Enabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.15	(L1) Ensure 'Notify a user that a browser relaunch or device restart is recommended or required' is set to 'Enabled: Show a recurring prompt to the user indication that a relaunch is required' specified	<input type="checkbox"/>	<input type="checkbox"/>
2.16	(L1) Ensure 'Proxy settings' is set to 'Enabled' and does not contain "ProxyMode": "auto_detect"	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
2.18	(L1) Ensure 'Set the time period for update notifications' is set to 'Enabled: 86400000'	<input type="checkbox"/>	<input type="checkbox"/>
3.2.1	(L1) Ensure 'Enable Google Cast' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
4.2.1	(L2) Ensure 'Control use of the Serial API' is set to 'Enable: Do not allow any site to request access to serial ports via the Serial API'	<input type="checkbox"/>	<input type="checkbox"/>
4.2.2	(L2) Ensure 'Default Sensors Setting' is set to 'Enabled: Do not allow any site to access sensors'	<input type="checkbox"/>	<input type="checkbox"/>
4.3.1	(L1) Ensure 'Enable submission of documents to Google Cloud print' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v8 IG 1 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.9	(L1) Ensure 'Determine the availability of variations' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
1.15	(L1) Ensure 'Enable component updates in Google Chrome' is set to 'Enabled'	<input type="checkbox"/>	<input type="checkbox"/>
1.29	(L1) Ensure 'Suppress the unsupported OS warning' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.1.1	(L1) Ensure 'Update policy override' is set to 'Enabled' with 'Always allow updates (recommended)' or 'Automatic silent updates' specified	<input type="checkbox"/>	<input type="checkbox"/>
2.15	(L1) Ensure 'Notify a user that a browser relaunch or device restart is recommended or required' is set to 'Enabled: Show a recurring prompt to the user indication that a relaunch is required' specified	<input type="checkbox"/>	<input type="checkbox"/>
2.18	(L1) Ensure 'Set the time period for update notifications' is set to 'Enabled: 86400000'	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v8 IG 2 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.2.1	(L1) Ensure 'Configure the list of domains on which Safe Browsing will not trigger warnings' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
1.2.2	(L1) Ensure 'Safe Browsing Protection Level' is set to 'Enabled: Standard Protection' or higher	<input type="checkbox"/>	<input type="checkbox"/>
1.3	(L1) Ensure 'Allow Google Cast to connect to Cast devices on all IP addresses' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
1.4	(L1) Ensure 'Allow queries to a Google time service' is set to 'Enabled'	<input type="checkbox"/>	<input type="checkbox"/>
1.7	(L1) Ensure 'Continue running background apps when Google Chrome is closed' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
1.8	(L2) Ensure 'Control SafeSites adult content filtering' is set to 'Enabled: Filter top level sites (but not embedded iframes) for adult content' specified	<input type="checkbox"/>	<input type="checkbox"/>
1.9	(L1) Ensure 'Determine the availability of variations' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
1.15	(L1) Ensure 'Enable component updates in Google Chrome' is set to 'Enabled'	<input type="checkbox"/>	<input type="checkbox"/>
1.21	(L1) Ensure 'Enables managed extensions to use the Enterprise Hardware Platform API' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
1.26	(L1) Ensure 'List of names that will bypass the HSTS policy check' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
1.28	(L1) Ensure 'Suppress lookalike domain warnings on domains' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
1.29	(L1) Ensure 'Suppress the unsupported OS warning' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.1.1	(L1) Ensure 'Update policy override' is set to 'Enabled' with 'Always allow updates (recommended)' or 'Automatic silent updates' specified	<input type="checkbox"/>	<input type="checkbox"/>
2.2.1	(L1) Ensure 'Control use of insecure content exceptions' is set to 'Enabled: Do not allow any site to load mixed content'	<input type="checkbox"/>	<input type="checkbox"/>
2.2.2	(L2) Ensure 'Control use of the Web Bluetooth API' is set to 'Enabled: Do not allow any site to request access to Bluetooth devices via the Web Bluetooth API'	<input type="checkbox"/>	<input type="checkbox"/>
2.2.3	(L2) Ensure 'Control use of the WebUSB API' is set to 'Enabled: Do not allow any site to request access to USB devices via the WebUSB API'	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
2.3.1	(L1) Ensure 'Blocks external extensions from being installed' is set to 'Enabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2	(L1) Ensure 'Configure allowed app/extension types' is set to 'Enabled: extension, hosted_app, platform_app, theme'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3	(L1) Ensure 'Configure extension installation blocklist' is set to 'Enabled: *'	<input type="checkbox"/>	<input type="checkbox"/>
2.4.1	(L1) Ensure 'Supported authentication schemes' is set to 'Enabled: ntlm, negotiate'	<input type="checkbox"/>	<input type="checkbox"/>
2.5.1	(L2) Ensure 'Configure native messaging blocklist' is set to 'Enabled: *'	<input type="checkbox"/>	<input type="checkbox"/>
2.7.1	(L1) Ensure 'Enable Google Cloud Print Proxy' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.8.1	Ensure 'Allow remote access connections to this machine' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.8.2	(L1) Ensure 'Allow remote users to interact with elevated windows in remote assistance sessions' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.8.3	(L1) Ensure 'Configure the required domain names for remote access clients' is set to 'Enabled' with a domain defined	<input type="checkbox"/>	<input type="checkbox"/>
2.8.4	(L1) Ensure 'Enable curtaining of remote access hosts' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.8.5	(L1) Ensure 'Enable firewall traversal from remote access host' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.8.6	(L1) Ensure 'Enable or disable PIN-less authentication for remote access hosts' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.8.7	(L1) Ensure 'Enable the use of relay servers by the remote access host' is set to 'Disabled'.	<input type="checkbox"/>	<input type="checkbox"/>
2.10	(L2) Ensure 'Allow proceeding from the SSL warning page' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.11	(L1) Ensure 'Disable proceeding from the Safe Browsing warning page' is set to 'Enabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.12	(L1) Ensure 'Enable Chrome Cleanup on Windows' is Configured	<input type="checkbox"/>	<input type="checkbox"/>
2.14	(L2) Ensure 'Force Google SafeSearch' is set to 'Enabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.15	(L1) Ensure 'Notify a user that a browser relaunch or device restart is recommended or required' is set to 'Enabled: Show a recurring prompt to the user indication that a relaunch is required' specified	<input type="checkbox"/>	<input type="checkbox"/>
2.18	(L1) Ensure 'Set the time period for update notifications' is set to 'Enabled: 86400000'	<input type="checkbox"/>	<input type="checkbox"/>
3.2.1	(L1) Ensure 'Enable Google Cast' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
4.2.1	(L2) Ensure 'Control use of the Serial API' is set to 'Enable: Do not allow any site to request access to serial ports via the Serial API'	<input type="checkbox"/>	<input type="checkbox"/>
4.2.2	(L2) Ensure 'Default Sensors Setting' is set to 'Enabled: Do not allow any site to access sensors'	<input type="checkbox"/>	<input type="checkbox"/>
4.3.1	(L1) Ensure 'Enable submission of documents to Google Cloud print' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v8 IG 3 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.2.1	(L1) Ensure 'Configure the list of domains on which Safe Browsing will not trigger warnings' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
1.2.2	(L1) Ensure 'Safe Browsing Protection Level' is set to 'Enabled: Standard Protection' or higher	<input type="checkbox"/>	<input type="checkbox"/>
1.3	(L1) Ensure 'Allow Google Cast to connect to Cast devices on all IP addresses' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
1.4	(L1) Ensure 'Allow queries to a Google time service' is set to 'Enabled'	<input type="checkbox"/>	<input type="checkbox"/>
1.7	(L1) Ensure 'Continue running background apps when Google Chrome is closed' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
1.8	(L2) Ensure 'Control SafeSites adult content filtering' is set to 'Enabled: Filter top level sites (but not embedded iframes) for adult content' specified	<input type="checkbox"/>	<input type="checkbox"/>
1.9	(L1) Ensure 'Determine the availability of variations' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
1.15	(L1) Ensure 'Enable component updates in Google Chrome' is set to 'Enabled'	<input type="checkbox"/>	<input type="checkbox"/>
1.21	(L1) Ensure 'Enables managed extensions to use the Enterprise Hardware Platform API' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
1.26	(L1) Ensure 'List of names that will bypass the HSTS policy check' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
1.28	(L1) Ensure 'Suppress lookalike domain warnings on domains' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
1.29	(L1) Ensure 'Suppress the unsupported OS warning' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.1.1	(L1) Ensure 'Update policy override' is set to 'Enabled' with 'Always allow updates (recommended)' or 'Automatic silent updates' specified	<input type="checkbox"/>	<input type="checkbox"/>
2.2.1	(L1) Ensure 'Control use of insecure content exceptions' is set to 'Enabled: Do not allow any site to load mixed content'	<input type="checkbox"/>	<input type="checkbox"/>
2.2.2	(L2) Ensure 'Control use of the Web Bluetooth API' is set to 'Enabled: Do not allow any site to request access to Bluetooth devices via the Web Bluetooth API'	<input type="checkbox"/>	<input type="checkbox"/>
2.2.3	(L2) Ensure 'Control use of the WebUSB API' is set to 'Enabled: Do not allow any site to request access to USB devices via the WebUSB API'	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
2.3.1	(L1) Ensure 'Blocks external extensions from being installed' is set to 'Enabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2	(L1) Ensure 'Configure allowed app/extension types' is set to 'Enabled: extension, hosted_app, platform_app, theme'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3	(L1) Ensure 'Configure extension installation blocklist' is set to 'Enabled: *'	<input type="checkbox"/>	<input type="checkbox"/>
2.4.1	(L1) Ensure 'Supported authentication schemes' is set to 'Enabled: ntlm, negotiate'	<input type="checkbox"/>	<input type="checkbox"/>
2.5.1	(L2) Ensure 'Configure native messaging blocklist' is set to 'Enabled: *'	<input type="checkbox"/>	<input type="checkbox"/>
2.7.1	(L1) Ensure 'Enable Google Cloud Print Proxy' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.8.1	Ensure 'Allow remote access connections to this machine' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.8.2	(L1) Ensure 'Allow remote users to interact with elevated windows in remote assistance sessions' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.8.3	(L1) Ensure 'Configure the required domain names for remote access clients' is set to 'Enabled' with a domain defined	<input type="checkbox"/>	<input type="checkbox"/>
2.8.4	(L1) Ensure 'Enable curtaining of remote access hosts' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.8.5	(L1) Ensure 'Enable firewall traversal from remote access host' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.8.6	(L1) Ensure 'Enable or disable PIN-less authentication for remote access hosts' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.8.7	(L1) Ensure 'Enable the use of relay servers by the remote access host' is set to 'Disabled'.	<input type="checkbox"/>	<input type="checkbox"/>
2.10	(L2) Ensure 'Allow proceeding from the SSL warning page' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.11	(L1) Ensure 'Disable proceeding from the Safe Browsing warning page' is set to 'Enabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.12	(L1) Ensure 'Enable Chrome Cleanup on Windows' is Configured	<input type="checkbox"/>	<input type="checkbox"/>
2.14	(L2) Ensure 'Force Google SafeSearch' is set to 'Enabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.15	(L1) Ensure 'Notify a user that a browser relaunch or device restart is recommended or required' is set to 'Enabled: Show a recurring prompt to the user indication that a relaunch is required' specified	<input type="checkbox"/>	<input type="checkbox"/>
2.16	(L1) Ensure 'Proxy settings' is set to 'Enabled' and does not contain "ProxyMode": "auto_detect"	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
2.18	(L1) Ensure 'Set the time period for update notifications' is set to 'Enabled: 86400000'	<input type="checkbox"/>	<input type="checkbox"/>
3.2.1	(L1) Ensure 'Enable Google Cast' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
4.2.1	(L2) Ensure 'Control use of the Serial API' is set to 'Enable: Do not allow any site to request access to serial ports via the Serial API'	<input type="checkbox"/>	<input type="checkbox"/>
4.2.2	(L2) Ensure 'Default Sensors Setting' is set to 'Enabled: Do not allow any site to access sensors'	<input type="checkbox"/>	<input type="checkbox"/>
4.3.1	(L1) Ensure 'Enable submission of documents to Google Cloud print' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: Change History

Date	Version	Changes for this version
May 23, 2017	1.2.0	_Status, Listing Order_ on **[Recommendation] 1.7.2 1.7.2 Configure extension installation whitelist** were updated.
Jun 19, 2018	1.3.0	_Status, Listing Order_ on **[recommendation] 1.12.1 (L1) Ensure 'Supported authentication schemes' is set to 'Enabled' (ntlm, negotiate)** were updated.
Jun 26, 2018	1.3.0	_Listing Order, Status_ on **[section] 1.10.1 New section being proposed by bhowson** were updated.
Jun 26, 2018	1.3.0	_Listing Order, Status_ on **[section] 1.10.2 1.10.1 (L1) Ensure 'Configure native messaging blacklist' is set to 'Enabled' ("*" for all messaging applications)** were updated.
Jan 28, 2019	1.4.0	_Listing Order_ on **[recommendation] 1.1.2.1P (L2) Ensure 'Default cookies setting' is set to 'Enabled' (Keep cookies for the duration of the session)** was updated.
Jan 28, 2019	1.4.0	_Listing Order_ on **[recommendation] 1.1.2.1P (L1) Ensure 'Default Flash Setting' is set to 'Enabled' (Click to Play)** was updated.
Jan 28, 2019	1.4.0	_Status_ on **[section] 2 Google Update** was updated.
Jan 29, 2019	1.4.0	_Status_ on **[section] 3 Applications** was updated.
Feb 6, 2019	1.4.0	_Listing Order_ on **[recommendation] 1.1.4.1P (L1) Ensure 'Configure extension installation blacklist' is set to 'Enabled' ("*" for all extensions)** was updated.
Feb 6, 2019	1.4.0	_Listing Order_ on **[recommendation] 1.1.8.1P (L1) Ensure 'Configure native messaging blacklist' is set to 'Enabled' ("*" for all messaging applications)** was updated.
Feb 6, 2019	1.4.0	_Listing Order_ on **[recommendation] 1.1.15P (L1) Ensure 'Block third party cookies' is set to 'Enabled'** was updated.

Date	Version	Changes for this version
Feb 6, 2019	1.4.0	_Listing Order_ on **[recommendation] 1.1.15P (L1) Ensure 'Block third party cookies' is set to 'Enabled'** was updated.
Feb 6, 2019	1.4.0	_Listing Order_ on **[recommendation] 1.1.15P (L1) Ensure 'Enable Site Isolation for every site' is set to 'Enabled'** was updated.
Feb 8, 2019	1.4.0	_Listing Order_ on **[recommendation] 1.1.15P (L1) Ensure 'Continue running background apps when Google Chrome is closed' is set to 'Disabled'** was updated.
Feb 8, 2019	1.4.0	_Listing Order_ on **[recommendation] 1.1.15P (L1) Ensure 'Block third party cookies' is set to 'Enabled'** was updated.
Feb 8, 2019	1.4.0	_Status, Listing Order_ on **[recommendation] 1.1.12.1 (L1) Ensure 'Choose how to specify proxy server settings' is not set to 'Enabled' with 'Auto detect proxy settings'** were updated.
Feb 20, 2019	1.4.0	_Listing Order, Status_ on **[recommendation] 1.1.1.5 (L1) Ensure 'Configure the required domain names for remote access clients' is set to 'Enabled' with a domain defined** were updated.
Feb 20, 2019	1.4.0	_Listing Order, Status_ on **[recommendation] 1.1.1.6 (L1) Ensure 'Allow remote users to interact with elevated windows in remote assistance sessions' is set to 'Disabled'** were updated.
Feb 20, 2019	1.4.0	_Listing Order, Status_ on **[recommendation] 1.1.1.7 (L1) Ensure 'Enable the use of relay servers by the remote access host' is set to 'Disabled'**. ** were updated.
Feb 20, 2019	1.4.0	_Listing Order, Status_ on **[recommendation] 1.1.1.8 (L1) Ensure 'Allow gubby authentication for remote access hosts' is set to 'Disabled'**. ** were updated.
Feb 20, 2019	1.4.0	_Listing Order, Status_ on **[recommendation] 1.1.2.3 (L1) Ensure 'Default geolocation setting' is set to 'Enabled' with 'Do not allow any site to track the users' physical location'** were updated.

Date	Version	Changes for this version
Feb 20, 2019	1.4.0	_Listing Order_ on **[recommendation] 1.1.2.1P (L2) Ensure 'Default cookies setting' is set to 'Enabled' (Keep cookies for the duration of the session)** was updated.
Mar 5, 2019	1.4.0	_Status, Listing Order, Remediation Procedure, Rationale Statement_ on **[recommendation] 1.1.5.1 (L1) Ensure 'Enable Google Cast' is set to 'Disabled'** were updated.
Mar 5, 2019	1.4.0	_Listing Order, Status_ on **[recommendation] 1.1.2.4 (L2) Ensure 'Default notification setting' is set to 'Enabled' with 'Do not allow any site to show desktop notifications'** were updated.
Mar 7, 2019	1.4.0	_Listing Order, Status, Remediation Procedure_ on **[recommendation] 1.1.25 (L1) Ensure 'Enable AutoFill for credit cards' is set to 'Disabled'** were updated.
Mar 7, 2019	1.4.0	_Listing Order, Status_ on **[recommendation] 1.1.26 (L1) Ensure 'Enable AutoFill for addresses' is set to 'Disabled'** were updated.
Mar 7, 2019	1.4.0	_Listing Order_ on **[recommendation] 1.1.1.1P (L1) Ensure 'Enable curtaining of remote access hosts' is set to 'Disabled'** was updated.
Mar 7, 2019	1.4.0	_Listing Order, Status, Remediation Procedure_ on **[recommendation] 1.1.2.5 (L2) Ensure 'Control use of the Web Bluetooth API' is set to 'Enabled' with 'Do not allow any site to request access to Bluetooth devices via the Web Bluetooth API'** were update
Mar 7, 2019	1.4.0	_Listing Order, Status, Remediation Procedure_ on **[recommendation] 1.1.2.6 (L2) Ensure 'Control use of the WebUSB API' is set to 'Enabled' with 'Do not allow any site to request access to USB devices via the WebUSB API'** were updated.
Mar 7, 2019	1.4.0	_Status, Listing Order, Remediation Procedure_ on **[recommendation] 1.1.4.2 (L1) Ensure 'Configure allowed app/extension types' is set to 'Enabled' with the values 'extension', 'hosted_app', 'platform_app', 'theme' specified** were updated.

Date	Version	Changes for this version
Mar 7, 2019	1.4.0	_Listing Order_ on **[recommendation] 1.1.4.1P (L1) Ensure 'Configure extension installation blacklist' is set to 'Enabled' ("*" for all extensions)** was updated.
Mar 7, 2019	1.4.0	_Listing Order_ on **[recommendation] 1.1.10.1P (L1) Ensure 'Enable saving passwords to the password manager' is set to 'Disabled'** was updated.
Mar 7, 2019	1.4.0	_Status, Listing Order, references_ on **[recommendation] 2.1.1.1 (L1) Ensure 'Update policy override' is set to 'Enabled' with 'Always allow updates (recommended)' or 'Automatic silent updates' specified** were updated.
Mar 7, 2019	1.4.0	_Status, Listing Order_ on **[recommendation] 2.1.2.1 (L1) Ensure 'Update policy override' is set to 'Enabled' with 'Always allow updates (recommended)' or 'Automatic silent updates' specified** were updated.
Mar 8, 2019	1.4.0	_Listing Order, Status, Remediation Procedure_ on **[recommendation] 1.1.27 (L1) Ensure 'Allow download restrictions' is set to 'Enabled' with 'Block dangerous downloads' specified.** were updated.
Mar 8, 2019	1.4.0	_Listing Order, Status, Remediation Procedure_ on **[recommendation] 1.1.28 (L1) Ensure 'Ask where to save each file before downloading' is set to 'Enabled'** were updated.
Mar 8, 2019	1.4.0	_Listing Order, Status_ on **[recommendation] 1.1.29 (L1) Ensure 'Control how Chrome Cleanup reports data to Google' is set to 'Disabled'** were updated.
Mar 8, 2019	1.4.0	_Listing Order, Status_ on **[recommendation] 1.1.30 (L1) Ensure 'Browser sign in settings' is set to 'Enabled' with 'Disabled browser sign-in' specified** were updated.
Mar 8, 2019	1.4.0	_Listing Order, Status_ on **[recommendation] 1.1.31 (L1) Ensure 'Disable proceeding from the Safe Browsing warning page' is set to 'Enabled'** were updated.

Date	Version	Changes for this version
Mar 8, 2019	1.4.0	_Listing Order, Status, Remediation Procedure_ on **[recommendation] 1.1.32 (L1) Ensure 'Disable saving browser history' is set to 'Disabled'** were updated.
Mar 8, 2019	1.4.0	_Listing Order, Status_ on **[recommendation] 1.1.33 (L1) Ensure 'Enable HTTP/0.9 support on non-default ports' is set to 'Disabled'** were updated.
Mar 8, 2019	1.4.0	_Listing Order, Status_ on **[recommendation] 1.1.34 (L1) Ensure 'Enable PAC URL stripping (for https://)' is set to 'Enabled'** were updated.
Mar 8, 2019	1.4.0	_Listing Order, Status, Remediation Procedure_ on **[recommendation] 1.1.35 (L1) Ensure 'Enable Translate' is set to 'Disabled'** were updated.
Mar 8, 2019	1.4.0	_Listing Order, Status, Remediation Procedure_ on **[recommendation] 1.1.36 (L1) Ensure 'Enable component updates in Google Chrome' is set to 'Enabled'** were updated.
Mar 8, 2019	1.4.0	_Listing Order, Status_ on **[recommendation] 1.1.37 (L1) Ensure 'Enable deprecated web platform features for a limited time' is set to 'Disabled'** were updated.
Mar 8, 2019	1.4.0	_Listing Order, Status_ on **[recommendation] 1.1.38 (L1) Ensure 'Enable network prediction' is set to 'Enabled' with 'Do not predict actions on any network connection' selected** were updated.
Mar 8, 2019	1.4.0	_Listing Order, Status, Remediation Procedure_ on **[recommendation] 1.1.39 (L1) Ensure 'Enable search suggestions' is set to 'Disabled'** were updated.
Mar 8, 2019	1.4.0	_Listing Order, Status, Remediation Procedure_ on **[recommendation] 1.1.40 (L1) Ensure 'Enable or disable spell checking web service' is set to 'Disabled'** were updated.
Mar 8, 2019	1.4.0	_Listing Order, Status, Remediation Procedure_ on **[recommendation] 1.1.41 (L1) Ensure 'Enable alternate error pages' is set to 'Disabled'** were updated.

Date	Version	Changes for this version
Mar 8, 2019	1.4.0	_Listing Order, Status, Remediation Procedure_ on **[recommendation] 1.1.42 (L1) Ensure 'Enable third party software injection blocking' is set to 'Enabled'** were updated.
Mar 8, 2019	1.4.0	_Listing Order, Status, Remediation Procedure_ on **[recommendation] 1.1.43 (L1) Ensure 'Extend Flash content setting to all content' is set to 'Disabled'** were updated.
Mar 8, 2019	1.4.0	_Listing Order, Status_ on **[recommendation] 1.1.44 (L1) Ensure 'Notify a user that a browser relaunch or device restart is recommended or required' is set to 'Enabled' with 'Show a recurring prompt to the user indication that a relaunch is required' spe
Mar 8, 2019	1.4.0	_Listing Order, Status_ on **[recommendation] 1.1.45 (L1) Ensure 'Set the time period for update notifications' is set to 'Enabled' with '86400000' (1 day) specified** were updated.
Mar 8, 2019	1.4.0	_Listing Order, Status, Remediation Procedure_ on **[recommendation] 1.1.46 (L1) Ensure 'Suppress the unsupported OS warning' is set to 'Disabled'** were updated.
Mar 8, 2019	1.4.0	_Listing Order, Status, Remediation Procedure_ on **[recommendation] 1.1.47 (L1) Ensure 'Whether online OCSP/CRL checks are performed' is set to 'Disabled'** were updated.
Mar 8, 2019	1.4.0	_Listing Order, Status, Remediation Procedure_ on **[recommendation] 1.1.48 (L2) Ensure 'Whether online OCSP/CRL checks are required for local trust anchors' is set to 'Enabled'** were updated.
Mar 8, 2019	1.4.0	_Listing Order, Status, Remediation Procedure_ on **[recommendation] 1.1.49 (L1) Ensure 'Allow WebDriver to Override Incompatible Policies' is set to 'Disabled'** were updated.

Date	Version	Changes for this version
Mar 8, 2019	1.4.0	_Listing Order, Status, Remediation Procedure_ on **[recommendation] 1.1.50 (L1) Ensure 'Control SafeSites adult content filtering.' is set to 'Enabled' with value 'Do not filter sites for adult content' specified** were updated.
Mar 8, 2019	1.4.0	_Listing Order, Status, Remediation Procedure_ on **[recommendation] 1.1.51 (L1) Ensure 'Disable support for 3D graphics APIs' is set to 'Enabled'** were updated.
Mar 8, 2019	1.4.0	_Listing Order, Status, Remediation Procedure_ on **[recommendation] 1.1.52 (L1) Ensure 'Disable synchronization of data with Google' is set to 'Enabled'** were updated.
Mar 8, 2019	1.4.0	_Listing Order, Status, Remediation Procedure_ on **[recommendation] 1.1.53 (L1) Ensure 'Enable Safe Browsing for trusted sources' is set to 'Disabled'** were updated.
Mar 8, 2019	1.4.0	_Listing Order, Status, Remediation Procedure_ on **[recommendation] 1.1.54 (L1) Ensure 'Origins or hostname patterns for which restrictions on insecure origins should not apply' is set to 'Disabled'** were updated.
Mar 8, 2019	1.4.0	_Listing Order, Status, Remediation Procedure_ on **[recommendation] 1.1.55 (L1) Ensure 'Enable URL-keyed anonymized data collection' is set to 'Disabled'** were updated.
Mar 8, 2019	1.4.0	_Listing Order, Status, Remediation Procedure_ on **[recommendation] 1.1.56 (L1) Ensure 'Enable Chrome Cleanup on Windows' is set to 'Disabled'** were updated.
Mar 8, 2019	1.4.0	_Listing Order, Status, Remediation Procedure_ on **[recommendation] 1.1.57 (L1) Ensure 'Disable Certificate Transparency enforcement for a list of Legacy Certificate Authorities' is set to 'Disabled'** were updated.
Mar 8, 2019	1.4.0	_Listing Order, Status, Remediation Procedure_ on **[recommendation] 1.1.58 (L1) Ensure 'Disable Certificate Transparency enforcement for a list of URLs' is set to 'Disabled'** were updated.

Date	Version	Changes for this version
Mar 8, 2019	1.4.0	_Listing Order, Status, Remediation Procedure_ on **[recommendation] 1.1.59 (L1) Ensure 'Disable Certificate Transparency enforcement for a list of subjectPublicKeyInfo hashes' is set to 'Disabled'** were updated.
Mar 8, 2019	1.4.0	_Listing Order, Status, Remediation Procedure_ on **[recommendation] 1.1.60 (L1) Ensure 'Use built-in DNS client' is set to 'Disabled'** were updated.
Mar 8, 2019	1.4.0	_Listing Order, Status_ on **[recommendation] 1.1.61 New recommendation being proposed by gojo** were updated.
Apr 4, 2019	1.4.0	_Listing Order, Status_ on **[recommendation] 1.1.62 (L1) Ensure 'Enable deleting browser and download history' is set to 'Disabled'** were updated.
May 3, 2019	2.0.0	**[recommendation] 2.2P (L1) Ensure 'Update policy override' is set to 'Enabled' with 'Always allow updates (recommended)' or 'Automatic silent updates' specified** was created.
Aug 16, 2021	2.1.0	DELETE - 1.5 (L1) Ensure 'Enable HTTP/0.9 support on non-default ports' is set to 'Disabled' (Ticket 11881)
Aug 16, 2021	2.1.0	DELETE - 1.6 (L1) Ensure 'Enable deprecated web platform features for a limited time' is set to 'Disabled' (Ticket 11882)
Aug 16, 2021	2.1.0	DELETE - 1.7 (L1) Ensure 'Extend Flash content setting to all content' is set to 'Disabled' (Ticket 13370)
Aug 16, 2021	2.1.0	DELETE - 1.9 (L1) Ensure 'Allow WebDriver to Override Incompatible Policies' is set to 'Disabled' (Ticket 13371)
Aug 16, 2021	2.1.0	DELETE - 2.1 (L1) Ensure 'Default Flash Setting' is set to 'Enabled' (Click to Play) (Ticket 13372)
Aug 16, 2021	2.1.0	DELETE - 2.11 (L1) Ensure 'Allow running plugins that are outdated' is set to 'Disabled' (Ticket 13375)
Sep 22, 2021	2.1.0	DELETE - Section 4 (Managment/visability\performance) (Ticket 13811)

Date	Version	Changes for this version
Sep 22, 2021	2.1.0	DELETE - Section 1.1 (Remote Access) (Ticket 13812)
Oct 7, 2021	2.1.0	DELETE - 1.1.2 (L1) Ensure 'Allow gnubby authentication for remote access hosts' is set to 'Disabled'. (Ticket 11879)
Oct 7, 2021	2.1.0	UPDATE - All Reference URLs in Recommendations Updated (Ticket 13664)
Oct 7, 2021	2.1.0	UPDATE - (L1) Ensure 'Configure allowed app/extension types' is set to 'Enabled' with the values 'extension', 'hosted_app', 'platform_app', 'theme' specified (Ticket 13373)
Oct 7, 2021	2.1.0	UPDATE - (L2) Ensure 'Configure native messaging blocklist' is set to 'Enabled' ("*" for all messaging applications) (Ticket 13016)
Oct 7, 2021	2.1.0	UPDATE - (L2) Ensure 'Whether online OCSP/CRL checks are required for local trust anchors' is set to 'Enabled' (Ticket 13854)
Oct 7, 2021	2.1.0	NEW - (L1) Ensure 'Allow cross-origin HTTP Basic Auth prompts' is set to 'Disabled' (Ticket 13909)
Oct 7, 2021	2.1.0	NEW - (L1) Ensure 'Set disk cache size, in bytes' is set to 'Enabled: 250609664' (Ticket 13907)
Oct 7, 2021	2.1.0	NEW - (L2) Ensure 'Enforce Google SafeSearch' is set to 'Disabled' (Ticket 13905)
Oct 7, 2021	2.1.0	NEW - (L1) Ensure 'Enable renderer code integrity' is set to 'Enabled' (Ticket 13902)
Oct 7, 2021	2.1.0	NEW - (L1) Ensure 'Enable use of ephemeral profiles' is set to 'Disabled' (Ticket 13904)
Oct 7, 2021	2.1.0	NEW - (L1) Ensure 'Enable security warnings for command-line flags' is set to 'Enabled' (Ticket 13903)
Oct 7, 2021	2.1.0	NEW - (L2) Ensure 'Enable guest mode' is set to 'Disabled' (Ticket 13901)
Oct 7, 2021	2.1.0	NEW - (L1) Ensure 'Enable globally scoped HTTP auth cache' is set to 'Disabled' (Ticket 13900)

Date	Version	Changes for this version
Oct 7, 2021	2.1.0	NEW - (L1) Ensure 'DNS interception checks enabled' is set to 'Enabled' (Ticket 13899)
Oct 7, 2021	2.1.0	NEW - (L1) Ensure 'Configure the list of types that are excluded from synchronization' is set to 'Enabled' (Ticket 13898)
Oct 7, 2021	2.1.0	NEW - (L1) Ensure 'Configure the list of names that will bypass the HSTS policy check' is set to 'Disabled' (Ticket 13897)
Oct 7, 2021	2.1.0	NEW - (L1) Ensure 'Allow websites to query for available payment methods' is set to 'Disabled' (Ticket 13896)
Oct 7, 2021	2.1.0	NEW - (L2) Ensure 'Allow users to proceed from the HTTPS warning page' is set to 'Disabled' (Ticket 13895)
Oct 7, 2021	2.1.0	NEW - (L1) Ensure 'Allow user feedback' is set to 'Disabled' (Ticket 13894)
Oct 7, 2021	2.1.0	NEW - (L2) Ensure 'Allow file selection dialog' is set to 'Disabled' (Ticket 13885)
Oct 7, 2021	2.1.0	NEW - (L1) Ensure 'Allow the audio sandbox to run' is set to 'Enabled' (Ticket 13893)
Oct 7, 2021	2.1.0	NEW - (L1) Ensure 'Allow queries to a Browser Network Time service' is set to 'Enabled' (Ticket 13892)
Oct 7, 2021	2.1.0	NEW - (L2) Ensure 'Allow or deny screen capture' is set to 'Disabled' (Ticket 13891)
Oct 7, 2021	2.1.0	NEW - (L1) Ensure 'Allow managed extensions to use the Enterprise Hardware Platform API' is set to 'Disabled' (Ticket 13890)
Oct 7, 2021	2.1.0	NEW - (L1) Ensure 'Allow importing of home page settings' is set to 'Disabled' (Ticket 13888)
Oct 7, 2021	2.1.0	NEW - (L1) Ensure 'Allow importing of autofill form data' is set to 'Disabled' (Ticket 13887)

Date	Version	Changes for this version
Oct 7, 2021	2.1.0	NEW - (L1) Ensure 'Allow Google Cast to connect to Cast devices on all IP addresses' is set to 'Disabled' (Ticket 13886)
Oct 7, 2021	2.1.0	NEW - (L1) Ensure 'Allow importing of search engine settings' is set to 'Disabled' (Ticket 13889)
Oct 7, 2021	2.1.0	NEW - (L2) Ensure 'Allow or deny video capture' is set to 'Disabled' (Ticket 13936)
Oct 7, 2021	2.1.0	NEW - (L2) Ensure 'Allow or block audio capture' is set to 'Disabled' (Ticket 13937)
Oct 7, 2021	2.1.0	NEW - (L2) Ensure 'Control use of the Serial API' is set to 'Enable: Do not allow any site to request access to serial ports via the Serial API' (Ticket 13939)
Oct 7, 2021	2.1.0	NEW - (L1) Ensure 'Determine the availability of variations' is set to 'Disabled' (Ticket 13940)
Oct 7, 2021	2.1.0	NEW - (L1) Ensure 'Suppress lookalike domain warnings on domains' is set to 'Disabled' (Ticket 13941)
Oct 7, 2021	2.1.0	NEW - (L1) Ensure 'Configure the list of domains on which Safe Browsing will not trigger warnings' is set to 'Disabled' (Ticket 13942)
Oct 7, 2021	2.1.0	NEW - (L1) Ensure 'Safe Browsing Protection Level' is set to 'Enabled: Standard Protection' or higher (Ticket 13943)
Oct 7, 2021	2.1.0	NEW - (L2) Ensure 'Controls the mode of DNS-over-HTTPS' is set to 'Enabled: secure' (Ticket 13944)
Oct 7, 2021	2.1.0	NEW - (L1) Ensure 'Allow remote access connections to this machine' is set to 'Disabled' (Ticket 13945)
Oct 7, 2021	2.1.0	UPDATE - (L1) Ensure 'Configure extension installation blacklist' is set to 'Enabled' ("*" for all extensions) (Ticket 11701)
Oct 7, 2021	2.1.0	NEW - (L1) Ensure 'Manage exposure of local IP addresses by WebRTC' is set to 'Disabled' - (Ticket 13906)

Date	Version	Changes for this version
Oct 7, 2021	2.1.0	UPDATE - (L1) Ensure 'Enable component updates in Google Chrome' is set to 'Enabled' (Ticket 13768)
Oct 7, 2021	2.1.0	UPDATE - (L1) Ensure 'Proxy settings' is set to 'Enabled' and does not contain "ProxyMode": "auto_detect" (Ticket 13374)
Oct 7, 2021	2.1.0	NEW - (L2) Ensure 'Incognito mode availability ' is set to 'Disabled' (Ticket 13949)
Oct 7, 2021	2.1.0	NEW - (L1) Ensure 'Blocks external extensions from being installed' is set to 'Enabled' (Ticket 13951)
Oct 7, 2021	2.1.0	NEW - (L1) Ensure 'Control use of insecure content exceptions' is set to 'Enabled: Do not allow any site to load mixed content' (Ticket 13953)
Nov 23, 2021	2.1.0	UPDATE - Recommendation grouping and ordering (Ticket 14181)
Dec 9, 2021	2.1.0	DELETE - (L2) Ensure 'Use built-in DNS client' is set to 'Disabled' (Ticket 13442)