CIS Benchmarks

CIS Google Chrome Benchmark

v2.0.0 - 06-18-2019

Terms of Use

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

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

Table of Contents

Overview

This document provides prescriptive guidance for establishing a secure configuration posture for Google Chrome Browser. This guide was tested against Google Chrome v75. To obtain the latest version of this guide, please visit http://benchmarks.cisecurity.org. If you have questions, comments, or have identified ways to improve this guide, please write us at feedback@cisecurity.org.

Intended Audience

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

Consensus Guidance

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

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

Typographical Conventions

The following typographical conventions are used throughout this guide:

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

Scoring Information

A scoring status indicates whether compliance with the given recommendation impacts the assessed target's benchmark score. The following scoring statuses are used in this benchmark:

Scored

Failure to comply with "Scored" recommendations will decrease the final benchmark score. Compliance with "Scored" recommendations will increase the final benchmark score.

Not Scored

Failure to comply with "Not Scored" recommendations will not decrease the final benchmark score. Compliance with "Not Scored" recommendations will not increase the final benchmark score.

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

CIS would like to thank all of the Google Cloud Team who helped validate and provide all of the great feedback which allowed us to improve the overall benchmark quality.

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

Editor
Brian Howson

Contributor
Jordan Rakoske GSEC, GCWN
Johannes Goerlich
Google Cloud Team

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 Remote access

This section contains recommendations related to Remote Access 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.

1.1.1 (L1) Ensure 'Enable curtaining of remote access hosts' is set to 'Disabled' (Scored)

Profile Applicability:

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

Description:

Chrome allows controls to prevent someone physically present at the host machine from seeing what a user is doing while a remote connection is in progress.

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.

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:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:RemoteAccessHostRequireCur
tain
```

Remediation:

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

```
Computer Configuration\Administrative Templates\Google\Google
Chrome\Configure remote access options\Enable curtaining of remote access
hosts
```

Impact:

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

Default Value:

Disabled.

References:

1. https://www.chromium.org/administrators/policy-list-3#RemoteAccessHostRequireCurtain

CIS Controls:

Version 6

9 Limitation and Control of Network Ports, Protocols, and Services
Limitation and Control of Network Ports, Protocols, and Services

1.1.2 (L1) Ensure 'Allow gnubby authentication for remote access hosts' is set to 'Disabled'. (Scored)

Profile Applicability:

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

Description:

Google Chrome offers to proxy gnubby authentication requests (U2F) across a remote host connection.

Rationale:

Proxying shall not be used to circumvent firewall restrictions.

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:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:RemoteAccessHostAllowGnubb
yAuth
```

Remediation:

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

```
Computer Configuration\Administrative Templates\Google\Google
Chrome\Configure remote access options\Allow gnubby authentication for remote
access hosts
```

Impact:

If this setting is disabled, gnubby authentication requests will not be proxied.

Default Value:

Disabled.

References:

1. https://www.chromium.org/administrators/policy-list-3#RemoteAccessHostAllowGnubbyAuth

CIS Controls:

Version 7

9 Limitation and Control of Network Ports, Protocols, and Services
Limitation and Control of Network Ports, Protocols, and Services

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

Profile Applicability:

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

Description:

Google Chrome offers 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.

Rationale:

Remote users shall not be able to escalate privileges.

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:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:RemoteAccessHostAllowUiAcc
essForRemoteAssistance
```

Remediation:

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

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

Impact:

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.

Default Value:

Disabled.

References:

1. https://www.chromium.org/administrators/policy-list-3#RemoteAccessHostAllowUiAccessForRemoteAssistance

CIS Controls:

Version 7

4 Controlled Use of Administrative Privileges
Controlled Use of Administrative Privileges

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

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.

Rationale:

If this setting is enabled, vulnerable or malicious plugins, apps and processes can continue running even after Chrome has closed.

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:

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

Impact:

If this policy is set to Disabled, background mode is disabled and cannot be controlled by the user in the browser settings.

Default Value:

Disabled.

References:

1. https://www.chromium.org/administrators/policy-list-3#BackgroundModeEnabled

CIS Controls:

Version 6

7 Email and Web Browser Protections
Email and Web Browser Protections

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

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.

Rationale:

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

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:

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

Impact:

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

Default Value:

Enabled. Ask user

References:

1. https://www.chromium.org/administrators/policy-list-3#PromptForDownloadLocation

2. https://www.ghacks.net/2017/05/18/you-should-disable-automatic-downloads-in-chrome-right-now/

CIS Controls:

Version 7

8 Malware Defenses
Malware Defenses

1.4 (L1) Ensure 'Disable saving browser history' is set to 'Disabled' (Scored)

Profile Applicability:

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

Description:

Google Chrome allows to save the browser history.

Rationale:

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

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:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:SavingBrowserHistoryDisabl
ed
```

Remediation:

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

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

Impact:

All user browser history will be saved.

Default Value:

Disabled.

References:

1. https://www.chromium.org/administrators/policy-list-3#SavingBrowserHistoryDisabled

CIS Controls:

Version 7

7.6 Log all URL requests

Log all URL requests from each of the organization's systems, whether onsite or a mobile device, in order to identify potentially malicious activity and assist incident handlers with identifying potentially compromised systems.

1.5 (L1) Ensure 'Enable HTTP/0.9 support on non-default ports' is set to 'Disabled' (Scored)

Profile Applicability:

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

Description:

Non-HTTP services' responses may be read via XHR as their response streams will be interpreted by Chrome as HTTP/0.9. This setting allows to enable HTTP/0.9 on ports other than 80 for HTTP and 443 for HTTPS.

Rationale:

DNS rebinding attacks can be mounted against non-HTTP services to steal their responses cross-protocol.

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:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:Http09OnNonDefaultPortsEna
bled
```

Remediation:

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

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Enable
HTTP/0.9 support on non-default ports
```

Impact:

If this setting is disabled, HTTP/0.9 will be disabled on non-default ports 80/443.

Default Value:

Disabled.

References:

1. https://www.chromium.org/administrators/policy-list-3#Http09OnNonDefaultPortsEnabled

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

1.6 (L1) Ensure 'Enable component updates in Google Chrome' is set to 'Enabled' (Scored)

Profile Applicability:

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

Description:

Google Chrome's Component Updater updates several components of Google Chrome (like the Adobe Flash Player, Widevine DRM, Chrome updater recovery component) on a regular basis.

Rationale:

Google Chrome Updater shall be used to keep the components bundled to Chrome up-to-date.

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:

```
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\Administrative Templates\Google\Google Chrome\Enable
component updates in Google Chrome
```

Impact:

Google Chrome Updater keeps the components bundled to Chrome up-to-date.

Default Value:

Enabled.

References:

1. https://www.chromium.org/administrators/policy-list-3#ComponentUpdatesEnabled

Notes:

To check the current components versions navigate to `chrome://components`.

CIS Controls:

Version 6

4.5 Use Automated Patch Management And Software Update Tools
Deploy automated patch management tools and software update tools for operating system and software/applications on all systems for which such tools are available and safe. Patches should be applied to all systems, even systems that are properly air gapped.

Version 7

3.4 Deploy Automated Operating System Patch Management Tools
Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.

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.

1.7 (L1) Ensure 'Enable deprecated web platform features for a limited time' is set to 'Disabled' (Scored)

Profile Applicability:

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

Description:

Google Chrome offers the ability to re-enable specific deprecated web platform features for a defined period of time.

Rationale:

Deprecated web platform features shall no longer be used.

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:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\EnableDeprecatedWebPlatfor
mFeatures:<number>
```

Remediation:

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

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Enable
deprecated web platform features for a limited time
```

Impact:

If this setting is disabled, deprecated web platform features are no longer being reactivated.

Default Value:

Disabled.

References:

1. https://www.chromium.org/administrators/policy-list-3#EnableDeprecatedWebPlatformFeatures

CIS Controls:

Version 7

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

1.8 (L1) Ensure 'Enable third party software injection blocking' is set to 'Enabled' (Scored)

Profile Applicability:

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

Description:

Google Chrome allows to prevented third party software from injecting executable code into Chrome's processes.

Rationale:

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

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:

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

Impact:

Third party software will be prevented from injecting executable code into Chrome's processes.

Default Value:

Enabled.

References:

1. https://www.chromium.org/administrators/policy-list-3#ThirdPartyBlockingEnabled

CIS Controls:

Version 7

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

1.9 (L1) Ensure 'Extend Flash content setting to all content' is set to 'Disabled' (Scored)

Profile Applicability:

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

Description:

Controls if all Flash content embedded on websites that have been set to allow Flash in content settings - either by the user or by enterprise policy - will be run, including content from other origins or small content.

Rationale:

Cross-domain Flash plugins or "hidden" flash content may be malicious and therefore shall be prevented from being displayed.

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:

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

Remediation:

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

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Extend
Flash content setting to all content
```

Impact:

Flash content from other origins or small content might be blocked.

Default Value:

Disabled.

References:

1. https://www.chromium.org/administrators/policy-list-3#RunAllFlashInAllowMode

CIS Controls:

Version 7

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

1.10 (L1) Ensure 'Suppress the unsupported OS warning' is set to 'Disabled' (Scored)

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.

Rationale:

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

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:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:SuppressUnsupportedOSWarni
ng
```

Remediation:

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

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

Impact:

Unsupported warnings will not be suppressed.

Default Value:

Disabled.

References:

1. https://www.chromium.org/administrators/policy-list-3#SuppressUnsupportedOSWarning

CIS Controls:

Version 7

2.2 Ensure Software is Supported by Vendor

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

1.11 (L1) Ensure 'Whether online OCSP/CRL checks are performed' is set to 'Disabled' (Scored)

Profile Applicability:

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

Description:

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

Rationale:

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.

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:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:EnableOnlineRevocationChec
ks
```

Remediation:

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

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Whether
online OCSP/CRL checks are performed
```

Impact:

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

Default Value:

Disabled.

References:

1. https://www.chromium.org/administrators/policy-list-3#EnableOnlineRevocationChecks
2. https://medium.com/@alexeysamoshkin/how-ssl-certificate-revocation-is-broken-in-practice-af3b63b9cb3

CIS Controls:

Version 7

7 Email and Web Browser Protections
Email and Web Browser Protections

1.12 (L1) Ensure 'Allow WebDriver to Override Incompatible Policies' is set to 'Disabled' (Scored)

Profile Applicability:

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

Description:

The WebDriver feature may override policies which can interfere with its operation. At time of writing this may affect the policies 'Enable Site Isolation for every site' and 'Enable Site Isolation for specified origins'.

Rationale:

Settings of policies shall not be circumvented by any features.

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:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:WebDriverOverridesIncompat
iblePolicies
```

Remediation:

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

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Allow
WebDriver to Override Incompatible Policies
```

Impact:

WebDriver will not be allowed to override incompatible policies.

Default Value:

Disabled.

References:

1. https://www.chromium.org/administrators/policy-list-3#WebDriverOverridesIncompatiblePolicies

CIS Controls:

Version 7

7 Email and Web Browser Protections
Email and Web Browser Protections

1.13 (L1) Ensure 'Control SafeSites adult content filtering' is set to 'Enabled' with value 'Do not filter sites for adult content' specified (Scored)

Profile Applicability:

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

Description:

Google Chrome allows to use the Google Safe Search API to classify URLs as pornographic or not.

Rationale:

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:

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

Remediation:

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

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

Impact:

Sites will not be filtered.

Default Value:

Do not filter sites for adult content.

References:

1. https://www.chromium.org/administrators/policy-list-3#SafeSitesFilterBehavior

CIS Controls:

Version 7

13 Data Protection
Data Protection

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

Profile Applicability:

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

Description:

Google Chrome allows to specify 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.

Rationale:

Insecure contexts shall always be labeled as insecure.

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:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\OverrideSecurityRestrictio
nsOnInsecureOrigin:<number>
```

Remediation:

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

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

Impact:

Insecure contexts are labeled as insecure.

Default Value:

Disabled.

References:

1. https://www.chromium.org/administrators/policy-list-3#OverrideSecurityRestrictionsOnInsecureOrigin

Notes:

This policy will override policy 'Origins or hostname patterns for which restrictions on insecure origins should not apply' UnsafelyTreatInsecureOriginAsSecure(deprecated in M69).

CIS Controls:

Version 7

7 Email and Web Browser Protections
Email and Web Browser Protections

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

Profile Applicability:

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

Description:

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

Rationale:

Legacy Certificate Authorities shall follow the Certificate Transparency policy.

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:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\CertificateTransparencyEnf
orcementDisabledForLegacyCas:<number>
```

Remediation:

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

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

Impact:

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

Default Value:

Disabled.

References:

1. https://www.chromium.org/administrators/policy-list-3#CertificateTransparencyEnforcementDisabledForLegacyCas

CIS Controls:

Version 7

7 Email and Web Browser Protections
Email and Web Browser Protections

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

Profile Applicability:

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

Description:

Google Chrome allows to specify URLs/hostnames for which Certificate Transparency will not be enforced.

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.

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:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\CertificateTransparencyEnf
orcementDisabledForUrls:<number>
```

Remediation:

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

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

Impact:

If this setting is disabled, no URLs are excluded from Certificate Transparency requirements.

Default Value:

Disabled.

References:

1. https://www.chromium.org/administrators/policy-list-3#CertificateTransparencyEnforcementDisabledForUrls

CIS Controls:

Version 7

7 Email and Web Browser Protections
Email and Web Browser Protections

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

Profile Applicability:

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

Description:

Google Chrome allows to exclude certificates by their subjectPublicKeyInfo hashes from enforcing Certificate Transparency requirements.

Rationale:

Certificate Transparency requirements shall be enforced for all certificates.

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:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\CertificateTransparencyEnf
orcementDisabledForCas:<number>
```

Remediation:

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

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

Impact:

If this setting is disabled, no certificates are excluded from Certificate Transparency requirements.

Default Value:

Disabled.

References:

1. https://www.chromium.org/administrators/policy-list-3#CertificateTransparencyEnforcementDisabledForCas

CIS Controls:

Version 7

7 Email and Web Browser Protections
Email and Web Browser Protections

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 (L1) Ensure 'Default Flash Setting' is set to 'Enabled' (Click to Play) (Scored)

Profile Applicability:

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

Description:

Allows you to set whether websites are allowed to automatically run plugins. Automatically running plugins can be either allowed for all websites or denied for all websites.

Rationale:

Malicious plugins can cause browser instability and erratic behavior so setting the value to 'Click to play' will allow a user to only run necessary plugins.

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:

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

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled` with `Click to play` selected from the drop down.

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Content
Settings\Default Flash Setting
```

Impact:

If this setting is enabled, users must click plugins to allow their execution

Default Value:

If this policy is left not set, the user will be able to change this setting manually.

References:

1. https://www.chromium.org/administrators/policy-list-3#DefaultPluginsSetting

CIS Controls:

Version 6

7.2 Uninstall/Disable Unnecessary or Unauthorized Browser Or Email Client Plugins
Uninstall or disable any unnecessary or unauthorized browser or email client plugins or add-on applications. Each plugin shall utilize application / URL whitelisting and only allow the use of the application for pre-approved domains.

Version 7

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

2.2 (L2) Ensure 'Default notification setting' is set to 'Enabled' with 'Do not allow any site to show desktop notifications' (Scored)

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.

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.

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:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:DefaultNotificationsSettin
g
```

Remediation:

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

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

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.

Default Value:

Enabled: AskNotifications.

References:

1. https://www.chromium.org/administrators/policy-list-3#DefaultNotificationsSetting
2. https://www.google.com/chrome/privacy/whitepaper.html#notifications
3. https://medium.com/@BackmaskSWE/push-messages-isnt-secure-enough-69121c683cc6

CIS Controls:

Version 7

7 Email and Web Browser Protections
Email and Web Browser Protections

2.3 (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' (Scored)

Profile Applicability:

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

Description:

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

Rationale:

A malicious website could exploit a vulnerable Bluetooth device.

Audit:

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

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:DefaultWebBluetoothGuardSe
tting
```

Remediation:

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

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

Impact:

If this setting is enabled and set to `Do not allow any site to request access to Bluetooth devices via the Web Bluetooth API`, websites no longer can access nearby Bluetooth device via the API and the user will never be asked.

Default Value:

Enabled: `Allow sites to ask the user to grant access to a nearby Bluetooth device`

References:

1. https://www.chromium.org/administrators/policy-list-3#DefaultWebBluetoothGuardSetting
2. https://webbluetoothcg.github.io/web-bluetooth/use-cases.html#security_privacy

CIS Controls:

Version 7

7 Email and Web Browser Protections
Email and Web Browser Protections

2.4 (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' (Scored)

Profile Applicability:

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

Description:

Google Chrome offers a API which allows the access to connected USB devices from the browser.

Rationale:

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

Audit:

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

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

Remediation:

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

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

Impact:

If this setting is enabled and set to `Do not allow any site to request access to USB devices via the WebUSB API`, websites can no longer access connected USB devices via the API which could also prevent 2FA USB devices from working properly.

Default Value:

Enabled: `Allow sites to ask the user to grant access to a connected USB device`

References:

1. https://www.chromium.org/administrators/policy-list-3#DefaultWebUsbGuardSetting
2. https://www.wired.com/story/chrome-yubikey-phishing-webusb/

CIS Controls:

Version 7

7 Email and Web Browser Protections
Email and Web Browser Protections

2.5 (L1) Ensure 'Configure extension installation blacklist' is set to 'Enabled' ("" for all extensions) (Scored)*

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 blacklisted.

NOTE: Chrome does offer a more granular permission based configuration called `Extension management settings` if blacklisting 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 policy, the benefit would allow access to more extensions to their end-users. See link in reference section

NOTE 2: If Chrome Cleanup is Disabled, users my want to configure the extension blacklist instead of using the Extension Management option. Chrome Cleanup can help protect against malicious extensions when paired with the Extension Management policy.

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 policy `Configure extension installation whitelist` or the policy `Extension management settings`.

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:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\ExtensionInstallBlacklist:
1
```

Remediation:

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

```
Computer Configuration\Administrative Templates\Google\Google
Chrome\Extensions\Configure Extension Installation Blacklist
```

Impact:

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

Default Value:

Disabled. users can install any extension in Google Chrome.

References:

1. https://www.chromium.org/administrators/policy-list-3#ExtensionInstallBlacklist
2. https://www.chromium.org/administrators/policy-list-3#ExtensionSettings

CIS Controls:

Version 6

7.2 Uninstall/Disable Unnecessary or Unauthorized Browser Or Email Client Plugins
Uninstall or disable any unnecessary or unauthorized browser or email client plugins or add-on applications. Each plugin shall utilize application / URL whitelisting and only allow the use of the application for pre-approved domains.

Version 7

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

2.6 (L1) Ensure 'Configure allowed app/extension types' is set to 'Enabled' with the values 'extension', 'hosted_app', 'platform_app', 'theme' specified (Scored)

Profile Applicability:

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

Description:

Enabling this setting allows you to specify which app/extensions types are allowed.

Rationale:

App or extension types that could be misused or are deprecated shall no longer be installed.

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:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\ExtensionAllowedTypes:1
```

Remediation:

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

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

Impact:

Extensions already installed will be removed if it's type is blacklisted and the extension itself is not whitelisted.

Default Value:

Disabled.

References:

1. https://www.chromium.org/administrators/policy-list-3#ExtensionAllowedTypes

CIS Controls:

Version 7

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

2.7 (L2) Ensure 'Configure native messaging blacklist' is set to 'Enabled' ("" for all messaging applications) (Scored)*

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.

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 blacklisted by default, requiring explicit administrative approval of applications for whitelisting. Examples of applications that use native messaging is the 1Password password manager.

Audit:

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

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\NativeMessagingBlacklist:1
```

Remediation:

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

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Native
Messaging\Configure native messaging blacklist
```

Impact:

A blacklist value of '*' means all native messaging hosts are blacklisted unless they are explicitly listed in the whitelist.

Default Value:

If this policy is left not set Google Chrome will load all installed native messaging hosts.

References:

1. https://www.chromium.org/administrators/policy-list-3#NativeMessagingBlacklist

CIS Controls:

Version 6

7.2 Uninstall/Disable Unnecessary or Unauthorized Browser Or Email Client Plugins
Uninstall or disable any unnecessary or unauthorized browser or email client plugins or add-on applications. Each plugin shall utilize application / URL whitelisting and only allow the use of the application for pre-approved domains.

Version 7

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

2.8 (L1) Ensure 'Enable saving passwords to the password manager' is Configured (Not Scored)

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.

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 ON 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.

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:

```
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\Administrative Templates\Google\Google Chrome\Password
manager\Enable the password manager
```

Impact:

If this settings is disabled, users cannot save new passwords but they may still use passwords that have been saved previously.

If this settings is enabled or not configured, users can save passwords.

Default Value:

Enabled.

References:

1. https://www.chromium.org/administrators/policy-list-3#PasswordManagerEnabled
2. https://www.ncsc.gov.uk/blog-post/what-does-ncsc-think-password-managers
3. https://pages.nist.gov/800-63-3/sp800-63b.html

CIS Controls:

Version 6

16 Account Monitoring and Control
Account Monitoring and Control

2.9 (L1) Ensure 'Supported authentication schemes' is set to 'Enabled' (ntlm, negotiate) (Scored)

Profile Applicability:

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

Description:

Specifies which HTTP authentication schemes are supported by Google Chrome.

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.

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:

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

Default Value:

Enabled: basic, digest, ntlm, negotiate

References:

1. https://www.chromium.org/administrators/policy-list-3#AuthSchemes

CIS Controls:

Version 6

16.13 User/Account Authentication Must Be Performed Over Encrypted Channels

Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.

Version 7

16.5 Encrypt Transmittal of Username and Authentication Credentials

Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.

2.10 (L1) Ensure 'Choose how to specify proxy server settings' is not set to 'Enabled' with 'Auto detect proxy settings' (Scored)

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).

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.

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:

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

Remediation:

To establish the recommended configuration via Group Policy, make sure the following UI path is not set to 'Enabled' with 'Auto detect proxy settings':

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Proxy
server\Choose how to specify proxy server settings
```

Impact:

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

Default Value:

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

References:

1. https://www.chromium.org/administrators/policy-list-3#ProxyMode
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:

Version 7

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.

2.11 (L1) Ensure 'Allow running plugins that are outdated' is set to 'Disabled' (Scored)

Profile Applicability:

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

Description:

Chrome enables the use of outdated plugins. By disabling this feature Chrome will not prompt the user to use an outdated plugin.

Rationale:

Running the most up-to-date version of a plugin can reduce the possibility of running a plugin that contains an exploit or security hole.

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:

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

Remediation:

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

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Allow
running plugins that are outdated
```

Impact:

If you disable this setting, outdated plugins will not be used and users will not be asked for permission to run them.

Default Value:

Enabled: Ask User

CIS Controls:

Version 6

7.1 Use Only Fully-supported Web Browsers And Email Clients

Ensure that only fully supported web browsers and email clients are allowed to execute in the organization, ideally only using the latest version of the browsers provided by the vendor in order to take advantage of the latest security functions and fixes.

Version 7

7.1 Ensure Use of Only Fully Supported Browsers and Email Clients

Ensure that only fully supported web browsers and email clients are allowed to execute in the organization, ideally only using the latest version of the browsers and email clients provided by the vendor.

2.12 (L1) Ensure 'Enable Google Cloud Print Proxy' is set to 'Disabled' (Scored)

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.

Rationale:

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

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:

```
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\Administrative Templates\Google\Google
Chrome\Printing\Enable Google Cloud Print Proxy
```

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.

Default Value:

Enabled.

References:

1. https://www.chromium.org/administrators/policy-list-3#CloudPrintProxyEnabled

CIS Controls:

Version 6

13 Data Protection
Data Protection

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

Profile Applicability:

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

Description:

This policy controls is every website will load into its own process.

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.

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:

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

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 IsolateOrigins policy setting to get the best of both worlds, isolation and limited impact for users, by using IsolateOrigins with a list of the sites you want to isolate.

Default Value:

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

References:

1. https://www.chromium.org/Home/chromium-security/site-isolation

CIS Controls:

Version 6

2.4 Use Of Virtual Machines For Risk Management
Virtual machines and/or air-gapped systems should be used to isolate and run applications that are required for business operations but based on higher risk should not be installed within a networked environment.

Version 7

2.10 Physically or Logically Segregate High Risk Applications
Physically or logically segregated systems should be used to isolate and run software that is required for business operations but incur higher risk for the organization.

2.14 (L1) Ensure 'Allow download restrictions' is set to 'Enabled' with 'Block dangerous downloads' specified. (Scored)

Profile Applicability:

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

Description:

Google Chrome allows to block certain types of downloads, and won't let users bypass the security warnings, depending on the classification of Safe Browsing.

Rationale:

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

Audit:

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

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

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled` with value 'Block dangerous downloads' selected from drop down:

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

Impact:

If this setting is enabled, all downloads are allowed, except for those that carry Safe Browsing warnings.

Default Value:

No special restrictions (usual security restrictions based on Safe Browsing analysis results).

References:

1. https://www.chromium.org/administrators/policy-list-3#DownloadRestrictions

CIS Controls:

Version 7

8 Malware Defenses
Malware Defenses

2.15 (L1) Ensure 'Disable proceeding from the Safe Browsing warning page' is set to 'Enabled' (Scored)

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.

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.

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:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:DisableSafeBrowsingProceed
Anyway
```

Remediation:

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

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

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.

Default Value:

Disabled.

References:

1. https://www.chromium.org/administrators/policy-list-3#DisableSafeBrowsingProceedAnyway

CIS Controls:

Version 7

8 Malware Defenses
Malware Defenses

2.16 (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' specified (Scored)

Profile Applicability:

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

Description:

Google Chrome offers to notify users that Google Chrome must be restarted to apply a pending update once the notification period defined by policy 'Set the time period for update notifications' is passed.

Rationale:

Security Updates shall be installed as soon as possible after release.

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:

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

Remediation:

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

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

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.

Default Value:

Enabled: Show a recurring prompt to the user indicating that a relaunch is recommended

References:

1. https://www.chromium.org/administrators/policy-list-3#RelaunchNotification

CIS Controls:

Version 7

3.4 Deploy Automated Operating System Patch Management Tools
Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.

2.17 (L1) Ensure 'Set the time period for update notifications' is set to 'Enabled' with '86400000' (1 day) specified (Scored)

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 Google Chrome must be relaunched to apply a pending update.

Rationale:

Security Updates shall be installed as soon as possible after release.

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:

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

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled` with value `86400000` specified:

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

Impact:

Over this time period, the user will be repeatedly informed of the need for an update until a Browser restart is completed.

Default Value:

Enabled: 604800000 (7 days).

References:

1. https://www.chromium.org/administrators/policy-list-3#RelaunchNotificationPeriod

CIS Controls:

Version 7

3.4 Deploy Automated Operating System Patch Management Tools
Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.

2.18 (L2) Ensure 'Whether online OCSP/CRL checks are required for local trust anchors' is set to 'Enabled' (Scored)

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').

Rationale:

Certificates shall always be validated.

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:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:RequireOnlineRevocationChe
cksForLocalAnchors
```

Remediation:

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

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Whether
online OCSP/CRL checks are required for local trust anchors
```

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.

Default Value:

Disabled. Google Chrome will use the existing online revocation checking settings.

References:

1. https://www.chromium.org/administrators/policy-list-3#RequireOnlineRevocationChecksForLocalAnchors

CIS Controls:

Version 7

7 Email and Web Browser Protections
Email and Web Browser Protections

2.19 (L1) Ensure 'Enable Chrome Cleanup on Windows' is Configured (Not Scored)

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 been found.

Rationale:

The Google Chrome Cleanup is ON 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.

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:

```
HKEY_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\Administrative Templates\Google\Google Chrome\Enable
Chrome Cleanup on Windows
```

Impact:

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.

Default Value:

Enabled.

References:

1. https://www.chromium.org/administrators/policy-list-3#ChromeCleanupEnabled

CIS Controls:

Version 7

8.1 Utilize Centrally Managed Anti-malware Software
Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.

2.20 (L2) Ensure 'Use built-in DNS client' is set to 'Disabled' (Scored)

Profile Applicability:

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

Description:

Google Chrome offers to use a built-in DNS client.

Rationale:

The built-in DNS client shall not be used to circumvent the usage of a trusted DNS server.

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:

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

Remediation:

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

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Use
built-in DNS client
```

Impact:

Users will not be able to use Google DNS-over-TLS and (in future) DNS-over-HTTPS if you disable the Chrome DNS stack.

Default Value:

Enabled.

References:

1. https://www.chromium.org/administrators/policy-list-3#BuiltInDnsClientEnabled

CIS Controls:

Version 7

7.7 Use of DNS Filtering Services

Use DNS filtering services to help block access to known malicious domains.

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

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.

Rationale:

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

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:

```
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` with value `Always allow updates (recommended)` or `Automatic silent updates only` selected from drop down:

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

Impact:

Latest updates are automatically applied at least periodically.

Default Value:

Inherit the value from 'Update policy override default'.

CIS Controls:

Version 6

4.5 Use Automated Patch Management And Software Update Tools
Deploy automated patch management tools and software update tools for operating system and software/applications on all systems for which such tools are available and safe. Patches should be applied to all systems, even systems that are properly air gapped.

Version 7

3.4 Deploy Automated Operating System Patch Management Tools
Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.

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

3 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 (L2) Ensure 'Default cookies setting' is set to 'Enabled' (Keep cookies for the duration of the session) (Scored)

Profile Applicability:

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

Description:

Allows you to set whether websites are allowed to set local data. Setting local data can be either allowed for all websites or denied for all websites.

Rationale:

Permanently stored cookies may be used for malicious intent.

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:

```
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` selected from the drop down.

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

Impact:

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

Default Value:

If this policy is left not set, `AllowCookies` will be used and the user will be able to change it.

References:

1. https://www.chromium.org/administrators/policy-list-3#DefaultCookiesSetting

CIS Controls:

Version 6

13 Data Protection
Data Protection

3.2 (L1) Ensure 'Default geolocation setting' is set to 'Enabled' with 'Do not allow any site to track the users' physical location' (Scored)

Profile Applicability:

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

Description:

Google Chrome supports to track 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.

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.

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:

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

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled` with `Do not allow any site to track the users' physical location` selected from the drop down:

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

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.

Default Value:

Enabled. Ask whenever a site wants to track the users' physical location

References:

1. https://www.chromium.org/administrators/policy-list-3#DefaultGeolocationSetting
2. https://www.w3.org/2010/api-privacy-ws/papers/privacy-ws-24.pdf

CIS Controls:

Version 7

13 Data Protection
Data Protection

3.3 (L1) Ensure 'Enable Google Cast' is set to 'Disabled' (Scored)

Profile Applicability:

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

Description:

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

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.

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:

```
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
```

Impact:

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

Default Value:

Enabled.

References:

1. https://www.chromium.org/administrators/policy-list-3#EnableMediaRouter

CIS Controls:

Version 6

7.2 Uninstall/Disable Unnecessary or Unauthorized Browser Or Email Client Plugins
Uninstall or disable any unnecessary or unauthorized browser or email client plugins or add-on applications. Each plugin shall utilize application / URL whitelisting and only allow the use of the application for pre-approved domains.

Version 7

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

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

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.

NOTE: Third Party Cookies and Tracking Protection are required for many business critical websites, including SalesForce and Office365.

Rationale:

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

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:

```
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
```

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.

Default Value:

Disabled. Third party cookies will be enabled but the user will be able to change that.

References:

1. https://www.chromium.org/administrators/policy-list-3#BlockThirdPartyCookies

CIS Controls:

Version 6

13 Data Protection
Data Protection

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

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.

NOTE: This policy 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.

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:

```
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
```

Impact:

If this setting is disabled, this information is not sent to Google.

Default Value:

Users is asked when first run unless this is enforced.

References:

1. https://www.chromium.org/administrators/policy-list-3#MetricsReportingEnabled

CIS Controls:

Version 6

13 Data Protection
Data Protection

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

Profile Applicability:

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

Description:

Chrome provides a Cleanup-feature to detect unwanted software. The results of the cleanup may be shared with Google to assist with future unwanted software detection. These results will contain file metadata, automatically installed extensions and registry keys.

Rationale:

Anonymous crash/usage data can be used to identify people, companies and information, which can be considered data ex-filtration from company systems.

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:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:ChromeCleanupReportingEnab
led
```

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
```

Impact:

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

Default Value:

Enabled. The user will be asked

References:

1. https://www.chromium.org/administrators/policy-list-3#ChromeCleanupReportingEnabled
2. https://www.google.com/chrome/privacy/whitepaper.html

CIS Controls:

Version 7

13 Data Protection
Data Protection

3.7 (L1) Ensure 'Browser sign in settings' is set to 'Enabled' with 'Disabled browser sign-in' specified (Scored)

Profile Applicability:

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

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.

NOTE: if an organization is a G Suite 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.

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:

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

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled` with value 'Disabled browser sign-in' selected from the drop down.

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

Impact:

If this setting is enabled the user can not sign in to the browser and use google account based services like Chrome sync.

Default Value:

Enabled. Browsers sign in is allowed.

References:

1. https://www.chromium.org/administrators/policy-list-3#BrowserSignin

CIS Controls:

Version 7

16 Account Monitoring and Control
Account Monitoring and Control

3.8 (L1) Ensure 'Enable Translate' is set to 'Disabled' (Scored)

Profile Applicability:

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

Description:

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

Rationale:

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

```
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
```

Impact:

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

Default Value:

Enabled.

References:

1. https://www.chromium.org/administrators/policy-list-3#SpellCheckServiceEnabled

CIS Controls:

Version 7

13 Data Protection

Data Protection

3.9 (L1) Ensure 'Enable network prediction' is set to 'Enabled' with 'Do not predict actions on any network connection' selected (Scored)

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. This feature might lead to connections to websites which the user has not navigated to and may never visit.

Rationale:

Opening connections to resources which may never be visited shall be prevented.

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:

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

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled` with value `Do not predict actions on any network connection` selected from the drop down:

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

Impact:

Users will not be presented with web page predictions.

Default Value:

Enabled.

References:

1. https://www.chromium.org/administrators/policy-list-3#NetworkPredictionOptions

CIS Controls:

Version 7

13 Data Protection
Data Protection

3.10 (L1) Ensure 'Enable search suggestions' is set to 'Disabled' (Scored)

Profile Applicability:

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

Description:

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

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.

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:

```
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
```

Impact:

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

Default Value:

Enabled.

References:

1. https://www.chromium.org/administrators/policy-list-3#SearchSuggestEnabled

CIS Controls:

Version 7

13 Data Protection

Data Protection

3.11 (L1) Ensure 'Enable or disable spell checking web service' is set to 'Disabled' (Scored)

Profile Applicability:

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

Description:

Google Chrome offers the usage of a Google web service to help resolve spelling errors.

Rationale:

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

```
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
```

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 policy only controls the usage of the online service.

Default Value:

Enabled.

References:

1. https://www.chromium.org/administrators/policy-list-3#SpellCheckServiceEnabled

CIS Controls:

Version 7

13 Data Protection
Data Protection

3.12 (L1) Ensure 'Enable alternate error pages' is set to 'Disabled' (Scored)

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'.

Rationale:

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

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:

```
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
```

Impact:

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

Default Value:

Enabled.

References:

1. https://www.chromium.org/administrators/policy-list-3#AlternateErrorPagesEnabled

CIS Controls:

Version 7

13 Data Protection
Data Protection

3.13 (L1) Ensure 'Disable synchronization of data with Google' is set to 'Enabled' (Scored)

Profile Applicability:

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

Description:

Google Chrome offers to synchronize browser data using Google-hosted synchronization services.

NOTE: if your organization allows synchronization of data with Google, then enabling this setting will synchronize saved passwords with Google.

Rationale:

Browser data shall not be synchronized into the Google Cloud.

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:

```
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
```

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.

Default Value:

Disabled.

References:

1. https://www.chromium.org/administrators/policy-list-3#SyncDisabled

CIS Controls:

Version 7

13 Data Protection
Data Protection

3.14 (L1) Ensure 'Enable Safe Browsing for trusted sources' is set to 'Disabled' (Scored)

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 policy 'Configure the list of domains on which Safe Browsing will not trigger warnings'.

Rationale:

Information requested from trusted sources shall not be sent to Google's safe browsing servers.

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:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:SafeBrowsingForTrustedSour
cesEnabled
```

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
```

Impact:

If this setting is disabled files downloaded from intranet resources will not be checked by Google Services.

Default Value:

Enabled.

References:

1. https://www.chromium.org/administrators/policy-list-3#SafeBrowsingForTrustedSourcesEnabled

CIS Controls:

Version 7

13 Data Protection
Data Protection

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

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.

Rationale:

Anonymized data collection shall be disabled, since it is unclear which information exactly is 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:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:UrlKeyedAnonymizedDataColl
ectionEnabled
```

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
```

Impact:

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

Default Value:

Enabled.

References:

1. https://www.chromium.org/administrators/policy-list-3#UrlKeyedAnonymizedDataCollectionEnabled

CIS Controls:

Version 7

13 Data Protection
Data Protection

3.16 (L1) Ensure 'Enable deleting browser and download history' is set to 'Disabled' (Scored)

Profile Applicability:

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

Description:

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

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.

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:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:AllowDeletingBrowserHistor
y
```

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
```

Impact:

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

Default Value:

Enabled.

References:

1. https://www.chromium.org/administrators/policy-list-3#AllowDeletingBrowserHistory

CIS Controls:

Version 7

13 Data Protection
Data Protection

4 Management/visibility/performance

This section contains recommendations around the management, visibility and performance of Google Chrome.

4.1 Remote access

This section contains recommendations that are related to remote access.

4.1.1 (L1) Ensure 'Enable firewall traversal from remote access host' is set to 'Disabled' (Scored)

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.

Rationale:

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

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:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:RemoteAccessHostFirewallTr
aversal
```

Remediation:

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

```
Computer Configuration\Administrative Templates\Google\Google
Chrome\Configure remote access options\Enable firewall traversal from remote
access host
```

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.

Default Value:

Enabled.

References:

1. https://www.chromium.org/administrators/policy-list-3#RemoteAccessHostFirewallTraversal

CIS Controls:

Version 6

9 Limitation and Control of Network Ports, Protocols, and Services
Limitation and Control of Network Ports, Protocols, and Services

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

Profile Applicability:

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

Description:

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

Rationale:

If this setting is enabled or not configured, users can opt to pair clients and hosts at connection time, eliminating the need to enter a 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:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:RemoteAccessHostAllowClien
tPairing
```

Remediation:

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

```
Computer Configuration\Administrative Templates\Google\Google
Chrome\Configure remote access options\Enable or disable PIN-less
authentication
```

Impact:

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

Default Value:

Enabled.

References:

1. https://www.chromium.org/administrators/policy-list-3#RemoteAccessHostAllowClientPairing

CIS Controls:

Version 6

9 Limitation and Control of Network Ports, Protocols, and Services
Limitation and Control of Network Ports, Protocols, and Services

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

Profile Applicability:

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

Description:

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

Rationale:

Relay servers shall not be used to circumvent firewall restrictions.

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:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:RemoteAccessHostAllowRelay
edConnection
```

Remediation:

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

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

Impact:

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

Default Value:

Enabled.

References:

1. https://www.chromium.org/administrators/policy-list-3#RemoteAccessHostAllowRelayedConnection

CIS Controls:

Version 7

9 Limitation and Control of Network Ports, Protocols, and Services
Limitation and Control of Network Ports, Protocols, and Services

4.1.4 (L1) Ensure 'Configure the required domain names for remote access clients' is set to 'Enabled' with a domain defined (Not Scored)

Profile Applicability:

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

Description:

Chrome allows the user to configure a list of required host domain that is imposed on remote access hosts. When enabled, hosts can only be shared using accounts that are registered to the specified domains.

Rationale:

Remote assistance connections shall be restricted.

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:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\RemoteAccessHostClientDoma
inList:<number>
```

Remediation:

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

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

Impact:

If this setting is enabled, clients from the specified domains only can connect to the host.

Default Value:

Disabled.

References:

1. https://www.chromium.org/administrators/policy-list-3#RemoteAccessHostClientDomainList

CIS Controls:

Version 7

9 Limitation and Control of Network Ports, Protocols, and Services
Limitation and Control of Network Ports, Protocols, and Services

5 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.

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

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.

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.

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:

```
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
```

Impact:

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

Default Value:

Enabled.

References:

1. https://www.chromium.org/administrators/policy-list-3#CloudPrintSubmitEnabled

CIS Controls:

Version 6

13 Data Protection
Data Protection

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

Profile Applicability:

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

Description:

This setting controls if saved passwords from the default browser can be imported.

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/.

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:

```
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
```

Impact:

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

Default Value:

Enabled. Ask user to import.

References:

1. https://www.chromium.org/administrators/policy-list-3#ImportSavedPasswords

CIS Controls:

Version 6

16 Account Monitoring and Control

Account Monitoring and Control

5.3 (L1) Ensure 'Enable AutoFill for credit cards' is set to 'Disabled' (Scored)

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.

Rationale:

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

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:

```
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
```

Impact:

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

Default Value:

Enabled.

References:

1. https://www.chromium.org/administrators/policy-list-3#AutofillCreditCardEnabled

CIS Controls:

Version 7

13 Data Protection
Data Protection

5.4 (L1) Ensure 'Enable AutoFill for addresses' is set to 'Disabled' (Scored)

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.

Rationale:

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

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:

```
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
```

Impact:

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

Default Value:

Enabled.

References:

1. https://www.chromium.org/administrators/policy-list-3#AutofillAddressEnabled

CIS Controls:

Version 7

13 Data Protection
Data Protection

Appendix: Summary Table

Control		Set Correctly	
		Yes	No
1	**Enforced Defaults**		
1.1	**Remote access**		
1.1.1	(L1) Ensure 'Enable curtaining of remote access hosts' is set to 'Disabled' (Scored)	□	□
1.1.2	(L1) Ensure 'Allow gnubby authentication for remote access hosts' is set to 'Disabled'. (Scored)	□	□
1.1.3	(L1) Ensure 'Allow remote users to interact with elevated windows in remote assistance sessions' is set to 'Disabled' (Scored)	□	□
1.2	(L1) Ensure 'Continue running background apps when Google Chrome is closed' is set to 'Disabled' (Scored)	□	□
1.3	(L1) Ensure 'Ask where to save each file before downloading' is set to 'Enabled' (Scored)	□	□
1.4	(L1) Ensure 'Disable saving browser history' is set to 'Disabled' (Scored)	□	□
1.5	(L1) Ensure 'Enable HTTP/0.9 support on non-default ports' is set to 'Disabled' (Scored)	□	□
1.6	(L1) Ensure 'Enable component updates in Google Chrome' is set to 'Enabled' (Scored)	□	□
1.7	(L1) Ensure 'Enable deprecated web platform features for a limited time' is set to 'Disabled' (Scored)	□	□
1.8	(L1) Ensure 'Enable third party software injection blocking' is set to 'Enabled' (Scored)	□	□
1.9	(L1) Ensure 'Extend Flash content setting to all content' is set to 'Disabled' (Scored)	□	□
1.10	(L1) Ensure 'Suppress the unsupported OS warning' is set to 'Disabled' (Scored)	□	□
1.11	(L1) Ensure 'Whether online OCSP/CRL checks are performed' is set to 'Disabled' (Scored)	□	□
1.12	(L1) Ensure 'Allow WebDriver to Override Incompatible Policies' is set to 'Disabled' (Scored)	□	□
1.13	(L1) Ensure 'Control SafeSites adult content filtering' is set to 'Enabled' with value 'Do not filter sites for adult content' specified (Scored)	□	□
1.14	(L1) Ensure 'Origins or hostname patterns for which restrictions on insecure origins should not apply' is set to 'Disabled' (Scored)	□	□
1.15	(L1) Ensure 'Disable Certificate Transparency enforcement	□	□

	for a list of Legacy Certificate Authorities' is set to 'Disabled' (Scored)		
1.16	(L1) Ensure 'Disable Certificate Transparency enforcement for a list of URLs' is set to 'Disabled' (Scored)	□	□
1.17	(L1) Ensure 'Disable Certificate Transparency enforcement for a list of subjectPublicKeyInfo hashes' is set to 'Disabled' (Scored)	□	□
2	**Attack Surface Reduction**		
2.1	(L1) Ensure 'Default Flash Setting' is set to 'Enabled' (Click to Play) (Scored)	□	□
2.2	(L2) Ensure 'Default notification setting' is set to 'Enabled' with 'Do not allow any site to show desktop notifications' (Scored)	□	□
2.3	(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' (Scored)	□	□
2.4	(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' (Scored)	□	□
2.5	(L1) Ensure 'Configure extension installation blacklist' is set to 'Enabled' ("*" for all extensions) (Scored)	□	□
2.6	(L1) Ensure 'Configure allowed app/extension types' is set to 'Enabled' with the values 'extension', 'hosted_app', 'platform_app', 'theme' specified (Scored)	□	□
2.7	(L2) Ensure 'Configure native messaging blacklist' is set to 'Enabled' ("*" for all messaging applications) (Scored)	□	□
2.8	(L1) Ensure 'Enable saving passwords to the password manager' is Configured (Not Scored)	□	□
2.9	(L1) Ensure 'Supported authentication schemes' is set to 'Enabled' (ntlm, negotiate) (Scored)	□	□
2.10	(L1) Ensure 'Choose how to specify proxy server settings' is not set to 'Enabled' with 'Auto detect proxy settings' (Scored)	□	□
2.11	(L1) Ensure 'Allow running plugins that are outdated' is set to 'Disabled' (Scored)	□	□
2.12	(L1) Ensure 'Enable Google Cloud Print Proxy' is set to 'Disabled' (Scored)	□	□
2.13	(L1) Ensure 'Enable Site Isolation for every site' is set to 'Enabled' (Scored)	□	□
2.14	(L1) Ensure 'Allow download restrictions' is set to 'Enabled' with 'Block dangerous downloads' specified. (Scored)	□	□
2.15	(L1) Ensure 'Disable proceeding from the Safe Browsing warning page' is set to 'Enabled' (Scored)	□	□
2.16	(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' specified (Scored)		
2.17	(L1) Ensure 'Set the time period for update notifications' is set to 'Enabled' with '86400000' (1 day) specified (Scored)	□	□
2.18	(L2) Ensure 'Whether online OCSP/CRL checks are required for local trust anchors' is set to 'Enabled' (Scored)	□	□
2.19	(L1) Ensure 'Enable Chrome Cleanup on Windows' is Configured (Not Scored)	□	□
2.20	(L2) Ensure 'Use built-in DNS client' is set to 'Disabled' (Scored)	□	□
2.21	(L1) Ensure 'Update policy override' is set to 'Enabled' with 'Always allow updates (recommended)' or 'Automatic silent updates' specified (Scored)	□	□
3	**Privacy**		
3.1	(L2) Ensure 'Default cookies setting' is set to 'Enabled' (Keep cookies for the duration of the session) (Scored)	□	□
3.2	(L1) Ensure 'Default geolocation setting' is set to 'Enabled' with 'Do not allow any site to track the users' physical location' (Scored)	□	□
3.3	(L1) Ensure 'Enable Google Cast' is set to 'Disabled' (Scored)	□	□
3.4	(L1) Ensure 'Block third party cookies' is set to 'Enabled' (Scored)	□	□
3.5	(L1) Ensure 'Enable reporting of usage and crash-related data' is set to 'Disabled' (Scored)	□	□
3.6	(L1) Ensure 'Control how Chrome Cleanup reports data to Google' is set to 'Disabled' (Scored)	□	□
3.7	(L1) Ensure 'Browser sign in settings' is set to 'Enabled' with 'Disabled browser sign-in' specified (Scored)	□	□
3.8	(L1) Ensure 'Enable Translate' is set to 'Disabled' (Scored)	□	□
3.9	(L1) Ensure 'Enable network prediction' is set to 'Enabled' with 'Do not predict actions on any network connection' selected (Scored)	□	□
3.10	(L1) Ensure 'Enable search suggestions' is set to 'Disabled' (Scored)	□	□
3.11	(L1) Ensure 'Enable or disable spell checking web service' is set to 'Disabled' (Scored)	□	□
3.12	(L1) Ensure 'Enable alternate error pages' is set to 'Disabled' (Scored)	□	□
3.13	(L1) Ensure 'Disable synchronization of data with Google' is set to 'Enabled' (Scored)	□	□
3.14	(L1) Ensure 'Enable Safe Browsing for trusted sources' is set to 'Disabled' (Scored)	□	□
3.15	(L1) Ensure 'Enable URL-keyed anonymized data collection' is set to 'Disabled' (Scored)	□	□

3.16	(L1) Ensure 'Enable deleting browser and download history' is set to 'Disabled' (Scored)	□	□
4	**Management/visibility/performance**		
4.1	**Remote access**		
4.1.1	(L1) Ensure 'Enable firewall traversal from remote access host' is set to 'Disabled' (Scored)	□	□
4.1.2	(L1) Ensure 'Enable or disable PIN-less authentication for remote access hosts' is set to 'Disabled' (Scored)	□	□
4.1.3	(L1) Ensure 'Enable the use of relay servers by the remote access host' is set to 'Disabled'. (Scored)	□	□
4.1.4	(L1) Ensure 'Configure the required domain names for remote access clients' is set to 'Enabled' with a domain defined (Not Scored)	□	□
5	**Data Loss Prevention**		
5.1	(L1) Ensure 'Enable submission of documents to Google Cloud print' is set to 'Disabled' (Scored)	□	□
5.2	(L1) Ensure 'Import saved passwords from default browser on first run' is set to 'Disabled' (Scored)	□	□
5.3	(L1) Ensure 'Enable AutoFill for credit cards' is set to 'Disabled' (Scored)	□	□
5.4	(L1) Ensure 'Enable AutoFill for addresses' is set to 'Disabled' (Scored)	□	□

Appendix: Change History

Date	Version	Changes for this version
10-30-15	1.0.0	Initial Release
3-15-16	1.1.0	text to update on benchmarks_rule_1.11.1_Set_Enable_the_password_manager_to_Disabled
3-15-16	1.1.0	Removed version from Title
3-15-16	1.1.0	Updated all recommendation titles to include level and new wording.
6-28-17	1.2.0	Added Controls Mappings to all recommendations
6-28-17	1.2.0	Set 'Allow invocation of file selection dialogs' to Enabled - description / rationale error – Ticket #5105
6-28-17	1.2.0	Remove - (L1) Ensure 'Allow users to show passwords in Password Manager' is set to 'Disabled' – Deprecated – Ticket #4767
6-28-17	1.2.0	Remove - (L1) Ensure 'Specify a list of Disabled Plugins' is set to 'Enabled' - Deprecated – Ticket #4764
6-28-17	1.2.0	Remove - Set 'Enable alternate error pages' to Disabled – Ticket #5106
8-15-18	1.3.0	UPDATE - Policy name/audit consistency – Ticket #6519
8-15-18	1.3.0	REMOVE- deprecated plugin sections – Ticket #6073
8-15-18	1.3.0	UPDATE - Policy is renamed to "Default Flash setting" – Ticket #6520
8-15-18	1.3.0	UPDATE - RemoteAccessHostClientDomain deprecated – Ticket #5519
8-15-18	1.3.0	UPDATE - 1.3.2 (L1) Ensure 'Configure the required domain name for remote access hosts' is set to 'Enabled' -- Unclear Guidance – Ticket #4765
8-15-18	1.3.0	UPDATE – Created new platform file to work on more installations. – Ticket #6249

8-15-18	1.3.0	UPDATE - 1.4.2 (L1) Ensure 'Default Plugin Setting' is set to 'Enabled' (Click to Play) - GPO wording does not match – Ticket #6117
8-15-18	1.3.0	UPDATE - 1.4.2 (L1) Ensure 'Default Plugin Setting' is set to 'Enabled' - Unclear Guidance – Ticket #4766
8-15-18	1.3.0	ADD - 1.1.8.1 (L1) Ensure `Configure native messaging blacklist` is set to 'Enabled' ("*" for all messaging applications) – Ticket #6852
8-15-18	1.3.0	ADD - 1.1.11.1 (L1) Ensure 'Supported authentication schemes' is set to 'Enabled' (ntlm, negotiate) – Ticket #6853
8-15-18	1.3.0	ADD -1.1.22 (L1) Ensure ‘Enable Site Isolation for every site’ is set to ‘Enabled’ – Ticket #6854
8-15-18	1.3.0	UPDATE – All sections according to the Group Policy Layout using the Newest ADMX templates.
6-18-19	2.0.0	UPDATE - Benchmark Structure Ticket #8360
6-18-19	2.0.0	ADD - 4.1 (L1) Ensure 'Enable the use of relay servers by the remote access host' is set to 'Disabled' Ticket #8038
6-18-19	2.0.0	ADD - 3 (L1) Ensure 'Default geolocation setting' is set to 'Enabled' with 'Do not allow any site to track the users' physical location' Ticket #8040
6-18-19	2.0.0	ADD - 2 (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' Ticket #8100
6-18-19	2.0.0	ADD - 2 (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' Ticket #8101
6-18-19	2.0.0	ADD - 2 (L2) Ensure 'Default notification setting' is set to 'Enabled' with 'Do not allow any site to show desktop notifications' Ticket #8102
6-18-19	2.0.0	ADD - 2 (L1) Ensure 'Configure allowed app/extension types' is set to 'Enabled' with the values 'extension', 'hosted_app', 'platform_app', 'theme' specified Ticket #8103
6-18-19	2.0.0	ADD - 3 (L1) Ensure 'Enable Google Cast' is set to 'Disabled' Ticket #8104

6-18-19	2.0.0	ADD - 5 (L1) Ensure 'Enable AutoFill for credit cards' is set to 'Disabled' Ticket #8105
6-18-19	2.0.0	ADD - 2 (L1) Ensure 'Update policy override' is set to 'Enabled' with 'Always allow updates (recommended)' or 'Automatic silent updates' specified Ticket #8107
6-18-19	2.0.0	ADD - 5 (L1) Ensure 'Enable AutoFill for addresses' is set to 'Disabled' Ticket #8106
6-18-19	2.0.0	ADD - 2 (L1) Ensure 'Allow download restrictions' is set to 'Enabled' with 'Block dangerous downloads' specified. Ticket #8115
6-18-19	2.0.0	ADD - 1 (L1) Ensure 'Ask where to save each file before downloading' is set to 'Enabled' Ticket #8116
6-18-19	2.0.0	ADD - 3 (L1) Ensure 'Control how Chrome Cleanup reports data to Google' is Configured Ticket #8117
6-18-19	2.0.0	ADD - 2 (L1) Ensure 'Disable proceeding from the Safe Browsing warning page' is set to 'Enabled' Ticket #8119
6-18-19	2.0.0	ADD - 1 (L1) Ensure 'Disable saving browser history' is set to 'Disabled' Ticket #8120
6-18-19	2.0.0	ADD - 1 (L1) Ensure 'Enable HTTP/0.9 support on non-default ports' is set to 'Disabled' Ticket #8121
6-18-19	2.0.0	ADD - 3 (L1) Ensure 'Browser sign in settings' is set to 'Enabled' with 'Disabled browser sign-in' specified Ticket #8118
6-18-19	2.0.0	ADD - 3 (L1) Ensure 'Enable Translate' is set to 'Disabled' Ticket #8123
6-18-19	2.0.0	ADD - 1 (L1) Ensure 'Enable component updates in Google Chrome' is set to 'Enabled' Ticket #8124
6-18-19	2.0.0	ADD - 1 (L1) Ensure 'Enable deprecated web platform features for a limited time' is set to 'Disabled' Ticket #8125
6-18-19	2.0.0	ADD - 3 (L1) Ensure 'Enable network prediction' is set to 'Enabled' with 'Do not predict actions on any network connection' selected Ticket #8126

6-18-19	2.0.0	ADD - 3 (L1) Ensure 'Enable search suggestions' is set to 'Disabled' Ticket #8127
6-18-19	2.0.0	ADD - 3 (L1) Ensure 'Enable or disable spell checking web service' is set to 'Disabled' Ticket #8128
6-18-19	2.0.0	ADD - 3 (L1) Ensure 'Enable alternate error pages' is set to 'Disabled' Ticket #8129
6-18-19	2.0.0	ADD - 1 (L1) Ensure 'Enable third party software injection blocking' is set to 'Enabled' Ticket #8130
6-18-19	2.0.0	ADD - 1 (L1) Ensure 'Extend Flash content setting to all content' is set to 'Disabled' Ticket #8131
6-18-19	2.0.0	ADD - 2 (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' specified Ticket #8132
6-18-19	2.0.0	ADD - 2 (L1) Ensure 'Set the time period for update notifications' is set to 'Enabled' with '86400000' (1 day) specified Ticket #8133
6-18-19	2.0.0	ADD - 1 (L1) Ensure 'Suppress the unsupported OS warning' is set to 'Disabled' Ticket #8134
6-18-19	2.0.0	ADD - 1 (L1) Ensure 'Whether online OCSP/CRL checks are performed' is set to 'Disabled' Ticket #8135
6-18-19	2.0.0	ADD - 2 (L2) Ensure 'Whether online OCSP/CRL checks are required for local trust anchors' is set to 'Enabled' Ticket #8136
6-18-19	2.0.0	ADD - 1 (L1) Ensure 'Allow WebDriver to Override Incompatible Policies' is set to 'Disabled' Ticket #8137
6-18-19	2.0.0	ADD - 1 (L1) Ensure 'Control SafeSites adult content filtering' is set to 'Enabled' with value 'Do not filter sites for adult content' specified Ticket #8138
6-18-19	2.0.0	ADD - 3 (L1) Ensure 'Disable synchronization of data with Google' is set to 'Enabled' Ticket #8140
6-18-19	2.0.0	ADD - 3 (L1) Ensure 'Enable Safe Browsing for trusted sources' is set to

		'Disabled' Ticket #8141
6-18-19	2.0.0	ADD - 1 (L1) Ensure 'Origins or hostname patterns for which restrictions on insecure origins should not apply' is set to 'Disabled' Ticket #8142
6-18-19	2.0.0	ADD - 3 (L1) Ensure 'Enable URL-keyed anonymized data collection' is set to 'Disabled' Ticket #8143
6-18-19	2.0.0	ADD - 1 (L1) Ensure 'Disable Certificate Transparency enforcement for a list of Legacy Certificate Authorities' is set to 'Disabled' Ticket #8145
6-18-19	2.0.0	ADD - 1 (L1) Ensure 'Disable Certificate Transparency enforcement for a list of URLs' is set to 'Disabled' Ticket #8146
6-18-19	2.0.0	ADD - 1 (L1) Ensure 'Disable Certificate Transparency enforcement for a list of subjectPublicKeyInfo hashes' is set to 'Disabled' Ticket #8147
6-18-19	2.0.0	ADD - 2 (L2) Ensure 'Use built-in DNS client' is set to 'Disabled' Ticket #8149
6-18-19	2.0.0	REMOVE - (L1) Ensure 'Enable AutoFill' is set to 'Disabled' Ticket #7247
6-18-19	2.0.0	UPDATE - 2 (L1) Ensure 'Enable saving passwords to the password manager' is Configured Ticket #8359
6-18-19	2.0.0	UPDATE - 4.1 (L1) Ensure 'Configure the required domain names for remote access hosts' is set to 'Enabled' Ticket #7405
6-18-19	2.0.0	UPDATE - 2 (L2) Ensure 'Configure native messaging blacklist' is set to 'Enabled' ("*" for all messaging applications) Ticket #8364