Center for Internet Security®

CIS Google Chrome Benchmark

v1.2.0 - 06-06-2017

The CIS Security Benchmarks division provides consensus-oriented information security products, services, tools, metrics, suggestions, and recommendations (the "SB Products") as a public service to Internet users worldwide. Downloading or using SB Products in any way signifies and confirms your acceptance of and your binding agreement to these CIS Security Benchmarks Terms of Use.

CIS SECURITY BENCHMARKS TERMS OF USE

BOTH CIS SECURITY BENCHMARKS DIVISION MEMBERS AND NON-MEMBERS MAY:

- Download, install, and use each of the SB Products on a single computer, and/or
- Print one or more copies of any SB Product that is in a .txt, .pdf, .doc, .mcw, or .rtf format, but only if each such copy is printed in its entirety and is kept intact, including without limitation the text of these CIS Security Benchmarks Terms of Use.

UNDER THE FOLLOWING TERMS AND CONDITIONS:

- **SB Products Provided As Is**. CIS is providing the SB Products "as is" and "as available" without: (1) any representations, warranties, or covenants of any kind whatsoever (including the absence of any warranty regarding: (a) the effect or lack of effect of any SB Product on the operation or the security of any network, system, software, hardware, or any component of any of them, and (b) the accuracy, utility, reliability, timeliness, or completeness of any SB Product); or (2) the responsibility to make or notify you of any corrections, updates, upgrades, or fixes.
- **Intellectual Property and Rights Reserved**. You are not acquiring any title or ownership rights in or to any SB Product, and full title and all ownership rights to the SB Products remain the exclusive property of CIS. All rights to the SB Products not expressly granted in these Terms of Use are hereby reserved.
- **Restrictions**. You acknowledge and agree that you may not: (1) decompile, dis-assemble, alter, reverse engineer, or otherwise attempt to derive the source code for any software SB Product that is not already in the form of source code; (2) distribute, redistribute, sell, rent, lease, sublicense or otherwise transfer or exploit any rights to any SB Product in any way or for any purpose; (3) post any SB Product on any website, bulletin board, ftp server, newsgroup, or other similar mechanism or device; (4) remove from or alter these CIS Security Benchmarks Terms of Use on any SB Product; (5) remove or alter any proprietary notices on any SB Product; (6) use any SB Product or any component of an SB Product with any derivative works based directly on an SB Product or any component of an SB Product; (7) use any SB Product or any component of an SB Product with other products or applications that are directly and specifically dependent on such SB Product or any component for any part of their functionality; (8) represent or claim a particular level of compliance or consistency with any SB Product; or (9) facilitate or otherwise aid other individuals or entities in violating these CIS Security Benchmarks Terms of Use.
- **Your Responsibility to Evaluate Risks**. You acknowledge and agree that: (1) no network, system, device, hardware, software, or component can be made fully secure; (2) you have the sole responsibility to evaluate the risks and benefits of the SB Products to your particular circumstances and requirements; and (3) CIS is not assuming any of the liabilities associated with your use of any or all of the SB Products.
- **CIS Liability**. You acknowledge and agree that neither CIS nor any of its employees, officers, directors, agents or other service providers has or will have any liability to you whatsoever (whether based in contract, tort, strict liability or otherwise) for any direct, indirect, incidental, consequential, or special damages that arise out of or are connected in any way with your use of any SB Product.
- **Indemnification**. You agree to indemnify, defend, and hold CIS and all of CIS's employees, officers, directors, agents and other service providers harmless from and against any liabilities, costs and expenses incurred by any of them in connection with your violation of these CIS Security Benchmarks Terms of Use.
- **Jurisdiction**. You acknowledge and agree that: (1) these CIS Security Benchmarks Terms of Use will be governed by and construed in accordance with the laws of the State of Maryland; (2) any action at law or in equity arising out of or relating to these CIS Security Benchmarks Terms of Use shall be filed only in the courts located in the State of Maryland; and (3) you hereby consent and submit to the personal jurisdiction of such courts for the purposes of litigating any such action.
- **U.S. Export Control and Sanctions laws**. Regarding your use of the SB Products with any non-U.S. entity or country, you acknowledge that it is your responsibility to understand and abide by all U.S. sanctions and export control laws as set from time to time by the U.S. Bureau of Industry and Security (BIS) and the U.S. Office of Foreign Assets Control (OFAC).

SPECIAL RULES FOR CIS MEMBER ORGANIZATIONS: CIS reserves the right to create special rules for: (1) CIS Members; and (2) Non-Member organizations and individuals with which CIS has a written contractual relationship. CIS hereby grants to each CIS Member Organization in good standing the right to distribute the SB Products within such Member's own organization, whether by manual or electronic means. Each such Member Organization acknowledges and agrees that the foregoing grants in this paragraph are subject to the terms of such Member's membership arrangement with CIS and may, therefore, be modified or terminated by CIS at any time.

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 v59.0.3071.86. 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

This document is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate Google Chrome.

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://community.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**

  Items in this profile intend to:

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

- **Level 2**

  This profile extends the

Acknowledgements

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

Contributor
Brian Howson
Philippe Langlois
Frank Lesniak MCSE

Editor
Edward Oechsner
Jordan Rakoske GSEC, GCWN

Recommendations

1 Computer Configuration

The following structure of this guide mirrors how it is structured in the Google Chrome Group Policy template.

1.1 Google Chrome

This section contains recommendations for Google Chrome.

1.1.1 (L2) Ensure 'Allow invocation of file selection dialogs' is set to 'Enabled' (Scored)

Profile Applicability:

- Level 2

Description:

Allows access to local files on the machine by allowing Google Chrome to display file selection dialogs.

Rationale:

Preventing users from uploading documents can help prevent the loss of sensitive information.

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:AllowFileSelectionDialogs
```

Remediation:

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

```
Computer Configuration\Administrative Templates\Classic Administrative
Template (ADM)\Google\Google Chrome\Allow invocation of file selection
dialogs
```

Impact:

If you enable this setting, users can open file selection dialogs as normal.

Default Value:

Not Configured

CIS Controls:

14 Controlled Access Based on the Need to Know
Controlled Access Based on the Need to Know

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

Profile Applicability:

- Level 1

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\Classic Administrative
Template (ADM)\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:

Not Configured

CIS Controls:

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.

1.1.3 (L1) Ensure 'Always runs plugins that require authorization' is set to 'Disabled' (Scored)

Profile Applicability:

- Level 1

Description:

Chrome allows plugins that are not outdated to run automatically. Disabling this setting allows the plugins to run only when permission is granted by the user.

Rationale:

Disabling plugins from automatically running can prevent unwanted and/or harmful plugins from running without the user's consent, preventing unauthorized data/remote access.

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:AlwaysAuthorizePlugins
```

Remediation:

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

```
Computer Configuration\Administrative Templates\Classic Administrative
Template (ADM)\Google\Google Chrome\Always runs plugins that require
authorization
```

Impact:

If this setting is disabled or not set, users will be asked for permission to run plugins that require authorization. These are plugins that can compromise security.

Default Value:

Not Configured

CIS Controls:

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.

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

Profile Applicability:

- Level 1

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 the cookies from being set.

Rationale:

Blocking third party cookies can help protect a users 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\Classic Administrative
Template (ADM)\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:

Not Configured

CIS Controls:

13 Data Protection
Data Protection

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

Profile Applicability:

- Level 1

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. Disabling this feature will stop all processes and background applications when the browser window is 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\Classic Administrative
Template (ADM)\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:

Not Configured

CIS Controls:

7 Email and Web Browser Protections
Email and Web Browser Protections

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

Profile Applicability:

- Level 1

Description:

Chrome enables the user to change the error pages that are built into Google Chrome. By disabling this feature the user is not able to change the error page to an alternate one.

Rationale:

Alternate error pages can be used to redirect users to custom websites that contain malicious links.

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\Classic Administrative
Template (ADM)\Google\Google Chrome\Enable alternate error pages
```

Impact:

If you disable this setting, alternate error pages are never used.

Default Value:

Not Configured

CIS Controls:

7 Email and Web Browser Protections
Email and Web Browser Protections

1.1.7 (L1) Ensure 'Enable AutoFill' is set to 'Disabled' (Scored)

Profile Applicability:

- Level 1

Description:

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

Rationale:

If an attacker gains access to a users machine where the user has stored auto save data, information could be harvested or used to gain access to more 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:AutoFillEnabled
```

Remediation:

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

```
Computer Configuration\Administrative Templates\Classic Administrative
Template (ADM)\Google\Google Chrome\Enable AutoFill
```

Impact:

If you disable this setting, AutoFill will be inaccessible to users.

Default Value:

Not Configured

CIS Controls:

13 Data Protection
Data Protection

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

Profile Applicability:

- Level 1

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 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:CloudPrintProxyEnabled
```

Remediation:

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

```
Computer Configuration\Administrative Templates\Classic Administrative
Template (ADM)\Google\Google Chrome\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 it's printers with Google Cloud Print.

Default Value:

Not Configured

CIS Controls:

13 Data Protection
Data Protection

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

Profile Applicability:

- Level 1

Description:

This Setting controls anonymous reporting of usage and crash-related data about Google Chrome to Google.

Rationale:

Anonymous crash/usage data can be used to identify people, companies and information, and can be considered data exfiltration 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\Classic Administrative
Template (ADM)\Google\Google Chrome\Enable reporting of usage and crash-
related data
```

Impact:

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

Default Value:

Not Configured

CIS Controls:

13 Data Protection
Data Protection

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

Profile Applicability:

- Level 1

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\Classic Administrative
Template (ADM)\Google\Google Chrome\Enable submission of documents to Google
Cloud print
```

Impact:

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

Default Value:

Not Configured

CIS Controls:

13 Data Protection
Data Protection

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

Profile Applicability:

- Level 1

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/.

If this setting is enabled, an attacker with access to a user’s machine with passwords stored that have been imported from another browser, credentials can be viewed in clear text and used to gain additional access.

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\Classic Administrative
Template (ADM)\Google\Google Chrome\Import saved passwords from default
browser on first run
```

Impact:

If disabled, the saved passwords are not imported.

Default Value:

Not Configured

CIS Controls:

16 Account Monitoring and Control
Account Monitoring and Control

1.1.12 (L1) Ensure 'Specify whether the plugin finder should be disabled' is set to 'Enabled' (Scored)

Profile Applicability:

- Level 1

Description:

Chrome allows for the automatic search and installation of missing plugins. Disabling this feature will stop plugins from being downloaded and installed without the users knowledge.

Rationale:

Disabling the feature that allows plugins to automatically be installed prevents plugins that may have vulnerabilities or be against company policy from being introduced to the computer without anyone's knowledge.

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:DisablePluginFinder
```

Remediation:

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

```
Computer Configuration\Administrative Templates\Classic Administrative
Template (ADM)\Google\Google Chrome\Specify whether the plugin finder should
be disabled
```

Impact:

If you set this setting to enabled the automatic search and installation of missing plugins will be disabled in Google Chrome.

Default Value:

Not Configured

CIS Controls:

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.

1.2 Allow Google Chrome Frame to Handle the Following Content Types

This section is intentionally blank and exists to ensure the structure of the Google Chrome benchmark is consistent in future releases.

1.3 Configure Remote Access Options

This section contains recommendations for Configuring Remote Access Options

1.3.1 (L1) Ensure 'Configure the required domain name for remote access hosts' is set to 'Enabled' (Scored)

Profile Applicability:

- Level 1

Description:

Chrome allows the user to configure a 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 domain.

Rationale:

If this setting is disabled or not set, then hosts can be shared using any account.

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:RemoteAccessHostDomain
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`and enter domain.

```
Computer Configuration\Administrative Templates\Classic Administative
Templates (ADM)\Google\Google Chrome\Configure remote access
options\Configure the required domain name for remote access hosts
```

Impact:

If this setting is enabled, then hosts can be shared only using accounts registered on the specified domain name.

Default Value:

Not Configured

CIS Controls:

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

1.3.2 (L1) Ensure 'Enable curtaining of remote access hosts' is set to 'Enabled' (Scored)

Profile Applicability:

- Level 1

Description:

Chrome allows the user to disable a remote user's physical input and output while the remote connection is in progress.

Rationale:

If this setting is disabled or not set, then both local and remote users can interact with the host when it is being shared.

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 `Enabled`.

```
Computer Configuration\Administrative Templates\Classic Administative
Templates (ADM)\Google\Google Chrome\Configure remote access options\Enable
curtaining of remote access hosts
```

Impact:

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

Default Value:

Not Configured

CIS Controls:

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

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

Profile Applicability:

- Level 1

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, then 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\Classic Administrative
Template (ADM)\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, then this machine will only allow connections from client machines within the local network.

Default Value:

Not Configured

CIS Controls:

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

Limitation and Control of Network Ports, Protocols, and Services

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

Profile Applicability:

- Level 1

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, then 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\Classic Administative
Templates (ADM)\Google\Google Chrome\Configure remote access options\Enable
or disable PIN-less authentication
```

Impact:

If this setting is disabled, then this feature will not be available.

Default Value:

Not Configured

CIS Controls:

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

1.4 Content Settings

This section contains recommendations for Content Settings

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

Profile Applicability:

- Level 2

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:

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

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`.

```
Computer Configuration\Administrative Templates\Classic Administrative
Template (ADM)\Google\Google Chrome\Content Settings\Default cookies setting
```

Impact:

If this policy is set to 'Keep cookies for the duration of the session' then cookies will be cleared when the session closes.

Default Value:

Not Configured

CIS Controls:

13 Data Protection

Data Protection

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

Profile Applicability:

- Level 1

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\Classic Administrative
Template (ADM)\Google\Google Chrome\Content Settings\Default Plugins Setting
```

Impact:

Click to play allows plugins to run but the user must click them to start their execution.

Default Value:

Not Configured

CIS Controls:

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.

1.5 Default HTML Renderer for Google Chrome Frame

This section is intentionally blank and exists to ensure the structure of the Google Chrome benchmark is consistent in future releases.

1.6 Default Search Provider

This section is intentionally blank and exists to ensure the structure of the Google Chrome benchmark is consistent in future releases.

1.7 Extensions

This section contains recommendations for Extensions

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

Profile Applicability:

- Level 1

Description:

Enabling this setting allows you to specify which extensions the users can NOT install. Extensions already installed will be removed if blacklisted.

Rationale:

This will block any extension that could 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 the extension whitelist.

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`.

```
Computer Configuration\Administrative Templates\Classic Administrative
Template (ADM)\Google\Google Chrome\Extensions\Configure Extension
Installation Blacklist
```

Impact:

Any installed extension will be removed unless it is specified on the extension whitelist.

Default Value:

Not Configured

CIS Controls:

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.

1.7.2 (L1) Ensure 'Configure extension installation whitelist' is Configured (Scored)

Profile Applicability:

- Level 1

Description:

Allows you to specify which extensions are not subject to the blacklist.

Rationale:

Allows you to specify which extensions are not subject to the blacklist.

A blacklist value of * means all extensions are blacklisted and users can only install extensions listed in the whitelist.

Audit:

Remediation:

Default Value:

By default, all extensions are whitelisted, but if all extensions have been blacklisted by policy, the whitelist can be used to override that policy.

References:

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

CIS Controls:

2.2 Deploy Application Whitelisting
Deploy application whitelisting technology that allows systems to run software only if it is included on the whitelist and prevents execution of all other software on the system. The whitelist may be very extensive (as is available from commercial whitelist vendors), so that users are not inconvenienced when using common software. Or, for some special-purpose systems (which require only a small number of programs to achieve their needed business functionality), the whitelist may be quite narrow.

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.

1.8 Home Page

This section is intentionally blank and exists to ensure the structure of the Google Chrome benchmark is consistent in future releases.

1.9 Locally Managed Users Settings

This section is intentionally blank and exists to ensure the structure of the Google Chrome benchmark is consistent in future releases.

1.10 Native Messaging

This section is intentionally blank and exists to ensure the structure of the Google Chrome benchmark is consistent in future releases.

1.11 Password Manager

This section contains recommendations for Password Manager

1.11.1 (L1) Ensure 'Enable the password manager' is set to 'Disabled' (Scored)

Profile Applicability:

- Level 1

Description:

Chrome will memorize passwords and automatically provide them when a user logs into a site. By disabling this feature the user will be prompted to enter their password each time they visit a website.

Rationale:

If you enable this setting, users can have Google Chrome memorize passwords and provide them automatically the next time they log in to a site. An intruder who has unrestricted access to your computer for even a minute can view and copy all of your saved passwords just by visiting an easy-to-remember settings page: 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:PasswordManagerEnabled
```

Remediation:

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

```
Computer Configuration\Administrative Templates\Classic Administrative
Template (ADM)\Google\Google Chrome\Password manager\Enable the password
manager
```

Impact:

If you disable this setting, users are not able to save passwords or use already saved passwords.

Default Value:

Not Configured

CIS Controls:

16 Account Monitoring and Control
Account Monitoring and Control

1.12 Policies for HTTP Authentication

This section is intentionally blank and exists to ensure the structure of the Google Chrome benchmark is consistent in future releases.

1.13 Proxy Server

This section is intentionally blank and exists to ensure the structure of the Google Chrome benchmark is consistent in future releases.

1.14 Startup Pages

This section is intentionally blank and exists to ensure the structure of the Google Chrome benchmark is consistent in future releases.

Appendix: Summary Table

Control		Set Correctly	
		Yes	No
1	**Computer Configuration**		
1.1	**Google Chrome**		
1.1.1	(L2) Ensure 'Allow invocation of file selection dialogs' is set to 'Enabled' (Scored)	☐	☐
1.1.2	(L1) Ensure 'Allow running plugins that are outdated' is set to 'Disabled' (Scored)	☐	☐
1.1.3	(L1) Ensure 'Always runs plugins that require authorization' is set to 'Disabled' (Scored)	☐	☐
1.1.4	(L1) Ensure 'Block third party cookies' is set to 'Enabled' (Scored)	☐	☐
1.1.5	(L1) Ensure 'Continue running background apps when Google Chrome is closed' is set to 'Disabled' (Scored)	☐	☐
1.1.6	(L1) Ensure 'Enable alternate error pages' is set to 'Disabled' (Scored)	☐	☐
1.1.7	(L1) Ensure 'Enable AutoFill' is set to 'Disabled' (Scored)	☐	☐
1.1.8	(L1) Ensure 'Enable Google Cloud Print Proxy' is set to 'Disabled' (Scored)	☐	☐
1.1.9	(L1) Ensure 'Enable reporting of usage and crash-related data' is set to 'Disabled' (Scored)	☐	☐
1.1.10	(L1) Ensure 'Enable submission of documents to Google Cloud print' is set to 'Disabled' (Scored)	☐	☐
1.1.11	(L1) Ensure 'Import saved passwords from default browser on first run' is set to 'Disabled' (Scored)	☐	☐
1.1.12	(L1) Ensure 'Specify whether the plugin finder should be disabled' is set to 'Enabled' (Scored)	☐	☐
1.2	**Allow Google Chrome Frame to Handle the Following Content Types**		
1.3	**Configure Remote Access Options**		
1.3.1	(L1) Ensure 'Configure the required domain name for remote access hosts' is set to 'Enabled' (Scored)	☐	☐
1.3.2	(L1) Ensure 'Enable curtaining of remote access hosts' is set to 'Enabled' (Scored)	☐	☐
1.3.3	(L1) Ensure 'Enable firewall traversal from remote access host' is set to 'Disabled' (Scored)	☐	☐
1.3.4	(L1) Ensure 'Enable or disable PIN-less authentication for remote access hosts' is set to 'Disabled' (Scored)	☐	☐
1.4	**Content Settings**		
1.4.1	(L2) Ensure 'Default cookies setting' is set to 'Enabled' (Keep cookies for the duration of the session) (Scored)	☐	☐

1.4.2	(L1) Ensure 'Default Plugin Setting' is set to 'Enabled' (Click to Play) (Scored)	☐	☐
1.5	**Default HTML Renderer for Google Chrome Frame**		
1.6	**Default Search Provider**		
1.7	**Extensions**		
1.7.1	(L1) Ensure 'Configure extension installation blacklist' is set to 'Enabled' ("*" for all extensions) (Scored)	☐	☐
1.7.2	(L1) Ensure 'Configure extension installation whitelist' is Configured (Scored)	☐	☐
1.8	**Home Page**		
1.9	**Locally Managed Users Settings**		
1.10	**Native Messaging**		
1.11	**Password Manager**		
1.11.1	(L1) Ensure 'Enable the password manager' is set to 'Disabled' (Scored)	☐	☐
1.12	**Policies for HTTP Authentication**		
1.13	**Proxy Server**		
1.14	**Startup Pages**		

Appendix: Change History

Date	Version	Changes for this version
6/6/17	1.2.0	REMOVE - Ensure 'Allow users to show passwords in Password Manager' Ticket #4767
6/6/17	1.2.0	REMOVE - Ensure 'Specify a list of Disabled Plugins' is set to 'Enabled' Ticket # 4764
6/6/17	1.2.0	UPDATE - Set 'Allow invocation of file selection dialogs' to Enabled Ticket # 5105
6/6/17	1.2.0	ADD – CIS Controls Mappings
6/6/17	1.2.0	UPDATE – all titles to conform to CIS Standard.