Guidance

# Browser Security Guidance: Google Chrome

Published

**Contents**



This ALPHA guidance builds on the End User Devices Platform Security Guidance and is applicable to devices running Google Chrome Browser on a supported and well configured version of Windows. This guidance was tested on 64-bit Windows 8.1 Enterprise edition running Chrome for Business versions 33 and 39.

Chrome Browser can be run as a normal Windows desktop application or as a Windows app (Chrome calls this "Windows 8 mode"). This guidance is applicable to both modes of use.

## 1. Usage scenario

Chrome Browser will be used to access a variety of web services including:

- accessing Intranet services hosted on an enterprise-provided OFFICIAL network
- accessing enterprise cloud services sourced from the Digital Marketplace
- accessing other Internet services and web resource

To support these scenarios, the following architectural choices are recommended:

- All data should be routed through a secure enterprise VPN to ensure the confidentiality and integrity of traffic intended for the enterprise Intranet
- All Internet data should be routed through an enterprise-hosted proxy to benefit from enterprise protective monitoring and logging solutions
- Arbitrary third-party extension installation by users is not permitted in the browser. A list of allowed trusted

apps and extensions can be configured in Group Policy

# 2. Summary of browser security

This browser has been assessed against each of the 12 security recommendations, and that assessment is shown in the table below. Explanatory text indicates that there is something related to that recommendation that the risk owners should be aware of. Rows marked [!] represent a more significant risk. See How the browser can best satisfy the security recommendations for more details about how each of the security recommendations is met.

| Recommendation | Risks |
|---|---|
| Protecting data-in-transit | Chrome does not support configuration to disable cryptographic cipher suites<br>[!] Users can override certificate warnings unless the site implements HSTS |
| Protecting data-at-rest | |
| Enabling user authentication | Built-in authentication schemes cannot be disabled for cleartext channels |
| Protecting privacy | |
| Plugin and renderer sandboxing | |
| Plugin and site whitelisting | |
| Malicious code detection and prevention | There is no differentiation between Internet sites and Intranet sites |
| Security policy enforcement | |
| External peripheral and sensitive API protection | |
| Update policy | No notification is given if updates fail |
| Event collection for enterprise analysis | [!] There is no facility for the enterprise to log or collect security-related events |
| Active scripting | |

## 2.1 Significant risks

The following significant risks have been identified:

- Chrome does not support configuration to disable cryptographic cipher suites. If a vulnerability is discovered

in a particular cryptographic cypher, users may be under increased risk as they will believe their encrypted traffic is protected appropriately

- Mixed content (ie an HTTPS site loading scripts and web resources from an unencrypted location) is blocked by default, but can be overridden by users on a per-page basis. Enabling mixed content breaks the security boundary between trusted and untrusted content. There is a risk of malicious content interacting with content in HTTPS web pages if the user allows the blocked content and the user's connection is subject to a man-in-the-middle attack
- HTTPS warning pages including those generated from OCSP checks can be bypassed by the user if a site does not use HSTS. There is a risk that secure connections may be subject to a man-in-the-middle attack using a forged certificate
- There is no differentiation or explicit separation between Intranet and Internet web pages. Intranet sites that are vulnerable to cross-site-scripting and cross-site-request-forgery are not protected from malicious Internet websites. If older and potentially vulnerable plugins need to be used on Intranet pages, they will also be exposed to attack by a malicious Internet website
- Built-in authentication schemes such as basic and digest cannot be disabled for unencrypted requests. There is a risk that credentials sent using these methods could be stolen via a man-in-the-middle attack
- The user or enterprise is not notified if updates to either the browser or the Safe Browsing list fail and so they will not be aware that it is outdated and susceptible to publically known vulnerabilities
- Chrome does not provide any built-in mechanism for logging events for enterprise analysis. It is therefore not possible to determine whether installations adhere to security policies, nor alert on security events such as on-screen security warnings or browser crashes

# 3. How the browser can best satisfy the security recommendations

## 3.1 Data-in-transit

Configure a gateway web proxy to ensure that all Internet traffic is routed through the enterprise for inspection and logging. Use the platform's data-in-transit protection to securely route all Intranet traffic back to the enterprise and provide access to the proxy.

## 3.2 Data-at-rest

The platform enforces user separation ensuring that temporary data and saved credentials can only be accessed by that user.

Use the platform's data-at-rest protection to encrypt profile data and temporary files. If required, enable ephemeral mode in Group Policy to prevent data from being stored on the disk after the browser is closed.

## 3.3 Authentication

Deploy any required enterprise client authentication certificates to the user's personal certificate store.

## 3.4 Privacy

Turn off features that collect data such as browsing history, bookmarks, saved passwords, typed website addresses, usage statistics and location data to submit to Google. Organisations should consider the privacy risk if choosing to not disable features such as spell checking and automatic translation.

Safe Browsing can be disabled if the trade-off between privacy and security is not acceptable.

Instruct users to enable the Do Not Track option in Chrome settings as this cannot be set by an administrator.

## 3.5 Plugin and renderer sandboxing

This requirement is met by the browser without additional configuration. Built-in sandboxed features are preferred over third party plugins. If plugins are required that do not run inside the Chrome sandbox, configure the browser to only use them on trusted Intranet sites.

## 3.6 Plugin and site whitelisting

Authorised apps, extensions and websites can be managed using a whitelist and the Web Store can be disabled. Experimental features and debugging interfaces can be disabled. Web protocols that are not supported by the enterprise proxy can be disabled in Group Policy.

## 3.7 Malicious code detection and prevention

Ensure that the platform's anti-malware protection is enabled and kept updated. Chrome Browser uses the Google Safe Browsing cloud service to detect known malicious sites and downloads. Configure this feature so that the user cannot choose to bypass its warnings.

## 3.8 Security policy enforcement

Settings applied through Group Policy cannot be removed by the user.

## 3.9 External peripheral and sensitive API protection

Access to the microphone and webcam, and hardware rendering using WebGL can be disabled.

## 3.10 Update policy

This requirement is met by the browser without additional configuration.

## 3.11 Event collection for enterprise analysis

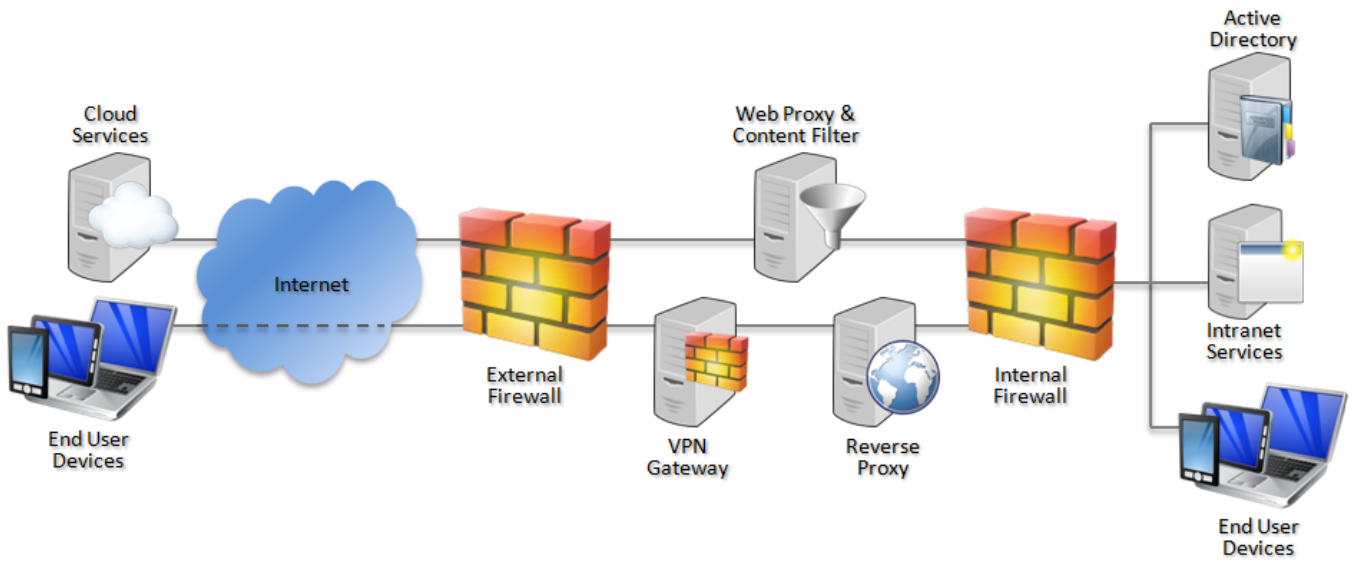
There is no facility for collecting logs or security events for enterprise analysis.

## 3.12 Active scripting

This requirement is met by the browser without additional configuration.

# 4. Network Architecture

Deploy a DMZ web proxy in an architecture based on the Internet Gateway Architectural Pattern. The following network diagram describes the recommended architecture for this browser. The proxy/content filter includes user and machine request logging, anti-malware and content inspection components.




**Recommended network architecture for deployments of Google Chrome on Windows**

# 5. Deployment process

The following steps should be followed to prepare the enterprise infrastructure for hosting a deployment of the browser and provision it to end user devices.

1. Procure, deploy and configure network components, including a web proxy/content filter.
2. Provision Windows in line with the EUD Platform Security Guidance.
3. Install the Google Chrome policy templates on the Group Policy management terminal.
4. Create Group Policies for users in accordance with the settings later in this section.
5. Deploy Google Chrome for Business to the EUDs.

# 6. Recommended configuration

The following settings can be applied using Group Policy.

All settings are found in `User Configuration > Policies > Administrative Templates > Google > Google Chrome`. For easy configuration, the custom CESG GPO settings described below can be provided to Government organisations on request through CESG enquiries.

| Group Policy | Value(s) |
|---|---|
| Allow or deny audio capture | Disabled |
| Allow or deny video capture | Disabled |
| Allow running plugins that are outdated | Disabled |
| Allow sign in to Chrome | Disabled |
| Block third party cookies | Enabled |
| Disable proceeding from the Safe Browsing warning page | Enabled |
| Disable synchronization of data with Google | Enabled |
| Enable Google Cloud Print proxy | Disabled |
| Enable or disable spell checking web service | Disabled |
| Enable reporting of usage and crash-related data | Disabled |
| Enable Safe Browsing | Enabled |
| Enable search suggestions | Disabled |
| Enable submission of documents to Google Cloud Print | Disabled |
| Enable Translate | Disabled |
| Hide the web store from the new tab page and app launcher | Enabled |

| | |
|---|---|
| Specify a list of disabled plugins | Enabled<br>List of disabled plugins: * |
| Specify a list of plugins that the user can enable or disable | Enabled<br>List of exceptions to the list of disabled plugins:<br>Shockwave Flash<br>Adobe Flash Player<br>Chrome PDF Viewer |
| Content Settings > Default geolocation setting | Enabled<br>Do not allow any site to track the users' physical location |
| Extensions> Configure extension installation blacklist | Enabled<br>Extension IDs the user should be prevented from installing: * |
| Block access to a list of URLs | chrome://flags<br>chrome://net-internals<br>chrome://tracing |

Group policy can be used to configure the web proxy. If only Chrome is to access the Internet, this can be done within Chrome's Group Policy. Otherwise Chrome can be configured to inherit the Windows proxy settings.

## 6.1 Chrome proxy settings

These settings will only affect Chrome, and will not be applied to other Windows applications.

| **Group Policy** | **Value(s)** |
|---|---|
| User Configuration > Policies > Administrative Templates > Google > Google Chrome > Proxy server > Choose how to specify proxy server settings | Enabled<br>Use fixed proxy servers |
| User Configuration > Policies > Administrative Templates > Google > Google Chrome > Proxy server > Address or URL of proxy server | Address of enterprise proxy |
| User Configuration > Policies > Administrative Templates > Google > Google Chrome > Proxy server > Proxy bypass rules | List of Intranet sites or IP addresses |

## 6.2 Windows proxy settings

These settings will be applied to all Windows applications, and will be inherited by Chrome.

| Group Policy | Value(s) |
|---|---|
| User Configuration > Policies > Administrative Templates > Google > Google Chrome > Proxy server > Choose how to specify proxy server settings | Enabled Use system proxy settings |
| User Configuration > Administrative Templates > Windows Components > Internet Explorer > Disable changing proxy settings | Enabled |
| User Configuration > Preferences > Control Panel Settings > Internet Settings > Internet Explorer 10 > Connections > Local Area Network (LAN) settings > Automatically detect settings | No |
| User Configuration > Preferences > Control Panel Settings > Internet Settings > Internet Explorer 10 > Connections > Proxy Settings > Use a proxy server for your LAN | Yes |
| User Configuration > Preferences > Control Panel Settings > Internet Settings > Internet Explorer 10 > Connections > Proxy Settings > Proxy server address for your LAN | Address and port of enterprise proxy |
| User Configuration > Preferences > Control Panel Settings > Internet Settings > Internet Explorer 10 > Connections > Proxy Settings > Do not use proxy servers for addresses beginning with | List of Intranet sites or IP addresses |

# 7. Enterprise considerations

## 7.1 Safe browsing

Google Safe Browsing is a security feature that aims to protect against phishing websites and malicious downloads. It works by sending hashes of some visited website addresses to Google. If Google reports that the page is unsafe, the page or file will not be downloaded or displayed to protect the user against malware and data theft.

Google states that it cannot derive the full website addresses from the information submitted as it only sends a partial URL fingerprint. Full website addresses are only sent if an organisation chooses to configure Chrome to send usage statistics to Google. Safe Browsing can be disabled entirely if the trade-off between privacy and security is not acceptable.

## 7.2 Chrome web store

The configuration above prevents users from installing apps and extensions from the Chrome web store.

If the Chrome web store is enabled, authorised apps and extensions can be managed using an allow list in the

Group Policy.

Organisations should consider the increased exposure to malware when enabling extensions that do not run inside a sandbox as both Internet and Intranet sites will be able to initialise them. A malicious extension or app will be able to read, interact with and modify any Internet and Intranet content accessed by the user including sites delivered over HTTPS.

## 7.3 Plugin sandboxing

Chrome supports the use of legacy plugins that by design cannot be sandboxed by the browser. They are usually used for video playback (eg Silverlight and QuickTime) or integration with enterprise tools (eg Java). A malicious website that successfully exploits such a plugin or browser extension can gain full user privilege including access to their data and web content.

Chrome applies its sandbox to built-in plugins such as Flash and the Chrome PDF reader. These plugins have therefore been enabled in the configuration above. If other plugins are required, Chrome should be configured to only allow them for a whitelisted set of trusted sites.

## 7.4 Chrome updates

Google Chrome integrates security patches and functionality updates into a single update mechanism. This means that an enterprise must be running the latest version of Chrome to remain fully patched.

Google Chrome Browser for Business automatically updates each endpoint using the Google Update Service. This polls the Internet for updates and applies them without user intervention. Google describes best practice for managing and optionally configuring these updates.

Google updates the install MSI with each major update allowing an organisation to manually download and install newer versions from an enterprise distribution server.

# Legal information

This guidance is issued by CESG, the UK's National Technical Authority on Information Assurance. One of the roles of CESG is to provide advice to UK government entities and organisations providing services to UK government. The guidance found here is provided and intended for use by this audience. It is provided 'as-is' as an example of how specific requirements could be met. It should be used to help inform risk management decisions on the use of the products described, but it should not be used for procurement decisions; it is not intended to be exhaustive, it does not act as an endorsement of any particular product or technology, and it is not tailored to individual needs. It is not a replacement for independent, specialist advice. Users should ensure that they take appropriate technical and legal advice in using this and other guidance published by CESG. This guidance is provided without any warranty of any kind, whether express or implied. It is provided without any representation as to the accuracy, completeness, integrity, content, quality, or fitness for purpose of all or any part of it. CESG cannot, then, accept any liability whatsoever for any loss or damage suffered or any costs incurred by any person as a result of, or arising from, either the disclosure of this guidance to you, or your subsequent use of it. 