

## Guidance

# Browser Security Guidance: Mozilla Firefox

Published

## Contents

1. Usage scenario
2. Summary of browser security
3. How the browser can best satisfy the security recommendations
4. Network architecture
5. Deployment process
6. Recommended configuration
7. Enterprise considerations

This ALPHA guidance builds on the [End User Devices Platform Security Guidance](#) and is applicable to devices running Mozilla Firefox on a supported and well configured version of Windows. This guidance was tested on 64-bit Windows 8.1 Enterprise edition running Firefox 31.1.1 ESR.

## 1. Usage scenario

Firefox 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 resources

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	Certificate pinning is not supported
Protecting data-at-rest	
Enabling authentication	Built-in authentication schemes cannot be disabled for cleartext channels
Protecting privacy	
Plugin and renderer sandboxing	[!] Firefox does not render web content in a sandbox
Plugin and site whitelisting	[!] Firefox does not allow plugins, add-ons and extensions to be controlled using an whitelist
Malicious code detection and prevention	Users can override Safe Browsing warnings Mozilla does not currently offer a 64-bit application There is no differentiation between Internet sites and Intranet sites
Security policy enforcement	Users can re-enable plugins that have been disabled [!] Users can bypass controls that prevent installation of add-ons and extensions
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:

- Mixed content is blocked by default, but can be overridden by users on a per-page basis. Allowing 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

- The browser does not support certificate pinning. There is a risk that secure connections may be subject to a man in the middle attack using a forged certificate
- Firefox does not render any web content or third party plugins in a sandbox. The Flash and Adobe Reader plugins implement their own sandbox, although this is not the case for most plugins including Java. Firefox may default to using in-built content renderers that are not sandboxed instead of sandboxed third party plugins. A malicious website that successfully exploits the browser renderer, JavaScript engine or a third party plugin can gain full user privilege including access to their data and web content
- Add-ons can be manually installed by the user into their browser profile, bypassing the controls in the browser. Such an add-in could maliciously interact with sensitive data being rendered by the browser or interfere with data on the underlying operating system. This interaction will not be visible to the user as add-ons can work silently in the background including sending data to the Internet
- If a web page is deemed to be in some way malicious by the Safe Browsing online reputational service, the user can choose to ignore the warning and load the page anyway. There is a risk that the blocked page will attempt to run malware, or the user will fall victim to social engineering attacks that result in identity theft
- 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
- 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. There is no built-in protection against cross-site scripting attacks. 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
- Firefox 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 Protecting 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 Protecting 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, set Firefox's [sanitizeOnShutdown](#) configuration to prevent data from being stored on the disk after the browser is closed.

### **3.3 Enabling authentication**

Deploy any enterprise client authentication certificates to the browser.

### **3.4 Protecting privacy**

Turn off features that collect data such as browsing history, typed URLs, usage statistics and location data to submit to Mozilla and its partners. Organisations should consider the privacy risk if choosing to not disable features such as spell checking.

### **3.5 Plugin and renderer sandboxing**

The browser provides no sandboxing capability. Choose third party plugins and apps that implement a sandbox in preference to equivalents that do not. Ensure that content is opened by plugins that implement a sandbox rather than allowing it to be previewed in Firefox outside of a sandbox.

### **3.6 Plugin and site whitelisting**

Install any extensions that are required and disable the ability for users to install any more. Web protocols that are not supported by the enterprise proxy can be disabled. Deploy a site whitelist on the web proxy if required.

### **3.7 Malicious code detection and prevention**

Ensure that the platform's anti-malware protection is enabled and kept updated. Firefox 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**

Enterprise-managed configuration cannot be changed 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

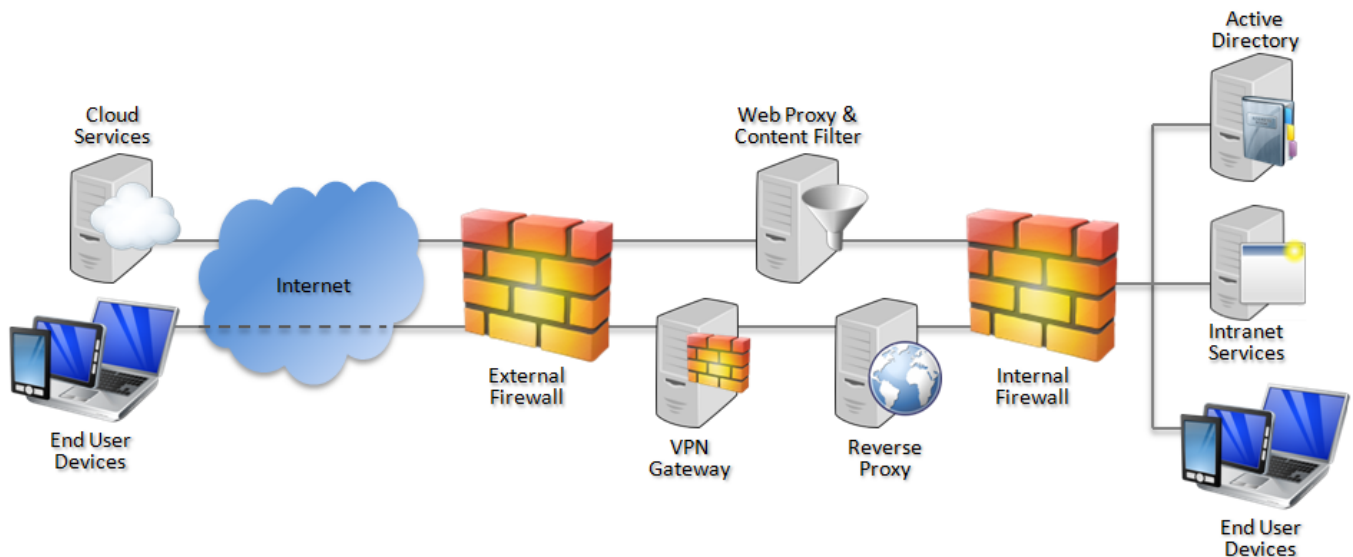
There is no facility for collecting logs or security events for enterprise analysis.

### 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 Mozilla Firefox on Windows

## 5. Deployment process

Mozilla does not provide an MSI installer for Firefox so it may be necessary to use third-party tools to deploy it at scale.

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. Deploy [Firefox Extended Support Release](#)  to EUDs.
4. Build a [lock file and prefs configuration file](#)  in accordance with the settings later in this section. This file should contain the settings which the organisation wishes to configure and enforce. Deploy it to the EUDs in %programfiles(x86)%\Mozilla Firefox\firefox.cfg and %programfiles(x86)%\Mozilla Firefox\defaults\pref\prefs.js.
5. Create Group Policy Preferences to deploy the registry settings to EUDs.

## 6. Recommended configuration

Firefox is configured using two configuration files:

### 6.1 prefs.js

This file defines the location of the enterprise configuration.

```
pref('general.config.filename', 'firefox.cfg');  
pref('general.config.obscure_value', 0);
```

### 6.2 firefox.cfg

This file should contain the settings that the organisation wishes the configuration to enforce.

#### Recommended configuration

```
// Disable telemetry and health reporting  
lockPref("toolkit.telemetry.enabled", false);  
lockPref("datareporting.healthreport.uploadEnabled", false);  
lockPref("datareporting.policy.dataSubmissionEnabled", false);  
lockPref("dom.ipc.plugins.flash.subprocess.crashreporter.enabled", false);  
lockPref("datareporting.healthreport.uploadEnabled", false);  
lockPref("toolkit.telemetry.enabled", false);  
lockPref("toolkit.telemetry.prompted", 2);  
  
// Disable sync  
lockPref("services.sync.serverURL", "");
```

```
lockPref("identity.fxaccounts.auth.uri", "");
lockPref("identity.fxaccounts.remote.force_auth.uri", "");
lockPref("identity.fxaccounts.remote.signin.uri", "");
lockPref("identity.fxaccounts.remote.signup.uri", "");
lockPref("identity.fxaccounts.settings.uri", "");
lockPref("services.sync.engine.addons", false);
lockPref("services.sync.engine.bookmarks", false);
lockPref("services.sync.engine.history", false);
lockPref("services.sync.engine.passwords", false);
lockPref("services.sync.engine.prefs", false);
lockPref("services.sync.engine.tabs", false);

// Turn on Do not Track
lockPref("privacy.donottrackheader.enabled", true);
lockPref("privacy.donottrackheader.value", 1);

// Disable features that have an impact on privacy
lockPref("geo.enabled", false);
lockPref("layout.spellcheckDefault", 0);
lockPref("accessibility.typeaheadfind", false);

// Disable certificate warning bypass
lockPref("browser.xul.error_pages.enabled", false);

// Enable support for Content Security Policy
lockPref("security.csp.enable", true);

// Turn on Safe Browsing anti-malware
lockPref("browser.safebrowsing.enabled", true);
lockPref("browser.safebrowsing.malware.enabled", true);

// Turn on XSS Filter
lockPref("browser.urlbar.filter.javascript", true);

// Restrict third party cookies
lockPref("network.cookie.cookieBehavior", 1);

// Prevent users installing installing add-ins using user interface
lockPref("xpinstall.enabled", false);
lockPref("xpinstall.whitelist.required", true);
lockPref("xpinstall.whitelist.add", "");
lockPref("xpinstall.whitelist.180.add", "");

// Implement plugin whitelist
// default all plugins to be disabled (though this doesn't prevent user changing setting)
lockPref("plugin.default.state", 0);
lockPref("plugin.defaultXpi.state", 0);

// Enable Flash as it's in a sandbox
```

```
lockPref("plugin.state.flash", 2);

// Disable Java unless required
lockPref("plugin.state.java", 0);
lockPref("plugin.state.npdeployjava1", 0);

// Disable webcam and microphone unless necessary
lockPref("media.navigator.enabled", false);
lockPref("media.navigator.video.enabled", false);
```


### Optional configuration

```
// Prevent the use of SPDY, Websockets and WebRTC if not supported by the web proxy
lockPref("media.peerconnection.enabled", false);
lockPref("media.websocket.enabled", false);
lockPref("network.websocket.enabled", false);
lockPref("media.http.spdy.enabled", false);

// Disable automatic form filling
lockPref("signon.autofillForms", false);
lockPref("signon.rememberSignons", false);

// Clear personal and temporary data on shutdown
lockPref("privacy.sanitize.sanitizeOnShutdown", true);
lockPref("privacy.clearOnShutdown.cookies", true);
lockPref("privacy.clearOnShutdown.downloads", true);
lockPref("privacy.clearOnShutdown.cache", true);
lockPref("privacy.clearOnShutdown.formData", true);
```

## 6.3 Crash reporter settings

The crash reporter cannot be disabled using the Firefox configuration files. Instead it can be manually disabled by setting a System environment variable. This setting can be [deployed](#)  using Group Policy:

Group Policy	Value(s)
Computer Configuration > Preferences > Windows Settings > Environment > Update > System Variable	Name = MOZ_CRASHREPORTER_DISABLE Value = 1

## 6.4 Proxy settings

The web proxy can be configured from inside Firefox, or the browser can inherit the Windows proxy settings.



## Firefox-controlled proxy settings

These settings will only affect Firefox, and will not be applied to other Windows applications. Change the proxy IP and port to match your organisation's network.

```
// HTTPS Proxy Configuration
lockPref("network.proxy.type", 1);
lockPref("network.proxy.ssl_port", 8080);
lockPref("network.proxy.ssl", "127.0.0.1");
```

## Windows-controlled proxy settings

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

```
// HTTPS Proxy Configuration
lockPref("network.proxy.type", 5);
```

Group Policy	Value(s)
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

Firefox uses Google's [Safe Browsing](#) service 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 Add-ons

The configuration above disables the user interface that allows users to install browser add-ons, encouraging them to only use ones deployed with the browser.

If add-on installation is enabled, they can be installed from both Mozilla.org or from elsewhere on the Internet. Firefox does not implement a list of allowed add-ons, but allows specific ones such as Flash selected ones to be disabled in the lock file. Organisations should ensure that unnecessary add-ons are removed and the remaining ones are kept up to date.

Organisations should consider the increased exposure to malware when enabling add-ons as they do not usually run inside a sandbox and will be able to access content from both Internet and intranet sites. A malicious add-on will be able to read, interact with and modify any Internet and intranet content accessed by the user including sites delivered over HTTPS. Firefox add-ons can include code that interacts with the platform. A malicious website that successfully exploits such an add-on can gain full user privilege including access to their data and web content. This interaction will not be visible to the user as plugins are able to get this access and send information to the internet in the background.

## 7.3 Firefox updates


Mozilla publishes an [Extended Support Release](#) (ESR) of Firefox that separates security patches from functionality improvements. This allows an enterprise to promptly apply security fixes while maintaining backwards compatibility with enterprise web services. Each ESR release is supported for approximately one year, making it necessary to schedule an annual full upgrade to ensure continued patch availability.

The mainstream (non-ESR) Firefox release integrates security patches and functionality updates into a single update mechanism. If an enterprise chooses to use the mainstream release rather than the ESR, it must be running the latest version of Firefox to remain fully patched.

Firefox automatically updates each endpoint using the Mozilla Maintenance Service. This polls the Internet for updates and applies them without user intervention. Mozilla does not provide an official MSI package as is required to automatically install or update Firefox natively using Active Directory. Organisations that choose to centrally manage software updates deployment instead of using the Internet-hosted maintenance service will need to make use of alternative software deployment mechanisms that may require third party tools.

## 7.4 Mozilla crash reporter

Like other browser vendors, Mozilla collects details of browser crashes to allow it to fix bugs. These reports include an amount of metadata describing the state of the browser and underlying platform and enough data to reproduce the crash. The submitted data will often include segments of the page being currently viewed, which may be sensitive if the user was accessing enterprise apps, cloud services or personal data at the time. Depending on how the web app works, it is possible for that data to include credentials or authentication tokens.

It is therefore advisable to disable such crash reporting mechanisms when accessing sensitive data. This is more important for Firefox as Mozilla automatically publishes the contents of submitted crash reports on the Internet on its [public site](#) .

It is not possible to disable the crash reporting mechanism using the Firefox configuration file. On Windows, it is possible to disable it using the System environment variable shown above. As this is not a fully documented feature, it is therefore a good idea to also block the submission URL at the enterprise proxy (if the enterprise proxy or firewall allow this), and monitor whether this URL changes in future versions.

## 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. This guidance is UK Crown Copyright. All Rights Reserved.