

# CIS Mozilla Firefox 102 ESR Benchmark

v1.0.0 - 02-06-2023

# 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

<b>Terms of Use .....</b>	<b>1</b>
<b>Table of Contents .....</b>	<b>2</b>
<b>Overview .....</b>	<b>5</b>
Intended Audience.....	5
Consensus Guidance .....	6
Typographical Conventions.....	7
<b>Recommendation Definitions.....</b>	<b>8</b>
Title.....	8
Assessment Status.....	8
Automated .....	8
Manual.....	8
Profile .....	8
Description.....	8
Rationale Statement .....	8
Impact Statement.....	9
Audit Procedure.....	9
Remediation Procedure.....	9
Default Value.....	9
References .....	9
CIS Critical Security Controls® (CIS Controls®) .....	9
Additional Information.....	9
Profile Definitions .....	10
Acknowledgements .....	11
<b>Recommendations .....</b>	<b>12</b>
<b>1 Configure Locked Preferences .....</b>	<b>12</b>
1.1 (L1) Create local-settings.js file (Automated) .....	13
1.2 (L1) Create mozilla.cfg file (Automated).....	14
1.3 (L1) Protect Firefox Binaries (Manual) .....	15
1.4 (L1) Set permissions on local-settings.js (Automated) .....	16
1.5 (L1) Set permissions on mozilla.cfg (Automated).....	17
<b>2 Updating Firefox .....</b>	<b>18</b>
2.1 (L1) Enable Automatic Updates (Automated).....	19
2.2 (L1) Set Search Provider Update Behavior (Automated) .....	21
2.3 (L1) Set Update Interval Time Checks (Automated) .....	22
2.4 (L1) Set Update Wait Time Prompt (Automated) .....	24

<b>3 Network Settings .....</b>	<b>26</b>
3.1 (L1) Disable Network Prefetch (Manual) .....	27
3.2 (L1) Disable NTLM v1 (Automated) .....	29
3.3 (L1) Disable WebRTC (Automated) .....	31
3.4 (L2) Enable IDN Show Punycode (Automated) .....	33
3.5 (L1) Set File URI Origin Policy (Automated) .....	34
3.6 (L1) Validate Proxy Settings (Manual) .....	35
<b>4 Encryption Settings .....</b>	<b>36</b>
4.1 (L1) Block Mixed Active Content (Automated) .....	37
4.2 (L2) Set OCSP Response Policy (Automated) .....	39
4.3 (L2) Set OCSP Use Policy (Automated) .....	41
4.4 (L1) Set Security TLS Version Maximum (Automated) .....	43
4.5 (L1) Set Security TLS Version Minimum (Automated) .....	45
4.6 (L2) Set SSL Override Behavior (Automated) .....	47
<b>5 JavaScript Settings .....</b>	<b>49</b>
5.1 (L1) Block Pop-up Windows (Automated) .....	50
5.2 (L1) Disable Closing of Windows via Scripts (Automated) .....	51
5.3 (L1) Disable Displaying JavaScript in History URLs (Automated) .....	52
5.4 (L1) Disable Moving or Resizing of Windows via Scripts (Manual) .....	53
5.5 (L1) Disable Raising or Lowering of Windows via Scripts (Manual) .....	55
<b>6 Privacy Settings .....</b>	<b>57</b>
6.1 (L2) Configure New Tab Page (Manual) .....	58
6.2 (L1) Disabled Browser Sign-ins (Manual) .....	61
6.3 (L1) Disable Firefox Shield Studies (Manual) .....	62
6.4 (L2) Disable Form Fill Assistance (Manual) .....	64
6.5 (L1) Disable Geolocation Services (Automated) .....	66
6.6 (L1) Disable Pocket (Manual) .....	67
6.7 (L1) Disable Sending Data (Manual) .....	69
6.8 (L1) Disallow Credential Storage (Automated) .....	70
6.9 (L1) Do Not Accept Third Party Cookies (Automated) .....	71
6.10 (L1) Enable Enhanced Tracking Protection (Manual) .....	73
6.11 (L1) Enable Tracking Protection (Automated) .....	74
6.12 (L1) Set Delay for Enabling Security Sensitive Dialog Boxes (Automated) .....	76
6.13 (L1) Disabled Delete Data Upon Shutdown (Manual) .....	78
<b>7 Extensions and Add-ons .....</b>	<b>80</b>
7.1 (L1) Disable Auto-Install of Add-ons (Automated) .....	81
7.2 (L1) Disable Development Tools (Manual) .....	83
7.3 (L1) Disable Encrypted Media Extensions (Manual) .....	85
7.4 (L1) Disable Popups Initiated by Plugins (Automated) .....	86
7.5 (L1) Disabled Recommended Extensions (Manual) .....	88
7.6 (L1) Enable Extension Auto Update (Automated) .....	90
7.7 (L1) Enable Extension Block List (Automated) .....	92
7.8 (L1) Enable Extension Update (Automated) .....	94
7.9 (L1) Enable Warning for External Protocol Handler (Automated) .....	96
7.10 (L1) Set Extension Update Interval Time Checks (Automated) .....	97
<b>8 Malware Settings .....</b>	<b>99</b>
8.1 (L1) Block Reported Attack Sites (Automated) .....	100
8.2 (L1) Block Reported Web Forgeries (Automated) .....	101
8.3 (L1) Enable Cryptomining Protection (Manual) .....	103

<b><i>Appendix: Summary Table .....</i></b>	<b><i>105</i></b>
<b><i>Appendix: Change History .....</i></b>	<b><i>108</i></b>

# Overview

All CIS Benchmarks focus on technical configuration settings used to maintain and/or increase the security of the addressed technology, and they should be used in **conjunction** with other essential cyber hygiene tasks like:

- Monitoring the base operating system for vulnerabilities and quickly updating with the latest security patches
- Monitoring applications and libraries for vulnerabilities and quickly updating with the latest security patches

In the end, the CIS Benchmarks are designed as a key **component** of a comprehensive cybersecurity program.

This document provides prescriptive guidance for establishing a secure configuration posture for the Mozilla Firefox 102 ESR Browser. This guide was tested against Mozilla Firefox 102.5.0 ESR on a Windows 10 Release 22H1 operating system. 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](mailto:feedback@cisecurity.org).

## Intended Audience

This benchmark 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 the Mozilla Firefox 102 ESR Browser.

## Consensus Guidance

This CIS Benchmark was created using a consensus review process comprised of a global community of subject matter experts. The process combines real world experience with data-based information to create technology specific guidance to assist users to secure their environments. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

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

## Typographical Conventions

The following typographical conventions are used throughout this guide:

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



# Recommendation Definitions

The following defines the various components included in a CIS recommendation as applicable. If any of the components are not applicable it will be noted or the component will not be included in the recommendation.

## Title

Concise description for the recommendation's intended configuration.

## Assessment Status

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

### Automated

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

### Manual

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

## Profile

A collection of recommendations for securing a technology or a supporting platform. Most benchmarks include at least a Level 1 and Level 2 Profile. Level 2 extends Level 1 recommendations and is not a standalone profile. The Profile Definitions section in the benchmark provides the definitions as they pertain to the recommendations included for the technology.

## Description

Detailed information pertaining to the setting with which the recommendation is concerned. In some cases, the description will include the recommended value.

## Rationale Statement

Detailed reasoning for the recommendation to provide the user a clear and concise understanding on the importance of the recommendation.

## **Impact Statement**

Any security, functionality, or operational consequences that can result from following the recommendation.

## **Audit Procedure**

Systematic instructions for determining if the target system complies with the recommendation

## **Remediation Procedure**

Systematic instructions for applying recommendations to the target system to bring it into compliance according to the recommendation.

## **Default Value**

Default value for the given setting in this recommendation, if known. If not known, either not configured or not defined will be applied.

## **References**

Additional documentation relative to the recommendation.

## **CIS Critical Security Controls® (CIS Controls®)**

The mapping between a recommendation and the CIS Controls is organized by CIS Controls version, Safeguard, and Implementation Group (IG). The Benchmark in its entirety addresses the CIS Controls safeguards of (v7) "5.1 - Establish Secure Configurations" and (v8) "4.1 - Establish and Maintain a Secure Configuration Process" so individual recommendations will not be mapped to these safeguards.

## **Additional Information**

Supplementary information that does not correspond to any other field but may be useful to the user.

## Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1**

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**

This profile extends the "Level 1" 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.

## 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:

Special thanks to the following contributors to previous CIS Benchmarks for Mozilla Firefox, from which this update drew heavily from: Waqas Nazir, Derek Armstrong, Andy Sampson, Blake Frantz, David Bailey, David Skrdla, Patrick McCafferty, Peter Thoenen, Ridley DiSiena, Ron Colvin, Steven Piliero, Tom Ueltschi.

### **Editor**

Jennifer Jarose

Matthew Woods

### **Contributor**

Randie Bejar

# Recommendations

## 1 Configure Locked Preferences

This section describes how to enable locked preferences for Firefox. The files outlined in this section are used to configure most of the other recommendations listed in this benchmark.

## 1.1 (L1) Create local-settings.js file (Automated)

### Profile Applicability:

- Level 1

### Description:

The `local-settings.js` file is used by Firefox to reference and load the `mozilla.cfg` file which contains all the locked preferences.

### Rationale:

Loading a custom configuration file is a primary mechanism for setting and enforcing security requirements within Firefox.

### Impact:

None.

### Audit:

Perform the following procedure:

1. Type `about:config` in the address bar
2. Type `app.update` in the filter
3. Ensure the preferences listed are set to the values specified below:

```
<span>general.config.obscure_value</span>=0  
g<span>eneral.config.filename=mozilla.cfg</span>
```

### Remediation:

Perform the following procedure:

1. Navigate to the `defaults/pref` directory inside the Firefox installation directory and create a file called `local-settings.js`.
2. Include the following lines in `local-settings.js`:

```
pref("general.config.obscure_value", 0);  
pref("general.config.filename", "mozilla.cfg");
```

### Default Value:

Not configured.

## 1.2 (L1) Create mozilla.cfg file (Automated)

### Profile Applicability:

- Level 1

### Description:

The `mozilla.cfg` file is used by Firefox to configure all the locked preferences.

### Rationale:

Loading a custom configuration file is a primary mechanism for setting and enforcing security requirements in Firefox.

### Impact:

None.

### Audit:

Perform the following procedure:

1. Navigate to the Firefox installation directory and ensure there is a file called `mozilla.cfg`.
2. Ensure the first line of the file is a comment:

```
//
```

### Remediation:

Perform the following procedure:

1. Navigate to the Firefox installation directory and create a file called `mozilla.cfg`.
2. The first line of the file must be a comment:

```
//
```

### Default Value:

Not configured.

## 1.3 (L1) Protect Firefox Binaries (Manual)

### Profile Applicability:

- Level 1

### Description:

Ensure that Firefox is installed and owned by an administrative account in order to protect the binaries and to prevent users from circumventing security settings.

### Rationale:

When Firefox is installed by an ordinary user, the software is installed into the user's profile / home directory. This avoids the requirement for administrative access during installation and upgrades, but also allows users to circumvent security settings defined in settings.js and mozilla.cfg files. Having the installation owned by an administrative user can also protect binary and configuration files from malware that is executed in an ordinary user's browser.

### Impact:

Ordinary users will not be able to update or patch Firefox; only Administrators can perform upgrades.

### Audit:

Confirm that Firefox is not installed in any individual user profiles or home directories.

### Remediation:

Install Firefox into a shared location that can be accessed by users but modified only by Administrators.

### Default Value:

N/A



## *1.4 (L1) Set permissions on local-settings.js (Automated)*

### **Profile Applicability:**

- Level 1

### **Description:**

Set permissions on `local-settings.js` so that it can only be modified or deleted by an Administrator.

### **Rationale:**

Any users with the ability to modify the `local-settings.js` file can bypass all security configurations by changing the file or deleting it.

### **Impact:**

Non-administrative users will not be able to write to the `local-settings.js`.

### **Audit:**

Ensure non-administrators do not possess the ability to write to `local-settings.js`.

### **Remediation:**

Deny non-administrators the ability to write to `local-settings.js`.

### **Default Value:**

Not configured.

## *1.5 (L1) Set permissions on mozilla.cfg (Automated)*

### **Profile Applicability:**

- Level 1

### **Description:**

Set permissions on `mozilla.cfg` so that it can only be modified or deleted by an Administrator.

### **Rationale:**

Any users with the ability to modify the `mozilla.cfg` file can bypass all security configurations by changing the file or deleting it.

### **Impact:**

Non-administrative user will not be able to write to the `mozilla.cfg` file.

### **Audit:**

Ensure non-administrators do not possess the ability to write to `mozilla.cfg`.

### **Remediation:**

Deny non-administrators the ability to write to `mozilla.cfg`.

### **Default Value:**

Not configured.

## 2 Updating Firefox

This section will discuss how to enable auto updates in Firefox.

## 2.1 (L1) Enable Automatic Updates (Automated)

### Profile Applicability:

- Level 1

### Description:

This setting configures Firefox to automatically download and install updates as they are made available.

### Rationale:

Security updates ensure that users are safe from known software bugs and vulnerabilities.

### Impact:

None - This is the default behavior.

### Audit:

Ensure that the following values are set to `true`:

- `app.update.enabled`
  - `app.update.auto`
  - `app.update.staging.enabled`
1. Type `about:config` in the address bar
  2. Type `app.update.enabled` in the filter
  3. Ensure the setting is set as prescribed.
  4. Type `app.update.auto` in the filter
  5. Ensure the setting is set as prescribed.
  6. Type `app.update.staging.enabled` in the filter
  7. Ensure the setting is set as prescribed.

## Remediation:

To establish the recommended configuration, set the following values to `true`:

- `app.update.enabled`
  - `app.update.auto`
  - `app.update.staging.enabled`
1. Type `about:config` in the address bar
  2. Type `app.update.enabled` in the filter
  3. Configure the setting as prescribed.
  4. Type `app.update.auto` in the filter
  5. Configure the setting as prescribed.
  6. Type `app.update.staging.enabled` in the filter
  7. Configure the setting as prescribed.

OR

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("app.update.enabled", true);  
lockPref("app.update.auto", true);  
lockPref("app.update.staging.enabled", true);
```







## Default Value:

`app.update.enabled=true`

`app.update.auto=true`

`app.update.staging.enabled=true`

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>7.4 Perform Automated Application Patch Management</b> Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.			
v7	<b>3.5 Deploy Automated Software Patch Management Tools</b> Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.			

## 2.2 (L1) Set Search Provider Update Behavior (Automated)

### Profile Applicability:

- Level 1

### Description:

This setting dictates whether Firefox will update installed search providers. Search providers allow the user to search directly from the "Search bar" which is adjacent to the URL bar.

### Rationale:

Software updates help ensure that users are safe from known software bugs and vulnerabilities.

### Impact:

None - This is the default behavior.

### Audit:

Ensure that `browser.search.update` is set to `true`:

1. Type `about:config` in the address bar
2. Type `browser.search.update` in the filter
3. Configure the setting as prescribed.

### Remediation:

To establish the recommended configuration, set `browser.search.update` to `true`:

1. Type `about:config` in the address bar
2. Type `browser.search.update` in the filter
3. Configure the setting as prescribed.

OR

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("browser.search.update", true);
```

### Default Value:

true

## 2.3 (L1) Set Update Interval Time Checks (Automated)

### Profile Applicability:

- Level 1

### Description:

This setting configures the amount of time the system waits in between each check for updates.

### Rationale:

Frequent checks for updates will help mitigate vulnerabilities.

### Impact:

`app.update.enabled` must be set to true for this preference to take effect.

### Audit:

Ensure that `app.update.interval` is set to 43200:

1. Type `about:config` in the address bar
2. Type `app.update.interval` in the filter
3. Configure the setting as prescribed.

### Remediation:

To establish the recommended configuration, set `app.update.interval` to 43200:

1. Type `about:config` in the address bar
2. Type `app.update.interval` in the filter
3. Configure the setting as prescribed.

OR




1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("app.update.interval", 43200);
```

### Default Value:

43200

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b><u>7.1 Establish and Maintain a Vulnerability Management Process</u></b> Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			



## 2.4 (L1) Set Update Wait Time Prompt (Automated)

### Profile Applicability:

- Level 1

### Description:

This setting determines the amount of time, in seconds, which the system will wait before displaying the Software Update dialogue box (after an unobtrusive alert has already been shown).

### Rationale:

Encouraging the user to update software as soon as possible mitigates the risk that a system will be left vulnerable.

### Impact:

For this preference to have an effect `app.update.enabled` must be true.

### Audit:

Ensure that `app.update.promptWaitTime` is set to 172800:

1. Type `about:config` in the address bar
2. Type `app.update.promptWaitTime` in the filter
3. Configure the setting as prescribed.

### Remediation:

To establish the recommended configuration, set `app.update.promptWaitTime` to 172800:

1. Type `about:config` in the address bar
2. Type `app.update.promptWaitTime` in the filter
3. Configure the setting as prescribed.

OR




1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("app.update.promptWaitTime", 172800);
```

### Default Value:

691200

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b><u>7.1 Establish and Maintain a Vulnerability Management Process</u></b> Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			

## 3 Network Settings

This section provides guidance for configuring portions of Firefox exposed via the Network Settings dialog.

### *3.1 (L1) Disable Network Prefetch (Manual)*

#### **Profile Applicability:**

- Level 1

#### **Description:**

This setting configures if Firefox is allowed to make URL requests without user consent.

#### **Rationale:**

Prefetching URLs could lead to misinformation on browser history such a a website that was not visited but the user hovered over the URL link. This can be misleading in a forensic investigation.

In addition, there is a chance that information can be leaked about a local network if connected to a public network.

#### **Impact:**

None - This is the default behavior.

#### **Audit:**

Ensure that `Network.dns.disablePrefetch` is set to `true`:

1. Type `about:config` in the address bar
2. Type `Network.dns.disablePrefetch` in the filter
3. Ensure the setting is set as prescribed.

## Remediation:

To establish the recommended configuration, set `Network.dns.disablePrefetch` to `true`:

1. Type `about:config` in the address bar
2. Type `Network.dns.disablePrefetch` in the filter
3. Ensure the setting is set as prescribed.

OR

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("Network.dns.disablePrefetch", true);
```



## Default Value:

False (Enabled).

## References:

1. <https://www.ghacks.net/2013/04/27/firefox-prefetching-what-you-need-to-know/>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>9.3 <u>Maintain and Enforce Network-Based URL Filters</u></b> Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.			

## 3.2 (L1) Disable NTLM v1 (Automated)

### Profile Applicability:

- Level 1

### Description:

This setting controls the use of NT Lan Manager (NTLM) v1 protocol that can be used for authentication to resources that request or require this authentication type.

### Rationale:

NTLM v1 contains cryptographic weaknesses that can be easily exploited to obtain user credentials.

### Impact:

This may affect websites and browsers that require the use of NTLM v1

### Audit:

Ensure that `network.auth.force-generic-ntlm-v1` is set to `false`:

1. Type `about:config` in the address bar
2. Type `network.auth.force-generic-ntlm-v1` in the filter
3. Ensure the setting is set as prescribed.

### Remediation:

To establish the recommended configuration, set `network.auth.force-generic-ntlm-v1` to `false`:

1. Type `about:config` in the address bar
2. Type `network.auth.force-generic-ntlm-v1` in the filter
3. Configure the setting as prescribed.

*OR*

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("network.auth.force-generic-ntlm-v1", false)
```

### Default Value:

False

**Additional Information:**

This configuration was previously set with "network.negotiate-auth.allow-insecure-ntlm-v1"

### 3.3 (L1) Disable WebRTC (Automated)

#### Profile Applicability:

- Level 1

#### Description:

These settings determine whether Web Real Time Communications (WebRTC) is allowed. WebRTC is used for peer-to-peer communication such as file sharing or video calls.

#### Rationale:

WebRTC can expose private information such as internal IP addresses and computer settings.

#### Impact:

WebRTC will not be accessible to users.

#### Audit:

Ensure that the following values are set to `false`:

- `media.peerconnection`
  - `media.peerconnection.use_document_iceservers`
1. Type `about:config` in the address bar
  2. Type `media.peerconnection` in the filter
  3. Ensure the setting is set as prescribed.
  4. Type `media.peerconnection.use_document_iceservers` in the filter
  5. Ensure the setting is set as prescribed.



## Remediation:

To establish the recommended configuration, set the following values to `false`:

- `media.peerconnection`
  - `media.peerconnection.use_document_iceservers`
1. Type `about:config` in the address bar
  2. Type `media.peerconnection` in the filter
  3. Ensure the setting is set as prescribed.
  4. Type `media.peerconnection.use_document_iceservers` in the filter
  5. Ensure the setting is set as prescribed.

*OR*

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("media.peerconnection.enabled", false);  
lockPref("media.peerconnection.use_document_iceservers", false);
```

## Default Value:

True

### 3.4 (L2) Enable IDN Show Punycode (Automated)

#### Profile Applicability:

- Level 2

#### Description:

This setting determines whether Internationalized Domain Names (IDNs) displayed in the browser are displayed as Punycode or as Unicode.

#### Rationale:

IDNs displayed in Punycode are easier to identify and therefore help mitigate the risk of accessing spoofed web pages.

#### Audit:

Ensure that `network.IDN_show_punycode` is set to `true`:

1. Type `about:config` in the address bar
2. Type `network.IDN_show_punycode` in the filter
3. Ensure the setting is set as prescribed.

#### Remediation:

To establish the recommended configuration, set `network.IDN_show_punycode` to `true`:

1. Type `about:config` in the address bar
2. Type `network.IDN_show_punycode` in the filter
3. Configure the setting as prescribed.

*OR*

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("network.IDN_show_punycode", true);
```

#### Default Value:

False

## 3.5 (L1) Set File URI Origin Policy (Automated)

### Profile Applicability:

- Level 1

### Description:

This setting determines the restrictions placed on the scripts and links loaded into the browser from local HTML files.

### Rationale:

Applying the same origin policy to local files will help mitigate the risk of unauthorized access to sensitive information.

### Impact:

None - This is the default behavior.

### Audit:

Ensure that `security.fileuri.strict_origin_policy` is set to `true`:

1. Type `about:config` in the address bar
2. Type `security.fileuri.strict_origin_policy` in the filter
3. Ensure the setting is set as prescribed.

### Remediation:

To establish the recommended configuration, set `security.fileuri.strict_origin_policy` to `true`:

1. Type `about:config` in the address bar
2. Type `security.fileuri.strict_origin_policy` in the filter
3. Configure the setting as prescribed.

OR

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("security.fileuri.strict_origin_policy", true);
```

### Default Value:

True

## 3.6 (L1) Validate Proxy Settings (Manual)

### Profile Applicability:

- Level 1

### Description:

Firefox can be configured to use one or more proxy servers. When a proxy server is configured for a given protocol (HTTP, FTP, Gopher, etc), Firefox will send applicable requests to that proxy server for fulfillment. It is recommended that the list of proxy servers configured in Firefox be reviewed to ensure it contains only trusted proxy servers.

### Rationale:

Depending on the protocol used, the proxy server will have access to read and/or alter all information communicated between Firefox and the target server, such a web site.

### Audit:

Perform the following procedure:

1. Drop down the `Firefox` menu
2. Click on `Settings`
3. Scroll down to the `Network Settings` section
4. Click on `Settings` Button
5. Ensure that the proxy listed (if any) is the one configured and approved by the enterprise.

### Remediation:

Perform the following procedure:

1. Drop down the `Firefox` menu
2. Click on `Settings`
3. Scroll down to the `Network Settings` section
4. Click on `Settings` Button
5. Ensure that the proxy listed (if any) is the one configured and approved by the enterprise.

### Default Value:

No proxy.

## 4 Encryption Settings

This section will discuss how to set up encryption settings in Firefox.

## 4.1 (L1) Block Mixed Active Content (Automated)

### Profile Applicability:

- Level 1

### Description:

This setting disables the ability to view HTTP content such as JavaScript, CSS, objects, and xhr requests.

### Rationale:

Blocking active mixed content minimizes the risk of man-in-the-middle attacks.

### Impact:

None - This is the default behavior.

### Audit:

Ensure that `security.mixed_content.block_active_content` is set to `true`:

1. Type `about:config` in the address bar
2. Type `security.mixed_content.block_active_content` in the filter
3. Ensure the setting is set as prescribed.

### Remediation:

To establish the recommended configuration, set `security.mixed_content.block_active_content` to `true`:

1. Type `about:config` in the address bar
2. Type `security.mixed_content.block_active_content` in the filter
3. Ensure the setting is set as prescribed.

OR





1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("security.mixed_content.block_active_content", true);
```

### Default Value:

True

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>9.6 <u>Block Unnecessary File Types</u></b> Block unnecessary file types attempting to enter the enterprise's email gateway.			
v7	<b>7.9 <u>Block Unnecessary File Types</u></b> Block all e-mail attachments entering the organization's e-mail gateway if the file types are unnecessary for the organization's business.			

## 4.2 (L2) Set OCSP Response Policy (Automated)

### Profile Applicability:

- Level 2

### Description:

This setting dictates whether Firefox will consider a given certificate to be invalid if it is unable to obtain an Online Certificate Status Protocol (OCSP) response for it.

### Rationale:

Requiring an OCSP response will reduce an adversary's ability to successfully leverage a compromised and revoked certificate.

### Impact:

Requiring an OCSP response increases opportunity for valid certificates to be deemed invalid. This may occur if OCSP server becomes unavailable or is not accessible.

### Audit:

Ensure that `security.ocsp.require` is set to `true`:

1. Type `about:config` in the address bar
2. Type `security.ocsp.require` in the filter
3. Ensure the setting is set as prescribed.

### Remediation:

To establish the recommended configuration, set `security.ocsp.require` to `true`:

1. Type `about:config` in the address bar
2. Type `security.ocsp.require` in the filter
3. Ensure the setting is set as prescribed.

OR

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("security.ocsp.require", true);
```

### Default Value:

False



## References:

1. <https://www.grc.com/revocation/ocsp-must-staple.htm>
2. <https://www.imperialviolet.org/2014/04/19/revchecking.html>
3. <https://blog.mozilla.org/security/2013/07/29/ocsp-stapling-in-firefox/>

### 4.3 (L2) Set OCSP Use Policy (Automated)

#### Profile Applicability:

- Level 2

#### Description:

This setting dictates whether Firefox will leverage Online Certificate Status Protocol (OCSP) to determine if a given certificate has been revoked.

#### Rationale:

Leveraging OCSP may help identify revoked certificates.

#### Impact:

None - This is the default behavior.

#### Audit:

Ensure that `security.OCSP.enabled` is set to 1:

1. Type `about:config` in the address bar
2. Type `security.OCSP.enabled` in the filter
3. Ensure the setting is set as prescribed.

**Note:** A configuration of 2 also conforms with this benchmark.

#### Remediation:

To establish the recommended configuration, set `security.OCSP.enabled` to 1:

1. Type `about:config` in the address bar
2. Type `security.OCSP.enabled` in the filter
3. Ensure the setting is set as prescribed.

OR

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("security.OCSP.enabled", 1);
```

**Note:** Configuring this setting to 2 also conforms with this benchmark.

#### Default Value:

1

## References:

1. [https://wiki.mozilla.org/CA:ImprovingRevocation#OCSP\\_Stapling](https://wiki.mozilla.org/CA:ImprovingRevocation#OCSP_Stapling)
2. <https://blog.mozilla.org/security/2013/07/29/ocsp-stapling-in-firefox/>

## 4.4 (L1) Set Security TLS Version Maximum (Automated)

### Profile Applicability:

- Level 1

### Description:

This setting sets the maximum required protocol version for the Transport Layer Security (TLS).

### Rationale:

Setting TLS 1.2 as the maximum authorized protocol version mitigates the risk of using an insecure connection.

### Audit:

Ensure that `security.tls.version.max` is set to 3:

1. Type `about:config` in the address bar
2. Type `security.tls.version.max` in the filter
3. Ensure the setting is set as prescribed.

### Remediation:

To establish the recommended configuration, set `security.tls.version.max` to 3:

1. Type `about:config` in the address bar
2. Type `security.tls.version.max` in the filter
3. Ensure the setting is set as prescribed.

*OR*





1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("security.tls.version.max", 3);
```

### Default Value:

4

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.10 <u>Encrypt Sensitive Data in Transit</u></b> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v7	<b>14.4 <u>Encrypt All Sensitive Information in Transit</u></b> Encrypt all sensitive information in transit.			

## 4.5 (L1) Set Security TLS Version Minimum (Automated)

### Profile Applicability:

- Level 1

### Description:

This setting sets the minimum protocol version that may be used when negotiating TLS/SSL sessions.

### Rationale:

Setting TLS 1.2 as the minimum protocol version mitigates the risk of negotiating an insecure protocol, such as TSL 1.0 or SSL 2.0.

### Impact:

Communications that require an older version of TLS/SSL will be blocked.

### Audit:

Ensure that `security.tls.version.min` is set to 3:

1. Type `about:config` in the address bar
2. Type `security.tls.version.min` in the filter
3. Ensure the setting is set as prescribed.

### Remediation:

To establish the recommended configuration, set `security.tls.version.min` to 3:

1. Type `about:config` in the address bar
2. Type `security.tls.version.min` in the filter
3. Ensure the setting is set as prescribed.

OR





1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("security.tls.version.min", 3);
```

### Default Value:

3

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.10 <u>Encrypt Sensitive Data in Transit</u></b> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v7	<b>14.4 <u>Encrypt All Sensitive Information in Transit</u></b> Encrypt all sensitive information in transit.			

## 4.6 (L2) Set SSL Override Behavior (Automated)

### Profile Applicability:

- Level 2

### Description:

This setting controls whether Firefox will or will not automatically fill in the URL text box and auto-fetch the certificate on behalf of the user. When Firefox encounters an invalid certificate and the user clicks "Add Exception", a dialog is displayed with a text box to fetch the certificate from the given URL.

### Rationale:

Requiring the user to manually enter the server's URL and fetch the certificate may provide additional opportunity to scrutinize the certificate before adding an exception for a potentially fraudulent certificate.

### Impact:

Setting this configuration to 0 forces the user to enter a URL and click the "Get Certificate" button before adding an exception for an invalid cert.

### Audit:

Ensure that `browser.ssl_override_behavior` is set to 0:

1. Type `about:config` in the address bar
2. Type `browser.ssl_override_behavior` in the filter
3. Ensure the setting is set as prescribed.



**Remediation:**

To establish the recommended configuration, set `browser.ssl_override_behavior` to 0:

1. Type `about:config` in the address bar
2. Type `browser.ssl_override_behavior` in the filter
3. Ensure the setting is set as prescribed.

*OR*

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("browser.ssl_override_behavior", 0);
```

**Default Value:**

2

## 5 JavaScript Settings

This section will provide guidance on how to use advanced JavaScript settings to guard against certain attacks.

## 5.1 (L1) Block Pop-up Windows (Automated)

### Profile Applicability:

- Level 1

### Description:

This setting allows for the configuration of the Firefox pop-up blocker.

### Rationale:

By enabling the pop-up blocker, all pop-ups will be blocked which will guard a user against malicious attacks launched using a pop-up window.

### Impact:

Legitimate pop-ups will be blocked.

### Audit:

Ensure that `privacy.popups.policy` is set to 1:

1. Type `about:config` in the address bar
2. Type `privacy.popups.policy` in the filter
3. Ensure the setting is set as prescribed.

### Remediation:

To establish the recommended configuration, set `privacy.popups.policy` to 1:

1. Type `about:config` in the address bar
2. Type `privacy.popups.policy` in the filter
3. Ensure the setting is set as prescribed.

*OR*

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("privacy.popups.policy", 1);
```

### Default Value:

1

## 5.2 (L1) Disable Closing of Windows via Scripts (Automated)

### Profile Applicability:

- Level 1

### Description:

This setting allows the configuration of how Firefox handles scripts from closing browser windows.

### Rationale:

Preventing an arbitrary web site from closing the browser window will reduce the probability of a user losing work or state being performed in another tab within the same window.

### Impact:

None - This is the default behavior.

### Audit:

Ensure that `dom.allow_scripts_to_close_windows` is set to `false`:

1. Type `about:config` in the address bar
2. Type `dom.allow_scripts_to_close_windows` in the filter
3. Ensure the setting is set as prescribed.

### Remediation:

To establish the recommended configuration, set `dom.allow_scripts_to_close_windows` to `false`:

1. Type `about:config` in the address bar
2. Type `dom.allow_scripts_to_close_windows` in the filter
3. Ensure the setting is set as prescribed.

*OR*

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("dom.allow_scripts_to_close_windows", false);
```

### Default Value:

False

## 5.3 (L1) Disable Displaying JavaScript in History URLs (Automated)

### Profile Applicability:

- Level 1

### Description:

This setting controls JavaScript URLs history from being displayed in the history bar.

### Rationale:

Various browser elements, even a simple link, can embed `javascript:` URLs and access the `javascript:` protocol. The JavaScript statement used in a `javascript:` URL can be used to encapsulate a specially crafted URL that performs a malicious function.

### Impact:

None - This is the default behavior.

### Audit:

Ensure that `browser.urlbar.filter.javascript` is set to `true`:

1. Type `about:config` in the address bar
2. Type `browser.urlbar.filter.javascript` in the filter
3. Ensure the setting is set as prescribed.

### Remediation:

To establish the recommended configuration, set `browser.urlbar.filter.javascript` to `true`:

1. Type `about:config` in the address bar
2. Type `browser.urlbar.filter.javascript` in the filter
3. Ensure the setting is set as prescribed.

OR

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("browser.urlbar.filter.javascript", true);
```

### Default Value:

True

## 5.4 (L1) Disable Moving or Resizing of Windows via Scripts (Manual)

### Profile Applicability:

- Level 1

### Description:

This setting allows the configuration of how Firefox handles scripts from moving or resizing browser windows.

### Rationale:

Arbitrary web sites can disguise an attack taking place in a minimized background window by moving or resizing browser windows.

### Impact:

Scripts will not be able to move or resize browser windows.

This is the default behavior.

### Audit:

Ensure that `dom.disable_window_move_resize` is set to `false`:

1. Type `about:config` in the address bar
2. Type `dom.disable_window_move_resize` in the filter
3. Ensure the setting is set as prescribed.

## Remediation:

To establish the recommended configuration, set `dom.disable_window_move_resize` to `false`:

1. Type `about:config` in the address bar
2. Type `dom.disable_window_move_resize` in the filter
3. Ensure the setting is set as prescribed.

*OR*


1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("dom.disable_window_move_resize", false);
```

## Default Value:

False (Disabled).

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>2.7 Allowlist Authorized Scripts</b> Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.			

## 5.5 (L1) Disable Raising or Lowering of Windows via Scripts (Manual)

### Profile Applicability:

- Level 1

### Description:

This setting allows the configuration of how Firefox handles scripts from raising or lowering browser windows.

### Rationale:

An arbitrary web site raising or lowering the browser window can cause improper input or can help disguise an attack taking place in a lowered window.

### Impact:

Scripts will not be able to raise or lower browser windows.

### Audit:

Ensure that `dom.disable_window_flip` is set to `false`:

1. Type `about:config` in the address bar
2. Type `dom.disable_window_flip` in the filter
3. Ensure the setting is set as prescribed.

### Remediation:

To establish the recommended configuration, set `dom.disable_window_flip` to `false`:

1. Type `about:config` in the address bar
2. Type `dom.disable_window_flip` in the filter
3. Ensure the setting is set as prescribed.

*OR*

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:


```
lockPref("dom.disable_window_flip", false);
```

### Default Value:

True (Enabled).



## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>2.7 Allowlist Authorized Scripts</b> Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.			

## 6 Privacy Settings

This section contains recommendations pertaining largely to privacy as it relates to browsing behaviors. While Firefox contains several settings that allow a user to sanitize and/or avoid persisting browsing artifacts, such as download history, caches, form data, etc, this section does not contain recommendations for configuring such settings. Users concerned with the privacy implications of such artifacts are encouraged to browse in a "Private Window". For more information on private browsing in Firefox, please see: <https://support.mozilla.org/en-US/kb/private-browsing-browse-web-without-saving-info>.

## 6.1 (L2) Configure New Tab Page (Manual)

### Profile Applicability:

- Level 2

### Description:

The New Tab page shows a list of built-in top sites, as well as the top sites the user has visited by default.

### Rationale:

Allowing the collection of browsing history by Firefox could inadvertently lead to sensitive data being exposed.

### Impact:

Top site and user history will not be available on a new tab.

### Audit:

Ensure that the following values are set to `false`:

- `browser.urlbar.suggest.history`
- `browser.newtabpage.activity-stream.feeds.topsites`
- `browser.newtabpage.activity-stream.feeds.snippets`
- `browser.newtabpage.activity-stream.feeds.section.topstories`
- `browser.newtabpage.activity-stream.section.highlights.includePocket`
- `browser.newtabpage.activity-stream.feeds.section.highlights`

1. Type `about:config` in the address bar
2. Type `browser.urlbar.suggest.history` in the filter
3. Ensure the setting is set as prescribed.
4. Type `browser.newtabpage.activity-stream.feeds.topsites` in the filter
5. Ensure the setting is set as prescribed.
6. Type `browser.newtabpage.activity-stream.feeds.snippets` in the filter
7. Ensure the setting is set as prescribed.
8. Type `browser.newtabpage.activity-stream.feeds.section.topstories` in the filter
9. Ensure the setting is set as prescribed.
10. Type `browser.newtabpage.activity-stream.section.highlights.includePocket` in the filter
11. Ensure the setting is set as prescribed.
12. Type `browser.newtabpage.activity-stream.feeds.section.highlights` in the filter
13. Ensure the setting is set as prescribed.

## Remediation:

To establish the recommended configuration, set the following values to `false`:

- `browser.urlbar.suggest.history`
  - `browser.newtabpage.activity-stream.feeds.topsites`
  - `browser.newtabpage.activity-stream.feeds.snippets`
  - `browser.newtabpage.activity-stream.feeds.section.topstories`
  - `browser.newtabpage.activity-stream.section.highlights.includePocket`
  - `browser.newtabpage.activity-stream.feeds.section.highlights`
1. Type `about:config` in the address bar
  2. Type `browser.urlbar.suggest.history` in the filter
  3. Configure the setting as prescribed.
  4. Type `browser.newtabpage.activity-stream.feeds.topsites` in the filter
  5. Configure the setting as prescribed.
  6. Type `browser.newtabpage.activity-stream.feeds.snippets` in the filter
  7. Configure the setting as prescribed.
  8. Type `browser.newtabpage.activity-stream.feeds.section.topstories` in the filter
  9. Configure the setting as prescribed.
  10. Type `browser.newtabpage.activity-stream.section.highlights.includePocket` in the filter
  11. Configure the setting as prescribed.
  12. Type `browser.newtabpage.activity-stream.feeds.section.highlights` in the filter
  13. Configure the setting as prescribed.

*OR*

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("browser.urlbar.suggest.history", false);
lockPref("browser.newtabpage.activity-stream.feeds.topsites", false);
lockPref("browser.newtabpage.activity-stream.feeds.snippets", false);
lockPref("browser.newtabpage.activity-stream.feeds.section.topstories",
false);
lockPref("browser.newtabpage.activity-
stream.section.highlights.includePocket", false);
lockPref("browser.newtabpage.activity-stream.feeds.section.highlights",
false);
```

**Default Value:**

`browser.urlbar.suggest.history = true`

`browser.newtabpage.activity-stream.feeds.topsites = true`

`browser.newtabpage.activity-stream.feeds.snippets = false`

`browser.newtabpage.activity-stream.feeds.section.topstories = true`

`browser.newtabpage.activity-stream.section.highlights.includePocket = true`

`browser.newtabpage.activity-stream.feeds.section.highlights = false`

## 6.2 (L1) Disabled Browser Sign-ins (Manual)

### Profile Applicability:

- Level 1

### Description:

This policy setting controls whether a user can sign into Firefox with an account to use services.

### Rationale:

Syncing user data especially from a personal account can contain data that is not appropriate for an enterprise environment.

### Impact:

Users will not be able to sign into the Firefox browser.

### Audit:

Ensure that `identity.fxaccounts.enabled` is set to `false`:

1. Type `about:config` in the address bar
2. Type `identity.fxaccounts.enabled` in the filter
3. Ensure the setting is set as prescribed.

### Remediation:

To establish the recommended configuration, set `identity.fxaccounts.enabled` to `false`:

1. Type `about:config` in the address bar
2. Type `identity.fxaccounts.enabled` in the filter
3. Ensure the setting is set as prescribed.

OR

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("identity.fxaccounts.enabled", false);
```

### Default Value:

True (Enabled).

## 6.3 (L1) Disable Firefox Shield Studies (Manual)

### Profile Applicability:

- Level 1

### Description:

Shield Studies are controlled tests that allow proposed changes to be compared to the current default version of Firefox for representative populations before releasing and pushing those changes to everyone else.

### Rationale:

If you decide to opt-in to Shield Studies, you agree to let Firefox collect data for their use. This data includes usage hours, what day Firefox was used on, study info (Study Name/ID, Experimental Branch), and study status transition events. Allowing this data to be shared with Firefox could lead to inadvertently sharing sensitive data.

### Impact:

Data will not be shared with Firefox.

### Audit:

Ensure that `app.shield.optoutstudies.enabled` is set to `true`:

1. Type `about:config` in the address bar
2. Type `app.shield.optoutstudies.enabled` in the filter
3. Ensure the setting is set as prescribed.

## Remediation:

To establish the recommended configuration, set `app.shield.optoutstudies.enabled` to `true`:

1. Type `about:config` in the address bar
2. Type `app.shield.optoutstudies.enabled` in the filter
3. Configure the setting as prescribed.

*OR*

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("app.shield.optoutstudies.enabled", true)
```

## Default Value:

True (Enabled).



## 6.4 (L2) Disable Form Fill Assistance (Manual)

### Profile Applicability:

- Level 2

### Description:

Form Fill Assistance allows Firefox to save data that has been entered into forms by users so that future operations are performed faster.

### Rationale:

This mitigates the risk of websites extracting information from prefilled text fields.

### Impact:

Prefilled text fields will not be enabled.

### Audit:

Ensure that `browser.formfill.enable` is set to `false`:

1. Type `about:config` in the address bar
2. Type `browser.formfill.enable` in the filter
3. Ensure the setting is set as prescribed.

### Remediation:

To establish the recommended configuration, set `browser.formfill.enable` to `false`:

1. Type `about:config` in the address bar
2. Type `browser.formfill.enable` in the filter
3. Ensure the setting is set as prescribed.

*OR*




1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("browser.formfill.enable", false);
```

### Default Value:

True (Enabled).

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.1 <u>Establish and Maintain a Data Management Process</u></b> Establish and maintain a data management process. In the process, address data sensitivity, data owner, handling of data, data retention limits, and disposal requirements, based on sensitivity and retention standards for the enterprise. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			

## 6.5 (L1) Disable Geolocation Services (Automated)

### Profile Applicability:

- Level 1

### Description:

This settings determines whether Firefox will provide geographic location information to websites.

### Rationale:

Geo-location services can expose private information to remote websites.

### Impact:

Geo-locations services will be unavailable. Site that use geo-location (Google Maps etc.) will not be able to attain information to pinpoint location.

### Audit:

Ensure that `geo.enabled` is set to `false`:

1. Type `about:config` in the address bar
2. Type `geo.enabled` in the filter
3. Ensure the setting is set as prescribed.

### Remediation:

To establish the recommended configuration, set `geo.enabled` to `false`:

1. Type `about:config` in the address bar
2. Type `geo.enabled` in the filter
3. Ensure the setting is set as prescribed.

OR

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("geo.enabled", false);
```

### Default Value:

True (Enabled).

## 6.6 (L1) Disable Pocket (Manual)

### Profile Applicability:

- Level 1

### Description:

Previously known as "Read It Later", Pocket is a social bookmark service that allows users to save a variety of content to one place and access it later from any device. This content includes web pages, blogs, videos, and news sources.

### Rationale:

When using Pocket, users agree to let Firefox collect information including their browser and device type. In addition, this information along with other information (including some personal information) related to Pocket user accounts may be provided to third parties. Firefox also asks users to provide usernames and passwords for third party sites in order to access articles and information published on them. Firefox states that cookies and other analytics tools are necessary for the Pocket website to function and cannot be switched off.

### Impact:

Data such as web pages, blogs, videos, and news sources will not be shared via Pocket.

### Audit:

Ensure that `extensions.pocket.enabled` is set to `false`:

1. Type `about:config` in the address bar
2. Type `extensions.pocket.enabled` in the filter
3. Ensure the setting is set as prescribed.

## Remediation:

To establish the recommended configuration, set `extensions.pocket.enabled` to `false`:

1. Type `about:config` in the address bar
2. Type `extensions.pocket.enabled` in the filter
3. Configure the setting as prescribed.

OR



1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("extensions.pocket.enabled", false)
```

## Default Value:

True (Enabled).

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>9.4 Restrict Unnecessary or Unauthorized Browser and Email Client Extensions</b> Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.			

## 6.7 (L1) Disable Sending Data (Manual)

### Profile Applicability:

- Level 1

### Description:

Firefox by default sends information about Firefox to Mozilla servers. This data can include, but is not limited to IP address, system specifications, browsing history, bookmarks, and open tabs.

### Rationale:

Sending data to Firefox could lead to sensitive data being exposed.

### Impact:

The browser will not send system information back to Firefox.

### Audit:

Ensure that `app.normandy.enabled` is set to `false`:

1. Type `about:config` in the address bar
2. Type `app.normandy.enabled` in the filter
3. Ensure the setting is set as prescribed.

### Remediation:

To establish the recommended configuration, set `app.normandy.enabled` to `false`:

1. Type `about:config` in the address bar
2. Type `app.normandy.enabled` in the filter
3. Ensure the setting is set as prescribed.

*OR*

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("app.normandy.enabled", false);
```

### Default Value:

True (Enabled).

## 6.8 (L1) Disallow Credential Storage (Automated)

### Profile Applicability:

- Level 1

### Description:

Firefox allows for credentials to be stored in its credential store for certain websites.

### Rationale:

Stored credentials may be harvested by an adversary that gains local privileges equal to or greater than the principal running Firefox, which may increase the scope and impact of a breach. However, preventing Firefox from storing credentials will not prevent such an adversary from harvesting credentials used while compromised.

### Impact:

Credentials will not be stored for websites.

### Audit:

Ensure that `signon.rememberSignons` is set to `false`:

1. Type `about:config` in the address bar
2. Type `signon.rememberSignons` in the filter
3. Ensure the setting is set as prescribed.

### Remediation:

To establish the recommended configuration, set `signon.rememberSignons` to `false`:

1. Type `about:config` in the address bar
2. Type `signon.rememberSignons` in the filter
3. Ensure the setting is set as prescribed.

OR

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("signon.rememberSignons", false);
```

### Default Value:

True (Enabled).

## 6.9 (L1) Do Not Accept Third Party Cookies (Automated)

### Profile Applicability:

- Level 1

### Description:

This setting enables or disables the ability for third-party cookies to be downloaded to the system. Third party cookies are cookies sent by a domain that differs from the domain in the browser's address bar.

### Rationale:

Third party cookies are often used for tracking user browsing behaviors, which has privacy implications. However, preventing third-party cookies does not completely mitigate privacy concerns as several other active tracking mechanisms exist [1].

### Impact:

Blocking third-party cookies may adversely affect the functionality of some sites.

### Audit:

Ensure that `network.cookie.cookieBehavior` is set to 1:

1. Type `about:config` in the address bar
2. Type `network.cookie.cookieBehavior` in the filter
3. Ensure the setting is set as prescribed.

### Remediation:

To establish the recommended configuration, set `network.cookie.cookieBehavior` to 1:

1. Type `about:config` in the address bar
2. Type `network.cookie.cookieBehavior` in the filter
3. Ensure the setting is set as prescribed.

OR

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("network.cookie.cookieBehavior", 1);
```

### Default Value:

5



## References:

1. <https://github.com/samyk/evercookie>

## 6.10 (L1) Enable Enhanced Tracking Protection (Manual)

### Profile Applicability:

- Level 1

### Description:

This setting controls whether Firefox's Enhanced Tracking Protection is enabled. Enhanced Tracking Protection will automatically block known third-party tracking cookies.

### Rationale:

Allowing third-party cookies could potentially allow tracking of your web activities by third-party entities which may expose information that could be used for an attack on the end-user.

### Impact:

Disabling third-party cookies could cause some websites to not function as expected.

### Audit:

Ensure that `browser.contentblocking.category` is set to `true`:

1. Type `about:config` in the address bar
2. Type `browser.contentblocking.category` in the filter
3. Ensure the setting is set as prescribed.

### Remediation:

To establish the recommended configuration, set `browser.contentblocking.category` to `true`:

1. Type `about:config` in the address bar
2. Type `browser.contentblocking.category` in the filter
3. Ensure the setting is set as prescribed.

*OR*

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("browser.contentblocking.category", true);
```

### Default Value:

True (Enabled).

## 6.11 (L1) Enable Tracking Protection (Automated)

### Profile Applicability:

- Level 1

### Description:

These settings configures what is allowed to be tracked by websites to which the browser connects.

### Rationale:

Enabling do not track instructs the browser to send an optional header in HTTP requests made from the app that indicates a preference not to be tracked by websites. This optional header is voluntary in nature, having no method to enforce adherence and providing no guarantee that web sites will honor the preference. However, a large number of websites do honor it so there is privacy benefit in enabling it.

### Audit:

Ensure that the following values are set to `true`:

- `privacy.donottrackheader.enabled`
  - `privacy.trackingprotection.enabled`
  - `privacy.trackingprotection.pbmode`
1. Type `about:config` in the address bar
  2. Type `privacy.donottrackheader.enabled` in the filter
  3. Ensure the setting is set as prescribed.
  4. Type `privacy.trackingprotection.enabled` in the filter
  5. Ensure the setting is set as prescribed.
  6. Type `privacy.trackingprotection.pbmode` in the filter
  7. Ensure the setting is set as prescribed.

## Remediation:

To establish the recommended configuration, set the following values to `true`:

- `privacy.donottrackheader.enabled`
  - `privacy.trackingprotection.enabled`
  - `privacy.trackingprotection.pbmode`
1. Type `about:config` in the address bar
  2. Type `privacy.donottrackheader.enabled` in the filter
  3. Ensure the setting is set as prescribed.
  4. Type `privacy.trackingprotection.enabled` in the filter
  5. Ensure the setting is set as prescribed.
  6. Type `privacy.trackingprotection.pbmode` in the filter
  7. Ensure the setting is set as prescribed.

*OR*

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("privacy.donottrackheader.enabled", true);  
lockPref("privacy.trackingprotection.enabled", true);  
lockPref("privacy.trackingprotection.pbmode", true);
```

## Default Value:

`privacy.donottrackheader.enabled=false`

`privacy.trackingprotection.enabled = false`

`privacy.trackingprotection.pbmode = false`

## Additional Information:

`privacy.trackingprotection.pbmode` is only available on FF43 and up (ESR is at v38). Leaving here because it does no harm and this benchmark is likely to be used by many for standard version.

## 6.12 (L1) Set Delay for Enabling Security Sensitive Dialog Boxes (Automated)

### Profile Applicability:

- Level 1

### Description:

This feature sets the amount of time in milliseconds that elapse before the buttons on security-sensitive dialog boxes are enabled.

### Rationale:

This delay help prevents Firefox users from inadvertently installing malicious software.

### Impact:

Buttons on security-sensitive dialog boxes will be delayed 2000 milliseconds.

### Audit:

Ensure that `security.dialog_enable_delay` is set to 2000:

1. Type `about:config` in the address bar
2. Type `security.dialog_enable_delay` in the filter
3. Ensure the setting is set as prescribed.

### Remediation:

To establish the recommended configuration, set `security.dialog_enable_delay` to 2000:

1. Type `about:config` in the address bar
2. Type `security.dialog_enable_delay` in the filter
3. Ensure the setting is set as prescribed.

*OR*

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("security.dialog_enable_delay", 2000);
```

### Default Value:

1000

**References:**

1. <http://www.squarefree.com/2004/07/01/race-conditions-in-security-dialogs/>

## 6.13 (L1) Disabled Delete Data Upon Shutdown (Manual)

### Profile Applicability:

- Level 1

### Description:

This setting allows for the deletion of user data upon closing the browser.

### Rationale:

Deleting browser data will delete information that may be important for a computer investigation and investigators such as Computer Forensics Analysts may not be able to retrieve pertinent information to the investigation.

### Impact:

None - This is the default behavior.

**Note:** This setting will preserve browsing history that could contain a user's personal browsing history. Please make sure that this setting is in compliance with organizational policies.

### Audit:

Ensure that `Privacy.sanitize.SanitizeOnShutdown` is set to `false`:

1. Type `Privacy.sanitize.SanitizeOnShutdown` in the address bar
2. Type `app.normandy.enabled` in the filter
3. Ensure the setting is set as prescribed.

**Remediation:**

To establish the recommended configuration, set `Privacy.sanitize.SanitizeOnShutdown` to `false`:

1. Type `about:config` in the address bar
2. Type `Privacy.sanitize.SanitizeOnShutdown` in the filter
3. Ensure the setting is set as prescribed.

*OR*

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("Privacy.sanitize.SanitizeOnShutdown", false);
```

**Default Value:**

False (Disabled).



## 7 Extensions and Add-ons

This section contains recommendations related to how Firefox manages extensions and add-ons.

## 7.1 (L1) Disable Auto-Install of Add-ons (Automated)

### Profile Applicability:

- Level 1

### Description:

This configuration will enable or disable the ability for websites to automatically install add-ons without an allow list. If this setting is enabled, a whitelist for add-ons that are approved must be created.

### Rationale:

Add-ons are extensions of the browser that add new functionality to Firefox or change its appearance. These run in a user's session allowing them to manipulate data and the behavior of the way Firefox interacts with other applications and user commands. If malicious add-ons are installed automatically, a user's security could be completely compromised.

### Impact:

Users will not be able to download and install add-ons from websites unless an allow list is created.

### Audit:

Ensure that `xpinstall.whitelist.required` is set to `true`:

1. Type `about:config` in the address bar
2. Type `xpinstall.whitelist.required` in the filter
3. Ensure the setting is set as prescribed.

## Remediation:

To establish the recommended configuration, set `xpinstall.whitelist.required` to `true`:

1. Type `about:config` in the address bar
2. Type `xpinstall.whitelist.required` in the filter
3. Ensure the setting is set as prescribed.

OR





1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("xpinstall.whitelist.required", true);
```

## Default Value:

True

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>9.4 Restrict Unnecessary or Unauthorized Browser and Email Client Extensions</b> Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.			
v7	<b>7.2 Disable Unnecessary or Unauthorized Browser or Email Client Plugins</b> Uninstall or disable any unauthorized browser or email client plugins or add-on applications.			

## 7.2 (L1) Disable Development Tools (Manual)

### Profile Applicability:

- Level 1

### Description:

This setting configures whether or not development tools are available to the user. Firefox Developer Tools is a set of web developer tools built into Firefox that can be used to examine, edit, and debug HTML, CSS, and JavaScript.

### Rationale:

Information needed by an attacker to begin looking for possible vulnerabilities in a web browser includes information about the web browser and plug-ins or modules being used. When debugging or trace information is enabled in a production web browser, information about the web browser, such as web browser type, version, patches installed, plug-ins and modules installed, type of code being used by the hosted application, and any back ends being used for data storage may be displayed. Because this information may be placed in logs and general messages during normal operation of the web browser, an attacker does not have to cause an error condition to gain this information.

### Impact:

Users with creative roles that require development tools will need additional permissions granted based on their role.

### Audit:

Ensure that `devtools.application.enabled` is set to `false`:

1. Type `about:config` in the address bar
2. Type `devtools.application.enabled` in the filter
3. Ensure the setting is set as prescribed.

## Remediation:

To establish the recommended configuration, set `devtools.application.enabled` to `false`:

1. Type `about:config` in the address bar
2. Type `devtools.application.enabled` in the filter
3. Ensure the setting is set as prescribed.

*OR*

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("devtools.application.enabled", false);
```

## 7.3 (L1) Disable Encrypted Media Extensions (Manual)

### Profile Applicability:

- Level 1

### Description:

This setting configures whether encrypted media extensions (EME) are downloaded automatically without user consent. EME is a JavaScript API for playing DRMed video content in HTML.

### Rationale:

Downloading media from the internet without user consent could lead to malicious content being downloaded and deployed to the system.

### Impact:

Users will have to consent to downloading EMEs.

### Audit:

Ensure that `media.eme.enabled` is set to `false`:

1. Type `about:config` in the address bar
2. Type `media.eme.enabled` in the filter
3. Ensure the setting is set as prescribed.

### Remediation:

To establish the recommended configuration, set `media.eme.enabled` to `false`:

1. Type `about:config` in the address bar
2. Type `media.eme.enabled` in the filter
3. Ensure the setting is set as prescribed.

OR

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("media.eme.enabled", false);
```

### Default Value:

True (Enabled).

## 7.4 (L1) Disable Popups Initiated by Plugins (Automated)

### Profile Applicability:

- Level 1

### Description:

This feature controls popups that are initiated by plug-ins.

### Rationale:

Disabling plug-in popups (except from white-listed sites) from being displayed, can guard against attacks that are launched using a pop-up.

### Impact:

Pop-ups will not be displayed.

### Audit:

Ensure that `privacy.popups.disable_from_plugins` is set to 2:

1. Type `about:config` in the address bar
2. Type `privacy.popups.disable_from_plugins` in the filter
3. Ensure the setting is set as prescribed.

### Remediation:

To establish the recommended configuration, set `privacy.popups.disable_from_plugins` to 2:

1. Type `about:config` in the address bar
2. Type `privacy.popups.disable_from_plugins` in the filter
3. Ensure the setting is set as prescribed.

OR





1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("privacy.popups.disable_from_plugins", 2)
```

### Default Value:

3

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>9.4 Restrict Unnecessary or Unauthorized Browser and Email Client Extensions</u> Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.			
v7	<u>7.2 Disable Unnecessary or Unauthorized Browser or Email Client Plugins</u> Uninstall or disable any unauthorized browser or email client plugins or add-on applications.			



## 7.5 (L1) Disabled Recommended Extensions (Manual)

### Profile Applicability:

- Level 1

### Description:

This setting configures if Firefox can send recommendations on extensions based on user data as they navigate the web.

### Rationale:

Enabling recommended extensions could allow data to be transmitted to a third-party, which could lead to sensitive data being exposed.

### Impact:

Recommendations on extensions will not be extended to users.

### Audit:

Ensure that `extensions.htmlaboutaddons.recommendations.enabled` is set to `false`:

1. Type `about:config` in the address bar
2. Type `extensions.htmlaboutaddons.recommendations.enabled` in the filter
3. Ensure the setting is set as prescribed.

### Remediation:

To establish the recommended configuration, set `extensions.htmlaboutaddons.recommendations.enabled` to `false`:

1. Type `about:config` in the address bar
2. Type `extensions.htmlaboutaddons.recommendations.enabled` in the filter
3. Ensure the setting is set as prescribed.

OR



1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("extensions.htmlaboutaddons.recommendations.enabled", false);
```

### Default Value:

True (Enabled).

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>9.4 Restrict Unnecessary or Unauthorized Browser and Email Client Extensions</u> Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.			

## 7.6 (L1) Enable Extension Auto Update (Automated)

### Profile Applicability:

- Level 1

### Description:

This feature configures Firefox to automatically download and install updates as they are made available.

### Rationale:

Security updates ensure that users are safe from known software bugs and vulnerabilities.

### Impact:

None - This is the default behavior.

### Audit:

Ensure that `extensions.update.autoUpdateDefault` is set to `true`:

1. Type `about:config` in the address bar
2. Type `extensions.update.autoUpdateDefault` in the filter
3. Ensure the setting is set as prescribed.

### Remediation:

To establish the recommended configuration, set `extensions.update.autoUpdateDefault` to `true`:

1. Type `about:config` in the address bar
2. Type `extensions.update.autoUpdateDefault` in the filter
3. Ensure the setting is set as prescribed.

OR







1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("extensions.update.autoUpdateDefault", true);
```

### Default Value:

True

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>7.4 <u>Perform Automated Application Patch Management</u></b> Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.			
v7	<b>3.5 <u>Deploy Automated Software Patch Management Tools</u></b> 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.			

## 7.7 (L1) Enable Extension Block List (Automated)

### Profile Applicability:

- Level 1

### Description:

This feature enables Mozilla Firefox to retrieve a list of blocked applications from the server.

### Rationale:

Enabling Mozilla to access the list of blocked applications mitigates the risk of installing a known malicious application.

### Impact:

None - This is the default behavior.

### Audit:

Ensure that `extensions.blocklist.enabled` is set to `true`:

1. Type `about:config` in the address bar
2. Type `extensions.blocklist.enabled` in the filter
3. Ensure the setting is set as prescribed.

### Remediation:

To establish the recommended configuration, set `extensions.blocklist.enabled` to `true`:

1. Type `about:config` in the address bar
2. Type `extensions.blocklist.enabled` in the filter
3. Ensure the setting is set as prescribed.

OR





1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("extensions.blocklist.enabled", true);
```

### Default Value:

True

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>9.4 Restrict Unnecessary or Unauthorized Browser and Email Client Extensions</u> Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.			
v7	<u>7.2 Disable Unnecessary or Unauthorized Browser or Email Client Plugins</u> Uninstall or disable any unauthorized browser or email client plugins or add-on applications.			

## 7.8 (L1) Enable Extension Update (Automated)

### Profile Applicability:

- Level 1

### Description:

This feature configures Firefox to prompt when updates are made available.

### Rationale:

Security updates ensure that users are safe from known software bugs and vulnerabilities.

### Impact:

None - This is the default behavior.

### Audit:

Ensure that `extensions.update.enabled` is set to `true`:

1. Type `about:config` in the address bar
2. Type `extensions.update.enabled` in the filter
3. Ensure the setting is set as prescribed.

### Remediation:

To establish the recommended configuration, set `extensions.update.enabled` to `true`:

1. Type `about:config` in the address bar
2. Type `extensions.update.enabled` in the filter
3. Ensure the setting is set as prescribed.

OR







1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("extensions.update.enabled", true);
```

### Default Value:

True

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>7.4 <u>Perform Automated Application Patch Management</u></b> Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.			
v7	<b>3.5 <u>Deploy Automated Software Patch Management Tools</u></b> 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.			



## 7.9 (L1) Enable Warning for External Protocol Handler (Automated)

### Profile Applicability:

- Level 1

### Description:

This feature configures whether a user is warned before opening an external application for pre-configured protocols where its behavior is undefined.

### Rationale:

Enabling a warning to appear before passing data to an external application mitigates the risk that sensitive information will be made vulnerable to outside threats.

### Impact:

None - This is the default behavior.

### Audit:

Ensure that `network.protocol-handler.warn-external-default` is set to `true`:

1. Type `about:config` in the address bar
2. Type `network.protocol-handler.warn-external-default` in the filter
3. Ensure the setting is set as prescribed.

### Remediation:

To establish the recommended configuration, set `network.protocol-handler.warn-external-default` to `true`:

1. Type `about:config` in the address bar
2. Type `network.protocol-handler.warn-external-default` in the filter
3. Ensure the setting is set as prescribed.

OR

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("network.protocol-handler.warn-external-default", true);
```

### Default Value:

True

## 7.10 (L1) Set Extension Update Interval Time Checks (Automated)

### Profile Applicability:

- Level 1

### Description:

This feature sets the amount of time the system waits between checking for updates.

### Rationale:

Setting a specific amount of time between automatically checking for updates mitigates the risk that a system will left vulnerable to known risks for an extended period of time.

### Impact:

None - This is the default behavior.

### Audit:

Ensure that `extensions.update.interval` is set to 86400:

1. Type `about:config` in the address bar
2. Type `extensions.update.interval` in the filter
3. Ensure the setting is set as prescribed.

**Note:** A value less than 86400 also conforms with this benchmark.

### Remediation:

To establish the recommended configuration, set `extensions.update.interval` to 86400:

1. Type `about:config` in the address bar
2. Type `extensions.update.interval` in the filter
3. Ensure the setting is set as prescribed.

OR

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("extensions.update.interval", 86400);
```

**Note:** Configuring this setting to a value less than 86400 also conforms with this benchmark.

**Default Value:**

86400

## 8 Malware Settings

This section contains recommendations for configuring Firefox's malware-related settings.

## 8.1 (L1) Block Reported Attack Sites (Automated)

### Profile Applicability:

- Level 1

### Description:

This setting can be configured to alert a user if they are visiting a known malicious website.

### Rationale:

Enabling this feature will decrease the probability of a user falling victim to a known malicious web site.

### Impact:

None - This is the default behavior.

### Audit:

Ensure that `browser.safebrowsing.malware.enabled` is set to `true`:

1. Type `about:config` in the address bar
2. Type `browser.safebrowsing.malware.enabled` in the filter
3. Ensure the setting is set as prescribed.

### Remediation:

To establish the recommended configuration, set `browser.safebrowsing.malware.enabled` to `true`:

1. Type `about:config` in the address bar
2. Type `browser.safebrowsing.malware.enabled` in the filter
3. Ensure the setting is set as prescribed.

OR

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("browser.safebrowsing.malware.enabled", true);
```

### Default Value:

True

## 8.2 (L1) Block Reported Web Forgeries (Automated)

### Profile Applicability:

- Level 1

### Description:

This setting can be configured to alert the user if they are visiting a known phishing website.

### Rationale:

Enabling this feature helps mitigate the threat of phishing attacks.

### Impact:

None - This is the default behavior.

### Audit:

Ensure that `browser.safebrowsing.phishing.enabled` is set to `true`:

1. Type `about:config` in the address bar
2. Type `browser.safebrowsing.phishing.enabled` in the filter
3. Ensure the setting is set as prescribed.

### Remediation:

To establish the recommended configuration, set `browser.safebrowsing.phishing.enabled` to `true`:

1. Type `about:config` in the address bar
2. Type `browser.safebrowsing.phishing.enabled` in the filter
3. Ensure the setting is set as prescribed.

OR




1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("browser.safebrowsing.phishing.enabled", true);
```

### Default Value:

True (Enabled).

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>9.2 <u>Use DNS Filtering Services</u></b> Use DNS filtering services on all enterprise assets to block access to known malicious domains.			

## 8.3 (L1) Enable Cryptomining Protection (Manual)

### Profile Applicability:

- Level 1

### Description:

This setting controls whether Firefox's Cryptomining Protection is enabled. Cryptomining Protection will automatically block known crypto mining domains that server crypto mining scripts. Crypto mining scripts utilize a computer's central processing unit (CPU) to invisibly mine cryptocurrency.

### Rationale:

This feature allows Firefox to stop potential malicious content from loading.

### Impact:

Legitimate scrips or content may not load properly.

### Audit:

Ensure that `privacy.trackingprotection.cryptomining.enabled` is set to `true`:

1. Type `about:config` in the address bar
2. Type `privacy.trackingprotection.cryptomining.enabled` in the filter
3. Ensure the setting is set as prescribed.

### Remediation:

To establish the recommended configuration, set `privacy.trackingprotection.cryptomining.enabled` to `true`:

1. Type `about:config` in the address bar
2. Type `privacy.trackingprotection.cryptomining.enabled` in the filter
3. Ensure the setting is set as prescribed.

OR

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("privacy.trackingprotection.cryptomining.enabled", true);
```

### Default Value:




True (Enabled).



## References:

1. <https://blog.mozilla.org/en/privacy-security/block-cryptominers-with-firefox/>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>9.2 Use DNS Filtering Services</b> Use DNS filtering services on all enterprise assets to block access to known malicious domains.			

# Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
<b>1</b>	<b>Configure Locked Preferences</b>		
1.1	(L1) Create local-settings.js file (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.2	(L1) Create mozilla.cfg file (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.3	(L1) Protect Firefox Binaries (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.4	(L1) Set permissions on local-settings.js (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.5	(L1) Set permissions on mozilla.cfg (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>2</b>	<b>Updating Firefox</b>		
2.1	(L1) Enable Automatic Updates (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2	(L1) Set Search Provider Update Behavior (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3	(L1) Set Update Interval Time Checks (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.4	(L1) Set Update Wait Time Prompt (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>3</b>	<b>Network Settings</b>		
3.1	(L1) Disable Network Prefetch (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.2	(L1) Disable NTLM v1 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3	(L1) Disable WebRTC (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.4	(L2) Enable IDN Show Punycode (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.5	(L1) Set File URI Origin Policy (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6	(L1) Validate Proxy Settings (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
<b>4</b>	<b>Encryption Settings</b>		
4.1	(L1) Block Mixed Active Content (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
4.2	(L2) Set OCSP Response Policy (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.3	(L2) Set OCSP Use Policy (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.4	(L1) Set Security TLS Version Maximum (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.5	(L1) Set Security TLS Version Minimum (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.6	(L2) Set SSL Override Behavior (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>5</b>	<b>JavaScript Settings</b>		
5.1	(L1) Block Pop-up Windows (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2	(L1) Disable Closing of Windows via Scripts (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.3	(L1) Disable Displaying JavaScript in History URLs (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.4	(L1) Disable Moving or Resizing of Windows via Scripts (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
5.5	(L1) Disable Raising or Lowering of Windows via Scripts (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
<b>6</b>	<b>Privacy Settings</b>		
6.1	(L2) Configure New Tab Page (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
6.2	(L1) Disabled Browser Sign-ins (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
6.3	(L1) Disable Firefox Shield Studies (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
6.4	(L2) Disable Form Fill Assistance (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
6.5	(L1) Disable Geolocation Services (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.6	(L1) Disable Pocket (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
6.7	(L1) Disable Sending Data (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
6.8	(L1) Disallow Credential Storage (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
6.9	(L1) Do Not Accept Third Party Cookies (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.10	(L1) Enable Enhanced Tracking Protection (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
6.11	(L1) Enable Tracking Protection (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.12	(L1) Set Delay for Enabling Security Sensitive Dialog Boxes (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.13	(L1) Disabled Delete Data Upon Shutdown (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
<b>7</b>	<b>Extensions and Add-ons</b>		
7.1	(L1) Disable Auto-Install of Add-ons (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
7.2	(L1) Disable Development Tools (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
7.3	(L1) Disable Encrypted Media Extensions (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
7.4	(L1) Disable Popups Initiated by Plugins (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
7.5	(L1) Disabled Recommended Extensions (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
7.6	(L1) Enable Extension Auto Update (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
7.7	(L1) Enable Extension Block List (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
7.8	(L1) Enable Extension Update (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
7.9	(L1) Enable Warning for External Protocol Handler (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
7.10	(L1) Set Extension Update Interval Time Checks (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>8</b>	<b>Malware Settings</b>		
8.1	(L1) Block Reported Attack Sites (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
8.2	(L1) Block Reported Web Forgeries (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
8.3	(L1) Enable Cryptomining Protection (Manual)	<input type="checkbox"/>	<input type="checkbox"/>

# Appendix: Change History

Date	Version	Changes for this version
02/06/2023	1.0.0	Initial Public Release