# CIS Mozilla Firefox ESR GPO Benchmark

v1.0.0 - 07-19-2024

# Terms of Use

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

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

# Table of Contents

# Overview

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 ESR Browser. This guide was tested against Mozilla Firefox 115.10 ESR on a Windows 11 Release 23H2 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.

## 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 ESR Browser via Group Policy Objects (GPOs).

## 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 |
|---|---|
| `Stylized Monospace font` | Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented. |
| `Monospace font` | Used for inline code, commands, UI/Menu selections or examples. Text should be interpreted exactly as presented. |
| `<Monospace font in brackets>` | Text set in angle brackets denote a variable requiring substitution for a real value. |
| *Italic font* | Used to reference other relevant settings, CIS Benchmarks and/or Benchmark Communities. Also, used to denote the title of a book, article, or other publication. |
| **Bold font** | Additional information or caveats things like **Notes**, **Warnings**, or **Cautions** (usually just the word itself and the rest of the text normal). |

# 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:

**Editor**
Jennifer Jarose
Matthew Woods

**Contributor**
Haemish Edgerton

# Recommendations

## 1 Mozilla

### 1.1 Firefox

### 1.1.1 Addons

This section contains recommendations for Addons settings.

This Group Policy section is provided by the Group Policy template `Firefox.admx/adml` that is included with Mozilla Firefox templates download.

## *1.1.1.1 (L1) Ensure 'Allow add-on installs from websites' is set to 'Disabled' (Automated)*

**Profile Applicability:**

- Level 1

**Description:**

This policy setting configures the ability for websites to automatically install add-ons without an allow list.

The recommended state for this setting is: `Disabled`.

**Note:** If this setting is enabled, an allow list will be needed for approved add-ons.

**Rationale:**

Add-ons are extensions of the browser that add new functionality to Firefox or change its appearance. These run in a user 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:**

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Mozilla\Firefox\InstallAddonsPermission:Default
```

**Remediation:**

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

```
Computer Configuration\Policies\Administrative
Templates\Mozilla\Firefox\Addons\Allow add-on installs from websites
```

**Note:** This Group Policy path does not exist by default. An additional Group Policy template (`firefox.admx/adml`) is required - it is available to download at this link.

**Default Value:**

Enabled.

**CIS Controls:**

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

### 1.1.2 Authentication

This section contains recommendations for Authentication settings.

This Group Policy section is provided by the Group Policy template `Firefox.admx/adml` that is included with Mozilla Firefox templates download.

## *1.1.2.1 (L1) Ensure 'NTLM' is set to 'Disabled' (Automated)*

**Profile Applicability:**

- Level 1

**Description:**

This policy setting controls the use of NT Lan Manager (NTLM) v1 protocol. This protocol is used for authentication to resources.

The recommended state for this setting is: `Disabled`.

**Rationale:**

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

**Impact:**

None - this is the default behavior.

**Audit:**

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is in effect when the following registry value `does not exist`.

```
HKLM\SOFTWARE\Policies\Mozilla\Firefox\Authentication\NTLM:1
```

**Remediation:**

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

```
Computer Configuration\Policies\Administrative
Templates\Mozilla\Firefox\Authentication\NTLM
```

**Note:** This Group Policy path does not exist by default. An additional Group Policy template (`firefox.admx/adml`) is required - it is available to download at this link.

**Default Value:**

Disabled.

**Additional Information:**

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

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 3.10 Encrypt Sensitive Data in Transit<br>Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH). |  | ● | ● |
| v7 | 16.5 Encrypt Transmittal of Username and Authentication Credentials<br>Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels. |  | ● | ● |

### 1.1.3 Bookmarks

This section is intentionally blank and exists to ensure the structure of the benchmark is consistent.

This Group Policy section is provided by the Group Policy template `Firefox.admx/adml` that is included with Mozilla Firefox templates download.

### 1.1.4 Certificates

This section is intentionally blank and exists to ensure the structure of the benchmark is consistent.

This Group Policy section is provided by the Group Policy template `Firefox.admx/adml` that is included with Mozilla Firefox templates download.

### 1.1.5 Clear data when browser is closed

This section contains recommendations for Clear data when browser is closed settings.

This Group Policy section is provided by the Group Policy template `Firefox.admx/adml` that is included with Mozilla Firefox templates download.

## *1.1.5.1 (L1) Ensure 'Active Logins' is set to 'Disabled' (Automated)*

**Profile Applicability:**

- Level 1

**Description:**

This policy setting allows for the user session to be cleared upon closing the browser.

The recommended state for this setting is: `Disabled`.

**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:**

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Mozilla\Firefox\SanitizeOnShutdown:Sessions
```

**Remediation:**

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

```
Computer Configuration\Policies\Administrative
Templates\Mozilla\Firefox\Clear data when browser is closed\Active Logins
```

**Note:** This Group Policy path does not exist by default. An additional Group Policy template (`firefox.admx/adml`) is required - it is available to download at this link.

**Default Value:**

Disabled.

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 0.0 Explicitly Not Mapped<br>Explicitly Not Mapped | | | |
| v7 | 0.0 Explicitly Not Mapped<br>Explicitly Not Mapped | | | |

## 1.1.5.2 (L1) Ensure 'Browsing History' is set to 'Disabled' (Automated)

**Profile Applicability:**

- Level 1

**Description:**

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

The recommended state for this setting is: `Disabled`.

**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:**

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Mozilla\Firefox\SanitizeOnShutdown:History
```

**Remediation:**

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

```
Computer Configuration\Policies\Administrative
Templates\Mozilla\Firefox\Clear data when browser is closed\Browsing History
```

**Note:** This Group Policy path does not exist by default. An additional Group Policy template (`firefox.admx/adml`) is required - it is available to download at this link.

**Default Value:**

Disabled.

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 0.0 Explicitly Not Mapped<br>Explicitly Not Mapped | | | |
| v7 | 0.0 Explicitly Not Mapped<br>Explicitly Not Mapped | | | |

## *1.1.5.3 (L1) Ensure 'Download History' is set to 'Disabled' (Automated)*

**Profile Applicability:**

- Level 1

**Description:**

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

The recommended state for this setting is: `Disabled`.

**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:**

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Mozilla\Firefox\SanitizeOnShutdown:Downloads
```

**Remediation:**

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

```
Computer Configuration\Policies\Administrative
Templates\Mozilla\Firefox\Clear data when browser is closed\Download History
```

**Note:** This Group Policy path does not exist by default. An additional Group Policy template (`firefox.admx/adml`) is required - it is available to download at this link.

**Default Value:**

Disabled.

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 0.0 Explicitly Not Mapped<br>Explicitly Not Mapped | | | |
| v7 | 0.0 Explicitly Not Mapped<br>Explicitly Not Mapped | | | |

## *1.1.5.4 (L1) Ensure 'Form & Search History' is set to 'Disabled' (Automated)*

**Profile Applicability:**

- Level 1

**Description:**

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

The recommended state for this setting is: `Disabled`.

**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:**

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Mozilla\Firefox\SanitizeOnShutdown:FormData
```

**Remediation:**

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

```
Computer Configuration\Policies\Administrative
Templates\Mozilla\Firefox\Clear data when browser is closed\Form & Search
History
```

**Note:** This Group Policy path does not exist by default. An additional Group Policy template (`firefox.admx/adml`) is required - it is available to download at this link.

**Default Value:**

Disabled.

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 0.0 Explicitly Not Mapped<br>Explicitly Not Mapped | | | |
| v7 | 0.0 Explicitly Not Mapped<br>Explicitly Not Mapped | | | |

## *1.1.5.5 (L1) Ensure 'Locked' is set to 'Enabled' (Automated)*

**Profile Applicability:**

- Level 1

**Description:**

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

The recommended state for this setting is: `Enabled`.

**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:**

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Mozilla\Firefox\SanitizeOnShutdown:Locked
```

**Remediation:**

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

```
Computer Configuration\Policies\Administrative
Templates\Mozilla\Firefox\Clear data when browser is closed\Locked
```

**Note:** This Group Policy path does not exist by default. An additional Group Policy template (`firefox.admx/adml`) is required - it is available to download at this link.

**Default Value:**

Enabled.

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 0.0 Explicitly Not Mapped<br>Explicitly Not Mapped | | | |
| v7 | 0.0 Explicitly Not Mapped<br>Explicitly Not Mapped | | | |

### 1.1.6 Cookies

This section contains recommendations for Cookies settings.

This Group Policy section is provided by the Group Policy template `Firefox.admx/adml` that is included with Mozilla Firefox templates download.

## *1.1.6.1 (L1) Ensure 'Cookie Behavior' is set to 'Enabled: Reject cookies for known trackers and partition third-party cookies' (Automated)*

**Profile Applicability:**

- Level 1

**Description:**

This policy setting configures 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.

The recommended state for this setting is: `Enabled: Reject cookies for known trackers and partition third-party cookies`.

**Rationale:**

Third party cookies are often used for tracking user browsing behaviors, which has privacy implications.

**Impact:**

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

**Audit:**

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_SZ` value of `reject-tracker-and-partition-foreign`.

```
HKLM\SOFTWARE\Policies\Mozilla\Firefox\Cookies:Behavior
```

**Remediation:**

To establish the recommended configuration via GP, set the following UI path to `Enabled: Reject cookies for known trackers and partition third-party cookies`:

```
Computer Configuration\Policies\Administrative
Templates\Mozilla\Firefox\Cookies\Cookie Behavior
```

**Note:** This Group Policy path does not exist by default. An additional Group Policy template (`firefox.admx/adml`) is required - it is available to download at this link.

**Default Value:**

Disabled. (Reject cookies for known trackers)

**References:**

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

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 0.0 Explicitly Not Mapped<br>Explicitly Not Mapped | | | |
| v7 | 0.0 Explicitly Not Mapped<br>Explicitly Not Mapped | | | |

## *1.1.6.2 (L1) Ensure 'Cookie Behavior in private browsing' is set to 'Enabled: Reject cookies for known trackers and partition third-party cookies' (Automated)*

**Profile Applicability:**

- Level 1

**Description:**

This policy setting configures 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.

The recommended state for this setting is: `Enabled: Reject cookies for known trackers and partition third-party cookies`.

**Rationale:**

Third party cookies are often used for tracking user browsing behaviors, which has privacy implications.

**Impact:**

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

**Audit:**

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_SZ` value of `reject-tracker-and-partition-foreign`.

```
HKLM\SOFTWARE\Policies\Mozilla\Firefox\Cookies:BehaviorPrivateBrowsing
```

**Remediation:**

To establish the recommended configuration via GP, set the following UI path to `Enabled: Reject cookies for known trackers and partition third-party cookies`:

```
Computer Configuration\Policies\Administrative
Templates\Mozilla\Firefox\Cookies\Cookie Behavior in private browsing
```

**Note:** This Group Policy path does not exist by default. An additional Group Policy template (`firefox.admx/adml`) is required - it is available to download at this link.

**Default Value:**

Disabled. (Reject cookies for known trackers and partition third-party cookies)

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 0.0 Explicitly Not Mapped<br>Explicitly Not Mapped | | | |
| v7 | 0.0 Explicitly Not Mapped<br>Explicitly Not Mapped | | | |

### 1.1.7 Disabled Ciphers

This section contains recommendations for Disabled Ciphers settings.

This Group Policy section is provided by the Group Policy template `Firefox.admx/adml` that is included with Mozilla Firefox templates download.

## 1.1.7.1 (L1) Ensure 'TLS_RSA_WITH_3DES_EDE_CBC_SHA ' is set to 'Enabled' (Automated)

**Profile Applicability:**

- Level 1

**Description:**

This policy settings controls the use of the TLS_RSA_WITH_3DES_EDE_CBC_SHA cipher suite. Cipher suites are a group of algorithms that help secure network connections.

The recommended state for this setting is: `Enabled`.

**Rationale:**

The Triple Data Encryption Algorithm (TDEA) also known as Triple DES (3DES) was deprecated in 2019 by NIST. 3DES is now considered an insecure cipher suite and should not be used.

**Impact:**

Some legacy software and hardware might be affected by disabling this cipher suite.

**Audit:**

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Mozilla\Firefox\DisabledCiphers:TLS_RSA_WITH_3DES_EDE_
CBC_SHA
```

**Remediation:**

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

```
Computer Configuration\Policies\Administrative
Templates\Mozilla\Firefox\Disabled Ciphers\TLS_RSA_WITH_3DES_EDE_CBC_SHA
```

**Note:** This Group Policy path does not exist by default. An additional Group Policy template (`firefox.admx/adml`) is required - it is available to download at this link.

**Default Value:**

If this setting is left unconfigured and depending on the version of Firefox used, this suite could be enabled or disabled.

**References:**

1. https://nvd.nist.gov/vuln/detail/CVE-2016-2183

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 3.10 Encrypt Sensitive Data in Transit<br>Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH). |  | ● | ● |

## 1.1.8 DNS Over HTTPS

This section is intentionally blank and exists to ensure the structure of the benchmark is consistent.

This Group Policy section is provided by the Group Policy template `Firefox.admx/adml` that is included with Mozilla Firefox templates download.

## 1.1.9 Encrypted Media Extensions

This section contains recommendations for Encrypted Media Extensions settings.

This Group Policy section is provided by the Group Policy template `Firefox.admx/adml` that is included with Mozilla Firefox templates download.

## *1.1.9.1 (L1) Ensure 'Lock Encrypted Media Extensions' is set to 'Enabled' (Automated)*

**Profile Applicability:**

- Level 1

**Description:**

This policy 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.

The recommended state for this setting is: `Enabled`.

**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:**

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Mozilla\Firefox\EncryptedMediaExtensions:Locked
```

**Remediation:**

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

```
Computer Configuration\Policies\Administrative
Templates\Mozilla\Firefox\Encrypted Media Extensions\Lock Encrypted Media
Extensions
```

**Note:** This Group Policy path does not exist by default. An additional Group Policy template (`firefox.admx/adml`) is required - it is available to download at this link.

**Default Value:**

Disabled.

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 0.0 Explicitly Not Mapped<br>Explicitly Not Mapped | | | |
| v7 | 0.0 Explicitly Not Mapped<br>Explicitly Not Mapped | | | |

### 1.1.10 Extensions

This section contains recommendations for Extensions settings.

This Group Policy section is provided by the Group Policy template `Firefox.admx/adml` that is included with Mozilla Firefox templates download.

## *1.1.10.1 (L1) Ensure 'Extension Update' is set to 'Enabled' (Automated)*

**Profile Applicability:**

- Level 1

**Description:**

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

The recommended state for this setting is: `Enabled`.

**Rationale:**

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

**Impact:**

None - this is the default behavior.

**Audit:**

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Mozilla\Firefox:ExtensionUpdate
```

**Remediation:**

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

```
Computer Configuration\Policies\Administrative
Templates\Mozilla\Firefox\Extensions\Extension Update
```

**Note:** This Group Policy path does not exist by default. An additional Group Policy template (`firefox.admx/adml`) is required - it is available to download at this link.

**Default Value:**

Enabled.

**CIS Controls:**

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

### 1.1.11 Firefox Suggest (US only)

This section is intentionally blank and exists to ensure the structure of the benchmark is consistent.

This Group Policy section is provided by the Group Policy template `Firefox.admx/adml` that is included with Mozilla Firefox templates download.

### 1.1.12 Flash

This section contains recommendations for Flash settings.

This Group Policy section is provided by the Group Policy template `Firefox.admx/adml` that is included with Mozilla Firefox templates download.

## *1.1.12.1 (L1) Ensure 'Activate Flash on websites' is set to 'Disabled' (Automated)*

**Profile Applicability:**

- Level 1

**Description:**

This policy setting configures the use of Flash on websites.

The recommended state for this setting is: `Disabled`.

**Rationale:**

Firefox ended support for Adobe Flash at the end of 2020. Unsupported software could lead to an attacker exploiting vulnerabilities that are not patched with updates.

**Impact:**

Adobe Flash will not be available, and some websites might not function properly.

**Audit:**

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Mozilla\Firefox\FlashPlugin:Default
```

**Remediation:**

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

```
Computer Configuration\Policies\Administrative
Templates\Mozilla\Firefox\Flash\Activate Flash on websites
```

**Note:** This Group Policy path does not exist by default. An additional Group Policy template (`firefox.admx/adml`) is required - it is available to download at this link.

**References:**

1. https://support.mozilla.org/en-US/kb/end-support-adobe-flash#:~:text=Adobe%20and%20other%20browsers%20also,to%20re%2Denable%20Flash%20support.

**CIS Controls:**

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

### 1.1.13 Home page

This section is intentionally blank and exists to ensure the structure of the benchmark is consistent.

This Group Policy section is provided by the Group Policy template `Firefox.admx/adml` that is included with Mozilla Firefox templates download.

### 1.1.14 PDF.js

This section is intentionally blank and exists to ensure the structure of the benchmark is consistent.

This Group Policy section is provided by the Group Policy template `Firefox.admx/adml` that is included with Mozilla Firefox templates download.

### 1.1.15 Permissions

This section contains recommendations for Permissions settings.

This Group Policy section is provided by the Group Policy template `Firefox.admx/adml` that is included with Mozilla Firefox templates download.

### 1.1.15.1 Autoplay

This section is intentionally blank and exists to ensure the structure of the benchmark is consistent.

This Group Policy section is provided by the Group Policy template `Firefox.admx/adml` that is included with Mozilla Firefox templates download.

### 1.1.15.2 Camera

This section is intentionally blank and exists to ensure the structure of the benchmark is consistent.

This Group Policy section is provided by the Group Policy template `Firefox.admx/adml` that is included with Mozilla Firefox templates download.

### 1.1.15.3 Location

This section contains recommendations for Locations settings.

This Group Policy section is provided by the Group Policy template `Firefox.admx/adml` that is included with Mozilla Firefox templates download.

## *1.1.15.1.1 (L1) Ensure 'Block new requests asking to access location' is set to 'Enabled' (Automated)*

**Profile Applicability:**

- Level 1

**Description:**

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

The recommended state for this setting is: `Enabled`.

**Rationale:**

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

**Impact:**

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

**Audit:**

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Mozilla\Firefox\Permissions\Location:BlockNewRequests
```

**Remediation:**

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

```
Computer Configuration\Policies\Administrative
Templates\Mozilla\Firefox\Permissions\Location\Block new requests asking to
access location
```

**Note:** This Group Policy path does not exist by default. An additional Group Policy template (`firefox.admx/adml`) is required - it is available to download at this link.

**Default Value:**

Disabled.

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 3.1 Establish and Maintain a Data Management Process<br>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. | ● | ● | ● |

## *1.1.15.1.2 (L1) Ensure 'Do not allow preferences to be changed' is set to 'Enabled' (Automated)*

**Profile Applicability:**

- Level 1

**Description:**

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

The recommended state for this setting is: `Enabled`.

**Rationale:**

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

**Impact:**

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

**Audit:**

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Mozilla\Firefox\Permissions\Location:Locked
```

**Remediation:**

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

```
Computer Configuration\Policies\Administrative
Templates\Mozilla\Firefox\Permissions\Location\Do not allow preferences to be
changed
```

**Note:** This Group Policy path does not exist by default. An additional Group Policy template (`firefox.admx/adml`) is required - it is available to download at this link.

**Default Value:**

Disabled.

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 0.0 Explicitly Not Mapped<br>Explicitly Not Mapped | | | |
| v7 | 0.0 Explicitly Not Mapped<br>Explicitly Not Mapped | | | |

### 1.1.16 Picture-in-Picture

This section is intentionally blank and exists to ensure the structure of the benchmark is consistent.

This Group Policy section is provided by the Group Policy template `Firefox.admx/adml` that is included with Mozilla Firefox templates download.

### 1.1.17 Popups

This section contains recommendations for Popups settings.

This Group Policy section is provided by the Group Policy template `Firefox.admx/adml` that is included with Mozilla Firefox templates download.

## *1.1.17.1 (L1) Ensure 'Block pop-ups from websites' is set to 'Enabled' (Automated)*

**Profile Applicability:**

- Level 1

**Description:**

This policy setting configures the Firefox pop-up blocker.

The recommended state for this setting is: `Enabled`.

**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 could be blocked.

**Audit:**

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Mozilla\Firefox\PopupBlocking:Default
```

**Remediation:**

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

```
Computer Configuration\Policies\Administrative
Templates\Mozilla\Firefox\Popups\Block pop-ups from websites
```

**Note:** This Group Policy path does not exist by default. An additional Group Policy template (`firefox.admx/adml`) is required - it is available to download at this link.

**Default Value:**

Enabled.

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 10.5 Enable Anti-Exploitation Features<br>Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™. |  | ● | ● |
| v7 | 8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies<br>Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables. |  | ● | ● |

## *1.1.17.2 (L1) Ensure 'Do not allow preferences to be changed' is set to 'Enabled' (Automated)*

**Profile Applicability:**

- Level 1

**Description:**

This policy setting configures if the Firefox pop-up blocker settings can be changed by the user.

The recommended state for this setting is: `Enabled`.

**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:**

None - this is the default behavior.

**Audit:**

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Mozilla\Firefox\PopupBlocking:Locked
```

**Remediation:**

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

```
Computer Configuration\Policies\Administrative
Templates\Mozilla\Firefox\Popups\Do not allow preferences to be changed
```

**Note:** This Group Policy path does not exist by default. An additional Group Policy template (`firefox.admx/adml`) is required - it is available to download at this link.

**Default Value:**

Enabled.

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 0.0 Explicitly Not Mapped<br>Explicitly Not Mapped | | | |
| v7 | 0.0 Explicitly Not Mapped<br>Explicitly Not Mapped | | | |

### 1.1.18 Preferences (Deprecated)

This section contains recommendations for Preferences (Deprecated) settings.

This Group Policy section is provided by the Group Policy template `Firefox.admx/adml` that is included with Mozilla Firefox templates download.

## *1.1.18.1 (L1) Ensure 'browser.safebrowsing.malware.enabled' is set to 'Enabled' (Automated)*

**Profile Applicability:**

- Level 1

**Description:**

This policy setting configures the use of alerts to users if they are visiting a known malicious website.

The recommended state for this setting is: `Enabled`.

**Rationale:**

Build-in anti-exploitation features can reduce the risk of a user falling victim to a known malicious web site.

**Impact:**

None - this is the default behavior.

**Audit:**

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Mozilla\Firefox\Preferences:browser.safebrowsing.malwa
re.enabled
```

**Remediation:**

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

```
Computer Configuration\Policies\Administrative
Templates\Mozilla\Firefox\Preferences
(Deprecated)\browser.safebrowsing.malware.enabled
```

**Note:** This Group Policy path does not exist by default. An additional Group Policy template (`firefox.admx/adml`) is required - it is available to download at this link.

**Default Value:**

Enabled.

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 10.5 Enable Anti-Exploitation Features<br>Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™. | | ● | ● |
| v7 | 8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies<br>Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables. | | ● | ● |

## *1.1.18.2 (L1) Ensure 'browser.safebrowsing.phishing.enabled' is set to 'Enabled' (Automated)*

**Profile Applicability:**

- Level 1

**Description:**

This policy setting configures the use of alerts to users if they are visiting a known malicious phishing website.

The recommended state for this setting is: `Enabled`.

**Rationale:**

Build-in anti-exploitation features can reduce the risk of a user falling victim to a known malicious phishing web site.

**Impact:**

None - this is the default behavior.

**Audit:**

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Mozilla\Firefox\Preferences:browser.safebrowsing.phish
ing.enabled
```

**Remediation:**

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

```
Computer Configuration\Policies\Administrative
Templates\Mozilla\Firefox\Preferences
(Deprecated)\browser.safebrowsing.phishing
```

**Note:** This Group Policy path does not exist by default. An additional Group Policy template (`firefox.admx/adml`) is required - it is available to download at this link.

**Default Value:**

Enabled.

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 10.5 Enable Anti-Exploitation Features<br>Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™. |  | ● | ● |
| v7 | 8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies<br>Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables. |  | ● | ● |

## *1.1.18.3 (L1) Ensure 'browser.search.update' is set to 'Enabled' (Automated)*

**Profile Applicability:**

- Level 1

**Description:**

This policy setting configures 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.

The recommended state for this setting is: `Enabled`.

**Rationale:**

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

**Impact:**

None - this is the default behavior.

**Audit:**

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Mozilla\Firefox\Preferences:browser.search.update
```

**Remediation:**

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

```
Computer Configuration\Policies\Administrative
Templates\Mozilla\Firefox\Preferences (Deprecated)\browser.search.update
```

**Note:** This Group Policy path does not exist by default. An additional Group Policy template (`firefox.admx/adml`) is required - it is available to download at this link.

**Default Value:**

Enabled.

**CIS Controls:**

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

## *1.1.18.4 (L1) Ensure 'dom.allow_scripts_to_close_windows' is set to 'Disabled' (Automated)*

**Profile Applicability:**

- Level 1

**Description:**

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

The recommended state for this setting is: `Disabled`.

**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:**

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Mozilla\Firefox\Preferences:dom.allow_scripts_to_close
_windows
```

**Remediation:**

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

```
Computer Configuration\Policies\Administrative
Templates\Mozilla\Firefox\Preferences
(Deprecated)\dom.allow_scripts_to_close_windows
```

**Note:** This Group Policy path does not exist by default. An additional Group Policy template (`firefox.admx/adml`) is required - it is available to download at this link.

**Default Value:**

Disabled.

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 2.7 Allowlist Authorized Scripts<br>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. | | | ● |
| v7 | 7.3 Limit Use of Scripting Languages in Web Browsers and Email Clients<br>Ensure that only authorized scripting languages are able to run in all web browsers and email clients. | | ● | ● |

## *1.1.18.5 (L1) Ensure 'dom.disable_window_flip' is set to 'Enabled' (Automated)*

**Profile Applicability:**

- Level 1

**Description:**

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

The recommended state for this setting is: `Enabled`.

**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:**

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Mozilla\Firefox\Preferences:dom.disable_window_flip
```

**Remediation:**

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

```
Computer Configuration\Policies\Administrative
Templates\Mozilla\Firefox\Preferences (Deprecated)\dom.disable_window_flip
```

**Note:** This Group Policy path does not exist by default. An additional Group Policy template (`firefox.admx/adml`) is required - it is available to download at this link.

**Default Value:**

Enabled.

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 2.7 Allowlist Authorized Scripts<br>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. | | | ● |
| v7 | 7.3 Limit Use of Scripting Languages in Web Browsers and Email Clients<br>Ensure that only authorized scripting languages are able to run in all web browsers and email clients. | | ● | ● |

## 1.1.18.6 (L1) Ensure 'dom.disable_window_move_resize' is set to 'Enabled' (Automated)

**Profile Applicability:**

- Level 1

**Description:**

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

The recommended state for this setting is: `Enabled`.

**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.

**Audit:**

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Mozilla\Firefox\Preferences:dom.disable_window_move_resize
```

**Remediation:**

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

```
Computer Configuration\Policies\Administrative
Templates\Mozilla\Firefox\Preferences
(Deprecated)\dom.disable_window_move_resize
```

**Note:** This Group Policy path does not exist by default. An additional Group Policy template (`firefox.admx/adml`) is required - it is available to download at this link.

**Default Value:**

Disabled.

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 2.7 Allowlist Authorized Scripts<br>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. | | | ● |
| v7 | 7.3 Limit Use of Scripting Languages in Web Browsers and Email Clients<br>Ensure that only authorized scripting languages are able to run in all web browsers and email clients. | | ● | ● |

## 1.1.18.7 (L1) Ensure 'extensions.blocklist.enabled' is set to 'Enabled' (Automated)

**Profile Applicability:**

- Level 1

**Description:**

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

The recommended state for this setting is: `Enabled`.

**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:**

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Mozilla\Firefox\Preferences:extensions.blocklist.enabl
ed
```

**Remediation:**

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

```
Computer Configuration\Policies\Administrative
Templates\Mozilla\Firefox\Preferences
(Deprecated)\extensions.blocklist.enabled
```

**Note:** This Group Policy path does not exist by default. An additional Group Policy template (`firefox.admx/adml`) is required - it is available to download at this link.

**Default Value:**

Enabled.

**CIS Controls:**

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

## *1.1.18.8 (L1) Ensure 'media.peerconnection.enabled' is set to 'Disabled' (Automated)*

**Profile Applicability:**

- Level 1

**Description:**

This policy setting determines whether Web Real Time Communications (WebRTC) is allowed. WebRTC is used for peer-to-peer communication such as file sharing or video calls.

The recommended state for this setting is: `Disabled`.

**Rationale:**

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

**Impact:**

WebRTC will not be accessible to users.

**Audit:**

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Mozilla\Firefox\Preferences:media.peerconnection.enabl
ed
```

**Remediation:**

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

```
Computer Configuration\Policies\Administrative
Templates\Mozilla\Firefox\Preferences
(Deprecated)\media.peerconnection.enabled
```

**Note:** This Group Policy path does not exist by default. An additional Group Policy template (`firefox.admx/adml`) is required - it is available to download at this link.

**Default Value:**

Enabled.

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software<br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |  | ● | ● |
| v7 | 15.6 Disable Peer-to-peer Wireless Network Capabilities on Wireless Clients<br>Disable peer-to-peer (adhoc) wireless network capabilities on wireless clients. |  | ● | ● |

## *1.1.18.9 (L2) Ensure 'network.IDN_show_punycode' is set to 'Enabled' (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.

The recommended state for this setting is: `Enabled`.

**Rationale:**

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

**Impact:**

IDNs will be displayed in Punycode.

**Audit:**

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Mozilla\Firefox\Preferences:network.IDN_show_punycode
```

**Remediation:**

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

```
Computer Configuration\Policies\Administrative
Templates\Mozilla\Firefox\Preferences (Deprecated)\network.IDN_show_punycode
```

**Note:** This Group Policy path does not exist by default. An additional Group Policy template (`firefox.admx/adml`) is required - it is available to download at this link.

**Default Value:**

Disabled.

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 10.5 Enable Anti-Exploitation Features<br>Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™. | | ● | ● |
| v7 | 8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies<br>Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables. | | ● | ● |

## *1.1.18.10 (L1) Ensure 'security.mixed_content.block_active_content' is set to 'Enabled' (Automated)*

**Profile Applicability:**

- Level 1

**Description:**

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

The recommended state for this setting is: `Enabled`.

**Rationale:**

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

**Impact:**

None - this is the default behavior.

**Audit:**

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Mozilla\Firefox\Preferences:security.mixed_content.blo
ck_active_content
```

**Remediation:**

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

```
Computer Configuration\Policies\Administrative
Templates\Mozilla\Firefox\Preferences
(Deprecated)\security.mixed_content.block_active_content
```

**Note:** This Group Policy path does not exist by default. An additional Group Policy template (`firefox.admx/adml`) is required - it is available to download at this link.

**Default Value:**

Enabled.

**CIS Controls:**

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

### 1.1.19 Proxy Settings

This section contains recommendations for Proxy Settings settings.

This Group Policy section is provided by the Group Policy template `Firefox.admx/adml` that is included with Mozilla Firefox templates download.

## *1.1.19.1 (L1) Ensure 'Connection Type' is set to 'Enabled: No Proxy' (Automated)*

**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.

The recommended state for this setting is: `Enabled: No Proxy`.

**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.

**Impact:**

None - this is the default behavior.

**Audit:**

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_SZ` value of `none`.

```
HKLM\SOFTWARE\Policies\Mozilla\Firefox\Proxy:Mode
```

**Remediation:**

To establish the recommended configuration via GP, set the following UI path to `Enabled: No Proxy`:

```
Computer Configuration\Policies\Administrative
Templates\Mozilla\Firefox\Proxy Settings\Connection Type
```

**Note:** This Group Policy path does not exist by default. An additional Group Policy template (`firefox.admx/adml`) is required - it is available to download at this link.

**Default Value:**

Disabled.

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software<br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |  | ● | ● |

## *1.1.19.2 (L1) Ensure 'Do not allow proxy settings to be changed' is set to 'Enabled' (Automated)*

**Profile Applicability:**

- Level 1

**Description:**

This policy setting configures whether users can change proxy settings.

The recommended state for this setting is: `Enabled`.

**Rationale:**

Proxy settings should be controlled by Administrators and set at the Company level.

**Impact:**

None - this is the default behavior.

**Audit:**

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Mozilla\Firefox\EnableTrackingProtection:Locked
```

**Remediation:**

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

```
Computer Configuration\Policies\Administrative
Templates\Mozilla\Firefox\Proxy Settings\Do not allow proxy settings to be
changed
```

**Note:** This Group Policy path does not exist by default. An additional Group Policy template (`firefox.admx/adml`) is required - it is available to download at this link.

**Default Value:**

Enabled.

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 0.0 Explicitly Not Mapped<br>Explicitly Not Mapped | | | |
| v7 | 0.0 Explicitly Not Mapped<br>Explicitly Not Mapped | | | |

### 1.1.20 Search

This section contains recommendations for Search settings.

This Group Policy section is provided by the Group Policy template `Firefox.admx/adml` that is included with Mozilla Firefox templates download.

## *1.1.20.1 (L2) Ensure 'Search Suggestions' is set to 'Disabled' (Automated)*

**Profile Applicability:**

- Level 2

**Description:**

This policy setting determines whether web search suggestions are used in Firefox.

The recommended state for this setting is: `Disabled`.

**Rationale:**

Characters that are typed by the user are sent to a search engine before the Enter key is pressed therefore, it is possible for unintended data to be sent.

**Impact:**

Users will not get customized web suggestions for search results; they will still receive local suggestions.

**Audit:**

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Mozilla\Firefox:SearchSuggestEnabled
```

**Remediation:**

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

```
Computer Configuration\Policies\Administrative
Templates\Mozilla\Firefox\Search\Search Suggestions
```

**Note:** This Group Policy path does not exist by default. An additional Group Policy template (`firefox.admx/adml`) is required - it is available to download at this link.

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software<br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. | | ● | ● |
| v7 | 9.2 Ensure Only Approved Ports, Protocols and Services Are Running<br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system. | | ● | ● |

### 1.1.21 Security Devices

This section is intentionally blank and exists to ensure the structure of the benchmark is consistent.

This Group Policy section is provided by the Group Policy template `Firefox.admx/adml` that is included with Mozilla Firefox templates download.

### 1.1.22 Tracking Protection

This section contains recommendations for Tracking Protection settings.

This Group Policy section is provided by the Group Policy template `Firefox.admx/adml` that is included with Mozilla Firefox templates download.

## *1.1.22.1 (L1) Ensure 'Cryptomining' is set to 'Enabled' (Automated)*

**Profile Applicability:**

- Level 1

**Description:**

This policy setting configures Firefox's Cryptomining Protection. Cryptomining Protection will automatically block known crypto mining domains that distribute crypto mining scripts.

The recommended state for this setting is: `Enabled`.

**Rationale:**

Crypto mining scripts utilize a computer's central processing unit (CPU) to invisibly mine cryptocurrency. This feature allows Firefox to stop this potential malicious content from loading.

**Impact:**

Legitimate scripts or content may not load properly.

**Audit:**

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Mozilla\Firefox\EnableTrackingProtection:Cryptomining
```

**Remediation:**

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

```
Computer Configuration\Policies\Administrative
Templates\Mozilla\Firefox\Tracking Protection\Cryptomining
```

**Note:** This Group Policy path does not exist by default. An additional Group Policy template (`firefox.admx/adml`) is required - it is available to download at this link.

**Default Value:**

Disabled.

**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 | 9.2 Use DNS Filtering Services<br>Use DNS filtering services on all enterprise assets to block access to known malicious domains. | ● | ● | ● |
| v7 | 7.7 Use of DNS Filtering Services<br>Use DNS filtering services to help block access to known malicious domains. | ● | ● | ● |

## *1.1.22.2 (L1) Ensure 'Do not allow tracking protection preferences to be changed' is set to 'Enabled' (Automated)*

**Profile Applicability:**

- Level 1

**Description:**

This policy setting determines if tracking protection preferences can be changed by the user.

The recommended state for this setting is: `Enabled`.

**Rationale:**

Allowing a user to change tracking preferences could lead to malicious activity on the system.

**Impact:**

Tracking preferences cannot be changed by the user.

**Audit:**

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Mozilla\Firefox\EnableTrackingProtection:Locked
```

**Remediation:**

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

```
Computer Configuration\Policies\Administrative
Templates\Mozilla\Firefox\Tracking Protection\Do not allow tracking
protection preferences to be changed
```

**Note:** This Group Policy path does not exist by default. An additional Group Policy template (`firefox.admx/adml`) is required - it is available to download at this link.

**Default Value:**

Disabled.

**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 | 0.0 Explicitly Not Mapped<br>Explicitly Not Mapped | | | |
| v7 | 0.0 Explicitly Not Mapped<br>Explicitly Not Mapped | | | |

## *1.1.22.3 (L1) Ensure 'Email Tracking' is set to 'Enabled' (Automated)*

**Profile Applicability:**

- Level 1

**Description:**

This policy setting configures Firefox's Enhanced Tracking Protection. Enhanced Tracking Protection will automatically block known third-party tracking cookies.

The recommended state for this setting is: `Enabled`.

**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:**

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Mozilla\Firefox\EnableTrackingProtection:EmailTracking
```

**Remediation:**

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

```
Computer Configuration\Policies\Administrative
Templates\Mozilla\Firefox\Tracking Protection\Email Tracking
```

**Note:** This Group Policy path does not exist by default. An additional Group Policy template (`firefox.admx/adml`) is required - it is available to download at this link.

**Default Value:**

Enabled. (Users can change.)

**CIS Controls:**

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

## *1.1.22.4 (L1) Ensure 'Enabled' is set to 'Enabled' (Automated)*

**Profile Applicability:**

- Level 1

**Description:**

This policy setting configures what is allowed to be tracked by websites from the browser.

The recommended state for this setting is: `Enabled`.

**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.

**Impact:**

None - this is the default behavior.

**Audit:**

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Mozilla\Firefox\EnableTrackingProtection:Value
```

**Remediation:**

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

```
Computer Configuration\Policies\Administrative
Templates\Mozilla\Firefox\Tracking Protection\Enabled
```

**Note:** This Group Policy path does not exist by default. An additional Group Policy template (`firefox.admx/adml`) is required - it is available to download at this link.

**Default Value:**

Enabled. (Users can change.)

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 0.0 Explicitly Not Mapped<br>Explicitly Not Mapped | | | |
| v7 | 0.0 Explicitly Not Mapped<br>Explicitly Not Mapped | | | |

## *1.1.22.5 (L1) Ensure 'Fingerprinting' is set to 'Enabled' (Automated)*

**Profile Applicability:**

- Level 1

**Description:**

This policy setting configures Firefox's Enhanced Tracking Protection. Enhanced Tracking Protection will automatically block known third-party tracking cookies.

The recommended state for this setting is: `Enabled`.

**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:**

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Mozilla\Firefox\EnableTrackingProtection:Fingerprintin
g
```

**Remediation:**

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

```
Computer Configuration\Policies\Administrative
Templates\Mozilla\Firefox\Tracking Protection\Fingerprinting
```

**Note:** This Group Policy path does not exist by default. An additional Group Policy template (`firefox.admx/adml`) is required - it is available to download at this link.

**Default Value:**

Disabled.

**CIS Controls:**

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

### 1.1.23 User Messaging

This section contains recommendations for User Messaging settings.

This Group Policy section is provided by the Group Policy template `Firefox.admx/adml` that is included with Mozilla Firefox templates download.

## *1.1.23.1 (L1) Ensure 'Extension Recommendations' is set to 'Disabled' (Automated)*

**Profile Applicability:**

- Level 1

**Description:**

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

The recommended state for this setting is: `Disabled`.

**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:**

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Mozilla\Firefox\UserMessaging:ExtensionRecommendations
```

**Remediation:**

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

```
Computer Configuration\Policies\Administrative
Templates\Mozilla\Firefox\UserMessaging\Extension Recommendations
```

**Note:** This Group Policy path does not exist by default. An additional Group Policy template (`firefox.admx/adml`) is required - it is available to download at this link.

**Default Value:**

Enabled.

**CIS Controls:**

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

## *1.1.24 (L1) Ensure 'Application Autoupdate' is set to 'Enabled' (Automated)*

**Profile Applicability:**

- Level 1

**Description:**

This policy setting configures whether Firefox automatically downloads and installs updates, as they are made available.

The recommended state for this setting is: `Enabled`.

**Rationale:**

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

**Impact:**

None - this is the default behavior.

**Audit:**

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Mozilla\Firefox:AppAutoUpdate
```

**Remediation:**

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

```
Computer Configuration\Policies\Administrative
Templates\Mozilla\Firefox\Application Autoupdate
```

**Note:** This Group Policy path does not exist by default. An additional Group Policy template (`firefox.admx/adml`) is required - it is available to download at this link.

**Default Value:**

Enabled. (Users can change the value.)

**CIS Controls:**

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

## *1.1.25 (L1) Ensure 'Background updater' is set to 'Enabled' (Automated)*

**Profile Applicability:**

- Level 1

**Description:**

This policy setting configures whether Firefox automatically downloads and installs the updates in the background, even when the application is not running.

The recommended state for this setting is: `Enabled`.

**Rationale:**

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

**Impact:**

None - this is the default behavior.

**Audit:**

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Mozilla\Firefox:BackgroundAppUpdate
```

**Remediation:**

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

```
Computer Configuration\Policies\Administrative
Templates\Mozilla\Firefox\Background updater
```

**Note:** This Group Policy path does not exist by default. An additional Group Policy template (`firefox.admx/adml`) is required - it is available to download at this link.

**Default Value:**

Enabled.

**CIS Controls:**

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

## *1.1.26 (L1) Ensure 'Disable Developer Tools' is set to 'Enabled' (Automated)*

**Profile Applicability:**

- Level 1

**Description:**

This setting configures whether 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.

The recommended state for this setting is: `Enabled`.

**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:**

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Mozilla\Firefox:DisableDeveloperTools
```

**Remediation:**

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

```
Computer Configuration\Policies\Administrative
Templates\Mozilla\Firefox\Disable Developer Tools
```

**Note:** This Group Policy path does not exist by default. An additional Group Policy template (`firefox.admx/adml`) is required - it is available to download at this link.

**Default Value:**

Disabled.

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software<br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |  | ● | ● |

## *1.1.27 (L1) Ensure 'Disable Feedback Commands' is set to 'Enabled' (Automated)*

**Profile Applicability:**

- Level 1

**Description:**

This policy setting configures accessibility to the Submit Feedback and Report Deceptive Site menu items in the help menu.

The recommended state for this setting is: `Enabled`.

**Rationale:**

Users should not be sending feedback to third-party vendors in an enterprise managed environment.

**Impact:**

The Submit Feedback and Report Deceptive Site menu items will not be available from the help menu.

**Audit:**

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Mozilla\Firefox:DisableFeedbackCommands
```

**Remediation:**

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

```
Computer Configuration\Policies\Administrative
Templates\Mozilla\Firefox\Disable Feedback Commands
```

**Note:** This Group Policy path does not exist by default. An additional Group Policy template (`firefox.admx/adml`) is required - it is available to download at this link.

**Default Value:**

Disabled.

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 0.0 Explicitly Not Mapped<br>Explicitly Not Mapped | | | |
| v7 | 0.0 Explicitly Not Mapped<br>Explicitly Not Mapped | | | |

## *1.1.28 (L1) Ensure 'Disable Firefox Accounts' is set to 'Enabled' (Automated)*

**Profile Applicability:**

- Level 1

**Description:**

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

The recommended state for this setting is: `Enabled`.

**Rationale:**

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

**Impact:**

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

**Audit:**

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Mozilla\Firefox:DisableFirefoxAccounts
```

**Remediation:**

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

```
Computer Configuration\Policies\Administrative
Templates\Mozilla\Firefox\Disable Firefox Accounts
```

**Note:** This Group Policy path does not exist by default. An additional Group Policy template (`firefox.admx/adml`) is required - it is available to download at this link.

**Default Value:**

Disabled.

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 3.1 Establish and Maintain a Data Management Process<br>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. | ● | ● | ● |

## 1.1.29 (L1) Ensure 'Disable Firefox Studies' is set to 'Enabled' (Automated)

**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.

The recommended state for this setting is: `Enabled`.

**Rationale:**

If it is decided to opt-in to Shield Studies, Firefox **will** 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 inadvertently lead to sharing sensitive data.

**Impact:**

Data will not be shared with Firefox.

**Audit:**

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Mozilla\Firefox:DisableFirefoxStudies
```

**Remediation:**

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

```
Computer Configuration\Policies\Administrative
Templates\Mozilla\Firefox\Disable Firefox Studies
```

**Note:** This Group Policy path does not exist by default. An additional Group Policy template (`firefox.admx/adml`) is required - it is available to download at this link.

**Default Value:**

Disabled.

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 3.1 Establish and Maintain a Data Management Process<br>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. | ● | ● | ● |

## *1.1.30 (L1) Ensure 'Disable Forget Button' is set to 'Enabled' (Automated)*

**Profile Applicability:**

- Level 1

**Description:**

This policy setting determines whether the Forget button is available. This feature is also known as eCleaner and allows a user to quickly delete browser data from a selected time frame without affecting the rest of the data.

The recommended state for this setting is: `Enabled`.

**Rationale:**

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

**Impact:**

The Forget button will not be available to users.

**Audit:**

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Mozilla\Firefox:DisableForgetButton
```

**Remediation:**

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

```
Computer Configuration\Policies\Administrative
Templates\Mozilla\Firefox\Disable Forget Button
```

**Note:** This Group Policy path does not exist by default. An additional Group Policy template (`firefox.admx/adml`) is required - it is available to download at this link.

**Default Value:**

Disabled.

## 1.1.31 (L2) Ensure 'Disable Form History' is set to 'Enabled' (Automated)

**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.

The recommended state for this setting is: `Enabled`.

**Rationale:**

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

**Impact:**

Prefilled text fields will not be enabled.

**Audit:**

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Mozilla\Firefox:DisableFormHistory
```

**Remediation:**

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

```
Computer Configuration\Policies\Administrative
Templates\Mozilla\Firefox\Disable Form History
```

**Note:** This Group Policy path does not exist by default. An additional Group Policy template (`firefox.admx/adml`) is required - it is available to download at this link.

**Default Value:**

Disabled.

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 3.1 Establish and Maintain a Data Management Process<br>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. | ● | ● | ● |

## *1.1.32 (L1) Ensure 'Disable Pocket' is set to 'Enabled' (Automated)*

**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.

The recommended state for this setting is: `Enabled`.

**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 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:**

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Mozilla\Firefox:DisablePocket
```

**Remediation:**

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

```
Computer Configuration\Policies\Administrative
Templates\Mozilla\Firefox\Disable Pocket
```

**Note:** This Group Policy path does not exist by default. An additional Group Policy template (`firefox.admx/adml`) is required - it is available to download at this link.

**Default Value:**

Disabled.

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software<br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |  | ● | ● |

## *1.1.33 (L1) Ensure 'Disable Private Browsing' is set to 'Enabled' (Automated)*

**Profile Applicability:**

- Level 1

**Description:**

This policy setting determines whether private browsing is allowed.

The recommended state for this setting is: `Enabled`.

**Rationale:**

Disabling Private Browsing for Firefox will ensure that browsing data is logged on the system, which may be important for forensics.

**Impact:**

Users will not be able to initiate the private browsing feature in Firefox.

**Audit:**

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Mozilla\Firefox:DisablePrivateBrowsing
```

**Remediation:**

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

```
Computer Configuration\Policies\Administrative
Templates\Mozilla\Firefox\Disable Private Browsing
```

**Note:** This Group Policy path does not exist by default. An additional Group Policy template (`firefox.admx/adml`) is required - it is available to download at this link.

**Default Value:**

Disabled.

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software<br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |  | ● | ● |
| v7 | 9.2 Ensure Only Approved Ports, Protocols and Services Are Running<br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system. |  | ● | ● |

## *1.1.34 (L1) Ensure 'Disable System Addon Updates' is set to 'Disabled' (Automated)*

**Profile Applicability:**

- Level 1

**Description:**

This policy setting configures the ability for Firefox to automatically download and install updates for Addons.

The recommended state for this setting is: `Disabled`.

**Rationale:**

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

**Impact:**

None - this is the default behavior.

**Audit:**

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Mozilla\Firefox:DisableSystemAddonUpdate
```

**Remediation:**

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

```
Computer Configuration\Policies\Administrative
Templates\Mozilla\Firefox\Disable System Addon Updates
```

**Note:** This Group Policy path does not exist by default. An additional Group Policy template (`firefox.admx/adml`) is required - it is available to download at this link.

**Default Value:**

Disabled.

**CIS Controls:**

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

## *1.1.35 (L1) Ensure 'Disable Telemetry' is set to 'Enabled' (Automated)*

**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.

The recommended state for this setting is: `Enabled`.

**Rationale:**

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

**Impact:**

The browser will not send system information back to Firefox.

**Audit:**

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Mozilla\Firefox:DisableTelemetry
```

**Remediation:**

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

```
Computer Configuration\Policies\Administrative
Templates\Mozilla\Firefox\Disable Telemetry
```

**Note:** This Group Policy path does not exist by default. An additional Group Policy template (`firefox.admx/adml`) is required - it is available to download at this link.

**Default Value:**

Disabled.

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software<br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |  | ● | ● |

## *1.1.36 (L1) Ensure 'Disable Update' is set to 'Disabled' (Automated)*

**Profile Applicability:**

- Level 1

**Description:**

This policy setting configures if the Firefox browser can receive updates.

The recommended state for this setting is: `Disabled`.

**Rationale:**

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

**Impact:**

None - this is the default behavior.

**Audit:**

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Mozilla\Firefox:DisableAppUpdate
```

**Remediation:**

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

```
Computer Configuration\Policies\Administrative
Templates\Mozilla\Firefox\Disable Update
```

**Note:** This Group Policy path does not exist by default. An additional Group Policy template (`firefox.admx/adml`) is required - it is available to download at this link.

**Default Value:**

Disabled.

**CIS Controls:**

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

## *1.1.37 (L1) Ensure 'Maximum SSL version enabled' is set to 'Enabled: TLS 1.3' (Automated)*

**Profile Applicability:**

- Level 1

**Description:**

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

The recommended state for this setting is: `Enabled:TLS 1.3`.

**Rationale:**

Setting TLS 1.3 as the maximum authorized protocol version mitigates the risk of using an insecure connection.

**Audit:**

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_SZ` value of `tls1.3`.

```
HKLM\SOFTWARE\Policies\Mozilla\Firefox:SSLVersionMax
```

**Remediation:**

To establish the recommended configuration via GP, set the following UI path to `Enabled:TLS 1.3`:

```
Computer Configuration\Policies\Administrative
Templates\Mozilla\Firefox\Maximum SSL version enabled
```

**Note:** This Group Policy path does not exist by default. An additional Group Policy template (`firefox.admx/adml`) is required - it is available to download at this link.

**Default Value:**

TLS 1.3.

**CIS Controls:**

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

## *1.1.38 (L1) Ensure 'Minimum SSL version enabled' is set to 'Enabled: TLS 1.2' (Automated)*

**Profile Applicability:**

- Level 1

**Description:**

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

The recommended state for this setting is: `Enabled:TLS 1.2`.

**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:**

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_SZ` value of `tls1.2`.

```
HKLM\SOFTWARE\Policies\Mozilla\Firefox:SSLVersionMin
```

**Remediation:**

To establish the recommended configuration via GP, set the following UI path to `Enabled:TLS 1.2`:

```
Computer Configuration\Policies\Administrative
Templates\Mozilla\Firefox\Minimum SSL version enabled
```

**Note:** This Group Policy path does not exist by default. An additional Group Policy template (`firefox.admx/adml`) is required - it is available to download at this link.

**Default Value:**

TLS 1.2.

**CIS Controls:**

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

## *1.1.39 (L1) Ensure 'Network Prediction' is set to 'Disabled' (Automated)*

**Profile Applicability:**

- Level 1

**Description:**

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

The recommended state for this setting is: `Disabled`.

**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:**

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Mozilla\Firefox:NetworkPrediction
```

**Remediation:**

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

```
Computer Configuration\Policies\Administrative
Templates\Mozilla\Firefox\Network Prediction
```

**Note:** This Group Policy path does not exist by default. An additional Group Policy template (`firefox.admx/adml`) is required - it is available to download at this link.

**Default Value:**

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 | 9.3 Maintain and Enforce Network-Based URL Filters<br>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. |  | ● | ● |
| v7 | 7.4 Maintain and Enforce Network-Based URL Filters<br>Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not. |  | ● | ● |

## *1.1.40 (L2) Ensure 'New Tab Page' is set to 'Disabled' (Automated)*

**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.

The recommended state for this setting is: `Disabled`.

**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:**

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Mozilla\Firefox:NewTabPage
```

**Remediation:**

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

```
Computer Configuration\Policies\Administrative Templates\Mozilla\Firefox\New
Tab Page
```

**Note:** This Group Policy path does not exist by default. An additional Group Policy template (`firefox.admx/adml`) is required - it is available to download at this link.

**Default Value:**

Enabled.

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 3.1 Establish and Maintain a Data Management Process<br>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. | ● | ● | ● |

## *1.1.41 (L1) Ensure 'Offer to save logins' is set to 'Disabled' (Automated)*

**Profile Applicability:**

- Level 1

**Description:**

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

The recommended state for this setting is: `Disabled`.

**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 on websites.

**Audit:**

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Mozilla\Firefox:OfferToSaveLogins
```

**Remediation:**

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

```
Computer Configuration\Policies\Administrative
Templates\Mozilla\Firefox\Offer to save logins
```

**Note:** This Group Policy path does not exist by default. An additional Group Policy template (`firefox.admx/adml`) is required - it is available to download at this link.

**Default Value:**

Enabled.

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 3.1 Establish and Maintain a Data Management Process<br>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. | ● | ● | ● |

## *1.1.42 (L1) Ensure 'Password Manager' is set to 'Disabled' (Automated)*

**Profile Applicability:**

- Level 1

**Description:**

This policy setting enables or disables the ability for users to save their passwords in Mozilla Firefox.

The recommended state for this setting is: `Disabled`.

**Rationale:**

Saving passwords in Firefox could lead to a user’s web passwords being breached if an attacker were to gain access to their web browser, especially in the case of an unattended and unlocked workstation.

**Impact:**

Users will be unable to utilize the Firefox built-in password manager.

**Audit:**

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Mozilla\Firefox:PasswordManagerEnabled
```

**Remediation:**

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

```
Computer Configuration\Policies\Administrative
Templates\Mozilla\Firefox\Password Manager
```

**Note:** This Group Policy path does not exist by default. An additional Group Policy template (`firefox.admx/adml`) is required - it is available to download at this link.

**Default Value:**

Enabled. (Password Manager is available in preferences.)

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software<br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |  | ● | ● |
| v7 | 9.2 Ensure Only Approved Ports, Protocols and Services Are Running<br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system. |  | ● | ● |

# Appendix: Summary Table

| CIS Benchmark Recommendation | | Set Correctly | |
|---|---|---|---|
| | | Yes | No |
| **1** | **Mozilla** | | |
| **1.1** | **Firefox** | | |
| **1.1.1** | **Addons** | | |
| 1.1.1.1 | (L1) Ensure 'Allow add-on installs from websites' is set to 'Disabled' (Automated) | □ | □ |
| **1.1.2** | **Authentication** | | |
| 1.1.2.1 | (L1) Ensure 'NTLM' is set to 'Disabled' (Automated) | □ | □ |
| **1.1.3** | **Bookmarks** | | |
| **1.1.4** | **Certificates** | | |
| **1.1.5** | **Clear data when browser is closed** | | |
| 1.1.5.1 | (L1) Ensure 'Active Logins’ is set to ‘Disabled’ (Automated) | □ | □ |
| 1.1.5.2 | (L1) Ensure 'Browsing History' is set to 'Disabled' (Automated) | □ | □ |
| 1.1.5.3 | (L1) Ensure 'Download History' is set to 'Disabled' (Automated) | □ | □ |
| 1.1.5.4 | (L1) Ensure 'Form & Search History' is set to 'Disabled' (Automated) | □ | □ |
| 1.1.5.5 | (L1) Ensure 'Locked' is set to 'Enabled' (Automated) | □ | □ |
| **1.1.6** | **Cookies** | | |
| 1.1.6.1 | (L1) Ensure 'Cookie Behavior' is set to 'Enabled: Reject cookies for known trackers and partition third-party cookies' (Automated) | □ | □ |

| CIS Benchmark Recommendation | | Set Correctly | |
|---|---|---|---|
| | | Yes | No |
| 1.1.6.2 | (L1) Ensure 'Cookie Behavior in private browsing' is set to 'Enabled: Reject cookies for known trackers and partition third-party cookies' (Automated) | □ | □ |
| **1.1.7** | **Disabled Ciphers** | | |
| 1.1.7.1 | (L1) Ensure 'TLS_RSA_WITH_3DES_EDE_CBC_SHA ' is set to 'Enabled' (Automated) | □ | □ |
| **1.1.8** | **DNS Over HTTPS** | | |
| **1.1.9** | **Encrypted Media Extensions** | | |
| 1.1.9.1 | (L1) Ensure 'Lock Encrypted Media Extensions’ is set to ‘Enabled’ (Automated) | □ | □ |
| **1.1.10** | **Extensions** | | |
| 1.1.10.1 | (L1) Ensure 'Extension Update' is set to 'Enabled' (Automated) | □ | □ |
| **1.1.11** | **Firefox Suggest (US only)** | | |
| **1.1.12** | **Flash** | | |
| 1.1.12.1 | (L1) Ensure 'Activate Flash on websites' is set to 'Disabled' (Automated) | □ | □ |
| **1.1.13** | **Home page** | | |
| **1.1.14** | **PDF.js** | | |
| **1.1.15** | **Permissions** | | |
| **1.1.15.1** | **Autoplay** | | |
| **1.1.15.2** | **Camera** | | |
| **1.1.15.3** | **Location** | | |
| 1.1.15.1.1 | (L1) Ensure 'Block new requests asking to access location' is set to 'Enabled' (Automated) | □ | □ |

| CIS Benchmark Recommendation | | Set Correctly | |
|---|---|---|---|
| | | Yes | No |
| 1.1.15.1.2 | (L1) Ensure 'Do not allow preferences to be changed' is set to 'Enabled' (Automated) | □ | □ |
| **1.1.16** | **Picture-in-Picture** | | |
| **1.1.17** | **Popups** | | |
| 1.1.17.1 | (L1) Ensure 'Block pop-ups from websites' is set to 'Enabled' (Automated) | □ | □ |
| 1.1.17.2 | (L1) Ensure 'Do not allow preferences to be changed' is set to 'Enabled' (Automated) | □ | □ |
| **1.1.18** | **Preferences (Deprecated)** | | |
| 1.1.18.1 | (L1) Ensure 'browser.safebrowsing.malware.enabled' is set to 'Enabled' (Automated) | □ | □ |
| 1.1.18.2 | (L1) Ensure 'browser.safebrowsing.phishing.enabled' is set to 'Enabled' (Automated) | □ | □ |
| 1.1.18.3 | (L1) Ensure 'browser.search.update' is set to 'Enabled' (Automated) | □ | □ |
| 1.1.18.4 | (L1) Ensure 'dom.allow_scripts_to_close_windows' is set to 'Disabled' (Automated) | □ | □ |
| 1.1.18.5 | (L1) Ensure 'dom.disable_window_flip' is set to 'Enabled' (Automated) | □ | □ |
| 1.1.18.6 | (L1) Ensure 'dom.disable_window_move_resize' is set to 'Enabled' (Automated) | □ | □ |
| 1.1.18.7 | (L1) Ensure 'extensions.blocklist.enabled' is set to 'Enabled' (Automated) | □ | □ |
| 1.1.18.8 | (L1) Ensure 'media.peerconnection.enabled' is set to 'Disabled' (Automated) | □ | □ |
| 1.1.18.9 | (L2) Ensure 'network.IDN_show_punycode' is set to 'Enabled' (Automated) | □ | □ |

| CIS Benchmark Recommendation | | Set Correctly | |
|---|---|---|---|
| | | Yes | No |
| 1.1.18.10 | (L1) Ensure 'security.mixed_content.block_active_content' is set to 'Enabled' (Automated) | □ | □ |
| **1.1.19** | **Proxy Settings** | | |
| 1.1.19.1 | (L1) Ensure 'Connection Type' is set to 'Enabled: No Proxy' (Automated) | □ | □ |
| 1.1.19.2 | (L1) Ensure 'Do not allow proxy settings to be changed' is set to 'Enabled' (Automated) | □ | □ |
| **1.1.20** | **Search** | | |
| 1.1.20.1 | (L2) Ensure 'Search Suggestions' is set to 'Disabled' (Automated) | □ | □ |
| **1.1.21** | **Security Devices** | | |
| **1.1.22** | **Tracking Protection** | | |
| 1.1.22.1 | (L1) Ensure 'Cryptomining' is set to 'Enabled' (Automated) | □ | □ |
| 1.1.22.2 | (L1) Ensure 'Do not allow tracking protection preferences to be changed' is set to 'Enabled' (Automated) | □ | □ |
| 1.1.22.3 | (L1) Ensure 'Email Tracking' is set to 'Enabled' (Automated) | □ | □ |
| 1.1.22.4 | (L1) Ensure 'Enabled' is set to 'Enabled' (Automated) | □ | □ |
| 1.1.22.5 | (L1) Ensure 'Fingerprinting' is set to 'Enabled' (Automated) | □ | □ |
| **1.1.23** | **User Messaging** | | |
| 1.1.23.1 | (L1) Ensure 'Extension Recommendations' is set to 'Disabled' (Automated) | □ | □ |
| 1.1.24 | (L1) Ensure 'Application Autoupdate' is set to 'Enabled' (Automated) | □ | □ |

| CIS Benchmark Recommendation | | Set Correctly | |
|---|---|---|---|
| | | Yes | No |
| 1.1.25 | (L1) Ensure 'Background updater' is set to 'Enabled' (Automated) | □ | □ |
| 1.1.26 | (L1) Ensure 'Disable Developer Tools' is set to 'Enabled' (Automated) | □ | □ |
| 1.1.27 | (L1) Ensure 'Disable Feedback Commands' is set to 'Enabled' (Automated) | □ | □ |
| 1.1.28 | (L1) Ensure 'Disable Firefox Accounts' is set to 'Enabled' (Automated) | □ | □ |
| 1.1.29 | (L1) Ensure 'Disable Firefox Studies' is set to 'Enabled' (Automated) | □ | □ |
| 1.1.30 | (L1) Ensure 'Disable Forget Button' is set to 'Enabled' (Automated) | □ | □ |
| 1.1.31 | (L2) Ensure 'Disable Form History' is set to 'Enabled' (Automated) | □ | □ |
| 1.1.32 | (L1) Ensure 'Disable Pocket' is set to 'Enabled' (Automated) | □ | □ |
| 1.1.33 | (L1) Ensure 'Disable Private Browsing' is set to 'Enabled' (Automated) | □ | □ |
| 1.1.34 | (L1) Ensure 'Disable System Addon Updates' is set to 'Disabled' (Automated) | □ | □ |
| 1.1.35 | (L1) Ensure 'Disable Telemetry' is set to 'Enabled' (Automated) | □ | □ |
| 1.1.36 | (L1) Ensure 'Disable Update' is set to 'Disabled' (Automated) | □ | □ |
| 1.1.37 | (L1) Ensure 'Maximum SSL version enabled' is set to 'Enabled: TLS 1.3' (Automated) | □ | □ |
| 1.1.38 | (L1) Ensure 'Minimum SSL version enabled' is set to 'Enabled: TLS 1.2' (Automated) | □ | □ |

| CIS Benchmark Recommendation | | Set Correctly | |
|---|---|---|---|
| | | Yes | No |
| 1.1.39 | (L1) Ensure 'Network Prediction' is set to 'Disabled' (Automated) | □ | □ |
| 1.1.40 | (L2) Ensure 'New Tab Page' is set to 'Disabled' (Automated) | □ | □ |
| 1.1.41 | (L1) Ensure 'Offer to save logins' is set to 'Disabled' (Automated) | □ | □ |
| 1.1.42 | (L1) Ensure 'Password Manager' is set to 'Disabled' (Automated) | □ | □ |

# Appendix: Change History

| Date | Version | Changes for this version |
|---|---|---|
| 07-19-2024 | 1.0.0 | Initial Public Release |