# CIS Mozilla Firefox STIG Benchmark

v1.0.0 - 08-12-2025

# 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/

For information on referencing and/or citing CIS Benchmarks in 3rd party documentation (including using portions of Benchmark Recommendations) please contact CIS Legal (legalnotices@cisecurity.org) and request guidance on copyright usage.

**NOTE**: It is ***NEVER*** acceptable to host a CIS Benchmark in ***ANY*** format (PDF, etc.) on a 3rd party (non-CIS owned) site.

# Table of Contents

# Overview

## Target Technology Details

Mozilla Firefox Secure Technical Implementation Guide (STIG)

Version: 6 Release: 6 Benchmark

Date: 02 Apr 2025

## 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 Mozilla Firefox and are looking to comply with the STIG guidance

# 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 (or rules) for securing a technology or a supporting platform. STIG Benchmark profiles are used to identify which Vulnerability Severity Category Code (CAT) each rule is associated with.

## Description

The Rule Title from the STIG.

## Rationale Statement

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

## Additional Information

References from the STIG Rule if applicable.

## Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **SEVERITY: CAT I**

  Items in this profile exhibit one or more of the following characteristics:

  - are considered to be high severity
  - are intended for environments or use cases where following STIG based security guidance is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

  This profile is intended for servers and workstations.

- **SEVERITY: CAT II**

  Items in this profile exhibit one or more of the following characteristics:

  - are considered to be medium severity
  - are intended for environments or use cases where following STIG based security guidance is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

  This profile is intended for servers and workstations.

- **SEVERITY: CAT III**

  Items in this profile exhibit one or more of the following characteristics:

  - are considered to be low severity
  - are intended for environments or use cases where following STIG based security guidance is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

  This profile is intended for servers and workstations.

# Acknowledgements

The Recommendations in this Benchmark are a representation of the Rules in the unclassified DISA STIG for Mozilla Firefox.

# Recommendations

## 1 STIG RULES

Mozilla Firefox ESR GPO Benchmark

Mozilla Firefox Secure Technical Implementation Guide (STIG)

Version: 6 Release: 6 Benchmark

Date: 02 Apr 2025

CLASSIFICATION unclassified

## *1.1 FFOX-00-000001 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT I

**Description:**

The installed version of Firefox must be supported.

```
GROUP ID: V-251545
RULE ID: SV-251545r961683
```

**Rationale:**

Using versions of an application that are not supported by the vendor is not permitted. Vendors respond to security flaws with updates and patches. These updates are not available for unsupported versions, which can leave the application vulnerable to attack.

**Audit:**

Run Firefox. Click the ellipsis button >> Help >> About Firefox, and view the version number.

If the Firefox version is not a supported version, this is a finding.

**Remediation:**

Upgrade the version of the browser to an approved version by obtaining software from the vendor or other trusted source.

**Additional Information:**

CCI-002605 Install security-relevant software updates within an organization-defined time period of the release of the updates.

- NIST SP 800-53 Revision 4::SI-2 c
- NIST SP 800-53 Revision 5::SI-2 c

## *1.2 FFOX-00-000002 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT I

**Description:**

Firefox must be configured to allow only TLS 1.2 or above.

```
GROUP ID: V-251546
RULE ID: SV-251546r961869
```

**Rationale:**

Use of versions prior to TLS 1.2 are not permitted. SSL 2.0 and SSL 3.0 contain a number of security flaws. These versions must be disabled in compliance with the Network Infrastructure and Secure Remote Computing STIGs.

**Audit:**

Type "about:policies" in the browser window.

If "SSLVersionMin" is not displayed under Policy Name or the Policy Value is not "tls1.2" or "tls1.3", this is a finding.

**Remediation:**

Windows group policy:

1. Open the group policy editor tool with "gpedit.msc".
2. Navigate to Policy Path: Computer Configuration\Administrative Templates\Mozilla\Firefox
    1. Policy Name: Minimum SSL version enabled
    2. Policy State: Enabled
    3. Policy Value: TLS 1.2 (or TLS 1.3)

macOS "plist" file:
Add the following:

```
<key>SSLVersionMin</key>
<string>tls1.2</string>   (or <string>tls1.3</string>)
```

Linux "policies.json" file:

Add the following in the policies section:

```
"SSLVersionMin": "tls1.2"   or ("SSLVersionMin": "tls1.3")
```

**Additional Information:**

CCI-001453 Implement cryptographic mechanisms to protect the integrity of remote access sessions.

- NIST SP 800-53::AC-17 (2)
- NIST SP 800-53A::AC-17 (2).1
- NIST SP 800-53 Revision 4::AC-17 (2)
- NIST SP 800-53 Revision 5::AC-17 (2)

## *1.3 FFOX-00-000003 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

Firefox must be configured to ask which certificate to present to a website when a certificate is required.

```
GROUP ID: V-251547
RULE ID: SV-251547r1067550
```

**Rationale:**

When a website asks for a certificate for user authentication, Firefox must be configured to have the user choose which certificate to present. Websites within DOD require user authentication for access, which increases security for DOD information. Access will be denied to the user if certificate management is not configured.

**Audit:**

Type "about:policies" in the browser address bar.

If "Preferences" is not displayed under Policy Name and the Policy Value does not include "security.default_personal_cert" with a value of "Ask Every Time" and status of "locked", this is a finding.

**Remediation:**

Windows group policy:

1. Open the group policy editor tool with "gpedit.msc".
2. Navigate to Policy Path: Computer Configuration\Administrative Templates\Mozilla\Firefox
3. 
4. Policy Name: Preferences
5. Policy State: Enabled
6. Policy Value:

```
{
  "security.default_personal_cert": {
    "Value": "Ask Every Time",
    "Status": "locked"
  }
}
```

macOS "plist" file:

Add the following:

```
<key>Preferences</key>
<dict>
  <key>security.default_personal_cert</key>
  <dict>
    <key>Value</key>
    <string>Ask Every Time</string>
    <key>Status</key>
    <string>locked</string>
  </dict>
</dict>
```

Linux "policies.json" file:

Add the following in the policies section:

```
"Preferences": {
  "security.default_personal_cert": {
    "Value": "Ask Every Time",
    "Status": "locked"
  }
}
```

**Additional Information:**

CCI-000187 For public key-based authentication, map the authenticated identity to the account of the individual or group.

- NIST SP 800-53::IA-5 (2)
- NIST SP 800-53A::IA-5 (2).1
- NIST SP 800-53 Revision 4::IA-5 (2) (c)
- NIST SP 800-53 Revision 5::IA-5 (2) (a) (2)

## *1.4 FFOX-00-000004 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

Firefox must be configured to not automatically check for updated versions of installed search plugins.

```
GROUP ID: V-251548
RULE ID: SV-251548r1067552
```

**Rationale:**

Updates must be controlled and installed from authorized and trusted servers. This setting overrides a number of other settings that may direct the application to access external URLs.

**Audit:**

Type "about:policies" in the browser address bar.

If "Preferences" is not displayed under Policy Name or the Policy Value does not include "browser.search.update" with a value of "false" and status of "locked", this is a finding.

**Remediation:**

Windows group policy:

1. Open the group policy editor tool with "gpedit.msc".
2. Navigate to Policy Path: Computer Configuration\Administrative Templates\Mozilla\Firefox
    1. Policy Name: Preferences
    2. Policy State: Enabled
    3. Policy Value:

```
{
  "browser.search.update": {
    "Value": false,
    "Status": "locked"
  }
}
```

macOS "plist" file:

Add the following:

```
<key>Preferences</key>
<dict>
  <key>browser.search.update</key>
  <dict>
    <key>Value</key>
    <false/>
    <key>Status</key>
    <string>locked</string>
  </dict>
</dict>
```

Linux "policies.json" file:

Add the following in the policies section:

```
"Preferences": {
  "browser.search.update": {
    "Value": false,
    "Status": "locked"
  }
}
```

**Additional Information:**

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

## *1.5 FFOX-00-000005 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

Firefox must be configured to not automatically update installed add-ons and plugins.

```
GROUP ID: V-251549
RULE ID: SV-251549r960963
```

**Rationale:**

Set this to false to disable checking for updated versions of the Extensions/Themes. Automatic updates from untrusted sites puts the enclave at risk of attack and may override security settings.

**Audit:**

Type "about:policies" in the browser window.

If "ExtensionUpdate" is not displayed under Policy Name or the Policy Value is not "false", this is a finding.

**Remediation:**

Windows group policy:

1. Open the group policy editor tool with "gpedit.msc".
2. Navigate to Policy Path: Computer Configuration\Administrative Templates\Mozilla\Firefox\Extensions
    1. Policy Name: Extension Update
    2. Policy State: Disabled

macOS "plist" file:
Add the following:

```
<key>ExtensionUpdate</key>
<false/>
```

Linux "policies.json" file:

Add the following in the policies section:

```
"ExtensionUpdate": false
```

**Additional Information:**

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

## *1.6 FFOX-00-000006 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

Firefox must be configured to not automatically execute or download MIME types that are not authorized for auto-download.

```
GROUP ID: V-251550
RULE ID: SV-251550r961194
```

**Rationale:**

Some files can be downloaded or execute without user interaction. This setting ensures these files are not downloaded and executed.

**Audit:**

Type "about:preferences" in the browser address bar.

Type "Applications" in the Find bar in the upper-right corner.

Determine if any of the following file extensions are listed: HTA, JSE, JS, MOCHA, SHS, VBE, VBS, SCT, WSC, FDF, XFDF, LSL, LSO, LSS, IQY, RQY, DOS, BAT, PS, EPS, WCH, WCM, WB1, WB3, WCH, WCM, AD.

If the entry exists and the "Action" is "Save File" or "Always Ask", this is not a finding.

If an extension exists and the entry in the Action column is associated with an application that does/can execute the code, this is a finding.

**Remediation:**

Remove any unauthorized extensions from the auto-download list.

**Additional Information:**

CCI-001242 The organization configures malicious code protection mechanisms to perform real-time scans of files from external sources at endpoints as the files are downloaded, opened, or executed in accordance with organizational security policy.

- NIST SP 800-53::SI-3 c
- NIST SP 800-53A::SI-3.1 (vi)
- NIST SP 800-53 Revision 4::SI-3 c 1

## *1.7 FFOX-00-000007 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

Firefox must be configured to disable form fill assistance.

```
GROUP ID: V-251551
RULE ID: SV-251551r960963
```

**Rationale:**

To protect privacy and sensitive data, Firefox provides the ability to configure the program so that data entered into forms is not saved. This mitigates the risk of a website gleaning private information from prefilled information.

**Audit:**

Type "about:policies" in the browser window.

If "DisableFormHistory" is not displayed under Policy Name or the Policy Value is not "true", this is a finding.

**Remediation:**

Windows group policy:

1. Open the group policy editor tool with "gpedit.msc".
2. Navigate to Policy Path: Computer Configuration\Administrative Templates\Mozilla\Firefox
    1. Policy Name: Disable Form History
    2. Policy State: Enabled

macOS "plist" file:
Add the following:

```
<key>DisableFormHistory</key>
<true/>
```

Linux "policies.json" file:

Add the following in the policies section:

```
"DisableFormHistory": true
```

**Additional Information:**

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

## *1.8 FFOX-00-000008 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

Firefox must be configured to not use a password store with or without a master password.

```
GROUP ID: V-251552
RULE ID: SV-251552r960963
```

**Rationale:**

Firefox can be set to store passwords for sites visited by the user. These individual passwords are stored in a file and can be protected by a master password. Autofill of the password can then be enabled when the site is visited. This feature could also be used to autofill the certificate PIN, which could lead to compromise of DoD information.

**Audit:**

Type "about:policies" in the browser window.

If "PasswordManagerEnabled" is not displayed under Policy Name or the Policy Value is not "false", this is a finding.

**Remediation:**

Windows group policy:

1. Open the group policy editor tool with "gpedit.msc".
2. Navigate to Policy Path: Computer Configuration\Administrative Templates\Mozilla\Firefox
    1. Policy Name: PasswordManager
    2. Policy State: Disabled

macOS "plist" file:
Add the following:

```
<key>PasswordManagerEnabled</key>
<false/>
```

Linux "policies.json" file:

Add the following in the policies section:

```
"PasswordManagerEnabled": false
```

**Additional Information:**

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

## *1.9 FFOX-00-000009 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

Firefox must be configured to block pop-up windows.

```
GROUP ID: V-251553
RULE ID: SV-251553r960963
```

**Rationale:**

Pop-up windows may be used to launch an attack within a new browser window with altered settings. This setting blocks pop-up windows created while the page is loading.

**Audit:**

Type "about:policies" in the browser address bar.

If "PopupBlocking" is not displayed under Policy Name or the Policy Value is not "Default" "true", this is a finding.

If "PopupBlocking" is not displayed under Policy Name or the Policy Value is not "Locked" "true", this is a finding.

"PopupBlocking" "Enabled" may be used to specify an allowlist of sites where pop-ups are desired, this is optional.

**Remediation:**

Windows group policy:

1. Open the group policy editor tool with "gpedit.msc".
2. Navigate to Policy Path: Computer Configuration\Administrative Templates\Mozilla\Firefox\Popups
    1. Policy Name: Block pop-ups from websites
    2. Policy State: Enabled
    3. Policy Name: Do not allow preferences to be changed
    4. Policy State: Enabled
    5. Optional:
    6. Policy Name: Allowed Sites
    7. Policy State: Enabled

Click "Show..." and enter a list of websites to be allowlisted.

macOS "plist" file:
Add the following:

```
<key>PopupBlocking</key>
  <dict>
    <key>Allow</key>
    <array>
      <string>http://example.mil</string>
      <string>http://example.gov</string>
    </array>
    <key>Default</key>
    <true/>
    <key>Locked</key>
    <true/>
  </dict>
```

Linux "policies.json" file:

Add the following in the policies section:

```
"PopupBlocking": {
      "Allow": ["http://example.mil/",
                "http://example.gov/"],
      "Default": true,
      "Locked": true}
```

**Additional Information:**

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

## *1.10 FFOX-00-000010 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

Firefox must be configured to prevent JavaScript from moving or resizing windows.

```
GROUP ID: V-251554
RULE ID: SV-251554r1067554
```

**Rationale:**

JavaScript can make changes to the browser's appearance. This activity can help disguise an attack taking place in a minimized background window. Configure the browser setting to prevent scripts on visited websites from moving and resizing browser windows.

**Audit:**

Type "about:policies" in the browser address bar.

If "Preferences" is not displayed under Policy Name or the Policy Value does not include "dom.disable_window_move_resize" with a value of "true" and status of "locked", this is a finding.

**Remediation:**

Windows group policy:

1. Open the group policy editor tool with "gpedit.msc".
2. Navigate to Policy Path: Computer Configuration\Administrative Templates\Mozilla\Firefox
    1. Policy Name: Preferences
    2. Policy State: Enabled
    3. Policy Value:

```
{
  "dom.disable_window_move_resize": {
    "Value": true,
    "Status": "locked"
  }
}
```

macOS "plist" file:

Add the following:

```
<key>Preferences</key>
<dict>
  <key>dom.disable_window_move_resize</key>
  <dict>
    <key>Value</key>
    <true/>
    <key>Status</key>
    <string>locked</string>
  </dict>
</dict>
```

Linux "policies.json" file:

Add the following in the policies section:

```
"Preferences": {
  "dom.disable_window_move_resize": {
    "Value": true,
    "Status": "locked"
  }
}
```

**Additional Information:**

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

## *1.11 FFOX-00-000011 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

Firefox must be configured to prevent JavaScript from raising or lowering windows.

```
GROUP ID: V-251555
RULE ID: SV-251555r1067556
```

**Rationale:**

JavaScript can raise and lower browser windows to cause improper input. Configure the browser setting to prevent scripts on visited websites from raising and lowering browser windows.

**Audit:**

Type "about:policies" in the browser address bar.

If "Preferences" is not displayed under Policy Name or the Policy Value does not include "dom.disable_window_flip" with a value of "true" and status of "locked", this is a finding.

**Remediation:**

Windows group policy:

1. Open the group policy editor tool with "gpedit.msc".
2. Navigate to Policy Path: Computer Configuration\Administrative Templates\Mozilla\Firefox
    1. Policy Name: Preferences
    2. Policy State: Enabled
    3. Policy Value:

```
{
  "dom.disable_window_flip": {
    "Value": true,
    "Status": "locked"
  }
}
```

macOS "plist" file:

Add the following:

```
<key>Preferences</key>
<dict>
  <key>dom.disable_window_flip</key>
  <dict>
    <key>Value</key>
    <true/>
    <key>Status</key>
    <string>locked</string>
  </dict>
</dict>
```

Linux "policies.json" file:

Add the following in the policies section:

```
"Preferences": {
  "dom.disable_window_flip": {
    "Value": true,
    "Status": "locked"
  }
}
```

**Additional Information:**

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

## *1.12 FFOX-00-000013 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

Firefox must be configured to disable the installation of extensions.

```
GROUP ID: V-251557
RULE ID: SV-251557r960963
```

**Rationale:**

A browser extension is a program that has been installed into the browser to add functionality. Where a plug-in interacts only with a web page and usually a third-party external application (e.g., Flash, Adobe Reader), an extension interacts with the browser program itself. Extensions are not embedded in web pages and must be downloaded and installed in order to work. Extensions allow browsers to avoid restrictions that apply to web pages.

For example, an extension can be written to combine data from multiple domains and present it when a certain page is accessed, which can be considered cross-site scripting. If a browser is configured to allow unrestricted use of extensions, plug-ins can be loaded and installed from malicious sources and used on the browser.

**Audit:**

Type "about:policies" in the browser address bar.

If "InstallAddonsPermission" is not displayed under Policy Name or the Policy Value is not "Default" "false", this is a finding.

**Remediation:**

Windows group policy:

1. Open the group policy editor tool with "gpedit.msc".
2. Navigate to Policy Path: Computer Configuration\Administrative Templates\Mozilla\Firefox\Addons
    1. Policy Name: Allow add-on installs from websites
    2. Policy State: Disabled

macOS "plist" file:
Add the following:

```
<key>InstallAddonsPermission</key>
<false/>
```

Linux "policies.json" file:

Add the following in the policies section:

```
"InstallAddonsPermission": {
      "Default": false
}
```

**Additional Information:**

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

## *1.13 FFOX-00-000014 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

Background submission of information to Mozilla must be disabled.

```
GROUP ID: V-251558
RULE ID: SV-251558r960963
```

**Rationale:**

Firefox by default sends information about Firefox to Mozilla servers. There should be no background submission of technical and other information from DoD computers to Mozilla with portions posted publicly.

**Audit:**

Type "about:policies" in the browser window.

If "DisableTelemetry" is not displayed under Policy Name or the Policy Value is not "true", this is a finding.

**Remediation:**

Windows group policy:

1. Open the group policy editor tool with "gpedit.msc".
2. Navigate to Policy Path: Computer Configuration\Administrative Templates\Mozilla\Firefox
    1. Policy Name: Disable Telemetry
    2. Policy State: Enabled

macOS "plist" file:
Add the following:

```
<key>DisableTelemetry</key>
<true/>
```

Linux "policies.json" file:

Add the following in the policies section:

```
"DisableTelemetry": true
```

**Additional Information:**

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

## *1.14 FFOX-00-000015 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT III

**Description:**

Firefox development tools must be disabled.

```
GROUP ID: V-251559
RULE ID: SV-251559r961167
```

**Rationale:**

Information needed by an attacker to begin looking for possible vulnerabilities in a web browser includes any 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.

**Audit:**

Type "about:policies" in the browser window.

If "DisableDeveloperTools" is not displayed under Policy Name or the Policy Value is not "true", this is a finding.

**Remediation:**

Windows group policy:

1. Open the group policy editor tool with "gpedit.msc".
2. Navigate to Policy Path: Computer Configuration\Administrative Templates\Mozilla\Firefox
    1. Policy Name: Disable Developer Tools
    2. Policy State: Enabled

macOS "plist" file:
Add the following:

```
<key>DisableDeveloperTools</key>
<true/>
```

Linux "policies.json" file:

Add the following in the policies section:

```
"DisableDeveloperTools": true
```

**Additional Information:**

CCI-001312 Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited.

- NIST SP 800-53::SI-11 b
- NIST SP 800-53A::SI-11.1 (iii)
- NIST SP 800-53 Revision 4::SI-11 a
- NIST SP 800-53 Revision 5::SI-11 a

## *1.15 FFOX-00-000016 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

Firefox must have the DOD root certificates installed.

```
GROUP ID: V-251560
RULE ID: SV-251560r1067559
```

**Rationale:**

The DOD root certificates will ensure that the trust chain is established for server certificates issued from the DOD Certificate Authority (CA).

**Audit:**

Type "about:preferences#privacy" in the browser window.

Scroll down to the bottom and select "View Certificates...".

In the Certificate Manager window, select the "Authorities" tab.

Scroll through the Certificate Name list to the U.S. Government heading. Look for the entries for DOD Root CA 3, DOD Root CA 4, and DOD Root CA 5.

If there are entries for DOD Root CA 3, DOD Root CA 4, and DOD Root CA 5, select them individually.

Click "View".

Verify the issuer name is "US Government".

If there are no entries for the appropriate DOD root certificates, this is a finding. If other AO-approved certificates are used, this is not a finding. If SIPRNet-specific certificates are used, this is not a finding.

Note: In a Windows environment, use of policy setting "security.enterprise_roots.enabled=true" will point Firefox to the Windows Trusted Root Certification Authority Store. This is not a finding. It can also be set via the policy Certificates >> ImportEnterpriseRoots, which can be verified via "about:policies".

**Remediation:**

Install the DOD root certificates. Other AO-approved certificates may also be used. Certificates designed for SIPRNet may be used as appropriate.

On Windows, import certificates from the operating system by using Certificates >> Import Enterprise Roots (Certificates) via policy or Group Policy Object (GPO).

**Additional Information:**

CCI-000185 For public key-based authentication, validate certificates by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information.

- NIST SP 800-53::IA-5 (2)
- NIST SP 800-53A::IA-5 (2).1
- NIST SP 800-53 Revision 4::IA-5 (2) (a)
- NIST SP 800-53 Revision 5::IA-5 (2) (b) (1)

## *1.16 FFOX-00-000017 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

Firefox must be configured to not delete data upon shutdown.

```
GROUP ID: V-252881
RULE ID: SV-252881r960963
```

**Rationale:**

For diagnostic purposes, data must remain behind when the browser is closed. This is required to meet non-repudiation controls.

**Audit:**

Type "about:policies" in the browser address bar.

If "SanitizeOnShutdown" is not displayed under Policy Name or the Policy Value does not have {"Cache":false,"Cookies":false,"Downloads":false,"FormData":false,"Sessions":false,"History":false,"OfflineApps":false,"SiteSettings":false,"Locked":true}, this is a finding.

**Remediation:**

Windows group policy:

1. Open the group policy editor tool with "gpedit.msc".
2. Navigate to Policy Path: Computer Configuration\Administrative Templates\Mozilla\Firefox\Clear data when browser is closed
    1. Policy Name: Cache, Cookies, Download History, Form & Search History, Browsing History, Active Logins, Site Preferences, Offline Website Data
    2. Policy State: Disabled
    3. Policy Name: Locked
    4. Policy State: Enabled

macOS "plist" file:
Add the following:

```
<key>SanitizeOnShutdown</key>
<dict>
  <key>Cache</key>
  <false/>
  <key>Cookies</key>
  <false/>
  <key>Downloads</key>
  <false/>
  <key>FormData</key>
  <false/>
  <key>History</key>
  <false/>
  <key>Sessions</key>
  <false/>
  <key>SiteSettings</key>
  <false/>
  <key>OfflineApps</key>
  <false/>
  <key>Locked</key>
  <true/>
</dict>
```

Linux "policies.json" file:

Add the following in the policies section:

```
"SanitizeOnShutdown": {
  "Cache": false,
  "Cookies": false,
  "Downloads": false,
  "FormData": false,
  "History": false,
  "Sessions": false,
  "SiteSettings": false,
  "OfflineApps": false,
  "Locked": true
}
```

**Additional Information:**

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

## *1.17 FFOX-00-000018 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

Firefox must prevent the user from quickly deleting data.

```
GROUP ID: V-251562
RULE ID: SV-251562r987660
```

**Rationale:**

There should not be an option for a user to "forget" work they have done. This is required to meet non-repudiation controls.

**Audit:**

Type "about:policies" in the browser address bar.

If "DisableForgetButton" is not displayed under Policy Name or the Policy Value is not "true", this is a finding.

**Remediation:**

Windows group policy:

1. Open the group policy editor tool with "gpedit.msc".
2. Navigate to Policy Path: Computer Configuration\Administrative Templates\Mozilla\Firefox
    1. Policy Name: Disable Forget Button
    2. Policy State: Enabled

macOS "plist" file:
Add the following:

```
<key>DisableForgetButton</key>
<true/>
```

Linux "policies.json" file:

Add the following in the policies section:

```
"DisableForgetButton": true
```

**Additional Information:**

CCI-002355 Enforce access control decisions based on organization-defined security or privacy attributes that do not include the identity of the user or process acting on behalf of the user.

- NIST SP 800-53 Revision 4::AC-24 (2)
- NIST SP 800-53 Revision 5::AC-24 (2)

## *1.18 FFOX-00-000019 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

Firefox private browsing must be disabled.

```
GROUP ID: V-251563
RULE ID: SV-251563r960963
```

**Rationale:**

Private browsing allows the user to browse the internet without recording their browsing history/activity. From a forensics perspective, this is unacceptable. Best practice requires that browser history is retained.

**Audit:**

Type "about:policies" in the browser window.

If "DisablePrivateBrowsing" is not displayed under Policy Name or the Policy Value is not "true", this is a finding.

**Remediation:**

Windows group policy:

1. Open the group policy editor tool with "gpedit.msc".
2. Navigate to Policy Path: Computer Configuration\Administrative Templates\Mozilla\Firefox
    1. Policy Name: Disable Private Browsing
    2. Policy State: Enabled

macOS "plist" file:
Add the following:

```
<key>DisablePrivateBrowsing</key>
<true/>
```

Linux "policies.json" file:

Add the following in the policies section:

```
"DisablePrivateBrowsing": true
```

**Additional Information:**

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

## *1.19 FFOX-00-000020 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

Firefox search suggestions must be disabled.

```
GROUP ID: V-251564
RULE ID: SV-251564r960963
```

**Rationale:**

Search suggestions must be disabled as this could lead to searches being conducted that were never intended to be made.

**Audit:**

Type "about:policies" in the browser window.

If "SearchSuggestEnabled" is not displayed under Policy Name or the Policy Value is not "false", this is a finding.

**Remediation:**

Windows group policy:

1. Open the group policy editor tool with "gpedit.msc".
2. Navigate to Policy Path: Computer Configuration\Administrative Templates\Mozilla\Firefox\Search
    1. Policy Name: Search Suggestions
    2. Policy State: Disabled

macOS "plist" file:
Add the following:

```
<key>SearchSuggestEnabled</key>
<false/>
```

Linux "policies.json" file:

Add the following in the policies section:

```
"SearchSuggestEnabled": false
```

**Additional Information:**

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

## *1.20 FFOX-00-000021 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT III

**Description:**

Firefox autoplay must be disabled.

```
GROUP ID: V-251565
RULE ID: SV-251565r960963
```

**Rationale:**

Autoplay allows the user to control whether videos can play automatically (without user consent) with audio content. The user must be able to select content that is run within the browser window.

**Audit:**

Type "about:policies" in the browser address bar.

If "Permissions" is not displayed under Policy Name or the Policy Value is not "Autoplay" with a value of "Default" and "Block-audio-video", this is a finding.

**Remediation:**

Windows group policy:

1. Open the group policy editor tool with "gpedit.msc".
2. Navigate to Policy Path: Computer Configuration\Administrative Templates\Mozilla\Firefox\Permissions\Autoplay
    1. Policy Name: Default autoplay level
    2. Policy State: Enabled
    3. Policy Value: Block Audio and Video

macOS "plist" file:
Add the following:

```
<key>Permissions</key>
<dict>
  <key>Autoplay</key>
  <dict>
    <string>block-audio-video</string>
  </dict>
</dict>
```

Linux "policies.json" file:

Add the following in the policies section:

```
"Permissions": {
  "Autoplay": {
    "Default": "block-audio-video"
  }
}
```

**Additional Information:**

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

## *1.21 FFOX-00-000022 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

Firefox network prediction must be disabled.

```
GROUP ID: V-251566
RULE ID: SV-251566r960963
```

**Rationale:**

If network prediction is enabled, requests to URLs are made without user consent. The browser should always make a direct DNS request without prefetching occurring.

**Audit:**

Type "about:policies" in the browser window.

If "NetworkPrediction" is not displayed under Policy Name or the Policy Value is not "false", this is a finding.

**Remediation:**

Windows group policy:

1. Open the group policy editor tool with "gpedit.msc".
2. Navigate to Policy Path: Computer Configuration\Administrative Templates\Mozilla\Firefox
    1. Policy Name: Network Prediction
    2. Policy State: Disabled

macOS "plist" file:
Add the following:

```
<key>NetworkPrediction</key>
<false/>
```

Linux "policies.json" file:

Add the following in the policies section:

```
"NetworkPrediction": false
```

**Additional Information:**

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

## *1.22 FFOX-00-000023 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

Firefox fingerprinting protection must be enabled.

```
GROUP ID: V-251567
RULE ID: SV-251567r960963
```

**Rationale:**

The Content Blocking/Tracking Protection feature stops Firefox from loading content from malicious sites. The content might be a script or an image, for example. If a site is on one of the tracker lists that Firefox is set to use, the fingerprinting script (or other tracking script/image) will not be loaded from that site.

Fingerprinting scripts collect information about browser and device configuration, such as operating system, screen resolution, and other settings. By compiling these pieces of data, fingerprinters create a unique profile that can be used to track the user around the web.

**Audit:**

Type "about:policies" in the browser address bar.

If "EnableTrackingProtection" is not displayed under Policy Name or the Policy Value is not "Fingerprinting" with a value of "true", this is a finding.

**Remediation:**

Windows group policy:

1. Open the group policy editor tool with "gpedit.msc".
2. Navigate to Policy Path: Computer Configuration\Administrative Templates\Mozilla\Firefox\Tracking Protection
    1. Policy Name: Fingerprinting
    2. Policy State: Enabled

macOS "plist" file:
Add the following:

```
<key>EnableTrackingProtection</key>
  <dict>
    <key>Fingerprinting</key>
 <true/>
  </dict>
```

Linux "policies.json" file:

Add the following in the policies section:

```
"EnableTrackingProtection": {
  "Fingerprinting": true
}
```

**Additional Information:**

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

## *1.23 FFOX-00-000024 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

Firefox cryptomining protection must be enabled.

```
GROUP ID: V-251568
RULE ID: SV-251568r960963
```

**Rationale:**

The Content Blocking/Tracking Protection feature stops Firefox from loading content from malicious sites. The content might be a script or an image, for example. If a site is on one of the tracker lists that Firefox is set to use, the fingerprinting script (or other tracking script/image) will not be loaded from that site.

Cryptomining scripts use a computer's central processing unit to invisibly mine cryptocurrency.

**Audit:**

Type "about:policies" in the browser address bar.

If "EnableTrackingProtection" is not displayed under Policy Name or the Policy Value is not "Cryptomining" with a value of "true", this is a finding.

**Remediation:**

Windows group policy:

1. Open the group policy editor tool with "gpedit.msc".
2. Navigate to Policy Path: Computer Configuration\Administrative Templates\Mozilla\Firefox\Tracking Protection
    1. Policy Name: Cryptomining
    2. Policy State: Enabled

macOS "plist" file:
Add the following:

```
<key>EnableTrackingProtection</key>
  <dict>
    <key>Cryptomining</key>
 <true/>
  </dict>
```

Linux "policies.json" file:

Add the following in the policies section:

```
"EnableTrackingProtection": {
  "Cryptomining": true
}
```

**Additional Information:**

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

## *1.24 FFOX-00-000025 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

Firefox Enhanced Tracking Protection must be enabled.

```
GROUP ID: V-251569
RULE ID: SV-251569r1067561
```

**Rationale:**

Tracking generally refers to content, cookies, or scripts that can collect browsing data across multiple sites.

It is detrimental for applications to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

Applications are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions).

Examples of nonessential capabilities include but are not limited to advertising software or browser plug-ins that are not related to requirements or provide a wide array of functionality not required for every mission but that cannot be disabled.

**Audit:**

Type "about:policies" in the browser address bar.

If "Preferences" is not displayed under Policy Name or the Policy Value does not include "browser.contentblocking.category" with a value of "strict" and status of "locked", this is a finding.

**Remediation:**

Windows group policy:

1. Open the group policy editor tool with "gpedit.msc".
2. Navigate to Policy Path: Computer Configuration\Administrative Templates\Mozilla\Firefox
    1. Policy Name: Preferences
    2. Policy State: Enabled
    3. Policy Value:

```
{
  "browser.contentblocking.category": {
    "Value": "strict",
    "Status": "locked"
  }
}
```

macOS "plist" file:

Add the following:

```
<key>Preferences</key>
<dict>
  <key>browser.contentblocking.category</key>
  <dict>
    <key>Value</key>
    <string>strict</string>
    <key>Status</key>
    <string>locked</string>
  </dict>
</dict>
```

Linux "policies.json" file:

Add the following in the policies section:

```
"Preferences": {
  "browser.contentblocking.category": {
    "Value": "strict",
    "Status": "locked"
  }
}
```

**Additional Information:**

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

## *1.25 FFOX-00-000026 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

Firefox extension recommendations must be disabled.

```
GROUP ID: V-251570
RULE ID: SV-251570r1067563
```

**Rationale:**

The Recommended Extensions program makes it easier for users to discover extensions that have been reviewed for security, functionality, and user experience. Allowed extensions are to be centrally managed.

**Audit:**

Type "about:policies" in the browser address bar.

If "Preferences" is not displayed under Policy Name and the Policy Value does not include "extensions.htmlaboutaddons.recommendations.enabled" with a value of "false" and status of "locked", this is a finding.

**Remediation:**

Windows group policy:

1. Open the group policy editor tool with "gpedit.msc".
2. Navigate to Policy Path: Computer Configuration\Administrative Templates\Mozilla\Firefox
    1. Policy Name: Preferences
    2. Policy State: Enabled
    3. Policy Value:

```
{
  "extensions.htmlaboutaddons.recommendations.enabled": {
    "Value": false,
    "Status": "locked"
  }
}
```

macOS "plist" file:

Add the following:

```
<key>Preferences</key>
<dict>
  <key>extensions.htmlaboutaddons.recommendations.enabled</key>
  <dict>
    <key>Value</key>
    <false/>
    <key>Status</key>
    <string>locked</string>
  </dict>
</dict>
```

Linux "policies.json" file:

Add the following in the policies section:

```
"Preferences": {
"extensions.htmlaboutaddons.recommendations.enabled": {
"Value": false,
"Status": "locked"
},
```

**Additional Information:**

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

## *1.26 FFOX-00-000027 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

Firefox deprecated ciphers must be disabled.

```
GROUP ID: V-251571
RULE ID: SV-251571r960963
```

**Rationale:**

A weak cipher is defined as an encryption/decryption algorithm that uses a key of insufficient length. Using an insufficient length for a key in an encryption/decryption algorithm opens up the possibility (or probability) that the encryption scheme could be broken.

**Audit:**

Type "about:policies" in the browser address bar.

If "DisabledCiphers" is not displayed under Policy Name or the Policy Value is not "TLS_RSA_WITH_3DES_EDE_CBC_SHA" with a value of "true", this is a finding.

**Remediation:**

Windows group policy:

1. Open the group policy editor tool with "gpedit.msc".
2. Navigate to Policy Path: Computer Configuration\Administrative Templates\Mozilla\Firefox\Disabled Ciphers
    1. Policy Name: TLS_RSA_WITH_3DES_EDE_CBC_SHA
    2. Policy State: Enabled

macOS "plist" file:
Add the following:

```
<key>DisabledCiphers</key>
  <dict>
    <key>TLS_RSA_WITH_3DES_EDE_CBC_SHA</key>
    <true/>
  </dict>
```

Linux "policies.json" file:

Add the following in the policies section:

```
"DisabledCiphers": {
  "TLS_RSA_WITH_3DES_EDE_CBC_SHA": true
}
```

**Additional Information:**

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

## *1.27 FFOX-00-000028 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

Firefox must not recommend extensions as the user is using the browser.

```
GROUP ID: V-251572
RULE ID: SV-251572r960963
```

**Rationale:**

The Recommended Extensions program recommends extensions to users as they surf the web.

The user must not be encouraged to install extensions from the websites they visit. Allowed extensions are to be centrally managed.

**Audit:**

Type "about:policies" in the browser address bar.

If "UserMessaging" is not displayed under Policy Name or the Policy Value is not "ExtensionRecommendations" with a value of "false", this is a finding.

**Remediation:**

Windows group policy:

1. Open the group policy editor tool with "gpedit.msc".
2. Navigate to Policy Path: Computer Configuration\Administrative Templates\Mozilla\Firefox\User Messaging
    1. Policy Name: Extension Recommendations
    2. Policy State: Disabled

macOS "plist" file:
Add the following:

```
<key>UserMessaging</key>
<dict>
  <key>ExtensionRecommendations</key>
  <false/>
</dict>
```

Linux "policies.json" file:

Add the following in the policies section:

```
"UserMessaging": {
  "ExtensionRecommendations": false
}
```

**Additional Information:**

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

## *1.28 FFOX-00-000029 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

The Firefox New Tab page must not show Top Sites, Sponsored Top Sites, Pocket Recommendations, Sponsored Pocket Stories, Searches, Highlights, or Snippets.

```
GROUP ID: V-251573
RULE ID: SV-251573r960963
```

**Rationale:**

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

It is detrimental for applications to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

Applications are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions).

Examples of non-essential capabilities include but are not limited to advertising software or browser plug-ins that are not related to requirements or provide a wide array of functionality not required for every mission but that cannot be disabled.

The new tab page must not actively show user activity.

**Audit:**

Type "about:policies" in the browser address bar.

- If "FirefoxHome" is not displayed under Policy Name or the Policy Value does not have "Search" with a value of "false", this is a finding.
- If "FirefoxHome" is not displayed under Policy Name or the Policy Value does not have "TopSites" with a value of "false", this is a finding.
- If "FirefoxHome" is not displayed under Policy Name or the Policy Value does not have "SponsoredTopSites" with a value of "false", this is a finding.
- If "FirefoxHome" is not displayed under Policy Name or the Policy Value does not have "Pocket" with a value of "false", this is a finding.
- If "FirefoxHome" is not displayed under Policy Name or the Policy Value does not have "SponsoredPocket" with a value of "false", this is a finding.
- If "FirefoxHome" is not displayed under Policy Name or the Policy Value does not have "Highlights" with a value of "false", this is a finding.
- If "FirefoxHome" is not displayed under Policy Name or the Policy Value does not have "Snippets" with a value of "false", this is a finding.
- If "FirefoxHome" is not displayed under Policy Name or the Policy Value does not have "Locked" with a value of "true", this is a finding.

**Remediation:**

Windows group policy:

1. Open the group policy editor tool with "gpedit.msc".
2. Navigate to Policy Path: Computer Configuration\Administrative Templates\Mozilla\Firefox

- Policy Name: Customize Firefox Home
- Policy State: Enabled
- Policy Value: Uncheck "Search"
- Policy Value: Uncheck "Top Sites"
- Policy Value: Uncheck "Sponsored Top Sites"
- Policy Value: Uncheck "Recommended by Pocket"
- Policy Value: Uncheck "Sponsored Pocket Stories"
- Policy Value: Uncheck "Download History"
- Policy Value: Uncheck "Snippets"
- Policy Value: Check "Do not allow settings to be changed"

macOS "plist" file:
Add the following:

```
<key>FirefoxHome</key>
<dict>
<key>Search</key>
  <false/>
<key>TopSites</key>
  <false/>
<key>SponsoredTopSites</key>
  <false/>
<key>Pocket</key>
  <false/>
<key>SponsoredPocket</key>
  <false/>
<key>Highlights</key>
  <false/>
<key>Snippets</key>
  <false/>
<key>Locked</key>
  <true/>
</dict>
```

Linux "policies.json" file:

Add the following in the policies section:

```
"FirefoxHome": {
  "Search": false,
  "TopSites": false,
  "SponsoredTopSites": false,
  "Pocket": false,
  "SponsoredPocket": false,
  "Highlights": false,
  "Snippets": false,
  "locked": true
}
```

**Additional Information:**

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

## *1.29 FFOX-00-000033 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

Firefox must be configured so that DNS over HTTPS is disabled.

```
GROUP ID: V-251577
RULE ID: SV-251577r960963
```

**Rationale:**

DNS over HTTPS has generally not been adopted in the DoD. DNS is tightly controlled.

It is detrimental for applications to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

Applications are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions).

Examples of non-essential capabilities include, but are not limited to, advertising software or browser plug-ins not related to requirements or providing a wide array of functionality not required for every mission, but cannot be disabled.

**Audit:**

Type "about:policies" in the browser address bar.

If "DNSOverHTTPS" is not displayed under Policy Name or the Policy Value does not have "Enabled" with a value of "false", this is a finding.

**Remediation:**

Windows group policy:

1. Open the group policy editor tool with "gpedit.msc".
2. Navigate to Policy Path: Computer Configuration\Administrative Templates\Mozilla\Firefox\DNS Over HTTPS
    1. Policy Name: Enabled
    2. Policy State: Disabled

macOS "plist" file:

```
<key>DNSOverHTTPS</key>
  <dict>
    <key>Enabled</key>
    <false/>
```

Linux "policies.json" file:

Add the following in the policies section:

```
"DNSOverHTTPS": {"Enabled": false}
```

**Additional Information:**

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

## *1.30 FFOX-00-000034 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

Firefox accounts must be disabled.

```
GROUP ID: V-251578
RULE ID: SV-251578r960963
```

**Rationale:**

Disable Firefox Accounts integration (Sync).

It is detrimental for applications to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

Applications are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions).

Examples of non-essential capabilities include but are not limited to advertising software or browser plug-ins that are not related to requirements or provide a wide array of functionality not required for every mission but that cannot be disabled.

**Audit:**

Type "about:policies" in the browser address bar.

If "DisableFirefoxAccounts" is not displayed under Policy Name or the Policy Value is not "true", this is a finding.

**Remediation:**

Windows group policy:

1. Open the group policy editor tool with "gpedit.msc".
2. Navigate to Policy Path: Computer Configuration\Administrative Templates\Mozilla\Firefox
    1. Policy Name: Disable Firefox Accounts
    2. Policy State: Enabled

macOS "plist" file:

```
<key>DisableFirefoxAccounts</key>
  <true/>
```

Linux "policies.json" file:

Add the following in the policies section:

```
"DisableFirefoxAccounts": true
```

**Additional Information:**

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

## *1.31 FFOX-00-000036 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

Firefox feedback reporting must be disabled.

```
GROUP ID: V-251580
RULE ID: SV-251580r960963
```

**Rationale:**

Disable the menus for reporting sites (Submit Feedback, Report Deceptive Site).

It is detrimental for applications to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

Applications are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions).

Examples of non-essential capabilities include but are not limited to advertising software or browser plug-ins that are not related to requirements or provide a wide array of functionality not required for every mission but that cannot be disabled.

**Audit:**

Type "about:policies" in the browser address bar.

If "DisableFeedbackCommands" is not displayed under Policy Name or the Policy Value is not "true", this is a finding.

**Remediation:**

Windows group policy:

1. Open the group policy editor tool with "gpedit.msc".
2. Navigate to Policy Path: Computer Configuration\Administrative Templates\Mozilla\Firefox
    1. Policy Name: Disable Feedback Commands
    2. Policy State: Enabled

macOS "plist" file:

```
<key>DisableFeedbackCommands</key>
  <true/>
```

Linux "policies.json" file:

Add the following in the policies section:

```
"DisableFeedbackCommands": true
```

**Additional Information:**

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

## *1.32 FFOX-00-000037 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

Firefox encrypted media extensions must be disabled.

```
GROUP ID: V-251581
RULE ID: SV-251581r960963
```

**Rationale:**

Enable or disable Encrypted Media Extensions and optionally lock it.

If "Enabled" is set to "false", Firefox does not download encrypted media extensions (such as Widevine) unless the user consents to installing them.

If "Locked" is set to "true" and "Enabled" is set to "false", Firefox will not download encrypted media extensions (such as Widevine) or ask the user to install them.

It is detrimental for applications to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

Applications are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions).

Examples of non-essential capabilities include but are not limited to advertising software or browser plug-ins that are not related to requirements or provide a wide array of functionality not required for every mission but that cannot be disabled.

**Audit:**

Type "about:policies" in the browser address bar.

If "EncryptedMediaExtensions" is not displayed under Policy Name or the Policy Value does not have "Enabled" set to "false" or the Policy Value does not have "Locked" set to "true", this is a finding.

**Remediation:**

Windows group policy:

1. Open the group policy editor tool with "gpedit.msc".
2. Navigate to Policy Path: Computer Configuration\Administrative Templates\Mozilla\Firefox\Encrypted Media Extensions
3. Policy Name: Enable Encrypted Media Extensions
    1. Policy State: Disabled
    2. Policy Name: Lock Encrypted Media Extensions
    3. Policy State: Enabled

macOS "plist" file:

```
<key>EncryptedMediaExtensions</key>
  <dict>
    <key>Enabled</key>
    <false/>
    <key>Locked</key>
    <true/>
```

Linux "policies.json" file:

Add the following in the policies section:

```
"EncryptedMediaExtensions": {
  "Enabled": false,
  "Locked": true
}
```

**Additional Information:**

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

## *1.33 FFOX-00-000038 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

Pocket must be disabled.

```
GROUP ID: V-252908
RULE ID: SV-252908r960963
```

**Rationale:**

Pocket, previously known as Read It Later, is a social bookmarking service for storing, sharing, and discovering web bookmarks. Data gathering cloud services such as this are generally disabled in the DoD.

**Audit:**

Type "about:policies" in the browser address bar.

If "DisablePocket" is not displayed under Policy Name or the Policy Value does not have a value of "true", this is a finding.

**Remediation:**

Windows group policy:

1. Open the group policy editor tool with "gpedit.msc".
2. Navigate to Policy Path: Computer Configuration\Administrative Templates\Mozilla\Firefox
    1. Policy Name: Disable Pocket
    2. Policy State: Enabled

macOS "plist" file:

```
<key>DisablePocket</key>
 <true/>
```

Linux "policies.json" file:

Add the following in the policies section:

```
"DisablePocket": true
```

**Additional Information:**

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

## *1.34 FFOX-00-000039 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

Firefox Studies must be disabled.

```
GROUP ID: V-252909
RULE ID: SV-252909r960963
```

**Rationale:**

Studies try out different features and ideas before they are released to all Firefox users. Testing beta software is not in the DoD user's mission.

**Audit:**

Type "about:policies" in the browser address bar.

If "DisableFirefoxStudies" is not displayed under Policy Name or the Policy Value does not have a value of "true", this is a finding.

**Remediation:**

Windows group policy:

1. Open the group policy editor tool with "gpedit.msc".
2. Navigate to Policy Path: Computer Configuration\Administrative Templates\Mozilla\Firefox
    1. Policy Name: Disable Firefox Studies
    2. Policy State: Enabled

macOS "plist" file:

```
<key>DisableFirefoxStudies</key>
 <true/>
```

Linux "policies.json" file:

Add the following in the policies section:

```
"DisableFirefoxStudies": true
```

**Additional Information:**

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

# Appendix: Summary Table

| CIS Benchmark Recommendation | | Set Correctly | |
|---|---|---|---|
| | | Yes | No |
| **1** | **STIG RULES** | | |
| 1.1 | FFOX-00-000001 (Manual) | ☐ | ☐ |
| 1.2 | FFOX-00-000002 (Manual) | ☐ | ☐ |
| 1.3 | FFOX-00-000003 (Manual) | ☐ | ☐ |
| 1.4 | FFOX-00-000004 (Manual) | ☐ | ☐ |
| 1.5 | FFOX-00-000005 (Manual) | ☐ | ☐ |
| 1.6 | FFOX-00-000006 (Manual) | ☐ | ☐ |
| 1.7 | FFOX-00-000007 (Manual) | ☐ | ☐ |
| 1.8 | FFOX-00-000008 (Manual) | ☐ | ☐ |
| 1.9 | FFOX-00-000009 (Manual) | ☐ | ☐ |
| 1.10 | FFOX-00-000010 (Manual) | ☐ | ☐ |
| 1.11 | FFOX-00-000011 (Manual) | ☐ | ☐ |
| 1.12 | FFOX-00-000013 (Manual) | ☐ | ☐ |
| 1.13 | FFOX-00-000014 (Manual) | ☐ | ☐ |
| 1.14 | FFOX-00-000015 (Manual) | ☐ | ☐ |
| 1.15 | FFOX-00-000016 (Manual) | ☐ | ☐ |
| 1.16 | FFOX-00-000017 (Manual) | ☐ | ☐ |
| 1.17 | FFOX-00-000018 (Manual) | ☐ | ☐ |
| 1.18 | FFOX-00-000019 (Manual) | ☐ | ☐ |
| 1.19 | FFOX-00-000020 (Manual) | ☐ | ☐ |

| CIS Benchmark Recommendation | | Set Correctly | |
|---|---|---|---|
| | | Yes | No |
| 1.20 | FFOX-00-000021 (Manual) | ☐ | ☐ |
| 1.21 | FFOX-00-000022 (Manual) | ☐ | ☐ |
| 1.22 | FFOX-00-000023 (Manual) | ☐ | ☐ |
| 1.23 | FFOX-00-000024 (Manual) | ☐ | ☐ |
| 1.24 | FFOX-00-000025 (Manual) | ☐ | ☐ |
| 1.25 | FFOX-00-000026 (Manual) | ☐ | ☐ |
| 1.26 | FFOX-00-000027 (Manual) | ☐ | ☐ |
| 1.27 | FFOX-00-000028 (Manual) | ☐ | ☐ |
| 1.28 | FFOX-00-000029 (Manual) | ☐ | ☐ |
| 1.29 | FFOX-00-000033 (Manual) | ☐ | ☐ |
| 1.30 | FFOX-00-000034 (Manual) | ☐ | ☐ |
| 1.31 | FFOX-00-000036 (Manual) | ☐ | ☐ |
| 1.32 | FFOX-00-000037 (Manual) | ☐ | ☐ |
| 1.33 | FFOX-00-000038 (Manual) | ☐ | ☐ |
| 1.34 | FFOX-00-000039 (Manual) | ☐ | ☐ |

# Appendix: Change History

| Date | Version | Changes for this version |
| --- | --- | --- |
| 08/12/2025 | v1.0.0 | Initial CIS Release |