CIS Benchmarks

CIS macOS Safari Benchmark

v2.0.0 - 11-28-2017

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

This is the archive of the CIS macOS Safari Benchmark. CIS encourages you to migrate to a more recent, supported version of this technology.

This document, provides prescriptive guidance for establishing a secure configuration posture for Apple Safari 11.0.1 running on macOS Sierra. This benchmark was tested using Safari 11.0.1 on macOS 10.12.6. To obtain the latest version of this guide, please visit http://cisecurity.org. If you have questions, comments, or have identified ways to improve this guide, please write us at support@cisecurity.org.

Intended Audience

This document 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 Apple's Safari Browser.

Consensus Guidance

This benchmark was created using a consensus review process comprised of subject matter experts. 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, or examples. Text should be interpreted exactly as presented.
<italic font in brackets>	Italic texts set in angle brackets denote a variable requiring substitution for a real value.
Italic font	Used to denote the title of a book, article, or other publication.
Note	Additional information or caveats

Scoring Information

A scoring status indicates whether compliance with the given recommendation impacts the assessed target's benchmark score. The following scoring statuses are used in this benchmark:

Scored

Failure to comply with "Scored" recommendations will decrease the final benchmark score. Compliance with "Scored" recommendations will increase the final benchmark score.

Not Scored

Failure to comply with "Not Scored" recommendations will not decrease the final benchmark score. Compliance with "Not Scored" recommendations will not increase the final benchmark score.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1**

  Items in this profile intend to:

  - 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 paramount
  - acts as defense in depth measure
  - may negatively inhibit the utility or performance of the technology

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
Paul Campbell, Anitian
Jordan Rakoske GSEC, GCWN

Recommendations

1 General

This section contains settings under the general tab of the Safari Browser.

1.1 (L1) Ensure 'Open "safe" files after downloading' is 'Disabled' (Scored)

Profile Applicability:

- Level 1

Description:

The Safari browser contains a feature which causes all files considered "safe" to be automatically opened once they have finished downloading.

Rationale:

This feature is meant to be a benefit but having the browser automatically open files that could be malicious and downloaded by mistake is a security risk.

Audit:

Follow the below steps and verify that `Open "safe" files after downloading` is `Disabled`:

1. Click `Safari`.
2. Click `Preferences`.
3. Click `General`.
4. Verify `Open "safe" files after downloading` is `unchecked`.

To verify the plist follow the below steps:

1. Open the `com.apple.Safari.plist`.
2. Find the token `<key>AutoOpenSafeDownloads</key>`
3. verify this token is immediately followed by `<false/>`

Remediation:

Follow the below steps to set `Open "safe" files after downloading` to `Disabled`:

1. Click `Safari`.
2. Click `Preferences`.
3. Click `General`.
4. Uncheck the `Open "safe" files after downloading` checkbox.

To configure the plist follow the below steps:

1. Open the `com.apple.Safari.plist`.
2. Find the token `<key>AutoOpenSafeDownloads</key>`
3. Ensure this token is immediately followed by `<false/>`

Default Value:

Enabled.

CIS Controls:

7 Email and Web Browser Protections
Email and Web Browser Protections

2 Tabs

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

3 AutoFill

This section contains settings under the AutoFill tab of the Safari Browser.

3.1 (L2) Ensure 'AutoFill web forms: User names and passwords' is 'Disabled' (Scored)

Profile Applicability:

- Level 2

Description:

Safari can utilize a user-level keychain for credential storage, and then access that information when revisiting websites on the same domain. By disabling this feature the user will be prompted to manually enter their credentials when they visit a website.

Rationale:

If this setting is enabled, users can have Safari store and retrieve passwords through a user-level keychain and provide them automatically the next time they visit a site. An intruder who has unrestricted access to your computer can gain access to secure site areas.

Audit:

Follow the below steps and verify that `AutoFill web forms: User names and passwords` is `Disabled`:

1. Click `Safari`.
2. Click `Preferences`.
3. Click `AutoFill`.
4. Verify `AutoFill web forms: User names and passwords` is `unchecked`.

To verify the plist follow the below steps:

1. Open the `com.apple.Safari.plist`.
2. Find the token `<key>AutoFillPasswords</key>`
3. verify this token is immediately followed by `<false/>`

Remediation:

Follow the below steps to set `AutoFill web forms: User names and passwords` to `Disabled`:

1. Click `Safari`.
2. Click `Preferences`.
3. Click `AutoFill`.
4. Uncheck `AutoFill web forms: User names and passwords`.

To configure the plist follow the below steps:

1. Open the `com.apple.Safari.plist`.
2. Find the token `<key>AutoFillPasswords</key>`
3. Ensure this token is immediately followed by `<false/>`

Default Value:

Enabled.

CIS Controls:

13 Data Protection
Data Protection

3.2 (L2) Ensure 'AutoFill web forms: Credit cards' is 'Disabled' (Scored)

Profile Applicability:

- Level 2

Description:

Safari can store and retrieve payment card information in the user-level keychain. The information is collected during an online purchase, following the user's permission. It is recommended that Safari be configured to not store payment card information in cases where security is paramount.

Rationale:

If a user's console session is compromised, credit card information may be auto-filled into a website for a malicious purpose.

Audit:

Follow the below steps and verify that `AutoFill web forms: Credit cards` is `Disabled`:

1. Click `Safari`.
2. Click `Preferences`.
3. Click `AutoFill`.
4. Verify `AutoFill web forms: Credit cards` is `unchecked`.

To verify the plist follow the below steps:

1. Open the `com.apple.Safari.plist`.
2. Find the token `<key>AutoFillCreditCardData</key>`
3. verify this token is immediately followed by `<false/>`

Remediation:

Follow the below steps to set `AutoFill web forms: Credit cards` to `Disabled`:

1. Click `Safari`.
2. Click `Preferences`.
3. Click `AutoFill`.
4. Uncheck `AutoFill web forms: Credit cards`.

To configure the plist follow the below steps:

1. Open the `com.apple.Safari.plist`.
2. Find the token `<key>AutoFillCreditCardData</key>`
3. Ensure this token is immediately followed by `<false/>`

Default Value:

Enabled.

CIS Controls:

13 Data Protection
Data Protection

3.3 (L2) Ensure 'AutoFill web forms: Other forms' is 'Disabled' (Scored)

Profile Applicability:

- Level 2

Description:

Safari can store the information typed in forms for later use on other websites. It is recommended that Safari be configured such that it does not store and auto-fill form contents.

Rationale:

If Safari or other applications executing at equal or higher security contexts is compromised, potentially sensitive, persisted, form data is at increased risk.

Audit:

Follow the below steps and verify that `AutoFill web forms: Other forms` is `Disabled`:

1. Click `Safari`.
2. Click `Preferences`.
3. Click `AutoFill`.
4. Verify `AutoFill web forms: Other forms` is `unchecked`.

To verify the plist follow the below steps:

1. Open the `com.apple.Safari.plist`.
2. Find the token `<key>AutoFillMiscellaneousForms</key>`
3. verify this token is immediately followed by `<false/>`

Remediation:

Follow the below steps to set `AutoFill web forms: Other forms` to `Disabled`:

1. Click `Safari`.
2. Click `Preferences`.
3. Click `AutoFill`.
4. Uncheck `AutoFill web forms: Other forms`.

To configure the plist follow the below steps:

1. Open the `com.apple.Safari.plist`.
2. Find the token `<key>AutoFillMiscellaneousForms</key>`
3. Ensure this token is immediately followed by `<false/>`

Default Value:

Enabled.

CIS Controls:

13 Data Protection
Data Protection

4 Passwords

This section contains settings under the Passwords tab of the Safari Browser.

4.1 (L2) Ensure 'AutoFill user names and passwords' is 'Disabled' (Scored)

Profile Applicability:

- Level 2

Description:

Safari can utilize a user-level keychain for credential storage, and then access that information when revisiting websites on the same domain. By disabling this feature the user will be prompted to manually enter their credentials when they visit a website.

Rationale:

If this setting is enabled, users can have Safari store and retrieve passwords through the user-level Keychain and provide them automatically the next time they log in to a site. An intruder who has unrestricted access to your computer for even a minute can gain access to secure site areas.

Audit:

Follow the below steps and verify that `AutoFill user names and passwords` is `Disabled`:

1. Click `Safari`.
2. Click `Preferences`.
3. Click `Passwords`.
4. Verify `AutoFill user names and passwords` is `unchecked`.

To verify the plist follow the below steps:

1. Open the `com.apple.Safari.plist`.
2. Find the token `<key>AutoFillPasswords</key>`
3. verify this token is immediately followed by `<false/>`

Remediation:

Follow the below steps to set `AutoFill user names and passwords` to `Disabled`:

1. Click `Safari`.
2. Click `Preferences`.
3. Click `Passwords`.
4. Uncheck the `AutoFill user names and passwords` checkbox.

To configure the plist follow the below steps:

1. Open the `com.apple.Safari.plist`.
2. Find the token `<key>AutoFillPasswords</key>`
3. Ensure this token is immediately followed by `<false/>`

Default Value:

Enabled.

CIS Controls:

13 Data Protection
Data Protection

5 Search

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

6 Security

This section contains settings under the Security tab of the Safari Browser.

6.1 (L1) Ensure 'Warn when visiting a fraudulent website' is 'Enabled' (Scored)

Profile Applicability:

- Level 1

Description:

Safari can be configured to alert the user that the site they are visiting is known to be malicious. It is recommended that this capability be enabled.

Rationale:

Users will be alerted about known malicious web sites, thus decreasing the probability of a user's browser or system being exploited by known malware or phishing site.

Audit:

Follow the below steps and verify that `Warn when visiting a fraudulent website` is `Enabled`:

1. Click `Safari`.
2. Click `Preferences`.
3. Click `Security`.
4. Verify `Warn when visiting a fraudulent website` is `checked`.

To verify the plist follow the below steps:

1. Open the `com.apple.Safari.plist`.
2. Find the token `<key>WarnAboutFraudulentWebsites</key>`
3. verify this token is immediately followed by `<true/>`

Remediation:

Follow the below steps to set `Warn when visiting a fraudulent website` to `Enabled`:

1. Click `Safari`.
2. Click `Preferences`.

3. Click `AutoFill`.
4. Check the `Warn when visiting a fraudulent website` checkbox.

To configure the plist follow the below steps:

1. Open the `com.apple.Safari.plist`.
2. Find the token `<key>WarnAboutFraudulentWebsites</key>`
3. Ensure this token is immediately followed by `<true/>`

Default Value:

Enabled.

CIS Controls:

7 Email and Web Browser Protections
Email and Web Browser Protections

6.2 (L2) Ensure 'Enable JavaScript' is 'Disabled' (Scored)

Profile Applicability:

- Level 2

Description:

JavaScript enables web site authors to create enhanced user interfaces. In support of this, JavaScript enables web sites to programmatically read and alter the document object model (DOM) for the rendered web site as well as instantiate various objects, such as asynchronous XML HTTP request (XHR) objects. It is recommended that JavaScript be disabled.

Rationale:

JavaScript continues to be an attack vector for exploiting vulnerabilities in the browser. Additionally, JavaScript is commonly leveraged by exploit authors to create a deterministic memory layout in support of increasing the reliability of exploits.

Audit:

Follow the below steps and verify that `Enable JavaScript` is `Disabled`:

1. Click `Safari`.
2. Click `Preferences`.
3. Click `Security`.
4. Verify `Enable JavaScript` is `unchecked`.

To verify the plist follow the below steps:

1. Open the `com.apple.Safari.plist`.
2. Find the token `<key>WebKitJavaScriptEnabled</key>`
3. verify this token is immediately followed by `<false/>`

Remediation:

Follow the below steps to set `Enable JavaScript` to `Disabled`:

1. Click `Safari`.
2. Click `Preferences`.
3. Click `AutoFill`.
4. Uncheck the `Enable JavaScript` checkbox.

To configure the plist follow the below steps:

1. Open the `com.apple.Safari.plist`.
2. Find the token `<key>WebKitJavaScriptEnabled</key>`
3. Ensure this token is immediately followed by `<false/>`

Default Value:

Enabled.

CIS Controls:

7.3 Limit Use Of Scripting Languages In Browsers And Email Clients
Limit the use of unnecessary scripting languages in all web browsers and email clients. This includes the use of languages such as ActiveX and JavaScript on systems where it is unnecessary to support such capabilities.

6.3 (L2) Ensure 'Block pop-up windows' is 'Enabled' (Scored)

Profile Applicability:

- Level 2

Description:

The `Block pop-up windows` feature is used to block pop-up windows which a website might open with or without any user interaction. Pop-ups can be used to open un-trusted malicious content. It is recommended that the Popup Blocker be enabled.

Rationale:

By enabling `Block pop-up windows`, pop-ups will be blocked which will reduce the likelihood of being redirected to a malicious site.

Audit:

Follow the below steps and verify that `Block pop-up windows` is `Enabled`:

1. Click `Safari`.
2. Click `Preferences`.
3. Click `Security`.
4. Verify `Block pop-up windows` is `checked`

To verify the plist follow the below steps:

1. Open the `com.apple.Safari.plist`.
2. Find the token `<key>WebKitJavaScriptCanOpenWindowsAutomatically</key>`
3. verify this token is immediately followed by `<false/>`

Remediation:

Follow the below steps to set `Block pop-up windows` to `Enabled`:

1. Click `Safari`.
2. Click `Preferences`.
3. Click `Security`.
4. Check the `Block pop-up windows` checkbox

To configure the plist follow the below steps:

1. Open the `com.apple.Safari.plist`.
2. Find the token `<key>WebKitJavaScriptCanOpenWindowsAutomatically</key>`
3. Ensure this token is immediately followed by `<false/>`

Default Value:

Enabled.

CIS Controls:

7 Email and Web Browser Protections
Email and Web Browser Protections

7 Privacy

This sections contains settings under the Privacy tab of the Safari Browser.

7.1 (L1) Ensure 'Cookies and website data' is set to 'Allow from websites I visit' (Scored)

Profile Applicability:

- Level 1

Description:

This setting `Allow from websites I visit` allows all first-party cookies and blocks all third-party cookies.

Rationale:

Blocking third party cookies can help protect a user's privacy by eliminating some tracking cookies.

Audit:

Follow the below steps and verify that `Cookies and website data` is set to `Allow from websites I visit`:

1. Click `Safari`.
2. Click `Preferences`.
3. Click `Privacy`.
4. Verify `Cookies and website data` is set to `Allow from websites I visit`.

To verify the plist follow the below steps:

1. Open the `com.apple.Safari.plist`.
2. Find the token `<key>BlockStoragePolicy</key>`
3. verify this token is immediately followed by `<integer>3</integer>`

Remediation:

Follow the below steps to set `Cookies and website data` to `Allow from websites I visit`:

1. Click `Safari`.
2. Click `Preferences`.
3. Click `Privacy`.
4. Set `Cookies and website data` to `Allow from websites I visit`.

To configure the plist follow the below steps:

1. Open the `com.apple.Safari.plist`.
2. Find the token `<key>BlockStoragePolicy</key>`
3. Ensure this token is immediately followed by `<integer>3</integer>`

Default Value:

Allow from websites I visit.

CIS Controls:

13 Data Protection
Data Protection

8 Websites

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

9 Extensions

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

10 Advanced

This section contains settings under the Advanced tab of the Safari Browser.

10.1 (L1) Ensure 'Show full website address' is 'Enabled' (Scored)

Profile Applicability:

- Level 1

Description:

This setting controls how the URL is displayed. With it enabled, the full path will be shown. With it disabled, only the high-level domain will be displayed.

Rationale:

By displaying the full URL, the user is better informed as to where they are browsing on a given site and may even see sensitive parameters that are being passed via URL.

Audit:

Follow the below steps and verify that `Show full website address` is set to `Enabled`:

1. Click `Safari`.
2. Click `Preferences`.
3. Click `Advanced`.
4. Verify the `Show full website address` checkbox is `checked`.

To verify the plist follow the below steps:

1. Open the `com.apple.Safari.plist`.
2. Find the token `<key>ShowFullURLInSmartSearchField</key>`
3. verify this token is immediately followed by `<true/>`

Remediation:

Follow the below steps to set `Show full website address` to `Enabled`:

1. Click `Safari`.
2. Click `Preferences`.
3. Click `Advanced`.
4. Check `Show full website address` checkbox.

To configure the plist follow the below steps:

1. Open the `com.apple.Safari.plist`.
2. Find the token `<key>ShowFullURLInSmartSearchField</key>`
3. Ensure this token is immediately followed by `<true/>`

Default Value:

Disabled. (Shortens URL)

CIS Controls:

7 Email and Web Browser Protections
Email and Web Browser Protections

11 Other

This section contains items not located within Safari Preferences.

11.1 (L1) Ensure 'Show Status Bar' is not 'Hidden' (Scored)

Profile Applicability:

- Level 1

Description:

This setting controls whether mousing over a link displays the full URL that the link will follow.

Rationale:

Showing the full URL allows users to validate that a link is performing the action it claims, and may prevent users from following malicious links.

Audit:

Follow the below steps and verify that `Show Status Bar` is not 'Hidden`:

1. Click `View`.
2. Verify `Hide Status bar` is displayed.

To verify the plist follow the below steps:

1. Open the `com.apple.Safari.plist`.
2. Find the token `<key>ShowOverlayStatusBar<key>`
3. Verify this token is immediately followed by `<true/>`.

Remediation:

Follow the below steps to set `Show Status Bar`:

1. Click `View`.
2. Click `Show Status Bar`.

To configure the plist follow the below steps:

1. Open the `com.apple.Safari.plist`.
2. Find the token `<key>ShowOverlayStatusBar<key>`
3. Ensure this token is immediately followed by `<true/>`

Default Value:

Hidden.

CIS Controls:

7 Email and Web Browser Protections
Email and Web Browser Protections

Appendix: Summary Table

Control		Set Correctly	
		Yes	No
1	**General**		
1.1	(L1) Ensure 'Open "safe" files after downloading' is 'Disabled' (Scored)	☐	☐
2	**Tabs**		
3	**AutoFill**		
3.1	(L2) Ensure 'AutoFill web forms: User names and passwords' is 'Disabled' (Scored)	☐	☐
3.2	(L2) Ensure 'AutoFill web forms: Credit cards' is 'Disabled' (Scored)	☐	☐
3.3	(L2) Ensure 'AutoFill web forms: Other forms' is 'Disabled' (Scored)	☐	☐
4	**Passwords**		
4.1	(L2) Ensure 'AutoFill user names and passwords' is 'Disabled' (Scored)	☐	☐
5	**Search**		
6	**Security**		
6.1	(L1) Ensure 'Warn when visiting a fraudulent website' is 'Enabled' (Scored)	☐	☐
6.2	(L2) Ensure 'Enable JavaScript' is 'Disabled' (Scored)	☐	☐
6.3	(L2) Ensure 'Block pop-up windows' is 'Enabled' (Scored)	☐	☐
7	**Privacy**		
7.1	(L1) Ensure 'Cookies and website data' is set to 'Allow from websites I visit' (Scored)	☐	☐
8	**Websites**		
9	**Extensions**		
10	**Advanced**		
10.1	(L1) Ensure 'Show full website address' is 'Enabled' (Scored)	☐	☐
11	**Other**		
11.1	(L1) Ensure 'Show Status Bar' is not 'Hidden' (Scored)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
11/28/17	2.0.0	Rewrite from Original