Apple iOS 14 and Apple iPadOS 14: Safari Common Criteria Configuration Guide

Document Version: 1.0
Date: July 2021

Prepared for:
Apple
One Apple Park Way
Cupertino, CA 95014

Prepared by:
intertek acumen security

2400 Research Blvd
Suite 395
Rockville, MD 20850

Revision History:

Version	Date	Changes
1.0	July 2021	Initial Release

Trademarks

Contents

1 Introduction

This guide provides instructions to configure and operate Apple iOS 14 and iPadOS 14: Safari in the common criteria evaluated configuration.

1.1 Target of Evaluation

The evaluated application is the Safari application that is bundled with Apple iOS 14 and iPadOS 14. Safari provides access and management of user contact information within the devices. Safari was evaluated on the following platforms:

Table 1 – Evaluated Platforms

Device Name	Model	OS	Processor
iPhone 12 Pro Max	A2342 A2410 A2411 A2412	iOS	Apple A14 Bionic
iPhone 12 Pro	A2341 A2406 A2407 A2408	iOS	Apple A14 Bionic
iPhone 12	A2172 A2402 A2403 A2404	iOS	Apple A14 Bionic
iPhone 12 mini	A2176 A2398 A2399 A2400	iOS	Apple A14 Bionic
iPhone 11 Pro Max	A2161 A2218 A2219 A2220	iOS	Apple A13 Bionic
iPhone 11 Pro	A2160 A2215 A2217	iOS	Apple A13 Bionic
iPhone 11	A2111 A2221 A2223	iOS	Apple A13 Bionic
iPhone SE (2nd generation)	A2275 A2296 A2298	iOS	Apple A13 Bionic
iPhone Xs Max	A1921 A2101 A2102 A2104	iOS	Apple A12 Bionic
iPhone Xs	A1920 A2097 A2098 A2099 A2100	iOS	Apple A12 Bionic
iPhone Xr	A1984 A2105	iOS	Apple A12 Bionic

Device Name	Model	OS	Processor
	A2106 A2107 A2108		
iPhone X	A1865 A1901 A1902	iOS	Apple A11 Bionic
iPhone 8 Plus	A1864 A1897 A1898 A1899	iOS	Apple A11 Bionic
iPhone 8	A1863 A1905 A1906 A1907	iOS	Apple A11 Bionic
iPhone 7 Plus	A1661 A1784 A1785 A1786	iOS	Apple A10 Fusion
iPhone 7	A1660 A1778 A1779 A1780	iOS	Apple A10 Fusion
iPhone 6s Plus	A1634 A1687 A1690 A1699	iOS	Apple A9
iPhone 6s	A1633 A1688 A1691 A1700	iOS	Apple A9
iPhone SE	A1662 A1723 A1724	iOS	Apple A9
iPad Air (4th generation)	A2316 A2324 A2072 A2325	iPadOS	Apple A14 Bionic
iPad Pro 12.9-inch (4th generation)	A2229 A2232 A2069 A2233	iPadOS	Apple A12Z Bionic
iPad Pro 11-inch (2nd generation)	A2228 A2068 A2230 A2331	iPadOS	Apple A12Z Bionic
iPad Pro 12.9-inch (3rd generation)	A1876 A1895 A1983 A2014	iPadOS	Apple A12X Bionic
iPad Pro 11-inch (1st generation)	A1980 A1934	iPadOS	Apple A12X Bionic

Device Name	Model	OS	Processor
	A1979 A2013		
iPad (8th generation)	A2270 A2428 A2429 A2430	iPadOS	Apple A12 Bionic
iPad Air (3rd generation)	A2123 A2152 A2153 A2154	iPadOS	Apple A12 Bionic
iPad mini (5th generation)	A2124 A2125 A2126 A2133	iPadOS	Apple A12 Bionic
iPad Pro 12.9-inch (2nd generation)	A1670 A1671 A1821	iPadOS	Apple A10X Fusion
iPad Pro (10.5-inch)	A1701 A1709 A1852	iPadOS	Apple A10X Fusion
iPad (7th generation)	A2198 A2199 A2200	iPadOS	Apple A10 Fusion
iPad (6th generation)	A1893 A1954	iPadOS	Apple A10 Fusion
iPad Pro (12.9-inch)	A1584 A1652	iPadOS	Apple A9X
iPad Pro (9.7-inch)	A1673 A1674 A1675	iPadOS	Apple A9X
iPad (5th generation)	A1822 A1823	iPadOS	Apple A9

1.2 Document Purpose and Scope

This document describes the installation and Common Criteria evaluation related usage of the Apple iOS 14 and iPadOS 14: Safari on iPhone and iPad.

This guide will show the administrator how to install and operate the software in a Common Criteria compliant manner. The administrator will learn:

- How to verify the application version
- The secure communication mechanisms employed by Safari
- Platform resources used by Safari
- Evaluated functionality

2 Installation/Update

Safari is loaded by default on Apple iOS 14 and iPadOS 14. However, if Safari is deleted from the platform, it may be re-installed via the Apple App Store. All applications found on the Apple App Store are digitally signed.

2.1 Checking the Version

Safari is a core Apple application. These applications are not updated separately from iOS and are versioned identically to the operating system. The application and OS version can be verified by completing the following steps:

1. Open the "Settings" app.
2. Tap the "General" option.
3. Tap the "About" option to view the current OS version.

An example of this version verification process for iOS can be found in Figure 1. Note that the Software Version field indicates version 14.6.

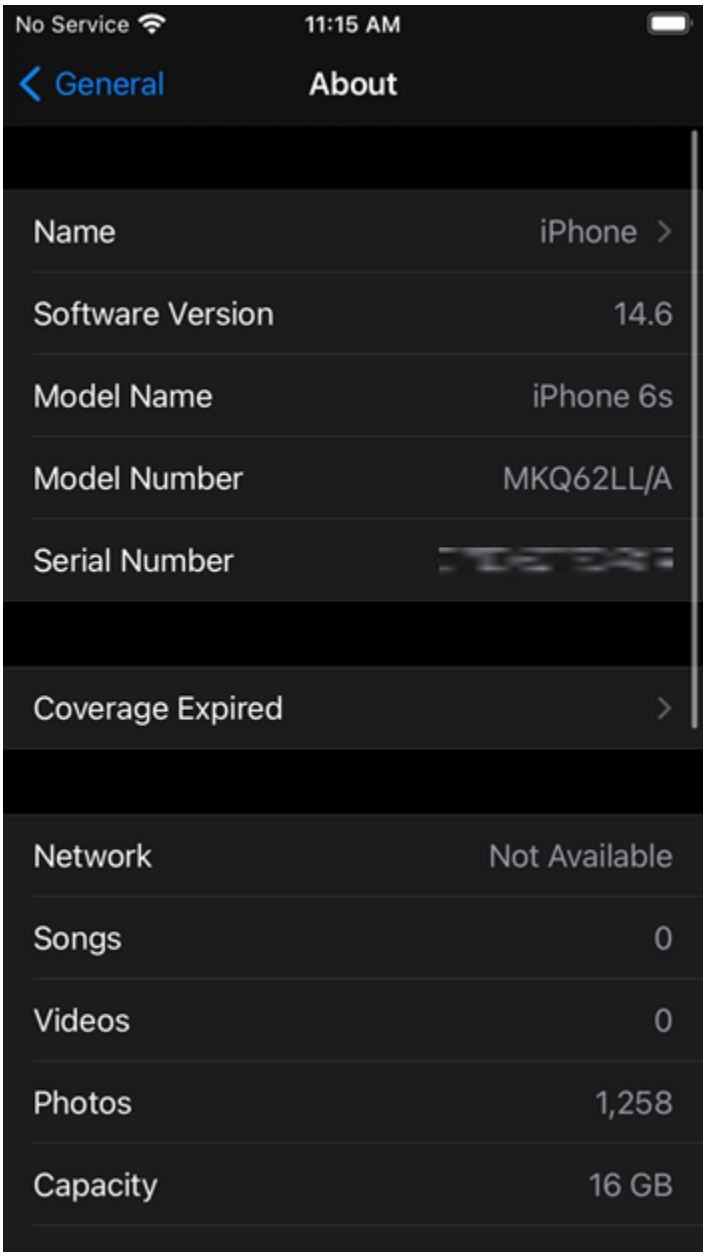

Figure 1 – iOS Version Verification

An example of this version verification process for iPadOS can be found in Figure 2. Note that the Software Version field indicates version 14.6.

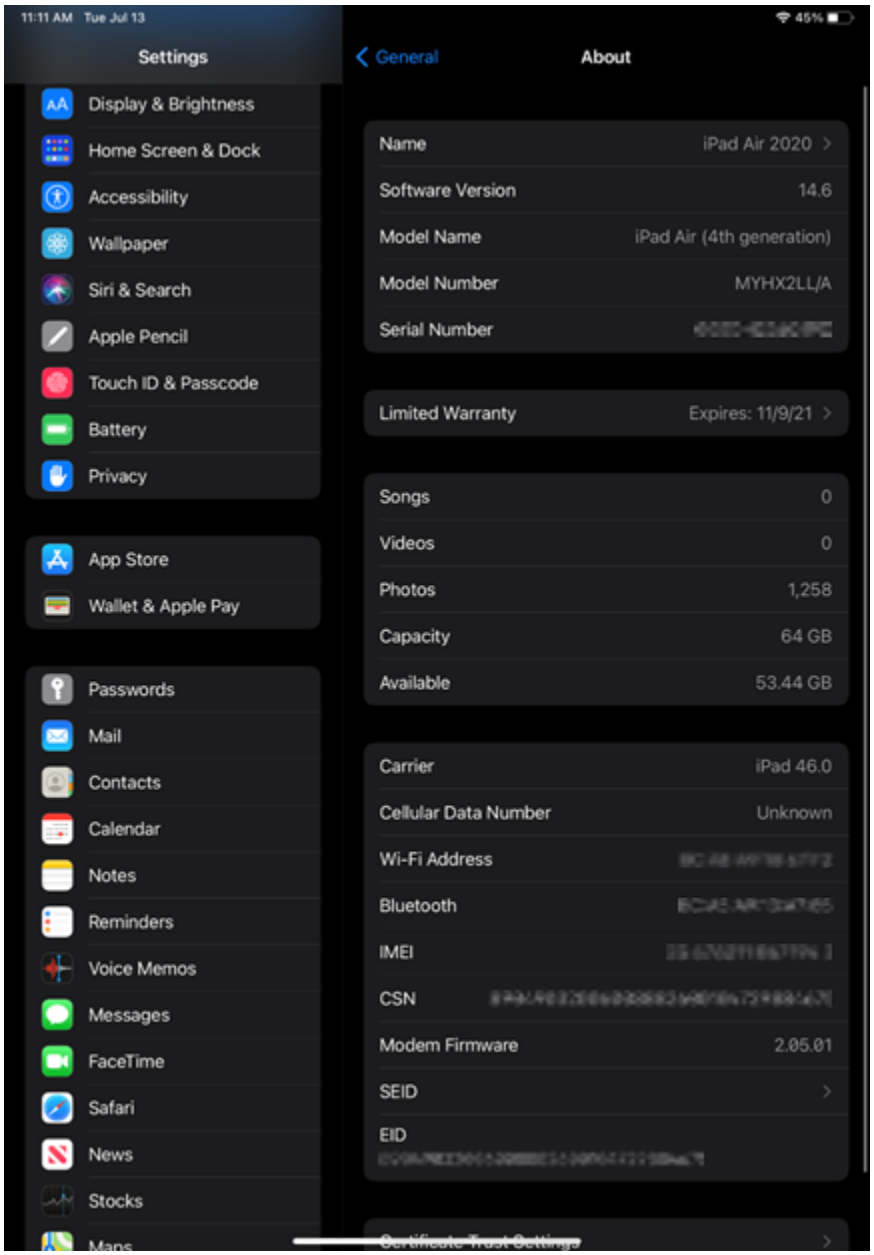

Figure 2 – iPadOS Version Verification

2.2 Installing Updates

Contacts is a core Apple application. These applications are not updated separately from iOS and are versioned identically to the operating system. The following steps are followed in order to verify the application (and OS version).

1. Open the "Settings" app.
2. Tap the "General" option.
3. Tap the "Software Update" option to view and install any updates.

2.3 Other Assumptions

In order to use Safari in the evaluated configuration, the Platform (i.e., the iPhone or iPad) must also be configured to meet the requirements of the Protection Profile for Application Software Version 1.3, the Extended Package for Web Browsers v2.0 as set forth in the Security Target and guidance documentation for the Apple iOS 14 and iPadOS 14 software operating on one of the hardware platforms listed in Table 1.

3 Secure Communications

3.1 TLS Configuration

Safari supports secure communications with webservers via HTTPS/TLS.

All configuration of these connections is handled exclusively by the underlying platform (Apple iOS and iPadOS). No additional configuration is required to ensure proper usage.

3.2 Digital Certificates

Safari leverages "Trusted" digital certificates that pre-installed in the iOS and iPadOS Trust Store. No configuration is required to facilitate the usage of these digital certificates. Additional information regarding the Apple iOS 14 and iPadOS 14 Trust Store may be found at: https://support.apple.com/HT210770. Additional trust anchors may be added by the user by performing the following steps:

1. Copy the CA certificate to the device.
2. Open the certificate.
3. Open the Settings app.
4. Select ‘Profile Downloaded’.
5. Tap ‘Install’.
6. Enter your passcode to authorize the installation.
7. Tap ‘Install’ to acknowledge the warning.
8. Tap ‘Install’ to confirm the installation.
9. In the Settings app, go to ‘General -> ‘About’ -> ‘Certificate Trust Settings’.
10. Tap the toggle next to the certificate to enable the certificate as a trust anchor.

Safari automatically creates the reference identifier from the DNS name or IP address of the website being accessed.

4 Resource Usage

Safari uses the following resources:

- Network Connectivity: This is required for Safari to facilitate communications with remote websites.
- Camera: This is required when a website requests access to the device's camera input.
- Microphone: This is required when a website requests access to the device's audio input.
- Location Services: This required to share location with websites.
- Keychain: This is required to store and auto fill usernames, passwords, and other fields for the user.
- Address Book: This is required to allow the autofill function.

5 User Data Protection

5.1 Local and Session Storage Separation

The browser shall separate local (permanent) and session (ephemeral) storage based on domain, protocol and port:

- Safari utilizes the platform OS process separation to isolate ephemeral/session storage. Each tab is a separate process, so the process separation prevents tabs from accessing any resources loaded by a different tab.
- The main Safari process provides the persistent/local storage. When a tab loads information into local storage, it also copies the data along with the origin to the main process for persistence. The main process enforces the same origin policy when determining if the local storage data should be shared with any other tabs that share the same origin.

No configuration is required to enforce this behavior.

5.2 Sandboxing of Rendering Process

The browser ensures that web page rendering is performed in a process that is restricted in the following manner:

- The rendering process can only directly access the area of the file system dedicated to the browser.
- The rendering process can only directly invoke inter-process communication mechanisms with its own browser processes.
- The rendering process has no other privilege with respect to other browser processes.

No configuration is required to enforce this behavior.

5.3 Tracking Information Collection

The browser shall provide notification to the user when tracking information for geolocation or browser preferences are requested by a website. An example notification is shown in Figure 3.

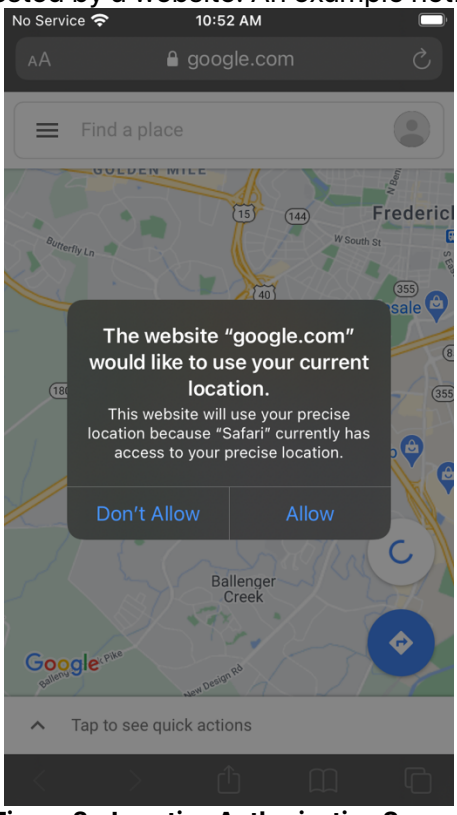

Figure 3 – Location Authorization Screen

No configuration is required to enforce this behavior.

5.4 Cookie Blocking, Tracking Behavior, and Other Security Features

Use the following configurations to enable or disable security features of Safari:

- To enable/disable storage of all cookies (including First-party cookies and Third party cookies), tap on Settings > Safari > Block All Cookies.
- To clear your browser history and cookies, tap Settings > Safari > Clear History and Website Data. Clearing your history, cookies, and browsing data from Safari won't delete your AutoFill information.
- To clear your AutoFill information, tap Settings > Safari > AutoFill. From here, you can toggle the information you wish to be saved, as well as review and delete saved information.
- To clear your cookies and keep your history, tap Settings > Safari > Advanced > Website Data > Remove All Website Data.
- To configure malicious application/URL detection, tap Settings > Safari > Fraudulent Website Warning.
- To enable/disable JavaScript, tap Settings > Safari > Advanced > JavaScript.

6 Self-Protection

6.1 File Downloads

Whenever a file is presented for download, a dialog box is presented to the user. The user must tap “Download” to allow the file to be downloaded. Safari does not automatically run any executable files once they have been downloaded. No configuration is required to enforce this behavior.

7 Administrator Configuration

iOS and iPadOS 14 allow for an administrator to install a profile to control specific settings on Safari.

The administrator should use Apple Configurator 2 on an Apple computer to configure and create the profile and install it on the devices.

On the Configurator, go to File > New Profile then change the name option on the first page. For example, Profile Name, Organization Name, Profile being removable by the user or not and Profile expiration as shown in Figure 4.

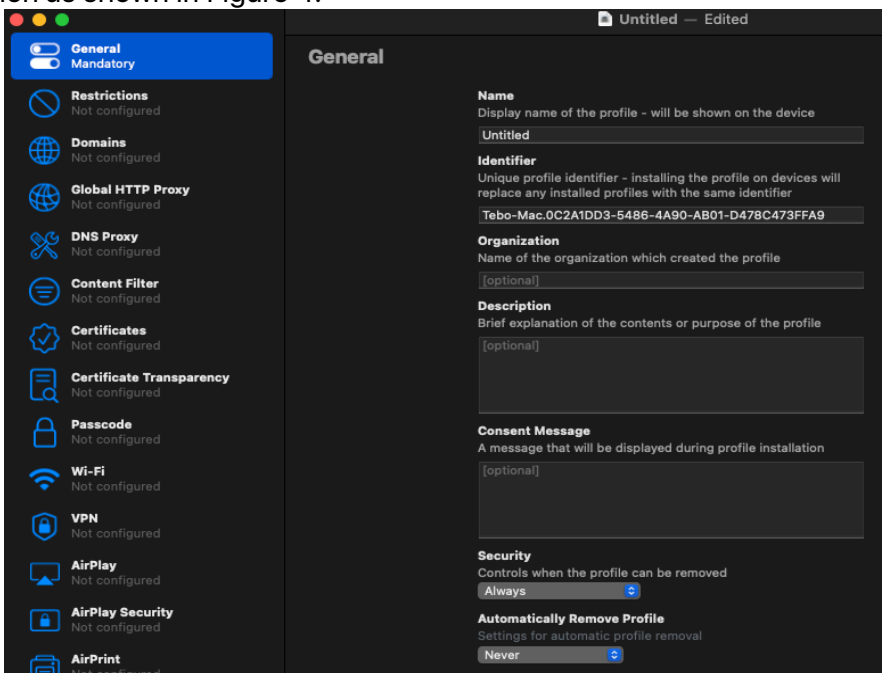

Figure 4 – Profile Creation Tab

To configure Safari, the administrator should use the Restrictions page, select Configure, go to the Apps tab and select the desired option to enforce on the device as shown in Figure 5.

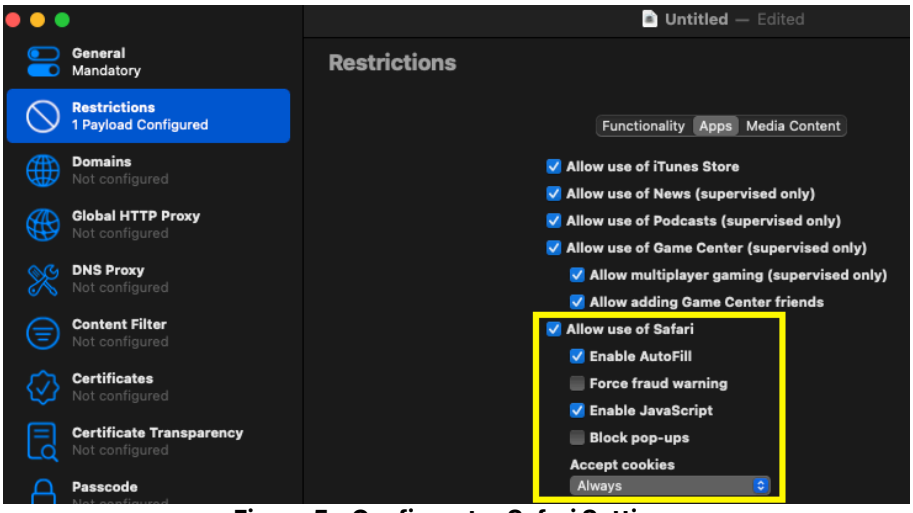

Figure 5 – Configurator Safari Settings

To upload the profile, connect the device to the device where Configurator 2 is installed. The device will appear in Configurator as shown in Figure 6.

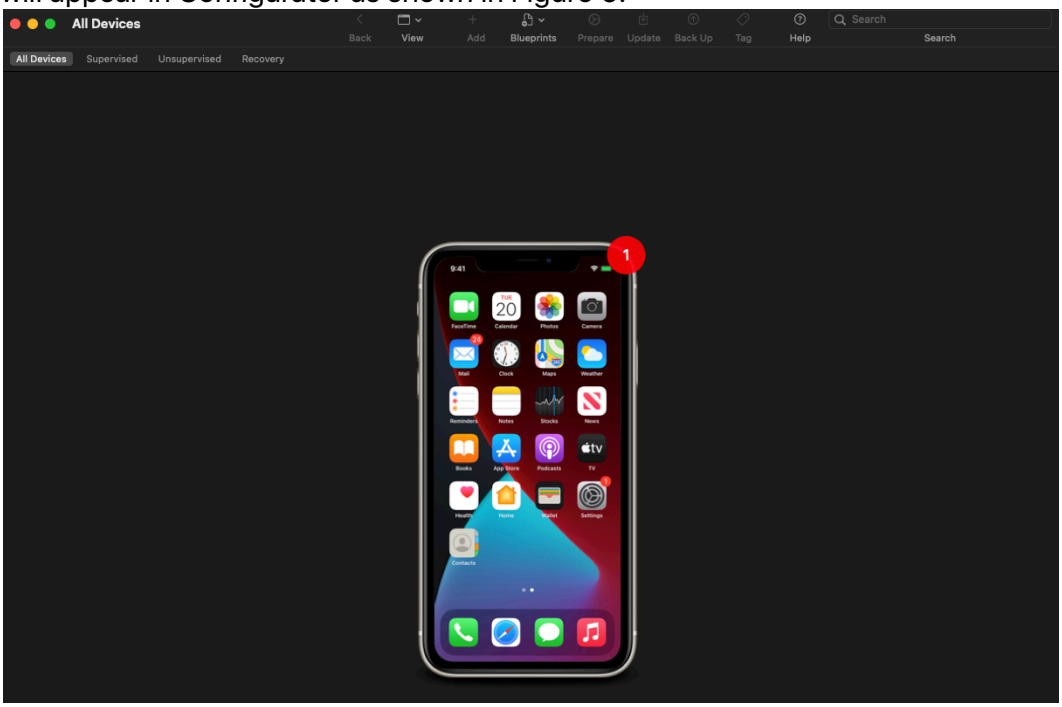

Figure 6 – Configurator Device Screen

Control-click on the device, select Add > Profiles and select the profile to upload.

8 Support for Add-ons

Safari does not support add-ons.

9 Acronyms

Table 2 – Acronyms

Acronym	Definition
DNS	Domain Name System
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol
OS	Operating System
TLS	Transport Layer Security

End of Document