Apple Inc.

Apple iOS and iPadOS 13 Safari Common Criteria Configuration Guide

June 2020

Version 1.5

Prepared for Apple Inc.

Prepared by Acumen Security LLC.

Contents

Revision History

Version	Date	Description
1.0	December 2019	Initial Version
1.1	February 2020	Updated Local and Session Storage description.
1.2	April 2020	Updated Heading for Resource Usage
1.3	April 2020	Removed references to Platform VID, updated TOE evaluated models,
1.4	June 2020	Updated the title
1.5	June 2020	Updated device identifiers

1 Introduction

1.1 Target of Evaluation

The evaluated application is the Safari web browser that is bundled with Apple iOS 13 and iPadOS 13. The product provides access to HTTPS/TLS connections via a browser for user connectivity. The evaluation covers the following platforms:

Device Name	Model	OS	Processor	WiFi	Bluetooth
iPhone 11 Pro Max	A2161 A2218 A2219 A2220	iOS	A13 Bionic	802.11a/b/g/n/ac/ax	5.0
iPhone 11 Pro	A2160 A2215 A2216 A2217	iOS	A13 Bionic	802.11a/b/g/n/ac/ax	5.0
iPhone 11	A2111 A2221 A2222 A2223	iOS	A13 Bionic	802.11a/b/g/n/ac/ax	5.0
iPhone SE (2nd Gen)	A2275 A2296 A2298	iOS	A13 Bionic	802.11a/b/g/n/ac/ax	5.0
iPhone Xs Max	A1921 A2101 A2102 A2103 A2104	iOS	A12 Bionic	802.11a/b/g/n/ac	5.0
iPhone Xs	A1920 A2097 A2098 A2099 A2100	iOS	A12 Bionic	802.11a/b/g/n/ac	5.0
iPhone XR	A1984 A2105 A2106 A2107 A2108	iOS	A12 Bionic	802.11a/b/g/n/ac	5.0
iPhone X	A1865 A1901 A1902 A1903	iOS	A11 Bionic	802.11a/b/g/n/ac	5.0
iPhone 8 Plus	A1864 A1897 A1898 A1899	iOS	A11 Bionic	802.11a/b/g/n/ac	5.0
iPhone 8	A1863 A1905	iOS	A11 Bionic	802.11a/b/g/n/ac	5.0

Device Name	Model	OS	Processor	WiFi	Bluetooth
	A1906 A1907				
iPhone 7 Plus	A1661 A1784 A1785 A1786	iOS	A10 Fusion	802.11a/b/g/n/ac	4.2
iPhone 7	A1660 A1778 A1779 A1780	iOS	A10 Fusion	802.11a/b/g/n/ac	4.2
iPhone 6S Plus	A1634 A1687 A1690 A1699	iOS	A9	802.11a/b/g/n/ac	4.2
iPhone 6s	A1633 A1688 A1691 A1700	iOS	A9	802.11a/b/g/n/ac	4.2
iPhone SE	A1662 A1723 A1724	iOS	A9	802.11a/b/g/n/ac	4.2
iPad Pro 12.9” (4th gen)	A2229 A2232 A2069 A2233	iPadOS	A12Z Bionic	802.11a/b/g/n/ac/ax	5.0
iPad Pro 11” (2nd gen)	A2228 A2068 A2230 A2331	iPadOS	A12Z Bionic	802.11a/b/g/n/ac/ax	5.0
iPad Pro 12.9-inch (3rd gen)	A1876 A1895 A1983 A2014	iPadOS	A12X Bionic	802.11a/b/g/n/ac	5.0
iPad Pro 11-inch	A1980 A1934 A1979 A2013	iPadOS	A12X Bionic	802.11a/b/g/n/ac	5.0
iPad Air (3rd gen)	A2123 A2152 A2153 A2154	iPadOS	A12 Bionic	802.11a/b/g/n/ac	5.0
iPad mini (5th gen)	A2124 A2125 A2126 A2133	iPadOS	A12 Bionic	802.11a/b/g/n/ac	5.0

Device Name	Model	OS	Processor	WiFi	Bluetooth
iPad Pro (12.9-inch 2nd gen)	A1670 A1671 A1821	iPadOS	A10X Fusion	802.11a/b/g/n/ac	4.2
iPad Pro (10.5-inch)	A1701 A1709 A1852	iPadOS	A10X Fusion	802.11a/b/g/n/ac	4.2
iPad (7th gen)	A2197 A2198 A2199 A2200	iPadOS	A10 Fusion	802.11a/b/g/n/ac	4.2
iPad (6th gen)	A1893 A1954	iPadOS	A10 Fusion	802.11a/b/g/n/ac	4.2
iPad Pro (12.9)	A1584 A1652	iPadOS	A9X	802.11a/b/g/n/ac	4.2
iPad Pro (9.7-inch)	A1673 A1674 A1675	iPadOS	A9X	802.11a/b/g/n/ac	4.2
iPad (5th gen)	A1822 A1823	iPadOS	A9	802.11a/b/g/n/ac	4.2
iPad Air 2	A1566 A1567	iPadOS	A8X	802.11a/b/g/n/ac	4.2
iPad mini 4	A1538 A1550	iPadOS	A8	802.11a/b/g/n	4.2

Table 1 Evaluated Platforms

1.2 Document Purpose and Scope

This document describes the installation and Common Criteria evaluation related usage of the Apple iOS 13 and iPadOS 13 Safari on iPhone and iPad.

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

- How to verify the application version
- The secure communication mechanisms employed by Safari
- How to configure user data and self-protection features
- Platform resources used by Safari
- Evaluated functionality

2 Installation/Update

Safari is loaded by default on Apple iOS 13 and iPadOS 13. It is not possible to delete Safari as it is a core OS application. All updates to it are released via OS update.

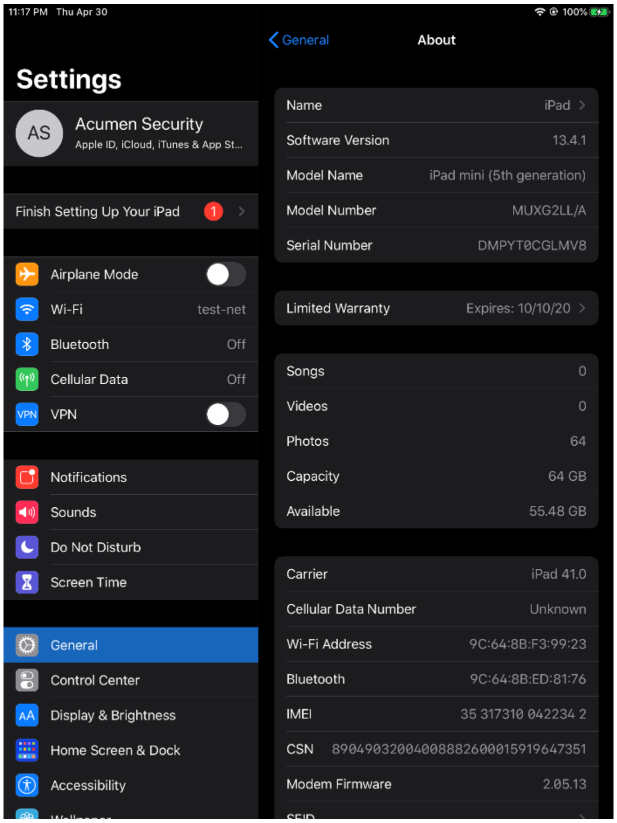
2.1 Verifying Product Version

Safari is a core OS application. Safari is not updated separately from iOS and iPadOS, and it is versioned identically to the OS. The following steps are followed in order to verify the application (and OS version).

- Tap the “Settings” application.
- Tap the “General” option.
- Tap the “About” option to view the current version.
- Tap the “Software Update” option to learn about OS updates, if any.

The following is an example of this verification on iPad:

Software Version: 13.4.1



11:17 PM Thu Apr 30

Settings

AS Acumen Security
Apple ID, iCloud, iTunes & App St...

Finish Setting Up Your iPad 1

Airplane Mode	
Wi-Fi	test-net
Bluetooth	Off
Cellular Data	Off
VPN	

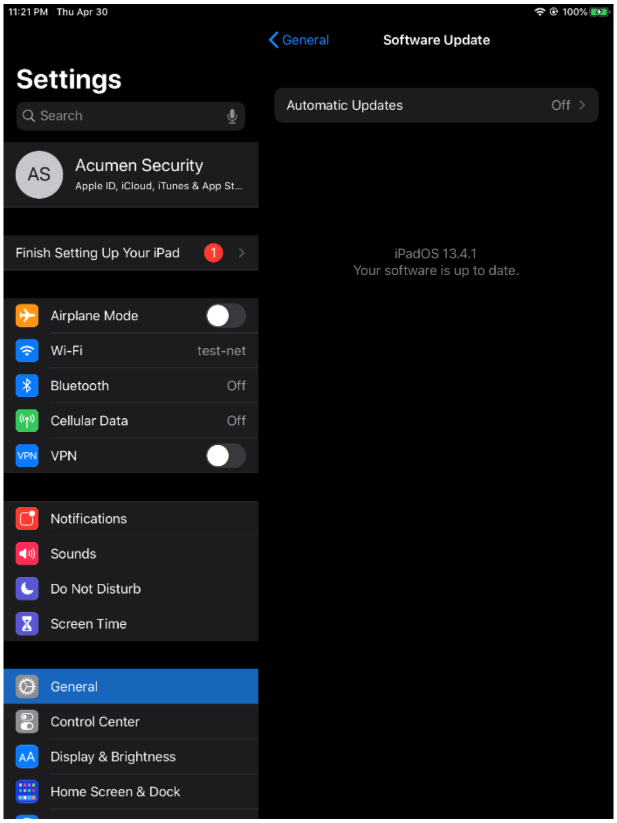
Notifications
Sounds
Do Not Disturb
Screen Time

General
Control Center
Display & Brightness
Home Screen & Dock
Accessibility

< General **About**

Name	iPad >
Software Version	13.4.1
Model Name	iPad mini (5th generation)
Model Number	MUXG2LL/A
Serial Number	DMPYT0CGLMV8
Limited Warranty	Expires: 10/10/20 >
Songs	0
Videos	0
Photos	64
Capacity	64 GB
Available	55.48 GB
Carrier	iPad 41.0
Cellular Data Number	Unknown
Wi-Fi Address	9C:64:8B:F3:99:23
Bluetooth	9C:64:8B:ED:81:76
IMEI	35 317310 042234 2
CSN	89049032004008882600015919647351
Modem Firmware	2.05.13
SEID	>

iPadOS 13.4.1 – Your Software is up to date



11:21 PM Thu Apr 30

Settings

Search

AS Acumen Security
Apple ID, iCloud, iTunes & App St...

Finish Setting Up Your iPad 1

Airplane Mode	
Wi-Fi	test-net
Bluetooth	Off
Cellular Data	Off
VPN	

Notifications
Sounds
Do Not Disturb
Screen Time

General
Control Center
Display & Brightness
Home Screen & Dock

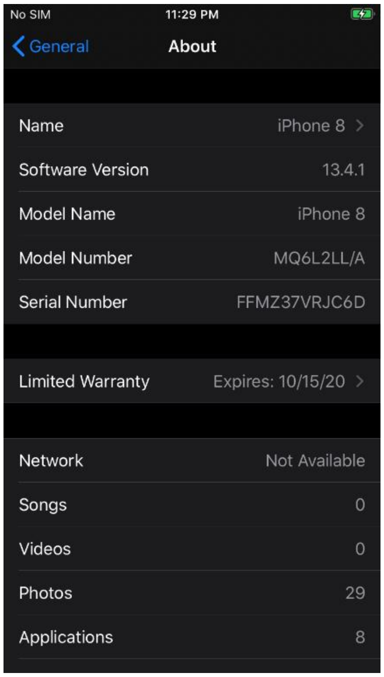
< General **Software Update**

Automatic Updates Off >

iPadOS 13.4.1
Your software is up to date.

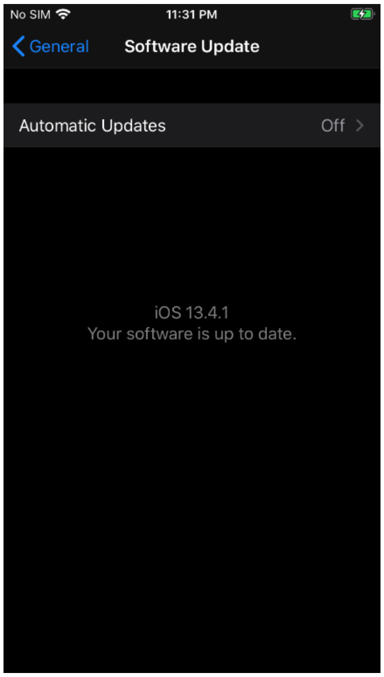
The following is an example of this verification on iPhone:

Software Version: 13.4.1



Name	iPhone 8
Software Version	13.4.1
Model Name	iPhone 8
Model Number	MQ6L2LL/A
Serial Number	FFMZ37VRJC6D
Limited Warranty	Expires: 10/15/20
Network	Not Available
Songs	0
Videos	0
Photos	29
Applications	8

iOS 13.4.1 – Your Software is up to date



Automatic Updates Off

iOS 13.4.1
Your software is up to date.

If a new version of the OS/Safari are available, it will be indicated on this screen.

2.2 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 Mobile Device Fundamentals Version 3.1 as set forth in the Security Target and guidance documentation for the Apple iOS 13 and iPadOS 13 software operating on one of the hardware platforms listed in Table 1.

3 Cryptographic Support

Safari utilizes platform provided HTTPS/TLS and Digital Certificates to provide secure communications with websites.

3.1 TLS Configuration

Safari supports secure communications with websites 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 installed in the iOS 13 and iPadOS 13 Trust Store. No configuration is required to facilitate the usage of these digital certificates. Additional information regarding the Apple iOS/iPadOS 13 Trust Store may be found at: https://support.apple.com/en-us/HT210770.

Safari automatically uses the domain name of the server being contacted as the reference identifier. Again, no configuration is required.

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.

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 TOE 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 persist. 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 Processes

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

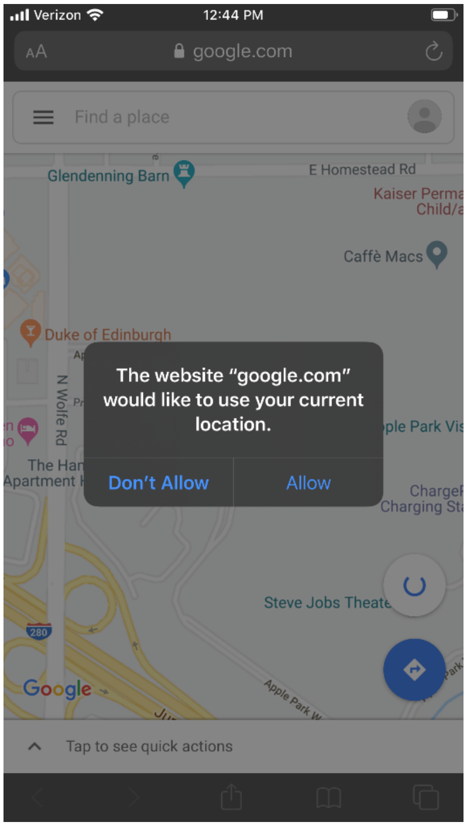
The rendering process can only directly access the area of the file system dedicated to the browser.

- 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. The following is an example,



The website “google.com” would like to use your current location.

No configuration is required to enforce this behavior.

5.4 Cookie Blocking and Other Tracking Behavior & Security Features

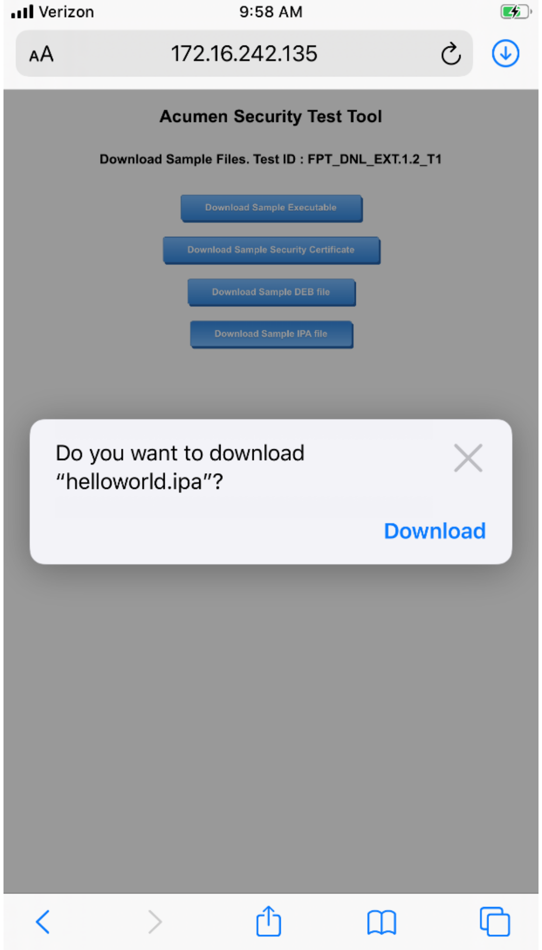
Use the following configurations to enable or disable security features of Safari.

- 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

The browser shall prevent downloaded content from launching automatically. Whenever a file is presented for download, a dialog box is presented. The file will not download without explicit user action. The following is an example of such dialog box:



Acumen Security Test Tool

Download Sample Files. Test ID : FPT_DNL_EXT.1.2_T1

Download Sample Executable
Download Sample Security Certificate
Download Sample DEB file
Download Sample IPA file

Do you want to download “helloworld.ipa”?

No configuration is required to enforce this behavior.

6.2 Support for Add-ons

Safari does not support add-ons.

7 Evaluated Functionality

The evaluated functionality is limited to the function specified in the Protection Profile for Application Software and Application Software Extended Package for Web Browsers.

End of Document