

Apple iOS 15: iPhones and Apple iPadOS 15: iPads

Common Criteria Configuration Guide

PP_MDF_V3.2
with
MOD_MDM_AGENT_V1.0,
MOD_BT_V1.0,
MOD_VPNC_V2.3,
PP_WLAN_CLI_EP_V1.0,
PKG_TLS_V1.1

Version 1.2
2022-09-23
VID: 11237+11238

Prepared for:
Apple Inc.
One Apple Park Way
MS 927-1CPS
Cupertino, CA 95014
www.apple.com

Prepared by:
atsec information security Corp.
9130 Jollyville Road, Suite 260
Austin, TX 78759
www.atsec.com

Table of Contents

1	<i>Revision History</i>	7
2	<i>Trademarks</i>	8
3	<i>Introduction</i>	9
3.1	Purpose	10
3.2	TOE Security Functionality	10
3.3	Supporting Apple Documentation	10
3.4	Evaluated Mobile Devices	14
3.5	Assumptions	19
3.5.1	Administrators	20
3.5.2	Mobile device users	20
3.5.3	Network	20
3.5.4	Other	20
3.6	Organizational Security Policies	21
3.7	Security Functional Requirements (SFRs) in the STs requiring configuration	21
3.8	Security Management Configuration	33
3.9	Un-evaluated Functionalities	38
3.9.1	Two-Factor Authentication	38
3.9.2	Bonjour	38
3.9.3	VPN Split Tunnel	39
3.9.4	Siri Interface	39
3.9.5	Shared iPad for education	39
3.9.6	Third-party MDM Agents	39
3.9.7	VPN Protocols and Authentication Methods	39
4	<i>Secure Delivery and Installation</i>	40
4.1	Prerequisites	40
4.2	Secure Delivery of the Devices	40
4.2.1	Obtaining the mobile device(s)	40
4.2.2	Verifying the device(s)	41
4.3	Mobile Device Supervision and Configuration	41
4.3.1	Mobile Device Enrollment into Management Configuration	42
4.3.2	Mobile Device Configuration	43
4.3.3	Configure MDM Agent and MDM Communications	44
4.3.4	Device Unenrollment Prevention	44
4.3.5	MDM Agent Alerts	44
4.3.6	The MDM Payload	45
5	<i>Mobile Device Configuration</i>	46

5.1	General Restrictions	46
5.1.1	Keys for General Restrictions	46
5.2	Cryptographic Support Functions	46
5.2.1	Key Generation, Signature Generation, and Verification	47
5.2.2	Key Establishment	47
5.2.3	Hashing	48
5.2.4	Random Number Generation	48
5.2.5	Keys/Secrets Import/Destruction	49
5.2.6	Keys for Configuring Cryptographic Functions	49
5.3	Network Protocols	50
5.3.1	EAP-TLS Configuration	50
5.3.2	TLS Configuration	51
5.3.3	IPsec Configuration	54
5.3.4	Bluetooth Configuration	55
5.3.5	VPN Configuration	56
5.3.6	Keys for Configuring Network Protocols	57
5.4	Data Protection	61
5.4.1	Data-At-Rest (DAR) Protection Configuration	61
5.4.2	Restrict Application Access to System Services	62
5.4.3	Wiping of Protected Data	63
5.4.4	Keys for Configuring Data Protection	64
5.5	Identification & Authentication	65
5.5.1	Passcode Authentication Configuration	65
5.5.2	Protected Authentication Feedback	66
5.5.3	Biometric Authentication Factors	66
5.5.4	Authentication Attempt Configuration	68
5.5.5	Re-Authentication Configuration	68
5.5.6	X.509 Certificate Configuration	69
5.5.7	Keys for Identification and Authentication	72
5.6	Security Management	73
5.6.1	Install/Remove Apps from the Device	73
5.6.2	Configure Access and Notification in Locked State	74
5.6.3	Device/Session Locking	76
5.6.4	Timestamp Configuration	76
5.6.5	Access Banner Configuration	77
5.6.6	Enable/Disable Cameras and Microphones	78
5.6.7	Enable/Disable Cellular, Wi-Fi, Wi-Fi Hotspot, Bluetooth, NFC, UWB	78
5.6.8	Enable/Disable Location Services	81
5.6.9	Enable/Disable iCloud Drive Documents and Data	81
5.6.10	Secure Software Updates	82
5.6.11	Enable/Disable Remote Backup	83
5.6.12	Configure Application Installation Policy	84
5.6.13	Importing keys/ shared secrets	84
5.6.14	Dictionary Keys for Management Functions	85
6	<i>Security Audit</i>	<i>86</i>

6.1	Audit Logging	86
6.2	Audit Storage	98
6.3	Configure the Auditable Items	99
7	<i>Installed Apps</i>	103
8	<i>References</i>	105
9	<i>Abbreviations and Acronyms</i>	106
10	<i>Appendix A: Configuration Profiles</i>	108
10.1	Configuration Profile 1: "MDF PP Configuration Profile AirPrint"	108
10.2	Configuration Profile 2: "MDF PP Configuration Profile for General Restrictions"	109
10.3	Configuration Profile 3: "MDF PP Configuration Profile Passcode Restrictions"	111
10.4	Configuration Profile 4: "MDF PP Configuration Profile VPN"	113
10.5	Configuration Profile 5: "MDF PP Configuration Profile WLAN"	117
11	<i>Appendix B: User Guide Screenshots</i>	120
11.1	Get information about your iPhone	120
11.2	Get information about your iPad	121
11.3	Set up and use Bluetooth accessories on iPhone	123
11.4	Set up and use Bluetooth accessories on iPad	125
11.5	Set a passcode on iPhone	126
11.6	Set a passcode on iPad	128
11.7	Erase iPhone	129
11.8	Erase iPad	130
11.9	Set up Face ID on iPhone	131
11.10	Set up Touch ID on iPhone	133
11.11	Set up Face ID on iPad	134
11.12	Set up Touch ID on iPad	135
11.13	Get apps in the App Store on iPhone	136
11.14	Get apps in the App Store on iPad	138
11.15	Remove apps from iPhone	140
11.16	Remove apps from iPad	141
11.17	Access features from the iPhone Lock screen	142
11.18	Access features from the iPad Lock screen	143

11.19	Change notification settings on iPhone	144
11.20	Change notification settings on iPad	146
11.21	View or change cellular data settings on iPhone	147
11.22	View or change cellular data settings on iPad (Wi-Fi + Cellular models)	149
11.23	Connect iPhone to the internet	151
11.24	Connect iPad to the internet	152
11.25	Share your internet connection from iPhone	153
11.26	Share your internet connection from iPad (Wi-Fi + Cellular)	155
11.27	Ultra Wideband information	157
11.28	Control the location information you share on iPhone	157
11.29	Control the location information you share on iPad	159
11.30	Set up iCloud Drive on iPhone	160
11.31	Set up iCloud Drive on iPad	161
11.32	Update iOS on iPhone	161
11.33	Update iPadOS	162
11.34	Back up iPhone	163
11.35	Back up iPad	165

Table of Tables

Table 1: Guidance Documents	14
Table 2: Mobile Devices Covered by the Evaluation, lists the iPhones that are covered by the VID11237 evaluation.	17
Table 3: Mobile Devices Covered by the Evaluation, lists the iPads that are covered by the VID11238 evaluation.	19
Table 4: SFR Configuration Requirements	33
Table 5: Required Mobile Device Management Functions	38
Table 6: Essential MDM Payload keys for the evaluated configuration	45
Table 7: Essential keys in the Restrictions Payload	46
Table 8: Essential keys for Configuring Cryptographic Functions	50
Table 9: EAP-TLS Ciphersuites	50
Table 10: TLS Ciphersuites	52
Table 11: Essential Payload Keys for TLS and EAP-TLS	57
Table 12: Essential Keys for the VPN Payload	61

Table 13: Essential keys for Data Protection	64
Table 14: Essential keys for Identification and Authentication	73
Table 15: Essential keys for Management functions	85
Table 16: Example audit log	86
Table 17: {MDF} auditable events	90
Table 18: {WLAN} auditable events	92
Table 19: {AGENT} auditable events	96
Table 20: {BT} auditable events	98
Table 21: Additional Audit Logs	102
Table 22: Built-in and Preinstalled Apps	104

1 Revision History

Version	Date	Change
1.2	2022-09-23	Final.

2 Trademarks

Apple's trademarks applicable to this document are listed in <https://www.apple.com/legal/intellectual-property/trademark/appletmlist.html>

Other company, product, and service names may be trademarks or service marks of others.

© Copyright Apple Inc. 2022. All Rights Reserved.

3 Introduction

This document is written for administrators and users of Apple mobile devices that are managed using a mobile device management (MDM) solution. The “Apple iOS 15: iPhones Security Target” [IOS_ST] and “Apple iPadOS 15: iPads Security Target” [IPADOS_ST] include security functional specifications for Wi-Fi, Bluetooth, and virtual private network (VPN) capabilities. This configuration guide applies to both NIAP certifications VID11237 (Apple iOS 15: iPhones) and VID11238 (Apple iPadOS 15: iPads). Where applicable, this guide points out the differences between iPhones and iPads.

According to the [IOS_ST] and the [IPADOS_ST], the evaluated devices are a series of Apple iPhone and iPad mobile devices running the iOS 15 and iPadOS 15 operating systems, respectively. The operating systems manage the mobile device hardware, provide mobile device agent functionality, and provide the technologies required to implement native applications (apps). The operating systems provide a built-in MDM application programming interface (API), giving management features that may be utilized by external MDM solutions and allowing enterprises to use Configuration Profiles to control some of the mobile device settings. The devices provide a consistent set of capabilities allowing for supervision. These capabilities include the preparation of devices for deployment, the subsequent management of the devices, and the termination of management. Some of the Configuration Profiles detailed in this configuration guide are listed in Appendix A: Configuration Profiles.

The devices are expected to be part of an MDM solution that enables the enterprise to control and administer all devices that are part of the enterprise MDM solution.

The devices do not contain any preinstalled third-party apps. The devices do include controls that limit the behavior of installed apps—third-party and other types.

For the user, the operating systems support end users by providing facilities for connectivity using the Wireless LAN radio client and functionality for the management of the Wi-Fi interface. Additionally, the operating systems support end users in an enterprise setting by providing always-on connectivity via an IPsec VPN tunnel to provide secure, reliable access to enterprise assets.

For clarity, the following conventions will be used throughout this document.

- Keys: This document will specify keys or attributes found in Configuration Profiles that will need to be set to certain values to configure the mobile devices into the evaluated configuration. When a key is mentioned, it will be written in the following font: *AlwaysOn*.
- GUI navigation: There are certain configurations or values that can be viewed by navigating to it on the mobile device itself. When instructions for these are mentioned, it will be written in the following font: *Settings » Siri & Search*
- Document sections: In the referenced Apple documentation, the navigation to relevant sections is indicated as: “*Hardware Security and Biometrics*” → “*Touch ID and Face ID*”

3.1 Purpose

This document is intended to provide information for the secure installation and use of the Target of Evaluation (TOE) for the Common Criteria (CC) evaluated configuration of the mobile devices. The TOE is the mobile devices specified in Table 2 and Table 3. Readers of this document may use the term “mobile device” synonymously with the term “TOE.” This guidance is based on the CC requirements and the requirements given in the following documents:

- Protection Profile for Mobile Device Fundamentals, Version 3.2, dated 2021-04-15 [PP_MDF_V3.2] with:
 - PP-Module for MDM Agents, Version 1.0, dated 2019-04-25 [MOD_MDM_AGENT_V1.0]
 - PP-Module for Bluetooth, Version 1.0, dated 2021-04-15 [MOD_BT_V1.0]
 - PP-Module for Virtual Private Network (VPN) Clients, Version 2.3, dated 2021-08-10 [MOD_VPNC_V2.3]
 - Extended Package (EP) for Wireless Local Area Network (WLAN) Clients, Version 1.0, dated 2016-02-08 [PP_WLAN_CLI_EP_V1.0]
 - Functional Package for Transport Layer Security (TLS), Version 1.1, dated 2019-02-12 [PKG_TLS_V1.1]

3.2 TOE Security Functionality

In the evaluated configuration, the mobile devices provide the following security functionality.

- Security audit
- Cryptographic support
- User data protection
- Identification and authentication
- Security management
- Protection of the TOE Security Functionality (TSF)
- TOE access
- Trusted path/channels

3.3 Supporting Apple Documentation

This document provides clarifications to the Apple documentation as related to configuring the mobile devices into the evaluated configuration. Because the purpose of this document is to configure and maintain the mobile devices as per the evaluated configuration, there may be conflicts in the configuration recommendations and usages between this document and other Apple documentation. In such cases, this document has precedence over other Apple documentation. The official Apple documentation should be referred to and followed only as

directed within this document. Table 1: Guidance Documents lists the guidance documents relevant to the configuration and operation of the mobile devices.

Reference	Document Name	Location
Mobile Device Administrator Guidance		
[CCGUIDE]	Apple iOS 15: iPhones and Apple iPadOS 15: iPads Common Criteria Configuration Guide (This document)	https://www.niap-ccevs.org/MMO/Product/st_vid11237-agd.pdf https://www.niap-ccevs.org/MMO/Product/st_vid11238-agd.pdf
[DEV_MAN]	Device Management (online)	https://developer.apple.com/documentation/devicemanagement
Mobile Device User Guidance		
[iPhone_UG]	iPhone User Guide for iOS 15.1 (2021) (This version is no longer available, but screenshots exist in section 11.)	The latest iPhone User Guide: https://support.apple.com/guide/iphone/welcome/ios
[iPad_UG]	iPad User Guide for iPadOS 15.1 (2021) (This version is no longer available, but screenshots exist in section 11.)	The latest iPad User Guide: https://support.apple.com/guide/ipad/welcome/ipados
[PASSCODE_Help] (March 28, 2022)	Use a passcode with your iPhone, iPad, or iPod touch	https://support.apple.com/en-us/HT204060 International: https://support.apple.com/HT204060
[BLUETOOTH_HELP] (November 19, 2021)	Pair a third-party Bluetooth accessory with your iPhone, iPad, or iPod touch	https://support.apple.com/en-us/HT204091 International: https://support.apple.com/HT204091
Mobile Device Management		
[AConfig]	Apple Configurator 2 User Guide (online)	https://support.apple.com/guide/apple-configurator-2/welcome/mac

Reference	Document Name	Location
[ABM_Guide] (April 27, 2022)	Apple Business Manager User Guide	https://support.apple.com/guide/apple-business-manager/welcome/web
[PM_Help]	Profile Manager User Guide for macOS Monterey	https://support.apple.com/guide/profile-manager/welcome/mac
Supporting Documents		
[DeployRef] (June 2022)	Apple Platform Deployment	https://support.apple.com/guide/deployment/welcome/web
[LOGGING]	Logging	https://developer.apple.com/documentation/os/logging?language=objc
[PROFS_LOGS]	Profiles and Logs (applies to both iOS and iPadOS)	https://developer.apple.com/bug-reporting/profiles-and-logs/?platforms=ios
[TRUST_STORE] (September 27, 2021)	List of available trusted root certificates in iOS 15, iPadOS 15, macOS 12, tvOS 15, and watchOS 8	https://support.apple.com/en-us/HT212773 International: https://support.apple.com/HT212773
[MANAGE_CARDS] (December 16, 2021)	Change or remove the payment cards that you use with Apple Pay	https://support.apple.com/en-us/HT205583 International: https://support.apple.com/HT205583
[PAY_SETUP] (March 18, 2022)	Set up Apple Pay	https://support.apple.com/en-us/HT204506 International: https://support.apple.com/HT204506
[CONTENT-CACHING]	Set up content caching on Mac	https://support.apple.com/guide/mac-help/set-up-content-caching-on-mac-mch13b6c3720/12.0/mac/12.0
[APFS_DOC]	File system formats available in Disk Utility on Mac	https://support.apple.com/en-euro/guide/disk-utility/dsku19ed921c/21.0/mac/12.0
App Developer Guidance		

Reference	Document Name	Location
[CKTSREF]	Certificate, Key, and Trust Services	https://developer.apple.com/documentation/security/certificate-key-and-trust-services
[KEYCHAINPG]	Keychain Services (Programming Guide)	https://developer.apple.com/documentation/security/keychain-services
[AP_SEC] (May 2022)	Apple Platform Security	https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf
[APFS_DEV_DOC]	About Apple File System	https://developer.apple.com/documentation/foundation/file_system/about-apple-file-system

Table 1: Guidance Documents

3.4 Evaluated Mobile Devices

Table 2 and Table 3 list the iPhone and iPad devices that are covered by the CC evaluation.

Processor	Device Name	Model Number
iPhones		
A9	iPhone 6s	A1633
		A1688
		A1691 (China)
		A1700 (China)
	iPhone 6s Plus	A1634
		A1687
		A1690 (China)
		A1699 (China)
	iPhone SE	A1662
		A1723 (China)
		A1724 (China)
	A10 Fusion	iPhone 7
A1779 (Japan)		
A1780 (China)		
A1778		
		A1661

Processor	Device Name	Model Number
	iPhone 7 Plus	A1785 (Japan)
		A1786 (China)
		A1784
A11 Bionic	iPhone 8	A1863
		A1906 (Japan)
		A1907
		A1905 (GSM)
	iPhone 8 Plus	A1864
		A1898 (Japan)
		A1899
		A1897 (GSM)
	iPhone X	A1865 (Japan)
		A1902 (Japan)
A1901		
A12 Bionic	iPhone Xs	A1920 (US/CA/HK)
		A2097
		A2098 (Japan)
		A2099 (Global)
		A2100 (China)
	iPhone Xs Max	A1921 (US/CA)
		A2101 (Global)
		A2102 (Japan)
		A2104 (China/HK)
	iPhone XR	A1984 (US/CA)
		A2105 (Global)
		A2106 (Japan)
		A2107 (US/CA)
		A2108 (HK/China)
	A13 Bionic	iPhone 11
A2221		
A2223		
iPhone 11 Pro		A2160
		A2215
		A2217
		A2161

Processor	Device Name	Model Number	
	iPhone 11 Pro Max	A2218	
		A2220	
	iPhone SE (2 nd gen)	A2275 (US/CA)	
		A2298 (China)	
		A2296 (Global)	
	A14 Bionic	iPhone 12 mini	A2176
A2398			
A2399			
A2400			
iPhone 12		A2172	
		A2402	
		A2403	
		A2404	
iPhone 12 Pro		A2341	
		A2406	
		A2407	
		A2408	
iPhone 12 Pro Max		A2342	
		A2410	
		A2411	
		A2412	
A15 Bionic	iPhone 13 mini	A2481	
		A2626	
		A2628	
		A2629	
		A2630	
	iPhone 13	A2482	
		A2631	
		A2633	
		A2634	
		A2635	
	iPhone 13 Pro	A2483	
		A2636	
		A2638	
		A2639	
			A2640
			A2484

Processor	Device Name	Model Number
	iPhone 13 Pro Max	A2641
		A2643
		A2644
		A2645

Table 2: Mobile Devices Covered by the Evaluation, lists the iPhones that are covered by the VID11237 evaluation.

Processor	Device Name	Model Number
iPads		
A9	iPad 9.7-inch (5 th gen)	A1822
		A1823
A9X	iPad Pro 9.7-inch	A1673
		A1674
		A1675
	iPad Pro 12.9-inch	A1584
A1652		
A10 Fusion	iPad 9.7-inch (6 th gen)	A1893
		A1954
	iPad 10.2-inch (7 th gen)	A2197
		A2199
		A2200
A2198 (Hong Kong)		
A10X Fusion	iPad Pro 12.9-inch (2 nd gen)	A1670
		A1671
		A1821 (China)
	iPad Pro 10.5-inch	A1701
		A1709
		A1852 (China)
A12 Bionic	iPad mini (5 th gen)	A2133
		A2125 (China)
		A2124
		A2126
	iPad Air 10.5-inch (3 rd gen)	A2152
		A2154 (China)
		A2123
		A2153
	iPad 10.2-inch (8 th gen)	A2270
		A2428
A2429		
A2430 (China)		
A12X Bionic	iPad Pro 11-inch	A1934 (US/CA)
		A1979 (China)
		A1980

		A2013 (US/CA)
		A2014 (US/CA)
	iPad Pro 12.9 inch (3 rd gen)	A1876
		A1895
		A1983 (China)
A12Z Bionic	iPad Pro 11-inch (2 nd gen)	A2228
		A2231 (China)
		A2230
		A2068
	iPad Pro 12.9-inch (4 th gen)	A2229
		A2069
		A2232
		A2233 (China)
A13 Bionic	iPad 10.2-inch (9 th gen)	A2602
		A2603
		A2604
		A2605
A14 Bionic	iPad Air (4 th gen)	A2316
		A2324 (US/CA)
		A2072 (Global)
		A2325 (China)
A15 Bionic	iPad mini (6 th gen)	A2567
		A2568
		A2569
M1	iPad Pro 11-inch (3 rd gen)	A2301
		A2377
		A2460
	iPad Pro 12.9-inch (5 th gen)	A2378
		A2379
		A2461
		A2462

Table 3: Mobile Devices Covered by the Evaluation, lists the iPads that are covered by the VID11238 evaluation.

3.5 Assumptions

The following assumptions apply when operating the mobile devices in the evaluated configuration. These assumptions must be valid within the organization to maintain security of the mobile devices.

3.5.1 Administrators

- One or more competent, trusted personnel who are not careless, willfully negligent, or hostile are assigned and authorized as the mobile device administrators and do so using and abiding by guidance documentation.
- Device administrators are trusted to follow and apply all administrator guidance in a trusted manner.
- Personnel configuring the mobile device and its operational environment will follow the applicable security configuration guidance.
- Device administrators will configure the mobile device's security functions correctly to create the intended security policy.

3.5.2 Mobile device users

- Mobile device users are not willfully negligent or hostile and use the mobile device within compliance of a reasonable enterprise security policy.
- The mobile device user exercises precautions to reduce the risk of loss or theft of the mobile device.
- The mobile device user will immediately notify the administrator if the mobile device is lost or stolen.
- Physical security, commensurate with the value of the mobile device and the data it contains, is assumed to be provided by the environment.

3.5.3 Network

- The mobile device relies on network connectivity to carry out its management activities. The mobile device will robustly handle instances when connectivity is unavailable or unreliable.
- Information cannot flow between the wireless client and the internal wired network without passing through the TOE.
- Information cannot flow onto the network to which the VPN client's host is connected without passing through the device.

3.5.4 Other

- The MDM Agent relies upon mobile platform and hardware evaluated against the [PP_MDF_V3.2] and assured to provide policy enforcement as well as cryptographic services and data protection. The mobile device platform provides trusted updates and software integrity verification of the MDM Agent.

3.6 Organizational Security Policies

The following requirements are for policies that must be implemented by the deploying organization in support of meeting the security requirements of the [IOS_ST] and the [IPADOS_ST].

- The mobile device administrators must adhere to the organizational security policies.
- The mobile device must be supervised using an MDM solution prior to connecting to the network.
- The mobile device user is held accountable for their actions while using the device.
- The mobile device user must promptly report their lost or stolen device to the mobile device administrator. The mobile device administrator must take appropriate actions using the MDM solution used to manage the mobile device.

3.7 Security Functional Requirements (SFRs) in the STs requiring configuration

In the evaluated configuration, the devices address each SFR in the following table. Table 4: *SFR Configuration Requirements* identifies each SFR specified in the Security Targets [IOS_ST] and the [IPADOS_ST] and provides references to sections within this document for information on the function in the “Related Section” column. The “Configurable?” column denotes if the function needs to or can be configured.

SFR ID	Function Description	Configurable?	Related Section
FAU_ALT_EXT.2 {AGENT}	Agent Alerts	No	Section 4.3.5
FAU_GEN.1 {MDF} {WLAN}	Audit Data Generation	Yes	Section 6.1
FAU_GEN.1.2 {MDF} {WLAN}	Audit Data Generation	Yes	Section 6.1
FAU_GEN.1.1(2) {AGENT}	Audit Data Generation	Yes	Section 6.1
FAU_GEN.1.2(2) {AGENT}	Audit Data Generation	Yes	Section 6.1
FAU_GEN.1.1/BT {BT}	Audit Data Generation	Yes	Section 6.1
FAU_GEN.1.2/BT {BT}	Audit Data Generation	Yes	Section 6.1
FAU_SEL.1(2) {AGENT}	Security Audit Event Selection	Yes	Section 6.2, Section 6.3

SFR ID	Function Description	Configurable?	Related Section
FAU_STG.1 {MDF}	Audit Storage Protection	No: Audit records are not accessible to device Administrators or Users and must be viewed on a trusted workstation or MDM server.	Section 6.2
FAU_STG.4 {MDF}	Prevention of Audit Data Loss	No: The default behavior is to overwrite the oldest entry.	Section 6.2
FCS_CKM.1 {MDF} {VPN}	Cryptographic Key Generation	No: The API allows specification of the requested key sizes and key types.	Section 5.2.1
FCS_CKM.1/WLAN {WLAN}	WLAN Cryptographic Key Generation (Symmetric Keys for WPA2 Connections)	No: Wireless LAN (WLAN) keys are generated for the cipher suite offered by the access point.	N/A
FCS_CKM.1/VPN {VPN}	VPN Cryptographic Key Generation (IKE)	No: IKEv2 is an available option. The API allows for the specification of the key size and key types.	Section 5.3.6
FCS_CKM.2/UNLOCKED {MDF} {VPN}	Cryptographic Key Establishment	No: The API allows specification of the requested key sizes and key types.	Section 5.2.2
FCS_CKM.2/LOCKED {MDF}	Cryptographic Key Establishment (While device is locked)	No: Key establishment is hard coded.	Section 5.2.2
FCS_CKM.2/WLAN {WLAN}	WLAN Cryptographic Key Distribution (GTK)	No: The WLAN protocol is implemented according to IEEE 802.11 2012.	N/A

SFR ID	Function Description	Configurable?	Related Section
FCS_CKM_EXT.1 {MDF}	Cryptographic Key Support (REK)	No: REK is permanently etched in silicon and is both unmodifiable as well as inaccessible by iOS/iPadOS and apps.	N/A
FCS_CKM_EXT.2 {MDF}	Cryptographic Key Random Generation (DEK)	No: Generation and maintenance of DEK are hard coded.	N/A
FCS_CKM_EXT.3 {MDF}	Cryptographic Key Generation (KEK)	No: Generation and maintenance of KEK are hard coded.	N/A
FCS_CKM_EXT.4 {MDF} {WLAN}	Key Destruction	No: Zeroization of keys is hard coded.	N/A
FCS_CKM_EXT.5 {MDF}	TSF Wipe	Yes	Section 5.4.1 – How to enable encryption. Section 5.4.3 – How to wipe the device.
FCS_CKM_EXT.6 {MDF}	Salt Generation	No: Generation and maintenance of Salt are hard coded.	N/A
FCS_CKM_EXT.7 {MDF}	Cryptographic Key Support (REK)	No: REK is permanently etched in silicon and is both unmodifiable as well as inaccessible by iOS/iPadOS and apps.	N/A
FCS_CKM_EXT.8 {BT}	Bluetooth Key Generation	No: ECDH key pairs are generated for each new connection attempt.	N/A
FCS_COP.1/ENCRYPT {MDF} {VPN}	Confidentiality Algorithms	No: For AES operations performed by the TSF. No: For AES operations performed by a third party where the API allows specification of the AES cipher type	Section 5.2.6

SFR ID	Function Description	Configurable?	Related Section
FCS_COP.1/HASH {MDF}	Hashing Algorithms	<p>No: For hash operations performed by the TSF for TLS.</p> <p>Yes: For hash operations performed for VPN</p> <p>No: For hash operations performed by a third party where the API allows specification of the hash cipher type.</p>	Section 5.2.3
FCS_COP.1/SIGN {MDF}	Signature Algorithms	<p>No: For signature operations performed by TSF.</p> <p>No: For signature operations performed by a third party where the API allows specification of the hash cipher type.</p>	Section 5.2.1
FCS_COP.1/KEYHMAC {MDF}	Keyed Hash Algorithms	<p>No: For HMAC operations performed by TSF</p> <p>No: For HMAC operations performed by a third party where the API allows specification of the hash cipher type.</p>	Section 5.2.3
FCS_COP.1/CONDITION {MDF}	Password-Based Key Derivation Functions	No: Generation and maintenance of PBKDF are hard coded.	N/A

SFR ID	Function Description	Configurable?	Related Section
FCS_HTTPS_EXT.1 {MDF}	HTTPS protocol	No: The used HTTPS cipher suite is defined by the HTTPS server where all cipher suites listed in the [IOS_ST] and the [IPADOS_ST] are always available.	Section 5.3.2
FCS_IPSEC_EXT.1 {VPN}	IPsec	Yes	Section 5.3.5, Section 5.3.3
FCS_IV_EXT.1 {MDF}	Initialization Vector Generation	No: Generation and maintenance of IVs are hard coded.	N/A
FCS_RBG_EXT.1 {MDF} ("Kernel and User space" and SEP iterations.)	Cryptographic Operation (Random Bit Generation)	No: Generation of random numbers is hard coded.	Section 5.2.4
FCS_SRV_EXT.1 {MDF}	Cryptographic Algorithm Services	No	Section 5.2
FCS_STG_EXT.1 {MDF}	Secure Key Storage	No	Section 5.6.13
FCS_STG_EXT.2 {MDF}	Encrypted Cryptographic Key Storage DEK and KEK encryption	No: Generation and maintenance of DEK and KEK are hard coded.	N/A
FCS_STG_EXT.3 {MDF}	Integrity of Encrypted Key Storage	No: Generation and maintenance of DEK and KEK are hard coded.	N/A
FCS_STG_EXT.4 {AGENT}	Cryptographic Key Storage	No	N/A
FCS_TLS_EXT.1 {TLS}	TLS Protocol	Yes	Section 5.3.2
FCS_TLSC_EXT.1 {TLS}	TLS Client Protocol	Yes	Section 5.3.2

SFR ID	Function Description	Configurable?	Related Section
FCS_TLSC_EXT.1/WLAN {WLAN}	Extensible Authentication Protocol-Transport Layer Security (EAP-TLS)	No: Used TLS cipher suites are defined by the TLS server where all cipher suites listed in the [IOS_ST] and the [IPADOS_ST] are always available. The API of the third-party application defines specific TLS protocol rules.	Section 5.3.1
FCS_TLSC_EXT.2 {TLS}	TLS Client Protocol for Mutual Authentication	No	Section 5.3.2
FCS_TLSC_EXT.4 {TLS}	TLS Client Support for Renegotiation	No	N/A
FCS_TLSC_EXT.5 {TLS}	TLS Client Support for Supported Groups Extension	No	N/A
FDP_ACF_EXT.1 {MDF}	Access Control for System Services	No: Access control settings are hard coded.	N/A
FDP_ACF_EXT.2 {MDF}	Access Control for System Resources	No	N/A
FDP_DAR_EXT.1 {MDF}	Protected Data Encryption	No: Data is always encrypted. TSF is hard coded to use the appropriate data protection levels based on classes. External storage must be formatted in the AFPS format with encrypted volumes. Unencrypted external storage is not allowed in the evaluated configuration.	Section 5.4

SFR ID	Function Description	Configurable?	Related Section
FDP_DAR_EXT.2 {MDF}	Sensitive Data Encryption	No: Data is always encrypted. TSF is hard coded to use the appropriate data protection level based on classes. External storage must be formatted in the AFPS format with encrypted volumes. Unencrypted external storage is not allowed in the evaluated configuration.	Section 5.4
FDP_IFC_EXT.1 {MDF} {VPN}	Subset Information Flow Control	Yes	Section 5.3.5, Section 5.3.3
FDP_IFC_EXT.1/VPN {VPN}	Subset Information Flow Control	Yes	Section 5.3.5
FDP_PBA_EXT.1 {MDF}	Storage of Critical Biometric Parameters	No	N/A
FDP_RIP.2 {VPN}	Full Residual Information Protection	No	N/A
FDP_STG_EXT.1 {MDF}	User Data Storage	No: The trust anchor database maintenance is hard coded. The mobile device administrator can add/remove their own Anchors of Trust to/from that database.	Section 5.5.6
FDP_UPC_EXT.1/APPS {MDF}	Inter-TSF User Data Transfer Protection (Applications)	Yes: Depending on the protocol used, configuration is possible (e.g., IPsec) while other options are not configurable	FTP_ITC_EXT.1 (Section 5.3) FCS_TLSC_EXT.1 (Section 5.3.2) FCS_IPSEC_EXT.1 (Section 5.3.5) FCS_HTTPS_EXT.1 (Section 5.3.2)

SFR ID	Function Description	Configurable?	Related Section
FDP_UPC_EXT.1/BLUETOOTH {MDF}	Inter-TSF User Data Transfer Protection (Bluetooth)	No: Only enable/disable of Bluetooth is supported.	Section 5.3.4
FIA_AFL_EXT.1 {MDF}	Authentication Failure Handling	Yes	Section 5.5.4
FIA_BLT_EXT.1 {BT}	Bluetooth User Authorization	No: The Bluetooth protocol allows different types of authorization that are supported by the mobile device. The used authorization type depends on the remote device capability.	Section 5.3.4
FIA_BLT_EXT.2 {BT}	Bluetooth Mutual Authentication	No: Bluetooth mutual authentication is required prior to data transfer.	Section 5.3.4
FIA_BLT_EXT.3 {BT}	Rejection of Duplicate Bluetooth Connections	No: No mobile device can establish duplicative Bluetooth connections.	N/A
FIA_BLT_EXT.4 {BT}	Secure Simple Pairing	No: Secure simple pairing cannot be disabled.	Section 5.3.4
FIA_BLT_EXT.6 {BT}	Trusted Bluetooth Device User Authorization	No	N/A
FIA_BLT_EXT.7 {BT}	Untrusted Bluetooth Device User Authorization	No	N/A
FIA_BMG_EXT.1 {MDF}	Accuracy of Biometric Authentication	No	N/A
FIA_BMG_EXT.2 {MDF}	Biometric Enrollment	No	Section 5.5.3
FIA_BMG_EXT.3 {MDF}	Biometric Verification	No	Section 5.5.3

SFR ID	Function Description	Configurable?	Related Section
FIA_BMG_EXT.5 {MDF}	Handling Unusual Biometric Templates	No	N/A
FIA_ENR_EXT.2 {AGENT}	Enrollment of Mobile Device into Management	Yes	Section 4.3.1
FIA_PAE_EXT.1 {WLAN}	Port Access Entity (PAE) Authentication	No: The WLAN protocol is implemented according to IEEE 802.11 2012.	N/A
FIA_PMG_EXT.1 {MDF}	Password Management	Yes	Section 5.5.1
FIA_TRT_EXT.1 {MDF}	Authentication Throttling	No: The authentication delay is hard coded.	N/A
FIA_UAU.5.1 {MDF}	Multiple Authentication Mechanisms	Yes	Section 5.5
FIA_UAU.5.2 {MDF}	Multiple Authentication Mechanisms	Yes	Section 5.5
FIA_UAU.6.1 {MDF}	Re-Authentication	No: Users must be re-authenticated before any changes to the password authentication factor can be made.	Section 5.5.5
FIA_UAU.6.2 {MDF}	Re-Authentication (Locked)	No	Section 5.5.5
FIA_UAU.7 {MDF}	Protected Authentication Feedback	No: Enabled by default.	Section 5.5.2
FIA_UAU_EXT.1 {MDF}	Authentication for Cryptographic Operations	Yes: The mobile device user must set a passphrase to enable authentication token protection.	Section 5.5.1
FIA_UAU_EXT.2.1 {MDF}	Timing of Authentication	No	Section 5.6.2

SFR ID	Function Description	Configurable?	Related Section
FIA_UAU_EXT.2.2 {MDF}	Timing of Authentication	No	Section 5.6.2
FIA_X509_EXT.1 {MDF}	Validation of Certificates	No: The certificate validation rules are hard coded.	N/A
FIA_X509_EXT.1/WLAN {WLAN}	X509 Certificate Validation (EAP-TLS)	Yes	Section 5.3, Section 5.5.6
FIA_X509_EXT.2 {MDF} {VPN}	X509 Certificate Authentication	Yes: The certificates required for authentication must be provided. Note that some root certificates are provided in the Apple Trust store.	Section 5.3, 5.5.6
FIA_X509_EXT.2/WLAN {WLAN}	X509 Certificate Authentication (EAP-TLS)	Yes	Section 5.5.6
FIA_X509_EXT.3 {MDF}	Request Validation of Certificates	No: The API is provided with certificate validation rules hard coded.	Section 5.5.6
FMT_MOF_EXT.1 {MDF}	Management of Security Functions Behavior	Yes	Section 3.8
FMT_POL_EXT.2 {AGENT}	Trusted Policy Update	No	N/A
FMT_SMF_EXT.1 {MDF} {VPN}	Specification of Management Functions	Yes	Section 3.8
FMT_SMF_EXT.1/BT {BT}	Specification of Management Functions	Yes	Section 5.3.4
FMT_SMF_EXT.1/ WLAN {WLAN}	Specification of Management Functions (WLAN)	Yes	Section 3.8
FMT_SMF.1/VPN {VPN}	Specification of Management Functions (VPN)	Yes	Section 3.8

SFR ID	Function Description	Configurable?	Related Section
FMT_SMF_EXT.2 {MDF}	Specification of Remediation Actions	Yes	Section 4.3.4, 5.4.3
FMT_SMF_EXT.4 {AGENT}	Specification of Management Functions (Agent)	No	N/A
FMT_UNR_EXT.1 {AGENT}	User Unenrollment Prevention	Yes	Section 4.3.4
FPT_AEX_EXT.1 {MDF}	Anti-Exploitation Services (ASLR)	No: The service is hard coded.	N/A
FPT_AEX_EXT.2 {MDF}	Anti-Exploitation Services (Memory Page Permissions)	No: The service is hard coded.	N/A
FPT_AEX_EXT.3 {MDF}	Anti-Exploitation Services (Overflow Protection)	No: The service is hard coded.	N/A
FPT_AEX_EXT.4 {MDF}	Domain Isolation	No: The service is hard coded.	N/A
FPT_JTA_EXT.1 {MDF}	JTAG Disablement	No: JTAG interfaces are not present on iOS/iPadOS devices.	N/A
FPT_KST_EXT.1 {MDF}	Key Storage	No: Keys are stored in secure enclave or in key chain. Wrapped keys are stored in Effaceable Storage.	N/A
FPT_KST_EXT.2 {MDF}	No Key Transmission	No: Keys are stored in secure enclave or in key chain.	N/A
FPT_KST_EXT.3 {MDF}	No Plaintext Key Export	No: Keys are stored in secure enclave that does not provide key export facility. The mobile device does not export keys stored in key chain.	N/A
FPT_NOT_EXT.1 {MDF}	Self-Test Notification	No	N/A
FPT_STM.1 {MDF}	Reliable Time Stamps	Yes	Section 5.6.4

SFR ID	Function Description	Configurable?	Related Section
FPT_TST_EXT.1 {MDF}	TSF Cryptographic Functionality Testing	No	Section 5.2
FPT_TST_EXT.1/VPN {VPN}	TSF Self-Test (VPN)	No	Section 5.2
FPT_TST_EXT.1/ WLAN {WLAN}	TSF Cryptographic Functionality Testing (WLAN)	No	Section 5.2
FPT_TST_EXT.2/PREKERNEL {MDF}	TSF Integrity Checking (Pre-Kernel)	No	N/A
FPT_TST_EXT.2/POSTKERNEL {MDF}	TSF Integrity Checking (Post-Kernel)	No	N/A
FPT_TST_EXT.3 {MDF}	TSF Integrity Testing	No	Section 5.5.6
FPT_TUD_EXT.1 {MDF}	Trusted Update: TSF Version Query	No	N/A
FPT_TUD_EXT.2 {MDF}	Trusted Update Verification	No	N/A
FPT_TUD_EXT.3 {MDF}	Application Signing	No	Section 5.6.10
FPT_TUD_EXT.4 {MDF}	Trusted Update Verification	No	Section 5.6.10
FPT_TUD_EXT.5 {MDF}	Application Verification	No	N/A
FPT_TUD_EXT.6 {MDF}	Trusted Update Verification	No	N/A
FTA_SSL_EXT.1 {MDF}	TSF and User-initiated Locked State	Yes	Section 5.6.3
FTA_TAB.1 {MDF}	Default TOE Access Banners	Yes	Section 5.6.5
FTA_WSE_EXT.1 {WLAN}	Wireless Network Access	Yes	Section 5.6.7
FTP_BLT_EXT.1 {BT}	Bluetooth Encryption	No: Enforced by default.	Section 5.3.4
FTP_BLT_EXT.2 {BT}	Persistence of Bluetooth Encryption	No	Section 5.3.4

SFR ID	Function Description	Configurable?	Related Section
FTP_BLT_EXT.3/BR {BT}	Bluetooth Encryption Parameters (BR/EDR)	No	Section 5.3.4
FTP_BLT_EXT.3/LE {BT}	Bluetooth Encryption Parameters (LE)	No	Section 5.3.4
FTP_ITC_EXT.1 {MDF} {VPN}	Trusted Channel Communication	Yes	Section 5.3
FTP_ITC_EXT.1(2) {AGENT}	Trusted Channel Communication	Yes	Section 5.3
FTP_ITC_EXT.1/WLAN {WLAN}	Trusted Channel Communication	Yes	Section 5.3
FTP_TRP.1(2) {AGENT}	Trusted Path (for Enrollment)	Yes	Section 5.3

Table 4: SFR Configuration Requirements

3.8 Security Management Configuration

In the evaluated configuration, the mobile devices perform the management functions listed in Table 5: Required Mobile Device Management Functions.

These management functions can be managed either by the mobile device user or by an authorized mobile device administrator (marked by 'X').

In addition, the Provided Guidance column references the section(s) in this document where guidance can be found to perform the respective management function. The management function values in parenthesis (e.g., F1, F2) in the following table correspond to the function values specified in the [IOS_ST] and the [IPADOS_ST] Table 6 plus the additional management functions specific to Bluetooth, Wi-Fi, and VPN management functionality also specified in the [IOS_ST] and the [IPADOS_ST].

Management Function	Restricted to the User	Administrator	Restricted to the Administrator	Provided Guidance
MDF (FMT_SMF_EXT.1)				
Configure password policy (F1)	-	X	X	Section 5.5.1
Configure session locking policy (F2)	-	X	X	Sections 5.6.3

Management Function	Restricted to the User	Administrator	Restricted to the Administrator	Provided Guidance
Enable/disable the VPN protection (F3)	-	X	-	Sections 5.3.5
Enable/disable Bluetooth, Wi-Fi, cellular radio, NFC, UWB ¹ (F4)	-	X	-	Section 5.6.7
Enable/disable cameras (F5)	-	X	-	Section 5.6.6
Transition to the locked state (F6)	-	X	-	Section 5.6.3
TSF wipe of protected data (F7)	-	X	-	Section 5.4.3
Configure application installation policy by denying installation of applications (F8)	-	X	X	Section 5.6.12
Import keys/secrets into the secure key storage (F9)	-	X	-	Section 5.2.5
Destroy imported keys/secrets and no other keys/secrets in the secure key storage (F10)	-	X	-	Section 5.2.5
Import X.509v3 certificates in the Trust Anchor Database (F11)	-	X	X	Section 5.5.6

¹ NFC and UWB only apply to devices supporting these radios.

Management Function	Restricted to the User	Administrator	Restricted to the Administrator	Provided Guidance
Remove imported X509v3 certificates and no other X509v3 certificates in the Trust Anchor Database (F12)	-	X	-	Section 5.5.6
Enroll the TOE in management (F13)	X	-	-	Section 4.3.1
Remove applications (F14)	-	X	X	Section 5.6.1
Update system software (F15)	-	X	-	Section 5.6
Install applications (F16)	-	X	X	Section 5.6.1
Remove Enterprise applications (F17)	-	X	-	Section 5.6.1
Enable/disable display notifications in the locked state of all notifications (F18)	-	X	-	Section 5.6.2
Enable data-at-rest protection (F19)	-	-	-	Section 5.4.1
Enable removable media's data-at-rest protection (F20)	-	X	X	Section 5.4.1
Enable/disable location services (across device and on a per-app basis) (F21)	-	X	-	Section 5.6.8

Management Function	Restricted to the User	Administrator	Restricted to the Administrator	Provided Guidance
Enable/disable the use of Biometric Authentication Factor (F22)	-	X	X	Section 5.5.3
Configure whether to allow/disallow establishment of a trusted channel if the peer/server certificate is deemed invalid. (F23)	X	-	-	Section 5.5.6.3
Wipe Enterprise data (F28)	-	X	-	Section 5.4.3
Configure whether to establish a trusted channel or disallow establishment if the TSF cannot establish a connection to determine the validity of a certificate (F30)	-	X	-	Section 5.5.6
Configure the unlock banner (F36)	-	X	X	Section 5.6.5
Configure the auditable items (F37)	-	X	-	Section 6.3
Unenroll the TOE from management (F44)	-	X	-	Section 4.3.4
Enable/disable the Always On VPN protection (F45)	-	X	X	Section 5.3.5
Enable/disable microphones on a per-app basis (F47)	-	X	-	Section 5.6.6

Management Function	Restricted to the User	Administrator	Restricted to the Administrator	Provided Guidance
Bluetooth (FMT_SMF_EXT.1/BT)				
Configure the Bluetooth trusted channel.				
Disable/enable the Discoverable (for BR/EDR) and Advertising (for LE) modes (FBT-1)	X	-	-	Section 5.3.4
Wi-Fi (FMT_SMF_EXT.1/WLAN)				
Configure security policy for Wi-Fi network	-	X	X	Section 5.3.6
Specify the CA(s) from which the TSF will accept WLAN authentication server certificates(s)	-	X	X	Section 5.3.6
Specify Wi-Fi security type	-	X	X	Section 5.3.6
Specify authentication protocol for Wi-Fi	-	X	X	Section 5.3.6
Specify client credentials used for Wi-Fi authentication	-	X	X	Section 5.3.6
Specify wireless networks (SSIDs) to which the TSF may connect	-	X	X	Section 5.3.5.3
VPN (FMT_SMF.1/VPN)				
Specify VPN gateways to use for connection	-	X	X	Section 5.3.6
Specify client credentials for connections	-	X	X	Section 5.3.6
Configure the reference identifier of the peer	-	X	X	Section 5.3.6

Management Function	Restricted to the User	Administrator	Restricted to the Administrator	Provided Guidance
Configure IKE protocol version(s) used	-	X	X	Section 5.3.6
Configure IKE authentication techniques used	-	X	X	Section 5.3.6
Configure cryptoperiod for established session keys	-	X	X	Section 5.3.6
Configure certificate revocation check	-	X	X	Section 5.3.6
Specify the algorithm suites that may be proposed and accepted during the IPsec exchanges	-	X	X	Section 5.3.6
Load X.509v3 certificates for VPN security functions	-	X	X	Section 5.3.6
Update TOE and verify updates	-	X	X	Section 5.3.6
Configure all security management functions identified in other sections of [MOD_VPNC_V2.3]	(See F45 in this table)	(See F45 in this table)	(See F45 in this table)	(See F45 in this table)

Table 5: Required Mobile Device Management Functions

3.9 Un-evaluated Functionalities

The following security functionalities were not evaluated and are, therefore, excluded from the secure configuration of the mobile devices.

3.9.1 Two-Factor Authentication

Two-factor authentication is an extra layer of security for an Apple ID used in the Apple store, iCloud, and other Apple services. It is designed to enhance the security on these online Apple accounts.

This feature is outside the scope of the evaluation.

3.9.2 Bonjour

Bonjour is Apple's standards-based, zero-configuration network protocol that lets devices find services on a network.

This feature is outside the scope of the evaluation.

3.9.3 VPN Split Tunnel

VPN split tunnel is not included in the evaluation and must be disabled in the mobile device configurations meeting the requirements of this CC evaluation.

While VPN split tunnel is not included, in the evaluated configuration, the VPN must be in its Always-On configuration. See section 5.3.5 VPN Configuration for more information.

3.9.4 Siri Interface

The Siri interface supports some commands related to configuration settings.

This feature is not included in the evaluation and must be disabled in the mobile device configurations that meet the requirements of this CC evaluation.

3.9.5 Shared iPad for education

Apple offers the ability to configure the iPad devices for multiple users. This configuration was not included in the evaluation and must not be used in the mobile device configurations that meet the requirements of this CC evaluation.

3.9.6 Third-party MDM Agents

Some third-party applications are available that provide functionality as a mobile device MDM Agent. No third-party MDM Agent applications were included in the evaluation and are outside the scope of the evaluated configuration.

3.9.7 VPN Protocols and Authentication Methods

The following Virtual Private Network (VPN) protocols are not included in the evaluation and must be disabled in the mobile device configurations that meet the requirements of this CC evaluation.

- Cisco IPsec
- Layer Two Tunneling Protocol (L2TP) over IPsec
- Secure Sockets Layer (SSL) VPN
- Shared secret authentication

4 Secure Delivery and Installation

4.1 Prerequisites

Prior to deploying the mobile device(s) onto the network, an MDM solution must be architected and deployed. The MDM solution will support the mobile device administrator in configuring and managing the mobile devices. There are various MDM solutions that can be used to achieve this.

A VPN gateway supporting IPsec and the necessary VPN settings discussed below must be architected and deployed. The VPN infrastructure will support secure communication with the devices. If the devices will be utilizing x509 certificates for authenticating to the VPN connection, then a public key infrastructure (PKI) system will need to be deployed by the organization which includes a certificate authority (CA) trusted both by the VPN gateway and the device, and an Online Certificate Status Protocol (OCSP) responder or published certificate revocation list (CRL) to service revocation checking requests.

4.2 Secure Delivery of the Devices

The evaluated mobile devices are intended for authorized mobile device users of entities such as business organizations and government agencies.

The mobile device administrator of the devices is responsible for performing the necessary configuration to ensure that the mobile devices are configured as specified by the evaluation.

4.2.1 Obtaining the mobile device(s)

To obtain a device listed in Table 2 and Table 3, follow the directions for the distribution channel that best fits your situation.

The normal distribution channels for obtaining these devices include the following.

- The Apple Store (either a physical store or online at <https://apple.com>)
- Apple retailers
- Service carriers (e.g., AT&T, Verizon)
- Resellers

Business-specific distribution channel

There is a distinct online store for Business customers with a link from the "Apple Store" to Apple and Business: (<https://www.apple.com/business/>). Additionally, the following link to "Shop for Business" is provided (<https://www.apple.com/retail/business/>).

Government-specific distribution channel

Government customers can use the link: <https://www.apple.com/r/store/government/>

Additional

Large customers can have their own Apple Store Catalog for their employees to purchase devices directly from Apple under their corporate employee purchase program.

4.2.2 Verifying the device(s)

When the mobile devices are received, the model number of the devices should be verified to ensure that the model number is one of those listed in Table 2 and Table 3. This can be accomplished using any of the following methods.

- Physically checking the back of the mobile devices.
- Once authenticated to the mobile device, the information is available to mobile device users in *Settings* » *General* » *About* under the “Model Number” entry.
- Mobile device administrators can query the mobile devices using the Mobile Device Management (MDM) protocol described in [DeployRef] under “MDM settings.” The Results Payload from the mobile device provides the requested information.
- Also see the following Apple support webpages.
 - a. <https://support.apple.com/en-us/HT208200>
 - b. <https://support.apple.com/en-us/HT201471>

The iOS/iPadOS version of the devices, which must be a version of iOS/iPadOS 15, should also be verified. This can be accomplished using either of the following methods.

- A mobile device user can obtain information about the iOS/iPadOS software on the mobile device by following these instructions. (Sections 11.1 and 11.2 contain screenshots from these documents.)
 - [iPhone_UG]: “Basics” → “Get information about your iPhone”
 - [iPad_UG]: “Basics” → “Get information about your iPad”
- Mobile device administrators can query the mobile devices using the MDM protocol described in [DeployRef] under “MDM settings.” The Results Payload from the mobile device provides the requested information.

4.3 Mobile Device Supervision and Configuration

In order to ensure that the devices are configured in a way that meets the requirements of this Common Criteria evaluation, the devices must be placed under management (supervised mode).

Once in supervised mode, the mobile devices are typically managed using an MDM solution. The process for doing this will vary based on the MDM solution chosen by the organization deploying the devices, and it is up to the mobile device administrator to determine the detailed steps as they apply to the organization’s chosen MDM solution. The mobile devices are configured through the use of Configuration Profiles that are specified by the mobile device administrator and deployed to the mobile devices.

4.3.1 Mobile Device Enrollment into Management Configuration

iOS/iPadOS natively includes an MDM agent. Mobile device users and/or device administrators can enroll the mobile device in management. Information for enrolling the mobile device is provided in the following document and section.

[DeployRef]: “[MDM settings](#)”

The MDM server identity is provided to the mobile device by sending an MDM payload in a Configuration Profile. Examples of Configuration Profiles can be found in Appendix A: Configuration Profiles.

The methods by which the mobile device can be enrolled for management are as follows.

- Using the Apple Business Manager (ABM), which provides an automated and enforced method of automatically enrolling new devices
- Using Apple’s Profile Manager, which provides a manual method of enrolling mobile devices
- Using the Apple Configurator 2, which provides both automated and manual methods of enrolling mobile devices
- Using Email or a Website, which provides a way to distribute an enrollment profile to a mobile device

4.3.1.1 Apple Business Manager

For the Apple Business Manager (ABM), each MDM server must be registered with Apple at the ABM management portal, which is made available by Apple at <https://business.apple.com>.

The ABM provides details about the server entity to identify it uniquely throughout the organization deploying the MDM server. Each server can be identified by either its system-generated universally unique identifier (UUID) or by a user-provided name assigned by one of the organization’s users. Both the UUID and server name must be unique within the organization.

The organization assigns iOS/iPadOS devices to Apple’s virtual MDM server using either Apple order numbers or device serial numbers. When the iOS/iPadOS device is powered on, the mobile device will automatically connect to the virtual MDM server during setup and will be assigned to the MDM server specified in the MDM payload sent by the virtual MDM server to the iOS/iPadOS device.

During the mobile device enrollment, the MDM enrollment service returns a JavaScript Object Notation (JSON) dictionary to the mobile device with the keys shown in Table 6: Essential MDM Payload.

Additional information on the ABM is provided in the [ABM_Guide]. Additional information on managing mobile devices is provided in [DeployRef] and [DEV_MAN].

4.3.1.2 Apple Profile Manager

For enrolling a device using Apple's Profile Manager, see the following document and section.

[PM_Help]: ["Mobile device management"](#)

4.3.1.3 Apple Configurator

For enrolling a device using the Apple Configurator 2, see the following document and sections.

[AConfig]: ["Automated device management"](#) → ["Automated device configuration"](#)

[AConfig]: ["Automated device management"](#) → ["Automated Device Enrollment"](#)

[AConfig]: ["Manually prepare devices"](#)

4.3.1.4 Other Methods

Other methods of enrollment may be specific to the MDM application being used by a deploying organization. In general, the Configuration Profile is made available to the mobile device often through a link provided on a website or by email to the mobile device user. Once the mobile device user clicks the link, the enrollment process is started.

4.3.2 Mobile Device Configuration

Many aspects of the security functionality of the mobile devices are configured using Configuration Profiles that are installed on the mobile devices. Configuration Profiles are Extensible Markup Language (XML) files that allow the distribution of configuration information to mobile devices. They may contain settings for a number of configurable parameters on the mobile device.

Configuration Profiles can be deployed in any one of the following ways.

- Using the Apple Configurator 2 tool, available from the Apple Store
- Via an email message
- Via a web page
- Using over-the-air configuration
- Using over-the-air configuration via an MDM application

iOS/iPadOS supports using encryption to protect the contents of Configuration Profiles, and Configuration Profiles can also be signed to guarantee data integrity.

Within a Configuration Profile, various Keys are used to specify the desired configuration. These are organized by topic into groups called "Payloads."

Detailed information on Configuration Profiles is given in the Device Management [DEV_MAN] document, and information on some of the Configuration Profiles used in this configuration guide can be found in Appendix A: Configuration Profiles.

The following mandatory configurations must be configured using Configuration Profiles.

4.3.3 Configure MDM Agent and MDM Communications

MDM Agent-Server communication is achieved securely using the MDM protocol, which is built on top of HTTP, transport layer security (TLS), and push notifications that use HTTP PUT over TLS (secure sockets layer (SSL)). A managed mobile device uses an identity to authenticate itself to the MDM server over TLS (SSL). This identity can be included in the profile as a Certificates Payload or can be generated by enrolling the mobile device with Simple Certificate Enrollment Protocol (SCEP).

The MDM Agent communications use the iOS/iPadOS Security Framework as described in section 5.3.2 TLS Configuration. Configuring the device's TLS protocol automatically configures the MDM Agent communications. If an additional CA certificate needs to be added to support the MDM Server, see section 5.3.2.3.

4.3.4 Device Unenrollment Prevention

During the enrollment process, a Configuration Profile including an MDM Payload is loaded onto the mobile device and used to associate the mobile device to an MDM Server. If the MDM Payload is removed, the mobile device will no longer be enrolled with the MDM server and can no longer be considered to be in the evaluated configuration.

As described in [DEV_MAN], the mobile device administrator can specify the *PayloadRemovalDisallowed* key to allow or disallow the ability of a mobile device user to remove the MDM Payload from the device.

The mobile device must be in Supervised Mode to lock the MDM Payload to the device.

An MDM Payload can have a removal password associated with it. If the *PayloadRemovalDisallowed* key is set to prevent unenrollment and the MDM Payload has a removal password associated with it, the mobile device user can unenroll the mobile device only if the mobile device user knows the removal password. The *PayloadRemovalDisallowed* key is described in the following document and section.

[DEV_MAN]: ["Profile-Specific Payload Keys"](#) → ["TopLevel"](#) → ["TopLevel"](#)

In the evaluated configuration, the TOE must be configured to disallow (prevent) unenrollment. If the administrator has allowed the ability for a mobile device user to unenroll the device, the user can remove the profile from the device by choosing [Settings](#) » [General](#) » [Profile & Device Management](#), selecting the appropriate profile, and removing the profile.

4.3.5 MDM Agent Alerts

The iOS/iPadOS MDM Agent generates and sends an alert in response to an MDM server request for applying a Configuration Profile and in response to receiving a reachability event. These responses are always enabled.

When the application of a Configuration Profile to a mobile device is successful, the MDM Agent replies with an MDM Result Payload with Status value "Acknowledged".

When the application of a Configuration Profile is unsuccessful, the MDM Agent replies with an MDM Result Payload with Status value "Error" or *CommandFormatError*, "Idle", and "NotNow".

[DEV_MAN]: [“Implementing Device Management”](#) → [“Sending MDM Commands to a Device”](#) → [“Execute the Command and Report Results”](#)

When a reachability event is received by the iOS/iPadOS MDM Agent, the MDM Agent replies with an MDM Result Payload to acknowledge that the mobile device received the event.

More information on the MDM Result Payloads is found in [DeployRef] and [DEV_MAN].

4.3.6 The MDM Payload

The Mobile Device Management (MDM) Payload, a simple property list, is designated by the “com.apple.mdm” value in the PayloadType field.

Payload	Key	Setting
MDM	<i>PayloadRemovalDisallowed</i>	Must be set to true
MDM	<i>AccessRights</i>	Must be set to a value that includes the logical OR with the value 8.

Table 6: Essential MDM Payload keys for the evaluated configuration

5 Mobile Device Configuration

This section provides more detailed guidance to configure the supervised mobile devices in the way that conforms to the requirements of the CC evaluation.

This section provides details of the dictionary key values that must be used, or where certain options for the key value are not allowed, in order to meet the requirements of the evaluated configuration described in the [IOS_ST] and the [IPADOS_ST].

For dictionary keys not mentioned in this document, please refer to the deploying organization's security policies.

5.1 General Restrictions

5.1.1 Keys for General Restrictions

Below are the essential keys in the Restrictions Payload.

Payload	Key	Description
Restrictions	<i>allowAssistant</i>	Must be set to 'false'. (Siri is not allowed in the evaluated configuration.)
Restrictions	<i>allowAssistantUserGeneratedContent</i>	Must be set to 'false'. (Siri is not allowed in the evaluated configuration.)
Restrictions	<i>allowAssistantWhileLocked</i>	Must be set to 'false'. (Siri is not allowed in the evaluated configuration.)
Restrictions	<i>allowLockScreenControlCenter</i>	Must be set to 'false'.
Restrictions	<i>allowEnablingRestrictions</i>	Must be set to 'false'.
Restrictions	<i>allowUSBRestrictedMode</i>	Must be set to 'true'.

Table 7: Essential keys in the Restrictions Payload

Additional keys can be found in the following document and section.

[DEV_MAN]: ["Profile-Specific Payload Keys"](#) → ["Restrictions"](#)

5.2 Cryptographic Support Functions

The mobile devices include three cryptographic modules that provide the cryptographic services via the following three cryptographic modules.

- Apple corecrypto Module v12.0 [Apple ARM, User, Software, SL1] (User Space)
- Apple corecrypto Module v12.0 [Apple ARM, Kernel, Software, SL1] (Kernel Space)

- Apple corecrypto Module v12.0 [Apple ARM, Secure Key Store, Hardware, SL2]

Warning: The use of other cryptographic engines beyond those listed above was neither evaluated nor tested during the mobile device's Common Criteria evaluation.

The approved mode of operation for these cryptographic modules is configured by default and cannot be changed by the mobile device user or administrator. If the mobile device starts up successfully, then the modules have passed all self-tests and are operating in the approved mode.

5.2.1 Key Generation, Signature Generation, and Verification

5.2.1.1 General information

The mobile devices generate the following asymmetric keys.

- Rivest-Shamir-Adleman (RSA) with key sizes of 2048 bits or greater
- Elliptic-curve cryptography (ECC) with NIST curves P-256 and P-384 with key sizes of 256 bits and 384 bits, respectively
- ECC curve 25519 with a key size of 256 bits
- Finite-field cryptography (FFC) with key sizes of 2048 bits or greater

5.2.1.2 Mobile device users

For the evaluated configuration, no configuration is required from the mobile device user.

5.2.1.3 Mobile device administrators

For the evaluated configuration, no configuration is required from the mobile device administrator.

5.2.2 Key Establishment

5.2.2.1 General information

The mobile devices use the following for key establishment.

- RSA-based scheme
- ECC-based scheme
- Diffie-Hellman (DH)-based scheme

Key establishment is used for TLS and IKE.

5.2.2.2 Mobile device users

For the evaluated configuration, no configuration is required from the mobile device user.

5.2.2.3 *Mobile device administrators*

For the evaluated configuration, no configuration is required from the mobile device administrator.

5.2.3 Hashing

5.2.3.1 *General information*

The mobile devices perform the hash functions secure hash algorithm SHA-1, SHA-256, SHA-384, and SHA-512 with message digest sizes 160, 256, 384, and 512 bits.

Functions to perform hashing are provided as part of the Apple corecrypto libraries. The invoking function dictates which SHA function is used. Neither the mobile device user nor the mobile device administrator has the ability to configure this choice.

Similarly, each TLS ciphersuite uses a specific and appropriate SHA function. Neither the mobile device user nor the mobile device administrator has the ability to configure this choice.

5.2.3.2 *Mobile device users*

For the evaluated configuration, no configuration is required from the mobile device user.

5.2.3.3 *Mobile device administrators*

For VPN connections with IKEv2, the integrity algorithm to be used is selectable by the mobile device administrator by setting the *IntegrityAlgorithm* key in the VPN payload. Note that setting *IntegrityAlgorithm* to 'SHA1-96' is not allowed in the evaluated configuration.

5.2.4 Random Number Generation

5.2.4.1 *General information*

For random bit generation, the mobile devices use a deterministic random bit generator (DRBG), seeded by an internal entropy source. That source accumulates entropy from software-based noise and seeds the DRBG with a minimum of 256 bits of entropy.

5.2.4.2 *Mobile device users*

For the evaluated configuration, no configuration is required from the mobile device user.

5.2.4.3 *Mobile device administrators*

For the evaluated configuration, no configuration is required from the mobile device administrator.

5.2.5 Keys/Secrets Import/Destruction

5.2.5.1 General information

Cryptographic keys are stored in keychains. In iOS/iPadOS, an application only has access to its own keychain items, so access restrictions are automatically satisfied.

The “Keychain Services Programming Guide” [KEYCHAINPG] describes how keychain items are created, managed, and deleted.

5.2.5.2 Mobile device users

For the evaluated configuration, no configuration is required from the mobile device user.

5.2.5.3 Mobile device administrators

For the evaluated configuration, no configuration is required from the mobile device administrator.

5.2.6 Keys for Configuring Cryptographic Functions

This section provides details of dictionary key values that must be used or that are not allowed to be used in order to meet the requirements of the evaluated configuration described in the [IOS_ST] and the [IPADOS_ST]. The following values can be found in [DEV_MAN] in the [VPN.IKEv2.IKESecurityAssociationParameters](#) section.

Payload	Key	Description
VPN	<i>EncryptionAlgorithm</i>	<p>Must be set to one of the following:</p> <ul style="list-style-type: none"> • 'AES-128' • 'AES-256' (Default) • 'AES-128-GCM' (16-octet ICV) • 'AES-256-GCM' (16-octet ICV) <p>Other values must not be used in the evaluated configuration.</p> <p>Note that 'AES-128' and 'AES-256' use the CBC mode of operation.</p>

Payload	Key	Description
VPN	<i>IntegrityAlgorithm</i>	Must be set to one of the following: <ul style="list-style-type: none"> 'SHA1-160' 'SHA2-256' (Default) 'SHA2-384' 'SHA2-512' Other values must not be used in the evaluated configuration.
VPN	<i>DiffieHellmanGroup</i>	Must be set to one of the following: '5', '14', '15', '19', or '20'. Other values must not be used in the evaluated configuration.

Table 8: Essential keys for Configuring Cryptographic Functions

5.3 Network Protocols

5.3.1 EAP-TLS Configuration

5.3.1.1 General information

For Extensible Authentication Protocol (EAP)-TLS, iOS/iPadOS implements TLS 1.0, TLS 1.1, and TLS 1.2 supporting the cipher suites listed in Table 9: EAP-TLS Ciphersuites.

In the evaluated configuration, the mobile devices must use only the EAP-TLS cipher suites.

Ciphersuite Name
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256

Table 9: EAP-TLS Ciphersuites

No additional configuration is needed for the automatic recovery of a broken Wi-Fi connection.

5.3.1.2 Mobile device user

For the evaluated configuration, no configuration is required from the mobile device user.

5.3.1.3 Mobile device administrator

The cipher suites in Table 9: EAP-TLS Ciphersuites above are automatically selected by the mobile devices (i.e., the mobile devices do not support the individual selection of EAP-TLS cipher suites) when Wi-Fi Protected Access (WPA)-EAP is configured via Configuration Profile as follows.

- *EncryptionType* key must be set to 'WPA2'.
- *AcceptEAPTypes* key must be set to '13', which is the value representing EAP-TLS.

Because the evaluation of the mobile devices included TLS versions 1.0, 1.1, and 1.2, setting the *TLSTLSMinimumVersion* and *TLSTLSMaximumVersion* keys is a matter for the deploying organization's policy. These keys configure the minimum and maximum TLS versions to be used with EAP-TLS authentication. The default minimum value is '1.0' and the default maximum value is '1.2'.

The *EncryptionType* key is described in the following document and section.

[DEV_MAN]: "Profile-Specific Payload Keys" → "Networking" → "WiFi"

The *AcceptEAPTypes*, *TLSTLSMinimumVersion* and *TLSTLSMaximumVersion* keys are described in the following document and section.

[DEV_MAN]: "Profile-Specific Payload Keys" → "Networking" → "WiFi" → "WiFi.EAPClientConfiguration"

5.3.2 TLS Configuration

5.3.2.1 General information

TLS is provided by the APIs of the iOS/iPadOS Security Framework, which uses the Apple corecrypto Module v12.0 [Apple ARM, User, Software, SL1].

The library implements TLS 1.0, 1.1, and 1.2 supporting the cipher suites listed in Table 10: TLS Ciphersuites. In the evaluated configuration, only TLS 1.2 is supported. The [IOS_ST] and the [IPADOS_ST] limit the cipher suites used by TLS connections in the evaluated configuration.

The supported cipher suites below are automatically selected by the mobile devices (i.e., the devices do not support the individual selection of TLS cipher suites). The TLS cipher suites available are defined by the TLS server where all cipher suites listed in the [IOS_ST] and the [IPADOS_ST] are always available. Thus, no additional configuration is required by the administrator.

Ciphersuite Name
TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

Ciphersuite Name
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

Table 10: TLS Ciphersuites

There are some trusted root certificates that are preinstalled with iOS/iPadOS in a Trust Anchor Database to establish a chain of trust. These certificates are automatically trusted, and do not need to be included when creating a Configuration Profile. A list of iOS/iPadOS trusted root certificates can be found at [TRUST_STORE].

There are also blocked and always-ask certificates in the Trust Anchor Database. Blocked certificates are believed to be compromised and are never trusted. Always-ask certificates prompt the user whether they want to trust the certificate. Lists of these certificates can also be found at [TRUST_STORE].

5.3.2.2 Mobile device users

For the evaluated configuration, no configuration is required from the mobile device user.

5.3.2.3 Mobile device administrators

TLS/HTTPS Configuration

The mobile device must be configured to automatically reject untrusted HTTPS certificates rather than prompting the user to ask whether to accept it. This is done by setting the *allowUntrustedTLSPrompt* key to 'false' in the Restrictions Payload.

Some restrictions must be placed on AirPrint to ensure that it uses only TLS and only trusted certificates for TLS communication. This is done by setting both the *ForceTLS* key in the AirPrint Payload and the *forceAirPrintTrustedTLSRequirement* key in the Restrictions Payload to 'true'.

The mobile device administrator must also configure the *TLSTrustedServerNames* and *PayloadCertificateAnchorUUID* dictionary keys in the Wi-Fi Payload EAPClientConfiguration Dictionary such that they specify which server certificate common names and certificates will be accepted by the mobile device.

Reference Identifier Configuration

Mobile device administrators can use the functions of the Certificate, Key, and Trust Services [CKTSREF] API to manage and manipulate certificates.

The iOS/iPadOS device implements a set of X.509 policy checks that cannot be altered. If an application wants to enforce additional checks, it can use the API detailed in [CKTSREF].

When interpreting the term "reference identifier" as the name of the remote peer whose certificate should be validated, the TOE TLS and IKE stacks set the FQDN of the remote peer with the X.509 protocol checker. This operation is hard coded and cannot be influenced by the user via any API when using TLS or IKE.

Guidance documentation for setting additional constraints in validating an X.509 certificate can be specified with the rule definitions found in the following document and section.

[CKTSREF]: ["Policies"](#) → ["Security Policy Keys"](#)

Certificate Authority (CA) Configuration

Additional CAs can be added to the mobile device by using a Configuration Profile with the *EAPClientConfiguration* dictionary, and the *PayloadCertificateAnchorUUID*, and *TLSTrustedReaderNames* dictionary keys in the Wi-Fi Payload.

The keys above are described in the following document and section.

[DEV_MAN]: ["Profile-Specific Payload Keys"](#) → ["WiFi"](#) → ["WiFi.EAPClientConfiguration"](#)

Client Certificate Configuration

A client certificate with its keys can be installed on the mobile device using a Certificates payload in the Configuration Profile, as described in [DEV_MAN]. Examples of Configuration Profiles can be found in Appendix A: Configuration Profiles.

Configuration of the Supported Elliptic Curves Extension

The supported elliptic curves below are automatically selected by the mobile devices (i.e., the mobile devices do not support the individual selection of elliptic curves). The [IOS_ST] and the [IPADOS_ST] limit the curves used by TLS connections in the evaluated configuration. The curves available are defined by the server where all curves listed in the [IOS_ST] and the [IPADOS_ST] are always available. This behavior does not require any additional configuration by the mobile device administrator.

The following curves are available.

- secp256r1 (P-256)
- secp384r1 (P-384)
- secp521r1 (P-521) (SigGen/SigVer only)

Curve25519 is also supported by the mobile devices and may be disabled in the operational environment.

5.3.3 IPsec Configuration

5.3.3.1 General information

The mobile devices implement IPsec natively, as part of their operating system, so any processing of packets used in IPsec communication takes place on the mobile device. IPsec VPN tunnels are configured and controlled by the Network Extension Framework, which is a part of the Core OS Layer of the mobile devices' operating system.

The Security Policy Database (SPD) is created and configured by defining exceptions for IP traffic routing in a Configuration Profile. By default, all IP traffic is sent through a protected channel between the devices and the desired endpoint (PROTECT in the SPD). Any deviations from the default routing behavior must be explicitly specified as exceptions in the Configuration Profile, using the Wi-Fi Payload. Examples of Configuration Profiles can be found in Appendix A: Configuration Profiles.

Packet processing exceptions can be created for applications that make use of Captive Networking Identifiers (Captive Networking Apps), as well as for VoiceMail, AirPrint, and CellularServices. The mobile device administrator will need to refer to their organization's security policies to determine whether exceptions should be created and how those exceptions should be configured.

Exceptions for Captive Networking Apps can be configured in the Wi-Fi Payload to allow traffic for these apps to pass outside the tunnel (BYPASS in the SPD). Exceptions for voicemail, AirPrint, and CellularServices can allow traffic to pass unencrypted outside the tunnel (BYPASS in the SPD) or drop the traffic entirely (DISCARD in the SPD).

When the VPN is configured as Always-On, the mobile device uses IKEv2 for security association (SA) establishment. Since the mobile device must be configured with Always-On VPN to ensure that it is in the evaluated configuration, the use of IKEv2 does not need to be configured separately.

5.3.3.2 Mobile device users

For the evaluated configuration, no configuration is required from the mobile device user.

5.3.3.3 Mobile device administrators

To configure exceptions for Voicemail, AirPrint, and CellularServices, the mobile device administrator can specify a *ServiceExceptions* array in the AlwaysOn dictionary of the VPN payload (VPN.AlwaysOn).

Each entry in a *ServiceExceptions* array lists a *ServiceName* key and a corresponding *Action* key. The allowed values for *ServiceName* and *Action* can be found in Table 12: Essential Keys for the VPN Payload. For each *ServiceName*, the corresponding *Action* can be set to 'Allow' (BYPASS in the SPD) or 'Drop' (DISCARD in the SPD).

To configure exceptions for Captive Networking Apps, the mobile device administrator can use the *AllowCaptiveWebSheet*, *AllowAllCaptiveNetworkPlugins*, and *AllowedCaptiveNetworkPlugins*

keys in the Configuration Profile. Information on these keys can be found in following document and section.

[DEV_MAN]: [“Profile-Specific Payload Keys”](#) → [“VPN”](#) → [“VPN.AwlaysOn”](#)

When the *VPNTType* key is set to 'AlwaysOn', a catch-all PROTECT rule is created in the SPD. Any traffic not covered by an exception will be covered by that rule.

The mobile device administrator must not declare conflicting traffic exceptions, e.g. declaring both an 'Allow' and a 'Drop' value for 'Voicemail'. This guarantees that the SPD is unambiguous and unaffected by the ordering of SPD entries.

5.3.4 Bluetooth Configuration

5.3.4.1 General information

On iOS/iPadOS, manual authorization for Bluetooth connections is implicitly configured, as Bluetooth pairing can only occur when the mobile device is explicitly made discoverable through the [Settings » Bluetooth](#) interface. When the mobile device is made discoverable in this manner, another device (or the mobile device itself) can send a pairing request. Commonly, a six-digit number is displayed on both sides which must be manually matched by a mobile device user, i.e., the PIN is shown and the user must accept it before the pairing will complete. If one device does not support this automatic exchange of a PIN, a window for entering a manual PIN is presented to the user. The PIN entered must match on both sides.

Two conditions must be met for the mobile device to become discoverable: Bluetooth must be enabled and the Bluetooth configuration panel must be both active and in the foreground. If the Bluetooth configuration panel is not the active panel, or if Bluetooth is disabled, the mobile device is not discoverable. There is no other method to make the mobile device discoverable or not discoverable.

Devices that want to pair with the evaluated devices via Bluetooth are required by iOS/iPadOS to use Secure Simple Pairing, which uses Elliptic Curve Diffie-Hellman- (ECDH) based authentication and key exchange.

iOS/iPadOS requires that remote Bluetooth devices use an encrypted connection. Connections via Bluetooth BR/EDR and LE are secured using AES-128 in CCM mode. Further information about Bluetooth security is found in [BT]. This behavior requires no additional configuration by the mobile device administrator.

5.3.4.2 Mobile device users

For instructions on how to turn Bluetooth on and off and how to pair and unpair a Bluetooth device, the mobile device user can refer to the following documents and sections. (Sections 11.3 and 11.4 contain screenshots from these documents.)

[iPhone_UG]: [“Accessories”](#) → [“Set up and use Bluetooth accessories on iPhone”](#)

[iPad_UG]: [“Accessories”](#) → [“Set up and use Bluetooth accessories on iPad”](#)

Bluetooth can be disassociated by the mobile device user via the Control Center.

Further information on enabling and disabling Bluetooth can be found in the document [BLUETOOTH_HELP].

5.3.4.3 Mobile device administrators

In the evaluated configuration, the mobile device administrator can allow or disallow the mobile device user from making modifications to Bluetooth settings on the mobile device by using the *allowBluetoothModification* key in the Restrictions Payload in a Configuration Profile.

5.3.5 VPN Configuration

5.3.5.1 General information

In the evaluated configuration, the VPN must be in its Always-On configuration. The Always-On VPN configuration enables the organization to have full control over supervised device traffic by tunneling all IP traffic back to the organization.

5.3.5.2 Mobile device users

For the evaluated configuration, no configuration is required from the mobile device user.

5.3.5.3 Mobile device administrators

The mobile device administrator uses the VPN Payload to configure a traditional systemwide VPN based on IPsec, to specify Internet Key Exchange Version 2 (IKEv2) settings, and to specify attributes such as:

- the Always-On VPN configuration
- the Certificate authentication method
- administrator-defined certificates

Always-On VPN must be enabled by setting the *VPNType* key to 'AlwaysOn' in the Configuration Profile. When 'AlwaysOn' is selected as the *VPNType* for a Configuration Profile, the corresponding *ProtocolType* key must be set to 'IKEv2'. The *Interfaces* array, which lists the interfaces a particular Always-On VPN configuration applies to, can optionally be specified as 'Cellular, WiFi' (Default), 'Cellular', or 'WiFi'.

The mobile device administrator must specify the Service Set Identifiers (SSIDs) that the iOS/iPadOS device can connect to. This is done by specifying an array of strings of allowed SSIDs using the *SSIDMatch* key in the OnDemandRules dictionary of the VPN payload.

IKEv2 must be configured using the IKEv2 Dictionary Keys. The mobile device administrator must specify the IP address or hostname of the VPN server via *RemoteAddress*, the client identifier via *LocalIdentifier*, the remote identifier via *RemoteIdentifier*, the authentication method as 'Certificate' via *AuthenticationMethod*, and the certificate to be used for authentication via *PayloadCertificateUUID*.

Optional keys can be configured, which allow:

- enabling extended authentication via *ExtendedAuthEnabled*.

- the specification of a username and password via *AuthName* and *AuthPassword*.
- the specification of the interval the connection is kept alive when the peer cannot be reached via *DeadPeerDetectionRate*.
- the specification of the Common Name of the server certificate issuer and/or the Common Name of their server certificate via *ServerCertificateIssuerCommonName* and *ServerCertificateCommonName*.
- the specification of *IKESecurityAssociationParameters* and *ChildSecurityAssociationParameters*, both of which allow the further specification of an *EncryptionAlgorithm*, an *IntegrityAlgorithm*, and a *DiffieHellmanGroup* as described in Table 13: Essential keys for Data Protection.

5.3.6 Keys for Configuring Network Protocols

This section provides details of the dictionary key values that must or must not be used in order to meet the requirements of the evaluated configuration described in the [IOS_ST] and the [IPADOS_ST].

For dictionary keys not mentioned in this document, please refer to the deploying organization's security policies.

5.3.6.1 TLS Configuration Keys

Payload	Key	Description
Restrictions	<i>allowUntrustedTLSPrompt</i>	Must be set to 'false'.
Restrictions	<i>forceAirPrintTrustedTLSRequirement</i>	Must be set to 'true'.
AirPrint	<i>ForceTLS</i>	Must be set to 'true'.
Wi-Fi	<i>EncryptionType</i>	Must be set to 'WPA2'.
EAPClientConfiguration Dictionary Keys		
Wi-Fi	<i>AcceptEAPTypes</i>	Must be set to '13' (EAP-TLS).
Wi-Fi	<i>PayloadCertificateAnchorUUID</i>	Must contain at least one UUID of a Certificates Payload that is to be trusted. Note that setting this key prevents the mobile device from asking the user if certificates are trusted.
Wi-Fi	<i>TLSTrustedServerNames</i>	Must be set.
Wi-Fi	<i>TLSCertificateIsRequired</i>	Must be set to 'true'.

Table 11: Essential Payload Keys for TLS and EAP-TLS

5.3.6.2 VPN Configuration keys

Payload	Key	Description
VPN	<i>VPNType</i>	Must be set to 'AlwaysOn'.
VPN	<i>OnDemandEnabled</i>	Must be set to '0'.
IKEv2 Dictionary Keys		
VPN	<i>RemoteAddress</i>	Must be set. Specifies the IP address or hostname of your organization's VPN server.
VPN	<i>LocalIdentifier</i>	Must be set.
VPN	<i>RemoteIdentifier</i>	Must be set.
VPN	<i>AuthenticationMethod</i>	Must be set to 'Certificate'.
VPN	<i>PayloadCertificateUUID</i>	Must be set. Specifies the universally unique identifier (UUID) of the identity certificate used as the account credential.
VPN	<i>CertificateType</i>	Must be set to one of the following: <ul style="list-style-type: none"> • RSA (Default) • ECDSA P-256 • ECDSA P-384 • Specifies the type of PayloadCertificateUUID used for IKEv2 machine authentication.
VPN	<i>ServerCertificateIssuerCommonName</i>	Must be set. Specifies the Common Name of the server certificate issuer. This key will cause IKE to send a certificate request to the server based on the specified certificate issuer.
VPN	<i>EnableCertificateRevocationCheck</i>	Must be set to '1'. Enables a certificate revocation check for IKEv2 connections.
VPN	<i>IKESecurityAssociationParameters</i>	Optional. A dictionary that specifies the parameters for IKEv2 IKE_SA_INIT and IKE_AUTH exchanges (Phase 1).

VPN	<i>ChildSecurityAssociationParameters</i>	Optional. A dictionary that specifies the parameters for IKEv2 child SAs (Phase 2). If parameters are not specified for Phase 2, the Phase 1 parameters will be used. If the corresponding Phase 1 parameters are also not specified, the default values for those parameters will be used.
IKESecurityAssociationParameters and ChildSecurityAssociationParameters Dictionary Keys		
VPN	<i>EncryptionAlgorithm</i>	Must be set to one of the following. <ul style="list-style-type: none"> • 'AES-128' • 'AES-256' (Default) • 'AES-128-GCM' (16-octet ICV) • 'AES-256-GCM' (16-octet ICV) Other values must not be used in the evaluated configuration. Note that 'AES-128' and 'AES-256' use the CBC mode of operation.
VPN	<i>IntegrityAlgorithm</i>	Must be set to one of the following. <ul style="list-style-type: none"> • 'SHA1-160' • 'SHA2-256' (Default) • 'SHA2-384' • 'SHA2-512' Other values must not be used in the evaluated configuration.
VPN	<i>DiffieHellmanGroup</i>	Set to one of the following: '5', '14', '15', '19', or '20'. Other values must not be used in the evaluated configuration.
VPN	<i>LifeTimeInMinutes</i>	Optional. SA lifetime (rekey interval) in minutes. Allowed values are '10' through '1440'. Defaults to '1440' (24 hours).
AlwaysOn Dictionary Keys		
VPN	<i>UIToggleEnabled</i>	Must be set to '0'. If set to '1', allows the mobile device user to disable this VPN configuration. Defaults to '0'.
		<i>ProtocolType</i> Must be set to 'IKEv2'

VPN	<i>TunnelConfigurations</i>	<i>Interfaces</i>	Optional. An array that lists the interfaces to which this configuration applies. Valid array entries are 'Cellular' and 'WiFi'. Defaults to 'Cellular, WiFi'.
VPN	<i>ServiceExceptions</i>	<i>ServiceName</i>	The name of a system service which is exempt from AlwaysOn VPN. May be set to one of the following. <ul style="list-style-type: none"> • VoiceMail • AirPrint • CellularServices
		<i>Action</i>	May be set to one of the following. <ul style="list-style-type: none"> • Allow • Drop
VPN	<i>AllowCaptiveWebSheet</i>	Optional. If set to '1', allows traffic from Captive Web Sheet outside the VPN tunnel. Defaults to '0'.	
VPN	<i>AllowAllCaptiveNetworkPlugins</i>	Optional. If set to '1', allows traffic from all Captive Networking apps outside the VPN tunnel to perform Captive network handling. Defaults to '0'.	
VPN	<i>AllowedCaptiveNetworkPlugins</i>	Optional. An array of dictionaries that describes Captive Networking apps whose traffic will be allowed outside the VPN tunnel to perform Captive network handling. Used only when <i>AllowAllCaptiveNetworkPlugins</i> is '0'. Each dictionary in this array must contain a <i>BundleIdentifier</i> key of type string, the value of which must be the application's bundle identifier.	
OnDemandRules Dictionary Keys			
VPN	<i>SSIDMatch</i>	Must be set. An array of allowed SSIDs must be given to which the iOS/iPadOS device is allowed to connect.	

DNS Dictionary Keys	
VPN	<p><i>SupplementalMatchDomains</i></p> <p>Must not be set. (This key is used to create a split DNS, which is not allowed in the evaluated configuration.)</p>

Table 12: Essential Keys for the VPN Payload

5.4 Data Protection

5.4.1 Data-At-Rest (DAR) Protection Configuration

5.4.1.1 General information

To ensure data-at-rest protection, establishment of a passcode on the mobile device is required.

The TOE only supports external storage encryption with storage devices formatted in the APFS format; other formats with encryption or encrypted volumes are not supported by the TOE.

In the evaluated configuration, external storage devices must be formatted in the APFS file format and volumes must be encrypted. All other storage formats are not allowed in the evaluated configuration.

Further information on the APFS format can be found in [APFS_DOC] and [APFS_DEV_DOC].

5.4.1.2 Mobile device users

Users can check that data-at-rest protection is enabled on their device with the following.

Face ID Device: [Settings » Face ID & Passcode](#)

Touch ID Device: [Settings » Touch ID & Passcode](#)

This screen allows the user to enable data protection on the device by enabling these ID features. No further configuration is required to enable data protection on the device. More information can be found on this topic in the following documents and sections. (Sections 11.5 and 11.6 contain screenshots from these documents.)

[iPhone_UG]: ["Security and privacy"](#) → ["Protect your iPhone"](#) → ["Set a passcode on iPhone"](#)

[iPad_UG]: ["Security and privacy"](#) → ["Protect your iPad"](#) → ["Set a passcode on iPad"](#)

Mobile device users can only use external storage devices formatted in the APFS format with encrypted volumes. No other file format is supported in the evaluated configuration, and the APFS-formatted device must have only encrypted volumes. An APFS-formatted device without encrypted volumes is not supported.

Instructions on formatting devices in the APFS format with encrypted volumes can be found in [APFS_DOC]. Further technical information on the APFS format with encrypted volumes can be found in [APFS_DEV_DOC].

5.4.1.3 Mobile device administrators

Mobile device administrators must ensure that mobile device users set a passcode by using the *forcePIN* key in the Passcode Payload. Other keys available in this payload allow administrators to configure passcode requirements to their deploying organizations policy.

See 5.5.1, Passcode Authentication Configuration, for more information on passcode configuration.

Mobile device administrators can restrict USB drive access in the Files app if desired by setting the *allowFilesUSBDriveAccess* key to 'false' in the "Restrictions" section of the Configuration Profile.

Mobile device administrators must ensure through organizational policies that mobile device users only use external storage devices formatted in the APFS format with encrypted volumes. Unencrypted volumes and other formats are not allowed in the evaluated configuration.

5.4.2 Restrict Application Access to System Services

5.4.2.1 General information

Access control to system services in the Core Services layer is hard coded and, thus, not configurable by the mobile device user or administrator.

Access control for applications to system services can be restricted on a per-app basis. In the operating systems, these services are as follows.

- Location Services
- Tracking
- Contacts
- Calendars
- Reminders
- Photos
- Bluetooth
- Local Network
- Nearby Interactions (iPhones only)
- Microphone
- Speech Recognition
- Camera
- Health (iPhones only)
- Research Sensor & Usage Data (iPhones only)
- HomeKit

- Media & Apple Music
- Files and Folders
- Motion & Fitness
- Focus
- Analytics & Improvements
- Apple Advertising
- Record App Activity

5.4.2.2 Mobile device users

A list of system services can be obtained from the mobile device [Settings » Privacy](#). For each system service, the Applications that have permission to use that service can be inspected and changed.

5.4.2.3 Mobile device administrators

Mobile device administrators can not specify access control for applications to system services.

5.4.3 Wiping of Protected Data

5.4.3.1 General information

A wipe operation is performed after the mobile device user exceeds the limit of the number of failed authentication attempts or upon receiving a request from an authorized administrator. The administrator can configure the number of failed attempts by using the following Configuration Profile key in the Passcode Payload: *maxFailedAttempts*. This key takes an integer value between '2' and '11'.

5.4.3.2 Mobile device users

Mobile device users can wipe the device themselves. This can be performed on the device using the following.

Device: [Settings » General » Transfer or Reset iPhone/iPad » Erase All Content and Settings](#)

More information can be found on this topic in the following documents and section. (Sections 11.7 and 11.8 contain screenshots from these documents.)

[iPhone_UG]: ["Restart, update, reset, and restore"](#) → ["Erase iPhone"](#)

[iPad_UG]: ["Restart, update, reset, and restore"](#) → ["Erase iPad"](#)

Depending on the organizational policy, the mobile device administrator can disable this function.

5.4.3.3 Mobile device administrators

It is mandatory that the mobile device administrator can issue a remote wipe command from the MDM server using the MDM protocol as described in [DeployRef] and [DEV_MAN].

The following key is required to execute a remote device wipe: *RequestType* with a value of 'EraseDevice' when sending the *EraseDeviceCommand.Command* command. Upon receiving this command, the device immediately erases itself. No warning is given to the user. This command is performed immediately even if the device is locked.

[DEV_MAN]: "Commands and Queries" → "Erase a Device" → "EraseDeviceCommand" → "EraseDeviceCommand.Command"

In order to execute this command successfully, Device Erase access rights must be set. To enable this access, the following MDM Payload-related key must be used: *AccessRights*. The value for this key is determined by a logical "OR" that includes the value '8', where 8 stands for allowing device erase rights.

Depending on the organizational policy, the mobile device administrator can disallow the mobile device user from wiping the device themselves. This ability can be configured by the mobile device administrator by setting the *allowEraseContentAndSettings* key to 'false' in the Restrictions Payload.

5.4.4 Keys for Configuring Data Protection

This section provides details of the dictionary key values that must be used, or where certain options for the key value are not allowed, in order to meet the requirements of the evaluated configuration described in the [IOS_ST] and the [IPADOS_ST].

For dictionary keys not mentioned in this document, please refer to the deploying organization's security policies.

Payload	Key	Description
MDM	<i>AccessRights</i>	A logical "OR" including the value "8"
Passcode	<i>maxFailedAttempts</i>	A value between '2' and '11' according to the organizations security policy
Restrictions	<i>allowEraseContentAndSettings</i>	Disables the option to erase all content and settings from the mobile device UI if set to 'false'
Restrictions	<i>allowFilesUSBDriveAccess</i>	Disables external storage via device connection

Table 13: Essential keys for Data Protection

5.5 Identification & Authentication

5.5.1 Passcode Authentication Configuration

5.5.1.1 General information

In the evaluated configuration, mobile devices must be configured to use either a numeric passcode or an alphanumeric passcode.

The Passcode Payload is described in [DEV_MAN] and describes the keys that can be used to set attributes such as:

- defining the minimum passcode length.
- defining requirements for the passcode complexity.
- defining the maximum passcode lifetime.
- defining the maximum time of inactivity after which the mobile device is locked automatically.
- defining the maximum number of consecutive authentication failures after which the mobile device is wiped.

The devices allow the following parameters for passcode complexity.

- Passcodes can be composed of any combination of upper- and lower-case letters, numbers, and special characters: "!", "@", "#", "\$", "%", "^", "&", "*", "(", ")"
- Passcode length must be between 1 and 16.

5.5.1.2 Mobile device users

In the evaluated configuration, the mobile device user cannot configure the passcode policy.

5.5.1.3 Mobile device administrators

It is mandatory that the mobile device administrator configure the passcode policy for the mobile device.

The Passcode Payload presents the administrator with an alphanumeric passcode entry mechanism, which allows for the entry of arbitrarily long and complex passcodes including the selection of special characters. To do this, set the configuration keys *allowSimple* to 'false' and *requireAlphanumeric* to 'true'.

Also, set the configuration key *minLength* to a value greater than zero, defined by the deploying organization's policy.

5.5.2 Protected Authentication Feedback

5.5.2.1 General information

All passcode entries are obscured by iOS/iPadOS. This is done by displaying a dot symbol in place of each character as the passcode entry user input occurs. No configuration of this feature is required from the mobile device administrator.

Biometric authentication inputs do not provide feedback to the user unless the input is rejected. Additionally, biometric authentication inputs do not relay authentication entry information and are inherently obscured. When an invalid fingerprint sample is given or a fingerprint sample cannot be authenticated, a simple error message is returned, which prompts the user to try again. When an invalid facial sample is given or a facial sample cannot be authenticated, the mobile device will vibrate. If three invalid biometric samples are presented, the mobile device will offer passcode entry. After five invalid biometric samples are presented passcode authentication is required.

Refer to [PASSCODE_Help] for more information on how to manage a passcode.

5.5.2.2 Mobile device users

Passcode entry is obscured by iOS/iPadOS; no configuration of this feature is required from the mobile device user.

5.5.2.3 Mobile device administrators

Passcode entry is obscured by iOS/iPadOS, no configuration of this feature is required from the mobile device administrator.

5.5.3 Biometric Authentication Factors

5.5.3.1 General information

Enrollment and management of biometric authentication factors and credentials is found on the device using the following.

Face ID Device: [Settings » Face ID & Passcode](#)

Touch ID Device: [Settings » Touch ID & Passcode](#)

More information can be found on this topic in the following documents and sections.

[iPhone_UG]: (Sections 11.9 and 11.10 of this document contain screenshots from [iPhone_UG].)

Face ID: ["Security and privacy"](#) → ["Protect your iPhone"](#) → ["Set up Face ID on iPhone"](#)

Touch ID: ["Security and privacy"](#) → ["Protect your iPhone"](#) → ["Set up Touch ID on iPhone"](#)

[iPad_UG]: (Sections 11.11 and 11.12 of this document contain screenshots from [iPad_UG].)

Face ID: ["Security and privacy"](#) → ["Protect your iPad"](#) → ["Set up Face ID on iPad"](#)

Touch ID: “[Security and privacy](#)” → “[Protect your iPad](#)” → “[Set up Touch ID on iPad](#)”

5.5.3.2 Mobile device users

In the evaluated configuration, the mobile device user cannot enable Touch ID or Face ID. Only the mobile device administrator can enable/disable Touch ID or Face ID using the Restrictions Payload. If the mobile device administrator has enabled these biometric authentication factors, the following is guidance on how the mobile user can configure Touch ID and Face ID.

Enrollment for Touch ID is typically accomplished during initial device configuration but can also be performed using the [Settings » Touch ID & Passcode](#) menus. Multiple fingerprints may be enrolled, named, and deleted from this menu. To remove a specific finger, a device user must tap the finger for removal followed by delete fingerprint. Mobile device users may place a finger on the Touch ID sensor to determine which biometric credential entry it is mapped to. Users may also disable Touch ID selectively for applications, or entirely, from the [Settings » Touch ID & Passcode](#) menu by authenticating using their passcode and turning off one or more of the following corresponding options.

- Unlock
- Apple Pay
- iTunes & App Store

Enrollment for Face ID is typically accomplished during initial device configuration but can also be performed using the [Settings » Face ID & Passcode](#) menu by tapping the “Set up Face ID” option. Mobile users can enroll an alternative appearance for Face ID, for a total of two enrollments per device. Mobile users may establish Face ID credentials by providing biometric samples. They may also remove biometric samples from the [Settings » Face ID & Passcode](#) menu by tapping the [Reset Face ID](#) option. This action removes all established Face ID credentials. Users may also disable Face ID selectively for applications, or entirely, from the [Settings » Face ID & Passcode](#) menu by turning off one or more of the following corresponding options.

- Unlock
- Apple Pay
- iTunes & App Store
- Safari AutoFill

5.5.3.3 Mobile device administrators

A mobile device administrator can configure to not allow a device user to enable Touch ID or Face ID by setting the key `allowFingerprintForUnlock` to false in a Configuration Profile using the Restrictions Payload.

5.5.4 Authentication Attempt Configuration

5.5.4.1 General information

Both Face ID and Touch ID allow up to five unsuccessful authentication attempts before passcode authentication is required. For the details, please see the following document and section.

[AP_SEC]: ["Hardware security and biometrics"](#) → ["Face ID and Touch ID"](#) → ["Face ID, Touch ID, passcodes, and passwords"](#)

5.5.4.2 Mobile device users

In the evaluated configuration, the mobile device user cannot configure the maximum number of failed authentication attempts.

5.5.4.3 Mobile device administrators

To limit/configure the number of consecutive failed authentication attempts for the passcode; the administrator can use the key *maxFailedAttempts*. This key takes an integer value between '2' and '11'. See the Passcode Payload in section 5.5.1, Passcode Authentication Configuration.

5.5.5 Re-Authentication Configuration

5.5.5.1 General information

When the use of a passcode is enabled, the mobile device automatically prompts the user for a passcode to unlock the device. No additional configuration is required.

Use of Touch ID or Face ID can be set in the [Settings » Touch ID & Passcode](#) or [Settings » Face ID & Passcode](#). The biometric authentication factor can be configured for device unlock, Apple Pay, iTunes, and App Store.

The Passcode Payload allows an administrator to enable/disable modification of Touch ID or Face ID through specification of the *allowFingerprintModification* key.

A passcode must be supplied for additional security validation in any of the following instances.

- The mobile device has just been turned on or restarted
- For device software updates
- To wipe the device
- To view or change passcode settings
- To install iOS/iPadOS Configuration Profiles
- The mobile device has not been unlocked for more than 48 hours
- The passcode has not been used to unlock the mobile device in the last 156 hours (six and a half days) and Face ID or Touch ID has not been used to unlock the mobile device in the last 4 hours

- The device has received a remote lock command
- After five unsuccessful biometric attempts (though, for usability, the device might offer entering a passcode instead of using biometrics after a smaller number of failures).
- After exiting power off/Emergency SOS by pressing and holding either volume button and the sleep/wake simultaneously for 2 seconds and then pressing Cancel.

Note that When Touch ID or Face ID is enabled on an iPhone or iPad, the device immediately locks when the sleep/wake is pressed, and the device locks every time it goes to sleep. Touch ID and Face ID require a successful match—or, optionally, the passcode—at every wake.

5.5.5.2 Mobile device users

In the evaluated configuration, the mobile device user cannot enable/disable the modification of Touch ID or Face ID.

5.5.5.3 Mobile device administrators

In the evaluated configuration, the mobile device administrator set the *allowFingerprintModification* key to a value defined by the organization's policy.

5.5.6 X.509 Certificate Configuration

5.5.6.1 General

X.509 certificates are configured by an administrator using the keys of the *Certificates Payload* in a Configuration Profile.

[DEV_MAN]: ["Profile-Specific Payload Keys"](#) → ["Certificates"](#)

Certificates have a certificate type that defines their respective application area. This ensures that only certificates defined for a specific application area are used. In addition, the database containing trust anchors for all certificates is protected via integrity check and write protection. The certificate types supported by the devices are as follows.

- AppleX509Basic
- AppleSSL
- AppleSMIME
- AppleEAP
- AppleIPsec
- AppleCodeSigning
- AppleIDValidation
- AppleTimeStamping

The list of supported certificate and identity formats is as follows.

- Certificate (PKCS1): cer, .crt, .der, X.509 certificates with RSA keys

- Identity (PKCS12): .pfx, .p12

For more information on the certificate and identity formats, see the following document and sections.

[DeployRef]: ["Ensure device security"](#) → ["Manage certificates"](#) → ["Intro to certificate management"](#)

[DeployRef]: ["MDM settings"](#) → ["MDM payload settings"](#) → ["Certificates payload settings"](#)

External entities can be authenticated using a digital certificate. Out of the box, the TOE includes a number of preinstalled root certificates.

Code signing certificates need to be assigned by Apple and can be imported into a device. The issue of such a certificate can be by app developers or by enterprises that want to deploy apps from their MDM to managed devices. All apps must have a valid signature that can be verified by a code signing certificate before they are installed on a device.

The mobile devices have a Trust Anchor Database, which contains trusted root certificates preinstalled with iOS/iPadOS to establish a chain of trust; see [TRUST_STORE]. These preinstalled trusted root certificates cannot be modified, are automatically trusted, and do not need to be included when creating a Configuration Profile. New certificates can be added to the Trust Anchor Database, or currently installed certificates can be removed.

There are also blocked and always-ask certificates in the Trust Anchor Database. Blocked certificates are believed to be compromised and are never trusted. Always-ask certificates prompt the user whether they want to trust the certificate. Lists of these certificates can also be found at [TRUST_STORE].

When attempting to establish a connection using a peer certificate (i.e., a certificate received from the other endpoint), the peer certificate is first checked to ensure it is valid as per RFC 5280. Certificates are validated against the Subject Alternative Name (SAN). It must contain a Fully Qualified Domain Name (FQDN). Wildcards are supported. The Common Name (CN) is ignored. If the SAN does not match the corresponding domain name system (DNS) or IP Address of the server being accessed, validation and subsequently the connection will fail. If the certificate is valid, the attempt to establish the connection continues. If the certificate is invalid, the next step is up to the application.

The iOS/iPadOS device, excluding WLAN, uses OCSP for validating the revocation status of certificates. When a connection cannot be established to the OCSP server to determine the revocation status of a certificate, the iOS/iPadOS device considers the certificate as not revoked.

As part of the certificate chain validation, the validity period of each certificate in the chain is verified. If the certificate is marked as an extended validation certificate, the iOS/iPad device performs an OCSP lookup to verify the validity (revocation status) of the certificate (except for WLAN certificate validation, which does not support OCSP). The basicConstraints extension and the Certificate Authority (CA) flag are checked. CA certificates must have the basicConstraints extension, the CA flag set to TRUE, and include the caSigning purpose. The extendedKeyUsage (EKU) is validated against the rules defined in FIA_X509_EXT.1 (which is a superset of the rules in FIA_X509_EXT.1/WLAN). Finally, the signature of the issuer of the certificate is verified. Only

when all checks succeed, the certificate is considered valid and the next certificate in the certificate chain is checked.

The certificate chain searches for the certificates in the trust store. The trust store is a combination of the trust store delivered with the iOS/iPadOS device and the certificates stored in the key chain and marked as trustworthy. Certificates from the trusted store are validated using the previously described checks at the time that they are used. Certificate path validation terminates with a certificate in the trust store.

Further information on certificates can be found in the Certificates section of [CKTSREF], in [DeployRef], and in [DEV_MAN].

5.5.6.2 Mobile device users

In the evaluated configuration, the mobile device user cannot import X.509v3 certificates into the Trust Anchor Database. However, if the mobile device is unsupervised, the mobile device user can install root certificates into the Trust Anchor Database.

Unless the administrator has disallowed the removal of the Configuration Profile that contains the certificate, mobile device users can manually remove certificates that have been installed on their device. Choose *Settings » General » Profile & Device Management*, select a profile, choose *More Details*, and then choose the appropriate certificate to remove.

In the evaluated configuration, the mobile device user can remove imported X.509v3 certificates but cannot remove other X.509v3 certificates in the Trust Anchor Database.

5.5.6.3 Mobile device administrators

In the evaluated configuration, mobile device administrators are allowed to modify the Trust Anchor Database. X.509 certificates can be configured by using a Configuration Profile.

Certificate identities can be deployed using the following two methods: 1) using Public Key Cryptography Standards (PKCS) #12 identity certificate and 2) Simple Certificate Enrollment Protocol (SCEP). The mobile device administrator should use the Certificates Payload of the Configuration Profile if using the first option and should use the SCEP Payload of the Configuration Profile if using the second option.

The mobile device administrator can also send the mobile device user an email with the certificate as an attachment or a link to a secure site hosting the certificate. The user will download the certificate, from the email or site, to install on the mobile device.

More information on certificate configuration can be found in [DeployRef] and subsection EAPClientConfiguration Dictionary of the Wi-Fi section of [DEV_MAN].

In the evaluated configuration, the mobile device administrator must disallow the removal of a Certificates Payload by a user in a Configuration Profile by setting the *PayloadRemovalDisallowed* key for that payload to 'true'. See the [DEV_MAN] section *ProfileListResponse.ProfileListItem*.

When configuring the devices to utilize EAP-TLS as part of a WPA2-protected Wi-Fi network, the CA certificate(s) to which the server's certificate must chain can be configured using the

PayloadCertificateAnchorUUID key in the Wi-Fi Payload of the Configuration Profile. More information can be found in the Wi-Fi Payload and subsection EAPClientConfiguration Dictionary of [DEV_MAN].

Mobile device administrators can view all certificates on a device and remove any certificates it has installed via the MDM protocol using the *RequestType* key with the content "CertificateList". The MDM protocol also allows for certificate removal.

A list of all available trusted root certificates on the iOS/iPadOS device can be found in [TRUST].

Certificate Validation

To configure the devices to reject untrusted certificates, the administrator can use the *PayloadCertificateAnchorUUID* and *TLSTrustedServerNames* dictionary keys in the Wi-Fi Payload EAPClientConfiguration Dictionary of the Configuration Profile, which enforces that untrusted certificates are not accepted and the authentication fails if such untrusted certificates are presented.

To enforce the verification of the server name defined with the X.509 certificate during the WPA-EAP handshake between the mobile device and the remote access point, the policy must contain the server name to be expected in the certificate with the *TLSTrustedServerNames* dictionary key in the Wi-Fi Payload EAPClientConfiguration Dictionary of the Configuration Profile.

Guidance and the API documentation related to certificate validation is provided in "Certificate, Key, and Trust Services" [CKTSREF] in the section "[Trust](#)."

5.5.7 Keys for Identification and Authentication

This section provides details of the dictionary key values that must be used, or where certain options for the key value are not allowed, in order to meet the requirements of the evaluated configuration described in the [IOS_ST] and the [IPADOS_ST].

Payload	Key	Setting
Passcode	<i>allowSimple</i>	Must be set to 'false'.
	<i>forcePIN</i>	Must be set to 'true'.
	<i>maxFailedAttempts</i>	Must be set to a value between 2 and 11 according to the deploying organization's policy.
	<i>maxInactivity</i>	Should be set to a value defined by the deploying organization's policy.
	<i>maxPINAgeInDays</i>	Should be set to a value defined by the deploying organization's policy.

Payload	Key	Setting
	<i>minComplexChars</i>	Should be set to a value defined by the deploying organization's policy.
	<i>minLength</i>	Should be set to a value defined by the organization's policy.
	<i>requireAlphanumeric</i>	Should be set to a value defined by the organization's policy.
	<i>pinHistory</i>	Should be set to a value defined by the organization's policy.
	<i>maxGracePeriod</i>	Must be set to 0.
	<i>changeAtNextAuth</i>	Should be set to a value defined by the organization's policy.
Restrictions	<i>allowFingerprintModification</i>	Should be set to a value defined by the organization's policy.

Table 14: Essential keys for Identification and Authentication

5.6 Security Management

5.6.1 Install/Remove Apps from the Device

5.6.1.1 General information

If the mobile device is enrolled in MDM, managed apps on the mobile device can be removed by an administrator remotely via the MDM System or when the mobile device user removes their own device from MDM. If a mobile phone is removed from MDM, the mobile device administrator has some control over what happens to the associated data. When a managed app is removed from a device, the associated data is removed with it.

For more information on managed apps, refer to the following document and section.

[DeployRef]: ["Distribute content"](#) → ["Distribute apps"](#)

5.6.1.2 Mobile device users

Mobile device users may be able to install or remove an application from their device. (This depends upon the organization's policy and the value of the dictionary keys in the Restrictions Payload for *allowAppRemoval* and *allowAppInstallation*.)

For more information on installing applications, see the following documents and section. (Sections 11.13 and 11.14 contain the screenshots from these documents.)

[iPhone_UG]: ["App Store"](#) → ["Get apps in the App Store on iPhone"](#)

[iPad_UG]: [“App Store”](#) → [“Get apps in the App Store on iPad”](#)

For more information on removing applications, see the following documents and section. (Sections 11.15 and 11.16 contain the screenshots from these documents.)

[iPhone_UG]: [“Personalize your iPhone”](#) → [“Customize the Home Screen”](#) → [“Remove apps from iPhone”](#)

[iPad_UG]: [“Personalize your iPad”](#) → [“Customize the Home Screen”](#) → [“Remove apps from iPad”](#)

5.6.1.3 Mobile device administrators

The mobile device administrator can install applications on the mobile device using an MDM system or Apple Configurator 2. Refer to the following documents and sections.

[DeployRef]: [“Distribute content”](#) → [“Distribute apps”](#)

[AConfig]: [“Distribute content”](#) → [“Add apps to a device”](#)

[DEV_MAN]: [“Commands and Queries”](#) → [“Install an App”](#)

If installing an enterprise application, refer to the following document and section.

[DEV_MAN]: [“Commands and Queries”](#) → [“Install an Enterprise App”](#)

The mobile device administrator can remove managed applications using MDM. To remove an application, the MDM server sends a command using the *RequestType* and *Identifier* keys. The below table provides additional information on these keys.

Key	Description
<i>RequestType</i>	This key must be set to: RemoveApplication
<i>Identifier</i>	The application’s identifier

More information can be found in the following document and section.

[DEV_MAN]: [“Commands and Queries”](#) → [“Remove an App”](#) → [“RemoveApplicationCommand”](#) → [“RemoveApplicationCommand.Command”](#)

5.6.2 Configure Access and Notification in Locked State

5.6.2.1 General information

By default, the following features are available when the mobile device is locked and authentication is not needed.

- Making emergency calls
- Using the camera

- Using the flashlight

Access to certain optional features can be allowed when the mobile device is in a locked state. These optional features include the following.

- Email notification
- Calendar appointment
- Text message notification

5.6.2.2 Mobile device users

To allow access to the optional features when the mobile device is locked, use the following on the device.

Face ID Device: [Settings » Face ID & Passcode](#)

Touch ID Device: [Settings » Touch ID & Passcode](#)

Enter the passcode and select the features you want to allow access under the [Allow Access When Locked](#) menu.

Those items may be restricted by a Configuration Profile installed by an administrator. For more information, refer to the following documents and sections. (Sections 11.17 and 11.18 contain the screenshots from these documents.)

[iPhone_UG]: ["Basics"](#) → ["Access features from the iPhone Lock screen"](#)

[iPad_UG]: ["Basics"](#) → ["Access features from the iPad Lock screen"](#)

Certain display notifications can be set when the mobile device is in the locked state. To enable/disable display notifications in the locked state, go to [Settings » Face ID & Passcode](#) or [Settings » Touch ID & Passcode](#) and enter the passcode. Once authenticated, turn on Notification Center (found in the [Allow Access When Locked](#) options list). For more information, refer to the following documents and sections. (Sections 11.19 and 11.20 contain the screenshots from these documents.)

[iPhone_UG]: ["Personalize your iPhone"](#) → ["Set up Focus, notifications, and Do Not Disturb"](#)
→ ["Change notification settings on iPhone"](#)

[iPad_UG]: ["Personalize your iPad"](#) → ["Set up Focus, notifications, and Do Not Disturb"](#) →
["Change notification settings on iPad"](#)

5.6.2.3 Mobile device administrators

The mobile device administrator can use the `allowLockScreenNotificationsView` key in the Restrictions Payload in a Configuration Profile to disallow the user from viewing past notifications (i.e., disable Notification history). However, the mobile device user can see notifications as they arrive. To disable displaying notifications on the lock screen for applications, the `ShowInLockScreen` key in the Notifications Payload must be set to 'true'.

Once the notification settings have been implemented by the mobile device administrator, the *allowNotificationsModification* key in the Restrictions Payload must be set to 'true' if the settings are not allowed to be modified.

Refer to [DEV_MAN] for more information.

5.6.3 Device/Session Locking

5.6.3.1 General information

The mobile device is locked after a configurable time of user inactivity. To unlock the mobile device, an authentication mechanism must be enabled. For example, the device user uses a passcode or Face ID or Touch ID for authentication.

5.6.3.2 Mobile device users

In the evaluated configuration, the mobile device user is not allowed to configure the auto-lock in *Settings » Display & Brightness » Auto-Lock*.

Mobile device users can transition to the locked state by pressing the side button (or for some mobile device models, the Sleep/Wake button).

5.6.3.3 Mobile device administrators

It is mandatory that mobile device administrators configure the device/session locking policy on the mobile devices. This is done by setting the Configuration Profile key *maxInactivity* in the Passcode Payload to the desirable time. The number of authentication failures allowed is set using the *maxFailedAttempts* key, in the same payload, to a value between '2' and '11'. Refer to [DEV_MAN] for additional information.

Additionally, the mobile device administrator can set the *RequestType* to 'DeviceLock' as described in the following document and section.

[DEV_MAN]: *"Commands and Queries" → "Lock a Device" → "LockDeviceCommand" → "LockDeviceCommand.Command"*

This key requires the Device Lock and Passcode Removal access rights. In the MDM payload, setting the *AccessRights* key to '4' allows for device lock and passcode removal.

5.6.4 Timestamp Configuration

5.6.4.1 General information

In the evaluated configuration, the mobile device must be configured to update its time automatically. Accurate timestamps are crucial when it comes to analyzing audit logs (see Section 6, Security Audit for information on audit logs). The devices can use several time sources to automatically update the time: Network, Identity and Time Zone (NITZ); Global Positioning Satellites (GPS); Network Time Protocol (NTP) standards; or the cellular carrier time service. When configured and maintained using one of these time sources, the time may be considered reliable. Only the NTP is configurable by the mobile device administrator.

5.6.4.2 Mobile device users

In the evaluated configuration, the mobile device user is not allowed to configure the automatic time update options.

5.6.4.3 Mobile device administrators

The mobile device administrator can configure the mobile device to connect to a time server. Using the Time Server Payload, the *timeServer* and *timeZone* keys should be used. The following table provides additional details about these keys.

Key	Description
<i>timeserver</i>	This value represents the network time protocol (NTP) server to connect to.
<i>timeZone</i>	This value represents the timezone. It must be an entry in the <code>/usr/share/zoneinfo/</code> . Examples include: "America/Denver" or "Zulu"

The mobile administrator can disallow the mobile user from turning off the "Set Automatically" option for the date and time. In the Restrictions Payload, setting the *forceAutomaticDateAndTime* key to true turns on the Date and Time "Set Automatically" feature and it cannot be turned off by the mobile device user.

Additional information on these settings can be found in [DEV_MAN].

5.6.5 Access Banner Configuration

5.6.5.1 General information

In the evaluated configuration, the mobile devices are required to display an access banner as an advisory warning message regarding unauthorized use of the mobile device.

5.6.5.2 Mobile device users

In the evaluated configuration, the mobile device user is not allowed to configure the access banner.

5.6.5.3 Mobile device administrators

Also, the access banner can be configured by creating a background picture with the relevant information and configuring that picture as the background for the lock screen as described in the following document and section.

[DEV_MAN]: ["Profile-Specific Payload Keys"](#) → ["Restrictions"](#)

This banner is not allowed to be changed by the mobile device user in the evaluated configuration. To prevent the changing of the banner, set the *allowWallpaperModification* key to 'false' as described in [DEV_MAN].

The image is sent as a Base64 encoded image (as part of the Wallpaper command). It must be either a PNG or JPEG.

Alternatively, a notice and consent warning message can be configured through an app that provides the requisite notice and acknowledgement functionality rather than through iOS/iPadOS itself. The implementing organization must deploy a customizable application that provides users notice of the banner (e.g., through the Apple Push Notification Service) and also the ability to acknowledge the banner content within the application.

5.6.6 Enable/Disable Cameras and Microphones

5.6.6.1 General information

The cameras and microphones on the iPhone and iPad can be managed across the devices or on a per-app basis.

Additional information on these settings can be found in [DEV_MAN].

5.6.6.2 Mobile device users

Mobile device users can optionally disable the use of the cameras on a per-app basis. This can be done on the iPhone or iPad from [Settings » Privacy » Camera](#). If the mobile device administrator has restricted the use of the camera, then this functionality will not work.

Mobile device users can optionally disable the use of the microphones on a per-app basis. This can be done on the iPhone or iPad from [Settings » Privacy » Microphone](#).

5.6.6.3 Mobile device administrators

The mobile device administrator can optionally disallow camera use across the mobile device by using the key `allowCamera` in the Restrictions Payload.

The mobile device administrator can optionally disallow camera use on a per-app basis using the key `Camera` in the Privacy Preferences Policy Control Payload.

The mobile device administrator can optionally disallow microphone use on a per-app basis using the key `Microphone` in the Privacy Preferences Policy Control Payload.

Refer to [DEV_MAN] for more information.

5.6.7 Enable/Disable Cellular, Wi-Fi, Wi-Fi Hotspot, Bluetooth, NFC, UWB

5.6.7.1 General information

The devices contain a variety of radios which can be configured by the users or administrators according to the organization's policy.

5.6.7.2 Mobile device users

Mobile device users can enable/disable cellular by following instructions provided in the following documents and sections. (Sections 11.21 and 11.22 contain the screenshots from these documents.)

[iPhone_UG]: [“Safety, handling, and support”](#) → [“View or change cellular data settings on iPhone”](#)

[iPad_UG]: [“Safety, handling, and support”](#) → [“View or change cellular data settings on iPad \(Wi-Fi + Cellular models\)”](#)

Mobile device users can enable/disable Bluetooth by following the instructions provided in the following documents and sections. (Sections 11.3 and 11.4 contain screenshots from these documents.)

[iPhone_UG]: [“Accessories”](#) → [“Set up and use Bluetooth accessories on iPhone”](#)

[iPad_UG]: [“Accessories”](#) → [“Set up and use Bluetooth accessories on iPad”](#)

Further information on enabling and disabling Bluetooth can be found in [BLUETOOTH_HELP].

Mobile device users can enable/disable Wi-Fi by following the instructions provided in the following documents and sections. (Sections 11.23 and 11.24 contain the screenshots from these documents.)

[iPhone_UG]: [“Set up and get started”](#) → [“Connect iPhone to the internet”](#)

[iPad_UG]: [“Set up and get started”](#) → [“Connect iPad to the internet”](#)

Mobile device users can enable/disable Wi-Fi hotspot by following the instructions provided in the following documents and sections. (Sections 11.25 and 11.26 contain the screenshots from these documents.)

[iPhone_UG]: [“Use iPhone with iPad, iPod touch, Mac, and PC”](#) → [“Share your internet connection from iPhone”](#)

[iPad_UG]: [“Use iPad with iPhone, iPod touch, Mac, and PC”](#) → [“Share your internet connection from iPad \(Wi-Fi + Cellular\)”](#)

NFC will be disabled if there are no passes and no payment cards including credit/debit cards or Apple Cash stored in the Apple Wallet application and there are no third-party applications with NFC functionality installed on the device. Passes are stored data representing physical cards such as boarding passes and credit cards. When the mobile user adds a pass, a credit/debit card, Apple Cash, or installs an application with NFC capabilities, NFC is automatically activated. The mobile device administrator is able to disable NFC using a Configuration Profile key; see section 5.6.7.3 for details.

Instructions for adding passes are located in [PAY_SETUP]. Instructions for removing passes are located in [MANAGE_CARDS].

Mobile device users can enable/disable Ultra Wideband (UWB) communications by following the instructions provided in the following document and section. (Section 11.27 contains the screenshots from these documents.)

[iPhone_UG]: [“Safety, handling, and support”](#) → [“Ultra Wideband information”](#)

Only the following iPhone models possess UWB communication chips; iPads do not have UWB chips.

- iPhone 11, iPhone 11 Pro, iPhone 11 Pro Max
- iPhone 12 mini, iPhone 12, iPhone 12 Pro, iPhone 12 Pro Max
- iPhone 13 mini, iPhone 13, iPhone 13 Pro, iPhone 13 Pro Max

To disable only the UWB functionality while maintaining cellular and Wi-Fi functions, mobile device users should turn off “[Location for Networking & Wireless](#)” by navigating on the device to [Settings](#) » [Privacy](#) » [Location Services](#) » [System Services](#) and setting the “[Networking and Wireless](#)” toggle to the OFF position, then, at the prompt, confirm by selecting “[Turn Off](#).”

5.6.7.3 Mobile device administrators

The mobile device administrator can optionally restrict the mobile device from using cellular data by specifying the Network Usage Rules Payload key *AllowCellularData* to ‘false’.

The mobile device administrator can optionally restrict the mobile device user from modifying any cellular data settings by using the Restrictions Payload key:

allowAppCellularDataModification

The mobile device administrator can optionally enable/disable the ability of the mobile device user to modify Bluetooth settings by using the following Restrictions Payload key:

allowBluetoothModification

The mobile device administrator can optionally enable/disable Wi-Fi hotspot functionality by using the *IsHotspot* key in the Wi-Fi Payload.

Wi-Fi can effectively be enabled/disabled by an administrator setting the Restrictions Payload key *forceWiFiToAllowedNetworksOnly*.

The mobile device administrator can specify the allowed SSID of the Wi-Fi network that the iOS/iPadOS device can connect to by using the *SSID_STR* Configuration Profile key in the Wi-Fi Payload. To use this method of specifying SSIDs, the *DomainName* key in the Wi-Fi Payload must not be set.

The mobile device administrator can optionally enable/disable NFC by using the following Restrictions Payload key: *allowNFC*. If set to ‘false’, this will disable NFC. This requires a supervised device.

NFC can also be disabled by not having any passes stored in the Apple Wallet application, having no credit/debit payment cards or Apple Cash stored in the application and by not having any third-party applications with NFC capabilities on the device. Passes are stored data representing physical cards such as boarding passes. If there are no passes stored and no credit/debit payment cards or Apple Cash, the mobile device administrator can disable the Wallet application using the Restrictions payload key *blockedAppBundleIDs* with a string array containing the “com.apple.Passbook” bundle ID value. If the Wallet application is not disabled, the mobile device user can add a pass and enable NFC.

Refer to [DEV_MAN] for more information.

5.6.8 Enable/Disable Location Services

5.6.8.1 General information

Additional information on enabling and disabling location services can be found in [DEV_MAN].

5.6.8.2 Mobile device users

Device users can enable/disable location services by following the instructions provided in the following documents and sections. (Sections 11.28 and 11.29 contain the screenshots from these documents.)

[iPhone_UG]: ["Security and privacy"](#) → ["Privacy protections on iPhone"](#) → ["Control the location information you share on iPhone"](#)

[iPad_UG]: ["Security and privacy"](#) → ["Privacy protections on iPad"](#) → ["Control the location information you share on iPad"](#)

5.6.8.3 Mobile device administrators

The mobile device administrator can enable/disable location services during initial setup of the mobile device. This can occur after a device wipe or when setting up the device for the first time. Setting the `skip_setup_items` key to 'Location' causes the Setup Assistant to skip the Location Services screens. By skipping these screens, Location Services will not be set up.

More information can be found in [DeployRef] and [DEV_MAN].

5.6.9 Enable/Disable iCloud Drive Documents and Data

5.6.9.1 General information

The devices have the functionality to upload files to iCloud. In the evaluated configuration, this functionality must be disabled.

Additional information on this setting can be found in [DEV_MAN] and in the following documents and section. (Sections 11.30 and 11.31 contain the screenshots from these documents.)

[iPhone_UG]: ["Files"](#) → ["Set up iCloud Drive on iPhone"](#)

[iPad_UG]: ["Files"](#) → ["Set up iCloud Drive on iPad"](#)

5.6.9.2 Mobile device users

In the evaluated configuration, the mobile device user is not allowed to configure the iCloud Drive Documents and Data functionality.

5.6.9.3 Mobile device administrators

It is mandatory that the mobile device administrator disable iCloud Drive Documents and Data during initial setup of the device. Using the Restrictions Payload, the `allowCloudDocumentSync`

key should be used to disable this on a supervised device. The following table provides additional details about these keys.

Payload	Key	Description
Restrictions	<i>allowCloudDocumentSync</i>	Should be set to 'false'. This disables document and key-value syncing to iCloud.

Additional information on these settings can be found in [DEV_MAN].

5.6.10 Secure Software Updates

5.6.10.1 General information

The mobile device startup process helps ensure that only Apple-signed code can be installed on a device. To prevent devices from being downgraded to older versions that lack the latest security updates, iOS/iPadOS uses a process called System Software Authorization. If downgrades were possible, an attacker who gains possession of a device could install an older version of iOS/iPadOS and exploit a vulnerability that has been fixed in the newer version.

Software updates to the mobile devices are released regularly to address emerging security concerns and also provide new features; these updates are provided for all supported devices simultaneously. A request is sent to the mobile device to pull the update from the servers. Updates are delivered wirelessly, encouraging rapid adoption of the latest security fixes, as well as downloadable through the iTunes and Finder applications.

Mobile device users receive iOS/iPadOS update notifications on the mobile device, through Finder on macOS versions 10.13.0 (High Sierra) and higher, or through iTunes on macOS versions prior to 10.15.0 (Catalina) and on PCs. Note that the iTunes application is not available on macOS versions 10.15.0 and higher. The mobile device user is notified of the availability of the update upon connection of the device via a USB cable.

iOS/iPadOS software updates can be installed automatically (if the Software 'Automatic Updates' Settings are turned ON in [Settings » General » Software Update » Automatic Updates](#) on the device) or manually using over-the-air (OTA) on the device. Software updates may also be installed manually using Finder on macOS versions 10.13.0 (High Sierra) and higher or manually using iTunes on macOS versions prior to 10.15.0 (Catalina) and on PCs. A USB connection between the computer and the device is necessary to perform updates using Finder or iTunes.

With Finder or iTunes, a full copy of iOS/iPadOS is downloaded and installed. OTA software updates download only the components required to complete an update, rather than downloading the entire OS, improving network efficiency. Additionally, software updates can be cached on a local network server running the caching service on macOS Server so that iOS/iPadOS devices do not need to access Apple servers to obtain the necessary update data. Software updates may also be cached on a standard macOS system using the built-in Caching

Service, which can be found in *System Preferences » Sharing » Content Caching*. More information about content caching on macOS can be found in [CONTENT-CACHING].

All iOS/iPadOS updates are digitally signed by Apple. The user can verify the software version installed on the mobile devices. Refer to section 4.2.2 Verifying the device(s) for more information.

More info about iOS/iPadOS application and system security as well as encryption and data protection can be found in [AP_SEC].

5.6.10.2 Mobile device users

The integrity and authenticity of software updates is ensured by the design of iOS/iPadOS. There is no configuration for a device user to change that. Mobile device users can update iOS/iPadOS software on their device. Additional information can be found in the following documents and sections. (Sections 11.32 and 11.33 contain the screenshots from these documents.)

[iPhone_UG]: ["Restart, update, reset, and restore"](#) → ["Update iOS on iPhone"](#)

[iPad_UG]: ["Restart, update, reset, and restore"](#) → ["Update iPadOS"](#)

5.6.10.3 Mobile device administrators

The integrity and authenticity of software updates is ensured by the design of iOS/iPadOS. There is no configuration for a device administrator to change that.

Mobile device administrators can delay iOS/iPadOS software updates by setting the *forceDelayedSoftwareUpdates* and *enforcedSoftwareUpdateDelay* keys in the Restrictions Payload. More information can be found in document and section.

[DEV_MAN]: ["Profile-Specific Payload Keys"](#) → ["Restrictions"](#)

5.6.11 Enable/Disable Remote Backup

5.6.11.1 General information

The devices have the functionality to back up remotely to iCloud. In the evaluated configuration, this functionality must be disabled.

Backups are done using iCloud on the device or by connecting the device to a computer using a USB cable and using Finder on macOS versions 10.15.0 (Catalina) and higher or using iTunes on macOS versions prior to 10.15.0 and on PCs. Note that the iTunes application is not available on macOS versions 10.15.0 and higher.

If backup is enabled, iCloud automatically backs up a device daily when the device is connected to power, locked, and on Wi-Fi. In the evaluated configuration, backups to iCloud are not allowed and must be restricted by the mobile device administrator using a configuration profile. This does not restrict mobile device users from backing up a device to a Mac or PC, which is allowed in the evaluated configuration.

Users can also sync their iTunes content on computers supporting iTunes to their iPhone/iPad.

5.6.11.2 Mobile device users

Device users can use disable remote backup to iCloud or enable backup to a Mac or PC by following the instructions provided in the following documents and sections. (Sections 11.34 and 11.35 contain the screenshots from these documents.)

[iPhone_UG]: “Restart, update, reset, and restore” → “Back up iPhone”

[iPad_UG]: “Restart, update, reset, and restore” → “Back up iPad”

Mobile device users should note that backup to a Mac or PC is done by connecting the device to a computer using a USB cable and using Finder on macOS versions 10.15.0 (Catalina) and higher or using iTunes on macOS versions prior to 10.15.0 and on PCs. Note that the iTunes application is not available on macOS versions 10.15.0 and higher.

5.6.11.3 Mobile device administrators

In the evaluated configuration, administrators must disable remote backup for the mobile device to iCloud by setting the *allowCloudBackup* key to ‘false’ in the Restrictions Payload.

This does not restrict mobile device users from backing up a device to a Mac or PC, which is allowed in the evaluated configuration.

Additional information on these settings can be found in [DEV_MAN], and example Configuration Profiles can be found in Appendix A: Configuration Profiles.

5.6.12 Configure Application Installation Policy

5.6.12.1 General information

Apple recommends that MDM is used to manage applications for an enterprise. MDM can be used to help users install enterprise apps.

5.6.12.2 Mobile device users

In the evaluated configuration, mobile device users cannot change the application installation policy.

5.6.12.3 Mobile device administrators

It is mandatory that mobile device administrators configure an application installation policy.

This is accomplished by setting *allowAppInstallation* to ‘false’ in the Restrictions Payload, which means that the App Store is disabled. Mobile device users are unable to install or update their applications.

5.6.13 Importing keys/ shared secrets

5.6.13.1 General information

It is mandatory that keys can be imported and destroyed on the mobile devices by the mobile device administrators.

All keys/secrets are automatically stored in secure key storage.

5.6.13.2 Mobile device users

In the evaluated configuration, mobile device users cannot import and destroy keys/secrets.

5.6.13.3 Mobile device administrators

Mobile device administrators can import keys/secrets into the secure key storage by specifying the value when using dictionary keys that are associated with keys/secrets.

5.6.14 Dictionary Keys for Management Functions

Payload	Key	Description
Cameras and Microphones		
Restrictions	<i>allowCamera</i>	If set to 'false', it will completely disable the cameras.
Privacy Preferences Policy Control	<i>Camera</i>	Provides the array of bundle IDs / binary installation path that is not allowed to use the camera.
Privacy Preferences Policy Control	<i>Microphone</i>	Provides the array of bundle IDs / binary installation path that is not allowed to use the microphone.
Access Banner		
Restrictions	<i>allowWallpaperModification</i>	Must be 'false'.
Date and Time		
Restrictions	<i>forceAutomaticDateAndTime</i>	Must be 'true'.

Table 15: Essential keys for Management functions

6 Security Audit

6.1 Audit Logging

iOS/iPadOS logging capabilities collect a wide array of information concerning device usage and configuration. The available commands and responses constitute audit records and must be configured by administrators using Configuration Profiles. The details for profile implementation and audit record collection are located in [DEV_MAN], [PROFS_LOGS], and [LOGGING].

Each audit record, at a minimum, contains the following:

- Date and time of the event
- Type of event (this is described as log level and log tag)
- Subject identity (this is described as PID and PPID)
- The outcome (success or failure) of the event
- Any applicable required additional information

Each field of the example log below corresponds with the above format.

Date and Time	Type of event	Subject identity	The outcome
Dec 10 15:22:29.546196	<Error>:	iPadAir2 neagent[446]	Certificate authentication data could not be verified. Failed to process IKE Auth packet.

Table 16: Example audit log

The following tables list the auditable events for the required SFRs and provide example audit records.

SFR from {MDF} specified in the ST	Auditable events	Additional audit record contents	Example of audit records
FAU_GEN.1 {MDF}	Start-up and shutdown of the audit functions	No additional information.	Dec 5 11:34:58 iPadAir2 mdmd(libdyld.dylib)[6307] <Notice>: mdmd starting... Dec 5 11:39:19 iPadAir2 mdmd(libdyld.dylib)[6314] <Notice>: mdmd preparing to stop.
	All auditable events for the [not selected] level of audit	No additional information.	Dec 5 11:34:58 iPadAir2 mdmd(libdyld.dylib)[6307] <Notice>: mdmd starting...

SFR from {MDF} specified in the ST	Auditable events	Additional audit record contents	Example of audit records
	All administrative actions	No additional information.	Dec 5 12:30:48 iPadAir2 dmd[3038] <Notice>: Received request: <DMFInstallProfileRequest: 0x100c207f0>, from client: <CATTaskSession: 0x100c2f620 { state = Connected, session = BCD262D5-C3B1-4E1F-879C-900ADAF490E, transport = <CATXPCTransport: 0x100c375b0 { state = Connected }> }>
	Start-up and shutdown of the OS	No additional information.	<p>Apr 27 14:39:22 iPad SpringBoard(SpringBoard)[57] <Notice>: Shutdown requested for with context: <SBShutdownContext:0x282a38940 - reason:'Powerdown UI'; fromUserPowerDown:YES></p> <p>Apr 27 14:39:22 iPad SpringBoard(FrontBoard)[57] <Notice>: [com.apple.Preferences] Executing termination for reason shutting down system with request: <FBSPProcessTerminationRequest: 0x283f717c0; label: "Shutdown (<SBShutdownContext:0x282a38940 - reason:'Powerdown UI'; fromUserPowerDown:YES>)">; exceptionCode: "Force Quit (0xFBFBFBFB)"; performGracefully: YES; reportType: (none); explanation: "Shutdown (<SBShutdownContext:0x282a38940 - reason:'Powerdown UI'; fromUserPowerDown:YES>)"></p> <p>Apr 27 14:39:22 iPad CommCenter(IMFoundation)[80] <Notice>: IMSystemMonitor: Updating to note that system is currently shutting down</p> <p>Apr 27 14:39:22 iPad rapportd(IMFoundation)[76] <Notice>: IMSystemMonitor: Received IMSystemMonitorSBShutdownCallback</p> <p>Apr 27 14:39:22 iPad rapportd(IMFoundation)[76] <Notice>: IMSystemMonitor: Updating to note that system is currently shutting down</p> <p>Apr 27 14:39:22 iPad contextstored(CoreDuet)[56] <Notice>: Got shutdown notification com.apple.springboard.deviceWillShutDown</p>

SFR from {MDF} specified in the ST	Auditable events	Additional audit record contents	Example of audit records
			<p>Apr 27 14:39:22 iPad contextstored(CoreDuet)[56] <Notice>: Calling shutdown handler for monitor <private>.</p> <p>Apr 27 14:39:22 iPad SpringBoard(RunningBoardServices)[57] <Notice>: Firing exit handlers for 190 with context <RBSPProcessExitContext; specific: <RBSPProcessExitStatus; domain: frontboard (10); code: 0xfbfbfbfb>; terminationContext: <RBSTerminateContext: 0x2831c9540; domain: 10; code: 0xFBFBFBFB; explanation: "Shutdown (<SBShutdownContext:0x282a38940 - reason:'Powerdown UI'; fromUserPowerDown:YES>)"</p>
	Insertion or removal of removable media	No additional information	<p>default 02:40:02.471883-0700 livefileproviderd ReallyMountVolume: Enter on behalf of process 2102 for provider com.apple.filesystems.UserFS.FileProvider mounting: /private/var/mobile/Library/LiveFiles/com.apple.filesystems.userfsd/Thumb</p> <p>default 02:40:53.494457-0700 livefileproviderd Unmounting /private/var/mobile/Library/LiveFiles/com.apple.filesystems.userfsd/Thumb how 03 on behalf of pid 2102</p>
FCS_STG_EXT.1 {MDF}	Import or key destruction	Identity of key. Role and identity of requestor.	<p>49506633: AKS unwrap_media_key_from_class succeeded for tag = 7</p> <p>49506633: aks_migrate_SEPUUID2b_to_classM_key() succeeded for AES, container = /dev/disk0s1</p> <p>49506633: AKS unwrap_media_key_from_class succeeded for tag = 7</p> <p>apfs_meta_crypto_state_unwrap:980: got key for volume 2F29025D-A75E-40CE-9EFE-61A6B8848880</p> <p>apfs_device_locked:3837: apfs Data is now UNlocked! (flags 0x40)</p>

SFR from {MDF} specified in the ST	Auditable events	Additional audit record contents	Example of audit records
FCS_STG_EXT.3 {MDF}	Failure to verify integrity of stored key.	Identity of key being verified.	apfs_unwrap_key:1263: AKS unwrap_key failed, error = e00002e2
FDP_DAR_EXT.1 {MDF}	Failure to encrypt/decrypt data.	No additional information.	Sep 25 09:19:38 iPad securityd[96] <Notice>: ks_encrypt_data (db): failed: AppleKeyStore: operation failed (pid: 156 sel: 17 ret: e00002c2 '-536870206')
FDP_DAR_EXT.2 {MDF}	Failure to encrypt/decrypt data.	No additional information.	Sep 25 09:19:38 iPad securityd[96] <Notice>: ks_encrypt_data (db): failed: AppleKeyStore: operation failed (pid: 156 sel: 17 ret: e00002c2 '-536870206')
FDP_STG_EXT.1 {MDF}	Addition or removal of certificate from Trust Anchor Database	Subject name of certificate	May 13 13:40:22 iPad mc_mobile_tunnel(MDM)[4225] <Notice>: Attempting to perform Supervised request: RemoveProfile May 13 13:40:22 iPad profiled[97] <Notice>: Removing profile \M-b\M^\M^\Testers-MacBook-Air.local.D3DACE3B-FD7E-489B-B20C-FC89E076C028\M-b\M^\M^\]... May 13 13:40:22 iPad profiled[97] <Notice>: Committing restrictions.
FIA_X509_EXT.1 {MDF}	Failure to validate x.509v3 certificate	Reason for failure of validation	default 14:49:33.115596+0200 nsurlsessiond boringssl_session_handshake_incomplete(191) [C5.1:2][0x10119f090] Early handshake return caused by SSL_ERROR_WANT_CERTIFICATE_VERIFY [16]
FPT_TST_EXT.1 {MDF}	Initiation of self-test	No additional information.	SEP: SEP: FIPS POST begin SEP: FIPSPOST_L4 fipspost_post:109: PASSED: (2 ms) - fipspost_post_integrity SEP: sks: FIPS POST Succeeded
	Failure of self-test	No additional information.	fipspost_post fipspost_post_integrity -POST_FAILURE: 0xFFFFFFFF
FPT_TST_EXT.2/PR EKERNEL {MDF}	Start-up of TOE	No additional information.	Darwin Kernel Version 19.0.0: Wed Oct 9 22:37:47 PDT 2019; root:xnu_development-6153.42.1~1/DEVELOPMENT_ARM64_T8010 iBoot version: iBoot-5540.40.51

Table 17: {MDF} auditable events

SFR from {WLAN} specified in the ST	Auditable events	Additional audit record contents	Example of audit records
FCS_TLSC_EXT.1/WLAN {WLAN}	Failure to establish an EAP-TLS session.	Reason for failure. Non-TOE device endpoint connection.	<p>May 13 15:28:40 iPad wifid(WiFiPolicy)[45] <Notice>: {ASSOC+} Attempting Apple80211AssociateAsync</p> <p>May 13 15:28:40 iPad wifid(WiFiPolicy)[45] <Notice>: Attempting to join EAP network: test</p> <p>May 13 15:28:41 iPad wifid(WiFiPolicy)[45] <Notice>: {ASSOC*} Completed Apple80211AssociateAsync (-3905 - 0xFFFFF0BF)</p> <p>May 13 15:28:41 iPad wifid(WiFiPolicy)[45] <Error>: {ASSOC-} Failed to join(-3905 - 0xFFFFF0BF): test</p>
	Establishment/termination of an EAP-TLS session.	Reason for failure. Non-TOE device endpoint connection.	<p>May 13 15:28:40 iPad wifid(WiFiPolicy)[45] <Notice>: {ASSOC+} Attempting Apple80211AssociateAsync</p> <p>May 13 15:28:40 iPad wifid(WiFiPolicy)[45] <Notice>: Attempting to join EAP network: test</p> <p>May 13 15:28:41 iPad wifid(WiFiPolicy)[45] <Notice>: {ASSOC*} Completed Apple80211AssociateAsync (-3905 - 0xFFFFF0BF)</p> <p>May 13 15:28:41 iPad wifid(WiFiPolicy)[45] <Error>: {ASSOC-} Failed to join(-3905 - 0xFFFFF0BF): test</p>
FIA_X509_EXT.1/WLAN {WLAN}	Failure to validate x.509v3 certificate	Reason for failure of validation	<p>default 14:49:33.115596+0200 nsurlsessiond boringssl_session_handshake_incomplete(191) [C5.1:2][0x10119f090] Early handshake return caused by SSL_ERROR_WANT_CERTIFICATE_VERIFY [16]</p>

SFR from {WLAN} specified in the ST	Auditable events	Additional audit record contents	Example of audit records
FPT_TST_EXT.1/WLAN {WLAN}	Execution of this set of TSF self-test.	No additional information.	corecrypto_kext_start called: tracing enabled FIPSPOST_KEXT fipspost_post:109: PASSED: (0 ms) - fipspost_post_integrity FIPSPOST_KEXT fipspost_post:115: PASSED: (0 ms) - fipspost_post_hmac FIPSPOST_KEXT fipspost_post:117: PASSED: (0 ms) - fipspost_post_aes_ecb FIPSPOST_KEXT fipspost_post:118: PASSED: (0 ms) - fipspost_post_aes_cbc FIPSPOST_KEXT fipspost_post:119: PASSED: (0 ms) - fipspost_post_aes_gcm FIPSPOST_KEXT fipspost_post:120: PASSED: (0 ms) - fipspost_post_aes_xts FIPSPOST_KEXT fipspost_post:121: PASSED: (0 ms) - fipspost_post_tdes_cbc FIPSPOST_KEXT fipspost_post:125: PASSED: (39 ms) - fipspost_post_rsa_sig FIPSPOST_KEXT fipspost_post:126: PASSED: (9 ms) - fipspost_post_ecdsa FIPSPOST_KEXT fipspost_post:127: PASSED: (2 ms) - fipspost_post_ecdh FIPSPOST_KEXT fipspost_post:128: PASSED: (0 ms) - fipspost_post_drbg_ctr FIPSPOST_KEXT fipspost_post:129: PASSED: (0 ms) - fipspost_post_drbg_hmac FIPSPOST_KEXT fipspost_post:136: all tests PASSED (129 ms)
FTA_WSE_EXT.1 {WLAN}	All attempts to connect to access points.	Identity of access point being connected to as well as success and failures (including	May 13 15:28:40 iPad wifid(WiFiPolicy)[45] <Notice>: {ASSOC+} Attempting Apple80211AssociateAsync May 13 15:28:40 iPad wifid(WiFiPolicy)[45] <Notice>: Attempting to join EAP network: test

SFR from {WLAN} specified in the ST	Auditable events	Additional audit record contents	Example of audit records
		reason for failure)	<p>May 13 15:28:41 iPad wifid(WiFiPolicy)[45] <Notice>: {ASSOC*} Completed Apple80211AssociateAsync (-3905 - 0xFFFFF0BF)</p> <p>May 13 15:28:41 iPad wifid(WiFiPolicy)[45] <Error>: {ASSOC-} Failed to join(-3905 - 0xFFFFF0BF): test</p>
FTP_ITC_EXT.1/WLAN {WLAN}	All attempts to establish a trusted channel.	Identification of the non-TOE device endpoint of the channel.	<p>Apr 27 15:36:58 iPad wifid(WiFiPolicy)[45] <Notice>: {ASSOC+} Attempting Apple80211AssociateAsync</p> <p>Apr 27 15:36:58 iPad wifid(WiFiPolicy)[45] <Notice>: Attempting to join WPA network: test</p> <p>Apr 27 15:36:59 iPad wifid(WiFiPolicy)[45] <Notice>: {ASSOC*} Completed Apple80211AssociateAsync (0 - 0x0)</p> <p>Apr 27 15:36:59 iPad wifid(WiFiPolicy)[45] <Notice>: {ASSOC-} Joined: test</p>

Table 18: {WLAN} auditable events

SFR from {AGENT} specified in the ST	Auditable events	Additional audit record contents	Example of audit records
FAU_ALT_EXT.2 {AGENT}	Success/failure of sending alert.	No additional information.	<p>Success: 15:20:20.164655-0500 default profiled Beginning profile installation for com.apple.config.mdm01.cc.atsec.us.mdm profiled com.apple.ManagedConfiguration 15:20:56.320020-0500 default profiled Profile "com.apple.config.mdm01.cc.atsec.us.mdm" installed. Profiled com.apple.ManagedConfiguration</p>

SFR from {AGENT} specified in the ST	Auditable events	Additional audit record contents	Example of audit records
			<p>13:30:52.778054-0500 default mdmd Accepted new connection. MDM mdmd 13:30:45.799798-0500 default profiled Sending MDM settings changed notification.</p> <p>Failure: 11:50:29.527861-0500 error profiled Cannot Check Out. Error: NSError: Desc : The Internet connection appears to be offline. Domain : NSURLErrorDomain Code : -1009 Type : DMCFatalError MDMClientLibrary.com.apple.devicemanagementclient</p>
FAU_GEN.1(2) {AGENT}	Start-up and shutdown of the MDM Agent	No additional information.	<p>Dec 5 11:34:58 iPadAir2 mdmd(libdyld.dylib)[6307] <Notice>: mdmd starting...</p> <p>Dec 5 11:39:19 iPadAir2 mdmd(libdyld.dylib)[6314] <Notice>: mdmd preparing to stop.</p>
	MDM policy updated.	No additional information.	<p>May 13 14:10:46 iPad profiled[97] <Notice>: Profile \M-b\M^\M^\Tester-MacBook-Air.local.D3DACE3B-FD7E-489B-B20C-FC89E076C028\M-b\M^\M^\M^\ is replacing an existing profile having the same identifier.</p>
	Any modification commanded by the MDM Server	No additional information.	<p>default 15:05:35.071156+0200 mdmd Received push notification.</p>
FAU_SEL.1(2) {AGENT}	All modifications to the audit configuration that occur while the audit collection functions are operating.	No additional information.	<p>May 13 14:40:22 iPad profiled[97] <Notice>: Profile \M-b\M^\M^\Tester-MacBook-Air.local.D3DACE3B-FD7E-489B-B20C-FC89E076C028\M-b\M^\M^\M^\ removed.</p>
			<p>May 13 13:40:22 iPad mc_mobile_tunnel(MDM)[4225] <Notice>: Attempting to perform Supervised request: RemoveProfile</p> <p>May 13 14:10:22 iPad mc_mobile_tunnel(MDM)[4225] <Notice>: Handling request type: RemoveProfile</p>

SFR from {AGENT} specified in the ST	Auditable events	Additional audit record contents	Example of audit records
			<p>May 13 13:40:22 iPad mc_mobile_tunnel(MDM)[4225] <Notice>: Attempting to perform Supervised request: RemoveProfile</p> <p>May 13 13:40:22 iPad profiled[97] <Notice>: Removing profile \M-b\M^\M^\Tester-MacBook-Air.local.D3DACE3B-FD7E-489B-B20C-FC89E076C028\M-b\M^\M^\M^\...</p> <p>May 13 13:40:22 iPad profiled[97] <Notice>: Committing restrictions.</p>
FCS_TLSC_EXT.1 {AGENT}	Failure to establish a TLS session	Reason for failure.	<p>May 13 15:28:40 iPad wifid(WiFiPolicy)[45] <Notice>: {ASSOC+} Attempting Apple80211AssociateAsync</p> <p>May 13 15:28:40 iPad wifid(WiFiPolicy)[45] <Notice>: Attempting to join EAP network: test</p> <p>May 13 15:28:41 iPad wifid(WiFiPolicy)[45] <Notice>: {ASSOC*} Completed Apple80211AssociateAsync (-3905 - 0xFFFFF0BF)</p> <p>May 13 15:28:41 iPad wifid(WiFiPolicy)[45] <Error>: {ASSOC-} Failed to join(-3905 - 0xFFFFF0BF): test</p>
	Failure to verify presented identifier	Presented identifier and reference identifier.	<p>May 13 15:28:40 iPad wifid(WiFiPolicy)[45] <Notice>: {ASSOC+} Attempting Apple80211AssociateAsync</p> <p>May 13 15:28:40 iPad wifid(WiFiPolicy)[45] <Notice>: Attempting to join EAP network: test</p> <p>May 13 15:28:41 iPad wifid(WiFiPolicy)[45] <Notice>: {ASSOC*} Completed Apple80211AssociateAsync (-3905 - 0xFFFFF0BF)</p> <p>May 13 15:28:41 iPad wifid(WiFiPolicy)[45] <Error>: {ASSOC-} Failed to join(-3905 - 0xFFFFF0BF): test</p>
	Establishment/termination of a TLS session.	Non-TOE device	May 13 15:28:09 iPad nsurlsessiond(CFNetwork)[162] <Notice>: Connection 571: enabling TLS

SFR from {AGENT} specified in the ST	Auditable events	Additional audit record contents	Example of audit records
		endpoint of connection.	
FIA_ENR_EXT.2 {AGENT}	Enrollment in management	Reference identifier of MDM Server.	<p>default 14:09:39.308624+0200 profiled Checking for MDM installation...</p> <p>default 14:09:39.312514+0200 profiled ...finished checking for MDM installation.</p> <p>default 14:09:39.318516+0200 profiled Beginning profile installation...</p> <p>default 14:09:39.318710+0200 profiled Beginning profile installation for com.apple.config.osxserver.atsec.com.mdm</p> <p>default 14:09:39.321386+0200 profiled Profile "com.apple.config.osxserver.atsec.com.mdm" is replacing an existing profile having the same identifier.</p> <p>default 14:09:39.346118+0200 profiled Refreshing MDM details.</p> <p>Default 14:09:39.346309+0200 profiled No MDM installation found.</p>
FMT_POL_EXT.2 {AGENT}	Failure of policy validation.	Reason for failure of validation.	<p>error 17:13:20.765096+0200 wifid {ASSOC-} Failed to join(-369033199 - 0xEA010011): test</p> <p>default 15:19:57.113029+0200 wifid {AUTOJOIN, ASSOC*} Failed to associate with test, reason -369033199</p>
FMT_SMF_EXT.4 {AGENT}	Outcome (Success/failure) of function.	No additional information.	default 15:05:35.071156+0200 mdmd Received push notification.
FMT_UNR_EXT.1 {AGENT}	Attempt to unenroll	No additional information.	<p>Default 19:43:43.048171-0800 Preferences _didHideAlertController: <UIAlertController: 0x10a025600> title="Remove Management" message="Removing your iPad from management will delete 14 apps and their data."</p> <p>Default 19:43:43.096961-0800 profiled Removing profile "00000000-0000-0000-A000-4A414D460003" on behalf of "com.apple.Preferences"...</p>

SFR from {AGENT} specified in the ST	Auditable events	Additional audit record contents	Example of audit records
FTP_ITC_EXT.1(2) {AGENT}	Initiation and termination of trusted channel.	Trusted channel protocol. Non-TOE device endpoint of connection.	Apr 27 15:36:58 iPad wifid(WiFiPolicy)[45] <Notice>: {ASSOC+} Attempting Apple80211AssociateAsync Apr 27 15:36:58 iPad wifid(WiFiPolicy)[45] <Notice>: Attempting to join WPA network: test Apr 27 15:36:59 iPad wifid(WiFiPolicy)[45] <Notice>: {ASSOC*} Completed Apple80211AssociateAsync (0 - 0x0) Apr 27 15:36:59 iPad wifid(WiFiPolicy)[45] <Notice>: {ASSOC-} Joined: test

Table 19: {AGENT} auditable events

SFR from {BT} specified in the ST	Auditable events	Additional audit record contents	Example of audit records
FAU_GEN.1/BT {BT}	Start-up and shutdown of the audit functions	No additional information.	Dec 5 11:34:58 iPadAir2 mdmd(libdyld.dylib)[6307] <Notice>: mdmd starting... Dec 5 11:39:19 iPadAir2 mdmd(libdyld.dylib)[6314] <Notice>: mdmd preparing to stop.
FIA_BLT_EXT.1 {BT}	Failed user authorization of Bluetooth device.	User authorization decision (e.g., user rejected connection, incorrect pin entry).	default 08:55:22.471374-0600 bluetoothd Session "com.apple.Preferences-MBF-419-0-unique-id-com.apple.Preferences-419" is asking to disconnect device " Test-Lab-System1" Decision: default 08:56:35.373472-0600 bluetoothd Rejecting SSP request for device 744DD52B
	Failed user authorization for local Bluetooth Service.	Bluetooth address and name of device. Bluetooth profile. Identity of local service with service ID.	default 08:53:41.365190-0600 bluetoothd Device found: CBDevice 9D6E9A89-6C27-273D-1295-B73EC2FDF868, BDA 7C:7A:91:E3:B1:00, Nm 'Test-Lab-System1', PID 0x0246 (?), VID 0x1D6B, VS 2, DsF 0x800000 < Pairing >, DvF 0x54000 < ClsP HIDG UsrC >, DvT LaptopComputer, RSSI -57, Color 0, FV '5.3.12', MicM Auto, Plcm M Enabled, srMd Disabled, CF 0x800000000000 < Attr > Local device ID:

SFR from {BT} specified in the ST	Auditable events	Additional audit record contents	Example of audit records
			<pre> default 08:50:11.358071-0600 cloudpaired Successfully sending message { MessageType = CloudPairing; "Version 1" = { DeviceName = "iPhone-A14_updated"; EncryptionType = Basic; MessageType = PairingRequest; PublicAddress = "8C:EC:7B:06:16:D5"; RequestedKeyLength = 16; RequestedKeyType = (EncryptionKeys, IdentityKeys); "Version 2" = { DeviceName = "iPhone-A14_updated"; EncryptionType = ECDH; MessageType = InitiatorPairingKeys; PublicAddress = "8C:EC:7B:06:16:D5"; RequestedKeyLength = 16; RequestedKeyType = (PublicKeys, IdentityKeys); RequestedKeys = { CloudNonce = {length = 16, bytes = 0xfd0dab7cea305af21fb7d8b7f86fe1a2}; CloudPublicKey = {length = 64, bytes = 0x27b6adf0 8b2b90ab cb344a1b 07b43042 ... f879146b 2e6b2adf }; IRK = {length = 16, bytes = 0xcd318d659b7febadf7f50c3623e86ac4}; TimeStamp = 751850567329; }; "Version 3" = { DeviceName = "iPhone-A14_updated"; EncryptionType = ECDH; MessageType = InitiatorPairingKeys; PublicAddress = "8C:EC:7B:06:16:D5"; RequestedKeyLength = 16; RequestedKeyType = (PublicKeys, IdentityKeys); RequestedKeys = { CloudNonce = {length = 16, bytes = 0xfd0dab7cea305af21fb7d8b7f86fe1a2}; CloudPublicKey = {length = 64, bytes = 0x27b6adf0 8b2b90ab cb344a1b 07b43042 ... f879146b 2e6b2adf }; </pre>

SFR from {BT} specified in the ST	Auditable events	Additional audit record contents	Example of audit records
			IRK = {length = 16, bytes = 0xcd318d659b7febadf7f50c3623e86ac4};}; TimeStamp = 751850567329};}
FIA_BLT_EXT.2 {BT}	Initiation of Bluetooth connection.	Bluetooth address and name of device.	default 08:54:05.557719-0600 bluetoothd Session "com.apple.Preferences-MBF-419-83-unique-idcom.apple.Preferences-419" is asking to connect device "Test-Lab-System1" default 08:53:41.365190-0600 bluetoothd Device found: CBDevice 9D6E9A89-6C27-273D-1295-B73EC2FDF868, BDA 7C:7A:91:E3:B1:00, Nm 'Test-Lab-System1', PID 0x0246 (?), VID 0x1D6B, VS 2, DsF 0x800000 < Pairing >, DvF 0x54000 < ClsP HIDG UsrC >, DvT LaptopComputer, RSSI -57, Color 0, FV '5.3.12', MicM Auto, Plcm M Enabled, srMd Disabled, CF 0x800000000000 < Attr >
	Failure of Bluetooth connection.	Reason for failure.	error 08:55:22.467318-0600 bluetoothd Connection to device 744DD52B failed - result was 705

Table 20: {BT} auditable events

Table 20 does not include FIA_BLT_EXT.3 {BT} because the rejections happen at the Host Controller Interface (HCI) layer; thus, the TOE does not generate audit records for Bluetooth duplicate connection attempts.

6.2 Audit Storage

Audit records cannot be directly accessed by device users, administrators, or MDM administrators on the iOS/iPadOS device regardless of the device's configuration. [AConfig] describes how to use the mobile device console to see all logged records. The device console is a function within Apple Configurator 2. While viewing the log files, Administrators have capabilities such as: marking selections, clearing the window to view specific events, or saving the log for troubleshooting.

Additionally, audit records cannot be modified in any way. All audit records can be synced to an MDM application using a Configuration Profile or manually via a trusted workstation using the Apple Configurator 2.

Depending on the underlying OS of the trusted workstation or MDM server, all of the mobile device audit records are transferred to the following locations.

macOS

- ~/Library/Logs/CrashReporter/MobileDevice/[Your_Device_Name]/

Windows

- C:\Users\[Your_User_Name]\AppData\Roaming\AppleComputer\Logs\CrashReporter\MobileDevice\[Your_Device_Name]\

Audit records are not confined by a global capacity limit and are instead predefined individual services depending on what information is being captured. More information may be found in [PROFS_LOGS].

iOS/iPadOS has a logging framework that is used to configure different logging levels for the various iOS/iPadOS subsystems. This framework is configured by creating and installing a logging configuration profile property list file (i.e., .plist file) into the appropriate directory. More information may be found in [LOGGING].

There is no configuration required for audit log locations because audit logs are stored in the locations specified in this section, by default. These locations cannot be changed.

If unified logging is used, log messages are written to centralized data store on disk instead of in different directories as text log files. More information may be found in [LOGGING].

6.3 Configure the Auditable Items

According to [PROFS_LOGS], additional logs can be specified by performing user actions on a device or through using a Configuration Profile. The table below shows which audit logs can be optionally gathered and how they can be initiated.

Log type	Device user	Configuration Profile
Third-party Apps for iOS	Instructions	
Accounts/AuthKit for iOS	Instructions	Profile
Ad Platforms for iOS	Instructions	Profile
AirTraffic for iOS	Instructions	
APNS (Apple Push Notification Service) for iOS	Instructions	Profile
App Store for iOS	Instructions	Profile
Apple Pay for iOS	Instructions	Profile
Background Networking for iOS	Instructions	
Baseband for iOS	Instructions	Profile
Battery Life for iOS	Instructions	Profile
Bluetooth for iOS	Instructions	Profile
Calendar/Reminders for iOS	Instructions	Profile
Carousel for iOS	Instructions	
CarPlay for iOS	Instructions	Profile

Log type	Device user	Configuration Profile
CFNetwork for iOS	Instructions	Profile
Charles Logs for iOS	Instructions	
Classroom for iOS	Instructions	Profile
CloudKit for iOS	Instructions	Profile
Console Logs for iOS	Instructions	
Contacts Data Export for iOS	Instructions	
Continuity (IDS) for iOS	Instructions	Profile
CoreMedia (HTTP Live Streaming) for iOS	Instructions	Profile
Crash Logs for iOS	Instructions	
Device-specific Information for iOS	Instructions	
Disk Space Diagnostics (FSMetadata) for iOS	Instructions	Profile
Enterprise SSO and Kerberos for iOS	Instructions	Profile
FaceTime for iOS	Instructions	Profile
Handoff for iOS	Instructions	
HangTracer (Slow UI)	Instructions	Profile
Health Database Extraction for iOS	Instructions	
HealthKit for iOS	Instructions	Profile
Home app/HomeKit for iOS	Instructions	Profile
HomePod for iOS	Instructions	Profile
iAP for iOS	Instructions	Profile
iCloud Backup for iOS	Instructions	Profile
iCloud Drive for iOS	Instructions	Profile
iCloud Photos for iOS	Instructions	Profile
iWork for iOS	Instructions	Profile
Location Services for iOS	Instructions	Profile
Mail for iOS	Instructions	Profile
Mail Sync Diagnostics for iOS	Instructions	
Managed Configuration (MDM) for iOS	Instructions	Profile
Maps for iOS	Instructions	Profile
mDNSResponder for iOS	Instructions	Profile

Log type	Device user	Configuration Profile
Media Player for iOS	Instructions	
Messages for iOS	Instructions	Profile
Multipeer Connectivity for iOS	Instructions	
Music for iOS	Instructions	
Network Diagnostics for iOS	Instructions	Profile
Notes for iOS	Instructions	Profile
Phone (General) for iOS	Instructions	Profile
Photos Logging for iOS	Instructions	Profile
Podcasts for iOS	Instructions	
Schoolwork/ClassKit	Instructions	Profile
Screenshots and Screen Recordings for iOS	Instructions	
Significant Locations for iOS	Instructions	Profile
Single Sign-On for iOS	Instructions	Profile
Siri for iOS	Instructions	Profile
Slow Launches (Launch Hangs) for iOS	Instructions	Profiles
Software Update for iOS	Instructions	Profile
Spotlight for iOS	Instructions	Profile
Stackshots for iOS	Instructions	
Sync Diagnostics (DataAccess) for iOS	Instructions	Profile
sysdiagnose for iOS	Instructions	Profile
Tailspin for iOS	Instructions	Profile
TCP Dump for iOS	Instructions	
Test Cases/Sample Projects for iOS	Instructions	
TestFlight for iOS	Instructions	Profile
Touch ID for iOS	Instructions	Profile
Unlock for iOS	Instructions	
Updater for iOS	Instructions	
VPN (Network Extension) for iOS	Instructions	Profile
Wallet for iOS	Instructions	Profile
Wi-Fi for iOS	Instructions	Profile

Table 21: Additional Audit Logs

7 Installed Apps

Table 22: Built-in and Preinstalled Apps lists the built-in and preinstalled applications on the mobile devices. Those marked “Built-in” cannot be removed. Those marked “Preinstalled” are included with purchased devices but may be removed by the user or administrator.

Devices purchased in accordance with section 4.2.1 “Obtaining the mobile device(s)” do not include any other third-party applications when purchased.

App Name	iPad	iPhone
App Store	Built-in	Built-in
Books	Built-in	Built-in
Calculator	Not Available	Built-in
Calendar	Built-in	Built-in
Camera	Built-in	Built-in
Clock	Built-in	Built-in
Compass	Not Available	Built-in
Contacts	Built-in	Built-in
FaceTime	Built-in	Built-in
Files	Built-in	Built-in
Find My	Built-in	Built-in
Health	Not Available	Built-in
Home	Built-in	Built-in
iTunes Store	Built-in	Built-in
Magnifier	Built-in	Built-in
Mail	Built-in	Built-in
Maps	Built-in	Built-in
Measure	Built-in	Built-in
Messages	Built-in	Built-in
Music	Built-in	Built-in
News	Built-in	Built-in
Notes	Built-in	Built-in
Phone	Not Available	Built-in
Photo Booth	Built-in	Not Available
Photos	Built-in	Built-in

App Name	iPad	iPhone
Podcasts	Built-in	Built-in
Reminders	Built-in	Built-in
Safari	Built-in	Built-in
Settings	Built-in	Built-in
Shortcuts	Built-in	Built-in
Siri	Built-in	Built-in
Stocks	Built-in	Built-in
Tips	Built-in	Built-in
Translate	Built-in	Built-in
TV	Built-in	Built-in
Voice Memos	Built-in	Built-in
Wallet	Not Available	Built-in
Watch	Not Available	Built-in
Weather	Not Available	Built-in
Apple Store	Preinstalled	Preinstalled
Clips	Preinstalled	Preinstalled
GarageBand	Preinstalled	Preinstalled
iMovie	Preinstalled	Preinstalled
Keynote	Preinstalled	Preinstalled
Numbers	Preinstalled	Preinstalled
Pages	Preinstalled	Preinstalled

Table 22: Built-in and Preinstalled Apps

8 References

Table 1: Guidance Documents, contains the references to the guidance documents used when configuring the mobile devices. Below are the references documents providing further more detailed technical information.

[BT] Specification of the Bluetooth System

<https://www.bluetooth.com/specifications>

[PP_MDF_V3.2] U.S. Government Approved Protection Profile - Protection Profile for Mobile Device Fundamentals, Version 3.2

<https://www.niap-ccevs.org/Profile/Info.cfm?PPID=455&id=455>

[MOD_MDM_AGENT_V1.0] U.S. Government Approved Protection Profile – PP-Module for MDM Agents Version 1.0

<https://www.niap-ccevs.org/Profile/Info.cfm?PPID=441&id=441>

[MOD_BT_V1.0] PP-Module for Bluetooth Version 1.0

<https://www.niap-ccevs.org/Profile/Info.cfm?PPID=425&id=425>

[MOD_VPNC_V2.3] PP-Module for VPN Client Version 2.3

<https://www.niap-ccevs.org/Profile/Info.cfm?PPID=461&id=461>

[PP_WLAN_CLI_EP_V1.0] Extended Package for WLAN Client Version 1.0

<https://www.niap-ccevs.org/Profile/Info.cfm?id=386>

[PKG_TLS_V1.1] Functional Package for Transport Layer Security (TLS) Version 1.1

<https://www.niap-ccevs.org/Profile/Info.cfm?PPID=439&id=439>

9 Abbreviations and Acronyms

ABM	Apple Business Manager	IV	Initialization Vector
AES	Advanced Encryption Standard	JSON	JavaScript Object Notation
API	Application Programming Interface	JTAG	Joint Test Action Group
APNS	Apple Push Notification Service	KEK	Key Encryption Key
ARM	Advanced RISC Machine	L2TP	Layer Two Tunneling Protocol
ASLR	Anti-Exploitation Services	LE	Low Energy
BR/EDR	Basic Rate/Enhanced Data Rate	LTE	Long-Term Evolution
CA	Certificate of Authority	MAC	Message Authentication Code
CBC	Cypher Block Chaining	MDF	Mobile Device Fundamentals
CC	Common Criteria	MDFPP	Mobile Device Fundamentals Protection Profile
CCM	Counter with CBC-MAC	MDM	Mobile Device Management
CRL	Certificate Revocation List	NITZ	Network Identity and Time Zone
DAR	Data-at-Rest	NFC	Near Field Communication
DEK	Data Encryption Key	NTP	Network Time Protocol
DEP	Device Enrollment Program	OCSP	Online Certificate Status Protocol
DES	Data Encryption Standard	OTA	Over-the-Air
DH	Diffie-Hellman	PAE	Port Access Entity
DRBG	Deterministic Random Bit Generator	PBKDF	Password Based Key Derivation Function
EAP	Extensible Authentication Protocol	PKCS	Public Key Cryptography Standards
EAP-TLS	Extensible Authentication Protocol-Transport Layer Security	PKI	Public Key Infrastructure
ECC	Elliptic Curve Cryptography	PP	Protection Profile
ECDH	Elliptic Curve Diffie-Hellman	REK	Root Encryption Key
ECDSA	Elliptic Curve Digital Signature Algorithm	RISC	Reduced Instruction Set Computing
EP	Extended Package	RSA	Rivest-Shamir-Adleman
FIA	Identification and Authentication	SA	Secure Association
FIPS	Federal Information Processing Standard	SCEP	Simple Certificate Enrollment Protocol
FQDN	Fully Qualified Domain Name	SEP	Secure Enclave Processor
GCM	Galois/Counter Mode	SFR	Security Functional Requirement
GPS	Global Positioning Satellites	SHA	Secure Hash Algorithm
GSM	Global System for Mobile Communications	SPD	Security Policy Database
GTK	Group Temporal Key	SSID	Service Set Identifier
HMAC	Keyed-Hash Message Authentication Code	SSL	Secure Sockets Layer
IKE	Internet Key Exchange	ST	Security Target
IPsec	Internet Protocol Security	TLS	Transport Layer Security
		TOE	Target of Evaluation
		TSF	TOE Security Functionality
		UI	User Interface
		UUID	Universally Unique Identifier

UI	User Interface	WPA2	Wi-Fi Protected Access 2
UWB	Ultra Wideband	XML	Extensible Markup Language
VPN	Virtual Private Network		
WLAN	Wireless Local Area Network		
WPA	Wi-Fi Protected Access		

10 Appendix A: Configuration Profiles

10.1 Configuration Profile 1: "MDF PP Configuration Profile AirPrint"

```

<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
  <key>AccessRights</key>
  <integer>8</integer>
  <key>ConsentText</key>
  <dict>
    <key>default</key>
    <string>Configuration profile achieving compliance with the security settings defined by the Common Criteria
evaluation.</string>
  </dict>
  <key>HasRemovalPasscode</key>
  <false/>
  <key>PayloadContent</key>
  <array>
    <dict>
      <key>AirPrint</key>
      <array>
        <dict>
          <key>ForceTLS</key>
          <true/>
        </dict>
      </array>
      <key>PayloadDescription</key>
      <string>AirPrint Configuration</string>
      <key>PayloadDisplayName</key>
      <string>AirPrint</string>
      <key>PayloadIdentifier</key>
      <string>com.apple.airprint.F0AC096F-52CD-4FAB-83A3-675259987CD7</string>
      <key>PayloadType</key>
      <string>com.apple.airprint</string>
      <key>PayloadUUID</key>
      <string>F0AC096F-52CD-4FAB-83A3-675259987CD7</string>
      <key>PayloadVersion</key>
      <integer>1</integer>
    </dict>
  </array>
  <key>PayloadDescription</key>
  <string>The configuration profile defining the AirPrint restrictions provides the general settings compliant to the
Common Criteria evaluated configuration following the Mobile Device Fundamentals Protection Profile.</string>
  <key>PayloadDisplayName</key>

```



```

<string>MDF PP Configuration Profile AirPrint</string>
<key>PayloadIdentifier</key>
<string>MDFPP2020.7F5C2634-0C2B-4610-9FCB-65B6298D8734</string>
<key>PayloadRemovalDisallowed</key>
<true/>
<key>PayloadType</key>
<string>Configuration</string>
<key>PayloadUUID</key>
<string>42FA88A0-76CF-4D15-90C3-EED747194B32</string>
<key>PayloadVersion</key>
<integer>1</integer>
</dict>
</plist>

```

10.2 Configuration Profile 2: "MDF PP Configuration Profile for General Restrictions"

```

<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
  <key>AccessRights</key>
  <integer>8</integer>
  <key>ConsentText</key>
  <dict>
    <key>default</key>
    <string>Configuration profile achieving compliance with the security settings defined by the Common Criteria
evaluation.</string>
  </dict>
  <key>HasRemovalPasscode</key>
  <false/>
  <key>PayloadContent</key>
  <array>
    <dict>
      <key>PayloadDescription</key>
      <string>Restriction Configuration</string>
      <key>PayloadDisplayName</key>
      <string>Restrictions</string>
      <key>PayloadIdentifier</key>
      <string>com.apple.applicationaccess.16FBE9FC-1D94-49F8-91EA-806F0CE6B3EC</string>
      <key>PayloadType</key>
      <string>com.apple.applicationaccess</string>
      <key>PayloadUUID</key>
      <string>16FBE9FC-1D94-49F8-91EA-806F0CE6B3EC</string>
      <key>PayloadVersion</key>
      <integer>1</integer>
    </dict>
  </array>
</dict>
</plist>

```

```

<key>allowAssistant</key>
<false/>
<key>allowAssistantUserGeneratedContent</key>
<false/>
<key>allowAssistantWhileLocked</key>
<false/>
<key>allowLockScreenControlCenter</key>
<false/>
<key>allowEnablingRestrictions</key>
<false/>
<key>allowUSBRestrictedMode</key>
<true/>

<key>allowUntrustedTLSPrompt</key>
<false/>
<key>forceAirPrintTrustedTLSRequirement</key>
<true/>

<key>allowWallpaperModification</key>
<true/>
<key>forceAutomaticDateAndTime</key>
<false/>

<!-- Optional settings to further restrict permissions

<key>allowEraseContentAndSettings</key>
<false/>

<key>allowCamera</key>
<false/>

-->
</dict>
</array>
<key>PayloadDescription</key>
<string>The configuration profile defining general restrictions locks various mechanisms to the secure settings
compliant to the Common Criteria evaluated configuration following the Mobile Device Fundamentals Protection
Profile.</string>
<key>PayloadDisplayName</key>
<string>MDF PP Configuration Profile for General Restrictions</string>
<key>PayloadIdentifier</key>
<string>MDFPP2020.7F5C2634-0C2B-4610-9FCB-65B6298D8732</string>
<key>PayloadRemovalDisallowed</key>
<true/>
<key>PayloadType</key>
<string>Configuration</string>
<key>PayloadUUID</key>
<string>1FAFA759-5DE3-4EEA-8F8E-8F742A2DADC2</string>

```

```

    <key>PayloadVersion</key>
    <integer>1</integer>
</dict>
</plist>

```

10.3 Configuration Profile 3: "MDF PP Configuration Profile Passcode Restrictions"

```

<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
  <key>AccessRights</key>
  <integer>8</integer>
  <key>ConsentText</key>
  <dict>
    <key>default</key>
    <string>Configuration profile achieving compliance with the security settings defined by the Common Criteria
evaluation.</string>
  </dict>
  <key>HasRemovalPasscode</key>
  <false/>
  <key>PayloadContent</key>
  <array>
    <dict>
      <key>PayloadDescription</key>
      <string>Passcode Restrictions</string>
      <key>PayloadDisplayName</key>
      <string>Code</string>
      <key>PayloadIdentifier</key>
      <string>com.apple.mobiledevice.passwordpolicy.41664EF5-450A-48C0-A19B-970C5E522638</string>
      <key>PayloadType</key>
      <string>com.apple.mobiledevice.passwordpolicy</string>
      <key>PayloadUUID</key>
      <string>41664EF5-450A-48C0-A19B-970C5E522638</string>
      <key>PayloadVersion</key>
      <integer>1</integer>
      <key>allowSimple</key>
      <false/>
      <key>forcePIN</key>
      <true/>

      <!-- Any value between 2 and 11 -->
      <key>maxFailedAttempts</key>
      <integer>10</integer>
    </dict>
  </array>
</dict>
</plist>

```

```

<!-- Any value defined by organization -->
<key>maxInactivity</key>
<integer>2</integer>

<!-- Any value defined by organization -->
<key>maxPINAgeInDays</key>
<integer>360</integer>

<!-- Any value defined by organization -->
<key>minComplexChars</key>
<integer>1</integer>

<!-- Any value defined by organization -->
<key>minLength</key>
<integer>6</integer>

<!-- Any value defined by organization -->
<key>minHistory</key>
<integer>1</integer>

<!-- Any value defined by organization -->
<key>maxGracePeriod</key>
<integer>0</integer>

<!-- Any value defined by organization -->
<key>allowFingerprintModification</key>
<true/>
</dict>
</array>
<key>PayloadDescription</key>
<string>The configuration profile template provides passcode restrictions compliant to the Common Criteria
evaluated configuration following the Mobile Device Fundamentals Protection Profile.</string>
<key>PayloadDisplayName</key>
<string>MDF PP Configuration Profile for Passcode Restrictions</string>
<key>PayloadIdentifier</key>
<string>MDFPP2020.7F5C2634-0C2B-4610-9FCB-65B6298D8733</string>
<key>PayloadRemovalDisallowed</key>
<true/>
<key>PayloadType</key>
<string>Configuration</string>
<key>PayloadUUID</key>
<string>754A56E0-6E64-444E-9675-FBBE0DE5CAB0</string>
<key>PayloadVersion</key>
<integer>1</integer>
</dict>
</plist>

```

10.4 Configuration Profile 4: "MDF PP Configuration Profile VPN"

```

<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
  <key>ConsentText</key>
  <dict>
    <key>default</key>
    <string>Configuration profile achieving compliance with the security settings defined by the Common Criteria
evaluation.</string>
  </dict>
  <key>HasRemovalPasscode</key>
  <false/>
  <key>PayloadContent</key>
  <array>
    <dict>
      <!-- Replace certificate -->
      <key>Password</key>
      <string>1234</string>
      <key>PayloadCertificateFileName</key>
      <string>client-certificate.p12</string>
      <key>PayloadContent</key>
      <data>
        INVALID
      </data>
      <key>PayloadDescription</key>
      <string>PKCS#12-formatted certificate that MUST be replaced</string>
      <key>PayloadDisplayName</key>
      <string>PKCS#12-formatted certificate that MUST be replaced</string>
      <key>PayloadIdentifier</key>
      <string>com.apple.security.pkcs12.51F4CAA0-B295-4557-8D91-C4BDFB4AE825</string>
      <key>PayloadType</key>
      <string>com.apple.security.pkcs12</string>
      <key>PayloadUUID</key>
      <string>51F4CAA0-B295-4557-8D91-C4BDFB4AE825</string>
      <key>PayloadVersion</key>
      <integer>1</integer>
    </dict>
    <dict>
      <key>AlwaysOn</key>
      <dict>
        <!-- Any value defined by organization is allowed -->
        <key>AllowedCaptiveNetworkPlugins</key>
        <array/>

```

```

<!-- Any value defined by organization is allowed -->
<key>ServiceExceptions </key>
<array/>

<key>TunnelConfigurations </key>
<array>
  <dict>
    <key>AuthenticationMethod </key>
    <string>Certificate </string>
    <key>ChildSecurityAssociationParameters </key>
    <dict>
      <!-- Allowed options: 5, 14, 15, 19, 20 -->
      <key>DiffieHellmanGroup </key>
      <integer>14 </integer>

      <!-- Allowed options: AES-128, AES-256, AES-128-GCM, AES-256-GCM -->
      <key>EncryptionAlgorithm </key>
      <string>AES-256 </string>

      <!-- Allowed options: SHA1-160, SHA2-256, SHA2-384, SHA2-512 -->
      <key>IntegrityAlgorithm </key>
      <string>SHA2-512 </string>

      <!-- Any value defined by organization is allowed -->
      <key>LifeTimeInMinutes </key>
      <integer>1440 </integer>
    </dict>

    <!-- Any value defined by organization is allowed -->
    <key>DeadPeerDetectionRate </key>
    <string>Medium </string>

    <key>IKESecurityAssociationParameters </key>
    <dict>
      <!-- Allowed options: 5, 14, 15, 19, 20 -->
      <key>DiffieHellmanGroup </key>
      <integer>14 </integer>

      <!-- Allowed options: AES-128, AES-256, AES-128-GCM, AES-256-GCM -->
      <key>EncryptionAlgorithm </key>
      <string>AES-256 </string>

      <!-- Allowed options: SHA1-160, SHA2-256, SHA2-384, SHA2-512 -->
      <key>IntegrityAlgorithm </key>
      <string>SHA2-512 </string>

      <!-- Any value defined by organization is allowed -->
      <key>LifeTimeInMinutes </key>

```

```

    <integer>1440</integer>
  </dict>

  <!-- Any value defined by organization is allowed -->
  <key>Interfaces</key>
  <array>
    <string>Cellular</string>
    <string>WiFi</string>
  </array>

  <!-- Any value defined by organization is allowed -->
  <key>LocalIdentifier</key>
  <string>client</string>

  <!-- Refer to certificate above -->
  <key>PayloadCertificateUUID</key>
  <string>51F4CAA0-B295-4557-8D91-C4BDFB4AE825</string>

  <!-- Allowed options: RSA -->
  <key>CertificateType</key>
  <string>RSA</string>

  <key>ProtocolType</key>
  <string>IKEv2</string>

  <!-- Any value defined by organization is allowed -->
  <key>RemoteAddress</key>
  <string>10.0.0.1</string>

  <!-- Any value defined by organization is allowed -->
  <key>RemoteIdentifier</key>
  <string>server</string>

  <!-- Any value defined by organization is allowed -->
  <key>ServerCertificateCommonName</key>
  <string>server</string>

  <!-- Any value defined by organization is allowed -->
  <key>ServerCertificateIssuerCommonName</key>
  <string>CN of CA certificate</string>
</dict>
</array>
</dict>
<key>IPv4</key>
<dict>
  <key>OverridePrimary</key>
  <integer>1</integer>
</dict>

```

```

    <key>PayloadDescription</key>
    <string>Configures VPN settings</string>
    <key>PayloadDisplayName</key>
    <string>VPN</string>
    <key>PayloadIdentifier</key>
    <string>com.apple.vpn.managed.CC967500-DE00-4AA4-B775-6563EEE7E26D</string>
    <key>PayloadType</key>
    <string>com.apple.vpn.managed</string>
    <key>PayloadUUID</key>
    <string>CC967500-DE00-4AA4-B775-6563EEE7E26D</string>
    <key>PayloadVersion</key>
    <real>1</real>
    <key>Proxies</key>
    <dict/>
    <key>UserDefinedName</key>
    <string>MDFPP Compliant VPN</string>
    <key>VPNTType</key>
    <string>AlwaysOn</string>
    <key>OnDemandEnabled</key>
    <integer>0</integer>
    <key>VendorConfig</key>
    <dict/>
  </dict>
</array>

  <key>PayloadDescription</key>
  <string>The configuration profile provides VPN settings compliant to the Common Criteria evaluated configuration
following the Mobile Device Fundamentals Protection Profile.</string>
  <key>PayloadDisplayName</key>
  <string>MDF PP Configuration Profile VPN Settings</string>
  <key>PayloadIdentifier</key>
  <string>MDFPP2020.7F5C2634-0C2B-4610-9FCB-65B6298D8736</string>
  <key>PayloadRemovalDisallowed</key>
  <true/>
  <key>PayloadType</key>
  <string>Configuration</string>
  <key>PayloadUUID</key>
  <string>125B2C0F-2EF0-4AA5-8381-8F1C752F4CF5</string>
  <key>PayloadVersion</key>
  <integer>1</integer>
  <key>AccessRights</key>
  <integer>8</integer>
</dict>
</plist>

```


10.5 Configuration Profile 5: "MDF PP Configuration Profile WLAN"

```

<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
  <key>AccessRights</key>
  <integer>8</integer>
  <key>ConsentText</key>
  <dict>
    <key>default</key>
    <string>Configuration profile achieving compliance with the security settings defined by the Common Criteria
evaluation.</string>
  </dict>
  <key>HasRemovalPasscode</key>
  <false/>
  <key>PayloadContent</key>
  <array>
    <dict>
      <!-- Replace certificate -->
      <key>PayloadCertificateFileName</key>
      <string>cacert.crt</string>
      <key>PayloadContent</key>
      <data>
INVALID
      </data>
      <key>PayloadDescription</key>
      <string>CA certificate to be replaced</string>
      <key>PayloadDisplayName</key>
      <string>CA certificate to be used for WLAN EAP-TLS</string>
      <key>PayloadIdentifier</key>
      <string>com.apple.security.root.EB096643-9B1C-468B-8471-EFC210017C60</string>
      <key>PayloadType</key>
      <string>com.apple.security.root</string>
      <key>PayloadUUID</key>
      <string>EB096643-9B1C-468B-8471-EFC210017C60</string>
      <key>PayloadVersion</key>
      <integer>1</integer>
    </dict>
    <dict>
      <key>AutoJoin</key>
      <true/>
      <key>EAPClientConfiguration</key>
      <dict>
        <key>AcceptEAPTypes</key>
        <array>
          <integer>13</integer>
        </array>
      </dict>
    </dict>
  </array>

```

```

    <!-- Use certificate defined above -->
    <key>PayloadCertificateAnchorUUID</key>
    <array>
      <string>EB096643-9B1C-468B-8471-EFC210017C60</string>
    </array>
    <key>TLSTrustedServerNames</key>
    <array/>

    <!-- This is default and may be removed -->
    <key>TLSCertificateIsRequired</key>
    <true/>
  </dict>
  <key>EncryptionType</key>
  <string>WPA2</string>

  <!-- Any value defined by organization is allowed for the following options -->
  <key>HIDDEN_NETWORK</key>
  <false/>
  <key>IsHotspot</key>
  <false/>
  <key>PayloadCertificateUUID</key>
  <string>35DC8662-79F1-4640-B628-A8F1CF9C85DA</string>
  <key>PayloadDescription</key>
  <string>Configures Wi-Fi settings</string>
  <key>PayloadDisplayName</key>
  <string>WiFi</string>
  <key>PayloadIdentifier</key>
  <string>com.apple.wifi.managed.9E1F3E37-2CEF-468A-B8C2-BBD5C92C6E7C</string>
  <key>PayloadType</key>
  <string>com.apple.wifi.managed</string>
  <key>PayloadUUID</key>
  <string>9E1F3E37-2CEF-468A-B8C2-BBD5C92C6E7C</string>
  <key>PayloadVersion</key>
  <real>1</real>
  <key>ProxyType</key>
  <string>None</string>
  <key>SSID_STR</key>
  <string>EAP-TLSWLAN</string>
</dict>
</array>
<key>PayloadDescription</key>
<string>The configuration profile template provides the Wireless LAN settings compliant to the Common Criteria
evaluated configuration following the Mobile Device Fundamentals Protection Profile.</string>
<key>PayloadDisplayName</key>
<string>MDF PP Configuration Profile WLAN Configuration</string>
<key>PayloadIdentifier</key>
<string>MDFPP2020.7F5C2634-0C2B-4610-9FCB-65B6298D8735</string>

```

```
<key>PayloadRemovalDisallowed</key>  
<true/>  
<key>PayloadType</key>  
<string>Configuration</string>  
<key>PayloadUUID</key>  
<string>12926851-84EE-4270-9EE2-7CCB87E7B00D</string>  
<key>PayloadVersion</key>  
<integer>1</integer>  
</dict>  
</plist>
```

11 Appendix B: User Guide Screenshots

This appendix contains screenshots from [iPhone_UG] and [iPad_UG].

11.1 Get information about your iPhone


Get information about your iPhone

View overall storage availability and storage used per app

Go to Settings  > General > iPhone Storage.

See the Apple Support articles [How to check the storage on your iPhone, iPad, and iPod touch](#) and [Manage your iCloud storage](#).


See battery usage

Go to Settings  > Battery to see the elapsed time since iPhone was charged as well as battery usage by app.

You can also display battery level as a percentage, turn Low Power Mode on or off, and check your battery's health.

See [Monitor the iPhone battery level](#).

View call time and cellular usage

Go to Settings  > Cellular. See [View or change cellular data settings on iPhone](#).

See more information about iPhone

Go to Settings  > General > About. The items you can view include:

- Name
- iOS software version
- Model name
- Part and model numbers. To the right of Model, the part number appears. To see the model number, tap the part number.
- Serial number
- Cellular network
- Number of songs, videos, photos, and apps
- Capacity and available storage space
- Carrier settings. To the right of Carrier, the carrier settings version number appears. To see additional carrier-specific information, tap the version number. Contact your carrier for more details.


- Wi-Fi and Bluetooth addresses
- IMEI (International Mobile Equipment Identity)
- ICCID (Integrated Circuit Card Identifier, or Smart Card) for GSM networks
- MEID (Mobile Equipment Identifier) for CDMA networks
- Modem firmware

To copy the serial number and other identifiers, touch and hold the identifier until Copy appears.

To see Legal & Regulatory information (including legal notices and license, warranty, and RF exposure information) and regulatory marks, go to Settings > General > Legal & Regulatory.

On [supported models](#), you can also find the IMEI on the SIM card tray and the model number in the SIM tray opening.

View or turn off diagnostic information


Go to Settings  > Privacy > Analytics & Improvements.

To help Apple improve products and services, iPhone sends diagnostic and usage data. This data doesn't personally identify you, but may include location information.

11.2 Get information about your iPad


Get information about your iPad

View overall storage availability and storage used per app

Go to Settings  > General > iPad Storage.

See the Apple Support articles [How to check the storage on your iPhone, iPad, and iPod touch](#) and [Manage your iCloud storage](#).

See battery usage

Go to Settings  > Battery to see the elapsed time since iPad was charged as well as battery usage by app. You can also display battery level as a percentage and turn Low Power Mode on or off. See [Charge the iPad battery](#).

View cellular usage

Go to Settings  > Cellular Data. See [View or change cellular data settings on iPad \(Wi-Fi + Cellular models\)](#).

See more information about iPad


Go to Settings  > General > About. The items you can view include:

- Name
- iPadOS software version
- Model name
- Part and model numbers. To the right of Model, the part number appears. To see the model number, tap the part number.
- Serial number
- Network (Wi-Fi + Cellular models)
- Number of songs, videos, photos, and apps
- Capacity and available storage space
- Carrier (Wi-Fi + Cellular models)
- Cellular Data Number (Wi-Fi + Cellular models)
- Wi-Fi and Bluetooth addresses
- IMEI (International Mobile Equipment Identity) (Wi-Fi + Cellular models)
- ICCID (Integrated Circuit Card Identifier, or Smart Card) for GSM networks (Wi-Fi + Cellular models)
- MEID (Mobile Equipment Identifier) for CDMA networks (Wi-Fi + Cellular models)
- Modem firmware

To copy the serial number and other identifiers, touch and hold the identifier until Copy appears.

To see Legal & Regulatory information (including legal notices, and license, warranty, and RF exposure information) and regulatory marks, go to Settings > General > Legal & Regulatory.

View or turn off diagnostic information

Go to Settings  > Privacy > Analytics & Improvements.

To help Apple improve products and services, iPad sends diagnostic and usage data. This data doesn't personally identify you, but may include location information.

11.3 Set up and use Bluetooth accessories on iPhone


Set up and use Bluetooth accessories on iPhone

Using a Bluetooth connection, you can use third-party devices such as wireless keyboards, headphones, speakers, car kits, game controllers, and more with iPhone.

Pair a Bluetooth headphone, car kit, game controller, or other device

1. Follow the instructions that came with the device to put it in discovery mode.


Note: To pair AirPods, see the [AirPods User Guide](#).

2. On iPhone, go to Settings  > Bluetooth, turn on Bluetooth, then tap the name of the device.

iPhone must be within about 33 feet (10 meters) of the Bluetooth device.


Customize a wireless game controller

After you pair a compatible game controller, you can customize it for supported games from Apple Arcade and the App Store.

1. Go to Settings  > General > Game Controller.
2. Tap the buttons you want to change.
3. To customize for a specific app, tap Add App.

Note: Apple Arcade availability varies by country or region.

Play audio from iPhone on a Bluetooth audio device

1. On your iPhone, open an audio app, such as Music, then choose an item to play.
2. Tap , then choose your Bluetooth device.

While audio is playing, you can change the playback destination on the Lock Screen or in Control Center.


The playback destination returns to iPhone if you move the device out of Bluetooth range.

For information about protecting your hearing from loud volume while listening to headphones with iPhone, see [Use headphone audio level features on iPhone](#).



WARNING: For important information about avoiding hearing loss and avoiding distractions that could lead to dangerous situations, see [Important safety information for iPhone](#).

Bypass your Bluetooth device for calls

To use the iPhone receiver or speaker for calls, do any of the following:

- Answer a call by tapping the iPhone screen.
- During a call, tap Audio, then choose iPhone or Speaker Phone.
- Turn off the Bluetooth device, unpair it, or move out of range.
- Go to Settings , tap Bluetooth, then turn off Bluetooth.


Unpair a Bluetooth device

Go to Settings  > Bluetooth, tap the information button  next to the name of the device, then tap Forget This Device.

If you don't see the Devices list, make sure Bluetooth is on.

If you have AirPods and you tap Forget This Device, they're automatically removed from other devices where you're [signed in with the same Apple ID](#).

Disconnect from Bluetooth devices

To quickly disconnect from all Bluetooth devices without turning Bluetooth off, [open Control Center](#), then tap .

To learn about Bluetooth privacy settings on iPhone, see the Apple Support article [If an app would like to use Bluetooth on your device](#). If you have trouble connecting a Bluetooth device, see the Apple Support article [If you can't connect a Bluetooth accessory to your iPhone, iPad, or iPod touch](#).

Note: The use of certain accessories with iPhone may affect wireless performance. Not all iOS accessories are fully compatible with iPhone. Turning on airplane mode may eliminate audio interference between iPhone and an accessory. Reorienting or relocating iPhone and the connected accessory may improve wireless performance.

See also

[Improve the accuracy of audio measurements for third-party Bluetooth headphones](#)

11.4 Set up and use Bluetooth accessories on iPad


Set up and use Bluetooth accessories on iPad

Using a Bluetooth connection, you can use third-party devices such as wireless keyboards, headphones, speakers, car kits, game controllers, and more with iPad.

Pair a Bluetooth headphone, keyboard, game controller, or other device

1. Follow the instructions that came with the device to put it in discovery mode.


Note: To pair AirPods, see the [AirPods User Guide](#).

2. On iPad, go to Settings  > Bluetooth, turn on Bluetooth, then tap the name of the device.

iPad must be within about 33 feet (10 meters) of the Bluetooth device.


Customize a wireless game controller

After you pair a compatible game controller, you can customize it for supported games from Apple Arcade and the App Store.

1. Go to Settings  > General > Game Controller.
2. Tap the buttons you want to change.
3. To customize for a specific app, tap Add App.

Note: Apple Arcade availability varies by country or region.

Play audio from iPad on a Bluetooth audio device

1. On your iPad, open an audio app, such as Music, then choose an item to play.
2. Tap , then choose your Bluetooth device.



While audio is playing, you can change the playback destination on the Lock Screen or in Control Center.

The playback destination returns to iPad if you move the device out of Bluetooth range.

For information about protecting your hearing from loud volume while listening to headphones with iPad, see [Use headphone audio-level features on iPad](#).

WARNING: For important information about avoiding hearing loss and avoiding distractions that could lead to dangerous situations, see [Important safety information for iPad](#).


Unpair a Bluetooth device

Go to Settings  > Bluetooth, tap the information button  next to the name of the device, then tap Forget This Device.

If you don't see the Devices list, make sure Bluetooth is on.

If you have AirPods and you tap Forget This Device, they're automatically removed from other devices where you're [signed in with the same Apple ID](#).

Disconnect from Bluetooth devices

To quickly disconnect from all Bluetooth devices without turning Bluetooth off, [open Control Center](#), then tap .

To learn about Bluetooth privacy settings on iPad, see the Apple Support article [If an app would like to use Bluetooth on your device](#). If you have trouble connecting a Bluetooth device, see the Apple Support article [If you can't connect a Bluetooth accessory to your iPhone, iPad, or iPod touch](#).

Note: The use of certain accessories with iPad may affect wireless performance. Not all iOS or iPadOS accessories are fully compatible with iPad. Turning on airplane mode may eliminate audio interference between iPad and an accessory. Reorienting or relocating iPad and the connected accessory may improve wireless performance.

See also


[Improve the accuracy of audio measurements for third-party Bluetooth headphones](#)

11.5 Set a passcode on iPhone

Set a passcode on iPhone

For better security, set a passcode that needs to be entered to unlock iPhone when you turn it on or wake it. Setting a passcode also turns on data protection, which encrypts your iPhone data with 256-bit AES encryption. (Some apps may opt out of using data protection.)

Set or change the passcode

1. Go to Settings , then do one of the following:
 - *On an iPhone with Face ID:* Tap Face ID & Passcode.
 - *On an iPhone with a Home button:* Tap Touch ID & Passcode.
2. Tap Turn Passcode On or Change Passcode.


To view options for creating a password, tap Passcode Options. The most secure options are Custom Alphanumeric Code and Custom Numeric Code.

Setting a passcode turns on data protection, which encrypts your iPhone data with 256-bit AES encryption. (Some apps may opt out of using data protection.)

After you set a passcode, you can [use Face ID](#) or [Touch ID](#) to unlock iPhone (depending on your model). For additional security, however, you must always enter your passcode to unlock your iPhone under the following conditions:


- You turn on or restart your iPhone.
- You haven't unlocked your iPhone for more than 48 hours.
- You haven't unlocked your iPhone with the passcode in the last 6.5 days, and you haven't unlocked it with Face ID or Touch ID in the last 4 hours.
- Your iPhone receives a remote lock command.
- There are five unsuccessful attempts to unlock your iPhone with Face ID or Touch ID.
- An attempt to use Emergency SOS is initiated (see [Make emergency calls on iPhone](#)).
- An attempt to view your Medical ID is initiated (see [Create a Medical ID](#)).

Change when iPhone automatically locks

Go to Settings  > Display & Brightness > Auto-Lock, then set a length of time.


Erase data after 10 failed passcodes

Set iPhone to erase all information, media, and personal settings after 10 consecutive failed passcode attempts.

1. Go to Settings , then do one of the following:
 - *On an iPhone with Face ID:* Tap Face ID & Passcode.
 - *On an iPhone with a Home button:* Tap Touch ID & Passcode.
2. Turn on Erase Data.

After all data is erased, you must [restore your device from a backup](#) or [set it up again as new](#).

Turn off the passcode

1. Go to Settings , then do one of the following:
 - *On an iPhone with Face ID:* Tap Face ID & Passcode.
 - *On an iPhone with a Home button:* Tap Touch ID & Passcode.
2. Tap Turn Passcode Off.

Reset the passcode

If you enter the wrong passcode six times in a row, you'll be locked out of your device, and you'll receive a message that says iPhone is disabled. If you can't remember your passcode, you can erase your iPhone with a computer or with recovery mode, then set a new passcode. (If you made an iCloud or computer backup before you forgot your passcode, you can restore your data and settings from the backup.)


See the Apple Support article [If you forgot the passcode on your iPhone, or your iPhone is disabled](#).

11.6 Set a passcode on iPad

Set a passcode on iPad

For better security, set a passcode that needs to be entered to unlock iPad when you turn it on or wake it. Setting a passcode also turns on data protection, which encrypts your iPad data with 256-bit AES encryption. (Some apps may opt out of using data protection.)

Set or change the passcode

1. Go to Settings , then depending on your model, tap one of the following:

- Face ID & Passcode
- Touch ID & Passcode
- Passcode

2. Tap Turn Passcode On or Change Passcode.


To view options for creating a password, tap Passcode Options. The most secure options are Custom Alphanumeric Code and Custom Numeric Code.

To view options for creating a password, tap Passcode Options. The most secure options are Custom Alphanumeric Code and Custom Numeric Code.

After you set a passcode, on supported models you can use [Face ID](#) or [Touch ID](#) to unlock iPad. For additional security, however, you must always enter your passcode to unlock your iPad under the following conditions:


- You turn on or restart your iPad.
- You haven't unlocked your iPad for more than 48 hours.
- You haven't unlocked your iPad with the passcode in the last 6.5 days, and you haven't unlocked it with Face ID or Touch ID in the last 4 hours.
- Your iPad receives a remote lock command.
- There are five unsuccessful attempts to unlock your iPad with Face ID or Touch ID.

Change when iPad automatically locks

Go to Settings  > Display & Brightness > Auto-Lock, then set a length of time.


Erase data after 10 failed passcodes

Set iPad to erase all information, media, and personal settings after 10 consecutive failed passcode attempts.

1. Go to Settings , then depending on your model, tap one of the following:
 - Face ID & Passcode
 - Touch ID & Passcode
 - Passcode
2. Turn on Erase Data.

After all data is erased, you must [restore iPad from a backup](#) or [set it up again as new](#).

Turn off the passcode

1. Go to Settings , then depending on your model, tap one of the following:
 - Face ID & Passcode
 - Touch ID & Passcode
 - Passcode
2. Tap Turn Passcode Off.

Reset the passcode


If you enter the wrong passcode six times in a row, you'll be locked out of your device, and you'll receive a message that says iPad is disabled. If you can't remember your passcode, you can erase your iPad with a computer or with recovery mode, then set a new passcode. (If you made an iCloud or computer backup before you forgot your passcode, you can restore your data and settings from the backup.)

See the Apple Support article [If you forgot the passcode on your iPad, or your iPad is disabled](#).

11.7 Erase iPhone

Erase iPhone

When you delete data, it's no longer accessible through the iPhone interface, but it isn't erased from iPhone storage. To remove all of your content and settings from storage, erase iPhone. For example, erase iPhone before you [sell it or give it away](#). If you want to save your content and settings, [back up](#) iPhone before erasing it.

You can erase iPhone from Settings . If you're unable to open Settings, you can use a computer to erase iPhone.

Erase all content and settings from iPhone

1. Go to Settings  > General > Transfer or Reset iPhone.


If you're erasing your iPhone because you're replacing it with a new iPhone that you have on hand, you can use extra free storage in iCloud to move your apps and data to the new device. Tap Get Started, follow the onscreen instructions, then return to Settings > General > Transfer or Reset iPhone.

2. Tap Erase All Content and Settings.

When iPhone restarts with all content and settings erased, you have the option to set up iPhone as new or restore it from a backup. See [Turn on and set up iPhone](#).

Note: If you're asked to enter your passcode and you've forgotten it, see [Reset the passcode](#). If you're asked to enter your Apple ID password and you've forgotten it, see the [Recover your Apple ID website](#).

Use a computer to erase all content and settings from iPhone

You can use a Mac or Windows PC to erase all data and settings from your iPhone, restore iPhone to factory settings, and install the latest version of iOS. For example, if you can't open Settings  on iPhone, you can use this approach to restore iPhone to factory settings.

Before iPhone is erased, you have the option to back it up. If you make a backup, you can use the backup to restore your data and settings on your iPhone or on a new device. See [Restore iPhone from a computer backup](#).

1. [Connect iPhone and your computer with a cable](#).
2. Do one of the following:
 - *In the Finder sidebar on your Mac:* Select your iPhone, click General at the top of the window, then click Restore iPhone.


To use the Finder to restore iPhone to factory settings, macOS 10.15 or later is required. With earlier versions of macOS, [use iTunes](#) to restore iPhone.
 - *In the iTunes app on a Windows PC:* Click the iPhone button near the top left of the iTunes window, click Summary, then click Restore iPhone.
3. Follow the onscreen instructions.

See the Apple Support article [If you can't update or restore your iPhone, iPad, or iPod touch](#).


11.8 Erase iPad

Erase iPad

When you delete data, it's no longer accessible through the iPad interface, but it isn't erased from iPad storage. To remove all of your content and settings from storage, erase iPad. For example, erase iPad before you [sell it or give it away](#). If you want to save your content and settings, [back up iPad](#) before erasing it.

You can erase iPad from Settings . If you're unable to open Settings, you can use a computer to erase iPad.

Erase all content and settings from iPad

1. Go to Settings  > General > Transfer or Reset iPad.


If you're erasing your iPad because you're replacing it with a new iPad that you have on hand, you can use extra free storage in iCloud to move your apps and data to the new device. Tap Get Started, follow the onscreen instructions, then return to Settings > General > Transfer or Reset iPad.

2. Tap Erase All Content and Settings.

When iPad restarts with all content and settings erased, you have the option to set up iPad as new or restore it from a backup. See [Turn on and set up iPad](#).

Note: If you're asked to enter your passcode and you've forgotten it, see [Reset the passcode](#). If you're asked to enter your Apple ID password and you've forgotten it, see the [Recover your Apple ID website](#).

Use a computer to erase all content and settings from iPad

You can use a Mac or Windows PC to erase all data and settings from your iPad, restore iPad to factory settings, and install the latest version of iPadOS. For example, if you can't open Settings  on iPad, you can use this approach to restore iPad to factory settings.

Before iPad is erased, you have the option to back it up. If you make a backup, you can use the backup to restore your data and settings on your iPad or on a new device. See [Restore iPad from a computer backup](#).

1. [Connect iPad and your computer with a cable](#).
2. Do one of the following:
 - *In the Finder sidebar on your Mac:* Select your iPad, click General at the top of the window, then click Restore iPad.
To use the Finder to restore iPad to factory settings, macOS 10.15 or later is required. With earlier versions of macOS, [use iTunes](#) to restore iPad.
 - *In the iTunes app on a Windows PC:* Click the iPad button near the top left of the iTunes window, click Summary, then click Restore iPad.
3. Follow the onscreen instructions.

See the Apple Support article [If you can't update or restore your iPhone, iPad, or iPod touch](#).


11.9 Set up Face ID on iPhone

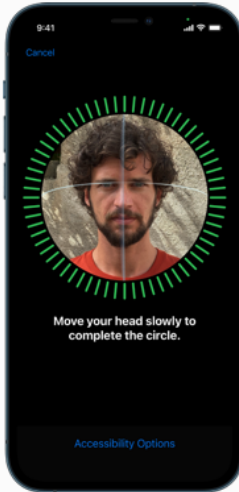
Set up Face ID on iPhone

Use Face ID ([supported models](#)) to securely and conveniently unlock iPhone, authorize purchases and payments, and sign in to many third-party apps by simply glancing at your iPhone.

To use Face ID, you must also [set up a passcode](#) on your iPhone.

Set up Face ID or add an alternate appearance

- If you didn't set up Face ID when you first set up your iPhone, go to Settings  > Face ID & Passcode > Set up Face ID, then follow the onscreen instructions.
- To set up an additional appearance for Face ID to recognize, go to Settings > Face ID & Passcode > Set Up an Alternate Appearance, then follow the onscreen instructions.



If you have physical limitations, you can tap Accessibility Options during Face ID set up. When you do this, setting up facial recognition doesn't require the full range of head motion. Using Face ID is still secure, but it requires more consistency in how you look at iPhone.

Face ID also has an accessibility feature you can use if you're blind or have low vision. If you don't want Face ID to require that you look at iPhone with your eyes open, go to Settings > Accessibility, then turn off Require Attention for Face ID. This feature is automatically turned off if you turn on VoiceOver when you first set up iPhone. See [Change Face ID and attention settings on iPhone](#).

Temporarily disable Face ID


You can temporarily prevent Face ID from unlocking your iPhone.

1. Press and hold the side button and either volume button for 2 seconds.
2. After the sliders appear, press the side button to immediately lock iPhone.

iPhone locks automatically if you don't touch the screen for a minute or so.

The next time you unlock iPhone with your passcode, Face ID is enabled again.

Turn off Face ID

1. Go to Settings  > Face ID & Passcode.
2. Do one of the following:
 - *Turn off Face ID for specific items only:* Turn off one or more options: iPhone Unlock, Apple Pay, iTunes & App Store, or Safari AutoFill.
 - *Turn off Face ID:* Tap Reset Face ID.

If your device is lost or stolen, you can prevent Face ID from being used to unlock your device with Find My iPhone Lost Mode. (See [Locate a device in Find My on iPhone](#).)

For more information about Face ID, see [About Face ID advanced technology](#).

See also

[Change when iPhone automatically locks](#)


11.10 Set up Touch ID on iPhone

Set up Touch ID on iPhone

Use Touch ID ([supported models](#)) to securely and conveniently unlock iPhone, authorize purchases and payments, and sign in to many third-party apps by pressing the Home button with your finger or thumb.

To use Touch ID, you must also [set up a passcode](#) on your iPhone.

Turn on fingerprint recognition


1. If you didn't turn on fingerprint recognition when you first set up your iPhone, go to Settings  > Touch ID & Passcode.
2. Turn on any of the options, then follow the onscreen instructions.

If you turn on iTunes & App Store, you're asked for your [Apple ID](#) password when you make your first purchase from the App Store, Apple Books, or the iTunes Store. When you make your next purchases, you're asked to use Touch ID.

Note: If you can't add a fingerprint or unlock your iPhone using Touch ID, see the Apple Support article [If Touch ID isn't working](#).

Add a fingerprint

You can add multiple fingerprints (both of your thumbs and forefingers, for example).

1. Go to Settings  > Touch ID & Passcode.
2. Tap Add a Fingerprint.
3. Follow the onscreen instructions.


Name or delete a fingerprint

1. Go to Settings  > Touch ID & Passcode.


If you added more than one fingerprint, place a finger on the Home button to identify its print.

2. Tap the fingerprint, then enter a name (such as "Thumb") or tap Delete Fingerprint.

Unlock iPhone by touching instead of pressing the Home button

Go to Settings  > Accessibility > Home Button, then turn on Rest Finger to Open.

Turn off Touch ID

Go to Settings  > Touch ID & Passcode, then turn off one or more of the options.

See also

[Change when iPhone automatically locks](#)


11.11 Set up Face ID on iPad

Set up Face ID on iPad

Use Face ID ([supported models](#)) to securely and conveniently unlock iPad, authorize purchases and payments, and sign in to many third-party apps by simply glancing at your iPad.

To use Face ID, you must also [set a passcode](#) on your iPad.

Set up Face ID or add an alternate appearance

- If you didn't set up Face ID when you first set up your iPad, go to Settings  > Face ID & Passcode > Set up Face ID, then follow the onscreen instructions.
- To set up an additional appearance for Face ID to recognize, go to Settings > Face ID & Passcode > Set Up an Alternate Appearance, then follow the onscreen instructions.

If you have physical limitations, you can tap Accessibility Options during Face ID set up. When you do this, setting up facial recognition doesn't require the full range of head motion. Using Face ID is still secure, but it requires more consistency in how you look at iPad.

Face ID also has an accessibility feature you can use if you're blind or have low vision. If you don't want Face ID to require that you look at iPad with your eyes open, go to Settings > Accessibility > Face ID & Attention, then turn off Require Attention for Face ID. This feature is automatically turned off if you turn on VoiceOver when you first set up iPad. See [Change Face ID and attention settings on iPad](#).

Temporarily disable Face ID


You can temporarily prevent Face ID from unlocking your iPad.

1. Press and hold the top button and either volume button for 2 seconds.
2. After the sliders appear, press the top button to immediately lock iPad.

iPad locks automatically if you don't touch the screen for a minute or so.

The next time you unlock iPad with your passcode, Face ID is enabled again.

Turn off Face ID

1. Go to Settings  > Face ID & Passcode.
2. Do one of the following:
 - *Turn off Face ID for specific items only:* Turn off one or more options: iPad Unlock, Apple Pay, iTunes & App Store, or Safari AutoFill.
 - *Turn off Face ID:* Tap Reset Face ID.

If your device is lost or stolen, you can prevent Face ID from being used to unlock your device with Find My iPhone Lost Mode. (See [Add your iPad to Find My.](#))

For more information about Face ID, see [About Face ID advanced technology.](#)

See also

[Change when iPad automatically locks](#)


11.12 Set up Touch ID on iPad

Set up Touch ID on iPad

Use Touch ID ([supported models](#)) to securely and conveniently unlock iPad, authorize purchases and payments, and sign in to many third-party apps by pressing the top button (ninth-generation iPad and fourth-generation iPad Air) or the Home button (other models) with your finger or thumb.

To use Touch ID, you must [set a passcode](#) on your iPad.

Turn on fingerprint recognition


1. If you didn't turn on fingerprint recognition when you first set up your iPad, go to Settings  > Touch ID & Passcode.
2. Turn on any of the options, then follow the onscreen instructions.

If you turn on iTunes & App Store, you're asked for your [Apple ID](#) password when you make your first purchase from the App Store, Apple Books, or the iTunes Store. When you make your next purchases, you're asked to use Touch ID.

Note: If you can't add a fingerprint or unlock your iPad using Touch ID, see the Apple Support article [If Touch ID isn't working](#).

Add a fingerprint

You can add multiple fingerprints (both of your thumbs and forefingers, for example).

1. Go to Settings  > Touch ID & Passcode.
2. Tap Add a Fingerprint.
3. Follow the onscreen instructions.


Name or delete a fingerprint

1. Go to Settings  > Touch ID & Passcode.


If you added more than one fingerprint, place a finger on the top button (iPad Air (4th generation)) or Home button (other models) to identify its print.

2. Tap the fingerprint, then enter a name (such as "Thumb") or tap Delete Fingerprint.

Unlock iPad by touching instead of pressing with your finger or thumb

Go to Settings  > Accessibility, tap Top Button (iPad Air (4th generation)) or Home Button (other models), then turn on Rest Finger to Open.

Turn off Touch ID


Go to Settings  > Touch ID & Passcode, then turn off one or more of the options.

See also

[Change when iPad automatically locks](#)

11.13 Get apps in the App Store on iPhone

Get apps in the App Store on iPhone

In the App Store app , you can discover new apps, featured stories, tips and tricks, and in-app events.



Note: You need an internet connection and an [Apple ID](#) to use the App Store. The availability of the App Store and Apple Arcade varies by country or region. See the Apple Support article [Availability of Apple Media Services](#).

Find apps

To discover apps, games, and in-app events, tap any of the following:

- *Today*: Browse featured stories, apps, and in-app events.
 - *Games*: Find your next game across dozens of categories including action, adventure, racing, puzzles, and more.
 - *Apps*: Explore new releases, see the top charts, or browse by category.
 - *Arcade*: Enjoy the curated collection of premium games from Apple Arcade (subscription required) without ads or in-app purchases.
 - *Search*: Enter what you're looking for, then tap Search on the keyboard.
- 🗨️ **Ask Siri.** You can also say something like: "Search the App Store for cooking apps" or "Get the Minecraft app." [Learn how to ask Siri.](#)


Get more info about an app

Tap an app to see the following information and more:

- Screenshots or previews
- In-app events
- Ratings and reviews
- Supported languages
- Game Center and Family Sharing support
- Compatibility with other Apple devices
- File size
- Privacy information; see [Review the privacy practices of apps](#)

Buy and download an app

1. Tap the price. If the app is free, tap Get.

If you see  instead of a price, you already purchased the app, and you can download it again without a charge.


2. If required, authenticate your [Apple ID](#) with Face ID, Touch ID, or your passcode to complete your purchase.

You can find the app in the Recently Added category in App Library. While the app is downloading, a progress indicator appears on the app icon. See [Find your apps in App Library on iPhone](#) and [Change where new apps get downloaded](#).


Get the App Store widget

See stories, collections, and in-app events right on your Home Screen. See [Add widgets on iPhone](#).

Share or give an app

1. Tap the app to see its details.
2. Tap , then choose a sharing option or tap Gift App (not available for all apps).

Redeem or send an Apple Gift Card

1. Tap  or your profile picture at the top right.
2. Tap one of the following:
 - Redeem Gift Card or Code
 - Send Gift Card by Email

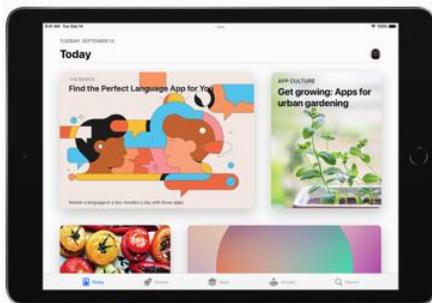
See also

[Apple Support article: If you can't redeem your Apple Gift Card or App Store & iTunes Gift Card](#)

11.14 Get apps in the App Store on iPad

Get apps in the App Store on iPad

In the App Store app , you can discover new apps, featured stories, tips and tricks, and in-app events.




Note: You need an internet connection and an [Apple ID](#) to use the App Store. The availability of the App Store and Apple Arcade varies by country or region. See the Apple Support article [Availability of Apple Media Services](#).

Find apps

To discover apps, games, and in-app events, tap any of the following:

- **Today:** Browse featured stories, apps, and in-app events.
- **Games:** Find your next game across dozens of categories including action, adventure, racing, puzzles, and more.
- **Apps:** Explore new releases, see the top charts, or browse by category.
- **Arcade:** Enjoy the curated collection of premium games from Apple Arcade (subscription required) without ads or in-app purchases.
- **Search:** Enter what you're looking for, then tap Search on the keyboard.

 **Ask Siri.** You can also say something like: "Search the App Store for cooking apps" or "Get the Minecraft app." [Learn how to ask Siri.](#)


Get more info about an app

Tap an app to see the following information and more:

- Screenshots or previews
- In-app events
- Ratings and reviews
- Supported languages
- Game Center and Family Sharing support
- Compatibility with other Apple devices
- File size
- Privacy information; see [Review the privacy practices of apps](#)

Buy and download an app

1. Tap the price. If the app is free, tap Get.

If you see  instead of a price, you already purchased the app, and you can download it again without a charge.


2. If required, authenticate your [Apple ID](#) with Face ID, Touch ID, or your passcode to complete your purchase.

You can find the app in the Recently Added category in App Library. While the app is downloading, a progress indicator appears on the app icon. See [Find your apps in App Library on iPad](#) and [Change where new apps get downloaded.](#)


Get the App Store widget

See stories, collections, and in-app events right on your Home Screen. See [Add widgets on iPad.](#)

Share or give an app

1. Tap the app to see its details.
2. Tap , then choose a sharing option or tap Gift App (not available for all apps).

Redeem or send an Apple Gift Card

1. Tap  or your profile picture at the top right.
2. Tap one of the following:
 - Redeem Gift Card or Code
 - Send Gift Card by Email

See also

[Apple Support article: If you can't redeem your Apple Gift Card or App Store & iTunes Gift Card](#)

11.15 Remove apps from iPhone

Remove apps from iPhone

You can easily remove apps from your iPhone. If you change your mind, you can download the apps again later.

Remove apps

Do any of the following:

- *Remove an app from the Home Screen:* Touch and hold the app on the Home Screen, tap Remove App, then tap Remove from Home Screen to keep it in App Library, or tap Delete App to delete it from iPhone.
- *Delete an app from App Library and Home Screen:* Touch and hold the app in App Library, tap Delete App, then tap Delete. (See [Find your apps in App Library.](#))

If you change your mind, you can [redownload apps](#) you've removed.

In addition to removing third-party apps from the Home Screen, you can remove the following built-in Apple apps that came with your iPhone:

- [Books](#)
- [Calculator](#)
- [Calendar](#)
- [Compass](#)
- [Contacts](#) (Contact information remains available through Phone, Messages, Mail, FaceTime, and other apps. To remove a contact, you must restore Contacts.)
- [FaceTime](#)
- [Files](#)
- [Home](#)
- [iTunes Store](#)
- [Mail](#)
- [Maps](#)

- [Measure](#)
- [Music](#)
- [News](#)
- [Notes](#)
- [Podcasts](#)
- [Reminders](#)
- [Shortcuts](#)
- [Stocks](#)
- [Tips](#)
- [Translate](#)

- [TV](#)
- [Voice Memos](#)
- [Watch](#)
- [Weather](#)

Note: When you remove a built-in app from your Home Screen, you also remove any related user data and configuration files. Removing built-in apps from your Home Screen can affect other system functionality. See the Apple Support article [Delete built-in Apple apps on your iOS 12, iOS 13, or iPadOS device or Apple Watch](#).

11.16 Remove apps from iPad

Remove apps from iPad

You can easily remove apps from your iPad. If you change your mind, you can download the apps again later.

Remove apps

Do any of the following:

- *Remove an app from the Home Screen:* Touch and hold the app on the Home Screen, tap Remove App, then tap Remove from Home Screen to keep it in App Library, or tap Delete App to delete it from iPad.
- *Delete an app from App Library and Home Screen:* Touch and hold the app in App Library, tap Delete App, then tap Delete. (See [Find your apps in App Library on iPad](#).)

If you change your mind, you can [redownload apps](#) you've deleted.

In addition to deleting third-party apps, you can delete the following built-in Apple apps that came with your iPad:

- [Books](#)
- [Calendar](#)

- **Contacts** (Contact information remains available through Messages, Mail, FaceTime, and other apps. To remove a contact, you must restore Contacts.)
- **FaceTime**
- **Files**
- **Home**
- **iTunes Store**
- **Mail**
- **Maps**
- **Measure**
- **Music**
- **News**
- **Notes**
- **Photo Booth**
- **Podcasts**
- **Reminders**
- **Shortcuts**
- **Stocks**
- **Tips**
- **TV**
- **Voice Memos**

Note: When you delete a built-in app from your Home Screen, you also delete any related user data and configuration files. Removing built-in apps from your Home Screen can affect other system functionality. See the Apple Support article [Delete built-in Apple apps on your iOS 12, iOS 13, or iPadOS device or Apple Watch](#).

11.17 Access features from the iPhone Lock screen


Access features from the iPhone Lock Screen

The Lock Screen, which shows the current time and date and your most recent notifications, appears when you turn on or wake iPhone. From the Lock Screen, you can see notifications, open Camera and Control Center, get information from your favorite apps at a glance, and more.




Access features and information from the Lock Screen

You can quickly access useful features and information from the Lock Screen, even while iPhone is locked. From the Lock Screen, do any of the following:

- *Open Camera:* Swipe left. On [supported models](#), you can touch and hold , then lift your finger. (See [iPhone camera basics](#).)
- *Open Control Center:* Swipe down from the top-right corner (on an iPhone with Face ID) or swipe up from the bottom edge of the screen (on other iPhone models). (See [Use and customize Control Center on iPhone](#).)
- *See earlier notifications:* Swipe up from the center. (See [View and respond to notifications on iPhone](#).)
- *View widgets:* Swipe right. (See [Add widgets on iPhone](#).)

To choose what you can access from the Lock Screen, see [Control access to information on the iPhone Lock Screen](#).

Show notification previews on the Lock Screen

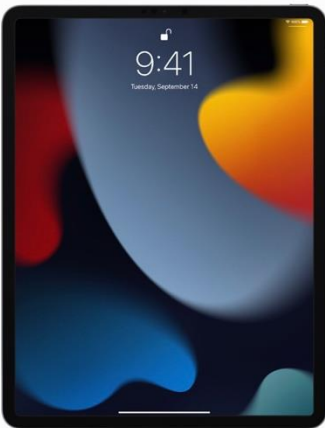
1. Go to Settings  > Notifications.
2. Tap Show Previews, then tap Always.

Notification previews include text from Messages, lines from Mail messages, and details about Calendar invitations. See [View and respond to notifications on iPhone](#).

11.18 Access features from the iPad Lock screen

Access features from the iPad Lock Screen

The Lock Screen, which shows the current time and date and your most recent notifications, appears when you turn on or wake iPad. From the Lock Screen, you can see notifications, open Camera and Control Center, get information from your favorite apps at a glance, and more.



Access features and information from the Lock Screen

You can quickly access the features and information you need most from the Lock Screen, even while iPad is locked.

- *Open Camera:* Swipe left. (See [Take photos with your iPad camera.](#))
- *Open Control Center:* Swipe down from the top-right corner. (See [Use and customize Control Center on iPad.](#))
- *See earlier notifications:* Swipe up from the center. (See [View and respond to notifications on iPad.](#))
- *View widgets:* Swipe right. (See [Add widgets on iPad.](#))
- *Start drawing and taking notes:* (on [supported models](#)) Tap Apple Pencil on the Lock Screen. Whatever you create is [saved in Notes.](#)

To choose what you can access from the Lock Screen, see [Control access to information on the iPad Lock Screen.](#)


Show notification previews on the Lock Screen

1. Go to Settings  > Notifications.
2. Tap Show Previews, then tap Always.

Notification previews include text from Messages, lines from Mail messages, and details about Calendar invitations. See [View and respond to notifications on iPad.](#)


11.19 Change notification settings on iPhone


Change notification settings on iPhone


In Settings , choose which apps can send notifications, change the alert sound, set up location-based alerts, allow government alerts, and more.

Change notification settings

Most notification settings can be customized for each app. You can turn app notifications on or off, have notifications play a sound, choose how and where you want app notifications to appear when your device is unlocked, and more.

1. Go to Settings  > Notifications.
2. To schedule a notifications summary, tap Scheduled Summary, then turn on Scheduled Summary.

Select the apps you want notifications for in your summary, set a time for delivery of your summary, then tap  at the top left. (See [schedule a notifications summary.](#))

3. To choose when you want most notification previews to appear, tap Show Previews, select an option—Always, When Unlocked, or Never—then tap  at the top left.

Previews can include things like text (from Messages and Mail) and invitation details (from Calendar). You can override this setting for individual apps.

4. Tap an app below Notification Style, then turn Allow Notifications on or off.

If you turn on Allow Notifications, choose when you want the notifications delivered—immediately or in the scheduled notifications summary—and turn Time Sensitive Notifications on or off.

For many apps, you can also set a notification banner style and turn sounds and badges on or off.

5. Tap Notification Grouping, then choose how you want the notifications grouped:
 - *Automatic*: The notifications from the app are grouped according to organizing criteria within the app, such as by topic or thread.
 - *By App*: All the notifications from the app are grouped together.
 - *Off*: Turn off grouping.


To turn off notifications selectively for apps, go to Settings > Notifications > Siri Suggestions, then turn off any app.

When you use Focus, it delays the delivery of notifications on iPhone to prevent interruptions. You can schedule a time to receive a summary of the notifications you missed. See [Schedule a notifications summary](#).

Set up or turn off location-based alerts

Some apps use your location to send you relevant alerts based on where you are. For example, you might get a reminder to call someone when you get to a specific place or when you leave for your next location.


If you don't want to see these types of alerts, you can turn them off.

1. Go to Settings  > Privacy > Location Services.
2. Turn on Location Services.
3. Tap an app (if any appear in the list), then choose whether you want to share your location while using that app.

See the Apple Support article [About privacy and Location Services](#).

Get government alerts


In some countries or regions, you can turn on alerts in the Government Alerts list. For example, on iPhone in the United States, you can receive presidential alerts, and you can turn AMBER, Public Safety, and Emergency Alerts (which include both Severe and Extreme Imminent Threat alerts) on or off (they're on by default). On iPhone in Japan, you can receive Emergency Earthquake Alerts from the Japan Meteorological Agency.

1. Go to Settings  > Notifications.
2. Scroll down to the Government Alerts section, then turn on the ones you want.

Government alerts vary by carrier and iPhone model, and may not work under all conditions. See the Apple Support article [About emergency and government alerts](#).


11.20 Change notification settings on iPad

Change notification settings on iPad

In Settings , choose which apps can send notifications, change the alert sound, set up location-based alerts, allow government alerts, and more.

Change notification settings

Most notification settings can be customized for each app. You can turn app notifications on or off, have notifications play a sound, choose how and where you want app notifications to appear when your device is unlocked, and more.

1. Go to Settings  > Notifications.
2. To schedule a notifications summary, tap Scheduled Summary, then turn on Scheduled Summary.

Select the apps you want notifications for in your summary, set a time for delivery of your summary, then tap < at the top left. (See [schedule a notifications summary](#).)
3. To choose when you want most notification previews to appear, tap Show Previews, select an option—Always, When Unlocked, or Never—then tap < at the top left.

Previews can include things like text (from Messages and Mail) and invitation details (from Calendar). You can override this setting for individual apps.

4. Tap an app below Notification Style, then turn Allow Notifications on or off.

If you turn on Allow Notifications, choose when you want the notifications delivered—immediately or in the scheduled notifications summary—and turn Time Sensitive Notifications on or off.

For many apps, you can also set a notification banner style and turn sounds and badges on or off.

5. Tap Notification Grouping, then choose how you want the notifications grouped:
 - *Automatic*: The notifications from the app are grouped according to organizing criteria within the app, such as by topic or thread.
 - *By App*: All the notifications from the app are grouped together.
 - *Off*: Turn off grouping.


To turn off notifications selectively for apps, go to Settings > Notifications > Siri Suggestions, then turn off any app.

When you use Focus, it delays the delivery of notifications on iPhone to prevent interruptions. You can schedule a time to receive a summary of the notifications you missed. See [Schedule a notifications summary](#).

Set up or turn off location-based alerts

Some apps use your location to send you relevant alerts based on where you are. For example, you might get a reminder to call someone when you get to a specific place or when you leave for your next location.

If you don't want to see these types of alerts, you can turn them off.

1. Go to Settings  > Privacy > Location Services.
2. Turn on Location Services.
3. Tap an app (if any appear in the list), then choose whether you want to share your location while using that app.

11.21 View or change cellular data settings on iPhone

View or change cellular data settings on iPhone

You can turn cellular data and roaming on or off, set which apps and services use cellular data, see cellular data usage, and set other cellular data options.

Note: For help with cellular network services, voicemail, and billing, contact your wireless service provider.

If iPhone is connected to the internet using the cellular data network, an icon identifying the cellular network appears in the [status bar](#).


5G, LTE, 4G, and 3G service on GSM cellular networks support simultaneous voice and data communications. For all other cellular connections, you can't use internet services while you're talking on the phone unless iPhone also has a Wi-Fi connection to the internet. Depending on your network connection, you may not be able to receive calls while iPhone transfers data over the cellular network—when downloading a webpage, for example.

- *GSM networks:* On an EDGE or GPRS connection, incoming calls may go directly to voicemail during data transfers. For incoming calls that you answer, data transfers are paused.
- *CDMA networks:* On EV-DO connections, data transfers are paused when you answer incoming calls. On 1xRTT connections, incoming calls may go directly to voicemail during data transfers. For incoming calls that you answer, data transfers are paused.

Data transfer resumes when you end the call.

If Cellular Data is off, all data services—including email, web browsing, and push notifications—use Wi-Fi only. If Cellular Data is on, carrier charges may apply. For example, using certain features and services that transfer data, such as Siri and Messages, could result in charges to your data plan.

Choose cellular data options for data usage, performance, battery life, and more

To turn Cellular Data on or off, go to Settings  > Cellular.

To set options when Cellular Data is on, go to Settings > Cellular > Cellular Data Options, then do any of the following:

- *Reduce cellular usage:* Turn on Low Data Mode, or tap Data Mode, then choose Low Data Mode. This mode pauses automatic updates and background tasks when iPhone isn't connected to Wi-Fi.
- *Turn Data Roaming on or off:* Data Roaming permits internet access over a cellular data network when you're in a region not covered by your carrier's network. When you're traveling, you can turn off Data Roaming to avoid roaming charges.


Depending on your iPhone model, carrier, and region, the following options may be available:

- *Turn Voice Roaming on or off:* (CDMA) Turn Voice Roaming off to avoid charges from using other carrier's networks. When your carrier's network isn't available, iPhone won't have cellular (data or voice) service.
- *Enable or disable 4G/LTE:* Using 4G or LTE loads internet data faster in some cases but may decrease battery performance. There may be options for turning off 4G/LTE or for selecting Voice & Data (VoLTE) or Data Only.

On iPhone 12 models and later, you can do the following:

- *Enable Smart Data mode to optimize battery life:* Tap Voice & Data, then choose 5G Auto. In this mode, your iPhone automatically switches to LTE when 5G speeds don't provide noticeably better performance.
- *Use higher-quality video and FaceTime HD on 5G networks:* Tap Data Mode, then choose Allow More Data on 5G.

Set up a Personal Hotspot to begin sharing the cellular internet connection from iPhone

1. Go to Settings  > Cellular, then turn on Cellular Data.
2. Tap Set up Personal Hotspot, then follow the instructions in [Share your internet connection from iPhone](#).

Set cellular data use for apps and services

Go to Settings  > Cellular, then turn Cellular Data on or off for any app (such as Maps) or service (such as Wi-Fi Assist) that can use cellular data.

If a setting is off, iPhone uses only Wi-Fi for that service.

Note: Wi-Fi Assist is on by default. If Wi-Fi connectivity is poor, Wi-Fi Assist automatically switches to cellular data to boost the signal. Because you stay connected to the internet over cellular when you have a poor Wi-Fi connection, you might use more cellular data, which may incur additional charges depending on your data plan. See the Apple Support article [About Wi-Fi Assist](#).

Lock your SIM card

If your device uses a SIM card for phone calls or cellular data, you can lock the card with a personal identification number (PIN) to prevent others from using the card. Then, every time you restart your device or remove the SIM card, your card locks automatically, and you're required to enter your PIN.

See [Use a SIM PIN for your iPhone or iPad](#).

See also

[Set up cellular service on iPhone](#)

11.22 View or change cellular data settings on iPad (Wi-Fi + Cellular models)

View or change cellular data settings on iPad (Wi-Fi + Cellular models)

You can activate cellular data service on iPad, turn cellular service on or off, and set which apps and services use cellular data. With some carriers, you can also change your data plan.

[Supported models](#) can connect to 5G networks. See the Apple Support article [Use 5G with your iPad](#).


Note: For help with cellular network services and billing, contact your wireless service provider.

If iPad is connected to the internet using the cellular data network, an icon identifying the cellular network appears in the [status bar](#).

If Cellular Data is off, all data services—including email, web browsing, and push notifications—use Wi-Fi only. If Cellular Data is on, carrier charges may be incurred. For example, using certain features and services that transfer data, such as Messages, could result in charges to your data plan.


Note: Wi-Fi + Cellular models don't support cellular phone service—they support cellular data transmission only. To make phone calls on iPad, [use Wi-Fi Calling and an iPhone](#).

Add a cellular plan to your iPad

If you previously set up a cellular plan, go to Settings  > Cellular, tap Add a New Plan, then follow the onscreen instructions.

If you haven't set up a plan, see [Set up cellular service on iPad \(Wi-Fi + Cellular models\)](#).

View or change your cellular data account

Go to Settings  > Cellular Data, then tap Manage *[account name]* or Carrier Services.

Choose cellular data options for data usage, performance, battery life, and more

To turn Cellular Data on or off, go to Settings  > Cellular.

To set options when Cellular Data is on, go to Settings > Cellular > Cellular Data Options, then do any of the following:

- *Reduce cellular usage:* Turn on Low Data Mode, or tap Data Mode, then choose Low Data Mode (depending on your iPad model). This mode pauses automatic updates and background tasks when iPad isn't connected to Wi-Fi.
- *Turn Data Roaming on or off:* Data Roaming permits internet access over a cellular data network when you're in a region not covered by your carrier's network. When you're traveling, you can turn off Data Roaming to avoid roaming charges.


Depending on your iPad model, carrier, and region, the following option may be available:

- *Turn LTE on or off:* Turning on LTE loads data faster.


On iPad Pro 12.9-inch (5th generation) (Wi-Fi + Cellular) and iPad Pro 11-inch (3rd generation) (Wi-Fi + Cellular), you can do the following:

- *Enable Smart Data mode to optimize battery life:* Tap Voice & Data, then choose 5G Auto. In this mode, your iPad automatically switches to LTE when 5G speeds don't provide noticeably better performance.
- *Use higher-quality video and FaceTime HD on 5G networks:* Tap Data Mode, then choose Allow More Data on 5G.

Set up a Personal Hotspot to begin sharing the cellular internet connection from iPad

1. Go to Settings  > Cellular, then turn on Cellular Data.
2. Tap Set up Personal Hotspot, then follow the instructions in [Share your internet connection from iPad \(Wi-Fi + Cellular\)](#).

Set cellular data use for apps and services

Go to Settings  > Cellular Data, then turn Cellular Data on or off for any app (such as Maps) or service (such as Wi-Fi Assist) that can use cellular data.

If a setting is off, iPad uses only Wi-Fi for that service.

Note: Wi-Fi Assist is on by default. If Wi-Fi connectivity is poor, Wi-Fi Assist automatically switches to cellular data to boost the signal. Because you stay connected to the internet over cellular when you have a poor Wi-Fi connection, you might use more cellular data, which may incur additional charges depending on your data plan. See the Apple Support article [About Wi-Fi Assist](#).

Lock your SIM card


If your device uses a SIM card for cellular data, you can lock the card with a personal identification number (PIN) to prevent others from using the card. Then, every time you restart your device or remove the SIM card, your card locks automatically, and you're required to enter your PIN. See [Use a SIM PIN for your iPhone or iPad](#).


11.23 Connect iPhone to the internet

Connect iPhone to the internet

Connect your iPhone to the internet by using an available Wi-Fi or cellular network.


Connect iPhone to a Wi-Fi network

1. Go to Settings  > Wi-Fi, then turn on Wi-Fi.
2. Tap one of the following:
 - *A network*: Enter the password, if required.
 - *Other*: Joins a hidden network. Enter the name of the hidden network, security type, and password.

If  appears at the top of the screen, iPhone is connected to a Wi-Fi network. (To verify this, open Safari to view a webpage.) iPhone reconnects when you return to the same location.

Join a Personal Hotspot


If an iPad (Wi-Fi + Cellular) or another iPhone is sharing a Personal Hotspot, you can use its cellular internet connection.

Go to Settings  > Wi-Fi, then choose the name of the device sharing the Personal Hotspot.

If asked for a password on your iPhone, enter the password shown in Settings > Cellular > Personal Hotspot on the device sharing the Personal Hotspot.

Connect iPhone to a cellular network

Your iPhone automatically connects to your carrier's cellular data network if a Wi-Fi network isn't available. If iPhone doesn't connect, check the following:

1. Verify that your SIM is activated and unlocked. See [Set up cellular service on iPhone](#).
2. Go to Settings  > Cellular.
3. Verify that Cellular Data is turned on. On [models with Dual SIM](#), tap Cellular Data, then verify the selected line. (You can choose only one line for cellular data.)

When you need an internet connection, iPhone does the following, in order, until the connection is made:

- Tries to connect to the most recently used available Wi-Fi network
- Shows a list of Wi-Fi networks in range and connects to the one you choose
- Connects to your carrier's cellular data network

On an [iPhone that supports 5G](#), iPhone may use your 5G cellular data instead of Wi-Fi. If so, you see Using 5G Cellular For Internet below the Wi-Fi network's name. To switch back to Wi-Fi, tap ⓘ next to the network name, then tap Use Wi-Fi for Internet.

Note: If a Wi-Fi connection to the internet isn't available, apps and services may transfer data over your carrier's cellular network, which may result in additional fees. Contact your carrier for information about your cellular data plan rates. To manage cellular data usage, see [View or change cellular data settings on iPhone](#).

See also

[Turn on iCloud Private Relay on iPhone](#)

[Apple Support article: Use 5G with your iPhone](#)


11.24 Connect iPad to the internet

Connect iPad to the internet

Connect your iPad to the internet by using an available Wi-Fi network. Wi-Fi + Cellular models can also connect to the internet by using a cellular network.

Connect iPad to a Wi-Fi network

1. Go to Settings ⓘ > Wi-Fi, then turn on Wi-Fi.
2. Tap one of the following:
 - *A network:* Enter the password, if required.
 - *Other:* Joins a hidden network. Enter the name of the hidden network, security type, and password.

If  appears at the top of the screen, iPad is connected to a Wi-Fi network. (To verify this, open Safari to view a webpage.) iPad reconnects when you return to the same location.

Join a Personal Hotspot


If an iPhone or an iPad (Wi-Fi + Cellular) is sharing a Personal Hotspot, you can use its cellular internet connection.

Go to Settings ⓘ > Wi-Fi, then choose the name of the device sharing the Personal Hotspot.

If asked for a password on your iPad, enter the password shown in Settings ⓘ > Cellular > Personal Hotspot on the device sharing the Personal Hotspot.


Connect iPad to a cellular network (Wi-Fi + Cellular models)

Your iPad automatically connects to your carrier's cellular data network if a Wi-Fi network isn't available. If iPad doesn't connect, check the following:

1. Verify that your SIM is activated and unlocked. See [Set up cellular service on iPad \(Wi-Fi + Cellular models\)](#).
2. Go to Settings  > Cellular Data.
3. Verify that Cellular Data is turned on.

When you need an internet connection, iPad does the following, in order, until the connection is made:

- Tries to connect to the most recently used available Wi-Fi network
- Shows a list of Wi-Fi networks in range and connects to the one you choose
- Connects to your carrier's cellular data network (Wi-Fi + Cellular models)

On an [iPad that supports 5G](#), iPad may use your 5G cellular data instead of Wi-Fi. If so, you see Using 5G Cellular For Internet below the Wi-Fi network's name. To switch back to Wi-Fi, tap  next to the network name, then tap Use Wi-Fi for Internet.

Note: If a Wi-Fi connection to the internet isn't available, apps and services may transfer data over your carrier's cellular network, which may result in additional fees. Contact your carrier for information about your cellular data plan rates. To manage cellular data usage, see [View or change cellular data settings on iPad \(Wi-Fi + Cellular models\)](#).

See also

[Turn on iCloud Private Relay on iPad](#)

[Apple Support article: Use 5G with your iPad](#)

[Apple Support article: Set up cellular data service on your Wi-Fi + Cellular model iPad](#)

11.25 Share your internet connection from iPhone


Share your internet connection from iPhone

You can use Personal Hotspot to share a cellular internet connection from your iPhone to other devices. Personal Hotspot is useful when the other devices don't have internet access from a Wi-Fi network. Instant Hotspot allows you to connect your devices to Personal Hotspot without entering a password.

If a nearby iPhone or iPad (Wi-Fi + Cellular models) is sharing its Personal Hotspot, you can use its cellular internet connection on your iPhone. See [Join a Personal Hotspot](#).

Note: Personal Hotspot is not available with all carriers. Additional fees may apply. The number of devices that can join your Personal Hotspot at one time depends on your carrier and iPhone model. Contact your carrier for more information.

Set up Personal Hotspot on iPhone

Go to Settings  > Cellular > Personal Hotspot, then turn on Allow Others to Join.

Note: If you don't see the option for Personal Hotspot, and Cellular Data is turned on in Settings > Cellular, contact your carrier about adding Personal Hotspot to your plan.


You can change the following settings:

- *Change the Wi-Fi password for your Personal Hotspot:* Go to Settings > Cellular > Personal Hotspot > Wi-Fi Password.
- *Change the name of your Personal Hotspot:* Go to Settings > General > About > Name.
- *Turn off Personal Hotspot and disconnect devices:* Go to Settings > Cellular > Personal Hotspot, then turn off Allow Others to Join.



On [models with Dual SIM](#), Personal Hotspot uses the line selected for cellular data.


Connect a Mac or PC to your Personal Hotspot

You can use a USB cable, Wi-Fi, or Bluetooth to connect a Mac or PC to your Personal Hotspot. Do one of the following:


- *Use USB:* [Connect iPhone and your computer with a cable](#). If you see an alert that says Trust this Computer?, tap Trust. In your computer's Network preferences, choose iPhone, then configure the network settings.
- *Use Wi-Fi and Instant Hotspot:* On your Mac, use the Wi-Fi status menu  in the menu bar to choose your iPhone from the list of available networks.

You need to be [signed in with the same Apple ID](#) on your Mac and iPhone, and have Bluetooth and Wi-Fi turned on.

The Wi-Fi status icon  in the menu bar changes to the Personal Hotspot icon  as long as your Mac remains connected to your Personal Hotspot.

- *Use Bluetooth:* To make sure your iPhone is discoverable, go to Settings  > Bluetooth and leave the screen showing. Then on your Mac or PC, follow the manufacturer directions to set up a Bluetooth network connection.

Connect iPad, iPod touch, or another iPhone to your Personal Hotspot

On the other device, go to Settings  > Wi-Fi, then choose your iPhone from the list of available networks.

If asked for a password on the other device, enter the password shown in Settings > Cellular > Personal Hotspot on your iPhone.

If your iPhone and the other device are set up as follows, then Instant Hotspot connects the devices without requiring a password:

- You're [signed in with the same Apple ID](#) on each device.
- Each device has Bluetooth turned on.
- Each device has Wi-Fi turned on.

When a device is connected, a blue band appears at the top of your iPhone screen. The Personal Hotspot icon  appears in the status bar of the connected device.

With Family Sharing, you can share your Personal Hotspot with any member of your family automatically or after they ask for approval. See [Set up Family Sharing on iPhone](#).

When you share a Personal Hotspot from your iPhone, it uses cellular data for the internet connection. To monitor your cellular data network usage, go to Settings > Cellular > Usage. See [View or change cellular data settings on iPhone](#).

If you need more help using Personal Hotspot, see the Apple Support article [If Personal Hotspot is not working](#).

11.26 Share your internet connection from iPad (Wi-Fi + Cellular)


Share your internet connection from iPad (Wi-Fi + Cellular)

If you have an active cellular data plan, you can use Personal Hotspot to share a cellular internet connection from your iPad (Wi-Fi + Cellular models) to other devices. Personal Hotspot is useful when the other devices don't have internet access from a Wi-Fi network. Instant Hotspot allows you to connect your devices to Personal Hotspot without entering a password.

If a nearby iPhone or iPad (Wi-Fi + Cellular models) is sharing its Personal Hotspot, you can use its cellular internet connection on your iPad. See [Join a Personal Hotspot](#).

Note: Personal Hotspot is not available with all carriers. Additional fees may apply. The number of devices that can join your Personal Hotspot at one time depends on your carrier and iPad model. Contact your carrier for more information.

Set up Personal Hotspot on iPad

Go to Settings  > Cellular > Personal Hotspot, then turn on Allow Others to Join.


Note: If you don't see the option for Personal Hotspot, but you have an active cellular data plan and Cellular Data is turned on in Settings > Cellular, contact your carrier about adding Personal Hotspot to your plan.

You can change the following settings:



- *Change the Wi-Fi password for your Personal Hotspot:* Go to Settings > Cellular > Personal Hotspot > Wi-Fi Password.
- *Change the name of your Personal Hotspot:* Go to Settings > General > About > Name.
- *Turn off Personal Hotspot and disconnect devices:* Go to Settings > Cellular > Personal Hotspot, then turn off Allow Others to Join.

Connect a Mac or PC to your Personal Hotspot


You can use a USB cable, Wi-Fi, or Bluetooth to connect a Mac or PC to your Personal Hotspot. Do one of the following:

- *Use USB:* [Connect iPad and your computer with a cable](#). If you see an alert that says Trust this Computer?, tap Trust. In your computer's Network preferences, choose iPad, then configure the network settings.
- *Use Wi-Fi and Instant Hotspot:* On your Mac, use the Wi-Fi status menu  in the menu bar to choose your iPad from the list of available networks.

You need to be [signed in with the same Apple ID](#) on your Mac and iPad, and have Bluetooth and Wi-Fi turned on.

The Wi-Fi status icon  in the menu bar changes to the Personal Hotspot icon  as long as your Mac remains connected to your Personal Hotspot.


Connect iPhone, iPod touch, or another iPad to your Personal Hotspot

On the other device, go to Settings  > Wi-Fi, then choose your iPad from the list of available networks.

If asked for a password on the other device, enter the password shown in Settings > Cellular > Personal Hotspot on your iPad.

If your iPad and the other device are set up as follows, then Instant Hotspot connects the devices without requiring a password:

- You're [signed in with the same Apple ID](#) on each device.
- Each device has Bluetooth turned on.
- Each device has Wi-Fi turned on.

When a device is connected, a blue band appears at the top of your iPad screen. The Personal Hotspot icon  appears in the status bar of the connected device.

With Family Sharing, you can share your Personal Hotspot with any member of your family automatically or after they ask for approval. See [Set up Family Sharing on iPad](#).




When you share a Personal Hotspot from your iPad, it uses cellular data for the internet connection. To monitor your cellular data network usage, go to Settings > Cellular > Usage. See [View or change your cellular data account](#).

If you need more help using Personal Hotspot, see the Apple Support article [If Personal Hotspot is not working](#).

11.27 Ultra Wideband information

Ultra Wideband information

Ultra Wideband is available on iPhone 11 and later models, and availability varies by region.


When use of Ultra Wideband is prohibited in your region, such as while traveling in aircraft, Ultra Wideband can be turned off by turning on airplane mode. To turn on airplane mode, [open Control Center](#), then tap . You can also turn airplane mode on or off in Settings . When airplane mode is on,  appears in the status bar.

Australia: Ultra Wideband transmitters must not be operated within a nominated distance from specified Australian radio-astronomy sites. For further information about nominated distance, please refer to the Radiocommunications (Low Interference Potential Devices) Class Licence 2015 published by the Australian Communications and Media Authority.

11.28 Control the location information you share on iPhone

Control the location information you share on iPhone


You control whether iPhone and apps have information about your location.

To figure out where you are when getting directions, setting up meetings, and more, Location Services uses information (when available) from GPS networks, your Bluetooth connections, your local Wi-Fi networks, and your cellular network. When an app is using Location Services,  appears in the status bar.

When you set up iPhone, you're asked if you want to turn on Location Services. Afterward, you can turn Location Services on or off at any time.


The first time an app wants location data from your iPhone, you receive a request with an explanation. Some apps may make a one-time only request for your location. Other apps may ask you to share your location now and in the future. Whether you grant or deny ongoing access to your location, you can change an app's access later.

Turn on Location Services

If you didn't turn on Location Services when you first set up iPhone, go to Settings  > Privacy > Location Services, then turn on Location Services.

Important: If you turn off Location Services, many important iPhone features stop working.

Review or change an app's ongoing access to location information

1. Go to Settings  > Privacy > Location Services.
2. To review or change access settings for an app or to see its explanation for requesting Location Services, tap the app.

To allow an app to use your specific location, leave Precise Location turned on. To share only your approximate location—which may be sufficient for an app that doesn't need your exact location—turn Precise Location off.

Note: If you set the access for an app to Ask Next Time, you're asked to turn on Location Services again the next time an app tries to use it.

To understand how a third-party app uses the information it's requesting, review its terms and privacy policy. See the Apple Support article [About privacy and Location Services](#).

Hide the map in Location Services alerts



When you allow an app to always use your location in the background, you may receive alerts about the app's use of that information. (These alerts let you change your permission, if you want to.) In the alerts, a map shows locations recently accessed by the app.

To hide the map, go to Settings  > Privacy > Location Services > Location Alerts, then turn off Show Map in Location Alerts.

With the setting off, you continue to receive location alerts, but the map isn't shown.

Review or change Location Services settings for system services

Several system services, such as location-based suggestions and location-based ads, use Location Services.

To see the status for each service, to turn Location Services on or off for each service, or to show  in the status bar when enabled system services use your location, go to Settings  > Privacy > Location Services > System Services.


See also

[Control access to information in apps on iPhone](#)

11.29 Control the location information you share on iPad

Control the location information you share on iPad


You control whether iPad and apps have information about your location.

To figure out where you are when getting directions, setting up meetings, and more, Location Services uses information (when available) from GPS networks (iPad models with Wi-Fi + Cellular), your Bluetooth connections, your local Wi-Fi networks, and your cellular network (iPad models with Wi-Fi + Cellular, if you have Cellular Data turned on). When an app is using Location Services,  appears in the status bar.

When you set up iPad, you're asked if you want to turn on Location Services. Afterward, you can turn Location Services on or off at any time.


The first time an app wants location data from your iPad, you receive a request with an explanation. Some apps may make a one-time only request for your location. Other apps may ask you to share your location now and in the future. Whether you grant or deny ongoing access to your location, you can change an app's access later.

Turn on Location Services

If you didn't turn on Location Services when you first set up iPad, go to Settings  > Privacy > Location Services, then turn on Location Services.

Important: If you turn off Location Services, many important iPad features stop working.

Review or change an app's ongoing access to location information

1. Go to Settings  > Privacy > Location Services.
2. To review or change access settings for an app or to see its explanation for requesting Location Services, tap the app.


To allow an app to use your specific location, leave Precise Location turned on. To share only your approximate location—which may be sufficient for an app that doesn't need your exact location—turn Precise Location off.

Note: If you set the access for an app to Ask Next Time, you're asked to turn on Location Services again the next time an app tries to use it.

To understand how a third-party app uses the information it's requesting, review its terms and privacy policy. See the Apple Support article [About privacy and Location Services](#).

Hide the map in Location Services alerts



When you allow an app to always use your location in the background, you may receive alerts about the app's use of that information. (These alerts let you change your permission, if you want to.) In the alerts, a map shows locations recently accessed by the app.

To hide the map, go to Settings  > Privacy > Location Services > Location Alerts, then turn off Show Map in Location Alerts.

With the setting off, you continue to receive location alerts, but the map isn't shown.

Review or change Location Services settings for system services

Several system services, such as location-based suggestions and location-based ads, use Location Services.


To see the status for each service, to turn Location Services on or off for each service, or to show  in the status bar when enabled system services use your location, go to Settings  > Privacy > Location Services > System Services.

See also

[Control access to information in apps on iPhone](#)

11.30 Set up iCloud Drive on iPhone

Set up iCloud Drive on iPhone


Use the Files app  to store files and folders in iCloud Drive. You can access them from all your devices where you're signed in with the same [Apple ID](#). Any changes you make appear on all your devices set up with iCloud Drive.

iCloud Drive is built into the Files app on devices with iOS 11, iPadOS 13, or later. You can also use iCloud Drive on Mac computers (OS X 10.10 or later) and PCs (iCloud for Windows 7 or later). Storage limits depend on your iCloud storage plan.

Turn on iCloud Drive

Go to Settings  > [your name] > iCloud, then turn on iCloud Drive.

Choose which apps use iCloud Drive

Go to Settings  > [your name] > iCloud, then turn each of the apps listed under iCloud Drive on or off.

Browse iCloud Drive

1. Tap Browse at the bottom of the screen.
2. Under Locations, tap iCloud Drive.


If you don't see Locations, tap Browse again. If you don't see iCloud Drive under Locations, tap Locations.

3. To open a folder, tap it.

See [View files and folders in Files on iPhone](#).

11.31 Set up iCloud Drive on iPad

Set up iCloud Drive on iPad


Use the Files app  to store files and folders in iCloud Drive. You can access them from all your devices where you're signed in with the same [Apple ID](#). Any changes you make appear on all your devices set up with iCloud Drive.

iCloud Drive is built into the Files app on devices with iOS 11, iPadOS 13, or later. You can also use iCloud Drive on Mac computers (OS X 10.10 or later) and PCs (iCloud for Windows 7 or later). Storage limits depend on your iCloud storage plan.

Turn on iCloud Drive

Go to Settings  > [your name] > iCloud, then turn on iCloud Drive.

Choose which apps use iCloud Drive

Go to Settings  > [your name] > iCloud, then turn each of the apps listed under iCloud Drive on or off.

Browse iCloud Drive

1. Tap Browse at the bottom of the screen.
2. Under Locations, tap iCloud Drive.

If you don't see Locations, tap Browse again. If you don't see iCloud Drive under Locations, tap Locations.

3. To open a folder, tap it.

See [View files and folders in Files on iPad](#).

11.32 Update iOS on iPhone


Update iOS on iPhone

When you update to the latest version of iOS, your data and settings remain unchanged.

Before you update, set up iPhone to [back up](#) automatically, or back up your device manually.

Update iPhone automatically


If you didn't turn on automatic updates when you first set up your iPhone, do the following:

1. Go to Settings  > General > Software Update > Automatic Updates.
2. Turn on Download iOS Updates and Install iOS Updates.

When an update is available, iPhone downloads and installs the update overnight while charging and connected to Wi-Fi. You're notified before an update is installed.

Update iPhone manually

At any time, you can check for and install software updates.

Go to Settings  > General > Software Update.

The screen shows the currently installed version of iOS and whether an update is available.

To turn off automatic updates, go to Settings > General > Software Update > Automatic Updates.

Update using your computer

1. [Connect iPhone and your computer with a cable.](#)
2. Do one of the following:
 - *In the Finder sidebar on your Mac:* Select your iPhone, then click General at the top of the window.

To use the Finder to update your iPhone, macOS 10.15 or later is required. With earlier versions of macOS, [use iTunes](#) to update your iPhone.
 - *In the iTunes app on your Windows PC:* Click the iPhone button near the top left of the iTunes window, then click Summary.
3. Click Check for Update.
4. To install an available update, click Update.

See the Apple Support articles [Update to the latest iOS](#) and [If you can't update or restore your iPhone, iPad, or iPod touch](#).

11.33 Update iPadOS


Update iPadOS

When you update to the latest version of iPadOS, your data and settings remain unchanged.

Before you update, set up iPad to [back up](#) automatically, or back up your iPad manually.

Update iPad automatically


If you didn't turn on automatic updates when you first set up your iPad, do the following:

1. Go to Settings  > General > Software Update > Automatic Updates.
2. Turn on Download iPadOS Updates and Install iPadOS Updates.

When an update is available, iPad downloads and installs the update overnight while charging and connected to Wi-Fi. You're notified before an update is installed.

Update iPad manually

At any time, you can check for and install software updates.

Go to Settings  > General > Software Update.

The screen shows the currently installed version of iPadOS and whether an update is available.

To turn off automatic updates, go to Settings > General > Software Update > Automatic Updates.

Update using your computer

1. [Connect iPad and your computer with a cable.](#)
2. Do one of the following:
 - *In the Finder sidebar on your Mac:* Select your iPad, then click General at the top of the window.


To use the Finder to update your iPad, macOS 10.15 or later is required. With earlier versions of macOS, [use iTunes](#) to update your iPad.
 - *In the iTunes app on your Windows PC:* Click the iPad button near the top left of the iTunes window, then click Summary.
3. Click Check for Update.
4. To install an available update, click Update.

See the Apple Support articles [Update to the latest iOS](#) and [If you can't update or restore your iPhone, iPad, or iPod touch](#).


11.34 Back up iPhone

Back up iPhone

You can back up iPhone using iCloud or your computer. To decide which method is best for you, see [About backups for iPhone, iPad, and iPod touch](#).

 **Tip:** If you replace your iPhone, you can use its backup to transfer your information to the new device. See [Restore all content to iPhone from a backup](#).

Back up iPhone using iCloud

1. Go to Settings  > [your name] > iCloud > iCloud Backup.
2. Turn on iCloud Backup.

iCloud automatically backs up your iPhone daily when iPhone is connected to power, locked, and connected to Wi-Fi.

Note: On [models that support 5G](#), your carrier may give you the option to back up iPhone using your cellular network. Go to Settings > [your name] > iCloud > iCloud Backup, then turn on or off Backup Over Cellular.

3. To perform a manual backup, tap Back Up Now.

To view your iCloud backups, go to Settings > [your name] > iCloud > Manage Storage > Backups. To delete a backup, choose a backup from the list, then tap Delete Backup.

Note: If you turn on an iCloud feature (such as iCloud Photos or Contacts) in Settings > [your name] > iCloud, its information is stored in iCloud. Because the information is automatically kept up to date on all your devices, it's not included in your iCloud backup. (See the Apple Support article [What does iCloud back up?](#))

Back up iPhone using your Mac

1. [Connect iPhone and your computer with a cable](#).
2. In the Finder sidebar on your Mac, select your iPhone.

To use the Finder to back up iPhone, macOS 10.15 or later is required. With earlier versions of macOS, [use iTunes](#) to back up iPhone.
3. At the top of the Finder window, click General.
4. Select "Back up all of the data on your iPhone to this Mac."
5. To encrypt your backup data and protect it with a password, select "Encrypt local backup."
6. Click Back Up Now.

Note: You can also connect iPhone to your computer wirelessly if you [set up Wi-Fi syncing](#).

Back up iPhone using your Windows PC

1. [Connect iPhone and your computer with a cable](#).
2. In the iTunes app on your PC, click the iPhone button near the top left of the iTunes window.
3. Click Summary.

4. Click Back Up Now (below Backups).
5. To encrypt your backups, select “Encrypt local backup,” type a password, then click Set Password.


To see the backups stored on your computer, choose Edit > Preferences, then click Devices. Encrypted backups have a lock icon in the list of backups.

Note: You can also connect iPhone to your computer wirelessly if you [set up Wi-Fi syncing](#).


11.35 Back up iPad

Back up iPad

You can back up iPad using iCloud or your computer. To decide which method is best for you, see [About backups for iPhone, iPad, and iPod touch](#).

 **Tip:** If you replace your iPad, you can use its backup to transfer your information to the new device. See [Restore all content to iPad from a backup](#).

Back up iPad using iCloud

1. Go to Settings  > [your name] > iCloud > iCloud Backup.
2. Turn on iCloud Backup.

iCloud automatically backs up your iPad daily when iPad is connected to power, locked, and connected to Wi-Fi.

Note: On WiFi + Cellular models [that support 5G](#), your carrier may give you the option to back up iPad using your cellular network. Go to Settings > [your name] > iCloud > iCloud Backup, the turn on or off Backup Over Cellular.

3. To perform a manual backup, tap Back Up Now.

To view your iCloud backups, go to Settings > [your name] > iCloud > Manage Storage > Backups. To delete a backup, choose a backup from the list, then tap Delete Backup.

Note: If you turn on an iCloud feature (such as iCloud Photos or Contacts) in Settings > [your name] > iCloud, its information is stored in iCloud. Because the information is automatically kept up to date on all your devices, it’s not included in your iCloud backup. (See the Apple Support article [What does iCloud back up?](#))

Back up iPad using your Mac

1. [Connect iPad and your computer with a cable](#).
2. In the Finder sidebar on your Mac, select your iPad.

To use the Finder to back up iPad, macOS 10.15 or later is required. With earlier versions of macOS, [use iTunes](#) to back up iPad.

3. At the top of the Finder window, click General.
4. Select "Back up all of the data on your iPad to this Mac."
5. To encrypt your backup data and protect it with a password, select "Encrypt local backup."
6. Click Back Up Now.

Note: You can also connect iPad to your computer wirelessly if you [set up Wi-Fi syncing](#).

Back up iPad using your Windows PC

1. [Connect iPad and your computer with a cable](#).
2. In the iTunes app on your PC, click the iPad button near the top left of the iTunes window.
3. Click Summary.
4. Click Back Up Now (below Backups).
5. To encrypt your backups, select "Encrypt local backup," type a password, then click Set Password.

To see the backups stored on your computer, choose Edit > Preferences, then click Devices. Encrypted backups have a lock icon in the list of backups.

Note: You can also connect iPad to your computer wirelessly if you [set up Wi-Fi syncing](#).