

Security Configuration Benchmark For

Apple iOS

Version 1.2.0

October 19, 2010

Copyright 2001-2010, The Center for Internet Security

<http://cisecurity.org>

feedback@cisecurity.org

Terms of Use Agreement

Background.

CIS provides benchmarks, scoring tools, software, data, information, suggestions, ideas, and other services and materials from the CIS website or elsewhere (“**Products**”) as a public service to Internet users worldwide. Recommendations contained in the Products (“**Recommendations**”) result from a consensus-building process that involves many security experts and are generally generic in nature. The Recommendations are intended to provide helpful information to organizations attempting to evaluate or improve the security of their networks, systems and devices. Proper use of the Recommendations requires careful analysis and adaptation to specific user requirements. The Recommendations are not in any way intended to be a “quick fix” for anyone’s information security needs.

No representations, warranties and covenants.

CIS makes no representations, warranties or covenants whatsoever as to (i) the positive or negative effect of the Products or the Recommendations on the operation or the security of any particular network, computer system, network device, software, hardware, or any component of any of the foregoing or (ii) the accuracy, reliability, timeliness or completeness of any Product or Recommendation. CIS is providing the Products and the Recommendations “as is” and “as available” without representations, warranties or covenants of any kind.

User agreements.

By using the Products and/or the Recommendations, I and/or my organization (“**we**”) agree and acknowledge that:

No network, system, device, hardware, software or component can be made fully secure;
We are using the Products and the Recommendations solely at our own risk;

We are not compensating CIS to assume any liabilities associated with our use of the Products or the Recommendations, even risks that result from CIS’s negligence or failure to perform;

We have the sole responsibility to evaluate the risks and benefits of the Products and Recommendations to us and to adapt the Products and the Recommendations to our particular circumstances and requirements;

Neither CIS, nor any CIS Party (defined below) has any responsibility to make any corrections, updates, upgrades or bug fixes or to notify us if it chooses at its sole option to do so; and

Neither CIS nor any CIS Party has or will have any liability to us whatsoever (whether based in contract, tort, strict liability or otherwise) for any direct, indirect, incidental, consequential, or special damages (including without limitation loss of profits, loss of sales, loss of or damage to reputation, loss of customers, loss of software, data, information or emails, loss of privacy, loss of use of any computer or other equipment, business interruption, wasted management or other staff resources or claims of any kind against us from third parties) arising out of or in any way connected with our use of or our inability to use any of the Products or Recommendations (even if CIS has been advised of the possibility of such damages), including without limitation any liability associated with infringement of intellectual property, defects, bugs, errors, omissions, viruses, worms, backdoors, Trojan horses or other harmful items.

Grant of limited rights.

CIS hereby grants each user the following rights, but only so long as the user complies with all of the terms of these Agreed Terms of Use:

Except to the extent that we may have received additional authorization pursuant to a written agreement with CIS, each user may download, install and use each of the Products on a single computer;

Each user may print one or more copies of any Product or any component of a Product that is in a .txt, .pdf, .doc, .mcw, or .rtf format, provided that all such copies are printed in full and are kept intact, including without limitation the text of this Agreed Terms of Use in its entirety.

Retention of intellectual property rights; limitations on distribution.

The Products are protected by copyright and other intellectual property laws and by international treaties. We acknowledge and agree that we are not acquiring title to any intellectual property rights in the Products and that full title and all ownership rights to the Products will remain the exclusive property of CIS or CIS Parties. CIS reserves all rights not expressly granted to users in the preceding section entitled "Grant of limited rights." Subject to the paragraph entitled "Special Rules" (which includes a waiver, granted to some classes of CIS Members, of certain limitations in this paragraph), and except as we may have otherwise agreed in a written agreement with CIS, we agree that we will not (i) decompile, disassemble, reverse engineer, or otherwise attempt to derive the source code for any software Product that is not already in the form of source code; (ii) distribute, redistribute, encumber, sell, rent, lease, lend, sublicense, or otherwise transfer or exploit rights to any Product or any component of a Product; (iii) post any Product or any component of a Product on any website, bulletin board, ftp server, newsgroup, or other similar mechanism or device, without regard to whether such mechanism or device is internal or external, (iv) remove or alter trademark, logo, copyright or other proprietary notices, legends, symbols or labels in any Product or any component of a Product; (v) remove these Agreed Terms of Use from, or alter these Agreed Terms of Use as they appear in, any Product or any component of a Product; (vi) use any Product or any component of a Product with any derivative works based directly on a Product or any component of a Product; (vii) use any Product or any component of a Product with other products or applications that are directly and specifically dependent on such Product or any component for any part of their functionality, or (viii) represent or claim a particular level of compliance with a CIS Benchmark, scoring tool or other Product. We will not facilitate or otherwise aid other individuals or entities in any of the activities listed in this paragraph.

We hereby agree to indemnify, defend and hold CIS and all of its officers, directors, members, contributors, employees, authors, developers, agents, affiliates, licensors, information and service providers, software suppliers, hardware suppliers, and all other persons who aided CIS in the creation, development or maintenance of the Products or Recommendations ("**CIS Parties**") harmless from and against any and all liability, losses, costs and expenses (including attorneys' fees and court costs) incurred by CIS or any CIS Party in connection with any claim arising out of any violation by us of the preceding paragraph, including without limitation CIS's right, at our expense, to assume the exclusive defense and control of any matter subject to this indemnification, and in such case, we agree to cooperate with CIS in its defense of such claim. We further agree that all CIS Parties are third-party beneficiaries of our undertakings in these Agreed Terms of Use.

Special rules.

CIS has created and will from time to time create special rules for its members and for other persons and organizations with which CIS has a written contractual relationship. Those special rules will override and supersede these Agreed Terms of Use with respect to the users who are covered by the special rules. CIS hereby grants each CIS Security Consulting or Software Vendor Member and each CIS Organizational User Member, but only so long as such Member remains in good standing with CIS and complies with all of the terms of these Agreed Terms of Use, the right to distribute the Products and Recommendations within such Member's own organization, whether by manual or electronic means. Each such Member acknowledges and agrees that the foregoing grant is subject to the terms of such Member's membership arrangement with CIS and may, therefore, be modified or terminated by CIS at any time.

Choice of law; jurisdiction; venue.

We acknowledge and agree that these Agreed Terms of Use will be governed by and construed in accordance with the laws of the State of Maryland, that any action at law or in equity arising out of or relating to these Agreed Terms of Use shall be filed only in the courts located in the State of Maryland, that we hereby consent and submit to the personal jurisdiction of such courts for the purposes of litigating any such action. If any of these Agreed Terms of Use shall be determined to be unlawful, void, or for any reason unenforceable, then such terms shall be deemed severable and shall not affect the validity and enforceability of any remaining provisions. We acknowledge and agree that we have read these Agreed Terms of Use in their entirety, understand them and agree to be bound by them in all respects.

Table of Contents

Terms of Use Agreement.....	2
Overview	6
Consensus Guidance.....	6
Intended Audience	6
Acknowledgements.....	7
Typographic Conventions.....	8
Configuration Levels	8
Level-I Benchmark settings/actions.....	8
Level-II Benchmark settings/actions	8
Scoring Status	8
Scorable	8
Not Scorable	8
Recommendations.....	9
Loss of Physical Custody of an iPhone and Compensating Controls.....	9
1. Settings on the iPhone.....	10
1.1 System Settings.....	10
1.1.1 Update firmware to latest version (Level 1, Not Scorable).....	10
1.1.2 Turn on Airplane Mode (Level 2, Not Scorable).....	10
1.1.3 Turn off Wi-Fi when not needed (Level 2, Not Scorable)	11
1.1.4 Forget networks to prevent automatic rejoin (Level 2, Not Scorable)	12
1.1.5 Turn off Ask to Join Networks (Level 2, Not Scorable)	12
1.1.6 Turn off Auto-Join for all Wi-Fi networks (Level 2, Not Scorable).....	13
1.1.7 Turn off VPN when not needed (Level 1, Not Scorable).....	14
1.1.8 Turn off Bluetooth when not needed (Level 1, Not Scorable).....	14
1.1.9 Turn off Location Services (Level 2, Not Scorable).....	15
1.1.10 Require Passcode on Device (Level 1, Not Scorable)	16
1.1.11 Configure an alphanumeric value (Level 2, Not Scorable)	16
1.1.12 Set auto-lock timeout (Level 1, Not Scorable)	17
1.1.13 Disable show SMS preview when iPhone is locked (Level 2, Not Scorable).....	18
1.1.14 Erase data upon excessive passcode failures (Level 1, Not Scorable)	18
1.1.15 Erase all data before return, repair, or recycle (Level 1, Not Scorable).....	19
1.2 Safari Settings.....	20
1.2.1 Disable JavaScript (Level 2, Not Scorable).....	20
1.2.2 Enable Fraud Warning (Level 1, Not Scorable)	20
1.2.3 Disable AutoFill (Level 2, Not Scorable).....	21
2. iPhone Settings in the iPCU.....	22
2.1 System Settings.....	22
2.1.1 Disallow profile removal (Level 1, Scorable).....	22
2.2 Passcode Settings	23
2.2.1 Require passcode on device (Level 1, Scorable)	23
2.2.2 Require alphanumeric value (Level 2, Scorable).....	23
2.2.3 Set minimum passcode length (Level 1, Scorable).....	24
2.2.4 Set a minimum number of complex characters (Level 2, Scorable)	24
2.2.5 Set auto-lock timeout (Level 1, Scorable).....	25

2.2.6	Erase data upon excessive passcode failures (Level 1, Scorable).....	26
3.	iPhone Settings in MS Exchange ActiveSync Policy.....	27
3.1	Passcode Settings	28
3.1.1	Require passcode on device (Level 1, Scorable)	28
3.1.2	Require alphanumeric value (Level 2, Scorable)	29
3.1.3	Set minimum passcode length (Level 1, Scorable).....	30
3.1.4	Set a minimum number of complex characters (Level 2, Scorable)	32
3.1.5	Set auto-lock timeout (Level 1, Scorable).....	33
3.1.6	Erase data upon excessive passcode failures (Level 1, Scorable).....	34
Appendix A:	References.....	37
Appendix B:	Change History.....	38
Appendix C:	Additional Security Notes	39
C.1	Set maximum passcode age (Informational).....	39
C.2	Set passcode history (Informational)	40
Appendix D:	Additional Information for Exchange ActiveSync Management.....	41
D.1	General ActiveSync Settings	42
D.1.1	Disallow non-provisionable devices (Level 1, Scorable)	42
D.2	General Resources for iOS Mobile Device ActiveSync Management.....	43

Overview

This document, *Security Configuration Benchmark for Apple iOS 4.1.0*, provides prescriptive guidance for establishing a secure configuration posture for the Apple iOS version 4.1.0. This guide was tested against the Apple iOS 4.1.0 and the iPhone Configuration Utility (iPCU) v3.1.0.256. To obtain the latest version of this guide, please visit <http://cisecurity.org>. If you have questions, comments, or have identified ways to improve this guide, please write us at feedback@cisecurity.org.

Consensus Guidance

This guide was created using a consensus review process comprised of volunteer and contract subject matter experts. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

Each CIS benchmark undergoes two phases of consensus review. The first phase occurs during initial benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the benchmark. This discussion occurs until consensus has been reached on benchmark recommendations. The second phase begins after the benchmark has been released to the public Internet. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in the CIS benchmark. If you are interested in participating in the consensus review process, please send us a note to feedback@cisecurity.org.

Intended Audience

This document is intended for system and application administrators, security specialists, auditors, help desk, end users, and platform deployment personnel who plan to use, develop, deploy, assess, or secure solutions that incorporate the Apple iOS 4.1.0.

Acknowledgements

This benchmark exemplifies the great things a community of users, vendors, and subject matter experts can accomplish through consensus collaboration. The CIS community thanks the entire consensus team with special recognition to the following individuals who contributed greatly to the creation of this guide:

Author

David Kane-Parry, Leviathan Security Group (v1.0.0)

Maintainers

Mike de Libero, MDE Development

David Skrdla, University of Oklahoma

Contributors and Reviewers

Blake Frantz, Center for Internet Security

Shawn Geddis, Apple Inc., Enterprise Division

Rebecca Heffel, University of Washington

Richard Haas, NASA Emerging Technology and Desktop Standards (ETADS)

Toon Mordijck, Atos Worldline

Adrian Sanábria

Joe Wulf, ProSync Technologies

Typographic Conventions

The following typographical conventions are used throughout this guide:

Convention	Meaning
<code>Stylized Monospace font</code>	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
Monospace font	Used for inline code, commands, or examples. Text should be interpreted exactly as presented.
<i><italic font in brackets></i>	Italic texts set in angle brackets denote a variable requiring substitution for a real value.
<i>Italic font</i>	Used to denote the title of a book, article, or other publication.
Note	Additional information or caveats

Configuration Levels

This section defines the configuration levels that are associated with each benchmark recommendation. Configuration levels represent increasing levels of security assurance.

Level-I Benchmark settings/actions

Level-I Benchmark recommendations are intended to:

- be practical and prudent;
- provide a clear security benefit; and
- not negatively inhibit the utility of the technology beyond acceptable means

Level-II Benchmark settings/actions

Level-II Benchmark recommendations exhibit one or more of the following characteristics:

- intended for environments or use cases where security is paramount
- act as defense in depth measure
- may negatively inhibit the utility or performance of the technology

Scoring Status

This section defines the scoring statuses used within this document. The scoring status indicates whether compliance with the given recommendation is discernable in an automated manner.

Scorable

The platform's compliance with the given recommendation can be determined via automated means.

Not Scorable

The platform's compliance with the given recommendation cannot be determined via automated means.

Recommendations

The settings recommended in this benchmark are those available through configuration of the device either directly through its local interface, through manufacturer-provided external configuration tools, and through configuration capabilities provided by Exchange ActiveSync mailbox policies. In considering the recommendations made in this benchmark, the device was considered both as a target itself and as a method of accessing other resources. These benchmark settings provide certain protections from remote attacks against the device and from unauthorized device access in the event the device is lost.

In determining the recommendations provided in this benchmark, the team considered the built-in encryption feature provided with the iPhone 3GS and iPhone 4 and has determined that this encryption feature does not obviate any of the recommendations made in the guide. The recommendations do not assert sufficient protections against advanced local attacks to gain device access or data recovery which may be possible in the event a device is lost.

Loss of Physical Custody of an iPhone and Compensating Controls

The combined *Set a passcode*, *Set auto-lock timeout*, and *Erase data upon excessive passcode failures* recommendations in the Level I and Level II Benchmark profiles provide a basic level of protection against unauthorized device and data access in the event of a lost device.

Certain non-configuration controls are available through 3rd-party and subscription-based tools and should be considered.

- A remote wipe feature can be activated as a compensating corrective control for iPhone devices, available through four mechanisms:
 - Exchange ActiveSync Mobile Administration Web Tool (MS Exchange Server 2003 and MS Exchange Server 2007)
 - Exchange Management Console (MS Exchange Server 2007)
 - Outlook Web Access (MS Exchange Server 2007)
 - Apple MobileMe Subscription Service
- In addition to supporting *Remote Wipe*, the MobileMe subscription service also supports a *Find My iPhone* feature (to locate an iPhone on a map), a *Set a passcode* feature (to remotely set a passcode on and lock an iPhone), and the option to display a message or play a sound on a lost iPhone.
- Third-party encryption apps are available to protect the confidentiality of data for advanced applications and should be considered where advanced protections are required.

Organizational policies and education/awareness programs to ensure device owners know to notify the appropriate channels in a timely manner for incident response, including the activation of remote wipe and related actions, are important to effectively realize the benefits the remote action features can provide.

1. Settings on the iPhone

This section provides guidance on the secure configuration of the iPhone.

1.1 System Settings

This section provides guidance on the secure configuration of system settings.

1.1.1 Update firmware to latest version (Level 1, Not Scorable)

Description:

iPhones ship with whichever version of the firmware was current when it was manufactured, but updates may have been released since then. It is recommended that the iPhone firmware remain current.

Rationale:

Firmware updates include not only new features and bug fixes but security fixes as well. Also, the iPhone must be running firmware version 4.1.0 for these benchmark recommendations to apply; if a newer version of the firmware is available, some recommendations may not apply.

Remediation:

1. Connect the iPhone to the computer.
2. Open iTunes.
3. Click on the iPhone under “Devices” in the source list.
4. Click on “Check for Update”.
5. Click “Download and Install”.
6. Do not disconnect the iPhone until the update is finished.

Audit:

1. Tap Settings.
2. Tap General.
3. Tap About.
4. Confirm that “Version” is 4.1.0.

Reference:

1. iPhone User Guide - For iOS 4 Software
http://manuals.info.apple.com/en_US/iPhone_iOS4_User_Guide.pdf

1.1.2 Turn on Airplane Mode (Level 2, Not Scorable)

Description:

The iPhone can be configured to disable all receivers and transceivers. This option is called Airplane Mode. When Airplane Mode is on, no phone, GPS, radio, Wi-Fi, or Bluetooth signals are emitted from or received by the iPhone. It is recommended that Airplane Mode be enabled when these capabilities are unneeded or where security is paramount.

Rationale:

If the user enters an environment where no signal transmission or reception is intended, Airplane Mode can be turned on to ensure that the iPhone does not initiate or respond to any signals. This reduces the remote attack surface of the device.

Remediation:

1. Tap Settings.
2. Turn on Airplane Mode.

Audit:

1. Tap Settings.
2. Confirm that Airplane Mode is on.

Reference:

1. iPhone User Guide - For iOS 4 Software
http://manuals.info.apple.com/en_US/iPhone_iOS4_User_Guide.pdf

1.1.3 Turn off Wi-Fi when not needed (Level 2, Not Scorable)

Description:

The iPhone can be configured to participate in Wi-Fi networks. It is recommended that Wi-Fi be disabled when not needed or where security is paramount.

If Wi-Fi is turned off, then the iPhone connects to the Internet via the cellular data network, when available. The iPhone can run Mail, Safari, YouTube, Stocks, Maps, Weather, and the App Store over a cellular data network connection, but there may be a limit on the maximum download size of an item from the iTunes Music Store depending on carrier.

Rationale:

Disabling the Wi-Fi interface will reduce the remote attack surface of the device. Additionally, at present, the cellular data network is a more difficult medium to sniff than Wi-Fi.

Remediation:

1. Tap Settings.
2. Tap Wi-Fi.
3. Turn off Wi-Fi.

Audit:

1. Tap Settings.
2. Tap Wi-Fi.
3. Confirm that Wi-Fi is turned off.

Reference:

1. iPhone User Guide - For iOS 4 Software
http://manuals.info.apple.com/en_US/iPhone_iOS4_User_Guide.pdf

1.1.4 Forget networks to prevent automatic rejoin (Level 2, Not Scorable)

Description:

The iPhone can be configured to forget Wi-Fi networks that it has previously associated with. By default, the iPhone will remember and automatically join networks that it has previously associated with. It is recommended that networks be forgotten after use in use cases where security is paramount.

Rationale:

A trusted but unauthenticated Wi-Fi network may be spoofed and automatically joined if it is not forgotten after last use. Additionally, if such a network has a common SSID, such as “default” or “linksys”, it is probable that the iPhone will encounter an untrusted instance of a same-named Wi-Fi network and automatically join it.

Remediation:

1. Tap Settings.
2. Tap Wi-Fi.
3. Tap the Wi-Fi network to forget.
4. Tap “Forget this network.”

Note: the Wi-Fi network must be in range for it to appear in the list of available networks to forget; if the Wi-Fi network is no longer in range, the user will not be able to selectively forget it, but instead must reset all network settings to forget all Wi-Fi networks.

Audit:

1. Tap Settings.
2. Tap General.
3. Tap Reset.
4. Tap Reset Network Settings.
5. Tap Reset Network Settings again.

Reference:

1. iPhone User Guide - For iOS 4 Software
http://manuals.info.apple.com/en_US/iPhone_iOS4_User_Guide.pdf

1.1.5 Turn off Ask to Join Networks (Level 2, Not Scorable)

Description:

When the user is trying to access the Internet, by using Safari or Mail for example, and the user is not in range of a Wi-Fi network the user has previously used, this option tells the iPhone to look for another network. The iPhone displays a list of all available Wi-Fi networks that the user can choose from. If “Ask to Join Networks” is turned off, the user must manually search for a network to connect to the Internet when a previously used network or a cellular data network is not available. It is recommended that this capability be disabled in environments where security is paramount.

Rationale:

Requiring the user to manually configure and join a Wi-Fi network reduces the risk of inadvertently joining a similarly named yet untrusted network (i.e. “default” vice “default”).

Remediation:

1. Tap Settings.
2. Tap Wi-Fi.
3. Turn off “Ask to Join Networks”.

Audit:

1. Tap Settings.
2. Tap Wi-Fi.
3. Confirm that “Ask to Join Networks” is turned off.

Reference:

1. iPhone User Guide - For iOS 4 Software
http://manuals.info.apple.com/en_US/iPhone_iOS4_User_Guide.pdf

1.1.6 Turn off Auto-Join for all Wi-Fi networks (Level 2, Not Scorable)

Description:

When Wi-Fi Auto-Join is turned on for a Wi-Fi network, the device remembers the network and login information and automatically reconnects to that Wi-Fi network whenever the device is in range. Some subscription Wi-Fi networks may not support Auto-Join and require a manual log in each time.

Rationale:

There are some potential risks in using this feature. For Wi-Fi networks that require HTTP(S) forms authentication, this feature will cause the iPhone to persist credentials on disk. If physical custody of the iPhone is lost, the confidentiality of the persisted credentials—and the resources protected by them—may be at risk if the attacker retrieves the iPhone’s contents prior to a remote wipe being successfully executed. Additionally, if the given forms-based authentication occurs over unencrypted HTTP, the confidentiality of the credentials is at risk while in transit. While this is also true in the absence of the Auto-Join feature, enabling the feature may expose credentials at unexpected times and locations.

Remediation:

1. Tap Settings.
2. Tap Wi-Fi.
3. From the Choose a Network list, locate the network SSID and tap the chevron next to the network to change.
4. Turn off Auto-Join.
5. Repeat steps 3 and 4 for each network SSID.

Audit:

1. Tap Settings.
2. Tap Wi-Fi.

3. From the Choose a Network list, locate the network SSID and tap the chevron next to the network to change.
4. Confirm that Auto-Join is turned off.
5. Repeat steps 3 and 4 for each network SSID.

References:

1. iPhone User Guide - For iOS 4 Software
http://manuals.info.apple.com/en_US/iPhone_iOS4_User_Guide.pdf
2. iPhone and iPod touch: Understanding subscription Wi-Fi networks
<http://support.apple.com/kb/HT3867>

1.1.7 Turn off VPN when not needed (Level 1, Not Scorable)

Description:

The iPhone can connect to VPNs that use the L2TP, PPTP, or Cisco IPSec protocols. VPN connections can be established over both Wi-Fi and cellular data network connections. It is recommended that VPN connections be disabled when not in use.

Rationale:

If the user has a VPN connection configured, it should only be turned on when VPN access is required. If the VPN is left on, the user may not be mindful of the nature of the information they are transmitting on the network. Additionally, malicious or exploited iPhone applications may access VPN resources.

Remediation:

1. Tap Settings.
2. Tap General.
3. Tap Network.
4. Tap VPN.
5. Turn off VPN.

Audit:

1. Tap Settings.
2. Tap General.
3. Tap Network.
4. Tap VPN.
5. Confirm that VPN is turned off.

Reference:

1. iPhone User Guide - For iOS 4 Software
http://manuals.info.apple.com/en_US/iPhone_iOS4_User_Guide.pdf

1.1.8 Turn off Bluetooth when not needed (Level 1, Not Scorable)

Description:

The iPhone can connect wirelessly to Bluetooth headsets and car kits for hands-free talking. It is recommended that Bluetooth be disabled when not in use.

Rationale:

If the user does not need Bluetooth enabled for hands-free talking, it should be disabled to prevent discovery of and connection to supported Bluetooth services.

Remediation:

1. Tap Settings.
2. Tap General.
3. Tap Bluetooth
4. Turn off Bluetooth.

Audit:

1. Tap Settings.
2. Tap General.
3. Tap Bluetooth.
4. Confirm that Bluetooth is turned off.

Reference:

1. iPhone User Guide - For iOS 4 Software
[http://manuals.info.apple.com/en_US/iPhone iOS4 User Guide.pdf](http://manuals.info.apple.com/en_US/iPhone_iOS4_User_Guide.pdf)

1.1.9 Turn off Location Services (Level 2, Not Scorable)

Description:

Location Services allows applications such as Maps and Camera to gather and use data indicating the user's location. The user's approximate location is determined using available information from cellular network data, local Wi-Fi networks (if the user has Wi-Fi turned on), and GPS if the user has an iPhone 3G or later. If the user turns off Location Services, the user will be prompted to turn it back on again the next time an application tries to use this feature. It is recommended that location services be disabled in environments where security is paramount.

Rationale:

The iOS enables the user to grant or deny individual applications access to location services. If the user does not intend to use location services at all, turning it off ensures that a previously allowed application will no longer be able to use location services by default.

Remediation:

1. Tap Settings.
2. Tap General.
3. Turn off Location Services.

Audit:

1. Tap Settings.
2. Tap General.
3. Confirm that Location Services is turned off.

Reference:

1. iPhone User Guide - For iOS 4 Software
http://manuals.info.apple.com/en_US/iPhone_iOS4_User_Guide.pdf

1.1.10 Require Passcode on Device (Level 1, Not Scorable)

Description:

The iPhone can be configured to require a passcode before allowing usage via the touch screen. By default, the iPhone does not require a passcode to unlock it. It is recommended that a passcode be set.

Rationale:

In the event of a physical security incident, a passcode will not guarantee data integrity, but it will raise the bar of effort required to compromise the device.

Remediation:

1. Tap Settings.
2. Tap General.
3. Tap Passcode Lock.
4. Tap in a four-digit passcode.
5. Tap in the same four-digit passcode.

Note: The passcode can also be set via the iPhone Configuration Utility (iPCU) as described in section [iPhone Settings in iPCU](#).

Audit:

1. Tap Settings.
2. Tap General.
3. Confirm that Passcode Lock is turned on.

Reference:

1. iPhone User Guide - For iOS 4 Software
http://manuals.info.apple.com/en_US/iPhone_iOS4_User_Guide.pdf

1.1.11 Configure an alphanumeric value (Level 2, Not Scorable)

Description:

The iPhone can be configured to allow a passcode comprised of numeric, alphabetic, and non-alphanumeric values. By default, the iPhone does not permit a complex passcode. It is recommended that numeric, alphabetic, and non-alphanumeric values comprise the passcode. Note that this configuration setting does not require that the password entered contain a letter, number, or symbol, it just allows that such characters from the alphanumeric keyboard be input in the passcode dialog.

Rationale:

Using a mix of alphabetical, numerical, and non-alphanumeric characters increases the complexity of the passcode an attacker may attempt to brute-force in order to gain access to the device.

Remediation:

1. Tap Settings.
2. Tap General.
3. Tap Passcode Lock
4. Turn off Simple Passcode.
5. Enter previous password when prompted.
6. Enter new complex passcode twice as prompted.

Note: Passcode complexity can also be set—and can be enforced—via the iPhone Configuration Utility (iPCU) as described in section [iPhone Settings in the iPCU](#).

Audit:

1. Tap Settings.
2. Tap General.
3. Tap Passcode Lock
4. Enter current passcode as prompted.
5. Confirm that Simple Passcode is turned off.

Reference:

1. iPhone User Guide - For iOS 4 Software
http://manuals.info.apple.com/en_US/iPhone_iOS4_User_Guide.pdf

1.1.12 Set auto-lock timeout (Level 1, Not Scorable)

Description:

The iPhone can be configured to auto-lock after a pre-defined inactivity period. By default, if a passcode is defined, the iPhone will automatically lock after one minute of inactivity. It is recommended that an inactivity timeout be set.

Rationale:

If the user has set an auto-lock interval of greater than five minutes, there is a greater risk that the iPhone will be in an unlocked state during a physical security breach.

Remediation:

1. Tap Settings.
2. Tap General.
3. Tap Auto-Lock.
- 4a. For typical use cases, tap “5 Minutes” or less.
- 4b. For high-security use cases, tap “1 Minute”.

Note: The auto-lock timeout can also be set via the iPhone Configuration Utility (iPCU) as described in section [iPhone Settings in the iPCU](#).

Audit:

1. Tap Settings.
2. Tap General.
- 3a. For typical use cases, confirm that the Auto-Lock is set to 5 minutes or less.
- 3b. For high-security use cases, confirm that the Auto-Lock is set to 1 minute.

Reference:

1. iPhone User Guide - For iOS 4 Software
http://manuals.info.apple.com/en_US/iPhone_iOS4_User_Guide.pdf

1.1.13 Disable show SMS preview when iPhone is locked (Level 2, Not Scorable)

Description:

If the iPhone is passcode locked and receiving SMS messages, the messages are still previewed on the display. It is recommended that SMS previews be disabled in environments where security is paramount.

Rationale:

Parties who do not know the passcode lock should not have read access to the iPhone's SMS traffic.

Remediation:

1. Tap Settings.
2. Tap Messages.
3. Turn off Show Preview.

Audit:

1. Tap Settings.
2. Tap Messages.
3. Confirm that Show Preview is turned off.

Reference:

1. iPhone User Guide - For iOS 4 Software
http://manuals.info.apple.com/en_US/iPhone_iOS4_User_Guide.pdf

1.1.14 Erase data upon excessive passcode failures (Level 1, Not Scorable)

Description:

The iPhone can be configured to erase the user's settings and data as stored on the device after excessive (10) passcode failures. It is recommended that this feature be enabled.

Rationale:

Excessive passcode failures typically indicate that the device is out of physical control of its owner. Upon such an event, erasing data on the phone will ensure the confidentiality of information stored on the device is protected when facing a novice attacker.

Remediation:

1. Tap Settings.
2. Tap General.
3. Tap Passcode Lock.
4. Turn on Erase Data.

Note: The “Erase data upon excessive password failures” setting can also be set via the iPhone Configuration Utility (iPCU) as described in section [iPhone Settings in the iPCU](#).

Audit:

1. Tap Settings.
2. Tap General.
3. Tap Passcode Lock.
4. Confirm that Erase Data is turned on.

Reference:

1. iPhone User Guide - For iOS 4 Software
http://manuals.info.apple.com/en_US/iPhone_iOS4_User_Guide.pdf

1.1.15 Erase all data before return, repair, or recycle (Level 1, Not Scorable)

Description:

In normal operations, the iPhone does not use a secure delete function to erase data from the disk, allowing it to persist in a recoverable state. Therefore, the disk should be overwritten via the “Erase All Content and Settings” setting before the iPhone is out of the user’s control.

Rationale:

Overwriting the iPhone’s disk before it is out of the user’s control will reduce an attacker’s ability to recover sensitive information from the device.

Remediation:

1. Tap Settings.
2. Tap General.
3. Tap Reset.
4. Tap Erase All Contents and Settings.

Audit:

To verify that the iPhone disk has been overwritten, it is necessary to install a warranty-voiding forensics recovery toolkit that is not within the scope of this document. Please review the references for more information.

References:

1. iPhone User Guide - For iOS 4 Software
http://manuals.info.apple.com/en_US/iPhone_iOS4_User_Guide.pdf
2. iPhone Forensics
<http://oreilly.com/catalog/9780596153588/>

1.2 Safari Settings

This section provides guidance on the secure configuration of settings related to the Safari application on the iPhone.

1.2.1 Disable JavaScript (Level 2, Not Scorable)

Description:

JavaScript lets web programmers control elements of the page—for example, a page that uses JavaScript might display the current date and time or cause a linked page to appear in a new pop-up page. It is recommended that JavaScript be disabled in environments where security is paramount.

Rationale:

JavaScript should only be enabled before browsing trusted sites.

Remediation:

1. Tap Settings.
2. Tap Safari.
3. Turn off JavaScript.

Audit:

1. Tap Settings.
2. Tap Safari.
3. Confirm that JavaScript is turned off.

Reference:

1. iPhone User Guide - For iOS 4 Software
http://manuals.info.apple.com/en_US/iPhone_iOS4_User_Guide.pdf

1.2.2 Enable Fraud Warning (Level 1, Not Scorable)

Description:

Fraud warning protects you from potentially fraudulent Internet sites. When you visit a suspicious site, Safari warns you about its suspect nature and doesn't load the page. It is recommended that the Fraud Warning feature be enabled.

Rationale:

Enabling a warning can help you avoid accidentally visiting some known phishing and other fraudulent sites covered by this feature.

Remediation:

1. Tap Settings.
2. Tap Safari.
3. Turn on Fraud Warning.

Audit:

1. Tap Settings.
2. Tap Safari.

3. Confirm that Fraud Warning is turned on.

Reference:

1. iPhone User Guide - For iOS 4 Software
http://manuals.info.apple.com/en_US/iPhone_iOS4_User_Guide.pdf

1.2.3 Disable AutoFill (Level 2, Not Scorable)

Description:

iPhone has a feature to remember information entered into common forms in order to automate the completion of forms in the browser. Information auto-filled can include information from Contacts as well as remembered names and passwords. By default, this feature is disabled.

- If Use Contact Info is turned on and contact information selected, Safari will use the selected information from Contacts to fill in contact fields on web forms.
- If Names & Passwords is turned on, Safari will remember names and passwords to websites visited and automatically fill in the information when you revisit the website.

It is recommended that the AutoFill be disabled.

Rationale:

Disabling AutoFill can help avoid the storage of credentials locally on the device, as well as reduces the likelihood of automated unauthorized access to a site in the event unauthorized access is gained to the device.

Remediation:

1. Tap Settings.
2. Tap Safari.
3. Turn off AutoFill.

Audit:

1. Tap Settings.
2. Tap Safari.
3. Confirm that AutoFill is turned off.

Reference:

1. iPhone User Guide - For iOS 4 Software
http://manuals.info.apple.com/en_US/iPhone_iOS4_User_Guide.pdf

2. iPhone Settings in the iPCU

This section provides guidance on the secure configuration of the iPhone with the iPhone Configuration Utility (iPCU), version 3.1.0.256. The iPhone Configuration Utility is a download available from Apple at <http://www.apple.com/support/iphone/enterprise> that lets users create, maintain, and sign configuration profiles, track and install provisioning profiles and authorized applications, and capture device information including console logs.

2.1 System Settings

This section provides guidance on the secure configuration of system settings.

2.1.1 Disallow profile removal (Level 1, Scorable)

Description:

The iPhone can be configured to always allow the removal of a profile, to allow the removal of a profile only with a profile-specific password, or to never allow the removal of a profile, on a per-profile basis. By default, the iPCU configuration allows the profile to be removed by the user. To ensure profile settings remain in effect, profile removal must be disallowed.

Rationale:

Restricting the removal of a configuration profile is necessary to enforce the settings contained within the respective profile. If a user can circumvent profile requirements simply by uninstalling the profile, the continued enforcement of profile controls cannot be assured and intended device security is highly reduced.

Remediation:

1. Open iPCU.
2. Click on “Configuration Profiles” in the left windowpane.
3. Click on the “General” tab in the lower right windowpane.
4. Click on the “Security” combo box in the lower right window pane.
5. Select “With Authentication”.
6. Install the configuration profile on the device.

Audit:

1. Open the configuration profile XML file.
2. Search for `<key>PayloadRemovalDisallowed</key>`.
3. Observe if the next line is `<true/>`.
4. Search for `<key>RemovalPassword</key>`.
5. Observe whether this value is present and whether a value is set.

Reference:

1. iOS Enterprise Deployment Guide - Second Edition, for Version 3.2 or later
http://manuals.info.apple.com/en_US/Enterprise_Deployment_Guide.pdf

2.2 Passcode Settings

This section provides guidance on the secure configuration of passcode settings.

2.2.1 *Require passcode on device (Level 1, Scorable)*

Description:

The iPhone can be configured to require a passcode before allowing access through the touchpad. By default, the iPhone does not require a passcode to unlock the device after a period of inactivity. It is recommended that a passcode be set.

Rationale:

Requiring a passcode to unlock the device increases the effort required to compromise the features and data of the iPhone in the event of a physical security breach.

Remediation:

1. Open iPCU.
2. Click on “Configuration Profiles” in the left windowpane.
3. Click on the “Passcode” tab in the lower right windowpane.
4. Click on the “Require passcode on device” checkbox in the lower right windowpane.
5. Install the configuration profile on the device.

Note: The passcode requirement can also be set via the iPhone UI as described in section [Settings on the iPhone](#).

Audit:

1. Open the configuration profile XML file.
2. Search for `<key>forcePIN</key>`.
3. Observe if the next line is `<true/>`.

Reference:

1. iOS Enterprise Deployment Guide - Second Edition, for Version 3.2 or later
http://manuals.info.apple.com/en_US/Enterprise_Deployment_Guide.pdf

2.2.2 *Require alphanumeric value (Level 2, Scorable)*

Description:

The iPhone can be configured to require that the passcode be comprised of both numeric and alphabetic values. By default, the iPhone does not enforce a passcode complexity policy. It is recommended that both numeric and alphabetic values comprise the passcode.

Rationale:

Requiring a mix of alphabetical and numerical characters increases the complexity of the passcode an attacker may attempt to brute-force in order to gain access to the device.

Remediation:

1. Open iPCU.
2. Click on “Configuration Profiles” in the left windowpane.
3. Click on the “Passcode” tab in the lower right windowpane.

4. Click on the “Require alphanumeric value” checkbox in the lower right windowpane.
5. Install the configuration profile on the device.

Audit:

1. Open the configuration profile XML file.
2. Search for `<key>requireAlphanumeric</key>`.
3. Observe if the next line is `<true/>`.

Reference:

1. iOS Enterprise Deployment Guide - Second Edition, for Version 3.2 or later
http://manuals.info.apple.com/en_US/Enterprise_Deployment_Guide.pdf

2.2.3 Set minimum passcode length (Level 1, Scorable)

Description:

The iPhone can be configured to require that the passcode be at least a pre-determined length. By default, the minimum passcode length is only four characters. It is recommended that passcode length be at least five (5) characters.

Rationale:

Requiring at least five characters increases the complexity of the passcode an attacker may attempt to brute-force in order to gain access to the device. Additionally, requiring at least five characters prevents a user from selecting typically weak values, such as a year, date, or last four digits of a phone number, for their passcode.

Remediation:

1. Open iPCU.
2. Click on “Configuration Profiles” in the left windowpane.
3. Click on the “Passcode” tab in the lower right windowpane.
4. Click on the “Minimum passcode length” textbox in the lower right windowpane.
5. Enter the number “5”.
6. Install the configuration profile on the device.

Audit:

1. Open the configuration profile XML file.
2. Search for `<key>minLength</key>`.
3. Observe if the next line is `<real>5</real>`.

Reference:

1. iOS Enterprise Deployment Guide - Second Edition, for Version 3.2 or later
http://manuals.info.apple.com/en_US/Enterprise_Deployment_Guide.pdf

2.2.4 Set a minimum number of complex characters (Level 2, Scorable)

Description:

The iPhone can be configured to require non-alphanumeric characters in the passcode. By default, the iPhone does not require complex characters in the passcode. It is recommended that a non-alphanumeric character be used in the passcode.

Rationale:

Requiring at least one complex character increases the complexity of the passcode an attacker may attempt to brute-force in order to gain access to the device.

Remediation:

1. Open iPCU.
2. Click on “Configuration Profiles” in the left windowpane.
3. Click on the “Passcode” tab in the lower right windowpane.
4. Click on the “Minimum number of complex characters” textbox in the lower right windowpane.
5. Enter the number “1”.
6. Install the configuration profile on the device.

Note: Passcode complexity can also be configured—but not enforced—via the iPhone UI as described in section [Settings on the iPhone](#).

Audit:

1. Open the configuration profile XML file.
2. Search for `<key>minComplexChars</key>`.
3. Observe if the next line is `<real>1</real>`.

References:

1. iOS Enterprise Deployment Guide - Second Edition, for Version 3.2 or later
http://manuals.info.apple.com/en_US/Enterprise_Deployment_Guide.pdf
2. NIST Electronic Authentication Guideline –
http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

2.2.5 Set auto-lock timeout (Level 1, Scorable)

Description:

The iPhone can be configured to auto-lock after a pre-defined inactivity period. By default, if a passcode is defined, the iPhone will automatically lock after one minute of inactivity. It is recommended that an inactivity timeout be set.

Rationale:

Preventing the user from setting a long inactivity period reduces the risk that the iPhone will be unlocked in the event of a physical security breach.

Remediation:

1. Open iPCU.
2. Click on “Configuration Profiles” in the left windowpane.
3. Click on the “Passcode” tab in the lower right windowpane.
4. Click on the “Auto-lock (in minutes)” drop-down menu in the lower right windowpane.
5. Select the number “5”.
6. Install the configuration profile on the device.

Note: The auto-lock timeout can also be set via the iPhone UI as described in section [Settings on the iPhone](#).

Audit:

1. Open the configuration profile XML file.
2. Search for `<key>maxInactivity</key>`.
3. Observe if the next line is `<real>5</real>`.

Reference:

1. iOS Enterprise Deployment Guide - Second Edition, for Version 3.2 or later http://manuals.info.apple.com/en_US/Enterprise_Deployment_Guide.pdf

2.2.6 Erase data upon excessive passcode failures (Level 1, Scorable)

Description:

The iPhone can be configured to erase the user's settings and data as stored on the device after excessive (configurable from 4 to 16) passcode failures. It is recommended that this feature be enabled.

Rationale:

Excessive password failures typically indicate that the device is out of physical control of its owner. Upon such an event, erasing data on the phone will ensure the confidentiality of information stored on the device is protected when facing a novice attacker.

Remediation:

1. Open iPCU.
2. Click on "Configuration Profiles" in the left windowpane.
3. Click on the "Passcode" tab in the lower right windowpane.
4. Click on the "Maximum number of failed attempts" combo box in the lower right windowpane.
5. Select the number "6".
6. Install the configuration profile on the device.

Note: The password failure limit can also be set via the iPhone UI as described in section [Settings on the iPhone](#).

Audit:

1. Open the configuration profile XML file.
2. Search for `<key>maxFailedAttempts</key>`.
3. Observe if the next line is `<integer>6</integer>`.

Reference:

1. iOS Enterprise Deployment Guide - Second Edition, for Version 3.2 or later http://manuals.info.apple.com/en_US/Enterprise_Deployment_Guide.pdf

3. iPhone Settings in MS Exchange ActiveSync Policy

This section provides guidance on the configuration of certain policies on the iPhone using Microsoft Exchange ActiveSync versions 2.5 and later. This guidance was developed and tested specifically with Exchange ActiveSync version 3.5 with the Client Access server role on Microsoft Exchange Server 2010.

All remediation and audit steps specified in this section apply to settings within an Exchange ActiveSync Mailbox policy, which are configured in the properties of the policy, accessed either via the Exchange Management Console (EMC) or the Exchange Management Shell.

To access the policy properties using the Exchange Management Console, follow the below steps:

1. Open the Exchange Management Console.
2. In the console tree, click on "Exchange ActiveSync" and then "Client Access" to open the Client Configuration work area.
3. Click on the "Exchange ActiveSync Mailbox Policies" tab.
4. Select the mailbox policy to modify.
5. Click on "Properties."

The remediation steps and the audit steps specified in this manual for the EMC apply to the "Properties" configuration window available once the above steps are completed.

For more information on using the Exchange Management Console (EMC) and the Exchange Management Shell, please refer to the additional information and resources provided in Appendix D.

3.1 Passcode Settings

This section provides guidance on the secure configuration of passcode settings.

3.1.1 Require passcode on device (Level 1, Scorable)

Description:

The iPhone can be configured to require a passcode before allowing access through the touchpad. By default, the iPhone does not require a passcode to unlock the device after a period of inactivity, and the default Exchange ActiveSync policy setting applied for users not assigned to a mailbox policy does not require a passcode. It is recommended that a passcode be set.

Rationale:

Requiring a passcode to unlock the device increases the effort required to compromise the features and data of the iPhone in the event of a physical security breach.

Remediation:

Using the Exchange Management Console (EMC):

In the "Properties" configuration window,

1. Click on the "Password" tab.
2. Click on the "Require passcode" checkbox
3. Click "OK".

Using the Exchange Management Shell:

At the Exchange Management Shell command prompt,

1. Enter the following command (all one line):

```
Set-ActiveSyncMailboxPolicy -Identity "<PolicyName>"  
-DevicePasswordEnabled: $true
```

where <PolicyName> is the name of the Exchange ActiveSync mailbox policy for which the configuration should be made (replace brackets and text with appropriate policy name).

Audit:

Using the Exchange Management Console (EMC):

In the "Properties" configuration window,

1. Click on the "Password" tab.
2. Observe if the "Require passcode" checkbox is selected.
3. Click "Cancel".

Using the Exchange Management Shell:

At the Exchange Management Shell command prompt,

1. Enter the following command (all one line):

```
Get-ActiveSyncMailboxPolicy -Identity "<PolicyName>"
```

where *<PolicyName>* is the name of the Exchange ActiveSync mailbox policy for which the audit validation should be made (replace brackets and text with appropriate policy name).

2. Search the outputted policy setting list for the "DevicePasswordEnabled :" configuration item.
3. Observe if the value following the colon is "True" as shown below:
`DevicePasswordEnabled : True`
4. Exit the Exchange Management Shell.

Reference:

1. Microsoft Technet Library Article: Configure Device Password Locking
<http://technet.microsoft.com/en-us/library/bb125004.aspx>

3.1.2 Require alphanumeric value (Level 2, Scorable)

Description:

The iPhone can be configured to require that the passcode be comprised of both numeric and alphabetic values. By default, the iPhone does not enforce a passcode complexity policy, and the default Exchange ActiveSync policy setting applied for users not assigned to a mailbox policy does not require an alphanumeric passcode. It is recommended that both numeric and alphabetic values comprise the passcode.

Rationale:

Requiring a mix of alphabetical and numerical characters increases the complexity of the passcode an attacker may attempt to brute-force in order to gain access to the device.

Remediation:

Using the Exchange Management Console (EMC):

In the "Properties" configuration window,

1. Click on the "Password" tab.
2. Click on the "Require alphanumeric passcode" checkbox
3. Click "OK".

Using the Exchange Management Shell:

At the Exchange Management Shell command prompt,

1. Enter the following command (all one line):

```
Set-ActiveSyncMailboxPolicy -Identity "<PolicyName>"  
-AlphanumericDevicePasswordRequired : $true
```

where *<PolicyName>* is the name of the Exchange ActiveSync mailbox policy for which the configuration should be made (replace brackets and text with appropriate policy name).

Audit:

Using the Exchange Management Console (EMC):

In the “Properties” configuration window,

1. Click on the “Password” tab.
2. Observe if the “Require alphanumeric passcode” checkbox is selected.
3. Click “Cancel”.

Using the Exchange Management Shell:

At the Exchange Management Shell command prompt,

1. Enter the following command (all one line):

```
Get-ActiveSyncMailboxPolicy -Identity "<PolicyName>"
```

where <PolicyName> is the name of the Exchange ActiveSync mailbox policy for which the audit validation should be made (replace brackets and text with appropriate policy name).

2. Search the outputted policy setting list for the "AlphanumericDevicePasswordRequired :" configuration item.
3. Observe if the value following the colon is "True" as shown below:

```
AlphanumericDevicePasswordRequired : True
```
4. Exit the Exchange Management Shell.

Reference:

1. Microsoft Technet Library Article: Configure Device Password Locking
<http://technet.microsoft.com/en-us/library/bb125004.aspx>

3.1.3 Set minimum passcode length (Level 1, Scorable)

Description:

The iPhone can be configured to require that the passcode be at least a pre-determined length. By default, the minimum passcode length is only four characters, and this is the default Exchange ActiveSync policy value applied for users not assigned to a mailbox policy if minimum password length checking is enabled. It is recommended that password length be at least five (5) characters.

Rationale:

Requiring at least five characters increases the complexity of the passcode an attacker may attempt to brute-force in order to gain access to the device. Additionally, requiring at least five characters prevents a user from selecting typically weak values, such as a year, date, or last four digits of a phone number, for their passcode.

Remediation:

Using the Exchange Management Console (EMC):

In the “Properties” configuration window,

1. Click on the “Password” tab.
2. Click on the “Minimum password length” checkbox.
3. Enter the number 5 in the box on the right hand side.
4. Click “OK”.

Using the Exchange Management Shell:

At the Exchange Management Shell command prompt,

1. Enter the following command (all one line):

```
Set-ActiveSyncMailboxPolicy -Identity "<PolicyName>"  
-MinDevicePasswordLength 5
```

where *<PolicyName>* is the name of the Exchange ActiveSync mailbox policy for which the configuration should be made (replace brackets and text with appropriate policy name).

Audit:

Using the Exchange Management Console (EMC):

In the "Properties" configuration window,

1. Click on the "Password" tab.
2. Observe if the "Minimum password length" checkbox is selected.
3. Observe if the minimum password length value is set to 5.
4. Click "Cancel".

Using the Exchange Management Shell:

At the Exchange Management Shell command prompt,

1. Enter the following command (all one line):

```
Get-ActiveSyncMailboxPolicy -Identity "<PolicyName>"
```

where *<PolicyName>* is the name of the Exchange ActiveSync mailbox policy for which the audit validation should be made (replace brackets and text with appropriate policy name).

2. Search the outputted policy setting list for the "MinDevicePasswordLength :" configuration item.
3. Observe if there is a value following the colon and that the value is set to 5 as shown below:

```
MinDevicePasswordLength : 5
```

4. Exit the Exchange Management Shell.

Reference:

1. Microsoft Technet Library Article: Configure Device Password Locking
<http://technet.microsoft.com/en-us/library/bb125004.aspx>

3.1.4 Set a minimum number of complex characters (Level 2, Scorable)

Description:

The iPhone can be configured to require non-alphanumeric characters in the passcode. By default, the iPhone does not require complex characters in the passcode, and the default minimum value Exchange ActiveSync policy applies for users not assigned to a mailbox policy is zero (0). It is recommended that a non-alphanumeric character be used in the passcode.

Rationale:

Requiring at least one complex character increases the complexity of the passcode an attacker may attempt to brute-force in order to gain access to the device.

Remediation:

Using the Exchange Management Console (EMC):

In the "Properties" configuration window,

1. Click on the "Password" tab.
2. The "Require alphanumeric passcode" checkbox should be checked. When this checkbox is checked, you may enter the "Minimum number of complex characters" in the box on the right hand side.
3. Enter the number 1 in the box on the right hand side.
4. Click "OK".

Using the Exchange Management Shell:

At the Exchange Management Shell command prompt,

1. Enter the following command (all one line):

```
Set-ActiveSyncMailboxPolicy -Identity "<PolicyName>"  
-AlphanumericDevicePasswordRequired $true  
-MinDevicePasswordComplexCharacters 1
```

where <PolicyName> is the name of the Exchange ActiveSync mailbox policy for which the configuration should be made (replace brackets and text with appropriate policy name).

Audit:

Using the Exchange Management Console (EMC):

In the "Properties" configuration window,

1. Click on the "Password" tab.
2. Observe if the "Require alphanumeric passcode" checkbox is selected.
3. Observe if the "Minimum number of complex characters" value is set to 1.
4. Click "Cancel".

Using the Exchange Management Shell:

At the Exchange Management Shell command prompt,

1. Enter the following command (all one line):

```
Get-ActiveSyncMailboxPolicy -Identity "<PolicyName>"
```

where *<PolicyName>* is the name of the Exchange ActiveSync mailbox policy for which the audit validation should be made (replace brackets and text with appropriate policy name).

2. Search the outputted policy setting list for the "MinDevicePasswordComplexCharacters : " configuration item.
3. Observe if there is a value following the colon and that the value is set to 1 as shown below:

```
MinDevicePasswordComplexCharacters : 1
```

4. Search the outputted policy setting list for the "AlphanumericDevicePasswordRequired : " configuration item.
5. Observe if the value following the colon is "True" as shown below:

```
AlphanumericDevicePasswordRequired : True
```

6. Exit the Exchange Management Shell.

References:

1. Microsoft Technet Library Article: Configure Device Password Locking
<http://technet.microsoft.com/en-us/library/bb125004.aspx>
2. NIST SP800-63, Electronic Authentication Guideline – Version 1.0.2
http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

3.1.5 Set auto-lock timeout (Level 1, Scorable)

Description:

The iPhone can be configured to auto-lock after a pre-defined inactivity period. By default, if a passcode is defined, the iPhone will automatically lock after one minute of inactivity, and the default Exchange ActiveSync policy setting applied for users not assigned to a mailbox policy sets an inactivity lock at 15 minutes. It is recommended that an inactivity timeout of no more than five (5) minutes be set.

Rationale:

Preventing the user from setting a long inactivity period reduces the risk that the iPhone will be unlocked in the event of a physical security breach.

Remediation:

Using the Exchange Management Console (EMC):

In the "Properties" configuration window,

1. Click on the "Password" tab.
2. Click on the "Time without user input before password must be re-entered (in minutes)" checkbox. When this checkbox is checked, you may enter the time in minutes for the auto-lock timeout in the box on the right hand side.
3. Enter the number 5 in the box on the right hand side.
4. Click "OK".

Using the Exchange Management Shell:

At the Exchange Management Shell command prompt,

1. Enter the following command (all one line):

```
Set-ActiveSyncMailboxPolicy -Identity "<PolicyName>"  
-MaxInactivityTimeDeviceLock: 00:05:00
```

where *<PolicyName>* is the name of the Exchange ActiveSync mailbox policy for which the configuration should be made (replace brackets and text with appropriate policy name).

Audit:

Using the Exchange Management Console (EMC):

In the "Properties" configuration window,

1. Click on the "Password" tab.
2. Observe if the "Time without user input before password must be re-entered (in minutes)" checkbox is selected.
3. Observe if the auto-lock timeout value is set to 5.
4. Click "Cancel".

Using the Exchange Management Shell:

At the Exchange Management Shell command prompt,

1. Enter the following command (all one line):

```
Get-ActiveSyncMailboxPolicy -Identity "<PolicyName>"
```

where *<PolicyName>* is the name of the Exchange ActiveSync mailbox policy for which the audit validation should be made (replace brackets and text with appropriate policy name).

2. Search the outputted policy setting list for the "MaxInactivityTimeDeviceLock:" configuration item.
3. Observe if there is a value following the colon and that the value is set to 5 as shown below:

```
MaxInactivityTimeDeviceLock : 5
```

4. Exit the Exchange Management Shell.

Reference:

1. Microsoft Technet Library Article: Configure Device Password Locking
<http://technet.microsoft.com/en-us/library/bb125004.aspx>

3.1.6 Erase data upon excessive passcode failures (Level 1, Scorable)

Description:

The iPhone can be configured to erase the user's settings and data as stored on the device after excessive (configurable from 4 to 16) passcode failures. , By default, the default Exchange ActiveSync policy setting applied for users not assigned to a mailbox policy configures the device to erase data after four (4) failed password attempts, if a password is configured on the device. It is recommended that this feature be enabled at six (6) failed password attempts.

Rationale:

Excessive password failures typically indicate that the device is out of physical control of its owner. Upon such an event, erasing data on the phone will ensure the confidentiality of information stored on the device is protected when facing a novice attacker.

Remediation:

Using the Exchange Management Console (EMC):

In the "Properties" configuration window,

1. Click on the "Password" tab.
2. Click on the "Number of failed attempts allowed:" checkbox. When this checkbox is checked, you may enter the maximum number of failed attempts in the box on the right hand side.
3. Enter the number 6 in the box on the right hand side.
4. Click "OK".

Using the Exchange Management Shell:

At the Exchange Management Shell command prompt,

1. Enter the following command (all one line):

```
Set-ActiveSyncMailboxPolicy -Identity "<PolicyName>"  
-MaxDevicePasswordFailedAttempts : 6
```

where <PolicyName> is the name of the Exchange ActiveSync mailbox policy for which the configuration should be made (replace brackets and text with appropriate policy name).

Audit:

Using the Exchange Management Console (EMC):

In the "Properties" configuration window,

1. Click on the "Password" tab.
2. Observe if the "Number of failed attempts allowed:" checkbox is selected.
3. Observe if the failed attempts value is set to 6.
4. Click "Cancel".

Using the Exchange Management Shell:

At the Exchange Management Shell command prompt,

1. Enter the following command (all one line):

```
Get-ActiveSyncMailboxPolicy -Identity "<PolicyName>"
```

where <PolicyName> is the name of the Exchange ActiveSync mailbox policy for which the audit validation should be made (replace brackets and text with appropriate policy name).

2. Search the outputted policy setting list for the "MaxDevicePasswordFailedAttempts" configuration item.
3. Observe if there is a value following the colon and that the value is set to 6 as shown below:

```
MaxDevicePasswordFailedAttempts : 6
```

4. Exit the Exchange Management Shell.

Reference:

1. Microsoft Technet Library Article: Configure Device Password Locking
<http://technet.microsoft.com/en-us/library/bb125004.aspx>

Appendix A: References

1. Apple, Inc. (2009). *iPhone User Guide - For i OS 4 Software*. Available: [http://manuals.info.apple.com/en_US/iPhone iOS4 User Guide.pdf](http://manuals.info.apple.com/en_US/iPhone_iOS4_User_Guide.pdf). Last accessed 7 September 2010.
2. Apple, Inc. (2009). *iOS Enterprise Deployment Guide - Second Edition, for Version 3.2 or later*. Available: [http://manuals.info.apple.com/en_US/Enterprise Deployment Guide.pdf](http://manuals.info.apple.com/en_US/Enterprise_Deployment_Guide.pdf). Last accessed 24 August 2010.
3. Apple, Inc. (2009). *iPhone and iPod touch: Understanding subscription Wi-Fi networks*. Available: <http://support.apple.com/kb/HT3867>. Last accessed 24 August 2010.
4. Jonathan Zdziarski (2008). *iPhone Forensics: Recovering Evidence, Personal Data, and Corporate Assets*. USA: O'Reilly.
5. National Institute of Standards and Technology. (2006). *NIST Special Publication 800-63: Electronic Authentication Guideline*. Available: http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf. Last accessed 24 August 2010.
6. National Institute of Standards and Technology. (2008). *NIST Special Publication 800-124: Guidelines on Cell Phone and PDA Security*. Available: <http://csrc.nist.gov/publications/nistpubs/800-124/SP800-124.pdf>. Last accessed 24 August 2010.

Appendix B: Change History

Date	Version	Changes for this version
27 March 2009	1.0.0	- Public Release
30 October 2009	1.1.0	<ul style="list-style-type: none"> - Page 8, "Loss of Physical Custody of an iPhone and Compensating Controls": Added discussion - Section 1.1.6, Turn off Auto-Join for all Wi-Fi networks: Inserted new section - Section 1.2.3, Enable Fraud Warning (Level 1, Not Scorable): Added new section - Section 1.2.4, Disable AutoFill (Level 2, Not Scorable): Added new section - Section 2.1, System Settings: Added new section - Section 2.1.1, Disallow Profile Removal (Level 1, Scorable): Added new section - Section 2.1.5, Set maximum passcode age: Removed recommendation and moved to Section C.1, Set maximum passcode age, as informational - Section 2.2.2, Require alphanumeric value: Changed configuration level from Level 1 to Level 2 - Section 2.2.6, Erase data upon excessive passcode failures: Changed configuration setting for maximum number of failed attempts from 10 to 6 - Appendix C, Additional Security Notes: Added appendix - Throughout: Updated software and hardware version references in document as necessary - Throughout: Updated formatting, typographical, and grammatical errors in document as necessary
19 October 2010	1.2.0	<ul style="list-style-type: none"> - Updated to cover iOS 4.1.0 - Section 1.1.12, Disable show SMS preview when iPhone is locked (Level 2, Not Scorable): Corrected errors in Remediation and Audit steps - Section 3, iPhone Settings in MS Exchange ActiveSync Policy: Added section - Section C.2, Set passcode history (Informational): Added new section - Appendix D, Additional Information for Exchange ActiveSync Management: Added appendix - Throughout: Updated software version references in document as necessary - Throughout: Updated formatting, typographical, and grammatical errors in document as necessary

Appendix C: Additional Security Notes

The items in this section are security configuration settings that are available within the iOS but have been determined to provide relatively little incremental security benefit, either due to other settings in the benchmark document or inherent applicability or effectiveness as a control.

These settings may be required to meet compliance requirements or in a unique situation may provide a security benefits that outweighs the administrative cost of performing them, as determined by an organization's own risk analysis. These settings are purely optional and may be applied or not at the discretion of local site administrators.

C.1 Set maximum passcode age (Informational)

Description:

The iPhone can be configured to expire the passcode after a pre-determined amount of time. By default, the iPhone does not expire passcodes.

Rationale:

Requiring a passcode to expire may in certain circumstances additionally reduce the window of opportunity for an attacker to guess the password beyond the constraints already imposed by the *Erase data upon excessive passcode failures* control described in sections 1.1.14 and 2.2.6.

Note:

- The number of days for expiration should be determined by the organization based on the specific reason and risk for which it chooses to implement this optional control. A value divisible by 7 helps ensure the expiration occurs on the same week day.
- Remember that as expiring passcodes with high frequency results in requiring the user to frequently type new/unfamiliar passwords, this setting can result in more initial password failures counted by the *Erase data upon excessive passcode failures* control, as well as affect productivity and usability. It can also unintentionally induce poor user password management behavior (such as using sequential passcodes/minor variations or recording passwords insecurely).

Remediation:

1. Open iPCU.
2. Click on “Configuration Profiles” in the left windowpane.
3. Click on the “Passcode” tab in the lower right windowpane.
4. Click on the “Maximum passcode age (in days)” textbox in the lower right windowpane.
5. Enter a number that is appropriate for the organization.
6. Install the configuration profile on the device.

Audit:

1. Open the configuration profile XML file.
2. Search for `<key>maxPINAgeInDays</key>`.
3. Observe if the next line is `<real><maxPasscodeAge></real>`, where `<maxPasscodeAge>` is the integer number of days corresponding to the desired maximum passcode age.

Reference

1. iOS Enterprise Deployment Guide - Second Edition, for Version 3.2 or later
http://manuals.info.apple.com/en_US/Enterprise_Deployment_Guide.pdf

C.2 Set passcode history (Informational)

Description:

The iPhone can be configured to check new passcode selections against previously-used passcodes to discourage reuse. If enabled, the previous passcode list used for comparison is configurable from 1 to 50. By default, the iPhone does not check passcode history.

Rationale:

When used in conjunction with passcode expiration (via setting maximum passcode age), checking a new passcode against previously used passcodes may help support the goals of password change requirements by preventing a password from being reused upon expiration.

Remediation:

1. Open iPCU.
2. Click on “Configuration Profiles” in the left windowpane.
3. Click on the “Passcode” tab in the lower right windowpane.
4. Click on the “Passcode history (1-50 passcodes, or none)” textbox in the lower right windowpane.
5. Enter a number that is appropriate for the organization.
6. Install the configuration profile on the device.

Audit:

1. Open the configuration profile XML file.
2. Search for `<key>pinHistory</key>`.
3. Observe if the next line is `<integer><PasscodeHistory></integer>`, where `<PasscodeHistory>` is the number of historical passcodes to be compared upon passcode change.

Reference

1. iOS Enterprise Deployment Guide - Second Edition, for Version 3.2 or later
http://manuals.info.apple.com/en_US/Enterprise_Deployment_Guide.pdf

Appendix D: Additional Information for Exchange ActiveSync Management

Microsoft Exchange ActiveSync is a Microsoft Exchange mobile device communication and synchronization protocol based on HTTP and XML that allows mobile devices to access information on a Microsoft Exchange server. Exchange ActiveSync enables mobile phone users to access e-mail, calendar, contacts, and tasks and provides access to certain features that allow for the enforcement of security policies on mobile devices. Multiple policies can be created as needed to reflect organizational groups, device types, or combinations as desired; however, the policies are applied to users/user mailboxes and not devices specifically, and a user can belong to only one Exchange ActiveSync mailbox policy at a time.

Security configuration items that can be applied include the initiation of a remote wipe of a managed device and the enforcement of five password configuration policies (specifically, requiring a passcode, setting a minimum passcode length, requiring an alphanumeric passcode, requiring a complex passcode, and setting an inactivity time lockout) through the creation and application of an Exchange ActiveSync mailbox policy for a user. These ActiveSync configuration items can be applied through one or more of the following management interfaces: the MS Exchange Management Console (EMC), the MS Exchange Management Shell, the Microsoft Exchange Server ActiveSync Web Administration Tool, and the Outlook Web Access Mobile Device Management interface.

The instructions in this section have the following prerequisites:

- The Client Access server role has been installed on the Exchange Server.
- The appropriate Client Access Permissions have been assigned to permit the indicated configurations.
- Exchange ActiveSync is enabled for the user.
- The device ID for the mobile device has not been specifically removed from the ActiveSyncAllowedDeviceIDs parameter list
- An Exchange ActiveSync mailbox policy to be configured has already been created.

Additional information on MS EAS and its setup, configuration, and management is available from Microsoft, including the TechNet Library Article *Understanding Exchange ActiveSync* available at <http://technet.microsoft.com/en-us/library/aa998357.aspx>

D.1 General ActiveSync Settings

This section provides guidance on the configuration of general ActiveSync settings.

D.1.1 Disallow non-provisionable devices (Level 1, Scorable)

Description:

For a given mailbox policy, Microsoft Exchange ActiveSync classifies a mobile device attempting to connect as one of two types—a provisionable device or a non-provisionable device—based on the device’s ability to comply with the policy. Provisionable devices are devices that are capable of fully applying and enforcing a specified policy. Non-provisionable devices are devices that are capable of applying and enforcing only a subset of a policy, or even none of a policy.

This ActiveSync policy setting specifies whether a mobile device that cannot support the application of all policy settings can connect to MS Exchange through Exchange ActiveSync. By default, Exchange ActiveSync allows non-provisionable devices to connect through Exchange ActiveSync. To ensure that mobile devices connect only when the full policy can be assured, non-provisionable devices must be disallowed.

Rationale:

Restricting the devices which can connect to MS Exchange through ActiveSync to only those which can fully support the policy specified is the only way that Exchange ActiveSync can assure that an iPhone is configured fully according to the specified policy. If a device that does not meet any or all of the policy configuration items can continue to connect to Exchange ActiveSync and access the resources provided through the ActiveSync connection, the initial and continued enforcement of policy controls cannot be assured and intended device security is highly reduced.

Remediation:

Using the Exchange Management Console (EMC):

1. Open the Exchange Management Console.
2. In the console tree, click on “Exchange ActiveSync” and then “Client Access to open the Client Configuration work area.
3. Click on the “Exchange ActiveSync Mailbox Policies” tab.
4. Select the mailbox policy to modify.
5. Click on “Properties.”
6. Click on the “General” tab.
7. Click on the “Allow non-provisionable devices” checkbox to remove any check mark.
8. Click “OK”.

Using the Exchange Management Shell:

1. Open the Exchange Management Shell.
2. Enter the following command (all one line):

```
Set-ActiveSyncMailboxPolicy -Identity "<PolicyName>"  
-AllownonProvisionableDevices $true
```

where *<PolicyName>* is the name of the Exchange ActiveSync mailbox policy for which the configuration should be made (replace brackets and text with appropriate policy name).

Audit:

Using the Exchange Management Console (EMC):

1. Open the Exchange Management Console.
2. In the console tree, click on "Exchange ActiveSync" and then "Client Access to open the Client Configuration work area.
3. Click on the "Exchange ActiveSync Mailbox Policies" tab.
4. Select the mailbox policy to modify.
5. Click on "Properties."
6. Click on the "General" tab.
7. Observe if the "Allow non-provisionable devices" checkbox is unchecked.
8. Click "Cancel".

Using the Exchange Management Shell:

1. Open the Exchange Management Shell.
2. Enter the following command (all one line):

```
Get-ActiveSyncMailboxPolicy -Identity "<PolicyName>"
```

where *<PolicyName>* is the name of the Exchange ActiveSync mailbox policy for which the audit validation should be made (replace brackets and text with appropriate policy name).

3. Search the outputted policy setting list for the "AllowNonProvisionableDevices:" configuration item.
4. Observe if the value following the colon is "False" as shown below:
`AllowNonProvisionableDevices : False`
5. Exit the Exchange Management Shell.

Reference:

1. Microsoft Technet Library Article: View or Configure Exchange ActiveSync Mailbox Policy Properties
<http://technet.microsoft.com/en-us/library/bb123994.aspx>

D.2 General Resources for iOS Mobile Device ActiveSync Management

This section provides references to general resources supporting the use and management of iOS mobile devices using Microsoft Exchange ActiveSync.

1. iOS Enterprise Deployment Guide - Second Edition, for Version 3.2 or later
http://manuals.info.apple.com/en_US/Enterprise_Deployment_Guide.pdf
2. Microsoft Technet Library Article: Exchange 2010 Client Access Cmdlet Set-ActiveSyncMailboxPolicy Parameter Information

- <http://technet.microsoft.com/en-us/library/bb123756.aspx>
3. Microsoft Technet Library Article: Exchange 2010 Client Access Cmdlet Get-ActiveSyncMailboxPolicy Parameter Information
<http://technet.microsoft.com/en-us/library/bb124900.aspx>
 4. New User's Guide to the Exchange Management Console
<http://technet.microsoft.com/en-us/library/bb245702%28EXCHG.80%29.aspx>
 5. A Primer on the Exchange Management Shell
<http://technet.microsoft.com/en-us/library/bb245704%28EXCHG.80%29.aspx>
 6. Exchange Management Shell in Exchange 2010
<http://technet.microsoft.com/en-us/library/dd795097.aspx>
 7. Exchange Management Console (MS Exchange 2010)
<http://technet.microsoft.com/en-us/library/bb123762.aspx>
 8. Exchange Management Shell (MS Exchange 2010)
<http://technet.microsoft.com/en-us/library/bb123778.aspx>
 9. iPhone in Business Device Configuration Overview
http://images.apple.com/iphone/business/docs/iPhone_Device_Configuration_Overview.pdf