the CENTER for INTERNET SECURITY

Security Configuration Benchmark For

Apple iOS 5.0.1

Version 1.4.0-A3
20 December 2011

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 it 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

Overview

This document, *Security Configuration Benchmark for Apple iOS 5.0.1*, provides prescriptive guidance for establishing a secure configuration posture for the Apple iOS version 5.0.1. This guide was tested against the Apple iOS 5.0.1 and the iPhone Configuration Utility (iPCU) v3.4.0.283. This benchmark covers the Apple iOS 5.0.1 and all hardware devices on which this iOS is supported. As of the publication of this guidance, mobile devices supported by iOS 5.0.1 include the following:

- iPhone 4S
- iPhone 4
- iPhone 3GS
- iPad 2
- iPad
- iPod touch (4th generation)
- iPod touch (3rd generation)

In determining recommendations, the current guidance treats all iOS mobile device platforms as having the same use cases and risk/threat scenarios. In all but a very few cases, configuration steps, default settings, and benchmark recommended settings are identical regardless of hardware platform; for the few cases where variation exists, the benchmark notes the difference within the respective section. 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 5.0.1.

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
Roland Grefer
Richard Haas, NASA Emerging Technology and Desktop Standards (ETADS)
Rebecca Heffel, University of Washington
Toon Mordijck, Atos Worldline
Adrian Sanábria
Brian Reilly
Richard Tychansky
Joe Wulf, ProSync Technologies

Typographic Conventions

The following typographical conventions are used throughout this guide:

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

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 discernible 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 directly through its local interface, through configuration profiles created via manufacturer-provided tools, and through configuration capabilities provided by Exchange ActiveSync mailbox policies. In considering the recommendations made in this benchmark, an iOS 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.

The recommendations provided in this benchmark are made in consideration of the built-in encryption capabilities provided by iOS 5.0.1-capable devices. The encryption features of these iOS devices work in conjunction with, and do not obviate, the recommendations made in the guide.

Loss of Physical Custody of iOS Device and Compensating Controls

iOS 5.0.1 Data Protection along with the combined passcode, auto-lock timeout, and data erasure recommendations in the Level I and Level II Benchmark profiles provide a measure of protection against unauthorized device and data access in the event of a lost device. Data Protection enhances the protection of e-mail and application data, but the actual protection level afforded by the hardware encryption relies on development choices made by app providers, as well as the strength of passcode enforced on the device. 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.

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 iOS 5.0.1 devices, available through various mechanisms, including:
    - 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 iCloud/MobileMe Accounts
    - A 3rd-Party Mobile Device Management (MDM) server (see Appendix E)
- In addition to supporting *Remote Wipe*, the Apple iCloud and MobileMe Accounts also support a *Find My iPhone/iPad/iPod touch* feature (to locate an iOS device on a map), a *Set a passcode* feature (to remotely set a passcode on and lock a device), and the option to display a message or play a sound on a lost device.
- Third-party encryption apps may 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 in the iOS User Interface

This section provides guidance on the secure configuration of iOS mobile devices using the device user interface.

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:
An iOS mobile device ships 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 device firmware remain current. iOS 5 devices can be updated via iTunes with cable connection, or via Over-the-Air Update. Over-the-Air updates may be initiated over Wi-Fi or cellular network. Not all iOS updates or carriers may support download over a cellular connection and may require a Wi-Fi network connection to download. iOS updates may require the device have a minimum remaining battery life and storage for update. To prevent loss of data, ensure that the device is backed up (to iCloud or via iTunes) before performing the update.

Rationale:
Firmware updates include not only new features and bug fixes but security fixes as well. Also, the device must be running firmware version 5.0.1 for these benchmark recommendations to apply; if a newer version of the firmware is available, some recommendations may not apply.

Device Default Value:
Not Applicable

Remediation:

Using iTunes:

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

Using Over-the-Air Update:

1. Tap Settings.
2. Tap General.
3. Tap Software Update
4. iOS will automatically check for available updates. If an update is available, tap Download when prompted to download the update.
5. Once the download has completed, tap Install to update the iOS.
6. Do not power off the device until the update is finished.

Audit:

1. Tap Settings.
2. Tap General.
3. Tap About.
4. Confirm that "Version" is 5.0.1.

References:

1. iOS: How to update your iPhone, iPad, or iPod touch http://support.apple.com/kb/HT4623
2. iOS 5: Updating your device to iOS 5 http://support.apple.com/kb/HT4972
3. iOS: How to back up http://support.apple.com/kb/HT1766

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

Description:
iOS can be configured to require a passcode before allowing usage via the touch screen. By default, a passcode is not required to unlock the screen. 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.

Device Default Value:
Passcode Lock: Off

Remediation:

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

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

Audit:

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

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

Description:
iOS can be configured to allow a passcode comprised of numeric, alphabetic, and non-alphanumeric values. By default, iOS 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-alphanumerical characters increases the complexity of the passcode an attacker may attempt to brute-force in order to gain access to the device.

Device Default Value:
Simple Passcode: On (complex passcode not permitted)

Remediation:
1. Tap Settings.
2. Tap General.
3. Tap Passcode Lock
4. Enter current passcode if configured.
5. Turn off Simple Passcode.
6. Enter previous password when prompted.
7. 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 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.

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

Description:
An iOS device can be configured to auto-lock after a pre-defined inactivity period. By default, if a passcode is defined, the device will automatically lock after two minutes of inactivity. It is recommended that an inactivity timeout of no more than five (5) minutes be set for typical use cases and no more than two (2) minutes for high-security use cases.

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

Device Default Value:
Auto-Lock: 2 Minutes

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 "2 Minutes".

Note: The auto-lock timeout can also be set via the iPhone Configuration Utility (iPCU) as described in section 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 Auto-Lock is set to 2 Minutes.

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

Description:
An iOS device 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.

Device Default Value:
Erase Data: Off

Remediation:
1. Tap Settings.
2. Tap General.
3. Tap Passcode Lock.
4. Enter current passcode as prompted.
5. Turn on Erase Data.
6. Tap "Enable" on confirmation dialog.

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

Audit:
1. Tap Settings.

2. Tap General.
3. Tap Passcode Lock.
4. Enter current passcode as prompted.
5. Confirm that Erase Data is turned on.

1.1.6 Forget Wi-Fi networks to prevent automatic rejoin (Level 2, Not Scorable)

Description:
An iOS device can be configured to forget Wi-Fi networks that it has previously associated with. By default, a device 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 iOS device will encounter an untrusted instance of a same-named Wi-Fi network and automatically join it.

Device Default Value:
Each Network SSID is Remembered for Automatic Join

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 Wi-Fi network you want to forget.
4. Tap "Forget this network."
5. Tap "Forget" on the confirmation dialog.

Note: Wi-Fi must be turned on and the Wi-Fi network must be in range for it to appear in the list of available networks to configure. The Wi-Fi network must be remembered or currently connected for the "Forget this network" option to be present. 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 Wi-Fi.
3. From the Choose a Network list, locate the network SSID and tap the chevron next to the Wi-Fi network to check.
4. Confirm that the network configuration does not have the "Forget this network" option available.

1.1.7 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 device to look for another network. A list of all available Wi-Fi networks that the user can choose from will be displayed. 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 "defualt").

Device Default Value:
Ask to Join Networks: On

Remediation:
1. Tap Settings.
2. Tap Wi-Fi.
3. Turn off "Ask to Join Networks".

Note: Wi-Fi must be turned on for the above Wi-Fi configuration option to appear.

Audit:
1. Tap Settings.
2. Tap Wi-Fi.
3. Confirm that "Ask to Join Networks" is turned off.

1.1.8 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 credentials to persist on disk. If physical custody of the device is lost, the confidentiality of the persisted credentials—and the resources protected by them—may be at risk if the attacker retrieves the device'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.

Device Default Value:
Auto-Join: On (for supported networks)

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.

Note: Wi-Fi must be turned on and the Wi-Fi network must be in range for it to appear in the list of available networks to configure. The Wi-Fi network must require network login credentials and must be remembered or currently connected for the Auto-Join option to be present.

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 review.
4. Confirm that Auto-Join is turned off.
5. Repeat steps 3 and 4 for each network SSID.

Reference:

1. iPhone, iPad, iPod touch: Understanding subscription Wi-Fi networks http://support.apple.com/kb/HT3867

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

Description:
iOS devices 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 on a device with cellular data service, connections to the Internet will occur via the cellular data network, when available. Applications such as Mail, Safari, YouTube, Stocks, Maps, Weather, and the App Store can be run over a cellular data network connection, but there may be a limit on the maximum download size of items for certain apps.

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

Device Default Value:
Wi-Fi: On

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.

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

Description:
iOS devices 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 if turned on.

Audit:

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

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

Description:
Bluetooth allows devices to connect wirelessly to headsets, car kits, and other accessories for various Bluetooth profile functionality. It is recommended that Bluetooth be disabled when not in use.

Rationale:
If the user does not need Bluetooth enabled, it should be disabled to prevent discovery of and connection to supported Bluetooth services.

Device Default Value:
Bluetooth: On

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. iOS: Supported Bluetooth Profiles
   http://support.apple.com/kb/ht3647

1.1.12 Turn off Personal Hotspot when not needed (Level 2, Not Scorable)

Description:
iPhone iOS devices (3GS and later) can be configured to share an active Cellular Data connection using Personal Hotspot via Wi-Fi (iPhone 4), Bluetooth, or USB. It is recommended that Personal Hotspot be disabled when not needed or where security is paramount.

Disabling Personal Hotspot prevents other computers and devices from connecting to the Internet using the Cellular Data connection on the iPhone. Turning off Personal Hotspot immediately disconnects connected users and prevents new connections.

Personal Hotspot networks using Wi-Fi require a password. Using a long password that contains a mix of alphabetical, numerical, and/or non-alphanumerical ASCII characters increases the complexity of the password that an attacker in range must attempt to guess to gain access to the hotspot.

Platform:
iPhone iOS Devices—iPhone 3GS, iPhone 4, iPhone 4S. Feature requires Personal Hotspot on Cellular Data plan.

Rationale:
Disabling the Personal Hotspot makes the hotspot unavailable to unauthorized access attempts and reduces the overall remote attack surface of the device.

Device Default Value:
Personal Hotspot: Off, Not Configured

Remediation:
1. Tap Settings.
2. Tap General.
3. Tap Network.
4. Tap Personal Hotspot.
5. Turn off Personal Hotspot.

Audit:
1. Tap Settings.
2. Tap General.
3. Tap Network.
4. Tap Personal Hotspot.
5. Confirm that Personal Hotspot is turned off.

Reference:
1. iOS: Understanding Personal Hotspot
   http://support.apple.com/kb/HT4517

1.1.13 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 as available. 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:
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.

Device Default Value:
Location Services: On

Remediation:
1. Tap Settings.
2. Tap Location Services.
3. Turn off Location Services.

Note: Location services can also be disabled/enabled on a per-app basis within the Locations Services configuration menu above.

Audit:

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

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

Description:
Mobile devices running iOS 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 device. 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 device does not initiate or respond to any signals. This reduces the remote attack surface.

Device Default Value:
Airplane Mode: Off

Remediation:

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

Audit:

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

1.1.15 Erase all data before return, recycle, reassignment, or other disposition (Level 1, Not Scorable)

Description:
In normal operations, iOS devices do 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 device is out of the user's control.

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

Device Default Value:

Not Applicable

Remediation:

1. Tap Settings.
2. Tap General.
3. Tap Reset.
4. Tap Erase All Contents and Settings.
5. If passcode is configured on device, enter passcode when prompted.

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 reference for more information.

Reference:

1. iPhone Forensics
   http://oreilly.com/catalog/9780596153588/

1.1.16 Disable View in Lock Screen for apps when device is locked (Level 2, Not Scorable)

Description:

If the iOS device is passcode locked and receiving notifications from any source, the notifications may still be displayed. It is recommended that View in Lock Screen be disabled for all apps for which message confidentiality is desired and in environments where security is paramount.

Rationale:

Parties who do not know the passcode lock should not have read access to the notifications displayed by the device.

Device Default Value:

View in Lock Screen: On (for apps in Notification Center)

Remediation:

1. Tap Settings.
2. Tap Notifications.
3. From the list of notification sources listed in the Notifications panel, locate the app or other notification source and tap the chevron next to the source to change.
4. Turn off View in Lock Screen.
5. Repeat steps 3 and 4 for each source.

Note: The notification sources will be grouped based on whether notifications are enabled in general for the app. Apps enabled for Notification Center will be listed in the section" In Notification Center" and apps disabled for Notification Center will be listed in the section "Not in Notification Center." Apps for which Notification Center is disabled will not have notifications active, including notifications in the lock screen.

Audit:

1. Tap Settings.
2. Tap Notifications.
3. From the list of notification sources listed in the Notifications panel, locate the app or other notification source and tap the chevron next to the source to review.
4. Confirm that View in Lock Screen is turned off.
5. Repeat steps 3 and 4 for each source.

1.2 Safari Settings

This section provides guidance on the secure configuration of settings related to the Safari application on the iOS mobile devices.

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.

Device Default Value:
JavaScript: On

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.

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 accidently visiting some known phishing and other fraudulent sites covered by this feature.

Device Default Value:
Fraud Warning: On

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.

1.2.3 Disable AutoFill (Level 2, Not Scorable)

Description:
The browser has a feature to remember information entered into common forms in order to automate the completion of later forms. 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.

Device Default Value:
AutoFill: Off (Use Contact Info: Off; Names and Passwords: Off)

Remediation:
1. Tap Settings.
2. Tap Safari.
3. Tap AutoFill.
4. Turn off “Use Contact Info”
5. Turn off “Names and Passwords”.

Audit:

1. Tap Settings.
2. Tap Safari.
3. Tap AutoFill
4. Confirm that AutoFill is turned off for the “Use Contact Info” setting.
5. Confirm that AutoFill is turned off for the “Names and Passwords” setting.

1.2.4 Turn On Private Browsing When Needed (Level 2, Not Scorable)

Description:
The Safari browser on iOS devices keeps a history of web pages visited, searches performed, and (if configured), and certain AutoFill information. The tracking of this information can be prevented for a browser session by enabling Private Browsing. When enabled, Safari bars will appear black or dark instead of blue or gray.

The Private Browsing option may not prevent Safari from collecting cookies from all websites. To more robustly reduce the ability of websites or local users to track activity, also ensure that the Accept Cookies option is turned off.

Rationale:
Enabling Private Browsing can protect certain private information and block some websites from tracking browser activity; enabled, Safari will not remember web pages visited, search history, or AutoFill information used within the Private Browsing session.

Device Default Value:
Private Browsing: Off

Remediation:
1. Tap Settings.
2. Tap Safari.
3. Turn off Private Browsing.

Audit:
1. Tap Settings.
2. Tap Safari.
3. Confirm that Private Browsing is turned off.

Reference:
1. iOS: Safari web settings
   http://support.apple.com/kb/HT1677

2. Settings in the iPCU

This section provides guidance on the secure configuration of iOS mobile devices with the iPhone Configuration Utility (iPCU), version 3.4.0.283. 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.

Configuration Profile Auditing and Distribution Note:

The configuration profiles created by the iPCU are stored as plain text XML files as iPCU application data in a location specific to the respective home/user-profile and operating system. The file names consist of an application-generated UUID for each profile and a .mobileconfig extension, and are not immediately recognizable by file name to the associated iPCU profile. Instead, to access a mobileconfig file for audit or distribution, export the respective configuration profile to a location of choice as described in the Enterprise Deployment Guide. Note that the "None" security option must be selected to produce a plain text file that can be easily read for auditing settings. The "Sign Configuration Profile" or "Sign and Encrypt Profile" export security options may be preferable for distribution depending on distribution method and target device requirements.

Configuration Profiles created in the iPCU can be distributed to an iOS device in multiple ways, including via a direct USB connection using the iPCU, Over-the-Air-Enrollment and Configuration, a Mobile Device Management (MDM) solution, e-mail attachment, or web link. Refer to the respective distribution instructions of the Installing Configuration Profiles section of the iPhone OS Enterprise Deployment Guide and the Installing Configuration Profiles section of the iPhone Configuration Utility online help.

Further Information:

More information on the iPCU and iOS configuration profiles is available in the *iPhone Configuration Utility* guide, *iPhone Configuration Utility* online help, and the *iOS Configuration Profile Reference* available from Apple at the following locations:

iPhone Configuration Utility (guide)
http://developer.apple.com/library/ios/featuredarticles/FA_iPhone_Configuration_Utility/FA_iPhone_Configuration_Utility.pdf

iPhone Configuration Utility (online help)
http://help.apple.com/iosdeployment-ipcu/

iOS Configuration Profile Reference
http://developer.apple.com/library/ios/featuredarticles/iPhoneConfigurationProfileRef/iPhoneConfigurationProfileRef.pdf.

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 device 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.

Device Default Value:
Not Applicable

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.

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 device can be configured to require a passcode before allowing access through the touchpad. By default, a passcode is not required 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 device in the event of a physical security breach.

Device Default Value:
Passcode Lock: Off

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. If a passcode is not currently required, you will be prompted to Configure Passcode Policy. Click on the "Configure" button in the prompt.
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 in the iOS User Interface.

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

2.2.2 Require alphanumeric value (Level 2, Scorable)

Description:
The device can be configured to require that the passcode be comprised of both numeric and alphabetic values. By default, a passcode complexity policy is not enforced. 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.

Device Default Value:
Simple Passcode: On

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/>`.

2.2.3 Set minimum passcode length (Level 1, Scorable)

Description:
The device 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.

Device Default Value:
Not Configured (With default *Simple Passcode: On* setting, a 4 digit number is enforced)

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 `<integer>5</integer>`.

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

Description:
The device can be configured to require non-alphanumeric characters in the passcode. By default, complex characters are not required 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.

Device Default Value:
Not Configured (With default *Simple Passcode: On* setting, complex characters are not permitted)

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 in the iOS User Interface.

Audit:

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

Reference:

1. NIST NIST SP800-63-1, Electronic Authentication Guideline – Revision 1 **http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf**

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

Description:
The device can be configured to auto-lock after a pre-defined inactivity period. By default, if a passcode is defined, an iPhone or iPod touch device will lock after two minutes of inactivity. It is recommended that an inactivity timeout of no more than five (5) minutes be set for typical use cases and no more than two (2) minutes for high-security use cases.

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

Device Default Value:
Auto-Lock: 2 Minutes

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.

5a. For typical use cases, select the number 5.
5b. For high-security use cases, select the number 2.

6. Install the configuration profile on the device.

Note: The auto-lock timeout can also be set via the iOS UI as described in section Settings in the iOS User Interface.

Audit:

1. Open the configuration profile XML file.
2. Search for `<key>maxInactivity</key>`.

3a. For typical use cases, observe if the next line is `<integer>5</integer>`.
3b. For high-security use cases, observe if the next line is `<integer>2</integer>`.

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

Description:
The device can be configured to erase the user's settings and data as stored on the device after excessive (configurable from 4 to 10) 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.

Device Default Value:
Erase Data: Off

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 iOS UI as described in section Settings in the iOS User Interface.

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

3. iOS Mobile Device Settings in MS Exchange ActiveSync Policy

This section provides guidance on the configuration of certain policies on iOS mobile devices 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.

Additional information on management of iOS device s using MS Exchange ActiveSync policies, is available in Apple’s Exchange ActiveSync and iOS Devices online guide, available at http://help.apple.com/iosdeployment-exchange/.

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 device can be configured to require a passcode before allowing access through the touchpad. By default, iOS devices do 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.

Device Default Value:
Passcode Lock: Off

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.

3.1.2 Require alphanumeric value (Level 2, Scorable)

Description:
The device can be configured to require that the passcode be comprised of both numeric and alphabetic values. By default, iOS devices do 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.

Device Default Value:
Simple Passcode: On (complex passcode not permitted)

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.

3.1.3 Set minimum passcode length (Level 1, Scorable)

Description:

The device 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.

Device Default Value:

Not Configured (With default *Simple Passcode: On* setting, a 4 digit number is enforced)

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.

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

Description:
The device can be configured to require non-alphanumeric characters in the passcode. By default, iOS devices do 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.

Device Default Value:
Not Configured (With default *Simple Passcode: On* setting, complex characters are not permitted)

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.

Reference:

1. NIST NIST SP800-63-1, Electronic Authentication Guideline – Revision 1 http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf

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

Description:
The device can be configured to auto-lock after a pre-defined inactivity period. By default, if a passcode is defined, an iOS device will automatically lock after two minutes 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 for typical use cases and no more than two (2) minutes for high-security use cases.

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.

Device Default Value:
Auto-Lock: 2 Minutes

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.

3a. For typical use case, enter the number 5 in the box on the right hand side.

3b. For high-security use cases, enter the number 2 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) and specifying the time in minutes as appropriate according to use case and device as described for the EMC above.

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 or 2 according to use case.
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 or 2 according to use case as shown below:

   ```
   MaxInactivityTimeDeviceLock : 5
   ```
4. Exit the Exchange Management Shell.

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

Description:

The device 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.

Device Default Value:

Erase Data: Off

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.

Appendix A: References

1. Apple, Inc. (2011). *Exchange ActiveSync and iOS Devices online guide*. Available: http://help.apple.com/iosdeployment-exchange/. Last accessed 16 December 2011.
2. Apple, Inc. (2011). *iOS Configuration Profile Reference*. Available: http://developer.apple.com/library/ios/featuredarticles/iPhoneConfigurationProfileRef/iPhoneConfigurationProfileRef.pdf. Last accessed 16 December 2011.
3. Apple, Inc. (2010). *iOS Enterprise Deployment Guide - Second Edition, for Version 3.2 or later*. Available: http://manuals.info.apple.com/en_US/Enterprise_Deployment_Guide.pdf. Last accessed 16 December 2011.
4. Apple, Inc. (2011). *iOS: How to back up*. Available: http://support.apple.com/kb/HT1766. Last accessed 16 December 2011.
5. Apple, Inc. (2011). iOS: How to update your iPhone, iPad, or iPod touch. Available: http://support.apple.com/kb/HT4623. Last accessed 16 December 2011.
6. Apple, Inc. (2011). iOS: Safari web settings. Available: http://support.apple.com/kb/HT1677. Last accessed 16 December 2011.
7. Apple, Inc. (2011). iOS: Understanding Personal Hotspot. Available: http://support.apple.com/kb/HT4517. Last accessed 16 December 2011.
8. Apple, Inc. (2011). iOS 5: Updating your device to iOS 5. Available: http://support.apple.com/kb/HT4972. Last accessed 16 December 2011.
9. Apple, Inc. (2011). *iOS: Supported Bluetooth Profiles.* http://support.apple.com/kb/ht3647. Last accessed 16 December 2011.
10. Apple, Inc. (2011). *iPad User Guide - For iOS 5.0 Software*. Available: http://manuals.info.apple.com/en_US/ipad_user_guide.pdf. Last accessed 16 December 2011.
11. Apple, Inc. (2011). *iPhone User Guide - For iOS 5.0 Software*. Available: http://manuals.info.apple.com/en_US/iphone_user_guide.pdf. Last accessed 16 December 2011.
12. Apple, Inc. (2011). *iPhone and iPad in Business - Deployment Scenarios*. Available: http://www.apple.com/iphone/business/docs/iOS_Business.pdf. Last accessed 16 December 2011.
13. Apple, Inc. (2011). *iPhone Configuration Utility* (guide). Available: http://developer.apple.com/library/ios/featuredarticles/FA_iPhone_Configuration_Utility/FA_iPhone_Configuration_Utility.pdf. Last accessed 16 December 2011.
14. Apple, Inc. (2011). *iPhone Configuration Utility* (online help). Available: http://help.apple.com/iosdeployment-ipcu/. Last accessed 16 December 2011.
15. Apple, Inc. (2010). *iPhone, iPad, iPod touch: Understanding subscription Wi-Fi networks*. Available: http://support.apple.com/kb/HT3867. Last accessed 16 December 2011.
16. Apple, Inc. (2011). *iPod touch User Guide - For iOS 5.0 Software*. Available: http://manuals.info.apple.com/en_US/ipod_touch_user_guide.pdf. Last accessed 16 December 2011.

17. Jonathan Zdziarski (2008). *iPhone Forensics: Recovering Evidence, Personal Data, and Corporate Assets*. USA: O'Reilly.
18. Microsoft Corporation (2011). *Microsoft Technet Library Article: Configure Device Password Locking*. Available: http://technet.microsoft.com/en-us/library/bb125004.aspx. Last accessed 16 December 2011.
19. Microsoft Corporation (2011). *Microsoft Technet Library Article: Understanding Exchange ActiveSync.* Available: http://technet.microsoft.com/en-us/library/aa998357.aspx. Last accessed 16 December 2011.
20. National Institute of Standards and Technology. (2011). *NIST Special Publication 800-63-1: Electronic Authentication Guideline*. Available: http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf. Last accessed 16 December 2011.
21. 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 16 December 2011.

Appendix B: Change History

Date	Version	Changes for this version
27 March 2009	1.0.0	- Public Release
30 October 2009	1.1.0	- 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	- 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
10 June 2011	1.3.0	- Expanded to cover iPad, iPod, and iPhone devices. - Throughout: Updated software version, iOS device

		references, and related details as necessary to reflect the latest version of iOS (4.3.3) and the devices supported - Throughout: Updated instructions in document as necessary to reflect changes in user interface and menus in 4.3.3 - Throughout: Updated formatting and organization and corrected typographical and grammatical errors in document as necessary
19 December 2011	1.4.0	- Page 9, "Recommendations": Updated description of hardware encryption capabilities and details around Data Protection and loss of physical custody. - Section 1.1.1, Update firmware to latest version (Level 1, Not Scorable): Added details on and remediation/audit steps for Over-the-Air updates - Section 1.1.4, Set auto-lock timeout (Level 1, Not Scorable): Changed configuration setting for high security use case timeout to 2 minutes for all devices - Section 1.1.12, Turn off Personal Hotspot when not needed (Level 2, Not Scorable): Added section - Section 1.1.15, Disable show SMS preview when iPhone is locked (Level 2, Not Scorable): Revised section to include all notifications and renamed as 1.1.16, Disable View in Lock Screen for apps when device is locked (Level 2, Not Scorable) - Section 1.2.4, Turn On Private Browsing When Needed (Level 2, Not Scorable): Added section - Page 25, "Configuration Profile Auditing and Distribution Note": Updated information on Configuration Profile distribution - Section 2.2.5, Set auto-lock timeout (Level 1, Scorable): Changed configuration setting for high security use case timeout to 2 minutes for all devices - Page 31, "iOS Mobile Device Settings in MS Exchange ActiveSync Policy": Provided additional reference on management of iOS devices using MS Exchange ActiveSync policies - Section 3.1.5, Set auto-lock timeout (Level 1, Scorable): Changed configuration setting for high security use case timeout to 2 minutes for all devices - Appendix E, Additional Information for Mobile Device Management (MDM): Added appendix - Throughout: Consolidated general references to Appendix A - Throughout: Added iOS *Device Default Value* and

	Platform configuration notations where applicable. - Throughout: Updated software version, iOS device references, and related details as necessary to reflect the latest version of iOS (5.0.1) and the devices supported. - Throughout: Updated instructions in document as necessary to reflect changes in user interface and menus in 5.0.1. - Throughout: Updated formatting and organization and corrected 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 iOS devices can be configured to expire the passcode after a pre-determined amount of time. By default, passcodes are not expired.

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 1.1.15 and 2.2.6. Values are configurable from 1 to 730 days, or none.

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 `<integer><`*`maxPasscodeAge`*`></integer>`, where <*maxPasscodeAge*> is the integer number of days corresponding to the desired maximum passcode age.

C.2 Set passcode history (Informational)

Description:
iOS devices 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, passcode history is not set.

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.

Appendix D: Additional Information for Exchange ActiveSync Management

Microsoft Exchange ActiveSync (EAS) 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 and iPad in Business - Deployment Scenarios
http://www.apple.com/iphone/business/docs/iOS_Business.pdf

Appendix E: Additional Information for Mobile Device Management (MDM)

Apple iOS 5 and iOS 5 devices support management by third-party Mobile Device Management (MDM) systems.

Through such systems, configuration profiles can be pushed to and removed from mobile devices to enforce appropriate administrative policies, including those that support the system and passcode settings described in Section 2, as well as other settings supported by configuration profiles such as the set up of

- application, content, and functionality restrictions,
- configurations for access to enterprise resources including e-mail, calendars, contact lists, Wi-Fi networks, VPN,
- certificate-based credentials and certificate enrollment connections,

and various other configuration-profile supported features.

MDM servers can also support the remote installation and removal of managed enterprise-developed and Apple App Store apps, as well as the management of iTunes or iCloud app backup, the remote audit and inventory of key device information, and the ability to take certain device security actions, including remote wipe/lock and passcode changes.

Audit and inventory information (including querying of the installed configuration profile, hardware encryption capability, and passcode presence), along with network information and the previously-described ability to perform remote device wipe or lock can collectively or individually provide an enterprise a powerful toolset to prevent or reduce the likelihood of a data breach due to a lost device and can support the location and recovery of lost devices.

Additional information on MDM in iOS is available from Apple at the following locations:

Deploying iPhone and iPad Mobile Device Management
http://images.apple.com/iphone/business/docs/iOS_MDM.pdf

Mobile Device Management in iOS
http://www.apple.com/iphone/business/integration/mdm/