Security Benchmarks™
A DIVISION OF CENTER FOR INTERNET SECURITY

CIS Apple iOS 7 Benchmark

v1.0.0 - 09-29-2013

The CIS Security Benchmarks division provides consensus-oriented information security products, services, tools, metrics, suggestions, and recommendations (the "SB Products") as a public service to Internet users worldwide. Downloading or using SB Products in any way signifies and confirms your acceptance of and your binding agreement to these CIS Security Benchmarks Terms of Use.

CIS SECURITY BENCHMARKS TERMS OF USE

BOTH CIS SECURITY BENCHMARKS DIVISION MEMBERS AND NON-MEMBERS MAY:

- Download, install, and use each of the SB Products on a single computer, and/or
- Print one or more copies of any SB Product that is in a .txt, .pdf, .doc, .mcw, or .rtf format, but only if each such copy is printed in its entirety and is kept intact, including without limitation the text of these CIS Security Benchmarks Terms of Use.

UNDER THE FOLLOWING TERMS AND CONDITIONS:

- **SB Products Provided As Is**. CIS is providing the SB Products "as is" and "as available" without: (1) any representations, warranties, or covenants of any kind whatsoever (including the absence of any warranty regarding: (a) the effect or lack of effect of any SB Product on the operation or the security of any network, system, software, hardware, or any component of any of them, and (b) the accuracy, utility, reliability, timeliness, or completeness of any SB Product); or (2) the responsibility to make or notify you of any corrections, updates, upgrades, or fixes.
- **Intellectual Property and Rights Reserved**. You are not acquiring any title or ownership rights in or to any SB Product, and full title and all ownership rights to the SB Products remain the exclusive property of CIS. All rights to the SB Products not expressly granted in these Terms of Use are hereby reserved.
- **Restrictions**. You acknowledge and agree that you may not: (1) decompile, dis-assemble, alter, reverse engineer, or otherwise attempt to derive the source code for any software SB Product that is not already in the form of source code; (2) distribute, redistribute, sell, rent, lease, sublicense or otherwise transfer or exploit any rights to any SB Product in any way or for any purpose; (3) post any SB Product on any website, bulletin board, ftp server, newsgroup, or other similar mechanism or device; (4) remove from or alter these CIS Security Benchmarks Terms of Use on any SB Product; (5) remove or alter any proprietary notices on any SB Product; (6) use any SB Product or any component of an SB Product with any derivative works based directly on an SB Product or any component of an SB Product; (7) use any SB Product or any component of an SB Product with other products or applications that are directly and specifically dependent on such SB Product or any component for any part of their functionality; (8) represent or claim a particular level of compliance or consistency with any SB Product; or (9) facilitate or otherwise aid other individuals or entities in violating these CIS Security Benchmarks Terms of Use.
- **Your Responsibility to Evaluate Risks**. You acknowledge and agree that: (1) no network, system, device, hardware, software, or component can be made fully secure; (2) you have the sole responsibility to evaluate the risks and benefits of the SB Products to your particular circumstances and requirements; and (3) CIS is not assuming any of the liabilities associated with your use of any or all of the SB Products.
- **CIS Liability**. You acknowledge and agree that neither CIS nor any of its employees, officers, directors, agents or other service providers has or will have any liability to you whatsoever (whether based in contract, tort, strict liability or otherwise) for any direct, indirect, incidental, consequential, or special damages that arise out of or are connected in any way with your use of any SB Product.
- **Indemnification**. You agree to indemnify, defend, and hold CIS and all of CIS's employees, officers, directors, agents and other service providers harmless from and against any liabilities, costs and expenses incurred by any of them in connection with your violation of these CIS Security Benchmarks Terms of Use.
- **Jurisdiction**. You acknowledge and agree that: (1) these CIS Security Benchmarks Terms of Use will be governed by and construed in accordance with the laws of the State of Maryland; (2) any action at law or in equity arising out of or relating to these CIS Security Benchmarks Terms of Use shall be filed only in the courts located in the State of Maryland; and (3) you hereby consent and submit to the personal jurisdiction of such courts for the purposes of litigating any such action.
- **U.S. Export Control and Sanctions laws**. Regarding your use of the SB Products with any non-U.S. entity or country, you acknowledge that it is your responsibility to understand and abide by all U.S. sanctions and export control laws as set from time to time by the U.S. Bureau of Industry and Security (BIS) and the U.S. Office of Foreign Assets Control (OFAC).

SPECIAL RULES FOR CIS MEMBER ORGANIZATIONS: CIS reserves the right to create special rules for: (1) CIS Members; and (2) Non-Member organizations and individuals with which CIS has a written contractual relationship. CIS hereby grants to each CIS Member Organization in good standing the right to distribute the SB Products within such Member's own organization, whether by manual or electronic means. Each such Member Organization acknowledges and agrees that the foregoing grants in this paragraph are subject to the terms of such Member's membership arrangement with CIS and may, therefore, be modified or terminated by CIS at any time.

Table of Contents

Overview

This document, *Security Configuration Benchmark for Apple iOS 7*, provides prescriptive guidance for establishing a secure configuration posture for the Apple iOS version 7.0.2. This guide was tested against the Apple iOS 7.0.2 and the iPhone Configuration Utility (iPCU) v3.6.2.300. This benchmark covers the Apple iOS 7.0.2 and all hardware devices on which this iOS is supported. As of the publication of this guidance, mobile devices supported by iOS 7.0.2 include the following:

- iPhone 5S
- iPhone 5C
- iPhone 5
- iPhone 4S
- iPhone 4
- iPad with Retina display
- iPad Mini
- iPad 2
- iPod Touch (5th 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://benchmarks.cisecurity.org. If you have questions, comments, or have identified ways to improve this guide, please write us at 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 7.0.2.

Consensus Guidance

This benchmark was created using a consensus review process comprised 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 published. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in the benchmark. If you are interested in participating in the consensus process, please visit https://community.cisecurity.org.

Typographical 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

Scoring Information

A scoring status indicates whether compliance with the given recommendation impacts the assessed target's benchmark score. The following scoring statuses are used in this benchmark:

Scored
Failure to comply with "Scored" recommendations will decrease the final benchmark score. Compliance with "Scored" recommendations will increase the final benchmark score.

Not Scored
Failure to comply with "Not Scored" recommendations will not decrease the final benchmark score. Compliance with "Not Scored" recommendations will not increase the final benchmark score.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1 - Apple iOS 7**

  Items in this profile apply to Apple iOS 7 and intend to:

  - Be practical and prudent.
  - Provide a clear security benefit.
  - Not inhibit the utility of the technology beyond acceptable means.
- **Level 2 - Apple iOS 7**

  This profile extends the "Level 1 - Apple iOS 7" profile. Items in this profile exhibit one or more of the following characteristics:

  - Intended for environments or use cases where security is paramount.
  - Act as defense in depth measures.
  - May negatively inhibit the utility or performance of the technology.
- **Level 1 - MS Exchange Server 2010**

  Items in this profile apply to Microsoft Exchange Server 2010 and intend to:

  - Be practical and prudent.
  - Provide a clear security benefit.
  - Not inhibit the utility of the technology beyond acceptable means.
- **Level 2 - MS Exchange Server 2010**

  This profile extends the "Level 1 - MS Exchange Server 2010" profile. Items in this profile exhibit one or more of the following characteristics:

  - Intended for environments or use cases where security is paramount.
  - Act as defense in depth measures.
  - May negatively inhibit the utility or performance of the technology.

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 Skrdla

Contributor
Adrian Sanabria
Brian Reilly
Joe Wulf RHCSA(RHEL6), FITSP-D, CISSP, VCP3, CPO(USN RET), *U.S. National Security Agency*
Richard Tychansky
Roland Grefer
Shawn Geddis
Toon Mordijck
Blake Frantz , *Center for Internet Security*

Editor
David Skrdla
Mike de Libero , *MDE Development, Inc.*

Recommendations

1 User Interface Settings

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 (Not Scored)

Profile Applicability:

- Level 1 - Apple iOS 7

Description:

This control ensures that the device firmware remains current.

Rationale:

Firmware updates often include critical security fixes that reduce the probability of an attacker exploiting the device.

Audit:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `About`.
4. Confirm that "Version" is 7.0.2 or later.

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.

References:

1. iOS: How to update your iPhone, iPad, or iPod touch. Available: http://support.apple.com/kb/HT4623
2. iOS: How to back up and restore your content. Available: http://support.apple.com/kb/HT1766

1.1.2 Enable Passcode Lock (Not Scored)

Profile Applicability:

- Level 1 - Apple iOS 7

Description:

This control determines whether a password is required before allowing access to the device via the touch screen. It is recommended that a password be set.

Rationale:

Requiring a password to unlock the device helps prevent unauthorized access to the device and increases the effort required to use the device or access data stored on it.

Audit:

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

Remediation:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Passcode Lock`.
4. Tap `Turn Passcode On`.

5. Tap in a passcode.
6. Tap `Next`.
7. Tap in the same passcode.
8. Tap `Next`.

1.1.3 Disallow Simple Passcode (Not Scored)

Profile Applicability:

- Level 2 - Apple iOS 7

Description:

This control determines whether passcodes other than 4-digit numbers are permitted for the passcode protecting access to the device via the touch screen. It is recommended that the device be configured to permit the use of passcodes longer than 4 characters and containing alphanumeric characters.

Rationale:

Permitting an alphanumeric password to be configured to unlock the device permits the user to increase the difficulty of determining the password by an attacker seeking unauthorized access.

Audit:

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

Remediation:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Passcode Lock`.
4. Enter current passcode if configured.
5. Turn off Simple Passcode.
6. Enter current password when prompted.
7. Enter new complex passcode when prompted.
8. Tap `Next`.
9. Re-enter new complex passcode when prompted.
10. Tap `Done`.

1.1.4 Set Auto-lock (Not Scored)

Profile Applicability:

- Level 1 - Apple iOS 7

Description:

This control defines the number of minutes the device can be inactive before requiring the password be reentered. The recommended setting is 2 minutes or less.

Rationale:

Automatically locking the device after a short period of inactivity reduces the probability of an attacker accessing the device without entering a password.

Audit:

1. Tap `Settings`.
2. Tap `General`.
3. Review the Auto-lock interval and confirm it is set to 2 minutes or less.

Remediation:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Auto-Lock`.
4. Tap the value to set the Auto-lock interval at `2 Minutes` or less.

1.1.5 Enable Erase Data (Not Scored)

Profile Applicability:

- Level 2 - Apple iOS 7

Description:

This configuration item determines whether the device will automatically wipe its contents after excessive (10) failed passcode attempts. 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 help to ensure the

confidentiality of information stored on the device is protected when facing a novice attacker.

Audit:

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

Remediation:

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

1.1.6 Forget Wi-Fi networks to prevent automatic rejoin (Not Scored)

Profile Applicability:

- Level 2 - Apple iOS 7

Description:

This configuration causes an iOS device to forget Wi-Fi networks with which it has previously associated. It is recommended that networks be forgotten after each 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 attempt to join it.

Audit:

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

3. From the Choose a Network list or from the active network listing, locate the network SSID to check and tap the Detail Disclosure button next to the Wi-Fi network.
4. Confirm that the network configuration does not have the "Forget this network" option available.

Remediation:

1. Tap `Settings`.
2. Tap `Wi-Fi`.
3. From the Choose a Network list or from the active network listing, locate the network SSID and tap the Detail Disclosure button next to the Wi-Fi network you want to forget (see note below).
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. When this action is taken for an active network SSID, the network connection is disconnected.

1.1.7 Turn off Ask to Join Networks (Not Scored)

Profile Applicability:

- Level 2 - Apple iOS 7

Description:

This option configures the device to look for another network and display a list of all available Wi-Fi networks that the user can choose from when the device is trying to access the Internet and is not in range of a Wi-Fi network it has previously used. It is recommended that "Ask to Join Networks" be turned off.

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").

Audit:

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

Remediation:

1. Tap `Settings`.
2. Tap `Wi-Fi`.
3. Turn off Ask to Join Networks (see note below).

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

1.1.8 Turn off Auto-Join for all Wi-Fi networks (Not Scored)

Profile Applicability:

- Level 2 - Apple iOS 7

Description:

Enabling Wi-Fi Auto-Join for a Wi-Fi network configures the device to remember the network and login information and automatically reconnect to that Wi-Fi network whenever the device is in range. It is recommended that Wi-Fi Auto-Join be turned off for all network connections where security is paramount.

Rationale:

Auto-Join may expose credentials at unexpected times and locations (e.g., if forms-based authentication occurs over unencrypted HTTP, or a spoofed SSID is encountered), and for Wi-Fi networks that require HTTP(S) forms authentication, this feature will cause credentials to persist on disk, potentially placing the confidentiality of the credentials at risk if physical custody of the device is lost.

Audit:

1. Tap `Settings`.
2. Tap `Wi-Fi`.
3. From the Choose a Network list, locate the network SSID and tap the Detail Disclosure button next to the network to review.
4. Confirm that Auto-Join is turned off.
5. Repeat steps 3 and 4 for each network SSID.

Remediation:

1. Tap `Settings`.
2. Tap `Wi-Fi`.
3. From the Choose a Network list, locate the network SSID and tap the Detail Disclosure button next to the network to change.
4. Turn off Auto-Join (see note below).
5. Repeat steps 3 and 4 for each network SSID.

Note: This feature is primarily applicable to the automatic joining of subscription Wi-Fi networks. 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.

References:

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

1.1.9 Turn off Wi-Fi when not needed (Not Scored)

Profile Applicability:

- Level 2 - Apple iOS 7

Description:

This configuration item determines whether the iOS device uses local Wi-Fi networks to connect to the Internet and other networks. It is recommended that Wi-Fi be disabled when not needed or when security is paramount.

Rationale:

Disabling the Wi-Fi interface reduces the remote attack surface of the device.

Audit:

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

Remediation:

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

1.1.10 Turn off VPN when not needed (Not Scored)

Profile Applicability:

- Level 1 - Apple iOS 7

Description:

iOS devices can natively connect to VPNs that use the L2TP over IPSec, 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 device 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.

Audit:

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

Remediation:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN`.
4. Turn off VPN if turned on.

1.1.11 Turn off Bluetooth when not needed (Not Scored)

Profile Applicability:

- Level 1 - Apple iOS 7

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:

Disabling Bluetooth when not needed reduces the remote attack surface of the device and prevents discovery of and connection to Bluetooth services.

Audit:

1. Tap `Settings`.

2. Tap `Bluetooth`.
3. Confirm that Bluetooth is turned off.

Remediation:

1. Tap `Settings`.
2. Tap `Bluetooth`.
3. Turn off Bluetooth.

1.1.12 Turn off Personal Hotspot when not needed (Not Scored)

Profile Applicability:

- Level 2 - Apple iOS 7

Description:

Personal Hotspot allows certain iOS 6 devices with cellular data connections to be configured to share an active Cellular Data connection via Wi-Fi, Bluetooth, or USB (see Note). It is recommended that Personal Hotspot be disabled when not needed or where security is paramount.

Rationale:

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

Audit:

1. Tap `Settings`.
2. Tap `Cellular`.
3. Check if `Personal Hotspot` is present.
   a) If present,
      i. Tap `Personal Hotspot`.
      ii. Confirm that `Personal Hotspot` is turned off.
   b) Alternatively, if `Set Up Personal Hotspot` is present, then Personal Hotspot is not configured.

Note: For devices supporting iOS 7, Personal Hotspot is available only on iPhone models and iPad (3rd generation) Wi-Fi + Cellular or later, and iPad mini Wi-Fi + Cellular. Personal Hotspot sharing via Wi-Fi is available only on iPhone models and iPad (3rd generation) Wi-Fi + Cellular or later, and iPad mini Wi-Fi + Cellular.

Remediation:

1. Tap `Settings`.
2. Tap `Cellular`.
3. Tap `Personal Hotspot`.
4. Turn off Personal Hotspot.

1.1.13 Turn off Location Services (Not Scored)

Profile Applicability:

- Level 2 - Apple iOS 7

Description:

Location Services allows applications such as Maps, Internet, and Camera to gather and use data indicating the user's location. It is recommended that Location Services be disabled in environments where security is paramount.

Rationale:

Disabling location services reduces the capability of an attacker to determine or track the user's location via websites, locally installed applications or other means.

Audit:

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

Remediation:

1. Tap `Settings`.
2. Tap `Privacy`.
3. Tap `Location Services`.
4. Turn off Location Services.
5. Tap `Turn off` on confirmation dialog.

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

1.1.14 Turn on Airplane Mode (Not Scored)

Profile Applicability:

- Level 2 - Apple iOS 7

Description:

Airplane Mode disables all receivers and transceivers on a mobile device. When Airplane Mode is on, no cellular voice, cellular data, 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 when 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.

Audit:

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

Remediation:

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

1.1.15 Erase all data before return, recycle, reassignment, or other disposition (Not Scored)

Profile Applicability:

- Level 1 - Apple iOS 7

Description:

This control effectively erases all data, including accounts, from the device's internal storage by securely discarding the block storage encryption key from Effaceable Storage, rendering all data unreadable. Device contents should be securely erased before the device is placed outside of the owner's control.

Rationale:

In normal operations, deleting data on an iOS device renders it inaccessible through the user interface but the data is not erased from the device. Erasing stored data by securely discarding the block storage encryption key before returning, recycling, disposing of, or otherwise placing a device out of the user's control reduces the probability of an attacker subsequently accessing confidential information previously stored on the device.

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.

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.

References:

1. iPhone and iOS Forensics: Investigation, Analysis and Mobile Security for Apple iPhone, iPad and iOS Devices. Available: http://textbooks.elsevier.com/web/product_details.aspx?isbn=9781597496599

1.1.16 Disable View in Lock Screen for apps when device is locked (Not Scored)

Profile Applicability:

- Level 2 - Apple iOS 7

Description:

This setting prevents notifications from any source from being displayed when the iOS device is passcode locked. 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.

Audit:

1. Tap `Settings`.
2. Tap `Notification Center`.
3. In the ACCESS ON LOCK SCREEN section, confirm that Notifications View is turned off.

4. From the list of notification sources listed in the Notification Center, locate the app or other notification source and tap the chevron next to the source to review.
5. Confirm that Show on Lock Screen is turned off.
6. Repeat steps 4 and 5 for each source.

Remediation:

1. Tap `Settings`.
2. Tap `Notification Center`.
3. In the ACCESS ON LOCK SCREEN section, turn off "Notifications View".
4. From the list of notification sources listed in the Notifications Center, locate the app or other notification source and tap the chevron next to the source to change.
5. Turn off Show on Lock Screen.
6. Repeat steps 4 and 5 for each source.

Note: The notification sources will be grouped based on whether notifications are included or excluded from the Notifications View. Apps enabled for Notification Center will be listed in the section ”INCLUDE” and apps disabled for Notification Center will be listed in the section “DO NOT INCLUDE”. Apps for which Show on Lock Screen is disabled will not independently show notifications in the lock screen. Apps for which "Show in Notification Center" is enabled will not show notifications via the Notification Center in the lock screen only if the Notifications View setting of the Notification Center is turned off.

1.1.17 Enable Automatic Downloads of App Updates (Not Scored)

Profile Applicability:

- Level 1 - Apple iOS 7

Description:

This control ensures that the application software remains current via automatic download and installation of app updates over-the-air.

Rationale:

App updates often include critical security fixes that reduce the probability of an attacker exploiting vulnerabilities in apps.

Audit:

1. Tap `Settings`.
2. Tap `iTunes & App Store`.
3. Confirm that Updates is turned on in the Automatic Downloads configuration list.

Remediation:

1. Tap `Settings`.
2. Tap `iTunes & App Store`.
3. Turn on Updates in the Automatic Downloads configuration list.

1.1.18 Turn Off AirDrop Discoverability (Not Scored)

Profile Applicability:

- Level 2 - Apple iOS 7

Description:

This setting keeps your device from being discoverable to everyone, including contacts.

Rationale:

Turning off AirDrop discoverability prevents the device from making itself discoverable to other devices for AirDrop functionality. It is recommended to restrict device discoverability when this functionality is not needed.

Audit:

1. Swipe up from the bottom of the iOS 7 screen to display the Control Center.
2. Confirm that the text next to the AirDrop symbol states simply "AirDrop" (and not AirDrop: Everyone or AirDrop: Contacts Only).

Remediation:

1. Swipe up from the bottom of the iOS 7 screen to display the Control Center.
2. Tap the AirDrop field at the bottom of the Control Center panel.
3. Tap `Off` on the menu dialog.

1.1.19 Disable Passcode Unlock for Fingerprints (Not Scored)

Profile Applicability:

- Level 2 - Apple iOS 7

Description:

Touch ID allows use of one or more fingerprints as a passcode, through touching the Home button allowing the Touch ID sensor to read a fingerprint and automatically unlocking the phone.

Rationale:

Disabling Passcode Unlock for Fingerprints can help avoid exposure to risk of unauthorized successful authentication via TouchID, by false positive or by intentional attacks (e.g., making use of latent fingerprints).

Platform: This configuration item applies to the iPhone 5S platform only.

Audit:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Passcode & Fingerprint`.
4. Tap `Fingerprint`.
5. Confirm that Passcode Unlock is turned off for the Fingerprints setting.

Remediation:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Passcode & Fingerprint`.
4. Tap `Fingerprint`.
5. Turn off Passcode Unlock for the Fingerprints setting.

1.1.20 Disable Access to Control Center on Lock Screen (Not Scored)

Profile Applicability:

- Level 2 - Apple iOS 7

Description:

This control disables access to the Control Center on the Lock Screen.

Rationale:

Disabling access to the Control Center on the Lock Screen can potentially mitigate future variations of iOS lock screen bypass exploits that may be possible for attacker who have gained physical access to the device.

Audit:

1. Tap `Settings`.
2. Tap `Control Center`.
3. Confirm that Access on Lock Screen is turned off.

Remediation:

1. Tap `Settings`.
2. Tap `Control Center`.
3. Turn off Access on Lock Screen.

1.1.21 Enable Find My iPhone (Not Scored)

Profile Applicability:

- Level 2 - Apple iOS 7

Description:

This control enables the remote tracking, remote wiping, remote custom message display, and Activation Lock features of the iOS device.

Rationale:

Enabling Find my iPhone in iOS 7 enables the abilities both to locate the device via the Find My iPhone iCloud application or iOS app and to display a custom message with phone number on the Lock screen, as well as prevents the taking of key actions with the iOS device without the entry of the associated Apple ID password, including preventing the erasure of device content and settings from the device via the Settings app, and the restoring of the device, through the Activation Lock feature.

Audit:

1. Tap `Settings`.
2. Tap `iCloud`.
3. Confirm that Find My iPhone is turned on.

Remediation:

1. Tap `Settings`.
2. Tap `iCloud`.
3. Turn on Find My iPhone.
4. Tap `OK` on confirmation dialog.

References:

1. Find My iPhone, iPad and Mac. Available: http://www.apple.com/icloud/find-my-iphone.html
2. iCloud: Find My iPhone Activation Lock in iOS 7. Available: http://support.apple.com/kb/ht5818

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 (Not Scored)

Profile Applicability:

- Level 2 - Apple iOS 7

Description:

This control disables JavaScript functionality which 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.

Audit:

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

Remediation:

1. Tap `Settings`.
2. Tap `Safari`.
3. Tap `Advanced`.
4. Turn off JavaScript.

1.2.2 Enable Fraudulent Website Warning (Not Scored)

Profile Applicability:

- Level 1 - Apple iOS 7

Description:

Enabling Fraudulent Website Warning configures Safari to display a warning and prevent the loading of the page when an attempt is made to visit a potentially fraudulent Internet site. It is recommended that the Fraudulent Website 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.

Audit:

1. Tap `Settings`.
2. Tap `Safari`.
3. Confirm that Fraudulent Website Warning is turned on.

Remediation:

1. Tap `Settings`.
2. Tap `Safari`.
3. Turn on Fraudulent Website Warning.

1.2.3 Disable Auto Fill for Contact Information (Not Scored)

Profile Applicability:

- Level 2 - Apple iOS 7

Description:

Auto Fill configures the browser to remember information entered into common forms in order to automate the completion of later forms.

Rationale:

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

Audit:

1. Tap `Settings`.
2. Tap `Safari`.
3. Tap `Passwords & AutoFill`.
4. Confirm that AutoFill is turned off for the "Use Contact Info" setting.

Remediation:

1. Tap `Settings`.
2. Tap `Safari`.
3. Tap `Passwords & AutoFill`.
4. Turn off AutoFill for the "Use Contact Info" setting.

1.2.4 Turn On Private Browsing When Needed (Not Scored)

Profile Applicability:

- Level 2 - Apple iOS 7

Description:

Enabling Private Browsing for a browser session prevents tracking of history of web pages visited, searches performed, and (if configured) certain AutoFill information.

Rationale:

Enabling Private Browsing can protect certain private information and block some websites from tracking browser activity.

Audit:

1. Tap the Safari app to launch it.
2. Observe if the top and bottom Safari menu bars are dark gray instead of the usual white color.
3. Tap the Safari tab button at the lower right of the screen.
4. Observe if the Private text button is surrounded by a gray background.

Remediation:

1. Tap the Safari app to launch it.
2. Tap the Safari tab button at the lower right of the screen.
3. Tap `Private`.
4. Select "Close All" or "Keep All" on the "Close All Pages?" dialog box.

1.2.5 Disable Auto Fill for Names and Passwords (Not Scored)

Profile Applicability:

- Level 2 - Apple iOS 7

Description:

Auto Fill configures the browser to remember information entered into common forms in order to automate the completion of later forms.

Rationale:

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

Audit:

1. Tap `Settings`.
2. Tap `Safari`.
3. Tap `Passwords & AutoFill`.
4. Confirm that AutoFill is turned off for the "Names and Passwords" item.

Remediation:

1. Tap `Settings`.
2. Tap `Safari`.
3. Tap `Passwords & AutoFill`.
4. Turn off AutoFill for the "Names and Passwords" item.

1.2.6 Disable Auto Fill for Credit Card Information (Not Scored)

Profile Applicability:

- Level 2 - Apple iOS 7

Description:

Auto Fill configures the browser to remember information entered into common forms in order to automate the completion of later forms.

Rationale:

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

Audit:

1. Tap `Settings`.
2. Tap `Safari`.
3. Tap `Passwords & AutoFill`.

4. Confirm that AutoFill is turned off for the "Credit Cards" setting.

Remediation:

1. Tap `Settings`.
2. Tap `Safari`.
3. Tap `Passwords & AutoFill`.
4. Turn off AutoFill for the "Credit Cards" setting.

2 iPhone Configuration Utility Settings

This section provides guidance on the secure configuration of iOS mobile devices with the iPhone Configuration Utility (iPCU), version 3.6.2.300. 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 Set Security to disallow profile removal (Scored)

Profile Applicability:

- Level 1 - Apple iOS 7

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.

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.

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.

2.2 Passcode Settings

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

2.2.1 Require passcode on device (Scored)

Profile Applicability:

- Level 1 - Apple iOS 7

Description:

This control determines whether a password is required before allowing access to the device via the touch screen.

Rationale:

Requiring a password to unlock the device helps prevent unauthorized access to the device and increases the effort required to use the device or access data stored on it.

Audit:

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

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.

2.2.2 Require alphanumeric value (Scored)

Profile Applicability:

- Level 2 - Apple iOS 7

Description:

This control determines whether alphanumeric characters (alphabetic and non-alphanumeric values in addition to numerals) are required for the passcode that protects access to the device via the touch screen.

Rationale:

Requiring a mix of alphabetical and numerical characters increases the complexity of the passcode and therefore the difficulty of determining the password by an attacker seeking unauthorized access.

Audit:

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

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.

2.2.3 Set minimum passcode length (Scored)

Profile Applicability:

- Level 1 - Apple iOS 7

Description:

This control specifies the minimum number of characters a passcode can contain. 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.

Audit:

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

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.

2.2.4 Set Minimum number of complex characters (Scored)

Profile Applicability:

- Level 2 - Apple iOS 7

Description:

This configuration item specifies the minimum number of non-alphanumeric characters (such as $, &, and !) that the passcode must contain. It is recommended that at least one non-alphanumeric character be required 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.

Audit:

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

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.

References:

1. NIST Special Publication (SP) 800-63-2, Electronic Authentication Guideline. Available: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf

2.2.5 Set Maximum Auto-lock (Scored)

Profile Applicability:

- Level 1 - Apple iOS 7

Description:

This control defines the number of minutes the device can be inactive before requiring the password be reentered. It is recommended that an inactivity timeout of no more than two (2) minutes be set.

Rationale:

Automatically locking the device after a short period of inactivity reduces the probability of an attacker accessing the device without entering a password.

Audit:

1. Open the configuration profile XML file.
2. Search for `<key>maxInactivity</key>`.
3. Review the configured Auto-lock interval to observe if the next line is `<integer>2</integer>` or less.

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 Auto-lock` drop-down menu in the lower right windowpane.
5. Select the number `2` or less to set the Auto-lock interval.
6. Install the configuration profile on the device.

2.2.6 Set Maximum number of failed attempts (Scored)

Profile Applicability:

- Level 1 - Apple iOS 7

Description:

This setting determines how many failed passcode attempts can be made before the device is wiped (configurable from 4 to 10).

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 help to ensure the confidentiality of information stored on the device is protected when facing a novice attacker.

Audit:

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

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.

2.2.7 Do Not Allow Simple Value (Not Scored)

Profile Applicability:

- Level 1 - Apple iOS 7

Description:

iOS devices can be configured via the iPCU to check passwords upon entry to disallow the use of repeating, ascending, and/or descending character sequences. By default, simple passcode values are permitted and checks for repeating, ascending, and descending character sequences are not performed. It is recommended that such sequences be disallowed for the passcode.

Rationale:

Simple passcodes such as those with repeating, ascending, or descending character sequences are easily guessed. Preventing the selection of passwords containing such sequences increases the complexity of the passcode and reduces the ease with which an attacker may attempt to guess the passcode in order to gain access to the device.

Audit:

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

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 to remove the `Allow simple value` checkbox in the lower right windowpane.
5. Install the configuration profile on the device.

2.3 Mail Settings

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

2.3.1 Enable Prevent Move for Sensitive Mail Accounts (Not Scored)

Profile Applicability:

- Level 2 - Apple iOS 7

Description:

This control determines whether a message can be moved from one mail account configured on the device to another account.

Rationale:

Permitting the movement of messages from one account to another intentionally or unintentionally can result in the exfiltration or loss of data from sensitive mail systems.

Audit:

1. Open the configuration profile XML file.
2. Search for `<string>MailAccountName</string>` where *MailAccountName* is the name of the mail account for which this restriction needs to be made, to locate the XML element for the configuration item.
3. Locate the child element `<key>PreventMove</key>`.
4. Observe if the next line is `<true/>`.
5. Repeat steps 2 through 4 for each mail account requiring this restriction.

Remediation:

1. Open iPCU.
2. Click on `Configuration Profiles` in the left windowpane.
3. Click on the `Mail` option from the payloads list in the lower right windowpane.
4. In the lower right windowpane, locate the mail account to configure.
5. Click to remove the `Allow Move` checkbox for the mail account.
6. Repeat steps 4 and 5 for each mail account requiring this restriction.
7. Install the configuration profile on the device.

2.3.2 Require Use Only in Mail for Sensitive Mail Accounts (Not Scored)

Profile Applicability:

- Level 2 - Apple iOS 7

Description:

This control determines whether a mail account can be used for sending messages from iOS apps other than the Mail app.

Rationale:

Permitting apps other than the Mail app to send messages from a mail account can limit an organization's ability to tightly control against the exfiltration or loss of sensitive data from an iOS device.

Audit:

1. Open the configuration profile XML file.

2. Search for `<string>MailAccountName</string>` where *MailAccountName* is the name of the mail account for which this restriction needs to be made, to locate the XML element for the configuration item.
3. Locate the child element `<key>PreventAppSheet</key>`.
4. Observe if the next line is `<true/>`.
5. Repeat steps 2 through 4 for each mail account requiring this restriction.

Remediation:

1. Open iPCU.
2. Click on `Configuration Profiles` in the left windowpane.
3. Click on the `Mail` option from the payloads list in the lower right windowpane.
4. In the lower right windowpane, locate the mail account to configure.
5. Tap the `Outgoing Mail` tab for the mail account.
6. Tap to check the `Use Only in Mail` checkbox for the mail account.
7. Repeat steps 4 through 6 for each mail account requiring this restriction.
8. Install the configuration profile on the device.

3 Microsoft Exchange ActiveSync Policy Settings

This section provides recommendations to securely configure and enforce Microsoft Exchange Server 2010, ActiveSync Mailbox policies for mobile devices managed by the server.

Please note the device supports adding multiple accounts and syncing information from multiple Exchange servers as well as other types of email accounts. Each of these accounts may have security policies that are enforced per account setup on the device. If accounts have conflicting security policy settings then the device enforces the strictest rules set by any account for each kind of policy. No account policy can relax the degree of security set by another account policy.

For more information about Microsoft Exchange Information Services and security policies supported see: http://en.wikipedia.org/wiki/Comparison_of_Exchange_ActiveSync_clients

3.1 Password Settings

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

Reference:

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

3.1.1 Enable 'Require password' (Scored)

Profile Applicability:

- Level 1 - MS Exchange Server 2010

Description:

This control determines whether a password is required before allowing access to the device via the touch screen. 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 password be set.

Rationale:

Requiring a password to unlock the device increases the effort required to use the device or access data stored on it.

Audit:

Using the Exchange Management Console (EMC):

In the "Properties" configuration window,

1. Click on the `Password` tab.
2. Observe if the `Require password` 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 policy setting output 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.

Remediation:

Using the Exchange Management Console (EMC):

In the "Properties" configuration window,

1. Click on the `Password` tab.
2. Click on the `Require password` 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).

References:

1. CIS Security Configuration Benchmark for Microsoft Exchange Server 2007, version 1.1.0, Section 8.16: Require ActiveSync Password.
2. Microsoft Technet Library Article: Configure Device Password Locking: http://technet.microsoft.com/en-us/library/bb125004.aspx

3.1.2 Enable 'Require alphanumeric value' (Scored)

Profile Applicability:

- Level 2 - MS Exchange Server 2010

Description:

This control determines if new passwords are required to satisfy a certain level of complexity. 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. The recommended settings are enable alpha-numeric device password.

Rationale:

Enforcing password complexity requirements reduces the probability of an attacker determining a valid credential.

Audit:

Using the Exchange Management Console (EMC):

In the "Properties" configuration window,

1. Click on the `Password` tab.
2. Observe if the `Require alphanumeric password` check box 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.

Remediation:

Using the Exchange Management Console (EMC):

In the "Properties" configuration window,

1. Click on the `Password` tab.
2. Click on the `Require alphanumeric password` check box
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).

References:

1. CIS Security Configuration Benchmark for Microsoft Exchange Server 2007, version 1.1.0, Section 8.17: Require ActiveSync Alphanumeric Password
2. Microsoft Technet Library Article: Configure Device Password Locking: http://technet.microsoft.com/en-us/library/bb125004.aspx

3.1.3 Set the 'minimum password length' (Scored)

Profile Applicability:

- Level 1 - MS Exchange Server 2010

Description:

This control defines the minimum number of characters a user password must contain. 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. The recommended setting is 5 or more characters.

Rationale:

Enforcing a minimum password length helps protect against brute force and dictionary attacks, and increases the efficacy of password-based authentication systems. 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 password.

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 or more characters`.
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 policy setting output 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.

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` or more 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).

References:

1. CIS Security Configuration Benchmark for Microsoft Exchange Server 2007, version 1.1.0, Section 8.18: Require ActiveSync Minimum Password Length
2. Microsoft Technet Library Article: Configure Device Password Locking: http://technet.microsoft.com/en-us/library/bb125004.aspx

3.1.4 Set the 'minimum number of character sets' (Scored)

Profile Applicability:

- Level 2 - MS Exchange Server 2010

Description:

This control determines if new passwords are required to satisfy a certain level of complexity. By default, iOS devices do not require such 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). The recommended setting is the minimum device password complexity is set to 1 or more characters.

Note: iOS devices implement the MinDeviceComplexCharacters configuration items as the number of special characters required in a passcode. This is an important distinction from some non-iOS EAS profile setting implementations in which this value specifies the number of character groups that are required to be present in the password (e.g., lower case alphabetical characters, upper case alphabetical characters, numerals, and non-alphanumeric characters; see MSDN Library topic on 2.2.2.36

MinDevicePasswordComplexCharacters at http://msdn.microsoft.com/en-us/library/ee201726%28v=exchg.80%29.aspx).

Rationale:

Enforcing password complexity requirements reduces the probability of an attacker determining a valid credential.

Audit:

Using the Exchange Management Console (EMC):

In the "Properties" configuration window,

1. Click on the `Password` tab.
2. Observe if the "Minimum number of complex characters" value is set to 1.
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 `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. Exit the Exchange Management Shell.

Remediation:

Using the Exchange Management Console (EMC):

In the Properties configuration window,

1. Click on the `Password` tab.
2. The `Require alphanumeric passcode` check box should be checked (per 3.1.2). When this check box is checked, you may enter the `Minimum number of complex characters` in the box on the right hand side.
3. Enter the number `1` or more 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>"
 -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).

References:

1. CIS Security Configuration Benchmark for Microsoft Exchange Server 2007, version 1.1.0, Section 8.17: Require ActiveSync Alphanumeric Password

3.1.5 Set the 'timeout' for 'Time without user input before password must be re-entered (in minutes)' (Scored)

Profile Applicability:

- Level 1 - MS Exchange Server 2010

Description:

This control defines the number of minutes the device can be inactive before requiring the password be reentered. 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. The recommended setting is 2 minutes or less.

Rationale:

Automatically locking the device after a short period of inactivity reduces the probability of an attacker accessing the device without entering a password.

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)` check box is selected.
3. Observe if the auto-lock timeout value is set to 2 or less minutes.
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 policy setting output for the "MaxInactivityTimeDeviceLock"configuration item.
3. Observe if there is a value following the colon and that the value is set to 2 or less as shown below:

```
MaxInactivityTimeDeviceLock : 2
```

4. Exit the Exchange Management Shell.

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)` check box. When this check box 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 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: 00:02:00
```

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.

References:

1. CIS Security Configuration Benchmark for Microsoft Exchange Server 2007, version 1.1.0, Section 8.26: Require ActiveSync Inactivity Lockout Time
2. Microsoft Technet Library Article: Configure Device Password Locking http://technet.microsoft.com/en-us/library/bb125004.aspx

3.1.6 Limit the 'Number of failed attempts allowed' (Scored)

Profile Applicability:

- Level 1 - MS Exchange Server 2010

Description:

If the password setting is enabled then this control defines the number of failed login attempts before all information stored on the device is deleted and the device is automatically reset to original factory settings. 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. The recommended setting is 6 or less failed attempts.

Rationale:

If the password setting is enabled then enforcing an account lockout threshold deletes data stored on the device reducing the probability of an attacker accessing confidential information stored on a lost or stolen device.

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:` check box is selected.
3. Observe if the failed attempts value is set to 6 or less failed login attempts.
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 policy setting output for the `MaxDevicePasswordFailedAttempts` configuration item.
3. Observe if there is a value following the colon and that the value is set to 6 or less as shown below:

```
MaxDevicePasswordFailedAttempts : 6
```

4. Exit the Exchange Management Shell.

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`: check box. When this check box is checked, you may enter the maximum number of failed attempts in the box on the right hand side.
3. Enter the number `6` or less 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).

References:

1. CIS Security Configuration Benchmark for Microsoft Exchange Server 2007, version 1.1.0, Section 8.24: Require ActiveSync Maximum Password Attempts
2. Microsoft Technet Library Article: Configure Device Password Locking http://technet.microsoft.com/en-us/library/bb125004.aspx

Appendix: Change History

Date	Version	Changes for this version
09-10-2013	1.0.0	Initial release.