Security Benchmarks™

A DIVISION OF CENTER FOR INTERNET SECURITY

CIS Google Android 4 Benchmark

v1.0.0

Export Date 10-01-2012

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 Android 4.0, provides prescriptive guidance for establishing a secure configuration posture for the Android 4.0 OS. This guide was tested against the Android 4.0 and the Android Virtual Device (AVD) contained in version 4.0.3 of the Android Software Development Kit (SDK). This benchmark covers Android 4.0 and all hardware devices on which this OS is supported. As of the publication of this guidance, mobile devices supported by Android 4.0 include the following:

- HTC One S (T-Mobile)
- HTC One X (AT&T)
- HTC EVO 4G LTE (Sprint)
- HTC Vivid (AT&T)
- HTC Amaze 4G (T-Mobile)
- HTC Sensation 4G (T-Mobile)
- Samsung Galaxy Nexus (Verizon, Sprint)
- Samsung Nexus S 4G (AT&T, Sprint)

In determining recommendations, the current guidance treats all Android 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. 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.

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

The recommendations do not assert sufficient protections against advanced local attacks to gain device access or data recovery that may be possible in the event a device is lost. They also do not discuss custom ROMs or 3rd-party features such as virus or root-kit detection.

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 use Android 4.

Consensus Guidance

This benchmark 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 benchmark. If you are interested in participating in the consensus review process, please send us a note to feedback@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 – Google Android 4**

  Items in this profile intend to:

  - be practical and prudent;
  - provide a clear security benefit; and
  - not negatively inhibit the utility of the technology beyond acceptable means.
- **Level 2 – Google Android 4**

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

  - are intended for environments or use cases where security is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.
- **Level 1 - MS Exchange Server 2010**

  Items in this profile intend to:

  - be practical and prudent;
  - provide a clear security benefit; and
  - not negatively inhibit the utility of the technology beyond acceptable means.
- **Level 2 - MS Exchange Server 2010**

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

  - are intended for environments or use cases where security is paramount.
  - acts as defense in depth measure.
  - 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
Robert Fritz

Contributor
Billy Glenn, *Pacific Gas & Electric*
Fernando Trias
John Fox
Jonathan Trull, *State of Colorado*
Yves Desharnais
Jiyoung Shin
Jeff Saxton, *IBM*

Editor
David Skrdla, *University of Oklahoma*

Recommendations

1 User Interface Settings

This section provides guidance for securing the mobile device configuration 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

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 remotely exploiting the device.

Audit:

1. Press the Menu button.
2. Tap `System Settings`.
3. Scroll down to the `System` section.
4. Tap `About Phone`.
5. Confirm that `Android version` is 4.0 or later.

Remediation:

Contact your telecommunications provider for their latest supported update.

References:

1. Android 4.0 User Guide https://docs.google.com/open?id=0BzJ3Uh61kQ8XX283eDd1MDVKbzg

1.1.2 Enable 'Password' (Not Scored)

Profile Applicability:

- Level 1

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 increases the effort required to use the device or access data stored on it.

Audit:

1. Press the Menu button.
2. Tap `System Settings`.
3. Scroll to `Personal` section.
4. Tap `Security`.
5. Verify `Screen lock` says "Secured with password."
6. Verify `Automatically lock` says "5 seconds after sleep."
7. Verify box for `Power button instantly locks` is checked.

Remediation:

1. Press the Menu button.
2. Tap `System Settings`.
3. Scroll to `Personal` section.
4. Tap `Security`.
5. Tap `Screen Lock`.
6. Tap `Password`.
7. Tap in a complex password.
8. Tap `Continue`.
9. Tap in the same complex password.
10. Tap `OK`.
11. Tap `Automatically lock`.
12. Tap `5 seconds`.
13. Tap `Power button instantly locks` if box is not checked.

References:

1. Android 4.0 User Guide https://docs.google.com/open?id=0BzJ3Uh61kQ8XX283eDd1MDVKbzg
2. The Simplest Security: A Guide To Better Password Practices: http://www.symantec.com/connect/articles/simplest-security-guide-better-password-practices

1.1.3 Enable 'Require alphanumeric value' (Not Scored)

Profile Applicability:

- Level 2

Description:

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

Rationale:

Requiring an alphanumeric password to unlock the device increases the difficulty of determining the password by an attacker seeking unauthorized access.

Audit:

N/A--the Android 4 UI does not provide a mechanism to determine whether a configured password is alphanumeric.

Remediation:

See 1.1.2 above.

1.1.4 Set 'timeout in minutes' for 'Sleep' (Not Scored)

Profile Applicability:

- Level 1

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. Press the Menu button.
2. Tap `System Settings`.

3. Scroll to `Personal` section.
4. Tap `Security`.
5. Confirm that `Automatically lock` is set to "2 minutes after sleep."
6. Press the Back button
7. Scroll to the `Device` section.
8. Tap `Display`.
9. Confirm that `Sleep` is set to "After 2 minutes of inactivity"

Remediation:

1. Press the Menu button.
2. Tap `System Settings`.
3. Scroll to the `Device` section.
4. Tap `Display`.
5. Tap `Sleep`.
6. Tap `2 minutes`.
7. Press the Back button
8. Scroll to `Personal` section.
9. Tap `Security`.
10. Confirm that `Automatically lock` is set to "2 minutes after sleep."

References:

1. Android 4.0 User Guide https://docs.google.com/open?id=0BzJ3Uh61kQ8XX283eDd1MDVKbzg

1.1.5 Remove Entries in 'Wi-Fi' (Not Scored)

Profile Applicability:

- Level 2

Description:

This control determines whether the device will forget Wi-Fi networks with which it has previously associated. It is recommended that networks be forgotten after use in use.

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 device will encounter an untrusted instance of a same-named Wi-Fi network and automatically join it. During test, a 2.1 device did not automatically rejoin an unauthenticated network with the same SSID as a previously-stored authenticated network. However, this behavior should not be assumed.

Audit:

1. Press the Menu button.
2. Tap `System settings`.
3. Scroll to Wireless & networks.
4. Tap `More...` if present
5. Tap `Wi-Fi`.
6. Confirm that all deleted Wi-Fi networks are forgotten.

Remediation:

1. Press the Menu button.
2. Tap `System settings`.
3. Scroll to Wireless & networks.
4. Tap `More...` if present
5. Tap `Wi-Fi`.
6. In the Wi-Fi settings, locate the network SSID and tap and hold down the entry for the network you wish to forget.
7. Tap `Forget`.

Note: Wi-Fi must be turned onto see the list of available networks to configure. The Wi-Fi network must be remembered or currently connected to "Forget" a network.

References:

1. Android 4.0 User Guide https://docs.google.com/open?id=0BzJ3Uh61kQ8XX283eDd1MDVKbzg

1.1.6 Disable 'Network Notification' (Not Scored)

Profile Applicability:

- Level 1

Description:

When the user is trying to access the Internet, by using the built-in browser 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. When selected and a new network is available, an icon will appear on the status bar, which in turn makes available a list of available networks from which the user can choose. If "Network notification" 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" vs. "default").

Audit:

1. Press the Menu button.
2. Tap `System settings`.
3. Tap `More...` if present
4. Tap `Wi-Fi Settings`.
5. Tap the Menu icon and choose `Advanced`.
6. Confirm that `Network notification` is unchecked.

Remediation:

1. Press the Menu button.
2. Tap `System settings`.
3. Tap `More...` if present
4. Tap `Wi-Fi Settings`.
5. Tap the Menu icon and choose `Advanced`.
6. Uncheck `Network notification`.

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

References:

1. Android 4.0 User Guide https://docs.google.com/open?id=0BzJ3Uh61kQ8XX283eDd1MDVKbzg

1.1.7 Disable 'Wi-Fi' (Not Scored)

Profile Applicability:

- Level 2

Description:

The device 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 the built-in Android browser, Gmail, Google Voice, Maps, News & Weather, and the Android Market 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.

Audit:

1. Press the Menu button.
2. Tap `System settings`.
3. Tap `Wireless & networks`.
4. Tap `More`.
5. Tap `Wi-Fi`.
6. Verify that the Wi-Fi switch is in the Off position.

Remediation:

1. Press the Menu button.
2. Tap `System settings`.
3. Tap `Wireless & networks`.
4. Tap `More`.
5. Tap `Wi-Fi`.
6. Slide the Wi-Fi switch to the Off position.

References:

1. Android 4.0 User Guide https://docs.google.com/open?id=0BzJ3Uh61kQ8XX283eDd1MDVKbzg

1.1.8 Disable 'Bluetooth' (Not Scored)

Profile Applicability:

- Level 1

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.

Audit:

1. Press the Menu button.
2. Tap `System settings`.
3. Scroll to `Wireless & networks`.
4. Confirm that the Bluetooth switch is Off.

Remediation:

1. Press the Menu button.
2. Tap `System settings`.
3. Scroll to `Wireless & networks`.
4. Slide the Bluetooth switch to Off.

References:

1. Android 4.0 User Guide https://docs.google.com/open?id=0BzJ3Uh61kQ8XX283eDd1MDVKbzg

1.1.9 Disable 'Location Services' (Not Scored)

Profile Applicability:

- Level 2

Description:

Location Services allows applications such as Maps and Internet websites 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 when not required.

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 the globe Browser icon.
2. Press the Menu button.
3. Tap `Settings`.
4. Tap `Privacy & security`.
5. Scroll to `Location`
6. Confirm `Enable location` is unchecked.
7. Press the Home button.
8. Press the Menu button.
9. Tap `System settings`.
10. Scroll to `Personal` section.
11. Tap `Location services`.
12. Confirm `Google's location service` is unchecked
13. Confirm `GPS satellites` is unchecked.

Remediation:

1. Tap the globe Browser icon.
2. Press the Menu button.
3. Tap `Settings`.
4. Tap `Privacy & security`.
5. Scroll to `Location`
6. Uncheck "Enable location."
7. Press the Home button.
8. Press the Menu button.
9. Tap `System settings`.
10. Scroll to `Personal` section.
11. Tap `Location services`.
12. Uncheck `Google's location service`
13. Uncheck `GPS satellites`.

References:

1. Android 4.0 User Guide https://docs.google.com/open?id=0BzJ3Uh61kQ8XX283eDd1MDVKbzg

1.1.10 Enable 'Airplane Mode' (Not Scored)

Profile Applicability:

- Level 2

Description:

This control determines whether all of the devices receivers and transceivers can receive and transmit radio signals. This option is called Airplane Mode ("Flight Mode" on some phones). When Airplane Mode is enabled, no phone, GPS, radio, Wi-Fi, or Bluetooth signals are emitted from or received by the device. The recommended setting is enabled when these capabilities are unnecessary.

Rationale:

If the user enters an environment where signal transmission or reception are unnecessary then enabling Airplane Mode eliminates the remote attack surface of the device.

Audit:

1. Press the Menu button.
2. Tap `System settings`.
3. Scroll to Wireless & networks.
4. Tap `More...` if present
5. Confirm that "Airplane Mode" is checked.

Remediation:

1. Press the Menu button.
2. Tap `System settings`.
3. Scroll to Wireless & networks.
4. Tap `More...` if present
5. Check "Airplane Mode."

References:

1. Android 4.0 User Guide https://docs.google.com/open?id=0BzJ3Uh61kQ8XX283eDd1MDVKbzg

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

Profile Applicability:

- Level 1

Description:

This control deletes all data, including accounts, from the device's internal storage and restores the device to factory default settings.

Rationale:

Deleting data stored on the device before returning, recycling or disposing of the device reduces the probability of an attacker subsequently accessing confidential information previously stored on the device.

Audit:

To verify that the Android device's storage has been overwritten, it is necessary to install a forensics recovery toolkit that is not within the scope of this document. Please review the references for more information.

Remediation:

1. Press the Menu button.
2. Tap `System settings`.
3. Scroll to Personal.
4. Tap `Backup & reset`.
5. Tap `Factory data reset`.
6. Check "Erase SD card."
7. Tap `Reset phone`.
8. Type password if requested.

9. Tap `Next`.
10. Tap `Erase everything`.

References:

1. Android Forensics http://www.syngress.com/digital-forensics/Android-Forensics/
2. Android 4.0 User Guide https://docs.google.com/open?id=0BzJ3Uh61kQ8XX283eDd1MDVKbzg

1.1.12 Disable 'Notifications' (Not Scored)

Profile Applicability:

- Level 2

Description:

This control determines whether notifications are displayed on screen when the device is locked. The recommended setting is disabled.

Rationale:

If the device becomes lost or is unattended then disabling notifications reduces the capability of an attacker to obtain confidential information displayed on the screen.

Audit:

1. Tap Messaging icon.
2. Press the Menu button.
3. Tap `Settings`.
4. Scroll to `Notifications`.
5. Verify that `Notifications` is unchecked.

Remediation:

1. Tap Messaging icon.
2. Press the Menu button.
3. Tap `Settings`.
4. Scroll to `Notifications`.
5. Uncheck `Notifications`.

References:

1. Android 4.0 User Guide https://docs.google.com/open?id=0BzJ3Uh61kQ8XX283eDd1MDVKbzg

1.1.13 Enable 'Lock SIM card' (Not Scored)

Profile Applicability:

- Level 1

Description:

On applicable phones, SIM cards often contain contact and other personal information. This setting will lock the SIM card so that it requires a PIN to access.

Rationale:

Parties who do not know the SIM PIN should not be able to view the SIM card's contents, nor use the SIM card in another mobile device.

Audit:

1. Press the Menu button.
2. Tap `System settings`.
3. Scroll to Personal.
4. Tap `Security`.
5. Scroll to SIM card lock.
6. Tap `Set up SIM card lock`.
7. Verify "Lock SIM card" is checked.

Remediation:

1. Press the Menu button.
2. Tap `System settings`.
3. Scroll to Personal.
4. Tap `Security`.
5. Scroll to SIM card lock.
6. Tap `Set up SIM card lock`.
7. Check "Lock SIM card" if not already checked.
8. Tap `Change SIM PIN`.
9. Type old SIM PIN if requested.
10. Tap `OK`.
11. Type in new SIM PIN.
12. Tap `OK`.
13. Re-type new SIM PIN.
14. Tap `OK`.

References:

1. Android 4.0 User Guide https://docs.google.com/open?id=0BzJ3Uh61kQ8XX283eDd1MDVKbzg

1.1.14 Disable 'make passwords visible' (Not Scored)

Profile Applicability:

- Level 1

Description:

This control determines whether passwords are displayed as they are typed. The recommended setting is disabled.

Rationale:

Enforcing this control reduces the capability of an attacker to observe user input and learn the device password.

Audit:

1. Press the Menu button.
2. Tap `System settings`.
3. Tap `Security`.
4. Verify `Make passwords visible` is unchecked.

Remediation:

1. Press the Menu button.
2. Tap `System settings`.
3. Tap `Security`.
4. Uncheck `Make passwords visible`.

References:

1. Android 4.0 User Guide https://docs.google.com/open?id=0BzJ3Uh61kQ8XX283eDd1MDVKbzg

1.1.15 Enable 'Encrypt phone' (Not Scored)

Profile Applicability:

- Level 1

Description:

Mobile devices not only contain information, they also contain passwords and other credentials that can enable an attacker to retrieve confidential data from other sources the device may interact with. Note that the encryption process requires an hour or more, a fully-charged battery, and that the phone remains plugged in until the process is complete. If the encryption process is interrupted, some or all data may be lost.

Rationale:

Once the phone is encrypted, a numeric PIN or password is required each time the phone is powered on, protecting personal data that would otherwise be easily recovered through a variety of methods. The phone cannot be unencrypted except by performing a factory data reset, which will erase all data on the phone.

A phone encrypted in this manner is better than an unencrypted phone. However, the particular way that Android implements their encryption deserves some caveats. The encryption technology used in Android 3 is dm-crypt. The encryption uses a symmetric key, which is derived from the password/PIN typed by the user; the derivation parameters are stored in a LUKS-formatted block on the device itself. Password derivation is salted and uses multiple iterations, with PBKDF2. One consequence of that is that an attacker can do an offline dictionary attack: when he gets the device, he does a raw dump of the partition into a PC, then "tries" passwords. The LUKS block contains enough information to verify whether a potential password is correct or not.

PBKDF2 uses salts and iterations to make the search less efficient, but there are limitations to what PBKDF2 can achieve. PBKDF2 makes key derivation (from the password) slow for the attacker and for the mobile phone itself alike. It must not use too many iterations, because the user is not ready to wait more than, say 3 or 4 extra seconds upon boot. An attacker can be expected to have more computing power and more patience (if the data is valuable, the attacker is ready to invest one hour or two of computation). Therefore, a 4-digit PIN will not last long in that situation. On the other hand, most users are not prepared to type in a long, high -entropy password on your phone at each boot.

Audit:

1. Press the Menu button.
2. Tap `System settings`.
3. Scroll to Personal.
4. Tap `Security`.
5. Validate phone is encrypted.

Remediation:

1. Press the Menu button.
2. Tap `System settings`.
3. Scroll to Personal.
4. Tap `Security`.
5. Scroll to the `Encryption` section.
6. Tap `Encrypt phone`.
7. Tap `Encrypt phone` again
8. Enter Lock screen PIN or password

9. Tap `Continue`.
10. Tap `Encrypt phone`.

References:

1. Android 4.0 for Galaxy Nexus: http://support.google.com/ics/nexus/bin/answer.py?hl=en&answer=1663755
2. Android 4.0 User Guide https://docs.google.com/open?id=0BzJ3Uh61kQ8XX283eDd1MDVKbzg
3. Relevant Security Exchange Forum Post: http://security.stackexchange.com/questions/10529/are-there-actually-any-advantages-to-android-full-disk-encryption

1.1.16 Disable 'developer options' (Not Scored)

Profile Applicability:

- Level 1

Description:

The operating system allows developers to change phone behavior, interact with the device, issue commands, and read storage. The recommended settings is disabled.

Rationale:

Disabling command and data functions reduces the attack surface of the device. Since the same port is used to charge the phone, combined with the common availability in airports and other public places for phone charging, it is important to ensure that charging the phone does not open an attack vector.

Audit:

1. Press the Menu button.
2. Tap `System settings`.
3. Scroll to System.
4. Tap `Developer options`.
5. Confirm that `USB debugging` is unchecked.
6. Confirm that `Stay awake` is unchecked.
7. Confirm that `Mock locations` is unchecked.

Remediation:

1. Press the Menu button.
2. Tap `System settings`.
3. Scroll to `System`.
4. Tap `Developer options`.
5. Uncheck `USB debugging`.

6. Uncheck `Stay awake`.
7. Uncheck `Mock locations`.

References:

1. Android 4.0 User Guide https://docs.google.com/open?id=0BzJ3Uh61kQ8XX283eDd1MDVKbzg

1.1.17 Disable 'Unknown sources' (Not Scored)

Profile Applicability:

- Level 1

Description:

This control determines whether applications can be installed from locations other than Google Play. The recommended setting is disabled.

Rationale:

Disabling installation from untrusted distribution channels protects
against inadvertent installation of untrusted or malicious applications.

Audit:

1. Press the Menu button.
2. Tap `System settings`.
3. Tap `Security`.
4. Scroll to `Device administration`.
5. Confirm `Unknown sources` is unchecked.

Remediation:

1. Press the Menu button.
2. Tap `System settings`.
3. Tap `Security`.
4. Scroll to `Device administration`.
5. Uncheck `Unknown sources`.

References:

1. Android 4.0 User Guide https://docs.google.com/open?id=0BzJ3Uh61kQ8XX283eDd1MDVKbzg

1.1.18 Limit the 'number of messages' for 'Text message limit' (Not Scored)

Profile Applicability:

- Level 2

Description:

This control limits the number of messages saved per thread of text messages. When the limit is reached older messages are deleted if 'Delete old messages' is enabled. The recommended setting is 100 or less messages saved.

Rationale:

Limiting the number of messages saved on the device potentially reduces the scope of information disclosure in the event of device compromise.

Audit:

1. Tap Message icon.
2. Press Menu button.
3. Tap `Settings`.
4. Verify `Delete old messages` is checked.
5. Verify `Text message limit` is set to "100 messages per conversation"

Remediation:

1. Tap Message icon.
2. Press Menu button.
3. Tap `Settings`.
4. Check `Delete old messages`.
5. Tap `Text message limit`.
6. Scroll to 100
7. Tap `Set`.

References:

1. Android 4.0 User Guide https://docs.google.com/open?id=0BzJ3Uh61kQ8XX283eDd1MDVKbzg

1.1.19 Limit the 'number of messages' for 'Multimedia message limit' (Not Scored)

Profile Applicability:

- Level 2

Description:

This control limits the number of messages saved per thread of multimedia messages. When the limit is reached older messages are deleted if 'Delete old messages' is enabled. The recommended setting is 20 or less messages saved.

Rationale:

Limiting the number of messages saved on the device potentially reduces the scope of information disclosure in the event of device compromise.

Audit:

1. Tap Message icon.
2. Press Menu button.
3. Tap `Settings`.
4. Verify `Delete old messages` is checked.
5. Verify `Multimedia message limit` is set to 20 messages.

Remediation:

1. Tap Message icon.
2. Press Menu button.
3. Tap `Settings`.
4. Check `Delete old messages`.
5. Tap `Multimedia message limit`.
6. Scroll to 20 messages
7. Tap `Set`.

References:

1. Android 4.0 User Guide https://docs.google.com/open?id=0BzJ3Uh61kQ8XX283eDd1MDVKbzg

1.2 Browser Settings

This section provides guidance on the secure configuration of settings related to the built-in browser.

1.2.1 Disable 'JavaScript' (Not Scored)

Profile Applicability:

- Level 2

Description:

This control determines whether JavaScript programming code is allowed run in the browser. The recommended setting is disabled.

Rationale:

JavaScript lets web programmers control elements of the page, for example: a page that uses JavaScript process may process login credentials or cause a linked page to appear in a new pop-up page. JavaScript should only be enabled when browsing trusted sites.

Audit:

1. Tap the globe Browser icon.
2. Press the Menu button.
3. Tap `Settings`.
4. Tap `Advanced`.
5. Confirm `Enable JavaScript` is unchecked.

Remediation:

1. Tap the globe Browser icon.
2. Press the Menu button.
3. Tap `Settings`.
4. Tap `Advanced`.
5. Uncheck `JavaScript`.

References:

1. Android 4.0 User Guide https://docs.google.com/open?id=0BzJ3Uh61kQ8XX283eDd1MDVKbzg

1.2.2 Enable 'Show security warnings' (Not Scored)

Profile Applicability:

- Level 1

Description:

This control determines whether the browser displays security warnings about websites with common security problems such as outdated or invalid certificates. The recommended setting is enabled.

Rationale:

Enforcing this control reduces the probability that invalid certificates can be used to provide unauthorized access to confidential information or breach its integrity.

Audit:

1. Tap the globe Browser icon.
2. Press the Menu button.
3. Tap `Settings`.
4. Tap `Privacy & security`.
5. Verify that `Show security warnings` is checked.

Remediation:

1. Tap the globe Browser icon.
2. Press the Menu button.
3. Tap `Settings`.
4. Tap `Privacy & security`.
5. Check `Show security warnings`.

References:

1. Android 4.0 User Guide https://docs.google.com/open?id=0BzJ3Uh61kQ8XX283eDd1MDVKbzg

1.2.3 Disable 'Form auto-fill' (Not Scored)

Profile Applicability:

- Level 1

Description:

This control determines whether data entered into web forms are stored enabling auto-completion of the form upon subsequent visits to the site. The recommended setting is disabled.

Rationale:

Enforcing this control reduces the probability of an attacker obtaining or using confidential information stored on the device such as names, credit card numbers and passwords.

Audit:

1. Tap the globe Browser icon.
2. Press the Menu button.
3. Tap `Settings`.
4. Tap `Privacy & security`.
5. Scroll to `Form data`.
6. Verify "`Remember form data`" is unchecked.

7. Press the Back button.
8. Tap `General`.
9. Uncheck `Form auto-fill`.
10. Verify that `Form auto-fill` is unchecked.

Remediation:

1. Tap the globe Browser icon.
2. Press the Menu button.
3. Tap `Settings`.
4. Tap `Privacy & security`.
5. Scroll to Form data.
6. Tap `Clear form data`,
7. Tap `OK` on the confirmation dialog.
8. Uncheck `Remember form data`.
9. Press the Back button.
10. Tap `General`.
11. Uncheck `Form auto-fill`.

References:

1. Android 4.0 User Guide https://docs.google.com/open?id=0BzJ3Uh61kQ8XX283eDd1MDVKbzg

1.2.4 Disable 'Accept Cookies' (Not Scored)

Profile Applicability:

- Level 2

Description:

This control determines whether the device browser will accept and store HTTP cookies sent by websites the user accesses. The recommended setting is `disabled`.

Rationale:

Disabling 'Accept Cookies' reduces the probability of an attacker tracking, altering or stealing confidential information. HTTP cookies may contain user-specific data such as usernames, passwords and account numbers.

Audit:

1. Tap the Globe icon.
2. Press the Menu button.
3. Tap `Settings`.
4. Tap `Privacy & security`.
5. Verify that "Accept cookies" is unchecked.

Remediation:

1. Tap the Globe icon.
2. Press the Menu button.
3. Tap `Settings`.
4. Tap `Privacy & security`.
5. Tap `Clear all cookie data`.
6. Tap `OK`.
7. Uncheck "Accept cookies."

References:

1. Android 4.0 User Guide https://docs.google.com/open?id=0BzJ3Uh61kQ8XX283eDd1MDVKbzg

1.2.5 Enable 'Block pop-ups' (Not Scored)

Profile Applicability:

- Level 1

Description:

The Pop-up Blocker is used to block pop-ups which a website might open with or without any user interaction. These pop-ups can be used to open untrusted malicious content. The recommended setting is `enabled`.

Rationale:

Enabling the Pop-up Blocker will block all pop-ups to guard a user against any attacks launched using pop-up windows.

Audit:

1. Tap Globe icon.
2. Press the Menu button.
3. Tap `Settings`.
4. Tap `Advanced`.
5. Verify that "Block pop-ups" is checked.

Remediation:

1. Tap Globe icon.
2. Press the Menu button.
3. Tap `Settings`.

4. Tap `Advanced`.
5. Check "Block pop-ups."

References:

1. Android 4.0 User Guide https://docs.google.com/open?id=0BzJ3Uh61kQ8XX283eDd1MDVKbzg

1.2.6 Disable 'plug-ins' (Not Scored)

Profile Applicability:

- Level 2

Description:

This control determines whether plug-ins are allowed run in the browser. The recommended setting is disabled.

Rationale:

Flash and other plug-ins let web programmers control elements of the page, for example: a page that uses Flash processing may process login credentials or cause a linked page to appear in a new pop-up page. Plug-ins should only be enabled when browsing trusted sites.

Audit:

1. Tap the globe Browser icon.
2. Press the Menu button.
3. Tap `Settings`.
4. Tap `Advanced`.
5. Confirm `Enable plug-ins` is set to Off.

Remediation:

1. Tap the globe Browser icon.
2. Press the Menu button.
3. Tap `Settings`.
4. Tap `Advanced`.
5. Tap `Enable plug-ins`.
6. Select `Off`.

References:

1. Android 4.0 User Guide https://docs.google.com/open?id=0BzJ3Uh61kQ8XX283eDd1MDVKbzg

1.2.7 Disable 'Remember passwords' (Not Scored)

Profile Applicability:

- Level 1

Description:

This control determines whether passwords entered into web forms are stored enabling auto-completion of the form upon subsequent visits to the site. The recommended setting is disabled.

Rationale:

Enforcing this control reduces the probability of an attacker obtaining or using passwords stored on the device.

Audit:

1. Tap the globe Browser icon.
2. Press the Menu button.
3. Tap `Settings`.
4. Tap `Privacy & security`.
5. Scroll to `Passwords`.
6. Verify `Remember passwords` is unchecked.

Remediation:

1. Tap the globe Browser icon.
2. Press the Menu button.
3. Tap `Settings`.
4. Tap `Privacy & security`.
5. Scroll to `Passwords`.
6. Tap `Clear passwords` and tap `OK` on the confirmation dialog.
7. Uncheck `Remember passwords`.

References:

1. Android 4.0 User Guide https://docs.google.com/open?id=0BzJ3Uh61kQ8XX283eDd1MDVKbzg

2 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

2.1 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

2.1.1 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. 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. For full details, please refer to the 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

2.1.2 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. 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

2.1.3 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. 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

2.1.4 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. The recommended setting is the minimum device password complexity is set to 1 or more characters.

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 passcode" check box 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.

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. 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>"
 -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).

References:

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

2.1.5 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. 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 following in the box on the right hand side: `2 or less minutes`
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

2.1.6 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 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

2.1.7 Set the 'number of days' for 'maximum password age' (Scored)

Profile Applicability:

- Level 2 - MS Exchange Server 2010

Description:

This control defined how many days a user can use the same password before it expires. The recommended state for this setting is 90 days or less.

Rationale:

Enforcing a reasonably short password age will increase the efficacy of password-based authentication systems by reducing the opportunity for an attacker to leverage a known credential.

Audit:

In EMC-> Microsoft Exchange-> Organization Configuration->Client Access->Exchange ActiveSync Mailbox Policies

1. Right Click on Policy, Select properties
2. Password Tab
3. Password Expiration

In EMShell:

1. Enter

```
Get-ActiveSyncMailboxPolicy | Select identity, DevicePasswordExpiration
```

2. Verify values, per remediation

Remediation:

In EMC-> Microsoft Exchange-> Organization Configuration->Client Access->Exchange ActiveSync Mailbox Policies

1. Right Click on Policy, Select properties
2. Select Password Tab
3. In Password Expiration: Checked, 90

In EMShell:

1. Enter

```
Set-ActiveSyncMailboxPolicy -identity <name> -DevicePasswordExpiration 90
```

References:

1. CIS Security Configuration Benchmark for Microsoft Exchange Server 2007, version 1.1.0, Section 8.19: Require ActiveSync Password Expiration.

2.1.8 Set the 'number of passwords' for 'password history' (Scored)

Profile Applicability:

- Level 2 - MS Exchange Server 2010

Description:

This control defines the number of unique passwords a user must leverage before a previously used password can be reused. The recommended state for this setting is 24 or more passwords remembered.

Rationale:

Enforcing a sufficiently long password history will increase the efficacy of password-based authentication systems by reducing the opportunity for an attacker to leverage a known credential. For example, if an attacker compromises a given credential that is then expired, this control prevents the user from reusing that same compromised credential.

Audit:

In EMC-> Microsoft Exchange-> Organization Configuration->Client Access->Exchange ActiveSync Mailbox Policies:

1. Right Click on Policy, Select properties
2. Password Tab
3. Enforce password history

In EMShell:

1. Enter:

```
Get-ActiveSyncM
```

2. Verify values, per remediation

Remediation:

In EMC-> Microsoft Exchange-> Organization Configuration->Client Access->Exchange ActiveSync Mailbox Policies

1. Right Click on Policy, Select properties
2. Password Tab
3. Enforce password history: 24

In EMShell:

1. Enter:

```
Set-ActiveSyncMailboxPolicy -identity <name> -DevicePasswordHistory 24
```

References:

1. CIS Security Configuration Benchmark for Microsoft Exchange Server 2007, version 1.1.0, Section 8.20: Require ActiveSync Password History

2.1.9 Enable 'Require encryption on the device' (Scored)

Profile Applicability:

- Level 1 - MS Exchange Server 2010

Description:

This setting enables storage card encryption on the device.

Rationale:

Enabling encryptions protects sensitive information, such as contacts or attachments, from being disclosed if either the device or storage card is lost or stolen.

Audit:

In MC-> Microsoft Exchange-> Organization Configuration-> Client Access-> Exchange ActiveSync Mailbox Policies:

1. Right Click on Policy, Select properties

2. Password Tab
3. Require encryption on device

In EMShell

1. Enter:

```
Get-ActiveSyncMailboxPolicy | Select identity, DeviceEncryptionEnabled
```

2. Verify values, per remediation.

Remediation:

In: EMC-> Microsoft Exchange-> Organization Configuration-> Client Access-> Exchange ActiveSync Mailbox Policies:

1. Right Click on Policy, Select properties
2. Password Tab
3. Require encryption on device: Checked

In EMShell:

1. Enter:

```
Set-ActiveSyncMailboxPolicy -identity <name> -DeviceEncryptionEnabled $true
```

2. Verify values per remediation

References:

1. CIS Security Configuration Benchmark for Microsoft Exchange Server 2007, version 1.1.0, Section 8.21: Require ActiveSync Encryption.

3 Appendices

3.1 Additional Information for Exchange ActiveSync Management

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

Security configuration items that can be applied include the initiation of a remote wipe of a managed device and the enforcement of five password configuration policies (specifically: requiring a password, setting a minimum password length, requiring an alphanumeric password, requiring a complex password, 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

3.1.1 General ActiveSync Settings

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

3.1.1.1 Disable 'Allow non-provisionable devices' (Not Scored)

Profile Applicability:

- Level 1 - MS Exchange Server 2010

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 Android device 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.

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" check box 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.

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" check box 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).

References:

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

3.1.2 General Resources for Android Mobile Device ActiveSync Management

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

1. Microsoft Corporation (2011). Microsoft Technet Library Article: Exchange 2010 Client Access Cmdlet Set-ActiveSyncMailboxPolicy Parameter Information. Available: http://technet.microsoft.com/en-us/library/bb123756.aspx. Last accessed 27 September 2012.
2. Microsoft Corporation (2011). Microsoft Technet Library Article: Exchange 2010 Client Access Cmdlet Get-ActiveSyncMailboxPolicy Parameter Information. Available: http://technet.microsoft.com/en-us/library/bb124900.aspx. Last accessed 27 September 2012.
3. Microsoft Corporation (2007). Microsoft Technet Library Article: New User's Guide to the Exchange Management Console. Available: http://technet.microsoft.com/en-us/library/bb245702%28EXCHG.80%29.aspx. Last accessed 27 September 2012.
4. Microsoft Corporation (2007). Microsoft Technet Library Article: A Primer on the Exchange Management Shell. Available: http://technet.microsoft.com/en-us/library/bb245704%28EXCHG.80%29.aspx. Last accessed 27 September 2012.
5. Microsoft Corporation (2009). Microsoft Technet Library Article: Exchange Management Shell in Exchange 2010. Available: http://technet.microsoft.com/en-us/library/dd795097.aspx. Last accessed 27 September 2012.
6. Microsoft Corporation (2011). Microsoft Technet Library Article: Exchange Management Console (MS Exchange 2010). Available: http://technet.microsoft.com/en-us/library/bb123762.aspx. Last accessed 27 September 2012.
7. Microsoft Corporation (2009). Microsoft Technet Library Article: Exchange Management Shell (MS Exchange 2010). Available: http://technet.microsoft.com/en-us/library/bb123778.aspx. Last accessed 27 September 2012.

3.2 Loss of Physical Custody of an Android and Compensating Controls

The combined "Set up screen lock," "Set up SIM card lock," and "Set a password for secure credential storage" recommendations in the Level I and Level II Benchmark profiles provide a basic level of protection against unauthorized device and data access in the event of a lost device.

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

- A remote wipe feature can be activated as a compensating corrective control, available through the following mechanisms:

- Exchange ActiveSync Mobile Administration Web Tool (MS Exchange Server 2007 and MS Exchange Server 2010)
- Exchange Management Console (MS Exchange Server 2010)

- Third-party encryption apps are available to protect the confidentiality of data for advanced applications and should be considered where advanced protections are required. User-level configuration was introduced in Android 3.0 (Honeycomb).

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.

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

Appendix: Change History

Date	Version	Changes for this version
10-01-2012	1.0.0	Initial release