Security Benchmarks™
A DIVISION OF CENTER FOR INTERNET SECURITY

Security Configuration Benchmark

CIS Google Android 4.x Benchmark

v2.0.0

Export Date 06-28-2012

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.

Considerations

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.

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 for Android 4.0 devices, available through the following mechanisms:

- Exchange ActiveSync Mobile Administration Web Tool (MS Exchange Server 2003 and MS Exchange Server 2007)
- Exchange Management Console (MS Exchange Server 2007)

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 by Android as of Android 4.0,
see: http://en.wikipedia.org/wiki/Comparison_of_Exchange_ActiveSync_clients

This document, CIS Google Android 4.x Benchmark v2.0.0, provides prescriptive guidance for establishing a secure configuration posture for Android 4.0. 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, and platform deployment personnel, who plan to develop, deploy, assess, or secure solutions that incorporate Android 4.0 –based devices.

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 – Basic Steps of general benefit with little risk**
- **Level 2 – More advanced activities that provide less benefit, or make the device less usable.**

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 / Maintainer: Robert Fritz, CISSP CSSLP
- Contributors and Reviewers:
    - Molly Maguire
    - Blake Frantz, Center for Internet Security
    - Steven Piliero, Center for Internet Security
    - Billy Glenn, Pacific Gas & Electric
    - Yves Desharnais
    - Fernando Trias, Athigo
    - John Fox, Athigo
    - Martin Walker, Information Defense

Recommendations

1 Settings in the Android User Interface

This section provides guidance on the secure configuration of Android 2.3 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
- Level 2

Description:

An Android 4.0 mobile device ships with whichever version of the firmware was current when it was manufactured, but updates may have been released since then. It is recommended that the device firmware remain current.

Rationale:

Firmware updates include not only new features and bug fixes but security fixes as well. Also, the device must be running build version 4.0 or later for these benchmark recommendations to apply; if a newer version of the firmware is available, some recommendations may not apply.

Audit:

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

Remediation:

Contact your telecommunications provider for their latest supported update.

1.1.2 Require Password on Device (Not Scored)

Profile Applicability:

- Level 1
- Level 2

Description:

Android 4.0 can be configured to require a password before allowing usage via the touch screen. By default, a password is not required to unlock the screen. It is recommended that a password be set. This setting is the same as the setting in Section 3.1.1.

Rationale:

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

The benchmark recommends using only alphanumeric passwords, since the pattern space is larger than that associated with visual patterns. In addition, visual pattern password complexity is not manageable or measureable. Finally, other password controls or metrics such as history and expiration are not available.

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. (See reference below)
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.

1.1.3 Configure an alphanumeric value (Not Scored)

Profile Applicability:

- Level 2

Description:

See 1.1.2 above. Also note this setting can be enforced in setting in Section 3.1.2

1.1.4 Set Screen timeout (Not Scored)

Profile Applicability:

- Level 1
- Level 2

Description:

An Android 4.0 device's screen can be configured to timeout after a pre-defined inactivity period. By default, if a password is defined, the device will automatically lock. It is recommended that an inactivity timeout be set.

Rationale:

If the user has set a screen timeout interval of greater than two minutes, there is a greater risk that the device will be in an unlocked state during a physical security breach.

Audit:

1. Press the Menu button.
2. Tap System Settings.
3. Scroll to Personal section.
4. Tap Security.

4a. For typical use cases, confirm that Automatically lock is set to 2 minutes after sleep.

4b. For high-security use cases, confirm that Automatically lock is set to 1 minute after sleep.

Remediation:

1. Press the Menu button.
2. Tap System Settings.
3. Scroll to Device section.
4. Tap Display.

5. Tap Sleep.

5a. For typical use cases, tap “2 Minutes”.

5b. For high-security use cases, tap “1 Minute”.

1.1.5 Erase data upon excessive password failures (Not Scored)

Profile Applicability:

- Level 1
- Level 2

Description:

This feature is not available in Android 4.0. This setting can be controlled using Exchange. See 3.1.6.

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

Profile Applicability:

- Level 2

Description:

An Android 4.0 device can be configured to forget Wi-Fi networks that it has previously associated with. By default, a device will remember and automatically join networks that it has previously associated with. It is recommended that networks be forgotten after use in use cases where security is paramount.

Rationale:

A trusted but unauthenticated Wi-Fi network may be spoofed and automatically joined if it is not forgotten after last use. Additionally, if such a network has a common SSID, such as “default” or “Linksys,” it is probable that the Android 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.
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 Wi-Fi.
5. In the Wi-Fi settings, locate the network SSID and tap and hold down the entry for the network you wish to forget.
6. 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.

1.1.7 Turn off Network Notification (Not Scored)

Profile Applicability:

- Level 1
- Level 2

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. “defualt”).

Audit:

1. Press the Menu button.
2. Tap System settings.
3. Tap More.
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.
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.

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

Profile Applicability:

- Level 1
- Level 2

Description:

Android 4.0 does not automatically join new networks. This setting is listed here for completeness because it is included in the CIS Benchmark for iOS and may be covered in future Android versions.

Rationale:

Audit:

Remediation:

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

Profile Applicability:

- Level 2

Description:

Android 4.0 devices can be configured to participate in Wi-Fi networks. It is recommended that Wi-Fi be disabled when not needed or where security is paramount.

If Wi-Fi is turned off on a device with cellular data service, connections to the Internet will occur via the cellular data network, when available. Applications such as 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.

1.1.10 Turn off VPN when not needed (Not Scored)

Profile Applicability:

- Level 1
- Level 2

Description:

Not applicable. Android 4.0 devices do not automatically connect to VPNs. This setting is listed here for completeness because it is included in the CIS Benchmark for iOS and may be covered in future Android versions.

1.1.11 Turn off Bluetooth when not needed (Not Scored)

Profile Applicability:

- Level 1
- Level 2

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 if Off.

Remediation:

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

1.1.12 Turn off 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 in environments where security is paramount.

Rationale:

Android 4.0 enables the user to enable or deny Internet websites to access to location services. In addition, any application in Android 4.0 may send location data if location data is available to the phone itself.

Audit:

1. Tap the globe Browser icon.
2. Press the Menu button.
3. Tap Settings.
4. Tap Privacy & security.
5. Scroll to Location and verify that Enable location is unchecked.
6. Press the Home button.
7. Press the Menu button.
8. Tap System settings.
9. Scroll to Personal section.
10. Tap Location services.
11. Verify that both Google's location service and GPS satellites are unchecked.

Remediation:

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

1.1.13 Turn on Airplane Mode (Not Scored)

Profile Applicability:

- Level 2

Description:

Mobile devices running Android 4.0 can be configured to disable all receivers and transceivers. This option is called Airplane Mode ("Flight Mode" on some phones). When Airplane Mode is on, no phone, GPS, radio, Wi-Fi, or Bluetooth signals are emitted from or received by the device. It is recommended that Airplane Mode be enabled when these capabilities are unneeded or where security is paramount.

Rationale:

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

Audit:

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

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

Profile Applicability:

- Level 1
- Level 2

Description:

In normal operations, Android 2.3 devices do not use a secure delete function to erase data from the disk, allowing it to persist in a recoverable state. Therefore, the device's storage, including the SD card, should be deleted via "Factory data reset" before the device is out of the user's control.

Rationale:

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

1.1.15 Disable SMS preview when Android is locked (Not Scored)

Profile Applicability:

- Level 2

Description:

If the Android 4.0 device is password locked and receiving SMS messages, the messages are still previewed briefly on the display. It is recommended that SMS previews be disabled in environments where security is paramount.

Rationale:

Parties who do not know the password lock should not be able to view the Android device's SMS traffic.

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.

1.1.16 Set up SIM card lock (Not Scored)

Profile Applicability:

- Level 1
- Level 2

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.

1.1.17 Disable visible passwords (Not Scored)

Profile Applicability:

- Level 1
- Level 2

Description:

Android has the ability to display passwords as they're typed, to minimize entry errors.

Rationale:

Password feedback, even if provided only one character at a time, can enable an individual watching the device to learn the password. It is recommended that this feature be disabled.

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.

1.1.18 Encrypt phone (formerly: Encrypt credentials storage) (Not Scored)

Profile Applicability:

- Level 2

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.

From: Relevant Security Exchange Forum
Post: http://security.stackexchange.com/questions/10529/are-there-actually-any-advantages-to-android-full-disk-encryption

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. Tap Encrypt phone section.
6. Tap Encrypt phone.
7. Enter Lock screen PIN or password and tap Continue.
8. Tap Encrypt phone.

1.1.19 Disable development features (Not Scored)

Profile Applicability:

- Level 1
- Level 2

Description:

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

Rationale:

Disabling command and data functions dramatically reduces the attack surface of the device.

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.

1.1.20 Disallow application installs from unknown source (Not Scored)

Profile Applicability:

- Level 1
- Level 2

Description:

By default, Android requires application developers to sign their applications and distribute them through the Android market.

Rationale:

Disabling installation from untrusted distribution channels increases the chance that the applications sought are the applications actually downloaded.

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.

1.1.21 SMS Text Message Expiration (Not Scored)

Profile Applicability:

- Level 2

Description:

Android 4.0 allows the user to configure Android to delete messages over a certain age. This feature is useful, as it minimizes the potential exposure of data if the device is compromised. We selected Level 2 for this item because some individuals may find the device has reduced functionality if the device does not contain a full history of their messaging.

Rationale:

The device can save messages for later viewing. Limit the number of saved messages to minimize information disclosure.

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.

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 and tap Set.

1.1.22 SMS Multimedia Message Expiration (Not Scored)

Profile Applicability:

- Level 2

Description:

Android 4.0 allows the user to configure Android to delete messages over a certain age. This feature is useful, as it minimizes the potential exposure of data if the device is compromised. We selected Level 2 for this item because some individuals may find the device has reduced functionality if the device does not contain a full history of their messaging.

Rationale:

The device can save messages for later viewing. Limit the number of saved messages to minimize information disclosure.

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 and tap Set.

1.2 Browser Settings

This section provides guidance on the secure configuration of settings related to the built-in browser on Android 4.0 mobile devices.

1.2.1 Disable JavaScript (Not Scored)

Profile Applicability:

- Level 2

Description:

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

Rationale:

JavaScript should only be enabled before browsing trusted sites.

Audit:

1. Tap the globe Browser icon.
2. Press the Menu button.
3. Tap Settings.
4. Tap Advanced.
5. Uncheck JavaScript.
6. Tap Enable plug-ins
7. Confirm Enable JavaScript is unchecked.
8. Confirm that 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. Uncheck JavaScript.
6. Tap Enable plug-ins
7. Select Off.

1.2.2 Enable basic SSL checks for websites (Not Scored)

Profile Applicability:

- Level 1
- Level 2

Description:

Although the built-in browser does not provide website black-list checking, it will provide common security checks, such as SSL certificate expiration and domain match.

Rationale:

Ensuring that standard security checks are enabled, can help warn in cases of some simple security issues.

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.

1.2.3 Disable Remember Form Data (Not Scored)

Profile Applicability:

- Level 2

Description:

The browser has a feature to remember information entered into common forms in order to automate the completion of later forms. Information auto-filled can include personal information, including names and passwords. It is recommended that Remember Form Data is disabled.

Rationale:

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

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. Scroll to Passwords.
8. Verify Remember passwords is unchecked.
9. Press the Back button.
10. Tap General.
11. Uncheck Form auto-fill.
12. 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, and tap OK on the confirmation dialog.
7. Uncheck Remember form data.
8. Scroll to Passwords.
9. Tap Clear passwords and tap “OK” on the confirmation dialog.
10. Uncheck Remember passwords.
11. Press the Back button.
12. Tap General.
13. Uncheck Form auto-fill.

1.2.4 Disable Cookies (Not Scored)

Profile Applicability:

- Level 2

Description:

The browser in Android, just like most other browser, has the ability to remember user-specific data in local storage called cookies. This configuration item disables that storage, eliminating an attack vector, but also eliminating some website functionality

Rationale:

Level 2 was selected because this setting represents a trade-off of security for functionality. In limited use cases, leaving this disabled may be completely functional, but more interactive use-cases may suffer significantly.

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.

1.2.5 Block pop-ups (Not Scored)

Profile Applicability:

- Level 1
- Level 2

Description:

This setting configures the Android browser to look for and prevent common pop-up techniques.

Rationale:

Pop-ups are often annoying; they consume bandwidth and are sometimes associated with attacks or malware. Useful functionality is rarely impacted by this setting.

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.

2 Settings in Android's Software Development Kit (SDK)

The Android Software Development Kit (SDK) and associated development tools create a rich environment for application development and some facility for configuration if the device's storage is mounted read-write, which is not normally the case. Discussing Android scripting and Application Programming Interface (API) usage is beyond the scope of this

document, but further information is available at:
http://developer.android.com/sdk/android-4.0.3.html

3 Android Mobile Device Settings in MS Exchange ActiveSync Policy

This section provides guidance on the configuration of ActiveSync policies applicable to Android 4.0 from the Microsoft Exchange Server 2007 Benchmark.

Please note Android 4.0 phones can add accounts and sync information from multiple Exchange servers; they can also add multiple Google accounts and other kinds of accounts. Each of these accounts may have security policies that are enforced by Android. If accounts have conflicting security policies, Android enforces the strictest rules set by any account for each kind of policy; in other words, 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 by Android 4.0,
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 Require password on device (Scored)

Profile Applicability:

- Level 1
- Level 2

Description:

The device can be configured to require a password before allowing access through the touchpad. By default, Android devices do not require a password 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 password. It is recommended that a password be set. This setting is the same as the setting in Section 1.1.2.

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.

Rationale:

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

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).

3.1.2 Require alphanumeric value (Scored)

Profile Applicability:

- Level 2

Description:

The device can be configured to require that the password be comprised of both numeric and alphabetic values. By default, Android devices do not enforce a password complexity policy, and the default Exchange ActiveSync policy setting applied for users not assigned to a mailbox policy does not require an alphanumeric password. It is recommended that both numeric and alphabetic values comprise the password. This setting is the same as the setting in Section 1.1.3, though automated enforcement is only available via Exchange policy.

For full details, please refer to the CIS Security Configuration Benchmark for Microsoft Exchange Server 2007, version 1.1.0, Section 8.17: Require ActiveSync Alphanumeric Password.

Rationale:

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

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" checkbox is selected.
3. Click "Cancel".

Using the Exchange Management Shell:
At the Exchange Management Shell command prompt,

Enter the following command (all one line):

```
1. 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" checkbox
3. Click "OK".

Using the Exchange Management Shell:
At the Exchange Management Shell command prompt,

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

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

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

3.1.3 Set minimum password length (Scored)

Profile Applicability:

- Level 1
- Level 2

Description:

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

For full details, please refer to the CIS Security Configuration Benchmark for Microsoft Exchange Server 2007, version 1.1.0, Section 8.18: Require ActiveSync Minimum Password Length.

Rationale:

Requiring at least five characters increases the complexity of the password an attacker may attempt to brute-force in order to gain access to the device. Additionally, requiring at least five characters prevents a user from selecting typically weak values, such as a year, date, or last four digits of a phone number, for their password. Android 4.0 supports passwords of up to 16 characters.

Audit:

Using the Exchange Management Console (EMC):
In the "Properties" configuration window,

1. Click on the "Password" tab.

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

Using the Exchange Management Shell:
At the Exchange Management Shell command prompt,

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

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

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

2. Search the 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 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).

3.1.4 Set a minimum number of complex characters (Scored)

Profile Applicability:

- Level 2

Description:

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

For full details, please refer to the CIS Security Configuration Benchmark for Microsoft Exchange Server 2007, version 1.1.0, Section 8.17: Require ActiveSync Alphanumeric Password

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:

Using the Exchange Management Console (EMC):

In the "Properties" configuration window,

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

Using the Exchange Management Shell:

At the Exchange Management Shell command prompt,

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

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

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

2. Search the outputted policy setting list for the "MinDevicePasswordComplexCharacters :" configuration item.
3. Observe if there is a value following the colon and that the value is set to 1 as shown below:
   `MinDevicePasswordComplexCharacters : 1`
4. Search the outputted policy setting list for the "AlphanumericDevicePasswordRequired :" configuration item
5. Observe if the value following the colon is "True" as shown below:
   `AlphanumericDevicePasswordRequired : True`
6. Exit the Exchange Management Shell.

Remediation:

Using the Exchange Management Console (EMC):

In the "Properties" configuration window,

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

Using the Exchange Management Shell:

At the Exchange Management Shell command prompt,

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

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

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

3.1.5 Set auto-lock timeout (Scored)

Profile Applicability:

- Level 1

- Level 2

Description:

The device can be configured to auto-lock after a pre-defined inactivity period. By default, if a password is defined, an Android device will automatically lock after one minute of inactivity, and the default Exchange ActiveSync policy setting applied for users not assigned to a mailbox policy sets an inactivity lock at 15 minutes. It is recommended that an inactivity timeout of no more than five (5) minutes be set for typical use cases, and one (1) or two (2) minutes depending on device capability for high-security use cases.

For full details, please refer to the CIS Security Configuration Benchmark for Microsoft Exchange Server 2007, version 1.1.0, Section 8.26: Require ActiveSync Inactivity Lockout Time.

Rationale:

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

Audit:

Using the Exchange Management Console (EMC):
In the "Properties" configuration window,

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

Using the Exchange Management Shell:
At the Exchange Management Shell command prompt:

1. Enter the following command (all one line)

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

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

2. Search the 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 5 or 1 according to use case as shown below:

```
MaxInactivityTimeDeviceLock :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 "Time without user input before password must be re-entered (in minutes)" checkbox. When this checkbox is checked, you may enter the time in minutes for the auto-lock timeout in the box on the right hand side.
3. Enter the following in the box on the right hand side:
    1. "5" for typical use cases
    2. "1" for high-security use cases
4. Click "OK".

Using the Exchange Management Shell:
At the Exchange Management Shell command prompt,

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

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

where <PolicyName> is the name of the Exchange ActiveSync mailbox policy for which the configuration should be made (replace brackets and text with appropriate policy name) and specifying the time in minutes as appropriate according to use case and device as described for the EMC above.

Impact:

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

3.1.6 Erase data upon excessive password failures (Scored)

Profile Applicability:

- Level 1
- Level 2

Description:

The device can be configured to reset itself to factory defaults (a local wipe) after excessive password failures. Android 2.3 supports a maximum of 31 password failures. The default Exchange ActiveSync policy setting applied for users not assigned to a mailbox policy configures the device to erase data after four (4) failed password attempts, if a password is configured on the device. It is recommended that this feature be enabled at six (6) failed password attempts.

For full details, please refer to the CIS Security Configuration Benchmark for Microsoft Exchange Server 2007, version 1.1.0, Section 8.24: Require ActiveSync Maximum Password Attempts.

Rationale:

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

Audit:

Using the Exchange Management Console (EMC):
In the "Properties" configuration window,

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

Using the Exchange Management Shell:
At the Exchange Management Shell command prompt,

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

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

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

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

Using the Exchange Management Shell:
At the Exchange Management Shell command prompt,

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

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

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

3.1.7 Require password expiration (Scored)

Profile Applicability:

- Level 2

Description:

Require ActiveSync passwords to expire every 60 days.

For full details, please refer to the CIS Security Configuration Benchmark for Microsoft Exchange Server 2007, version 1.1.0, Section 8.19: Require ActiveSync Password Expiration.

Rationale:

The longer a password is used the less secure it becomes. Require users to change passwords every 60 days or what is in sync with corporate security policies.

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, 60

In EMShell:

1. Enter

```
Set-ActiveSyncMailboxPolicy -identity <name> -DevicePasswordExpiration 60
```

3.1.8 Require password history (Scored)

Profile Applicability:

- Level 2

Description:

Store a password history of 5 passwords for ActiveSync.

For full details, please refer to the CIS Security Configuration Benchmark for Microsoft Exchange Server 2007, version 1.1.0, Section 8.20: Require ActiveSync Password History.

Rationale:

Storing password history ensures that passwords are not reused within a reasonable period of time.

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: 5

In EMShell:

1. Enter:

```
Set-ActiveSyncMailboxPolicy -identity <name> -DevicePasswordHistory 5
```

3.1.9 Require encryption (Scored)

Profile Applicability:

- Level 1
- Level 2

Description:

This controls the storage card encryption on the device.

For full details, please refer to the CIS Security Configuration Benchmark for Microsoft Exchange Server 2007, version 1.1.0, Section 8.21: Require ActiveSync Encryption.

Rationale:

Storage cards often hold downloaded attachments, contact lists, and other sensitive company information. Requiring ActiveSync encryption helps to minimize the risk in the case of a lost device or storage card.

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

4 Supplemental Materials

4.1 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
3. Android Forensics: http://www.syngress.com/digital-forensics/Android-Forensics/
4. Security policies supported by Android 4.0 in Microsoft Exchange Information Services: http://en.wikipedia.org/wiki/Comparison_of_Exchange_ActiveSync_clients

5. Android Software Development Kit (SDK) Documentation: http://developer.android.com/sdk/android-4.0.html
6. National Institute of Standards and Technology. (2006). NIST Special Publication 800-63: Electronic Authentication Guideline. Available: http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf. Last accessed 24 August 2010.
7. National Institute of Standards and Technology. (2008). NIST Special Publication 800-124: Guidelines on Cell Phone and PDA Security. Available: http://csrc.nist.gov/publications/nistpubs/800-124/SP800-124.pdf . Last accessed 24 August 2010.

4.2 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

4.2.1 General ActiveSync Settings

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

4.2.1.1 Disallow non-provisionable devices (Scored)

Profile Applicability:

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" checkbox is unchecked.
8. Click "Cancel".

Using the Exchange Management Shell:

1. Open the Exchange Management Shell.

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

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

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

3. Search the outputted policy setting list for the "AllowNonProvisionableDevices :" configuration item.

4. Observe if the value following the colon is "False" as shown below:

AllowNonProvisionableDevices : False

5. Exit the Exchange Management Shell.

Remediation:

Using the Exchange Management Console (EMC):

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

Using the Exchange Management Shell:

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

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

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

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

Appendix: Change History

Date	Version	Changes for this version