the CENTER for INTERNET SECURITY

Security Configuration Benchmark For

Google Android 2.3 (Gingerbread)

Version 1.0.0

December 1, 2011

http://cisecurity.org

feedback@cisecurity.org

Terms of Use Agreement

Background

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

No representations, warranties and covenants

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

User agreements

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

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

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

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

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

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

Grant of limited rights

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

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

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

Retention of intellectual property rights, limitations on distribution

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

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

Special rules

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

Choice of law, jurisdiction; venue

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

Table of Contents

Overview

This document, *Security Configuration Benchmark for Android 2.3*, provides prescriptive guidance for establishing a secure configuration posture for the Android 2.3 OS. This guide was tested against the Android 2.3 and the Android Virtual Device (AVD) contained in version 2.3.3 of the Android Software Development Kit (SDK). This benchmark covers Android 2.3 and all hardware devices on which this OS is supported. As of the publication of this guidance, mobile devices supported by Android 2.3include the following:

- HTC: the Incredible S, Google Nexus 1, Sensation 4G
- Motorola: Droid X, Droid 3, Galaxy S ii
- Archos: 7C Home Tablet
- Vizio: Tablet

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.

Consensus Guidance

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

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

Intended Audience

This document is intended for system and application administrators, security specialists, auditors, help desk, end users, and platform deployment personnel who plan to use, develop, deploy, assess, or secure solutions that use Android 2.3.

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, CISSP CSSLP

Maintainers
Robert Fritz, CISSP, CSSLP

Editors
Steven Piliero, *Center for Internet Security*

Testers
Robert Fritz, CISSP, CSSLP

Contributors and Reviewers
Yves Desharnais
John Fox, *Athigo*
Blake Frantz, *Center for Internet Security*
Billy Glenn, *Pacific Gas & Electric*
Molly Maguire
Steven Piliero, *Center for Internet Security*
Fernando Trias, *Athigo*
Jonathan Trull, *State of Colorado*

Typographic Conventions

The following typographical conventions are used throughout this guide:

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

Configuration Levels

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

Level-I Benchmark settings/actions

Level-I Benchmark recommendations are intended to:

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

Level-II Benchmark settings/actions

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

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

Scoring Status

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

Scorable

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

Not Scorable

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

Recommendations

The settings recommended in this benchmark are those available through configuration of the device 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 consideredboth as a target itself and as a method of accessing other resources. These benchmarksettings 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.

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 2.3 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 2.3, see:
http://www.google.com/help/hc/pdfs/mobile/ExchangeAndAndroid2.2and2.3-003.pdf

1. Settings in the Android User Interface

This section provides guidance on the secure configuration of Android2.3 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 (Level 1, Not Scorable)

Description:
An Android2.3 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 2.3.3, with kernel version 2.6.29for these benchmark recommendations to apply; if a newer version of the firmware is available, some recommendations may not apply.

Remediation:
Contact your telecommunications provider for their latest supported update.

Audit:

1. Press the Menu button.
2. Tap Settings.
3. Tap About Phone.
4. Confirm that Build number contains 2.3.3 and Kernel version contains 2.6.29.

Default State:
N/A

Reference:

1. Android 2.3 User Guide
   http://www.google.com/googlephone/AndroidUsersGuide-2.3.pdf

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

Description:
Android2.3 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.

Remediation:

1. Press the Menu button.
2. Tap Settings.
3. Tap Location & Security.
4. Tap Set up screen lock.

5. Tap Password.
6. Tap in a complex password. (See reference below)
7. Tap in the same complex password.

Audit:
1. Press the Menu button.
2. Tap Settings.
3. Tap Location & Security.
4. Tap Change screen lock.
5. Verify that "Change screen lock" is an option under the "Screen unlock" section.

Default State:
Not Set

Reference:
1. Android 2.3 User Guide
   http://www.google.com/googlephone/AndroidUsersGuide-2.3.pdf
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 Configure an alphanumeric value (Level 2, Not Scorable)

See 1.1.2 above. This setting is the same as the setting in Section 3.1.2.

1.1.4 Set Screen timeout (Level 1, Not Scorable)

Description:
An Android2.3 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.

Remediation:
1. Press the Menu button.
2. Tap Settings.
3. Tap Display.
4. Tap Screen timeout.

4a. For typical use cases, tap "2 Minutes".
4b. For high-security use cases, tap "1 Minute".

Audit:
1. Press the Menu button.
2. Tap Settings.
3. Tap Display.
4. Tap Screen timeout.

4a. For typical use cases, confirm that Screen timeout is set to 2 minutes.
4b. For high-security use cases, confirm that Screen timeout is set to 1 minute.

Default State:
1 Minute

Reference:
1. Android 2.3 User Guide
   http://www.google.com/googlephone/AndroidUsersGuide-2.3.pdf

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

See 3.1.6. This setting can be controlled using Microsoft Exchange, Active Sync mailbox policies.

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

Description:
An Android 2.3 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.

Remediation:
1. Press the Menu button.
2. Tap Settings.
3. Tap Wireless & network settings.
4. Tap Wi-Fi settings.
5. In the Wi-Fi network section, locate the network SSID and tap and hold down the entry for the network you wish to forget.
6. Tap "Forget" in the confirmation dialog.

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.

Audit:
1. Press the Menu button.
2. Tap Settings.
3. Tap Wireless & network settings.
4. Tap Wi-Fi settings.
5. Confirm that all deleted Wi-Fi networks are forgotten.

Default State:
Networks are remembered as used.

Reference:
1. Android 2.3 User Guide
   http://www.google.com/googlephone/AndroidUsersGuide-2.3.pdf

1.1.7 Turn off Network Notification (Level 2, Not Scorable)

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").

Remediation:
1. Press the Menu button.
2. Tap Settings.
3. Tap Wi-Fi Settings.
4. Turn off "Network notification."

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

Audit:
1. Press the Menu button.
2. Tap Settings.
3. Tap Wi-Fi Settings.
4. Confirm that "Network notification" is unchecked.

Default State:
Notification enabled

Reference:
1. Android 2.3 User Guide
   http://www.google.com/googlephone/AndroidUsersGuide-2.3.pdf

1.1.8 Turn off Auto-Join for all Wi-Fi networks (Level 1, Not Scorable)

Not applicable. Android 2.3 does not automatically join new networks.

This setting is listed here for completeness because it is included in the CIS Benchmark for Apple iOS.

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

Description:
Android2.3 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.

Remediation:
1. Press the Menu button.
2. Tap Settings.
3. Tap Wireless & networks.
4. Tap Wi-Fi if box is checked.

Audit:
1. Press the Menu button.
2. Tap Settings.
3. Tap Wireless & networks.
4. Confirm that Wi-Fi is unchecked.

Default State:
Disabled

Reference:
1. Android 2.3 User Guide
   http://www.google.com/googlephone/AndroidUsersGuide-2.3.pdf

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

Not applicable. Android 2.3 devices do not automatically connect to VPNs.

This setting is listed here for completeness because it is included in the CIS Benchmark for Apple iOS.

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

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

Rationale:

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

Remediation:

1. Press the Menu button.
2. Tap Settings.
3. Tap Wireless & networks.
4. Tap Bluetooth if option is checked.

Audit:

1. Press the Menu button.
2. Tap Settings.
3. Tap Wireless & networks.
4. Confirm that Bluetooth is unchecked.

Default State:
Bluetooth Disabled

Reference:

1. Android 2.3 User Guide
   http://www.google.com/googlephone/AndroidUsersGuide-2.3.pdf

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

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:
Android2.3 enables the user to enable or deny Internet websites to access to location services. In addition, any application in Android 2.3 may send location data if location data is available to the phone itself.

Remediation:

1. Tap the globe Browser icon.
2. Press the Menu button.
3. Tap More.
4. Tap Settings.
5. Scroll down and uncheck "Enable location."

1. Tap Home.
2. Press the Menu button.
3. Tap Location & security.
4. Scroll down to "Security Settings."

5. Uncheck "Use wireless networks" and "Use GPS satellites."

Audit:

1. Tap the globe Browser icon.
2. Press the Menu button.
3. Tap More.
4. Tap Settings.
5. Confirm that "Enable location" is unchecked.
6. Tap Home.
7. Press the Menu button.
8. Tap Location & security.
9. Scroll down to "Security Settings."
10. Confirm that "Use wireless networks" and "Use GPS satellites" are unchecked.

Default State:

Browser location data, Use wireless networks, and Use GPS satellites all default to enabled.

Reference:

1. Android 2.3 User Guide http://www.google.com/googlephone/AndroidUsersGuide-2.3.pdf

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

Description:

Mobile devices running Android 2.3 can be configured to disable all receivers and transceivers. This option is called Airplane Mode or Flight Mode. When Airplane Mode is on, no phone, GPS, radio, Wi-Fi, or Bluetooth signals are emitted from or received by the device. It is recommended that Airplane Mode be enabled when these capabilities are unneeded or where security is paramount.

Rationale:

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

Remediation:

1. Press the Menu button.
2. Tap Settings.
3. Tap Wireless & networks.
4. Uncheck Airplane Mode.

Audit:

1. Press the Menu button.
2. Tap Settings.
3. Tap Wireless & networks.
4. Confirm that Airplane Mode is unchecked.

Default State:

Airplane mode is disabled.

Reference:

1. Android 2.3 User Guide
   http://www.google.com/googlephone/AndroidUsersGuide-2.3.pdf

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

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.

Remediation:

1. Press the Menu button.
2. Tap Settings.
3. Tap Privacy.
4. Tap Factory data reset.
5. Check "Erase SD card."

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.

Default State:
N/A

References:

1. Android 2.3 User Guide
   http://www.google.com/googlephone/AndroidUsersGuide-2.3.pdf
2. Android Forensics
   http://www.syngress.com/digital-forensics/Android-Forensics/

1.1.15 Disable SMS preview when Android is locked (Level 2, Not Scorable)

Description:
If the Android2.3 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.

Remediation:

1. Tap Messaging.
2. Press the Menu button.
3. Tap Settings.
4. Uncheck the "Notifications" setting.

Audit:

1. Tap Messaging.
2. Press the Menu button.
3. Tap Settings.
4. Confirm that the "Notifications" setting is unchecked.

Default State:
SMS preview is enabled by default.

Reference:

1. Android 2.3 User Guide
   http://www.google.com/googlephone/AndroidUsersGuide-2.3.pdf

1.1.16 Set up SIM card lock (Level 1, Not Scorable)

Description:
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.

Remediation:

1. Press the Menu button.
2. Tap Location and security.
3. Tap Set up SIM card lock.
4. Check Lock SIM card.
5. Type in new SIM PIN on Lock SIM card dialog.

Audit:

1. Press the Menu button.
2. Tap Location and security.
3. Tap Set up SIM card lock.
4. Ensure Lock SIM card is checked.

Default State:
SIM card is disabled.

Reference:

1. Android 2.3 User Guide
   http://www.google.com/googlephone/AndroidUsersGuide-2.3.pdf

1.1.17 Disable visible passwords (Level 1, Not Scorable)

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.

Remediation:
1. Press the Menu button.
2. Tap Settings.
3. Tap Location and security.
4. Uncheck Visible passwords.

Audit:
1. Press the Menu button.
2. Tap Settings.
3. Tap Location and security.
4. Verify Visible passwords in unchecked.

Default State:
Visible passwords is enabled by default.

Reference:
1. Android 2.3 User Guide
   http://www.google.com/googlephone/AndroidUsersGuide-2.3.pdf

1.1.18 Encrypt credentials storage (Level 2, Not Scorable)

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.

Rationale:
Encrypting the credential store and removing application access to secure credentials limits the exposure of personal data to solely that which is on the device. Using these settings together protects against both local attack, application attack, and some forms of remote attack.

Remediation:
1. Press the Menu button.
2. Tap Settings.
3. Tap Location and security.
4. Scroll down to "Credential storage" section.

5. Tap Set password.
6. Type and confirm new password in dialog box.
7. Tap OK.
8. Uncheck Use secure credentials.

Audit:

1. Press the Menu button.
2. Tap Settings.
3. Tap Location and security.
4. Scroll down to "Credential storage" section.
5. Confirm that Use secure credentials option is not grayed-out and is unchecked.

Default State:
Secure credential storage is disabled by default.

Reference:

1. Android 2.3 User Guide
   http://www.google.com/googlephone/AndroidUsersGuide-2.3.pdf

1.1.19 Disable development features (Level 1, Not Scorable)

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.

Remediation:

1. Press the Menu button.
2. Tap Settings.
3. Tap Applications.
4. Tap Development.
5. Uncheck USB debugging.
6. Uncheck Stay awake.
7. Uncheck Mock locations.

Audit:

1. Press the Menu button.
2. Tap Settings.
3. Tap Applications.
4. Tap Development.
5. Confirm that USB debugging is unchecked.
6. Confirm that Stay awake is unchecked.
7. Confirm that Mock locations is unchecked.

Default State:
SDK virtual device enables developer options by default. Carrier phones likely disable by default.

Reference:
1. Android 2.3 User Guide
   http://www.google.com/googlephone/AndroidUsersGuide-2.3.pdf

1.1.20 Disallow application installsfrom unknown source (Level 1, Not Scorable)

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.

Remediation:
1. Press the Menu button.
2. Tap Settings.
3. Tap Applications.
4. Uncheck Unknown sources.

Audit:
1. Press the Menu button.
2. Tap Settings.
3. Tap Applications.
4. Confirm Unknown sources isunchecked.

Default State:
SDK virtual device enables developer options by default. Carrier phones likely disable by default.

Reference:
1. Android 2.3 User Guide
   http://www.google.com/googlephone/AndroidUsersGuide-2.3.pdf

1.2 Browser Settings

This section provides guidance on the secure configuration of settings related to the built-in browser on Android 2.3 mobile devices.

1.2.1 Disable JavaScript (Level 2, Not Scorable)

Description:
JavaScript lets web programmers control elements of the page, for example: a page that uses JavaScript might display the current date and time or cause a linked page to appear in

a new pop-up page. It is recommended that JavaScript and plug-ins be disabled in environments where security is paramount.

Rationale:
JavaScript should only be enabled before browsing trusted sites.

Remediation:
1. Tap the globe Browser icon.
2. Tap Settings.
3. Scroll down to Enable Java Script.
4. Uncheck JavaScript.
5. Tap Enable plug-ins.
6. Select "Off."

Audit:
1. Tap the globe Browser icon.
2. Tap Settings.
3. Scroll down to Enable Java Script.
4. Confirm that JavaScript is unchecked.
5. Tap Enable plug-ins.
6. Confirm that "Off" is checked.

Default Status:
JavaScript is enabled by default.

Reference:
1. Android 2.3 User Guide http://www.google.com/googlephone/AndroidUsersGuide-2.3.pdf

1.2.2 Enable basic SSL checks for websites (Level 1, Not Scorable)

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.

Remediation:
1. Tap the globe Browser icon.
2. Tap Settings.
3. Scroll to Security settings.
4. Check "Show security warnings."

Audit:
1. Tap the globe Browser icon.
2. Tap Settings.
3. Scroll to Security settings.

4. Ensure "Show security warnings" is checked.

Default Status:
Show security is enabled by default.

Reference:
1. Android 2.3 User Guide
   http://www.google.com/googlephone/AndroidUsersGuide-2.3.pdf

1.2.3 Disable Remember Form Data (Level 2, Not Scorable)

Description:
The browser has a feature to remember information entered into common forms in order to automate the completion of later forms. Information auto-filled can include 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.

Remediation:
1. Tap the globe Browser icon.
2. Press the Menu button.
3. Tap More.
4. Tap Settings.
5. Scroll to "Privacy Settings."
6. Tap Clear form data, and tap "OK" on the confirmation dialog.
7. Uncheck Remember form data.
8. Scroll to "Security Settings."
9. Tap Clear passwords and tap "OK" on the confirmation dialog.
10. Uncheck Remember passwords.

Audit:
1. Tap the globe Browser icon.
2. Press the Menu button.
3. Tap More.
4. Tap Settings.
5. Scroll to "Privacy Settings."
6. Confirm Remember Form Data is unchecked.
7. Scroll to "Security Settings."
8. Confirm Remember passwords is unchecked.

Default Status:
Remember form data is enabled by default.

Reference:

1. Android 2.3 User Guide
   http://www.google.com/googlephone/AndroidUsersGuide-2.3.pdf

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-2.3.4.html

3. Android Mobile Device Settings in MS Exchange ActiveSync Policy

This section provides guidance on the configuration of certain policies on Android mobile devices using Microsoft Exchange ActiveSync versions 2.5 and later. This guidance was developed and tested specifically with Exchange ActiveSync version 3.5 with the Client Access server role on Microsoft Exchange Server 2010, and updated to reflect the relevant configurations for this benchmark.

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

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

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

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

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

Please note Android 2.3 phone 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 2.3, see:
http://static.googleusercontent.com/external_content/untrusted_dlcp/www.google.com/en//help/hc/pdfs/mobile/ExchangeAndAndroid2.2and2.3-003.pdf

3.1 Password Settings

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

3.1.1 Require password on device (Level 1, Scorable)

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.

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.

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).

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

Reference:

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

3.1.2 Require alphanumeric value (Level 2, Scorable)

Description:

The devicecan 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.

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.

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).

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,

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

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

   where<*PolicyName*> is the name of the Exchange ActiveSync mailbox policy for which the audit validation should be made (replace brackets and text with appropriate policy name).
2. Search the outputted policy setting list for the "AlphanumericDevicePasswordRequired :" configuration item.
3. Observe if the value following the colon is "True" as shown below:
   ```
   AlphanumericDevicePasswordRequired :True
   ```
4. Exit the Exchange Management Shell.

Reference:

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

3.1.3 Set minimum password length (Level 1, Scorable)

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.

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 2.3 supports passwords of up to 16 characters.

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>"
-MinDevicePasswordLength5
```

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

Audit:

Using the Exchange Management Console (EMC):

In the "Properties" configuration window,

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

Using the Exchange Management Shell:

At the Exchange Management Shell command prompt,

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

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

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

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

```
MinDevicePasswordLength : 5
```

4. Exit the Exchange Management Shell.

Reference:

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

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

This Exchange policy is not supported by Android 2.3.

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

Description:

The device can be configured to auto-lock after a pre-defined inactivity period. By default, if a 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.

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.

Remediation:

Using the Exchange Management Console (EMC):

In the "Properties" configuration window,

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

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

3b. For high-security use cases, enter the number 1.

4. Click "OK".

Using the Exchange Management Shell:

At the Exchange Management Shell command prompt,

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

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

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

Audit:

Using the Exchange Management Console (EMC):

In the "Properties" configuration window,

1. Click on the "Password" tab.
2. Observe if the "Time without user input before password must be re-entered (in minutes)" checkbox is selected.
3. Observe if the auto-lock timeout value is set to 5 or 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 outputted policy setting list for the "MaxInactivityTimeDeviceLock:"configuration item.
3. Observe if there is a value following the colon and that the value is set to 5 or 1according to use case as shown below:

```
MaxInactivityTimeDeviceLock :5
```

4. Exit the Exchange Management Shell.

Reference:

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

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

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.

Rationale:

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

Remediation:

Using the Exchange Management Console (EMC):

In the "Properties" configuration window,

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

Using the Exchange Management Shell:

At the Exchange Management Shell command prompt,

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

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

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

Audit:

Using the Exchange Management Console (EMC):

In the "Properties" configuration window,

1. Click on the "Password" tab.
2. Observe if the "Number of failed attempts allowed:" checkbox is selected.

3. Observe if the failed attempts value is set to 6.
4. Click "Cancel".

Using the Exchange Management Shell:

At the Exchange Management Shell command prompt,

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

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

   where<*PolicyName*> is the name of the Exchange ActiveSync mailbox policy for which the audit validation should be made (replace brackets and text with appropriate policy name).
2. Search the outputted policy setting list for the "MaxDevicePasswordFailedAttempts" configuration item.
3. Observe if there is a value following the colon and that the value is set to 6 as shown below:

   ```
   MaxDevicePasswordFailedAttempts : 6
   ```
4. Exit the Exchange Management Shell.

Reference:

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

Appendix A:References

1. Android 2.3 User Guide
   http://www.google.com/googlephone/AndroidUsersGuide-2.3.pdf

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 2.3 in Microsoft Exchange Information Services
   http://static.googleusercontent.com/external_content/untrusted_dlcp/www.google.com/en//help/hc/pdfs/mobile/ExchangeAndAndroid2.2and2.3-003.pdf

5. Android Software Development Kit (SDK) Documentation
   http://developer.android.com/sdk/android-2.3.4.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.

Appendix B: Change History

Date	Version	Changes for this version
September 18, 2011	0.1	- Draft adopted from iOS benchmark document version 1.3.0.
September 25, 2011	0.2	- Added Bluetooth default
October 23, 2011	0.3	- Incorporated community comments.
December 1, 2011		- Published

Appendix C: Additional Security Notes

The items in this section are security configuration settings that are available within the Android 2.3 operating system, but have been determined to provide relatively little incremental security benefit, either due to other settings in the benchmark document or inherent applicability or effectiveness as a control.

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

C.1 Set maximum password age (Informational)

This configuration setting is not available in Android 2.3.

C.2 Set password history (Informational)

This configuration setting is not available in Android 2.3.

C.3 General sync settings (Informational)

Description:
Android operating system allows applications to manage and synchronize data automatically. If the mobile phone user utilizes applications like email, this can be useful to avoid having to wait for the application to download while the user is using the application. If the user does not use applications like this, then there is no reason to allow applications to control dataflow asynchronously.

Rationale:
Limiting the access applications have to the network and your data minimizes perform activities that are not directly relevant to user requests.

Remediation:

1. Press the Menu button.
2. Tap Settings.
3. Tap Accounts & sync.
4. Uncheck Auto-sync.
5. Uncheck Background data.
6. Tap OK.

Audit:

1. Press the Menu button.
2. Tap Settings.
3. Tap Accounts & sync.
4. Confirm that Auto-sync and Background data are unchecked.

Default Status:
Auto-sync and background data are enabled by default.

Appendix D: Additional Information for Exchange ActiveSync Management

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

Security configuration items that can be applied include the initiation of a remote wipeof 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

D.1 General ActiveSync Settings

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

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

Description:

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

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

Rationale:

Restricting the devices which can connect to MS Exchange through ActiveSync to only those which can fully support the policy specified is the only way that Exchange ActiveSync can assure that an 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.

Remediation:

Using the Exchange Management Console (EMC):

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

Using the Exchange Management Shell:

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

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

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

Audit:

Using the Exchange Management Console (EMC):

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

Using the Exchange Management Shell:

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

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

   where<*PolicyName*> is the name of the Exchange ActiveSync mailbox policy for which the audit validation should be made (replace brackets and text with appropriate policy name).
3. Search the outputted policy setting list for the "AllowNonProvisionableDevices :" configuration item.
4. Observe if the value following the colon is "False" as shown below:

```
AllowNonProvisionableDevices : False
```

5. Exit the Exchange Management Shell.

Reference:

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

D.2 General Resources for 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