GOV.UK

Guidance

End User Devices Security Guidance: Android 4.4

Published 10 June 2014

Contents

This guidance is applicable to devices running Android 4.4.x. This guidance was developed following testing performed on Nexus 5 and Motorola Moto G devices running Android 4.4.

1. Changes since previous guidance

This document is an update of the previous Android 4.3 guidance made to cover Android 4. 4 No changes to the recommended configuration have been made, although references are now made to the SELinux policies included in Android 4.4 in enforcing mode, device monitoring warnings, certificate pinning and verified boot.

2. Usage Scenario

Android devices will be used remotely over 3G, 4G and non-captive Wi-Fi networks to enable a variety of remote working approaches such as accessing OFFICIAL email; reviewing and commenting on OFFICIAL documents, and accessing the internet and other web-resources.

To support these scenarios, the following architectural choices are recommended:

- All data should be routed over a secure enterprise VPN to ensure the confidentiality and integrity of the traffic, and to allow the devices and data on them to be protected by enterprise protective monitoring solutions. The

VPN should be configured in always-on mode where possible.

- Arbitrary third-party application installation by users is not permitted on the device. An enterprise application catalogue should be used to whitelist and distribute approved applications to devices.

3. Summary of Platform Security

This platform has been assessed against each of the twelve security recommendations, and that assessment is shown in the table below. Explanatory text indicates that there is something related to that recommendation that the risk owners should be aware of. Rows marked [!] represent a more significant risk. See How the Platform Can Best Satisfy the Security Recommendations for more details about how each of the security recommendations is met.

Recommendation	Rationale
1. Assured data-in-transit protection	The VPN can be disabled by the user. The built-in VPN has not been independently assured to Foundation Grade, and no suitable assured third-party products exist.
2. Assured data-at-rest protection	Android data encryption has not been independently assured to Foundation Grade. Encryption keys protecting sensitive data remain in device memory when the device is locked.
3. Authentication	
4. Secure boot	
5. Platform integrity and application sandboxing	
6. Application whitelisting	Users can run applications from unapproved sources.*
7. Malicious code detection and prevention	
8. Security policy enforcement	[!] MDM control can be disabled by the user. The MDM APIs only offer a limited set of controls.*
9. External interface protection	Interfaces such as USB, Wi-Fi, and Bluetooth cannot be controlled by policy.*
10. Device update policy	The enterprise cannot force the user to update their device software.
11. Event collection for enterprise analysis	[!] There is no facility for collecting detailed logs remotely from a device.
12. Incident response	

Some vendors implement proprietary extensions allowing more comprehensive security policies to be enforced by the MDM. For example, Samsung SAFE enables risks associated with requirements 6, 8 and 9 (marked with asterisks) to be effectively mitigated.

3.1 Significant Risks

The following significant risks have been identified:

- The VPN has not been independently assured to Foundation Grade, and currently does not support some of the mandatory requirements expected from assured VPNs. Without assurance in the VPN there is a risk that data transiting from the device could be compromised.
- The VPN can be disabled by the user, leading to potential for data leakage onto untrusted networks.
- Android data encryption has not been independently assured to Foundation Grade, and does not support some of the mandatory requirements expected from assured full disk encryption products. Without assurance there is a risk that data stored on the device could be compromised.
- Android devices do not use any dedicated hardware to protect data encryption keys. If an attacker can get physical access to the device, they can extract password hashes and perform an offline brute-force attack to recover the encryption password.
- Encryption keys protecting sensitive data remain in device memory when the device is locked. This means that if the device is attacked while powered on and locked, keys and data on the device may be compromised without the attacker knowing the password.
- Data stored on the emulated SD card (the “data” partition) will be encrypted during the device encryption process. However if a specific manufacturer chooses to store enterprise data anywhere external to this partition it will not be encrypted. Android does not provide native support for encryption of external SD cards.
- Any sensitive data stored on the external SD card (on devices which support this), will not be erased by the wipe operation.
- Procedural controls are used to achieve some of the requirements where no technical controls could be used, which means that users have to be trusted not to alter certain settings on the device, or perform actions which may impact the security of the device. These controls are discussed in later sections.
- Users can choose not to apply device updates, this may lead to security issues not being patched.
- Users can install unauthorised apps (e.g. from the Play store) which have not been approved by an administrator. A malicious or vulnerable application which was not detected during the store’s automated reviews could exfiltrate or leak sensitive data from the device.
- User may override security policy relating to external interfaces. Enabling external interfaces means additional attack surface could be exposed and data could be inadvertently or maliciously leaked without enterprise visibility.

4. How the Platform Can Best Satisfy the Security Recommendations

This section details the platform security mechanisms which best address each of the security recommendations.

4.1 Assured data-in-transit protection

Use the native IPsec VPN client until a Foundation Grade VPN client for this platform becomes available.

4.2 Assured data-at-rest protection

Use the device's native data encryption. The data is protected when powered off, but it is not protected when the device is locked.

4.3 Authentication

The user has a strong 9-character password to authenticate to the device. There is no dedicated hardware protection for Android passwords. Android provides native support for the use of X.509v3 client certificates, which can be saved into the device's credential storage area during provisioning. The native mail and Chrome browser applications are able to use these. This device-specific client certificate can be used to provide two-factor authentication to services.

4.4 Secure boot

Administrators should only provision Android devices with locked bootloaders.

On most devices unlocking the bootloader should wipe a device, however if the bootloader is unlocked at provisioning time, or unlocked by exploiting a platform vulnerability, then the device will remain in an insecure state.

It is possible to unlock a device, modify it, and then relock it. It cannot be assumed that any device received other than directly from the vendor, is in its original state. The kernel dm-verity functionality could be used to protect against such modifications if supported by the vendor.

4.5 Platform integrity and application sandboxing

This requirement is met by the platform without additional configuration. SELinux in enforcing mode significantly enhances platform integrity and sandboxing.

4.6 Application whitelisting

Whitelisting is not supported as standard on Android platforms. Specific handset manufacturers have enhanced the Android operating system to provide this functionality which can be then be enforced through a supporting MDM solution.

4.7 Malicious code detection and prevention

Several third-party anti-malware products exist which attempt to detect malicious code for this platform and can be used if desired. Where possible an enterprise application catalogue can be used which should only contain vetted apps. Content-based attacks can be filtered by scanning capabilities in the enterprise.

Google Play scans applications for potentially harmful or malicious activity prior to making them available for download. Side-loaded applications are scanned automatically by the Google Play application on devices with this application installed and enabled.

Android 4.4 shows an alert if trusted credentials are installed that enable the ability to intercept encrypted communications. Certificate pinning is also used in certain Google applications to prevent interception and modification of SSL traffic. The potential to use certificate pinning for non-vendor applications is also possible but would need to be managed via an MDM supporting such functionality.

4.8 Security policy enforcement

The security policy can be managed centrally via the MDM to enforce security settings, however some security related settings are configured only by the user, including those for VPN and Bluetooth. The user can also disable the MDM via the settings menu.

4.9 External interface protection

No technical controls exist to prevent users from enabling Wi-Fi and Bluetooth, or using USB. It is possible to reduce the opportunity to attack some devices via USB by disabling USB debugging completely, or enabling Secure USB debugging on devices running Android 4.2.2 or later.

4.10 Device update policy

MDM software can be used to audit which apps and OS versions are installed on a device. The enterprise cannot control when the applications or OS software are updated. These updates rely on user interaction. Carriers are responsible for rolling out device updates in a timely manner. As the average duration to patch varies between manufacturers and carriers, care should be taken when choosing which platforms to deploy to ensure that the selected manufacturers and carriers have a good historic record of patching devices.

4.11 Event collection for enterprise analysis

Android does not support remote or local historic detailed event collection. It is not possible to display or collect many security related events, including failed device logins. MDM servers can be used to retrieve some information from the device, such as:

- Installed applications
- Android version information
- Last time device seen by MDM
- Compliancy status (depending on the compliancy rules setup on the MDM server)

- Enrolment status
- Location information
- Roaming Status

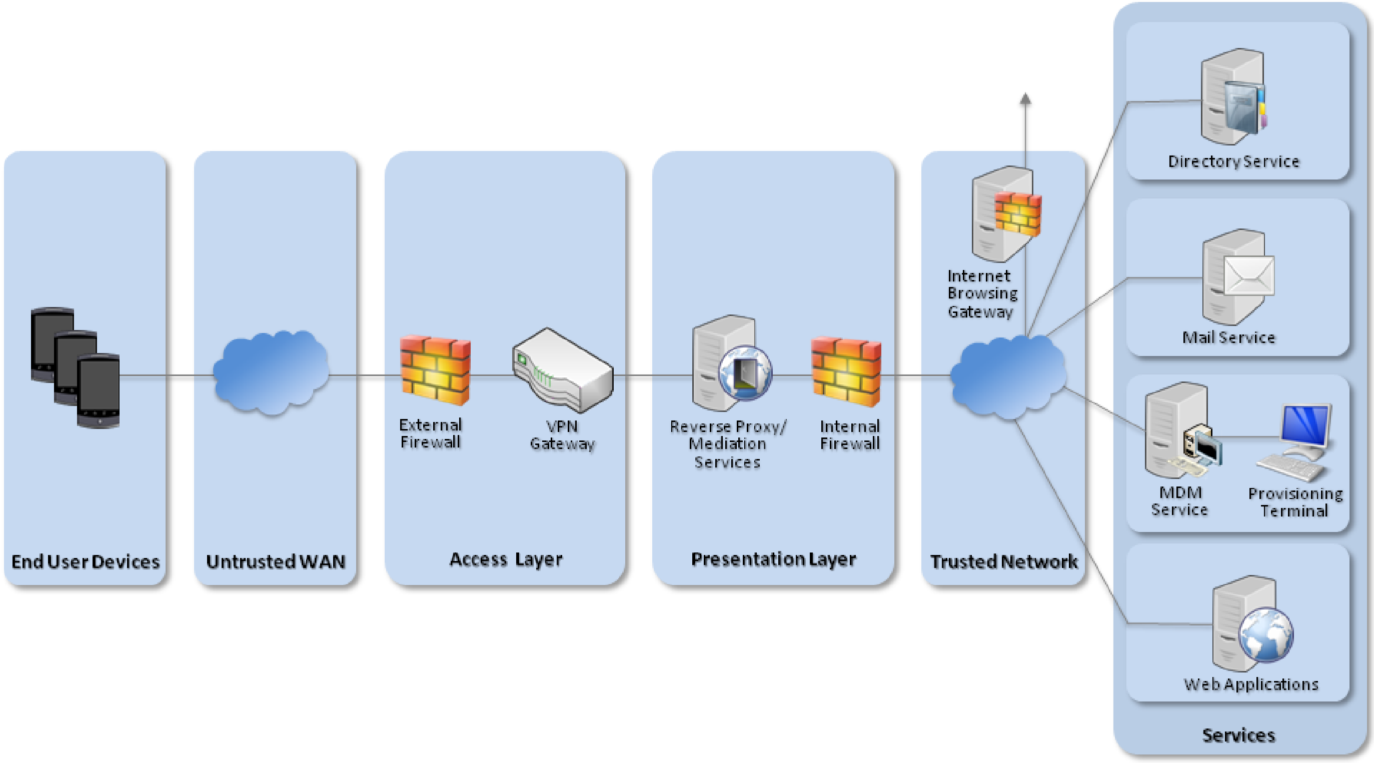
4.12 Incident response

Android's administrative API provides support for wiping the contents of the device's internal storage. This includes both the /data partition and the emulated SD card if present. MDMs which support this API can be used to remotely wipe devices if lost or stolen.

Access to the enterprise network can be prevented by revoking the VPN client certificate associated with a lost or stolen device, though this should only be done after the remote wipe command has been confirmed or a certain amount of time has passed; otherwise the device will be unable to connect to the MDM server to receive the wipe command. Additionally, the client certificates for any other enterprise servers (such as email) that are stored on the device should be revoked.

5. Network Architecture

It is recommended that all remote or mobile working scenarios use a typical remote access architecture based on the Walled Garden Architectural Pattern.



Recommended network architecture for Android 4.4 deployments

6. Deployment Process

For an enterprise deployment of Android devices that is suitable for organisations working with OFFICIAL data, administrators should:

1. Deploy and configure the requisite network components as described above
2. Procure and set up an MDM server that is compatible with Android and is able enforce all the settings given in the Policy Recommendations section below.
3. Create MDM security profiles for the Android devices in line with the guidance given in Policy Recommendations section, and associate these profiles with the devices.

7. Provisioning Steps

The following steps should be followed to provision each end user device onto the enterprise network to prepare it for distribution to end users.

1. Provision CA and client certificates by either:
    1. Provision the client certificates using a locally-enrolled MDM server;
    2. Deploy the Android Development Tools (ADT) bundle and device-specific USB drivers onto a dedicated provisioning terminal. This will allow the client certificates to be manually deployed onto the device via the Android Debug Tool (adb). Note that access from previously authorised computers should be revoked and USB debugging should be disabled once provisioning is complete.
    3. Installing .cer files using the browser over a trusted network or SD card

    Note it may be necessary to load client certificates onto the device through the MDM to ensure these certificates are wiped from the device should a user attempt to deactivate the MDM device administrator – this may require the install of a third-party email client):

    Certificates needed are:

    - Enterprise CA certificate (used to validate the server certificates presented by the VPN endpoint and reverse proxy)
    - VPN client certificate (for authentication to the enterprise VPN endpoint)
    - SSL client certificate (for authentication to the reverse proxy for intranet services).
2. Install the MDM agent app, and enrol the device into the MDM
3. Install any apps required for enterprise productivity, including a supported secure e-mail client.
4. Ensure that only trusted apps are installed and enabled on the device (disable unnecessary apps including Google Play)
5. Configure on-device security settings
6. Configure the VPN client to connect to the enterprise VPN endpoint, using the device-specific client certificate that has been loaded onto the device. Enable ‘Always-On’ VPN.

7. Configure the email client to connect to the enterprise server using client certificate authentication.

8. Policy Recommendations

The following settings should be applied from the MDM interface. As all MDMs vary, the text accompanying the setting may be slightly different to that shown below.

Policy Setting	**Recommended Value**
Enrolment Rules	Enrolment of devices is only possible for an approved administrator as part of the device provisioning process
Compliance Rules	If a non-whitelisted application is detected on the device, take appropriate mitigating action such as notifying an administrator or blocking further access to corporate resources.
Email Rules	Access should be prevented for non-enrolled devices.
Password Complexity	
Allow non-provisioned devices	False
Require password	True
Require complex password	True
Minimum number of upper case characters	1
Minimum number of lower case characters	1
Minimum number of symbols	1
Require encryption on device	True
Allow simple password	No
Number of failed attempts allowed	5
Minimum password length	9
Time without user input before password must be re-entered	10 (minutes)
Password expiration	90 (days)
Enforce password history	8

Show Data on Lock Screen Widgets	False

ActiveSync Settings (if used)

Enable Security Restrictions	True
Allow Data Backup	False

9. Enterprise Considerations

The following points are in addition to the common enterprise considerations, and contain specific issues for Android deployments.

9.1 VPN

On Android users can alter the configuration of the VPN which can adversely affect the security of the device. Procedural controls must be present in the user security procedures to prohibit the altering of any settings related to the VPN.

9.2 Cloud Integration

Android devices do not need to be associated with a Google account to operate as required within the enterprise. For example, it is still possible to receive push notifications through Google Cloud Messaging, and Google Play can scan installed apps without using a Google account. Procedural controls will therefore be necessary to prevent users from associating their device with a Google account and potentially storing sensitive data in the cloud.

9.3 Privacy Concerns

Android devices are usually configured by default to send anonymous usage data (including location, device ID etc.) to Google servers. This can be disabled through device settings and will need to be enforced through procedural controls. Applications will often use application tracking services that may leak device information. These may be monitored and blocked when a VPN is active. Android 4.4 may use location services and generate Wi-Fi beacons even when in airplane mode. This configuration can be disabled in advanced Wi-Fi settings.

9.4 Application Whitelisting

It is recommended that Android devices which have been enhanced by the manufacturers to support application whitelisting via the MDM are selected.

9.5 Time to Patch

Due to the number of separate entities involved in the creation, approval and distribution of updates for Android devices the time between a vulnerability being exposed and an update being made available for a specific device can vary considerably. When selecting Android devices, it is important to select a device vendor and carrier who have a good track record of supporting the latest released platforms and releasing security fixes promptly.

Legal Information

This guidance is issued by CESG, the UK's National Technical Authority on Information Assurance. One of the roles of CESG is to provide advice to UK government entities and organisations providing services to UK government. The guidance found here is provided and intended for use by this audience. It is provided 'as-is' as an example of how specific requirements could be met. It should be used to help inform risk management decisions on the use of the products described, but it should not be used for procurement decisions; it is not intended to be exhaustive, it does not act as an endorsement of any particular product or technology, and it is not tailored to individual needs. It is not a replacement for independent, specialist advice. Users should ensure that they take appropriate technical and legal advice in using this and other guidance published by CESG. This guidance is provided without any warranty of any kind, whether express or implied. It is provided without any representation as to the accuracy, completeness, integrity, content, quality, or fitness for purpose of all or any part of it. CESG cannot, then, accept any liability whatsoever for any loss or damage suffered or any costs incurred by any person as a result of, or arising from, either the disclosure of this guidance to you, or your subsequent use of it.