GOV.UK

Guidance

End User Devices Security Guidance: Android 5.x

Published

Contents

1. About this guidance

The End User Devices Security and Configuration Guidance is for Risk Owners and Administrators to understand the risks, security advantages and recommended configuration of Android 5.x within a remote working environment at the OFFICIAL and OFFICIAL SENSITIVE classification. Risk owners are encouraged to read the Risk Owners' Summary and Enterprise Considerations sections. Administrators and system integrators are encouraged to read the whole document.

This guidance is applicable to Android 5.1 devices configured in Device Owner mode (i.e. corporate liable) which provides an organisation with the highest level of control over a standard Android device. This guidance does not cover the use of Android 5 in a scenario in which personal use of the phone is done in a separate profile.

This guidance is an update of the previously provided guidance for Android 4.4. Android 5+ is a major update from an enterprise point of view due to the introduction of Android for Work. The guidance was developed following testing performed on a Nexus 6 device running Android 5.1.1 and test versions of Google Device Policy Client.

It is important to remember that any guidance points given here are just recommendations; none of the suggestions are mandatory. Risk owners and administrators should agree a configuration which balances the business requirements, usability and security of the platform and use this guidance for advice where needed.

2. Risk owners’ summary

When using Android 5.1 as part of a remote working scenario, the following architectural choices are recommended to minimise risk:

- 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.
- Publicly available apps that are required by the enterprise should be whitelisted and either pushed to devices automatically or made available within Google Play for Work. In-house applications should be defined within the MDM and distributed via a Google Play for Work private channel.

When configured in this way, risk owners should be aware of the following technical risks associated with this platform:

Associated security principle	**Explanation of risks**
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.
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. Android does not natively support encryption of external media (e.g. SD cards).
External interface protection	Interfaces such as Wi-Fi and Bluetooth cannot be fully controlled by policy.
Device update policy	The enterprise cannot force the user to update their device software.
Event collection for enterprise analysis	[!] There is no facility for collecting detailed logs remotely from a device.

3. Administrators’ deployment guide

3.1 Overview

To meet the principles outlined in the End User Devices Security Framework, several recommendations are given in the table below.

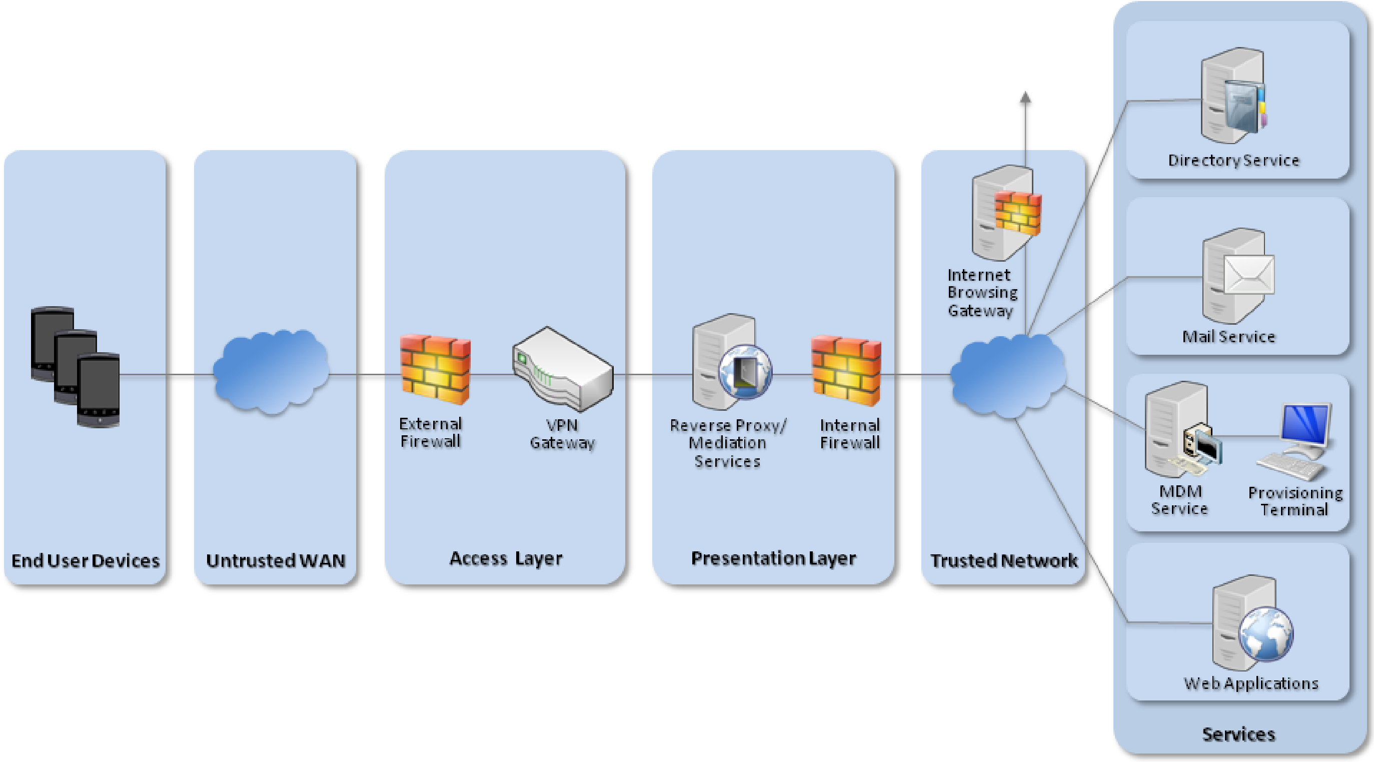
Security Principle	Explanation
Assured data-in-transit protection	Use the native Android IPSec VPN client until a Foundation Grade VPN client for this platform becomes available. Use procedural controls to prevent users from disabling the Always-On VPN option.
Assured data-at-rest protection	Use the device's native data encryption. This can be enforced through MDM security policy. For some Android devices, the encryption key is hardware protected against brute-force attacks if the manufacturer has implemented the relevant technology. Devices should be procured from vendors that do support this. To check for this feature, in the Security settings menu, look for 'Credential Storage', 'Storage type' being shown as 'Hardware-backed'. Devices should be procured that do not support external storage (e.g. no external SD slot). Or, devices should be procured from vendors that enhance the Android to include encryption of external storage (e.g. SD cards). To prevent users from making local backups to untrusted machines it is recommended that adb is disabled through MDM security policy. However, vendors may implement alternative backup processes which may not be disabled through this setting.
Authentication	The user has a strong 9-character password to authenticate to the device. In addition, 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.
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.
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.
Application Whitelisting	Administrators can automatically push apps to devices or whitelist apps that are then made available for download within Google Play for Work. Enterprise applications can be distributed in a non-public manner using Google Play for Work and private catalogues. Applications can be hosted on enterprise infrastructure but Google Play will be used to co-ordinate the distribution to users' devices. Users can be prevented from installing applications from unauthorised sources.
Malicious code detection and	Several third-party anti-malware products exist which attempt to detect malicious code for this platform and can be used if desired.

prevention	Only approved applications should be permitted to be installed via Google Play for Work. Content-based attacks can be filtered by scanning capabilities in the enterprise. Google Play checks for potentially harmful applications at the time of install as well as at regular intervals in the background. Android displays 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 solution supporting such functionality.
Platform integrity and application sandboxing	This requirement is met by the platform without additional configuration. The scope of SELinux has been enhanced within Android 5.0. SELinux Enforcing mode significantly enhances platform integrity and sandboxing.
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 the native VPN, Bluetooth and NFC. The user cannot disable Device Owner mode (unless the MDM vendor enables this); they can only cause a factory reset.
External interface protection	USB debugging can be disabled completely. In Device Owner mode, MDM controls can be used to prevent the user from configuring Wi-Fi and Bluetooth.
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 as these are dependent on user interaction (or can be configured by the user to be dependent 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 track record of patching devices. The WebView implementation is now updated via Google Play which should reduce the time to patch. However, Google Play auto-updates can be disabled by the user.
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 detailed failed device login information. However, MDM solutions can be used to retrieve some information from the device, such as: - Installed applications - Android version information - Last time device seen by MDM - Number of failed password attempts - Network state - Compliancy status (depending on the compliancy rules set up on the MDM server) - Enrolment status - Location information - Roaming Status

Incident Response	Android now supports wiping of both internal and external storage (previously it was just the internal storage). MDM solutions which support this 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.

3.2 Recommended 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 5.x deployments

3.3 Preparation for deployment

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 supports Android for Work Device Owner mode of operation and is able to enforce the settings given in the Policy Recommendations section below.
3. Set up a dedicated Wi-Fi provisioning network.
4. Create MDM security profiles for the Android devices in line with the guidance given in the Policy Recommendations section, and associate these profiles with the devices.
5. Define the apps that should be automatically installed onto devices including a Secure Email Client. Optional apps should be whitelisted and made available within Google Play for Work. Internal apps should be made available via Google Play for Work private channels. Internal applications can be hosted on enterprise infrastructure but Google Play will be used to co-ordinate the distribution to users' devices.

3.4 Device 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. Sign up for Android for Work by creating a Google admin account for the company's domain and verifying administration rights over the domain. Retrieve the EMM token from Google and bind to the chosen MDM.
2. Add and create a Google user account within the MDM (the primary email address will use the company domain). Depending on the MDM solution it may be possible to create users based on an existing Active Directory structure.
3. Configure the client certificates for each user within the MDM solution. The following certificates are required:
   - 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)
4. Provision the handsets into Device Owner mode using one of the following two methods:
   - NFC Provisioning App: Download and install the MDM NFC provisioning application onto a dedicated provisioning handset. The method of provisioning will

be unique to each MDM, therefore follow the instructions provided by the vendor. In general, the process may include the following steps:

1. Perform an NFC bump between the provisioning handset and the target handset to install the Device Policy Client (DPC) app onto the end user’s device.
2. Configure the provisioning app with the user enrollment details and perform a second bump to enroll a specific user with the MDM.
3. Manually enter a password for the corporate Google account tied to the enrollment user.

- Activation Code: The MDM may offer an alternative method of provisioning through the use of an activation code. Again the method of provisioning will be unique to each MDM, and so the instructions provided by the vendor should be followed. The activation code provisioning method can be initiated by selecting the ‘Add Work Account’ from the setup wizard.

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.

4. Recommended policies and settings

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**
Compliance Rules (or 'Safety Net')	If an insecure device is identified (e.g. device found to be rooted) 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.
Allow non-provisioned devices	False
Password Policy	
Require password	True
Require complex password	True
Minimum number of upper case characters	1

Minimum number of lower case characters	1
Minimum number of numeric characters	1
Minimum number of symbols	1
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
Disable all keyguard features (includes disabling display of data on Lock Screen Widgets and Smart Lock)	True
User Restrictions	
Disallow add secondary user	True
Disallow remove user	True
Disallow tethering configuration	True
Disallow debugging features	True
Disallow install from unknown sources	True
Disallow adding or removing accounts	True
Disallow mounting of physical media (e.g. SD cards). NB. Use this if SD card slot is available, but vendor does not enhance encryption mechanism to include external storage.	True
Disallow outgoing beam	True
Disallow USB file transfer	True
Ensure verify apps	True
Disallow credential changes	True
Other	

Require encryption on device	True
Disable Account Management	True
Application Specific Restrictions	Use where available (e.g. Chrome)
Use Auto Time	True
Disable ADB	True
Disable Screen Capture	True
Bluetooth	Off (procedural controls required to prevent user turning Bluetooth on)

On device Settings

Play store > Auto-update apps	Select either 'Auto-update apps at any time. Data charges may apply' or 'Auto-update apps over Wi-Fi only'.
NFC	Off (procedural controls required to prevent user turning NFC on)

ActiveSync Settings (if used)

Enable Security Restrictions	True
Allow Data Backup	False

5. Enterprise considerations

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

5.1 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.

5.2 Cloud integration and privacy

Android for Work devices require a user to have a Google work account for management, though this account is prevented from using other Google services such as Google Apps and Google Docs. Use of this Google account could result in unexpected data leakage to cloud services.

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. Location services can be disabled via MDM. Individual applications will often use application tracking services that may leak device information. These could be monitored and blocked when a VPN is active. Android may use location services and generate Wi-Fi beacons even when in airplane mode. This configuration can be disabled in advanced Wi-Fi settings.

5.3 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. Many vendors are now committed to issuing monthly security updates, and these vendors should be preferred where possible. MDM products can be used to track which security updates have been applied to each device in order to help update or upgrade those devices.

As of Android 5.0 the WebView implementation (often targeted by malicious users) is now updated through Google Play. The WebView will therefore be automatically updated unless the user disables automatic app updates.

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. This guidance is UK Crown Copyright. All Rights Reserved.