Google for Work | Android

Android mobility best practice advisory

July 2016

Whether it's managing a few employee phones or an international fleet of devices, IT leaders face many challenges when navigating the complexity of configuration options and mobile partners.

To help address these challenges, this is the first in a series of advisories aimed at laying out a set of best practices for IT decision makers to consider when using Android for Work. While not an exhaustive list, we recommend customers reference these guidelines when evaluating vendors and setting up their mobility environment.

Executive summary

When deploying Android in the enterprise, security best practices should be applied throughout a device's lifecycle.

While setting up a device, company and personal data should be stored separately to ensure corporate data can't be accessed by personal apps. Enterprises should require company data be encrypted on the device to protect it in the event of device loss. App distribution is another key aspect of mobile deployment, and Play for Work provides a sophisticated first line of defense against potentially harmful apps by using Google's automatic malware detection capabilities. To minimize the risk of malware being installed on the device, Android recommends disabling installation of apps via other, or unknown, sources.

Once a device is provisioned, use the latest management APIs supported by your EMM on each device to avoid taking a "lowest common denominator" approach to fleet management. Finally, regular security patches play a critical role in maintaining a device's security. IT decision makers should take into account the device manufacturer's commitment to security updates when making purchasing decisions and considering which devices to support in their environment.

Don't allow application installation from "Unknown Sources".

Many Android devices have a security setting, often referred to as “Allow unknown sources”, that determines whether applications can be installed from sources outside of the Google Play store. To protect against potentially harmful applications (PHAs), Google recommends customers deploy a policy to disallow installation of apps from sources other than Google Play.

As described in the 2015 Android Security Year in Review, apps from sources outside of Google Play store are more likely to be potentially harmful. Devices that allow apps to be installed from “unknown sources” had a 10x higher incidence rate of PHAs than devices that required apps be installed via Google Play.

Google Play provides an important first line of defense against malicious apps. Using techniques including static analysis, machine learning, and manual inspection, apps are first reviewed before being made available to users. This process ensures that apps conform with Google’s policies, and protects against potentially harmful applications from being installed via the Google Play store.

For customers with internal corporate apps, Google Play for Work provides a secure way to develop and distribute internal apps without allowing untrusted apps to be installed in the device’s corporate profile.

Consider security updates when determining devices to support

While security measures such as application isolation and profile separation provide protection of enterprise data from other unauthorized apps, OS updates are equally important to ensure those measures have continued effectiveness by patching identified bugs in a timely manner.

In 2015, Android launched a security update program in which security patches are published on a monthly basis along with a bulletin describing the bugs fixed. Once a patch is issued, OEMs work with their carrier partners to update affected devices.

The Nexus product line and certain devices from Samsung and Blackberry come with commitments to support monthly security patches within a specified time-period, while others may not issue security patches after a device is purchased. To reduce exposure to known vulnerabilities, Google recommends customers consider availability of monthly Android security updates when selecting devices and granting access to sensitive applications or data.

To check the update status of your managed devices, Android devices report their security patch version via a build property on the device, which is displayed in device settings as a meaningful date and can be verified programmatically by any application. Customers should work with their EMM to verify the update status of their devices and use that information as a signal when assigning an appropriate level of access.

Store work and personal data separately on the device

Bring your own device (BYOD) environments provide both cost savings for the company and convenience for employees. But they can also pose challenges if personal and corporate data isn't stored separately on a device.

Separation of work and personal data ensures that personal apps can't maliciously or inadvertently access, modify, or leak corporate information. Similarly, users may be uncomfortable with their personal apps being monitored -- companies risk inadvertently collecting personally identifiable information, or deleting personal data on a lost device, if personal and work data are stored together.

Google recommends splitting work and personal data on BYOD devices by storing them separately (e.g., in different profiles) to avoid accessing personal information in corporate apps. This approach provides for better protection of work data from personal apps, and allows IT to enforce more granular policies, such as data encryption, remote wipe capabilities, network proxies, and monitoring of work apps, while preserving the privacy of the employee's personal data.

Require encryption of all work data

Physical security is an obvious concern for corporate data on mobile devices. Full disk encryption was introduced in Android 3.0, and support is required on all capable Android 6.0+ devices meeting clearly defined hardware requirements found in the Android 6.0 Compatibility Definition Documentation.

To protect data at rest, Google recommends enforcing a policy that requires work data be encrypted before a device is given access to sensitive information.

For additional security, consider requiring full disk encryption and a PIN or password to be entered when starting the device. New devices running Android N may also support Direct Boot and allow for encrypting work data separately.

Use the latest management API on a device

Device Admin APIs were introduced in Android 2.2 to support an initial set of device management scenarios. In Android 5.0, new Profile Owner and Device Owner APIs were added to provide more granular controls better suited to BYOD and corporate-liable environments.

Many EMMs support using the newest APIs available on a given device, even if those APIs aren't supported on all managed devices. Android for Work encourages customers and EMMs to take a "best available" approach to management and use the latest profile or device owner APIs, rather than reverting to the "lowest common denominator" supported across their fleet. Older Device Admin APIs have been used in abuse scenarios and their scope will be reduced starting in Android N.