Enterprise Policy, Mitigation M1012 - Mobile

Archived: 2026-04-05 18:16:31 UTC

Mobile T1517 Access Notifications

On Android devices with a work profile, the `DevicePolicyManager.setPermittedCrossProfileNotificationListeners` method can be used to manage the list of applications running within the personal profile that can access notifications generated within the work profile. This policy would not affect notifications generated by the rest of the device. The `DevicePolicyManager.setApplicationHidden` method can be used to disable notification access for unwanted applications, but this method would also block that entire application from running.[1]

Mobile T1661 Application Versioning

Enterprises can provision policies to mobile devices for application allow-listing, ensuring only approved applications are installed onto mobile devices.

Mobile T1521 .003 Encrypted Channel: SSL Pinning

Certain enterprise policies can be applied to prevent users from adding certificates to the device and to prevent applications from being able to install their own certificates.

Mobile T1428 Exploitation of Remote Services

Configuration of per-app VPN policies instead of device-wide VPN can restrict access to internal enterprise resource access via VPN to only enterprise-approved applications

Mobile T1629 Impair Defenses

An EMM/MDM can use the Android `DevicePolicyManager.setPermittedAccessibilityServices` method to set an explicit list of applications that are allowed to use Android's accessibility features.

.001 Prevent Application Removal

An EMM/MDM can use the Android `DevicePolicyManager.setPermittedAccessibilityServices` method to set an explicit list of applications that are allowed to use Android's accessibility features.

Mobile T1417 Input Capture

When using Samsung Knox, third-party keyboards must be explicitly added to an allow list in order to be available to the end-user.[2] An EMM/MDM can use the Android `DevicePolicyManager.setPermittedAccessibilityServices` method to set an explicit list of applications that are allowed to use Android's accessibility features.

.001 Keylogging

When using Samsung Knox, third-party keyboards must be explicitly added to an allow list in order to be available to the end-user.[2]

.002 GUI Input Capture

An EMM/MDM can use the Android `DevicePolicyManager.setPermittedAccessibilityServices` method to set an explicit list of applications that are allowed to use Android's accessibility features.

Mobile T1516 Input Injection

An EMM/MDM can use the Android `DevicePolicyManager.setPermittedAccessibilityServices` method to set an explicit list of applications that are allowed to use Android's accessibility features.

Mobile T1430 Location Tracking

If devices are enrolled using Apple User Enrollment or using a profile owner enrollment mode for Android, device controls prevent the enterprise from accessing the device’s physical location. This is typically used for a Bring Your Own Device (BYOD) deployment.

.001 Remote Device Management Services

If devices are enrolled using Apple User Enrollment or using a profile owner enrollment mode for Android, device controls prevent the enterprise from accessing the device’s physical location. This is typically used for a Bring Your Own Device (BYOD) deployment.

Mobile T1461 Lockscreen Bypass

Enterprises can provision policies to mobile devices that require a minimum complexity (length, character requirements, etc.) for the device passcode, and cause the device to wipe all data if an incorrect passcode is entered too many times. Both policies would mitigate brute-force, guessing, or shoulder surfing of the device passcode. Enterprises can also provision policies to disable biometric authentication, however, biometric authentication can help make using a longer, more complex passcode more practical because it does not need to be entered as frequently.

Mobile T1663 Remote Access Software

When devices are enrolled in an EMM/MDM using device owner (iOS) or fully managed (Android) mode, the EMM/MDM can collect a list of installed applications on the device. An administrator can then act on, for example blocking, specific remote access applications from being installed on managed devices.

Mobile T1458 Replication Through Removable Media

Enterprise policies should prevent enabling USB debugging on Android devices unless specifically needed (e.g., if the device is used for application development).

Mobile T1513 Screen Capture

Enterprise policies should block access to the Android Debug Bridge (ADB) by preventing users from enabling USB debugging on Android devices unless specifically needed (e.g., if the device is used for application development). An EMM/MDM can use the Android `DevicePolicyManager.setPermittedAccessibilityServices` method to set an explicit list of applications that are allowed to use Android's accessibility features.

Mobile T1451 SIM Card Swap

Enterprises should monitor for SIM card changes on the Enterprise Mobility Management (EMM) or the Mobile Device Management (MDM).

Mobile T1632 Subvert Trust Controls

On iOS, the `allowEnterpriseAppTrust` and `allowEnterpriseAppTrustModification` configuration profile restrictions can be used to prevent users from installing apps signed using enterprise distribution keys.

.001 Code Signing Policy Modification

On iOS, the `allowEnterpriseAppTrust` and `allowEnterpriseAppTrustModification` configuration profile restrictions can be used to prevent users from installing apps signed using enterprise distribution keys.
