Mobile@Work 10.7.0.0 for Android Release Notes

June 24, 2020

For complete product documentation, see Mobile@Work for Android Product Documentation Home Page.

About Mobile@Work for Android

Mobile@Work for Android is the MobileIron client app that works with MobileIron Core. Device users download Mobile@Work, which automatically configures the device to function in an enterprise environment by enforcing the configuration and security policies that you set on MobileIron Core.

Mobile@Work works with MobileIron Core to:

- configure corporate email, Wi-Fi, VPN, and security certificates to create a clear separation between personal and business information.
- install the enterprise app storefront so that device users can browse and install the mobile applications that you make available to them.
- allow device users to access web resources and content repositories that sit behind the firewall.

New features and enhancements summary

This section provides summaries of new features and enhancements developed for the current release of Mobile@Work for Android. References to documentation describing these features are also provided, when available.

For new features and enhancements provided in previous releases, see the release notes for those releases, available in Mobile@Work for Android Product Documentation.

Mobile@Work features and enhancements

This section summarizes new features and enhancements that are common to all platforms.

- **Rebranding:** MobileIron has updated the Mobile@Work for Android icon and user interface color scheme.
- **Password policy attributes enhanced:** All reported password policy attributes on devices with Android 10 through the latest version as supported by MobileIron that cannot be supported due to Device Admin mode deprecation. In Core, the security policy will display as "applied" and the device will display as compliant. For more information, see "Password policy attribute" in the *MobileIron Core Device Management Guide for Android and Android enterprise Devices.*
- **Custom APN on Android devices:** Mobile@Work uses the Access Point Name (APN) settings to set up a connection to the gateway between the carrier's network and the internet. Administrators can create a

custom APN on Android devices in Work managed device mode (DO) and Managed device with work profile mode (COMP.) This is applicable on Android devices version 9.0 through the most recently released version as supported by MobileIron. For more information, see "Using custom APN with Android devices" in the *MobileIron Core Device Management Guide for Android and Android enterprise Devices.*

- **Allow Mobile@Work work calendar sharing with personal profile:** Administrators can now allow calendar sharing of work calendar information with the personal profile. This is so apps can display work events alongside personal events in device user's personal profile (for example, calendar apps like Google calendar.) Applies to Managed devices with work profiles. For more information, see "Lockdown policy fields for Android enterprise devices in Work Profile mode and Managed Device with Work Profile mode" in the *Getting Started with MobileIron Core.*
- **Authenticator Only mode:** Users can register their unmanaged device in Authenticator Only mode. Registering a device in Authenticator Only mode designates an unmanaged mobile device as a user's identity and authentication factor. Designating a mobile device as the user's identity allows users to take advantage of zero sign-on features, which allow passwordless access to SaaS applications and other business services.

  Authenticator Only requires MobileIron Core 10.7.0.0 and MobileIron Access 40.

  For information about deploying and registering devices in auth-only mode, see "Authenticator only with MobileIron Access" in the *MobileIron Access Guide.*
- **Passcode expiry notification text changed:**
  - **Before quarantine:** In previous Mobile@Work versions, before a device was put into quarantine, the device user received a notification: "Your device passcode is about to expire. Please set up a new passcode." With this version, the new text is: "Update screen lock code - Your screen unlock code will soon expire. Set up a new code to continue having seamless access to your work data."
  - **After quarantine:** In previous Mobile@Work versions, after a device was put into quarantine, the device user received a notification:“MobileIron detected threat(s) that required device to be quarantined." With this version, the new text is: “MobileIron detected threat(s) that required blocking access to your work data.”
- **Ability to pass custom attributes as part of registration added:** For Zero Touch, Knox Mobile Enrollment (KME) or QR Code, the ability to pass custom attributes as part of registration was added. Core will apply the Android Enterprise configuration for Work managed device (DO) mode and Managed device with Work profile (COMP) mode. For more information, see "Zero Touch enrollment with custom attributes" in the *MobileIron Core Device Management Guide for Android and Android enterprise Devices.*
- **Zebra firmware downloaded and installed on Zebra devices:** A Zebra firmware policy can now be downloaded and applied to Zebra devices (running on Android version 8.0 through the latest version as supported by MobileIron) in Work managed device (Device Owner) mode and Managed Device with Work Profile mode. Once the policy is applied, the firmware is downloaded and installed on the Zebra device as per the configured parameters (schedule is one of them.) For more information, see "Zebra Support" in the *MobileIron Core Device Management Guide for Android and Android enterprise Devices.*
- **Zebra Support-multiple download re-tries:** If a Zebra OTA (Over-the-Air) service download fails on a device, Mobile@Work will retry using the option to get a new token. An audit log event is recorded for every retry and new token. For more information, see "Zebra Support" in the *MobileIron Core Device Management Guide for Android and Android enterprise Devices.*
- **Check the device firmware download status for Zebra and Android devices:** Once the Zebra firmware policy is pushed to devices, administrators can check the status of the Zebra device system

update, along with other Zebra-related items. Details include: Zebra Build Fingerprint, Zebra Device Build Id, Zebra Device System Update, Zebra OTA Capable and Zebra Patch Version. Values returned are Available, Downloading, Pending, Current and Unknown. "Unknown" is reported for older clients. If "Error" displays, it means the firmware download / install failed on the device. For more information, see "Zebra Support" in the *MobileIron Core Device Management Guide for Android and Android enterprise Devices.*

- **Enhancement to Mobile@Work registration enrollment options:** Increased ability for administrators to provide different registration enrollment options based on enrollment types (In-App, Zero Touch, Samsung Knox Mobile Enrollment (KME), and QR code.) Depending upon the enrollment type, when registrering, device users may be asked to enter a username, password, registration PIN or all three. For more information see "Registering Android devices" in the *MobileIron Core Device Management Guide for Android and Android enterprise Devices.*
- **Administrators can now grant additional delegation permissions:** Administrators can now grant additional delegation permissions: For Android 8.0 and above devices, Mobile@Work allows delegation permissions for apps in Managed device with Work profile (COPE) mode.
    - For Public or Self Hosted Apps (Google Play Private channel apps) pushed by Managed Google Play or regular Google Play:

      - Apps are assigned to device in Managed device with Work profile (COPE) mode and will be pushed and installed silently by Google Play services inside the managed work profile.

      - After the app is installed in the Managed device with Work profile, delegated permissions is applied by Mobile@Work.

      - This is supported for Samsung and non-Samsung devices running Android 8.0 through the latest version as supported by MobileIron.

    - For In house Apps (Apps pushed by Core):

      - Apps are assigned to devices in Managed device with Work profile (COPE) mode and will be installed silently by Mobile@Work on the personal (device owner) side.

      - After the app is installed, delegated permissions are applied by Mobile@Work.

      - This is supported for Samsung and non-Samsung devices running Android 8.0 through the latest version as supported by MobileIron.

    - For In house Apps on Samsung Knox V3 devices (Android 8.0 and above):

      - Apps are assigned to device in Managed device with Work profile (COPE) mode and whitelisted for Knox V3 workspace.

      - Apps are silently installed by Mobile@Work on the personal (device owner) side and then immediately hidden and moved to the Knox V3 workspace (managed profile.)

      - At the time the app is moved into the Knox V3 workspace, delegated permissions are applied.

      NOTE: Installing regular In house apps inside the Managed device with Work profile is not supported.

      MobileIron Core version 10.4.0.0 through the latest version is required for this feature. "Delegated permissions for Google Play apps" or "Delegated permissions for in-house apps" in the MobileIron Core Apps@Work Guide." in the *MobileIron Core Apps@Work Guide.*

- **Added STIG compliance for Passcode policy APIs in device administrator (DA) mode for Samsung devices:** Password policy now can now be successfully applied to Samsung 10 devices running Android 10 in device administrator (DA) mode. This includes smart lock settings and biometrics.
- **Notify administrator when PIN expiration prompt was skipped by device user:** Administrators can now identify devices that have prompted the device user to change the password / PIN but the device user skipped the prompt. For more information, see "Setting an alert that a device's PIN change request was skipped" in the *MobileIron Core Device Management Guide for Android and Android enterprise Devices*.

Wear OS watch app features and enhancements

This section summarizes new features and enhancements related to the Wear OS watch app that requires and pairs with the latest version of Mobile@Work for Android.

There are no new features and enhancements for the Wear OS watch app.

MobileIron Threat Defense features

MobileIron Threat Defense protects managed devices from mobile threats and vulnerabilities affecting device, network, and applications. For information on MobileIron Threat Defense-related features, as applicable for the current release, see the MobileIron Threat Defense Solution Guide for Core, available on the MobileIron Threat Defense for Core Documentation Home Page at MobileIron Community.

NOTE: Each version of the MobileIron Threat Defense Solution guide contains all MobileIron Threat Defense features that are currently fully tested and available for use on both server and client environments. Because of the gap between server and client releases, MobileIron releases new versions of the MobileIron Threat Defense guide as the features become fully available.

Support and compatibility

The information in this section includes the components MobileIron supports with this product.

NOTE: This information is current at the time of this release. For MobileIron product versions released after this release, see that product version's release notes for the most current support and compatibility information.

Support policy

MobileIron defines *supported* and *compatible* as follows:

Term	Definition
Supported product	The functionality of the product and version with currently supported releases was

Term	Definition
versions	systematically tested as part of the current release and, therefore, will be supported.
Compatible product versions	The functionality of the product and version with currently supported releases has not been systematically tested as part of the current release, and therefore not supported. Based on previous testing (if applicable), the product and version is expected to function with currently supported releases.

Mobile@Work for Android support and compatibility

Component	Supported Version	Compatible Version
MobileIron Core	10.5.1.1, 10.5.2.1, 10.6.0.1, 10.7.0.0	10.3.0.3, 10.4.0.4
Android	5.0, 5.1, 6.0, 7.0, 7.1, 8.0, 8.1, 9.0, 10.0	(All listed versions are tested and supported.)
Wear OS on watch	2.9, 2.10, 2.11, 2.12	2.0, 2.1, 2.2, 2.3, 2.6, 2.7, 2.8
MobileIron Threat Defense	management console: zConsole 4.27.4 GA NOTE: MobileIron Connected Cloud does not support the use of MobileIron Threat Defense.	Not applicable

Language support for Android devices and Mobile@Work Wear OS (watch app)

MobileIron Core supports the following languages and locales in client apps on Android devices:

- Chinese (Simplified)
- Chinese (Traditional)
- Dutch (Netherlands)
- English
- French (France)
- German (Germany)
- Italian (Italy)
- Japanese

- Korean
- Polish
- Portuguese (Brazil)
- Romanian (Romania)
- Russian
- Slovak
- Spanish (Latin America)

Resolved issues

This section describes the following resolved issues fixed in the current release of Mobile@Work for Android. For resolved issues provided in previous releases, see the "Resolved issues" sections in the release notes for those releases, available in Mobile@Work for Android Product Documentation.

This release includes the following resolved issues:

- **AC-19898:** During the Mobile@Work for Android registration process, the french language page stating "Continuer avec les autorisations" was not displaying the full message. This issue has been fixed.
- **AC-19880:** On Android 10 devices, a complex PIN was not taken into account while choosing the complexity level for the screen lock password. This issue has been fixed.
- **AC-19784:** The Mobile@Work Android Quick Setup Policy was not ignored when device user was setting the new work challenge. This issue has been fixed.
- **AC-19779:** Device email was defaulting to 2 weeks and not honoring the email sync period setting in Core > Exchange configuration. This was related to Samsung Mail and on Android enterprise Device Admin mode. This issue has been fixed.
- **AC-19723:** The Unlock command issued to devices provisioned in Work Profile (PO) mode changed the Work Challenge to the default setting of 0000 when the Work Challenge was not enabled in an Android enterprise configuration. This issue has been fixed.
- **AC-19698:** Mobile@Work on Android devices intermittently failed to parse the Certificate Revocation List (CRL) when mutual authentication was enabled. This issue has been fixed.
- **AC-19691:** German translation errors were occurring on some Mobile@Work screens. This issue has been fixed.
- **AC-19609:** MobileIron Tunnel disconnects when Mobile@Work performs a check-in. This was occurring in Android enterprise deployments and with AlwaysOnVPN configurations. This issue has been fixed.
- **AC-19580:** Phishing URLs were not getting blocked from Managed device with Work profile mode in Samsung Galaxy S10/10.0 devices. This issue has been fixed.
- **AC-19545:** Some Android devices were sometimes quarantined due to wrongly detected condition of device password being insufficient. It usually happened after device reboot when device was locked and did not detect the device's locked state after reboot on Zebra TC57 device with Android 8. Consequently, that device's quarantine state was declared randomly after device reboot before it was unlocked by the device user. This issue has been fixed.

- **AC-19543:** Mobile@Work upgrade not prompting the screen lock preferences: When the device user was trying to provision certificates on Android 10, the Mobile@Work prompted the device user to set the screen lock preferences. This issue occurred if the screen lock was not configured by the administrator. This issue has been fixed.
- **AC-19503:** Every time the Mobile@Work Android Enterprise Kiosk activity was resumed (unlocking device, navigating between other Kiosk screens, etc.), Mobile@Work downloaded the background image. This has been fixed.
- **AC-19483:** Devices in Work Profile (Profile owner) mode were intermittently being moved to quarantine after the device was rebooted. This issue has been fixed.
- **AC-19465:** The Knox licenses were showing false license errors even though Knox premium license privileges were still intact. This issue has been fixed.
- **AC-19399:** Fixed the issue of Mobile@Work running with Mutual Authentication not connecting to Core on port 443.
- **AC-19375:** Fixed the issue of built-in camera not available due to permission issues in Android shared kiosk policy under Work managed device mode (DO).
- **AC-19334:** Fixed the issue of Mobile@Work crashing upon launch of Ranger X2 X86 64-bit device.
- **AC-19324:** Old versions of Mobile@Work app were being downloaded onto Zebra devices without camera. This issue has been fixed.
- **AC-19305:** Mobile@Work Work Profile allows personal email accounts to be added by device users with Google domain bindings. This issue has been fixed - personal email accounts added during work profile inflation will be removed.
- **AC-19288:** Fixed the issue of not being able to set the Work challenge again after quarantine was removed.
- **AC-19270:** Fixed the issue of Android enterprise account Managed device with work profile (COPE) mode not getting removed from the personal side.
- **AC-19211:** When any app is updated in Android kiosk mode, Android kiosk exits and does not automatically return to kiosk mode. This issue has been fixed.
- **AC-19064:** If a Samsung device has VPN clients working, after device reboot, Mobile@Work displayed the error "VPN creation failed." This error continued to display until the Knox Workspace was unlocked. This issue has been fixed.
- **AC-19000:** Apache Access logs were displaying the password during multi-user/v1/login API call. This issue has been fixed.
- **AC-18614:** Fixed the issue of Mobile@Work sending an empty application inventory when SyncApp was set to catalog apps.

Known issues

This section describes the following known issues that are found in the current release of Mobile@Work for Android. For known issues found in previous releases, see the "Known issues" sections in the release notes for those releases, available in Mobile@Work for Android Product Documentation.

There are known issues for this release:

- **AC-19469:** If Zebra Firmware is downloaded to any version of Mobile@Work less than version 10.6.0.0 and is in an ERROR state, and if the app is then upgraded to Mobile@Work 10.6.0.0, the client will stay in the ERROR state. The Zebra firmware download/install will not happen unless the Zebra policy is removed and reapplied with Core 10.6.0.0. Zebra OTA (Over-the-Air) is only supported with Core 10.6.0.0 and Mobile@Work 10.6.0.0.
- **AC-19391:** The OS Update system notification is not displaying after the Zebra Firmware is downloaded on the device for the first time.

Limitations

This section describes the following limitations (typically third-party limitations) that are found in the current release of Mobile@Work for Android. For limitations found in previous releases, see the "Limitations" sections in the release notes for those releases, available in Mobile@Work for Android Product Documentation.

There are third-party limitations in this release:

- **AC-19860:** When a device is hidden as a result of the device being quarantined, Google services re-installs the app automatically. This occurs when the App Catalog > Edit app > Android enterprise > Auto Install Mode field is set to "Force Install," resulting in the corporate app getting installed without setting a PIN code.

  Workaround: Set the App Catalog > Edit app > Android enterprise > Auto Install Mode field to "Install Once."
- **AC-19766:** The Man-in-the-middle SSL Strip threat is not detected in some Android devices.
- **AC-19745:** After a device retires, calendar events are removed from the device if calendar sharing is enabled by the administrator. This affects calendar events between work and personal profiles for Android enterprise deployments. This is a platform limitation and there is no workaround.
- **AC-19657:** In Android enterprise Work Profile (PO) mode, the Work Profile password is applied to the device. When the Work Challenge is disabled in Core, the password on the device cannot be removed and there is no option to change it in the device's password settings.
- **AC-19616:** Users should not remove all user or VPN credentials or certificates in Android security settings when working with MobileIron Tunnel. Doing so causes the Tunnel app to flicker and become unresponsive.
- **Workaround:** To recover the certificates, go to Mobile@Work > Settings and reinstall the certificates.
- **AC-19583:** Zero Password is unable to perform QR code scan on Android 10 devices registered in Android Enterprise modes.

  Workaround: Clear Google Play services data on the device.
- **AC-19155:** Unable to scan the QR code on unmanaged Samsung devices running Android 10 when it is provisioned in Work managed device (DO) mode or Managed device with work profile (COPE) mode.

- **AC-18845:** If known secure WiFi SSIDs are being detected as network threats, to avoid known secure networks from being scanned for network threats, the SSID can be whitelisted by administrators in the zConsole: Manage > Whitelisting > WiFi Access Points.

Documentation resources

MobileIron product documentation is available at https://help.mobileiron.com/s/mil-productdocumentation.