Mobile@Work 10.8.0.0 for Android Release Notes

September 9, 2020

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

Contents

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 administrators 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 administrators 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.

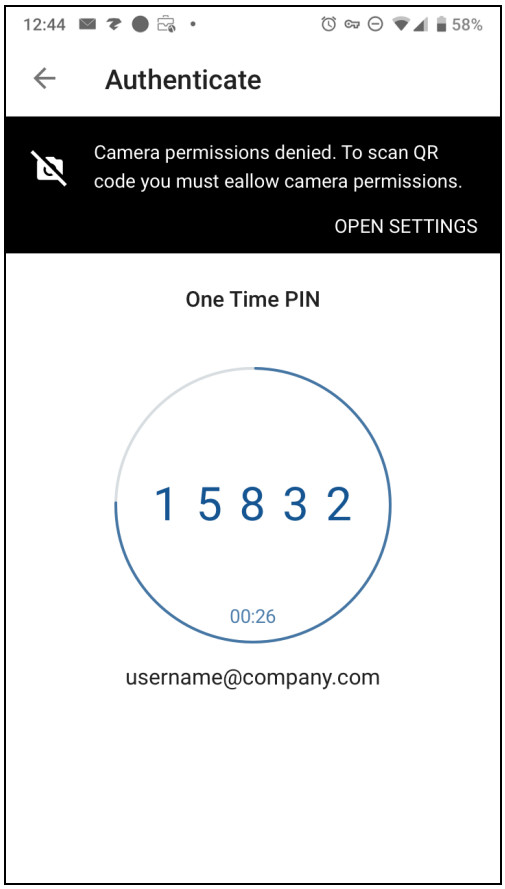
For new features and enhancements provided in previous releases, see the release notes for those releases, available in Mobile@Work for Android Product Documentation.

Mobile@Work features and enhancements

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

- **Compliance push notification for devices in Authenticator Only mode:** Compliance push notifications are now supported for devices in Authenticator Only mode. Device users see out of compliance push notifications if the administrator has configured the option in the policy.
  - For information about deploying Authenticator Only, see "Authenticator Only with MobileIron Access" in the *MobileIron Access Guide.*
  - For information about configuring compliance actions in MobileIron Core, see "Managing Compliance" in the *MobileIron Core Device Management Guide* for your operating system.

- **Support to logout from browser for Zero Sign-on:** The Zero Sign-on session can now be logged out from Settings at any time. The option is available below Authenticate (enabled only when there is an active session). This option can be leveraged in case browser closure or termination does not clean up the active Zero Sign-on session.
- **One Time PIN for Camera Permissions on Android devices:** Camera permissions are no longer part of the Core Zero Sign On policy. Instead, permissions are displayed whenever the device camera is accessed. After permission denials by the device user, the One Time PIN is shown in the Authenticate page stating that camera permissions have been denied. A count-down is given to indicate to the device user the amount of time left to tap **Open Settings** to allow camera permissions.



- **New registration support added to accommodate the new Android enterprise "Work Profile on Company-Owned Devices" mode for Android 11 devices:** With the introduction of a new Android enterprise mode of deployment called "Work Profile on Company Owned Devices" for Android 11 devices, the following registration support has been added:
  - Device users can register using QR code or Zero Touch
  - Core administrators are now able to run a search on 'Registration Status" to verify devices are running in Work Profile on Company Owned Devices mode

    NOTE: Retire of "Work Profile on Company Owned Devices" forces a device factory reset (this is different from Work Profile mode.)

- **Support for freeze period in system update:** Administrators can now freeze firmware updates for up to 90 days. This is helpful if your company needs time to figure out the migration plan for changing from Managed Device with Work Profile (COPE) mode to Work Profile on Company Owned devices mode. Applicable to Android 11 devices in Device Owner mode and Android 9+ devices in Managed Device with Work Profile (COPE) mode. For more information, see "Setting the system update policy for Android devices" in the *MobileIron Core Device Management Guide for Android and Android enterprise Devices.*
- **Zero Sign-on authentication for new work profile:** For devices enrolled in Managed Device with Work Profile (COPE) mode with Zero Sign-on authentication provisioned and biometric authentication registered, upgrade to Android 11 with the following:
  - Switch to Work Profile on Company Owned Device mode
  - Biometric authentication needs to be re-registered one time to have it active inside the managed profile
- **Support to whitelist dialer/system packages on Android Device Owner devices in Kiosk mode:** In the Kiosk mode Settings under Kiosk Mode Allowed Apps, the administrator should whitelist the following dialer/system packages to make them functional in Kiosk mode for enabling dialer functionality in Kiosk mode on Samsung devices.
  - Call – com.samsung.android.incallui
  - Phone – com.samsung.android.dialer (should be whitelisted and the administrator should select hide option for this package to avoid issues with two dialer options)
  - Call – com.sec.phone
  - Call Setting – com.samsung.android.app.telephonyui
  - Assisted Dialing – com.sec.providers.assisteddialing
  - Call Log Backup / Restore – com.android.calllogbackup
  - Dialer Storage – com.android.providers.telephony
  - Phone – com.android.server.telecom
  - Phone – com.android.phone
  - Smart Call – com.samsung.android.smartcallprovider
  - WiFi Calling – com.sec.unifiedwfc
- **Support to receive and dial calls inside Device Owner (DO) Kiosk mode:** For Samsung 9 and Pixel2XL 10.0 devices, device users are able to dial and receive calls inside Device Owner (DO) Kiosk mode irrespective of Lock Task mode enabled / disabled.
- **Root CA certificate installation unsupported on on Android 11 devices:** On Android 11 devices in Device Admin (DA) mode, the Root CA certificate will be flagged as unsupported. Identity certificates installation is not affected.
- **Advanced Lock Task Features added for Android 9 devices in Device Owner (DO) mode:** The administrator now has the ability to add advanced settings to the Android Kiosk App Setting Policy.
  - **System Info** - When selected, displays the date/time, connectivity, battery, vibration mode on the status bar.
  - **Keyguard** - Enables the keyguard in lock task mode.

- **Global Actions** - Enables the menu that is displayed when the device user long-presses the power button. If this option is disabled, the device user may not be able to power off the device.
- **Home button** - When enabled, displays the following sub-options:
  - Overview - Enables the Overview button and the Overview screen during lock task mode.
  - Notifications - Enables notifications during Kiosk Lock Task mode. This includes notification icons on the status bar, heads-up notifications, and the expandable notification shade. Apps' notifications are read-only and not interactive.

These Advanced Lock Task features are only applicable to Android 9 devices in Device Owner (DO) mode.

Upon upgrade, existing policies get the above default settings. For more information, see "Setting kiosk policy for Android Managed devices" 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 versions	The functionality of the product and version with currently supported releases was 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, 10.8.0.0	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, 11.0	(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 4.28.7 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-20299:** When establishing a connection the Core server requires downloading of a large CRL (certificate revocation list), Mobile@Work client crashes and blocks registration on some low memory devices. Also, on some devices, Mobile@Work crashes when Samsung Common Criteria Mode (CC mode) is enabled due to unneeded enforcement of CRL check.
- **AC-20241:** When a too-short device user's name (three characters or less) is used while attempting to authenticate the device user's biometrics, Mobile@Work client crashes. This issue has been fixed.
- **AC-20162:** VPN chaining was configured only for MobileIron Tunnel VPN configuration - but not for any other VPN provider. This issue has been fixed.
- **AC-20135:** When the MTD Security policy did not require a password, "Passcode not set" MTD threat was not ignored and triggered quarantine. Also, "Passcode not set" MTD threat was not ignored during registration when the device user still did not have a chance to set up device password/PIN. This issue has been fixed.
- **AC-20129:** The Knox license activation was triggered by unexpected license errors even though license-related privileges were intact. This issue has been fixed.
- **AC-20088:** For all Android enterprise modes, adding a Google account with an email address that contained capital letters resulted in Moble@Work prompting the device user to add the Google account again. This issue has been fixed.

- **AC-19970:** For Android enterprise devices in Managed Device in Work Profile (COPE) mode, the "Account action required" notification does not go away when client is upgraded from Mobile@Work 10.5.1.0 to Mobile@Work 10.7.0.0. This issue has been fixed.
- **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.

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 no known issues for this release.

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-20286:** A Samsung limitation prevents devices running MobileIron Go for Android 10 and above in Android enterprise mode from disabling risky Wi-Fi connections. Until a patch is released, if disabling risky Wi-Fi with an alert has been enabled in Local Actions, the user will see an erroneous alert that the Wi-Fi has been disabled.
- **AC-20285:** This is a Samsung device limitation for Kiosk. Device users can receive incoming calls only when on the Kiosk Home screen. There is no UI indication to accept incoming calls. If any other application (for example, Chrome) is in the foreground in Kiosk mode, device users can hear the ringtone, but they cannot respond to the call even after opening the dialer app. This issue is observed in the following combination of Kiosk settings and OS versions.
  - Kiosk Lock Task mode is enabled and Disable Quick Settings is enabled: This issue is observed on Samsung devices with OS version 9.0 and older versions.
  - Kiosk Lock Task mode is enabled and Disable Quick Settings is disabled: This issue is observed on Samsung devices with OS version 8.0 and older versions.
- **AC-20284:** This is a Samsung limitation. When the Lock Task Mode is enabled, the following behavior is observed on Samsung devices with OS version 6.0.
  - On incoming calls - Users can hear the ringtone but there is no indication in the UI for accepting the call.

  - On outgoing calls - When a number is dialed, the Dialer app does not give any indication in the UI that the call is made. But the call is successful, and users can talk to other party.

- **AC-19860:** When an Android enterprise app is hidden as a result of the device being quarantined, Google Play services might re-install the app automatically. This occurs when the App Catalog > Edit app > Android enterprise > Auto Install Mode field is set to "Force Install" on the Core server. This may result in the 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-19859**: For Samsung devices with Android 10, the first attempt to configure a CBA (Certificate Based Authentication) Exchange account with the native Samsung email client fails and has to be re-tried.

  Workaround: Second attempt usually resolves this limitation.

- **AC-19858**: For Samsung devices with Android 9, the first attempt to configure a CBA (Certificate Based Authentication) Exchange account with the native Samsung email client fails and has to be re-tried.

  Workaround: Second attempt usually resolves this limitation.

- **AC-19766:** The Man-in-the-middle SSL Strip MTD threat is not detected in some Android devices.

- **AC-19787:** QR code scanning does not work immediately after factory reset during Android enterprise Device Owner (DO) mode provisioning due to lack of Google Play Services update. The problem fixes itself after some time when the Google Play Services are auto-updated to an error-free version.

  Work-around: Manual reset of Google Play Services' data sometimes helps; this can be done via device settings. MobileIron recommends waiting until all system/Google apps are updated after the factory reset.

- **AC-19091:** Knox Email is getting reconfigured upon device reboot.

Documentation resources

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