Mobile@Work 11.1.0.0 for Android Release Notes

March 4, 2021

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

Revision history

TABLE 1. REVISION HISTORY

Date	Revision
March 4, 2021	Removed support for Android 5.0 and 5.1. As of March 1, 2021, MobileIron no longer provides support for these OS versions. See Support and compatibility.

Contents

Revision history 3

About Mobile@Work for Android 5

New features and enhancements summary 5

Mobile@Work features and enhancements 5

Wear OS watch app features and enhancements 6

MobileIron Threat Defense features 6

Support and compatibility 7

Support policy 7

Mobile@Work for Android support and compatibility 7

Language support for Android devices and Mobile@Work Wear OS (watch app) 8

Resolved issues 8

Known issues 9

Limitations 10

Documentation resources 10

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.

- Mobile@Work features and enhancements
- Wear OS watch app features and enhancements
- MobileIron Threat Defense features

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.

- **Android Enterprise apps can now be auto-launched after installation:** Administrators can now force the auto-launching of Android Enterprise apps after their installation. A typical use case would be for a security/VPN app that needs to be configured by the device user before the device can be protected. Applicable to Android devices version 6.0 through the latest version as supported by MobileIron.
- **Support for Samsung Knox Dual Encryption (DualDAR):** Support for Dual Encryption (DualDAR) has been added to further secure and protect sensitive data on devices. Samsung Knox includes a FIPS 140-2 certified encryption module within the inner layer of the encryption. DualDAR is applicable to Knox v3 on Android 8.0 devices through the latest version as supported by MobileIron. It applies to Android Enterprise

Work Profile mode, and Managed Device with Work Profile mode.

- **Sending feedback and Log files instructions updated:** The text in **Settings > Send Logs** has been updated to make instructions clearer to the device user.
- **Ability to control Unknown sources:** Administrator can use two Lockdown options to control unknown sources. Both options are available in Android Enterprise settings:
    - Allow unknown sources in personal profile option is one of the Work Profile Lockdown Settings.
    - Allow install from unknown sources on the device option is one of the Managed Devices with Work Profile Lockdown Settings.
- **OAuth endpoint for mutual certification authentication:** New mutual authentication device endpoints are available for use by Android clients for all communications needed to support self-service (My Devices) portal.
- **Support Direct Boot mode:** Direct Boot mode allows administrators to perform the Unlock and Wipe device actions even when the device is locked after reboot. This mode is supported on Android 7.0 through the latest version as supported by MobileIron.
- **FIDO (Fast ID Online) devices appear in the Authenticate list:** Mobile@Work includes FIDO authenticators and FIDO registered desktops on the Authenticate screen when Mobile@Work prompts the device user to authenticate. The device user can select the FIDO device and remove it.
- **Zero Sign-on notifications Yes/No buttons switched:** For customers' ease, in the Zero Sign-on and FIDO notifications, the Yes/No action buttons have been switched. "Yes" now appears on the right and "No" appears on the left.
- **Cross profile whitelisting of Apps:** In the Lockdown policy, the "Enable Cross profile whitelisting of Apps" setting, when enabled, allows the users to share information from specific apps from within the work profile to the personal side of the Android 11+ devices. This setting is under the Android 11+ settings and is disabled by default.

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	10.8.0.0, 11.0.0.0, 11.1.0.0	10.2.0.0 through 10.7.0.0
Android	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	Not applicable

Component	Supported Version	Compatible Version
	the use of MobileIron Threat Defense.	

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)
- Hungarian
- Italian (Italy)
- Japanese
- Korean
- Polish
- Portuguese (Brazil)
- Romanian (Romania)
- Russian
- Slovak
- Spanish (Latin America)
- Swedish

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-20791:** After 30-60 minutes of changing the password in the Microsoft Azure portal, the client Authentication failed. This issue has been fixed.
- **AC-20788:** Email+, Docs@Work, and MobileIron Tunnel apps could not be closed. This issue has been fixed.
- **AC-20758:** With mutual authentication enabled and the Android Notification Mechanism in Sync policy set to "Push notification URL", check-ins from device to the Core server are delayed for ten minutes. This issue has been fixed.
- **AC-20721:** Provisioning in Android Enterprise Managed Device or Managed Device with Work Profile mode sometimes resulted in device factory reset when the Android for Work configuration was associated with dynamic labels that took too long to evaluate. This is now fixed; a one-minute grace period has been implemented that forces Mobile@Work to wait until the Android for Work configuration is pushed in subsequent check-ins with the Core server.
- **AC-20646:** The provisioning of Managed Profile on Samsung devices running Android 9.0 sometimes left the Mobile@Work client visible on the personal side of the device. 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 known issues for this release.

- **AC-20820:** Post-migration of Mobile@Work in Work Profile on Company Owned Device mode, when the device user tries to send logs from Mobile@Work, it is exiting instead.

  Workaround: Reboot the device and then try to send logs. Device user will be prompted with the list of available apps on the device and Mobile@Work will not exit.

- **AC-20780:** For Android Enterprise devices in Managed Device with Work Profile mode, after migration, the device user is prompted to "Enable Phishing protection." Even though the device user has set the client as the default browser before migration, Mobile@Work gets stuck in a loop.

  Workaround: Reboot the device and launch the migrated client. The "Enable Phishing protection" will not display and the UI is loaded properly.
- **AC-20349:** Previously, device users were able to access the Mobile@Work Home screen and browse the internet on a Chrome browser without completing device enrollment in Android Enterprise Work Managed device (DO) mode. There is no workaround.
- **AC-19878:** Microsoft Intune Device Compliance Support - generate notification: If a device does not check-in with AAD, a notification is sent to Core. If Mobile@Work fails to get the deviceID on subsequent check-ins, an error message displays. There is no workaround.
-

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 for this release.

- **AC-20763:** In Samsung Galaxy M31s devices, mandatory apps that are marked for silent installation are not getting installed silently. This applies to Device Admin mode and there is no workaround. A ticket has been logged with Samsung about this issue.

Documentation resources

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