Mobile@Work 11.0.0.0 for Android Release Notes

Revised February 23, 2021

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

Revision history

TABLE 1. REVISION HISTORY

Date	Revision
February 23, 2021	Known issue AC-20417 became AC-20419 and the text was updated for clarity. See Known issues.

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.

- 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.

- **Common Criteria and alphanumeric device passcode:** An Alphanumeric device password is no longer a requirement for Common Criteria mode for Android devices. The following settings are required to enable the Common Criteria mode:
  - Device Encryption is enabled
  - SD Card Encryption is enabled
  - Password history is disabled
  - Max password failed attempts is greater than 0

For information about these settings, see "Security policies" in the *Getting Started with MobileIron Core*.

- **Support Samsung devices on Android 11:** This client version supports Samsung devices running Android 11.
- **Email+ whitelisted and allowed to access keystore inside locked Samsung devices:** Previously, the Email+ app could not access the keystore to fetch certificates while running inside managed profiles (Work Profile (PO) mode or Managed device with Work profile (COPE) mode) when the profile was locked. With this release, the Email+ app is whitelisted using Knox APIs and allows it to access the keystore inside locked managed profiles on Samsung devices.
- **Support for app restrictions with in-house applications for Android non-GMS devices:** For devices registered to Core in a non-GMS mode, administrators can apply in-house app restrictions to these devices. Administrators can also distribute those apps and its configurations as in-house applications directly to Mobile@Work clients without using Google mobile services. For more information, see "App restrictions with in-house applications for Android" in the *MobileIron Core Apps@Work Guide*.
- **Support for Swedish and Hungarian language added:** Mobile@Work client now supports Swedish and Hungarian languages as the system default language.
- **Device users are prompted to enable location services during registration:** During the registration process, the device user may be prompted to enable the location setting. If the device user does not grant permission, the device user may have limited ability in Mobile@Work.
- **New warning banner to display upon device rebooting:** For Android devices, administrators can add a warning banner that displays upon device reboot. This is helpful for companies that require all approved mobile operating systems, such as Android 9.0, to be managed according to a security baseline / guidance. Device users will see the warning banner upon device reboot and will have to acknowledge it before continuing use of the device.
- **Support for closed network / AOSP deployment:** There are situations where the onboarding, registration and management of devices is limited and requires a different approach. Examples of these kinds of situations are:
  - In an environment that does not have connectivity to Google mobile services (GMS) due to restrictions in the organization or due to a closed network.
  - In countries where Google mobile services are not available.
  - Where devices that do not have Google mobile services but vendors have enabled Android Enterprise AOSP (Android Open Source Project.)

  With the 11.0.0.0 release, Mobile@Work now supports a new mode of deployment:
  - Integrated deployment (GMS/Non-GMS) - the entire Core instance serves devices in full Android enterprise mode (for example, Samsung devices) and also devices that do not have GMS (for example, AR/VR devices.)

  This feature applies to Android 6 devices through the latest version as supported by MobileIron.

  For more information, see this KB article.

- **Microsoft Intune Device Compliance Support added:** MobileIron Core now supports Microsoft Intune device compliance. Organizations can update the device compliance status in the Microsoft Azure Active Directory (AAD.) Using conditional access from AAD, if the device is non-compliant, administrators can block the device from accessing apps. By connecting Core to the Microsoft Azure, administrators will be able to use the device compliance status of MobileIron's managed devices for conditional access to Microsoft 365 apps. If a device does not check-in with AAD, a notification is sent to Core.

  Note The Following:

  - If the Authenticator App is not loaded on the device, the device user needs to:
    1. Open **Mobile@Work** and go to **Settings**.
    2. Tap **Microsoft 365 Access**.
    3. Device user is redirected to the Google Play Store to download the Authenticator app.
    4. In Mobile@Work, go to **Settings > Microsoft 365 Access**.
    5. Enter Microsoft credentials.
    6. Mobile@Work connects with Microsoft Azure and gives the deviceID to Azure. (Device users will see a green check next to the Microsoft 365 Access icon.)
  - If the Authenticator app is installed and the device user directly logs in, or is not logged into Mobile@Work, the device user will need to reenter credentials from within Mobile@Work.
    1. Open **Mobile@Work** and go to **Settings**.
    2. Tap **Microsoft 365 Access**.
    3. Enter Microsoft credentials.
  - If there is no MDM installed on the device, when the device user tries to access Microsoft 365 apps, the device user will be presented with registering Mobile@Work. Tap **Enroll Now** and follow the prompts.
  - Once the device is set up to connect with Azure, the device reports its compliance status to Azure. This is required to access the Microsoft 365 apps. The access token is valid for 60 minutes, afterwards, the device user will be denied access to the app.
  - If the device is not in compliance and the device user tries to access a Microsoft 365 app, an error page displays.
    1. Tap on the device management portal link.
    2. The Authenticator app opens. Select the account and login with Microsoft credentials.
    3. Select whether to stay signed in.
    4. The Microsoft portal page opens explaining why the device is not compliant.
    5. Tap This device cannot access company resources.
    6. The page refreshes with information as to why the device cannot access company resources and what actions the device user can take. Under "Your device does not meet the requirements set by

your organization," tap Show more.

7. Tapping **How to resolve this** will open the RemediationURL link. The page will have further details about steps required to resolve the issue.

If further assistance is required, contact MobileIron Technical Support.

Zero Sign-On

- **Support for new Zero Sign-on user interface:** Passwordless authentication with Zero Sign-on now supports a new user interface.
- **Support for multiple device activation for a user:** When a user tries to log in, a push notification is sent to all active devices. When the user allows push notification on any appropriate device, access is granted for the session. However, on all other devices, the sessions become invalid.
- **Support for FIDO (Fast IDentity Online) authentication:** The Android client supports FIDO with the following use cases:
  - MobileIron Authenticate
  - Cloud services login on MobileIron or Third-party Managed Desktop
  - Desktop login on MobileIron or Third-party Managed Desktop

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)
- 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-20594:** This release of Mobile@Work and later prompts Google Pixel 4 device users for the backup PIN or passcode for SaaS sign-on if face ID is blocked due to invalid attempts.
- **AC-20589:** A key PIN (in uppercase) was not processed correctly during client provisioning using QR code generated to encapsulate MIRP URL, for example, mirp://sscc01.mi-labs.es?server=sscc01.mi-labs.es&user=miexuser&**PIN**=987474. This is issue is now fixed.

- **AC-20533:** The Email+ app failed to sync with the Exchange server while running in background on locked Samsung devices in Work managed device (DO) mode due to the device entering deep doze mode. This is now fixed - Knox API is used to add the Email+ app to the list of doze mode exempts.
- **AC-20446:** When newer Mobile@Work clients provisioned in Kiosk mode supporting kiosk global actions were used with an old Core server, due to no support in the kiosk policy, the device power button became inoperational. This is now fixed - kiosk global actions are disabled in Mobile@Work if an old Core server is detected.
- **AC-20392:** After a work profile was deleted by system due to maximum number of failed unlocking attempts in Work profile (PO) mode, the profile was successfully recreated by Mobile@Work but the certificates were not reinstalled. This issue has been fixed.
- **AC-20340:** Attempts to parse large CRL (Certificate Revocation List) caused an Out-of-Memory crash on some low-end devices. This issue is now fixed.
- **AC-20298:** After provisioning devices in Work Profile on Company Owned Device mode, inactive instances of Mobile@Work client was not hidden on the personal side and thus caused confusion among device users. This issue is now fixed.
- **AC-20294:** During device wipe, the Mobile@Work client attempted to delete all files from an external SD card that was inserted in the device. This issue has been fixed. File deletion off an external SD card will not occur.

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.

This release includes the following known issues.

- **AC-20633:** The following message appears on German language devices multiple times instead of as designed, only once, when the user tries to activate passwordless sign in with Wi-Fi turned off:
  "Aktivierung fehlgeschlagen - Beim Abschluss der Aktivierungsanforderung ist ein Fehler aufgetreten. Bitte versuchen Sie es erneut." (Activation Failed - An error occurred while completing the activation request. Please try again)
- **AC-20577:** After the Microsoft Azure Active Directory (AAD) device registration is completed, the compliance status and AAD device details are uploaded to the Azure portal through the server during the next device check in.
  Workaround: After completing registration, perform a Force Device Check-In.
- **AC-20419:** If the same Azure tenant is used in multiple Core instances and this Azure tenant is de-provisioned from one Core, the Azure Device compliance status report is not updated on the remaining

Core instances.

Workaround: Disconnect and reconnect the account from another Core.

- **AC-20371:** The AAD Device Compliance feature is not supported on Android devices in Managed Device with Work Profile (COPE) mode.

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.

This release includes the following third-party limitations.

- **AC-20557:** The Mobile@Work client cannot get location when the device user sets location permission as **Allow all the time**.
- **AC-20555:** After unlocking an Oculus device from Core, the Password is reset to 0000 which is working as expected. However, upon entering the 0000 password to unlock, a blank screen displays and does not go away.

  Workaround: After the device user presses the Home (Oculus) button, the device screen displays after 5 seconds.
- **AC-20541:** During the client upgrade to Mobile@Work version 11.0.0.0, a "Grant Phone Permissions" prompt displays while the device is granting READ_PHONE_NUMBERS permission in the background. (The normal upgrade process is silent / does not require user input.)

  Workaround: Device user taps Continue to dismiss the Grant Phone Permissions prompt.

Documentation resources

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