Mobile@Work 12.4.0 for iOS Release Notes

September 15, 2020

For complete product documentation see:
Mobile@Work for iOS Product Documentation Home Page

Contents

About Mobile@Work for iOS **4**

About these release notes 4

MobileIron Mobile@Work upgrade note **4**

New features and enhancements summary **4**

General features and enhancements 4

MobileIron Threat Defense (MTD) features and enhancements 5

Support and compatibility **5**

Support policy 5

Mobile@Work for iOS supported and compatible table 6

Language Support **6**

Resolved issues **7**

Known issues **7**

Limitations **8**

Documentation resources **8**

About Mobile@Work for iOS

Mobile@Work for iOS 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 the administrator set in MobileIron Core.

About these release notes

These release notes only contain resolved and known issues, limitations, and upgrade information particular to this patch release. For new feature and other information about the major release, please see the release notes for that release.

MobileIron Mobile@Work upgrade note

This section describes the following upgrade note for the current release of Mobile@Work.

- To fix an AppConnect startup issue in Wrapped apps, before upgrading to Mobile@Work 12.3.0 or later, wrap all AppConnect wrapper apps using AppConnect 4.5.2 for iOS. For more information, see AppConnect for iOS: Mandatory Updates for Client App Compatibility in the MobileIron Support Community.

New features and enhancements summary

This section provides summaries of new features and enhancements available in this release of Mobile@Work for iOS. References to documentation describing these features are also provided, when available.

- General features and enhancements
- MobileIron Threat Defense (MTD) features and enhancements

For new features and enhancements provided in previous releases, see the release notes for those releases. Documentation for previous releases is available in Mobile@Work for iOS Product Documentation Home Page. MobileIron Support credentials are required to access the site.

General features and enhancements

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

- **User Enrollment for Apple Business Manager added to Mobile@Work:** An enrollment option designed for companies implementing BYOD (Bring Your Own Device). When the administrator assigns

the device user to User Enrollment mode, the In-App registration will download the User Enrollment Profile to the device. User Enrollment is a modified version of the MDM protocol with a much greater focus on user privacy, implemented with a level of security that enterprises need.

User Enrollment utilizes the user's managed Apple ID, which is required and associated with all enterprise apps and data on the device and in iCloud Drive. Managed Apple IDs were first utilized by Apple School Manager and are now utilized by Apple Business Manager for User Enrollment.

User Enrollment is not to be confused with device enrollment. User Enrollment applies to devices iOS 13.0 beta 7 through the latest version as supported by MobileIron. Devices lower than iOS 13.0 will be considered "device enrollment" regardless if the device user has been enabled for User Enrollment.

For more information, see "User Enrollment with Apple Business Manager" in the MobileIron Core Device Management Guide for iOS and macOS Devices.

- **New permission prompt added upon first launch of Mobile@Work:** On devices running iOS version 14.0 through the most recently released version as supported by MobileIron, device users will see the following text message: "MobileIron would like to find and connect to devices on your local network. Local network usage information is required for MobileIron Threat Defense." The message displays after updating to iOS 14.0 and restarting the device, or upon first launch of the app after installation. Device users must click OK to enable man-in-the-middle (MITM) threat detection on the device.

MobileIron Threat Defense (MTD) features and enhancements

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.

Support policy

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

TABLE 1. SUPPORTED AND COMPATIBLE DEFINITIONS

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 iOS supported and compatible table

The following table summarizes supported and compatible product versions for Mobile@Work for iOS.

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

TABLE 2. SUPPORTED AND COMPATIBLE PRODUCT VERSIONS FOR MOBILEIRON FOR IOS

Component	Supported Version	Compatible Version
MobileIron Core	10.5.2.1, 10.6.0.2, 10.7.0.1, 10.8.0.0	8.0.0.0 - 10.4.0.4
iOS	iOS 11.0 - iOS 13.7, iOS 14.0 beta 7	iOS 10.0
Standalone Sentry	9.8.5	7.6.0 - 9.7.2
MobileIron Threat Defense	management console: zConsole 4.28.7	Not applicable

Language Support

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

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

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

Resolved issues

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

There are no resolved issues in this release.

Known issues

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

There are known issues in this release.

- **IOS-16050:** When installing the AppConnect app, Mobile@Work is taking too long to display the Touch ID for "MobileIron" prompt. This causes the Mobile@Work app checkin interval to expire.
- **IOS-16041:** Mobile@Work requests passcode even though Face ID is enabled. This occurs when Face ID is enabled on Core without using the device passcode as a fallback mechanism.
- **IOS-16039:** During Mobile@Work registration with Connected Cloud, a "Connection Error" message displays in the My Devices tab.
- **IOS-15913:** Pasteboard related issues: The Mobile@Work client on iOS 14 beta releases continues to use the pasteboard for backward compatibility for apps built using existing versions of the AppConnect SDK. On iOS 14 beta releases, device users will see a banner notification whenever a flip takes place between AppConnect apps and the MobileIron client. See also AP-5497 and AP-5421 in Limitations.

Limitations

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

There are limitations in this release.

- **IOS-16087:** On iOS 14 devices with a previous Mobile@Work release, when the device user accepts the untrusted certificate, the Zero Sign-on identity certificate is removed from the device.
  Workaround: Reinstall the Mobile@Work app or have the Core server re-push the Zero Sign-on configuration.
- **IOS-16053:** The SAM login status is incorrect after inactivity timeout. Despite the AppConnect app flipping to the client after biometric authentication, the login status is not updated. The fix requires that the AppConnect app be built using an updated SDK. This issue will be resolved with the next client and AppConnect release.
- **AP-5497:** On iOS 12 or earlier, end users are being prompted for biometric authentication more than once.
- **AP-5421:** iOS 14 beta 7 does not work well with AppConnect apps using UIWebView. The recommendation is to move from UIWebView to WKWebView in the device's AppConnect app. There is no way to resolve this without a fix in the OS.

Documentation resources

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