Mobile@Work 12.3.0 for iOS Release Notes

July 6, 2020

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

Contents

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 you set on 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.

The following features that were disabled in Mobile@Work 12.2.2 have been enabled in this release:

- **Block or retire device if password retry count exceeded the maximum number of retry attempts:** Administrators can set AppConnect Passcode options in the AppConnect Global policy to either block or retire the device if the AppConnect passcode retry attempts exceed the configured maximum number of failed attempts.
- **SSO to access My Devices tab on Mobile@Work:** Device users who register Mobile@Work will need to enter the password the first time My Devices is accessed. After registration, it is no longer necessary for the device user to re-enter the password each time the My Devices tab is accessed. If upgrading from prior versions of Mobile@Work, in order for this feature to work, device users will need to enter the password once after upgrading. In the case of iReg Registration, when the device user launches MyDevices for the first time, the device user will be prompted to enter credentials. After that, it is no longer necessary for the device user to re-enter the password each time the My Devices tab is accessed.

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, 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.

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.

NOTE: Before authenticating the device user with the MobileIron Zero Trust solution, Mobile@Work first verifies that the device is not Jailbroken. If the device is Jailbroken, Mobile@Work does not allow the device user to use the device for the Zero Trust solution. This is the normal functionality of the MobileIron Zero Trust solution.

- **Rebranding:** MobileIron has updated the Mobile@Work for iOS icon and user interface color scheme.
- **Enable split tunneling using MobileIron Tunnel:** Support for handling AppTunnel rules through MobileIron Tunnel rather than through AppTunnel. The feature is enabled by configuring the *Enable split tunneling using MobileIron Tunnel* option available in the AppConnect App Configuration, Docs@Work configuration, and Web@Work configuration on the MobileIron Core Admin Portal. The option on MobileIron Core is provided as a workaround due to the planned deprecation of the UIWebView API by Apple. The feature requires MobileIron Core 10.7.0.0 and MobileIron Tunnel 4.1.0 for iOS.
  - For information about the UIWebView API deprecation, see UIWebView Deprecation and AppConnect Compatibility.
  - For information about configuring AppConnect App Configuration, see "AppConnect app configuration" in the *MobileIron Core AppConnect and AppTunnel Guide*.
- **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*.

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	10.5.0.2, 10.6.0.1, 10.7.0.0	8.0.0.0 - 10.4.4.0
iOS	iOS 11.0 - iOS 13.3, 13.4.1	iOS 10
Standalone Sentry	9.8.0	7.6.0 - 9.7.2
MobileIron Threat Defense	management console: zConsole 4.27.3	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 resolved issues in this release:

- **IOS-15362:** To fix an AppConnect startup issue in Wrapped apps, before upgrading to Mobile@Work 12.3.0, 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.
- **IOS-14966:** Previously, for MTD-enabled customers, Mobile@Work crashed on a Jailbroken device. This issue has been fixed.

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-15592:** If the passcode requirement was disabled in Core, and Mobile@Work and the AppConnect app were both terminated, the password creation prompt does not display when the passcode requirement is re-enabled on Core.
- **IOS-15777:** In a Zero Sign-On authentication workflow, when device users tap to approve a push notification and also authenticate using biometrics, sometimes the Access granted message is instantly replaced with an authentication error message. This issue is seen intermittently.
- **IOS-15819:** In Dark mode, the Username/Password screen does not display clearly.

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 no limitations in this release.

Documentation resources

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