



Mobile@Work 12.2.0 for iOS Release Notes

March 10, 2020

For complete product documentation see:

[Mobile@Work for iOS Product Documentation Home Page](#)

Copyright © 2009 - 2020 MobileIron, Inc. All Rights Reserved.

Any reproduction or redistribution of part or all of these materials is strictly prohibited. Information in this publication is subject to change without notice. MobileIron, Inc. does not warrant the use of this publication. For some phone images, a third-party database and image library, Copyright © 2007-2009 Aeleeeta's Art and Design Studio, is used. This database and image library cannot be distributed separate from the MobileIron product.

“MobileIron,” the MobileIron logos and other trade names, trademarks or service marks of MobileIron, Inc. appearing in this documentation are the property of MobileIron, Inc. This documentation contains additional trade names, trademarks and service marks of others, which are the property of their respective owners. We do not intend our use or display of other companies' trade names, trademarks or service marks to imply a relationship with, or endorsement or sponsorship of us by, these other companies.



Contents

About Mobile@Work for iOS	4
About these release notes	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	7
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 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](#).

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.

- **Added a disclaimer that displays before Mobile@Work registration:** "As required by Apple policy, we do not share any data collected by our service with any third parties for any reason" now displays before the registration of Mobile@Work.
- **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.
- **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.

- This feature requires MobileIron Core 10.6.0.0.
- For information about configuring the AppConnect Global policy, see the *MobileIron AppConnect and AppTunnel Guide for MobileIron Core*.
- **AppConnect passcode update alert:** If the passcode policy on the MobileIron UEM is changed, device users are alerted to update their AppConnect passcode when they check for updates or do a forced device check-in. For information on resetting the AppConnect passcode, see "Resetting the secure apps passcode - administrator initiated" in the *MobileIron AppConnect and AppTunnel Guide for MobileIron Core*.

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



Term	Definition
	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	10.4.0.3, 10.5.0.2, 10.6.0.0	8.0.0.0 - 10.3.0.3
iOS	iOS 11.0 - iOS 13.3	iOS 10
Standalone Sentry	9.8.0	7.6.0 - 9.7.2
MobileIron Threat Defense	management console: zConsole 4.26.1	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-15276:** MobileIron identified an issue that is causing Mobile@Work 12.1.1 clients to crash intermittently. If you are experiencing this issue, please contact MobileIron Support for remediation instructions. Alternatively, upgrading to Mobile@Work 12.2.0 will resolve this issue.
- **IOS-15183:** Before authenticating the device user with the MobileIron Zero Trust solution, Mobile@Work verifies that the device is not jailbroken. If the device is jailbroken, Mobile@Work does not allow the device user use the device for the Zero Trust solution.

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 no known issues in this release.

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-15018:** The "Maximum number of failed attempts" value in the AppConnect Global policy and related actions are only applicable to the AppConnect passcode. iOS does not allow tracking failed attempts when authenticating using Touch/Face ID or Device passcode. As a result, if an iOS device is set up for both



Touch ID and Device passcode, then iOS blocks the AppConnect app if the Device passcode retries exceed the predefined number in the operating system. iOS blocks the AppConnect app irrespective of the setting for "Maximum number of failed attempts action" in the AppConnect global policy.

- **IOS-14966:** For MTD-enabled customers, Mobile@Work crashes on a Jailbroken device. This is a vendor issue and MobileIron is working on a fix.

Workaround: Un-jailbreak the device.

- **IOS-14665:** Pull client logs is not implemented when Mutual Authentication is enabled on the server. In such instances, the administrator will have to request the device owner to explicitly push logs.

Documentation resources

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

