



Mobile@Work 12.2.2 for iOS Release Notes

March 16, 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
- Resolved issues** 4
- Known issues** 4
- Documentation resources** 5



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 delivered in Mobile@Work 12.2.0 have been disabled 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.

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:

- Mobile@Work 12.2.1 had intermittent issues with the keychain on device reboot. This release resolves these issues.

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-15321:** Users migrating from MobileIron Core to Cloud might see a "Device was reset" message and be asked to re-register.

Workaround: Instead of re-entering the username and password, device users should:

1. Uninstall Mobile@Work.
2. Remove MDM profiles from the Device Settings -> General -> Profiles & Device Management.
3. Install MobileIron Go from the App Store. This is because MobileIron Go is designed to work with MobileIron Cloud Services.

- **IOS-15320:** On jailbroken devices with Checkra1n, the app may crash intermittently.

Workaround: Device user needs to un-install Checkra1n and re-launch Mobile@Work.

- **IOS-15304:** On some devices, where the device user is forced to re-enter credentials on the Mobile@Work client, Zero Password will not work.

Workaround: The steps below must be performed by the system administrator.

1. Remove the Zero Password Label and force device check-in.
2. Add the label back to Zero Password and force device check-in.

Once these actions are completed, the Zero Password functionality becomes available on the device.

Documentation resources

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

