Mobile@Work 12.11.0 for iOS Release Notes

Revised: November 20, 2020

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

Contents

Revision history **4**

About Mobile@Work for iOS **5**

MobileIron Mobile@Work upgrade information **5**

New features and enhancements summary **5**

General features and enhancements 5

Zero Sign-on features 7

MobileIron Threat Defense (MTD) features and enhancements 8

Support and compatibility **8**

Support policy 8

Mobile@Work for iOS supported and compatible table 9

Language Support **9**

Resolved issues **10**

Known issues **10**

Limitations **10**

Documentation resources **10**

Revision history

TABLE 1. REVISION HISTORY

Date	Revision
November 20, 2020	Updated steps in the "Microsoft Intune Device Compliance Support added" bullet in New features and enhancements summary .

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 administrators set in MobileIron Core.

MobileIron Mobile@Work upgrade information

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

To fix an AppConnect startup issue in Wrapped apps, before upgrading to Mobile@Work version 12.3.0 through the latest version of MobileIron, wrap all AppConnect wrapper apps using AppConnect 4.5.2 for iOS.

NOTE: AppConnect apps built with SDKs older than version 4.5.2 will no longer work.

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
- Zero Sign-on features
- 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.

- **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 noncompliant, 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 Apple 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:

  1. Device user will need to reenter credentials from within Mobile@Work.
  2. Open **Mobile@Work** and go to **Settings**.
  3. Tap **Microsoft 365 Access**.
  4. 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**.

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

  If further assistance is required, contact MobileIron Technical Support.

- **Deactivate notifications for sign in:** Device users can now deactivate notifications for sign in. On the device, go to Settings and then tap Authenticate. Switch on **Passwordless Sign-In**. A dialog box displays asking confirmation of deactivating passwordless sign in such as notifications on the device. Confirm by tapping **Deactivate**.

Zero Sign-on features

This section summarizes new Zero Sign-on features supported on MobileIron Access 44, targeted to release in December 2020. For more information, see "Zero Sign-on with MobileIron Access" in the *MobileIron Access Guide*.

- **Configuring Zero Sign-on on UEM:** When the new version of Zero Sign-on is configured on the UEM server, the Zero Sign-on configuration has a new option for enabling authentication. If Zero Sign-on is disabled, then only authentications in Fast Identity Online (FIDO) code and push notification format is accepted.

  NOTE: If the UEM server is FIDO-enabled and users are running MobileIron applications that are not FIDO capable, you must re-push the Zero Sign-on configuration after users have upgraded to the FIDO version of MobileIron applications.

- **Client upgrade:** After the client is upgraded, it registers the new Zero Sign-on settings even though the FIDO flag is disabled in SaaS sign-on configuration from UEM. Also, the application attempts to register even if the server is still not a FIDO release.
- **Support for Authenticator Only mode:** The Authenticator Only mode allows employees to use their unmanaged mobile device as their identity and authentication factor. Using their device as their identity enables employees to take advantage of Zero Sign-on features that allow passwordless access to SaaS applications and other business services.
- **Support for multiple device activation for a user:** When a device user tries to log in, a push notification is sent to all active devices. When the device user allows push notification on any appropriate device, access is granted for the session.
- **Receiving FIDO notifications:** If the FIDO flag is disabled or client is retired, client will unregister from FIDO and the client will not receive the FIDO notifications.
- **Support for a new authentication settings screen:** If Session management is enabled on MobileIron Access, a new end browser session option in Settings > Authenticate displays. There is a Passwordless Sign-in toggle switch to activate and deactivate the setting. This option ends all the open browser sessions for Access.
- **Support for greater security:** When the FIDO flag is enabled, the desktop unlock feature is supported and device users can log in to desktop only by approving a push notification. This always requires

managed iOS devices. It also has the ability to retrieve and remove all Zero Sign-on related push notifications from the notification center.

- **Zero Sign-on camera:** The iOS native camera supports scanning FIDO and non-FIDO QR codes. The process to scan and authenticate the two types of QR codes is identical, although, if an error occurs, error messages are reported differently.

  NOTE: If both Mobile@Work and MobileIron Go are installed on the same device, it might cause problems when scanning QR codes with the native camera. Only one of these applications should be installed at a time.

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

Component	Supported Version	Compatible Version
MobileIron Core	10.7.0.1, 10.8.0.0, 11.0.0.0	8.0.0.0 - 10.4.0.4 10.5.2.1, 10.6.0.2
iOS	iOS 11.0 - 14.1	iOS 10.0
Standalone Sentry	9.9.0	7.6.0 - 9.8.5
MobileIron Threat Defense	management console: zConsole 4.28.11	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-16294:** FIDO Registration of iOS Mobile@Work client fails when the selected algorithm is other than ES256 in the Access FIDO Key settings.
- **IOS-16283:** 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, the device user can do a Force Device Check-in.

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-16241:** Device is not getting removed from the Microsoft Azure portal when device is de-registered from the Microsoft Authenticator portal. There is no workaround for this issue.
- **IOS-16175:** For iOS 14.0 devices, if Safari is not set as the default browser, the profile is not downloaded automatically. For more information, see this KB article.

Documentation resources

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