MobileIron Go 76 for iOS Release Notes

March 23, 2021

For complete product documentation, see:

MobileIron Go for iOS Documentation Home Page

Contents

About MobileIron Go for iOS

MobileIron Go for iOS securely connects your iOS device to your company network so that you can easily access email and other work resources. With MobileIron Go, you can:

- Easily get access to corporate resources such as email, calendar, and contacts on your iOS device.
- Connect automatically to corporate Wi-Fi and VPN networks.
- Discover and install work-related applications on your device wherever you are.
- Automatically comply with corporate security policies.
- Locate lost or stolen devices and remotely manage them.

MobileIron Go works in conjunction with MobileIron Cloud supported by your company's IT organization. Please follow the instructions from your IT organization to use this app. MobileIron Go is required to access corporate resources and therefore should not be removed without first consulting your IT organization. Learn about Mobile Device Management (MDM) at https://www.mobileiron.com/en/solutions/multi-os-management/ios.

New features summary

This section covers new features for this release of MobileIron Go for iOS.

- Zero Sign-on
- AppConnect

For new features provided in previous releases, see the "New features summary" sections in the release notes for those releases, available in MobileIron Go for iOS Product Documentation.

Zero Sign-on

- **FIDO (Fast ID Online) devices appear in the Authenticate list**: When the devices prompt the device user to authenticate, MobileIron Go now displays the list of authenticator and FIDO registered desktops in the Authenticate screen. The device user can remove/de-register the FIDO devices from the list.

AppConnect

- **AppConnect passcode user interaction updates**: This release streamlines and provides improvements in the authentication user experience for AppConnect apps. The following describes the AppConnect passcode user interaction updates:

- If the AppConnect passcode expires, users see an alert that the passcode has expired after they authenticate. Previously, the alert was visible during authentication.
- Passcode history is preserved even after AppConnect is disabled and re-enabled. Previously, the passcode history was lost when AppConnect was disabled and re-enabled.
- After a passcode reset due to too many incorrect authentication attempts, the client does not flip to the AppConnect app. Previously, the client automatically flipped to the AppConnect app.
- If Touch ID or Face ID authentication is enabled on Cloud, when users first launch an AppConnect app they are prompted to authenticate using Touch ID or Face ID. They are not prompted for the AppConnect passcode. Previously, users were prompted for their AppConnect passcode when the AppConnect app was first launched.
- When changing or disabling Face ID or Touch ID, users are prompted to authenticate only if they were not already authenticated. Previously, users were always prompted to authenticate with Face ID or Touch ID.

See "**iOS AppConnect Devices field description**" and "**Secure apps on iOS Devices - User Perspective**" in the MobileIron AppConnect Guide for Cloud for the AppConnect passcode settings field descriptions and device user experience.

Upgrade notes:

- After an upgrade to MobileIron Go, if an AppConnect passcode is required, device users are prompted to set up a new AppConnect passcode when they first launch MobileIron Go or launch an AppConnect app.
- If the AppConnect passcode policy is changed to require a new passcode and the Go client is upgraded, device users are prompted to set a new AppConnect passcode or biometric when they launch the Go client or launch an AppConnect app. After some time, they are prompted again for their AppConnect passcode or biometric.

Support and compatibility

The information in this section includes the components MobileIron supports with this product.

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

Support policy

MobileIron defines supported and compatible as follows:

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.

MobileIron Go for iOS supported and compatible table

This version of MobileIron Go for iOS is supported and compatible with the following product version:

Product	Supported	Compatible
MobileIron Cloud	75, 76	74
iOS	iOS 12 to iOS 14.4	iOS 11
MobileIron Threat Defense	Management console: zConsole 4.28.14	Not Applicable

Resolved issues

For resolved issues identified in previous releases, see MobileIron Go for iOS Product Documentation for that release.

There are no resolved issues in this release.

Known issues

For known issues identified in previous releases, see MobileIron Go for iOS Product Documentation for that release.

This release includes the following known issues.

- **AIOS-5152**: The Enter Passcode prompt for AppConnect apps is not seen if the Go client is sent to the background after the prompt is first displayed.
  Workaround: Bring Go to the foreground to view the Enter Passcode prompt.

- **AIOS-5154**: When users cancel Touch ID authorization, they are shown a '**Contact Admin**' error message instead of a '**Failed to authenticate**' user error message.

Limitations

For third-party limitations identified in previous releases, see MobileIron Go for iOS Product Documentation for that release.

This release includes the following third-party limitations.

- **AIOS-5153**: The device is not removed from the Microsoft Azure portal when the device is de-registered from the Microsoft Authenticator portal. There is no workaround for this issue.

Documentation resources

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

For complete product documentation, see MobileIron Go for iOS Documentation Home Page.

MobileIron Support credentials are required to access documentation in the Support Community.