MobileIron Go 75 for iOS Release Notes

February 02, 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.

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.

AAD device compliance

- **Microsoft Intune Device Compliance Support added:** MobileIron Cloud 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 Cloud 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 Cloud. This feature is supported on Cloud 75 through the most recently released version as supported by MobileIron.

  Note The Following:

- If the Authenticator App is not loaded on the device, the device user needs to:
  1. Open **MobileIron Go** 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 MobileIron Go, go to **Settings > Microsoft 365 Access**.
  5. Enter Microsoft credentials.
  6. MobileIron Go connects with Microsoft Azure and gives the deviceID to Azure. (Device users will see a check mark 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 MobileIron Go:
  1. Device user will need to reenter credentials from within MobileIron Go.
  2. Open **MobileIron Go** 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 MobileIron Go. 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.

General features

- **Option to send AppConnect logs added**: This release of MobileIron Go for iOS had added the ability to send AppConnect logs.
- **Settings screen improvements**: The **Settings** screen is improved to make it intuitive and enhanced the overall look and feel.

MobileIron Threat Defense features

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 Cloud, available on the MobileIron Threat Defense for Cloud documentation page at MobileIron Community.

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.

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	74
iOS	iOS 12 to iOS 14.3	iOS 11
MobileIron Threat Defense	Management console: zConsole 4.28.13	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-5019**: 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 the registration, the device user can do a Force Device Check in.
- **AIOS-4967**: The policy violation notification on the iOS Go client app is not saved on the **Notification** tab. Instead, the manually triggered push notification is saved on the **Notification** tab.

Limitations

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

There are no third-party limitations in this release.

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.