MobileIron Go 75 for Android Release Notes

February 11, 2021

For complete information, see the MobileIron Go for Android Documentation Home Page.

Contents

About MobileIron Go for Android

MobileIron Go for Android securely connects your Android 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 Android 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/android.

New features summary

For the summary of new features introduced in previous releases, see MobileIron Go Client for Android Product Documentation for that release.

This release includes the following new features and enhancements:

- **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). By connecting Cloud to Microsoft Azure, administrators will be able to use the device compliance status of MobileIron's managed devices for conditional access to Microsoft 365 apps. Using conditional access from AAD, if the device is non-compliant, administrators can block the device from accessing 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**. Note the status of Microsoft 365 Access is listed as "Off."
    3. Device user is redirected to the Google Play Store to download the Microsoft Authenticator app.
    4. In MobileIron Go, go to **Settings > Microsoft 365 Access**.

5. Enter Microsoft credentials.
6. MobileIron Go connects with Microsoft Azure and receives the deviceID from Azure. (In Settings, Microsoft 365 Access lists as "On.")

- If the Authenticator application is installed and the device user directly logs in, or is not logged into MobileIron Go, the device user will need to reenter credentials from within MobileIron Go.
  1. Open **MobileIron Go** and go to **Settings**.
  2. Tap **Microsoft 365 Access**. Note the status of Microsoft 365 Access is listed as "Off."
  3. Enter Microsoft credentials.
  4. Tap **Enroll Now** and follow the prompts.
  5. When finished, The status of Settings > Microsoft 365 Access lists as "On."
- 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.
- A status bar notification informs the user of this new feature. If device user taps on the notification, it open to Notifications.
- An in-app notification occurs when action from the device user is needed.
- If device user dismisses the notification without doing the required action, the notification will appear again upon the next compliance check.
- 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 Microsoft 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**.
  7. 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.

- **Auto-restart for Zebra devices after full OS update:** Zebra devices now restart automatically after a full OS update, removing the requirement for the device user to restart the device to complete the update.

- **FIDO (Fast ID Online) devices appear in the Authenticate list:** MobileIron Go includes FIDO authenticators and FIDO registered desktops on the Authenticate screen when MobileIron Go prompts the device user to authenticate. The device user can select FIDO device (FIDO Authenticators + FIDO registered desktops), and also remove FIDO devices from the list.
- **Support for bulk enrollment**: Bulk enrollment is now supported for devices being provisioned as a work profile on company-owned device when using Provisioner, Google Zero Touch, or Knox Mobile Enrollment.
- **Full access to all device apps, controls, and settings after MobileIron Cloud administrator relinquishes ownership** A device user with a device in enhanced Work Profile mode can use the device as a personal device, with full access to all device apps, controls, and settings, after the MobileIron Cloud administrator uses the Relinquish Ownership capability against that device. Relinquishing ownership of a device in Work Profile on Company Owned Device removes the work profile and retires the device from MobileIron Cloud, without affecting personal apps and data.
- **Suspend personal apps when device falls out of compliance:** Administrators can configure MobileIron Cloud policies offering quarantine actions to suspend apps on the personal side of the quarantined device to indicate that device user needs to address the compliance issues on the device to make it functional. Supported on Android 11+ devices provisioned as a Work Profile on Company Owned Device.
- **Suspend personal apps when Work Profile turned off for specified time:** Administrators can configure the MobileIron Cloud Lockdown & Kiosk: Android enterprise configuration to set a maximum time that the device user can turn off the work profile before MobileIron Cloud suspends personal apps on the device. The device user sees a notification prompting to turn on the work profile to enable suspended apps. Available for Android 11+ devices in Work Profile on Company Owned Device.
- **Disabled the camera within the Work Profile:** Administrators can configure the Lockdown & Kiosk: Android enterprise configuration to disable the camera within the work profile. Coupled with the existing ability to disable the camera on the personal side of the device, this affords administrators greater flexibility. Available for Android 11+ devices in Work Profile on Company Owned Device.
- **Disabled screen capture on personal side of device:** Administrators can configure the Lockdown & Kiosk: Android enterprise configuration to disable screen capture. When selected, screen capture is disabled on the personal side of the device. Coupled with the existing ability to disable screen captures within the Work Profile, this affords administrators greater flexibility. Available for Android 11+ devices.

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 Cloud 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 Android supported and compatible table

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

Product	Supported	Compatible
MobileIron Cloud	R73, R74	R71, R72
Android	5, 6, 7, 7.1, 8, 8.1, 9, 10, 11	Not Applicable (All listed versions are tested and supported)
MobileIron Threat Defense	Management console: zConsole 4.28.12-GA	Not Applicable

Language Support

The following languages and locales are supported in this version of MobileIron Go for Android:

- Arabic
- Chinese (Simplified)
- Chinese (Traditional)
- Croatian
- Dutch
- English
- Finnish
- French (France)
- German (Germany)
- Hungarian
- Italian (Italy)
- Japanese
- Korean
- Portuguese (Brazil)
- Spanish (Latin America)
- Spanish (Spain)
- Swedish

Resolved issues

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

This release does not include any new resolved issues.

Known issues

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

This release does not include any new known issues.

Limitations

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

This release includes the following new limitations:

- **ACP-11013**: Chrome app crashes in Device Owner mode.
- **ACP-11129**: After the device is unlocked in direct boot mode, the work profile passcode prompt may reappear on the device for up to 30 seconds after changing the passcode.
  Workaround: Wait for the prompt to clear automatically.
- **ACP-11350**: Sometimes after sending an unlock command, the lock screen does not accept the original password or 0000.
  Workaround: Turn the screen off and back on. 0000 should then be accepted.

Documentation resources

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

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