Android for Work: Deploying ginlo Business with MobileIron

June 2019

Prerequisite

MobileIron Core/Cloud must be enabled for Android for Work in order to use Android for Work apps. To enable MobileIron Core/Cloud to provide Android for Work features, you must perform setup steps with Google, MobileIron Support, and MobileIron Core/Cloud Admin Console. Please ensure these steps are completed first.

Core Admin Guide: https://community.mobileiron.com/docs/DOC-3664

Cloud Admin Guide: https://community.mobileiron.com/docs/DOC-2999

Overview

ginlo Business is a fast, easy to use, and secure messaging app. Sending messages with ginlo Business is completely safe and private – no eavesdropping possible! Chat with true end-to-end encryption.

ginlo Business improves the internal communication with colleagues and teams and increases their productivity. Users can send 1:1 and group messages, exchange video and voice messages, share photos, files, and much more. All data send can be set to self-destruct, leaving no traces behind. The service complies with European data protection standards and is run on German servers exclusively. The app can be easily managed for the whole organization and ensures company-wide compliance.

App Availability

The ginlo Business app is available in the official Google Play Store under:
https://play.google.com/store/apps/details?id=business.de.dpag.simsme

To use the app, you will need a valid ginlo Business license. You can purchase a single user license either via in-app purchase or you can order any number of licenses for your whole team or organization on the ginlo Business website:
https://www.ginlo.net/en/business

Device Compatibility

This app requires version Android 5.0 (API version 14) or above.

App Deployment

1. Import the app into MobileIron Core.
   MobileIron Core Admin Portal > Apps > App Catalog > Store Import > Google Play > Google Play Store Search for the app > click Import.
2. Enable Android for Work for your app.
   MobileIron Core Admin Portal > Apps > App Catalog > Search for your app > Edit App > In “Android for Work” section > Enable “Install this app for Android for Work”.
3. Configure the app.
   MobileIron Core Admin Portal -> Apps -> App Catalog -> Search for your app -> Edit App -> In “Configurations” section -> List of key-value pairs will be pre-populated if the developer has provided them in the app.
4. Apply Label to App.
   MobileIron Core Admin Portal -> Apps -> App Catalog -> Select your app -> More Actions -> Apply Label.
   MobileIron Cloud Admin Portal

App-Specific Configuration

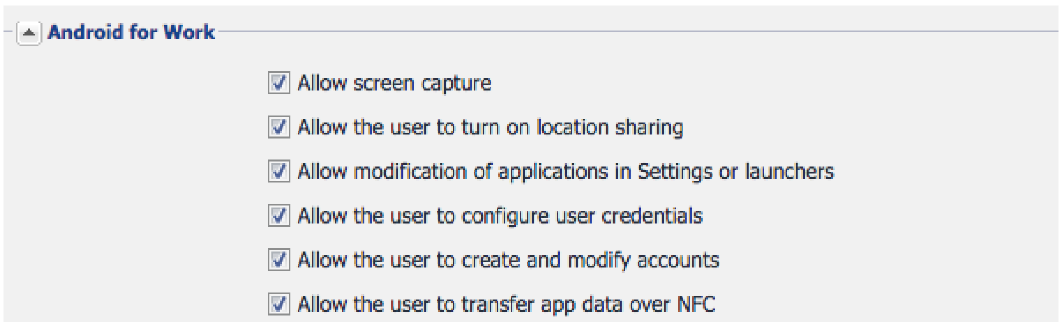
Key	Description	Default if the key-value pair is not configured
disableNoPwLogin	Boolean: true/false If set to true, the option "Ask password at startup" is set and the user can't disable it.	The user can disable the password at startup.
simsLockApplicationDelay	Integer: 0-10 After how many minutes the application asks for the password if the app was in background.	The user can choose the value by themselves.
forceComplexPin	Boolean: true/false If set to true, the user must use a complex code, no PIN code.	The user can choose if they want a complex password or a simple PIN code.
simsPasswordTries	Integer: 3,5,10 The application wipes the data if the user entered the wrong password 3, 5, or 10 times.	Wiping data is disabled.
disableSaveToCameraRoll	Boolean: true/false If set to true, saving automatically to the camera roll is disabled.	The user can save images automatically to the camera roll.

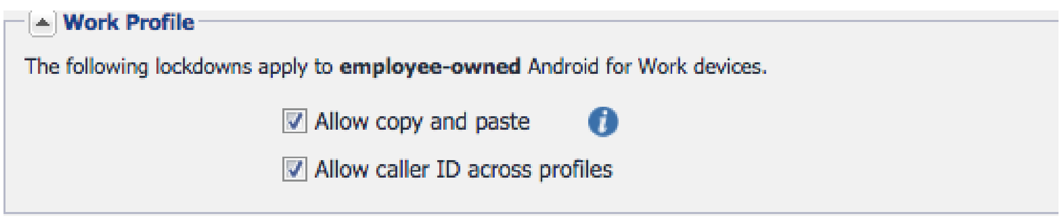
Key	Description	Default if the key-value pair is not configured
disableSendMedia	Boolean: true/false If set to true, only text messages can be sent, no images, videos, or files.	The user can send all kind of messages.
disableOpenIn	Boolean: true/false If set to true, images can't be saved to the camera roll and received files can't be opened.	The user can save images and open files.
passwordMinLength	Integer: 0-99 Minimum length of password	No minimum password length is defined.
passwordMinSpecialChar	Integer: 0-99 Minimum number of special characters like #-/ required	No special characters are required for the password.
passwordMinDigit	Integer: 0-99 Minimum number of digits are required	No digits are required for the password.
passwordMinLowercase	Integer:0-99 Minimum number of lowercase characters required	No lowercase characters are required for the password.
passwordMinUppercase	Integer: 0-99 Minimum number of uppercase characters required	No uppercase characters are required for the password.
passwordMinClasses	Integer: 0-4 How many different groups of characters (digits, special characters, lowercase, uppercase) are required	No special requirements are defined for the password.
passwordMaxDuration	Integer: 0-65535 If set, the user must change their password after the specified number of days.	The user must not change the password regularly.

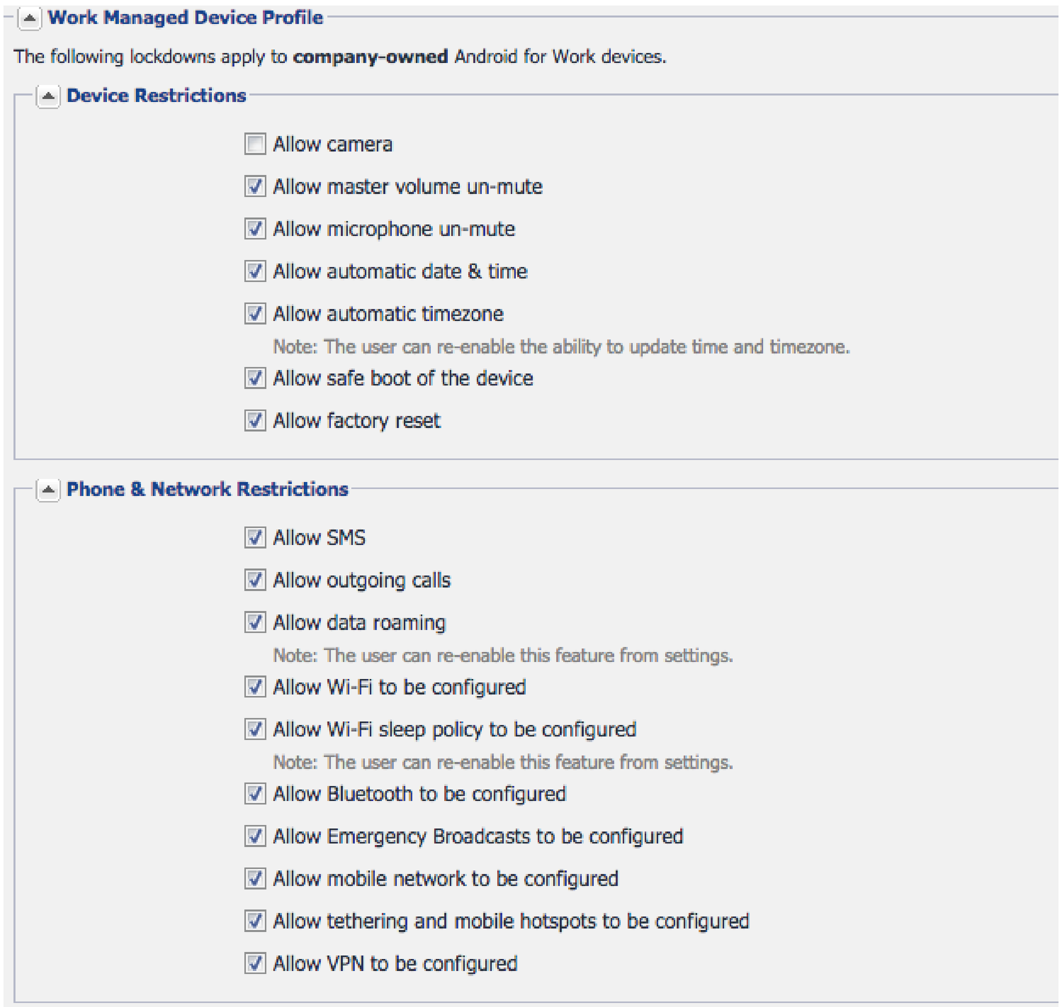
Key	**Description**	**Default if the key-value pair is not configured**
passwordReuseEntries	Integer: 0-100 If set, the application will check if the new password was already used. The application will only remember as many passwords as defined.	The user can reuse their last password.
disableExportChat	Boolean: true/false If set to true, the user can't export chats.	The user can export chats

Security Controls

Current list of MobileIron supported Lockdown policies: Policies & Configs > Policies > Add New > Lockdown







NOTE: Each of the above features are described in complete detail in DOC-3664. Future core releases could introduce new Lockdown options

MobileIron Core: https://community.mobileiron.com/docs/DOC-3664

Secure Tunneling Support

In the current version, Secure Tunneling is not supported.

Contact Details

For more information about ginlo Business, please visit our website https://www.ginlo.net/en/business or get in touch with us: https://www.ginlo.net/en/contact/

If you have questions or technical issues, please reach out to our support team who is glad to help you: b2b-support@ginlo.net