



iOS Managed Configuration: Deploying ginlo Business with MobileIron

June 2019

[Overview](#)

[App Availability](#)

[Device Compatibility](#)

[App Deployment](#)

[App-Specific Configuration](#)

[Security Controls](#)

[Secure Tunneling Support](#)

[Contact Details](#)



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.

Our APPLE-ID is: 1125705539

Our Bundle ID is: releaseba.de.dpag.simsme>

App Availability

The ginlo Business app is available in the official Apple AppStore under:

<https://itunes.apple.com/de/app/simsme-business/id1125705539?l=en&mt=8>

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:

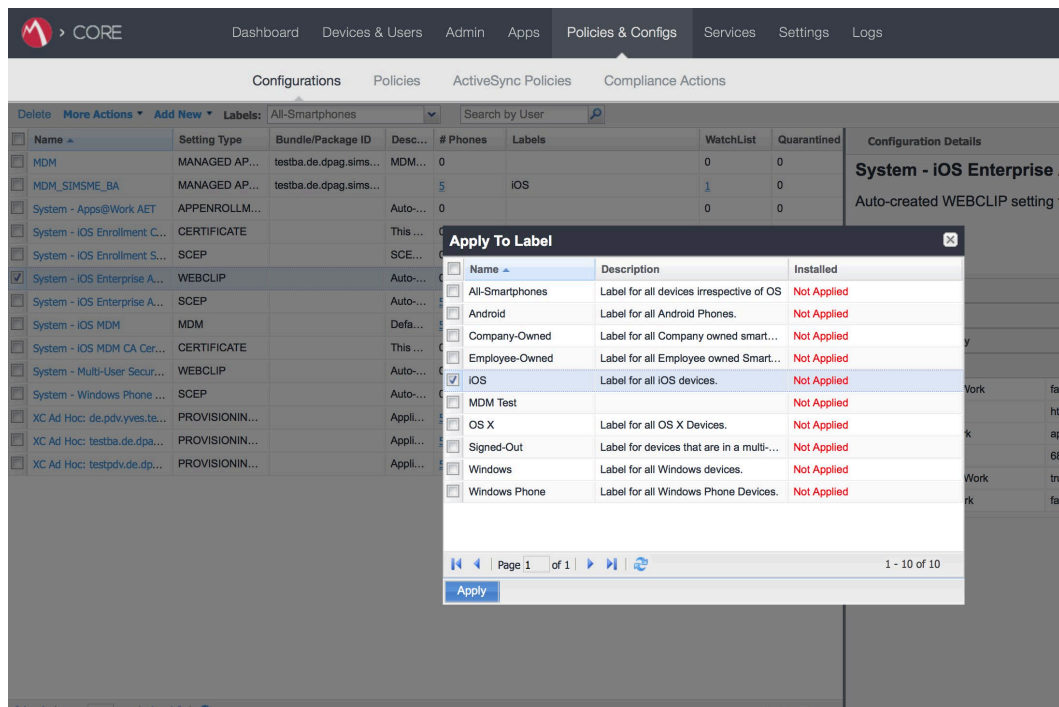
<https://www.ginlo.net/de/business/>

Device Compatibility

The app requires iOS 8 or above. Compatible with iPhone, iPad, and iPod touch.

App Deployment

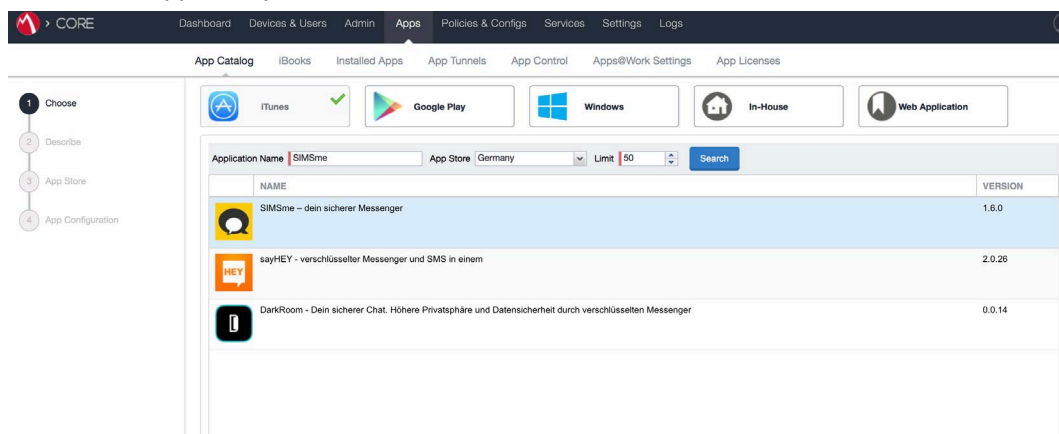
1. Enable MobileIron's iOS Enterprise AppStore WebClip to be available to the registered device.
MobileIron Core Admin Portal -> Policies & Configs -> Configurations -> Select "iOS Enterprise AppStore" -> Assign "iOS" label to this WEBCLIP



The screenshot shows the MobileIron Core Admin Portal interface. The main table lists various configurations. A modal dialog titled "Apply To Label" is open, showing a list of labels to be applied to the selected configuration. The "iOS" label is selected.

| Name | Description | Installed |
|--|--|-------------|
| <input type="checkbox"/> All-Smartphones | Label for all devices irrespective of OS | Not Applied |
| <input type="checkbox"/> Android | Label for all Android Phones. | Not Applied |
| <input type="checkbox"/> Company-Owned | Label for all Company owned smart... | Not Applied |
| <input type="checkbox"/> Employee-Owned | Label for all Employee owned Smart... | Not Applied |
| <input checked="" type="checkbox"/> iOS | Label for all iOS devices. | Not Applied |
| <input type="checkbox"/> MDM Test | | Not Applied |
| <input type="checkbox"/> OS X | Label for all OS X Devices. | Not Applied |
| <input type="checkbox"/> Signed-Out | Label for devices that are in a multi... | Not Applied |
| <input type="checkbox"/> Windows | Label for all Windows devices. | Not Applied |
| <input type="checkbox"/> Windows Phone | Label for all Windows Phone Devices. | Not Applied |

2. If the app is available in the App Store, import the app into MobileIron Server.
MobileIron Core Admin Portal -> Apps -> App Catalog -> App Store -> Search for the app -> Import

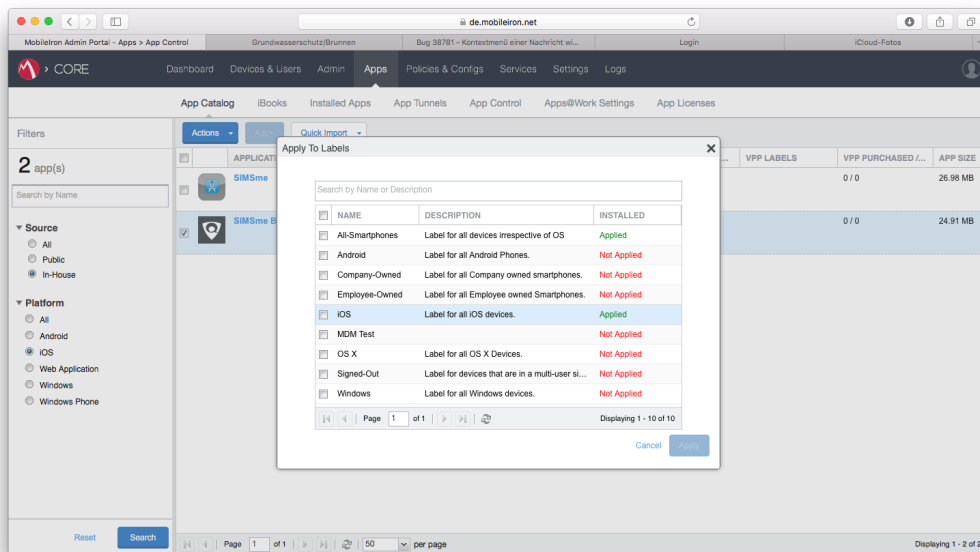


The screenshot shows the MobileIron Core Admin Portal interface for the App Catalog. The search results are displayed for the App Store, showing a list of applications with their names and versions.

| NAME | VERSION |
|--|---------|
| SIMSme - dein sicherer Messenger | 1.6.0 |
| sayHEY - verschlüsselter Messenger und SMS in einem | 2.0.26 |
| DarkRoom - Dein sicherer Chat. Höhere Privatsphäre und Datensicherheit durch verschlüsselten Messenger | 0.0.14 |



3. Assign a label; select the imported app in the above step -> Actions -> Apply Label.



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. |
| 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. |

| Key | Description | Default if the key-value pair is not configured |
|------------------------|---|--|
| 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 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. |
| 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 |



MobileIron Core Admin Portal: Policies & Configs -> Configurations -> Add New > iOS and OS X > Managed App Config

Edit Managed App Configuration with Name, Description, and Bundle ID and select the external file (PLIST) that contains the app-specific key-value pair configurations required for the app.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
  "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
  <key>disableNoPwLogin</key>
  <false/>
  <key>simsLockApplicationDelay</key>
  <integer>0</integer>
  <key>forceComplexPin</key>
  <false/>
  <key>simsPasswordTries</key>
  <integer>10</integer>
  <key>disableSaveToCameraRoll</key>
  <false/>
  <key>disableSendMedia</key>
  <false/>
  <key>disableOpenIn</key>
  <false/>
  <key>passwordMinLength</key>
```



```
<integer>6</integer>
<key>passwordMinSpecialChar</key>
<integer>1</integer>
<key>passwordMinDigit</key>
<integer>0</integer>
<key>passwordMinLowercase</key>
<integer>1</integer>
<key>passwordMinUppercase</key>
<integer>0</integer>
<key>passwordMinClasses</key>
<integer>0</integer>
<key>passwordMaxDuration</key>
<integer>0</integer>
<key>passwordReuseEntries</key>
Secur<integer>0</integer>
  <key>disableExportChat</key>
  <false/>
</dict>
</plist>
```




Security Controls

MobileIron Core Admin: App Catalog -> Edit App -> Managed App Settings:

MANAGED APP SETTINGS

| | |
|---|-----|
| Prevent backup of the app data | Yes |
| Remove app when MDM profile is removed | Yes |
| Remove app when device is quarantined or signed out | Yes |
| Send installation request on device registration or sign-in | No |

MobileIron Core Admin: Policies & Configs -> Configurations -> Add New -> iOS and IOS X -> Restrictions

- Allow documents from managed apps to unmanaged apps **License Required** ⓘ (iOS 7.0 and later)
- Allow documents from unmanaged apps to managed apps **License Required** ⓘ (iOS 7.0 and later)

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/de/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