MobileIron Support-Dokumentation

Inhaltsverzeichnis

1 EINLEITUNG 2

2 KOMPONENTEN 2

3 MOBILEIRON NUTZER UND GERÄTE HINZUFÜGEN 3

3.1 IM BROWSER HINZUFÜGEN 3

3.2 AUF IOS-GERÄT HINZUFÜGEN 6

4 APPS MIT MOBILEIRON VERWALTEN 7

4.1 APP HINZUFÜGEN 7

4.2 UPDATE EINER APP HINZUFÜGEN 10

5 EINSTELLUNGEN DER APP KONFIGURIEREN 10

5.1 EINSTELLUNGEN ANLEGEN 10

5.1.1 Plist konfigurieren 10

5.1.2 Einstellungen unter MobileIron einspielen 11

5.2 LISTE DER MÖGLICHEN PARAMETER 14

1 Einleitung

ginlo Business ist der sichere Instant Messenger der Brabbler AG. Das Senden von Nachrichten mit ginlo Business ist dank der Ende-zu-Ende-Verschlüsselung absolut sicher und vertraulich. ginlo Business verbessert die interne Kommunikation mit Kollegen und Teams und erhöht ihre Produktivität. Nutzer können in Einzel- oder Gruppenchats vertraulich Textnachrichten, Video- und Sprachnachrichten, Fotos, Dateien und vieles mehr austauschen. Der Service entspricht den europäischen Datenschutzstandards und wird ausschließlich auf deutschen Servern betrieben. Ihre Vorteile:

- Ein Messenger für die gesamte mobile Kommunikation innerhalb der Organisation
- Schnelle und sichere Echtzeit-Kommunikation zur Steigerung der Team- und Projekt-Effizienz
- Klare Trennung zwischen geschäftlicher und privater Kommunikation der Mitarbeiter
- Kontrollierte Kommunikation und Security-Einstellungen über Mobile Device Management
- Hosting und Betrieb auf deutschen Servern (DSGVO-konform, ISO-zertifiziert)

Die App kann leicht für die gesamte Organisation verwaltet werden und sorgt für Compliance. Ob Sie BYOD für Ihre Mitarbeiter anbieten, Corporate Phones oder eine Mischung aus beidem verwenden – mit ginlo Business setzen Sie auf eine sichere, unternehmensweite Kommunikation.

2 Komponenten

Die folgenden Komponenten werden für die Nutzung der ginlo Business App mit AppConfig über die Mobile-Device-Management-Plattform von MobileIron gebraucht:

MobileIron Administration Platform – Eine Server-basierte Konsole von MobileIron, die es dem Unternehmen ermöglicht, AppConfig-unterstützte Apps wie ginlo Business automatisch zu konfigurieren, im Unternehmen zu distribuieren, Richtlinien für die Verwendung zu erstellen, App-Funktionen zu steuern und ggf. die Anwendung auf bestimmten Geräten zu löschen.

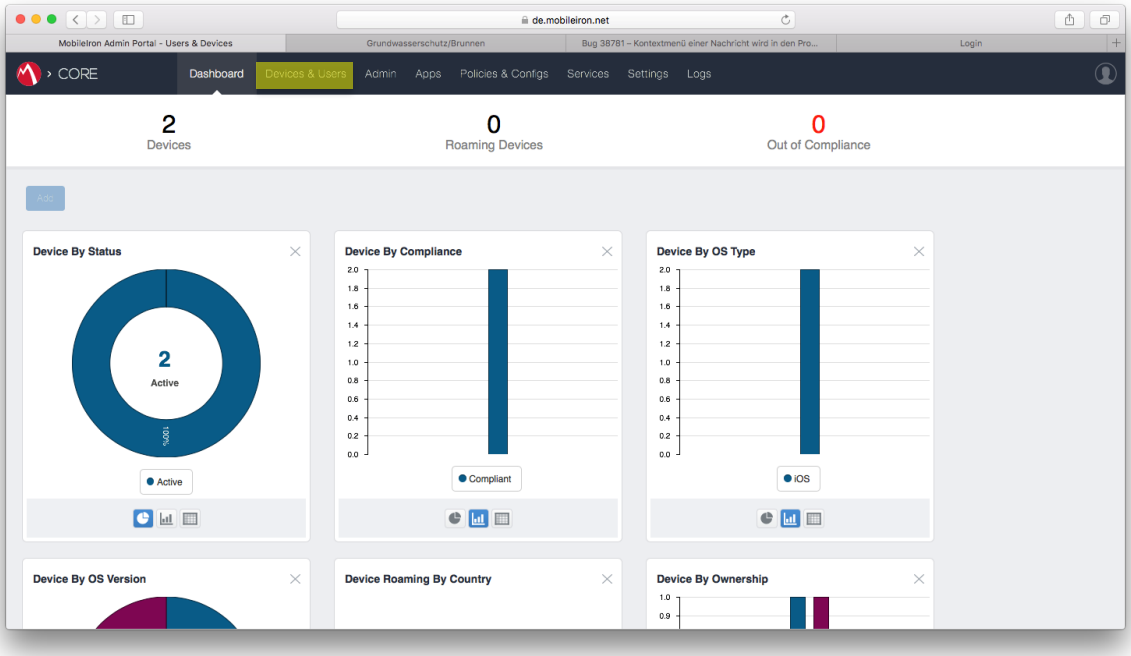
AppConfig Community - Die AppConfig Community vereinfacht die Einführung und den Einsatz von mobilen Enterprise-Anwendungen unter einem einheitlichen Ansatz. Die umfangreichen Konfigurations- und Sicherheitsmöglichkeiten basieren auf der von Apple bereitgestellten „Managed App Configuration“ unter iOS 8 und höher.

ginlo Business iOS App – Die Standard-Business-Version von ginlo für iOS unterstützt „Managed App Configuration“ und ermöglicht so die in diesem Dokument beschriebene Steuerung der Parameter. Die App ist erhältlich im iTunes App Store und erfordert für die Nutzung eine Nutzerlizenz, die auf der ginlo Website bestellt werden kann.

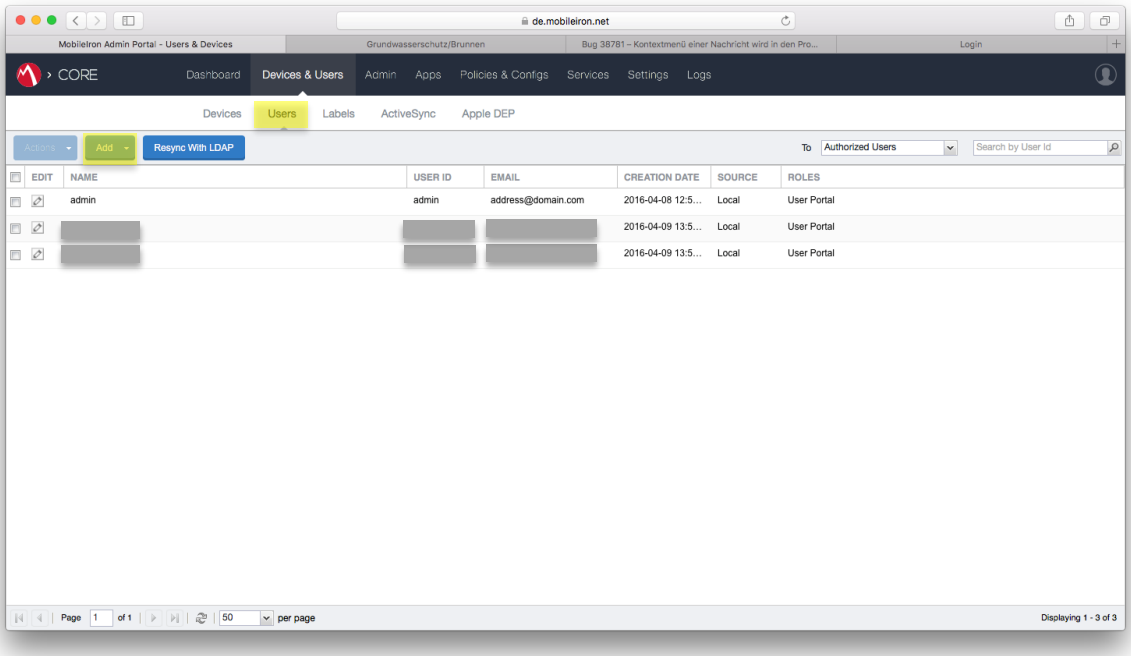
3 MobileIron Nutzer und Geräte hinzufügen

3.1 Im Browser hinzufügen

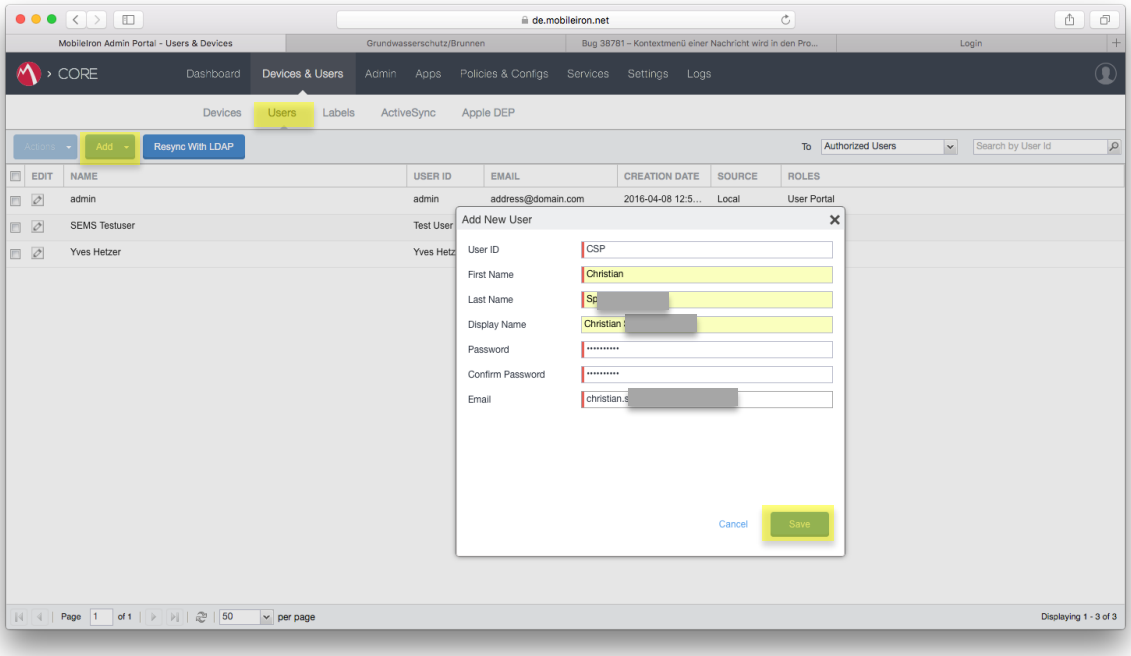
1. Öffnen Sie die MobileIron Konsole im Browser und melden sich an.



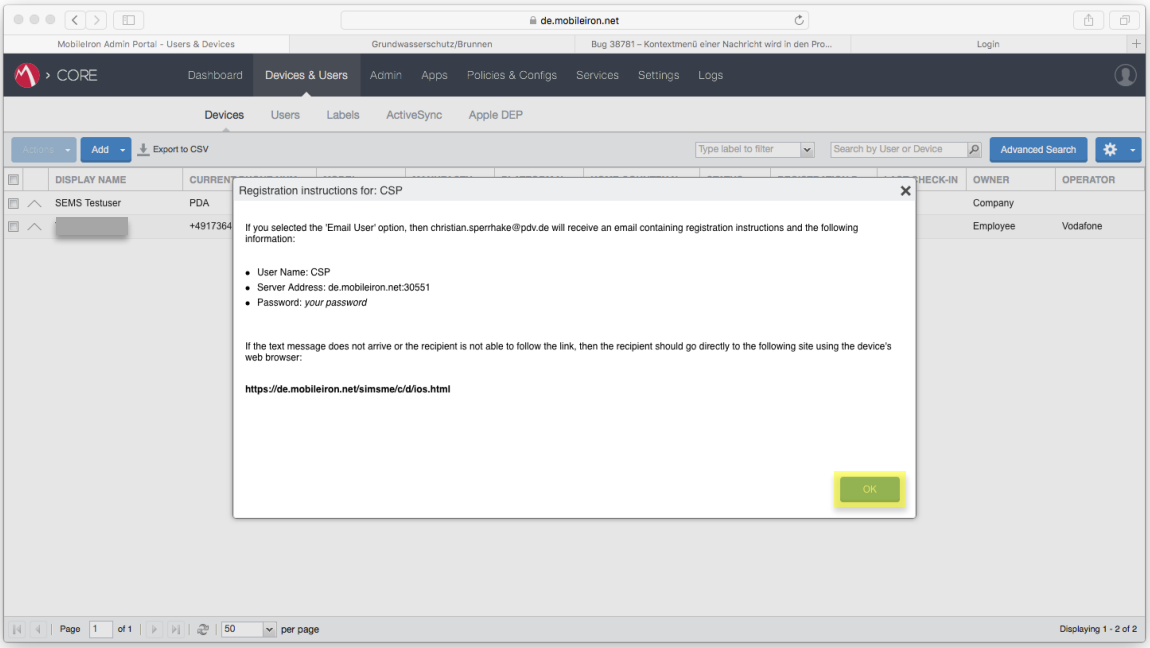
2. Zum Anlegen eines Nutzers wählen Sie den Reiter „Devices & Users“ aus und klicken auf „Users“.



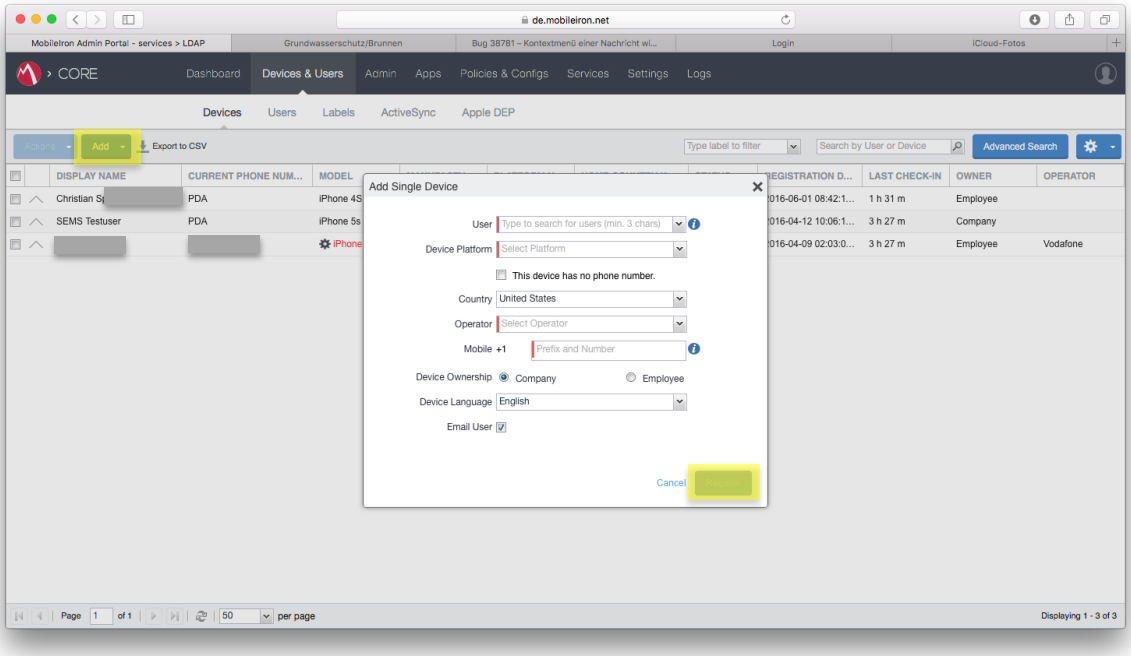
3. Klicken Sie im Reiter „Users“ auf „Add“/„Add Local User“, geben die Nutzerdaten ein und speichern mit „Save“.



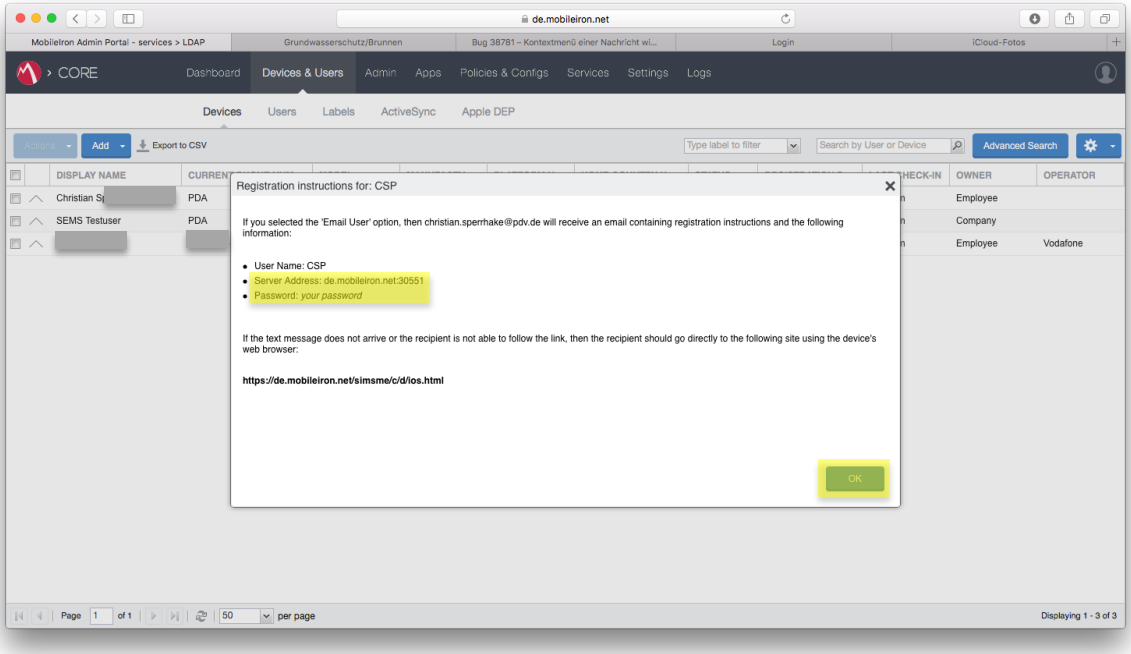
4. Der Nutzer wurde erfolgreich angelegt.



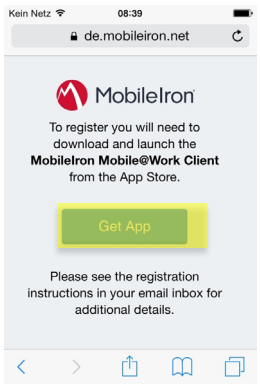
5. Um ein Gerät anzulegen, wechseln Sie zum Reiter „Devices“ und öffnen „Add“/„Single Device“. Wählen Sie in der Maske den gewünschten Nutzer und die Device Platform aus und bestätigen mit „Register“.



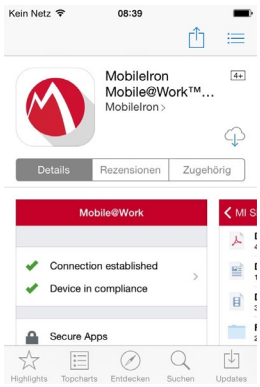
6. Die Zugangsdaten werden angezeigt und an die zuvor angegebene E-Mail-Adresse geschickt.



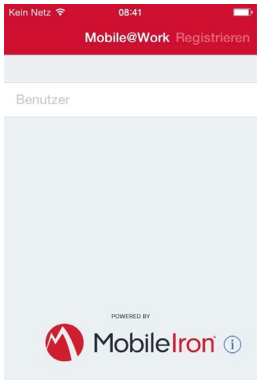
3.2 Auf iOS-Gerät hinzufügen



1. Browser auf iOS-Gerät öffnen, URL aus E-Mail eingeben und mit „Get App“ bestätigen.



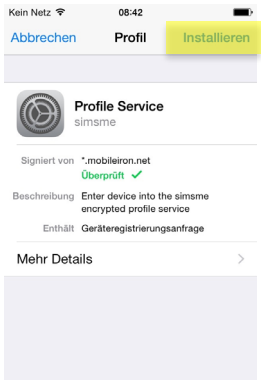
2. App aus App Store installieren.



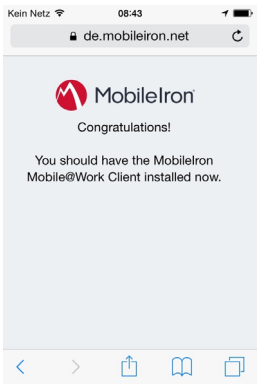
3. Benutzername eingeben.

4. Server und Passwort eingeben.
5. Registrierung bestätigen.

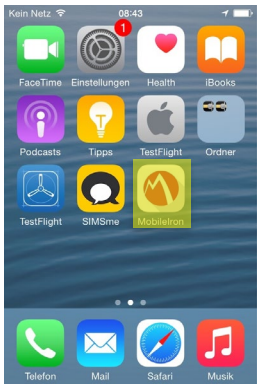
6. Datenschutz durch das Betätigen von „Weiter“ akzeptieren.



7. Profil komplett installieren.



8. Browser wird erneut geöffnet, Erfolgsmeldung wird angezeigt.



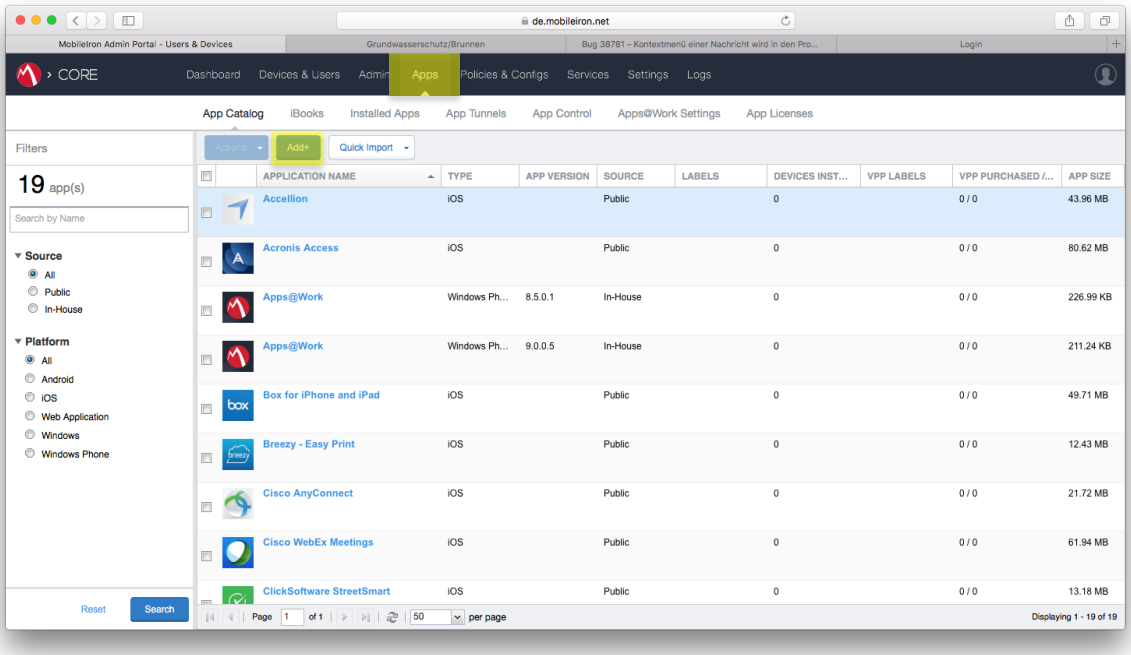
9. MobileIron App ist nach Abschluss der Profilinstallation auf dem iOS-Gerätvorhanden.
10. Über die MobileIron App kann der Verbindungsstatus zum MDM angezeigt werden.

Gerät ist nun in Konsole verfügbar.

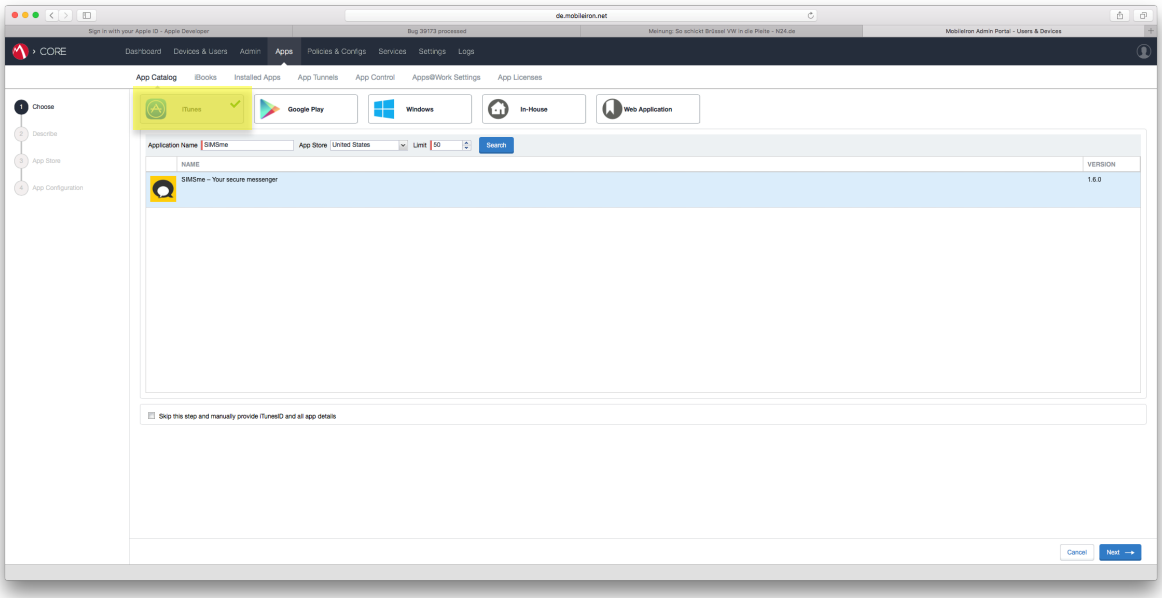
4 Apps mit MobileIron verwalten

4.1 App hinzufügen

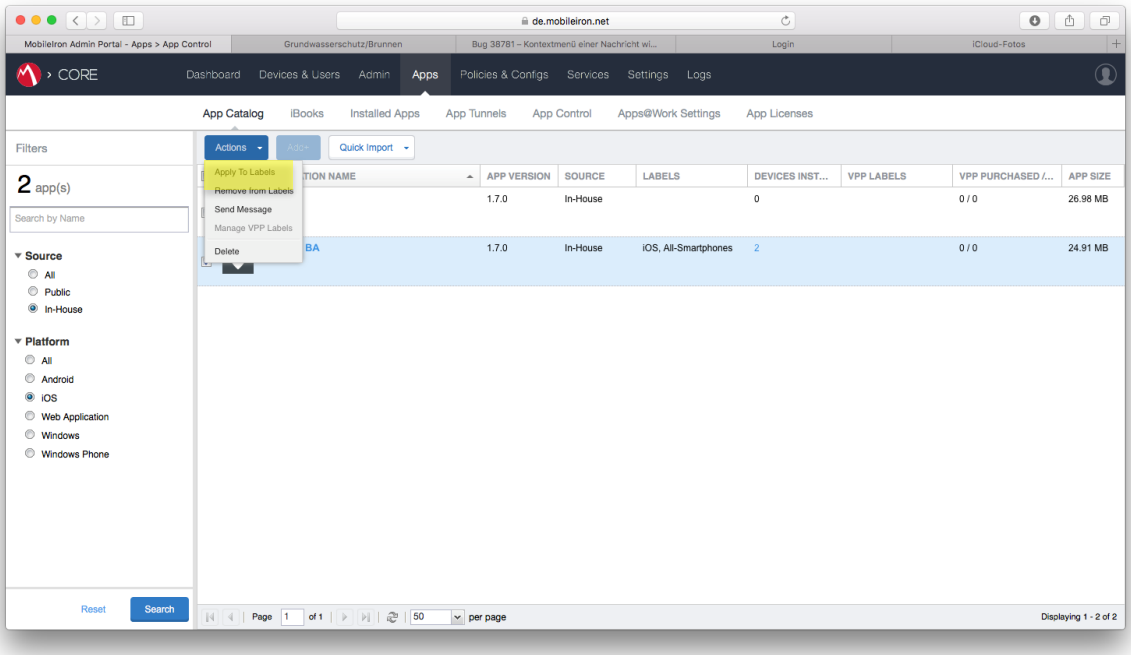
1. Um eine App wie ginlo Business der MobileIron Konsole hinzuzufügen und auf die Geräte der Nutzer zu distribuieren, wählen Sie in der Navigation den Reiter „Apps“ aus und klicken auf „Add“.



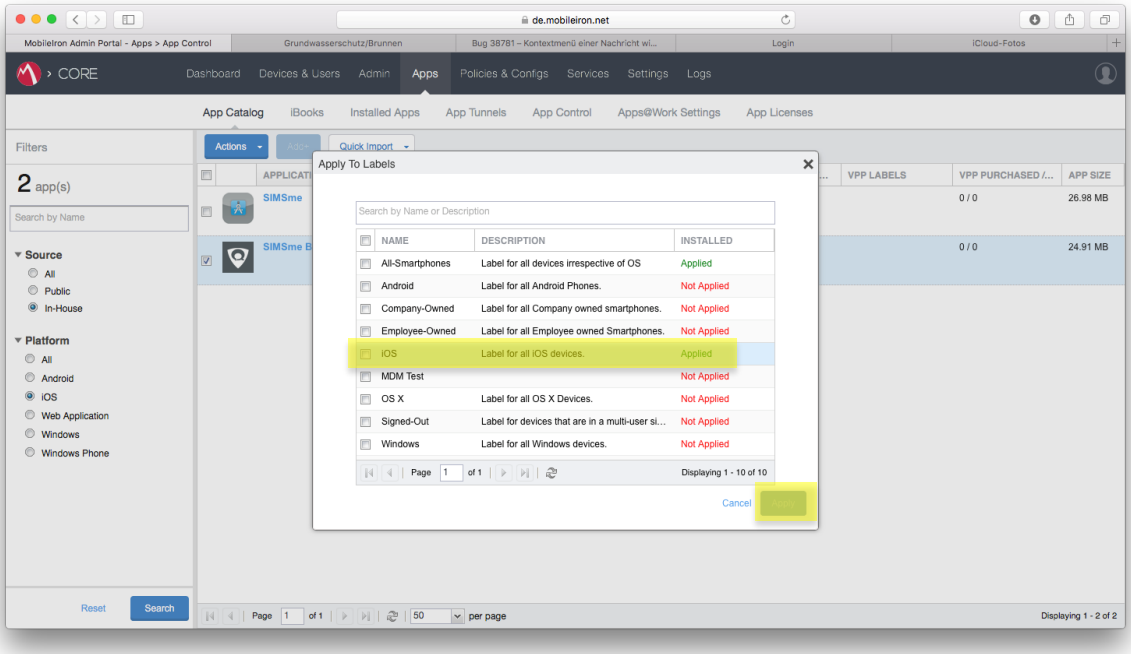
2. Wählen Sie als Quelle „Apple iTunes“ oder bei kundenspezifischen Apps ggf. „In-House“ aus.



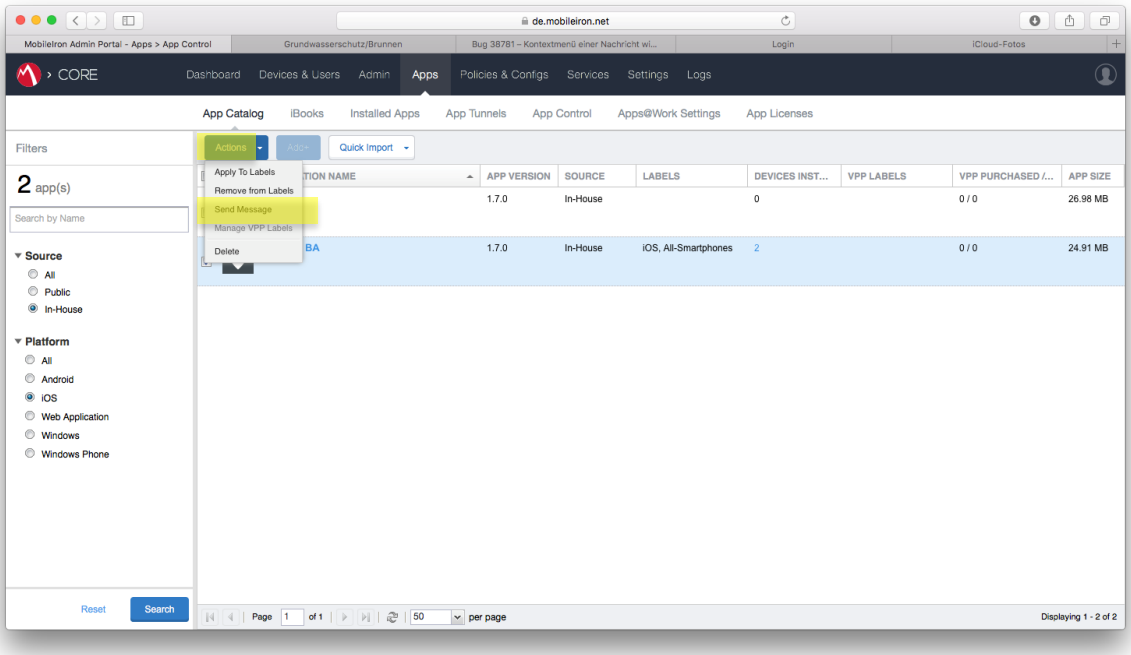
3. Suchen Sie im App-Verzeichnis nach ginlo Business und bestätigen die App. Die Anwendung wird nun unter der Source iTunes im App Catalog angezeigt. Wählen Sie die Anwendung im App Catalog aus und bestätigen unter „Actions“ mit „Apply To Labels“.



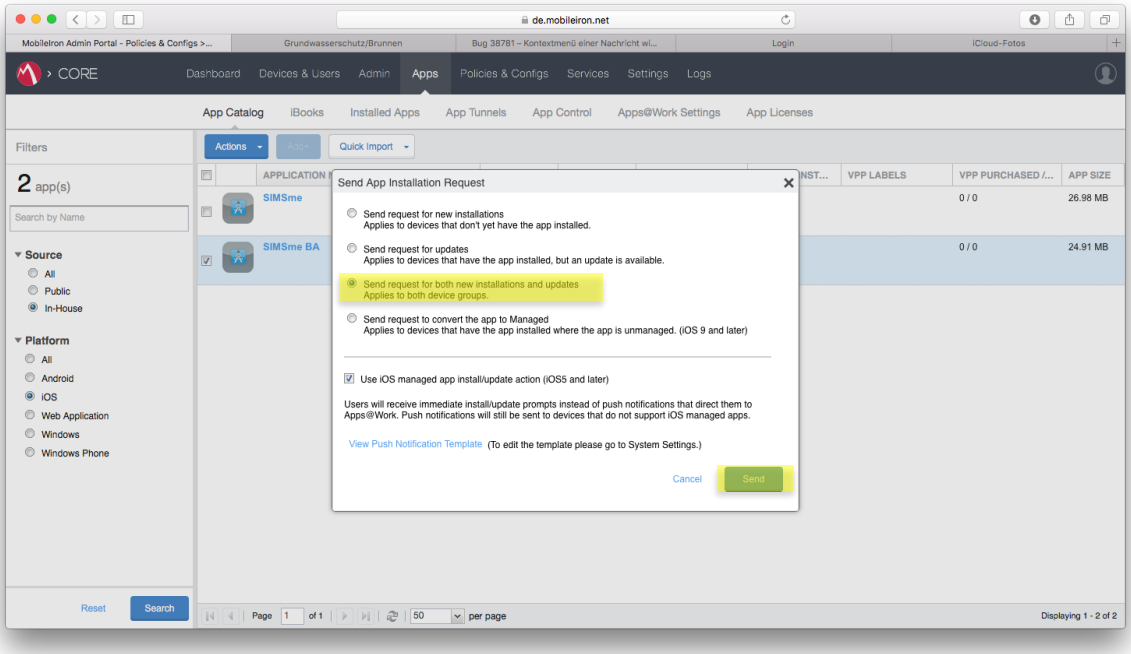
4. Um die Anwendung einem Geräte-Label zuzuweisen, wählen Sie in der Liste z. B. das Label iOS aus und bestätigen mit „Apply“.



5. Um die Anwendung nun an die Nutzer zu distribuieren, wählen Sie die Anwendung im App Catalog aus und wählen unter „Actions“ die Funktion „Send Message“.



6. Vergewissern Sie sich, dass „Send request for both installations and updates“ aktiv ist, und bestätigen Sie mit „Send“.



7. Nach kurzer Zeit wird auf den zugeordneten Geräten eine Push-Nachricht angezeigt, die zur Installation der Anwendung auffordert.

4.2 Update einer App hinzufügen

Für das Hinzufügen einer neuen Version ist der Ablauf derselbe wie für das Hinzufügen einer neuen Anwendung (siehe 4.1). Wenn die App denselben Bundle Identifier und dasselbe Provisioning Profile besitzt, wird sie durch das Senden eines Update Requests an die Geräte verteilt, die dem zugewiesenen Label angehören. Der Upload einer neuen Version ist nur möglich, wenn Versionsnummer und Revisionsnummer höher sind als die der vorhandenen Anwendung.

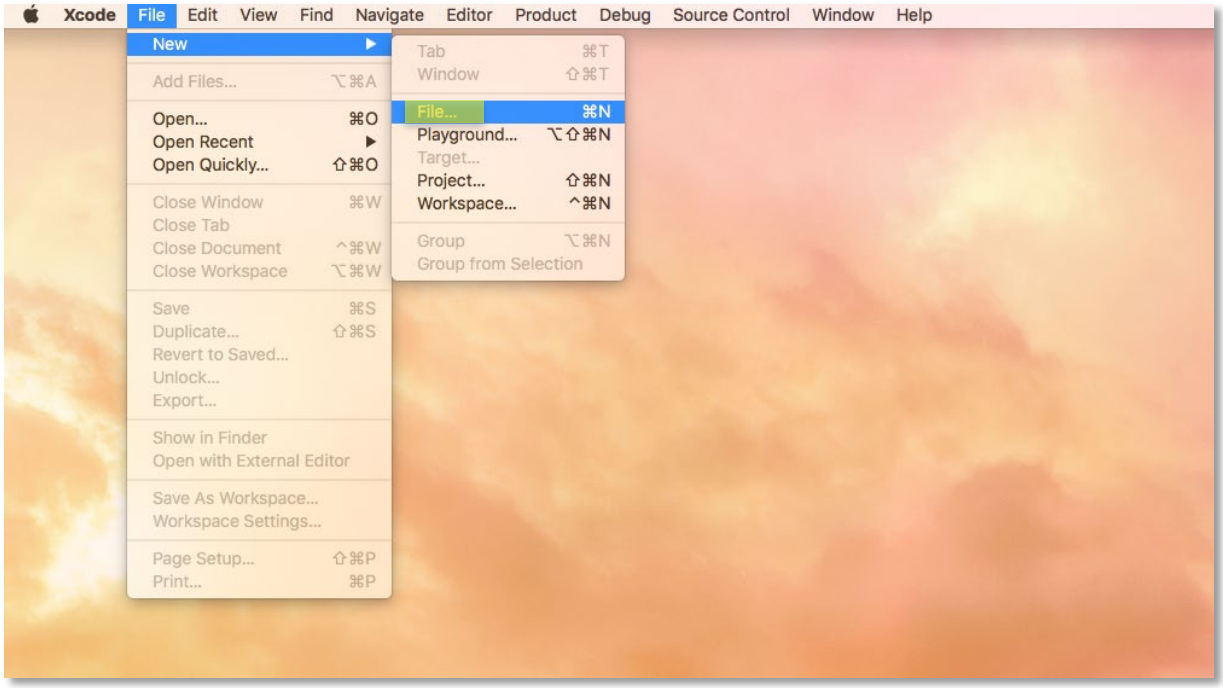
5 Einstellungen der App konfigurieren

Um die mittels AppConfig möglichen Einstellungen der App zu konfigurieren, wird in die MobileIron Konsole die „Plist“ („Property List“) mit der Konfiguration der möglichen ginlo Business Parameter eingespielt.

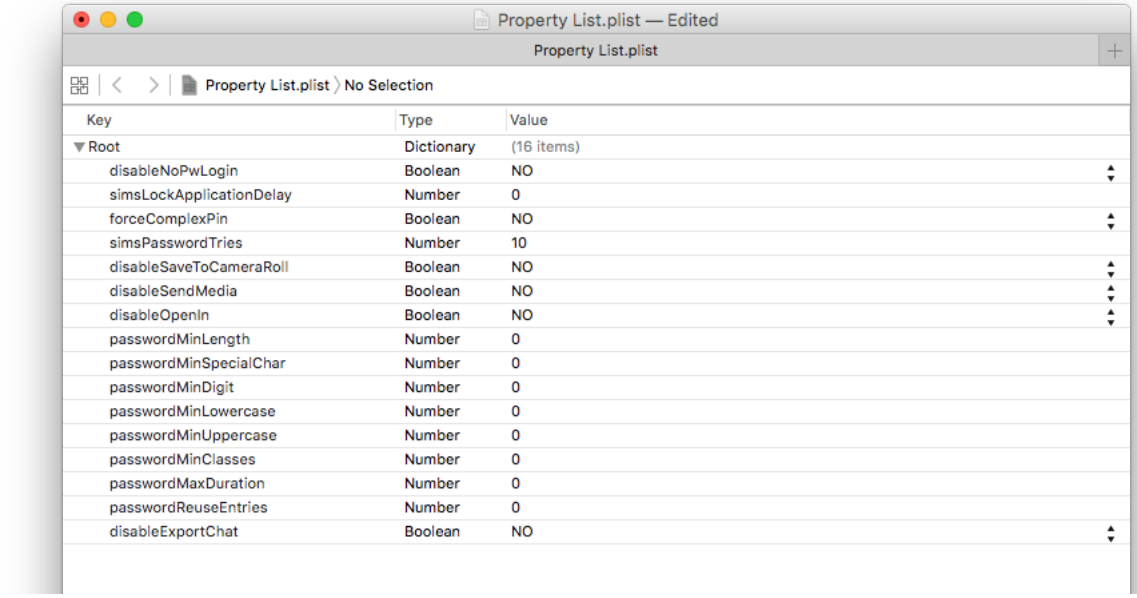
5.1 Einstellungen anlegen

5.1.1 Plist konfigurieren

1. Um die gewünschten Einstellungen in der Plist vorzunehmen, öffnen Sie einen Texteditor zum Bearbeiten der Plist. Im folgenden Screenshot wird die Datei über Xcode auf einem Mac geöffnet unter (File/New/File...). Wählen Sie die Plist unter Ihren lokalen Dateien aus – Sie finden die Vorlage der Plist im Download-Bereich der ginlo Website.

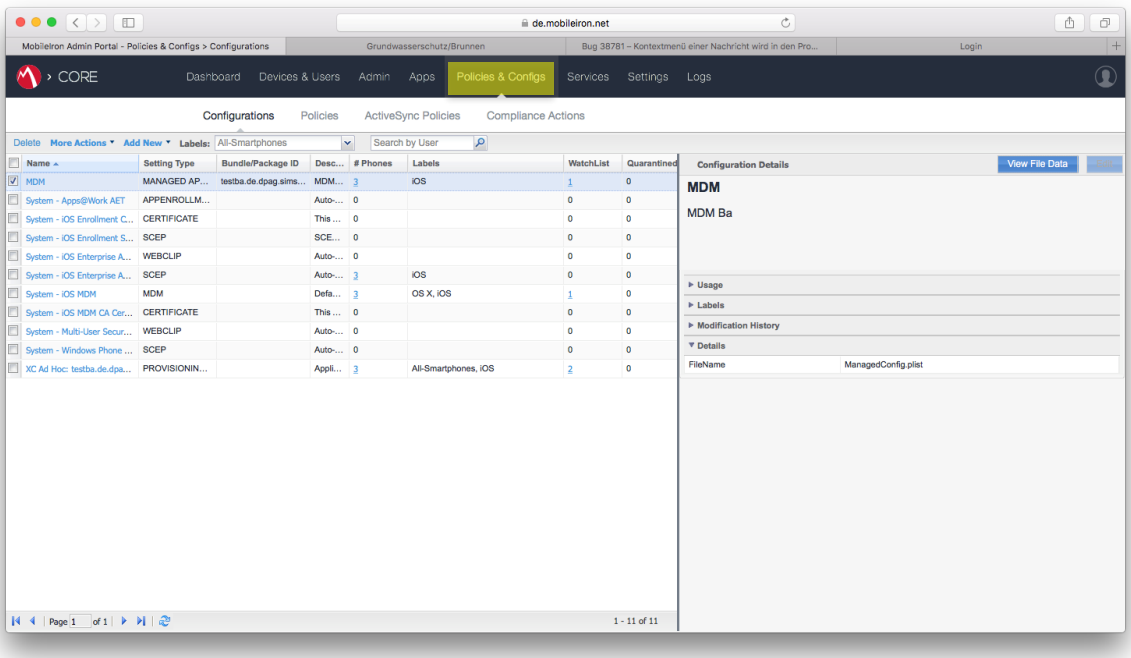


2. Sie können nun Einträge zur Plist mit Key, Type und Value zur Liste hinzufügen und entsprechend Ihrer IT-Security-Vorgaben konfigurieren. Details siehe hierzu finden Sie in der Liste der möglichen Parameter in Kapitel 5.2.

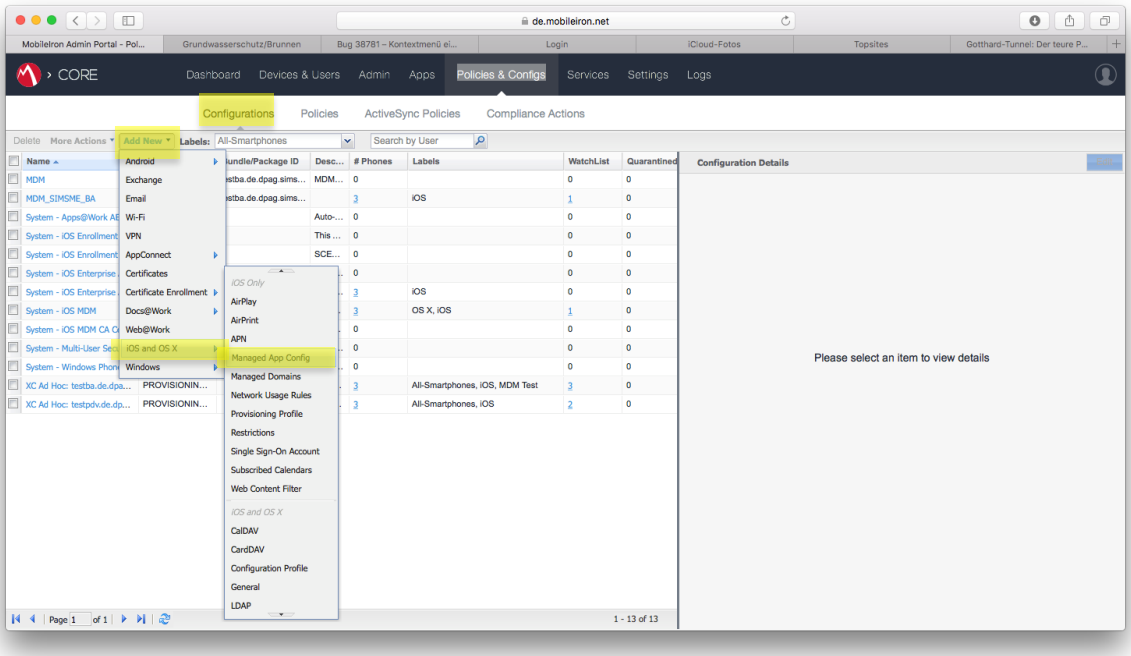


5.1.2 Einstellungen unter MobileIron einspielen

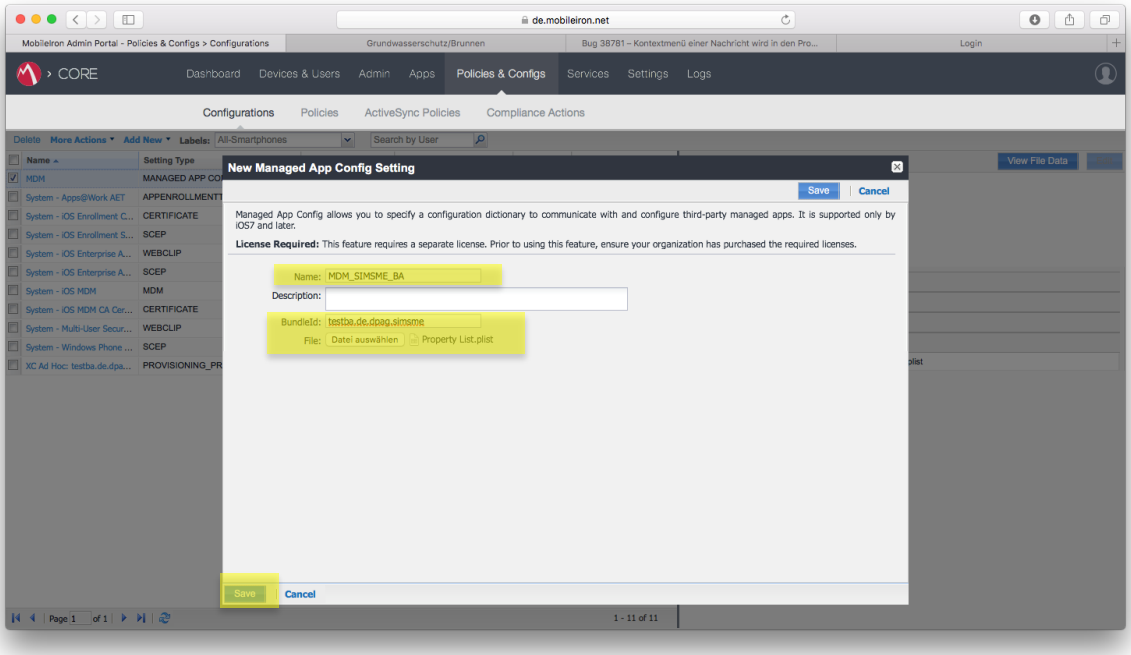
1. Um die über die Plist gesetzte Konfiguration in MobileIron einzuspielen und wirksam auf die App anzuwenden, öffnen Sie den Reiter „Policies & Configs“.



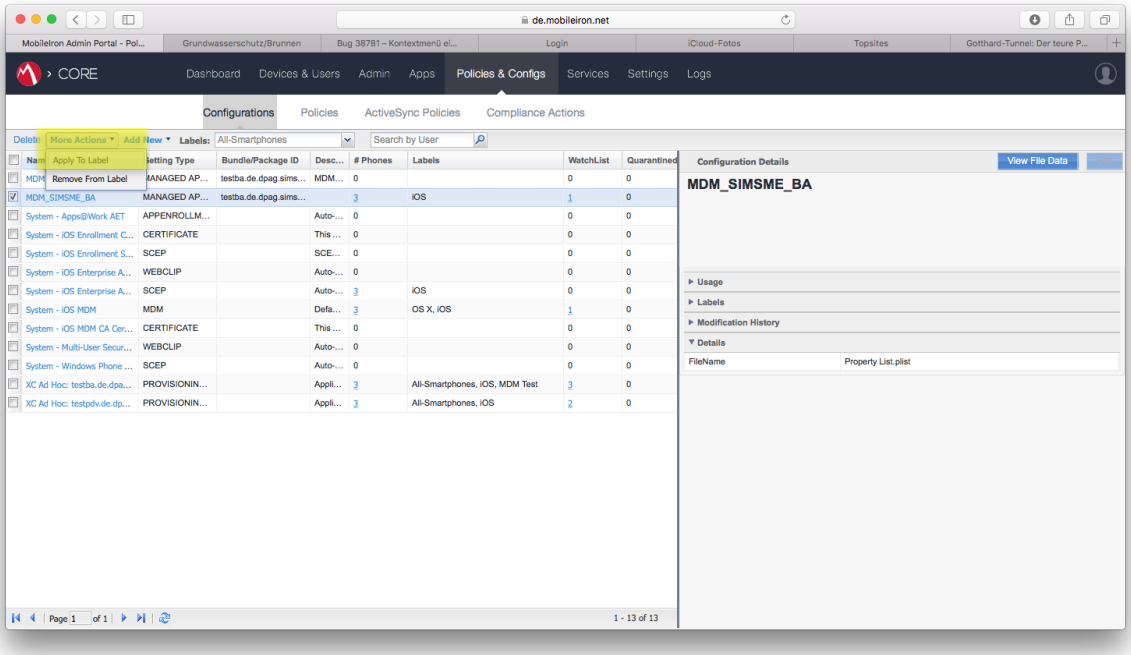
2. Wählen Sie im Reiter „Configurations“ den Button „Add New“. Wählen Sie im geöffneten Drop-down-Menü „iOS and OS X“ und dann „Managed App Config“.



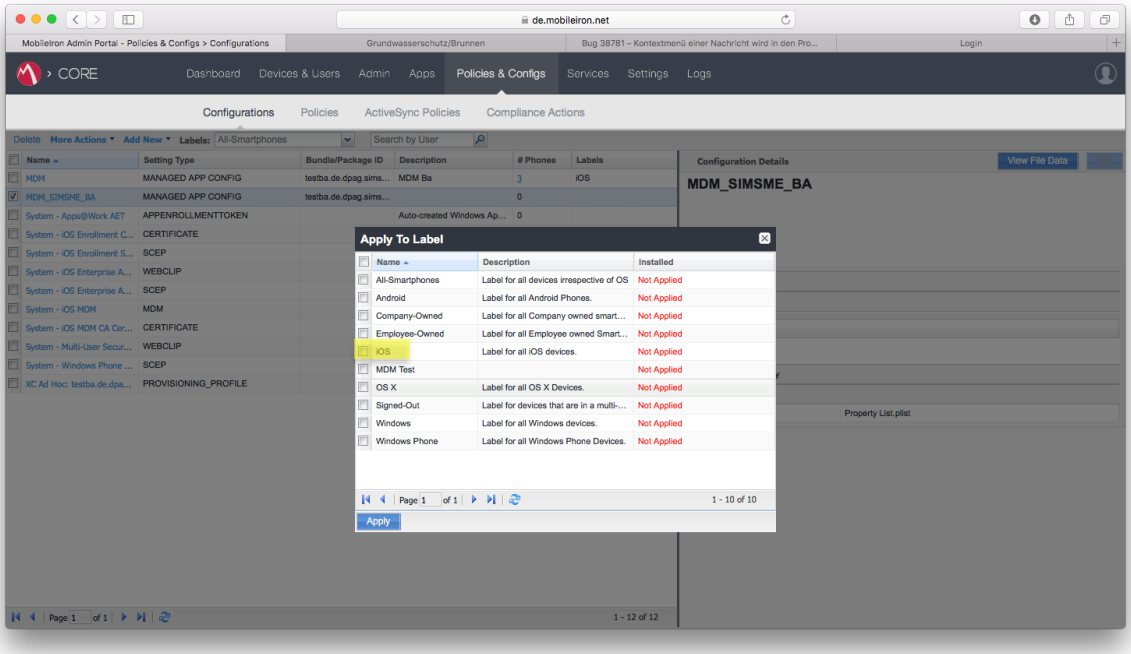
3. Tragen Sie im Fenster „New Managed App Config Setting“ einen Namen ein, z. B. MDM_ginlo, sowie die Bundle-ID und den Speicherort der Plist. Bestätigen Sie mit „Save“.



4. Wählen Sie die neu angelegte Konfiguration aus, klicken auf „More Actions“ und wählen im geöffneten Drop-down-Menü „Apply To Label“ aus.



5. Weisen Sie in der Liste die neu angelegte Konfiguration einem Label zu, z. B. iOS, und bestätigen Sie mit „Apply“. Die Konfiguration ist dann für das Label und die App wirksam und wird App-seitig entsprechend im User Interface und den Funktionen umgesetzt.



5.2 Liste der möglichen Parameter

Anf.	Key	Typ	Wertebereich	Beschreibung
1	disableNoPwLogin	Boolean	true/false	Toggle „Passwort beim Start abfragen“ fällt weg und ist implizit auf true gesetzt. Eventuelle Keychain-Einträge werden entfernt. Siehe Anmerkung 2)
2	simsLockApplicationDelay	Integer	0-10	Die Einstellung wird 1:1 in die Einstellungen übernommen. Einstellung „Passwort abfragen nach...“ entfällt.
3	forceComplexPin	Boolean	true/false	Der Toggle „Einfacher Code“ entfällt. Siehe auch Anmerkung 3)
4	simsPasswordTries	Integer	3,5,10	Wenn gesetzt, entfällt die Einstellung „Daten löschen“.
5	disableSaveToCameraRoll	Boolean	true/false	Wenn gesetzt, entfällt die Einstellung „Medien sichern“
6	disableSendMedia	Boolean	true/false	Wenn gesetzt, können nur noch Texte geschrieben werden.
7	disableOpenIn	Boolean	true/false	Wenn gesetzt, können Bilder und Videos nicht mehr gespeichert werden, und Dateien können nicht mehr angezeigt werden.
8	passwordMinLength	Integer	0-99	Siehe Anmerkung 3)
9	passwordMinSpecialChar	Integer	0-99	Siehe Anmerkung 3)
10	passwordMinDigit	Integer	0-99	Siehe Anmerkung 3)
11	passwordMinLowercase	Integer	0-99	Siehe Anmerkung 3)
12	passwordMinUppercase	Integer	0-99	Siehe Anmerkung 3)
13	passwordMinClasses	Integer	0-4	Siehe Anmerkung 3)
14	passwordMaxDuration	Integer	0-65535	Siehe Anmerkung 4)
15	passwordReuseEntries	Integer	0-100	Siehe Anmerkung 5)
16	disableExportChat	Boolean	true/false	Wenn gesetzt, können Chats nicht mehr in eine Textdatei exportiert werden.

Anmerkung 1) Einfache Einstellungen werden in den NSUserDefaults gespeichert. Wenn sich die MDM-Konfiguration hierfür ändert, dann werden die Einstellungen in die NSUserDefaults übernommen.

Anmerkung 2) Wenn „TouchId“ oder „Start ohne Passwort“ deaktiviert wird, dann werden zusätzlich die entsprechenden Schlüssel in der KeyChain gelöscht.

Anmerkung 3) Wenn sich die Konfiguration bezüglich der Passwörter geändert hat, wird zunächst das Passwort abgefragt. Dies erfolgt unabhängig davon, ob das Passwort beim Start immer abgefragt wird. Dies ist erforderlich, weil wir die Passwörter nur indirekt speichern und einem Angreifer keine Informationen über das Passwort bereitstellen wollen. Das alte Passwort wird dann gegen die Passwort-Policies geprüft. Entspricht es nicht mehr den Passwort-Policies, dann wird der Nutzer gezwungen, sein Passwort zu ändern. Dabei wird natürlich auch geprüft, ob das Passwort den Policies entspricht.

Anmerkung 4) Beim Ändern des Passworts wird anhand des aktuellen Datums und der MaxDuration berechnet, wann das Passwort abläuft. Aus Performance-Gründen wird zunächst das Datum des Geräts genommen. Ändert sich die Einstellung, wird das neue Fälligkeitsdatum berechnet.

Anmerkung 5) Um dieses Feature zu realisieren, ist es notwendig, die Passwörter sicher auf dem Gerät zu hashen. Dazu wird das Passwort zunächst per Bcrypt mit einer festen Anzahl Runden gehasht. Die gehashten Passwörter werden nicht direkt gespeichert, sondern per AES-Schlüssel verschlüsselt. Der AES-Schlüssel selbst ist mit dem RSA-Schlüssel des Gerätes verschlüsselt.

Sollten Sie Fragen zu dem dokumentierten Vorgehen oder den möglichen Parametern haben, wenden Sie sich gerne an unseren Support unter b2b-support@ginlo.net