MATRIX42
SMARTER WORKSPACE – BETTER LIFE

Matrix42 Silverback

Quick Start Guide for iOS

Version 2.0e

July 27, 2015

Copyright © 2000 - 2015 Matrix42 AG

This documentation is copyright protected. All rights are reserved by Matrix42 AG.

Any other use, in particular the disclosure to third parties, storage in a data system, dissemination, processing, presentation, performance and demonstration are prohibited. This applies to the entire document, as well as parts thereof.

Subject to change. Reprint, also in excerpts, is permitted only with the written consent of Matrix42 AG.

The software described in this document is subject to a permanent development due to which there may be differences in the documentation and the actual software. This documentation is not entitled to the actual functionality of the software.

Apple and **Mac OS X** are registered trademarks of Apple Inc.
Citrix® software or **Citrix® server** are Trademarks and Registered Trademarks of Citrix Systems, Inc. in the United States and other countries.
cygwin is copyrighted by Red Hat Inc. 1996-2003.
expat is copyrighted by Thai Open Source Software Center Ltd.
gSOAP is copyrighted by Robert A. van Engelen, Genivia, Inc. All rights reserved.
Iconv is copyrighted by 1999-2003 Free Software Foundation, Inc.
Iperf is copyrighted by the University of Illinois, except for the gnu_getopt.c, gnu_getopt_long.c, gnu_getopt.h files, and inet_aton.c, which are under the GNU General Public License.
Libmspack (C) 2003-2004 by Stuart Caie <kyzer@4u.net>.
OpenSSL This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit.
PuTTY is copyrighted by Simon Tatham. Portions copyright Robert de Bath, Joris van Rantwijk, Delian Delchev, Andreas Schultz, Jeroen Massar, Wez Furlong, Nicolas Barry, Justin Bradford, Ben Harris, Malcolm Smith, Ahmad Khalifa, Markus Kuhn, and CORE SDI S.A.
RSA Data Security, Inc. MD5 Message-Digest Algorithm is copyrighted by RSA Data Security Inc. Created 1991. All rights reserved.
rsync is an open source utility that provides fast incremental file transfer. rsync is freely available under the GNU General Public License version 2.
runcontrol The Initial Developer of the Original Code is James Clark. Portions created by James Clark are Copyright (c) 1998 James Clark. All rights reserved.
SNMP++ Copyright (c) 1996 Hewlett-Packard Company.
VMware, the **VMware "boxes" logo and design, Virtual SMP, VMotion vSphere, vSphere Hypervisor (ESXi), ESX, View, ThinApp, vCenter** and **vCloud** are registered trademarks or trademarks of VMware, Inc. in the United States and/or other jurisdictions.
Windows, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows 8, and **Windows Server 2012** are registered trademarks of Microsoft Corporation.

Others, at this point not explicitly listed, company, brand and product names are trademarks or registered trademarks of their respective owners and are subject to trademark protection.

Table of Content

1. Quick Start Guide for Apple iOS 4
1.1. Requirements 4
1.1.1. Matrix42 Account 4
1.1.2. Server name of your Silverback server 4
1.1.3. Administrator login credentials 4
1.2. Login into the Silverback Admin Console 5
1.2.1. Check your language is English 5
1.2.2. Change your admin console password 5
1.3. Create iOS APNS certificate 6
1.3.1. APNS Best Practices & Important Notes 6
1.3.2. Create 'Complete CSR' Request 7
1.3.3. Download the CSR request for Apple 8
1.3.4. Login to Apple Push Certificate Center 8
1.3.5. Upload and close CSR request in 9
1.4. Create a local user 10
1.5. Enrollment Process 11
1.5.1. Enrollment with SMS 11
1.5.2. Enrollment without SMS 13
1.6. Display Device Details 15
1.7. Managed Device Actions 16
1.7.1. Clear Passcode 16
1.7.2. Manually Block / Unblock Devices 17
1.8. Using Tags for Profile, Apps & Policies 18
1.8.1. Create a Passcode Profile 18
1.8.2. Create a Exchange ActiveSync (EAS) Profile 20
1.9. Deploy Apps 22
1.9.1. Add Public App Store Apps to Silverback App Portal 22
1.9.2. Add Internal Enterprise Apps to Silverback App Portal 24
1.9.3. Assign App to Tag 25
1.9.4. Using iOS App Portal to Download Apps 27
2. Appendix 28
2.1. From Cloud to On-Premises Migration 28
2.2. Internal App PLIST file 28
2.3. M42 Silverback System Variables 30

1. Quick Start Guide for Apple iOS

The goal of this guide is to provide a short way to get an iOS device enrolled and do basic mobile device management actions.

1.1. Requirements

1.1.1. Matrix42 Account

A Matrix42 Account is needed for different purposes. For example it will be used to create an Apple iOS APNS certificate. Please do the following steps:

- Open a web browser and go to https://accounts.matrix42.com
- Register with your company email address
- If you are the first employee of your company who is registering for an Matrix42 account, please checkmark '*Create company account*'. In case you do not know if you are the first one, simply checkmark '*Create company account*'. If you get an error message that the company account already exists you simply uncheck '*Create a company account'*.

Please store Matrix42 credentials safely. You will need it in the future for various and important tasks.

1.1.2. Server name of your Silverback server

You will receive the name of your Silverback server. This server URL is required for the following:

- Log into the Silverback admin console to manage your devices.

Open https://<SilverbackServer>/admin to login.

- Log into the Silverback self-service portal (SSP) for end-users to enrol devices.

Open https://SilverbackServer> in your browser and you will be automatically be forwarded to https://<SilverbackServer>/ssp .

1.1.3. Administrator login credentials

You will receive your login credentials during the Matrix42 Silverback registration process.

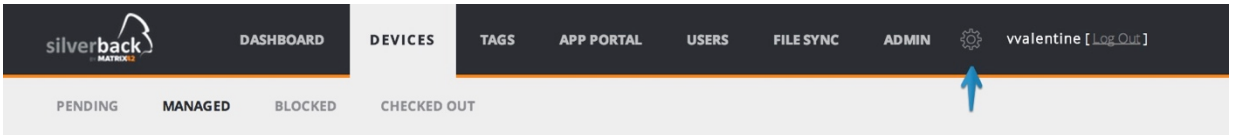
1.2. Login into the Silverback Admin Console

Please login into the Silverback admin console by opening the console login URL https://<SilverbackServer>/admin in your browser.

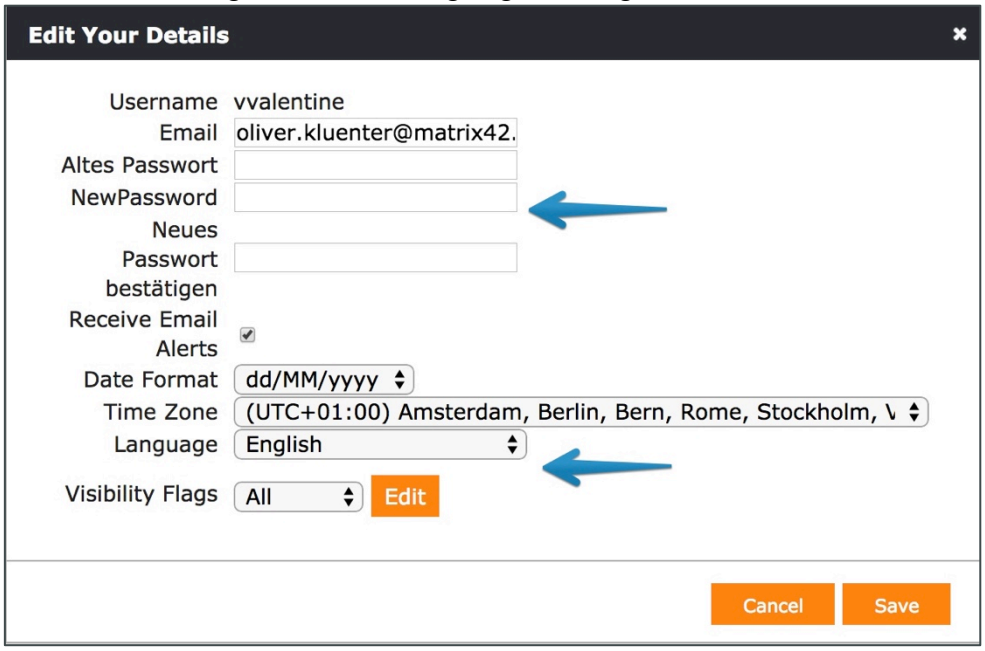
1.2.1. Check your language is English

By default the solution detects your browser language and automatically switches the console language. Matrix42 is currently translating it's Silverback solution into German. We are not fully finished yet so we suggest you fix your language to English. Matrix42 plans to have a full translated version with the upcoming release 4.7 in January, 2015.

Please click on the **'Settings'-icon** on the top right.



You can now change or fix the language to English.



1.2.2. Change your admin console password

Please change your default admin console password in the same admin settings menu as above.

1.3. Create iOS APNS certificate

Apple requires a company individual APNS certificate to enrol and manage iOS devices. The certificate is valid for one year. According to Apple this certificate must re-newed before the expiration of the certificate otherwise you must re-enrol all devices again.

Make sure you meet the following prerequisites **before** you start the APNS creation process:

1 Matrix42 Account

This step is already described above.

2 Apple ID

The Apple ID is mandatory by Apple to create and renew your company APNS certificate. Please ensure that you successfully logged into the Apple Push Certificates Port before you start with the APNS generate process.

For trials you can use your personal Apple ID. For production environments we strongly suggest to follow the '*APNS Best Practices & Important Notes*' below.

1.3.1. APNS Best Practices & Important Notes

For production purposes Matrix42 strongly advises to **use a non-personalised company Apple ID** that still exists if an employee leaves the company.

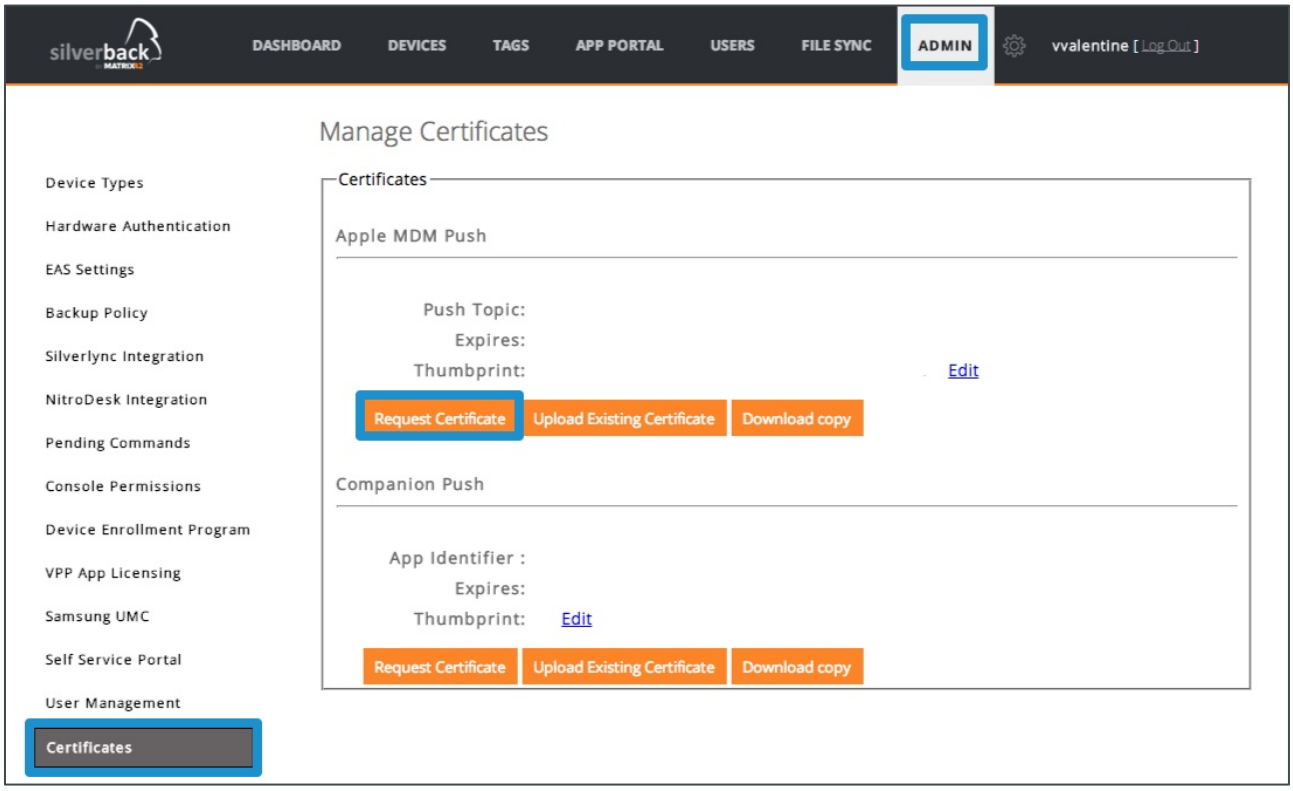
Furthermore Matrix42 strongly recommends **linking a company group email address** to that Apple ID during the creation process so that all email group members receive important Apple emails like APNS certificate expiration notifications.

Additionally **note down the Apple ID** you use during the APNS certificate creation process. The APNS will expire in 12 months and needs to be renewed. For renewing you must use the Apple ID otherwise all your iOS devices get out of MDM management control.

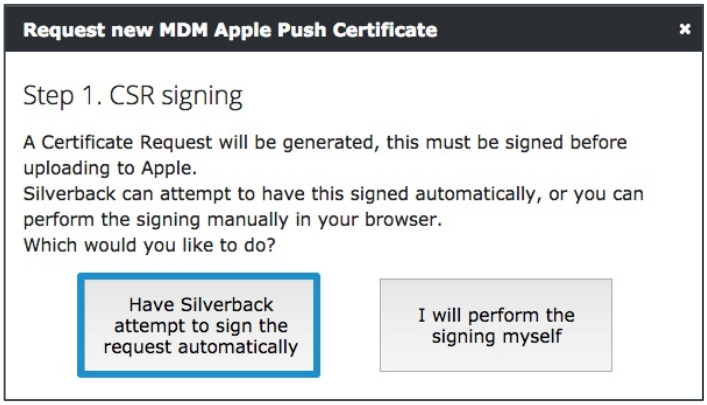
For renewing the APNS you must **extend the initial certificate entry** in the Apple Push Certificates Portal.

1.3.2. Create 'Complete CSR' Request

Select the 'Admin' tab and select 'Certificates' on the left side. In the 'Apple MDM Push' area select *'Request Certificate'*.



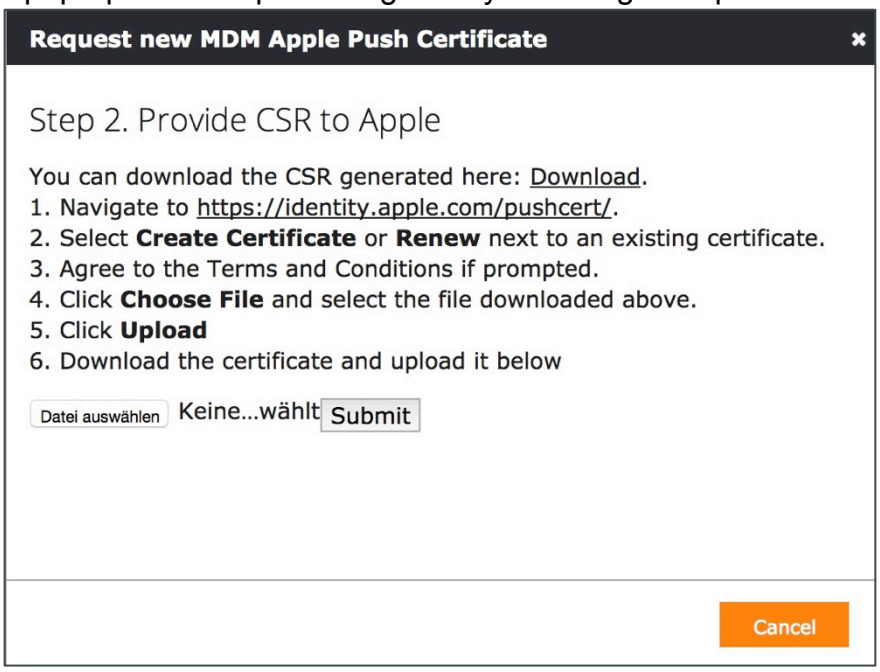
In the next pop-up you are asked to define who is signing the initial APNS CSR request for the Apple Push Certificates Portal. Please select '*Have Silverback attempt to sign the request automatically*'.



Quick Start Guide for iOS

If you are not logged into your Matrix42 Account you will get a pop-up. You can now log into your Matrix42 Account.

Now a pop-up screen open and guides you through the process.



1.3.3. Download the CSR request for Apple

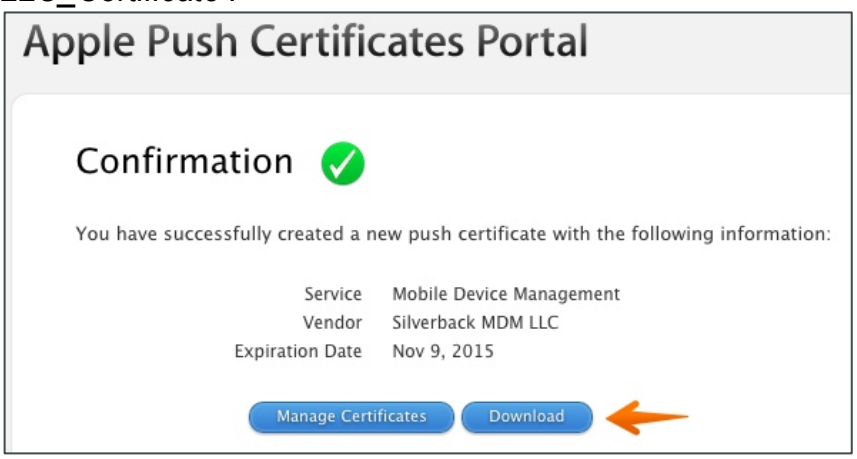
Click on 'Download' in the top area to download the CSR request. You will receive a file called *Mdm_certificateRequest.txt*.

1.3.4. Login to Apple Push Certificate Center

Click on the corresponding link in the pop-up and go to https://identity.apple.com/pushcert/ . You will now require your company Apple ID. One logged in do the following:

- In the main menu click on *Create a Certificate*.
- Agree to the terms and conditions.

- When entering notes for the APNS certificates only use letters and spaces.
- Click Choose file and upload your Mdm_certificateRequest.txt.
- Click the *Upload* button.
- Click the *Download* button – you receive a *pem* file called '*MDM_ Silverback MDM LLC_Certificate*'.

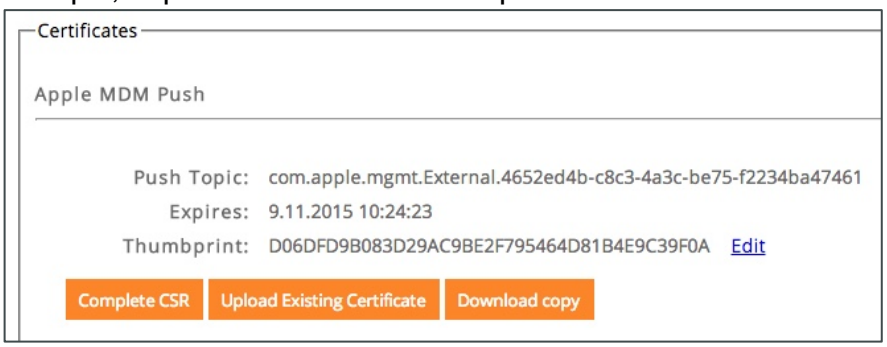


1.3.5. Upload and close CSR request in

Switch back to the Silverback admin console and do the following:

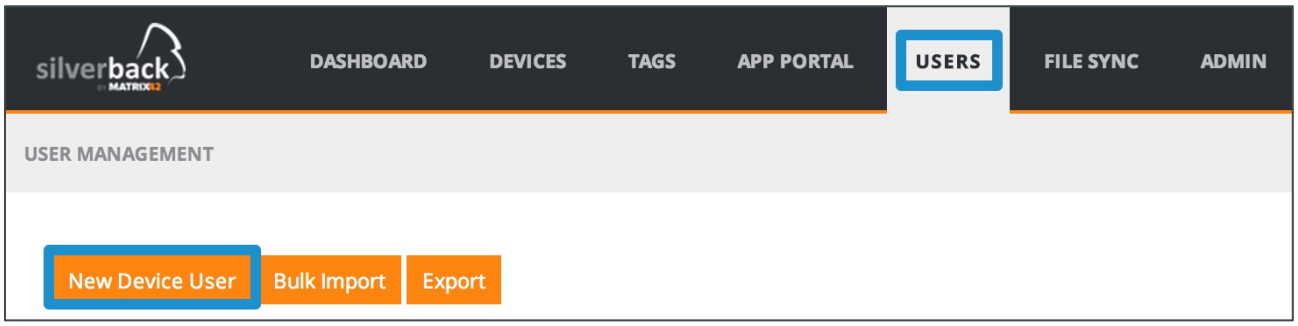
- Click on *Select a file*.
- Choose and upload the PEM file you received from Apple Push Certificates Portal.
- Click on Submit to finish the process.

In the MDM console you should now see the new Apple MDM Push (APNS) certificate with its push topic, expiration date and thumbprint.

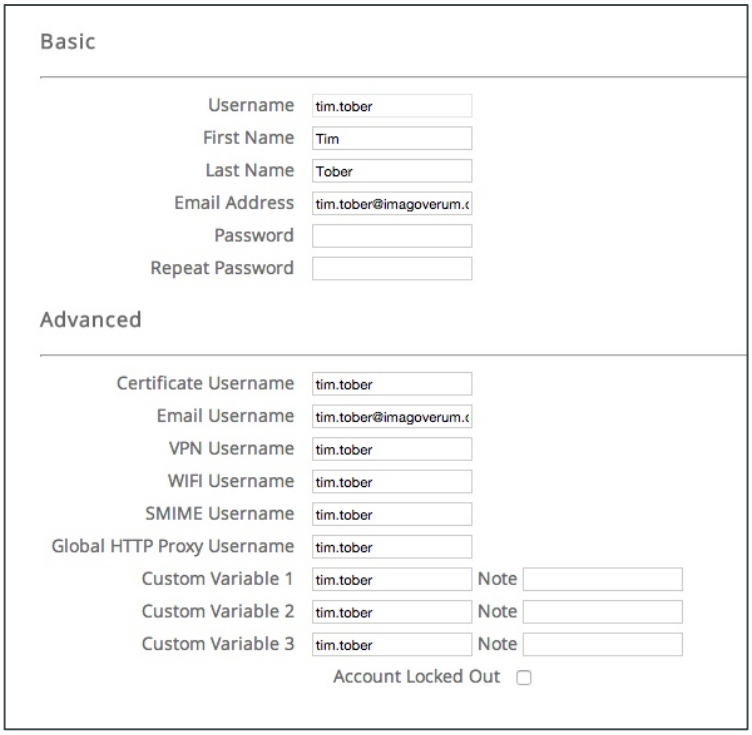


1.4. Create a local user

For the quick start we will user so called local users which you create manually in the Silverback admin console. Please note that if decide to buy or Silverback by Matrix42 Cloud service you will be able to securely connect your LDAP / Active Directory using the M42 Cloud Connector.



In the Silverback admin console choose 'USERS' tab and click on *New Device User*. You can fill out the form.



The basic settings cover the user's main settings. When entering the *Username*, the advanced user fields below will get pre-filled out automatically. You can individually change the advanced user fields if required.

The advanced user fields can be used later on as lookup fields to automatically deploy user specific information into an MDM profile, e.g. when creating an email profile.

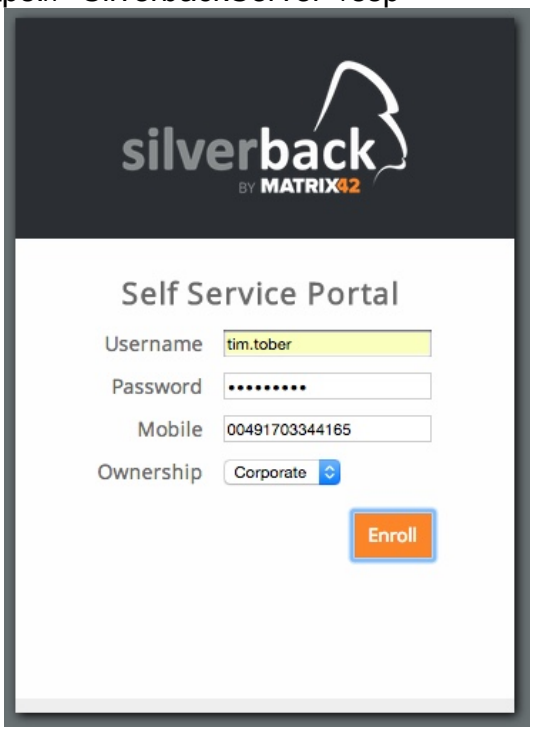
When completed click on *Save*.

1.5. Enrollment Process

1.5.1. Enrollment with SMS

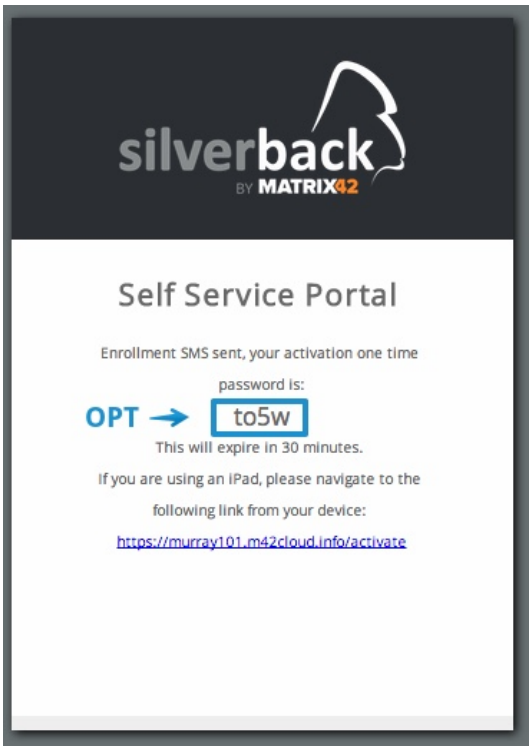
To get your iOS device enrolled please do the following steps:

- Open a web browser on your **desktop**.
- Open a new browser tab and enter the Silverback Self-Service Portal (**SSP**) address https://<SilverbackServer>/ssp

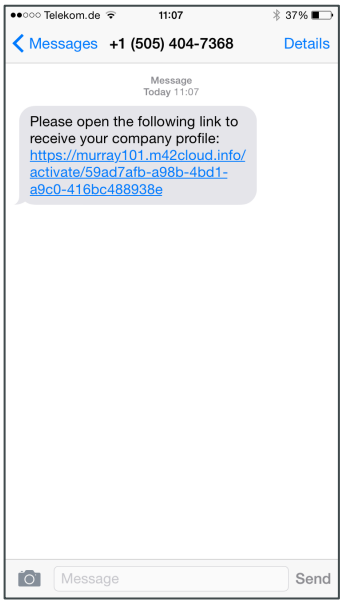


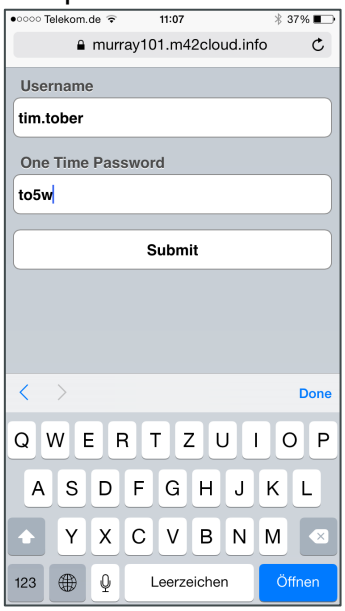
- Enter your name & password. If your device can receive SMS you enter your mobile number like in the following example:
  - *004917047119876*
  - *+4917047119876*
- Afterwards you select the *Ownership* for this device.
- When clicking on *Enroll* a new webpage in your desktop browser will open.

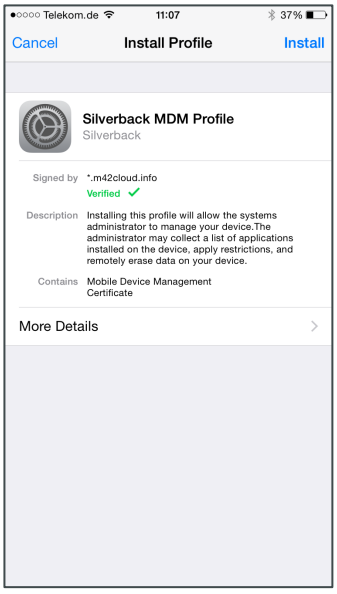
Quick Start Guide for iOS



- Once you receive the SMS on your device you simply click on the URL link.
- The Safari browser open, and you type in the One Password Token (**OTP**)
  Please enter your **One Time Password (OTP)** for the device.
  Note: The OTP is valid for one single try – so enter correctly first time. Otherwise you need to re-start from the beginning and open a new browser tab and enter the Silverback Self-Service Portal (**SSP**) address https://<SilverbackServer>/ssp
- Follow the iOS MDM enrollment process and '**trust**' when asked.

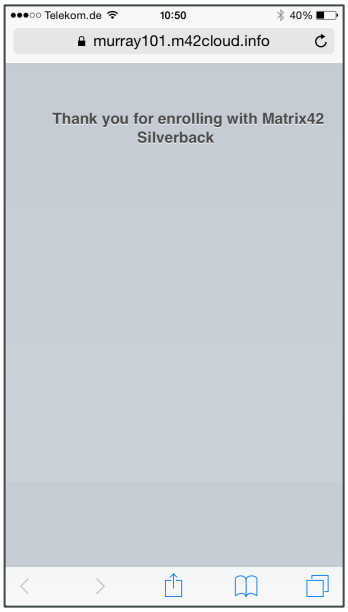


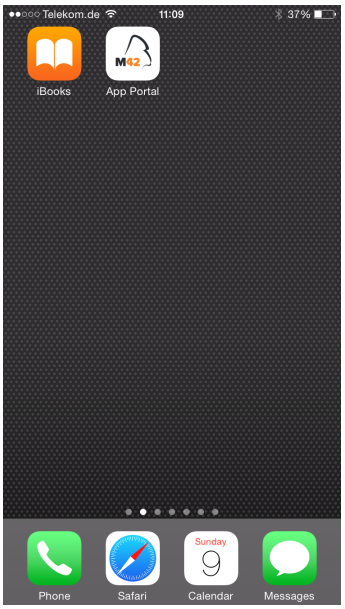




- After iOS MDM enrollment you should see automatically Safari browser success note.
- Press the home button. Within 60 to 90 seconds you should see the M42 Silverback App Port icon on your homescreen.

Quick Start Guide for iOS



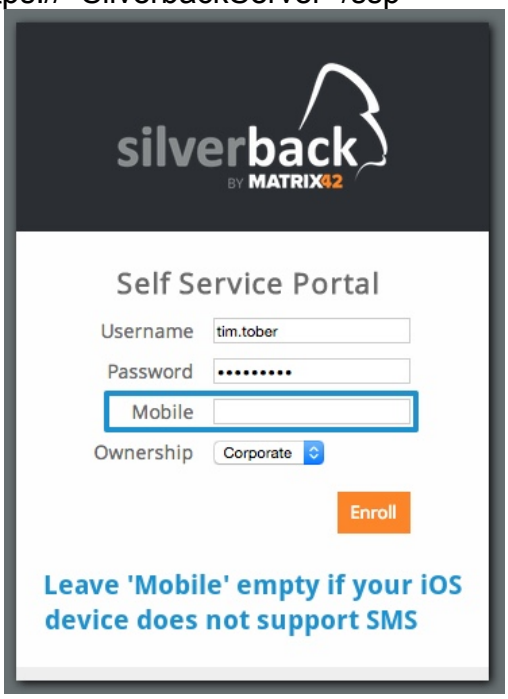


Once you see the App Portal icons your device is under Matrix42 Silverback management and you know that the MDM APNS process is working.

1.5.2. Enrollment without SMS

Even though a lot of iPad user have an iPhone and can receive SMS on their iPad with iOS 8.1, you can enroll the device without an SMS. The process is close to be same:

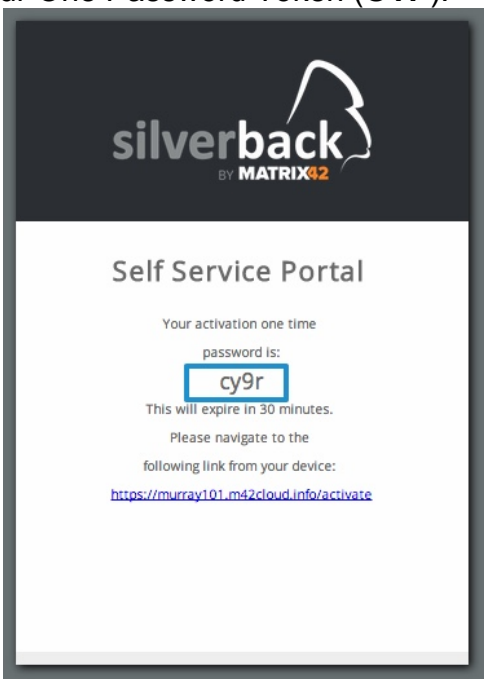
- Open a web browser on your **desktop**.
- Open a new browser tab and enter the Silverback Self-Service Portal (**SSP**) address https://<SilverbackServer>/ssp



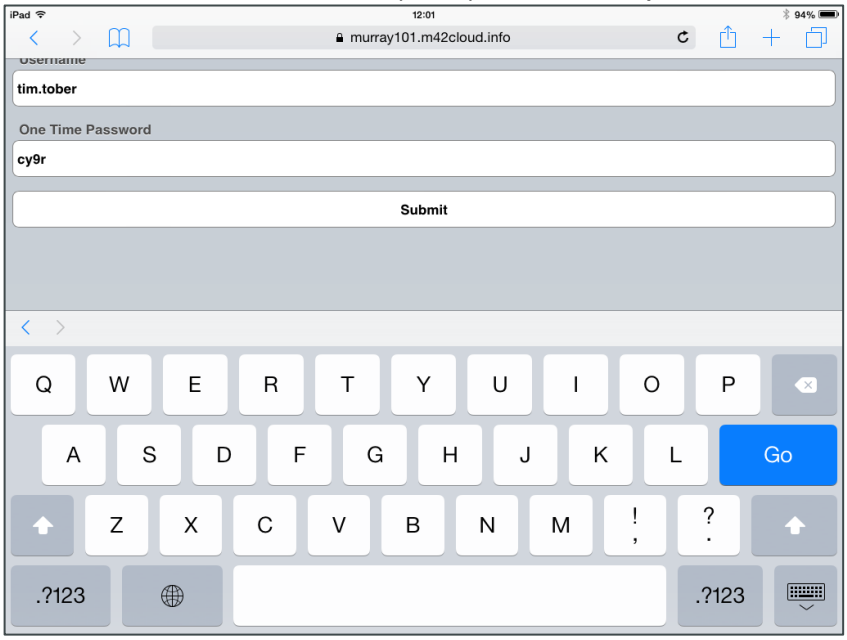
- Enter your name & password and leave the ‘Mobile’ field empty if your device cannot receive an SMS.
- Afterwards you select the *Ownership* for this device.

Quick Start Guide for iOS

- When clicking on *Enroll* a new webpage in your desktop browser will open and show up your One Password Token (**OTP**).



- Switch to your iPad and open the following URL in the Safari browser https://<SilverbackServer>/**activate**.
- Enter again your username and the One Password Token (**OTP**).
  Note: The OTP is valid for one single try – so enter correctly first time. Otherwise you need to re-start from the beginning and open a new browser tab and enter the Silverback Self-Service Portal (**SSP**) address https://<SilverbackServer>/ssp



- **Hint:** Press on the left side in the username and OTP field in case the Safari does not take your action first time.
- Follow the iOS MDM enrollment process and '**trust**' when asked.
- After iOS MDM enrollment you should see automatically Safari browser success note.

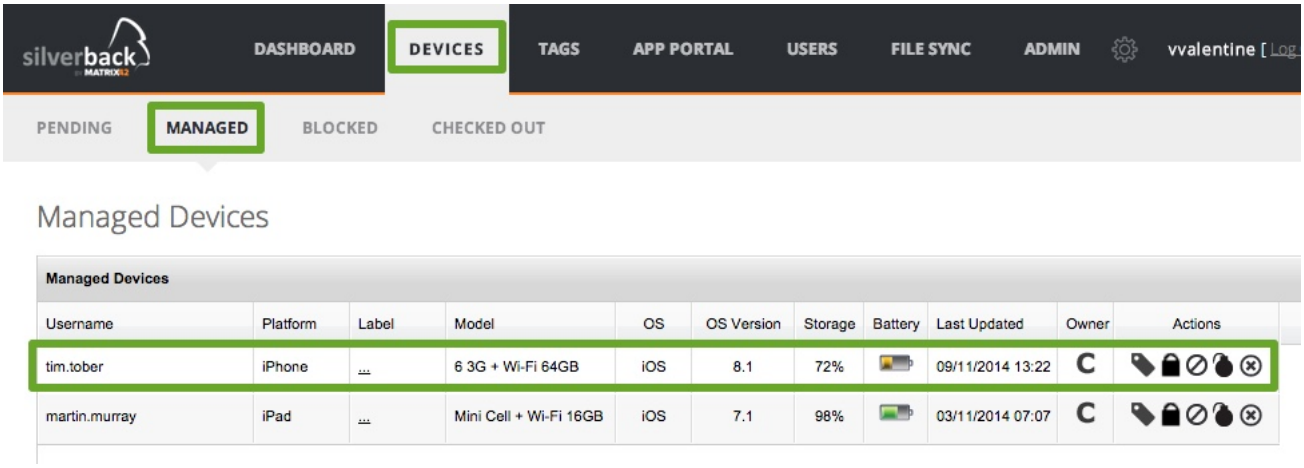
Quick Start Guide for iOS

- Press the home button. Within 60 to 90 seconds you should see the M42 Silverback App Port icon on your homescreen (see also picture in section 'Enrollment with SMS').

Once you see the App Portal icons your device is under Matrix42 Silverback management and you know that the MDM APNS process is working.

1.6. Display Device Details

Once your device is enrolled and the '*App Portal*' icon is visible on the iOS device, you will see the device under 'Devices' in the 'Managed' section.

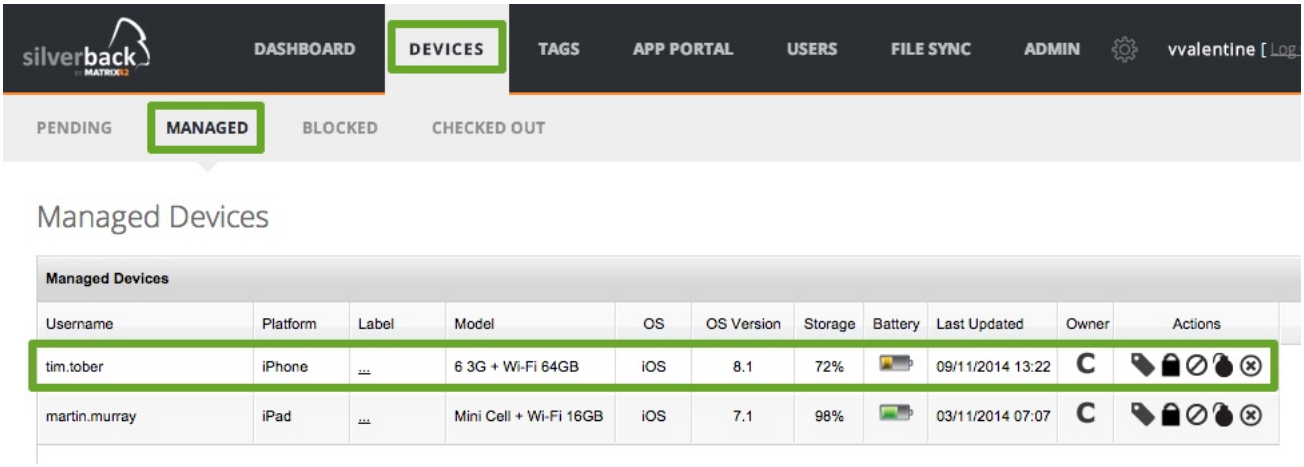


From here double click on the device to display the device details like

- Device info last updated
- General device information (e.g. Model and serial number, IMEI, Mac addresses)
- Assigned Tags
- Encryption and Passcode info
- Profile, provisioning and certificate lists
- Application list

1.7. Managed Device Actions

Once your device is enrolled and the '*App Portal*' icon is visible on the iOS device, you will see the device under 'Devices' in the 'Managed' section.



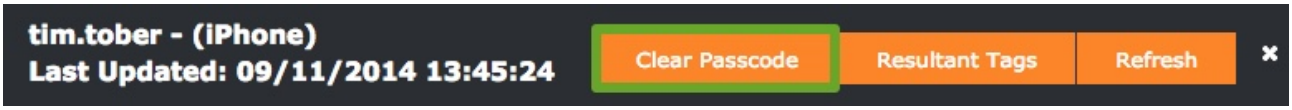
From here you can initiate the following MDM commands to the device

- Tag: Manually assign additional Tags to a device (see chapter 'Tags' for more details).
- Lock: Lock the device. The user needs to re-enter his passcode to get access.
- Block: Move device into '*Blocked*' tab and remove all company Tags (Profiles, Apps except device restrictions).
  Note: The device is still under MDM management.
- Factory Wipe: This options performs a full device wipe to factory defaults!
  Note: The device is completely wiped and all company & user data gets erased.
- Delete Business Data: Move 'device into 'Checked out' tab and will delete the main MDM management profile.
  Note: This will remove all company apps, profiles & data from device but leave the private data of the user untouched.

1.7.1. Clear Passcode

If the user forgot his device passcode you can simply clear the passcode by doing the following steps:

- In the '*Devices*' - '*Managed*' section double click on the user / device.
- Click on '*Clear Passcode*'.



On the iOS device the user has now direct access to the device but needs to re-enter a passcode.

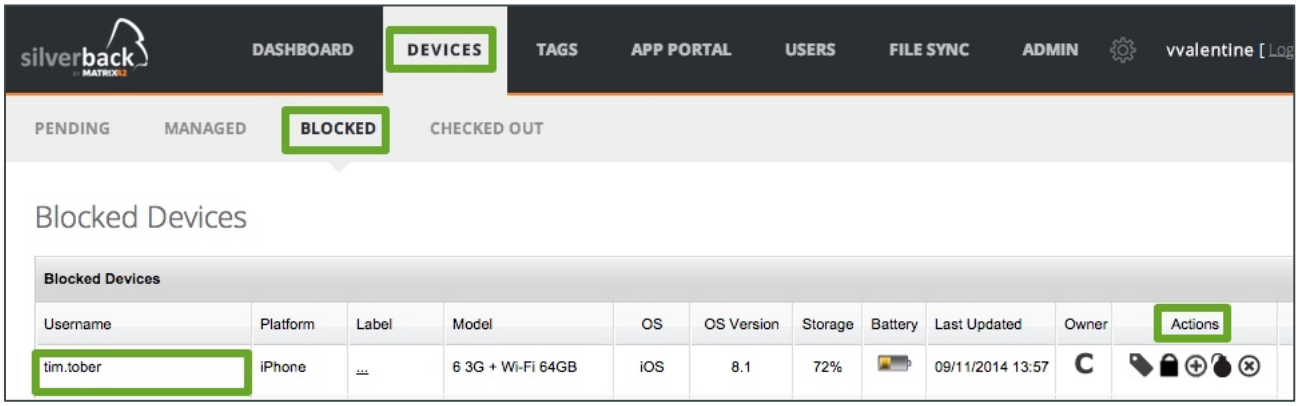
1.7.2. Manually Block / Unblock Devices

Matrix42 Silverback allows you to put devices into quarantine either manually or automatically. This section covers to manually block and unblock a device. The automated process is described later in conjunction with an application blacklist.

To manually block a device do the following:

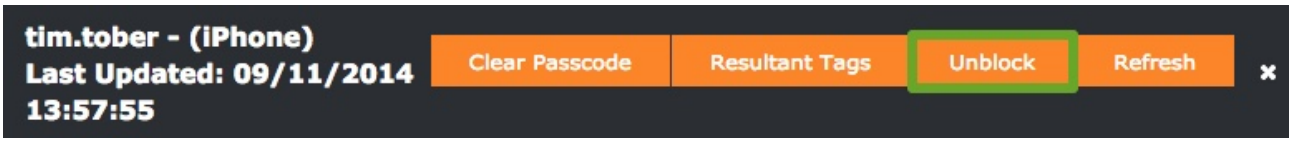
- In the '*Devices*' - '*Managed*' section select the block option on the right side (⊘)

The device will be moved into 'Devices' - '*Blocked*' tab shortly and all company Tags (Profiles, Apps) are removed. However please **note** the device is still under MDM management. You should see the Matrix42 Silverback '*App Portal*' disappear.



To manually unblock the device do the following:

- In the '*Devices*' - 'Blocked' section select the unblock option on the right side (⊕).
- In the pop-up windows please select '*Unblock*'.



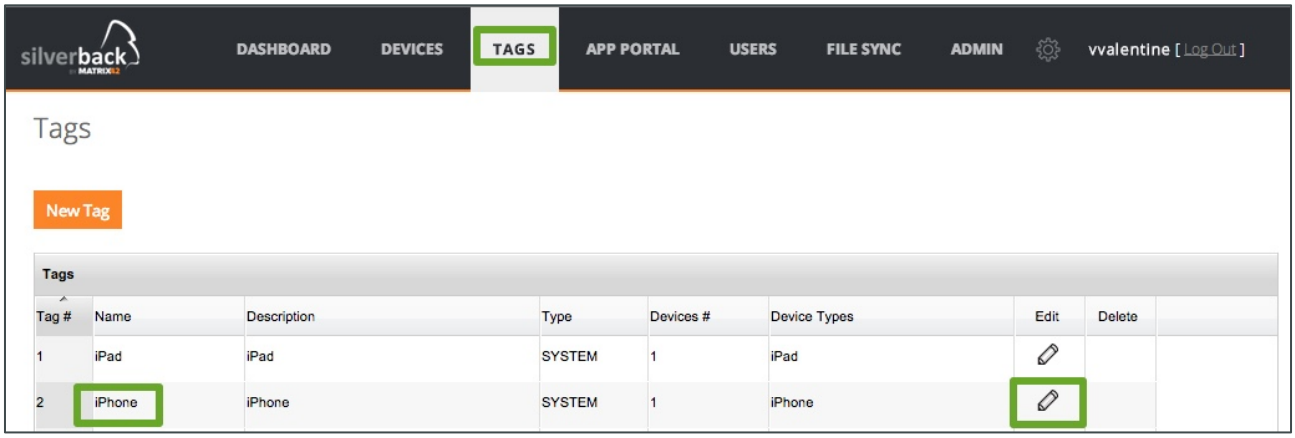
The device will moved back into 'Devices' - '*Managed*' tab shortly and all company Tags (Profiles, Apps) will be re-applied. You should see the Matrix42 Silverback '*App Portal*' reappear.

1.8. Using Tags for Profile, Apps & Policies

Silverback 'Tags' are the central place to assign profiles, apps and policies to a device type. By default Matrix42 Silverback provide you with the following iOS system tags which will be deployed to all iOS devices automatically:

- iPhone
- iPad

When doing your trial we suggest to use the existing system tags. However please note that you can create additional tags that can be automatically assigned to AD/LDAP groups once you connect your AD/LDAP with the Matrix42 Silverback Connector. Further information you will find in section 2.

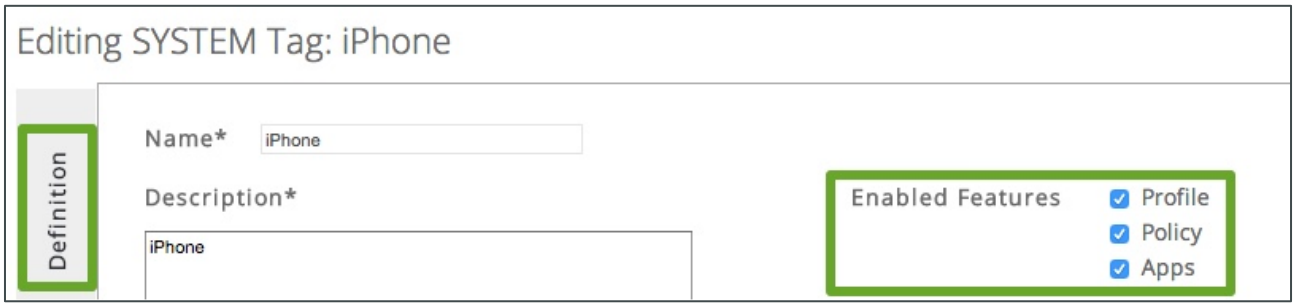


The following examples are for the iPhone. For iPads you simply edit the 'iPad' system tag.

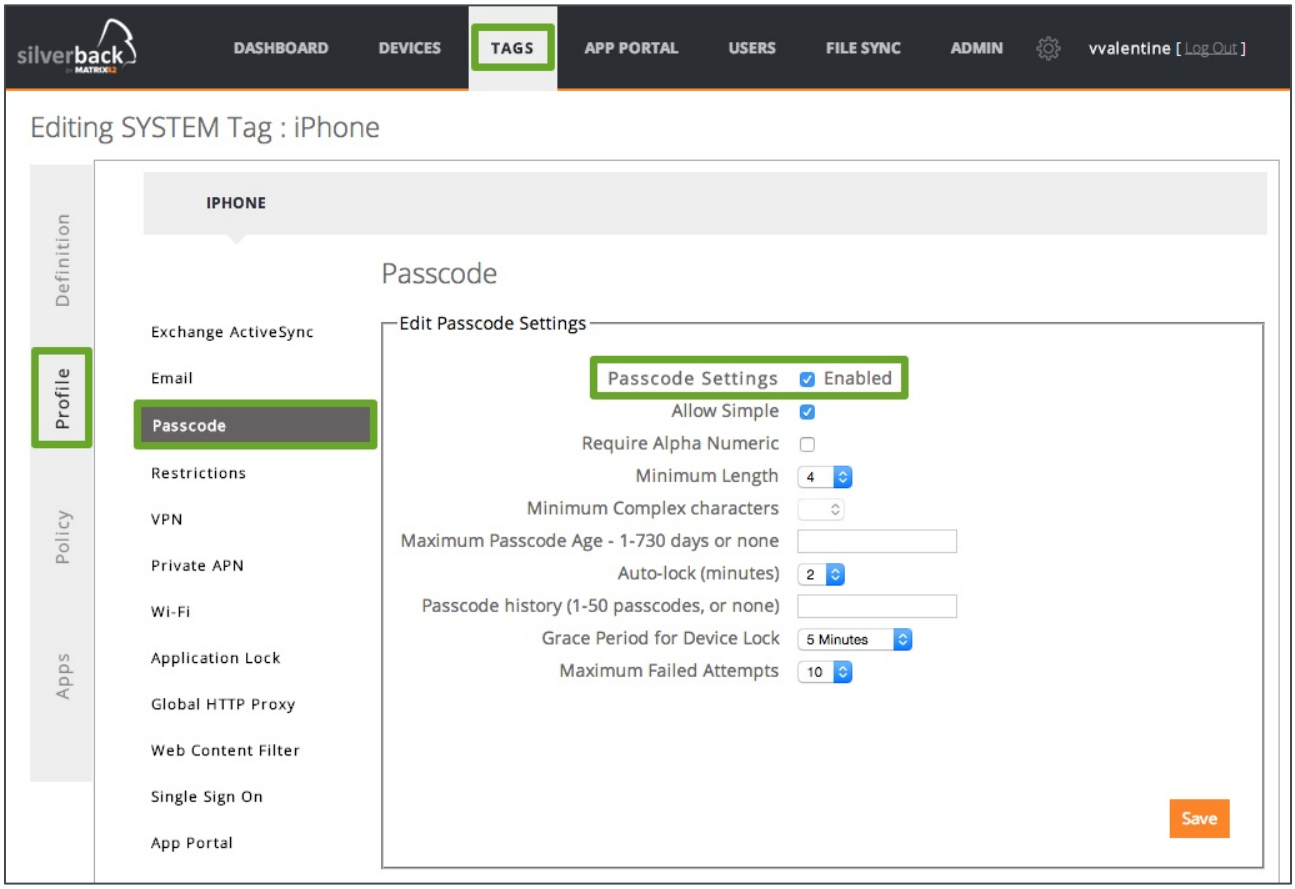
1.8.1. Create a Passcode Profile

To create or change a passcode profile you do the following steps:

- In the main menu switch to '*Tags*'.
- Edit the iPhone system tag by clicking on the 'Edit' icon on the right side.
- You are now in the '*Definition*' tabs on the left side. Ensure that '*Profile*' is enabled on the right side.



- On the left tab bar switch to '*Profile*'.
- Select the profile type '*Passcode*' on the left side.



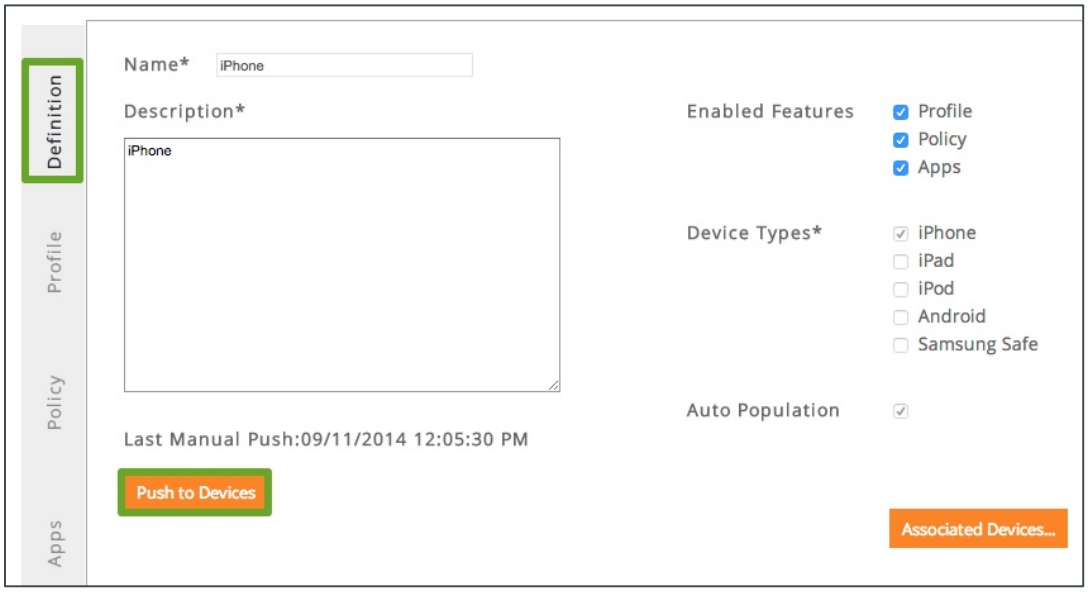
- Enable the passcode setting on the right side.
- Apply your company or trial passcode settings.
- Press '*Save*'.

1.8.1.1. Manual Push of Tag Settings to Devices

Once you save the profile Matrix42 Silverback will automatically deploy the profiles in the next deploy schedule in a few minutes.

If you want to manually push the updated Tag to all associated devices immediately you can do the following:

- Within the Tag on the left tab bar you switch back to '*Definition*'.
- Down left click on '*Push to Devices*'.

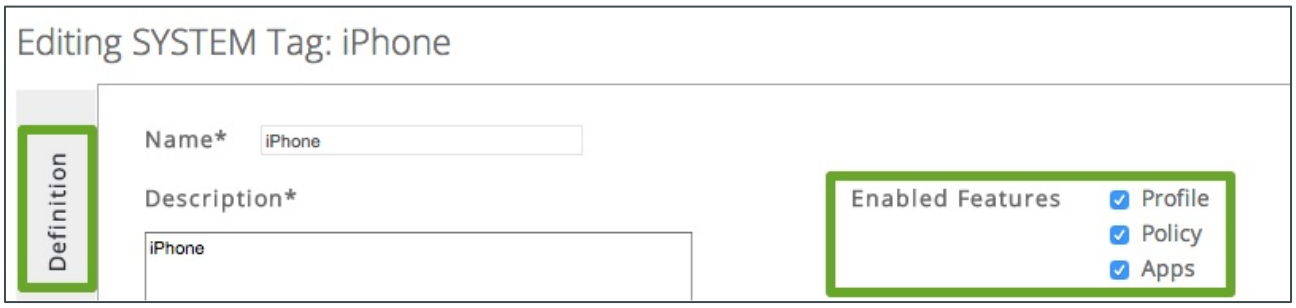


1.8.2. Create a Exchange ActiveSync (EAS) Profile

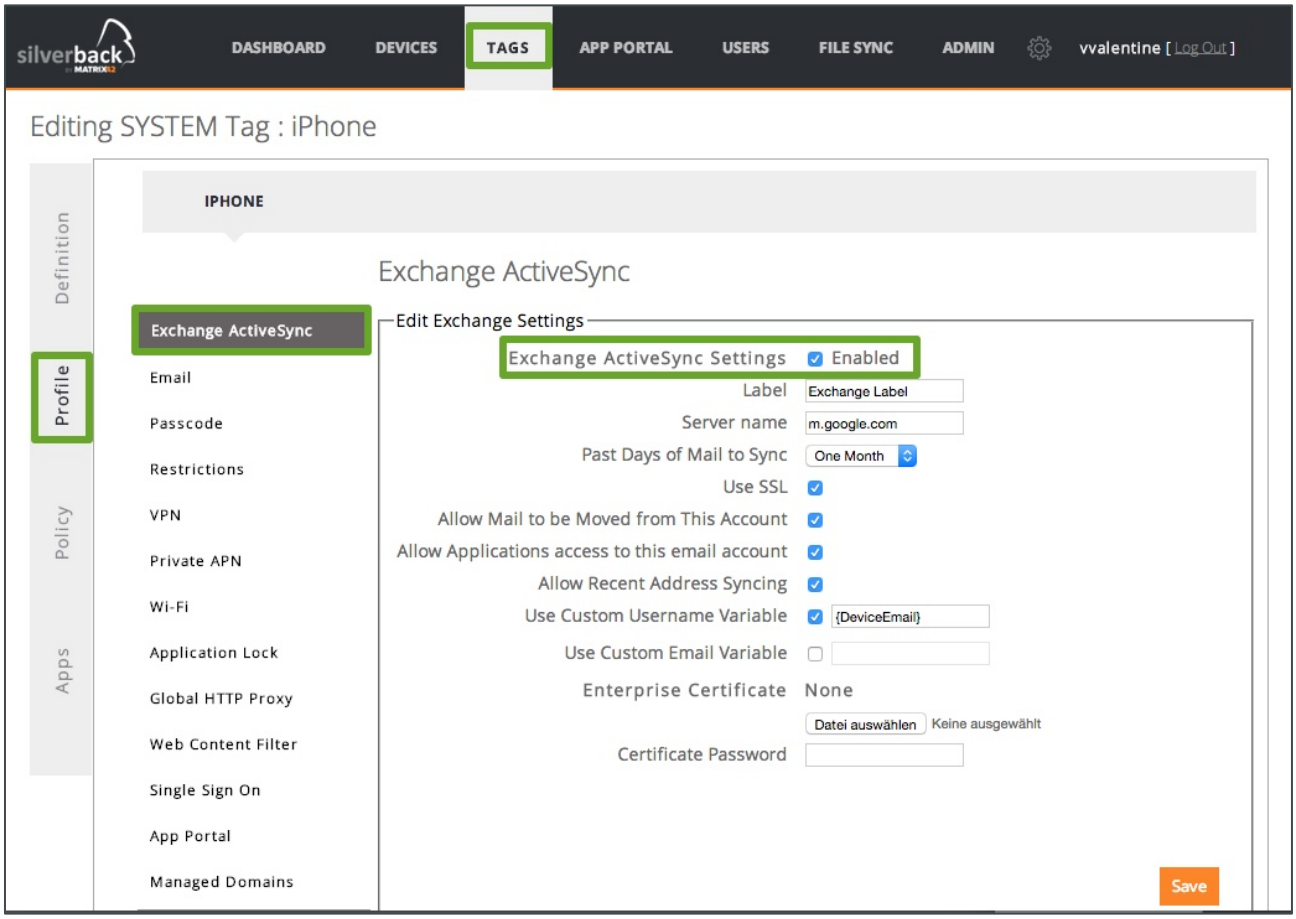
In order to access your corporate email server from the mobile device, the email server needs to be accessible with an external DNS address from the internet.

To create an EAS profile you do the following steps:

- In the main menu switch to '*Tags*'.
- Edit the iPhone system tag by clicking on the 'Edit' icon on the right side.
- You are now in the '*Definition*' tab on the left side. Ensure that '*Profile*' is enabled on the right side.



- On the left tab bar switch to '*Profile*'.
- Select the profile type '*Exchange ActiveSync*' on the left side.



- Enable the Exchange ActiveSync setting on the right side.
- Apply your company or trial EAS settings.
  - Enter a meaningful ‘Label’ that appears the in the iOS email accounts overview.
  - Enter the ‘Server name’.
  - Enter additional info and put checkmarks as required.
- Press ‘*Save*’.

1.8.2.1. Define user specific Exchange Account Username

By default Matrix42 Silverback will take the following settings to provision the EAS profile with user specific settings.

- Silverback Basic Username = Exchange Account Username.
- Silverback Basic Email Address = Exchange Email Address.

You can cross check the values when accessing the user details via ‘Users’ and edit a sample user. If you need to change one of the Exchange values you can replace the EAS username or account name with a specific Silverback system variable. The following example uses the email address as the Exchange account name which is required for Google EAS profile:

- Checkmark ‘*Use Customer Username Variable*’.
- Set ‘*Use Customer Username Variable*’ = {DeviceEmail}

For a full list of all available Silverback system variable please refer to the appendix.

1.8.2.2. Prevent unmanaged devices accessing Exchange ActiveSync

In productive environments customer want to prevent users to have access to the corporate email server by simply adding their email account credentials into their unmanaged private devices at home. Matrix42 Silverback offers the following solutions to prevent this:

- Powershell Integration: Safely interconnect your EAS server with our Matrix42 Silverback solution by using Powershell. Put your EAS Server into quarantine mode to only allow whitelisted devices access. Matrix42 Silverback will whitelist all managed devices on the EAS server. Non-managed device will not get access to the EAS server.
- PKI Integration: Safely interconnect your Microsoft CA with our Matrix42 Silverback solution. Configure your EAS server to allow only access with individual user / device certificates. Matrix42 Silverback will deploy the EAS certificates using MDM EAS profiles to the devices. Devices without EAS certificates will not get access to the EAS server.

1.9. Deploy Apps

Matrix42 allows you to provision public App Store apps and internal, self-developed Enterprise apps. Public App Store apps will be installed from the App Store to the device. Internal Enterprise apps will be pushed directly from the Matrix42 Silverback Server to the device.

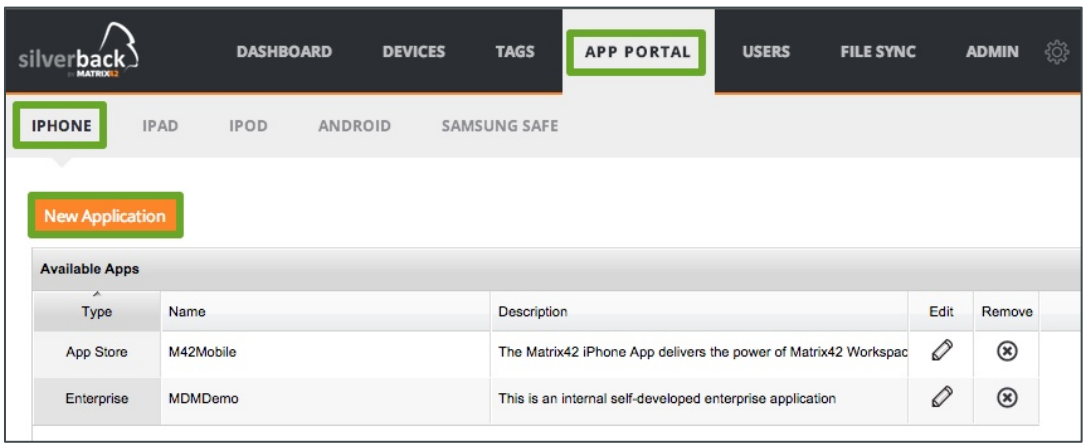
In order to deploy apps you need to do the following general steps:

- Add App Store apps to the Silverback App Portal
- Add Enterprise apps to the Silverback App Portal
- Assign public and internal apps to device Tags

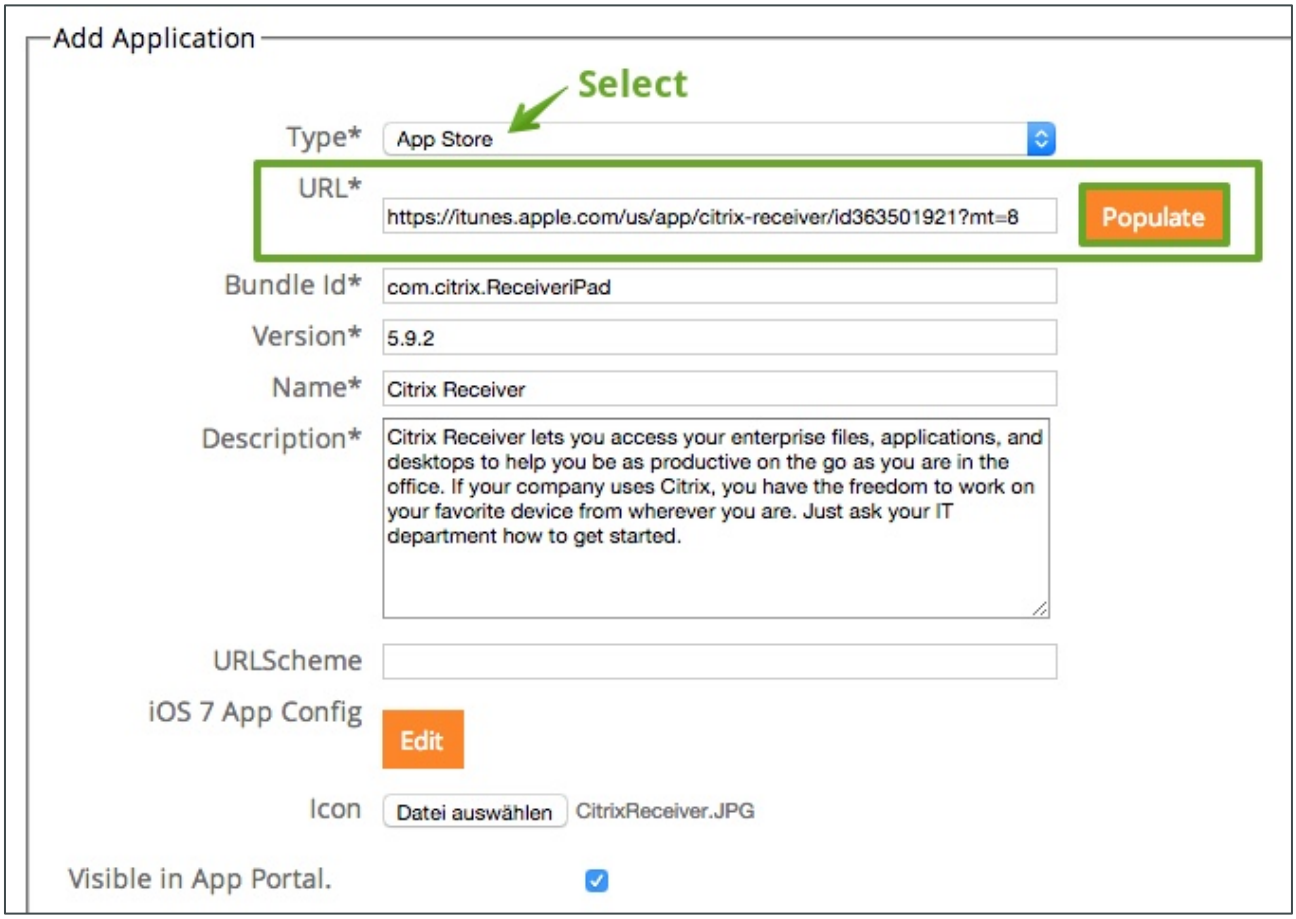
1.9.1. Add Public App Store Apps to Silverback App Portal

Please do the following steps to add a public App Store app to the Silverback App Portal:

- Choose '*App Portal*' in the main menu bar.
- Select the device type in secondary menu bar below, e.g. iPhone or iPad.
- Click on 'New Application''.



Quick Start Guide for iOS



- In the upper area you define the basic application details:
  - Select 'App Store' in the '*Type*' field.
  - Copy & paste the public App Store URL into the '*URL*' field.
    E.g. use iTunes application to get the link and copy & paste the app icon.

  - Click on '*Populate*' to automatically retrieve public app store info into M42 Silverback.
  - Checkmark '*Visible in App Portal*' to make this app visible in the Silverback App Portal on the iOS device.

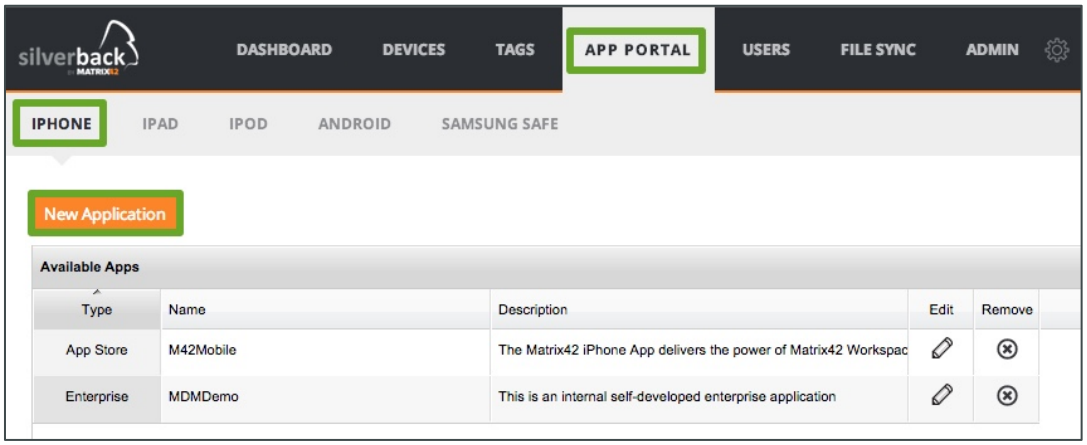
- In the 'iOS App Management' area checkmark your iOS app settings.
  - E.g. checkmark '*Automatically push to managed devices*'.

Matrix42 is currently working on providing a Silverback built-in online auto-lookup to select & retrieve Apple App Store Apps.

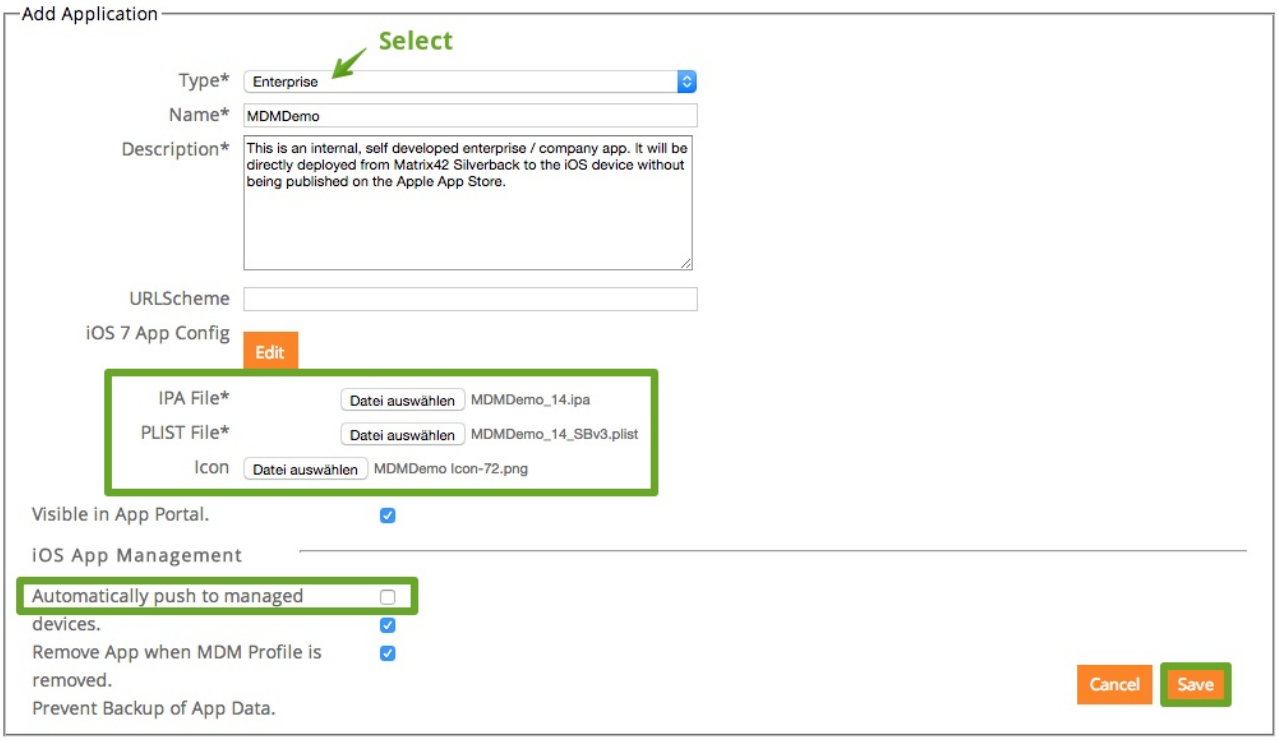
1.9.2. Add Internal Enterprise Apps to Silverback App Portal

Please do the following steps to add an internal, self-developed app to the Silverback App Portal:

- Choose '*App Portal*' in the main menu bar.
- Select the device type in secondary menu bar below, e.g. iPhone or iPad.
- Click on 'New Application''.



- In the upper area you define the basic application details:
  - Select 'App Store' in the '*Type*' field.
  - Copy & paste the public App Store URL into the '*URL*' field.
    E.g. use iTunes application to get the link and copy & paste the app icon.



- Checkmark '*Visible in App Portal*' to make this app visible in the Silverback App Portal on the iOS device.
- In the 'iOS App Management' area checkmark your iOS app settings.
  - E.g. checkmark '*Automatically push to managed devices*'.

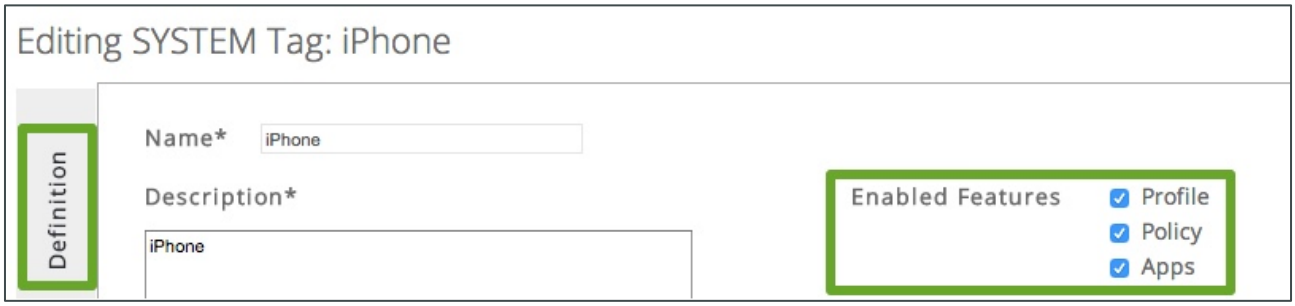
Please refer to the Appendix to get an example of a PLIST file that you can individually modify and upload into the M42 Silverback admin console.

1.9.3. Assign App to Tag

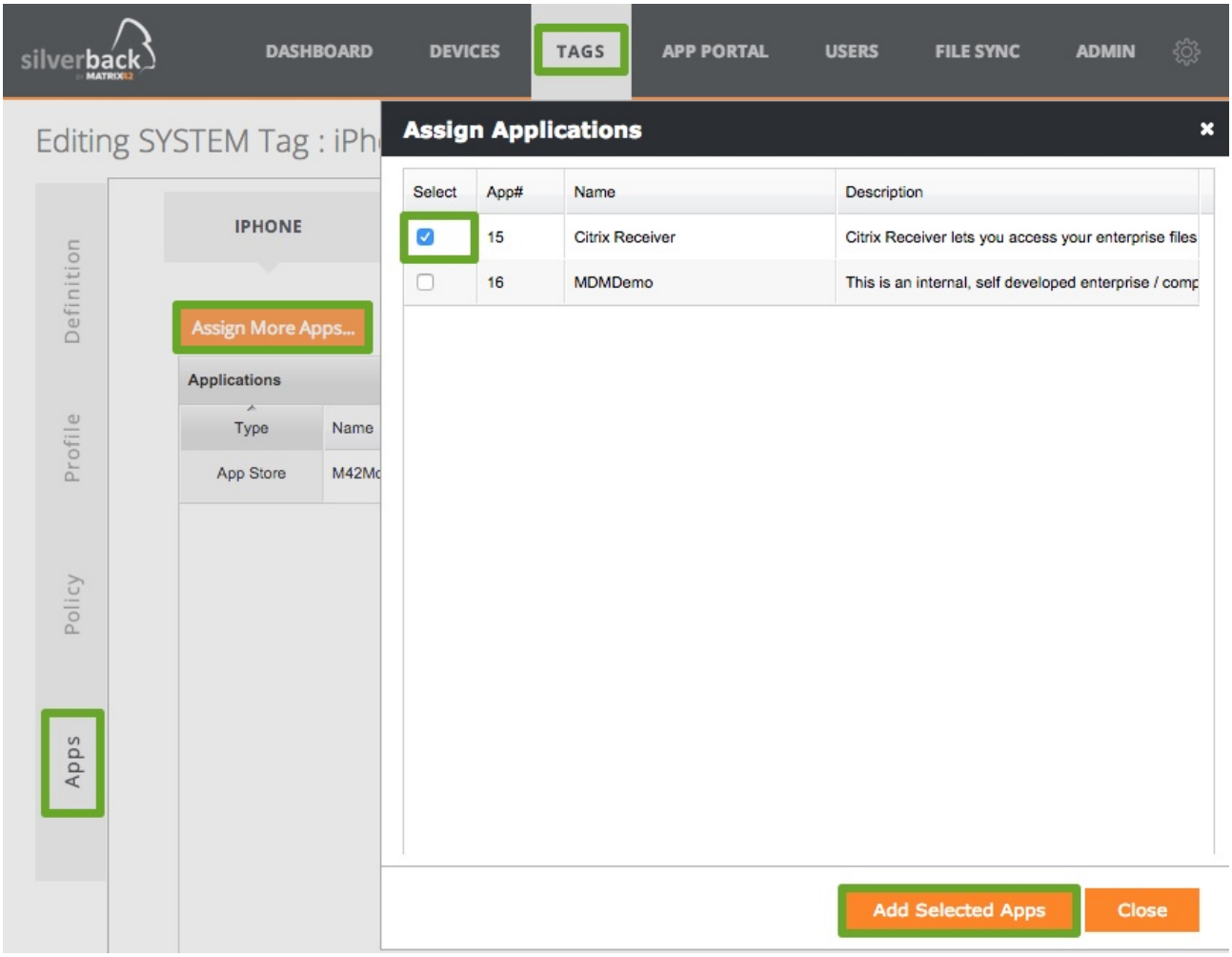
Please do the following steps to assign an App Portal app to a Tag:

- In the main menu bar select 'Tag'.
- Edit the iPhone system tag by clicking on the 'Edit' icon on the right side.
  - Select iPad system tag if applicable.
- You are now in the '*Definition*' tabs on the left side. Ensure that '*Apps*' is enabled on the right side.

Quick Start Guide for iOS



- On the left tab bar switch to '*Apps*'.
- Select the App Store and Enterprise apps you want to add to the Tag.
- Click on '*Add Selected Apps*'.



After these steps apps with '*Automatically push to managed devices*' settings will cause a pop-up on the user's device to install the app.

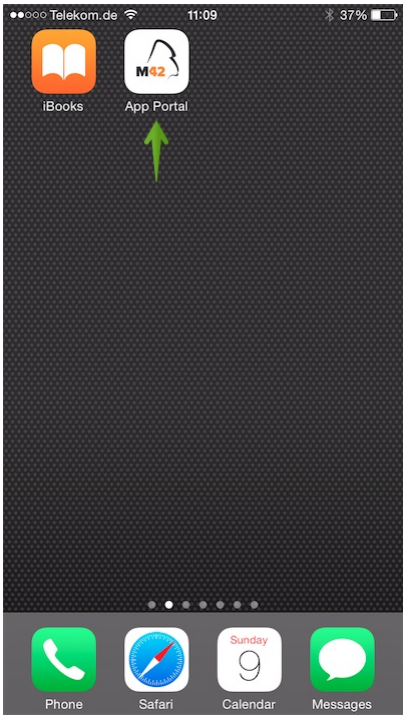
If the setting '*Automatically push to managed devices*' are de-activated the user can manually install the app by himself using the Matrix42 Silverback App Portal on the iOS device.

Quick Start Guide for iOS

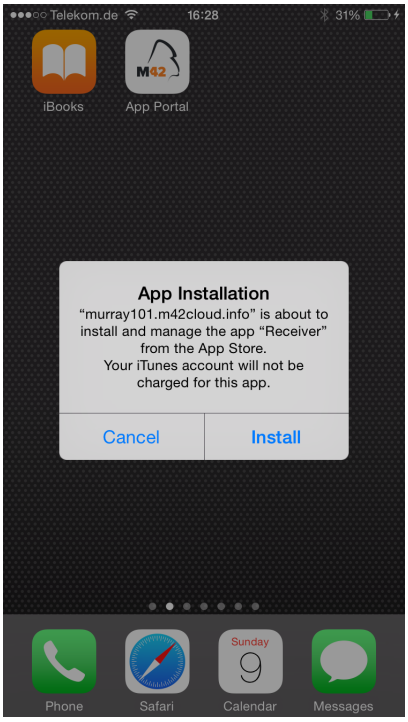
1.9.4. Using iOS App Portal to Download Apps

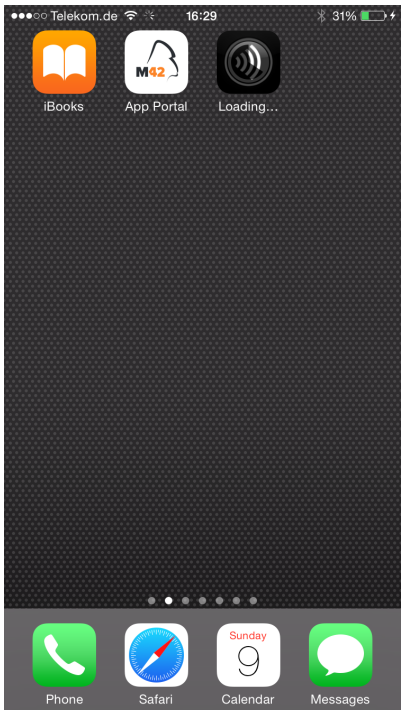
If the setting for App Store and Enterprise apps '*Automatically push to managed devices*' are de-activated, the user can manually install the apps by himself using the Matrix42 Silverback App Portal on the iOS device.

In the below example the end-user opens the App Portal on the iOS device and presses 'Install' to deploy the public App Store app 'Citrix Receiver' on its device.



Once the user pressed 'Install', the Silverback server will initiate the download of the app. After a couple of seconds the user will receive a pop-up asking for the installation of the app. Once confirmed the app is going to be installed on the device.





2. Appendix

2.1. From Cloud to On-Premises Migration

If you are a Matrix42 Cloud customer and you plan to migrate Matrix42 Silverback to an on-premise installation at a later stage, you should do the following steps:

- Before getting productive in the Matrix42 Cloud you contact Matrix42 Helpdesk.
- Please ask to use one of your company external DNS addresses (e.g. Silverback.YourCompanyName.xyz) for the Matrix42 Silverback Cloud Services.

By doing this you ensure that all enrolled devices are linked to your company DNS address. This will allow you to migrate from Cloud to on-premise at a later stage without having to re-enroll the existing devices.

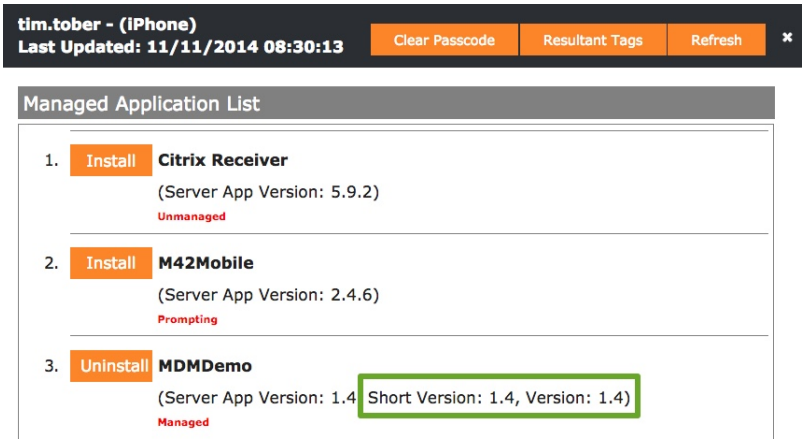
2.2. Internal App PLIST file

Use the following text template below to create your individual PLIST file for your Enterprise app. You need to change the following XML tags for your Enterprise app:

- <key>**url**</key>: Replace this value with the external Silverback server URL. Make sure you keep the '/mdm' at the end of the value
- <key>**bundle-identifier**</key>: You will get the bundle ID from your developer or by inspecting the info.plist file within the IPA your developer provides.
- <key>**bundle-version**</key>: You will get the version number from your developer.
- <key>**title**</key>: This is a descriptive text for the name of the app that appears on the iOS device once the app is deployed.

Please save this file as a pure text file and upload it into the applicable App Portal entry.

Note: If the app get frequently updated on the iOS device you need to recheck the exact version number, apply it to the PLIST file, and upload it again in the App Portal. Once the app is deployed on the device you can easily cross check by checking the app list in the Silverback console. The correct version number – that should be in the PLIST file – is the 'short version' or 'version' number in the device details.



```
<?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>items</key>
     <array>
          <dict>
               <key>assets</key>
               <array>
                    <dict>
                         <key>kind</key>
                         <string>software-package</string>
                         <key>url</key>

     <string>https://emm5.m42cloud.info/mdm</string>
                    </dict>
               </array>
               <key>metadata</key>
               <dict>
                    <key>bundle-identifier</key>
                    <string>com.matrix42.MDMDemo</string>
                    <key>bundle-version</key>
                    <string>1.4</string>
                    <key>kind</key>
                    <string>software</string>
                    <key>title</key>
                    <string>MDMDemo</string>
               </dict>
          </dict>
     </array>
</dict>
</plist>
```

2.3. M42 Silverback System Variables

Silverback has included in it certain 'System Variables' that can be used in various fields throughout the Administrator Console. A full list of these is shown below:

System Variable	Description
{Certificate}	This is the User's Certificate.
{CertificatePassword}	This is the Password for the User's Certificate.
{CustLdapVar0}	A Variable that can be assigned to any LDAP Attribute, captured at enrollment.
{CustLdapVar1}	A Variable that can be assigned to any LDAP Attribute, captured at enrollment.
{CustLdapVar2}	A Variable that can be assigned to any LDAP Attribute, captured at enrollment.
{DeviceEmail}	The Email Address associated with the User's Device, captured at enrollment.
{EmailDomain}	The Domain Suffix for the Silverback Environment. Uses the following format '@company.com'.
{firstname}	The First Name of the user, captured at enrollment.
{lastname}	The Last Name of the user, captured at enrollment.
{SilverbackActivationUrl}	The Silverback Activation URL (https://silverback.company.com/activate)
{SilverbackAdminUrl}	The Silverback Admin URL (https://silverback.company.com/admin)
{SilversyncSyncUrl}	The Silversync Admin URL (https://silverback.company.com/syncadmin)
{UserCert}	The Username associated with the Certificate to be used when requesting a 'User Certificate' for the enrolling device, captured at enrollment.
{UserEmail}	The Email Address associated with the user, captured at enrollment.
{UserName}	The Username associated with the user, captured at enrollment.
{UserPassword}	The User's Password, captured at enrollment (only if Silverback is configured to do so – not enabled by default).
{UserSMIME}	The Username associated with the S/MIME Certificate to be used when requesting an S/MIME Certificate for the user, captured at enrollment.
{UserVPN}	The Username associated with the user's VPN credentials, captured at enrollment.
{UserWifi}	The Username associated with the user's Wi-Fi credentials, captured at enrollment.
{UserWifiProxy}	The Username associated with the user's Wi-Fi Proxy Server credentials, captured at enrollment.
{DeviceStatus}	The Status of the Device in the Silverback system. (Managed, Blocked etc.)
{DeviceUDID}	The UDID of the Device.

Matrix42 AG
Elbinger Str. 7
60487 Frankfurt
Germany
Tel.: +49 (0)6102 - 816-0
Fax: +49 (0)6102 - 816-100
Email: info@matrix42.com
Web: http://www.matrix42.com