MATRIX42
SMARTER WORKSPACE – BETTER LIFE

Matrix42

Silverback by Matrix42 Admin Guide Version 5.1 U3

Version 5.1.3.7

9. December 2016

Copyright © 2000 - 2014 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.

MATRIX42
SMARTER WORKSPACE – BETTER LIFE

1. Device Enrollment 8
1.1. Secure one-time password 9
2. Management Studio Overview 11
2.1. Silverback Role Based Access Levels 12
2.2. Update Active User Details 14
3. Dashboard Tab 15
3.1. Information Tab 15
3.2. Device Summary 17
3.3. OS Version Summary 18
3.4. Device Summary 19
3.5. Compliance Tab 20
4. Devices Tab 21
4.1. Managed Devices 22
4.1.1. Managed Device Information 22
4.1.2. Managed Actions 23
4.1.3. Delete Serial Number 23
4.1.4. Device Lock Information 24
4.1.5. Device Lock Prompt for a Device Running iOS 7 25
4.1.6. Device Lock Prompt for a Device Running OS X 25
4.1.7. Device Lock Prompt for a Windows Phone device 26
4.1.8. Individual Device Information 26
4.1.9. Individual Device Information – Details and Information 28
4.1.10. Blocked Devices 29
4.1.11. Blocked Reason 29
4.1.12. Pending Devices 30
4.1.13. Provision User 31
4.1.14. Provisioned User Details 32
4.1.15. Bulk Provision Users 33
4.1.16. New Bulk Provision 33
4.1.17. Bulk Provision Status 34
4.1.18. Checked Out Devices 35
4.1.19. Device Labels 36
4.1.20. Device Visibility Flags 37
5. Tags Tab 38
5.1. Tags 40
5.1.1. Adding an Admin Tag 41
5.1.2. Tag Auto-Population – Device Conditions 43
5.1.3. Device Variable Logic Operators 43
5.1.4. Tag Auto-Population – LDAP Filter 45
5.1.5. Defining Individual Tag Properties 46

5.2. Profile Feature 48
5.2.1. Exchange ActiveSync 49
5.2.2. Email 51
5.2.3. Passcode 53
5.2.4. Restrictions 56
5.2.5. VPN 57
5.2.6. Private APN 60
5.2.7. Wi-Fi 61
5.2.8. Android for Work 62
5.2.9. Application Lock 63
5.2.10. Global HTTP Proxy 66
5.2.11. Web Content Filter 68
5.2.12. Single Sign On 69
5.2.13. Adding a Single Sign On 70
5.2.14. App Portal 71
5.2.15. M42 Mobile 72
5.2.16. Certificate Trusts 73
5.2.17. Certificate 75
5.2.18. Custom Profiles 76
5.2.19. Adding a Custom Profile 77
5.2.20. Web Clips 78
5.2.21. Adding a Web Clip 79
5.3. KNOX Feature 80
5.3.1. Adding or Editing a KNOX Container 81
5.3.2. Restrictions 81
5.3.3. Password 82
5.3.4. Exchange ActiveSync 84
5.3.5. Apps 86
5.3.6. Assign More Apps 87
5.4. Policies Feature 88
5.4.1. OS Version Compliance 89
5.4.2. Automatically Approve New iOS Versions 89
5.4.3. Hardware Compliance 90
5.4.4. Unknown Device Types 90
5.4.5. Application Blacklist 91
5.4.6. Lockdown 93
5.4.7. Lockdown Policies 95
5.4.8. Lockdown Actions 96
5.4.9. Companion 97
5.4.10. Companion Certificates 106

5.4.11. Adding an Enterprise Certificate 107
5.4.12. Adding a Certificate Authority Certificate 108
5.4.13. Companion Individual Messages 108
5.4.14. Companion Bulk Messages 109
5.4.15. Network Usage Rules 110
Apps Feature 110
5.4.16. Assigning Apps to a Tag 112
5.4.17. Integrating Apple's Volume Purchase Program 113
5.5. Content Feature 114
5.5.1. Cloud Content Providers 115
5.5.2. Silversync Content Provider 115
6. App Portal Tab 117
6.1.1. Managed Apps 118
6.1.2. Adding an iOS Enterprise Application 119
6.1.4. iOS 7 App Config 121
6.1.5. Adding an Apple iTunes App Store Application 122
6.1.6. VPP Applications 124
6.1.7. Take Management of Apps 126
6.1.8. iOS App Portal URL Schema Variables 126
6.1.9. Adding an Android/Samsung Safe Market Application 127
6.1.10. Adding an Android for Work Marketplace Application 129
6.1.11. Adding an Android/Samsung Safe Enterprise Application 132
6.1.12. Adding a Windows Phone Marketplace Application 133
6.1.13. Adding a Windows Phone Enterprise Application 135
6.1.14. Adding a Windows MSI 136
7. Users Tab 138
7.1. Creating a Local User 139
7.2. Bulk Import of Local Users 141
8. Admin Tab 142
8.1. Device Types 143
8.1.1. Create Device Types 144
8.1.2. Bulk Model Number Import 144
8.2. Hardware Authentication 145
8.2.1. Bulk Import Device Serial Number, Label, Name and Visibility Flag 146
8.3. EAS Settings 148
8.4. Email Templates 149
8.4.1. Email Templates 149
8.4.2. SMS Template 151
8.5. Backup Policy 151
8.6. Silverlync Integration 153

8.7. NitroDesk Integration 154
8.8. Pending Commands 155
8.8.1. Managed App Feedback Collection 155
8.8.2. Pending Commands 155
8.8.3. Concurrency Statistics 157
8.9. Console Permissions 159
8.9.1. Access Section 159
8.9.2. Device Privacy Section 160
8.10. Silversync Servers 161
8.10.1. Adding a Server 161
8.10.2. Configuring Silversync 163
8.10.3. Binding Push 170
8.11. Device Enrollment Program 173
8.11.1. Home Section 173
8.11.2. Devices Section 174
8.12. VPP App Licensing 179
8.12.1. Overview Section 179
8.12.2. Associating Users 180
8.12.3. Associating Licenses 181
8.12.4. Assets Section 181
8.12.5. Licenses Section 182
8.12.6. Users Section 183
8.12.7. VPP Users Export 185
8.12.8. VPP Licenses Export 185
8.13. Samsung UMC 186
8.13.1. Profile Section 186
8.13.2. Edit or Add a Profile 187
8.13.3. Settings Section 188
8.14. Android for Work 189
8.15. Self-Service Portal 191
8.16. User Management 193
8.16.1. Adding a New System User 195
8.16.2. Using Visibility Flags 196
8.16.3. Unlocking an ‘Locked’ Silverback Management Account 197
8.16.4. API Tokens 197
8.17. Licenses 198
8.17.1. License Information 198
8.17.2. Remove Duplicate Devices 198
8.17.3. Limit Devices Per User 199
8.17.4. Samsung Licenses 199

8.17.5. Certificates 199
8.18. App Portal 199
8.19. Lockdown Interval 200
8.20. EPiC 202
8.21. Logs 204
8.21.1. Activation Lock Bypass 205
8.21.2. Error Logs 206
8.21.3. Audit Logs 207
8.22. Queue Service 208
8.22.1. Command Queue 208
8.22.2. Scheduled Queue 209
8.23. MDM Settings 210
8.23.1. WP Settings 210
8.23.2. Windows settings 210
8.23.3. OS X Settings 210
9. Silverback Appendix 211
9.1. Internal Silverback System Variables 211
9.2. Custom LDAP Attributes 213
9.3. Bulk Import Local User CSV Format 214
9.4. Status Integration Endpoints 215

Silverback by Matrix42 Admin Guide Version 5.1 U3

1. Device Enrollment

The Silverback solution was designed with the Bring Your Own Device (BYOD) model in mind. Silverback allows the enrollment of both corporate and individually liable devices with zero touch from the system administrators.

Administrators can define Application Blacklists and Whitelists, Hardware Type and OS software version control with the ability to automatically restrict access or remove corporate data & access privileges from devices if any of those policies are violated. The Silverback platform also provides hardware serial authentication, which allows systems administrators to pre-register device serial number for access to corporate data as well as reporting on Device Ownership using data captured during the enrollment process.

The settings themselves are applied through a layered model that gives the Administrator the freedom to set a base level of security for the entire system, then to build upon this with individually configured Tags which can comprise of more restrictive and secure security policies, or populate other devices for a rollout of Corporate Applications and Mail Accounts.

Silverback provides a secure & easy end user self-service enrollment process. By utilizing a one-time-password, it prevents the exposure of corporate directory services and stops sensitive credentials from being entered on untrusted devices from unknown networks. The system administrator can set the length, complexity and validity period of that one-time password to ensure Silverback meets the most stringent of security needs. With the Self Service Provisioning Portal, Silverback provides the fastest enrollment & device provisioning in the market whilst maintaining a secure two factor enrollment mechanism.

The Silverback solution integrates with a Microsoft Certificate Authority to provide certificate information in a user's profile, as well as associates the certificate with the user's account as a logon credential, which is required for advanced identity certificate-based authentication with enterprise applications such as Microsoft Exchange ActiveSync.

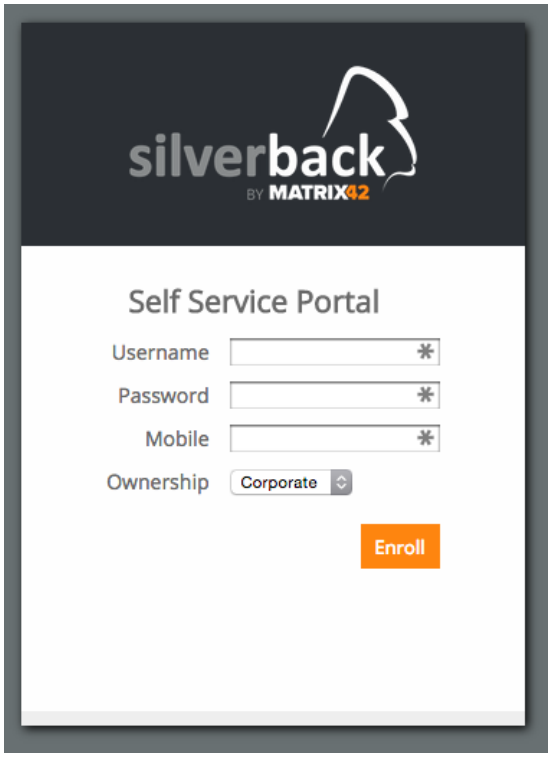
The key benefits of Silverback's unique enrollment process for the enterprise are:

- Fastest self-service end-user enrolment process with zero touch device provisioning for administrators.
- Simple provisioning of client certificates on iOS devices – create, deploy and manage client certificates within seconds
- Secure delivery of profiles and certificates using public key cryptography
- All without exposing AD/LDAP externally:
  - No AD/LDAP password stored on the device
  - Protect against password guessing
  - Protect against password lockouts that are:
    - Malicious via distributed denial of service attacks, or

- Accidental (most common reason end users raises a support call)
- Continuous syncing throughout password rotation process.

1.1. Secure one-time password

From a computer that is connected to the corporate network, the user opens a browser and navigates to the Silverback self-service portal.



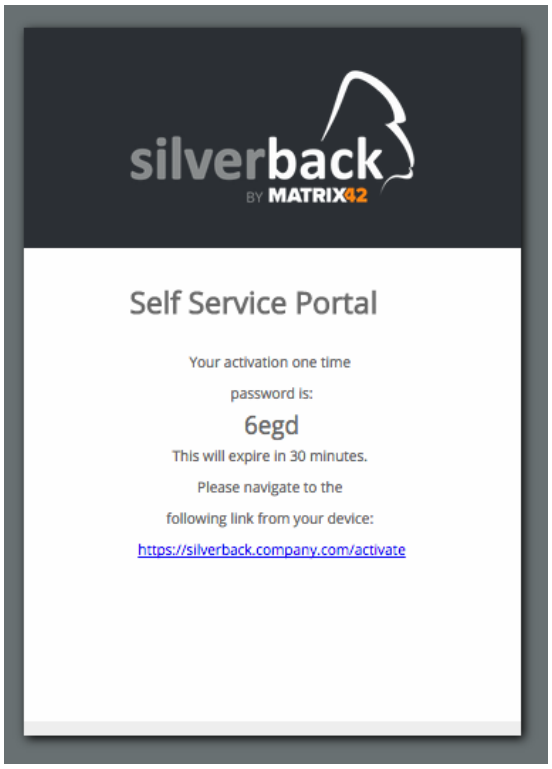
In the **Username** and **Password** fields, the user enters their User Principal Name (*UPN*) and network Password. If you don't already use your current UPN suffix for authentication, you can change the user's UPN to match their email address, allowing the user to effectively authenticate by entering their email address. The following Microsoft link describes how to add UPN suffixes to a forest http://support.microsoft.com/kb/243269

NOTE: When using Local Users for authentication, the users should enter the username provided, not their UPN.

In the **Mobile** field, the user enters the mobile number of the device they wish to enroll. If the device does not have a mobile number (e.g. iPad or iPod), they enter their contact mobile number.

In the **Ownership** field, the user selects whether they own the device ('Personal') or if it is owned by their organization ('Corporate').

The user clicks **Enroll and** receives their OTP like the one below, and an SMS will be sent to the number entered.



NOTE: The Device Ownership field is an option that is controlled on the **Admin – Self Service Portal** tab of the admin console.

2. Management Studio Overview

The Silverback administrator console is web based and accessible from within the corporate network and is optimized for the Mac and PC as well as the iPad. Silverback leverages the latest .NET standards to provide a scalable, intuitive user interface, advanced filters and searches with rapid data processing.

All admin level access is designed to occur via HTTPS and is controlled by a role-based access scheme.

The Management Studio consists of the following tabs:

- Dashboard
- Devices
- Tags
- App Portal
- Users
- Admin

A detailed description of the purpose, function and capability of each of the tabs is provided in the sections below.

Some pop-up windows such as the Device Info popup will occupy most of the screen and will increase in size as you scale your browser. Most of these pop-ups can also be closed by pressing escape on your keyboard as a shortcut.

2.1. Silverback Role Based Access Levels

Silverback supports three user roles with different levels of authorization with different levels of access to parts of Silverback.

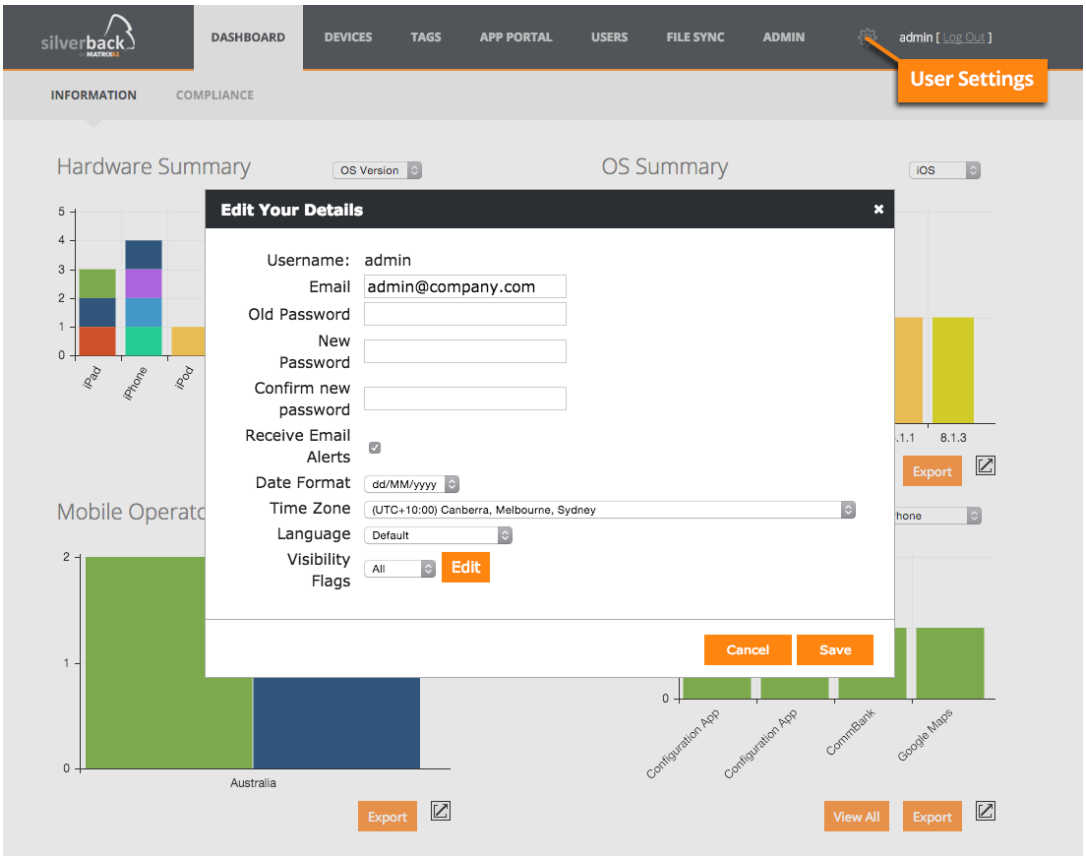
	Admin	Super Helpdesk	Helpdesk	App Manager	Reporting	Settings Administrator
Dashboard Tab	✓	✓	✓	✓	✓	
View Information Graphs	✓	✓	✓	✓	✓	
Export Information Graphs	✓	✓	✓	✓	✓	
View Compliance Information	✓	✓	✓	✓	✓	
View User Summaries	✓	✓	✓	✓	✓	
Devices Tab	✓	✓	✓			
Pending	✓	✓	✓			
Provision Device	✓	✓				
Managed	✓	✓	✓			
Blocked	✓	✓	✓			
Checked Out	✓	✓	✓			
Lock/Block/Unblock/Wipe Delete	✓	✓	✓			
Clear Device Passcode	✓	✓				
Tags Tab	✓					
View Definition	✓					
Create / Edit / Delete Tags	✓					
Tags > Profile Feature	✓					
Tags > Policy Feature	✓					
Tags > App Feature	✓					
App Portal Tab	✓			✓		
Admin Tab	✓					
Users Tab	✓					
View User Information	✓	✓	✓	✓	✓	
Add New Users	✓	✓				
Delete Users	✓	✓				
Bulk Import Users	✓	✓				
Export Users	✓	✓	✓	✓	✓	
System Settings Section						✓

NOTE: The ‘Admin’ account within the Silverback Management Console is a SYSTEM user that cannot be deleted. It is used by Silverback Engineers for troubleshooting issues with your Silverback Installation should the need arise. If you feel uncomfortable with this, simply change the account password using the additional account that you have been supplied with.

NOTE: The Settings Administrator Role is the only role with access to the System Settings page. No other role can access this, and when a Settings Administrator user logs in, they are taken directly to the Settings Page.

2.2. Update Active User Details

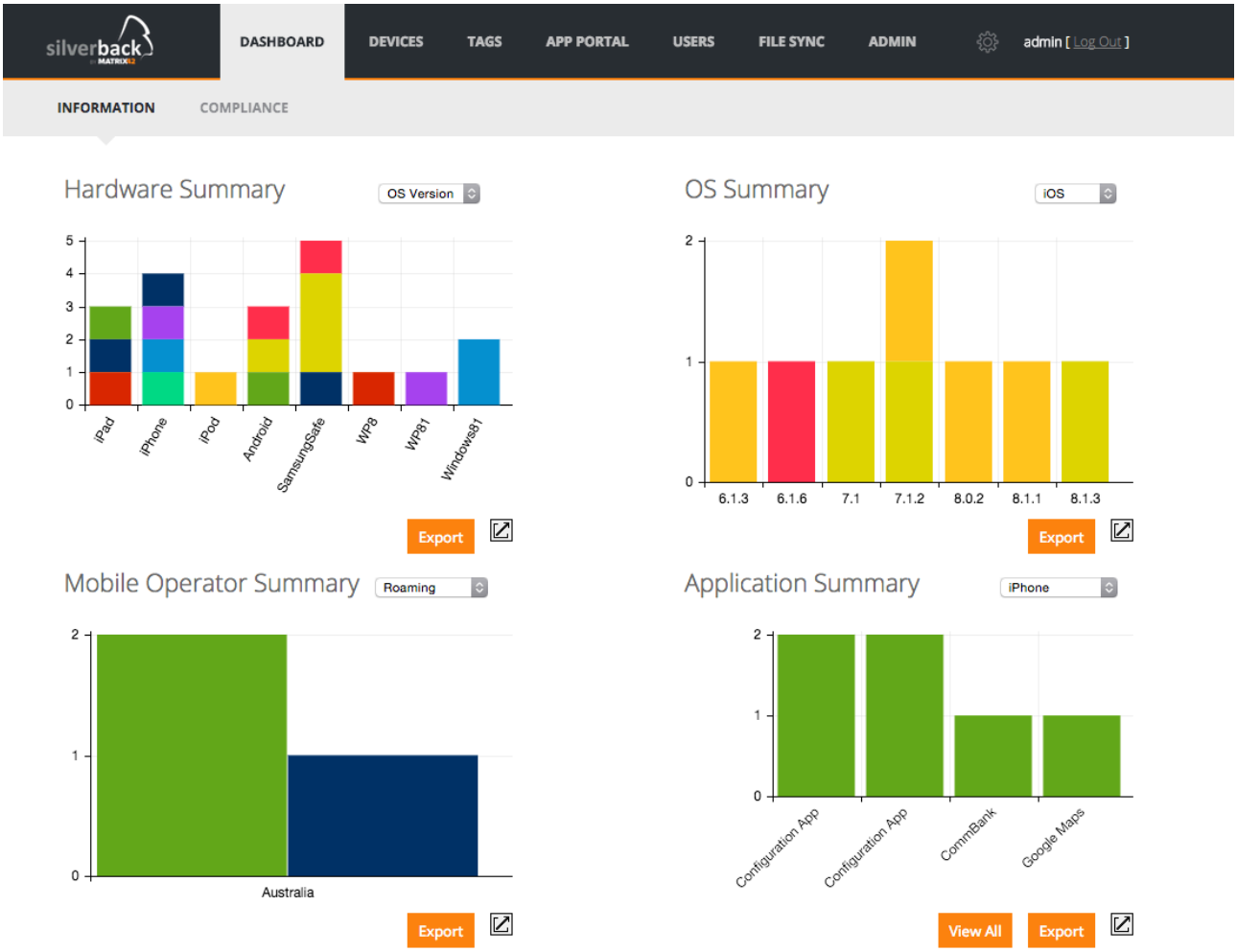
Modifying the current user's details can be done by clicking on the User Settings icon in the Silverback Management Console Page.



Field	Description
Email	Email Address for the logged in user
Old Password	Current Password for the user (required when changing the users password).
New Password	Field for entering in a new User Password
Confirm New Password	Field for re-entering in the new User Password for confirmation.
Receive Email Alerts	Checkbox to enable Administrative Alerts from Silverback.
Date Format	Sets the local date formatting for the current logged in user.
Time Zone	Sets the time zone for the current logged in user.
Language	Sets the console language for the user
Visibility Flags	Determines what devices the user can see

3. Dashboard Tab

The Dashboard tab provides an overview of the devices Silverback manages and allows you to drill down to a specific device/user level as well. It provides an easy to navigate overview of device Information and Compliance for enrolled devices.

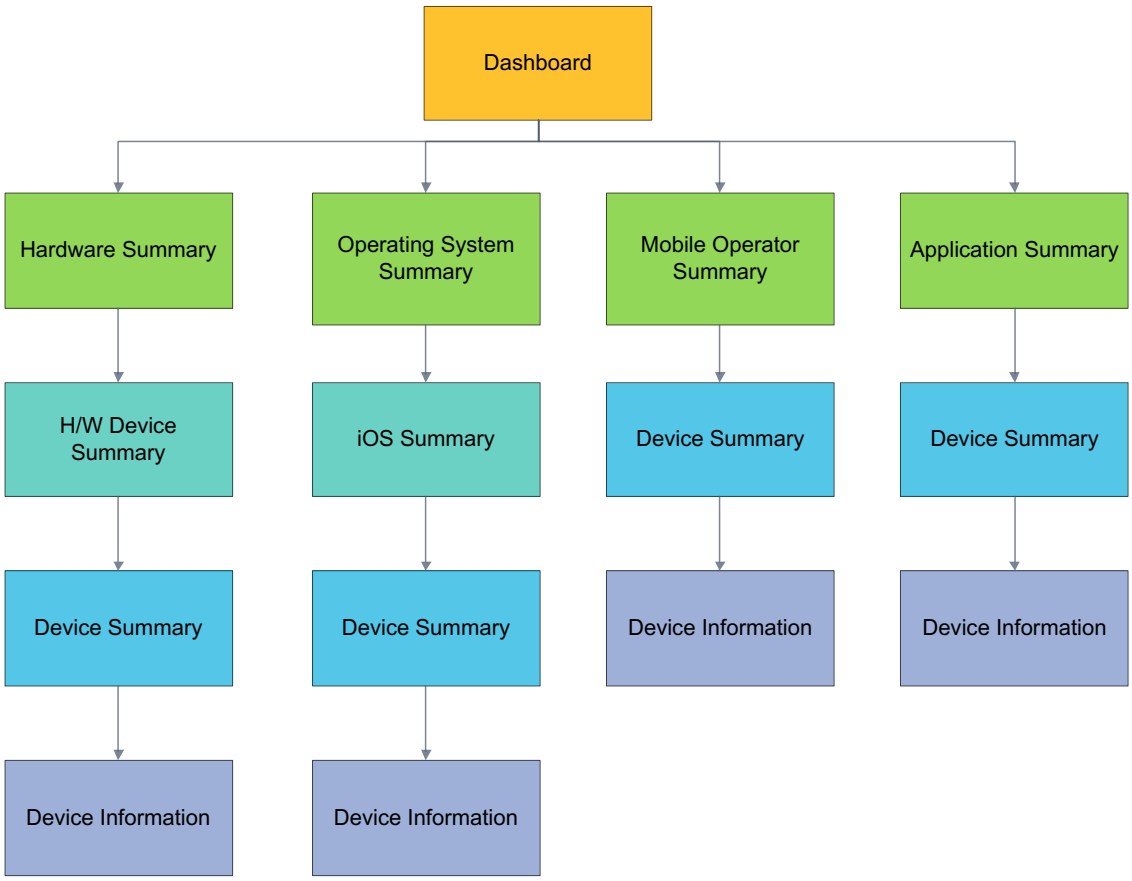


3.1. Information Tab

Export	**The** Export **button will export the detail for the displayed information to** Excel **as an** XLSX File **format.**
	The **Maximize** button will expand the selected graph to display greater detail.
View All	The **View All** button will display all Apps detected by Silverback for the selected Device Type.

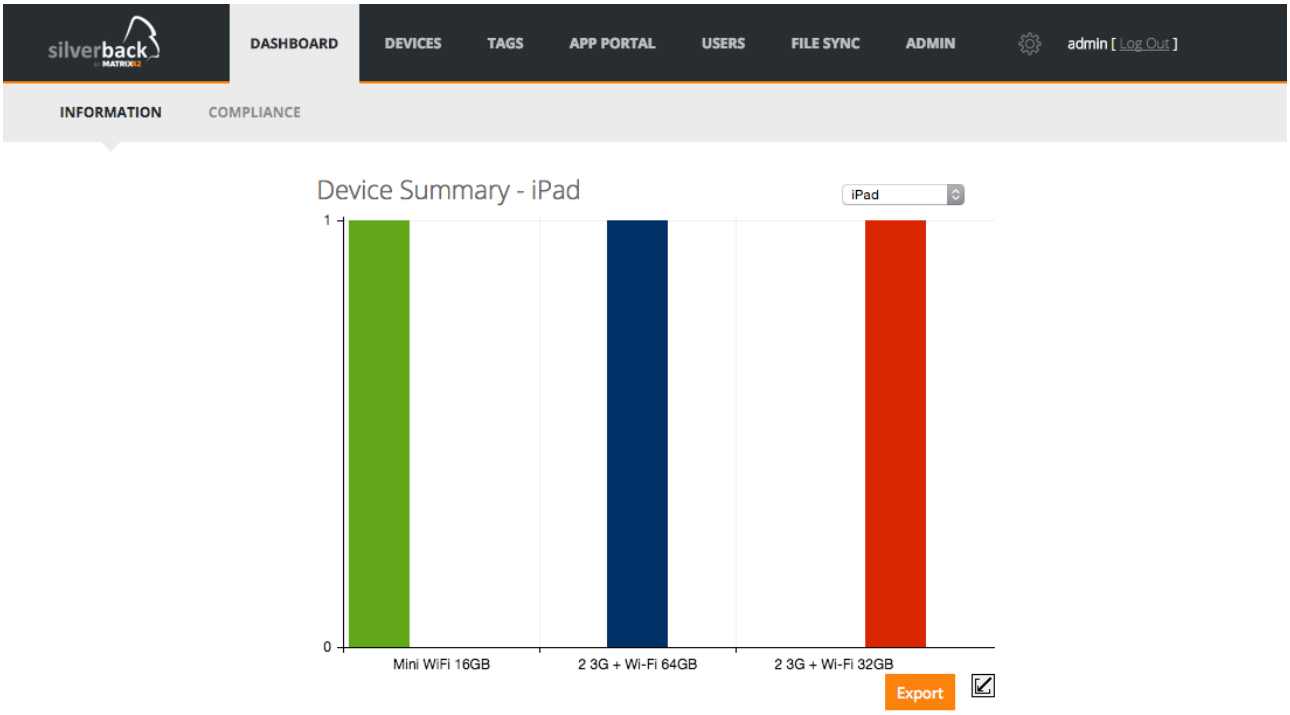
Graph	Description
Hardware Summary	Provides overview of the types of device hardware. Can be broken down by **OS Version** or **Ownership** (Personal or Corporate).
Operating System Summary	Breaks down devices by **OS Version**. Columns are further broken down by **Device Type**.
Mobile Operator Summary	Displays the breakdown of **Mobile Operators** for devices with cellular connections. Can display summary for **Roaming Devices** as well as **Non-Roaming Devices**.
Application Summary	Provides an overview of the Top 10 Applications for the selected Device Type. It is also possible to view all Applications installed in an exportable report.

Clicking on different segments of different graphs will navigate through to more detailed graphs or device summaries. The figure below details the navigation flow through the graphs and summaries.



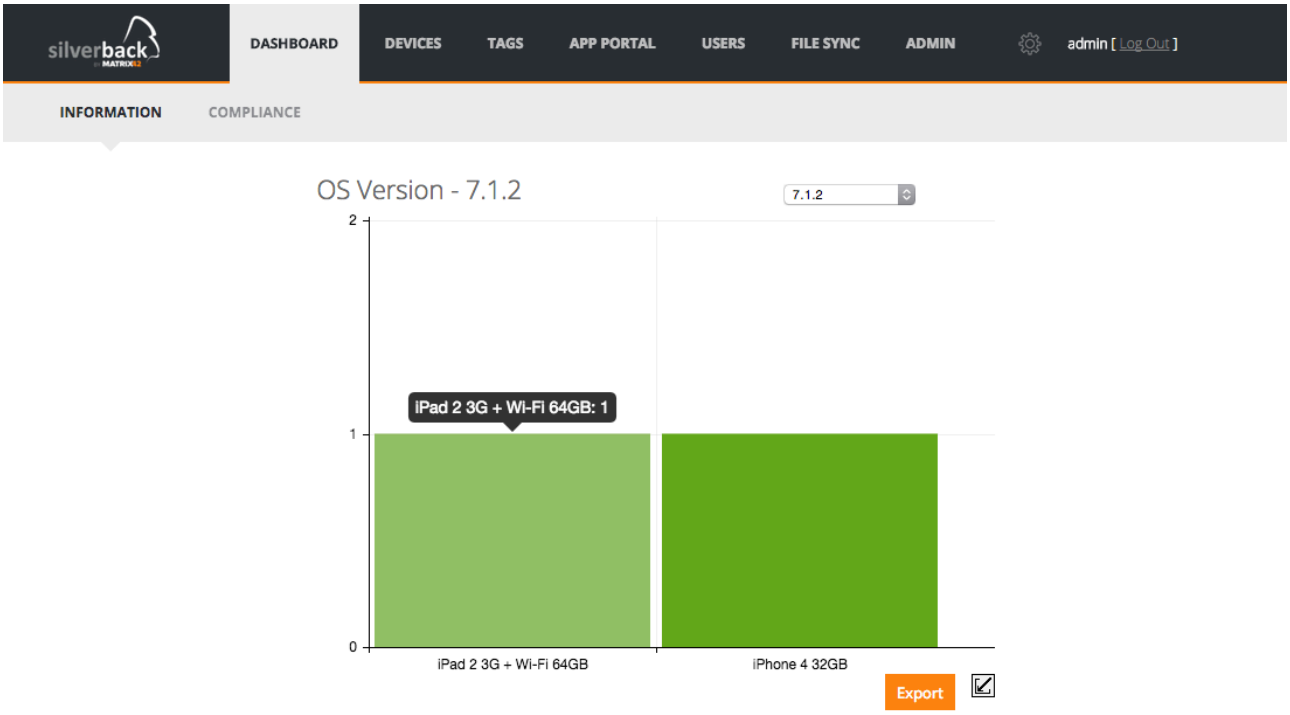
3.2. Device Summary

Clicking on a segment in the hardware summary graph will navigate to the device summary graph. This graph displays the detailed information for the hardware type selected in the hardware summary graph. The menu at the top allows users to switch between different hardware types for convenient navigation. Further detail can be viewed by clicking on a segment in the graph, which will display a device summary of the devices in that segment.



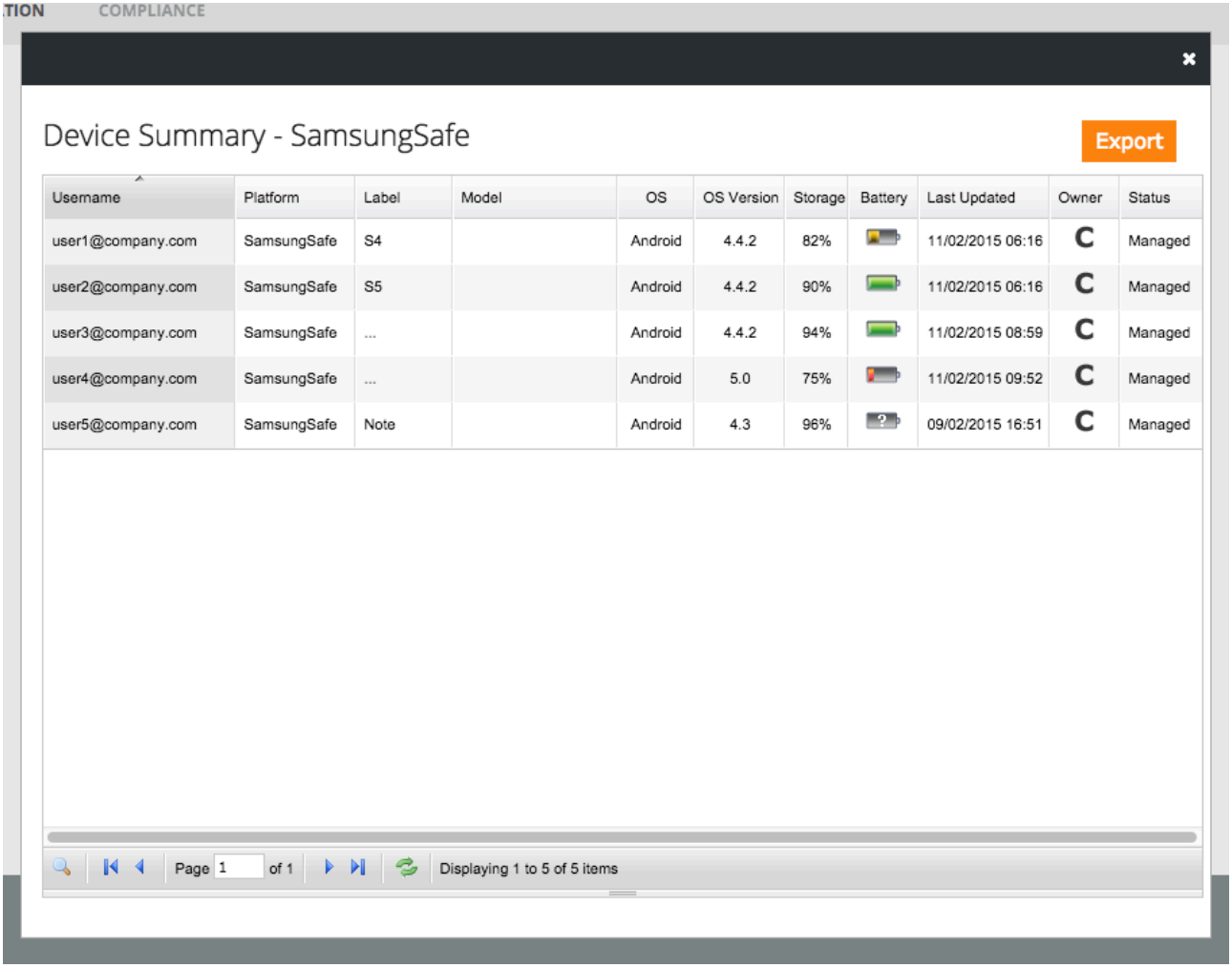
3.3. OS Version Summary

Clicking on a segment in the Operating System summary will take you to the OS Version Summary. This provides a detailed view on devices with the OS version selected. Further detail can be viewed by clicking on a segment in the graph, which will display a device summary of the devices in that segment.



3.4. Device Summary

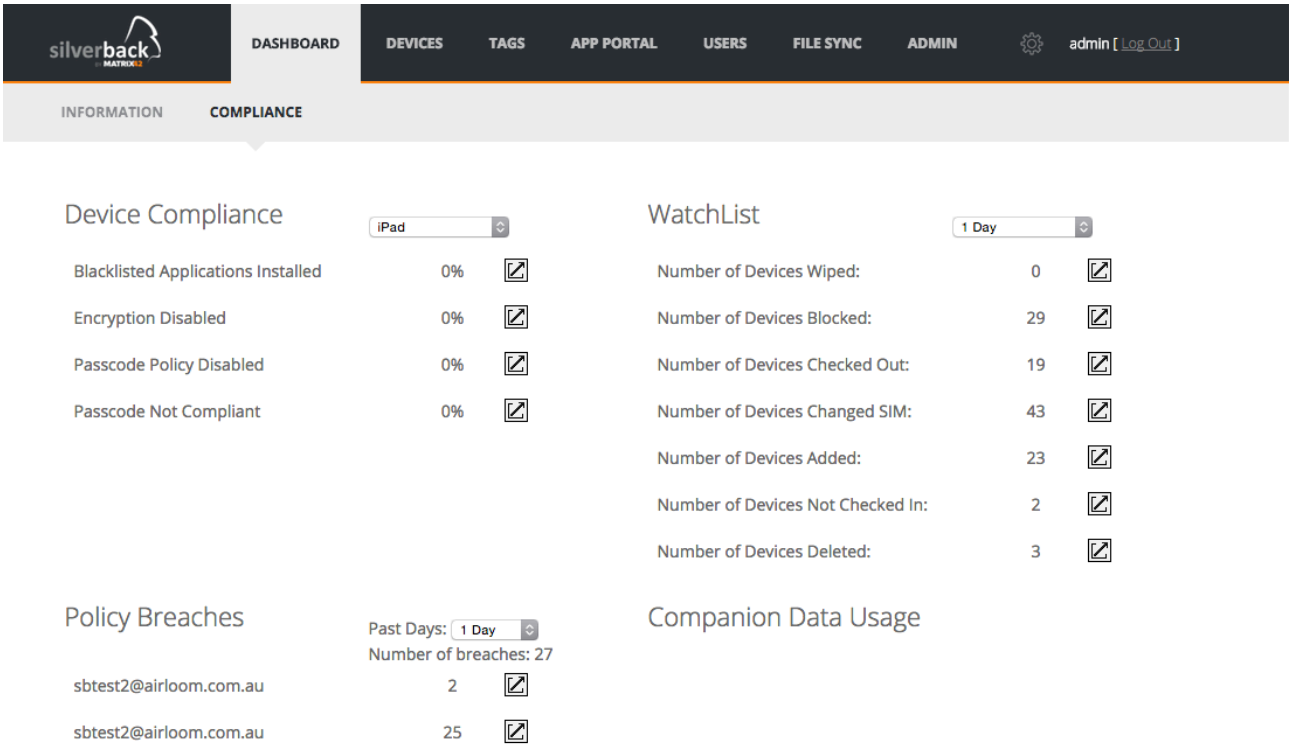
The device summary provides device-level information based on the selection criteria. Device summaries will display the devices that compose the segment of the graph that has been selected.



Username	Platform	Label	Model	OS	OS Version	Storage	Battery	Last Updated	Owner	Status
user1@company.com	SamsungSafe	S4		Android	4.4.2	82%		11/02/2015 06:16	C	Managed
user2@company.com	SamsungSafe	S5		Android	4.4.2	90%		11/02/2015 06:16	C	Managed
user3@company.com	SamsungSafe	...		Android	4.4.2	94%		11/02/2015 08:59	C	Managed
user4@company.com	SamsungSafe	...		Android	5.0	75%		11/02/2015 09:52	C	Managed
user5@company.com	SamsungSafe	Note		Android	4.3	96%		09/02/2015 16:51	C	Managed

3.5. Compliance Tab

The Compliance Tab will display important statistics about the devices enrolled when compared against policies defined within Silverback. It contains details about Device Compliance, who has broken Corporate Policies and Device Interactions for the specified time period.



Compliance Group	Description
Device Compliance	Displays the number of devices violating Compliance Policies grouped by Device Type.
Policy Breaches	Shows a list of users who have broken Compliance Policies – and how many they have broken.
Watchlist	Displays a list of actions Silverback has performed against devices that it has encountered. From enrolling new devices to devices not checking in.
Companion Data Usage	Displays information about Companion Users and their data usage if enabled.

NOTE: All of the above fields can be expanded upon by clicking the button next to the displayed statistic. This will show all devices that are associated with affected policy.

4. Devices Tab

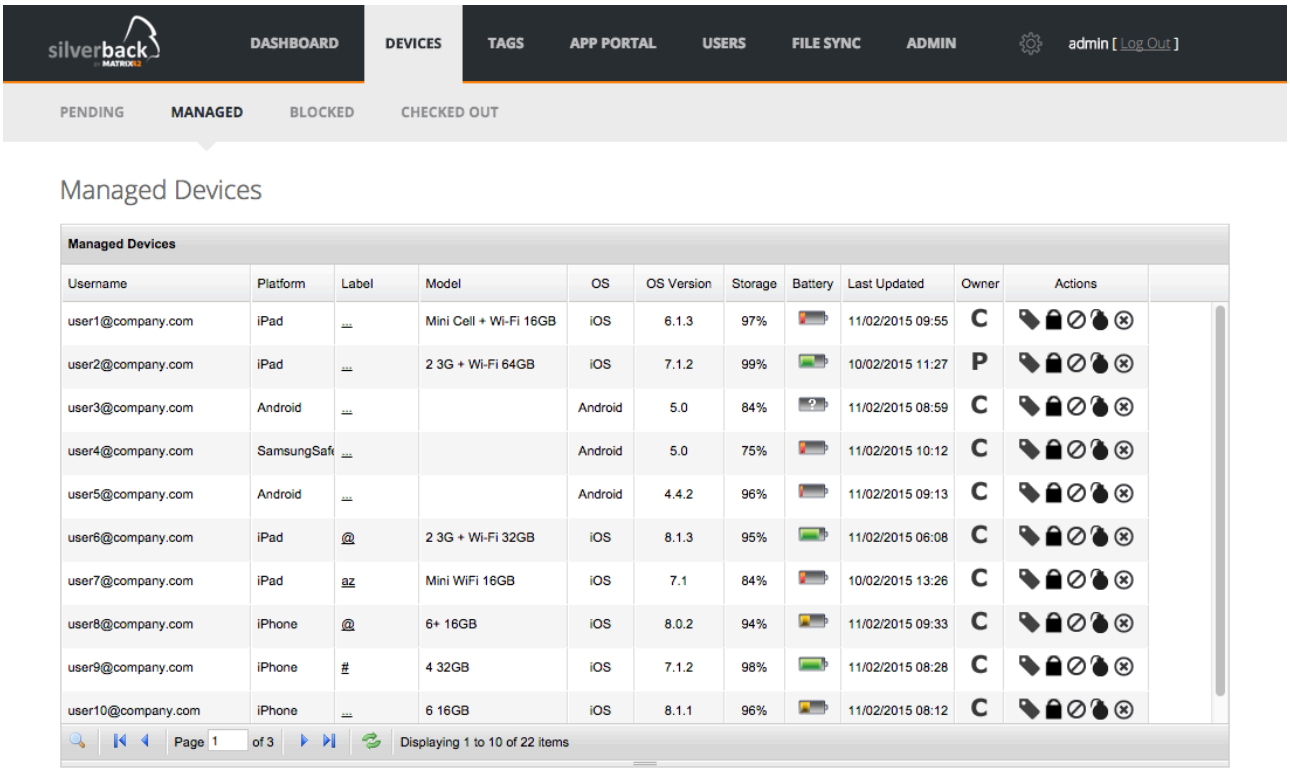
The Devices Tab is where a Silverback user can view information relating to the devices that are currently enrolled, or enrolling into Silverback. The four sections are;

- Pending – For Users have outstanding Pending Enrollment Requests with Silverback. This means that the user has entered in their credentials into the Silverback Self Service Portal and received a One Time Password for enrolling their device.
- Managed – Will contain Devices that have successfully enrolled into Silverback and conform to the set of Policies applied to them via their own set of Tags. – sees 'Tags' section.
- Blocked – Contains Devices that have enrolled into Silverback, but do not conform to their set of Policies. This means they have been isolated from the rest of Active Devices and will also have all Corporate Data removed from them.
- Checked Out - Is where a device will appear if Silverback detects that the user has manually un-enrolled their devices themselves. (Currently, this is limited to iOS only).

4.1. Managed Devices

A full listing of managed devices can be viewed from Devices > Managed Devices. Managed devices have access to all the configured profiles for that device type.

This will list all the Enrolled Devices that are conforming with Corporate Policies. From here you can manage each device individually, their settings will change dynamically based on their Platform and OS Types.



Username	Platform	Label	Model	OS	OS Version	Storage	Battery	Last Updated	Owner	Actions
user1@company.com	iPad	...	Mini Cell + Wi-Fi 16GB	iOS	6.1.3	97%		11/02/2015 09:55	C	
user2@company.com	iPad	...	2 3G + Wi-Fi 64GB	iOS	7.1.2	99%		10/02/2015 11:27	P	
user3@company.com	Android	...		Android	5.0	84%		11/02/2015 08:59	C	
user4@company.com	SamsungSafe	...		Android	5.0	75%		11/02/2015 10:12	C	
user5@company.com	Android	...		Android	4.4.2	96%		11/02/2015 09:13	C	
user6@company.com	iPad	@	2 3G + Wi-Fi 32GB	iOS	8.1.3	95%		11/02/2015 06:08	C	
user7@company.com	iPad	az	Mini WiFi 16GB	iOS	7.1	84%		10/02/2015 13:26	C	
user8@company.com	iPhone	@	6+ 16GB	iOS	8.0.2	94%		11/02/2015 09:33	C	
user9@company.com	iPhone	#	4 32GB	iOS	7.1.2	98%		11/02/2015 08:28	C	
user10@company.com	iPhone	...	6 16GB	iOS	8.1.1	96%		11/02/2015 08:12	C	

4.1.1. Managed Device Information

Detail	Description
Username	The username associated with the provisioned device.
Platform	Denotes the platform type the device has been built for.
Label	A Custom Label for the device.
Model	The model associated with the device hardware.
OS	The Operating System running on the device.

Detail	Description
OS Version	The OS version running on the device
Storage	The amount of unused storage on the device
Battery	Indicates the device's battery level (Requires iOS5+ for Apple Products)
Last Updated	The time the device last contacted the server
Owner	Users nominate during enrollment whether the device is corporate or personal.
First Name	Hidden By Default, this will display the users First Name as retrieved from LDAP.
Surname	Hidden By Default, this will display the users Surname as retrieved from LDAP.
Supervised	Hidden By Default, this will display "Yes/No" depending on whether the device is Supervised or not.
Samsung KNOX	Hidden By Default. This indicates whether the device is Samsung KNOX Capable.
Actions	The actions that can be performed on the device (see below)

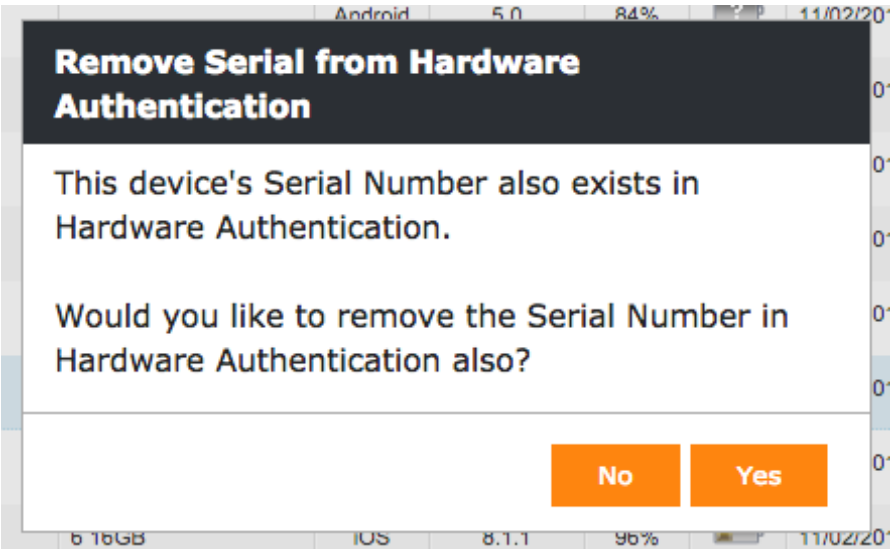
4.1.2. Managed Actions

Action	Icon	Description
Tags		Edits the current set of Tags associated with the device. – see 'Tags' section.
Lock		Activates the Screen Lock on the device. Prompts for extra optional information on iOS 7.
Block		Moves the Selected Device to the Blocked Container – Removing any Corporate Data or Apps associated with Silverback from the device.
Wipe		Hard resets the device and is restored to default factory settings, clearing all data and configurations from the device.
Delete		Deletes the Selected Device from Silverback – Removing any Corporate Data or Apps associated with Silverback from the device.

4.1.3. Delete Serial Number

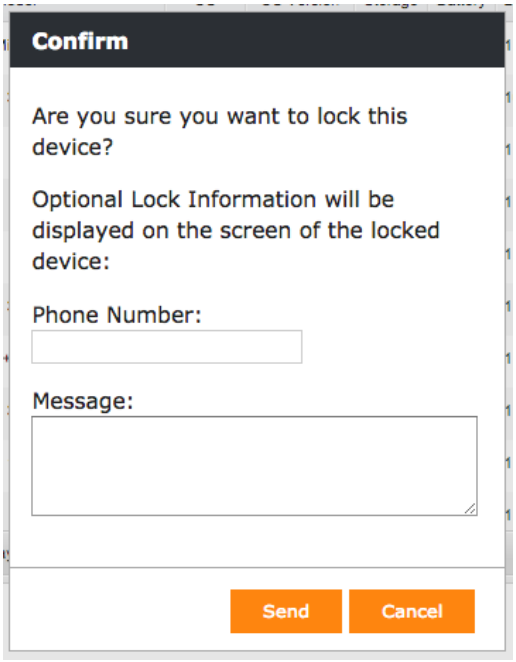
If the device being deleted, also has it's serial or IMEI number listed in Hardware Authentication, the Silverback administrator will be prompted to optionally remove this as

well. If you don't want to delete the serial or IMEI number from Hardware Authentication, you can dismiss this prompt.



4.1.4. Device Lock Information

If the device being locked is running iOS 7 or greater, the Silverback administrator will have extra options available when locking the device. The Silverback administrator will be prompted to enter a Phone Number and Message to be displayed on the device screen when locked. Both of these fields are optional.

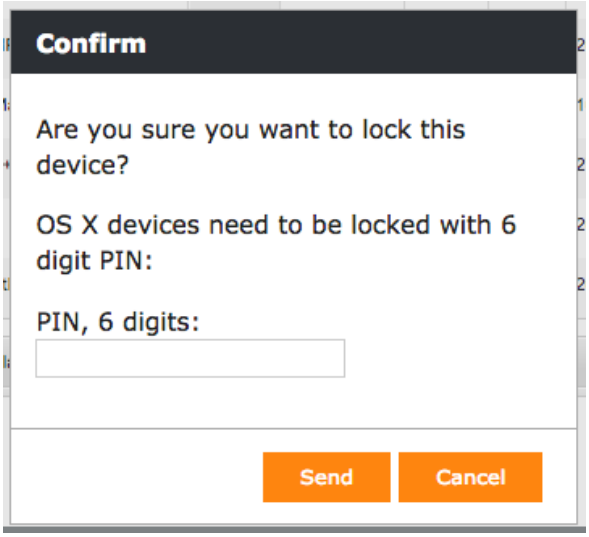


4.1.5. Device Lock Prompt for a Device Running iOS 7

When this lock is sent to the device, the information is shown on the screen. For iPhone devices, the person with access to the phone has the option to dial the number on the screen. Note that if the device does not have a passcode configured, this information will not show on the device.

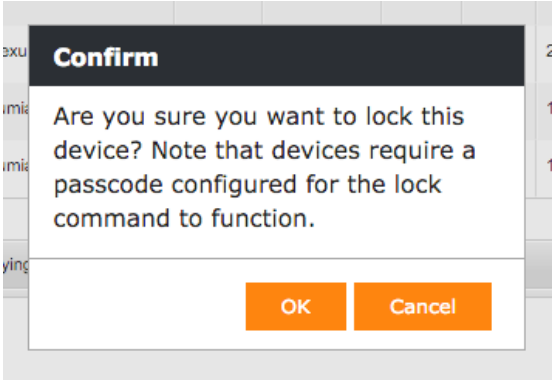
4.1.6. Device Lock Prompt for a Device Running OS X

OS X Devices require a pin code to be sent with the lock. When you click lock you need to enter this code. This code needs to be entered on the device to unlock it.



4.1.7. Device Lock Prompt for a Windows Phone device

Windows Phone devices require a passcode to lock. When you perform a lock you will be prompted.

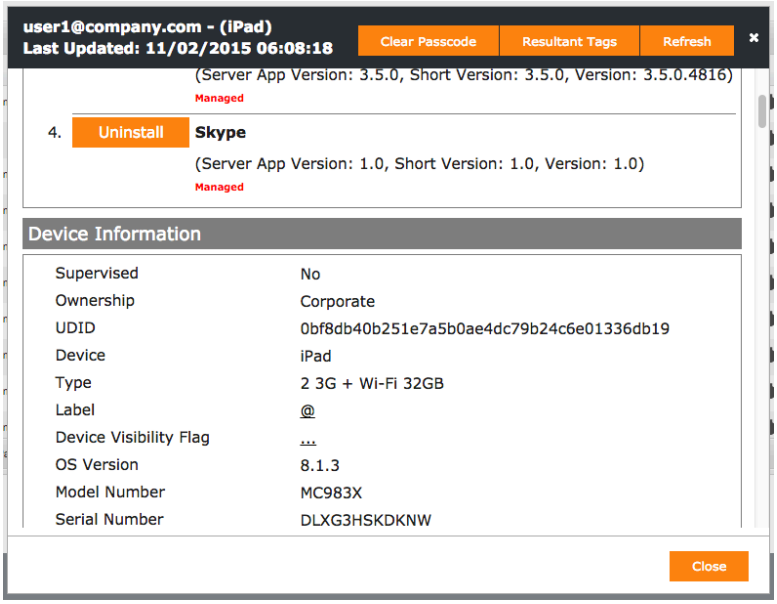


4.1.8. Individual Device Information

To view information about an individual device, simply click on the specified device and the Device Information window will present itself.

From this screen, the Silverback Administrator can view the device's information, request information updates, block or unblock the device, manage applications and clear the passcode on the device.

The Device Information list is generated using the latest information from the time the device last checked in, and will only display information that the device OS makes available.



Viewing the Device Information of a specific device will present the administrator with specific device information as well as a 'Managed Application List'.

NOTE: Managed Application List applies to iOS 5 (or higher) devices only, and allows the Administrator to send prompts to the Selected Device, asking the user to 'Install the App'. These Apps are read from the Silverback App Portal, and the Status associated with them is updated on the Installed Applications list.

NOTE: The Clear Passcode Feature can be disabled – please ask your Silverback Engineer if you want this disabled.

NOTE: If the Passcode setting has been activated and someone sends a Clear Passcode command to a device, it will prompt the user to input a new passcode as soon as it is unlocked.

4.1.9. Individual Device Information – Details and Information

Detail	Description
Reset KNOX Password (Samsung SAFE Only)	Will reset the password on a KNOX Container
Message	Sends an individual APNS message to the device with Companion installed
Clear Passcode	Clears the Passcode on the device
Refresh	Refreshes the Device Information
Resultant Tags	Displays a new window outlining the combination of all tags on the selected device. – see 'Tags' section
Managed Application List (iOS Only)	Lists all the Applications currently installed on the device.
Device Information	Hardware Information about the device
Network Information	Cellular Network Information relating to the device
Restrictions Information	Lists the restrictions Silverback has in place on the device
Security Information	Details information about state of security on the device
Single Application Mode Profile	If enabled for the device, allows you to override Single App Mode Status on the device.
Profile List	Lists all Configuration Profiles installed on the device
Provisioning Profile List (iOS Only)	Lists all the Provisioning Profiles installed on the device
Certificate List	Lists SSL Certificates installed on the device
Application List	A list of all applications installed on the device.
Available OS Updates	A list of Updates available for iOS and OS X Devices
OS X User Information	Displays information about the user on the device for OS X devices.

4.1.10. Blocked Devices

A Blocked Device has had the Corporate Mail Account and any other Privileges from the device issued via Silverback removed. The device is still managed and will maintain any security policies and device restrictions that have been put in place. Devices that are blocked are moved from the **Managed Devices to Blocked Devices.**

The information displayed in the Blocked Devices view mirrors that shown in managed devices. However, administrators have access to different actions detailed below:

Action	Icon	Description
Unblock	⊕	Restores the Corporate Mail Account and any other Privileges that were removed from the device as well as any authentication certificates issued via Silverback.

NOTE: Devices with Companion installed will also receive a Message Notification when they move from Managed to Blocked.

4.1.11. Blocked Reason

Unblocking can be dependent upon rectification of policy violations. By clicking on a device in the blocked devices table you can view the device information and the list of policy violations.

Policy violations **appearing in red must be rectified** in order to be able to unblock the device. When policy violations in red are present, the unblock button is disabled. Policy violations in black do not prevent the device from being unblocked; however still display information about policy violations.

Policy violation **appearing in black are not critical,** this means that the device can still exist within the Managed container while violating the policy.

When the end user has rectified the policy breach on the device, the Administrator clicks ‘Refresh’ on the top right to refresh the device information to activate the Unblock button.

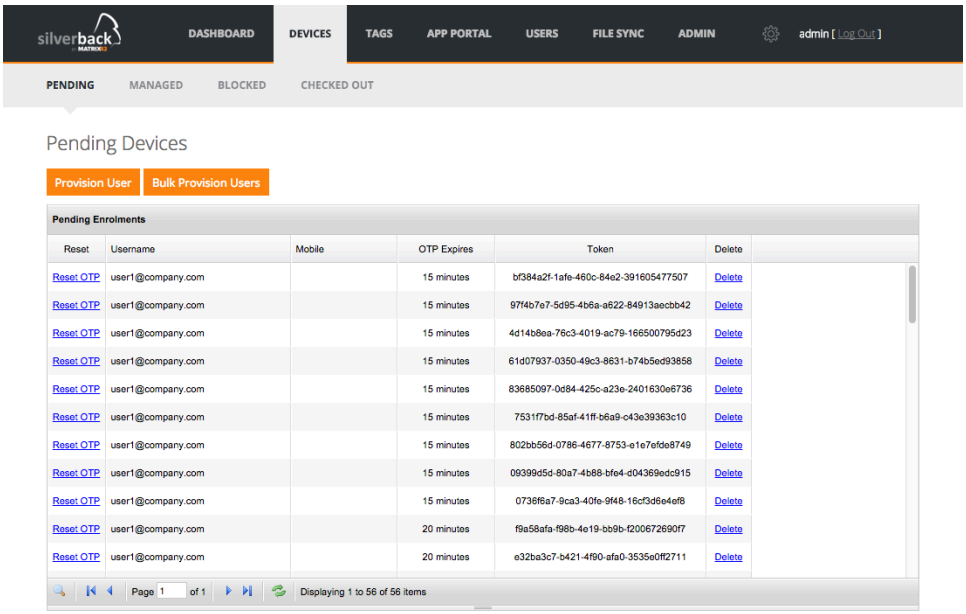
To Unblock a device - Click on the Unblock button on the top right of the Device Information display.

4.1.12. Pending Devices

Once a user has created their Enrollment Request through the Silverback Self Service Portal, they will appear in the Pending container with their Username and the information associated with their current enrollment.

If the user for any reason forgets their OTP during the enrollment the Administrator can either Reset their OTP and inform the user of the new one, or simply Delete the Enrollment Request and ask the user to try again.

If the user enters in the wrong OTP then the Enrollment Request will be deleted and the user will also have to restart the enrollment request again. The Administrator can customize the content and length of the OTP in the Admin Section of the Silverback Console.

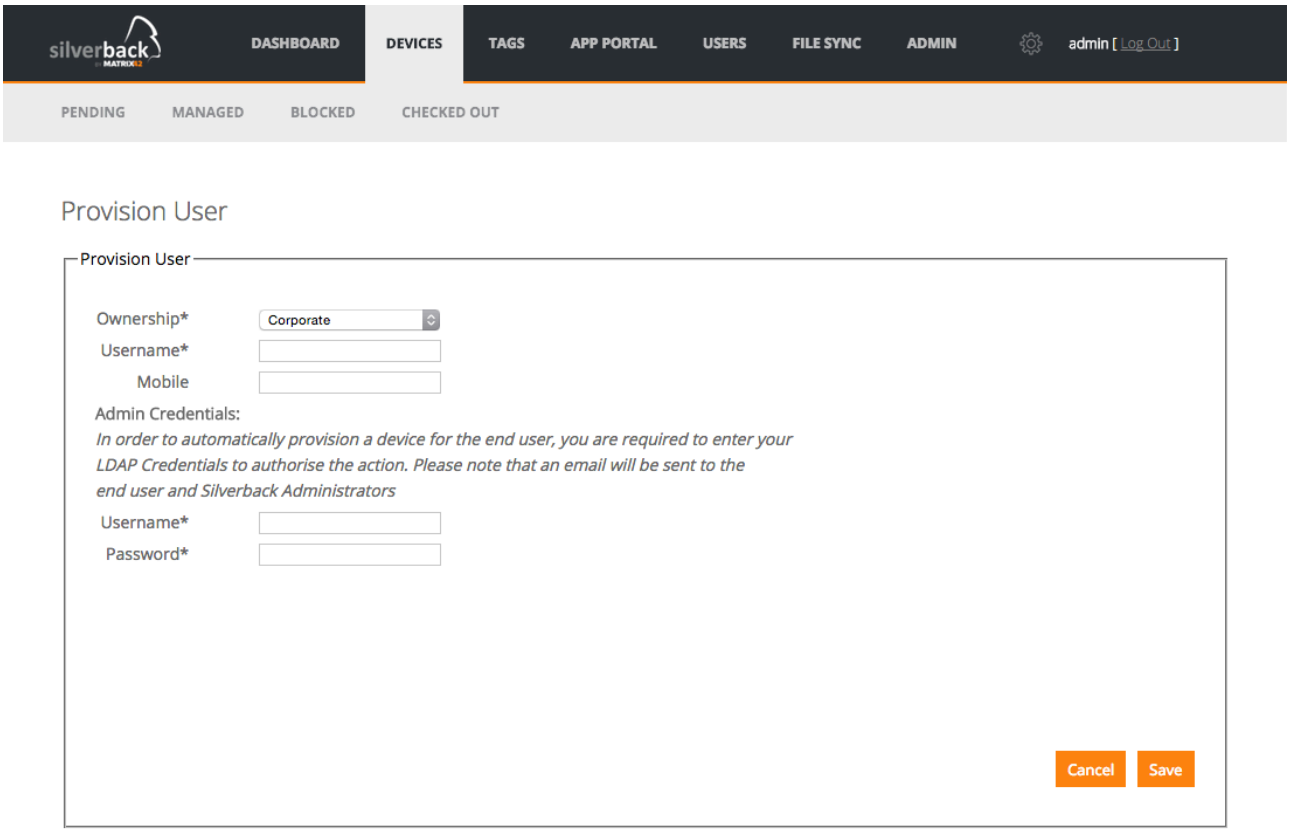


Detail	Description
Reset OTP	Reset the OTP – Generating a new one for the Admin on-screen
Username	Username associated with device attempting to be enrolled
Mobile	The Phone Number entered in the SSP during Enrollment
OTP Expires	The time remaining before the OTP expires
Token	The Unique ID for the Enrollment Request
Delete	Deletes the corresponding Enrollment Request

4.1.13. Provision User

An Administrator can setup a device on behalf of a user via the Provision User function. The administrator must specify the user's information and also provide valid LDAP credentials to validate the request. If Silverback is configured to use Username and Password authentication for things like Exchange ActiveSync, the user will still need to enter their password to synchronize once the device is enrolled.

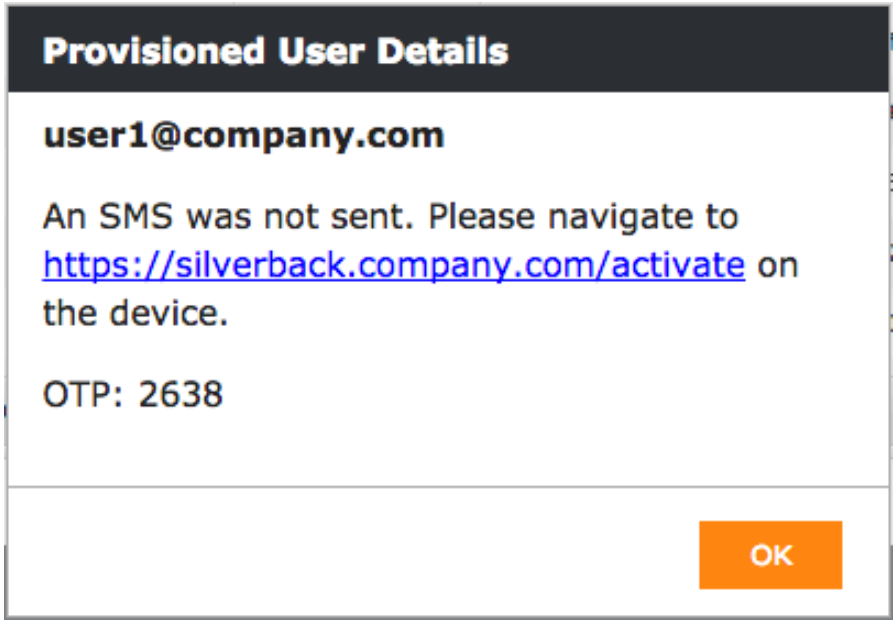
When a user has their device setup for them in this manner, an alert is sent to the user as well as all Silverback Administrators in the form of an email to provide an audit trail and record of the fact that a device has been provisioned on behalf of a user by a third party.



Detail	Description
Ownership	Set the ownership flag for the users device
Username	The Username of the user to enroll
Mobile	The Mobile Number of the user to enroll
Username	The administrator's LDAP Username in UPN format
Password	The administrator's LDAP Password

4.1.14. Provisioned User Details

Once the pending enrollment has been created for the user, the Administrator who created the enrollment will be presented with the user's OTP so they can complete the enrollment handshake. The enrollment process then proceeds as normal. Once the device has been enrolled, the configured device can then be handed to the user.



NOTE: If no mobile number is included with the Enrollment Request then you will need to manually visit the Activate Page on the target device.

NOTE: If a user has reached their Maximum Device Count Limit, an Administrator can override this restriction and provision another device using this method.

4.1.15. Bulk Provision Users

An Administrator can setup multiple devices on behalf of users via the Bulk Provision Users function. This allows a large number of enrollments to be created in a single run, to speed up large rollouts and simplify the process. When entering the Bulk Provision Users section, a table is shown displaying previous bulk enrollments that have been created.

Detail	Description
ID	Unique Identifier for the Bulk Provision request
Status	Status of the request. To indicate if it is still in progress, or available for download
Created Date	The date and time the Bulk Provision Request was created
Created By	The username of the administrator who created the request
Action	Allows an administrator to remove an existing Bulk Provision Request

4.1.16. New Bulk Provision

When creating a new request, the Bulk Provision Users settings page is shown. This page lets administrators configure the details of the bulk enrollment. After submitting all the details, the administrator can then submit the request, or cancel it. If submitted, the request is added to a queue, which the system will process sequentially, and the status of this can be seen from the previous page.

Detail	**Description**
Choose File	Field to upload the list of users to be provisioned. This is a CSV, with each row containing: username,email,mobile. Username is mandatory, whereas email and mobile are optional.
OTP Expiry	Number of hours the enrollments that are created will be valid.
Email User Details	Elect whether to send the user an email with the enrollment request details.
SMS User Details	Elect whether to send the user an SMS with the enrollment request details.
Define OTP	Elect whether to pre-define the OTP. Enabling this means every enrollment will have the same OTP.
OTP	Mandatory if “Define OTP” is enabled. This is the

Detail	Description
	OTP to be used for all enrollment requests.
Ownership	Set the ownership flag for the users device
Username	The administrator's LDAP Username in UPN format
Password	The administrator's LDAP Password

4.1.17. Bulk Provision Status

When a request is completed, the Status from the main page will let administrators Download the CSV file containing the details of each enrollment.

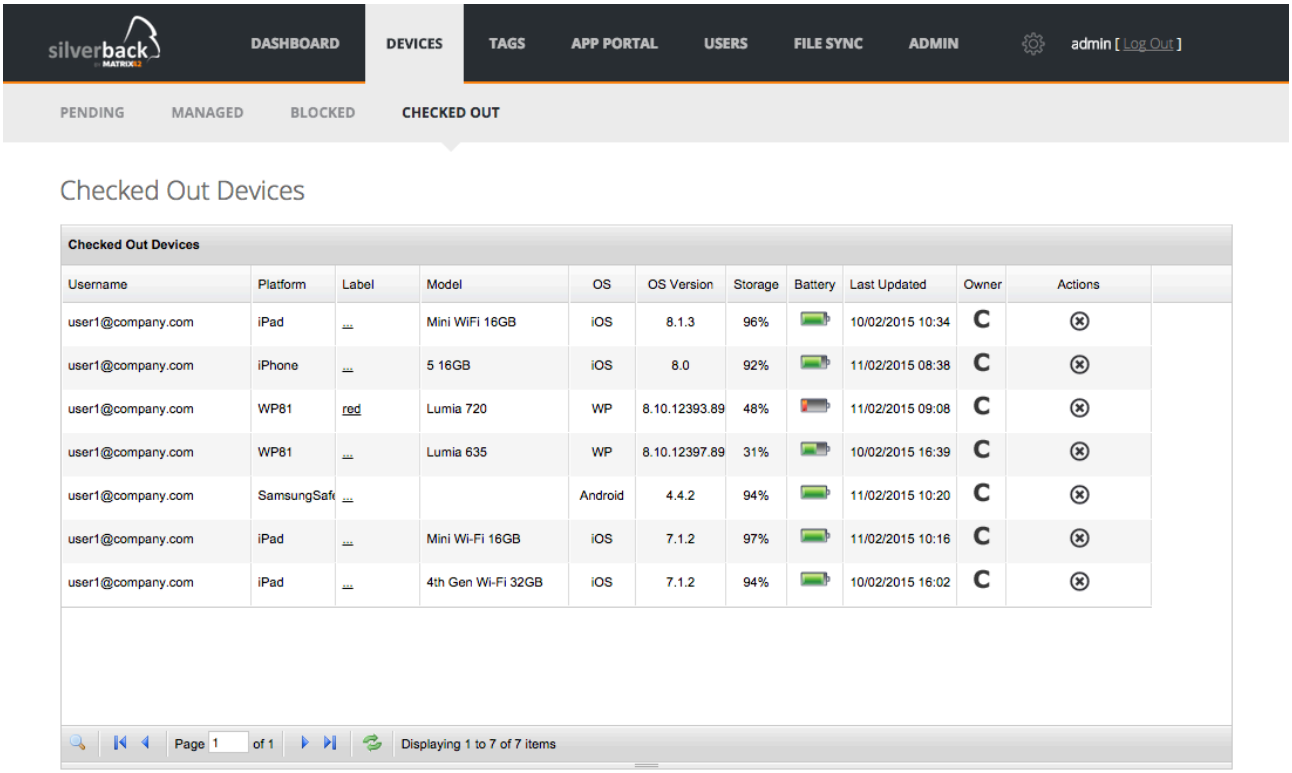
	A	B	C	D	E	F
1	Username	Email	Phone Number	Success	One Time Password	Reason for failure
2	user1	user1@company.com	40404040	TRUE	8741	
3	user2	user2@company.com	40404041	TRUE	5803	
4	user3	user3@company.com	40404042	TRUE	6082	
5	user4	user4@company.com	40404043	TRUE	8613	
6	user5	user5@company.com	40404044	TRUE	4278	
7	user6	user6@company.com	40404045	TRUE	3568	
8	user7	user7@company.com	40404046	TRUE	5612	
9	user8	user8@company.com	40404047	TRUE	4612	
10	user9	user9@company.com	40404048	TRUE	761	

Detail	Description
Username	Username for the pending enrollment
Email	Email for the pending enrollment
Phone Number	Phone number for the pending enrollment
Success	Indicates whether the enrollment was created successfully or not
One Time Password	The generated or pre-defined OTP for the enrollment
Reason for failure	If the enrollment failed, a reason will be indicated here

4.1.18. Checked Out Devices

In the event that a user has manually un-enrolled their device so that it is no longer under MDM control, Silverback will move this device from Managed or Blocked Devices into the Checked Out devices container.

Before deleting the device, it is best practice to contact the user and ascertain why they removed the MDM profile.



Username	Platform	Label	Model	OS	OS Version	Storage	Battery	Last Updated	Owner	Actions
user1@company.com	iPad	...	Mini WiFi 16GB	iOS	8.1.3	96%		10/02/2015 10:34	C	
user1@company.com	iPhone	...	5 16GB	iOS	8.0	92%		11/02/2015 08:38	C	
user1@company.com	WP81	red	Lumia 720	WP	8.10.12393.89	48%		11/02/2015 09:08	C	
user1@company.com	WP81	...	Lumia 635	WP	8.10.12397.89	31%		10/02/2015 16:39	C	
user1@company.com	SamsungSafe	...		Android	4.4.2	94%		11/02/2015 10:20	C	
user1@company.com	iPad	...	Mini Wi-Fi 16GB	iOS	7.1.2	97%		11/02/2015 10:16	C	
user1@company.com	iPad	...	4th Gen Wi-Fi 32GB	iOS	7.1.2	94%		10/02/2015 16:02	C	

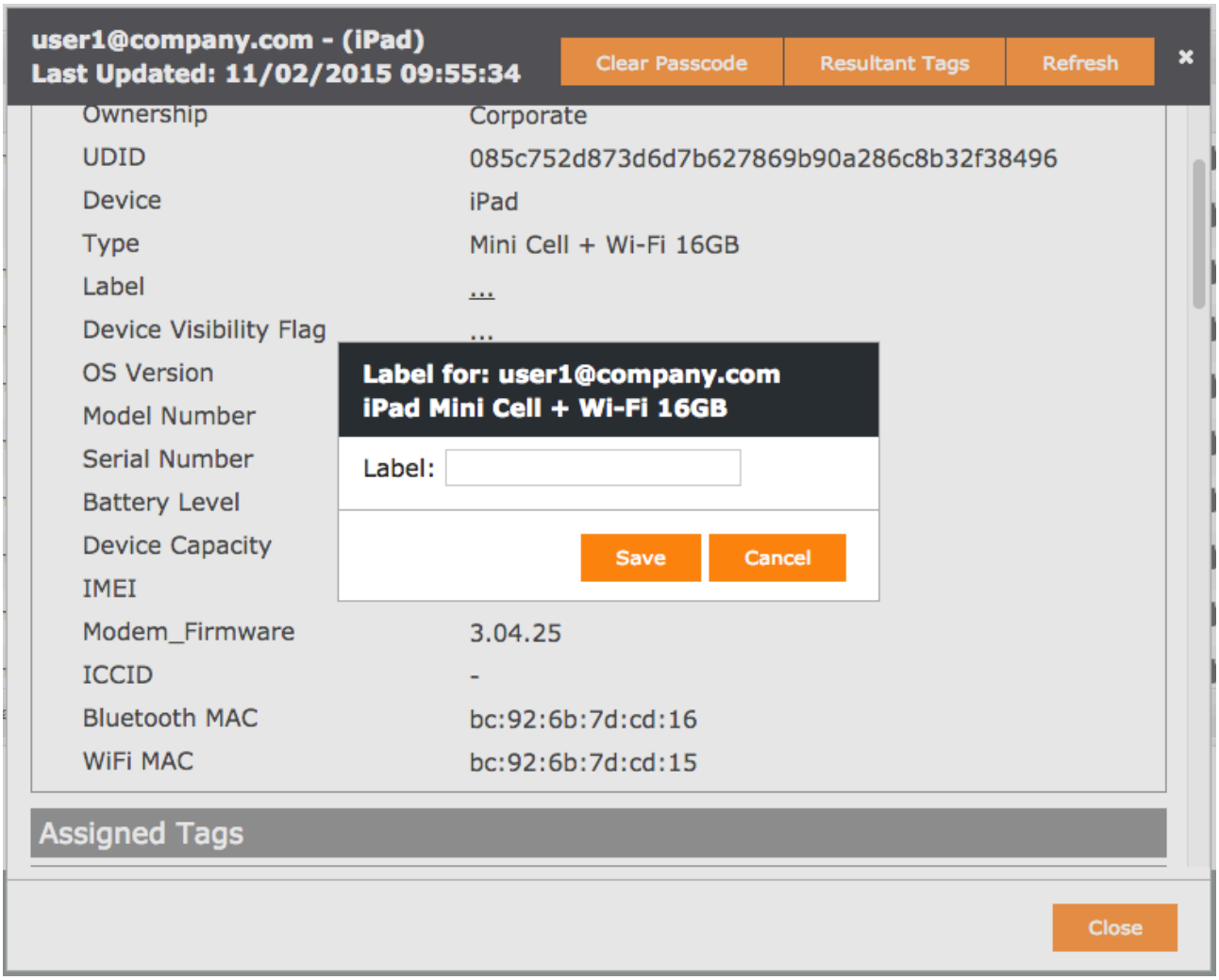
NOTE: Checked Out Devices still use a Device License, so be sure to clean out any stale devices you may find in here.

4.1.19. Device Labels

As it is possible to enroll multiple devices under the one username in Silverback, you can easily differentiate between these by adding a Device Label within the Silverback Console.

A Device Label can be applied either through the Manage/Blocked screen views, from within the Device Information Screen once a device has been enrolled. Using this method, the Device Label will stay associated with the device as long as the device remains in the system.

An alternative way to assign a Device Label is to associate it with a Device Serial Number in the Hardware Authentication section of Silverback. Applying a Device Label using this method will enable the console to constantly remember the label even if the device is temporarily removed from Silverback.

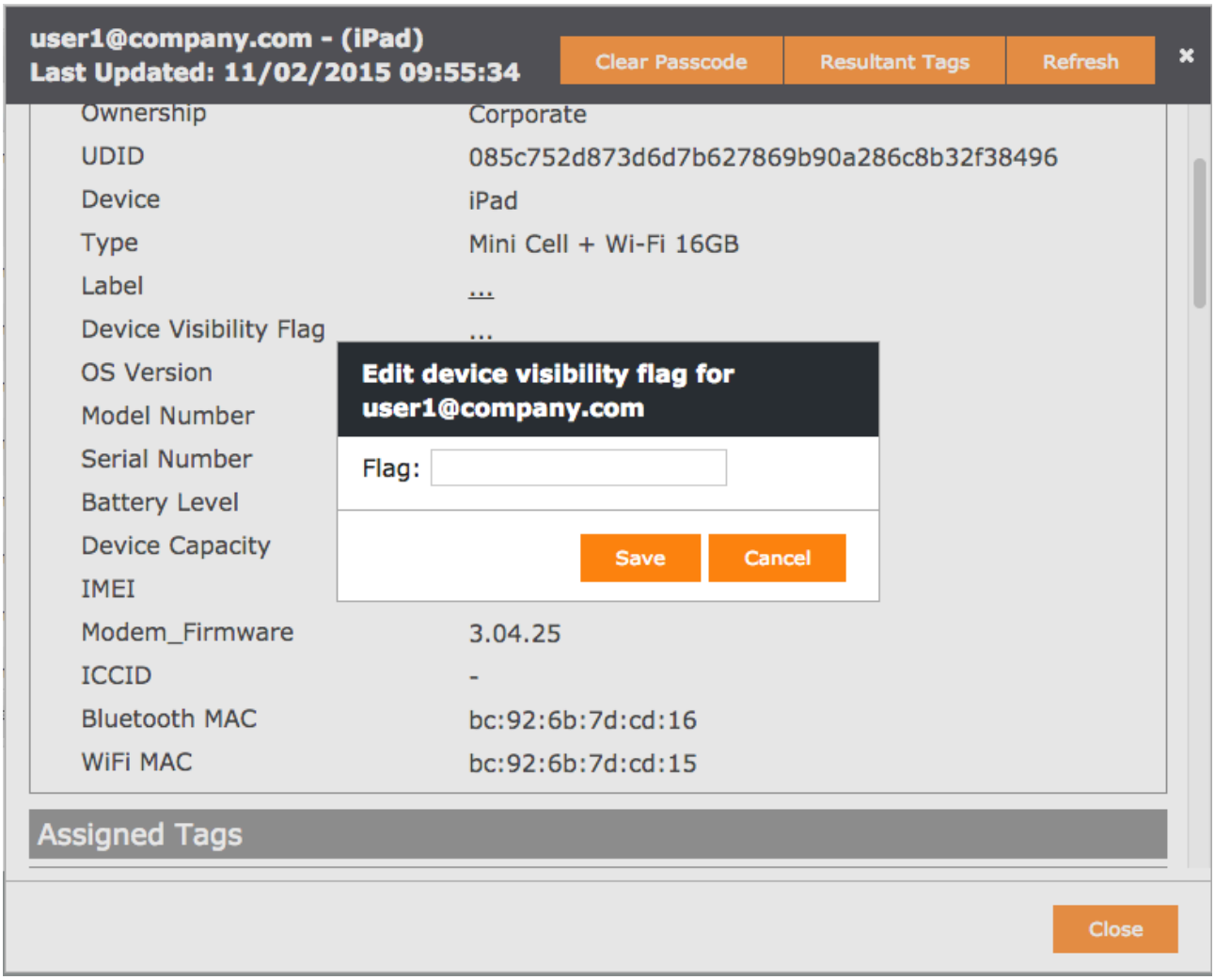


4.1.20. Device Visibility Flags

Using the Visibilty Flags assigned to administrators, it's possible to determine what devices administrators can see in the console.

The flags can be assigned when importing serial numbers into the system, or also by editing them in the device information popup.

The function for assigning these to administrators is explained later in the document.



5. Tags Tab

Tags offer an extremely dynamic way of managing different 'Groups' of devices. Using the base SYSTEM Tags that are created by default with the Silverback Installation, an administrator can create a 'Base Level' of settings for devices as they enter the system.

It is important to understand the concept of how the Tags system works so that you can effectively manage the security of your Silverback Installation.

There are currently 9 SYSTEM Tags that are installed by default for a Silverback Installation, these are:

- iPhone
- iPad
- iPod
- Android
- Samsung SAFE
- WP8 (Windows Phone 8)
- WP (Windows Phone 8.1 +10)
- Windows (Windows 8.1 + 10)
- OS X

Basic Concept

1 User Enrolls their Device

2 Silverback detects the Device Type and associates it with its SYSTEM Tag.

3 The Device then has all SYSTEM settings applied to it and is checked to ensure it is compliant with the SYSTEM policies. (Settings and Policies for each Device Type are covered later in their respective sections).

4 Once the device has been enrolled into Silverback and exists in either the Managed or Blocked container Administrators can assign it to additional Tags. These additional Tags will simply overlay their settings over the top of the SYSTEM Tags – which outlines the 'layered' approach to Device Security.

5 Administrator associates the additional Tag with enhanced Restrictions to the Target Device.

6 The Device receives updated settings that incorporate settings from both sets of Tags.

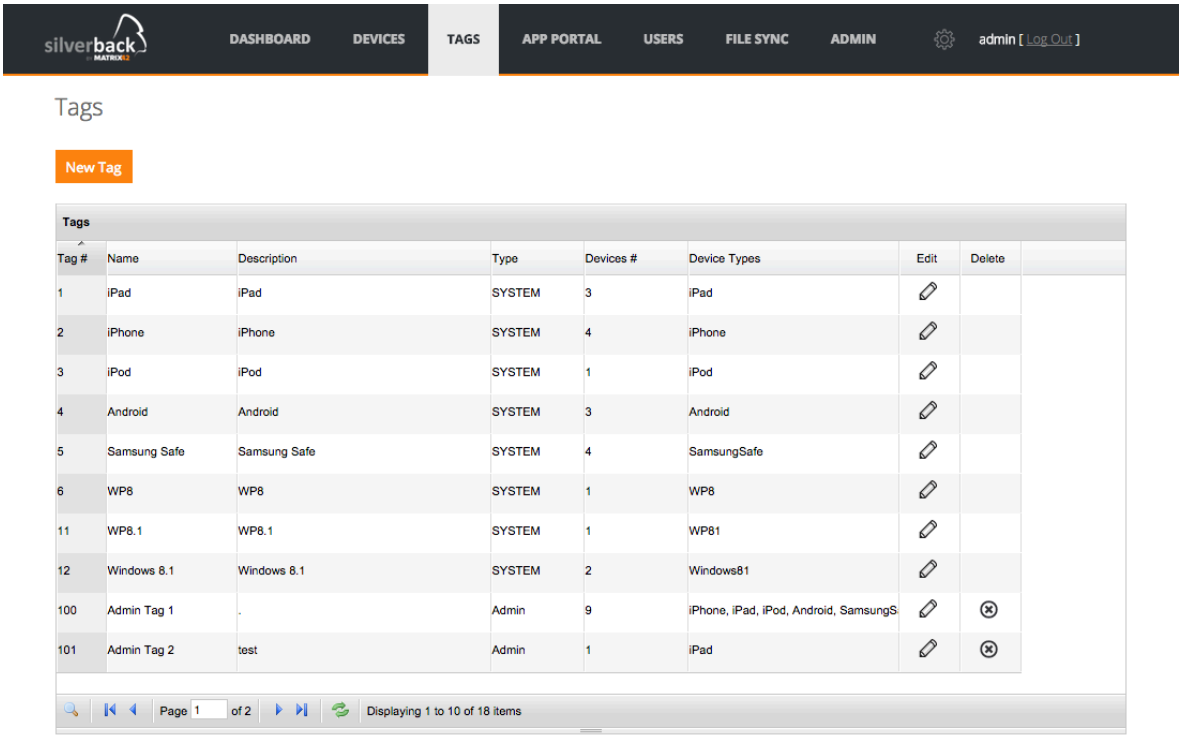
The end result is that the device will contain settings from both Tags, below is a quick example of Passcode Settings being applied via 2x Tags (System & Enhanced Security).

	SYSTEM TAG (Default)	ENHANCED SECURITY	DEVICE SETTINGS
Passcode Enabled	**X**	**X**	**X**
Allow Simple	**X**		
Require Alpha Numeric		**X**	**X**
Min Length	**4**	**7**	**7**
Min Complex Characters	**n/a**	**2**	**2**
Max Passcode Age	**0**	**30**	**30**
Auto-Lock	**5**	**2**	**2**
Passcode History	**0**	**2**	**2**
Grace Period	**5**	**2**	**2**
Failed Attempts	**10**	**5**	**5**

5.1. Tags

The Tags screen will list all the currently 'active' tags within the Silverback Environment, even if they do not have any devices associated with them. The SYSTEM Tags will be created by default upon Silverback Installation as there is one for each particular device that Silverback supports; the iPad, iPhone, iPod, Android and Windows Phone.

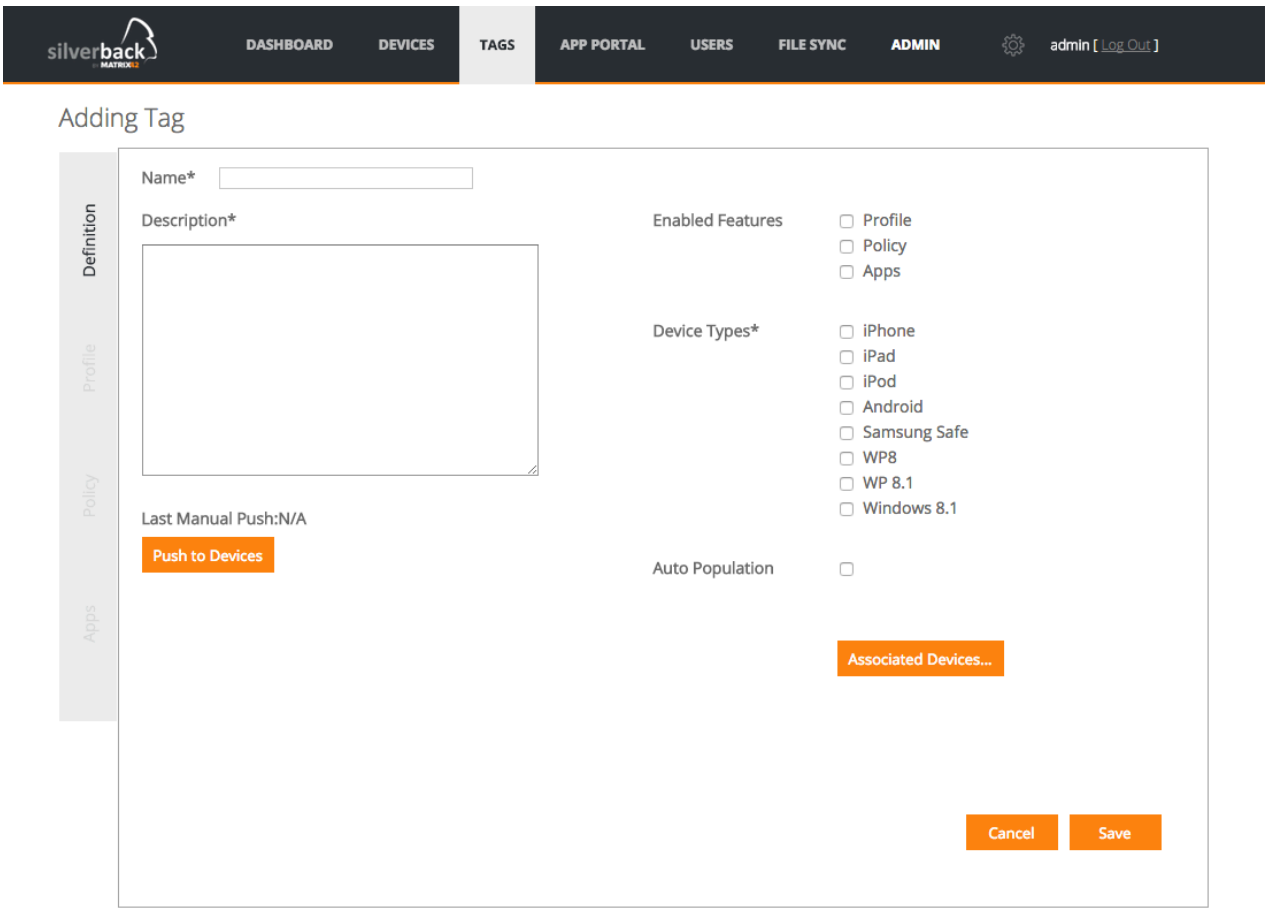
These Tags define the 'Baseline of Security' for your system, as each device is enrolled – they receive the settings in these tags.



Detail	Description
New Tag	Takes the Administrator to the Add Admin Tag screen.
Tag #	The ID Number of the Tag
Name	The Friendly Name associated with the Tag
Description	A General Description of the Tag
Type	The Type of Tag. (SYSTEM or ADMIN)
Devices #	The Number of Devices associated with it.
Device Types	The Types of Devices that the Tag is designed for.
Edit	Edits the Selected Tag
Delete	Deletes the Selected Tag.

5.1.1. Adding an Admin Tag

Adding additional Admin Tags allows Administrators to specify Groups or levels of security to their Silverback Installation. Once a Device is enrolled it should already have its 'Base Level of Security' so Administrators can now create additional Tags and apply these to Selected Devices which will then receive the updated settings.



Once you've named your Tag and filled out the required information, click the Save button to then continue defining other Settings and Policies intended for this Tag. – see next section 'Defining Individual Tag Properties'.

NOTE: The 'Push to Devices' and 'Associate Devices' buttons are not currently available in this screenshot as the Tag has not been saved yet and does not exist and cannot affect Enrolled Devices.

Detail	Description
Name	The Friendly name associated with the Tag you're creating.
Description	A short description of the Tag and its intended purpose.
Enabled Features	What the Tag is capable of doing, adjusting individual Profile, Policy and App settings.
Device Types	The Device Types that this tag is intended to effect.
Auto Population	Enables the 'Auto Population' feature of this Tag.
Device Variable Key	The Variable that Silverback monitors enrolling devices for to determine to auto-apply this tag.
Device Variable Value	The Custom Value that Silverback compares against the Device Variable for determining devices that apply this tag.
Edit	Changes the Selected Ownership of Devices associated with this Tag
Associated Devices	A button that displays a list of Currently Enrolled Devices for the Administrator to select for association with this Tag.
Cancel	Cancels the creation of this Tag
Save	Saves the Tag and its current settings.
Push to Devices	Button that will send a signal for all devices associated with Tag to 'Phone Home' and check in for updated settings.

5.1.2. Tag Auto-Population – Device Conditions

Once an Admin Tag has been created, you can set up conditions so that devices enrolling into Silverback are auto-assigned upon enrollment. Using the information captured during enrollment, Silverback will determine if the incoming device needs to have Tags associated with it.

The conditions that Silverback will monitor are listed below:

- Device Type
- OS Version
- Model Number
- Current Country
- MDM Version (SAFE Only)

- Current Cell Network
- Subscriber Country
- Subscriber Network
- Populated Device Label
- Device Label
- Roaming Devices
- IP Address
- iTunes Account Present
- Wi-Fi SSID

5.1.3. Device Variable Logic Operators

The Device Variable field does not always have to be 'absolute', by using a wildcard (*) character in the Device Variable Value field the scope of the Auto-Population is widened to allow more devices.

Operator	Function	Purpose
*	Wildcard	Allows the Administrator to specify Wildcards when filtering devices.
>	Greater Than	Used for Numerical Fields, will allow the Admin to specify values Greater than a value.
<	Less Than	Used for Numerical Fields, will allow the Admin to specify values Less than a value.

Device Variable Key	Description
Type	Device Model Name (e.g. Lumia 620)
OS Version	The OS version reported by the device (e.g. 6.1.3)
Model Number	Device Model Number (e.g. MD543X)
Current Country	Device Current Country (e.g. Australia)
Current Network	Device Current Network (e.g. OPTUS)
Subscriber Country	The country that the device reported on enrollment (e.g. Guam)
Subscriber Network	The network that the device reported on enrollment (e.g. Telstra)
Label	Device Label as specified in the console
Roaming	The tag is assigned to roaming devices
IP Address	The IP address of the device(e.g. 192.168.1.100/32) The acceptable formats are: Single IP address (10.10.1.1) IP range with hyphen (10.10.1.1-10.10.1.200) IP range using CIDR notation (e.g. 10.0.0.0/24) IP range using wildcard (10.10.1.*) **Note:** The IP addresses are captured during normal Silverback operation and are also reported by Companion.
SSID	The name of the WiFi SSID that device is connected to The acceptable formats are: Full SSID name (e.g. Airport) Wildcarded SSID name (e.g. Airp*) Multiple SSID values using + as delimiter (e.g. Airport+Linksys) **Note:** This value is only reported by Companion client
MDM Version	Samsung SAFE MDM Version for the device. (e.g. 4.1)
iTunes Account	For iOS devices, set to true or false to populate if the user has an iTunes account configured.

5.1.4. Tag Auto-Population – LDAP Filter

Auto Populating an Admin Tag can also be done using containers that exist within your LDAP schema (or Active Directory). This means that if you have setup distribution groups for individual departments, you can auto assign Tags based on these groups.

When adding an LDAP Filter it must be done in Full DN Syntax (Distinguished Name), which can be found using Active Directory User and Computers or another LDAP Browser. An example of Full DN Syntax is displayed below:

Full DN Syntax Example for a Sales Department Distribution group.

MemberOf=CN=Sales Department, CN=Groups,DC=Company,DC=com

In some scenarios, it is necessary to specify the Base DN where the filter should be performed. The Base DN should be entered into the text box provided, and is also specified in Full DN Syntax. When provided, this specifies where the filter should be applied.

The option for “Ignore Empty Results” will tell the server to not remove users from the Tag, if the response from LDAP is empty. In some scenarios an LDAP source can return a valid, successful result however without any LDAP results. Normally this would cause Silverback to remove all users from this Tag. If your LDAP source is returning empty results validly, then use this option to ensure minimal user interruption.

5.1.5. Defining Individual Tag Properties

Once you have saved your custom Admin Tag, it can be edited the same way as the SYSTEM Tags. The Highlighted Section on the side of the screenshot below contains the features that are being applied to this particular Tag, and the devices that will be associated with the Tag.

Each of the individual features can be broken down as follows:

- Definition The Setup and Overview of the Tag
- Profile Device Security and Privileges that will be sent to the device
- Policy Determines Device Security and Silverback Policy Settings.
- Apps Determines App Policy and Behavior on Subscribed Devices.

If not all of the Features are listed, then please ensure that you have them enabled on the Definitions page.

5.1.6. Exporting a List of Users from a Specific Tag

To Export a list of users associated with a specific Tag, use the following steps:

1. Log in to the Silverback Admin Console and navigate to the Tags section.
2. Edit the Desired Tag and click the 'Associated Devices' button. (You should see the screen below).
3. Click the Export button and choose the location to save the output file (in XLS Format).

5.2. Profile Feature

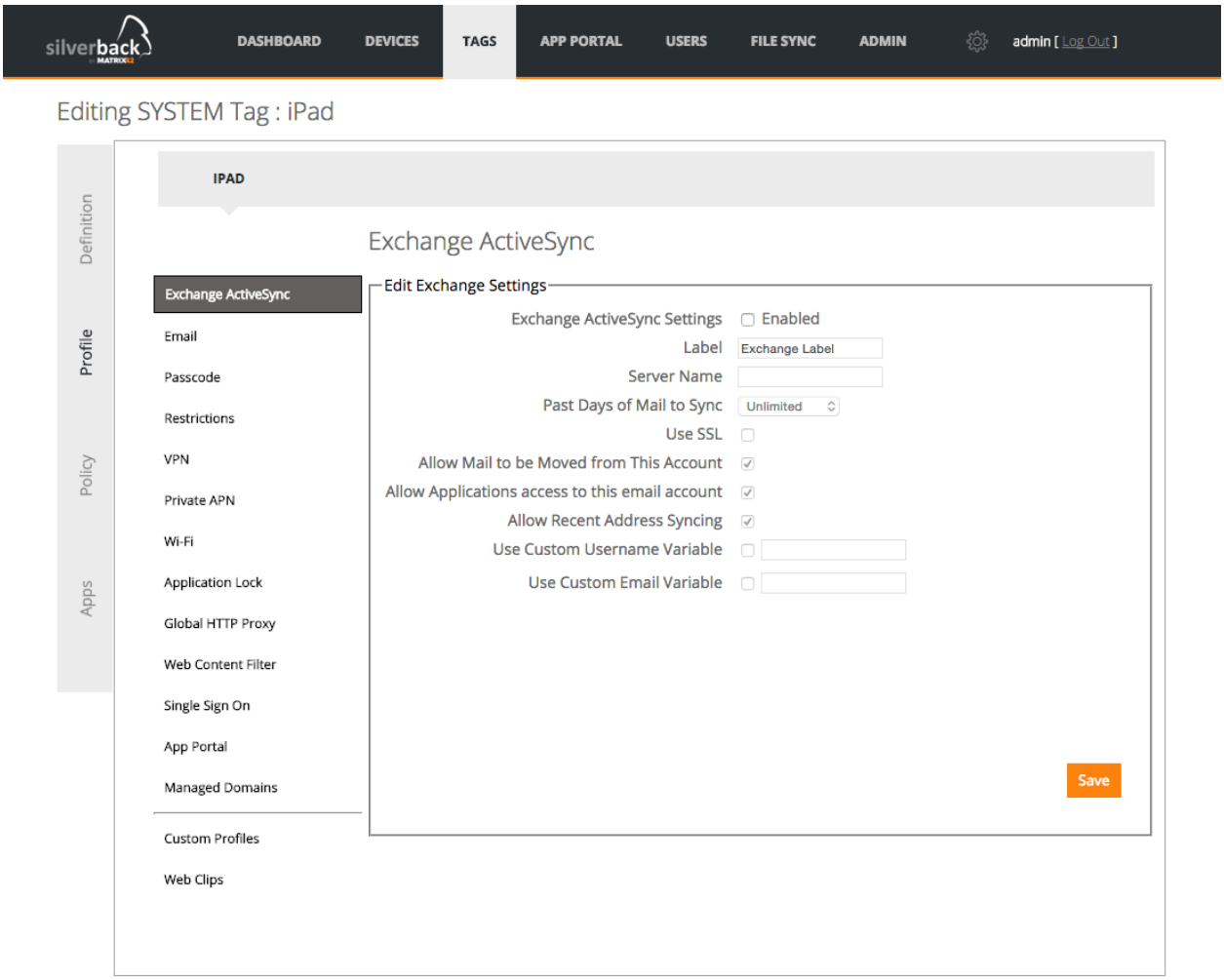
Profiles for each device type (iPhone, iPad, iPod, Android, Samsung Safe, Windows Phone 8, Windows Phone and Windows) are managed independently allowing separate configuration and management of profiles for each device type. When a device is provisioned, it will be provisioned with the profile configuration at the time the device was enrolled. When a profile change is made, new devices will receive the new configuration as well as devices that are currently managed and/or blocked.

The screens for the different device types are similar but not identical, and for this reason, only one of each screen is described below. As different OS types and devices have different capabilities, only the applicable functions for each device type are displayed within the respective Profiles.

When any Profiles are changed, ensure the settings are correct as these will be applied immediately to all applicable devices. Please ensure you click on the Save button on the bottom right of the screen to commit your changes before selecting another page.

NOTE: Care should be taken to note which platform is being affected when modifying policies through Silverback. The active device type that is being modified is in Orange. If the Profile Settings are available for your desired platform then it will be Grey with White Text. If the style is Grey with Black Text then the platform does not support that feature.

5.2.1. Exchange ActiveSync



Configuration	Description
Exchange Type	Only available for Samsung SAFE and Android devices. This determines if the Exchange settings should apply to the native email client (SAFE only), Gmail or within an Android for Work Container.
Label	The Label for the Email Account as it appears on the device.
Servername	The External Mail Server URL
Domain	The Internal Domain Suffix for the Exchange Server
Sync Interval	How often the Device is due to Synchronize the Mail Account Configured.
Past Days of Mail to Sync	Period of mail to synchronize to the device
Use SSL	If the URL for the External Mail Server is protected by an SSL Certificate then use SSL.

Configuration	Description
Allow Mail to be moved from this account (iOS Only)	If disabled, prevents the user forwarding emails from Corporate Email using a secondary email account
Allow Applications access to this email account (iOS Only)	If disabled, prevents the user from using this email account in third-party apps to forward content
Allow Recent Address Syncing (iOS Only)	If disabled, no email addresses are replicated for contacts that were recently used but do not exist in the standard Contacts list.
Use Custom Username Variable	Define a Custom Variable Attribute for the Username for the EAS Profile.
Use Custom Email Attribute	Define a Custom Variable Attribute for the Email Address for the EAS Profile.
Path (OS X Only)	Specifies a different path for the Exchange client to connect
Port (OS X Only)	Specifies a different port for the Exchange client to connect to
External Host (OS X Only)	If the external network address is different, you can specify this. This ensures the user will sync mail in the office and at home if the URLs are different
External SSL (OS X Only)	Determines if the external connection should use SSL
External Port (OS X Only)	Sets the external TCP port the Exchange Client should use
External Path (OS X Only)	Sets the external path for the Exchange client
Peak Schedule (SAFE Only)	Sets the default behaviour for the “Peak” period.
Off-Peak Schedule (SAFE Only)	Sets the default behaviour for the Off-Peak period.
Peak Start Time	Sets the time of day in hours that the Peak period starts.
Peak End Time	Sets the time of day in hours that the Peak period ends. Outside of these two settings is considered “Off-Peak”.
Peak Days	Which days should use the Peak settings. Days not selected here will be considered Off-Peak.
Max Attachment Size (bytes) (Android for Work Only)	Sets the maximum size in bytes that users can send attachments. This is for Android for Work Exchange profiles only.
Trust All Certificates (Android for Work Only)	Required for client certificate authentication with the Gmail app, if the device doesn’t trust the certificates correctly.

NOTE: For Exchange settings on Android device types, this requires Android for Work configured and the Managed Profile enabled for this Tag.

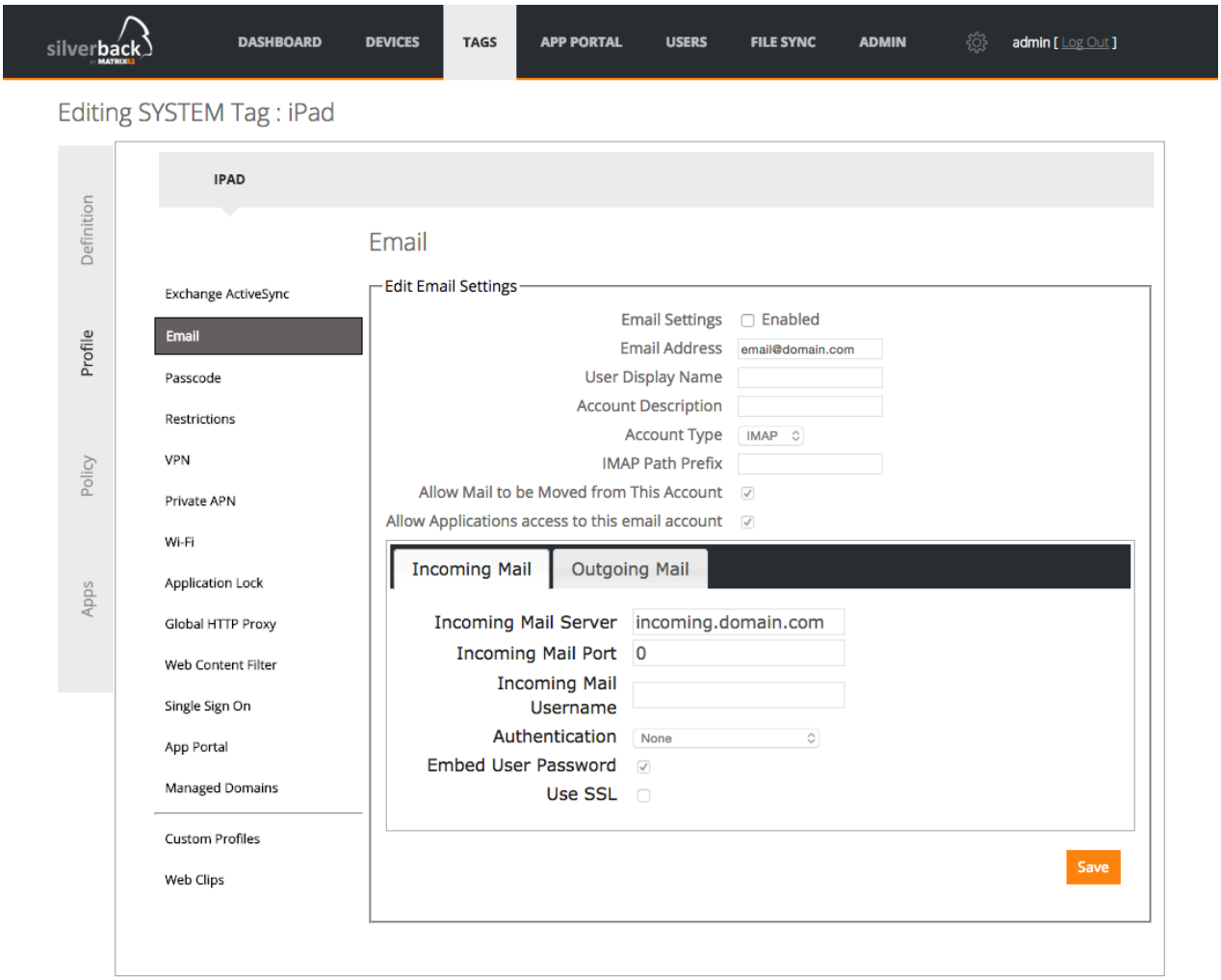
NOTE: For OS X, the additional Path, Port and External Exchange server settings must be configured correctly or the device will reject the profile, and will move to blocked. Most environments will not need these settings, but if you do, ensure the settings are correct.

NOTE: To dynamically populate the Email Address and Username fields use the Custom LDAP Attributes feature. This is explained in greater detail in Appendix: Custom LDAP Attributes

5.2.2. Email

Some device types have the ability to have additional email accounts configured via Silverback.

Silverback by Matrix42 Admin Guide Version 5.1 U3



Configuration	Description
Email Address	The Email Address of the Account
User Display Name	The Display Name of the User for this Email Account
Account Description	The Friendly Name of this Email Account
Account Type	Toggles between IMAP and POP Account Types
Domain (WP8 Only)	The Internal Domain Suffix for the Mail Server
Auth Name (WP8 Only)	The Username used when performing authenticating.
Auth Password (WP8 Only)	The Password used when authenticating.
Sync Interval (WP8 Only)	How often the device should check for new Mail Items.
Allow Mail to be moved from this account (iOS Only)	If disabled, prevents the user forwarding emails from Corporate Email using a secondary email account
Allow Applications access to this email	If disabled, prevents the user from using this email account in third-party apps to forward content

Configuration	Description
account (iOS Only)	
Incoming Mail	Server settings for the Incoming Mail Server
Outgoing Mail	Server settings for the Outgoing Mail Server

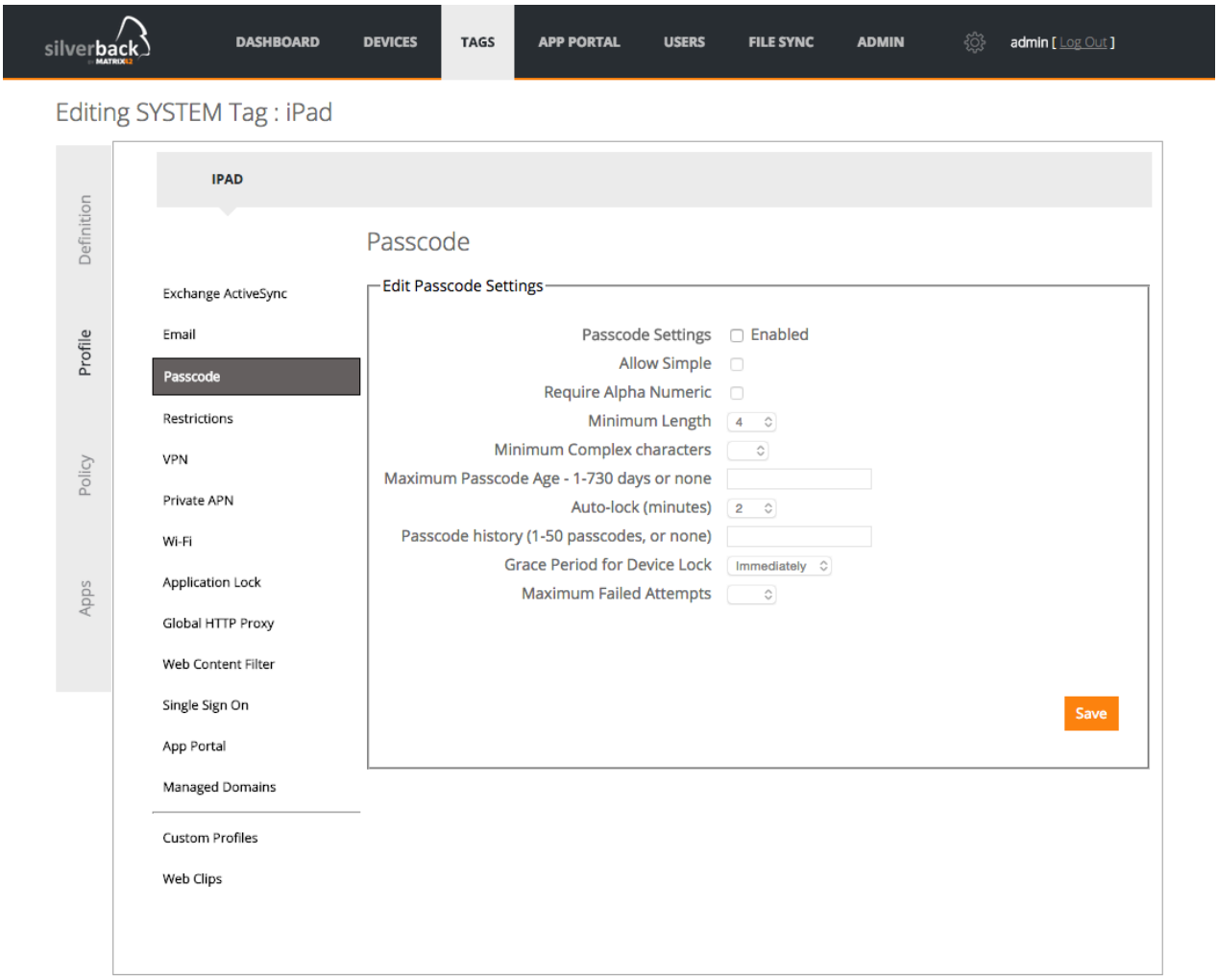
NOTE: Only the 'iOS Device Family', OS X, WP8 and WP currently support adding additional email accounts.

NOTE: To dynamically populate the Email Address and User Display Name fields use the Custom LDAP Attributes feature. This is explained in greater detail in Appendix: Custom LDAP Attributes

5.2.3. Passcode

Passcode settings control how strict the device's security settings are for the user to access their phone. This is either when first turning on their device or when 'unlocking' it from a prolonged period of inactivity.

Silverback by Matrix42 Admin Guide Version 5.1 U3

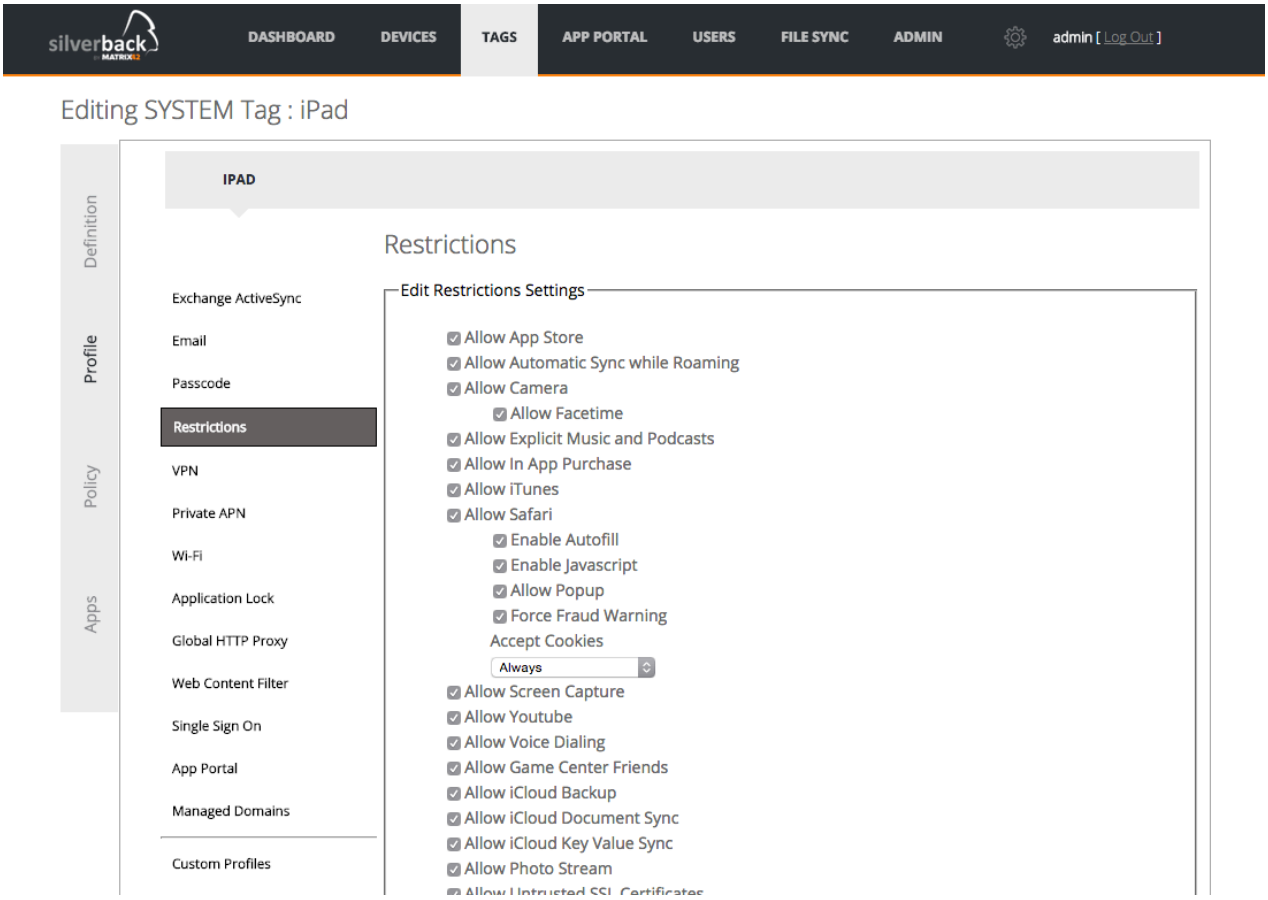


Configuration	Description
Passcode Settings	Enforces the Passcode Policy on selected devices.
Allow Simple	Permit the use of repeating, ascending or descending characters
Require Alpha Numeric	Require passcodes to contain at least one letter
Minimum Length	The smallest number of passcode characters allowed
Minimum complex characters	Smallest number of non-alphanumeric characters allowed. If ‘Allow Simple’ is checked, then this configuration is disabled.
Maximum passcode Age (days)	How often passcode must be changed.
Auto lock (minutes)	Device automatically locks due to inactivity after this time period.
Passcode history	The number of unique passcodes required before reuse.

Configuration	Description
	User cannot reuse same password again until X passwords have been used)
Grace Period for device lock	Amount of time device screen can sleep before device locks.
Maximum failed attempts	Number of passcode entry attempts allowed before **the device is reset to factory settings**
Complexity (Windows)	Character groups that required to be used in the User's passcode

5.2.4. Restrictions

Certain Platforms have other Restrictions built into their Operating System that Silverback can interact with to change the device's security and interface. This screen will change dynamically depending on the Device Type selected.



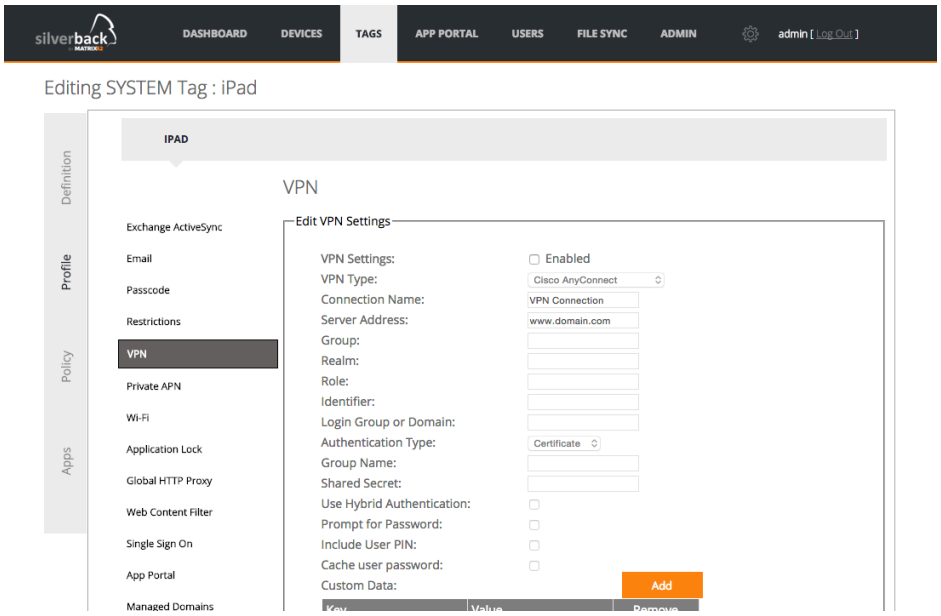
To allow a function for the desired device type, simply ensure the corresponding checkbox is ticked and click Save at the bottom of the page.

NOTE: For the iOS platform; In the event that 'Allow App Store' has been disabled, users will still be able to install approved applications from within the Silverback Application Portal.

NOTE: iOS Restrictions located in '*Supervised Devices Only' section require the device to be configured in 'Supervised Mode' via the Apple Configurator, or via Apple DEP Enrollment.

5.2.5. VPN

Silverback also has the ability to send Virtual Private Network (VPN) settings to managed devices, giving the device a secure tunnel to either their corporate network or for their entire Internet browsing experience.



NOTE: This feature of Silverback is only configuring a client device for an existing VPN configuration. Silverback does not work as a VPN itself.

The settings on the next page are for the accompanying screenshot. These settings may differ depending on the VPN Type selected and will update automatically, as each VPN Type may require unique settings.

The list of Supported VPN Types:

Check Point Mobile VPN

CISCO AnyConnect

F5 SSL

IPSec (CISCO)

Juniper SSL

SonicWall Mobile

Custom SSL

IKEv2

Configuration	Description
VPN Type	Selects the type of VPN being configured
Connection/Profile Name	The name given to the connection settings
Server Address	The FQDN of the VPN Appliance
Authentication Type	Configures Certificate or Username & Password authentication methods
Cache User Password	Tells the VPN profile to cache the individuals password once entered **(only available if Authentication is set to Password)**
Enable VPN on Demand	Enables the VPN on Demand Feature **(only available if Authentication is set to Certificate)**
VPN on Demand Matrix	FQDN Matrix where administrators can set specific VPN conditions or rules for certain Internet addresses and locations
Enable Per-App VPN	Allows a UUID VPN profile generation **(iOS7 only).**
Enable Dial On-Demand for Apps	Enables the UUID VPN profile generation per managed apps bundle ids **(iOS7 only).**
Application Matrix	Allows the administrator to add the managed apps distributed by the same tag to the per-app VPN UUID profile generation **(iOS7 only).**
Proxy Type	Enables and sets a proxy for the VPN connection
Proxy Server URL	The Proxy Server URL
Proxy Server FQDN	The Proxy Server FQDN
Proxy Port	The Port number to connect to the proxy server on
Use Individual Usernames	Sets user-level authentication for the proxy server
Group Username	General username for the proxy server

iOS VPN Settings

Configuration	Description
VPN Settings	Enables and Disables VPN for the Tag
VPN Type	Determines which VPN client will be used.
Profile Name	Name of the VPN Profile visible to the user on the device
Authentication	Currently limited to EAP **(WP)**
Use Custom EAP Thumbprint	Allows the definition of a custom EAP thumbprint **(WP)**
Enable Proxy	Enable or disable a proxy for the VPN **(WP)**
Bypass Proxy for local addresses	If enabled, the device will not use the proxy for addresses local to the device's network **(WP)**
Proxy Server	Address of the proxy server. **(WP)**
Proxy Port	The port the proxy server is listening on. **(WP)**
Tunnel Type	Whether the VPN should be established automatically or manually **(Windows)**
All User Connection	Allow all users of the device to use the VPN Profile **(Windows)**
Enable Auto Trigger	Should the VPN be automatically triggered **(Windows)**
Remember Credentials	Cache credentials if authentication is successful **(Windows)**
Use Win Logon Credentials	Use the user's windows login credentials **(Windows)**
Idle Disconnect Time	Idle time before disconnect **(Windows)**
Network Allowed List	The CIDR ranges of IP Addresses that will be protected by the VPN connection.
Namespace Allow List	The list of domain zones protected by the VPN connection.
DNS Suffix Search List	The list of DNS suffixes to try for non-qualified server name resolution.
Root CA Certificate	The root certificate for server trust. This is required for the client to establish trust with the server and it's issued certificate
Intermediate CA Certificates	If used, an Intermediate CA can be specified here, or multiple
CA Certificate Thumbprints	Additional CA Certificate thumbprints that the device should use to establish trust for the server VPN certificate.

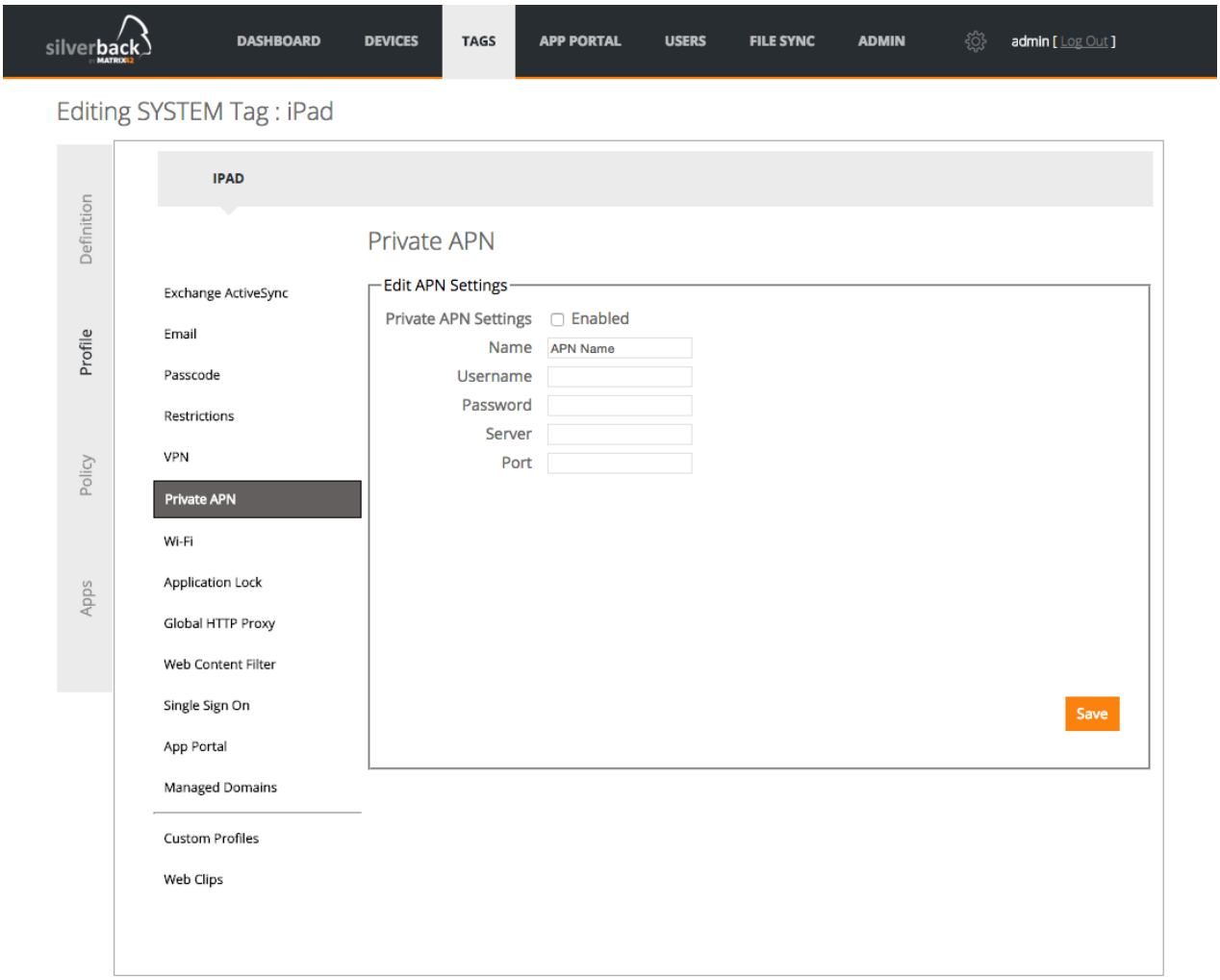
Windows Family VPN Settings

Configuration	Description
VPN Settings	Enables and Disables VPN for the Tag
VPN Type	Currently only Cisco AnyConnect
Connection Name	Name of the VPN Profile visible to the user on the device
Server Address	Network Address of the VPN Service
Authentication	Currently only Certificate

Samsung SAFE VPN Settings

5.2.6. Private APN

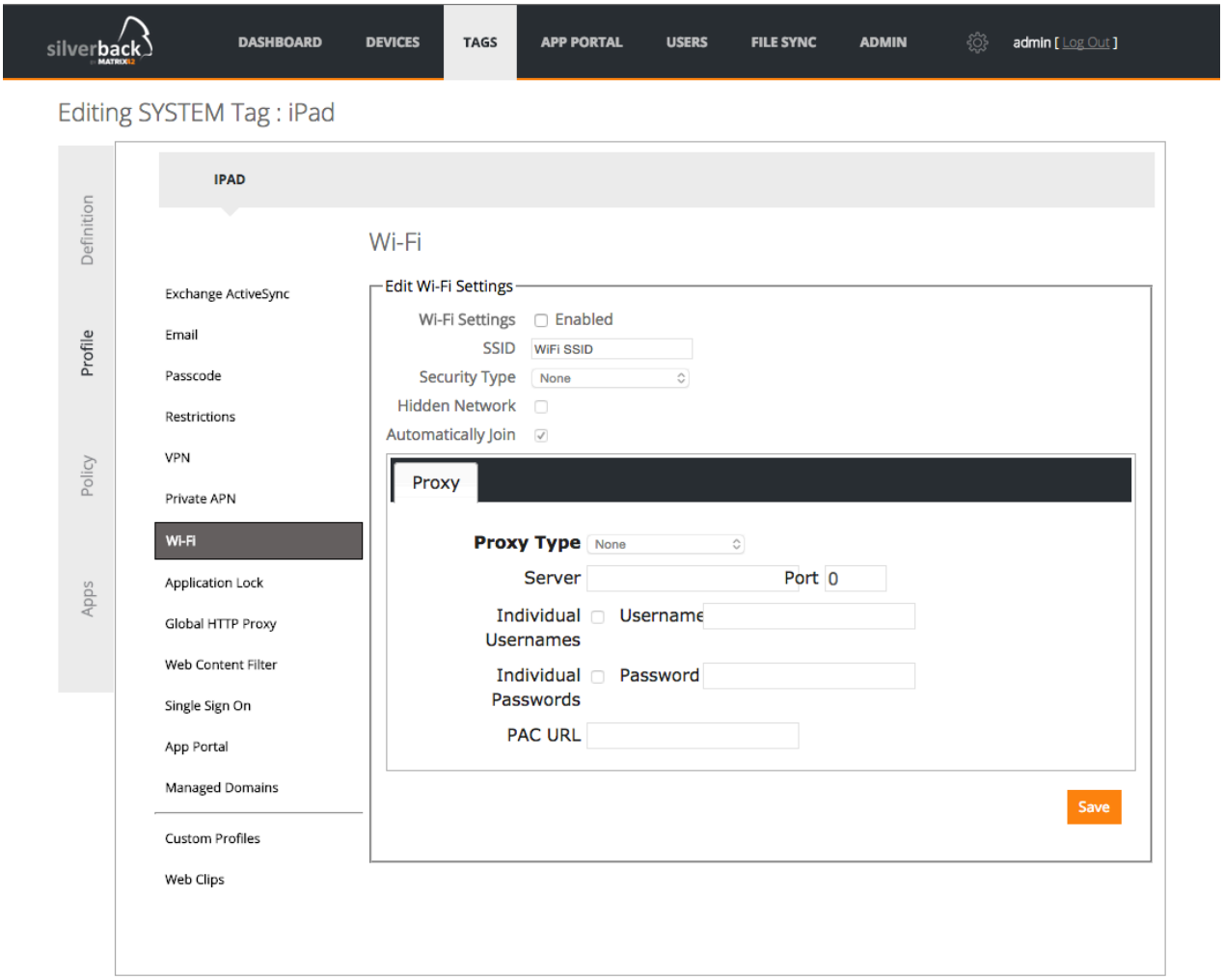
If you have a Private Access Point Name (APN) for your SIM Cards, then Silverback has the ability to configure this for you on the managed devices.



Configuration	Description
Private APN Settings	Enables the Private APN Feature on Selected Devices.
Name	The name of the carrier (GPRS/3G) access point
Username	The user name to connect to the access point
Password	The password to connect to the access point
Server	The fully qualified address of the proxy server
Port	The proxy port number

5.2.7. Wi-Fi

Silverback also has the ability to pre-populate Wi-Fi settings on your devices, so the user does not need to know the password for these networks themselves.



Configuration	Description
Wi-Fi Settings	Enables the sending of Wi-Fi settings to Selected
SSID	Service Set Identifier of the wireless network to
Encryption Type	Wireless network encryption to use when
Hidden Network	Enable if the target network is not open or
Automatically Join	The device will automatically join a Wi-Fi network if
Password	Password for authenticating to the wireless network
Proxy	Ensures the device talks to the necessary Proxy
Protocols	The protocol utilized by encryption type
Authentication	The authentication mechanism used

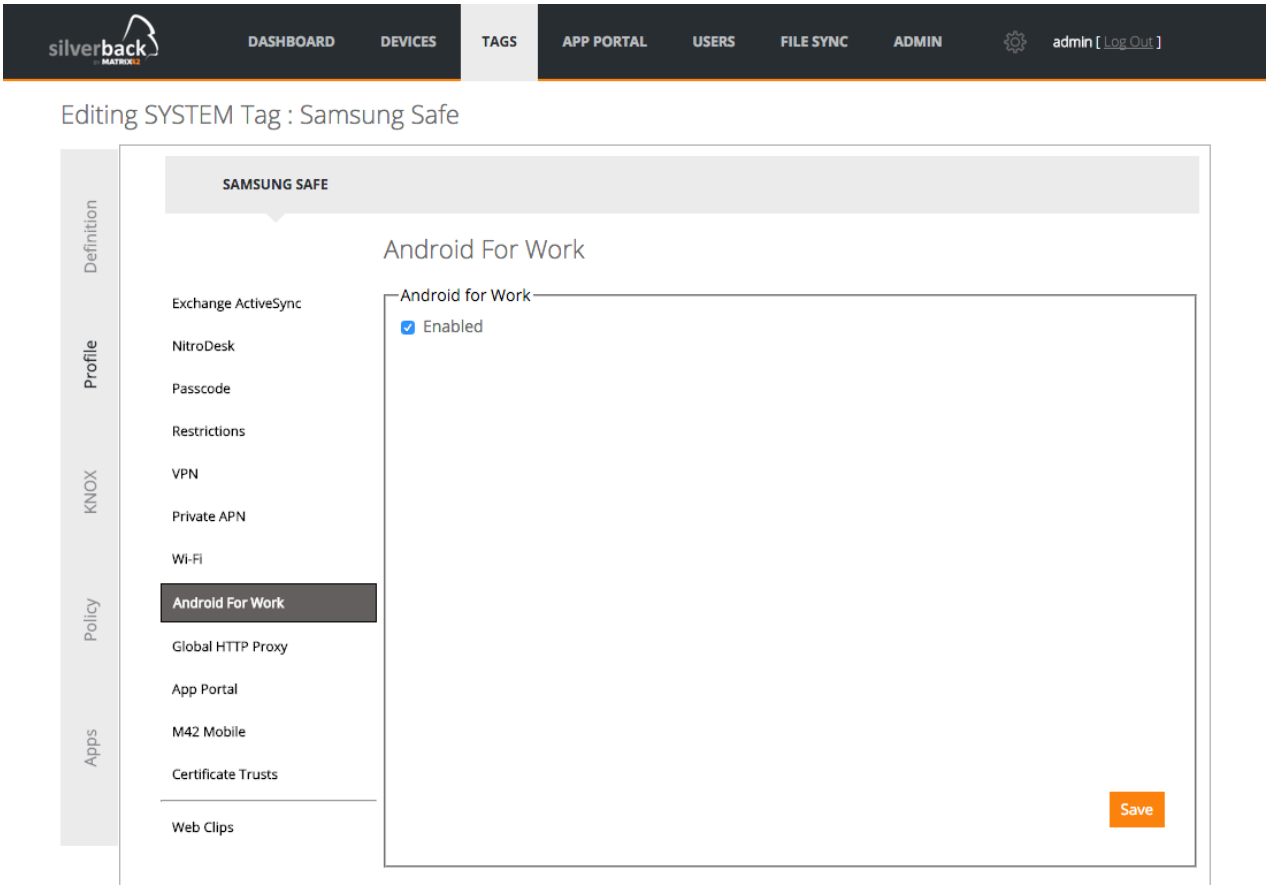
Configuration	Description
Trust	Trusted certificates and servers

NOTE: Due to the way OS X handles WiFi profile installation, if the WiFi network pushed to an OS X device is not available, the profile will fail to install. This may cause the device to move to blocked, as it does not have privileges installed.

5.2.8. Android for Work

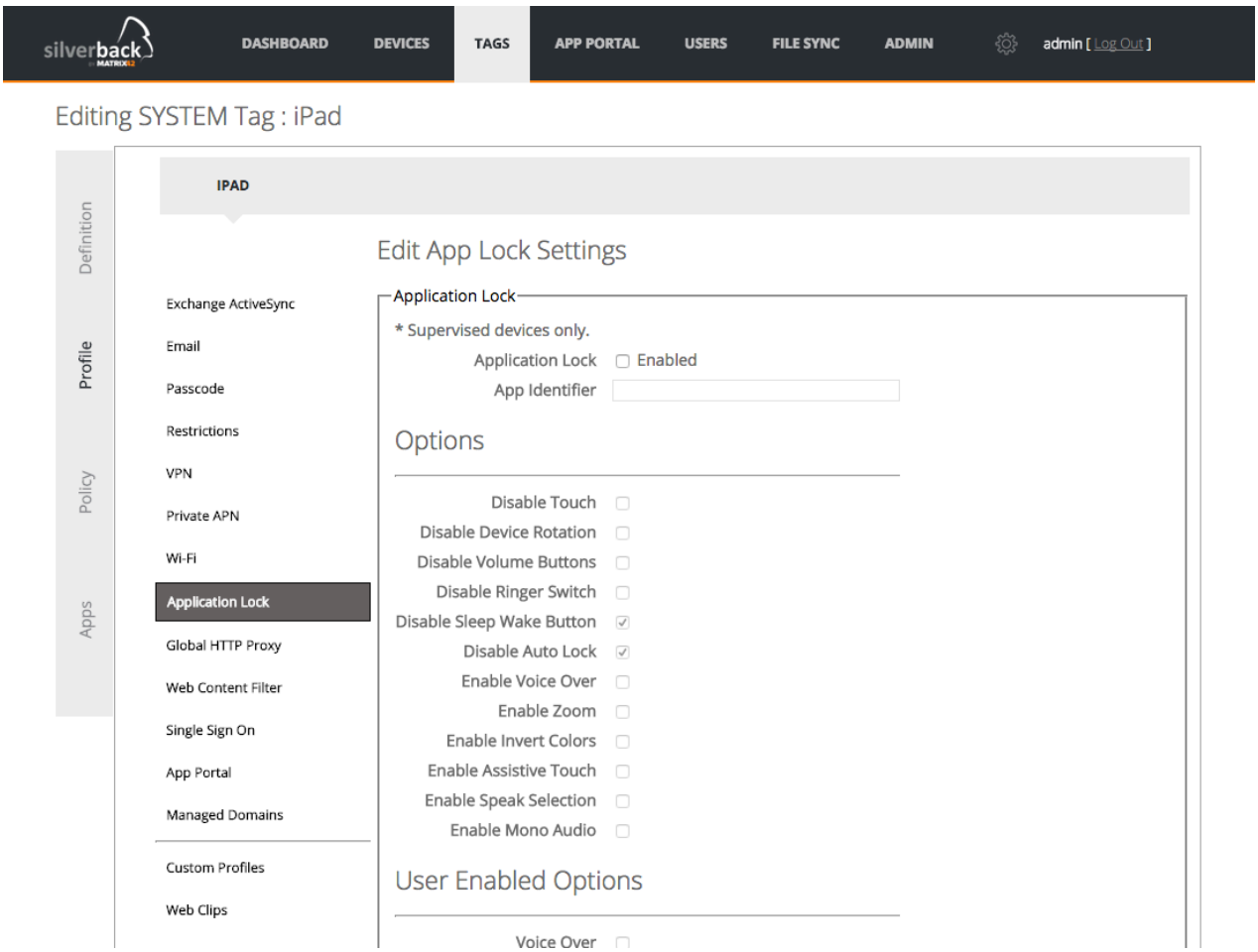
Android for Work is activated by enabling the Android for Work option on devices running Android 5.0 and above. This is available for both Android and Samsung SAFE Tags. When enabled, the device will automatically activate Android for Work on the device, and enable the Android for Work feature on the device.

Configuration	Description
Android for Work Enabled	Will activate Android for Work features on the devices in this Tag.



5.2.9. Application Lock

Through the use of the Application Lock feature, you can now 'Lock' a specific App to the screen of the device, meaning that the user cannot minimize or close the specified App from the screen.



Configuration	Description
Enabled	Enables the application of Custom Wallpapers.
App Identifier	The Identification String of the App that you want 'Locked' to the screen.
Disable Touch	Disables the users' ability to interact with the screen **(iOS7+ only)**
Disable Device Rotation	Disables the screen orientation change **(iOS7+ only)**
Disable Volume Buttons	Disables the hardware volume buttons on the device **(iOS7+ only)**
Disable Ringer Switch	Disables the hardware ringer switch on the device **(iOS7+ only)**

Configuration	Description
Disable Sleep Wake Button	Disables the hardware power button **(iOS7+ only)**
Disable Auto Lock	Controls whether the device will automatically lock screen **(iOS7+ only)**
Enable Voice Over	Forces the voice over feature on the device **(iOS7+ only)**
Enable Zoom	Forces the zoom feature on the device **(iOS7+ only)**
Enable Invert Colors	Forces the inverted colors feature on the device **(iOS7+ only)**
Enable Assistive Touch	Enables the assistive touch menu for one handed operation on the device **(iOS7+ only)**
Enable Speak Selection	Enables the speak selection control on the device **(iOS7+ only)**
Enable Mono Audio	Forces the mono audio on the device **(iOS7+ only)**
User Enabled Options	Enabling any options below will add a menu on the device that allows the user to configure the application lock settings locally
Voice Over	Allows the user to control voice over **(iOS7+ only)**
Zoom	Allows the user to control zoom **(iOS7+ only)**
Invert Colors	Allows the user to control color inversion **(iOS7+ only)**
Assistive Touch	Allows the user to control voice over **(iOS7+ only)**

NOTE: Only the 'iOS Device Family' (iPhone, iPad, iPod) on iOS 6 or higher currently supports a single application lock.

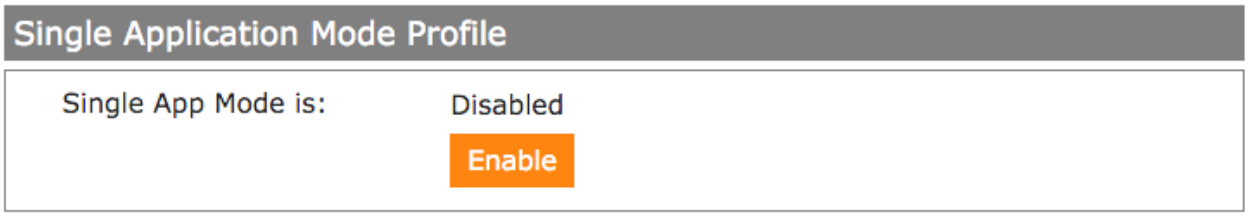
NOTE: To use the following feature, the iOS device is required to be configured in 'Supervised Mode' via the Apple Configurator software or by Apple DEP Enrollment.

5.2.9.1. Updating Application Lock Apps

Applications locked in Single App Mode cannot be updated due to a restriction in iOS. In Silverback a workflow is implemented that allows for these apps to be updated. This means that when you attempt to update a Single App Mode Locked app, the system will **automatically disable Single App Mode** and attempt to update the app. The system will continue to attempt this until the application is updated. The number of attempts to check this is determined by a setting in the Settings Administration page. Please refer to the Settings Administration document for information about this.

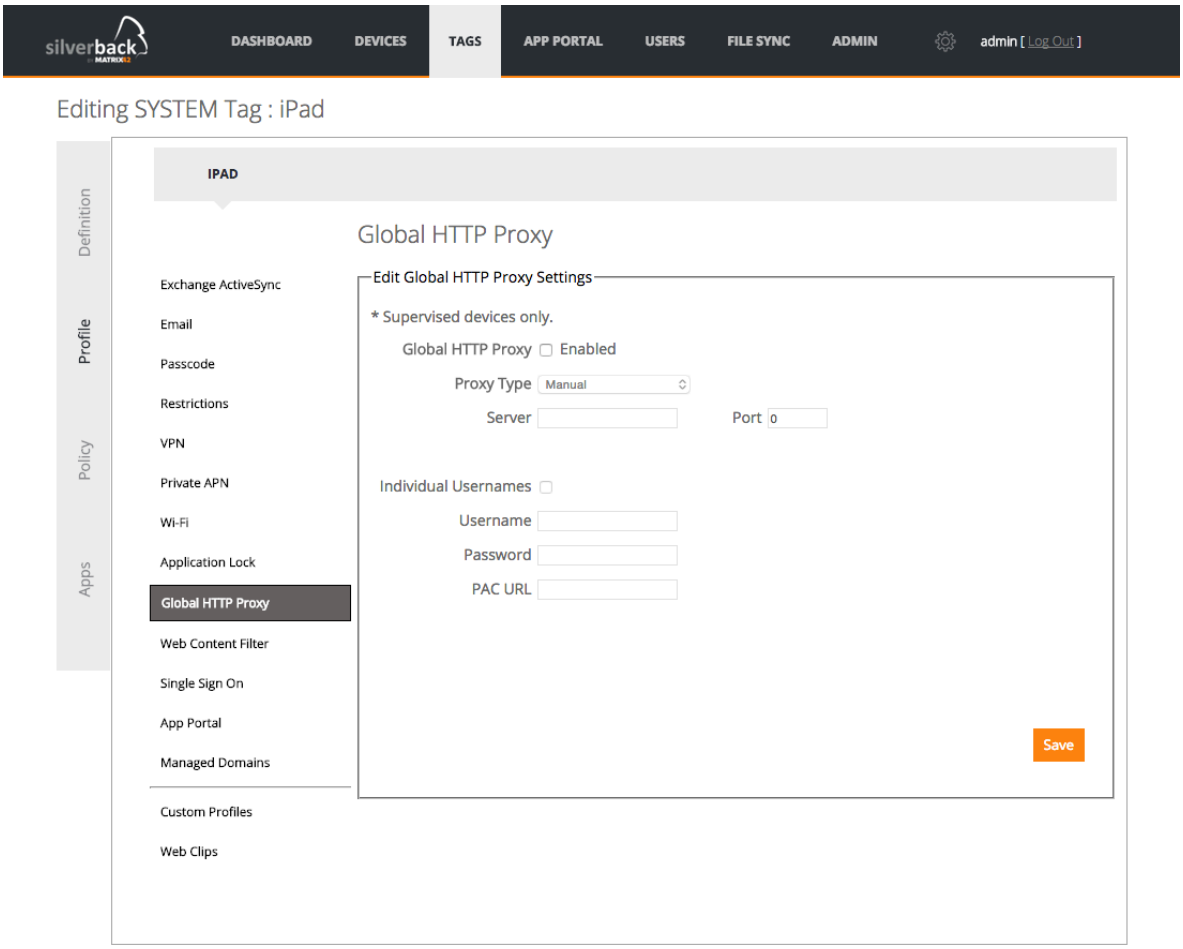
5.2.9.2. Manual Override of Application Lock

In some scenarios its necessary to force an individual device to enable or disable Single App Mode for troubleshooting. This can be done from the device info pop-up for a device that has Single App Mode settings applied. Note that once the device checks in, it may lock or unlock again based on it's Tag settings.



5.2.10. Global HTTP Proxy

Enabling the Global HTTP Proxy will force all Network Traffic through a designated proxy server.



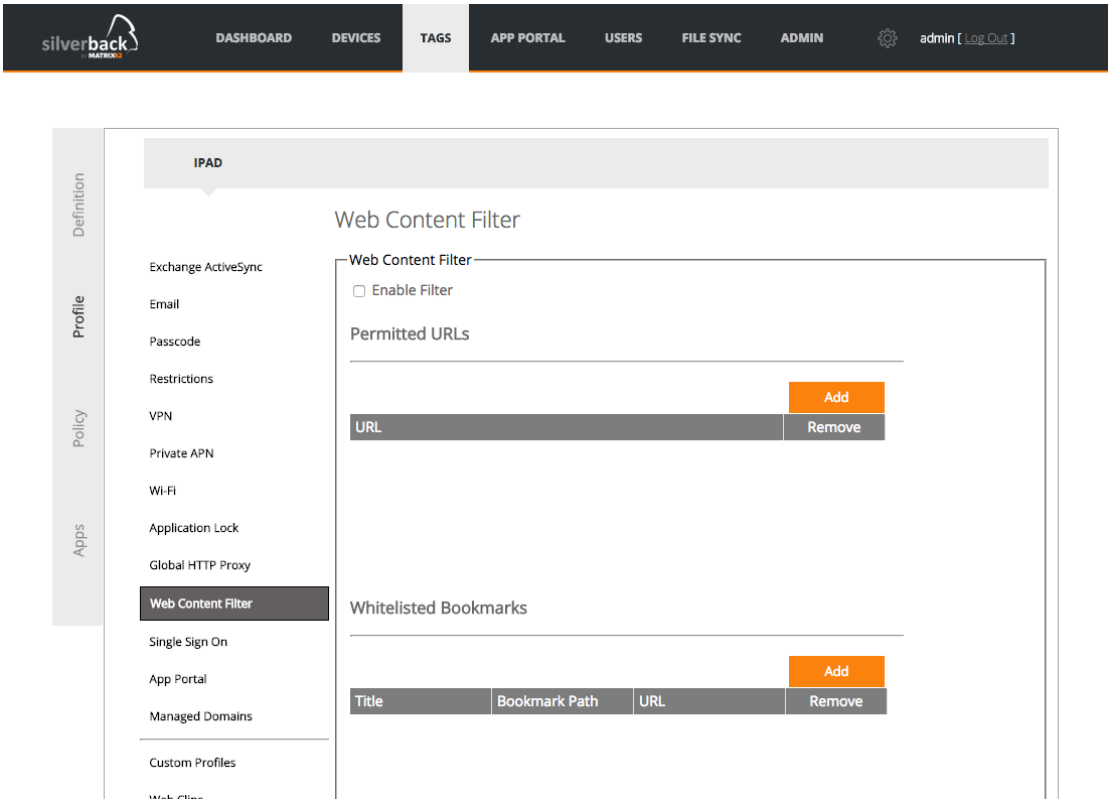
Configuration	Description
Enabled	Enables the Global HTTP proxy
Proxy Type	Allows the administrator to select a proxy type
Server	The FQDN or IP address of the proxy server
Port	The port of the proxy server
Individual usernames	Controls the user ability to enter their own credentials
Username	Allows the administrator to define the group username
Password	Allows the administrator to define the group password
PAC URL	Allows the administrator to specify the location of the PAC script

NOTE: To use the following feature on an iOS device, the device is required to be configured in ‘Supervised Mode’ via the Apple Configurator or by Apple DEP Enrollment.

5.2.11. Web Content Filter

Web Content Filter settings allow the administrator to control URLs accessible on the iOS7+ devices from Safari.

NOTE: The setting requires the device to be configured in 'Supervised Mode' via the Apple Configurator or Apple DEP Enrollment.

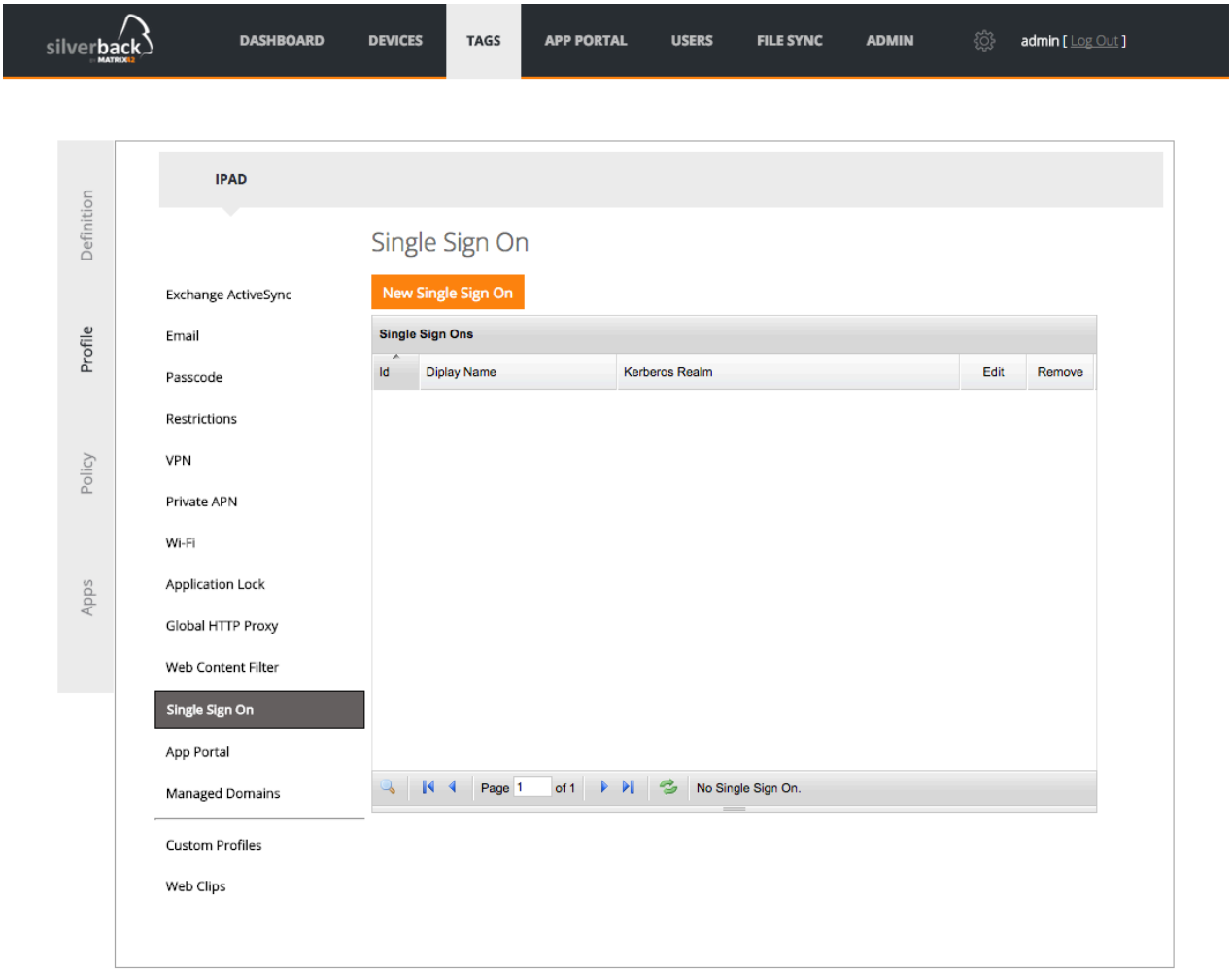


Configuration	Description
Enabled	Enables the Web Content Filter on the devices. If no URLs are specified, the users may not be able to browse the web.
Permitted URLs	URLs specified in this matrix will be permitted on the device.
Whitelisted bookmarks	If any URLs are specified in this matrix, the address bar is disabled in Safari. Instead, the user gets the bookmarks menu with folders specified and can only access these bookmarks. The folders are to be specified like so: \Root Folder\Subfolder
Blacklisted URLs	The URLs specified in this matrix are not accessible on the device.

NOTE: The URL has to pass ALL filters for the device to allow navigation to it.

5.2.12. Single Sign On

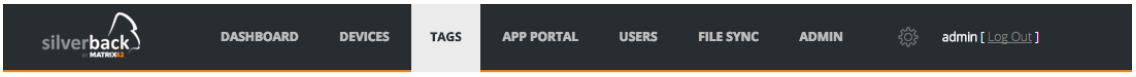
Single Sign On feature allows the administrator to configure per session Kerberos authentication across multiple sites in the same realm for an iOS7+ device.

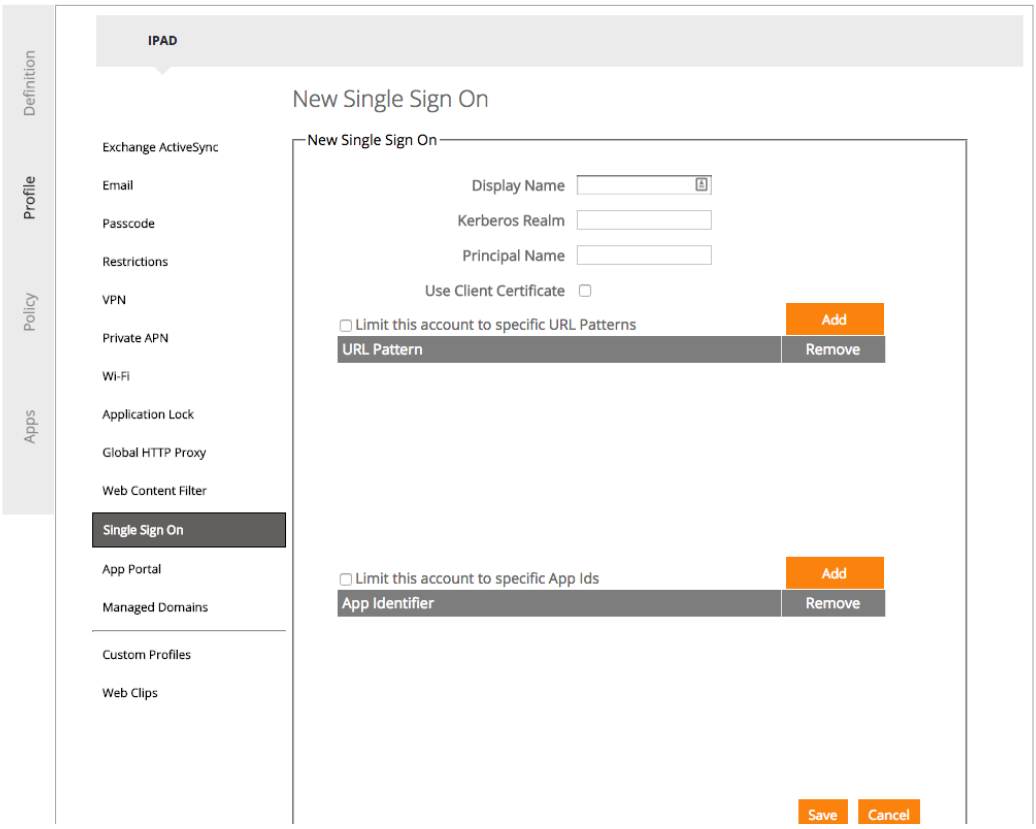


Configuration	Description
New Single Sign On	Allows the administrator to specify the new single sign on configuration
Single Sign On matrix	Lists the current single sign on configurations.

5.2.13. Adding a Single Sign On

Single Sign On feature allows the administrator to configure per session Kerberos authentication across multiple sites in the same realm for an iOS7 device.





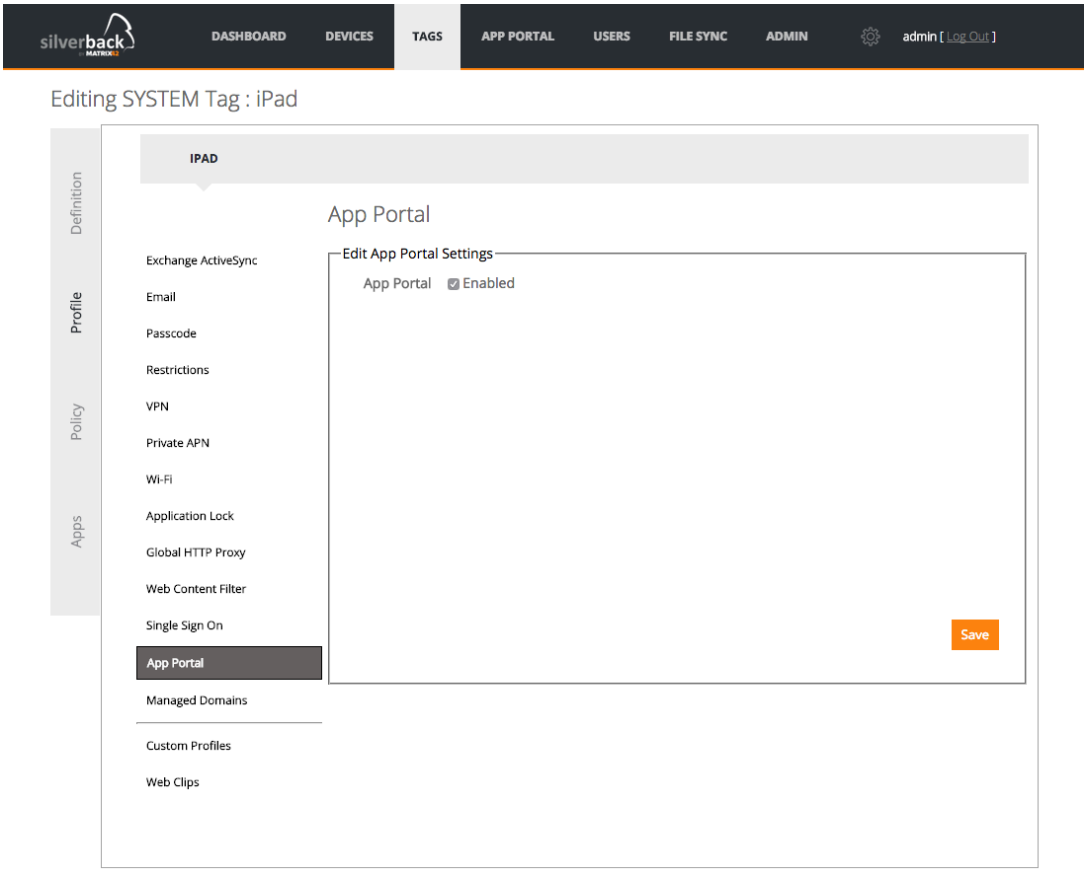
Configuration	Description
Display Name	The display name for the SSO configuration
Kerberos Realm	The Kerberos realm name
Principal Name	The value of the user principal name for the Kerberos realm. This field supports the configuration variables.
Limit this account to specific URL patterns	**Required.**
Limit this account to specific App Ids	**Required.**

NOTE: The URL has to pass ALL filters for the device to allow navigation to it.

5.2.14. App Portal

The Application portal is where devices can access Enterprise applications and recommended Third Party applications via a web clip icon.

To enable access to the Application portal for end users and push the app portal web clip icon to devices, ensure App Portal Enabled box is ticked.



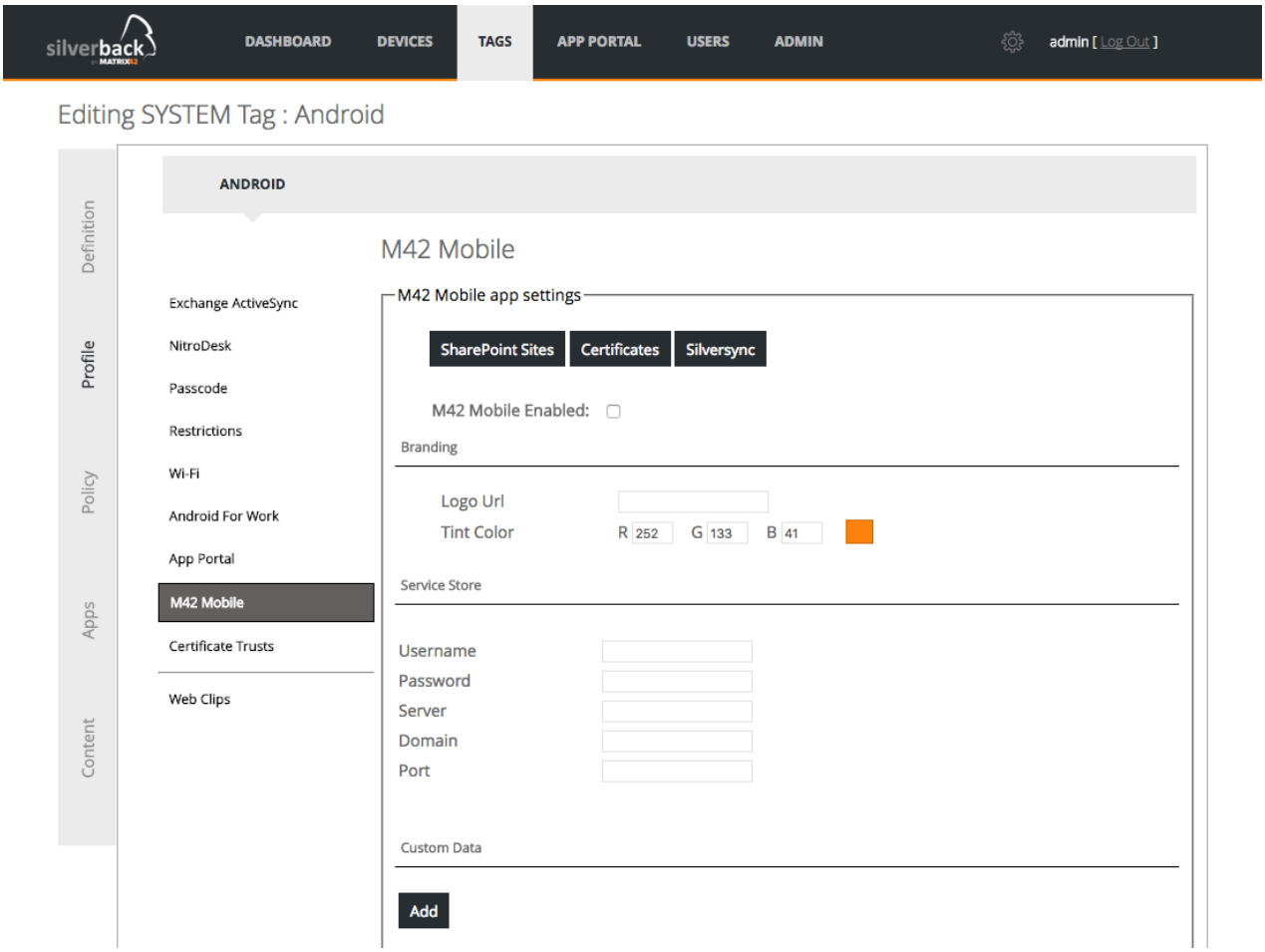
Configuration	Description
Enabled	Enables the App Portal Icon on enrolled devices.

The App Portal Tab (see section titled App Portal Tab below) is where you add and remove applications to be accessed via the App portal icon.

NOTE: It is possible to customize both the Icon and Text associated with the App Portal, see the App Portal section under the Admin Tab for this feature.

5.2.15. M42 Mobile

The M42 Mobile section allows you to configure data sources for users who use the M42 Mobile client on Samsung SAFE or Android devices. The configuration of the data-sources is identical to configuration for Companion iOS devices.



For the other settings available, the following configuration options are available:

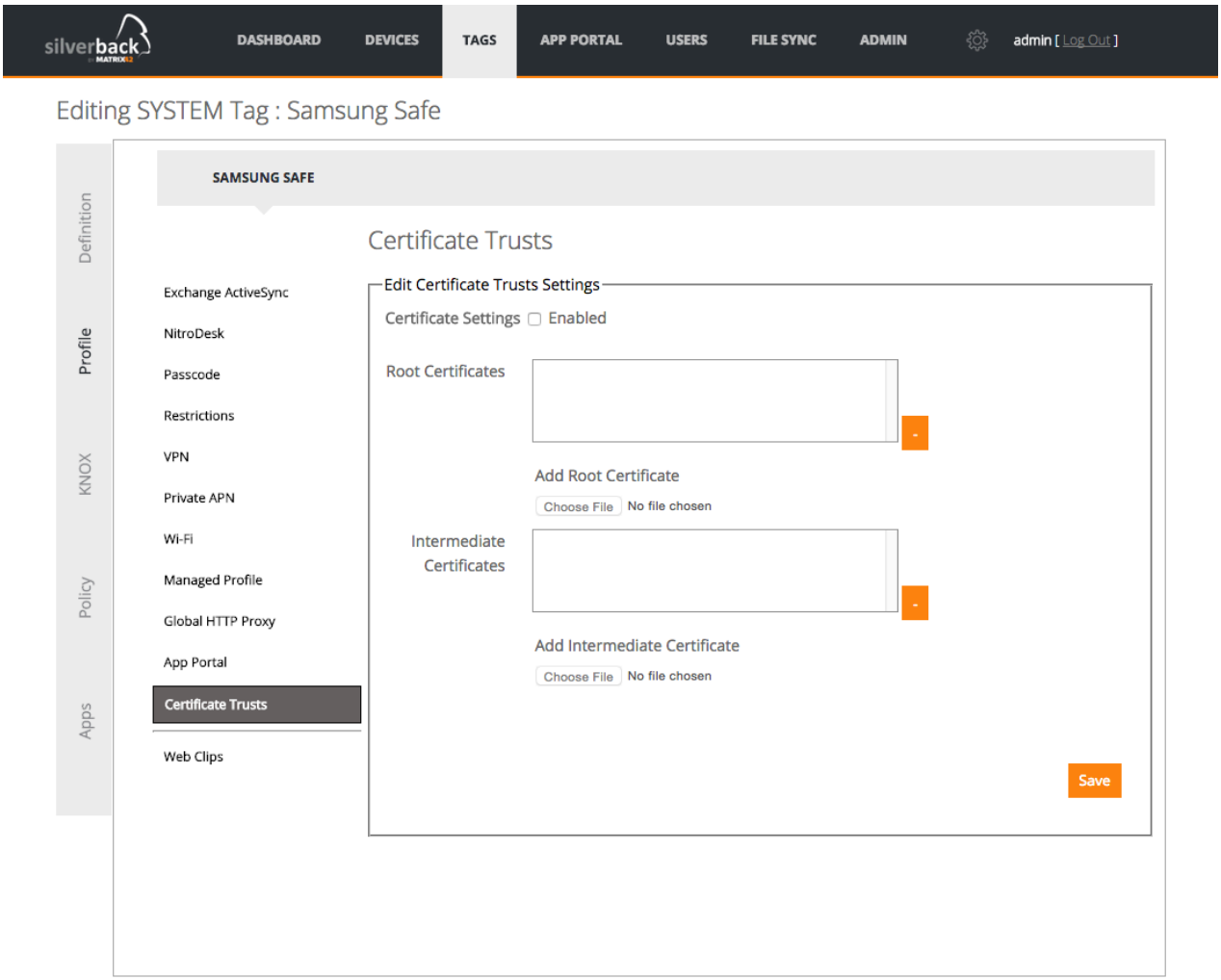
Configuration	Description
M42 Mobile Enabled	Enables M42 Mobile Settings for this Tag
Logo URL	Allows you to override the default Matrix42 Logo with a custom logo. Enter the URL of the logo file that clients should download.
Tint Colour	The RGB value of the main colour of the M42 Mobile App. This will visually change the colour of UI elements on the device.
Username	If using Service Store, this pre-populates the Username field. This accepts System Variables.
Password	If using Service Store, this pre-populates the Password field. This accepts System Variables.
Server	If using Service Store, this pre-populates the Service

Configuration	Description
	Store Server URL.
Domain	If using Service Store, this pre-populates the Domain field.
Port	If using Service Store, this pre-populates the Port field.
Custom Data	This should only be used when directed by Matrix42. This allows custom fields to be defined, for example if a new M42Mobile app is being tested but not publicly available, this could be used to add new configurable fields.

5.2.16. Certificate Trusts

For iOS, Windows Phone, Windows and Samsung SAFE devices, arbitrary certificate trusts can be defined. These certificates will be deployed to the root or intermediate trust stores on the devices.

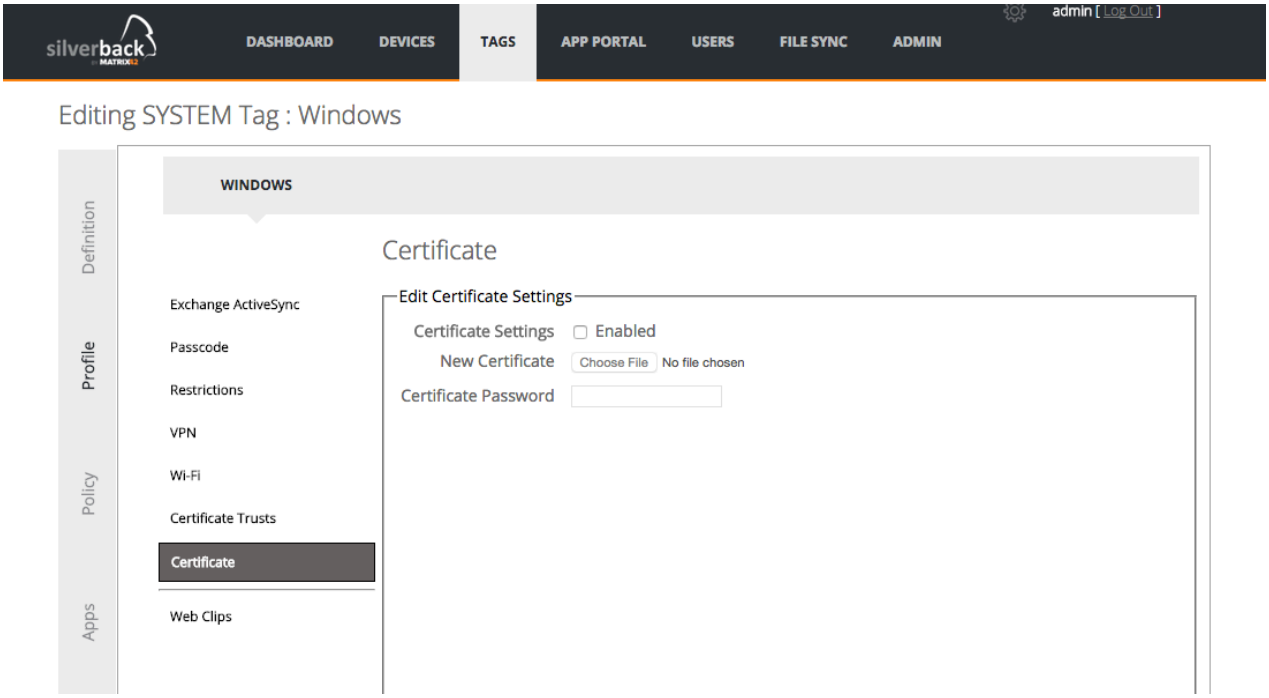
Silverback by Matrix42 Admin Guide Version 5.1 U3



Autor: Matrix42 Cloud & Mobile Management

5.2.17. Certificate

For Windows Phone and Windows devices, configuration of the certificate used within a Tag for authentication, e.g. WiFi or Exchange is configured here. If the system is configured for individual certificate authentication, then you can configure this. If the system is configured for Enterprise certificate authentication, then you can provide a P12/PFX file for upload.



5.2.17.1. Individual Certificate Authentication

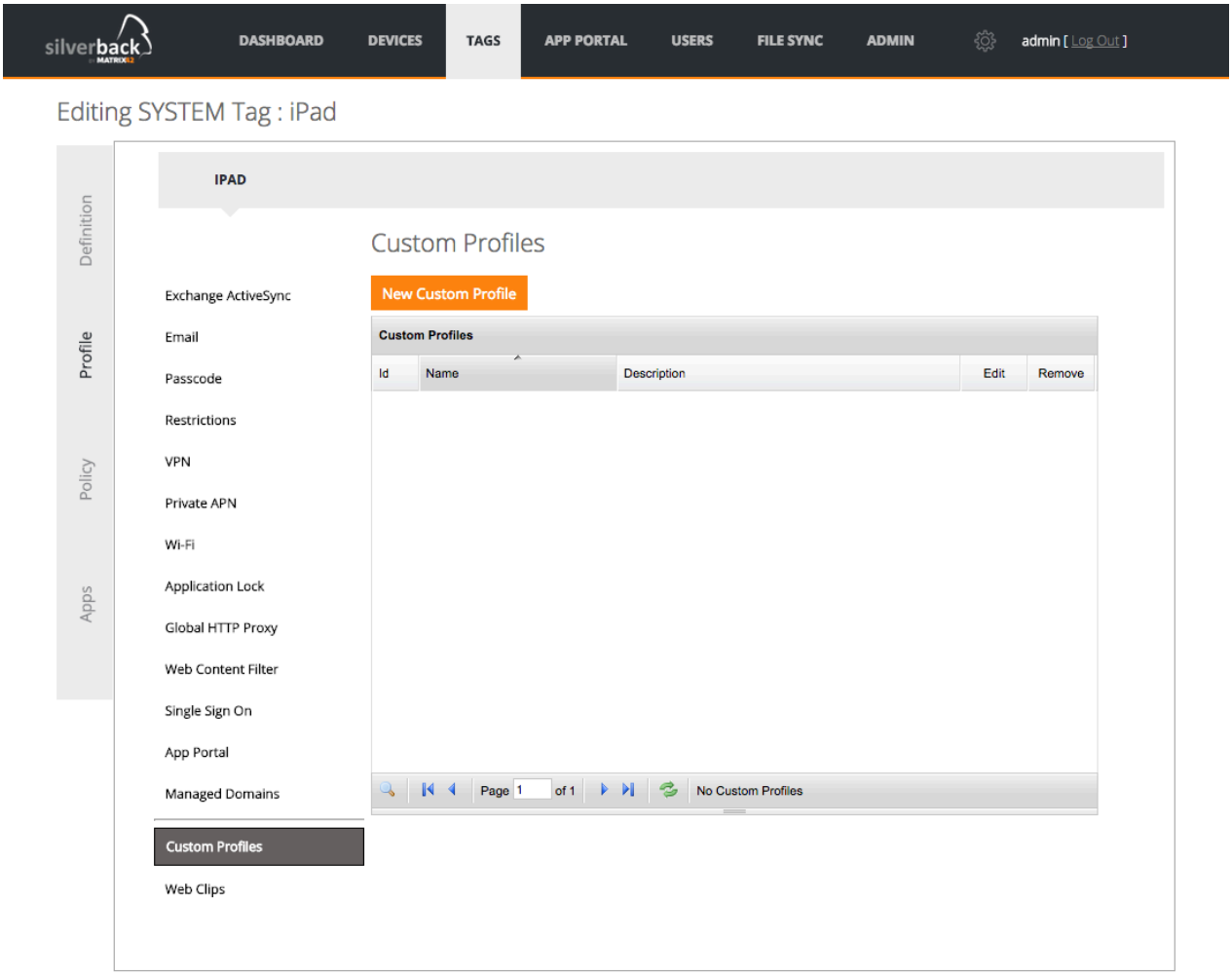
Configuration	Description
Certificate Settings	Enables the certificate settings for this Tag
Template Name	The certificate template name on the CA to use
Use Custom Subject Name Variable	If needed, a custom Subject Name for the certificate
Use Custom UPN San Variable	If needed, a custom UPN SAN for the certificate
Use Custom RFC 822 SAN Variable	If needed, a custom variable, compliant with RFC 822 for the certificate

5.2.17.2. Enterprise Certificate Authentication

Configuration	Description
Certificate Settings	Enables the certificate settings for this Tag
New Certificate	Upload a P12/PFX certificate to use for authentication
Certificate Password	The password for the above file

5.2.18. Custom Profiles

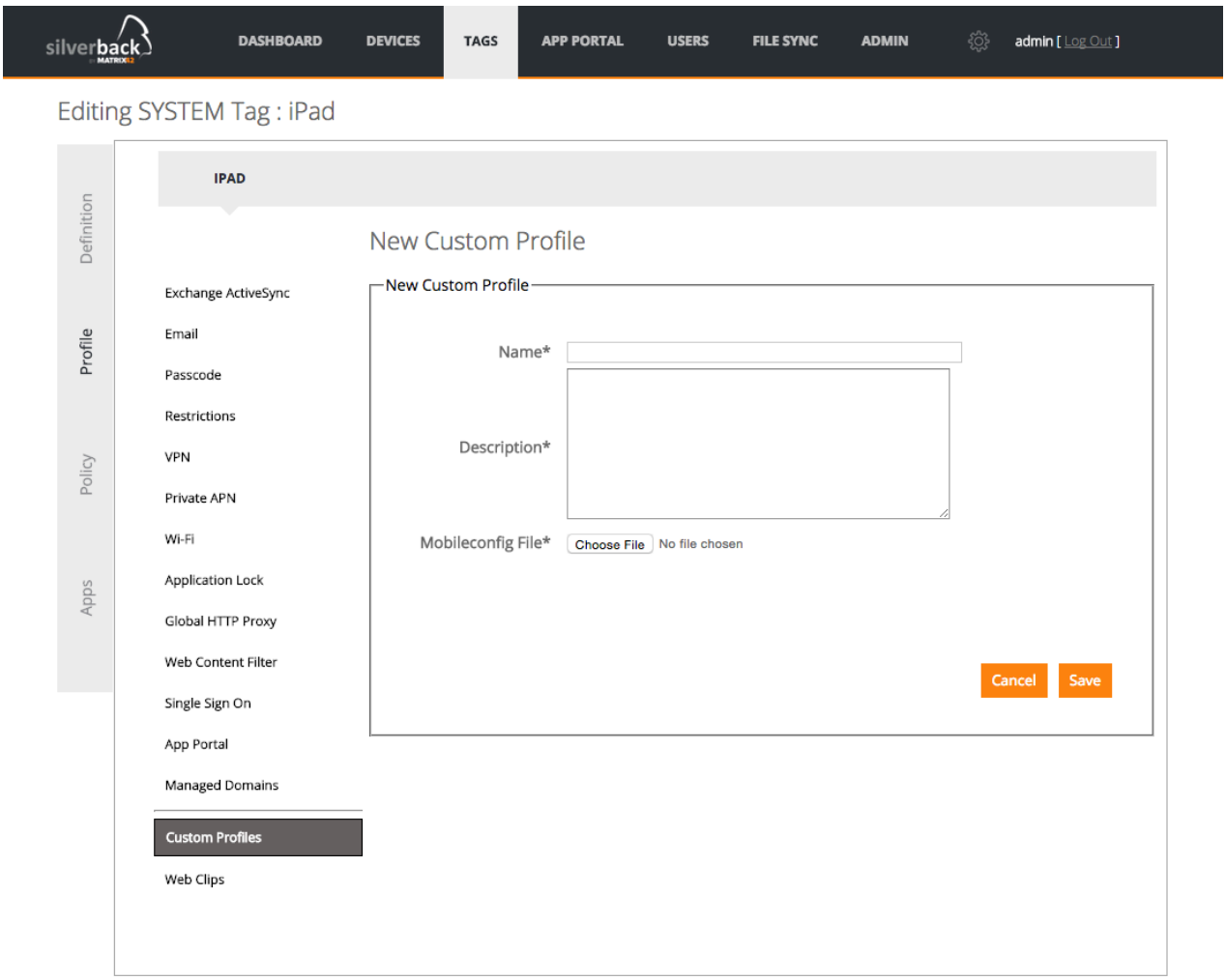
For iOS and OS X devices, administrators can upload their own User-Defined Configuration.



Field	Description
ID	System ID Number for the Custom Profile
Name	The General Name of the Custom Profile
Description	A short description of what the Custom Profile is for
Edit	Button for Editing the Custom Profile
Remove	Deletes the selected Custom Profile

5.2.19. Adding a Custom Profile

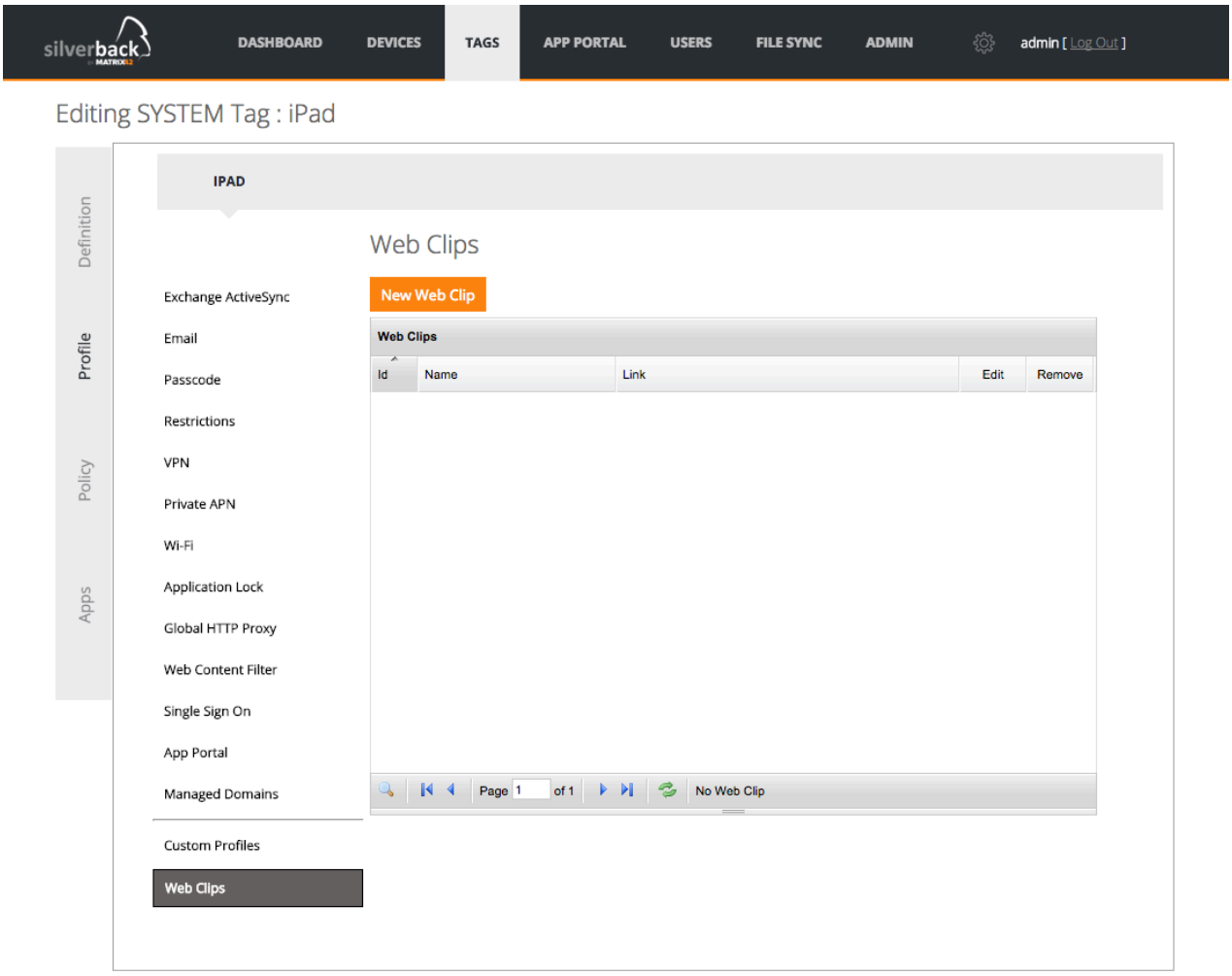
Clicking on the 'New Custom Profile' button will display the screen below. From here the administrator is able to select the custom profile that they've created, name it and provide a brief description of what it does. Clicking 'Save' will make it available to every Managed Device of that particular device type.



Field	Description
Name	The display name of the custom profile being uploaded
Description	The description of the custom profile to display
MobileConfig File	The MOBILECONFIG file of the custom profile itself

5.2.20. Web Clips

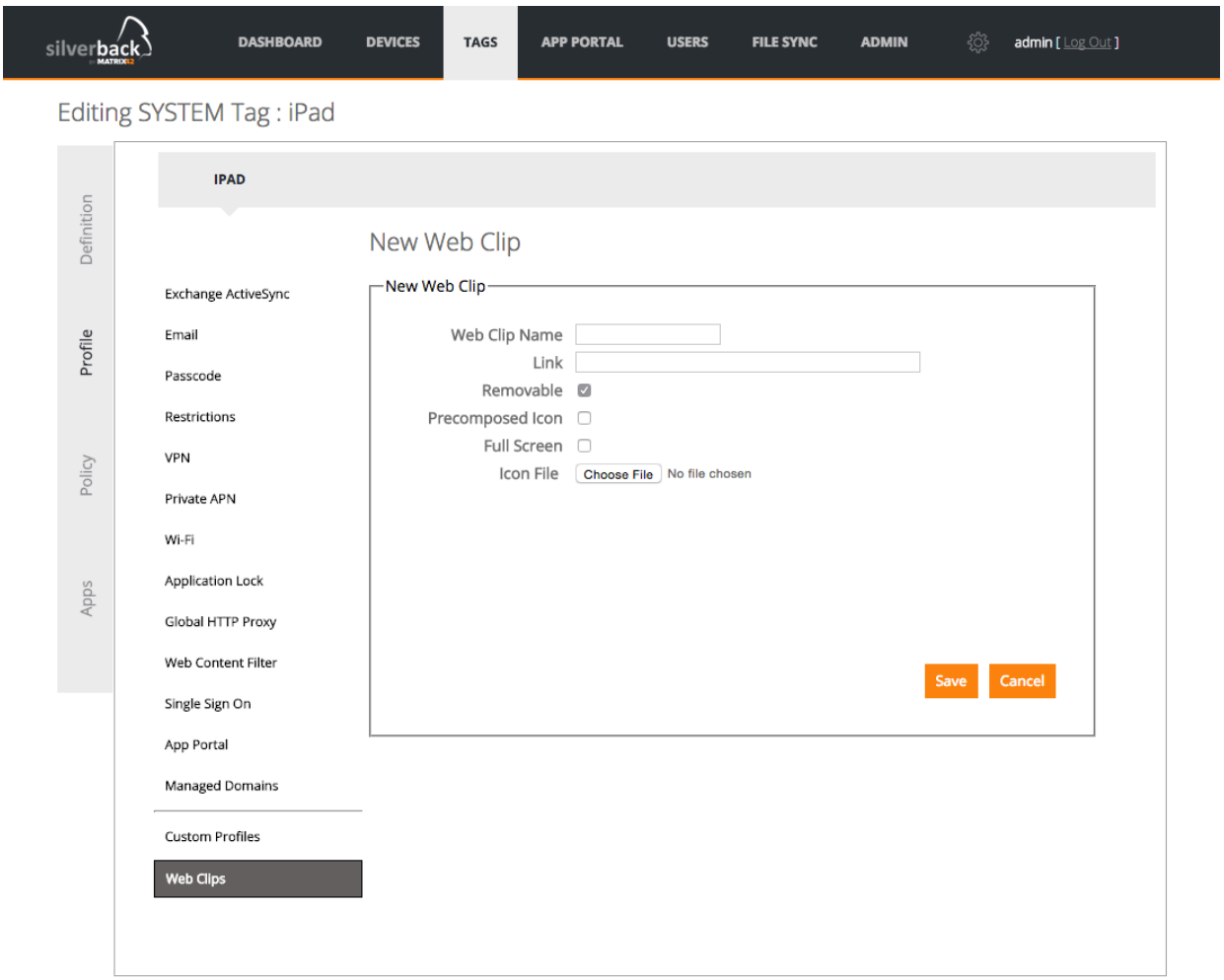
Silverback allows administrators to push down Internet shortcuts to their Managed Devices, giving users easy access to the websites the administrator wants.



Field	Description
ID	System ID Number for the Web Clip
Name	The General Name of the Web Clip
Description	A short description of what the Web Clip is for
Edit	Button for Editing the Web Clip
Remove	Deletes the selected Web Clip

5.2.21. Adding a Web Clip

Clicking on the 'New Web Clip' button will bring up the screen below. From here the administrator is able to create a Web Clip that will appear as a shortcut on all enrolled devices.



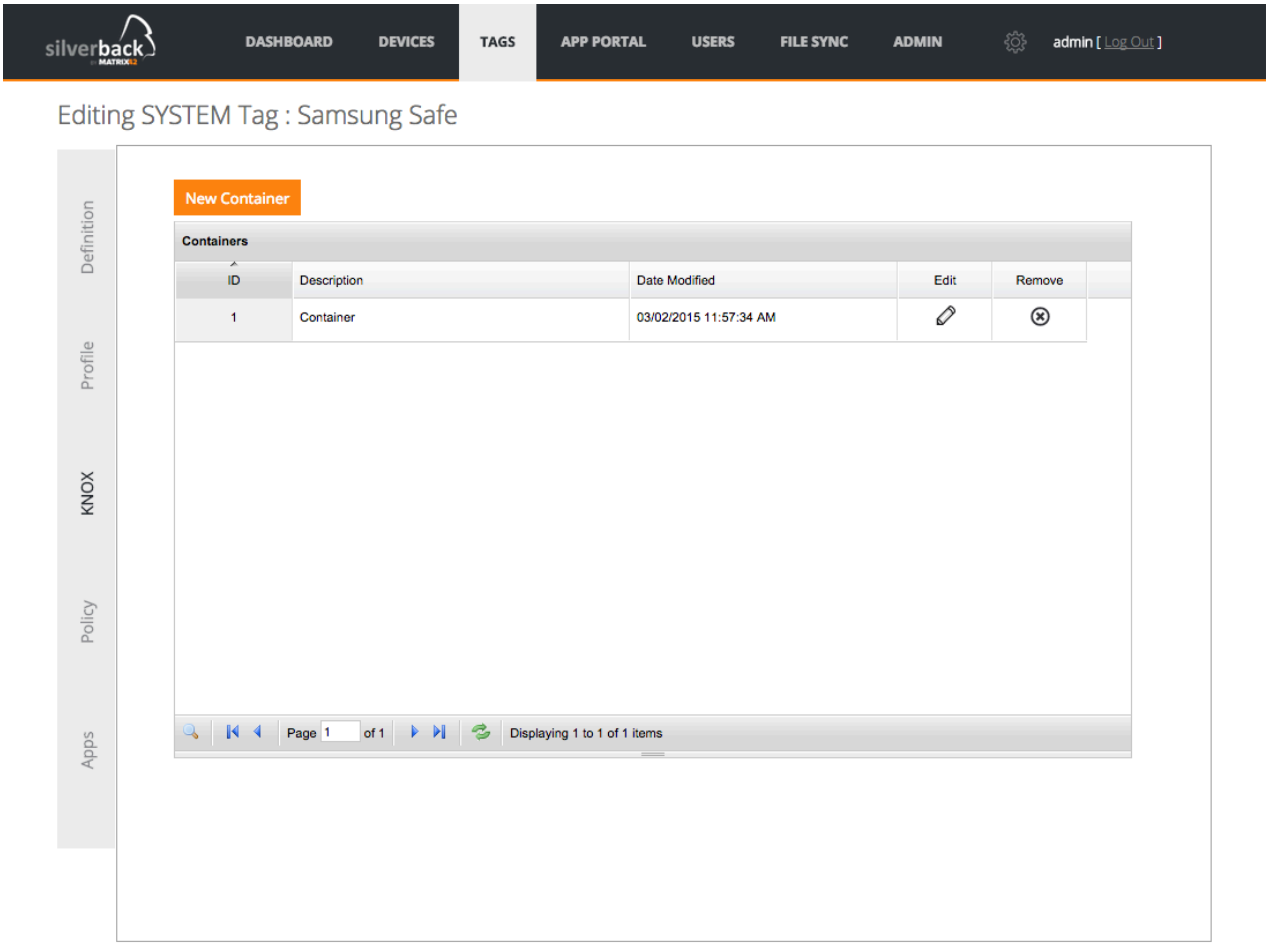
Field	Description
Web Clip Name	A Name for the new Web Clip
Link	The URL to be embedded within the Web Clip
Removable (iOS Only)	Give the user the option to remove the shortcut from the device
Precomposed Icon (iOS Only)	If disabled, iOS adds the gloss effect to the icon when displaying on the device.
Full Screen (iOS Only)	Hides the Safari Browser Interface, displaying the website in Full Screen.
Upload	A button for uploading a Custom Icon (must be 96x96 Pixels)
Save	Saves the Web Clip to Silverback and sends it to enrolled

Field	Description
	devices.

5.3. KNOX Feature

KNOX is a section where Administrators can configure settings for Samsung KNOX Enabled devices. The KNOX Section is only available when a Tag is enabled for Samsung SAFE devices, and the appropriate license is configured in the Admin Tab Licensing section.

Settings available beneath the KNOX Section are similar to what is available to a Tag in general, but as these are containerized settings, they exist in Containers within a Tag.



Field	Description
ID	System ID Number for the KNOX Container
Description	A Short description to label the KNOX Container
Date Modified	Date and Time that the KNOX Container was last modified

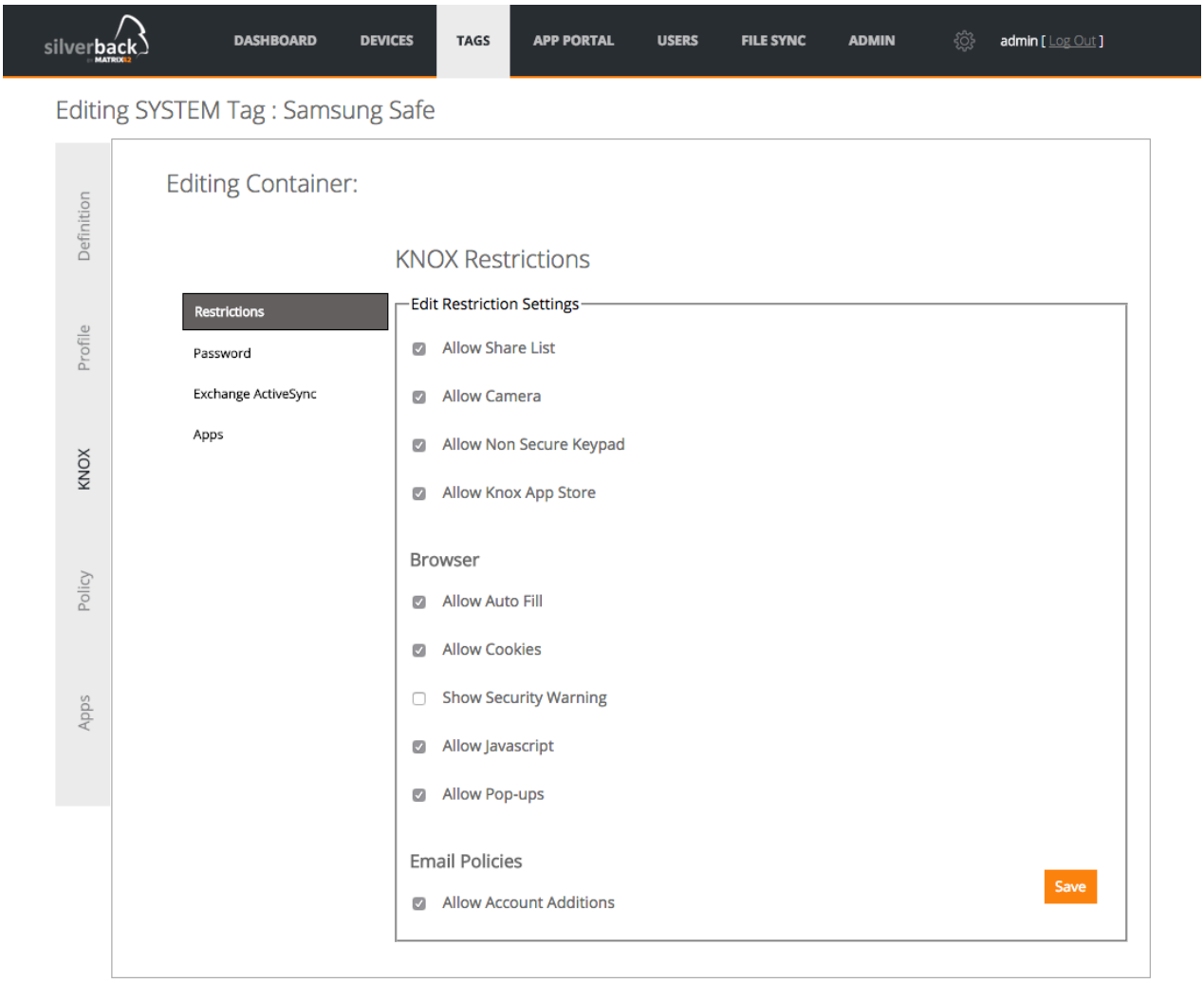
Field	Description
Edit	Button for Editing the KNOX Container
Remove	Deletes the selected KNOX Container

5.3.1. Adding or Editing a KNOX Container

By clicking on the 'New Container' or editing an existing Container, will take you to a screen that allows you to edit the various settings of a Container. The individual Sections within a Container explained below:

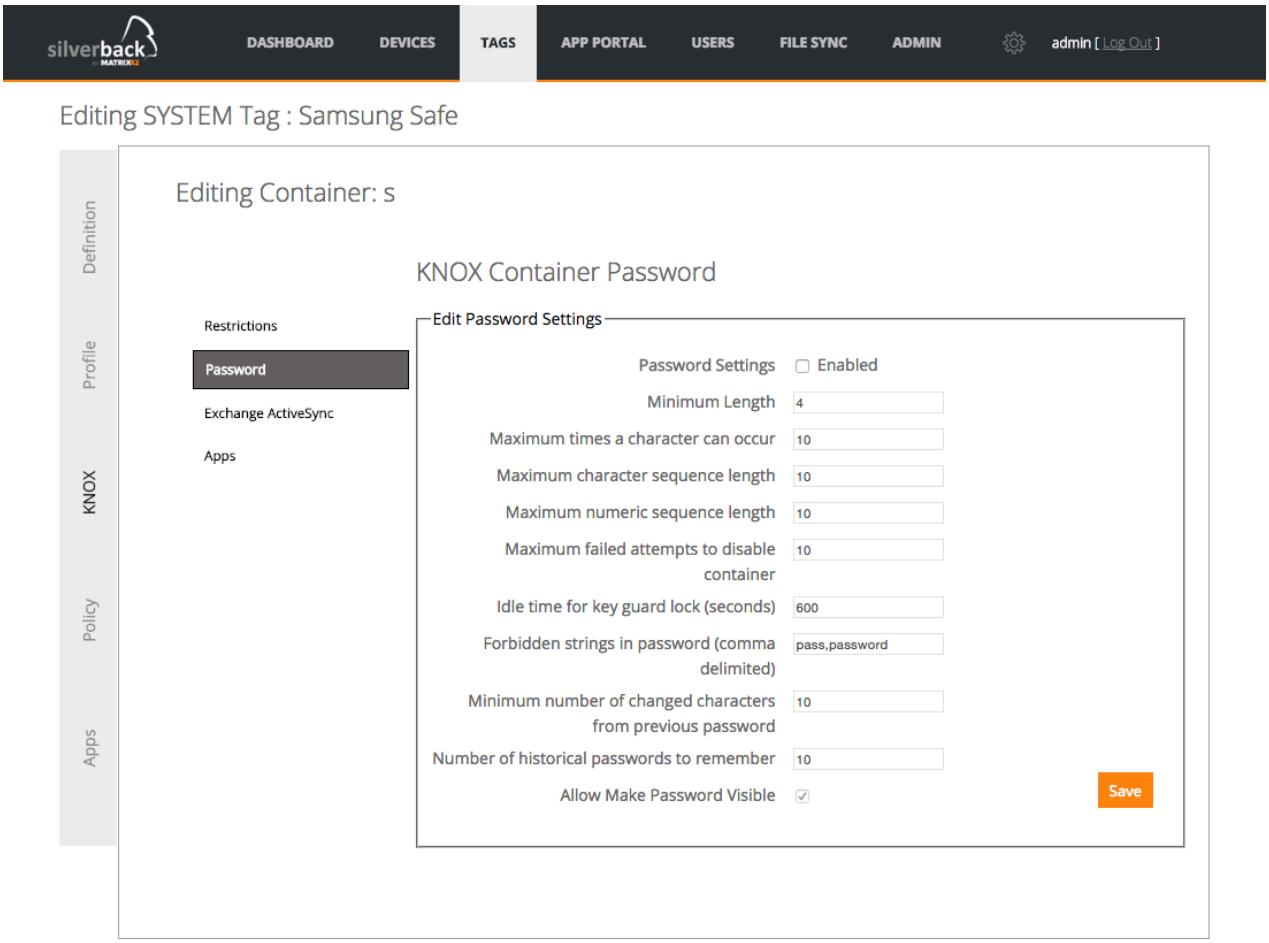
5.3.2. Restrictions

To allow a function for the Container you are creating or editing, simply ensure the corresponding checkbox is ticked and click Save at the bottom of the page.



5.3.3. Password

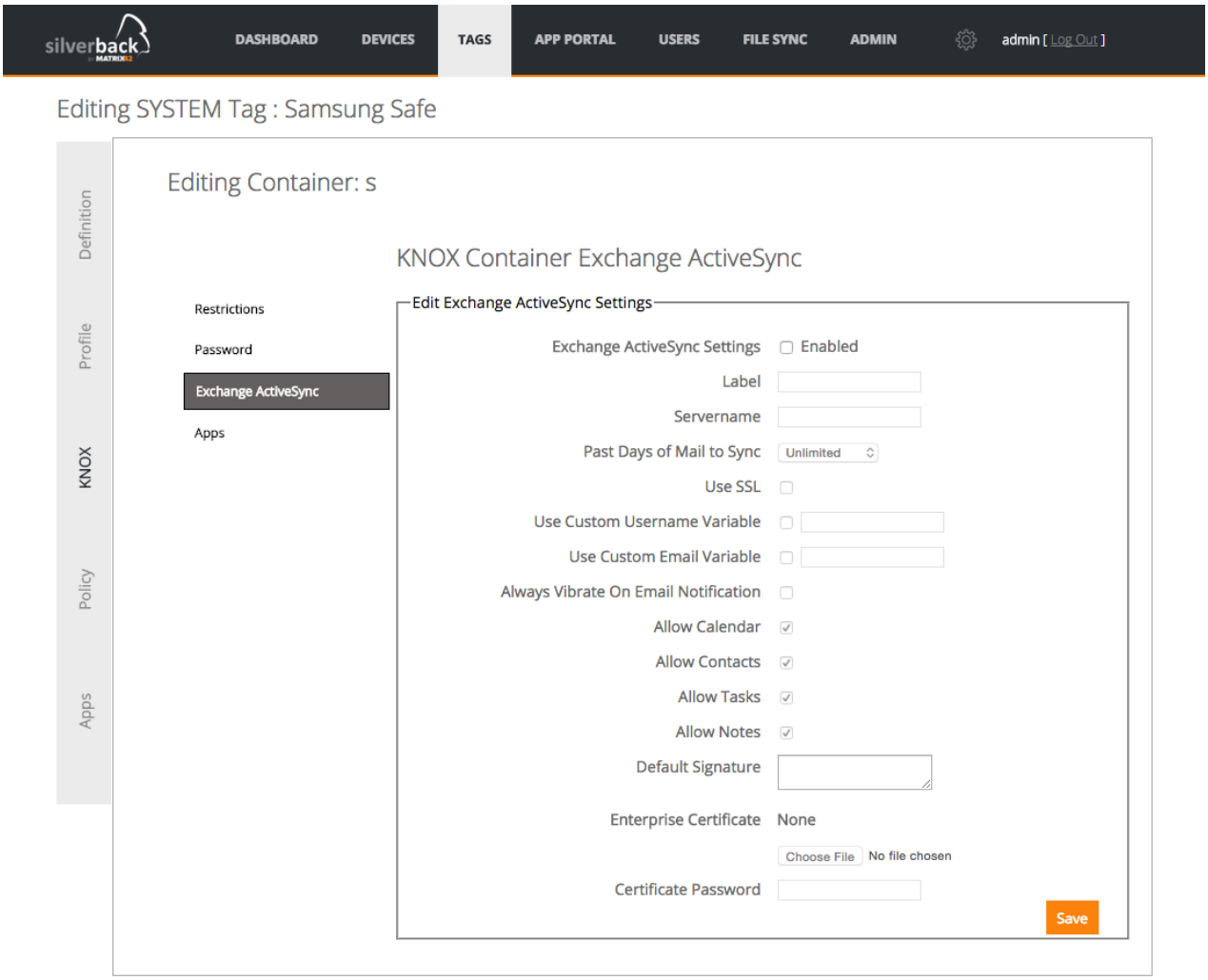
This section governs the security level of the password for the specific Container if enabled.



Configuration	Description
Password Settings	Enables or disables Password settings for this Container
Minimum Length	The minimum number of characters required for the Container Password
Maximum times a character can occur	Maximum times an individual character can occur in the password
Maximum character sequence length	Maximum sequence for letters, for example a maximum of 3 would allow “abc” but not “abcd”
Maximum numeric sequence length	Maximum sequence for numbers, for example a maximum of 3 would allow “123” but not “1234”
Maximum failed attempts to disable container	Number of times the user can enter an incorrect password before access to the Container is disabled
Idle time for key guard lock	Amount of time before the device automatically locks when not interacted with
Forbidden strings in password	List of words or numbers, delimited by comma, that are not allowed to exist within the password as a whole. For example, a setting of “word” would not allow the password “password”
Minimum number of changed characters from previous password	Number of characters that must be different from the previous password, this prevents the user using the same password and incrementing a tailing number for example
Number of historical passwords to remember	Number of passwords to remember that the user cannot use again
Allow make password visible	Allow the user to make their password visible when editing it

5.3.4. Exchange ActiveSync

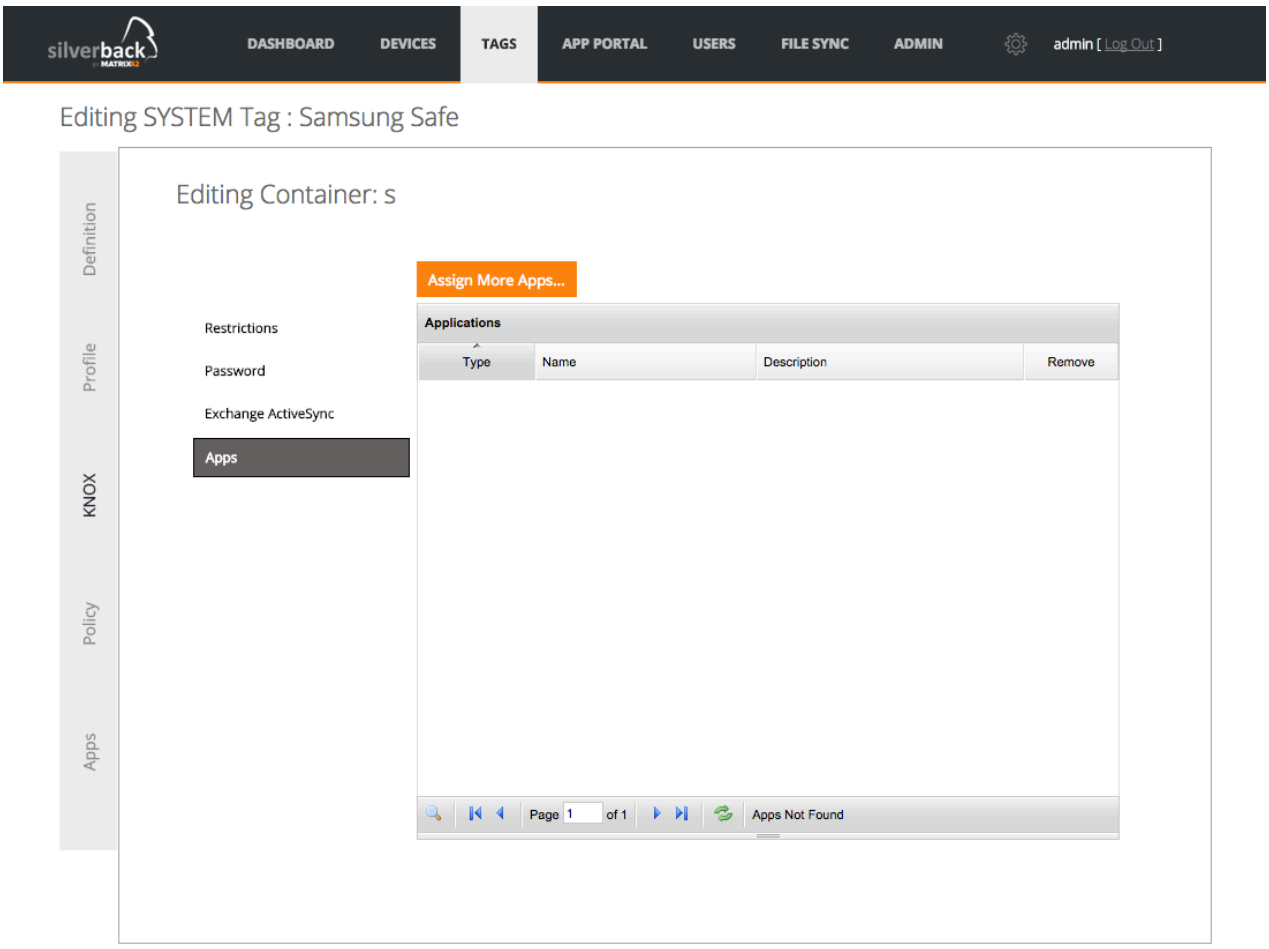
To allow a function for the Container you are creating or editing, simply ensure the corresponding checkbox is ticked and click Save at the bottom of the page.



Configuration	Description
Label	The Label for the Email Account as it appears on the device.
Servername	The External Mail Server URL
Past Days of Mail to Sync	Period of mail to synchronize to the device
Use SSL	If the URL for the External Mail Server is protected by an SSL Certificate then use SSL.
Use Custom Username Variable	Define a Custom Variable Attribute for the Username for the EAS Profile.
Use Custom Email Attribute	Define a Custom Variable Attribute for the Email Address for the EAS Profile.
Always Vibrate on Email Notification	Sets the mail settings to vibrate when receiving a mail
Allow Calendar	Determines whether the user can use the calendar associated with the Exchange ActiveSync Account
Allow Contacts	Determines whether the user can use the contacts associated with the Exchange ActiveSync Account
Allow Tasks	Determines whether the user can use the tasks associated with the Exchange ActiveSync Account
Allow Notes	Determines whether the user can use the notes associated with the Exchange ActiveSync Account
Default Signature	Pre-Define a signature for the account

5.3.5. Apps

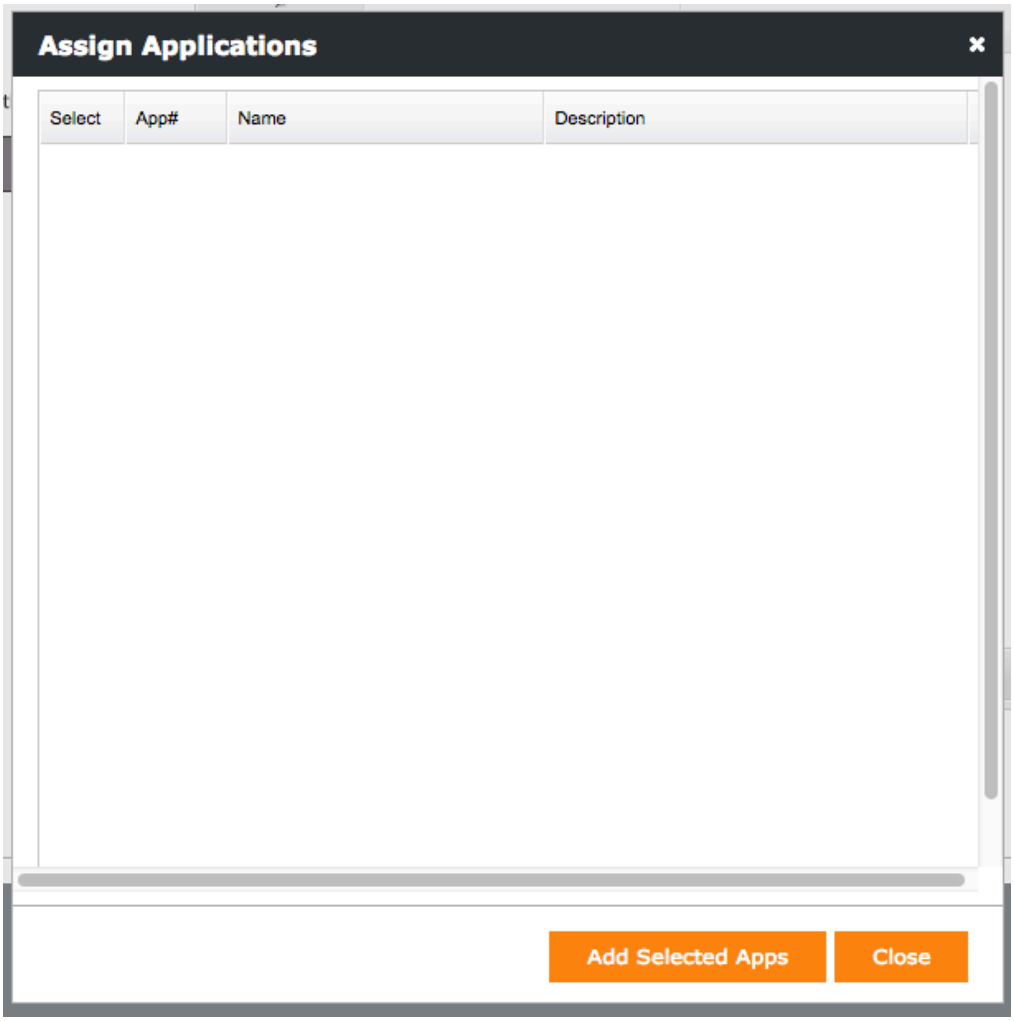
Apps that have been nominated as “KNOX Signed” when being uploaded to the App Portal section can be assigned to KNOX Containers. These apps will be deployed within the Container on the device. This page lists the currently assigned apps, and lets you assign more to the Container.



Action	Description
Assign More Apps	Button that displays the Assign Applications popup window (see below).
Type	Displays the App type
Name	The Name of the App.
Description	The App Description
Remove	Removes the App from the Tag

5.3.6. Assign More Apps

After clicking Assign More Apps, a list of applicable apps will be shown. The apps listed on this screen are those that are both assigned to Samsung SAFE Device types, and have the KNOX Signed option ticked. To assign an app, tick the checkbox associated, and then click Add Selected Apps

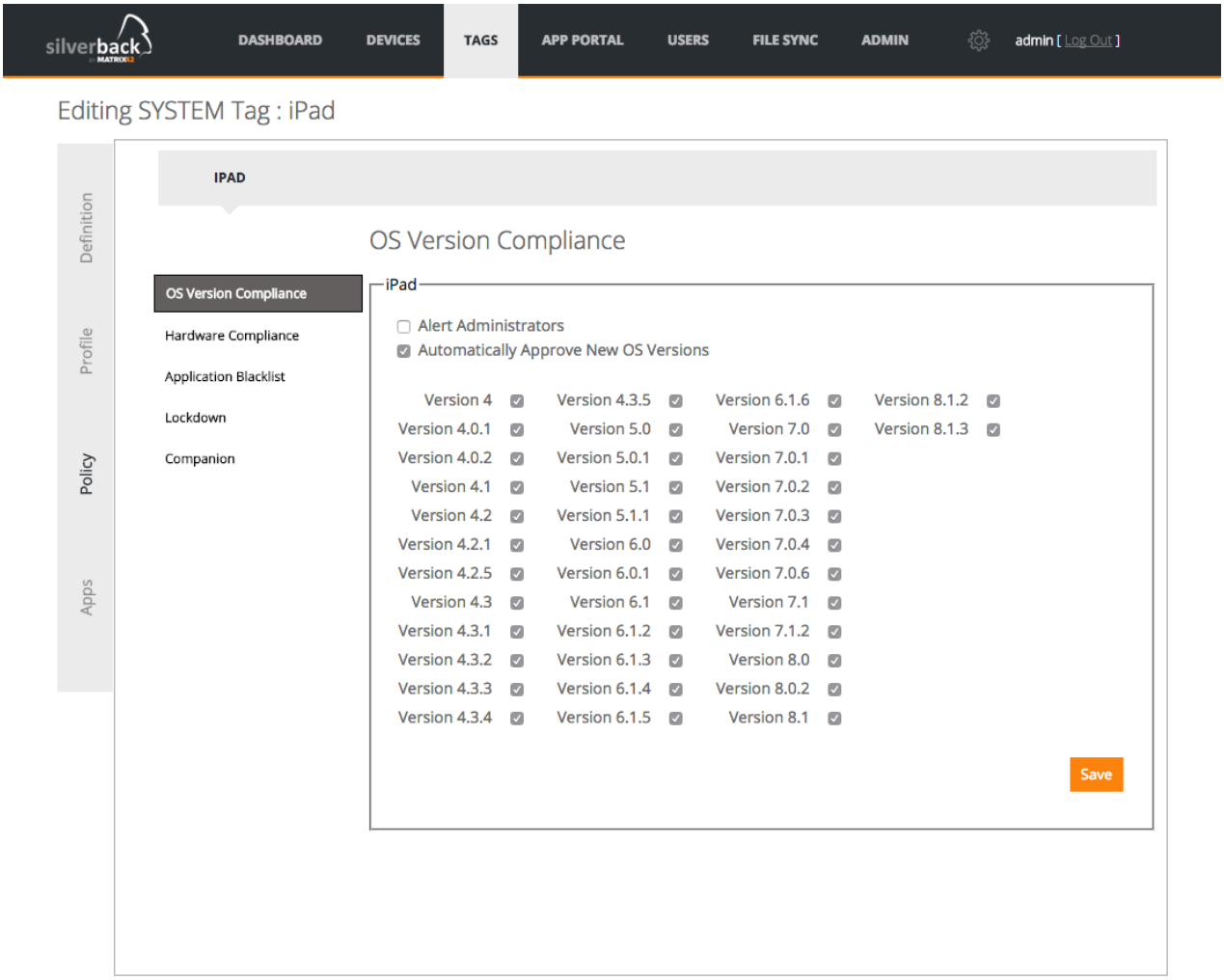


Action	Description
Assign More Apps	Button that displays the Assign Applications popup window (see below).
Type	Displays the App type
Name	The Name of the App.
Description	The App Description
Remove	Removes the App from the Tag

5.4. Policies Feature

Policy is a feature where the Administrator has the ability to enforce rules with Silverback, such as enforcing what Apps are installed on the devices, what Cellular Networks the device is on through to enforcing the Serial Numbers of the devices as they are enrolled into the system.

These are the environmental conditions that Silverback will continue to monitor for and 'police' for any devices that are associated with the Tag.



5.4.1. OS Version Compliance

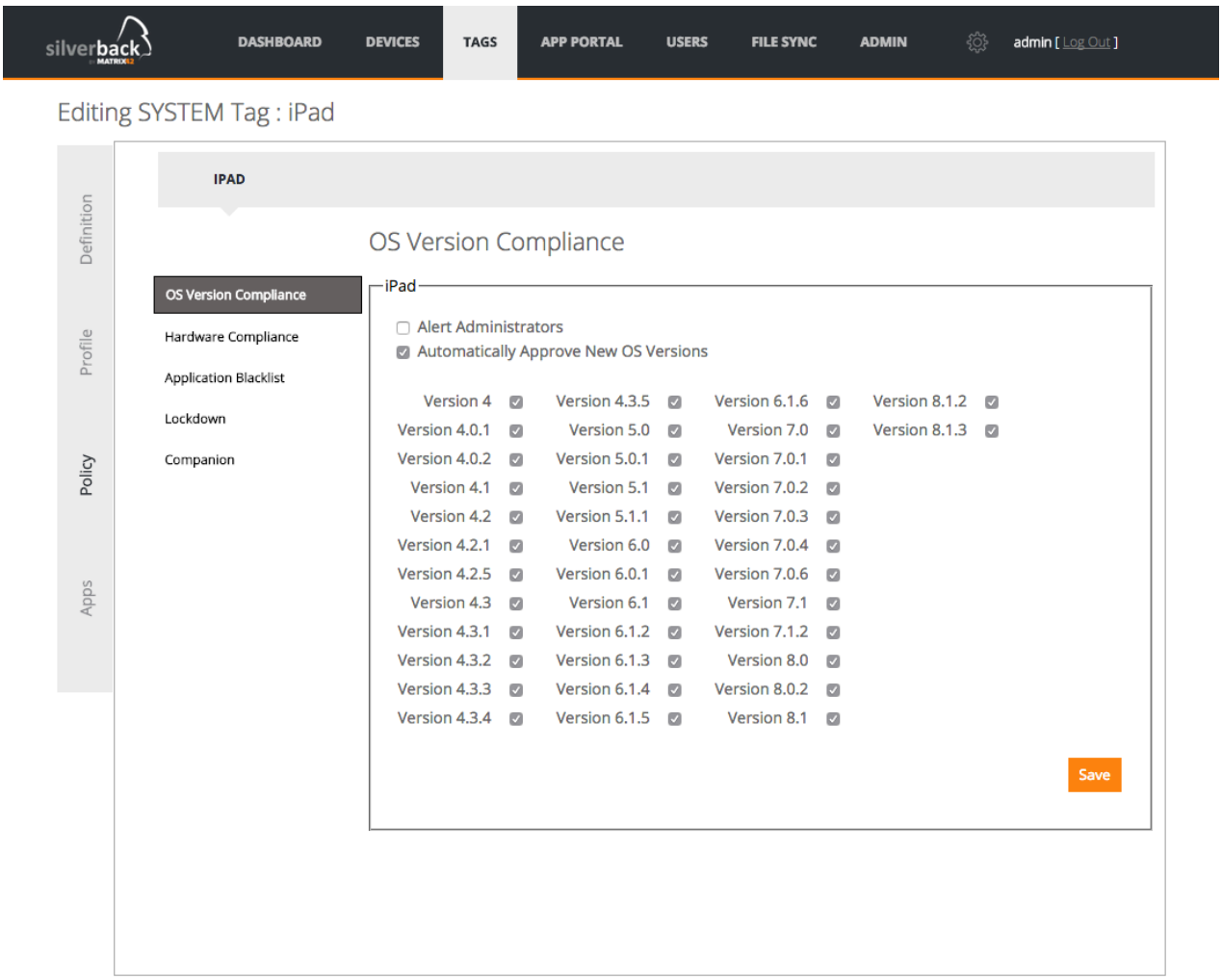
Administrators have the ability to control which OS versions are allowed within their environment. To allow an OS version, simply ensure the checkbox next to the respective OS version is ticked. Enrolling a device with a disabled OS version will result in the device automatically being blocked (see Blocked Devices section for more information).

When the 'Alert Administrators' checkbox is checked, all administrators will receive an email when a device that violates OS compliance is detected, or when a new OS version is discovered.

5.4.2. Automatically Approve New iOS Versions

When an OS platform is enrolled to Silverback for the first time, the OS is automatically added to the list. By default, unknown OS platforms are disabled and relevant devices will be blocked.

To automatically authorize new OS versions as they are discovered, ensure the 'Automatically Approve new OS Versions' checkbox is ticked e.g. use this feature where you do not want devices to be automatically blocked when a user upgrades their device to a new future OS version that is released by their software vendor.



5.4.3. Hardware Compliance

Administrators have the ability to enforce a hardware compliance policy through Silverback. Simply uncheck the boxes for hardware types that should not be supported and any devices that match the hardware type and are managed by Silverback will be blocked.

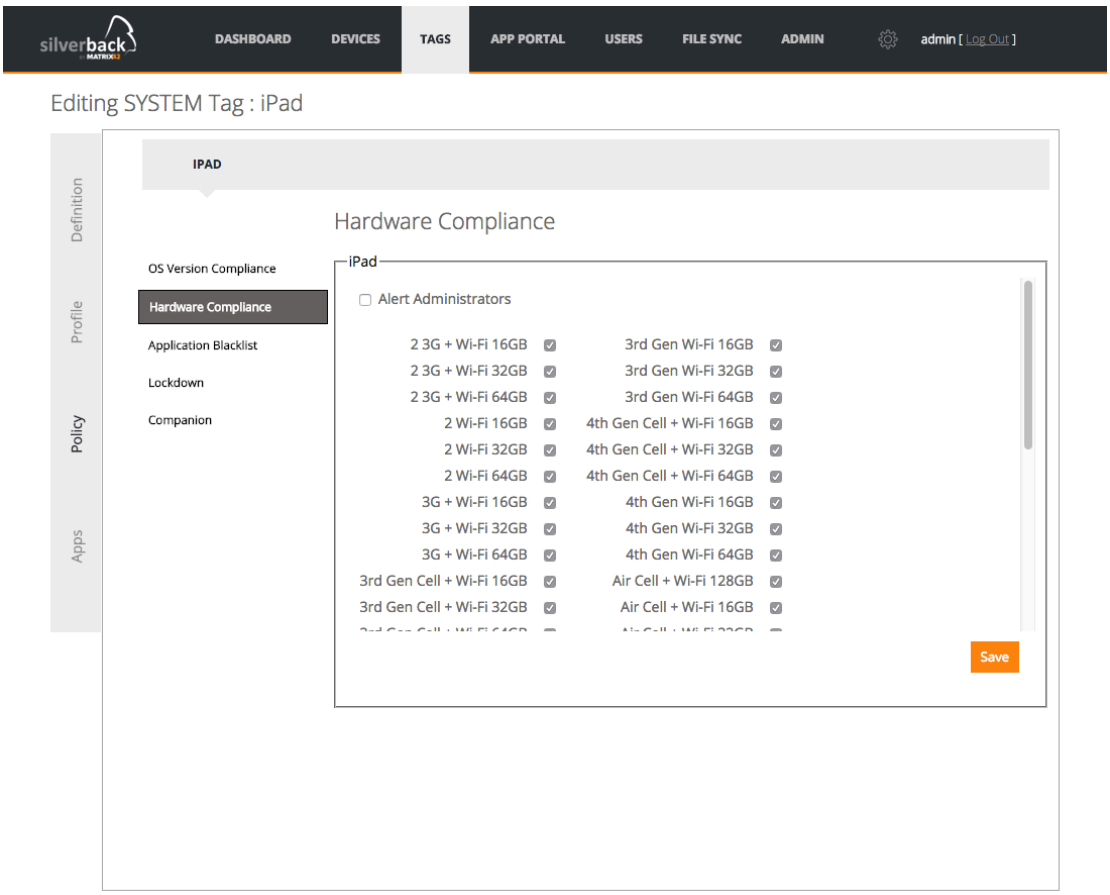
Checking the 'Alert Administrators' checkbox will ensure that administrators receive an email when a device that violates hardware compliance is detected.

The list of hardware types is managed via the Device Types option in the Admin Tab of the Silverback Console. If a mapping from device type to hardware type exists, the hardware type will be displayed in the hardware compliance list.

5.4.4. Unknown Device Types

When a Device Manufacturer release a new version of their hardware the model numbers may not be known by Silverback, in this case Silverback will 'learn' them and store them as 'Unknown' in the Device Types section under the Admin Tab where the Administrator can update them manually.

To allow these devices into your system you enable the 'Unknown' checkbox option. This will allow the device into your Silverback Environment, you can later re-classify this device type in the Admin > Device Types section of the Silverback Management Console.



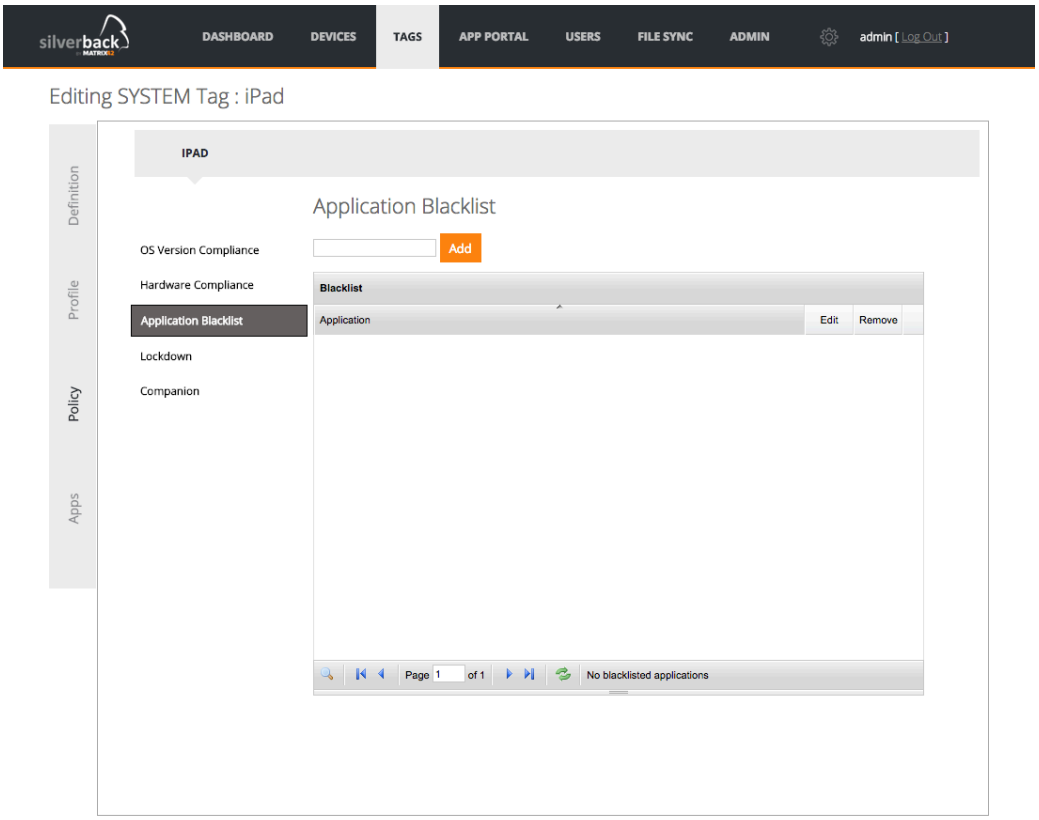
5.4.5. Application Blacklist

Silverback maintains a blacklist of application names to ensure the detection and management of devices with blacklisted applications. The blacklist works by matching application names of applications on devices against the strings in the blacklist. The blacklist employs a case-insensitive substring search algorithm to determine policy violations.

To add an application name to the blacklist, simply enter in the name of the application in the text box and click Add. The table below provides as an example of the applications which are considered a match and which are not when 'kick' is added as a Blacklist Entry:

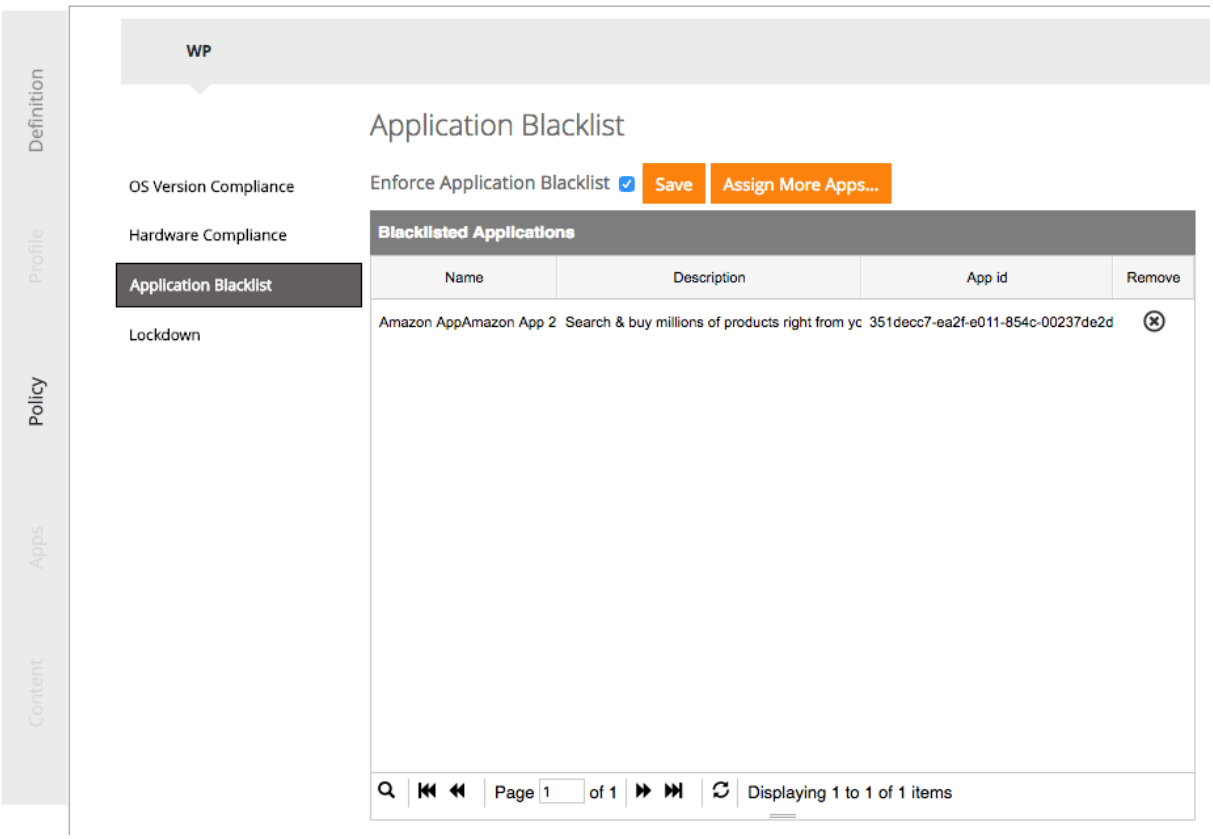
Match	No Match
Kicker	Kic
High Kick	Ki ck
Rekick	Rick
Kicking	K I C K

For Samsung SAFE Devices, enforcing the blacklist on the device is supported, but this requires entering the specific application identifier. E.g. "com.company.appname". If "Force" is selected as the Policy Lockdown option, then these applications will not be able to be installed or launched on the device.



Action	Description
Edit	Edit the selected value in the blacklist
Remove	Delete the value from the blacklist

For Windows Phone devices, the Blacklist functions slightly differently. Because we need to provide a very specific identifier to the device, the applications must be first added to the App Portal and then added to the blacklist:



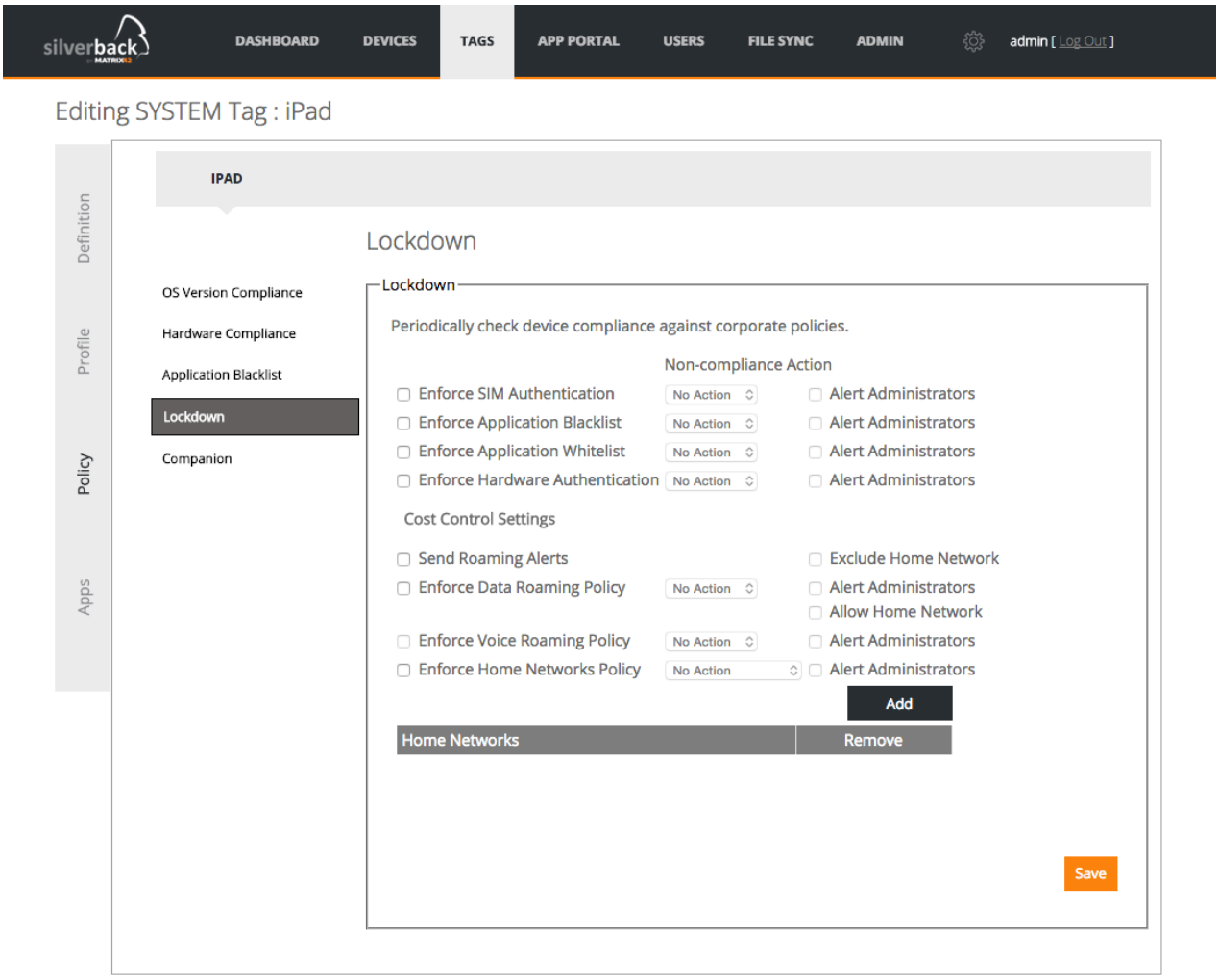
Action	Description
Enable	Enables and disables the Application Blacklist for this Tag
Save	Saves the changes you've made.
Assign More Apps…	Allows you to choose Apps to add to the list. This list of apps is based on the apps assigned to WP in the App Portal tab.

5.4.6. Lockdown

The Lockdown screen allows you to determine what device compliance policies are enabled and what action should automatically occur when a violation is detected. Each policy is enabled/disabled through their associated checkbox.

Enabling a lockdown policy ensures that the device is inspected to ensure it is compliant with that policy during the initial enrollment as well as at regular intervals as defined by the 'Perform check every' drop down.

Silverback by Matrix42 Admin Guide Version 5.1 U3



Autor: Matrix42 Cloud & Mobile Management

5.4.7. Lockdown Policies

The following policy configurations can be managed from this screen:

Policy	Configuration
SIM Authentication	The first SIM Silverback detects on a managed device will be considered the 'canonical' SIM. Any subsequent changes to the SIM (e.g. removal of the SIM from the device or changing the SIM on the device) are considered a policy violation.
Application Blacklist	See the blacklist section for more information on this configuration. The blacklist can be enabled or disabled from this screen.
Application Whitelist	Application Whitelist will ensure that each iOS device has only applications approved by a system administrator that reside in the Silverback App Portal. Whitelist is derived from the Application Name. Ensure applications in the App Portal are labelled correctly prior to enabling Application Whitelist. For Windows Phone devices, the whitelist can be select to block all apps, block all non-Microsoft apps, or block all non-Microsoft apps and Facebook. While Facebook is not a Microsoft App, the OS considers it to be, so a distinction is made.
Hardware Authentication	See the hardware authentication for more information on this configuration. Hardware authentication can be enabled or disabled from this screen.
Send Roaming Alerts	Enabling this will send an alert to all Silverback Administrators when a device starts Roaming for any reason (Voice/Data). **Note** 'Exclude Home Network' checkbox allows the Administrator to disable roaming alerts for devices roaming on Home Networks
Data Roaming	You can choose which lockdown action to apply when a device has data roaming enabled. Availability of this setting on the device is dependent on the Carrier. **Note** 'Allow Home Network' checkbox allows the user to roam on Home Networks without triggering lockdown action
Push While Roaming **(Samsung SAFE Only)**	You can choose which lockdown action to apply when a device has push enabled while roaming. To disable it completely, select Force as the Non-Compliance Action. **Note** 'Allow Home Network' checkbox allows the user to use push on Home Networks without triggering lockdown action
Sync While Roaming **(Samsung SAFE Only)**	You can choose which lockdown action to apply when a device has sync enabled while roaming. To disable it completely, select Force as the Non-Compliance Action. **Note** 'Allow Home Network' checkbox allows the user to sync on Home Networks without triggering lockdown action
Voice Roaming	Voice Roaming is when the device has Voice Roaming Enabled = YES on the device. Availability of this setting on the device is dependent on the Carrier.
Enforce Home Networks Policy	Enables the 'Home Networks' policy, meaning Silverback Admins can specify what data networks are classed as 'Home Networks'.

Policy	Configuration
Home Networks	This Grid is where Silverback Admins can specify their 'Home Networks'.
Full Disk Encryption	Determines if OS X devices require Full Disk Encryption or not.

5.4.8. Lockdown Actions

The following actions can be automatically performed on the device when a violation is detected:

Action	Description
Lock	A lock command is sent to the device which will lock the screen of the device. See 'device management' for more information.
Block	The device is blocked, and the device is moved to the blocked devices table. See 'device management' for more information.
Wipe	The device is hard reset to factory default settings. See 'device management' for more information.
Re-Apply (iOS Only)	For Data / Voice Roaming Policy Only – this will re-apply the iOS Setting that disables the ability for the device to roam for voice or data.
No Action	No action is performed on the device; however alerting administrators may be performed if configured.
Force (Samsung SAFE Only)	This has the same behaviour as "Re-Apply" for iOS, with the exception that the setting is forced upon the user. For application black list in particular, this will prevent the application from launching or being installed on the device.
Alert administrator	Emails are sent to all administrators notifying them of the policy violation when it is detected. This can be configured independently of other configurations.
Block All (WP Only)	For Windows Phone devices, will block all apps on the device
Block Non Microsoft (WP Only)	Will block anything that isn't distributed by Microsoft
Block Non Microsoft and Facebook (WP Only)	Will block anything that isn't distributed by Microsoft, including Facebook (technically this is distributed by Microsoft).

5.4.9. Companion

Companion extends end point security provided by EPiC into a secure workspace for your users. Users can store and edit files locally within the application, ensuring that these documents are kept securely and cannot be accessed by other applications or users. Companion also allows users and administrators to manage data usage on the device and configure policy settings around this.

Access to SharePoint sites and other websites can also be added to Companion clients for your users, ensuring any content they access through Companion remains secure.

Companion allows the administrator to control data allowance and specify lockdown actions for the excess data usage.

To Enable Companion for the Tag, enable the checkbox “Companion Enabled”. Then configure the various settings as documented below.

As of version 4.7, Companion for iOS is also available from iTunes. If you want to utilise this version, select “Install Companion App Store” from the Companion settings. In the scenario where one Tag uses App Store, and another Tag uses Enterprise Companion, the App Store setting will win.

It’s also possible to use VPP licensing to deploy the App Store version of Companion. This is helpful if you don’t want your users to use iTunes accounts, and you utilise Device Based VPP licensing. This requires that you have an active configured VPP account, and also that you have Companion licenses in that VPP program.

5.4.9.1. Companion Settings

The settings in this group control the Bookmarks and SharePoint sites that are being deployed to the users

.

Setting	Description
Bookmarks	Displays a list of Bookmarks being pushed to Companion Clients.
SharePoint Sites	Displays a list of SharePoint Website URLs being pushed to Companion Clients.
Certificates	Displays a list of certificates that can be configured and then assigned to Bookmarks and SharePoint Sites
Bulk Message	Sends a message to all Companion users within the given tag.

5.4.9.2. EPiC Settings

The settings in this group control the behavior of the EPiC module of Companion.

Setting	Description
Secure Enrollment	Enables EPiC Secure Enrollment for devices.
Offline Grace Period	Companion modules will be blocked if the device doesn’t check in during this period.
Custom Epic Text	Configure custom text to be displayed to the user.

Setting	Description
Show Blocked Reasons	Configures whether the user is told why they have been blocked. If this is disabled the user is not told why, simply that they are blocked.
Allow Automated Unblocking	Companion can allow users to rectify a block where it was triggered by a policy violation. For example if the user violated an application blacklist, they may remove the app and then scan with Companion to automatically become unblocked..

5.4.9.3. File Settings

The settings in this group control the behavior of the File module of Companion.

Setting	Description
Allow Files	Determines whether the Files, Bookmarks and SharePoint sites modules are available to the users.
Disable on Blocked	Disables the Files module when Silverback blocks the device.
Require PIN	Determines whether the users are required to have a PIN code protecting Companion.
Allow Email Out	Allow the user to email files out of Companion or not.

5.4.9.4. Data Cost Control Settings

The settings in this group control the general behaviour of the Data Usage module of Companion.

Setting	Description
Allow Usage	Determines whether the Data Usage module is available to the users.
Disable on Blocked	Disables the Data Usage module when Silverback blocks the device.
Allow User to Change Settings	Allow the user to change settings within the Companion Client. If not, the administrator must define settings.
Rollover Day	Determines the day for the Data Usage to be reset on the device.

5.4.9.5. Local Data Cost Control Settings

The settings in this group control the behaviour of the Data Usage module of Companion for the users on the local cellular network.

Setting	Description
Allow User to Reset Usage	Allow the user the ability to reset their local Data Usage within the Companion client.

Setting	Description
Data Allowance (MB)	The Amount of local Cellular Data the user is allowed, until the user is alerted and the configured action is performed.
Action on Local Data Limit Reached	The MDM action that is carried out when the local data limit is reached.
Alert Administrators	Determines whether the administrative e-mail alert is sent out when a device reached the data limit.
Consumed Usage Alert Threshold	Determines the threshold value for the local Data Allowance usage alert. When this threshold is reached, the user receives a notification on the device.

5.4.9.6. Roaming Data Cost Control Settings

The settings in this group control the behaviour of the Data Usage module of Companion for the users on the roaming cellular network.

Setting	Description
Allow User to Reset Usage	Allow the user the ability to reset their roaming Data Usage within the Companion client.
Data Allowance (MB)	The Amount of roaming Cellular Data the user is allowed, until the user is alerted and the configured action is performed.
Action on Roaming Data Limit Reached	The MDM action that is carried out when the roaming data limit is reached.
Alert Administrators	Determines whether the administrative e-mail alert is sent out when a device reached the data limit.
Consumed Usage Alert Threshold	Determines the threshold value for the roaming Data Allowance usage alert. When this threshold is reached, the user receives a notification on the device.

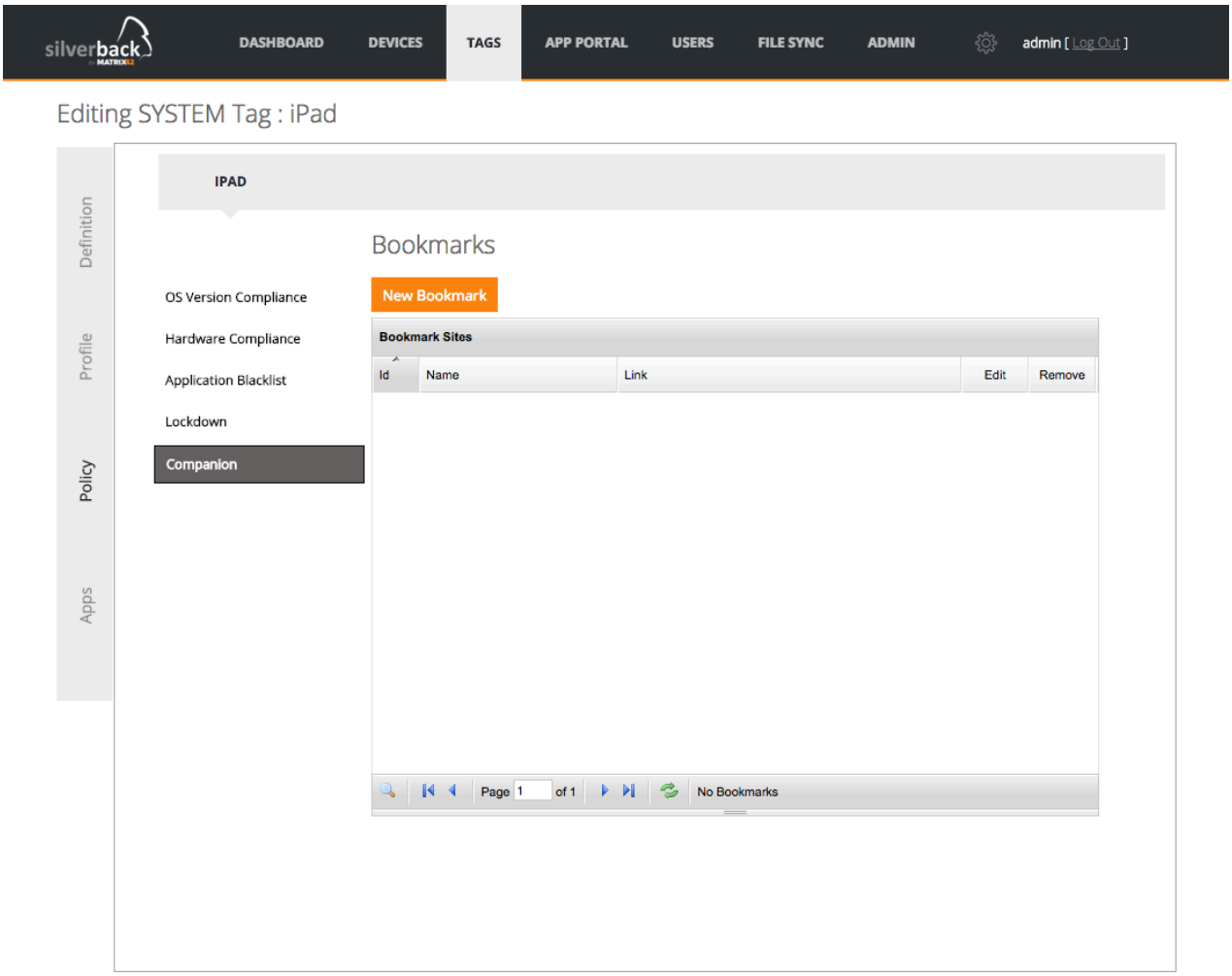
5.4.9.7. License Message Settings

This setting controls the message displayed to the users when no valid Companion license is available.

Setting	Description
Invalid License Message	The text message displayed on the users' devices.

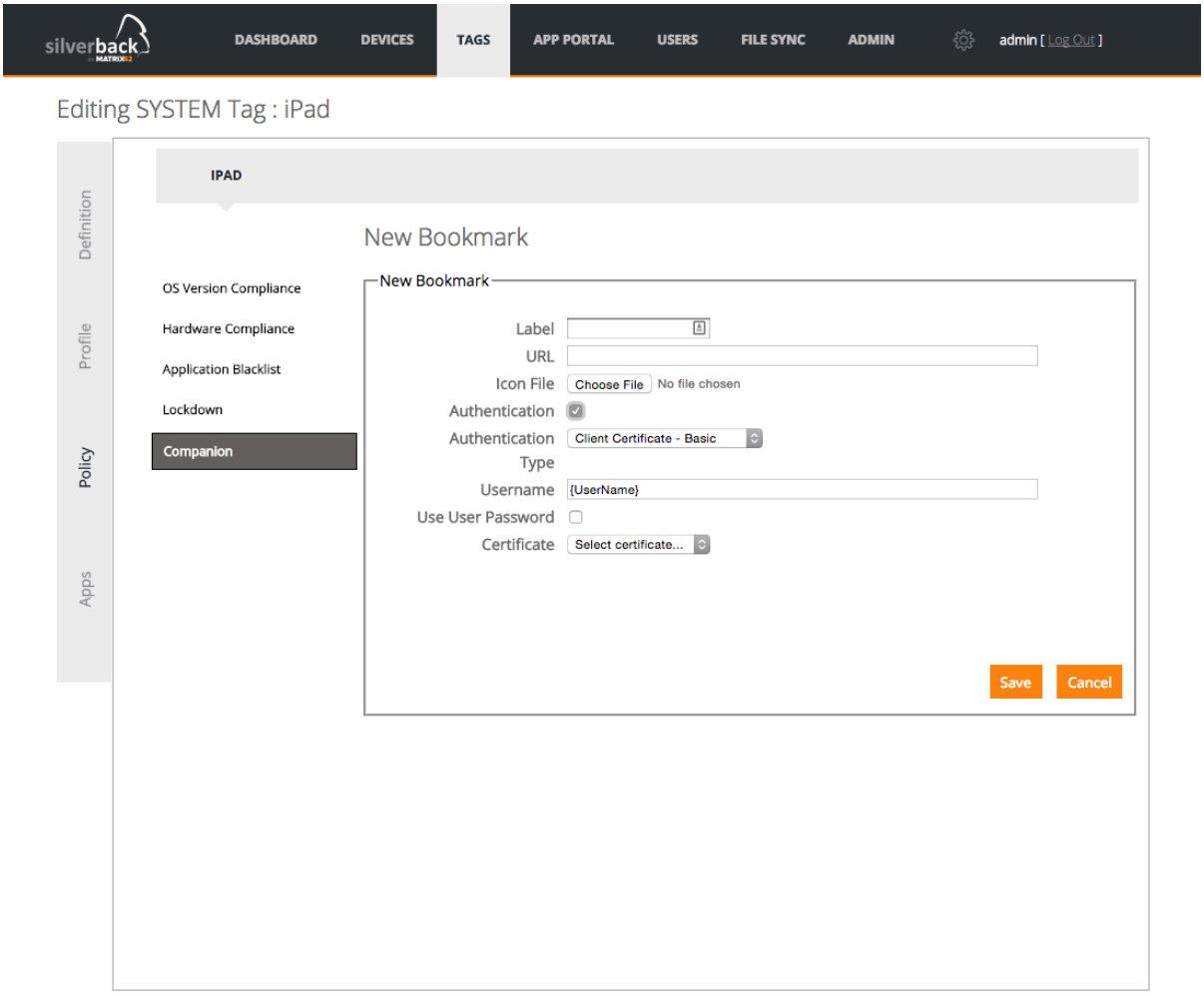
5.4.9.8. Companion Bookmarks

Companion Bookmarks are a way to deliver sensitive URLs to end-users within the Companion Client itself, to add an extra level of security to these Bookmarks.



Field	Description
New Bookmark	Button to the New Bookmark Screen.
ID	ID Number for the listed Bookmark.
Name	The Name of the listed Bookmark.
Edit	Edit the listed Bookmark.
Remove	Deletes the listed Bookmark.

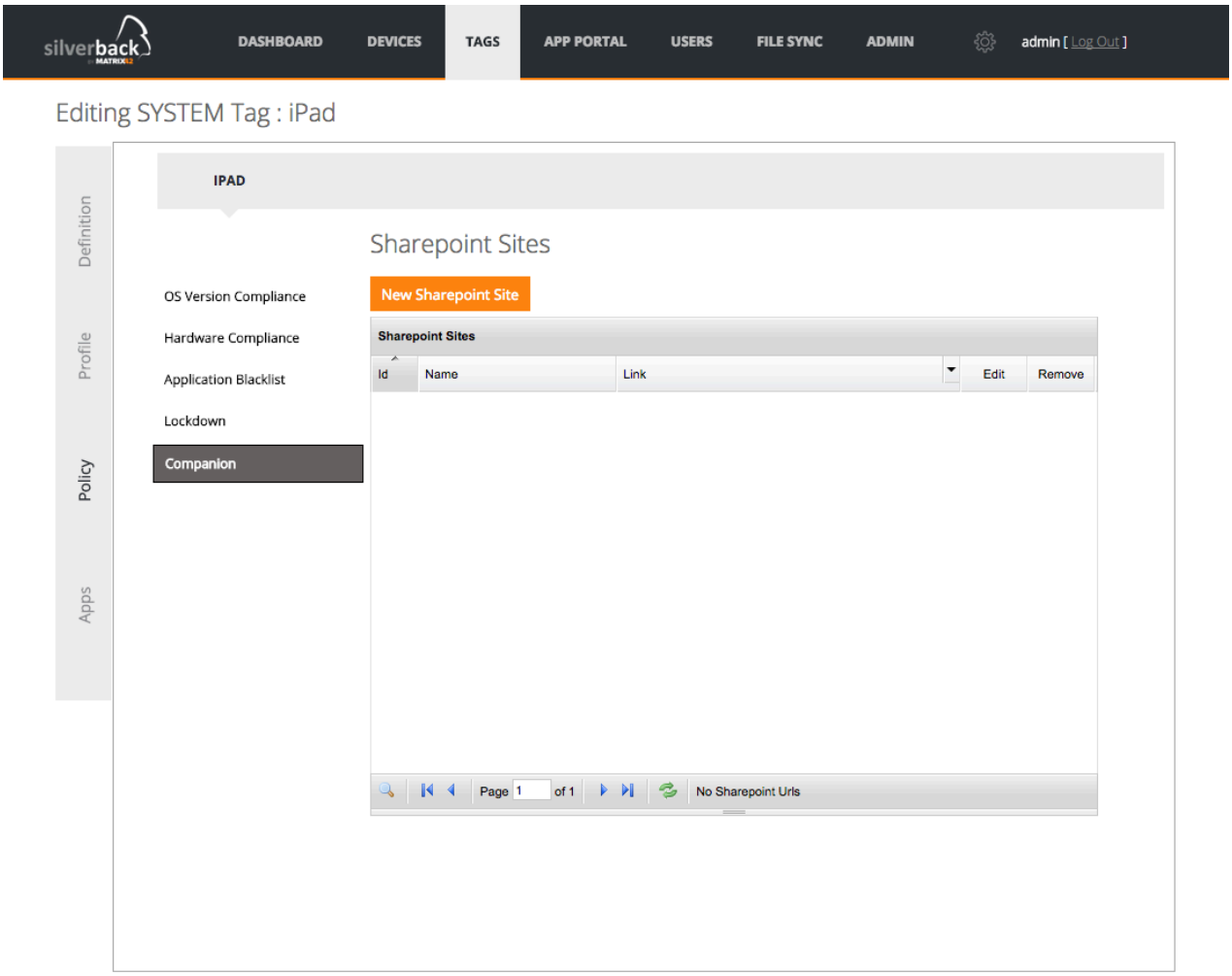
5.4.9.9. Adding a Companion Bookmark



Field	Description
Label	Display Name of the bookmark.
URL	Website Address.
Icon File	Allows the user to select an icon file.
Authentication	Enables or disables authentication options for the Bookmark
Authentication Type	Choose between Basic and Kerberos for Authentication
Username	Username to use for authentication, accepts System Variables
Use User Password	If available, send the user's password with the settings
Certificate	Select Pre-Defined Certificate payload to use.
Save	Save the new Bookmark.
Cancel	Cancel creating the new Bookmark.

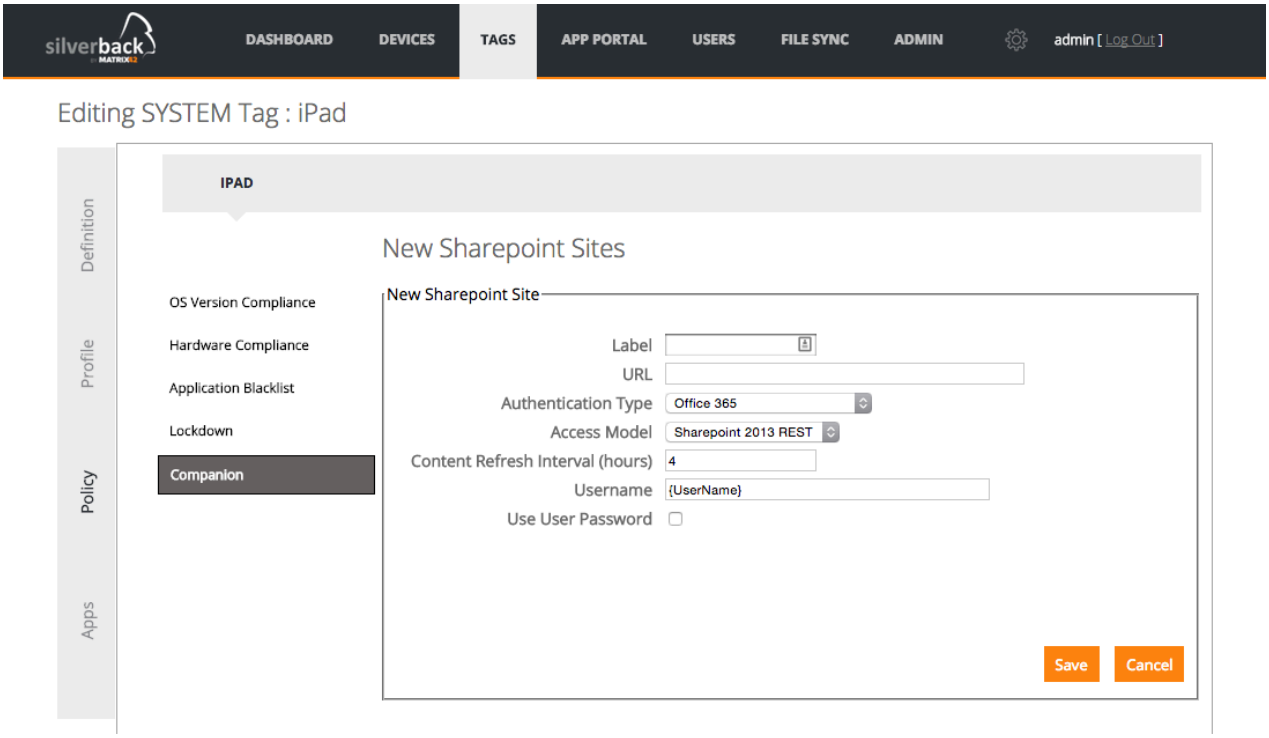
5.4.9.10. Companion SharePoint Sites

The Companion Client also accepts delivery of Sharepoint Site URLs, so your end users can access more secure corporate content, ensuring that any content downloaded from Sharepoint is secure within Companion.



Field	Description
New Sharepoint Site	Button to the New Sharepoint Site Screen.
ID	ID Number for the listed Sharepoint Site.
Name	The Name of the listed Sharepoint Site.
Edit	Edit the listed Sharepoint Site.
Remove	Deletes the listed Sharepoint Site.

5.4.9.11. Adding a Companion Sharepoint Site

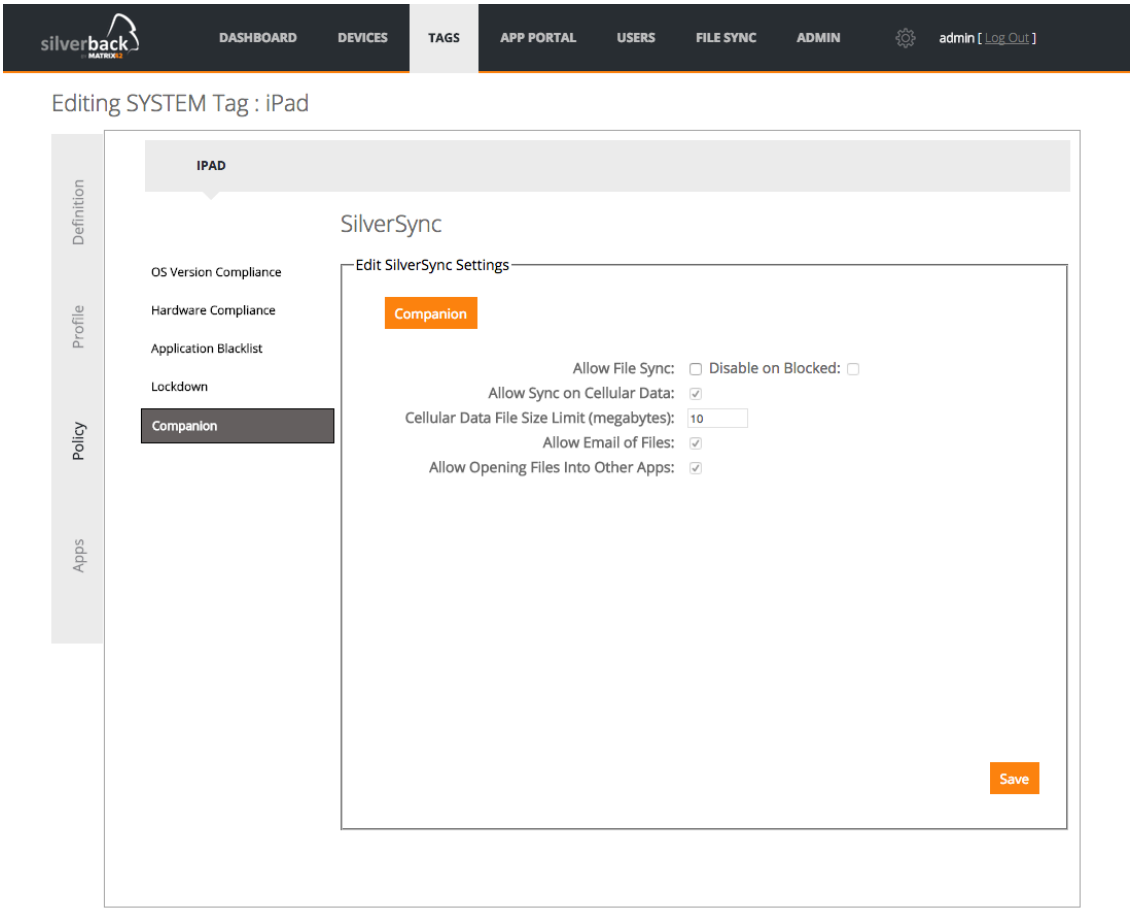


Field	Description
Label	Display Name of the Sharepoint Site.
URL	Sharepoint Site Address.
Authentication Type	The Authentication Model that Companion should use for the target site: Office 365 authentication is only available for Office 365 Basic authentication sends the credentials of the user in the Authorization header Form authentication is a headless authentication method for Sharepoint site configured for Form Based Authentication Webforms authentication requires the user to type their credentials in the web view Client Certificate - Basic will provide a specified certificate to the user to use in conjunction with Basic authentication Client Certificate - Kerberos will provide a specified certificate to the user to use in conjunction with Kerberos authentication
Access Model	The Access Model that Companion should use. Sharepoint 2013 Access Model is recommended for best

Field	Description
	experience.
Content Refresh Interval (hours)	The Interval for Companion to check Sharepoint for Updates.
Username	Field to Specify the Username for the Companion Client. Custom LDAP attributes can be used in this field.
Use User Password	Specifies that the client should automatically use the User's Password (this is only available when Password is Cached or on initial enrollment)
Certificate	Select Pre-Defined Certificate payload to use.
Save	Save the new Sharepoint Site.
Cancel	Cancel creating the new Sharepoint Site.

5.4.9.12. Companion Silversync

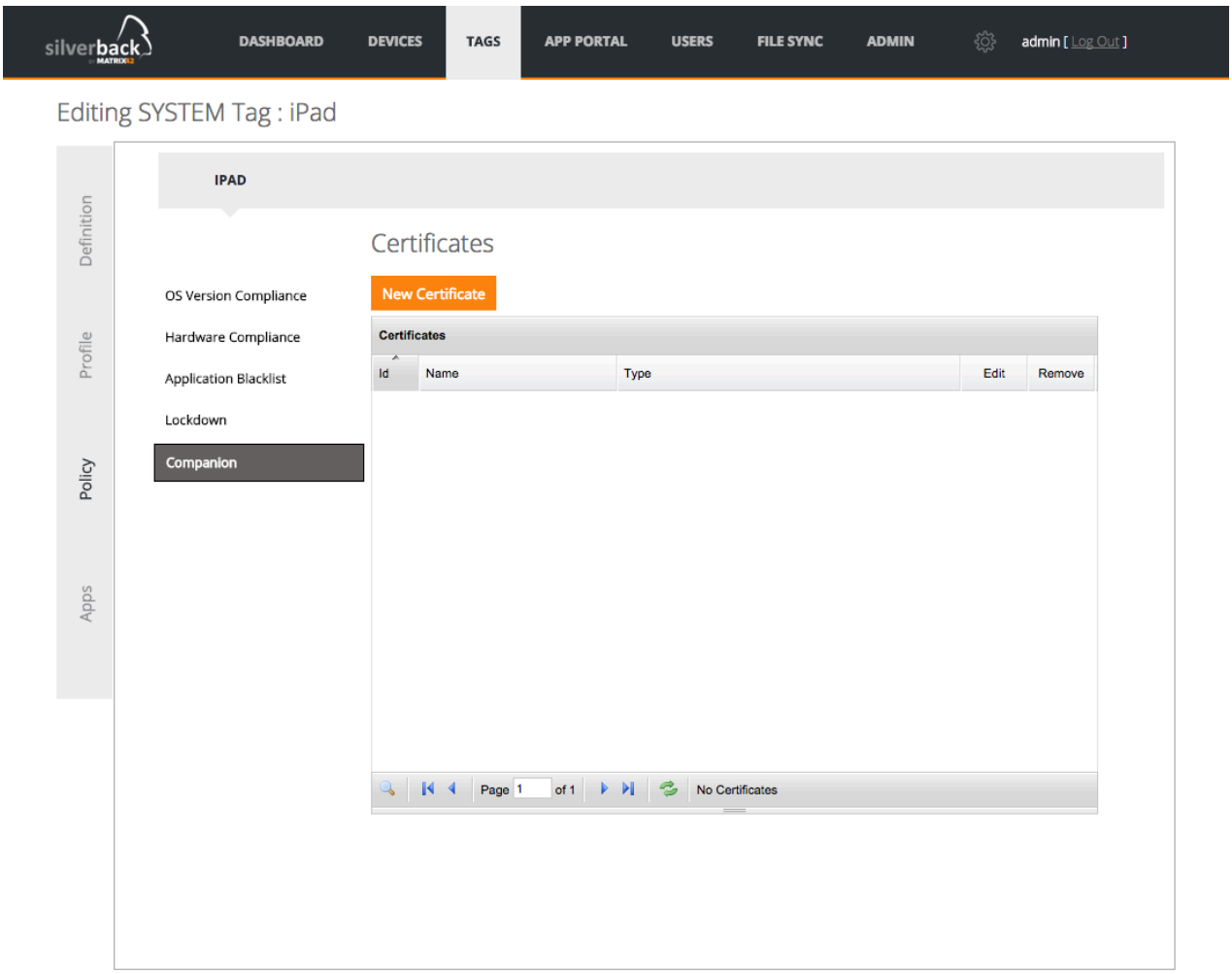
Companion has a file synchronization module called Silversync. Settings for this module can be configured for your devices by ticking Allow File Sync for a Tag.



Field	Description
Allow File Sync	Enables or disables Silversync for this Tag
Disable on Blocked	Will block the user from the module if they are blocked.
Allow Sync on Cellular Data	Determines if users can synchronize over a cellular data connection.
Cellular Data File Size Limit	If the user is allowed to synchronize over cellular data, this will be the maximum individual file size allowed. Files not larger than this will be synchronized next time the user synchronizes over a Wi Fi connection.
Allow Email of Files	Determines whether the user can email files out of the Silversync Module
Allow Opening Files Into Other Apps	Determines whether the user can open synchronized files into other applications on the device.

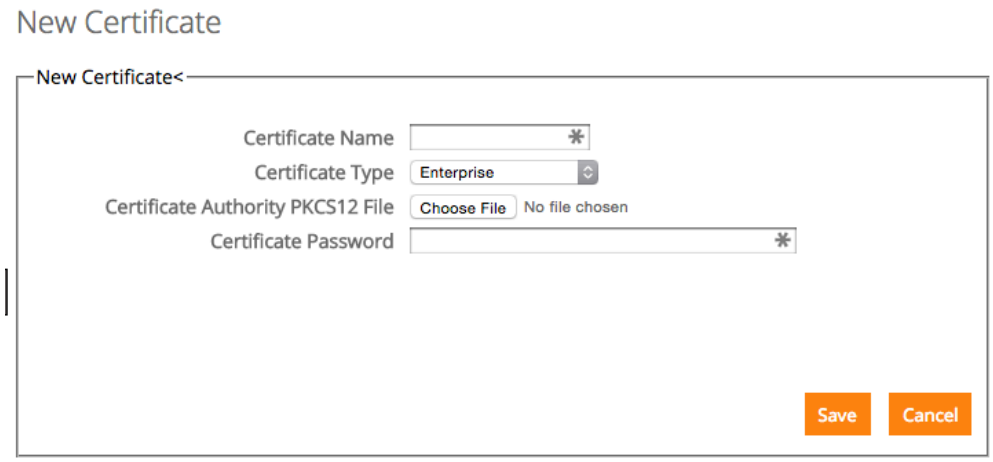
5.4.10. Companion Certificates

Within the Companion settings, certificates can be defined for use with authentication. As the same certificate is sometimes needed for both Sharepoint and Bookmarks, the certificates are defined separately, and then applied where needed.



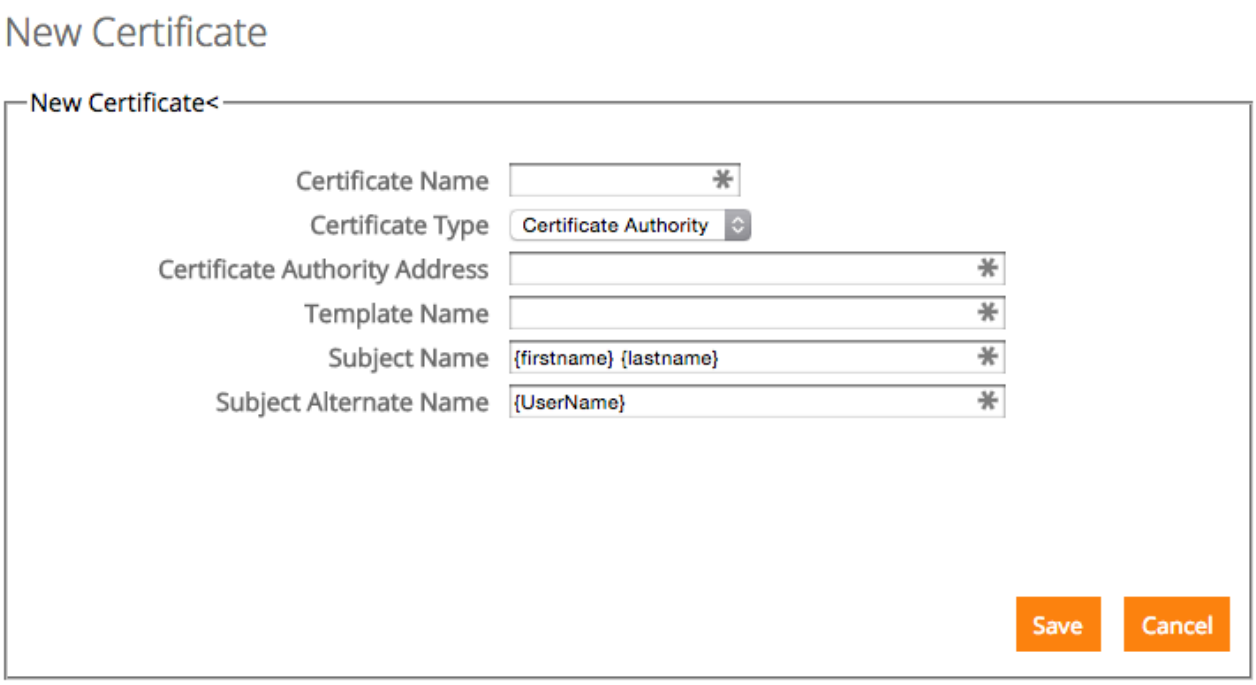
Field	Description
New Certificate	Takes the admin to the New Certificate screen
ID	Unique identifier for the configured certificate
Name	Custom name for the certificate, provided when the Admin creates the certificate.
Type	Determine if the Certificate is from an Enterprise (single PKCS12 Certificate) or Certificate Authority (Certificate is generated per user)
Edit	Edits a particular Certificate
Remove	Removes a particular Certificate

5.4.11. Adding an Enterprise Certificate



Field	Description
Certificate Name	A name that will be used to identify the Certificate settings
Certificate Authority PKCS12 File	A PKCS12 Certificate that will be used to generate client certificates for devices.
Certificate Password	The password for the PKCS12 Certificate Authority Certificate

5.4.12. Adding a Certificate Authority Certificate

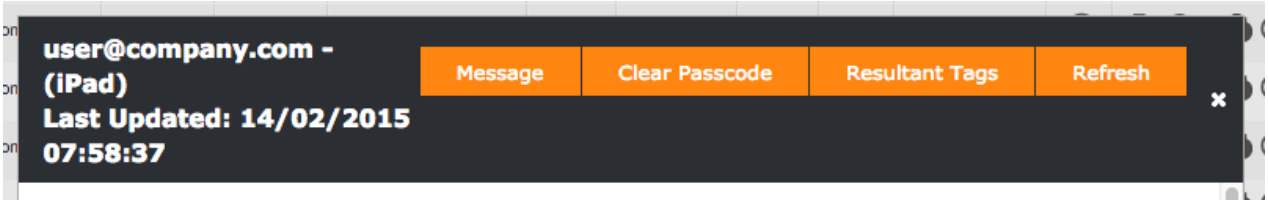


Field	Description
Certificate Name	A name that will be used to identify the Certificate settings
Certificate Authority Address	Network address for the Certificate Authority
Template Name	The template name to be used for Certificate Requests
Subject Name	Subject Name of the certificate (supports variables)
Subject Alternate Name	Subject Alternate Name of the certificate (supports variables)

5.4.13. Companion Individual Messages

The Silverback Companion Client can also receive Text-Based Messages sent from the Silverback Administrator Console in the form of an App Notification when the app is minimized.

Sending a message to an individual device is done from the Device Information Popup Window, which is accessed via the Managed Devices screen.



Field	Description
Enter Message Text	The Message Text that will be sent
Send	Sends the Message Text to all devices associated with this TAG
Cancel	Cancels the send Bulk Message window

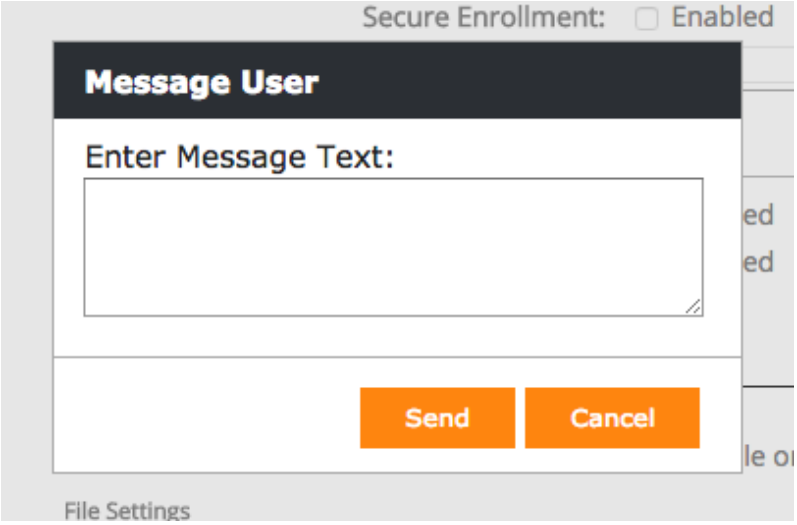
NOTE: The Message Button will only become visible in the User Device Information Screen if Silverback can detect an Installed Companion Client.

NOTE: Device with Companion installed will also receive a Message Notification when they move from Managed to Blocked.

5.4.14. Companion Bulk Messages

Silverback has the ability to send 'Bulk Messages' to Companion Clients that are associated with a specific Silverback Tag.

Below you can see a screenshot of the Companion Bulk Message Screen for the iPad System Tag.

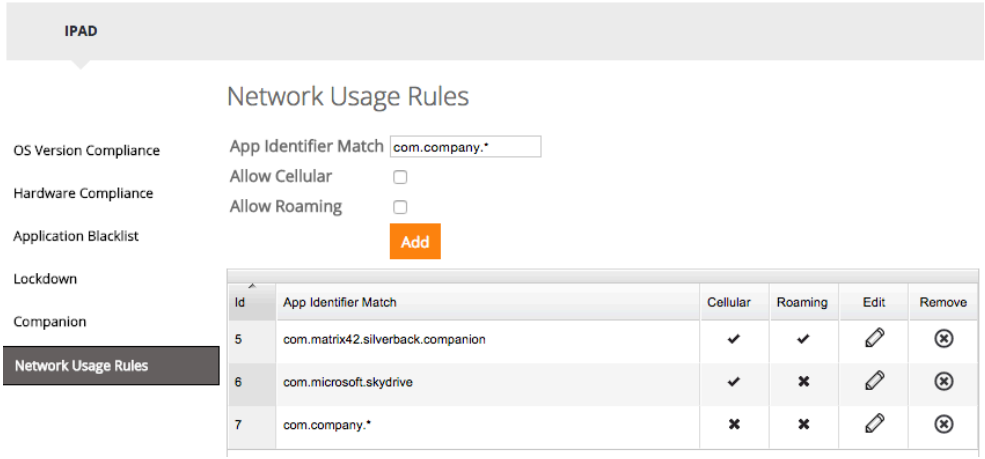


Field	Description
Enter Message Text	The Message Text that will be sent
Send	Sends the Message Text to all devices associated with this TAG
Cancel	Cancels the send Bulk Message window

5.4.15. Network Usage Rules

From iOS 9 and above, it's now possible to define network usage rules for applications. What this means is you can restrict data connectivity on local and roaming networks for specific App IDs. This only applies to Managed Applications.

When entering an App Identifier, you will be presented with a list of applications that Silverback is aware of to help you enter the data quicker. The values also support wild-cards, so entering "com.company.*" would match any identifiers that begin with "com.company"



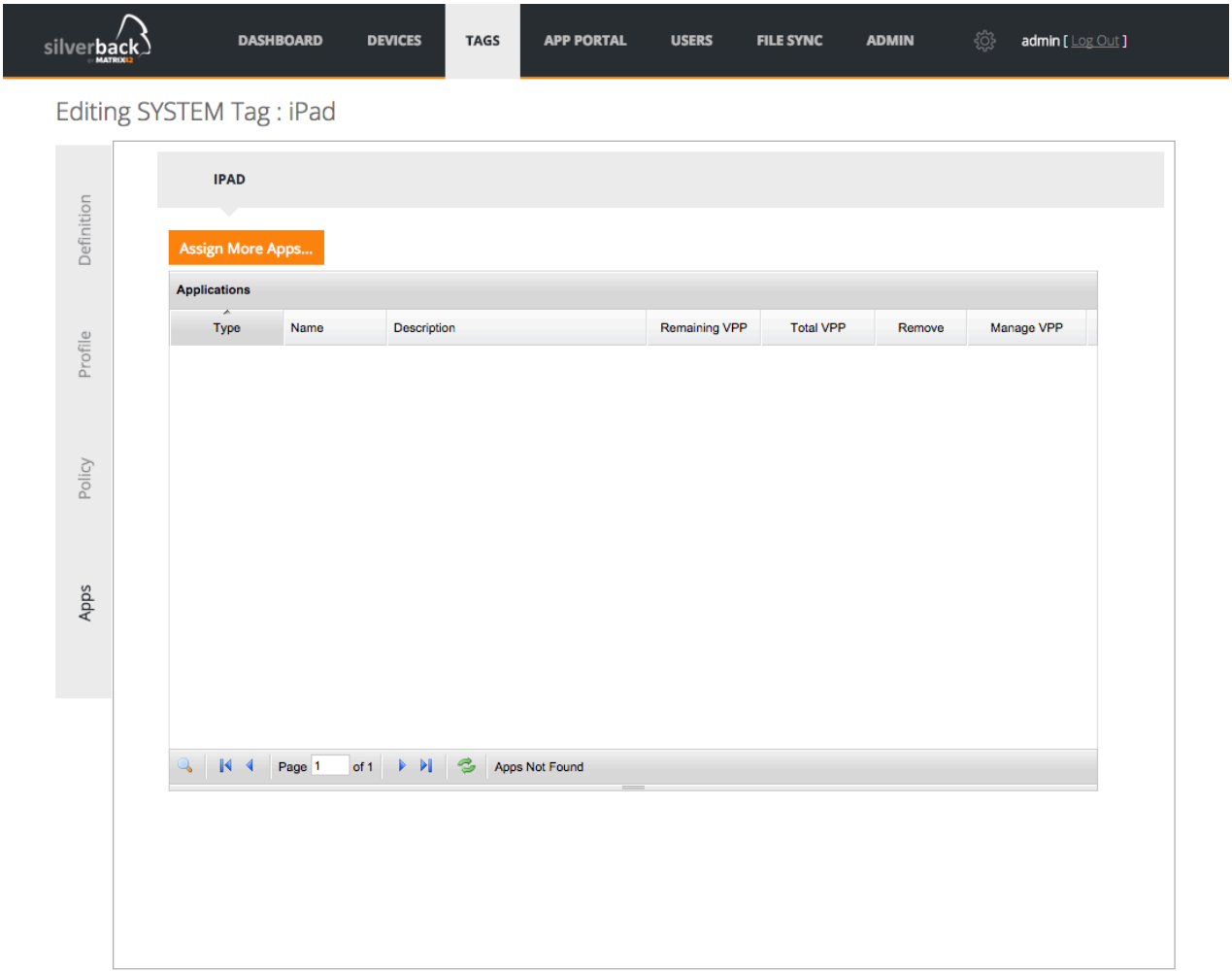
Field	Description
App Identifier Match	The managed app identifier that the rule should apply to
Allow Cellular	Whether the application is allowed to use cellular data
Allow Roaming	Whether the application is allowed to use roaming data

Apps Feature

The Apps Feature Section is how Administrators can automate the distribution of Device Apps for specific groups of users. Before you can begin assigning Apps to the Tag you

first need to have the uploaded into the Silverback App Portal – *for more information on this see the App Portal Tab Section*.

Once you have Apps in the Silverback App Portal, they can be distributed using the Apps Feature associated with your Tag.



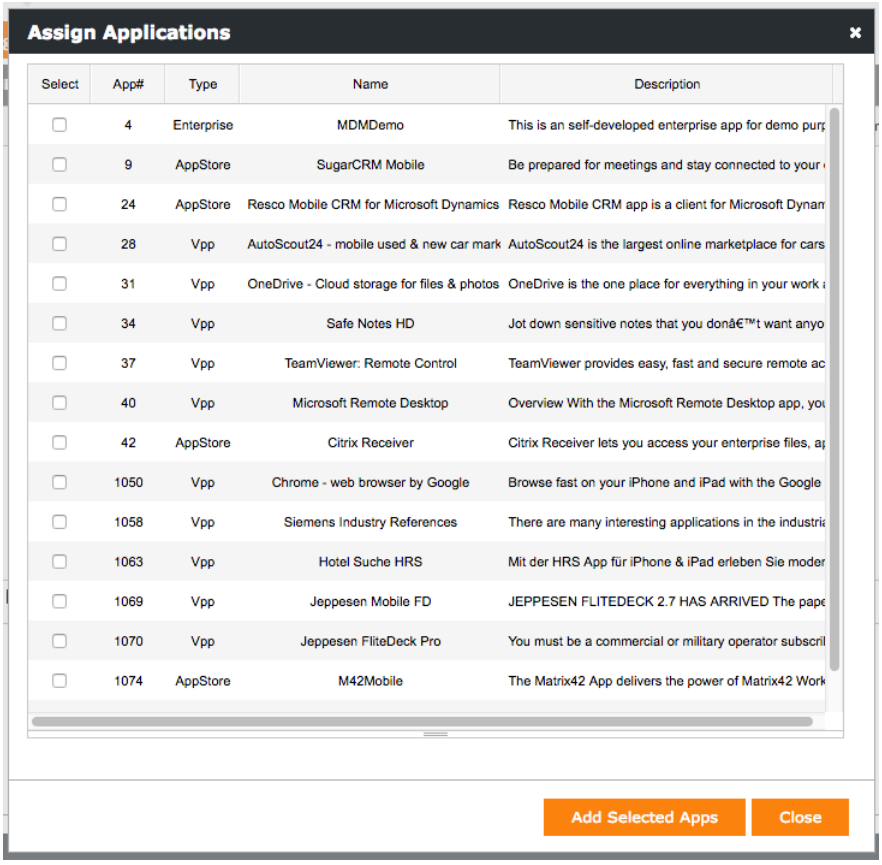
NOTE: The Apps Feature section of Silverback is for assigning pre-configured apps for distribution. For information of Configuring Apps for the Silverback App Portal see the App Portal Tab Section.

NOTE: VPP Stands for Apple's Volume Purchase Program. It is a method for distributing Paid Apps for business customers; please contact Apple for further Information.

Action	Description
Assign More Apps	Button that displays the Assign Applications popup window (see below).
Type	Displays the App type, either App Store or Enterprise.
Name	The Name of the App.
Description	The App Description
Remaining VPP's (iOS Only)	The Remaining Number of VPP Codes
Total VVP's (iOS Only)	The Total Number of VPP Codes for the App
Remove	Removes the App from the Tag
Manage VPP (iOS Only)	Displays the VPP Management screen for the selected App (see Next Page).

5.4.16. Assigning Apps to a Tag

Once Apps are uploaded into the Silverback App Portal Tab, they can be distributed to devices via a Tag they have been associated with.



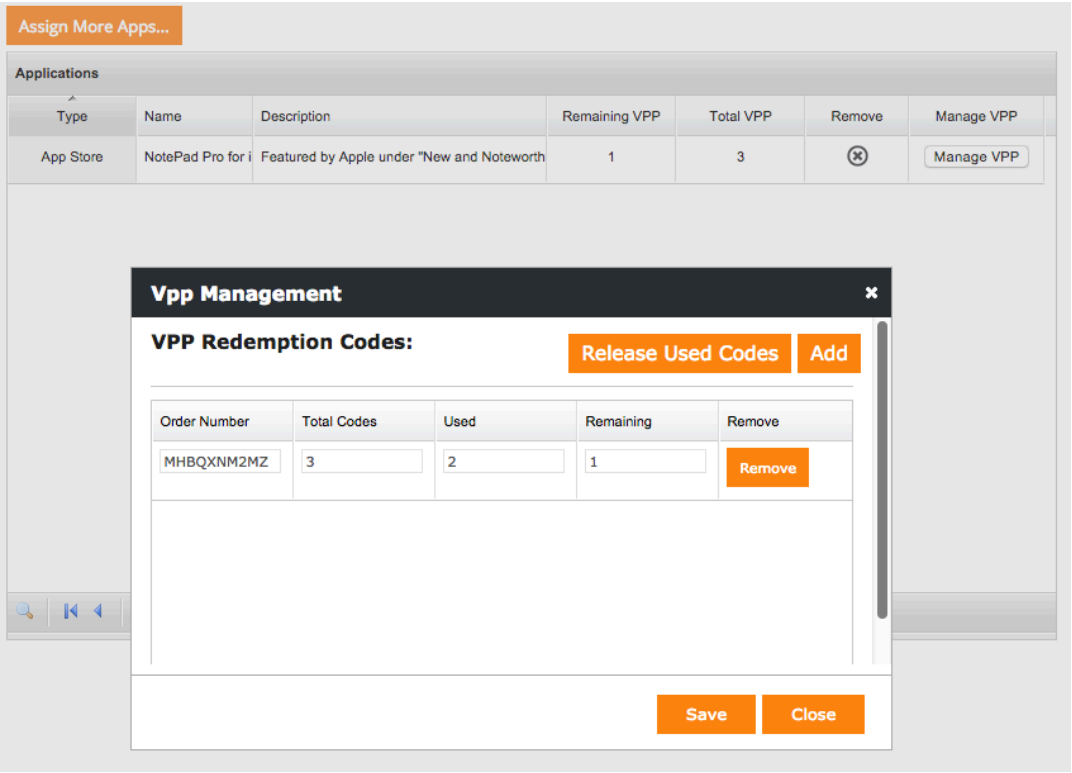
5.4.17. Integrating Apple's Volume Purchase Program

Silverback has incorporated the ability to use Apple's Volume Purchase Program (VPP) to help ensure your device rollout and provisioning process is made faster and easier.

Once that App has been associated with the desired Tag, simply click the **Manage VPP** button visible next to its listing. From there you are able to add and remove old VPP Redemption files.

The nature of the VPP Code Program is that when the user is prompted for installation of the App, Silverback has actually sent a Product Code along with a VPP Code to the iTunes App Store for redemption. Then the device is prompted to install the app from iTunes itself, this is why the user is asked for their iTunes credentials; the VPP Code is being tied to the user account at the time of installation.

The ability to manage these codes is Apple's original VPP method. Since then it's also possible to assign licenses directly to users and devices without the need for a spreadsheet upload. For more information about this process see the VPP section later in the document.



The **Release Used Codes** button has been implemented as a way for Silverback to perform a 'Check' on all the VPP Codes it has used to determine which codes are still available. It will reset the used count to zero (0) freeing up all codes for use again. If the iTunes App Store is sent a used code, it simply requests another code until it receives a valid code; all the while Silverback will be correcting its own internal count.

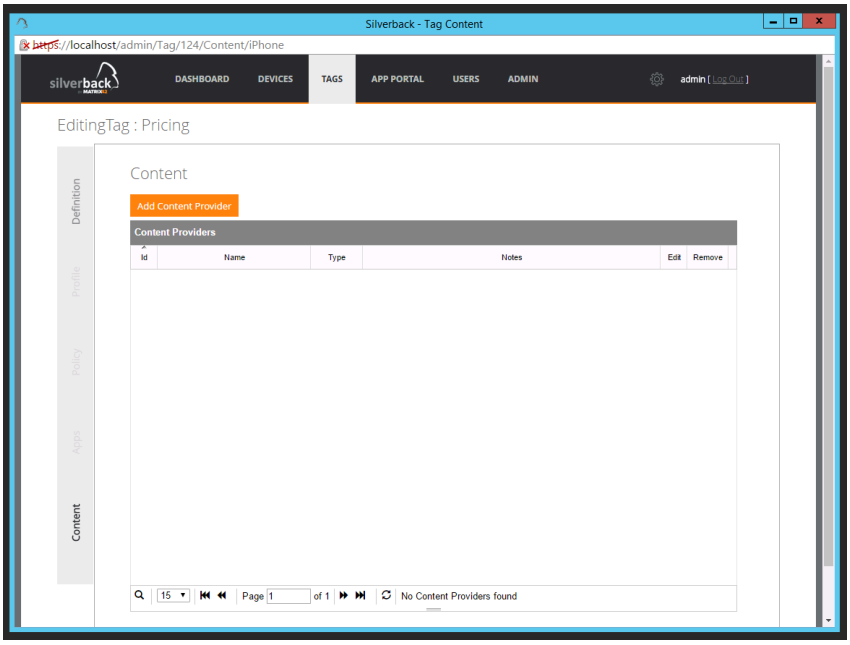
NOTE: Once Silverback determines that there are no valid VPP Codes for use, the user will be re-directed to the App Store to purchase the App Manually.

NOTE: Due to the nature of how Apple has implemented the VPP Program, the count indicated by Silverback may not always be 100% accurate. If the Used License count in Silverback seems high, please manually check your license usage through the Apple VPP Portal.

5.5. Content Feature

The Content Tab is where content locations are provided for users. These are defined at a Tag level which means only users in this Tag will receive these content settings in their M42Mobile app.

The “Content” Tab should be available from the left menu, click this to go to the Content Providers section:



Click Add Content Provider and you will be able to define the settings for the Content Provider, give the settings a name and a note if required. It might be useful to use the note field to explain to other administrators what these settings are and what content they map to.

5.5.1. Cloud Content Providers

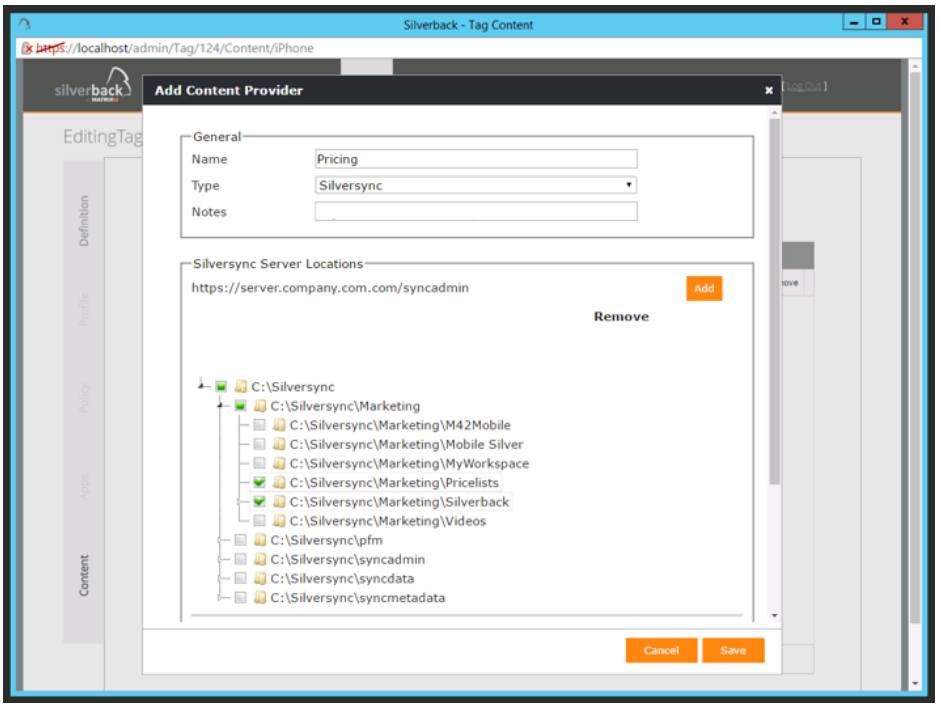
Unlike Silversync Content Providers (mentioned below), you can also configure public content applications for users. Currently supported are:

- Box
- Dropbox
- Google Drive
- OneDrive
- ownCloud

Note that all of these support a common configuration, that is username and password, except for ownCloud, which also requires a server address. The Username and Password fields support system variables, so you can dynamically configure these for all users.

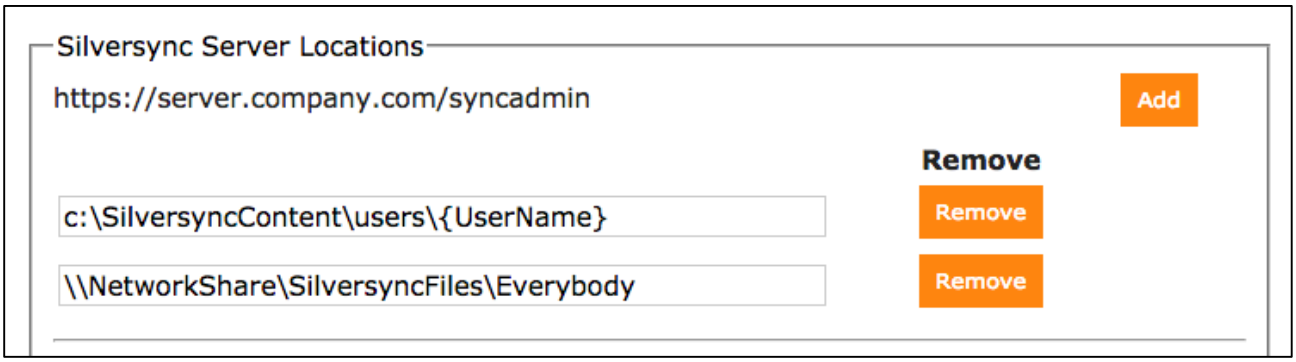
5.5.2. Silversync Content Provider

For assigning content with Silversync, there are generally two ways to do this, either by selecting the folders from the Content Tree or typing in file paths manually. You can expand and collapse folders if you want to assign content at a level down in the file system.



Note the Content Tree is only available for Server Based Authentication. If you are using User Based Authentication you will not be able to see this tree structure, and you must assign the content manually by typing in file paths.

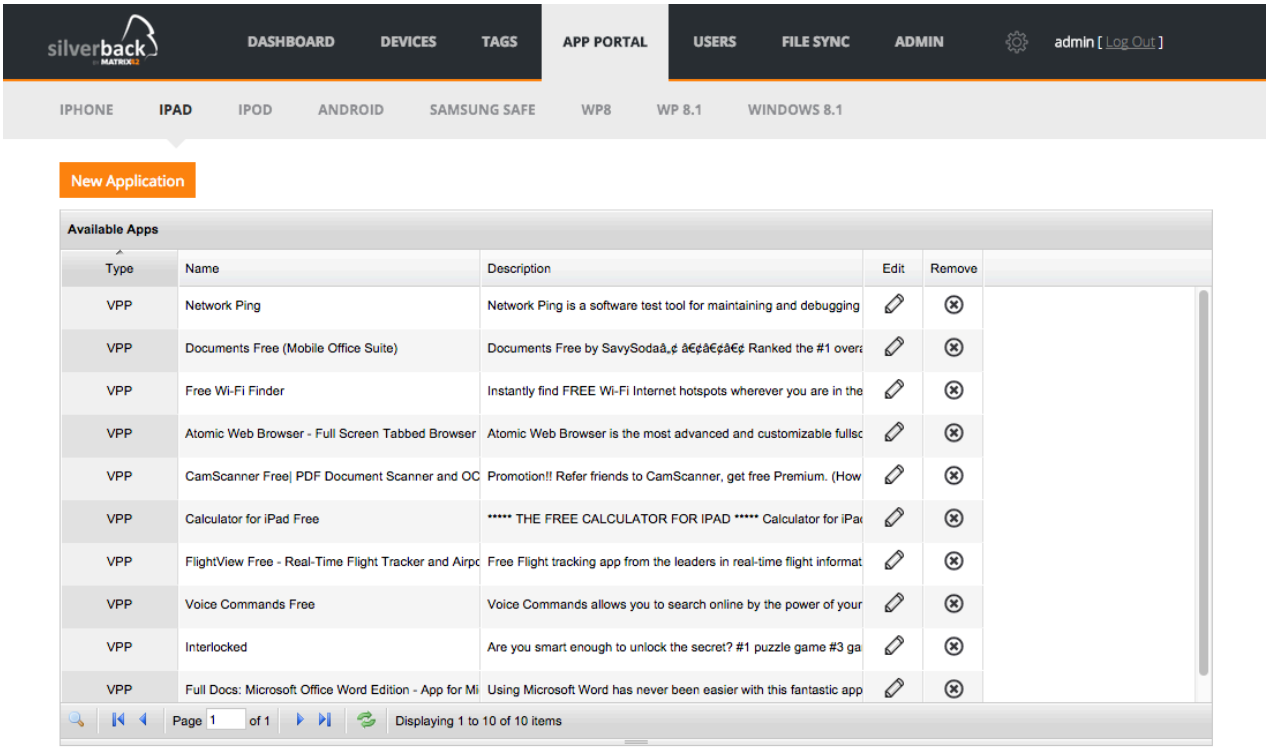
You can also assign content by clicking “Add” and typing a file path directly:



It’s important to note that these paths support system variables. In the example above “{UserName}” will be replaced with that unique user’s username. This is useful for mapping to a home drive network share for example.

6. App Portal Tab

The App Portal Tab is the Central Repository for All Apps that are going to be administered by the Silverback System. This is where Administrators can specify 'Public Facing Apps' or upload 'Custom Made Enterprise Apps' for distribution to their managed devices.



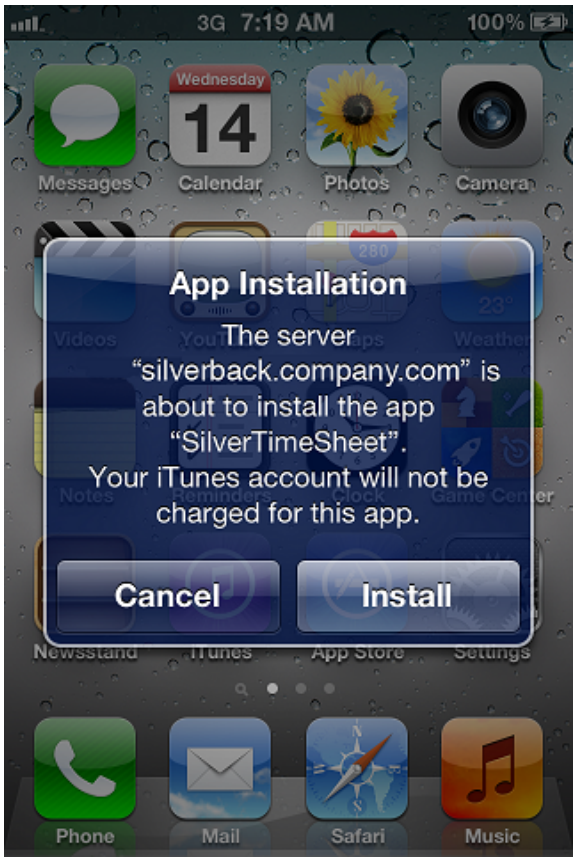
Action	Description
New Application	Add a new Enterprise or Third Party application to the app portal by clicking on the 'New Application' button. See below for more information. New additions to the app portal are published immediately.
Edit	Edit an application by pressing the relevant 'Edit' button to edit the details of an application in the app portal. Once modified the changes are reflected on the app portal site.
Remove	Remove an application from the app portal by clicking on the appropriate 'Remove' button. This will remove the application from the app portal and the application is no longer managed.

NOTE: All applications added to the Silverback App Portal are part of the Applications Whitelist for that Device Type.

6.1.1. Managed Apps

The ability to manage certain apps on devices enrolled in Silverback is done when that particular app is designated to do so when it is configured in the Silverback App Portal.

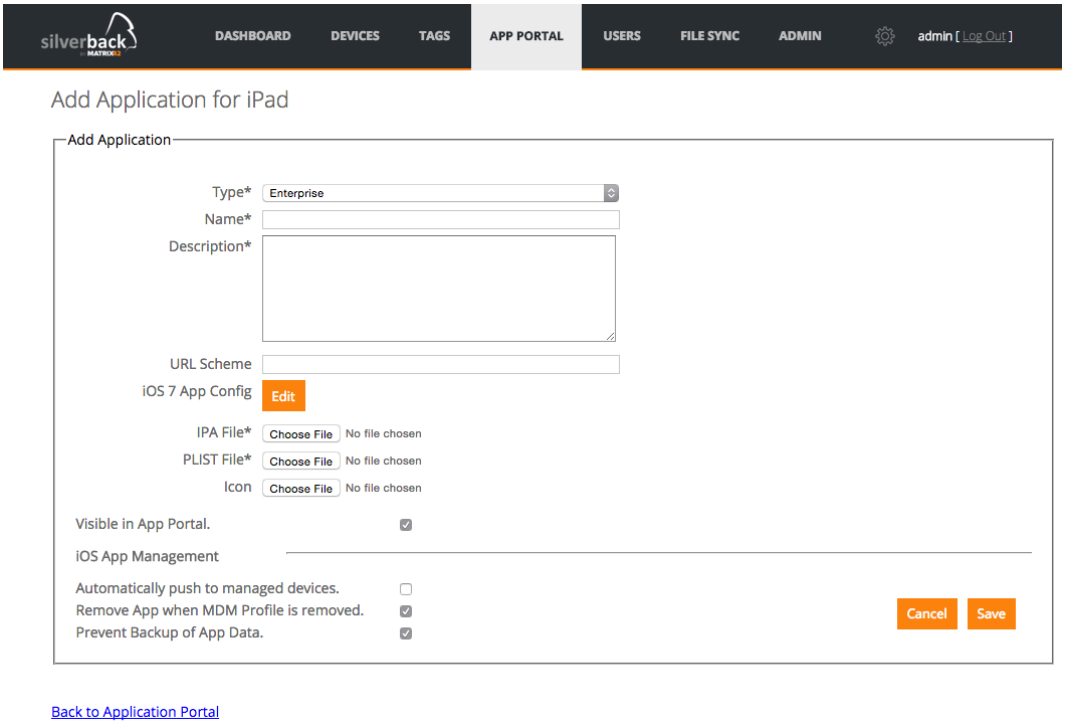
Once an App has been configured to be 'Managed' by Silverback, Administrators not only have the ability to send installation requests to target devices (individually or upon 118nrolment) or uninstall the Application from the device if they feel that it is no longer needed or the device has been compromised.



6.1.2. Adding an iOS Enterprise Application

Enterprise applications can be uploaded for iOS Devices as long as they have been 'Signed for Enterprise Distribution'. This means that you have been provided with two files (ipa and plist files).

A '.plist' file is created at the same time the '.ipa' file is created, so please check with your iOS Developer if they have not provided one with your Enterprise App.



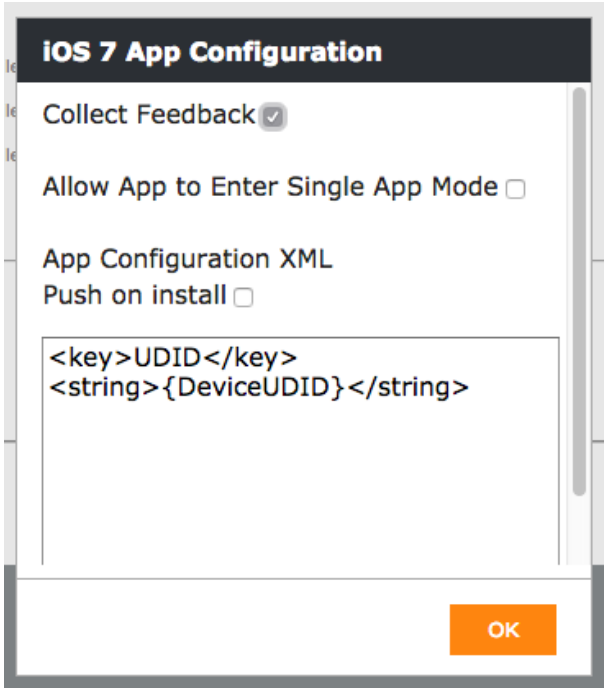
Field	Description
Type	The Type of App being added to Silverback
Name	The display name of the application being uploaded
Description	The description of the application to display
URL Scheme (iOS Only)	URL for passing application configuration settings to a device.
iOS 7 App Config	Shows the iOS 7 App Config Prompt
IPA File	The IPA file or build file of the application itself
PLIST File	The PLIST file associated with the IPA file
Icon	The icon to display in the app portal. It must meet the following specifications: Dimensions: 175x175 Format: PNG If no icon is specified, a default, blank icon will be used.
Visible in App Portal	Makes the App Visible to users in the Silverback App Portal.
Automatically Push to Managed Device	Installs the App on the device when enrolled into Silverback, or when upgrades are made.
Remove App when MDM Profile is removed	Removes the App from the device when MDM Profile is removed from Silverback. (Same as deleting from Silverback Console)
Prevent Backup of App Data	Prevents iTunes from backing up any information from this client to a computer when tethered
VPP Operation Mode	For VPP apps, which method should be used to assign licenses to users and devices, and in which order.

6.1.4. iOS 7 App Config

For devices running iOS 7 and above, it is possible to configure some advanced options for applications. It is possible for administrators to define a list of applications that are allowed to enter Single App Mode on the device. By checking the “Allow App to Enter Single App Mode” checkbox, Silverback will allow this application to enter Single App Mode autonomously. This feature needs to be programmed into the selected application.

By populating the “App Configuration XML” text area, you can define information that Silverback will push the application silently. Data should be defined in XML Key-Value pairs. Administrators can also elect whether this information should be sent with the Install command, or sent afterwards by changing the “Push on install” checkbox.

Applications will be able to access this data from the keychain if they require it. System variables are accepted, so information can be dynamic per user.

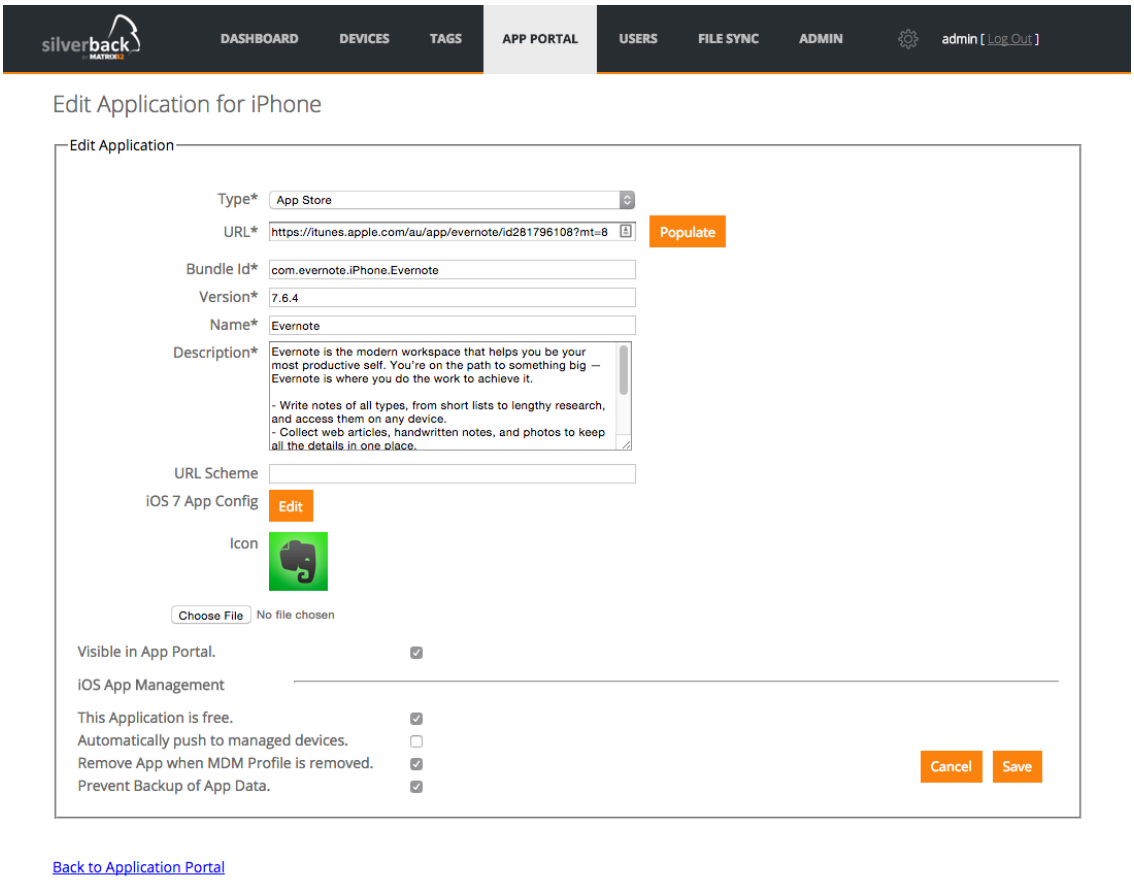


By enabling the “Collect Feedback” option, Silverback will request Managed Application Feedback from devices. This information will be visible in the Device Information window for a particular device:

NOTE: These settings are stored unencrypted on the device. It is not recommended to store sensitive information in App Configuration.

6.1.5. Adding an Apple iTunes App Store Application

With an Apple iTunes App Store app, the application itself is not loaded to the app portal, but rather a link to the application on the app store is provided through the app portal.



The process for adding an Official iTunes App Store App is quite easy, and is done using the using the following steps:

Using your Web Browser and the iTunes Preview website, please ensure you change the Country Code at the end of the URL to be your native country code. For example: http://itunes.apple.com/us/ or http://itunes.apple.com/au/

Find the App you want to manage with Silverback and copy the URL in the Web Browser. It should look similar to below: http://itunes.apple.com/us/app/ibooks/id364709193?mt=8

Paste this into the URL Field in the above screenshot and click **Populate.**

NOTE: For Paid Apps the user will be re-directed to the App Store for purchase of this App, unless there is a valid VPP Code for use.

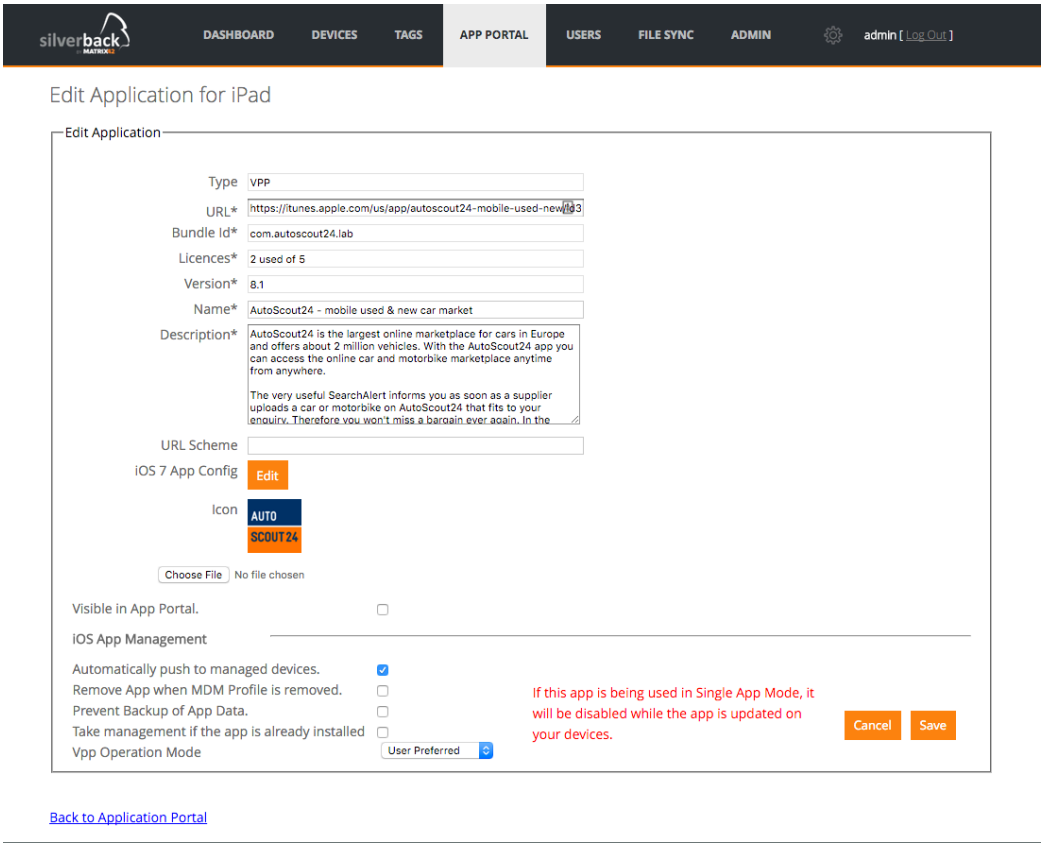
NOTE: The App Description returned may be longer than the Silverback Maximum (500 Characters). Please be sure to make any adjustments necessary to ensure that it is still human-readable.

NOTE: App Store Apps can still be distributed if the App Store Restriction has been enabled on the target device.

Field	Description
Type	The Type of App being added to Silverback
URL	The URL of the App in iTunes Preview
Bundle ID	The Unique Bundle ID of the App
Version	Version of the iOS Application
Name	The display name of the application being uploaded.
Description	The description of the application to display.
URL Scheme (iOS Only)	URL for passing application settings to a device.
Icon	The icon to display in the app portal. It must meet the following specifications: Dimensions: 144x144 Format: PNG If no icon is specified, a default, blank icon will be used.
Visible in App Portal	Makes the App Visible to users in the Silverback App Portal.
This Application is Free	This marks the iTunes Store App as being free, meaning that it can be Managed by Silverback without the use of VPP codes.
Automatically Push to Managed Device	Installs the App on the device when enrolled into Silverback If the Allow App Store restriction has been disabled, App Store Apps will not be automatically pushed to Managed Devices.
Remove App when MDM Profile is removed.	Removes the App from the device when MDM Profile is removed from Silverback.
Prevent Backup of App Data	Prevents iTunes from backing up any information from this client to a computer when tethered.
Take Management if the app is already installed	For iOS 9 and above, its possible to take management of the application if the user installed this themselves outside of management. This is silent for supervised devices and will normally prompt the user
iOS 7 App Config	Shows the iOS 7 App Config Prompt

6.1.6. VPP Applications

When integrating with Apple's VPP Program (using managed codes, instead of VPP Spreadsheets) VPP applications will automatically show in the App Portal. These cannot be added manually and will be imported by the system.



NOTE: The App Description returned may be longer than the Silverback Maximum (500 Characters). Please be sure to make any adjustments necessary to ensure that it is still human-readable. For VPP Apps this is imported automatically and **may** need to be manually trimmed down in size before saving changes.

Field	Description
Type	The Type of App being added to Silverback
URL	The URL of the App in iTunes Preview
Bundle ID	The Unique Bundle ID of the App
Licenses	The number of managed VPP licenses remaining
Version	Version of the iOS Application
Name	The display name of the application being uploaded.
Description	The description of the application to display.
URL Scheme (iOS Only)	URL for passing application settings to a device.
Icon	The icon to display in the app portal. It must meet the

Field	Description
	following specifications: Dimensions: 144x144 Format: PNG If no icon is specified, a default, blank icon will be used.
Visible in App Portal	Makes the App Visible to users in the Silverback App Portal.
Automatically Push to Managed Device	Installs the App on the device when enrolled into Silverback If the Allow App Store restriction has been disabled, App Store Apps will not be automatically pushed to Managed Devices.
Remove App when MDM Profile is removed.	Removes the App from the device when MDM Profile is removed from Silverback.
Prevent Backup of App Data	Prevents iTunes from backing up any information from this client to a computer when tethered.
Take Management if the app is already installed	For iOS 9 and above, its possible to take management of the application if the user installed this themselves outside of management. This is silent for supervised devices and will normally prompt the user
iOS 7 App Config	Shows the iOS 7 App Config Prompt
VPP Operation Mode	For VPP apps, allows you to specify how licenses should be assigned to users and devices, and in what order of preference. User Preferred will attempt to assign licenses to Users first, and failing that Devices. Device Preferred will attempt assign licenses to Devices first and failing that, Users User/Device Only will only allow this app to be assigned to Users/Devices respectively. These settings can be set to a default value in the VPP section of the Admin Tab.

6.1.7. Take Management of Apps

With iOS 9 and above it's possible to "take management" of an app if the user had already installed this. What this means is that if your company uses an application and want to manage this, but the user already has this installed before they enrol you can convert this to a managed application. For a supervised device, this process is totally silent, and if the application is set to automatically push it will happen as soon as Silverback detects the app. For non-supervised devices, the user will be prompted if they want the server to take management. They can confirm or deny this.

For apps that are not set to automatically push, you can take management from the device info popup for a user.

To take management manually, open the device info popup and where possible, the action button will be "Manage".

6.1.8. iOS App Portal URL Schema Variables

Using Silverback's ability to manage apps on iOS Devices it is possible to pass configuration settings to certain applications – essential automating their setup for the end user. This is the recommended app configuration process, if your devices are running Pre-iOS 7 versions.

All the user needs to do is first download the desired App and make sure it is fully downloaded/installed on the device, then click on a second 'Settings' link that will populate the target application with its configuration.

By entering the Variable names below, in braces, e.g. {UserName}, the device specific value for that variable will be sent.

Variable	Replaced with
SilverbackAdminUrl	Silverback server address
SilversyncSyncUrl	Silversync server address
UserName	As defined by the LDAP Variable in the Silverback config files
UserPassword	The Password of the enrolling user.
UserCert	As defined by the LDAP Variable in the Silverback config files
UserEmail	As defined by the LDAP Variable in the Silverback config

Variable	Replaced with
	files
UserVPN	As defined by the LDAP Variable in the Silverback config files
UserWifi	As defined by the LDAP Variable in the Silverback config files
UserWifiProxy	As defined by the LDAP Variable in the Silverback config files
UserSMIME	As defined by the LDAP Variable in the Silverback config files

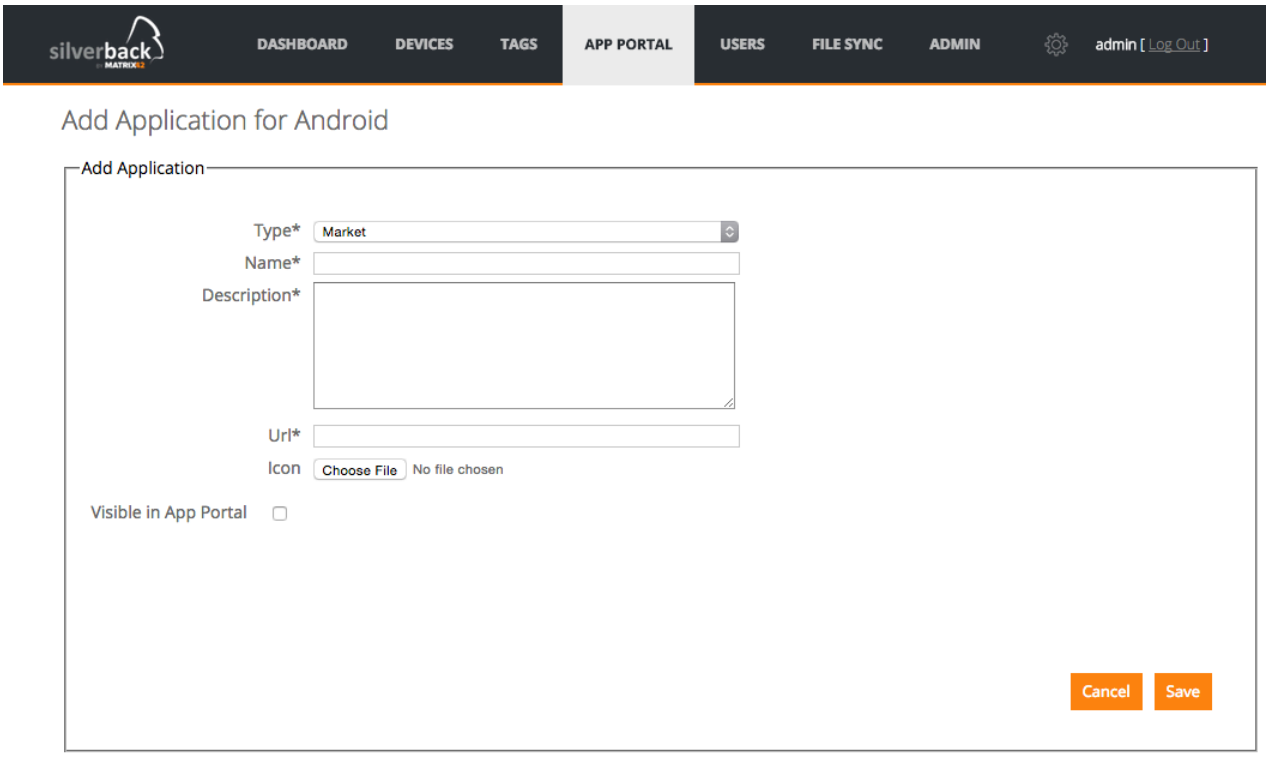
NOTE: Use of the UserPassword variable is reliant on a custom Silverback configuration file. It enables Silverback to cache a user password at the time of enrollment for use later. Contact Silverback support for more information.

NOTE: By Default, Silverback uses the UPN (UserPrincipalName) Attribute for authentication with Microsoft's Active Directory. Most of the above fields will be populated using this attribute at the time of enrollment.

NOTE: Silverback Config Files are setup by your Silverback Technician at the time of the initial install. Silverback uses these files when the website and services are started. When a user enrolls in the system, Silverback will query your LDAP Schema for the variables configured in these files and store them in its database.

6.1.9. Adding an Android/Samsung Safe Market Application

With an Android Market App, the application itself it not loaded into Silverback, rather a link is presented to the device that redirects the device to download it from the official Android Marketplace.



The process for adding an Official Android Market Apps is quite easy, and is done using the using the following steps:

Using your Web Browser and the Android Market, found using the following link: https://play.google.com/store/apps

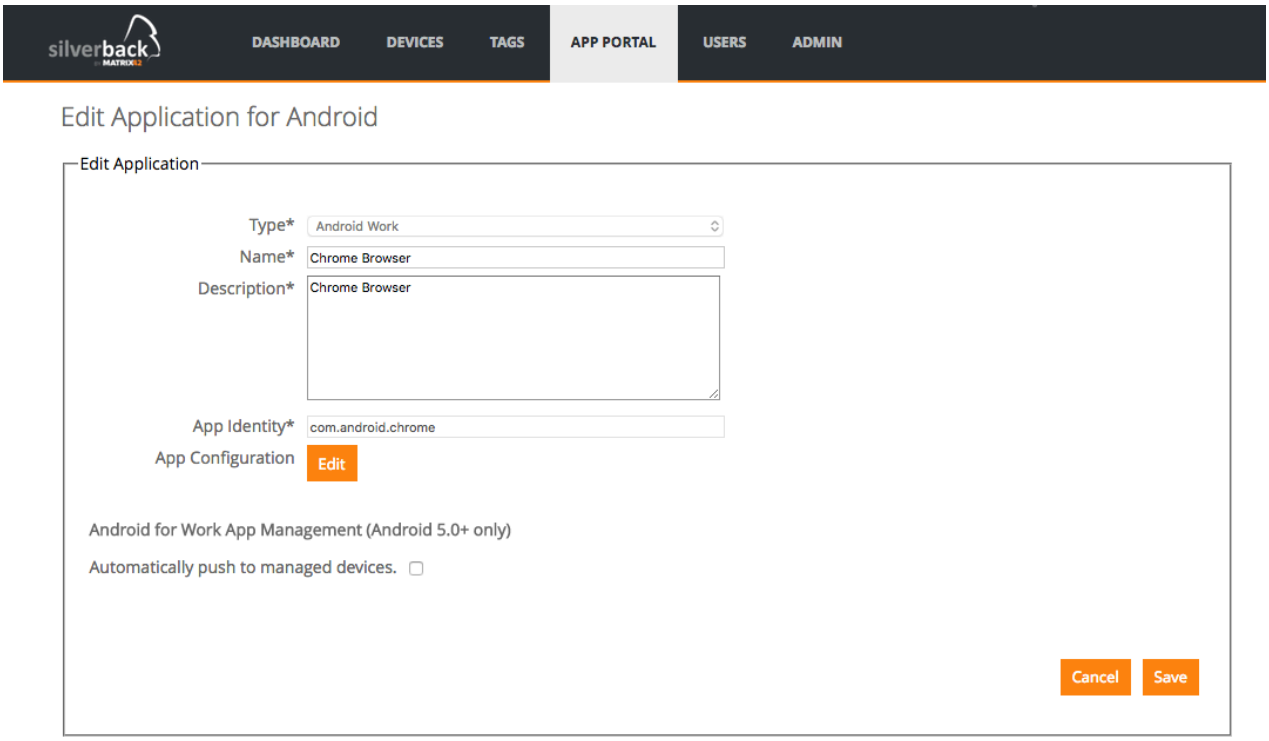
Find the App you want to manage with Silverback and copy the URL in the Web Browser. It should look similar to below: https://play.google.com/store/apps/details?id=com.google.earth

Paste this into the URL Field then fill out the remaining information required.

Field	Description
Name	The display name of the application being uploaded.
Description	The description of the application to display.
URL	The URL to the Android Market page for the application.
Icon	The icon to display in the app portal. It must meet the following specifications: Dimensions: 114x114 Format: PNG If no icon is specified, a default, blank icon will be used.
Visible in App Portal	Makes the App Visible to users in the Silverback App Portal.

6.1.10. Adding an Android for Work Marketplace Application

With Android for Work, applications are installed into the Managed Profile on the device, and the process of adding these applications to Silverback is slightly different to a normal marketplace application.



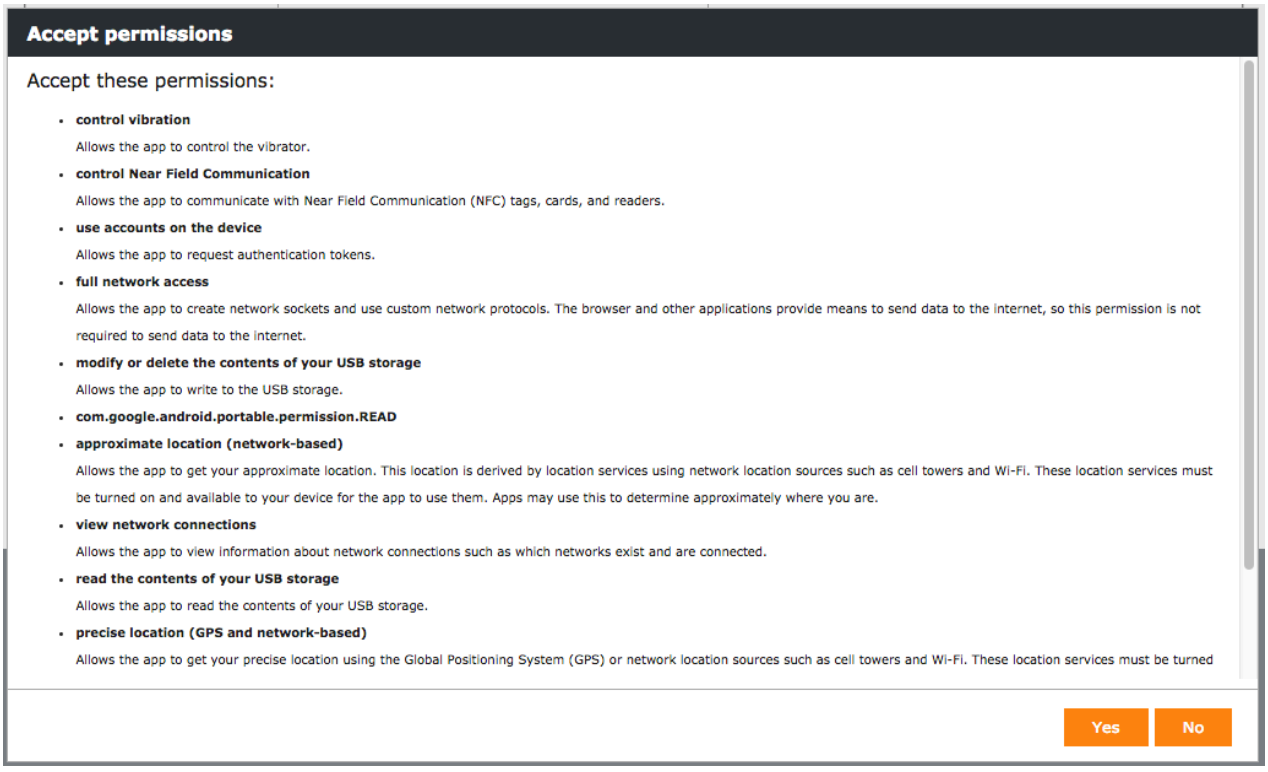
The process for adding an Android for Work App is done using the using the following steps:

Using your Web Browser and the Android Market, found using the following link: https://play.google.com/store/apps

Find the App you want to manage with Silverback and copy the URL in the Web Browser. It should look similar to below: https://play.google.com/store/apps/details?id=com.google.earth

Copy the Application Identity portion (after id=) and paste this into the “App Identity” field, for the above URL, this would be: com.google.earth

When you save the application, you will need to accept permissions for the users. This is because the applications will be installed silently. If this application’s permissions have not been accepted before, you will be prompted to accept them:



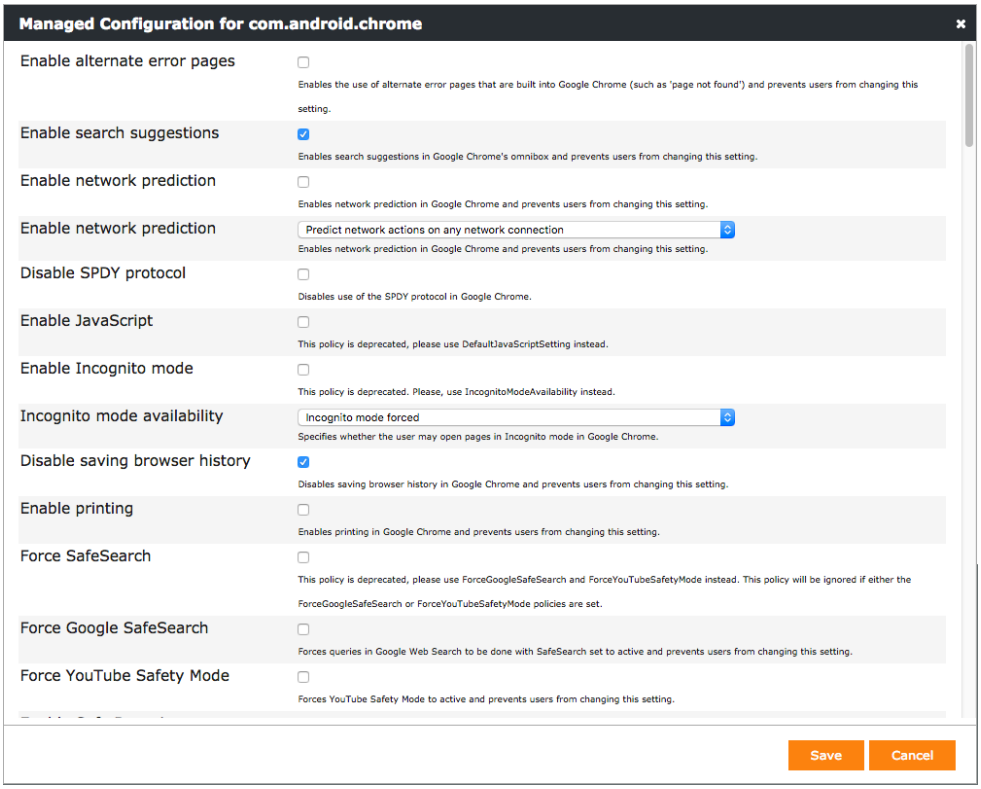
Field	Description
Name	The display name of the application being uploaded.
Description	The description of the application to display.
App Identity	The Application Identifier for the app.
App Configuration	For some applications, developers will allow configuration of settings. Clicking the Edit button here will allow you to edit that configuration.
Automatically Push to Managed Devices	Will automatically install the app on devices that have Android for Work enabled.

6.1.10.1. App Configuration

For applications that support this, clicking the Edit button will allow you to edit the configuration settings for that app. These settings are determined by the developer, so you will be presented with all the settings that are available for that app.

In the example below, you can see the configuration settings for Google Chrome. The configuration for each app will be different, and if no configuration is available you will not see any configuration items.

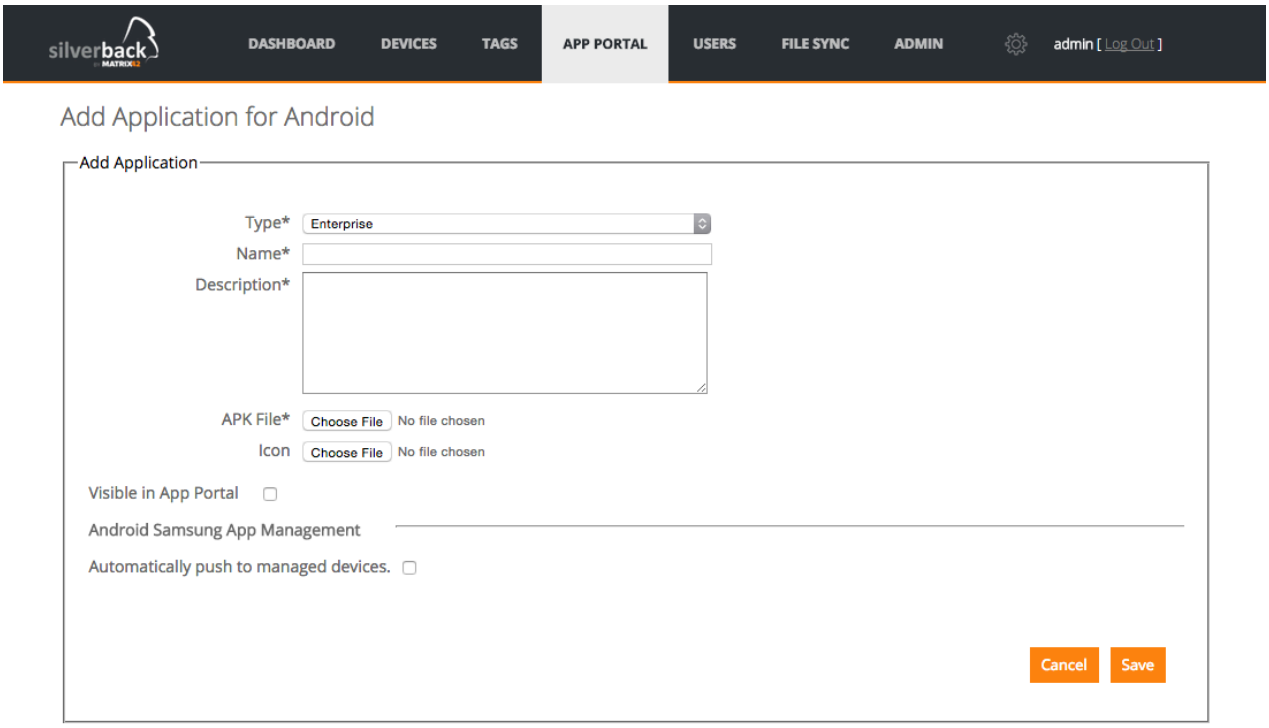
The configurations also support system variables, which means you can populate settings with things such as {UserName} to dynamically fill the user name for each user.



6.1.11. Adding an Android/Samsung Safe Enterprise Application

Enterprise applications can be uploaded for Android Devices as long as you have the supplied .apk file that is required to install the Application.

The user will have to change Security Settings on their Android Device to allow installation of these apps as they do not come from the Official Android Market Store.

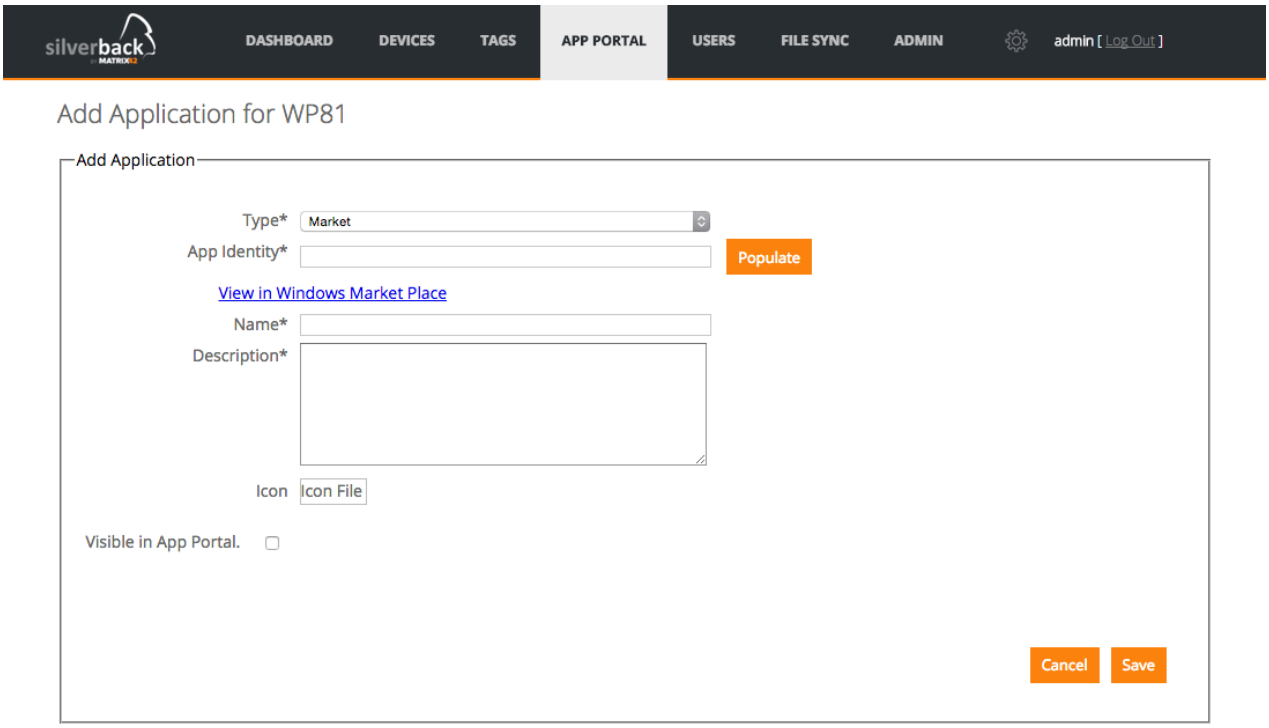


Field	Description
Name	The display name of the application being uploaded.
Description	The description of the application to display.
APK File	The APK file for the supplied Enterprise Application
Icon	The icon to display in the app portal. It must meet the following specifications: Dimensions: 114x114 Format: PNG If no icon is specified, a default, blank icon will be used.
Visible in App Portal	Makes the App Visible to users in the Silverback App Portal.
KNOX Signed App	Nominates that the app has been signed by Samsung as a KNOX Signed App. This will make the app applicable to KNOX Containers.

Field	Description
Automatically Push to Managed Devices (Samsung Safe Only)	Silently installs the app on the Samsung Safe device when it becomes managed.

6.1.12. Adding a Windows Phone Marketplace Application

With Windows Phone Apps, the application itself is not loaded to the Silverback App Portal, but rather a link to the application on the Official Marketplace is provided through Silverback.



The process for adding a Windows Marketplace App is quite easy, and is done using the following steps:

Using your Web Browser and the Windows Phone Marketplace web-store: http://www.windowsphone.com/marketplace

Find the App you want to manage with Silverback and copy the URL in the Web Browser. It should look similar to below: http://www.windowsphone.com/en-us/store/app/silverback-mdm/884bb1fd-fb41-472a-83bf-3e09910e2f5b

Paste the unique number after /apps/app name into the AppIdentity Field in the above screenshot and click **Populate.**

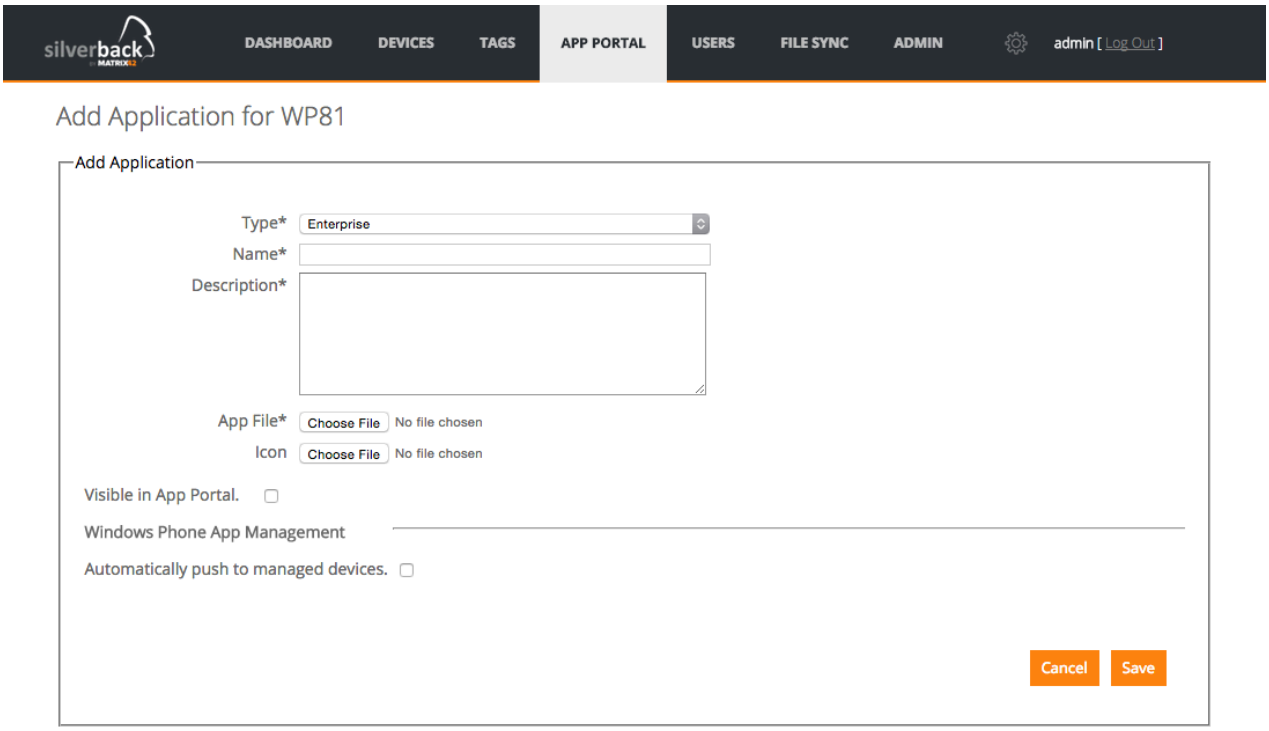
NOTE: The App Description returned may be longer than the Silverback Maximum (500 Characters). Please be sure to make any adjustments necessary to ensure that it is still human-readable.

NOTE: Due to the implementation of the Windows Marketplace, the Name and Description displayed in the Administrator Console will not affect the how the users receive the link on the device. The Apps are displayed on the device as they are displayed in the Official Marketplace App.

Field	Description
AppIdentity	The Unique String associated with the App from the Windows Marketplace
View in Windows Marketplace	URL Link opens a new Browser Window displaying the App in the official Windows Marketplace.
Name	The Name of the App as presented in the Administrator Console.
Description	Description of the App as presented in the Administrator Console.
Icon	The Icon of the App
Visible in App Portal	Makes the App Visible to enrolled devices.

6.1.13. Adding a Windows Phone Enterprise Application

Enterprise applications can be uploaded for Windows Phone Devices as long as you have the supplied file that is required to install the Application.

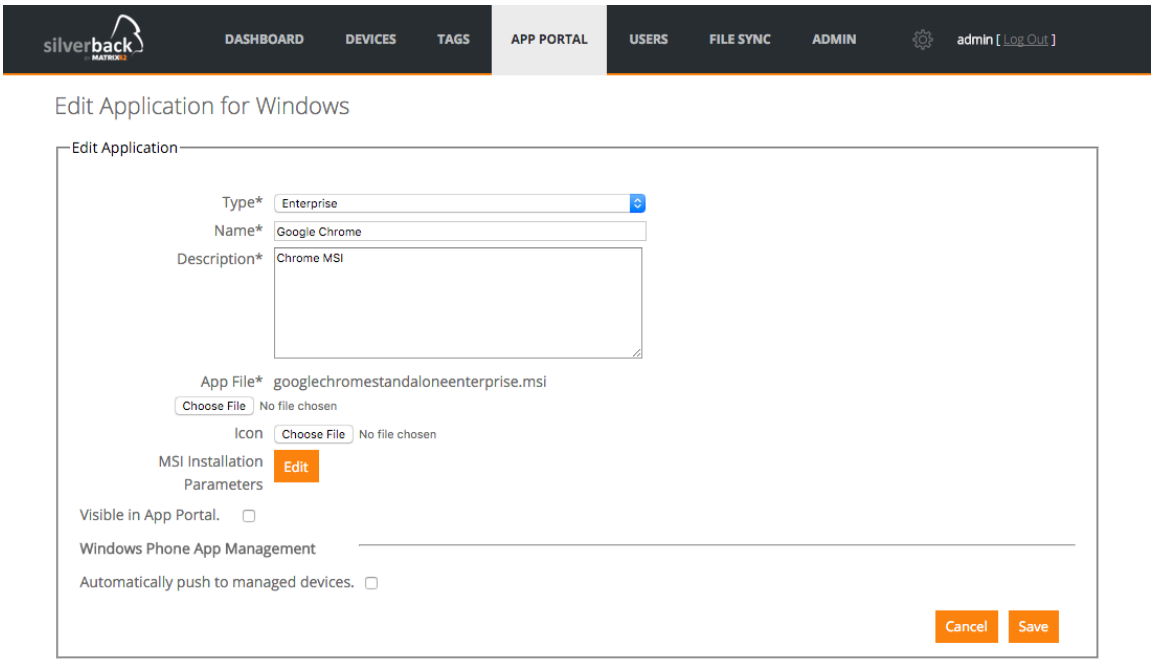


Field	Description
Name	The display name of the application being uploaded.
Description	The description of the application to display.
App File	The file for the supplied Enterprise Application
Icon	The icon to display in the app portal. It must meet the following specifications: Dimensions: 114x114 Format: PNG If no icon is specified, a default, blank icon will be used.
Visible in App Portal	Makes the App Visible to users in the Silverback App Portal.
Automatically Push to Managed Devices	Silently installs the app on the device when it becomes managed.

6.1.14. Adding a Windows MSI

MSI Installation files can be added for Windows devices. Do do this, select the Windows tab of the App Portal, and when adding a new app choose “Enterprise”.

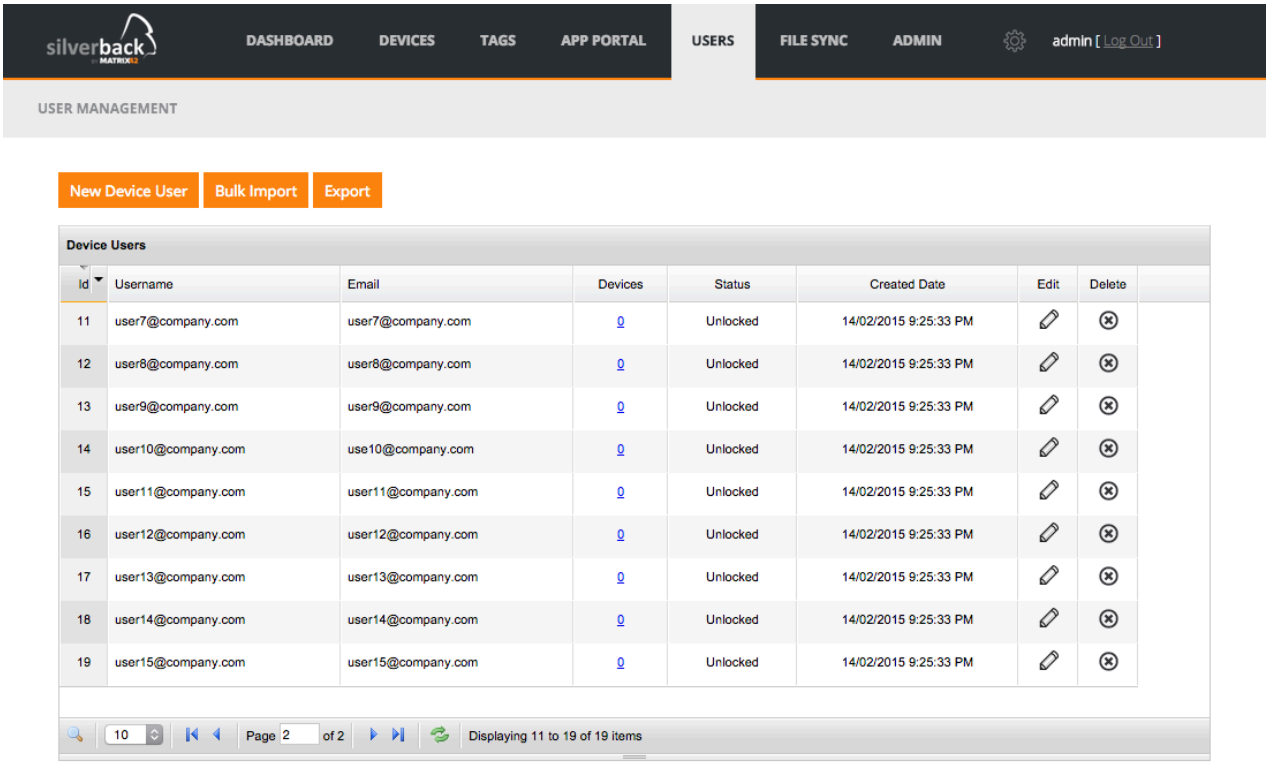
The process is similar for other platforms Enterprise apps, but you can also provide MSI parameters. If the app supports a special parameter for installation you can provide this in the “MSI Installation Parameters” section.



Field	Description
Name	The display name of the application being uploaded.
Description	The description of the application to display.
App File	The MSI Installation File
Icon	The icon to display in the app portal. It must meet the following specifications: Dimensions: 114x114 Format: PNG If no icon is specified, a default, blank icon will be used.
MSI Installation Parameters	If the MSI supports it, provide the installation parameters here. E.g. “/quiet” would initiate a silent installation.
Visible in App Portal	Makes the App Visible to users in the Silverback App Portal.
Automatically Push to Managed Devices	Silently installs the app on the device when it becomes managed.

7. Users Tab

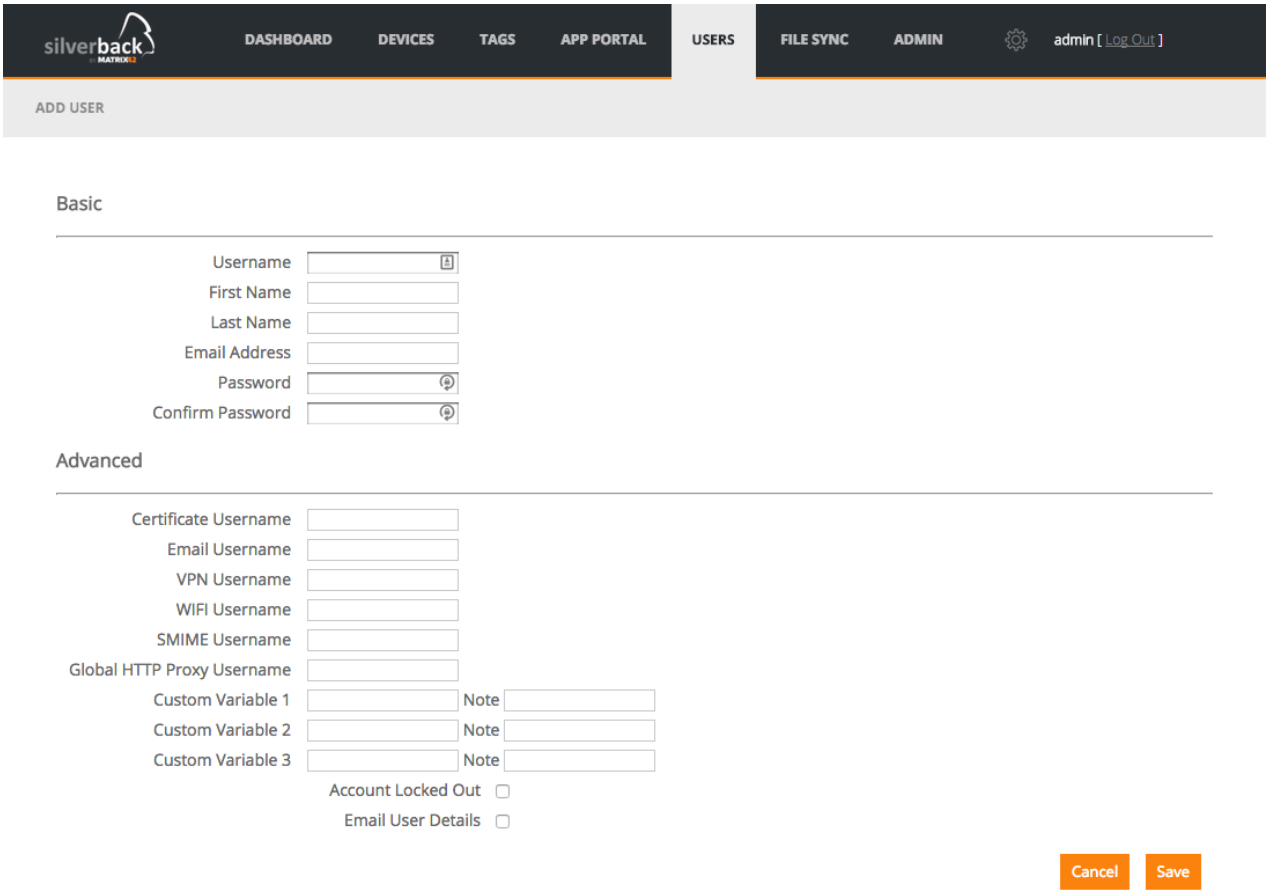
As well as being able to use an LDAP Source for its users, Silverback is also able to create and store local users itself. This mean that you can simply create and delete users from within Silverback and not have it affect the rest of your Internal Infrastructure (or any production users).



Detail	Description
New Device User	Takes the Administrator to the New Device User Screen.
Bulk Import	Allows the Administrator to Bulk Import New Users
Export	Export the current list of Local Users
Username	The Username of the Local User
Email Address	The Email Address of the Local User
Devices	The number of devices the Local User has associated with them.
Status	The Status of the Local Account
Create Date	The data the Local Account was created
Edit	Edit the Local Accounts Details
Delete	Deletes the Local User

7.1. Creating a Local User

Creating a Local User in Silverback requires that the user have all the necessary attributes that are collected from a device at the time of enrollment, such as the users First & Last Name, through to the Username that should be presented for a VPN or Wireless Access Point.



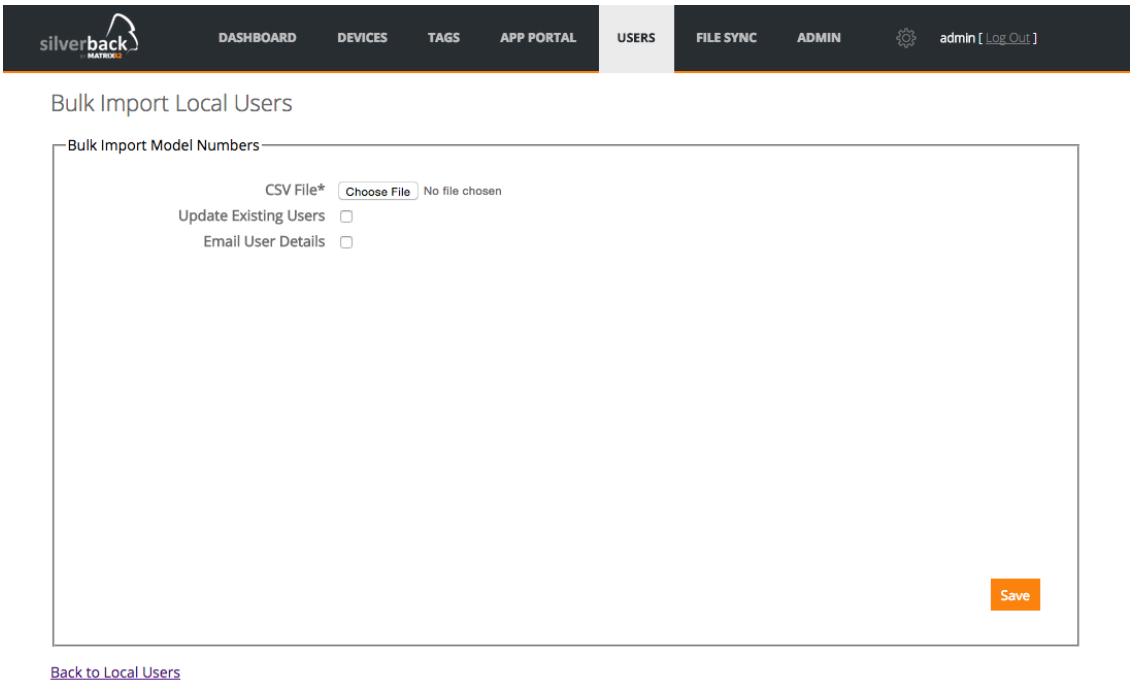
NOTE: If Silverback is configured for both Local Users and an LDAP Source, the Local User will take precedence over the LDAP Users. This means that if you have an LDAP user 'user01@company.com' and you create a Local User also called 'user01@company.com' Silverback will use the Local Users details and not the LDAP Users details.

Any devices enrolled with the LDAP user credentials will be transferred to the local user. If you delete the local user, any devices with that username will be deleted from the console.

Attribute	Description
Username	The Username for the user, to be entered into the Self-Service Portal to create an enrollment.
First Name	The Local User's First Name
Last Name	The Local User's Surname
Email Address	The Local User's Email Address
Password	The Password for the Local User
Repeat Password	The Password Repeated for Confirmation
Certificate Username	The Username Silverback will use for any Certificate Fields
Email Username	The Username to be used in conjunction with Email Settings
VPN Username	The Username to be used in conjunction with VPN Settings
WiFi Username	The Username to be used in conjunction with WiFi Settings
SMIME Username	The Username Silverback will use for any S/MIME Username Fields.
Global HTTP Proxy Username	The Username to be used in conjunction with a Global HTTP Proxy
Custom Variable 1	A Custom Variable that can be populated with Custom Information
Custom Variable 2	A Custom Variable that can be populated with Custom Information
Custom Variable 3	A Custom Variable that can be populated with Custom Information
Note Fields	A Note Field for each Custom Variable field so Administrators can leave notes as to what each custom variable is being used for.
Account Locked Out	Checkbox to show if the user is locked out or not.
Email User Details	Email the User's Details to them upon Local Account Creation – the Email Address field will be used for delivery of this email.

7.2. Bulk Import of Local Users

It is also possible to 'Bulk Import' users into Silverback using a CSV File by uploading it through the Silverback Administrator Console.



Attribute	Description
CSV File	Browse to find the CSV file on your local computer.
Update Existing Users	Will overwrite an existing user's details if they are found in the CSV file being uploaded.
Email User Details	Enable this to email each user a copy of Silverback Local User Details.

NOTE: To see the correct CSV Format for the Bulk Import of Local Users, please see the Silverback Appendix.

NOTE: If Silverback is configured for both Local Users and an LDAP Source, the Local User will take precedence over the LDAP Users. This means that if you have an LDAP user 'user01@company.com' and you create a Local User also called 'user01@company.com' Silverback will use the Local Users details and not the LDAP Users details.

Any devices enrolled with the LDAP user credentials will be transferred to the local user. If you delete the local user, any devices with that username will be deleted from the console.

8. Admin Tab

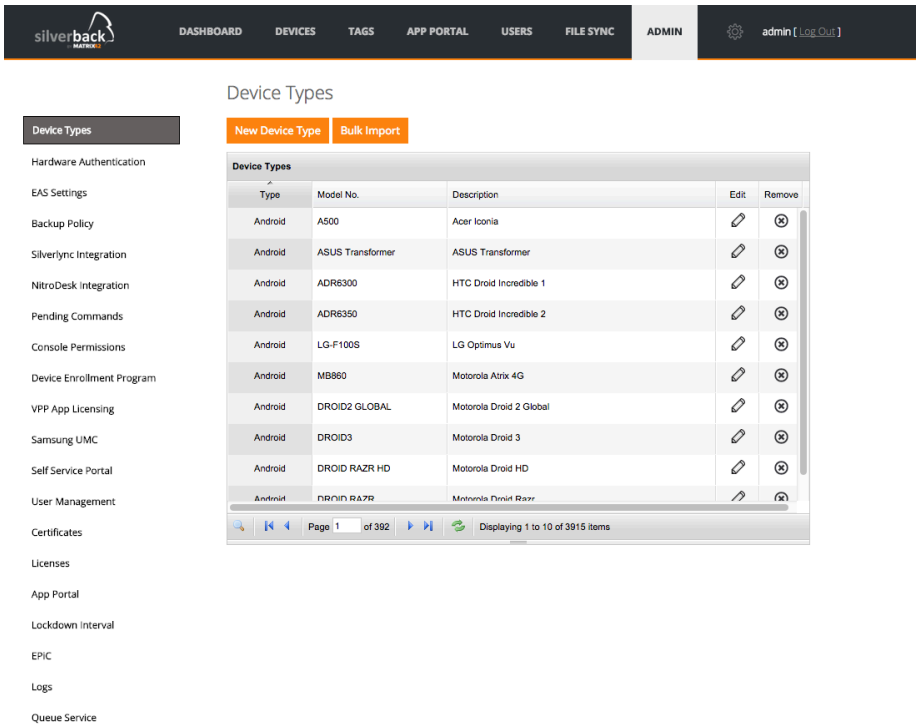
The Admin Tab allows the Administrator to configure some of the core settings of Silverback installation.

From within this Tab the Administrator has the ability to do some of the following tasks:

- Customize the Look and feel of specific elements, such as the Self Service Portal, or App Store Icon.
- Create and Configure Users and give those individual users different levels of access to the Silverback Console.
- Configure the Device Types Silverback is aware of.
- Capture a list of Serial Numbers and Usernames associated with them.
- Setup and Enable Advanced System Settings.
- View Device or Server Logging Information.
- View Important License Information.

8.1. Device Types

Each type of device can be mapped to a description for easy reading and categorization. By default, known device types are already mapped by Silverback however more device types can be added as they become available. If a device enrols in the system and Silverback does not recognize its model number, the model number will be added to the system with a black description, allowing the Administrator to define it later.

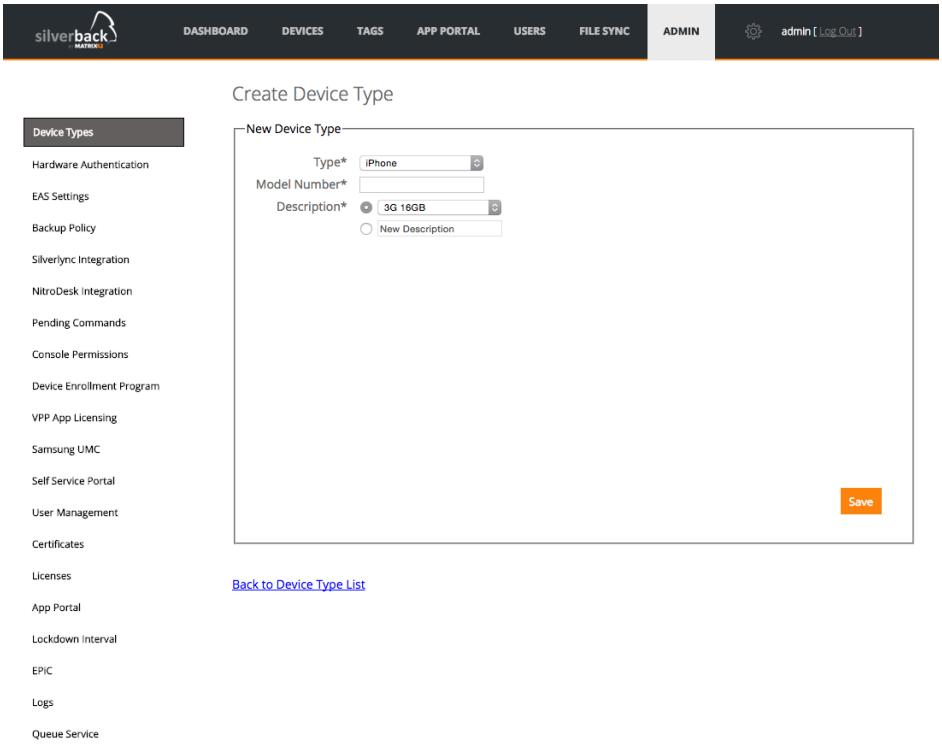


Control	Description
Edit	Edit an existing device type mapping by clicking on the edit button
Remove	Remove a device type mapping by clicking on the remove button
New Device Type	Create a new device type mapping by clicking on the 'New Device Type' button. This button will create a new mapping from a device model number to the type of device and its description
Bulk Import	Allows an Administrator to Bulk Import a list of Device Model Numbers with their Descriptions.

NOTE: When a Hardware Vendor releases a new device, Silverback may not know the Model Number of the device, in this case the new device model number will be listed in the Device Types datagrid, but its description will be Unknown. You will need to edit this and assign it an appropriate Device Type and Description.

8.1.1. Create Device Types

When an unknown device type enrols to Silverback, a new device type will appear in the device type list, however only the model field will be filled in. Simply edit the new device type and fill in the appropriate details for this model number to be managed.



8.1.2. Bulk Model Number Import

The Bulk Model Number CSV file needs to be done in the following format:
DEVICE_TYPE_ID, Device Description, Model Number

The DEVICE_TYPE_ID is relative to Silverback; guidelines are:

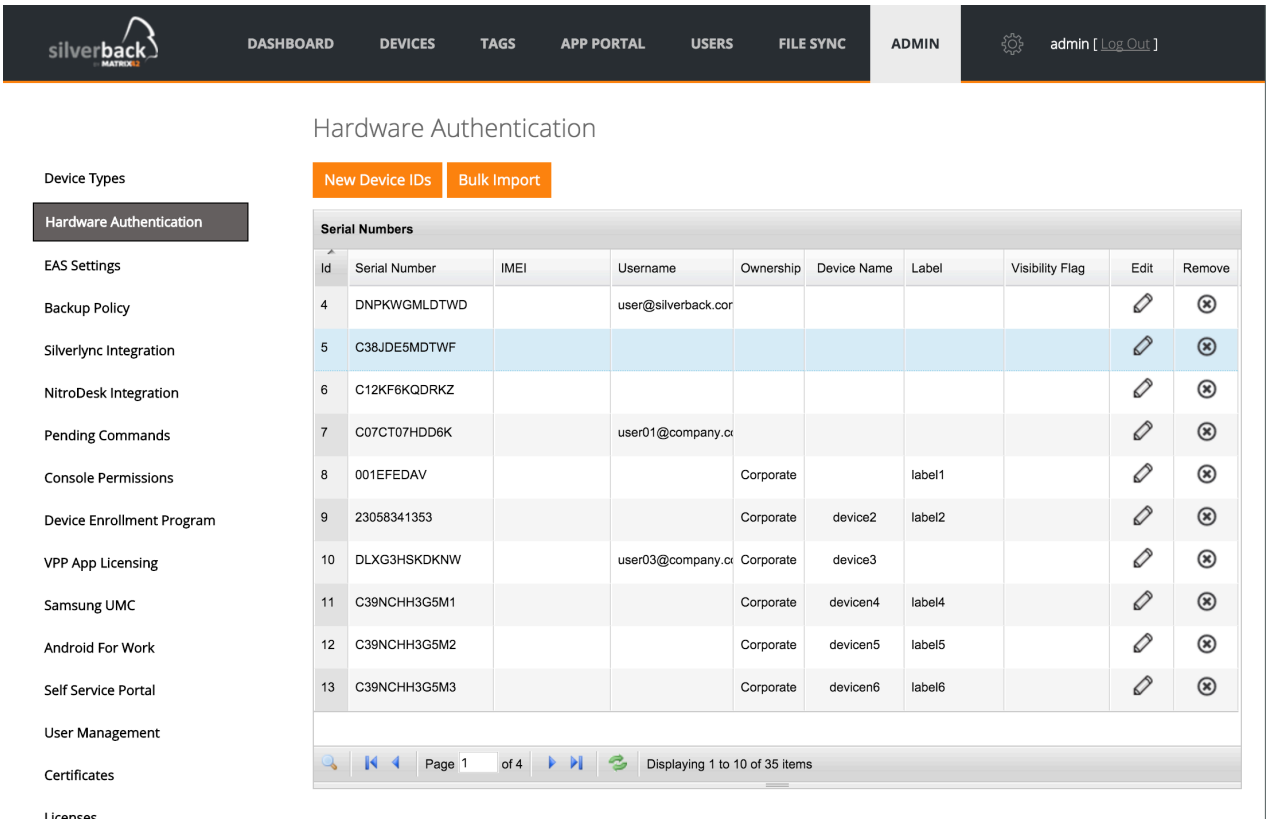
1 – iPad
2 – iPhone
3 – iPod
4 – Android
5 – Samsung Safe
6 – Windows Phone 8
11 – Windows Phone
12 – Windows
13 – OS X

Example File:
1, 3rd Gen Wi-Fi 32GB, MC706LL
4, Motorola RAZR, XT910
2, 4S 16GB, MD237X

8.2. Hardware Authentication

Hardware authentication is a form of access control to Silverback and when enabled can ensure only pre-authorized devices are allowed to become 'managed' devices e.g. Corporate owned devices that are issued and are fixed assets of the business.

During the enrolment process, Silverback will verify the serial number and or IMEI of the device against the pre-authorized list and only if the serial number or IMEI is recognized and there are no other policy restrictions will the device be managed and not be 'blocked'.



8.2.1. Bulk Import Device Serial Number, Label, Name and Visibility Flag

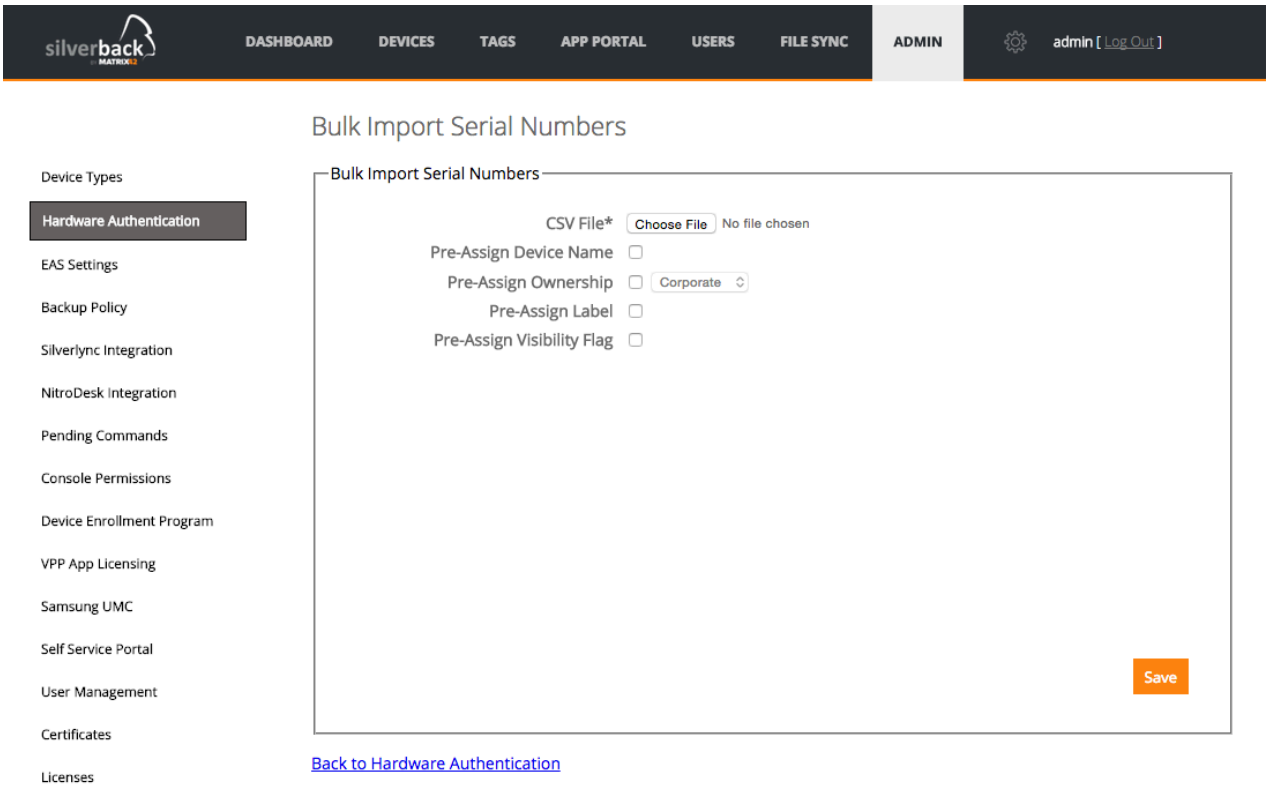
Silverback offers the convenient option to bulk import serial numbers. The file simply needs to be in CSV format with serial numbers as values in Column 1, IMEI number in Column 2, Device Label in Column 3, Device Name in Column 4 and Visibility Flag in Column 5. Simply upload the CSV file and the values will be automatically populated in the hardware authentication page.

Note that either Serial or IMEI is required, but one must exist. It's also allowed to populate both serial and IMEI in one row, but this will match either or (i.e. it will not make sure the device matches both values, it will find the first match and allow this).

CSV Example Formatting:

SNXXXXXXXXX,Label,Device Name,Visibility Flag,IMEI
SNXXXXXXXXX,Tech_Device,Jims iPad,Corporate Flag,3555757575757575757575
SNXXXXXXXXX,Test_Device,Sallys iPad,Corporate Flag,
SNXXXXXX,Jim's Personal Device,Jims iPod,Private Device,355676767676767676767

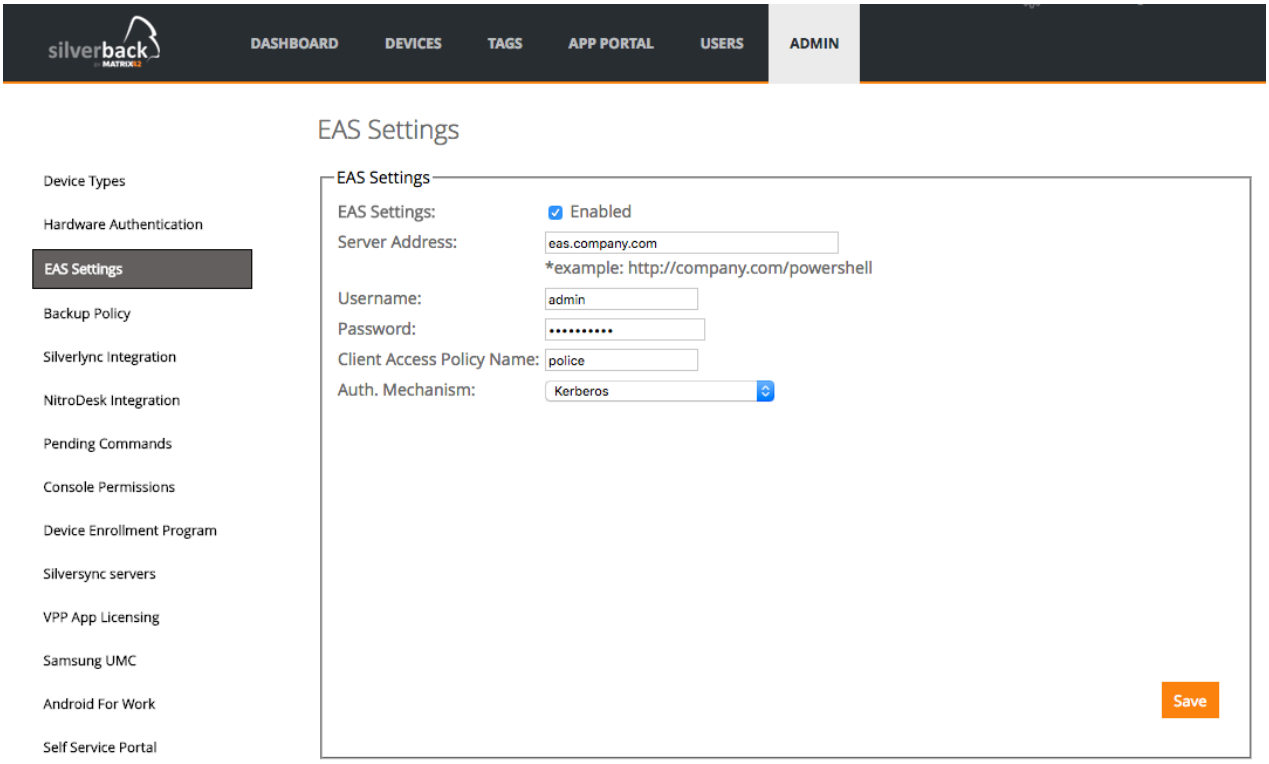
Column	Description
Serial	The serial number of the device. This is what is used to associate the other columns of information to the device.
Label	A label for the device. This can be used to visually indicate something to console users, and also used as a Tag population variable. Label is also editable from the device information popup.
Device Name	The name for the device. This is primarily used in iOS, where it is possible to set the device name for a supervised device. If a device enrolls that is compatible with this feature, the device name will be set.
Visibility Flag	Used to determine if admins should be able to view this device or not. To nominate visibility to a Visibility Flag for console users, edit the Visibility Flags for that user account by editing it.
IMEI	The IMEI number of the device.



Control	Description
CSV File	The file containing the serial numbers to import
Pre-Assign Device Name	If enabled, the Device Name column in the CSV will be used to populate the device name value for this serial number
Pre-Assign Ownership	If enabled, the console user can select the Ownership that will be assigned to the imported devices, either Corporate or Personal
Pre-Assign Label	If enabled, the Label column in the CSV will be used to populate the label value for this serial number
Pre-Assign Visibility Flag	If enabled, the Visibility Flag column in the CSV will be used to populate the visibility flag value for this serial number.

8.3. EAS Settings

EAS Settings will enable your Silverback Server to send commands to your Exchange Server to Blacklist/Whitelist Exchange ActiveSync devices so they cannot sync even outside of Silverback Management. (this requires Exchange 2010 and for 'Quarantine Mode' to be enabled').



Control	Description
Server Address	The internal address for the Exchange Server.
Username	The Username the Silverback Server will use for authentication
Password	The Password for the User Account
Client Access Policy	The name of the Client Access Policy that Silverback is manipulating on the Exchange Server.
Auth. Mechanism	This is what authentication mechanisms are allowed in the system. Typically, this will be Basic or Kerberos, but we provide all possible items in case the environment dictates these.

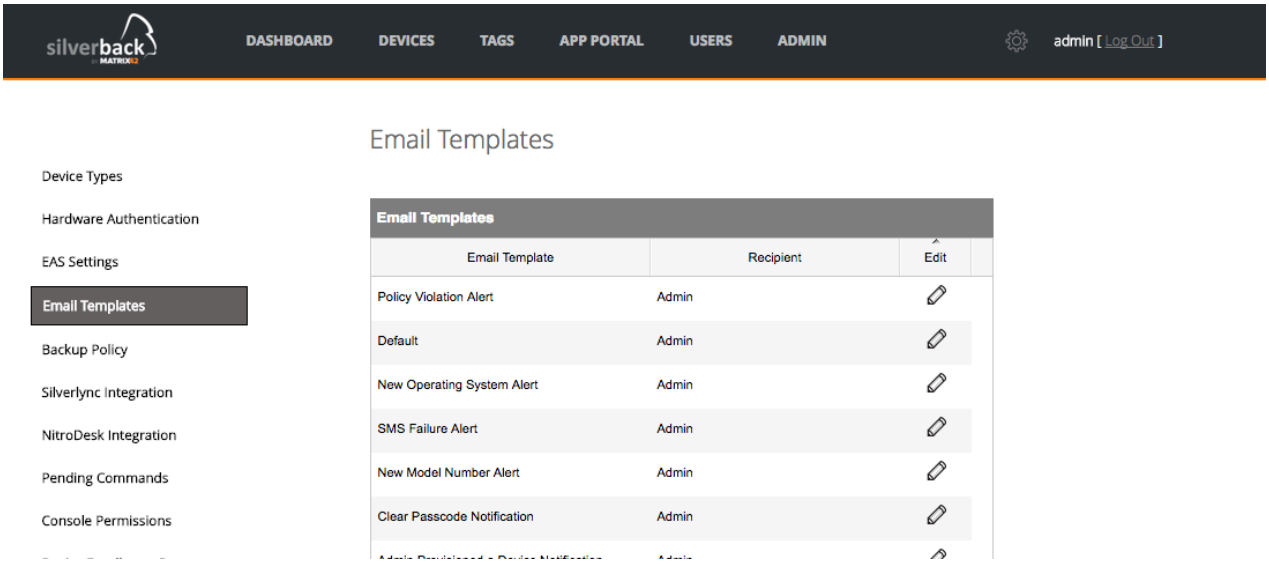
NOTE: If the Username and Password fields are left blank, then Silverback will attempt to connect to the Exchange Server using the Local Computer Account. For this to work, the Local Computer Account will need permissions on the Exchange Server itself.

8.4. Email Templates

The Email Templates section lets you modify the emails that are sent to users and administrators, and also modify the SMS that is sent to end users.

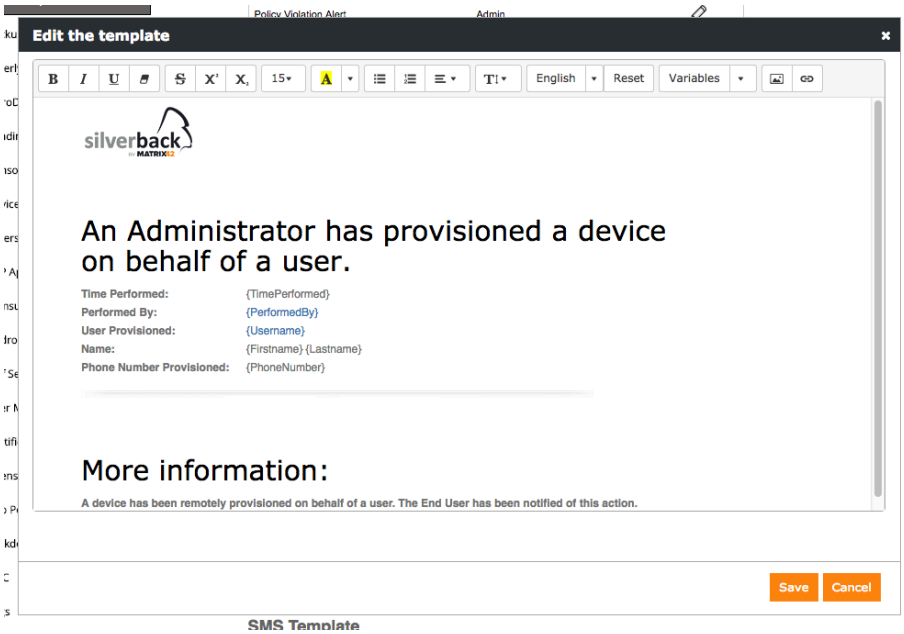
8.4.1. Email Templates

For email templates, every email generated by Silverback is available in the list. By clicking on Edit, you can customise what the email templates contain. This includes adding images, modifying the text and input system variables.



8.4.1.1. Editing an Email Template

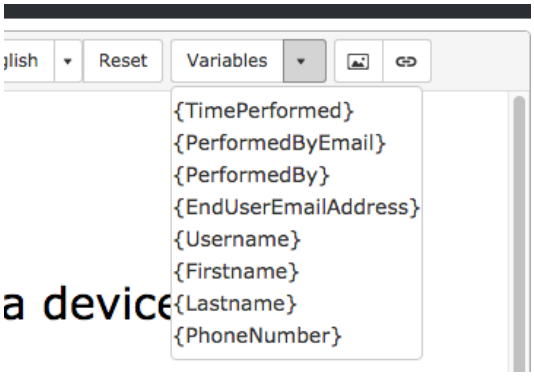
When you click Edit on a template, a window will appear showing you the contents of the template.



You can use the controls at the top of this window to modify the template itself. It's important to note that every language in the system has its own template. This means if you modify the template for English, these changes won't affect the German template.

You can change the language currently being edited by clicking on the language drop down menu at the top. Note that language sent with the email depends on some conditions. For Admin emails, the language of the destination administrator will be used. For user enrolment based emails, the language of the user's device using the SSP will be used. For user emails triggered by admins, the language of the admin will be used.

It's also possible to use System Variables in each template. The availability of the variables depends on the template you are working with. By clicking the Variables drop down menu, you can choose the variable to add and also see what is available for that template.



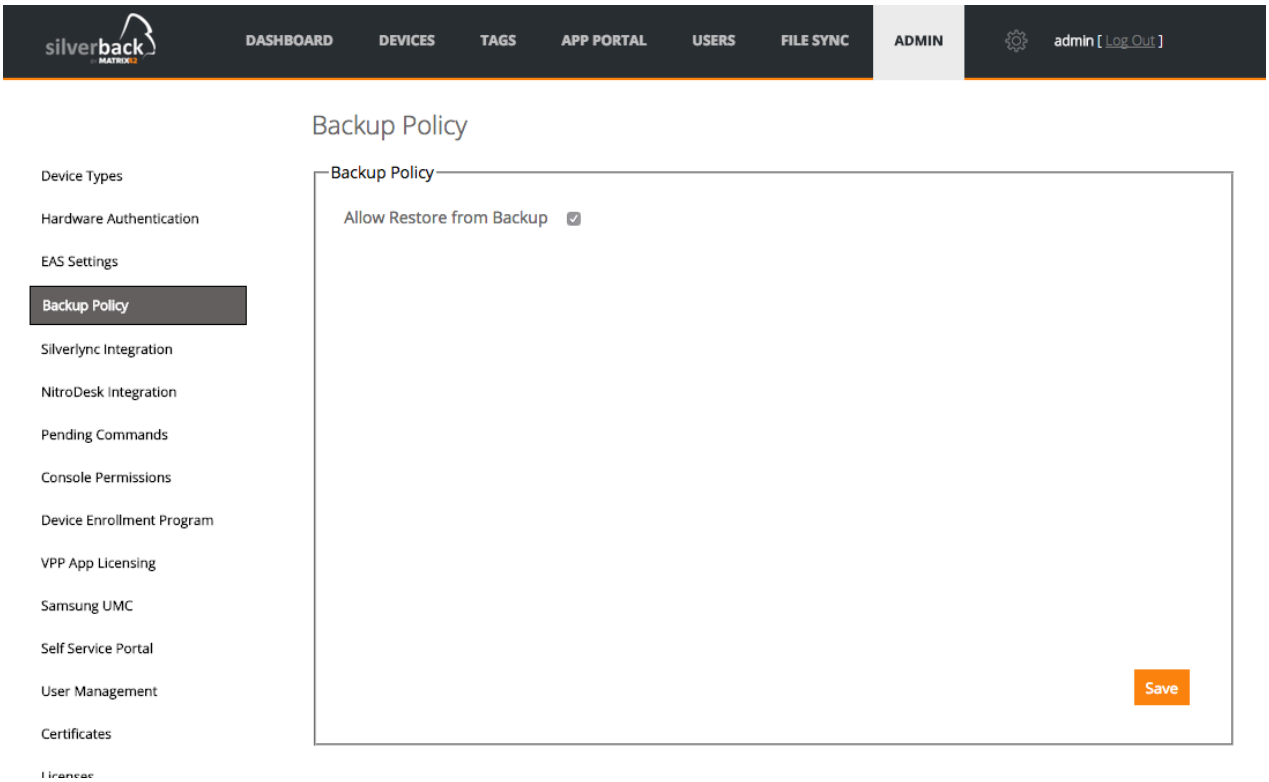
8.4.2. SMS Template

You can also modify the SMS message that is sent to users on enrolment. You can modify the message individually per language. The only variable available for SMS message is {0}, and this will be replaced with the user's enrolment link automatically.

8.5. Backup Policy

Administrators have the ability to allow or deny iOS devices to be restored from backup and maintain access to corporate information. By default this setting is disabled for security reasons, to prevent a user's backup being restored to another device. There are certain situations where a Restore from Backup is required, such as major iOS upgrades and it is recommended this setting be enabled only for the duration of the fleet upgrade.

If this setting is disabled, when a device is restored from backup, Silverback will detect this and send a command to the device, removing all corporate data.

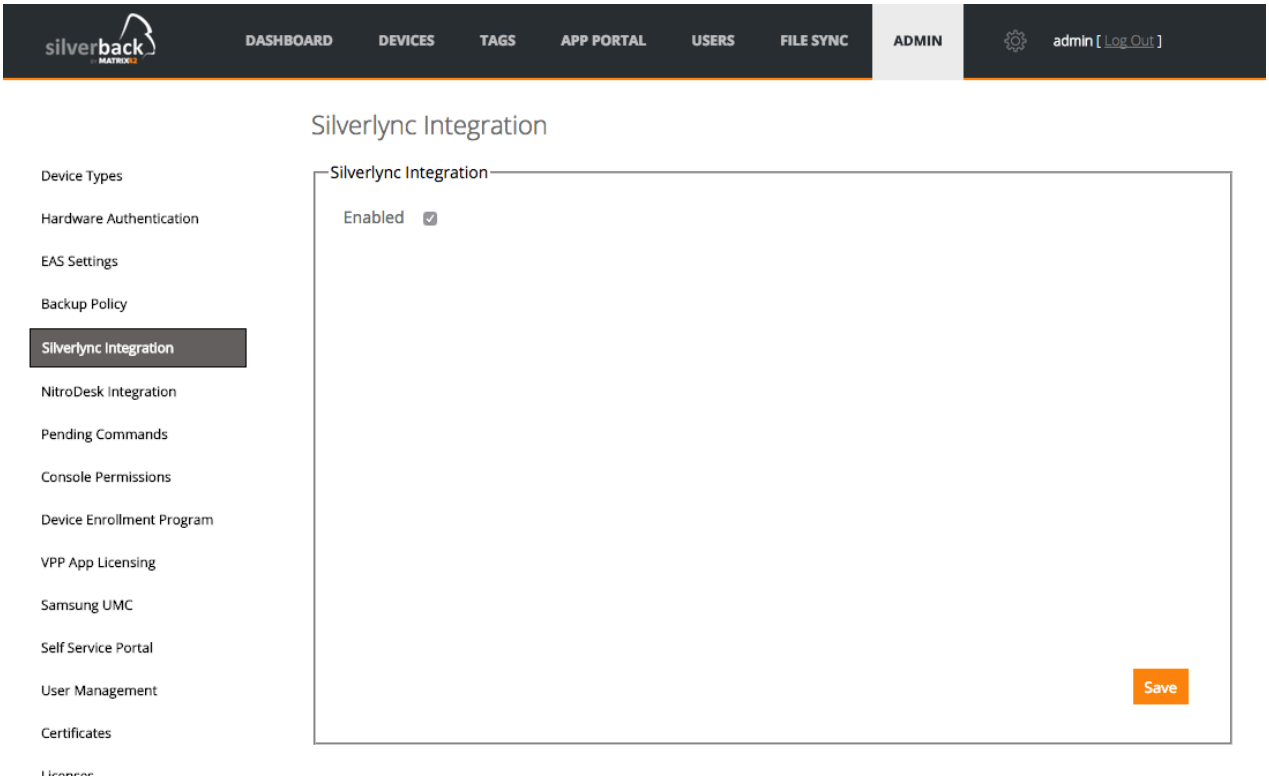


NOTE: This setting may also affect devices with Modified Operating Systems (Jailbroken / Rooted / Developer Unlocked / etc). Be sure to take this into account when dealing with such devices.

8.6. Silverlync Integration

Silverlync Integration allows certain VPN appliances to connect to Silverback and get information on the state of its enrolled devices.

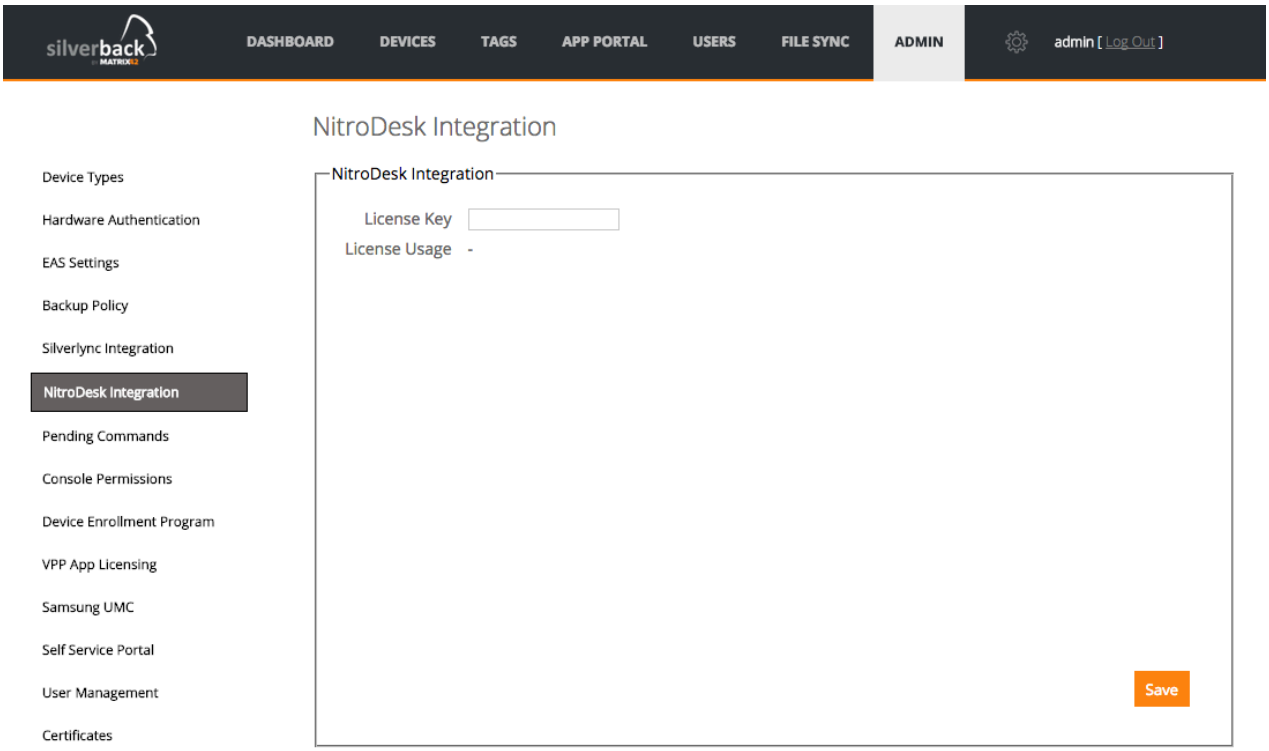
An example of this would be a VPN Appliance getting information on a user with a blocked device, and then disabling this device's ability to connect to corporate data at the network perimeter.



NOTE: For Silverlync Integration to work, your VPN Appliance must support this feature, please check with your VPN Appliance Manufacturer for more information on this.

8.7. NitroDesk Integration

Once you have your NitroDesk License, you will need to add this into your Silverback Installation so it can be distributed to your clients.



Control	Description
License Key	Your NitroDesk License Key
License Usage	How many devices are currently using a NitroDesk License

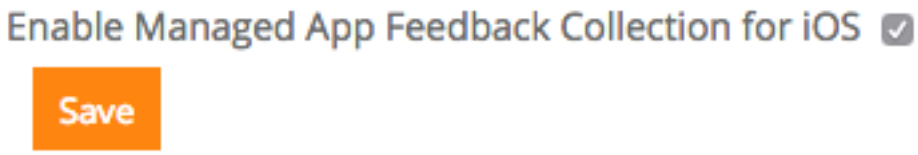
NOTE: Currently only the Android and Samsung Safe devices can use the NitroDesk settings configurable via Silverback.

NOTE: NitroDesk support is being deprecated.

8.8. Pending Commands

8.8.1. Managed App Feedback Collection

With iOS 7 and above, application developers can add information to their applications that a third party system like Silverback can retrieve. Enabling this setting will make sure that managed applications will be checked for application feedback. The application feedback is viewed from the Device Information Popup.



8.8.2. Pending Commands

iOS, OSX Samsung SAFE and Android devices have pending commands stored in a form of queue. This means when a given device checks in to the system, the system will find commands for that device in the queue and execute them.

This table shows you what pending commands exist in the system and also let you search and sort them, or even delete them.

Refresh | Delete Selected

Pending Commands

Username	Platform	Command	Queued	Not Now	Delete
0133c77a-1f0d-49fe-af58-	iPod	DeviceInformation	05/08/2016 06:00	0	
0133c77a-1f0d-49fe-af58-	iPod	DeviceInformation	05/08/2016 06:00	0	
0133c77a-1f0d-49fe-af58-	iPod	CertificateList	05/08/2016 06:00	0	
0133c77a-1f0d-49fe-af58-	iPod	ProfileList	05/08/2016 06:00	0	
0133c77a-1f0d-49fe-af58-	iPod	InstalledApplicationList	05/08/2016 06:00	0	
0133c77a-1f0d-49fe-af58-	iPod	ManagedApplicationList	05/08/2016 06:00	0	
0133c77a-1f0d-49fe-af58-	iPod	Restrictions	05/08/2016 06:00	0	
0133c77a-1f0d-49fe-af58-	iPod	ProvisioningProfileList	05/08/2016 06:00	0	
0133c77a-1f0d-49fe-af58-	iPod	SecurityInfo	05/08/2016 06:00	0	
0133c77a-1f0d-49fe-af58-	iPod	InstalledApplicationList	05/08/2016 06:00	0	
0133c77a-1f0d-49fe-af58-	iPod	InstalledApplicationList	06/08/2016 06:00	0	
0133c77a-1f0d-49fe-af58-	iPod	InstalledApplicationList	07/08/2016 06:00	0	
0133c77a-1f0d-49fe-af58-	iPod	InstalledApplicationList	08/08/2016 06:00	0	

25 | Page 1 of 695 | Displaying 1 to 25 of 17362 items

The various elements of the Pending Commands table are explained below:

Control	Description
Username	The username of the user who's device has the command queued
Platform	The OS type of the device, e.g. iOS, OSX, Samsung SAFE
Command	The actual command that is queued. You will notice patterns here, for example if you click "Refresh" on a device from the Devices Tab, you will see a certain set of commands appear in this list for that device.
Queued	The date and time that the command was queued
Not Now	If the device is not ready for a command, generally in the case of iOS it will reply with a "Not Now", meaning that its not ready. This could be for example if you attempt to install an application on the device, but the screen is locked.
Delete	This will delete the command from the table. Care should be taken as this is permanent, and if the command was important for the device's function, it will not execute.

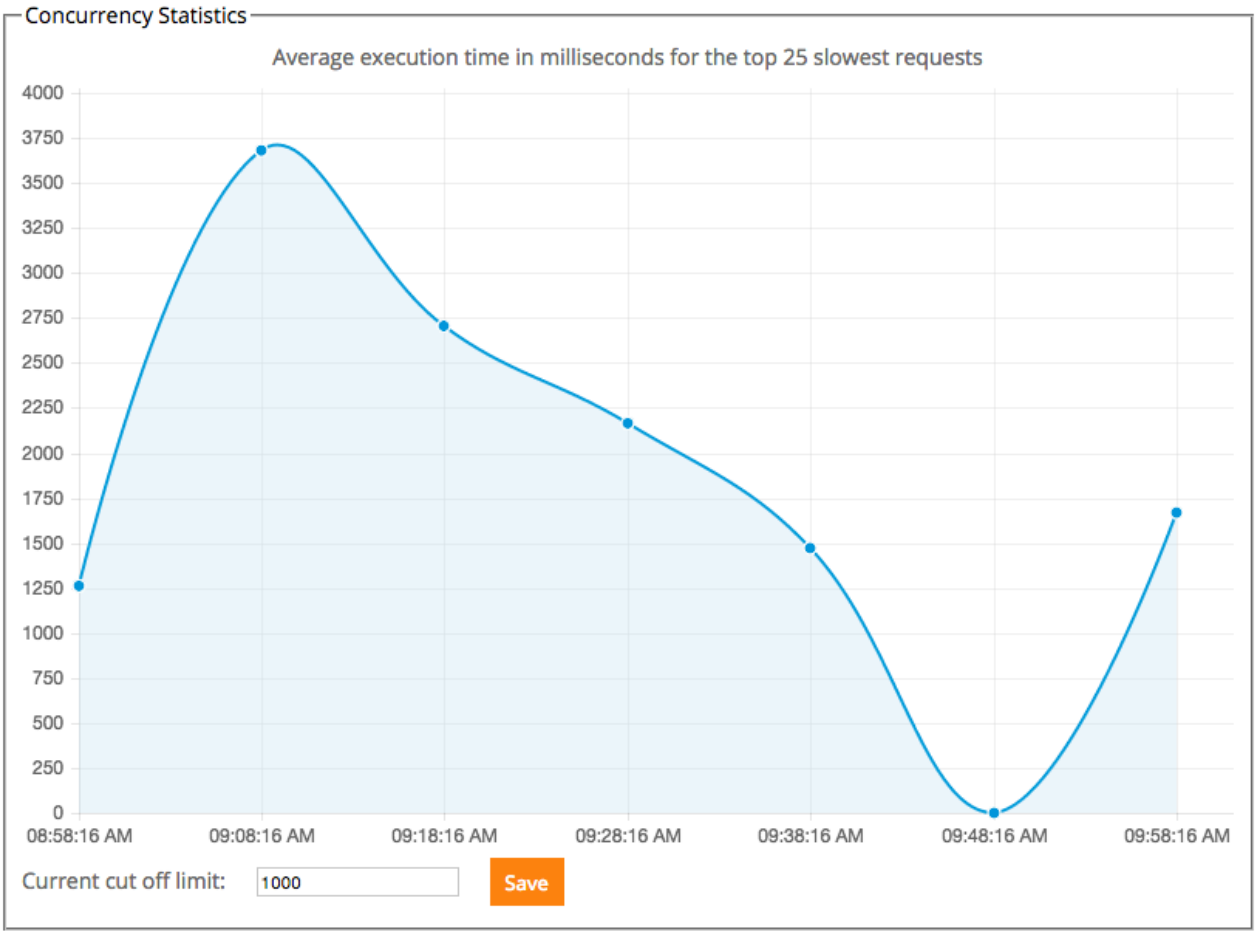
8.8.3. Concurrency Statistics

NOTE: These settings will only be visible if the settings for concurrency in the Settings Administration page allow it. See the Settings Administration guide for enabling this.

Concurrency Statistics gives you an overview of how long commands are taking to execute in your environment. The graph will display the average execution time for the top slowest requests.

The “Current cut off limit” is the maximum number of devices that can connect to the system at any one time (this excludes enrolling devices). In large deployments, this means that a steady load can be achieved on the server. When a device attempts to connect and this number is consumed, the device will be told to “go away”, and attempt to connect later.

Use the average execution time in the graph to determine your system limit. If the times are getting too high, reduce the cut off limit.



MATRIX42
SMARTER WORKSPACE – BETTER LIFE

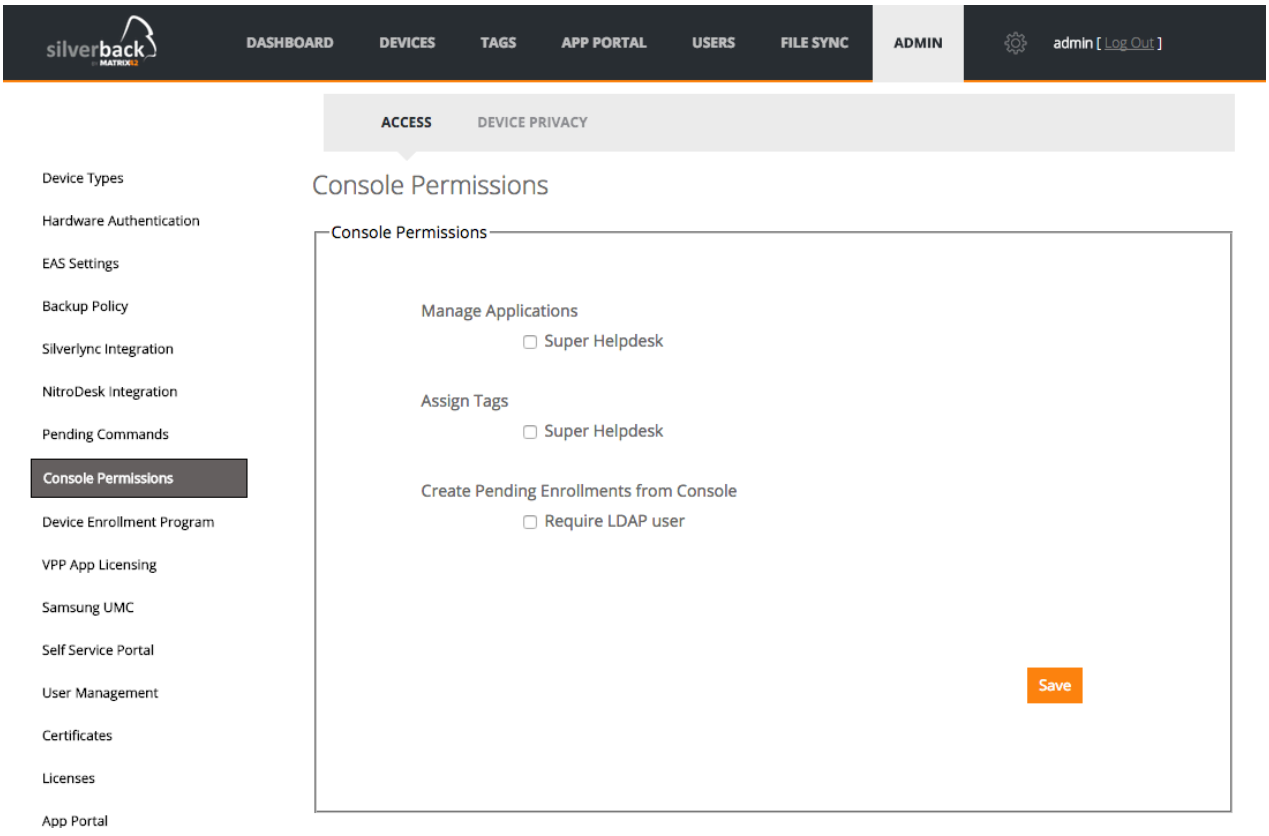
Silverback by Matrix42 Admin Guide Version 5.1 U3

Autor: Matrix42 Cloud & Mobile Management

8.9. Console Permissions

8.9.1. Access Section

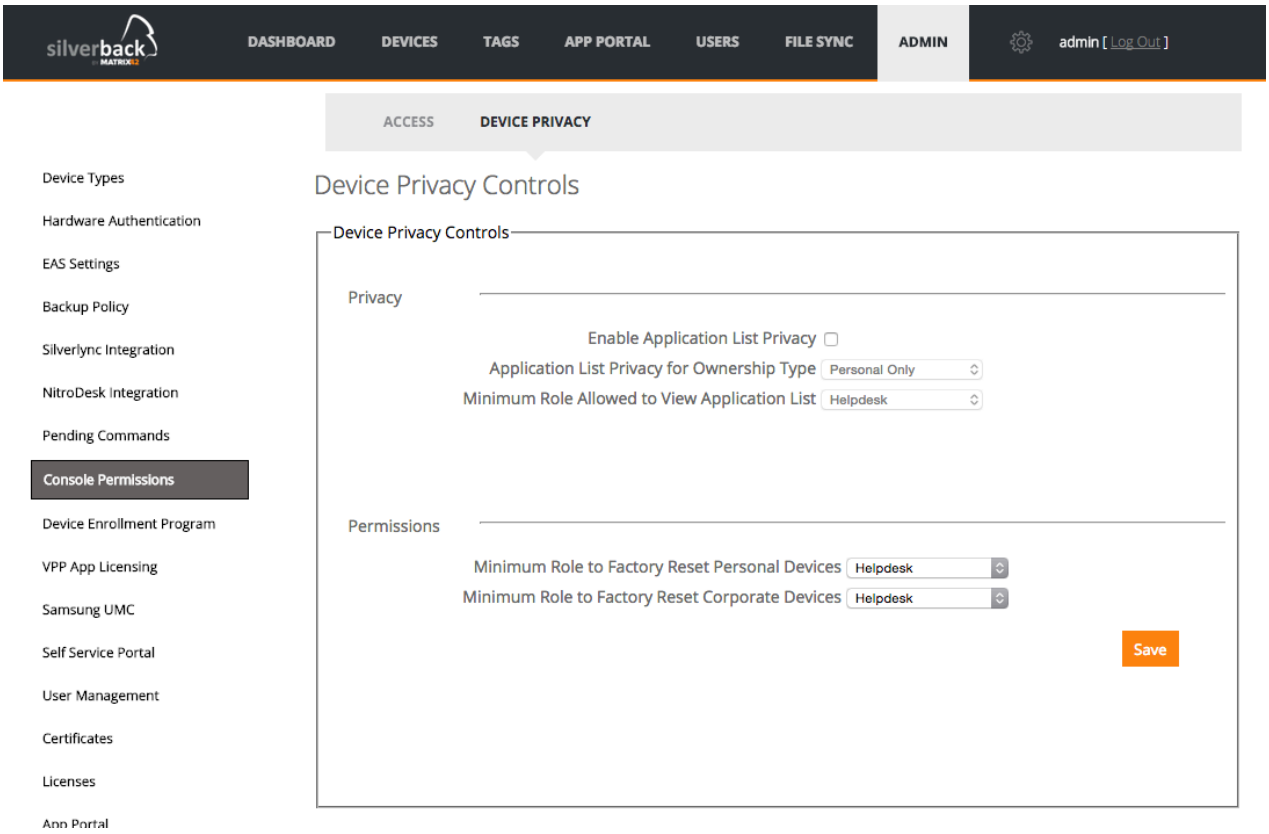
In addition to the normal permissions granted to the various console user roles, some of these can be additionally configured from the Console Permissions, Access section.



Control	Description
Managed Applications	When enabled, grants the Super Helpdesk role the ability to Manage Applications
Assign Tags	When enabled, grants the Super Helpdesk role the ability to Assign Tags to devices
Create Pending Enrollments from Console	When enabled, local user accounts cannot be used to authorize pending enrollments. An LDAP account must be used.

8.9.2. Device Privacy Section

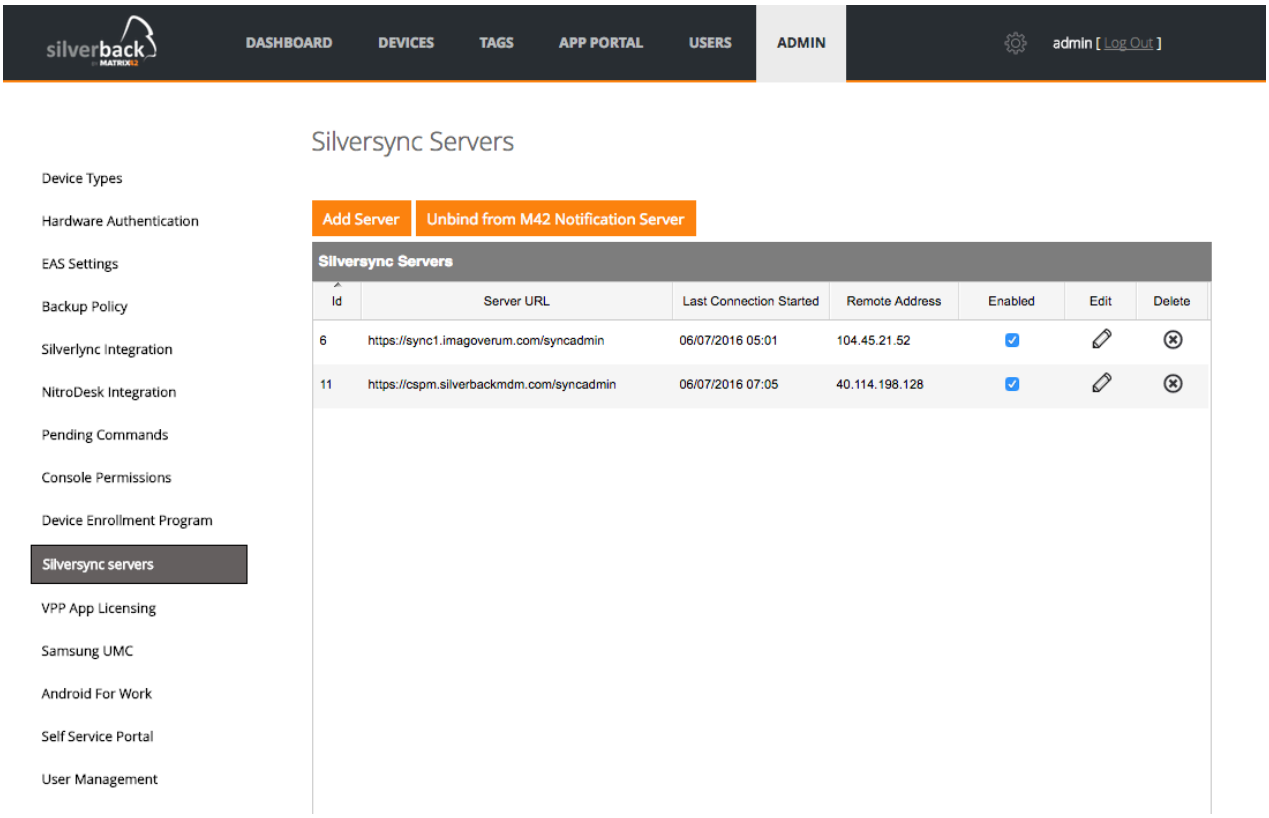
Silverback allows the administrator to control visibility of applications installed on devices. Administrators can also control the permissions of the system users to view the applications list and perform the factory reset on the managed devices.



Control	Description
Enable Application List Privacy	Enables and disables the privacy control
Application List Privacy for Ownership Type	The ownership type that the applications are kept private for
Minimum Role Allowed to View Application List	Controls the user role required to see the applications list
Minimum Role to Factory Reset Personal Devices	Controls the user role required to factory reset a personal device
Minimum Role to Factory Reset Corporate Devices	Controls the user role required to factory reset a corporate device

8.10. Silversync Servers

As of Silverback version 5.0 Update 2, the old Silversync admin console has been moved to this location in the Silverback admin console. This means that you can now manage all aspects of Silverback and Silversync from one location.

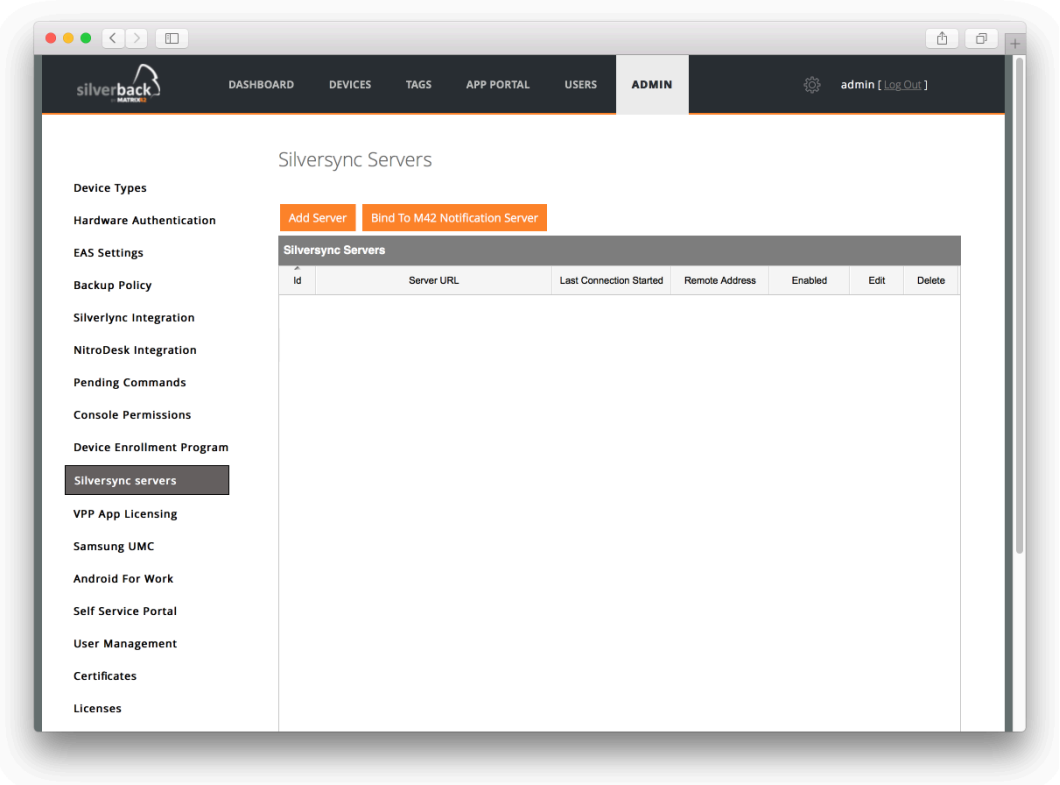


This main page lets you see the list of Silversync servers currently configured in your system.

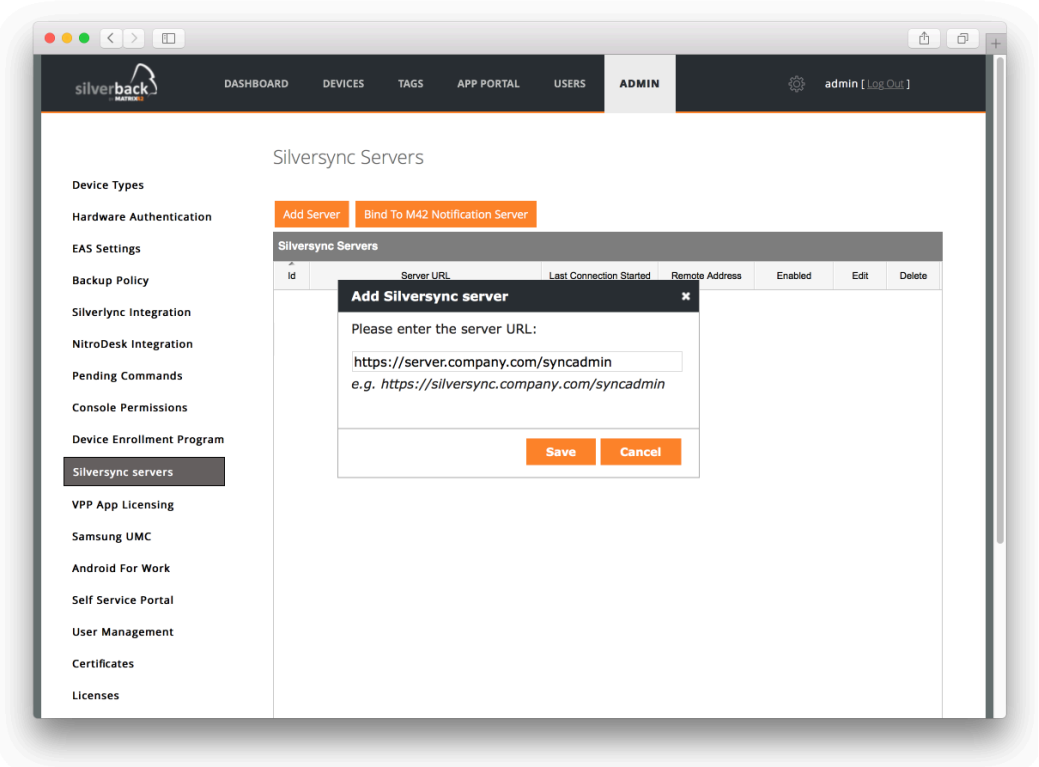
8.10.1. Adding a Server

Click Add Server

Silverback by Matrix42 Admin Guide Version 5.1 U3

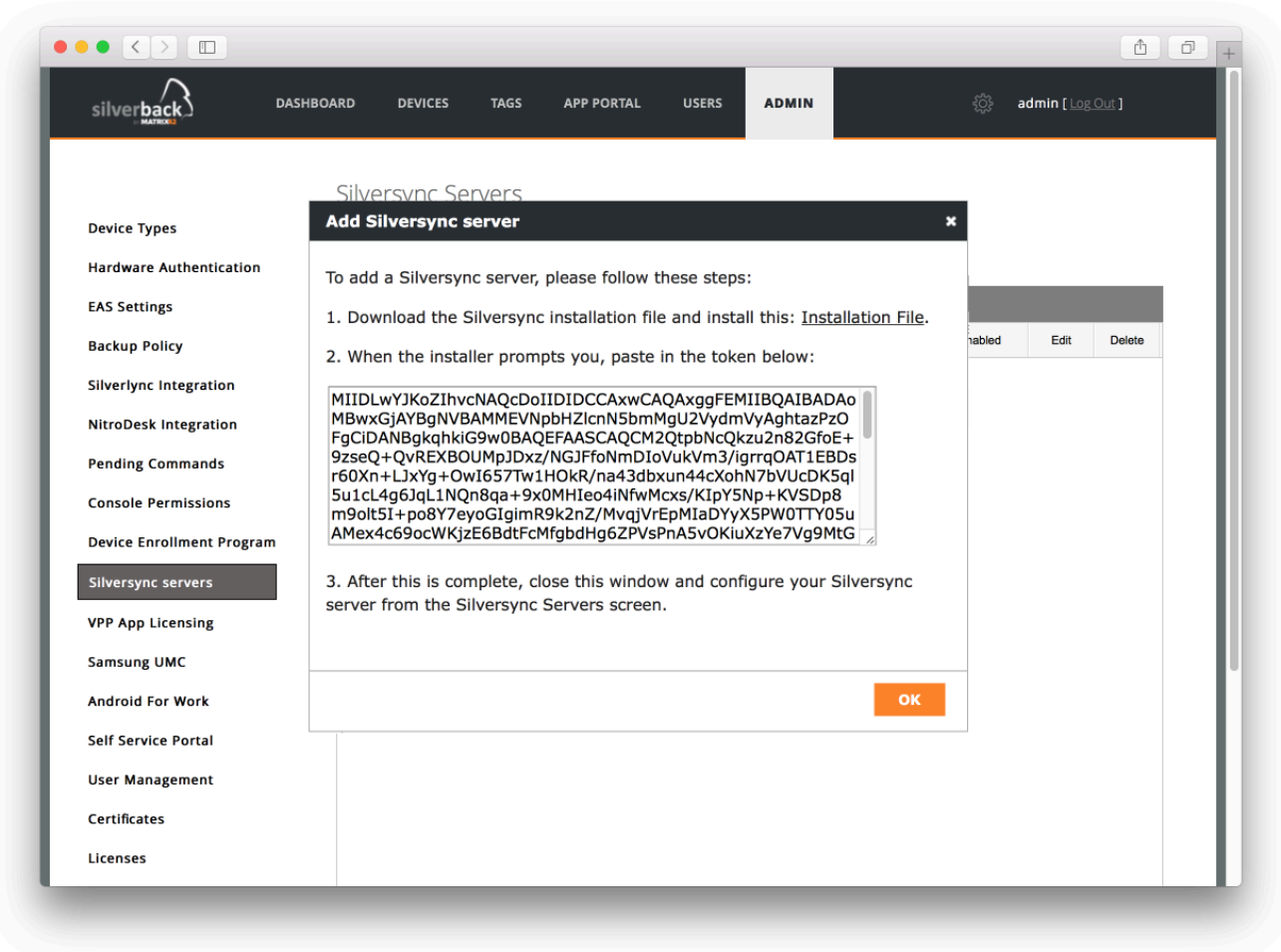


Enter your server URL and click Save. Note that this should match the DNS entry users will use to sync to your Silversync server. You should also ensure to enter https:// and add /syncadmin to the end of the URL.



Autor: Matrix42 Cloud & Mobile Management

On the following prompt, click the Installation File link to download the Silversync installer. Copy this file to the intended Silversync server. Also while you have this page open, you should copy the token displayed in the text area. This token is used to bind your Silversync server to this Silverback server.



After downloading the installation file from the Silverback console, launch the installer. This should be launched on the Silversync server as an account with local administrator privileges. It's also important that if you intend to use User Based authentication for syncing users, that you are a Domain Administrator account.

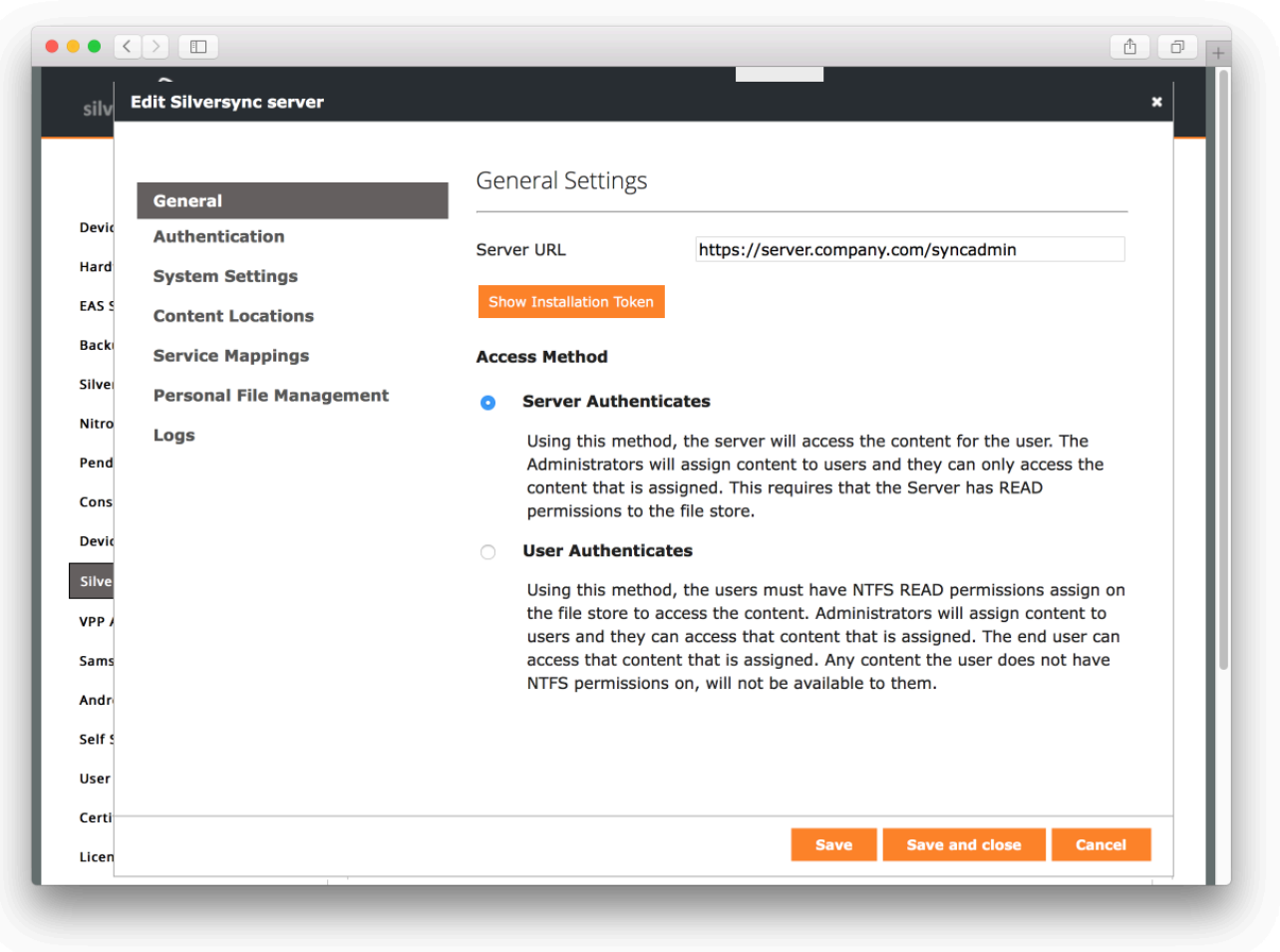
For more details on the installation, please see the Silversync installation guide.

8.10.2. Configuring Silversync

8.10.2.1. General Section

On the General tab you need to specify the Access method. This determines how users will access files:

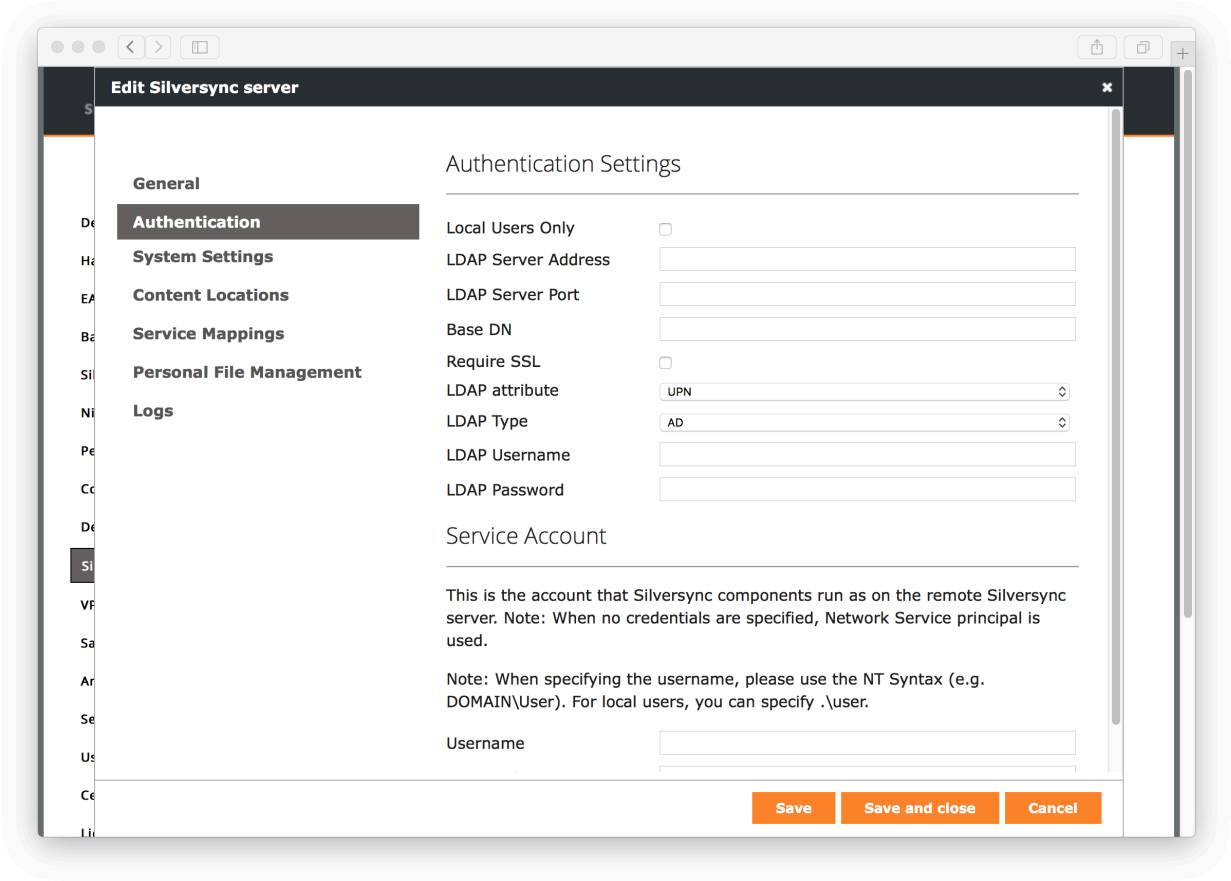
- Server Based authentication means that the service account on the server will access the files on behalf of the user. This means only the service account for the Silversync server needs access to the files.
- User Based authentication means that the individual user's file permissions are used. This means that a user must be granted read permissions on a file before they will be able to sync it.



Note: If you do not see the "User Authenticates" option, this likely means that your Silversync server is not domain joined. This is a requirement for User based authentication.

8.10.2.2. Authentication Section

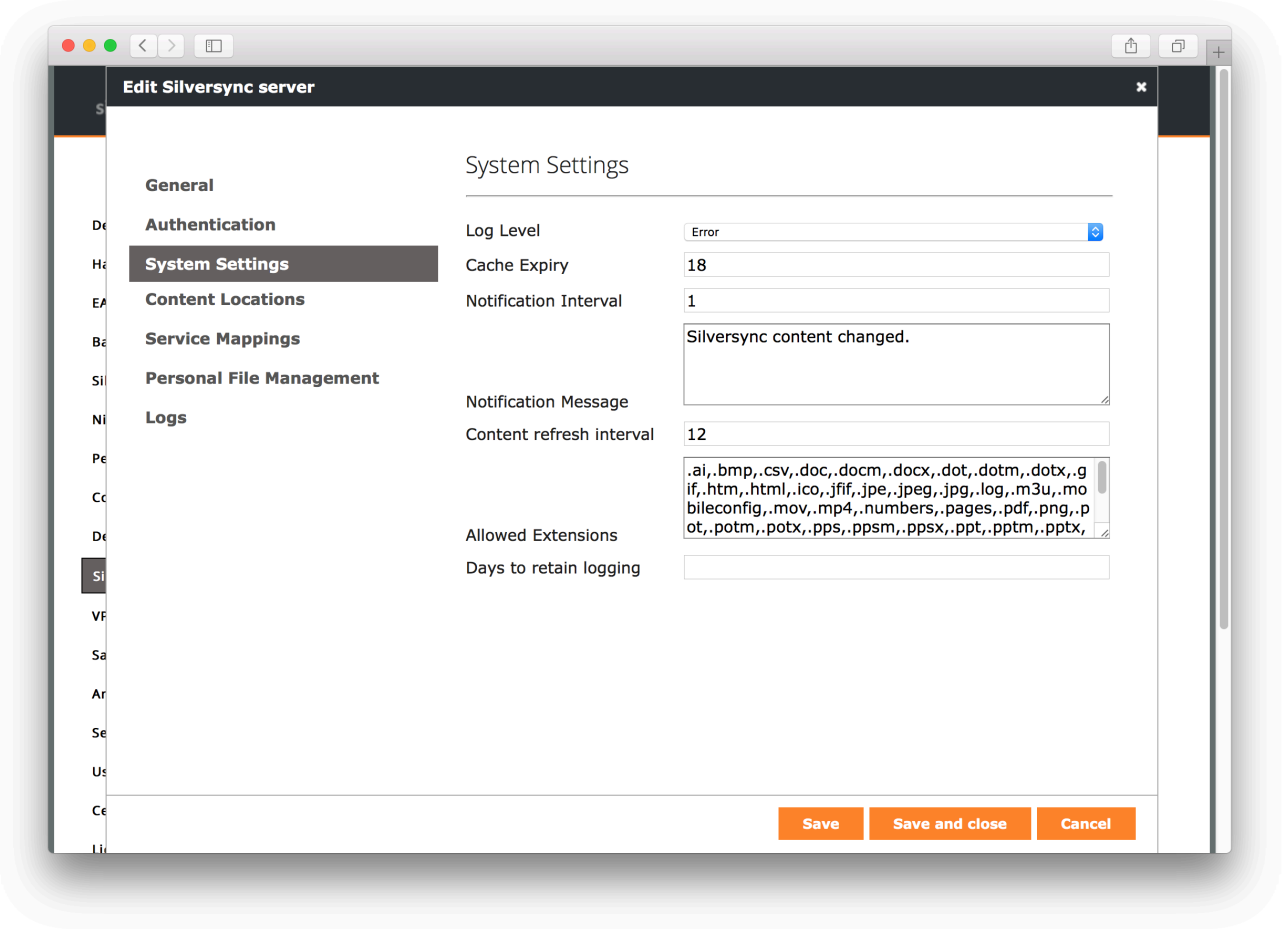
The authentication section lets you define the access settings for LDAP users and also the service account.



Setting	Description
Local Users Only Authentication	Will only allow Local Silverback Users to synchronise
LDAP Server Address	Network address or FQDN of the LDAP Server
LDAP Server Port	TCP Port for LDAP Communications
Base DN	The base container where Silverback will look for users
SSL Required	Defines if LDAP/S is being used
LDAP Identifying Attribute	LDAP Attribute to use for authentication
LDAP Username	LDAP Lookup account used when searching for users
LDAP User Password	Password for the LDAP Lookup account
LDAP Server Type	The Type of LDAP Source being connected to.
Service Account Username	Let's you determine which account Silversync will run as. If empty, Network Service is used.
Service Account Password	Let's you determine which account Silversync will run as. If empty, Network Service is used.

8.10.2.3. System Settings

System Settings lets you determine some environmental defaults for this Silversync server:



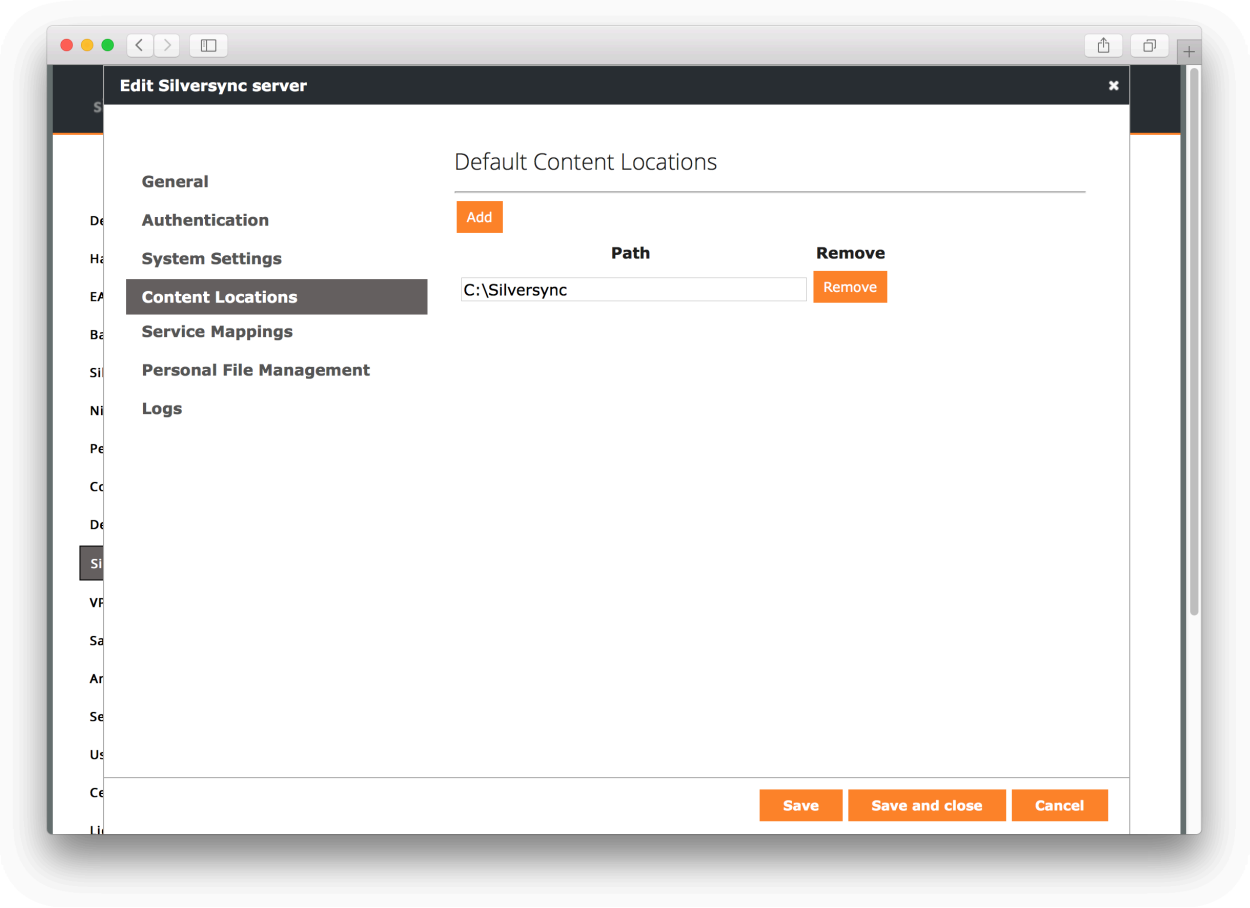
The settings affect the system in the following way:

- Log Level – This is the amount of detail included in the logging, this should mainly be changed for troubleshooting purposes
- Cache Expiry – How long until the cached will be cleared. Caching the content helps speed up synchronization, but it should not last for a long time as it takes system resources to maintain.
- Notification Interval – How long in minutes the system should wait before sending another push to a user. This prevents the user from being notified multiple times when copying several files. This prevents the user from getting, for example five notifications instantly if you copy five files to the content location.
- Notification Message – This is the message that is sent to the user when content changes are detected
- Content Refresh Interval – How long until the system will refresh the entire content location for the users. In general, this can be left, as individual file changes are automatically detected.

- Allowed Extensions – This lets you determine what file types should be recognised by Silversync. Files not on this list will be excluded which is helpful for filtering out system files, or file types that users might not be able to open.
- Days to retain logging – How many days should the Silversync logging be kept before being removed.

8.10.2.4. Content Locations

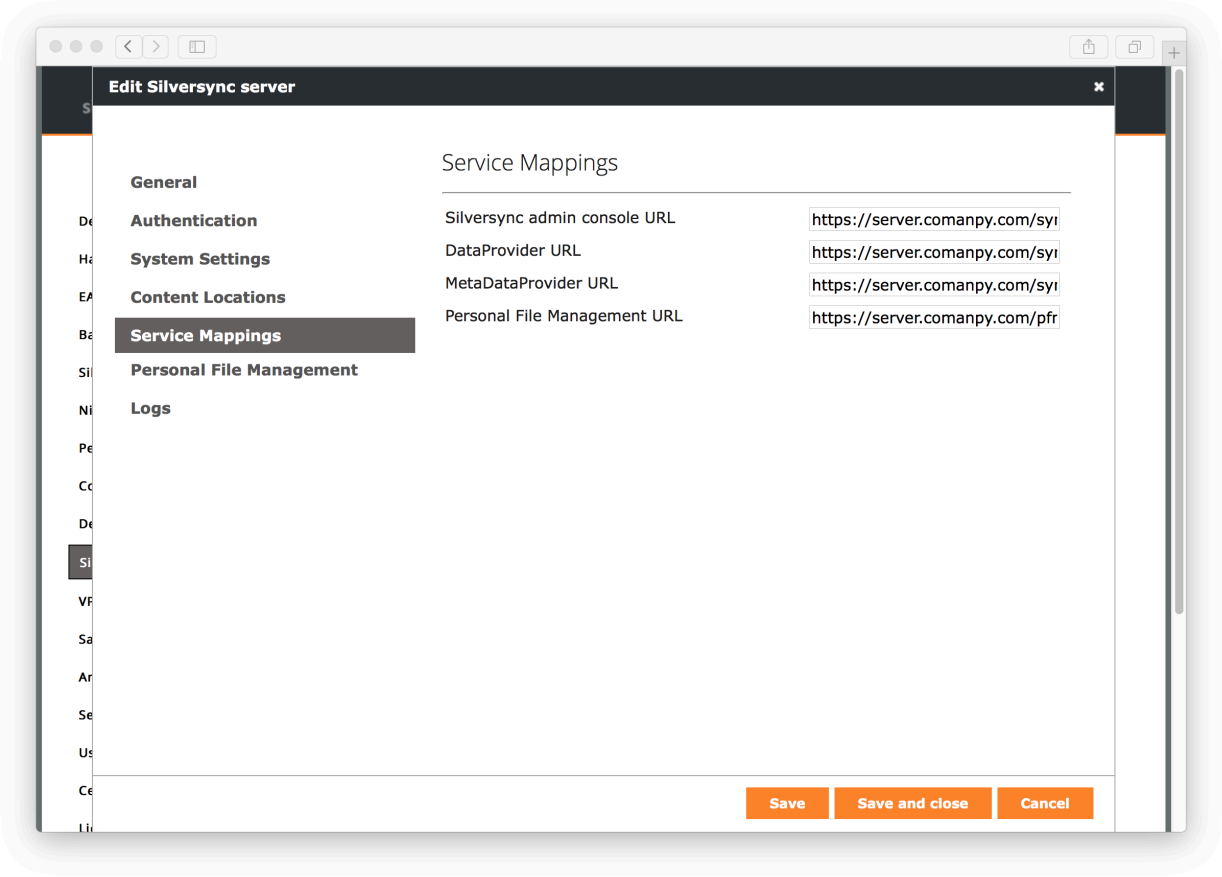
Content locations are the base level file system locations for users to sync content. A file location must exist here before it can be assigned to Tags and Users.



Note that Content locations can be local to the server (e.g. C:\SilversyncContent\) or on a remote Windows file share (e.g. \\RemoteServer\Share).

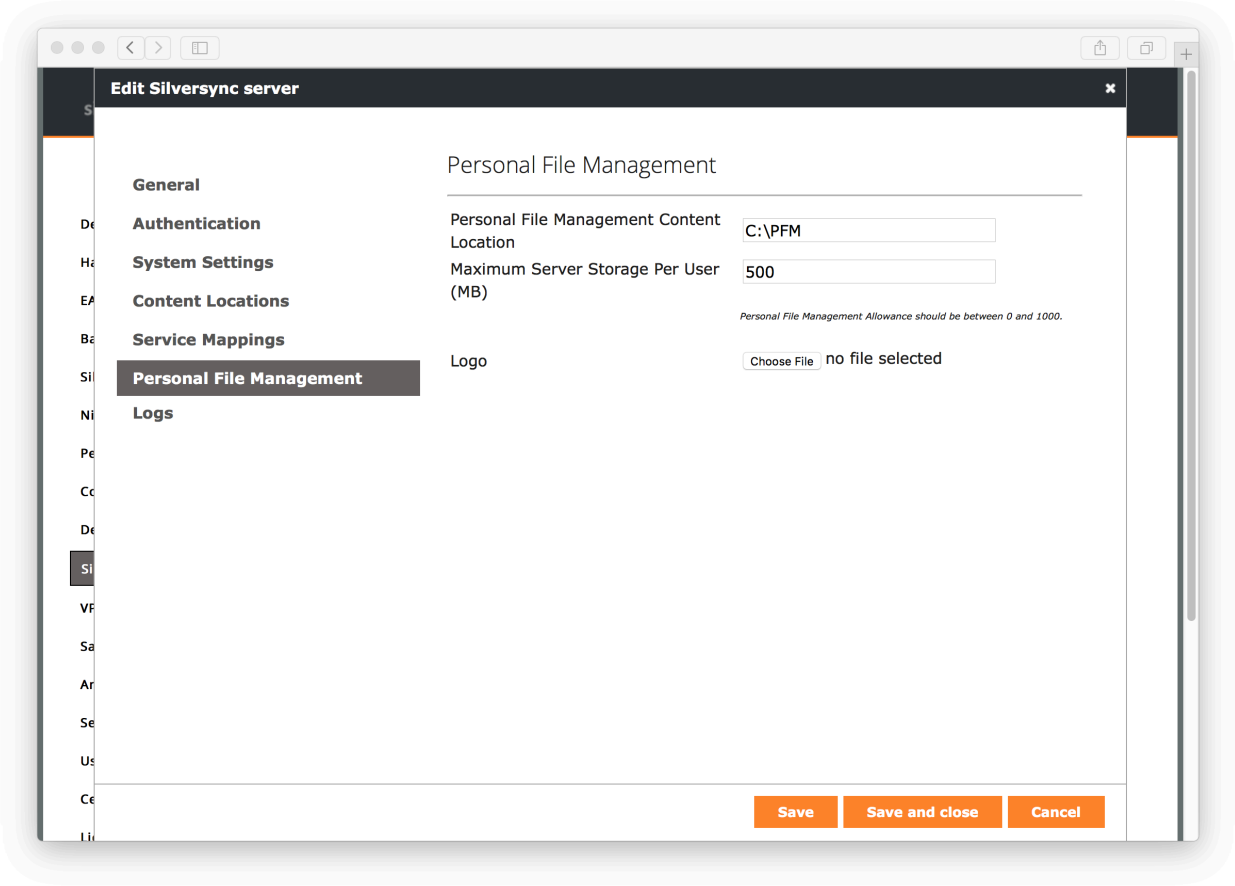
8.10.2.5. Service Mappings

Service Mappings determine the location of web services for access by users and applications. It's recommended to leave these as default, but also ensure you check that it matches the DNS entry for your Silversync server. It should be automatically populated with your server URL:



8.10.2.6. Personal File Management

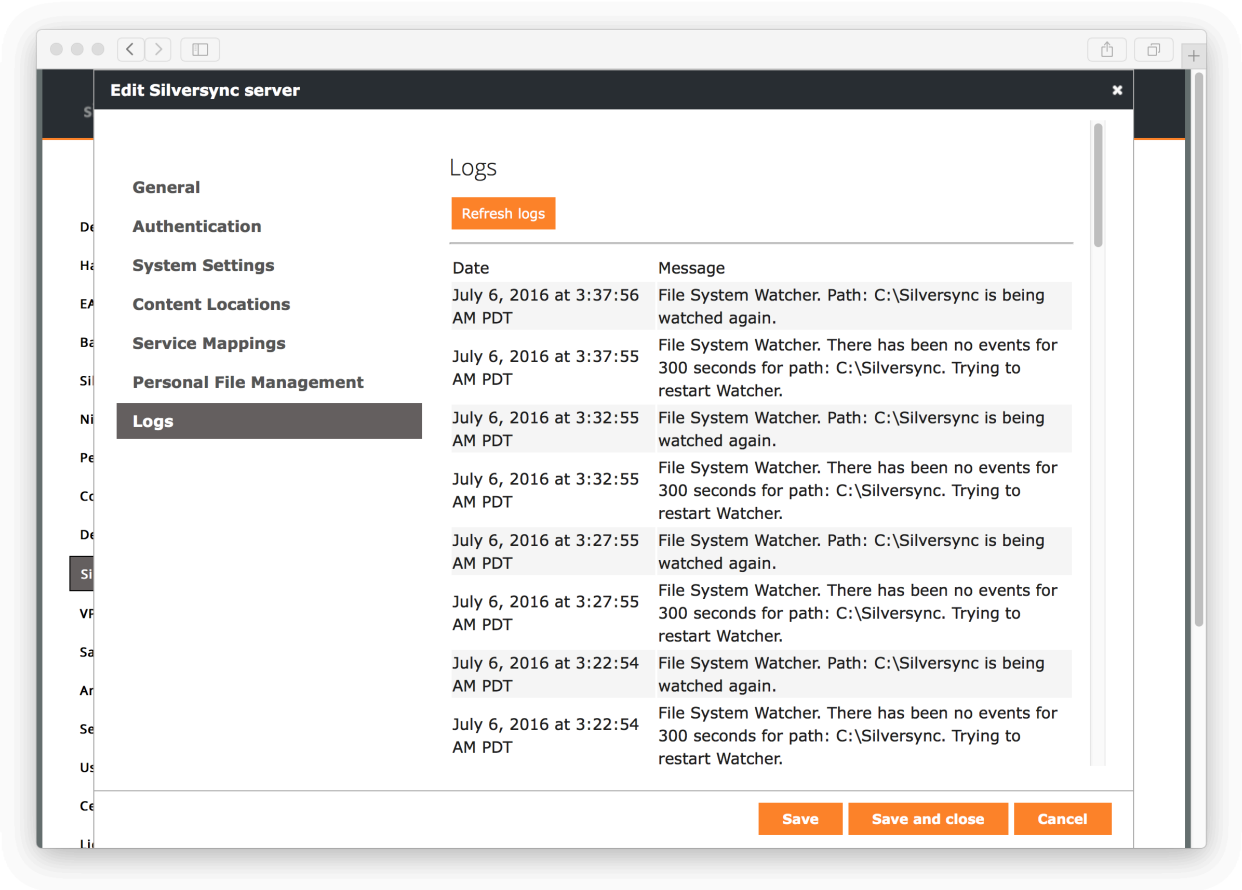
This optional module lets users upload their own content into Silversync. Note that the files in normal Content Locations defined above are READ only. Personal File Management is a user's own personal storage space. The settings on this page let you configure the requirements for this.



- Personal File Management Content Location – This is the location relative to the Silversync server to store Personal File Management uploads by users. Leave this blank if you do not wish to use PFM.
- Maximum Server Storage Per User – The maximum size in megabytes that a user is allowed to consume on the server. This is per user, so keep this in mind when planning available storage, that this number should multiply with every new user in the system.
- Logo – Lets you upload a logo file that will be shown to users in the PFM console. This helps with branding to give users a common feel with your other company pages.

8.10.2.7. Logs

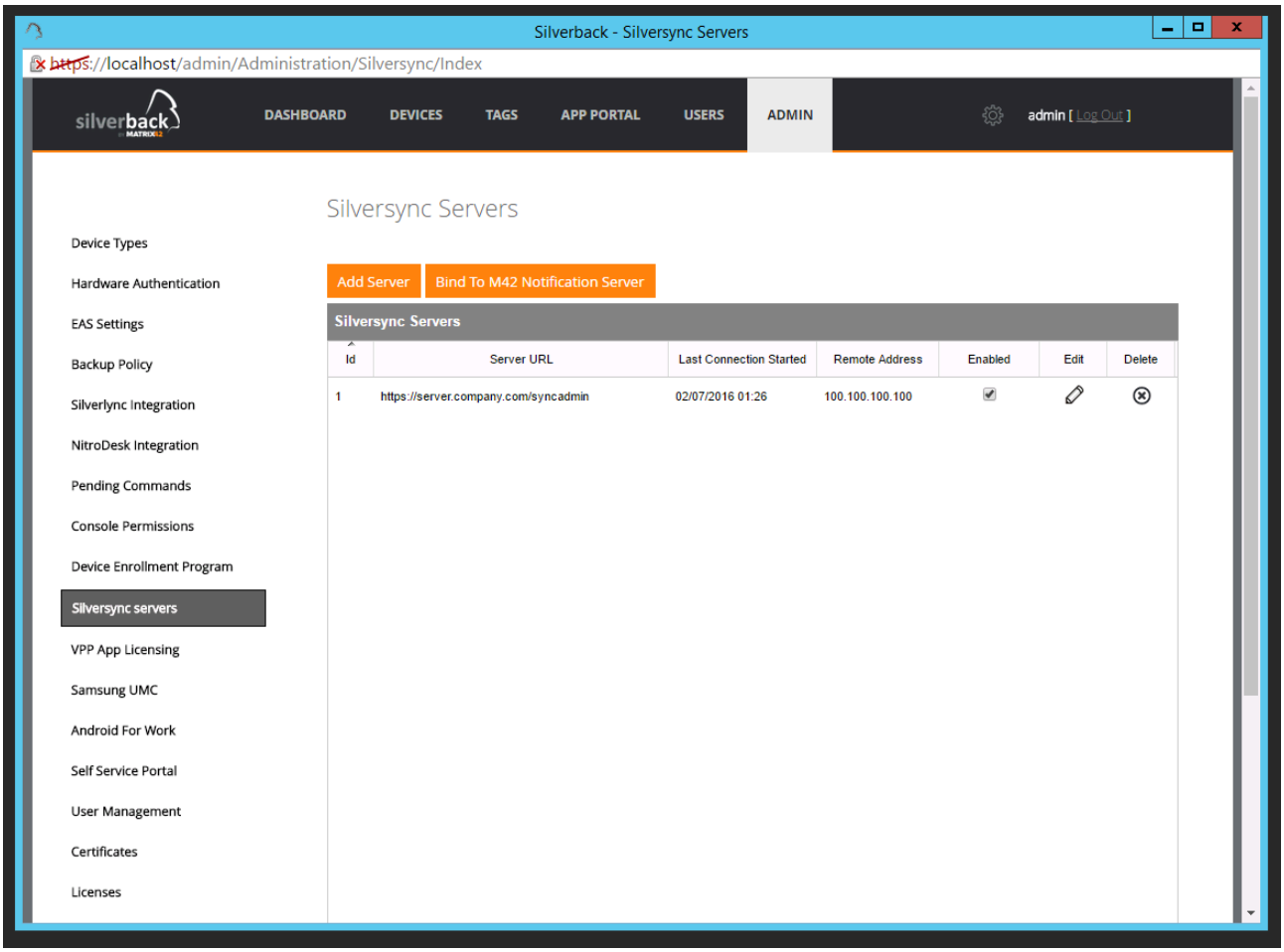
Logs doesn't offer the ability to configure anything, but its useful to know how to access this page. This is where logging can be found for your Silversync server. If you need to troubleshoot a problem, or confirm that new content is being picked up, you can check this page.



8.10.3. Binding Push

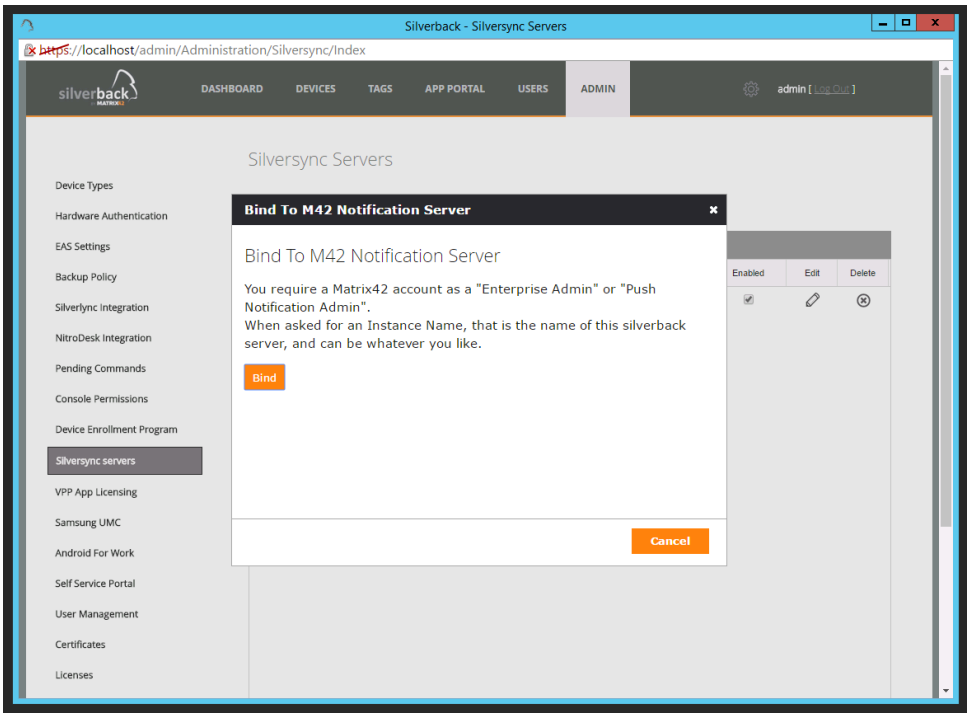
Previously Silversync used its own push certificate for notifying users of new content. In this version, Silverback connects to the Matrix42 push service for you to handle push notifications.

To enable this, you need to bind your server to the M42 Notification Server. This is done from the Admin console in the Silversync Servers menu item, by clicking “Bind to M42 Notification Server”.

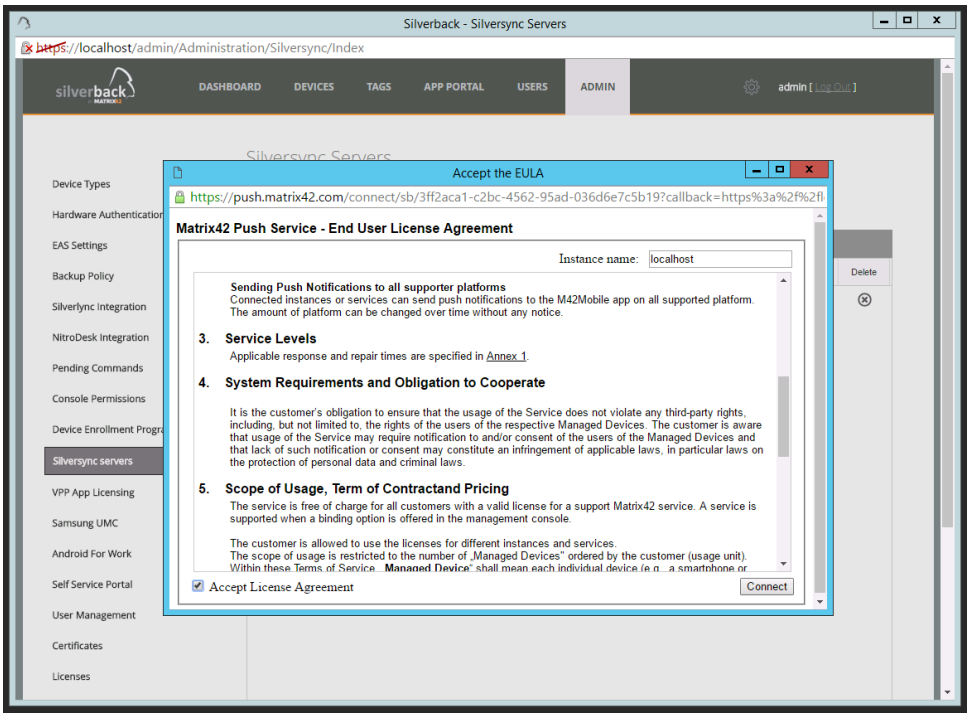


You will get a popup to complete the binding. Ensure you have a Matrix42 account that matches the requirements in the popup, and then click Bind:

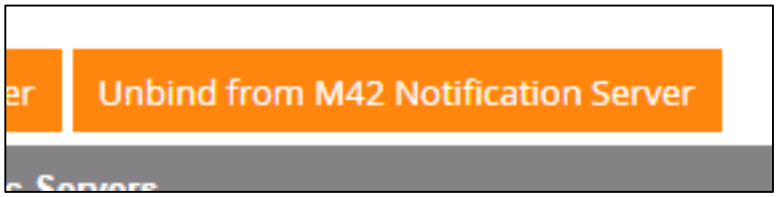
Silverback by Matrix42 Admin Guide Version 5.1 U3



Login with your Matrix42 account, accept the EULA and click Connect:



If this completed successfully, the button should change to “Unbind from M42 Notification Server”:



8.11. Device Enrollment Program

Apple's Device Enrollment Program can be managed from this section in the Admin Tab. The Device Enrollment Program allows you to have devices enroll into Silverback on first setup, rather than having the user navigate to the Silverback website after setup.

8.11.1. Home Section

The main page gives an overview of the status and information relating to your DEP (Device Enrollment Program) account. The organization and server information displayed is configured when settings up DEP for your server with Apple.

The Account Overview section indicates how many devices are currently in your DEP account and how many are currently enrolled in Silverback.

Device Enrollment Program

Device Enrollment Program ☑ Enable

Refresh | Devices | Settings | Logs

Information: Last Updated: 2015-09-30 04:34:04 by admin

Company Settings: Valid

Server Name:	Server01
Server UUID:	0AA303FED341456AHD152DB687604F4C
Facilitator ID:	user@company.com
Organization Name:	Silverback MDM LLC
Organization Email:	user@company.com
Organization Phone:	6505555555
Organization Address:	641 Lexington Ave 14th Floor NY, 10022 (USA)

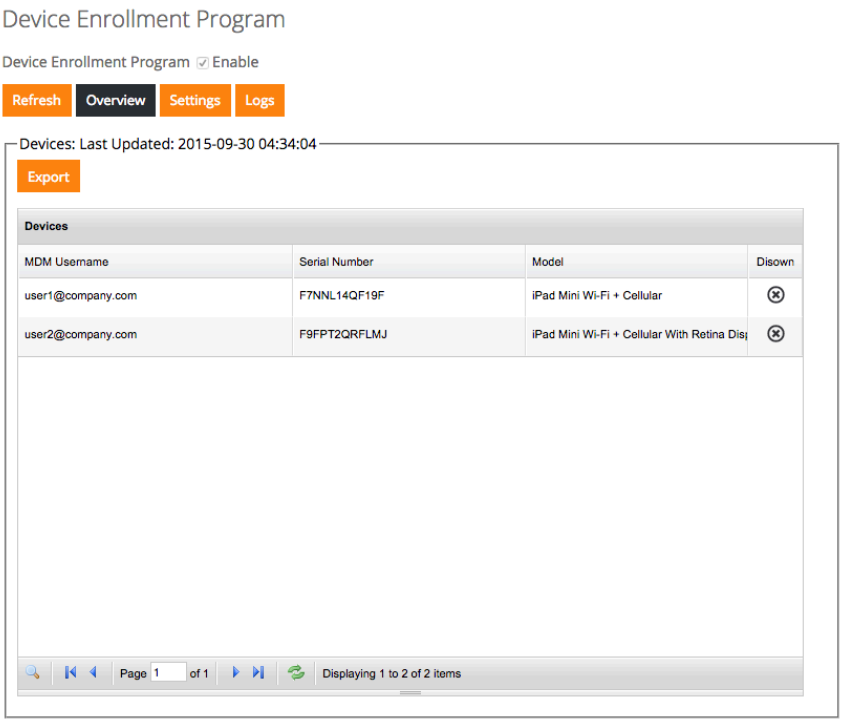
Account Overview:

Total Devices:	2
Devices Enrolled in MDM:	1

8.11.2. Devices Section

The Devices section lists the devices in your DEP account, and an associated username if the user is enrolled.

****Note: The disown function will permanently remove a device from current and future DEP accounts. It is recommended to not use this.****

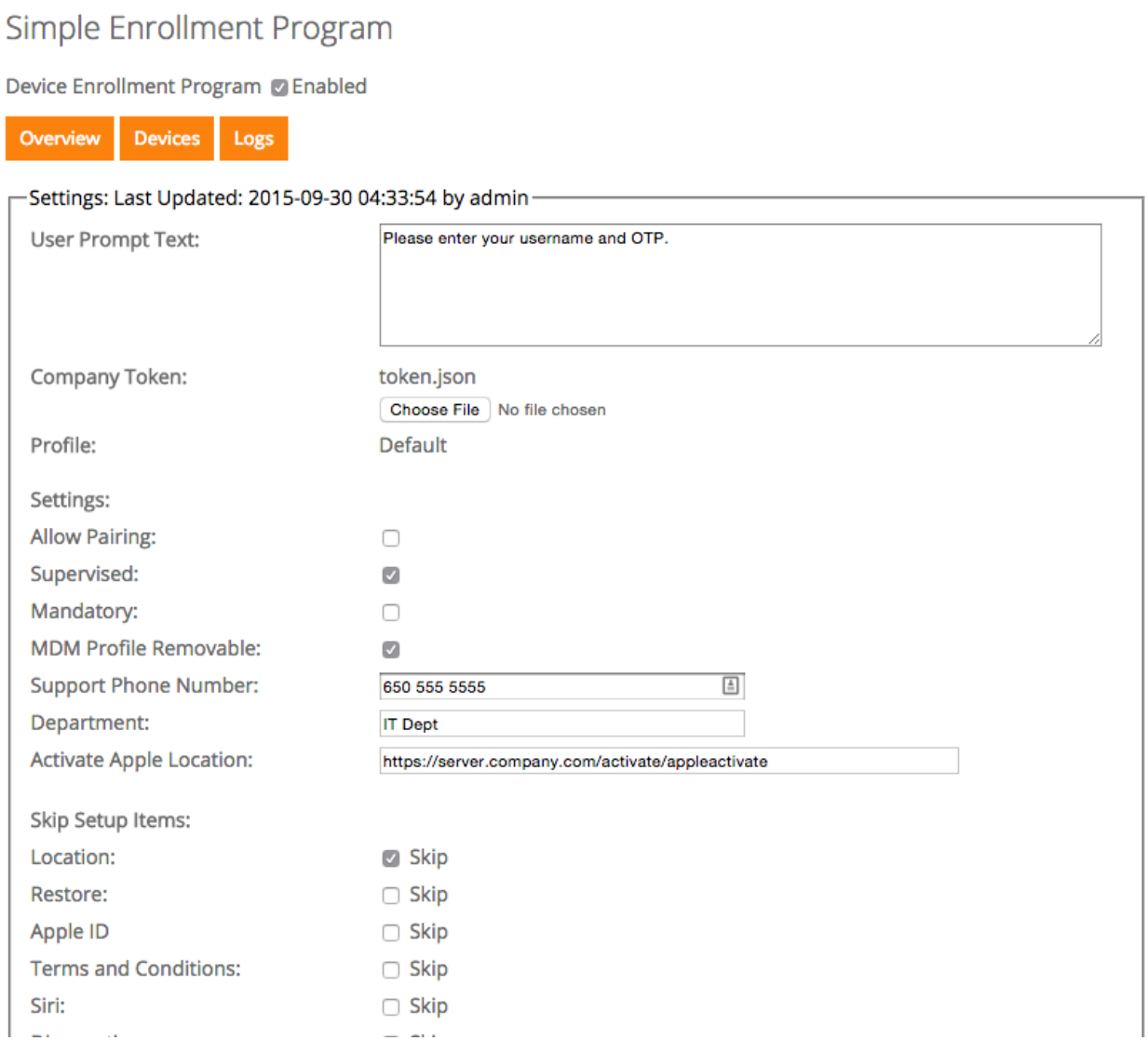


The table shows a list of all users in your DEP program, regardless of whether they are enrolled in Silverback. The list can also be exported by clicking the Export button. The table shows the following details:

Column	Description
MDM Username	If the serial number matches a currently enrolled user, it will be displayed here
Serial Number	The serial number of the device in your DEP program
Model	The model description of the device
Disown	Removes the device from the current and future DEP accounts. **THIS IS IRREVERSIBLE, IT IS NOT RECOMMENDED TO DISOWN DEVICES**

8.11.2.1. Settings Section

The Settings section allows you to configure your integration with Apple's DEP program and determine the device behavior.



Control	Description
User Prompt Text	The text presented to the user on enrollment.
Company Token	The token file provided by Apple.
Allow Pairing	Determines if the device can be paired with a computer.
Supervised	Determines whether the device will be supervised.
Mandatory	Determines if the user can skip the enrollment process. Note: The device will be unusable unless enrolled in Silverback.
MDM Profile Removable	Determines whether the MDM profile can be removed by the user after enrollment
Support Phone Number	Displayed to the user in the About section on enrollment.

Control	Description
Department	Displayed to the user in the About section on enrollment.
Activate Apple Location	Location for the devices to activate on enrollment. This should be changed to reflect your server address.
Location	Skip Location Services setup
Restore	Skip Restore from backup
Apple ID	Skip entering Apple ID information
Terms and Conditions	Skip Terms and Conditions Agreement
Siri	Skip Siri Setup
Diagnostics	Skip Send Diagnostics prompt
Passcode	Skip Passcode Setup
Registration (OS X)	Skip OS X Registration
Touch ID	Skip Touch ID Setup
Apple Pay	Skip Apple Pay setup
Zoom	Skip Zoom Setup
Move from Android	Skip the migration from Android prompt
FileVault Setup (OS X)	Skip File Vault setup for Mac
Anchor Certificates	Additional root certificates to be trusted by the device.
Supervising Certificates	If Allow Pairing is disabled, enter supervising computer certificates to allow the device to connect to that machine.
Save	Saves settings

8.11.2.2. Logs Button

Clicking the Logs button will export a CSV of actions that have been performed specifically on the DEP. This covers administrators making changes and also events that relate to the Silverback server connecting to Apple.

8.12. VPP App Licensing

Apple's VPP App Licensing program is an improvement on the old process of assigning VPP codes via a downloadable spreadsheet to users. VPP App Licensing is a service end point that Apple provides, where by licenses can be dynamically assigned to users and/or devices automatically and also revoked.

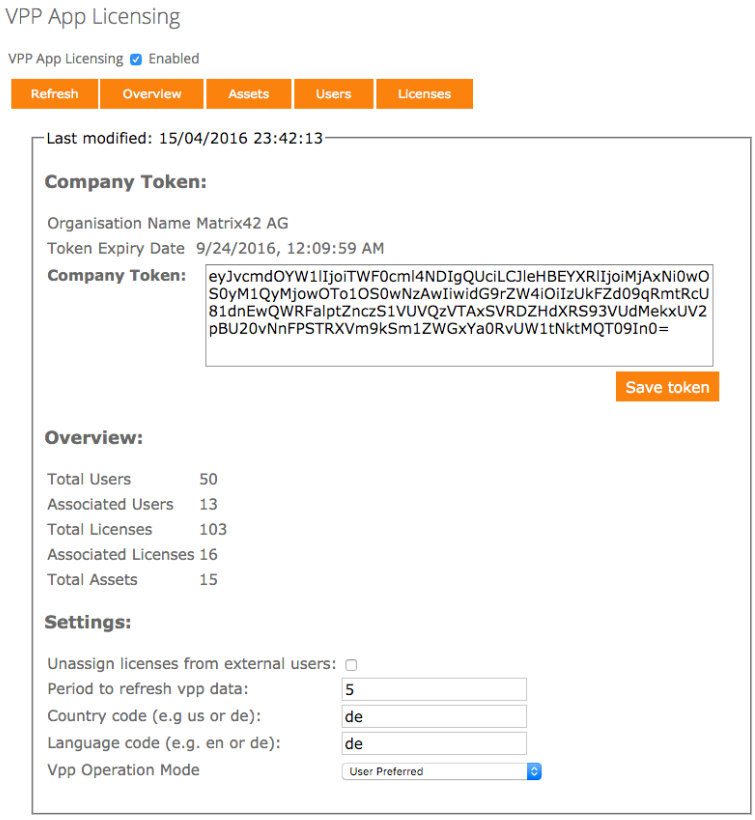
Silverback handles the assignment of users and devices to your VPP Program automatically when the users enroll in the system. Licenses purchased are also retrieved from Apple, and automatically populated into the App Portal where they can then be assigned to Tags.

Users and Devices are assigned licenses when they are present in a Tag that has a VPP Application assigned to it. Users and Devices have assigned licenses revoked when they transition out of a Tag with a VPP Application assigned.

Information is automatically synchronized with Apple, and can also be forced by clicking the Refresh button from the VPP App Licensing section. For troubleshooting, Logs can be exported by clicking the Logs button.

8.12.1. Overview Section

The Overview Section provides a high level view of your VPP Account, and lets you enter the company token.



Item	Description
Information	Shows the last time Silverback retrieved updated information from Apple.
Organization Name	The name associated with your VPP Account. This is provided when you sign up for the VPP Program
Token Expiry Date	The date that the VPP Token will expire. New tokens can be retrieved from the VPP Program website from Apple. The token can be managed from the Settings Section
Company Token	Text area for providing the VPP Company Token provided by Apple. This is required for VPP to function.
Total Users	Total users that have been added to your account, whether the user has associated themselves or not.
Associated Users	Users that are assigned to VPP and have also accepted and associated their iTunes account with your VPP Program
Total Licenses	Total licenses purchased for your VPP account, whether assigned to users or not.
Associated Licenses	Total number of licenses that are assigned to users in your system.
Total Assets	The number of applications in the system (regardless of the number of licenses per app).
Un-assign licenses from external users	Will instruct Silverback to automatically remove licenses from users it's not aware of. This is helpful when migrating from another solution that managed VPP for you, without you needing to manually un-assign all licenses.
Period to refresh VPP data	Time in minutes before VPP information should be updated.
Country code	Country code of the VPP apps you wish to install
Language code	Language code of the VPP apps you wish to install. Note this should be the same as Country code.
VPP Operation Mode	Allows you to determine the default behaviour when assigning VPP apps to devices or users. This can be overridden on an individual app from the App Portal Tab also.

8.12.2. Associating Users

When a user enrols in Silverback and VPP App Licensing is enabled, and they are assigned an application, they will be added to your VPP account with Apple. The user's devices are also sent a command, telling the device to prompt the user for association

with your account. The user must accept an agreement prompt, and log in with their iTunes account. Note that the iTunes account does not necessarily need to match their Silverback username. After the user associates their iTunes account, they can be assigned applications from your VPP program. If using Device Based assignment. The device will automatically be associated when a license is assigned.

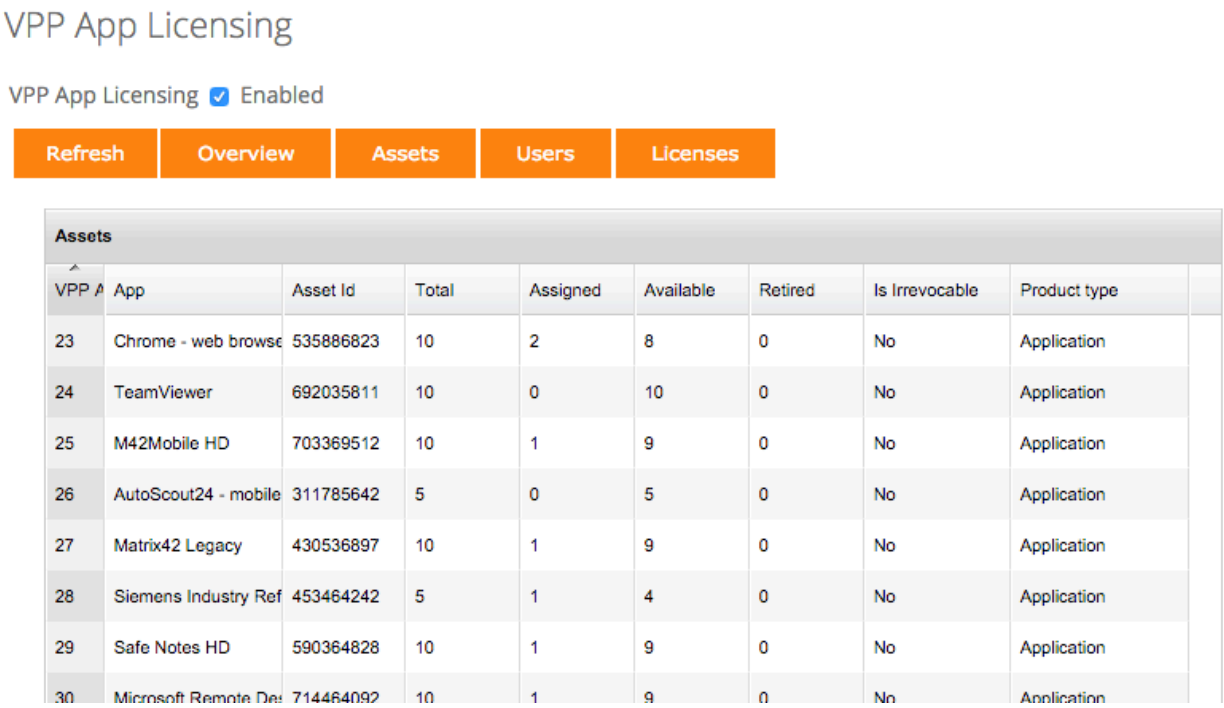
It's important to note that users are associated by their iTunes account. This means that if the user has multiple devices enrolled. Those devices will also get access to the VPP Applications assigned. Also, the user elects which iTunes account to sign in with. It is important to communicate this to users if you require specific accounts to be used.

8.12.3. Associating Licenses

VPP Applications are automatically added to the App Portal tab when Silverback retrieves this information from Apple. Administrators can then assign these applications to Tags. Any user that exists in a Tag with a VPP Application assigned is eligible for that application. If the user is associated to your VPP Program, then they will have access to that application. Users that are in Tags with VPP Applications assigned but have not associated their iTunes account will not have access to the application. If Device based assignment is being used. The licenses will automatically be assigned to the devices.

8.12.4. Assets Section

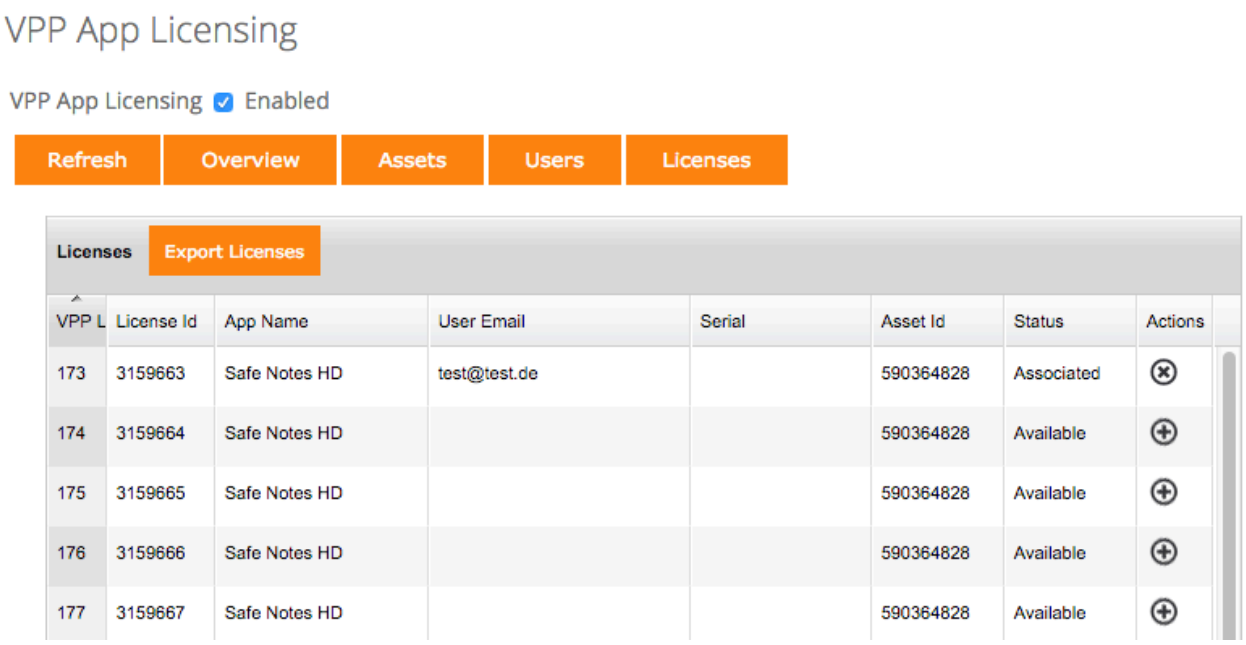
The assets section gives you a list of all applications in the system (essentially grouped licenses by App).



VPP A	App	Asset Id	Total	Assigned	Available	Retired	Is Irrevocable	Product type
23	Chrome - web browse	535886823	10	2	8	0	No	Application
24	TeamViewer	692035811	10	0	10	0	No	Application
25	M42Mobile HD	703369512	10	1	9	0	No	Application
26	AutoScout24 - mobile	311785642	5	0	5	0	No	Application
27	Matrix42 Legacy	430536897	10	1	9	0	No	Application
28	Siemens Industry Ref	453464242	5	1	4	0	No	Application
29	Safe Notes HD	590364828	10	1	9	0	No	Application
30	Microsoft Remote De	714464092	10	1	9	0	No	Application

8.12.5. Licenses Section

The licensing section allows you to view the users, devices and licenses associated with your account. The main view is a table which shows you the licenses in your account, and the information associated with it. You can also export a list of licenses, and manually assign and un-assign licenses from users.

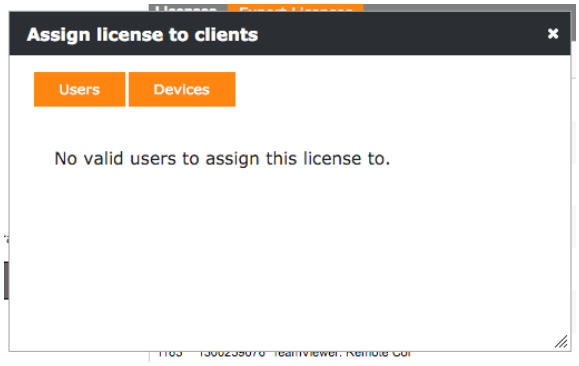


Item	Description
Export Licenses	Exports all licenses in your VPP Account in a CSV format
Licese ID	The apply license id for this license
App Name	The iTunes store name for the app
User Email	The email of the user who owns the license, if associated.
Serial	The serial of the device, if available.
Status	The status of this license in your system. **Available** – The license is not in use by any user, and is available to be assigned **Associated** – The license is assigned to a user.
Asset ID	The asset ID number for the app the license is from.

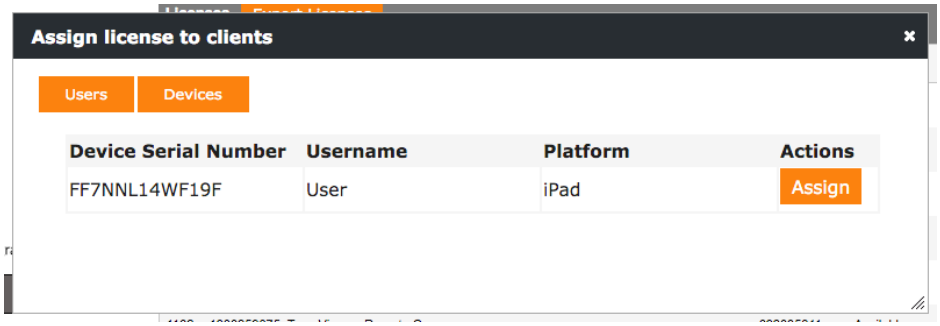
Item	Description
Actions	Lets you manually assign or un-assign a licence. When clicking assign, only valid users and devices will be selectable from the list.

8.12.5.1. Manually Assigning Licenses

When you click the icon in the action column on a license that is assigned, the license will be removed from the user or device. If the action button is to Assign, you will be given a pop-up to assign the license. By default, you will see the valid users that this can be assigned (if available) to and choose one:

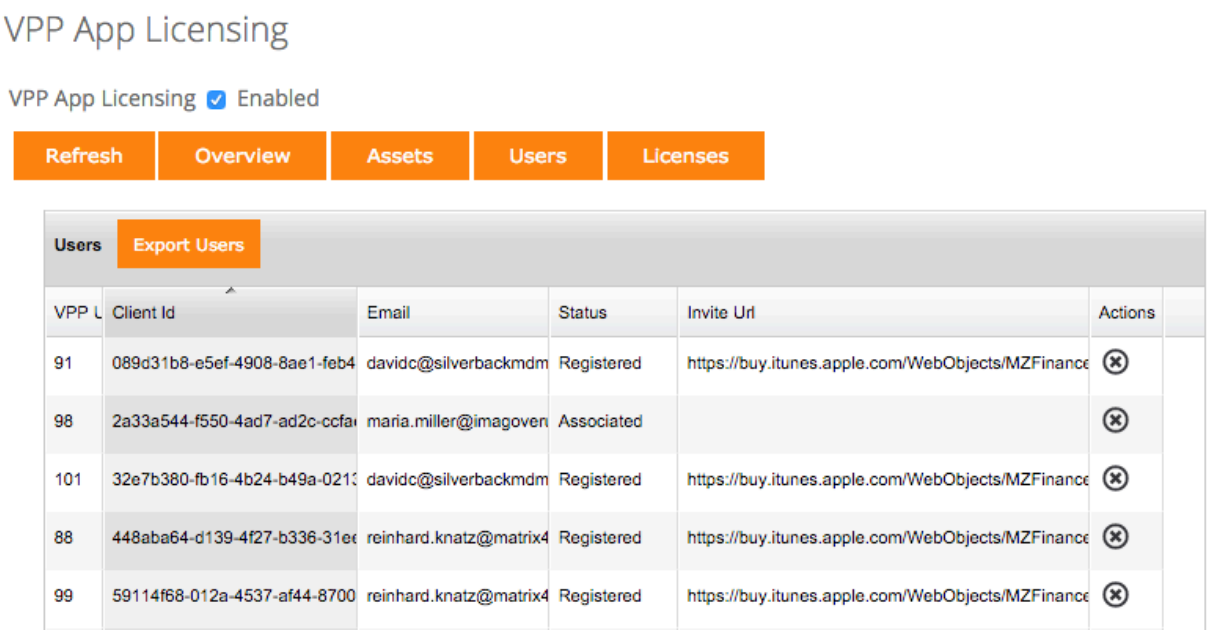


When you click Devices, you will see valid devices this license can be assigned to.



8.12.6. Users Section

Display all the users in your VPP account and their status.



Item	Description
Export Users	Allows you to export the list of users in the system.
Client ID	The unique identifier for the user in your VPP account
Email	The email address of the user entry in your account
Status	The status of this user in your system: **Registered** – The user has been added to your account, but the user has not yet associated their iTunes account. Registered users will not receive VPP App Licenses **Associated** – The user has been added to your account and also associated their iTunes account. Associated users are eligible to receive VPP Applications
Invite URL	If the user isn't associated, you can see the invite URL here. Users should be invited automatically, but you can also distribute this URL to the user to let them enrol in the system.
Actions	Retire user. This will remove the user from the VPP account and release all licenses. This is not permanent, the user can be re-invited to your system at a later date.

8.12.7. VPP Users Export

The CSV export for users contains the following fields:

Item	Description
VPP User ID	Silverback's ID for the user
Client ID	The unique ID of the user in Apple's VPP system.
Email	The email address of the user entry in your account
Status	The status of this user in your system: **Registered** – The user has been added to your account, but the user has not yet associated their iTunes account. Registered users will not receive VPP App Licenses **Associated** – The user has been added to your account and also associated their iTunes account. Associated users are eligible to receive VPP Applications

8.12.8. VPP Licenses Export

The CSV export for licenses contains the following fields:

Item	Description
License ID	Apple's unique ID for the license
Adam ID	Apple's ID for the Application
App Name	The name of the Application as it appears in iTunes
Status	The status of this license in your system. **Available** – The license is not in use by any user, and is available to be assigned **Associated** – The license is assigned to a user.
User Email	The email of the user, if associated
Serial	The serial for the device, if associated.

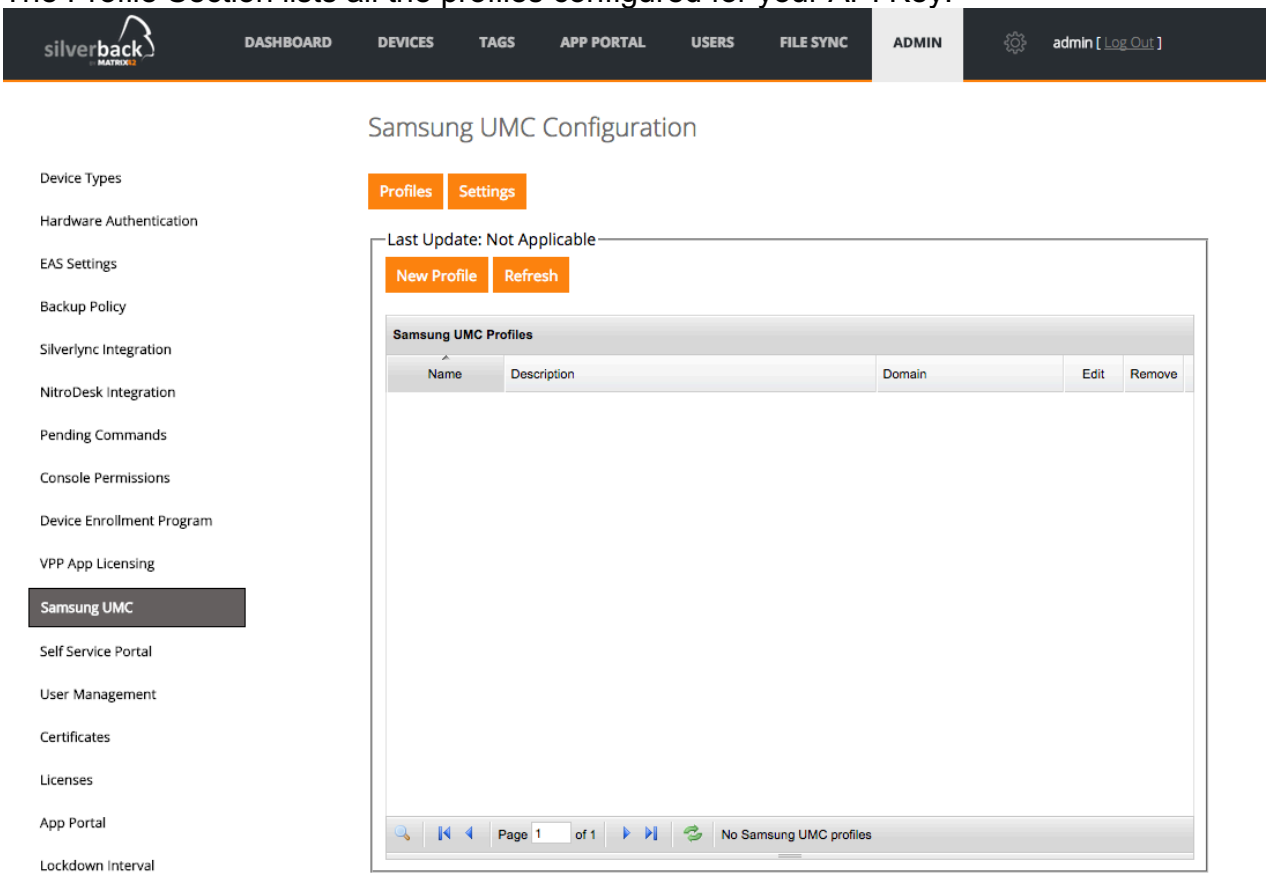
8.13. Samsung UMC

Samsung Universal MDM Client allows users to enroll in Silverback without needing to first download an Agent application. This functions similarly to Apple's Device Enrollment Program. Users enrolling will be redirected to automatically use UMC if enabled for a much more streamlined enrollment process.

Samsung UMC is managed by two sections in the tab; Profiles, which lets you configure profiles for your devices and Settings, which lets you define your API Key and other core settings.

8.13.1. Profile Section

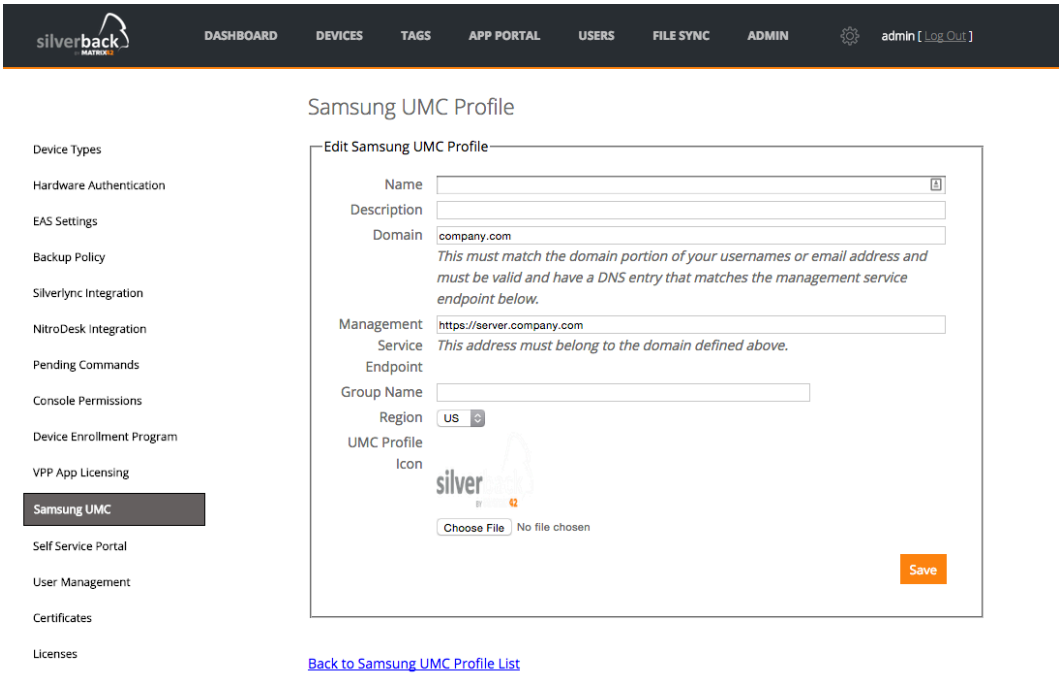
The Profile Section lists all the profiles configured for your API Key.



Control	Description
New Profile	Add a new Profile
Refresh	Fetch the latest data from Samsung
Edit	Edit an existing profile
Remove	Remove an existing profile

8.13.2. Edit or Add a Profile

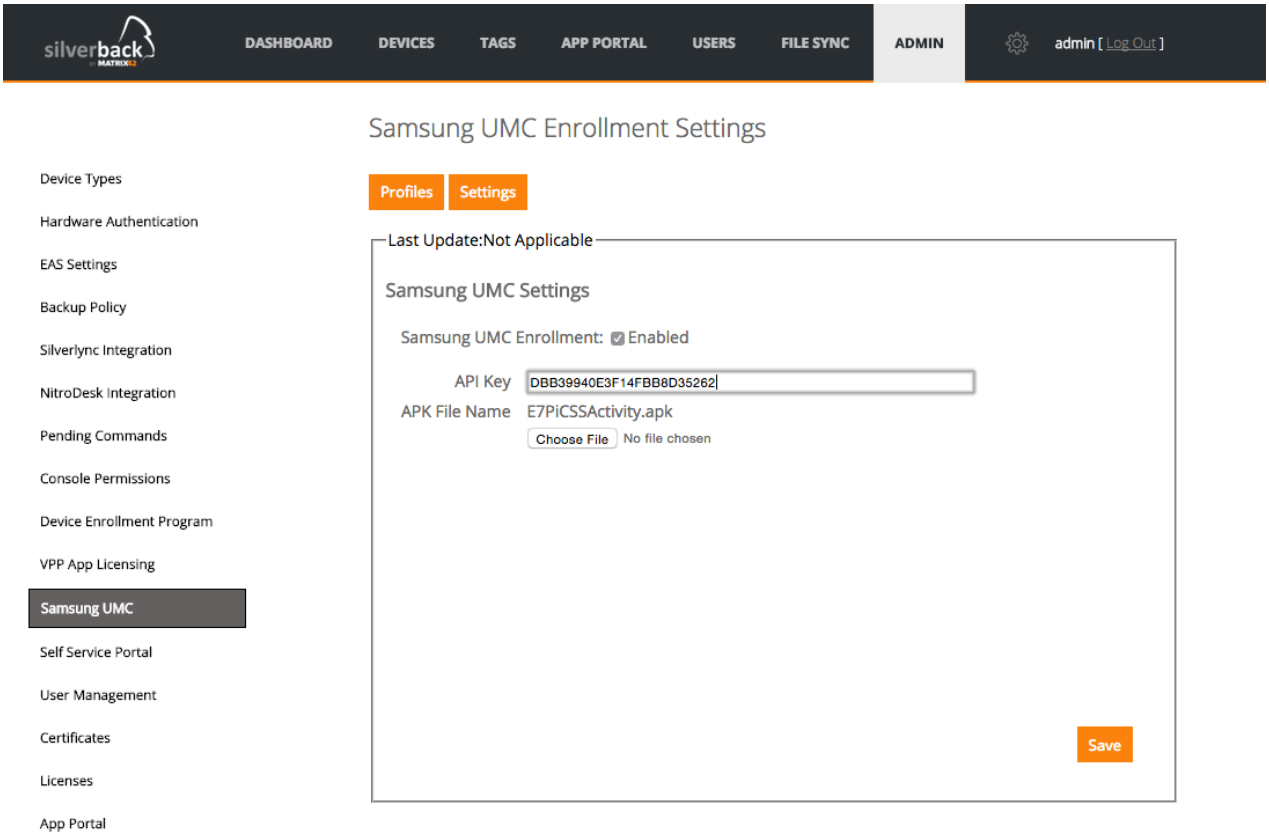
When editing or adding a new profile, the same screen is shown where settings are defined for the devices:



Control	Description
Name	The Name of the profile
Description	A description explaining the purpose of the profile
Domain	The domain. This must match what the user enters as their email address when enrolling. Usernames that match this domain will use this profile
Management Server	Server address for the devices to connect. Note: This **must** match the Domain. If you are configuring multiple domains, then multiple DNS, SSL Certificates and redirections must be configured.
Group Name	A name for a group that users with this profile will fall in to. This is mainly useful if you have two types of users enrolling in the same server. If you were to configure two profiles with the same server, but different groups (e.g. Sales, Exec), the users would be prompted on enrollment to choose a group.
Region	The region where the users are expected to be. This is not critical, as the profiles are replicated to all regions.
UMC Profile Icon	This will be shown to the user on the device when the UMC client is configured.

8.13.3. Settings Section

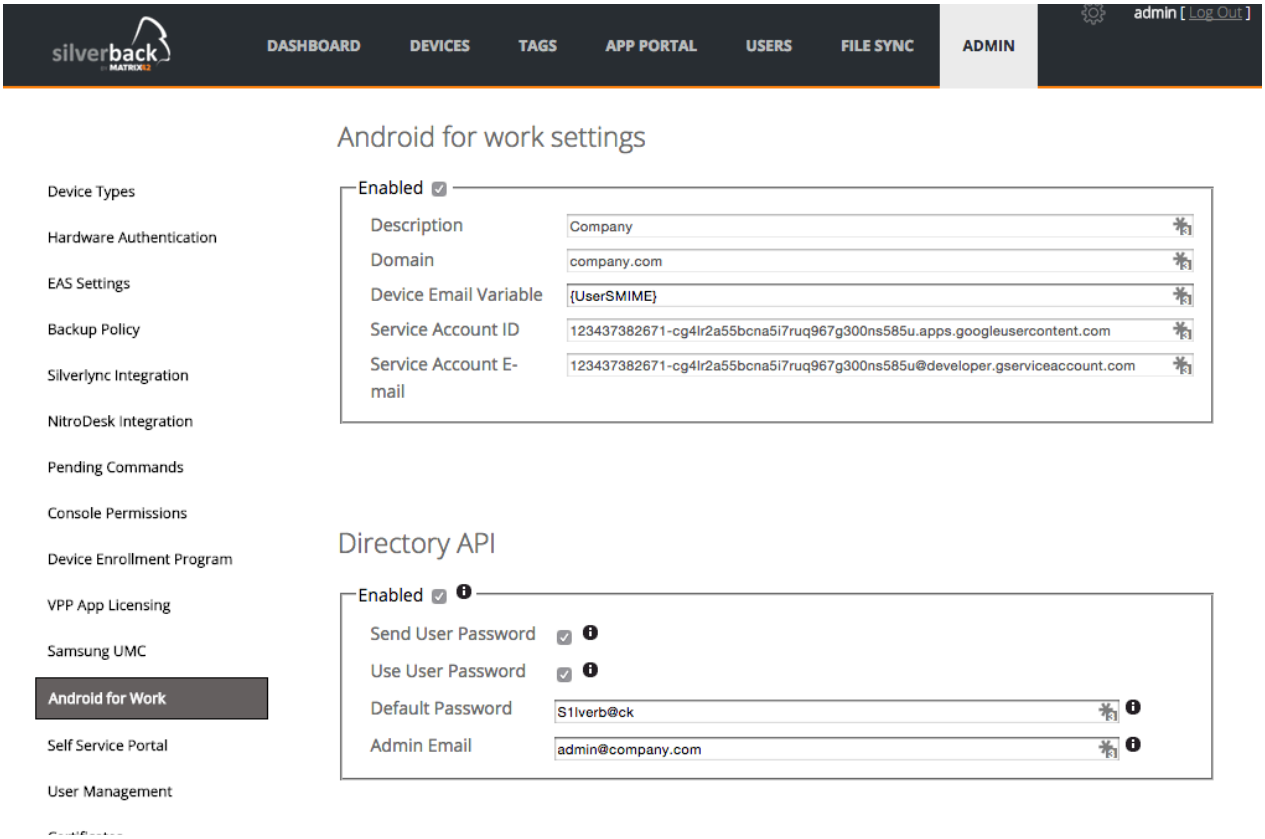
The Settings section is where you define the core components for UMC to work. This includes the Samsung API Key, which is provided by Samsung, and the UMC Silverback client that is provided by Silverback.



Control	Description
API Key	Samsung UMC API Key, provided to you by Samsung
AOK File	UMC Specific Silverback client for UMC Enrollments, provided by Silverback

8.14. Android for Work

Android for Work settings are enabled by first pairing the server with a Google Management domain. The pairing process if covered in the document Silverback by Matrix42 Android for Work Enablement. When the server is paired, the following settings can be configured.



For basic Android for Work enablement:

Control	Description
Description	The description of the pairing configured
Domain	The domain name of the Managed Google domain. This must match the domain extension of the users to be managed by Silverback.
Device Email Variable	The variable that will be used for creating users. This can be any Silverback System Variable but must match the value that is expected when Silverback automatically creates users for Android for Work enrolment.
Server Account ID	The client ID of the service account created for managing Silverback users in Android for Work
Server Account E-mail	The email name of the service account created for managing Silverback users in Android for Work

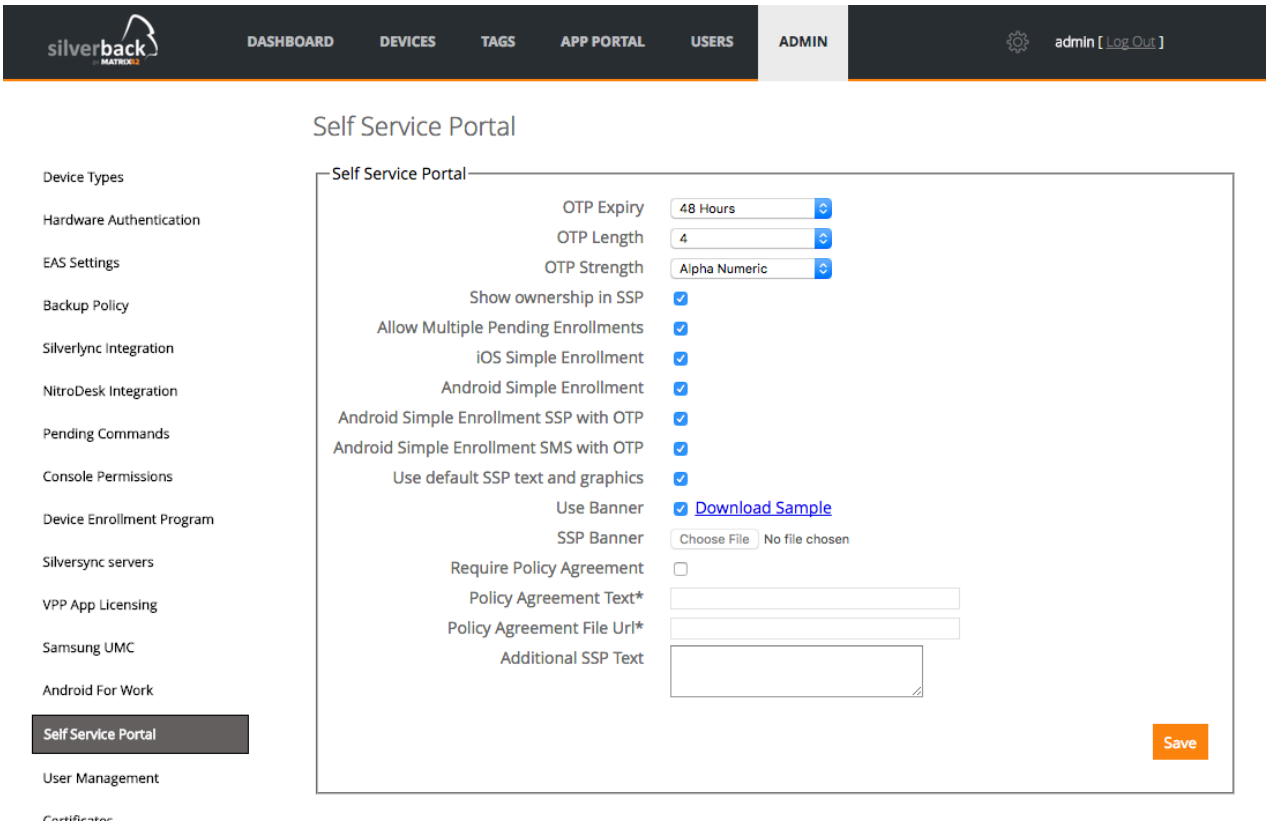
For Directory API Integration, enabled separately as part of the Android for Work enablement, the following settings should be configured. This is only required if you want Silverback to create and manage users automatically for your server:

Control	Description
Send User Password	Determines if Silverback should pre-assign passwords for users when they created. If this is not set, then users must determine their own passwords.
Use User Password	Determines if Silverback should send the password value from the Enrolment Creation to Google. This means the user password will be the same value that the user entered when creating the enrolment.
Default Password	The value that will be sent (if configured to do so) to create the user's account. This will be the Google account password for the user if no other value is available.
Admin Email	This is mandatory if the Directory API feature is being used. This must be the email address of a user that has administrative permissions on the Google Managed Domain. Silverback will impersonate this email when creating and managing users.

If you make changes and don't want these to be saved, simply navigate away from the page without clicking Save, or press the revert changes button:

8.15. Self-Service Portal

End users interface with Silverback through the Self-service portal. The self-service portal can be customized to provide a recognizable look and feel for end users.



With the Require Policy Agreement setting enabled the user must agree to a Corporate Policy before they are able to begin the enrolment process.

Enabling this policy will change the layout of the Self Service Portal to include an ‘Agreement Checkbox’ with an additional, customizable text that is displayed under the Self Service Portal Window.

Control	Description
OTP Expiry	How long each OTP will last before it expires.
OTP Length	The Length of the OTP that is generated for the user.
OTP Strength	The Complexity of the OTP that is generated for the user.
Show Ownership in SSP	Allow the user to specify the ownership of their device at 192nrol192ent.
Allow Multiple Pending Enrollments	Allow the user to 192nrol several iOS devices with the same username at the same time
iOS Simple Enrollment	Determines if iOS Simple Enrollment is enabled or not.
Android Simple Enrollment	Determines if Android Simple Enrollment is enabled or not.
Android Simple Enrolment SSP with OTP	Allow android users to skip entering username and OTP on the device if they are enrolling directly through the Self Service Portal
Android Simple Enrolment SMS with OTP	Allow android users to skip entering username and OTP on the device if they receive the enrolment SMS
Use Default SSP Text and Graphics	Use the default Silverback Logo and Text for the Self-Service Portal.
Use Banner	Modifies the SSP to display a Banner Image instead of Logo/Text.
Header Text	The header text is the title text at the top of the Self-service Portal screen.
Logo	Upload a custom SSP Logo
Require Policy Agreement	Enables the 'Require Policy Agreement' setting for Silverback
Policy Agreement Text	The name of the policy as listed on the Self Service Portal
Policy Agreement File URL	The URL Location where the Policy can be read
Additional SSP Text	Additional Text displayed under the SSP Window.

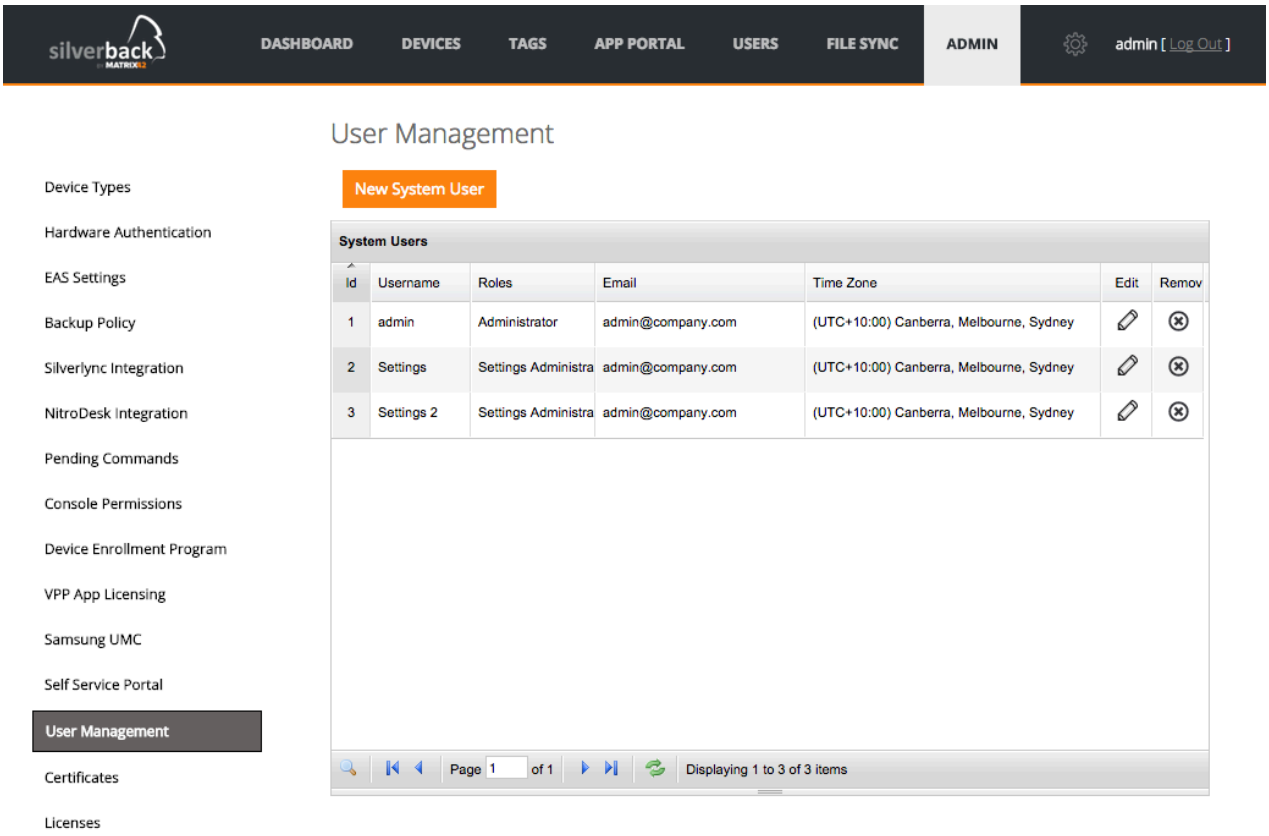
8.16. User Management

The User Management section is where an Administrator can create additional users with one of the following user roles:

- Administrator
- Content Manager
- Settings Administrator
- Helpdesk
- Super Helpdesk
- Reporting
- App Manager
- File Sync Manager

The different access levels are explained in the Silverback Role Based Access Levels section.

Silverback by Matrix42 Admin Guide Version 5.1 U3

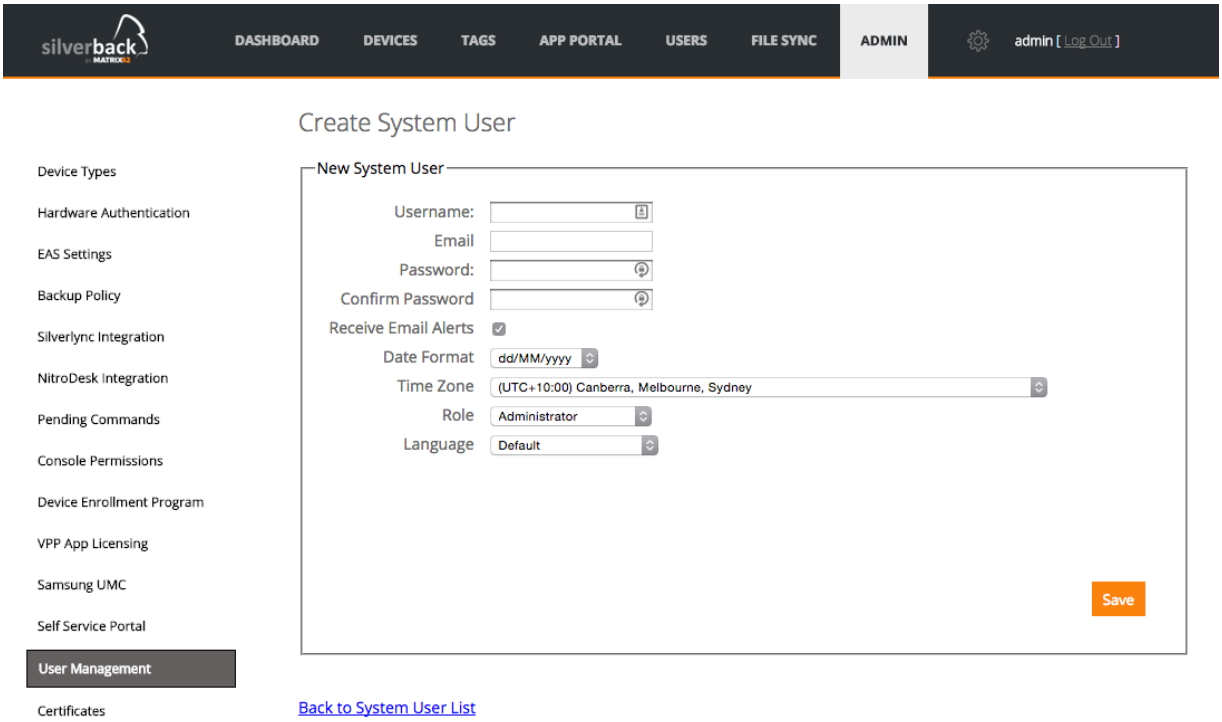


Configuration	Description
Add	Create a new administrator or helpdesk user by clicking on the 'New System User' button
Edit	Edit the details of the selected user
Delete User	Delete the user account from the system.

NOTE: The 'Admin' account within the Silverback Management Console is a SYSTEM user that cannot be deleted. It is used by Silverback Engineers for troubleshooting issues with your Silverback Installation should the need arise. If you feel uncomfortable with this, simply change the account password using the additional account that you have been supplied with.

8.16.1. Adding a New System User

Clicking on the 'New System User' button will display the screen below. From here the administrator is able to create other users to manage the Silverback environment. These users can consist of Administrators, Super Helpdesk, Helpdesk, Reporting or App Manager Users.



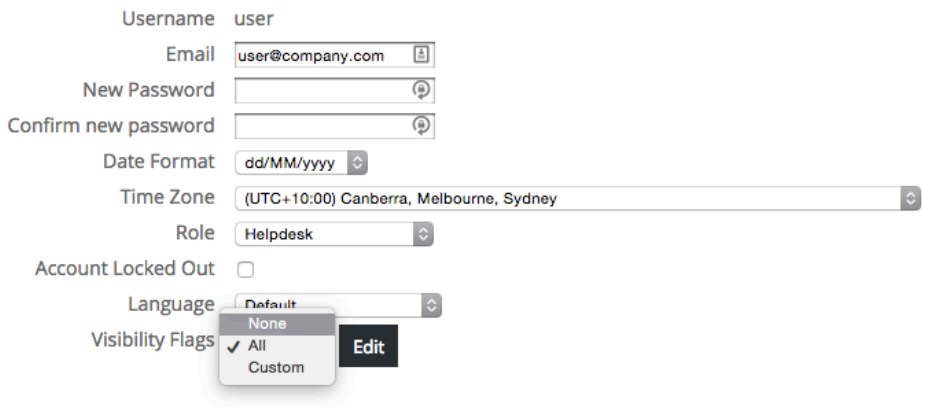
NOTE: When creating a new System User, it is important to ensure you correctly select their Local Time Zone, as this will adjust the date/time for all events caused by this user, ensuring that all Silverback Logs, Administrative Email Alerts, and User Actions will all display the local time for the user viewing them.

Configuration	Description
Username	The username of the new user to be created.
Email	A Valid Email address for the user.
Password	A Password for the user.
Confirm Password	To Ensure the password is set correctly.
Receive Email Alerts	Enables Administrative Alerts for this user.
Date Format	Change the Date/Time format depending on your region.
Time Zone	The Time Zone the user is located in.
Role	Sets the Level of access for the user.
Visibility Flags	Configures the devices that this user is allowed to see in

Configuration	Description
	the console
Language	Sets the default language that will be displayed when this user logs in. If Default is selected, Silverback will attempt to use the browser's language setting.
Create API Token	Allows you to create API tokens for the user. Note that this is only available for users of the Administrator role.
Active API Tokens	Lists the current API Tokens for this user, their permissions scope, and also allows deleting of tokens.

8.16.2. Using Visibility Flags

It's possible with Silverback to configure devices so that console users can or cannot see them. At a high level, this is achieved by assigning a Visibility Flag to a device. A Visibility Flag is simply a piece of text. You then configure console user accounts to either see, or not see these flags.



From the Edit or New User screen, the Visibility Flags have the following top-level options:

- **None**
  The console user will see **no** devices
- **All**
  The console user will see **all** devices
- **Custom**
  The console user will see the Visibility Flags selected in the "Edit" popup:

8.16.2.1. Custom Visibility Flag Options

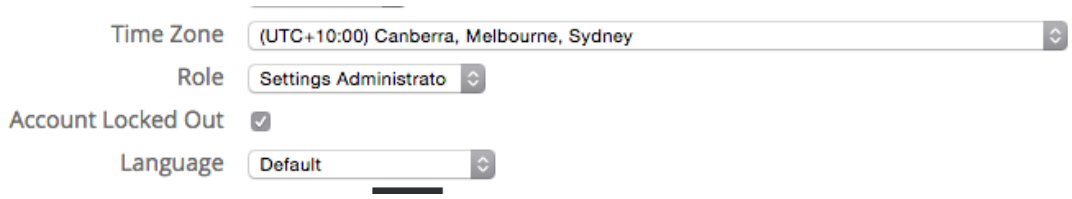
From the Custom Flags popup, you can define the individual flags the console user should see. The only option that is **always** present here is "No Flag Assigned", this is the default value for a device (no visibility flag defined). All other items in this list come directly from the flags that are assigned to your devices.

8.16.3. Unlocking an 'Locked' Silverback Management Account

Silverback will automatically lock out any Management Account if the password has been incorrectly entered a specified number of times. By Default this is set to 10.

Once a user's account has been 'Locked Out' due to incorrect password attempts, you will need to follow the steps below to unlock it:

- Log into the Silverback Management Console with another user.
- Visit the User Management Section (Under the Admin Tab in Silverback).
- Click **Edit** next to the Locked Out account – you should see a screenshot similar to below:



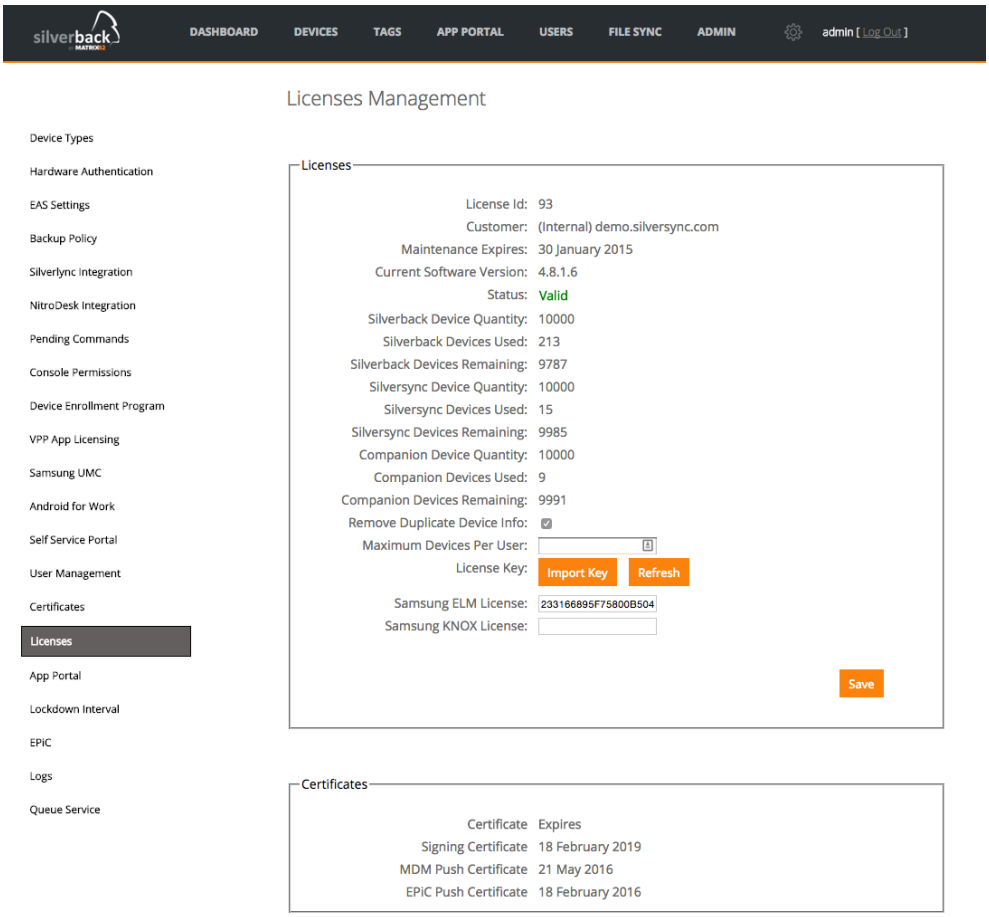
Make sure the **Account Locked Out** checkbox is UNCHECKED and click Save.

8.16.4. API Tokens

Currently API Tokens are use internally only. In the next release, the API will be documented for customers to use in third party applications.

8.17. Licenses

As well as displaying the current Silverback Device Count and License summary, you can also set a limit on how many devices a user is able to enrol, and also check on the Certificate Expiry Dates for all key Silverback Certificates.



8.17.1. License Information

The Silverback License information is important as it will not only tell you how many devices are enrolled into Silverback, it can also tell you how many Silversync licenses have been consumed and when you're Maintenance Period Expires.

The Maintenance Period is the period of time in which you are able to receive Silverback Upgrades. Once this has expired, you will need to renew your Support Contract to regain access to the latest Silverback Upgrades.

8.17.2. Remove Duplicate Devices

Remove Duplicate devices will attempt to detect if a device enrolling already exists, and remove it. This is because some devices do not provide a unique identifier, if this setting

is enable, Silverback will attempt to match existing data, such as IMEI number, Serial number and remove the previous entry if it detects one.

8.17.3. Limit Devices Per User

Within this screen you can also set a limit on the number of devices an individual user can enroll into Silverback, allowing for more control over the Silverback License Count. If the user has too many devices enrolled they will be met with a warning on the Self Service Portal when trying to create a new Pending Enrollment.

8.17.4. Samsung Licenses

Samsung KNOX and ELM Licensing is also configured via this page in the appropriate text boxes.

8.17.5. Certificates

Finally, the Certificates section on this page will display the expiration dates of the SSL Certificate that Silverback is using. This is important to note as when these certificates expire so they can be renewed **ahead of time**. In some cases when a certificate expires devices will no longer be able to communicate with Silverback.

NOTE: Administrators should receive an email notification warning them if/when an SSL Certificate is due to expire.

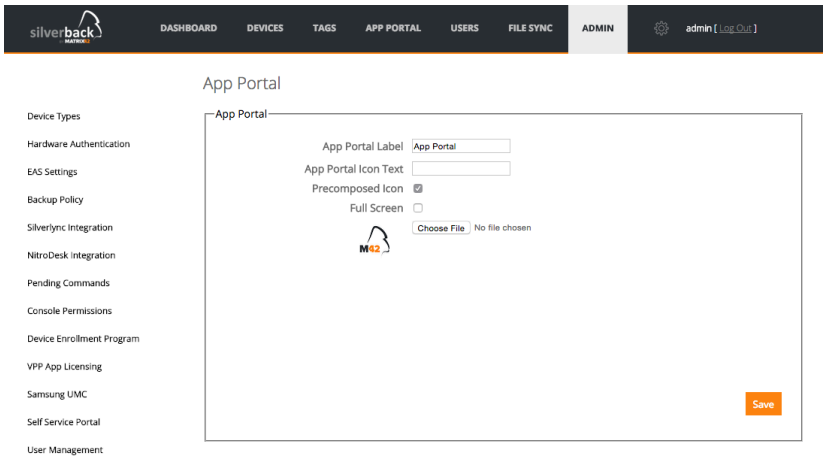
8.18. App Portal

The Application portal is where devices can access Enterprise applications and recommended Third Party applications via a web clip icon.

Customization of the App Portal, when done in this location, will replicate system wide for all Device Types with the App Portal enabled. For it to work properly the icon must meet the following specifications:

Dimensions: 59x60 pixels

Format: PNG



Configuration	Description
App Portal Label	Customize the Header Text within the Silverback App Portal
App Portal Icon Text	Customize the text associated with the App Portal
Precomposed Icon (iOS Only)	Adds the gloss effect to the icon when displaying on the device.
Full Screen	Makes the App Portal appear Full Screen in Safari
Browse/Choose File	Customize the App Portal Icon

NOTE: Changing the icon here will change it for all devices system wide.

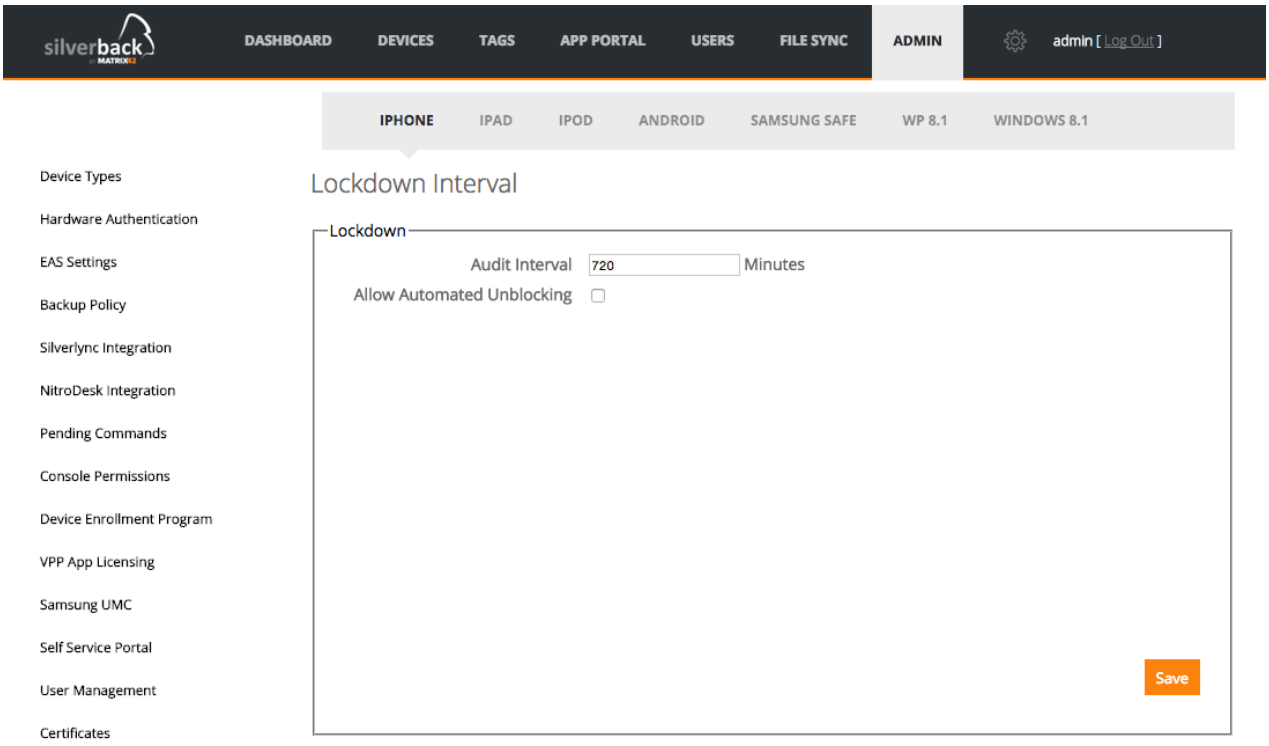
8.19. Lockdown Interval

The Lockdown Interval setting will determines how often Silverback asks each device that is enrolled to 'Check in' to ensure it is still complying with corporate policy.

Silverback will automatically 'stagger' these calls out, so that not all devices are asked to check in at the same time, so keep this in mind if you are seeing some delay between different devices.

Also, if the device is unable to connect to the Internet, or communicate with APNS (Apple's Push Notification Service) then it will not be able to check in – but should do so as soon as it is introduced to a connection where these services are available.

The final thing to take into consideration is that the Check In messages sent using APNS may have an impact on device battery and data consumption so it is important to set these to sometime sensible.



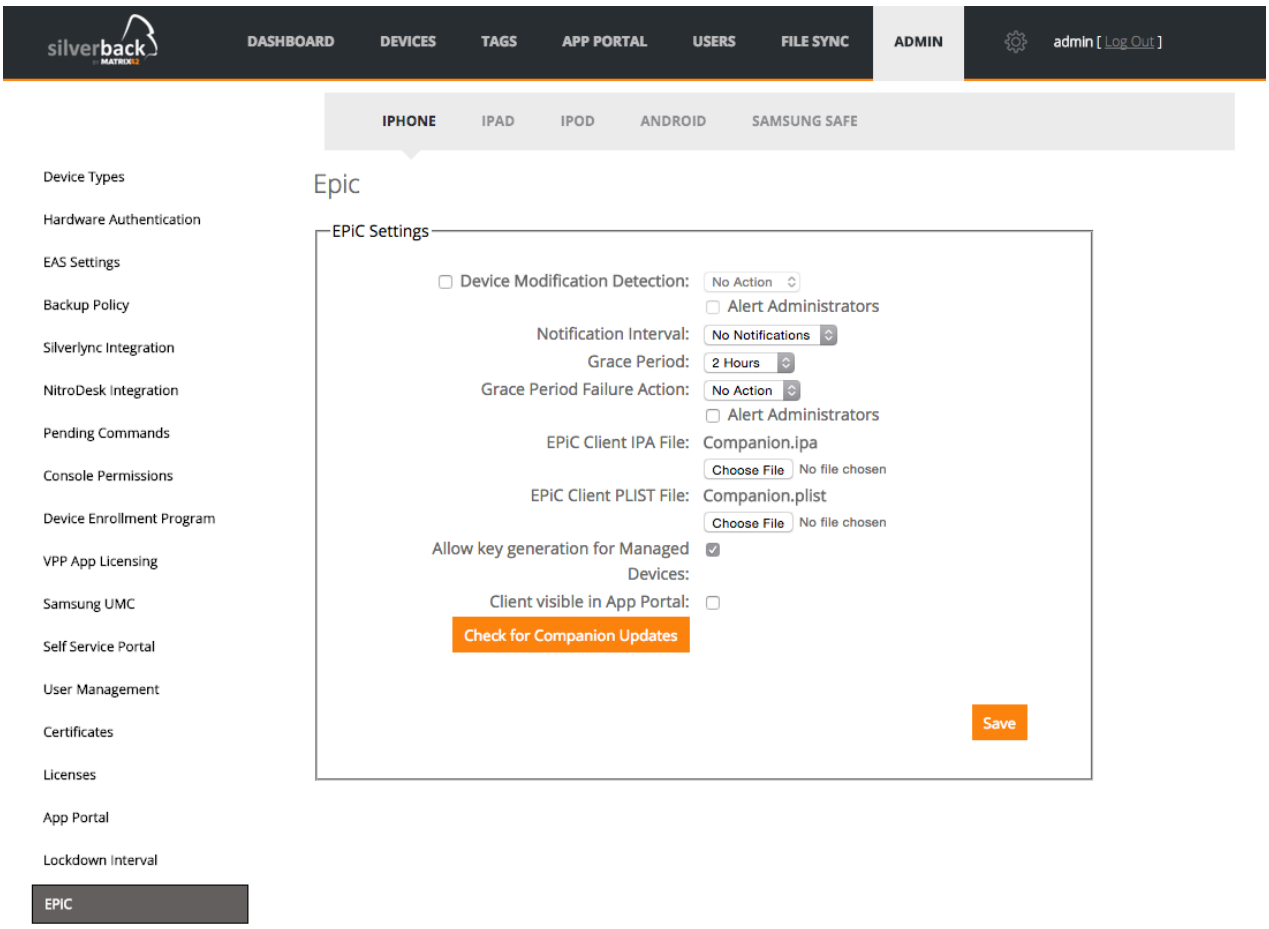
"Allow Automated Unblocking", Allows the system to automatically unblock a device if it no longer violates policy. By default, unblocking requires Admin intervention. By configuring this, if the device checks in and the system detects that a blocking policy is no longer violated, the user will be unblocked automatically, with one exception; admin initiated blocked. These still require the Administrator to manually unblock the device.

8.20. EPiC

Silverback's advanced End Point Intelligent Control (EPiC™) lets you enforce granular access control rules for iOS end point environments. EPiC conducts robust pre-authentication interrogation of remote end point devices to identify the device, as well as determining the ongoing integrity of the device leveraging pre-defined end point criteria.

Silverback 3.7 and above are integrated with a multi-purpose Companion app that contains EPiC as a module. If you have licensed Companion, the controls on this page allow you to configure EPiC module of Companion.

The Settings and Policies that are applied on this screen are set System Wide. This means that any devices assigned to a Tag with Secure Enrollment Enabled must comply with these settings as well.



Action	Description
Device Modification Detection	Enables Device Modification Detection (Jailbreak Detection)
Modification Detection Action	Action to be performed if device modification has been detected
Notification interval (iOS Only)	How often the end user will receive a notice to launch EPiC
Grace Period (iOS Only)	The maximum allowable time a device has to perform an integrity check
Grace Period Failure Action (iOS Only)	Action to be performed if grace period is exceeded
EPiC Client IPA File (iOS Only)	The IPA file or build file of the EPiC or Companion application
EPiC Client PLIST File (iOS Only)	The PLIST file associated with the EPiC or Companion IPA file

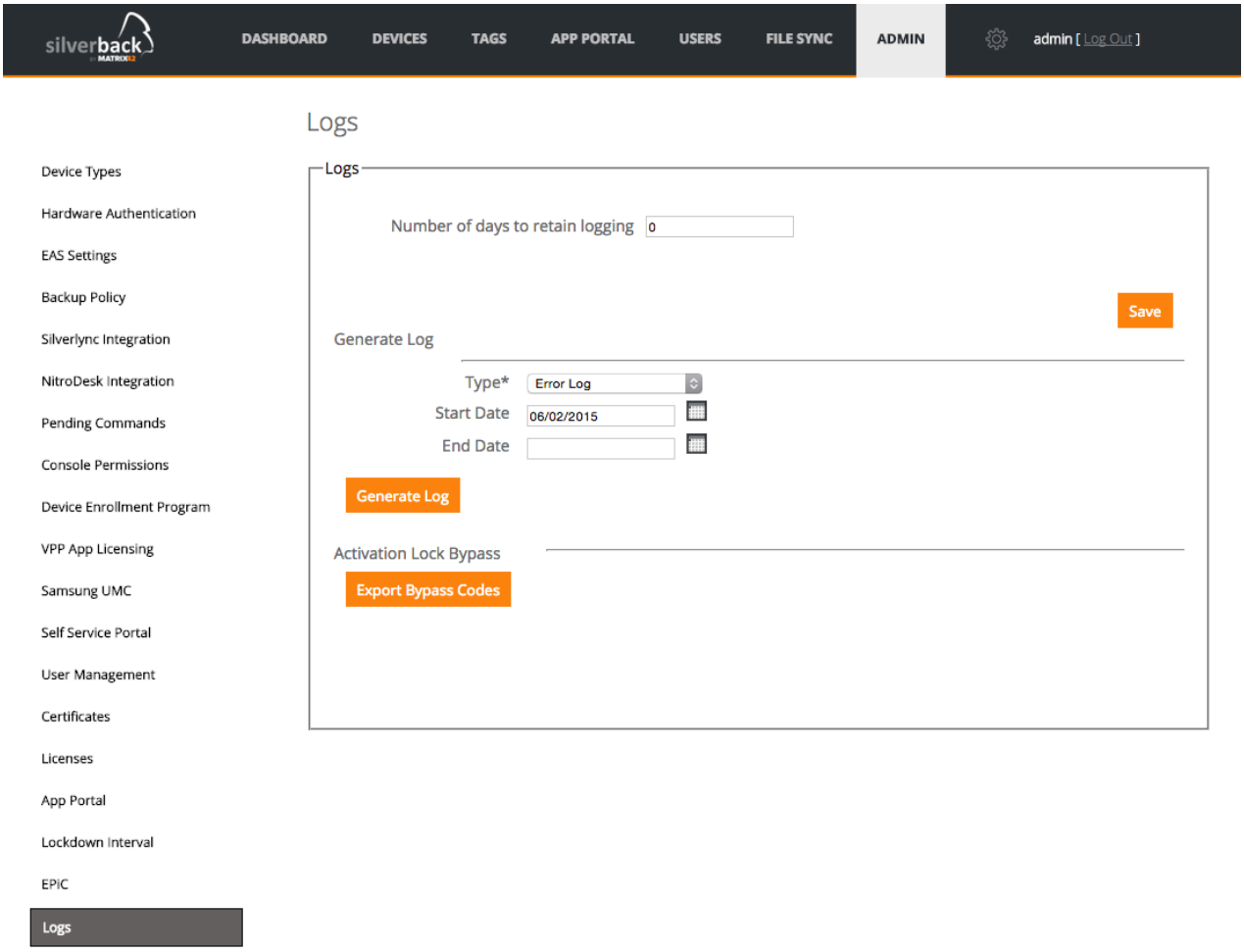
If any of your users decline to install EPiC or Companion during enrollment, the install command can be reissued to the device from the device properties pop up in the 'Blocked' container on the 'Devices' tab.

If you intend to use the Companion App Store version, you do not need to provide the EPiC IPA and PLIST file

8.21. Logs

Administrators have the ability to export the error log from Silverback, containing any error messages generated by Silverback. Administrators can filter the results based on date, using the 'Start Date' and 'End Date' parameters. Simply select the date range and the log generated will return the errors that occurred within that date range.

Administrators can also export an Action Audit log using the same parameters. The Action Audit details actions performed by Administrators and Help Desk users on devices. The Action Audit records when Management Console users log in and out and also when they perform actions on the devices.



Action	Description
Number of days to retain logging	The number of days Silverback should keep logging information.
Save	Save's the number of days to retain logging
Type	The type of log to export (Error Log or Audit Log)
Start Date	Specifies the Start Date of the Exported Log
End Date	Specifies the End Date of the Exported Log
Generate Log	Generates the log files in CSV format

8.21.1. Activation Lock Bypass

For devices running iOS 7.1 or higher, it's possible to override devices that have had Activation Lock enabled on them. For the bypass to work, three conditions must be met:

The device must be running iOS 7.1 or above

The device must be supervised

"Allow Activation Lock" must be enabled in restrictions for that device.

When the device enrols, Silverback will request a bypass code from the device, whether the user has enabled Activation Lock or not.

To bypass the Activation Lock, click **Export Bypass Codes** from the Logs page. A CSV file will be downloaded containing all of the bypass codes that Silverback has collected. Due to the fact that a device may have been deleted from Silverback, this CSV file shows codes for all devices, not just current devices.

Locate the device by using either the UDID, Last MDM Username or IMEI Number, and then note down the Activation Lock Bypass Code.

A	B	C	D	E
Device UDID	Last MDM User Name	Serial Number	IMEI Number	Activation Lock Bypass Code
1234dea9594a9	user@companyname.c	DLX1111111M	99 0000000000 2	1234-ABCD-5678-EFGH-9012-IJKL

On the device, when prompted for the previous user's iTunes account information, leave the Username field empty, and enter the bypass code in the password field.

NOTE: Do not include hyphens when typing in the code.

8.21.2. Error Logs

Silverback manages its enrolled devices through a series of commands that are sent and received by these devices over either a Wireless or Cellular connection. If for any reason one of these devices responds with an error, Silverback will log it in this error log for the Administrator to find.

The Error log is generated with the following headers:

Column Header	Description
DeviceID	The Devices unique ID from the Database
Username	The Username associated with the device that generated the error.
LdapFirstNameUserField	The Users First Name as read from LDAP
LdapSurnameUserField	The Users Surname as read from LDAP
MdmCommand	The MDM Command Silverback tried to send
MdmErrorChainId	The Unique Number for this error in Silverback
MdmDeviceCmdId	The Unique Number ID for this error encountered by Silverback
Mdm_ErrorCode	The MDM Error Code as documented by Apple
Mdm_ErrorDomain	The MDM Error Message as documented by Apple
Mdm_USEnglishDescription	The Error Message displayed in English
Mdm_LocalizedDescription	The Error Message displayed in the Local Regional Language (as configured on the device).
CreatedDate	The Date the Error was recorded by Silverback.

8.21.3. Audit Logs

The Audit Logs will help Silverback Administrators keep a track of which user performed which action within the Silverback Management Console.

The Audit Log is generated with the following headers:

Column Header	Description
ID	The Unique Action ID Number
Action Time	The time that the action was performed
ActionUser	The Username of the Silverback Administrator that performed the Action.
ActionAddress	The IP Address of the Computer that the action was performed on.
ActionAction	The Action that the User tried to perform
ActionDestination	The Device the action was performed against OR, the TAG/Setting that was manipulated by the user.

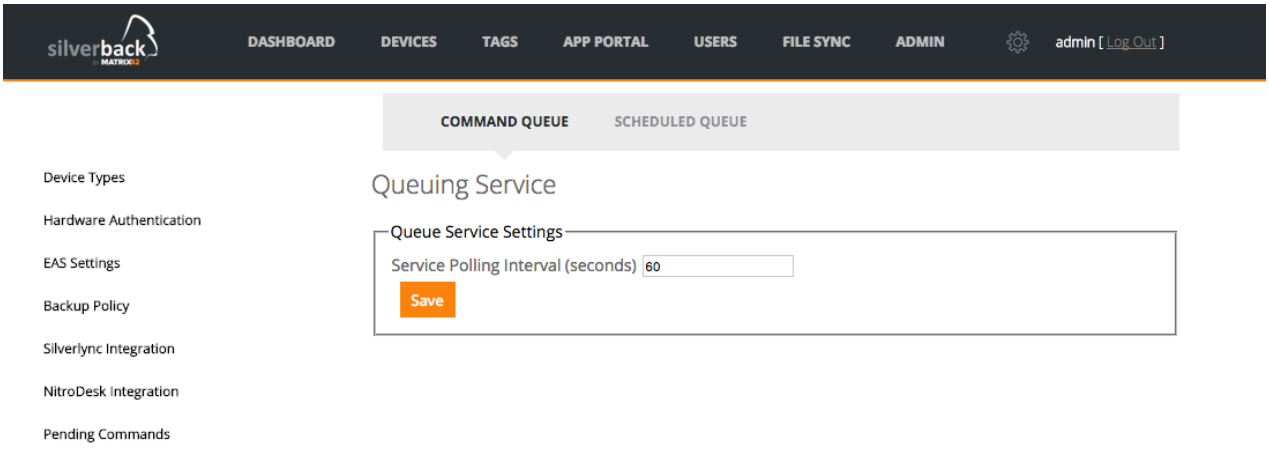
8.22. Queue Service

The queuing service is an underlying service that creates an efficient way for Silverback to manage command execution. Currently this is used by the Apple Device Enrolment program, Samsung UMC and also for handling LDAP information processing.

There are two key components for the Queue Service, the Command Queue and the Schedule Queue.

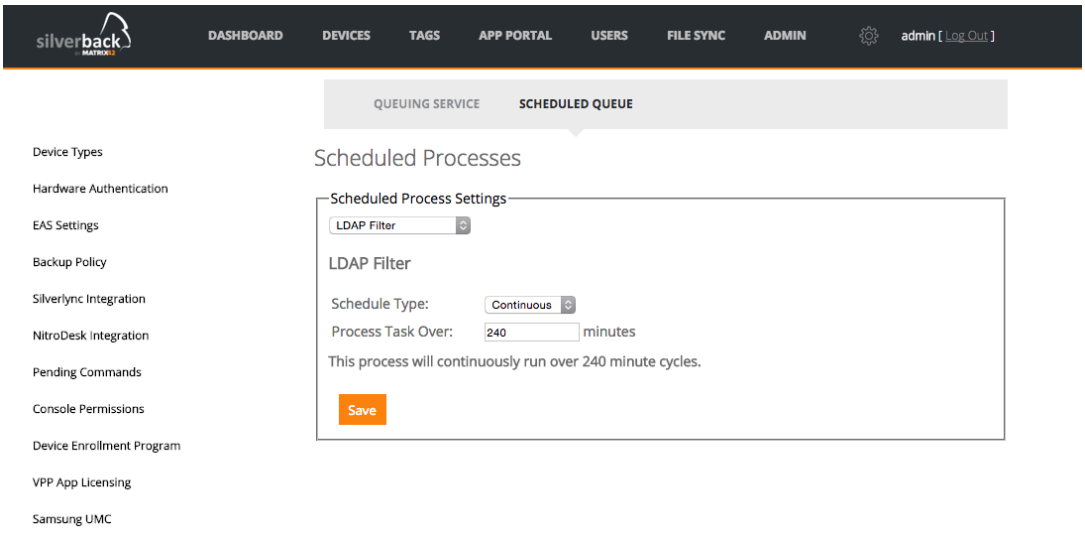
Command Queue is for item that should execute at a device interval and are not typically time sensitive, items are added to a queue and are checked at the defined interval. Schedule Queue is for items that need to be processed regularly and within an expected time frame, such as LDAP information processing.

8.22.1. Command Queue



Control	Description
Service Polling Interval	The time in seconds that the Command Queue should be checked. Currently only Device Enrollment Program, and Samsung UMC Commands are used by this feature. If you do not utilize either of these, then this value can be safely set to a large value.

8.22.2. Scheduled Queue



Control	Description
Process Selector	Determines which items settings you are editing. LDAP Filter is for processing LDAP Filters for Tag population, whereas LDAP Device Update is for fetching LDAP information for current users and devices.
Schedule Type	Either Continuous or Daily. Continuous will process everything within the defined time frame, and then repeat when that time period has expired, continuously. Daily will execute the LDAP requests once daily, and execute over the defined start and end time.
Process Task Over	For the Continuous cycle, this is the time that LDAP requests will be processed within.
Start / End Time	For the Daily cycle. This is the time window that the items should be processed each day.

For the above settings, the choice between Daily and Continuous will depend on how 'live' the LDAP data needs to be and the Time Interval settings will depend on the load. One scenario would be a large amount of LDAP information that takes a long time to process, for this you would ideally select Daily, and specify the time window to be early morning or late night so the server can process this when the server is not too busy.

Another scenario would be the need to have the LDAP data as live as possible. For this you would select continuous, and then adjust the "Process Task Over" time to allow for the amount of data you need to process.

8.23. MDM Settings

MDM Settings contains settings that are specific to MDM for certain platforms. These generally are settings that affect the user experience enrolling In or using MDM on your system.

8.23.1. WP Settings

WP Settings govern what information is shown to users on enrolment from a Windows Phone device.

Control	Description
Support Phone Number	The support phone number shown to users on the device.
Support Website	The support website shown to users on the device.
Support Email Address	The support email address shown to users on the device.

8.23.2. Windows settings

Windows Settings govern what information is shown to users on enrolment from a Windows device.

Control	Description
Support Phone Number	The support phone number shown to users on the device.
Support Website	The support website shown to users on the device.
Support Email Address	The support email address shown to users on the device.

8.23.3. OS X Settings

OS X Settings govern the default passcode for OS X devices when the passcode is reset from the console.

Control	Description
Default PIN for Policy Actions	When the system automatically locks an OS X device, this is the default PIN that will be set. For OS X, it's mandatory that a PIN be provided when locking or wiping the device, and this will be the value that is set.

9. Silverback Appendix

9.1. Internal 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,

System Variable	Description
	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.

9.2. Custom LDAP Attributes

As some of the features configurable in Silverback will require dynamic entries (email username / passwords), we have added a '*Custom LDAP Variables*' section to Silverback that will collect these fields when a user initially enrolls their device.

Currently there are three (3) customizable LDAP Variables that can be configured to look at the Active Directory Schema of a user at the time of enrollment.

{CustLdapVar0} {CustLdapVar1} {CustLdapVar2}

When Silverback is installed it is given some details about your Active Directory infrastructure so that it knows where to look for Users, and what LDAP Attributes to save about the user enrolling. Once these have been populated they can then be used within the Silverback Management Console.

Custom Email Example:

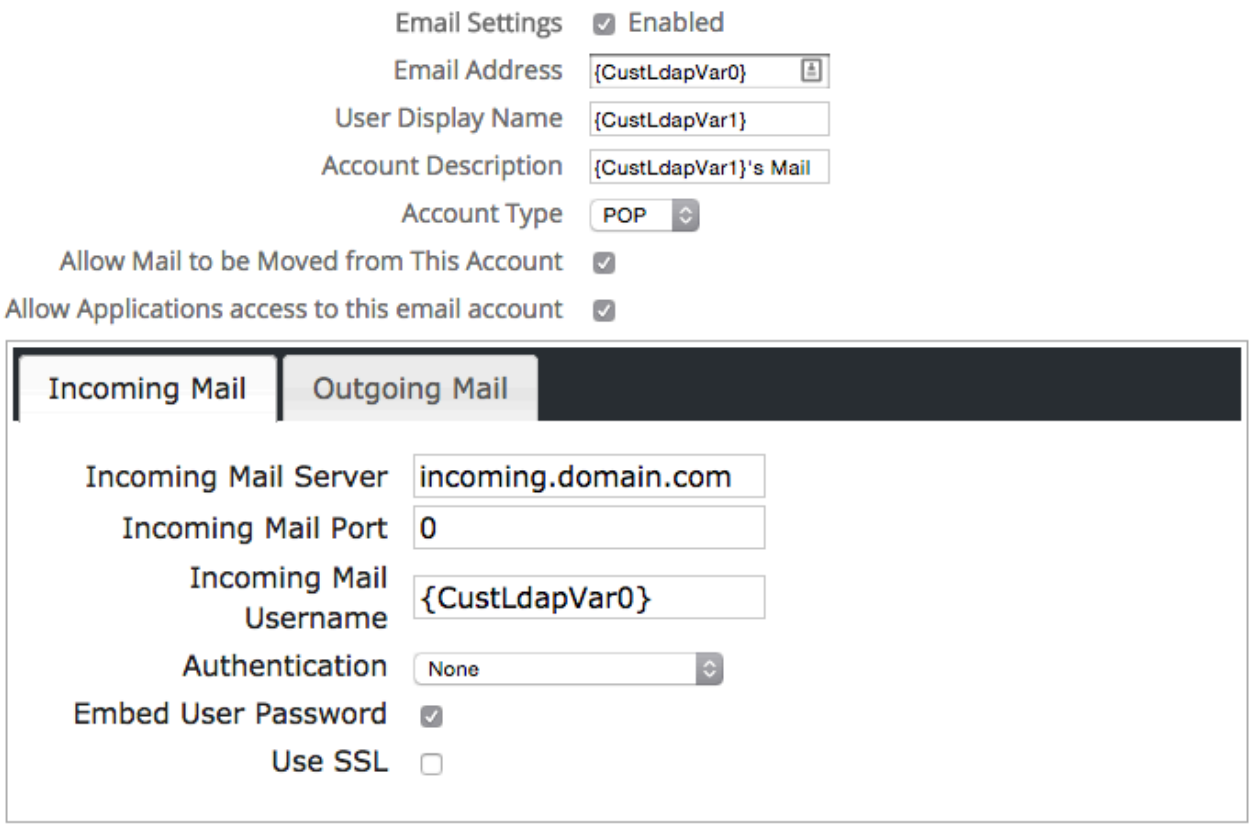
{CustLdapVar0} has been mapped to the LDAP Attribute: extensionAttribute1

{CustLdapVar1} has been mapped to the LDAP Attribute : displayName

{CustLdapVar2} is still not in use.

extensionAttribute1 is the user's custom Email Address (user@outlook.com)

displayName is the user's real world name (John Smith).



9.3. Bulk Import Local User CSV Format

The CSV File that is imported into Silverback to create multiple Local Users must have the following Column Headers:

Column Header	Example Attribute	Description
Username	john.smith@company.com	The Username for the user
FirstName	John	The Users First Name
LastName	Smith	The Users Last Name
Email	john.smith@company.com	The Email Address for the user
Password		The user's password
CertUsername	john.smith@company.com	The Username presented for Certificate Authentication.
EmailUsername	john.smith@company.com	The Username presented for Email Authentication
VPNUsername	john.smith@company.com	The Username presented for VPN Authentication
WifiUsername	john.smith@company.com	The Username presented for WiFi Authentication
SMIMEUsername	john.smith@company.com	The Username presented for S/MIME Email
GlobalProxyUsername	john.smith@company.com	The Username presented for Global HTTP Proxy Authentication
Custom1		A Custom LDAP Attribute
Custom2		A Custom LDAP Attribute
Custom3		A Custom LDAP Attribute

9.4. Status Integration Endpoints

Silverback publishes the availability of backend systems relative to itself. To check the availability of SQL and LDAP the ServiceStatus endpoint can be queried. Network hardware or administrators can perform an HTTP GET request to the URL https://silverback.company.com/mdm/ServiceStatus the response to this is a binary sequence to indicate whether LDAP or SQL is up, represented by a number “1” or “0”. The first digit represents SQL availability and the second, LDAP.

First Digit	Second Digit	Status
0	0	SQL and LDAP are unavailable
0	1	SQL is unavailable, LDAP is available
1	0	SQL is available, LDAP is unavailable
1	1	Both SQL and LDAP are available.

The current Silverback version can also be queried by using the ServicesVersion endpoint in the same manner. The URL for this endpoint is https://silverback.company.com/mdm/ServicesVersion. The response will be the current version, for example “4.2”.