MATRIX42
SMARTER WORKSPACE – BETTER LIFE

Silverback by Matrix42

Settings Administration 5.1 U3

Version 5.1.3.7

09/12/2016

Copyright © 2000 - 2015 Matrix42 AG

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

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

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

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

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

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

Table of Contents

1. Overview 4
2. Accessing Settings 5
2.1. Settings Administrator Role 5
2.2. Creating a Settings Administrator 5
2.3. Logging in as a Settings Administrator 5
3. Settings 6
3.1. General Section 6
3.2. MDM Payload Section 8
3.3. LDAP Section 11
3.4. App Portal and SMS Section 12
3.5. APNS Settings Section 14
3.6. Services Section 14
3.7. SMTP Section 17
3.8. Wi-Fi Client Certificates Section 17
3.9. EPiC Section 19
3.10. Silversync Section 19
3.11. Allowed Device Type Section 20
3.12. Android Settings Section 20
3.13. WP Settings Section 21
3.14. Cached Password Policy Section 22
3.15. LDAP Mapping Section 23
3.16. Cloud Connector Settings Section 23
3.17. WP MDM Section 24
3.18. Export and Import 27
3.19. Pending Commands 27
3.20. Connection String 28

Settings Administration 5.1 U3

1. Overview

As of Silverback by Matrix42 Version 4.7, the underlying system settings are managed via the Silverback Admin Console. Prior to this, these settings were accessed via a special Configuration Generator. For customers that upgrade to Silverback Version 4.7 from a previous version, these settings will be migrated automatically as part of the upgrade.

The settings are not available to all console users, there is a special role just to manage these, and users of this role can **only** manage the settings, not the rest of the environment. An overview of this role and how to configure it is available in the Accessing Settings section.

It's also important to note that there are some settings if configured incorrectly can be destructive to your Silverback by Matrix42 Environment. Also note that some settings, if changed **after** users have enrolled could cause the users to lose management with the server. If you need to change a setting and are unsure of the consequences, please contact support.

2. Accessing Settings

2.1. Settings Administrator Role

Settings Administrator is a special console user role that only has access to manage system settings. Because the settings available can be destructive tot he environment, it's important that the Settings Administrator role is delegated very carefully.

A Settings Administrator will only have access to System Settings, and have no access to the rest of the Silverback console. While all users login to the same console URL, only the Settings Administrator role will see the settings.

2.2. Creating a Settings Administrator

There is no default Settings Administrator account, so one must be created first. To create one, follow these steps:

1 Login to your Silverback by Matrix42 Admin console as an Administrator. The Admin URL is typically https://silverbackserver.yourcompany.com/admin

2 After logging in, click the **Admin Tab**

3 From the Admin Tab, click **User Management**

4 From User Management, click **New System User**

5 Enter the user information and configure the settings, and ensure that **Settings Administrator** is selected for the **Role** field.

6 Save the user

2.3. Logging in as a Settings Administrator

Settings Administrators login to the same page that normal console users do, that is the Admin page typically located at: https://silverbackserver.yourcompany.com/admin

3. Settings

3.1. General Section

CA Certificate Settings

Silverback deploys certificates to devices that enrol. For security, an individual certificate is generated for each device. Silverback contains a Root Certificate Authority Internally that issues certificates to the devices; the settings that are set with the certificates are configured in this section.

The Certificate Deployment option, relates to certificates deployed with things such as Exchange ActiveSync.

Setting Name	Description
Certificate Thumbprint	The thumbprint of the Silverback Root CA certificate. This certificate must be located in the Local Computer Certificate Store.
Country	The country that will be placed in the certificate information for devices.
Organisation	The organisation that will be placed in the certificate information for devices.
Location	The location that will be placed in the certificate information for devices.
Expiry Length (years)	How long the device issued certificates should last before expiring.
Certificate Deployment	**Enterprise Certificate –** Administrators will provide a single certificate to be issued to all users for things such as Exchange ActiveSync. **Individual Client -** If this is selected, a Microsoft Enterprise Certificate Authority will be contacted when a user enrols and certificate generated for that user. By default, the Certificate Authority Address is DEFAULT, which will tell the computer to automatically find the Certificate Authority. If you have the network address and instance name of the Certificate Authority, enter this here. Note that enabling this setting will automatically generate a certificate for all users in your Certificate Authority.

Settings Administration 5.1 U3

Certificate Renewal Settings

This section is only enabled if Individual Client certificates are enabled. This section determines certificate renewal settings.

Setting Name	Description
Renew certificates when expiry is within: (days)	When Silverback detects that a certificate it issued will expire this many days from today's date, it will renew the certificate. For example if this setting is set to 180, and the certificate expiry is 1 year, it will automatically renew half-way through the year.

Sites Settings

The Site Settings section contains mainly settings that are used to communicate with devices where certain endpoints are. In the majority of deployments, these settings should remain default unless extra configuration has occurred on the server.

In addition to this, some basic settings that affect the user experience are configured here.

Setting Name	Description
Admin URL	The URL for the admin console – This shouldn't be changed unless the website on the server itself has been changed first.
SSP URL	The URL for the Self Service Portal– This shouldn't be changed unless the website on the server itself has been changed first.
EPiC URL	The URL for Companion Clients to Checkin– This shouldn't be changed unless the website on the server itself has been changed first.
Activation URL	The URL for Activations– This shouldn't be changed unless the website on the server itself has been changed first.
Sharepoint URL	The URL for Companion Clients to Access Sharepoint Details– This shouldn't be changed unless the website on the server itself has been changed first.
Excel Connection String	Connection string the server uses to generate reports from the system. This is required so that the Excel documents are rendered correctly.
Include User Password in Exchange Profile	This determines if the Exchange ActiveSync profile should include the user's password. This password is only used if the user enrolled from the SSP, and is not used for Admin Provisioned Devices.

Settings Administration 5.1 U3

Setting Name	Description
Show Ownership option in SSP	This determines if the user can select Corporate/Personal ownership when creating an enrolment. If disabled, devices will default to Corporate Ownership.
Allow Admins to Clear Passcodes	This determines if administrators will have the ability to reset passcodes on devices.
Allow Admins to provision devices on behalf of users	This determines if administrators will have the ability to provision devices on behalf of users.
Maximum Failed Login Attempts for Console Users	The number of failed attempts before console user's accounts are locked out. Once locked out, another administrator will need to unlock the account.

3.2. MDM Payload Section

MDM Payload Settings

This section contains settings that are sent tot he device as part of MDM Enrolment. The URLs for Checkin and MDM should not be reconfigured unless the Silverback Websites have been reconfigured first.

The VPP Service Endpoint is specific to Apple and should not be reconfigured.

Setting Name	Description
Checkin URL	The URL for enrolling devices to check in for MDM Functions– This shouldn't be changed unless the website on the server itself has been changed first.
MDM URL	The URL for devices to establish MDM Sessions – This shouldn't be changed unless the website on the server itself has been changed first.
VPP Service Endpoint	This URL is used to communicate with Apple for VPP App Licensing. This should not be changed.

Block App Store Settings

To allow you to block access to the Apple iTunes store and still allow users to install App Store Applications, a special mechanism will enable the App Store momentarily and then disable it again. While the App Store is Unblocked, Silverback will attempt to install the application according to the Max Attempts setting, sleeping for the Sleep Time in between events, until the user has installed or cancelled the app installation.

Note that during this window, the user may be able to install another application, however the Application Whitelist policy will detect this, and perform the appropriate action on the user's device.

Settings Administration 5.1 U3

Setting Name	Description
Max Attempts	The number of times Silverback will attempt app installation when the App Store is blocked.
Sleep Time (seconds)	The amount of time in seconds between attempts that the Silverback server will wait before sending another request.

iOS Single App Mode Re-enablement Automation Workflow

For devices that are locked into Single Application Mode these applications cannot be updated while the device is locked. This can cause issues because sometimes these apps need to be updated and it's not viable to manually update the devices apps. The workflow is designed to remove the device from Single App Mode, Update the application and then lock the device again.

Unfortunately the device does not tell the server when it's done upgrading so the server needs to check constantly to ensure the device is locked as soon as the app is done updating. This setting determines how many times the server will "check" the device to see if the app is updated before stopping. If the applications are large or your users are in poor coverage, it's recommended to increase this value to allow the devices adequate time to update before we attempt to lock again.

Setting Name	Description
Maximum number of times to check if application is installed before attempting to re-enable SAM.	The number of times Silverback will attempt app installation when the App Store is blocked.

Signing Certificate Settings

For iOS devices, if the profile is signed, the user will see this as "trusted". Note that the user can still install an untrusted profile, so this should be used as verification for the user only. As of iOS 8, this is less important, as the user has less visibility as to whether profiles are signed or not.

Setting Name	Description
Certificate Thumbprint	For iOS device enrolments, the profiles can be signed so the user sees them as “trusted”. This thumbprint should match a signing certificate installed in the Local Computer Certificate Store.

MDM Concurrency Settings

From Silverback Server version 4.8 Update 1 and above, it’s now possible to limit the number of devices that can communicate with the server at any given time. These settings control the system behavior for this.

Setting Name	Description
Minimum number of devices in the system before concurrency limit is enabled.	Once the number of devices that exist in the console reaches this limit the concurrency settings will be enabled. The graph in Pending Commandsm will not show until this number is reached.
Period in minutes between limit flush to db	The amount of time in minutes before the device limit (defined in the Admin tab > Pending Commands section) will be saved to the database. It’s recommended to set this value to be large if you don’t intend to change the limit.
Minutes before device count cache is cleared	The number of devices in the system is cached. This means that potentially the above limit could be exceeded before the concurrency settings are enabled. This setting defines how long until the number of devices in the system is refreshed.
Seconds before statistics SQL query will timeout	The graph in the admin page may timeout if the request is large or the system is under load. This setting determines how long the SQL query will execute before timing out.
Interval for getting statistics data in minutes	How often the system should get updated statistics data.
Limit of rows for statistics request	How much data should be sampled for the statistics. The sytem will query the executed commands, sort by how long the commands took (descending) and then take this number of items for it’s statistics.
Percentage of request limit before statistics check	The system will recalculate how many devices should be checking in, this is the percentage of the current limit that the system should wait for, before checking statistics.

3.3. LDAP Section

LDAP Settings

These settings govern how the system connects to LDAP sources, and also what information should be brought back for users.

Setting Name	Description
Account Field	The LDAP Property used for the user's username
Distinguished Name	The DN used for LDAP users lookup, this is a fall back if the item in the **LDAP Mapping** section does not work.
Email Field	The LDAP Property used for the user's email address
LDAP Filter	Users must match this filter when using the SSP, or they cannot create enrolments, this is a fall back if the item in the **LDAP Mapping** section does not work.
LDAP Server	The network address of the LDAP Server
LDAP Port	The network port to use for LDAP Server connections
LDAP Type	The type of LDAP Source.
LDAP SSL	Determines if LDAP/S is used or not
Certificate User Field	The LDAP Property used for the user's certificate username
Email User Field	The LDAP Property used for the user's email username
VPN User Field	The LDAP Property used for the user's vpn username
LDAP WiFi Field	The LDAP Property used for the user's WiFi username
LDAP WiFI Proxy User Field	The LDAP Property used for the user's WiFi Proxy Username
LDAP WiFi SMIME User Field	The LDAP Property used for the user's SMIME Certificate Username – This is used for WiFi Certificate Generation
LDAP Global HTTP Proxy User Field	The LDAP Property used for the user's Proxy settings if enabled by profiles
LDAP First Name User Field	The LDAP Property used for the user's First Name
LDAP Surname User Field	The LDAP Property used for the user's Last Name
LDAP Lookup Username	If needed, a Bind username for LDAP Lookups, anonymous binds will be used if this is not specified
LDAP Lookup Password	If needed, a Bind password for LDAP Lookups
LDAP Request Page Size	How many items should return per page in LDAP request. For large LDAP Results, this can reduce issues with missing users for Tag Population
LDAP Referral Chasing Option	Determines if the server should "chase" referrals to other LDAP Sources
Number of LDAP Request Retries	How many attempts should be made for an LDAP request before the system will fail.

Custom LDAP Variables

These variables are used for System Variables when generating profiles. These are useful if you need to populate a miscellaneous value into a profile for a user that isn't covered by the normal values above.

Setting Name	Description
Custom LDAP Var0	Custom Variable to be returned for the user
Custom LDAP Var1	Custom Variable to be returned for the user
Custom LDAP Var2	Custom Variable to be returned for the user

3.4. App Portal and SMS Section

App Portal Settings

These settings control the behaviour of the App Portal for devices, and also how application information is retrieved from Apple.

Setting Name	Description
URL	The URL for devices to access the App Portal – This shouldn't be changed unless the website on the server itself has been changed first.
Device App Portal Refresh Interval	While the user has the App Portal open on their device, the page will automatically refresh for them at this interval. This ensures the user's available application list is always up to date.
Device App Portal Managed App List Interval	While the user has the App Portal open on their device, the server will request a managed app list from the device at this interval. This ensures that the status for managed apps (Install, Uninstall, Upgrade etc.) is current.
iOS AppInfo URL Template	This is the URL used to retrieve app information from Apple. This should not be changed.

Settings Administration 5.1 U3

SMS Server Settings

Silverback integrates with SMS Providers so that user's can receive SMS messages when they create enrolments. Currently, Silverback by Matrix42 supports the RedCoal SMS Provider for Australian customers, AerialLink and MessageBird for the rest of the world. Note that Aerialink is depricated and will no longer be supported. Customers should select Aerialink v4 if using Aerialink or use MessageBird.

Setting Name	Description
Send Provisioning SMS to Users	Determines if the server should send SMSs to users.
SMS Sender Label	If supported by the SMS Provider, this will appear as the "From:" label for the users.
SMS Provider	Selects the SMS Provider, either RedCoal or AerialLink
AerialLink URL	**AerialLink Only:** The AerialLink SMS Endpoint – This should not be changed.
AerialLink SID	**AerialLink Only:** The identifier for the AerialLink account – This should not be changed.
AerialLink Token	**AerialLink Only:** The access token for the AerialLink account – This should not be changed.
Serial Number	**RedCoal Only:** The serial number for the RedCoal account – This should not be changed.
SMS Key	**RedCoal Only:** The authentication key for the RedCoal account, this should not be changed.
Endpoint URL	**RedCoal Only:** The RedCoal API endpoint – This should not be changed.
AeriaLink URL	**AerialLink V4 Only:** The SMS Endpoint – This should not be changed
AeriaLink V4 API Code	**AerialLink V4 Only:** The API Code for access to sending SMS, this should not be changed.
AeriaLink V4 API Key	**AerialLink V4 Only:** The API Key for access to sending SMS, this should not be changed.
AeriaLink V4 API Secret	**AerialLink V4 Only:** The API Secert for access to sending SMS, this should not be changed.
Use International Number Format	**AerialLink V4 Only:** Determines if the endpoint should expect international SMS in + format. Generally this should be left to the default settings.
API URL	**MessageBird Only:**The URL for the MessageBird API – This should not be changed
Authorisation Token	**MessageBird Only:**The access token for connecting and sending messages – This should not be changed
Country Code for Local Numbers	**MessageBird Only:**If you want to use a local number format to send messages, enter the default country code here.

3.5. APNS Settings Section

APNS Settings

This section should generally not be modified. These settings are static and control how iOS MDM Certificates are requested and also how the server should connect to Apple to send push messages.

Setting Name	Description
Matrix 42 Accounts URL	Used when generating an iOS MDM Push Certificate
Matrix 42 Signing API URL	Used when generating an iOS MDM Push Certificate
APNS Port	The port to communicate with Apple for push messages
APNS Gateway	The Apple server to send push message requests to

3.6. Services Section

Silverback Windows Services Settings

These settings mainly govern the timing of backend events in the system. The Silverback service runs on the server constantly in the background and follows these settings. While in most cases these settings can be tuned to be as “live” as possible, if performance degradation is experienced, these settings can be tuned to even out the load on the server.

Setting Name	Description
Daily Inventory Start Time	The hour of the day that the daily inventory task should start.
Send Daily Inventory Every (hours)	The number of hours since the last inventory task before another will be started. E.g. If the Poll Time is 6:00, and the Poll Interval is set to 1, then every hour after 6:00 a full inventory will be performed.
Data Retention Poll Time	The time of day that the system should commence the data retention clean up. Data retention is the period in which things like Logs are kept. The clean up task can be SQL intensive, so its recommend this Poll Time is set to a quiet period for user activity.
Clear Pending Records (minutes)	How often the system should clean up expired pending enrolments. Pending enrolments may no longer be valid, but they still exist in the system and should be cleaned up regularly.
Check for pending emails to	Emails sent by Silverback are first queued in the database.

Settings Administration 5.1 U3

Setting Name	Description
send every (minutes)	This task determines when the system will check for pending emails and send them.
Send Inventory Requests in batches of	The daily inventory will send this many requests in a group, before waiting for the Delayed Interval (below).
Send Inventory Request Batches every (minutes)	The number of minutes before sending the next group of device inventory tasks. This should be configured particularly for large deployments. For example, if the Total Messages to Send is “20” and this setting is “10”, then 20 devices will be told to check in for inventory every 10 minutes at the Poll Interval.
Refresh LDAP User Info every (minutes)	How many minutes should pass before the system refreshes user data from LDAP. This lookup refreshes user information, for example if a user was to marry and change their surname in LDAP, this task would detect the change and update the user information in the console.
Attempt pushes to removed devices for (days)	Removed devices in some scenarios may still have an MDM profile installed, for example if the device is deleted, but the MDM Profile fails to be removed. Silverback will continue to push to removed devices, to ensure that the MDM Profile is removed. It will continue for the number of days configured in this setting.
Attempt pushes to removed devices every (minutes)	How long the system should wait before sending pushes to removed devices.
LDAP Info Update Service Task	Wether the system should update user information from LDAP.
Bulk Import Processing Task Interval (minutes)	Bulk import jobs (e.g. for Bulk Pending Enrolments) are queued in the database. This task will start processing the bulk jobs and this interval is how often the system will look for jobs to start.
Data Retention Task Timeout (minutes)	The data retention task, as mentioned above can be SQL intensive, and depending on the number of users, may take a long time to execute. This timeout can be increased if the data retention job is not completing.
Compliance Dashboard Task Timeout (minutes)	The Compliance Dashboard, harvests data from the database to display, this can be quite SQL intensive, so in the event that this job is failing, the timeout can be increased to allow appropriate time to execute.

Settings Administration 5.1 U3

EPiC Windows Services

The EPiC Service runs on the server and manages notifications to Companion Clients. The APNS Settings should not be changed.

Setting Name	Description
Message Companion Users to checkin every (minutes)	For Companion clients, how often the users should be told to check in via push notification. This is currently a global setting that overrides the notification settings in the EPiC setting of the admin console.
Check for grace period violations every (minutes)	The amount of time that the system will check for grace period violations. That is, the system will check, at this interval for devices that haven't checked in within the grace period defined in the EPiC settings in the admin console.
APNS Port	The port to communicate with Apple for push messages
APNS Gateway	The Apple server to send push message requests to

Batch Application Install Requests

Because applications stored on the server can be potentially large, and also sent to a large number of users, Silverback will send the app installation pushes in "batches", to ensure a steady load on the server. In this section you nominate how many pushes to send in a batch, and how often the batches should be sent.

Setting Name	Description
Send app installations in batches of	When pushing an application to a large number of devices, the system can be slowed by too many devices downloading the app at once. This setting allows you to send app installations in batches to ensure smooth load
Send batches every (minutes)	How long the system should wait before sending the next batch of app installation pushes.

3.7. SMTP Section

SMTP Server Settings

Emails are sent for various functions in Silverback. This may be informing a user of an enrolment, or email administrators about users violating policy. Generally an SMTP Relay that supports anonymous relaying internally would be used. If you require authentication on the proxy, please specify the username and password.

Setting Name	Description
SMTP Server	The network address oft he SMTP Server or Relay
SMTP Port	The SMTP Port to use
Use SSL	Whether or not the system uses SSL with SMTP
Username	If the SMTP server requires authentication, specify the username. If no username is provided it is assumed tob e anonymous
Password	If the SMTP server requires authentication, specify the password. If no password is provided it is assumed tob e anonymous

Email Template Settings

This section governs settings surrounding the email template. At this point in time, this is essentially just who the user sees the email came from.

Setting Name	Description
Sent From	The address that should appear as the “From“ address when the user receives the email

3.8. Wi-Fi Client Certificates Section

Wi-Fi Client Certificate Details Settings

If you use client certificate authentication for your Wi-Fi network, this section should be configured. When a Wi-Fi profile is set to use client certificate authentication in the admin console, these settings will be used to generate the certificates for users.

Setting Name	Description
Wi-Fi Enterprise Certificate CA	The Microsoft Enterprise Certificate Authority
Template ActiveSync Certificate Name	The template used for ActiveSync User Certificates
Exchange Certificate Template Validity	The expiry, in days for the certificate. Silverback will use this to automatically renew the certificate, if it can’t get the

Settings Administration 5.1 U3

Setting Name	Description
	expiry information from the certificate itself.
Template Wi-Fi Certificate Name	The template used for Wi-Fi User Certificates
Wi-Fi Certificate Template Validity	The expiry, in days for the certificate. Silverback will use this to automatically renew the certificate, if it can't get the expiry information from the certificate itself.
Template Certificate User Field	The template field that should be populated with the user's UPN
Agent Cert Thumbprint	An Agent certificate may be required to request certificates on behalf of a user. This certificate should be installed in the Local Computer Certificate Store, and the Network Service should have permission to manage the private key. Then specify the thumbprint fort he certificate here.

3.9. EPiC Section

Companion EPiC/Grace Period Push Message

Setting Name	Description
Companion Grace Period Push Message	The message to send to the user to remind them to check in

Queue Device Inventory on Checkin

Setting Name	Description
Queue Device Inventory on EPiC Checking	Whether the Silverback server should perform a full device inventory when the Companion Client checks in. This is usefull if you allow automated unblocked, as the user will be able to rectify the problem, then scan Companion to get unblocked.

Companion Blocked Message

Setting Name	Description
Companion Blocked Message	The push message sent tot he user's Companion client when they are blocked

Companion Unblocked Message

Companion Unlocked Message	The push message sent tot he user's Companion client when they are unblocked

3.10. Silversync Section

Silversync Content

Setting Name	Description
STS URL	The URL for the Secure Token Service. This shouldn't be changed unless the website on the server itself has been changed first.
Silversync Remote Configuration Endpoint URL	The URL for the system to communicate with Silversync. This shouldn't be changed unless the website on the server itself has been changed first.
Silversync Security Principal	The account that Silversync should run as. Generally this

Setting Name	Description
	shouldn't be changed.
M42 Push Notification Host URL	The endpoint for push notifications for Silversync clients. Generally this shouldn't be changed.

3.11. Allowed Device Type Section

Allowed Device Types

Setting Name	Description
Allowed Device Types	Generally these could all be left enabled, this determines what device types you want to allow in your system. If you environment has very specific requirements, for example you only use iPads, the other device types can be disabled which will now allow prevent enrolment, but also remove the other device type's settings from the console which can make managing settings easier.

3.12. Android Settings Section

Android GCM Settings

This determines the company information used to push to users. In most installations, the generic Silverback settings are used. If you require your own internal push settings for any reason, this is where you configure them.

Setting Name	Description
GCM Send URL	The endpoint to send GCM Pushes to devices, this should not be changed
GCM Project ID	The Project ID to be used for push, this should not be changed
GCM Auth Key	The Authentication token to be used for push, this should not be changed

Google Play Settings

This setting should not be modified. This tells Silverback which Google Play app to use for Android device enrolment.

Setting Name	Description
Google Play Enabled	Determines if Silverback should use the Google Play Companion Client, this should not be changed

Setting Name	Description
Google Play App URL	The Google Play link fort he Companion App, this should not be changed

3.13. WP Settings Section

WP Settings

This section covers settings for WP7 enrolment, which are largely deprecated. The remaining Application ID setting is no longer used and can be ignored.

The EAS settings however, govern some basic settings for Exchange Protection features. In general these settings should not be changed.

Setting Name	Description
EAS Datetime Format	The date format to use for EAS Display items for Exchange ActiveSync Quarantine.
EAS Schema URL	The schema location for EAS – This should not be changed

WP Marketplace Settings

These settings determine how Silverback should query the Windows Marketplace for App Information. These settings should not be changed or app lookups may not work.

Setting Name	Description
AppInfo Template URL	The lookup end point for app information – This should not be changed
AppIcon Template URL	The lookup end point for app icon downloads – This should not be changed
AppDownload Template URL	The lookup end point to search for applications – This should not be changed

Windows 8.1 Family Device Settings

These settings are for Windows 8.1 devices and their enrolment. At the time of writing, Silverback requires that you generate a fake application to enable push connectivity for devices. Soon Silverback will pre-generate this information for you.

Setting Name	Description

Settings Administration 5.1 U3

Setting Name	Description
WNS App ID	The App ID generated when creating the fake push application for 8.1 devices.
WNS Package Family Name (PFN)	The PFN token generated when creating the fake push application for 8.1 devices.
WNS App Store URI	The URI generated when creating the fake push application for 8.1 devices.
WNS App Secret	The authentication token generated when creating the fake push application for 8.1 devices.
Enrolment Issuing CA Thumbprint	The Thumprint of the CA that will issue certificates to the 8.1 devices. This should be in the Local Computer store, and the Network Service account should have permissions to manage the private key.
CEP Encryption Agent Thumbprint	RA Certificate thumbprint for certificate enrolment
EAO Signature Agent Thumbprint	RA Certificate thumbprint for certificate enrolment

3.14. Cached Password Policy Section

Cached Password Policy

Silverback has the option to cache passwords the user enters when creating enrolments. The passwords (if cached) are stored encrypted in the database and embedded into profiles sent to the user's devices. If your company policy dictates that passwords can not be cached, then choose to never cache them. Otherwise, the passwords can be cached for a number of uses before being destroyed. If you want the users to have passwords pre-configured for them its recommended you nominate the number of uses to match the number of profiles that **need** the password.

If you have no concerns for the amount of time a password is cached, enter a large number and this will ensure the users shouldn't need to ever enter a password.

Setting Name	Description
Cache User Passwords	Whether user passwords should be cached from enrolment (encrypted) and used to inject into profiles, like Exchange ActiveSync, so the user doesn't have to enter the password
Cache user passwords for number of uses	If you allow caching, you nominate how many times this password can be used before being cleared. While the passwords are encrypted, it's still never good to leave these in the database. After this number of uses, the password will be cleared.

Setting Name	Description
	It's suggested you set this to the number of settings you want to push that need a password. For example, if the user only needs the password for Exchange ActiveSync and your WiFi settings, enter "2", this will ensure that after the user has all their needed profiles, the password will be cleared.

3.15. LDAP Mapping Section

Base DN Mappings

In this section you can configure how user's UPNs should map to LDAP. If your environment has multiple UPN suffixes, then these can be specified in each row. When a user enrols and enters their username, the UPN suffix is used and matched to this list, if a match is found, the Base DN and Filter will be used to ensure the user can enrol.

Setting Name	Description
UPN Suffix	The UPN Suffix to match when the user enrols
Base DN	The BASE DN to use for lookups for this UPN Suffix
LDAP Filter	The LDAP Filter to use for lookups for this UPN Suffix

3.16. Cloud Connector Settings Section

Cloud Connector Settings

The cloud connector allows Silverback servers outside of your LAN to communicate with your local resources. The cloud connector is an outbound only session and is mutually authenticated and encrypted. This means that the cloud connector client (not covered in this document) must be configured to use the Silverback server's public key, so that the server can decrypt the client traffic.

Setting Name	Description
Tunnel URL	The URL for cloud connector connectivity – This shouldn't be changed unless the website on the server itself has been changed first.
Send LDAP Requests through Tunnel	Wether or not LDAP Requests should be sent down the cloud connector tunnel
Request Client Certificates through Tunnel	Whether or not Client Certificate Generation should be sent down the cloud connector tunnel
Enable Exchange Protection	Whether or not Exchange Quarantine functions are sent down the cloud connector tunnel
Exchange Task Interval	This is the interval at which exchange protection will be

Setting Name	Description
	executed. Note that by default this setting is quite large. This is due to the fact that if exchange protection is enabled, but not configured correctly, large amount of traffic can be generated against the Exchange Environment. If Exchange protection is configured then this setting should be reduced to the desired frequency. Ideally 1 minute.
Max Exchange Concurrency	Maximum number of concurrent Exchange Protection Requests to send at one time
Exchange Protection Max Try	The number of times the server should retry if it was unable to use the Exchange Quarantine function
Enable Traffic Log	Whether traffic information from the Cloud Connector should be logged. This should only be enabled for troubleshooting
Tunnel Security Principal	The local account that is running the cloud connector tunnel on the server
Client Certificate Thumbprint (public key)	The public key thumbprint of the cloud connector client certificate. Used to encrypt traffic sent to the cloud connector client
Silverback Server Tunnel Certificate (private key)	The private key thumbprint of the server's client certificate, Used to decrypt traffic sent to the server from the client.

3.17. WP MDM Section

WP8 MDM Settings

This section covers settings relating specifically to WP8 enrolment. In general these settings shouldn't be changed.

Setting Name	Description
Enrollment URL	The URL for WP8 device connectivity – This shouldn't be changed unless the website on the server itself has been changed first.
Use Indentation	Internal WP setting, do not change.
WPMDM_OmaDmRetry NumRetries	The number of initial polls after enrolment
WPMDM_OmaDmRetry RetryInterval	The time in between polls after enrolment
WPMDM_OmaDmRetry AuxNumRetries	The number of polls to attempt AFTER the first series of polls have been used.
WPMDM_OmaDmRetry	The time in between polls after the first retry interval has

Settings Administration 5.1 U3

Setting Name	Description
AuxRetryInterval	been used.
WPMDM_OmaDmRetry Aux2NumRetries	After the above settings have been exhausted, this number of retries will be followed. Note that this should be set to 0, and never changed. This ensures the device will continue to check in. If this is changed to another number, the device will check in that many times, and then stop.
WPMDM_OmaDmRetry Aux2RetryInterval	The interval between check-ins for the above setting.
Exchange Profile Includes Random Password When Empty	In some scenarios, the exchange profile will fail to install if there is no password specified. This setting tells the server to insert a random password if it doesn't have the users password. This will ensure that the profile is installed, and the user will be prompted for their password.

Company Hub Settings

For WP8 management and enrollment, you require a Symantec Certificate, this is covered in a separate document, however the Symantec Certificate information should be populated here.

Setting Name	Description
Enterprise ID	ID From Symantec Certificate
Enrollment Token	AET Token generated with the Symantec Certificate
Store Product ID	The Windows Marketplace Identifier of the Silverback WP8 App Store App
Store Name	Internal Application setting, this should not be changed.
Company Hub App Title	Internal Application setting, this should not be changed.
Company Hub URL	The URL for WP8 Company Hub – This shouldn't be changed unless the website on the server itself has been changed first.

Windows Devices Inventory Intervals

For Windows devices, because the checkin interval can be driven by the client, to reduce load the tasks that are performed each checkin can be limited. The settings in this table determine how often these should be queried on a device when it checks in – **not** how often a push will be sent to query these. For example, for Certificate List, these settings mean that if a device checks in, and it has been X minutes since the last certificate list was gathered from the device, a certificate list query will be executed.

Setting Name	Description
Queue Certificate List after	Number of minutes since the last certificate list, before it will be queued again
Queue Push Token Info after	Number of minutes since the last push token information query, before it will be queued again
Queue Device Info after	Number of minutes since the last device information query, before it will be queued again
Queue Security Info after	Number of minutes since the last security info check, before it will be queued again
Queue Installed App List after	Number of minutes since the last installed application list, before it will be queued again
Queue Managed App List after	Number of minutes since the last managed application list, before it will be queued again

Assigned Access

For Windows devices, it's now possible to configure Assigned Access. This gives administrators greater control over the device including the ability to compeltely customise the home screen and what functions are available to users.

There is a very large risk that if the configuration XML for this is not carefully checked, that devices can be "Bricked" and no longer usable. Because of this, this is disabled by default and must be enabled here first.

3.18. Export and Import

Export and Import

This section allows you to export the Settings Administration settings so that you can keep a backup of these settings or move these to another server. The export and import will retain all settings, but it's critical that the web settings encryption certificate (configured in the config generator at installation) is the same, or when uploaded, the import will not be able to be read by the server.

Setting Name	Description
Download Export	Clicking the link will download a full export of all the settings. Note that this is encrypted with the servers web settings encryption certificate.
Import	Upload a previously exported configuration file. This will only be readable by the server if the same web settings encryption certificate is used.

3.19. Pending Commands

Pending Commands

This section displays a count for all pending commands in the system. In certain troubleshooting scenarios it might be nesesary to clear these commands. This should generally be avoided because primarily it can cause a large amount of load on the system while the commands are cleared, but also that devices may lose important commands that were previously queued for them. If devices lose these commands, it might be nesesary to block and unblock the device, or re-enroll the device to recitfy.

Setting Name	Description
Clear Pending Commands	Clicking this will clear all of the pending commands in the system.

3.20. Connection String

Connection String

In previous versions of Silverback, the database connection information was stored within the web.config files located on the server. As of version 5.1 Update 1, these settings have been migrated to this page.

These settings mainly govern the connection information for the database.

Setting Name	Description
Database Server Address	The network address or DNS name of the SQL server that holds the Silverback database.
Failover Database Server Address	If needed, you can also specify a separate server to fail-over to in the event the database server is un-reachable.
Database Name	The name of the Silverback database
Use SQL Authentication	Whether Silverback should use a defined username and password for SQL, or assume permissions for itself (e.g. if the Silverback server is granted permissions on the database, then it will authenticate as itself).
Username	If using SQL authentication, the username.
Password	If using SQL authentication, the password.
Web Settings Certificate Thumbprint	The web settings encryption certificate. This is used to encrypt the web settings in this page. If you migrate to another server you must move the certificate so this thumbprint matches a certificate that is available on the local machine for Silverback.