MATRIX42
SMARTER WORKSPACE – BETTER LIFE

Silverback by Matrix42

Release Notes 4.8 Update 1

Version 4.1.8.4

25/08/2015

Copyright © 2000 - 2015 Matrix42 AG

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

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

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

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

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

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

Table of Contents

1. New Features and Improvements 4
1.1. OS X Support 4
1.2. Performance Improvements 4
1.3. Duplicate Device Handling 5
1.4. API Improvements 5
1.4.1. Help Pages 6
1.4.2. Application Lists 6
1.4.3. Metadata 6
2. Minor Changes and Fixes 7
3. Known Issues 8

Release Notes 4.8 Update 1

1. New Features and Improvements

1.1. OS X Support

Silverback by Matrix42 version 4.8 U1 is the first version to support OS X devices. OS X devices enrol into Silverback in the same way as iOS devices, and currently the supported features for OS X are:

- Device Inventory Auditing
- Device Actions (e.g. Lock, Block, Wipe)
- Exchange ActiveSync Including Client Certificate Authentication
- Email Profiles (IMAP/POP)
- Passcode Settings
- Wi-Fi Payloads Including Client Certificate Authentication
- Custom Profiles
- Restrictions
- VPN Settings
- Web Clips

1.2. Performance Improvements

With 4.8.1.3, substantial improvements have been made into the handling of device requests. Not only static improvements to some device requests, but also tuneable and scalable configuration options to help ease the load in large deployments.

- Windows Devices Inventory Intervals

  Via the Settings Admin page, it's possible to tune how often Silverback will request certain information form WP 8.1 devices. Previously, every device check-in would result in a full device inventory. In larger deployments, this would put substantial load on the server.

  Each inventory item has a configurable interval, in minutes, that will determine how often that inventory item is executed. This means if the setting was set to "60" for "Certificate List", then Silverback would ensure each device is audited for certificate list a maximum of once every 60 minutes.

  Note that this does not trigger a push every 60 minutes, this merely makes sure that on device check-in, the inventory for certificates was executed within the last 60 minutes, and if not, queues it again.

  This is configurable from the WP MDM section of the settings admin page, under "Windows devices Inventory Intervals"

- MDM Concurrency Settings

  For larger deployments, a simple action like updating an Application, or requesting a device refresh for a Tag could trigger thousands of devices to attempt to connect at once.

  What this would mean is the system resource usage would grow, slowing down subsequent requests and ultimately taking a long time to execute all the check-ins.

  It's now possible to configure a maximum concurrent devices setting which will ensure that no more than a certain amount of devices can check-in at once.

  From the Pending Commands section in the Admin Tab, there is a new Concurrency graph and setting. The graph will display how long commands are taking to execute on your fleet. If these commands are too high, then the maximum concurrent device setting should be decreased, allowing a smoother operation.

1.3. Duplicate Device Handling

Traditionally in Silverback, Devices are identified by their unique identifiers. Some devices however will generate a new identifier when re-enrolled or wiped. What this would mean is that a device might appear twice in the Silverback console if it was re-enrolled or wiped.

With this update, Silverback now identifies devices re-enrolling by hardware identifiers and optionally removes an existing entry for that device. This means that not only will the existing device not show in the console, it will also not consume an additional license.

- Removing Duplicates:

To enable the removal of detected duplicates, navigate to the Admin Tab > Licenses section, and check the "Remove Duplicate Device Info" checkbox. What this will do is when a device enrols, the system will compare unique hardware identifiers to existing devices, and if a match is detected, it will remove it.

- API Duplicates:

In addition to removing duplicates on enrolment, the system will also have a unique identifier for every device that is generated internally. This means that each device returned by the API will be a valid, unique device.

1.4. API Improvements

The API as mentioned above will no longer return duplicate device entries, but in addition to this, several changes to the API have been made:

1.4.1. Help Pages

The API Document previously available has been replaced with an on-server help page. This means that the documentation for a specific server version will be bundled with that version. To access the help pages, navigate to https://silverback.company.com/api/help (where silverback.company.com is your Silverback by Matrix42 server).

1.4.2. Application Lists

The Silverback by Matrix42 API now supports returning the application list for devices. Previously this would only return dummy data, but now is a live application list.

1.4.3. Metadata

To help with integration, the Silverback API now has a Metadata endpoint. This endpoint will essentially handle lookup data, where the system will return a state code or identifier, the metadata endpoint can be used to get a human readable value for it.

The first iteration of the Metadata endpoint covers the enrolment status code for devices. By requesting /api/v1/metadata/enrollmentStatuses the system will return localised descriptions for each enrolment status.

In addition, to help third party systems detect devices in their systems that are in Silverback too, we provide a “Matching Data” metadata end point. This provides key fields per device type that should be used to “pair” devices in Silverback. This endpoint will return for example “imei” as a matching data point, the third party system would then attempt to match the imei number for that device to their own system. This can be accessed via /api/v1/metadata/matchingidentifier.

2. Minor Changes and Fixes

- Published app icons for WP8 were incorrect
- Compliance Dashboard logic now shows the correct data for number of devices
- Resolved issue with 8.1 apps not deploying
- Resolved issue with Samsung Safe “Past Days of Mail to Sync” setting not working correctly.
- Added option to queue a stop command for Windows Phone devices to prevent recurring check-ins
- Resolved issue with Windows Phone devices constantly requesting app installs if the app install was invalid.
- Ensure that Windows devices reporting an invalid application installation will not attempt to install the app infinitely
- Resolved issue with dashboard graphs not displaying sections when there are a large number of devices.
- App Portal tabs hidden for device types that don’t support apps
- Added option to disable Simple Enrolment for Android completely
- Improved dashboards to handle very large sections of one device type
- Adjusted AfW Portal URL
- Adjusted AeriaLink SMS Provider URL
- Adjusted default Apple App Store Lookup URL to be HTTPS

3. Known Issues

- OS X Exchange has additional Path configuration options – If these are not correct, the profile will not install and the device may remain in Blocked. If your environment does not require these settings, leave them empty.
- OS X WiFi Payloads will not install if the WiFi network is not available. This may prevent the device from unblocking. This is currently expected Apple MDM behaviour.
- OS X Client Certificate with Exchange must be manually selected by the user after the profile is deployed. This can be done from the Mail > Preferences page, by selecting a “TLS Certificate” and choosing the certificate deployed by Silverback. Note that this field may not be visible on some versions of OS X.