MATRIX42
SMARTER WORKSPACE – BETTER LIFE

Silverback by Matrix42

Release Notes 5.0

Version 5.0.0.10

11/02/2016

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. New Features and Improvements 4
1.1. IMEI Based Hardware Authentication 4
1.2. API Changes 4
1.2.1. Hardware Authentication 4
1.2.2. Certificates 4
1.2.3. Pending Enrolments 4
1.3. Certificate Subject Field for Enterprise WiFi 4
1.4. Certificate Trusts for iOS 5
1.5. MSI Application Management for Windows 10 5
1.6. Whitelisting for Windows Phone 5
1.7. VPP System Revision 5
2. Minor Changes and Fixes 6

Release Notes 5.0

1. New Features and Improvements

1.1. IMEI Based Hardware Authentication

With this version of Silverback by Matrix42, the Hardware Authentication feature has been expanded to include IMEI number as well as serial number. Keep in mind that not all devices have an IMEI number, so use this in planning your use of this feature.

From the Hardware Authentication section of the Admin Tab, its now possible to define an IMEI or Serial Number or both for each entry. The logic for this doesn't require both serial and IMEI exist for an entry to work, so you can have two separate entries for IMEI and Serial for one device for example. When a device checks in, if the policy dictates that hardware authentication is enabled, any entry that includes the device's serial OR IMEI will allow that device to pass.

In addition to this, you can now add IMEI as a column to the devices table optionally and search and sort by this. Also IMEI number is now available as a device variable in the system. This means anywhere that system variables can be used, {DeviceImei} can be entered to use the IMEI number.

1.2. API Changes

1.2.1. Hardware Authentication

It's now possible to manage Hardware Authentication via the API. The feature functions the same way as the admin UI for this. See the API Integration guide, or the API help pages for information on how to use this.

1.2.2. Certificates

It's also possible to view the certificates on devices via the API. See the API help pages or API Integration Guide for information on how to use this.

1.2.3. Pending Enrolments

Management of pending enrolments is available from the API now also, this means that pending enrolments can be viewed, deleted, or have their OTP changed. See the API integration guide or API help pages for more information.

1.3. Certificate Subject Field for Enterprise WiFi

You can now manually define the subject name for enterprise WiFi certificate configurations for iOS and Android devices. To use this, go to your Enterprise WiFi

configuration and enter text in the certificate subject field. Note that if this is left blank (i.e. for existing customers) the current logic will still apply.

This field allows the use of system variables also, so the certificate subject can be dynamic per device/user.

1.4. Certificate Trusts for iOS

It's now possible to configure certificate trusts for iOS as a separate profile. Within the Profile settings of an iOS enabled Tag, navigate to the Certificate Trusts section and upload your root and intermediate certificates. These will be pushed to the devices as a separate profile and the device should then trust these certificates.

1.5. MSI Application Management for Windows 10

Windows 10 devices can now have MSI applications deployed to them. This functions the same as enterprise apps for other device types. To use an MSI application, upload it from the App Portal tab, choose Windows as the device type and then select Enterprise as the application type.

1.6. Whitelisting for Windows Phone

For Tags that are WP type, and for devices running Windows 10 Mobile, it's now possible to whitelist applications on the device. Currently this has three options: Block all non-Silverback apps, Block all except for Microsoft apps, and Block all except for Microsoft apps and Facebook. This can be enabled from the Tag Policy settings beneath Lockdown.

1.7. VPP System Revision

Major work has been done to overhaul the VPP implementation. Generally, the functionality can be considered to be the same but more robust with some additional features:

- You can optionally automatically un-assign VPP users from other EMM platforms. This means that users not recognised by Silverback (for example in the case of a migration), can have their apps unassigned.
- You can specify the Language and Country code for VPP apps. This means that if your VPP account is in the "de" region, you can specify that should be used for your VPP apps.
- You can manually assign and un-assign licenses from users.

2. Minor Changes and Fixes

- Improved handling of certificate trusts with Android devices
- Resolved issue with API routes for pending enrolments
- OS Class for Windows now displays correctly
- Added UI for VPP Changes
- Added Importing for VPP Apps
- Added scheduled refresh for VPP Apps
- Added Re-inviting for VPP Users
- Added VPP Audit
- Added assigning and un-assigning VPP licenses manually
- Added warning for Windows Phone lock requiring a passcode
- Bundled renewed Companion App Store Push Certificate
- Updated text in the certificate expiry emails
- Fixed issue uninstalling VPP app when license was unassigned
- Fixed issue with retired users that were not deleted from the database, could not be re-invited to VPP
- Removed links to editing apps from VPP assets and display app names for all device types
- Added support for fetching IdP metadata from ACS endpoints
- Added support for "order by" query for devices API endpoint
- IMEI is included in hardware authentication violation e-mails
- IMEI can be searched with or without spaces in the devices views
- New login UI for Pandora UI
- Resolved issue with M42 Mobile Certificates not being delivered to Android/Samsung devices
- Improved handling of DEP mandatory fields
- VPP App description is truncated further on import to resolve issues with special characters
- Removed SMS Sender from non RedCoal SMS providers
- Added support for Windows 10 MSI Upgrades
- Changed LDAP label for bulk provisioning to indicate local users can be used also
- Resolved resultant Tags issue with blacklist/whitelist
- Adjusted Blacklist/Whitelist App IDs for System Apps
- Resolved issue with MSIs not being removed when removed from App Portal