MATRIX42
SMARTER WORKSPACE – BETTER LIFE

Silverback by Matrix42

On Premise Solution Design Brief 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. Solution Architecture 4
1.1. Server Hardware and Software Requirements 4
1.2. Setup, Admin and User Requirements 4
1.3. Account Requirements 6
2. Environmental Requirements 8
2.1. Network Requirements 8
2.2. DNS Setup 9
2.3. Domain and Forest Functional level 10
2.4. SQL Database Requirements 10
2.4.1. Automated SQL Deployment 10
2.4.2. Manual SQL Deployment 10
2.5. SMTP Server Requirements 11
2.6. Active Directory Group Requirements 11
2.7. SSL Certificate Requirements 11
2.8. Exchange ActiveSync Requirements 12
2.9. Web Proxy Requirements 13
2.10. Google Settings for Android for Work 13
2.11. Windows Certificate Enrolment 13
2.12. SAMSUNG KNOX 13

On Premise Solution Design Brief 5.1 U3

1. Solution Architecture

1.1. Server Hardware and Software Requirements

Silverback Server

- Windows Server 2012 R2 – Windows Server 2008 onwards is supported, but it is recommended to use 2012 R2.
- 64 Bit CPU, 2.6 GHz Xeon or faster
- 4GB RAM
- 10GB of free disk space
- SCSI or SAS speed disks or equivalent SAS
- 1GB Network Interface Cards
- The server must exist in the same LAN as the SQL Server. 10ms latency minimum is required to the SQL Server
- The same data and time as the Silverback SQL Database Server
- The server must be configured for US English including:
  - Use the date and time format DD/MM/YYYY
  - Use English System Locale for non-unicode programs
  - Use English Display Language and Input Language for all users, including “Network Service”

SQL Server

- SQL Server 2008 to 2016
- 10GB of space per 1000 devices – This will change depending on individual requirements for logging and data retention.
- The SQL Compatibility Level must be 100 (this is SQL 2008 and 2008 R2) this is set by the script on the Silverback database automatically.
- The server/instance collation must be either:
  - SQL_Latin_General_CP1_CI_AS
  - SQL_Latin1_General_CP1_CI_AS

To facilitate an efficient and trouble free installation we require that any server hardening be enforced after the Silverback software has been installed and configured.

1.2. Setup, Admin and User Requirements

Additional Software Dependencies

On Premise Solution Design Brief 5.1 U3

Silverback requires that the following be installed on the server; these are readily available by configuring server roles or for download from Microsoft:

- Silverlight
- Microsoft Access Database Engine x64 2010
- .NET 3.5
- .NET 4.0
- .NET 4.5
- .NET (Pre-Installed with Server 2012 R2)
- IIS 8
  - For IIS, the following IIS Role Services must be enabled:

- [x] Web Server (IIS)
  - [x] Web Server
    - [x] Common HTTP Features
      - [x] Default Document
      - [x] Directory Browsing
      - [x] HTTP Errors
      - [x] Static Content
      - [x] HTTP Redirection
      - [ ] WebDAV Publishing (Not installed)
    - [x] Health and Diagnostics
      - [x] HTTP Logging
      - [ ] Custom Logging (Not installed)
      - [ ] Logging Tools (Not installed)
      - [ ] ODBC Logging (Not installed)
      - [ ] Request Monitor (Not installed)
      - [ ] Tracing (Not installed)
    - [x] Performance
      - [x] Static Content Compression
      - [ ] Dynamic Content Compression (Not installed)
    - [x] Security
      - [x] Request Filtering
      - [ ] Basic Authentication (Not installed)
      - [ ] Centralized SSL Certificate Support (Not installed)
      - [ ] Client Certificate Mapping Authentication (Not installed)
      - [ ] Digest Authentication (Not installed)
      - [ ] IIS Client Certificate Mapping Authentication (Not installed)
      - [ ] IP and Domain Restrictions (Not installed)
      - [ ] URL Authorization (Not installed)
      - [ ] Windows Authentication (Not installed)

- [x] Application Development
  - [x] .NET Extensibility 3.5
  - [x] .NET Extensibility 4.5
  - [ ] Application Initialization (Not installed)
  - [ ] ASP (Not installed)
  - [ ] ASP.NET 3.5 (Not installed)
  - [x] ASP.NET 4.5
  - [ ] CGI (Not installed)
  - [x] ISAPI Extensions
  - [x] ISAPI Filters
  - [ ] Server Side Includes (Not installed)
  - [x] WebSocket Protocol
- [ ] FTP Server (Not installed)
- [x] Management Tools
  - [x] IIS Management Console
  - [ ] IIS 6 Management Compatibility (Not installed)
  - [ ] IIS Management Scripts and Tools (Not installed)
  - [ ] Management Service (Not installed)
- [ ] Windows Deployment Services (Not installed)

Silverback Helpdesk, System Admin and End User Access

Access to Silverback for End Users, Help Desk and System Administrators is via a web-based console. Supported browsers are:

- Safari 4 and above
- Internet Explorer 9 and above
- Safari on an iPad

To provision a device, End Users must have access to the Silverback Self Service Portal. If a web proxy processes the user's web traffic, then we need to make sure the proxy server can serve the Silverback SSP web site. If this is not possible, proxy server exclusions must be set to allow direct access to the site.

1.3. Account Requirements

Silverback Server

To install the Silverback Server a domain account that is a member of the Local Administrators group is needed.

Microsoft SQL Database Server

The database will be deployed automatically when the server starts after installation or upgrade. The account on SQL should have the db_creator role to perform an installation, and should have db_owner on the Silverback database for upgrades.

If an automated deployment of SQL isn't an option, the database is built using a SQL script, which will be given to a Database Administrator to run after the server is installed.

On Premise Solution Design Brief 5.1 U3

Service Account

If utilizing LDAP user accounts instead of Local Users, Silverback requires READ access to LDAP so Silverback has the ability to find users within your LDAP schema. A service account must be created that has delegated Read permission to Active Directory.

Security Groups

The Silverback server requires two groups to be created in Active Directory:

Name: Silverback Mobile Device Manager
Type: Global Group
Members: $SilverbackComputerAccount

Name: Silverback Enterprise Device Management
Type: Universal Group
Members: Silverback Mobile Device Manager

Active Directory Permissions

The 'Silverback Enterprise Device Management' group must also be delegated Read permission to Active Directory.

SQL Permissions

The Silverback server stores its entire configuration in a SQL database, by default 'silverback'. The 'Silverback Enterprise Device Management' group must be given db_creator permissions on SQL, or if manually executing SQL scripts after installation, delegated 'Database Owner' permission to the 'silverback' database.

Exchange PowerShell Connectivity (Exchange 2010 Protection Only)

Silverback can be configured to use Microsoft Exchange's Device Quarantine Mode to block devices from syncing with the Exchange Server at a device level. For this to work, you must configure the following extra Active Directory Permissions on the *Silverback Enterprise Device Manager* group:

- Organization Management
- Server Management
- Exchange Recipient Management
- Server Management Groups

2. Environmental Requirements

2.1. Network Requirements

Silverback External Firewall Rules

Traffic source	Destination	Port/Protocol
Device (Internet)	TMG Server or Reverse Proxy (External NIC) (DMZ)	443/tcp

Silverback Publishing Firewall Rules

Traffic source	Destination	Port/Protocol
TMG Server or Reverse Proxy (Internal NIC) (LAN)	Silverback Server (LAN)	443/tcp

Silverback Server Function Firewall Rules

Traffic source	Destination	Port/Protocol
Silverback (LAN)	SQL Server (LAN)	1433/tcp
Silverback (LAN)	Domain Controller (Production)	389,636/tcp
Silverback (LAN)	SMTP Server (Production)	25/tcp
Silverback (LAN)	Exchange Server (Production) *Required for Exchange 2010 Protection Only*	443/tcp
Silverback (LAN)	APNS (gateway.push.apple.com, mdmenrollment.apple.com, vpp.itunes.apple.com) 17.0.0.0/8 (Internet) *Required for iOS only*	2195/tcp 443/tcp
Silverback (LAN)	iTunes (itunes.apple.com) http://support.apple.com/kb/TS1379	80/tcp 443/tcp
Silverback (LAN)	GCM (android.googleapis.com/gcm/send) Google's ASN IP Block - 15169 *Required for Android only*	443/tcp
Silverback (LAN)	Microsoft Push Network *Required for Windows 8.1 and Windows Phone 8.1 only*	443/tcp
Silverback (LAN)	**North America, Europe and the rest of the world** SMS (api.aerialink.net, rest.messagebird.com) (Internet)	443/tcp

Traffic source	Destination	Port/Protocol
	Australian Customers Only SMS (sms.silverbackmdm.com) (Internet) 59.154.43.98	

User & Management Firewall Rules

Traffic source	Destination	Port/Protocol
User Workstation (Intranet)	Silverback (LAN)	443/tcp
User Devices (Wi-Fi)	APNS (gateway.push.apple.com) 17.0.0.0/8 (Internet)	5223/tcp
User Devices (Android)	GCM (android.googleapis.com/gcm/send)	5228/tcp 5229/tcp 5230/tcp
Wi-Fi Only User Devices (KNOX)	KNOX Registration (gslb.secb2b.com, eu-prod-klm.secb2b.com)	80/tcp 443/tcp
Wi-Fi Only User Devices (Windows 8.1 Family)	Microsoft Push Network	443/tcp

The solution requires LAN speed; therefore we need at least 100Mbps network connections, with latency under 10ms between all internal systems

2.2. DNS Setup

As Silverback requires devices to connect via DNS, The appropriate DNS entries must be setup for your server. Internally and externally the DNS name should ideally be the same, so devices can resolve the server address inside your network and outside. For example: **silverback.yourdomainname.com.**

For Android Based devices, a DNS SRV record lookup is performed to find the server based on the username entered in the client. If the user enters “user@company.com” , then a SRV service record lookup is performed against “company.com” for the _silverback SRV record.

The SRV record should be setup like this:

```
Service:        _silverback
Protocol:       _tcp
Priority:       0
Weight:         0
```

```
Port Number:                443
Host offering this service:   <Silverback Server FQDN>
```

For Windows 8.1, Windows Phone 8 and Windows Phone 8.1 devices, a DNS entry must be created for **enterpriseenrollment.yourdomainname.com** that resolves to the Silverback Server.

2.3. Domain and Forest Functional level

Silverback supports Windows Server 2003 and Windows Server 2008 Active Directory domain and forest functional levels. Silverback supports installation in Active Directory domains at the “Windows Server 2003”, “Windows Server 2008” and “Windows Server 2008 R2” domain and forest functional levels.

2.4. SQL Database Requirements

2.4.1. Automated SQL Deployment

A user with the db_creator role should be created for deployment. The Silverback database will be created automatically as part of the installation process.

2.4.2. Manual SQL Deployment

A database "silverback" needs to be created on the SQL server. The database is created using an initialization script during the installation process.

The Initial size of the database DATA file should be set to 500MB, in order to minimize database resizing load on the database, and the Auto growth value to 100MB. Set the database LOG file to 100MB, growing by 10%.

Approximately 10 GB of storage should be allocated for the database and transaction logs. This is dependent upon usage, number of users and verbosity of logging. This is a guideline for a standard deployment and may charge according to usage patterns. Please monitor and review the available space and allow database growth to increase space as required.

The users do not connect directly to the SQL database server. Only the Silverback server will connect to the SQL database.

2.5. SMTP Server Requirements

Silverback will notify administrators about key events in the system if configured to do so. The SMTP Server details are required for alerts. The SMTP Server must allow anonymous relay within the company domain.

2.6. Active Directory Group Requirements

To allow users to access the Self Service Portal they must be a member of an Active Directory group. This group will be populated with all users that have received business approval to access their Exchange information from smartphone and tablet devices. Any users that have not been added to this group will not be able to provision a device using Silverback. This group can either be a Global or Universal group and can exist in any location within Active Directory. It is recommended to use a Global Security Group. This group must exist in the production Domain.

This feature is not required and can be disabled if desired.

2.7. SSL Certificate Requirements

Silverback Web Site Certificate

The Silverback solution utilises a device management protocol that requires an established trust relationship between the device and server. This allows the server to provision and manage your mobile fleet securely.

The Silverback web service requires one (1) certificate signed by a Certificate Authority trusted by the devices. The certificate must also match the DNS Name outlined in Section 2.2.

NOTE: If you are going to support Windows Phone 8 Enrollment it is strongly recommended you use a Wildcard (or SAN) SSL Certificate as this will save purchasing multiple SSL Certificates for the Silverback Website.

NOTE: If you are going to utilize Samsung UMC enrolment and have multiple email domains, a website must be setup on the Silverback Server matching the domain extension for that email. This website needs an SSL certificate trusted by the device, and must redirect to the Silverback main website.

A full list of iOS trusted Certificate Authorities is available at:
http://support.apple.com/kb/HT5012.

The Silverback Website Certificate is a core requirement for Silverback to function, please have the PFX/P12 Certificate Bundle available for installation.

2.8. Exchange ActiveSync Requirements

Silverback is used to manage deployment of Exchange ActiveSync client configurations. This document assumes Exchange ActiveSync is currently configured and is in a working state. The network requirements specified in this document assume this configuration is working correctly and any Exchange ActiveSync network requirements are not included.

2.9. Web Proxy Requirements

The Silverback MDM solution is web based and this must be taken into consideration if there are any corporate web proxies on the network. If your workforce uses a web proxy to browse the internet then they need to be configured to allow the Silverback solution to function effectively:

Ensure that each web browser (that has a proxy set) has an exclusion set for the Silverback server URL outlined in section “2.2 DNS Setup”.

- Configure each web proxy to allow traffic destined for the Silverback server to reach its destination unaltered.
- Ensure that any devices connected to Wi-Fi have access to the Apple push network via this proxy, as outlined in “2.1 User & Management Firewall Rules”.
- Ensure that any Android devices enrolled in Silverback are able to access GCM via this proxy, as outlined in “2.1 User & Management Firewall Rules”.

2.10. Google Settings for Android for Work

To utilise Android for Work, a Google Managed Domain is required and must be paired with Silverback. An API Service Account must also be created to help manage these settings.

For the configuration of this, refer to the document **Silverback by Matrix42 - Android for Work Enablement v3.1**

2.11. Windows Certificate Enrolment

Silverback is also capable of enrolling user certificates for devices from an Enterprise Certificate Authority. For detailed information on this see the document titled **Silverback by Matrix42 - Microsoft CA Integration for WP8-V1.1**

2.12. SAMSUNG KNOX

If you wish to manage Samsung KNOX settings for your devices, licenses for this must be purchased through Samsung and entered into the Silverback Admin Console. For information on obtaining licenses for KNOX, please visit:

https://www.samsungknox.com/en/solutions/knox-workspace.