MATRIX42
SMARTER WORKSPACE – BETTER LIFE

Silverback by Matrix42

Installation Guide Version 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. Introduction 5
1.1. Overview 5
2. Preparation 6
2.1. System Requirements 6
2.2. Software Prerequisites 6
2.3. Environmental Requirements 9
2.4. Firewall Requirements 9
2.5. DNS Requirements 10
2.6. SSL Certificate Requirements 10
2.7. Windows Certificate Enrolment 11
2.8. Samsung KNOX and UMC Enrolment 11
2.9. Google Settings for Android for Work 11
3. Installation and Configuration 12
3.1. Overview 12
3.2. Step 1: Certificates 12
3.2.1. Generate Certificates 12
3.2.2. Install Certificates and Set Permissions 13
3.2.3. Record Certificate Thumbprints 13
3.3. Step 2: SQL Configuration 14
3.3.1. Automated SQL Setup 14
3.3.2. Manual SQL Setup 14
3.3.3. Configure Permissions 14
3.4. Step 3: Silverback Installation 15
3.4.1. Launch the Installer 15
3.4.2. Prerequisites Check 15
3.4.3. License Agreement 17
3.4.4. Customer Information 18
3.4.5. Installation Location 19
3.4.6. Choose Installation Type 20
3.4.7. Confirm Installation is ready 21
3.4.8. Wait for Installation 22
3.4.9. Launch Admin Console 23
3.4.10. Database Connection Settings 24
3.4.11. Database Setup 26
3.4.12. Cloud Connector Setup 26
3.5. Step 4: Post-Installation System Setup and Configuration 27
3.5.1. Configure IIS Bindings 27
3.5.2. Login 29
3.5.3. Enter license 29

Inhaltsverzeichnis

3.5.4. Change the default admin password 29
3.5.5. Create Settings Admin Account 30
3.5.6. Configure the Base System Settings 30
4. Installation Verification and More Information 32
4.1. Installation Verification 32
4.2. Additional Settings 32
4.3. Further Reading 32
4.3.1. Best Practice Documentation 32
5. Appendix A – Cloud Connector Setup 33
5.1. Certificate Generation 33
5.1.1. Install Certificates and Set Permissions for the server 34
5.1.2. Record Certificate Thumbprint for the server 34
5.1.3. Install Certificates and Set Permissions for the Cloud Connector 35
5.1.4. Record Certificate Thumbprint for the client 35
5.1.5. Run the Client Setup 36
5.1.6. Welcome Prompt 36
5.1.7. Select Install Location 37
5.1.8. Enter the number of clients 38
5.1.9. Confirm Installation 39
5.1.10. Wait for Installation to Complete 40
5.1.11. Complete Installation 41
5.1.12. Extract Cloud Connector Configuration Generator Files 42
5.1.13. Launch the Configuration Generator 43
5.1.14. Configure the Individual Cloud Connector Clients 44
5.1.15. Configure the server side 45
5.1.16. Start the Cloud Connector Services 46
6. Appendix B – Example Region Format Screenshots 47

Installation Guide Version 5.1 U3

1. Introduction

1.1. Overview

This document will guide you through a typical installation of Silverback by Matrix42 and offer guidance on configuring the system for a successful deployment.

Included is a Preparation section, which will show you the prerequisites for an installation of Silverback.

This guide will show a common setup, but every environment is different! For advanced configuration or special requirements, talk to your technical contact or raise a support ticket to cover your needs.

2. Preparation

2.1. System Requirements

Silverback generally requires the following for the Silverback server itself:

- 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”

See Appendix B for example screenshots

The SQL Server used to host the database, requires:

- 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

2.2. Software Prerequisites

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

Installation Guide Version 5.1 U3

- .NET 4.0
- .NET 4.5
- .NET 4.5.1 (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

Installation Guide Version 5.1 U3

- ☐ FTP Server (Not installed)
- ☐ Management Tools
  - ☑ 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)

Author: Matrix42 Cloud & Mobile Management

2.3. Environmental Requirements

For normal configuration, Silverback requires the following environmental items. These may or may not apply to your deployment:

- Service Account with READ access to your Active Directory Environment – This is used to perform lookups for new users and group alignment if used.
- The Silverback server itself or another account to have 'Database Owner' to the Silverback database
- If using Exchange Quarantine features, the Silverback server must have the following permissions in Active Directory so it can properly manage the Exchange Quarantine list:
  - Organization Management
  - Server Management
  - Exchange Recipient Management

2.4. Firewall Requirements

As Silverback connects to many external systems, such as Apple for push management to devices, you need to ensure that the following connectivity items are configured:

Traffic Source	Destination	Port/Protocol
Devices (External)	Silverback	443/tcp
Silverback	SQL Server	1433/tcp
Silverback	Domain Controller	389,636/tcp
Silverback	SMTP Server	25/tcp
Silverback	Exchange Server (quarantine)	443/tcp
Silverback	Gateway.push.apple.com, mdmenrollment.apple.com, vpp.itunes.apple.com	2195/tcp 443/tcp
Silverback	Itunes.apple.com	80, 443/tcp
Silverback	Android.googleapis.com	443/tcp
Silverback	Microsoft Push Network	443/tcp
Silverback	api.aerialink.net, sms.silverbackmdm.com rest.messagebird.com	443/tcp

2.5. DNS Requirements

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.

2.6. SSL Certificate Requirements

Communication between Silverback and your devices is done via HTTPS communication. As such the server should have SSL Certificates configured for the appropriate DNS entries that are trusted by the devices. If the devices don’t trust the SSL Certificate provided by the server, then communication may not work. We recommend purchasing a “wildcard” or SAN SSL Certificate; this ensures that if you are using Windows devices, the “enterpriseenrollment.yourdomainname.com” entry can use the same certificate.

2.7. 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**

2.8. Samsung KNOX and UMC Enrolment

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.

2.9. 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**

3. Installation and Configuration

3.1. Overview

Before beginning the installation, ensure that you've confirmed all the items in Section 2. Preparation and that you have the following available:

- Silverback Installation Files
- Silverback License

3.2. Step 1: Certificates

3.2.1. Generate Certificates

As part of normal operation in a standard configuration, Silverback will generate certificates for devices on it's own Certificate Authority. For security, we need to ensure that no two environments use the same certificate. Because of this, it's necessary to create a Certificate Authority specifically for your server.

To create the Root Certificate Authority:

1 Launch IIS Manager from the Start Menu
2 From the Connections Panel on the left, select the Default Server
3 From the Features Panel in the middle, double click on Server Certificates
4 From the Actions Panel on the right, click Create Self-Signed Certificate
5 Enter a descriptive name for the certificate, for example Silverback Root CA
6 Click OK
7 In the Server Certificates panel, you will now see the new certificate, Right click this and click Export
8 Specify a file location for the export and enter a password to protect the private key
9 Click OK

If you are configuring the Cloud Connector, an additional certificate is required, see Appendix A

3.2.2. Install Certificates and Set Permissions

To ensure the Silverback Services can access the certificates, you need to ensure they are in the correct certificate store and the permissions are set correctly. You should also perform the steps below for the Web Server Certificate, so that this can be used by the Silverback Website in IIS, and also by Silverback to sign certificates.

To Import the certificate:

1 Press Windows Key + R to launch the Run prompt
2 Enter “mmc” and press Ok
3 From the MMC Screen, Select File then Add/Remove Snap-In
4 From the Available span-ins panel, Select Certificates and click Add
5 From the following prompt, select Computer account and click Next
6 Leave Local computer selected and click Next
7 From the following screen, expand out Certificates (Local Computer), then Personal
8 Right Click on the Certificates folder, then select All Tasks, then select Import
9 Navigate to and select the certificate from step 3.2.1, you may need to change the file filter on the right to display .pfx files, Click Open
10 Click Next
11 Enter the password you specified, ensure that the private key is marked as Exportable and click Next
12 Ensure Personal is set at the Certificate Store, and click Next
13 Click Finish and Confirm the Success Prompt

To set permissions on the certificate:

1 In the MMC Screen, right click the newly imported certificate, then select All Tasks, Manage Private Keys
2 From the Permissions window, Click Add
3 Enter “NETWORK SERVICE” and Click Check Names to Confirm
4 Click OK
5 Ensure NETWORK SERVICE has Full Control and Read Allowed
6 Click Apply

3.2.3. Record Certificate Thumbprints

To record the certificate thumbprint for use later in configuration:

1 Double-Click the certificate in the MMC Window
2 From the popup, select the Details Tab
3 Scroll down until you see Thumbprint and select this
4 Copy the text for the thumbprint and note this value, as this is needed later for configuration

3.3. Step 2: SQL Configuration

3.3.1. Automated SQL Setup

Silverback will attempt to configure its database automatically after the installer has run. To perform this action, Silverback needs the db_creator role on the SQL server.

Make sure either the computer you are running the installation on has the db_creator role in SQL, or if you are using SQL Authentication make sure the SQL user you use has the db_creator role.

3.3.2. Manual SQL Setup

3.3.2.1. Set SQL Command Mode

To execute the Silverback Database Script, SQL Command Mode is required:

1 Open the Microsoft SQL Server Management Studio

2 Click New Query

3 Click the **Query Menu**

4 Click SQL Command Mode

3.3.2.2. Prepare SQL Script

After SQL Command Mode is set, paste in the contents of the Silverback SQL Script in the New Query Window and confirm in the script the following items:

- **Database Name** This will be the name of the Silverback database.
- **Data File Location** This is where the database files for Silverback will be stored. This location must exist for the script to execute successfully
- **Compatibility Level Default** By Default, the database will be set to SQL 2008 Compatibility Mode (100: is SQL 2008 and 2008 R2) currently this is the only supported compatibility mode.

3.3.2.3. Execute SQL Script

After verifying the above, click **Execute** to run the script. Monitor the script output to ensure this executes successfully.

The database should now be created, and you can proceed to set permissions on the database to ensure Silverback has the necessary access permissions.

3.3.3. Configure Permissions

For a deployment where SQL is located on the same server as Silverback (this is only recommended for small deployments with under 20 users, or test environments as SQL will compete with IIS for system resources):

- SYSTEM account must be given the db_owner role on the database
- NETWORK SERVICE account must be given the db_owner role on the database

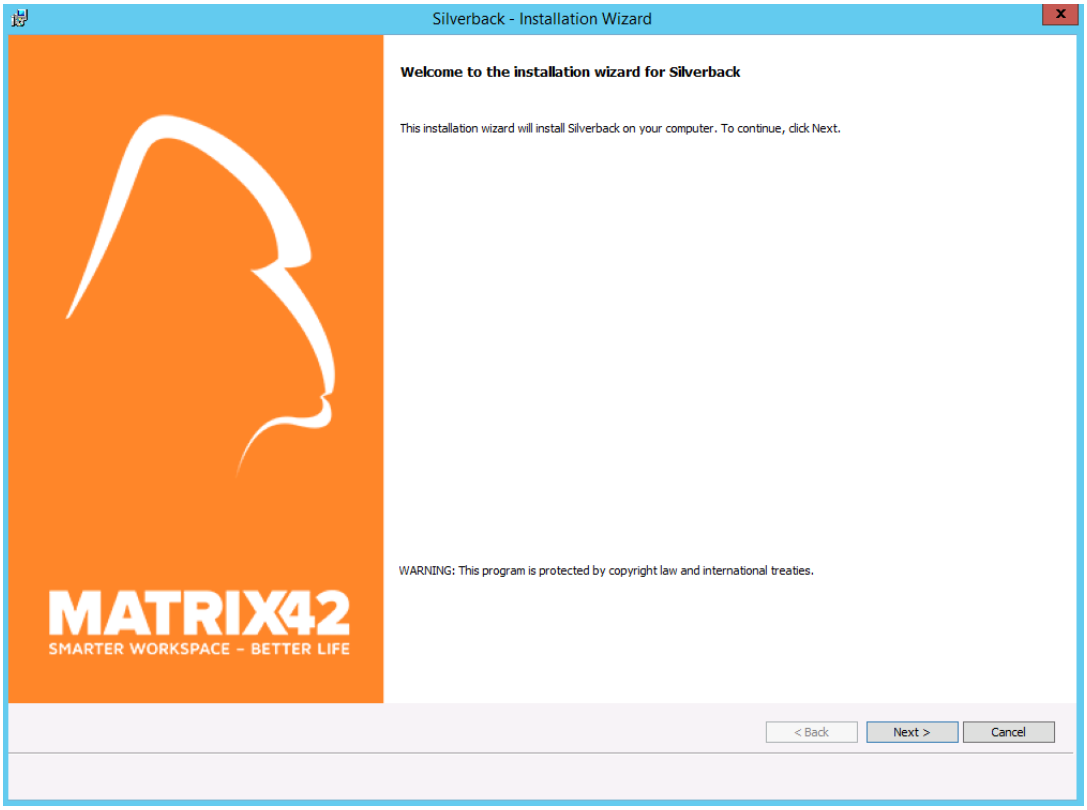
For a deployment where SQL is located on a separate, dedicated SQL Server you can either:

- Create a SQL User Account, assign this the db_owner role on the database
- If the servers are in a domain, permission can be delegated to the Silverback server by creating adding the Silverback server as a user in SQL, then assigning the server the db_owner role

3.4. Step 3: Silverback Installation

3.4.1. Launch the Installer

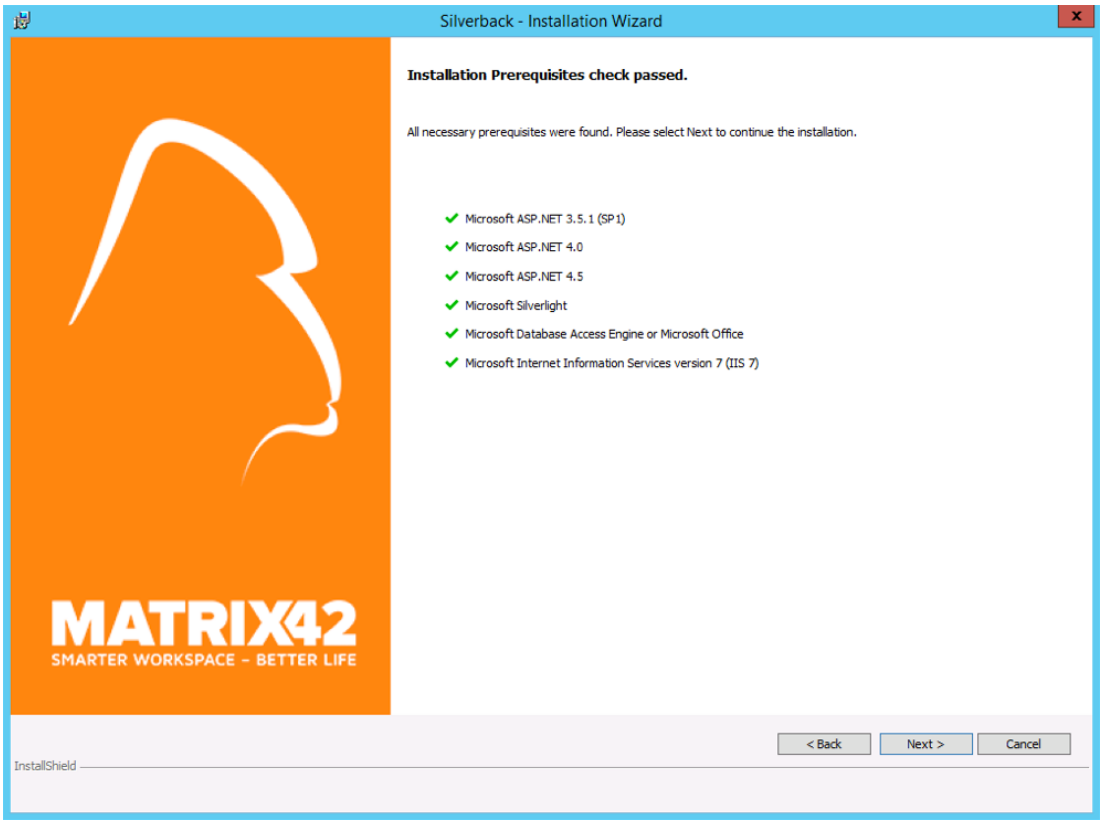
Launch the installer executable, and click Next to begin.



3.4.2. Prerequisites Check

Ensure all prerequisites are installed and configured and click Next

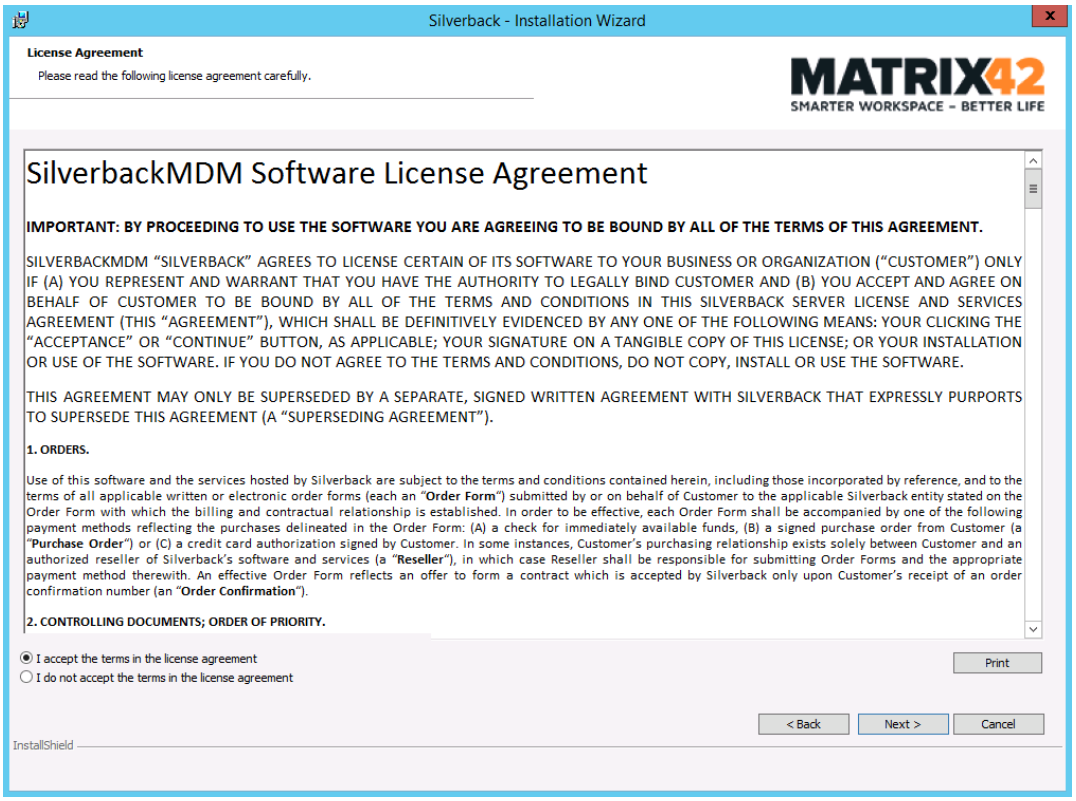
Installation Guide Version 5.1 U3



Author: Matrix42 Cloud & Mobile Management

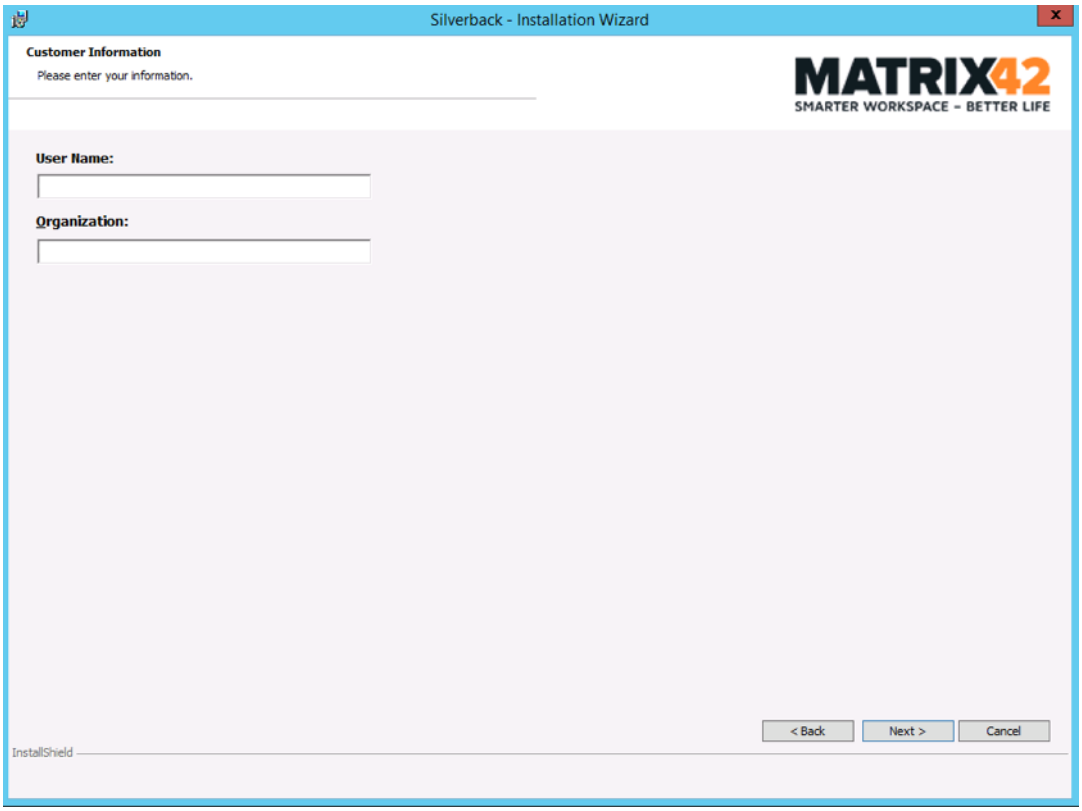
3.4.3. License Agreement

Carefully read the license agreement. If you accept the terms, select „I accept the terms in the agreement“ and press Next to continue. You can also print the agreement if needed for documentation.



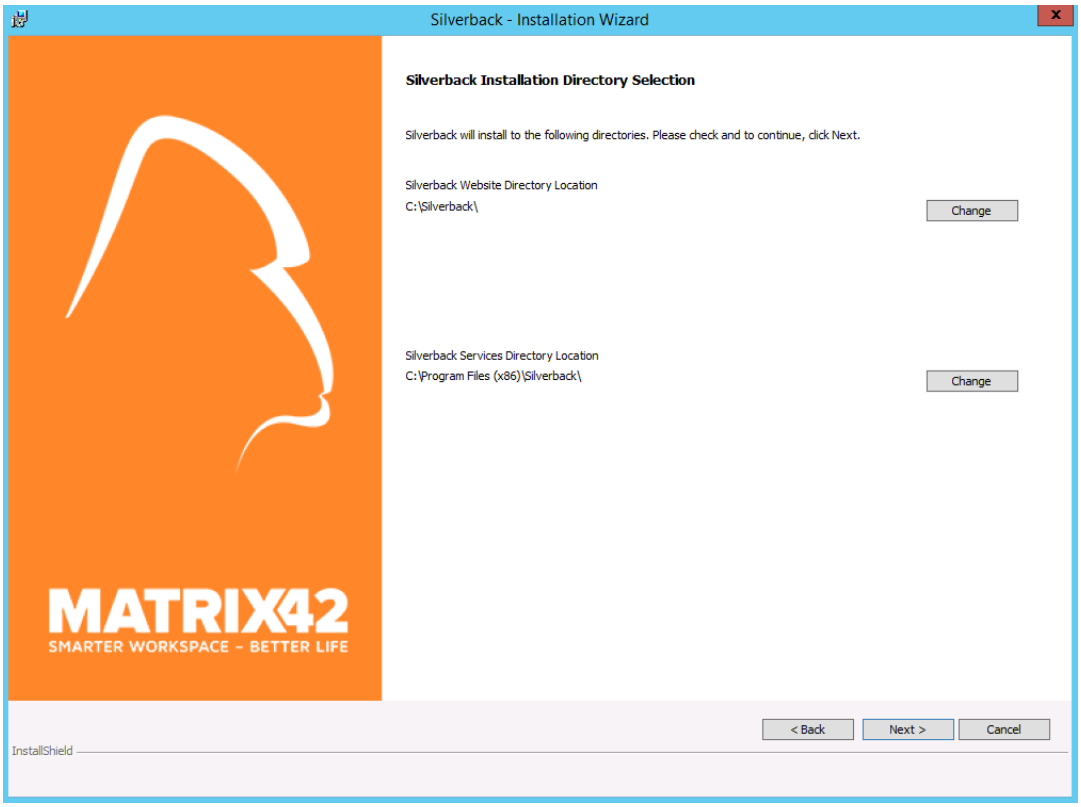
3.4.4. Customer Information

Enter a username and organisation name for auditing purposes. This information is stored with Windows to track the installation, this information is only stored locally and is not sent anywhere.



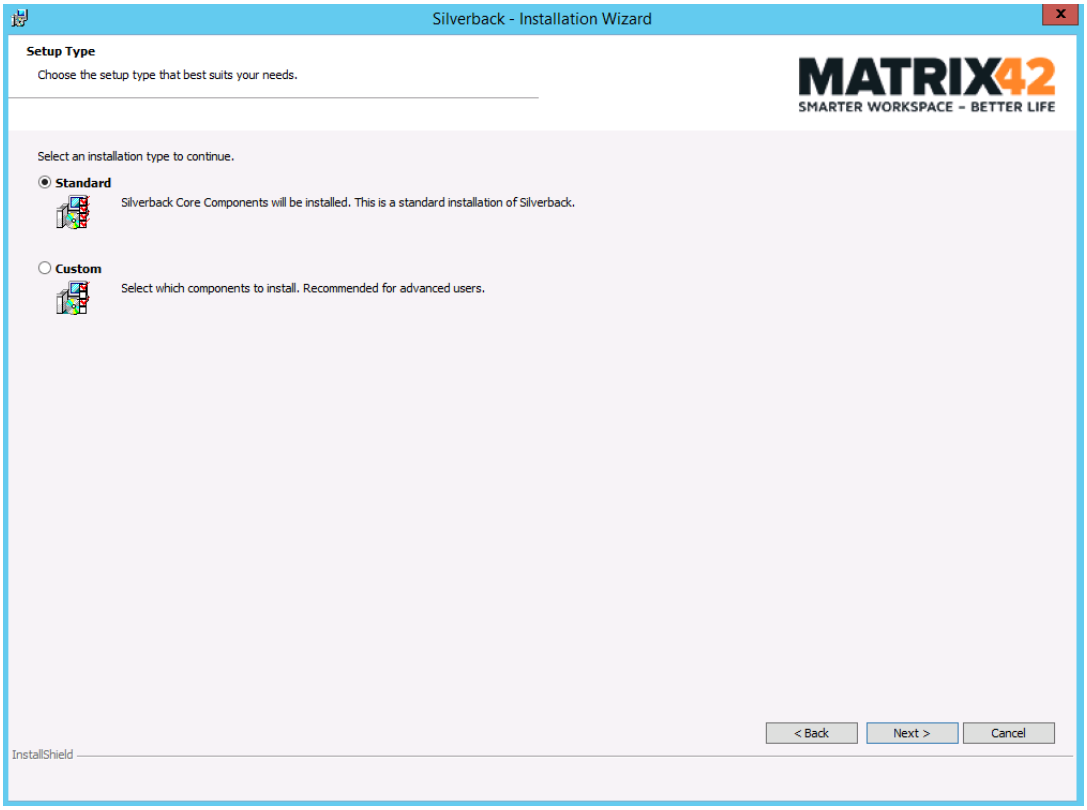
3.4.5. Installation Location

Enter the location for the Silverback Website files and the Services install location. The website location must be accessible by IIS as this is where IIS will host the web site and applications from.



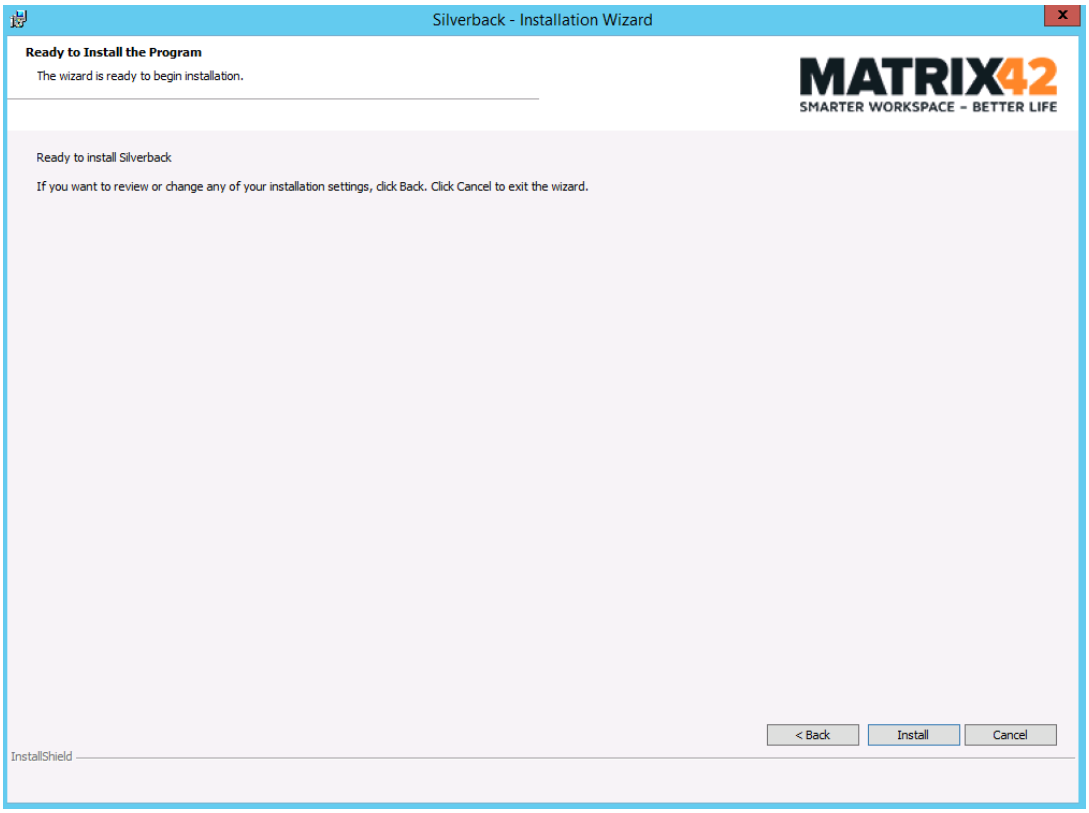
3.4.6. Choose Installation Type

Select Standard and click Next



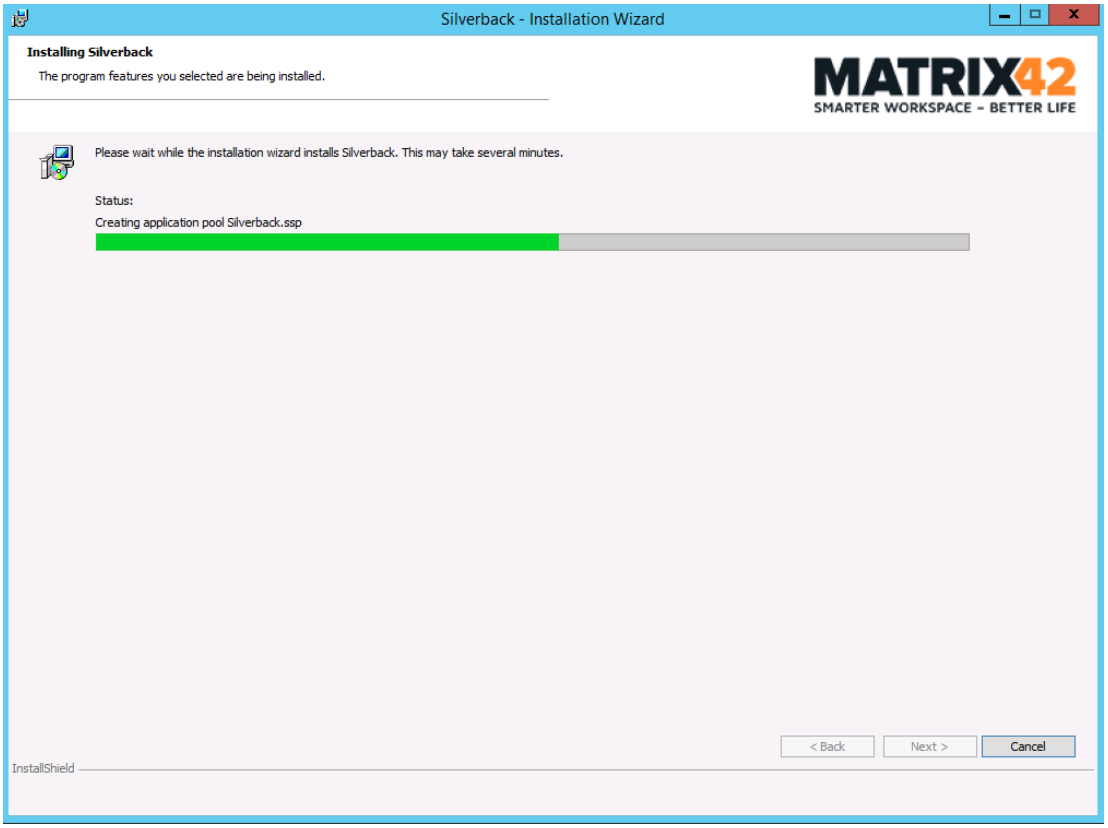
3.4.7. Confirm Installation is ready

If you are done configuring the aspects of the installation, click Install



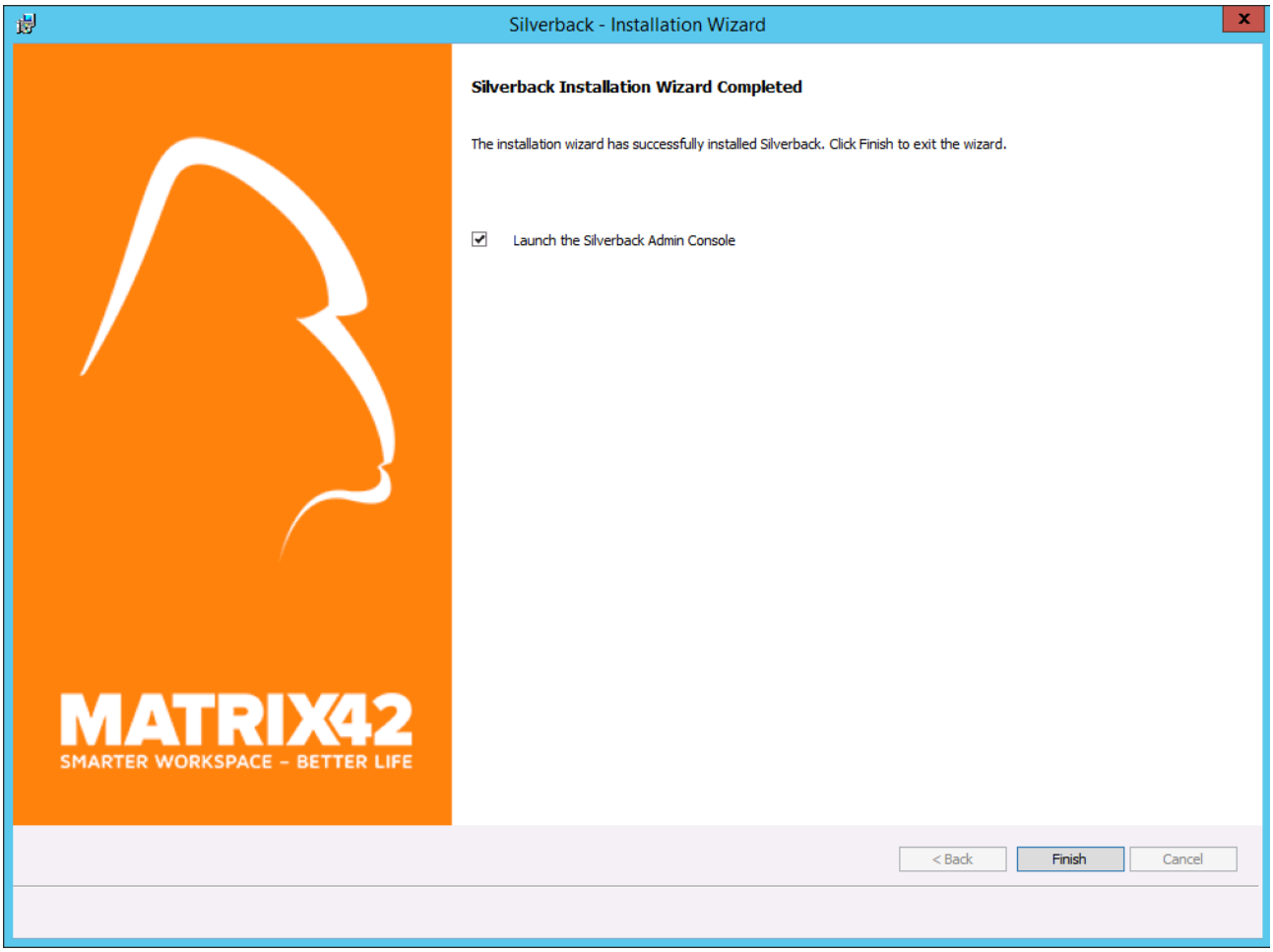
3.4.8. Wait for Installation

When the installation is finished, the Next button will become activate. Click this to continue.



3.4.9. Launch Admin Console

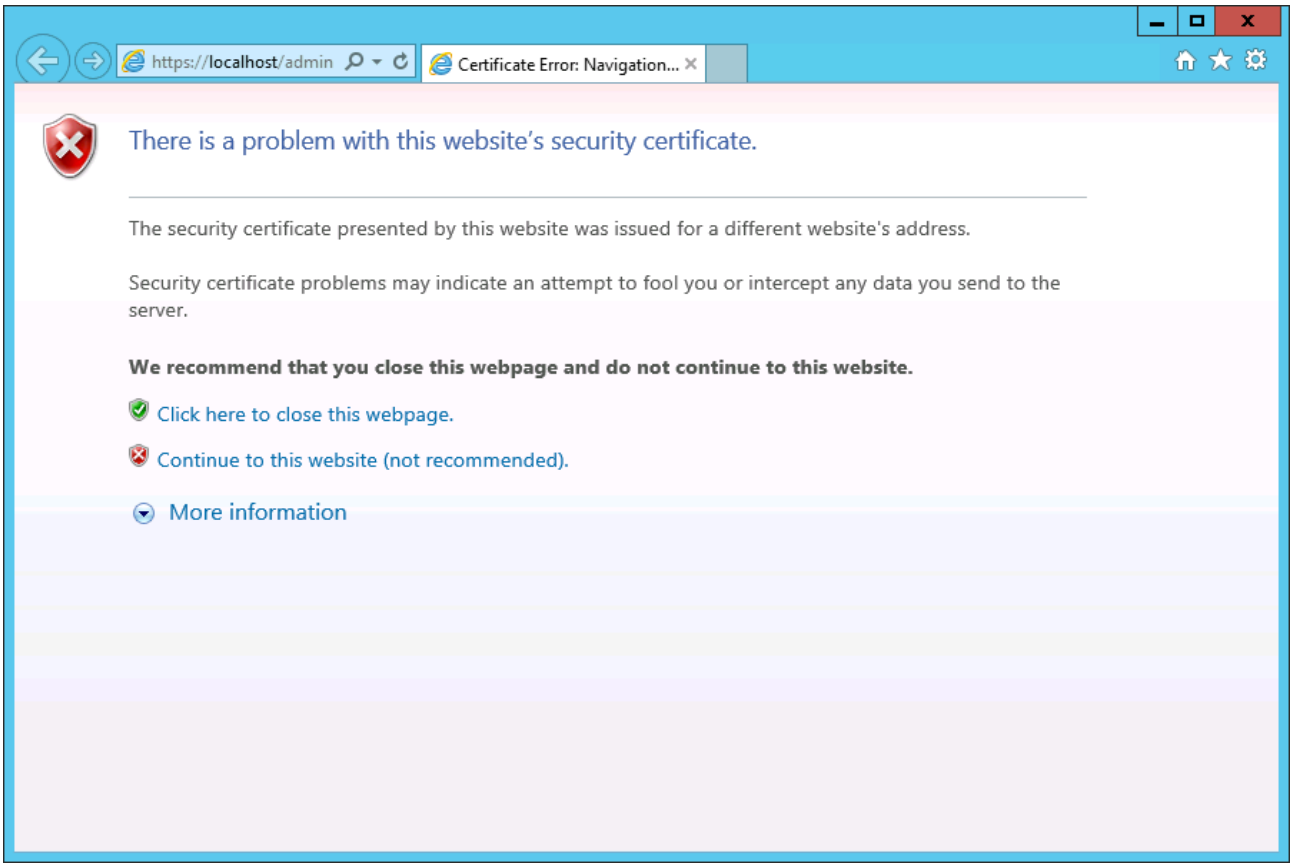
Silverback must be configured to connect to your database, so ensure you check „Launch the Silverback Admin Console“ and click Finish.



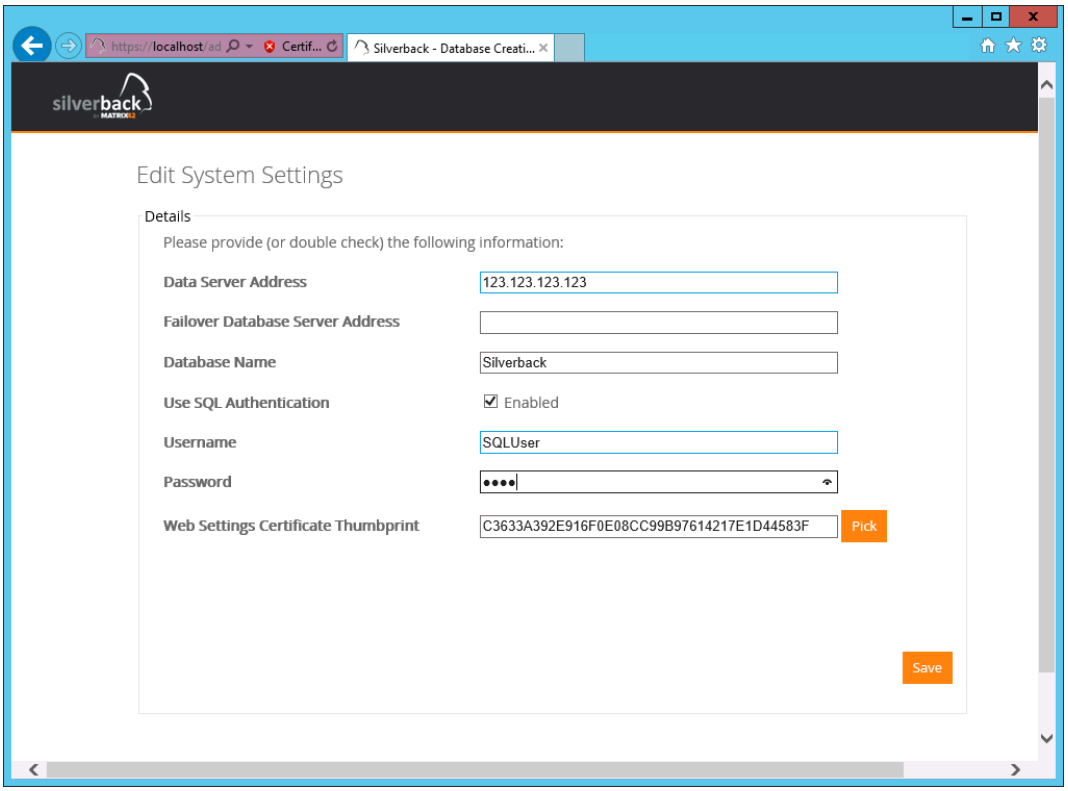
3.4.10. Database Connection Settings

Silverback must be configured to connect to your database, and some additional settings need to be configured. When you first load the admin console, if these are not configured you will be prompted to configure them.

First, accept the certificate warning.



Then you should see the database connection settings. Note that if you enter a database that doesn't exist, Silverback will attempt to create this.



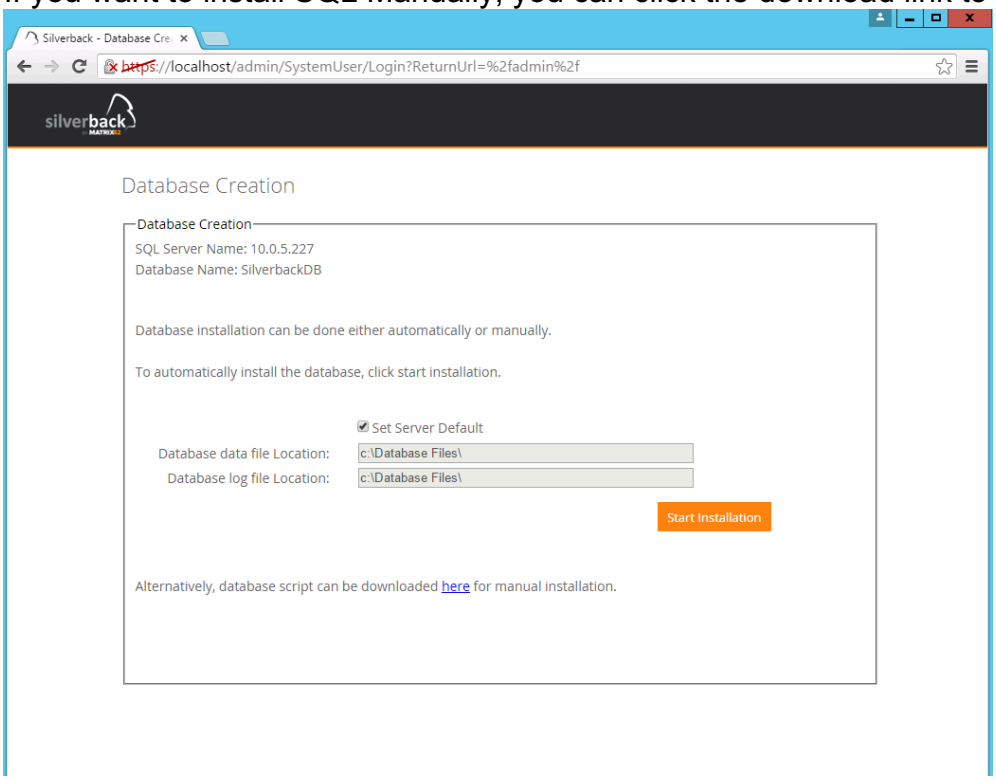
The settings that can be configured are:

Setting	Description	Mandatory
Data Server Address	Network location of the SQL Server	Yes
Failover Database Server Address	If using, an optional SQL server that will be used if the primary is not available	
Database Name	Database name that Silverback will use	Yes
Use SQL Authentication	By default, Silverback will use Windows permissions to access the SQL Server. If you want to use SQL Authentication you can check this, and you will be required to enter a username and password	
Web Settings Certificate Thumbprint	Silverback encrypts settings using this certificate. The installer will automatically generate this for you. Note that if this field is empty after a fresh install, this means that an encryption certificate already exists so the installer didn't create one. Most likely from a previous installation. You can choose an existing certificate by clicking "Pick" and then choosing the certificate.	Yes

3.4.11. Database Setup

After the connection information is entered, the database needs to be prepared. Click Start Installation and wait for it to complete.

If you want to install SQL Manually, you can click the download link to get the SQL Scripts.



3.4.12. Cloud Connector Setup

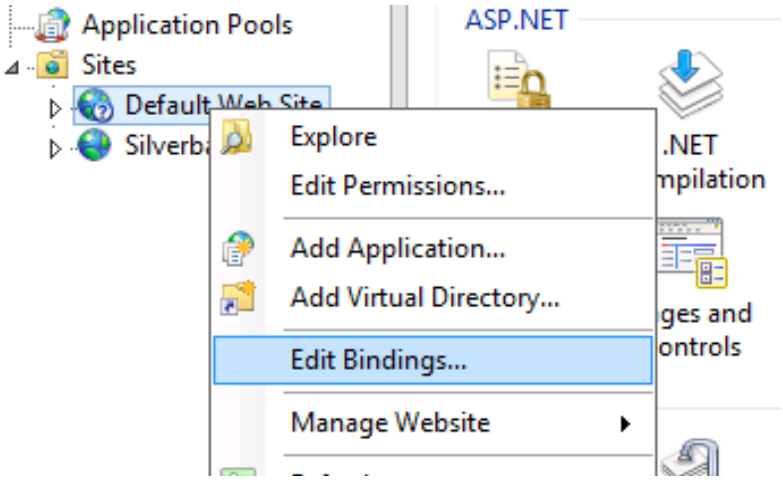
If you will be utilising the Cloud Connector, please reference Appendix A

3.5. Step 4: Post-Installation System Setup and Configuration

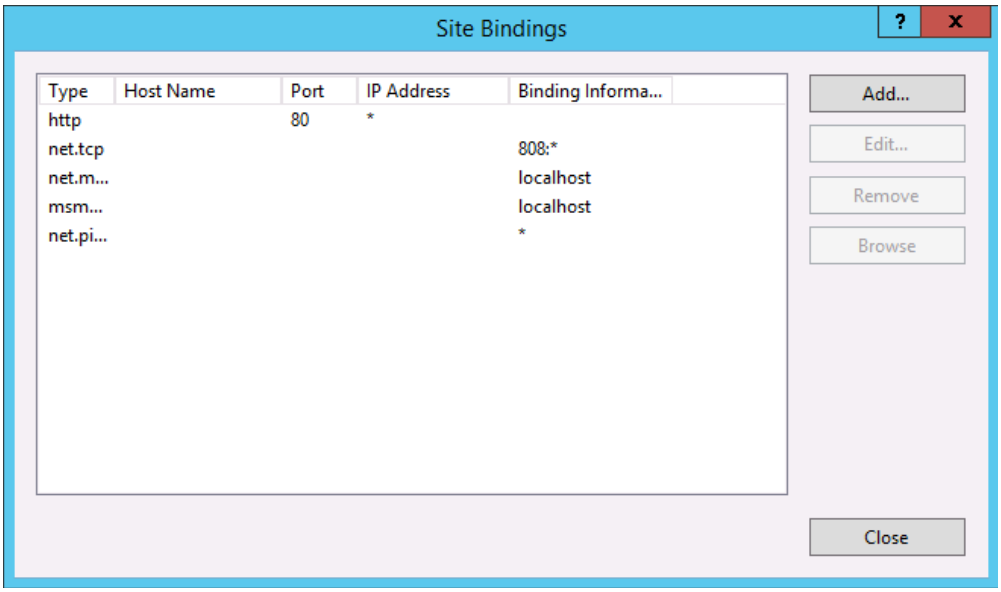
3.5.1. Configure IIS Bindings

To have the system running securely, you need to ensure that Silverback will only listen for traffic on HTTPS/TCP, and not plain text HTTP traffic. Launch IIS Manager and perform the following.

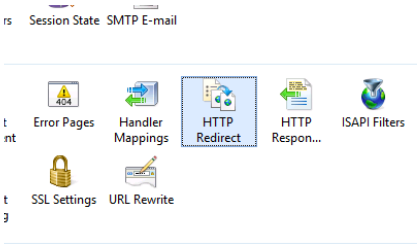
1 Right click on the Default Website item and select Edit Bindings



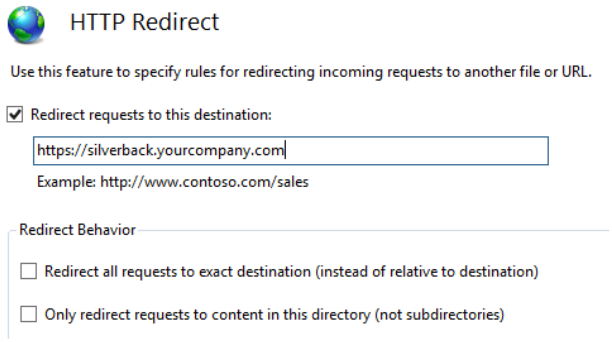
2 Ensure that there are no https entries for port 443. If there are, select and remove them



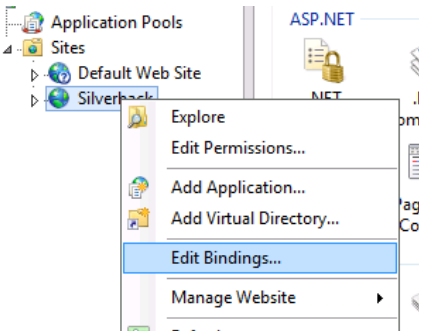
3 Open the HTTP Redirect Feature



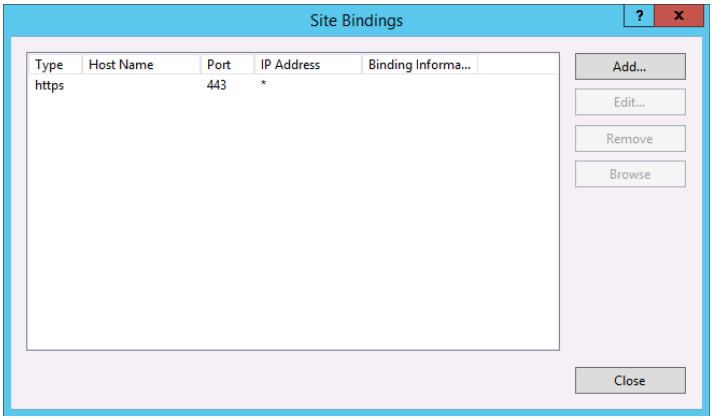
4 Enter your server address, but ensure you use https. For example https://silverback.yourcompany.com (replacing silverback.yourcompany.com with your server address). Also ensure that both checkboxes beneath this are **unchecked.**



5 Right click on the Silverback Website item, and select Edit Bindings



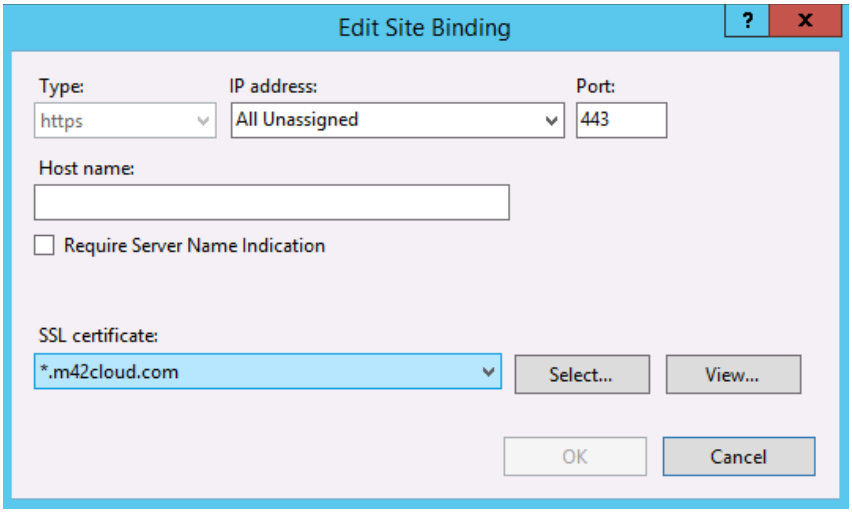
6 Ensure that there is only an entry for https and not http on port 80.



7 Select the https entry and click Edit…

8 Select the SSL Certificate you wish to use to present to your devices. This SSL Certificate must be issued by a trusted certificate authority and installed on your server before it will show in this list. Host name should be left empty, as you will need to

access the server on https://localhost to complete the installation. If a hostname needs to be specified, ensure that localhost is entered as well.



3.5.2. Login

After installation and IIS configuration, some additional Silverback configuration is required, firstly:

1 Navigate to the server address configured during installation, with /admin appended to the url, e.g. silverback.yourcompanyname.com/admin
2 Enter the default username: admin
3 Enter the default password: S1lverb@ck

3.5.3. Enter license

After logging in you will be prompted to enter the Silverback license to activate the system. Paste the key into the text box and confirm.

3.5.4. Change the default admin password

Change the default password by:

1 Clicking on the settings icon
2 Enter the current password in the Old Password field
3 Enter your new password in the New Password and Confirm New Password fields
4 Click Save

It's very important this new password is remembered, as this is the default admin account for the system. Unless you make further admin accounts, this is the only admin account.

3.5.5. Create Settings Admin Account

In order to configure the Silverback System Settings, a special account is required. To create this account:

1 Navigate to the Admin Tab
2 Navigate to the User Management Section
3 Click New System User
4 Populate the Username, Email, Password and Confirm Password fields
5 Select Settings Administrator for the Role field
6 Click the Save button.

3.5.6. Configure the Base System Settings

The Settings Administrator Role is a special role, and is the only role that can access the System Settings page. If you are currently logged in with another account, click Log Out from the top right, and then login with the newly created Settings Administrator account.

There are several critical things that must be configured before the Silverback Server can be fully operational.

3.5.6.1. Configure the General Tab

In the General Tab of the settings page, the following settings should be configured:

Setting Name	Description
Certificate Thumbprint	This should match the thumbprint that you configured in Step 1 of Installation and Configuration. This certificate is used to create the client certificates for Silverback clients to use for enrolment and other services.
Country, Organisation and Location	These are used in the certificates that are generated for devices as information only to identify the issuer of the certificates
Expiry Length	The certificates issued to clients will expire after this time period. Ideally this should be as long as possible to prevent the need for certificates to be renewed.
Email Domain	This should match the domain your company uses for primary email addresses.
System URLS: Admin, SSP, EPiC, Activation, Sharepoint	These should be edited to match the Silverback Server address. It's important to retain the trailing extension, e.g. /admin

3.5.6.2. Configure the MDM Tab

In he MDM Payload Tab, the following need to be configured:

Setting Name	Description
System URLS: Checkin, MDM	These should be edited to match the Silverback Server address. It's important to retain the trailing extension, e.g. /mdm
Signing Certificate Thumbprint	This certificate is used to sign profiles being sent to iOS devices. It's recommended to use the SSL Certificate for the Silverback website, as this will be trusted by the devices.

3.5.6.3. Configure the App Portal and SMS Tab

In the App Portal and SMS Payload Tab, the following need to be configured:

Setting Name	Description
System URL	This should be edited to match the Silverback Server address. It's important to retain the trailing extension, e.g. /apps
SMS Provider	For Australian customers, this should be RedCoal, for the rest of the world, select Aeriallink V4 or MessageBird

4. Installation Verification and More Information

4.1. Installation Verification

To verify that your installation functions as expected. Follow the following document:
Matrix42 Silverback Quick Start Guide for iOS v02d-OKL.pdf

4.2. Additional Settings

For reference on the features and settings new to this version of Silverback by Matrix42, refer to the Release Notes: **Silverback by Matrix42 5.0 U2 Release Notes.pdf**

For reference on the entire console and function of Silverback by Matrix42, refer to the Admin Guide: **Silverback by Matrix42 Admin Guide v5.0 U2.pdf**

4.3. Further Reading

4.3.1. Best Practice Documentation

Best Practice - Apple Enterprise Developer Requirements - Jan2014.pdf

Best Practice - Google GCM Requirements - Jan2014.pdf

Best Practice - User Authentication for AD.pdf

Silverback by Matrix42 Windows 8.1 App Management 4.8.pdf

Silverback by Matrix42 Windows 8.1 Certificate Enrolment 4.8.pdf

5. Appendix A – Cloud Connector Setup

5.1. Certificate Generation

To generate the certificate for the Cloud Connector, the process is the same as generating the Silverback Root CA Certificate. The cloud connector requires two public/private key-pairs, one for the server and one for the Cloud Connector Client

To create the Cloud Connector Client Certificate:

1 Launch IIS Manager from the Start Menu
2 From the Connections Panel on the left, select the Default Server
3 From the Features Panel in the middle, double click on Server Certificates
4 From the Actions Panel on the right, click Create Self-Signed Certificate
5 Enter a descriptive name for the certificate, for example Silverback Cloud Connector
6 Click OK
7 In the Server Certificates panel, you will now see the new certificate, Right click this and click Export
8 Specify a file location for the export and enter a password to protect the private key
9 Click OK

To create the Cloud Connector Server Certificate:

1 Launch IIS Manager from the Start Menu
2 From the Connections Panel on the left, select the Default Server
3 From the Features Panel in the middle, double click on Server Certificates
4 From the Actions Panel on the right, click Create Self-Signed Certificate
5 Enter a descriptive name for the certificate, for example Silverback Cloud Connector Server
6 Click OK
7 In the Server Certificates panel, you will now see the new certificate, Right click this and click Export
8 Specify a file location for the export and enter a password to protect the private key
9 Click OK

5.1.1. Install Certificates and Set Permissions for the server

To ensure the Silverback Services can access the certificate, you need to ensure it is in the correct certificate store and the permissions are set correctly.

To Import the certificate (Server Side):

1 Press Windows Key + R to launch the Run prompt
2 Enter “mmc” and press Ok
3 From the MMC Screen, Select File then Add/Remove Snap-In
4 From the Available span-ins panel, Select Certificates and click Add
5 From the following prompt, select Computer account and click Next
6 Leave Local computer selected and click Next
7 From the following screen, expand out Certificates (Local Computer), then Personal
8 Right Click on the Certificates folder, then select All Tasks, then select Import
9 Navigate to and select the certificate for Cloud Connector Server, you may need to set the filter on the right to display .pfx files, Click Open
10 Click Next
11 Enter the password you specified, ensure that the private key is marked as Exportable and click Next
12 Ensure Personal is set at the Certificate Store, and click Next
13 Click Finish and Confirm the Success Prompt

To set permissions on the certificate:

1 In the MMC Screen, right click the newly imported certificate, then select All Tasks, Manage Private Keys
2 From the Permissions window, Click Add
3 Enter “NETWORK SERVICE” and Click Check Names to Confirm
4 Click OK
5 Ensure NETWORK SERVICE has Full Control and Read Allowed
6 Click Apply

5.1.2. Record Certificate Thumbprint for the server

To record the certificate thumbprint for use later in configuration:

7 Double-Click the certificate in the MMC Window
8 From the popup, select the Details Tab
9 Scroll down until you see Thumbprint and select this
10 Copy the text for the thumbprint and note this value, as this is needed later for configuration

5.1.3. Install Certificates and Set Permissions for the Cloud Connector

To ensure the Cloud Connector can access the certificate, you need to ensure it is in the correct certificate store and the permissions are set correctly.

To Import the certificate (Server Side):

11 Press Windows Key + R to launch the Run prompt

12 Enter “mmc” and press Ok

13 From the MMC Screen, Select File then Add/Remove Snap-In

14 From the Available span-ins panel, Select Certificates and click Add

15 From the following prompt, select Computer account and click Next

16 Leave Local computer selected and click Next

17 From the following screen, expand out Certificates (Local Computer), then Personal

18 Right Click on the Certificates folder, then select All Tasks, then select Import

19 Navigate to and select the certificate for Cloud Connector Client, you may need to set the filter on the right to display .pfx files, Click Open

20 Click Next

21 Enter the password you specified, ensure that the private key is marked as Exportable and click Next

22 Ensure Personal is set at the Certificate Store, and click Next

23 Click Finish and Confirm the Success Prompt

To set permissions on the certificate:

24 In the MMC Screen, right click the newly imported certificate, then select All Tasks, Manage Private Keys

25 From the Permissions window, Click Add

26 Enter “NETWORK SERVICE” and Click Check Names to Confirm

27 Click OK

28 Ensure NETWORK SERVICE has Full Control and Read Allowed

29 Click Apply

5.1.4. Record Certificate Thumbprint for the client

To record the certificate thumbprint for use later in configuration:

30 Double-Click the certificate in the MMC Window

31 From the popup, select the Details Tab

32 Scroll down until you see Thumbprint and select this

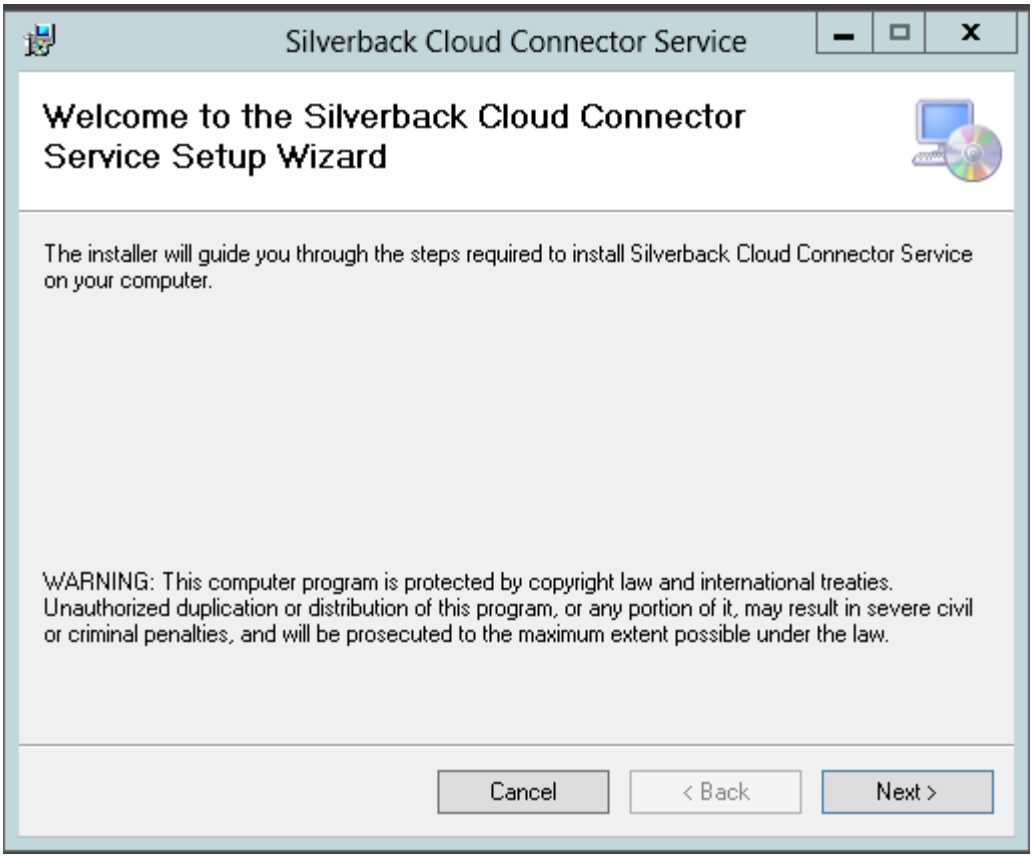
33 Copy the text for the thumbprint and note this value, as this is needed later for configuration

5.1.5. Run the Client Setup

Launch the setup for the Cloud Connector on the server in your environment and follow the prompts:

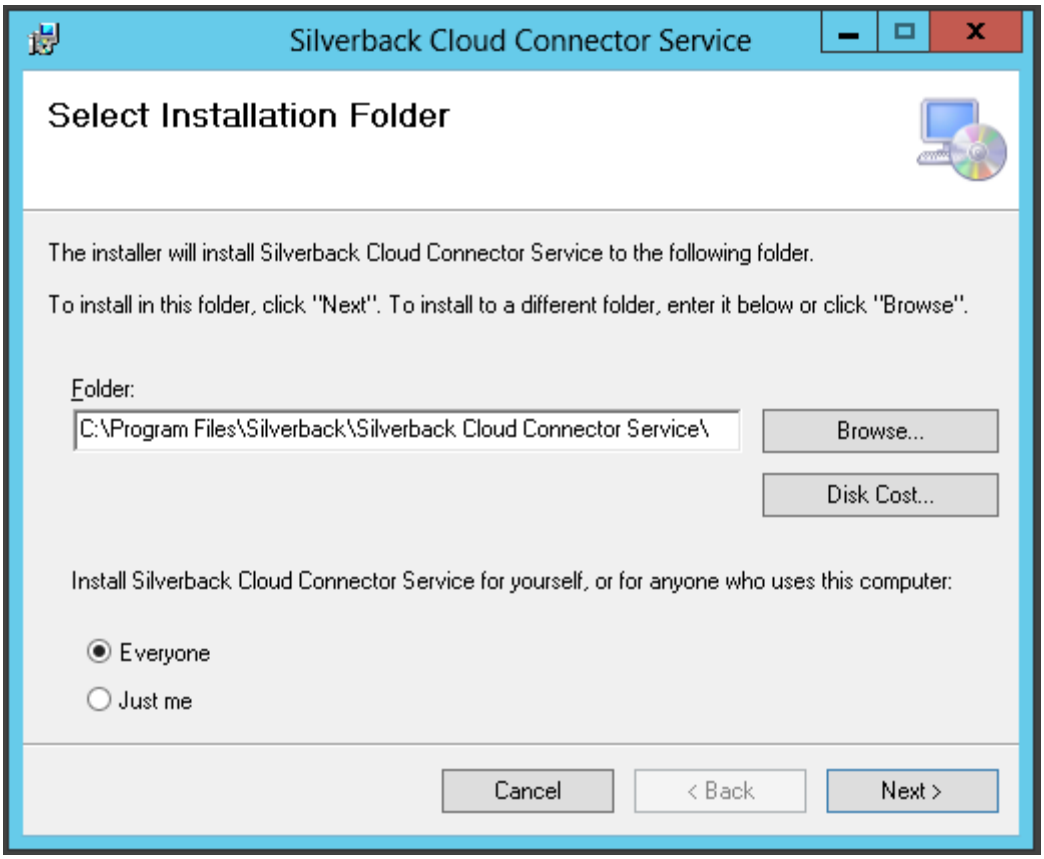
5.1.6. Welcome Prompt

Click Next



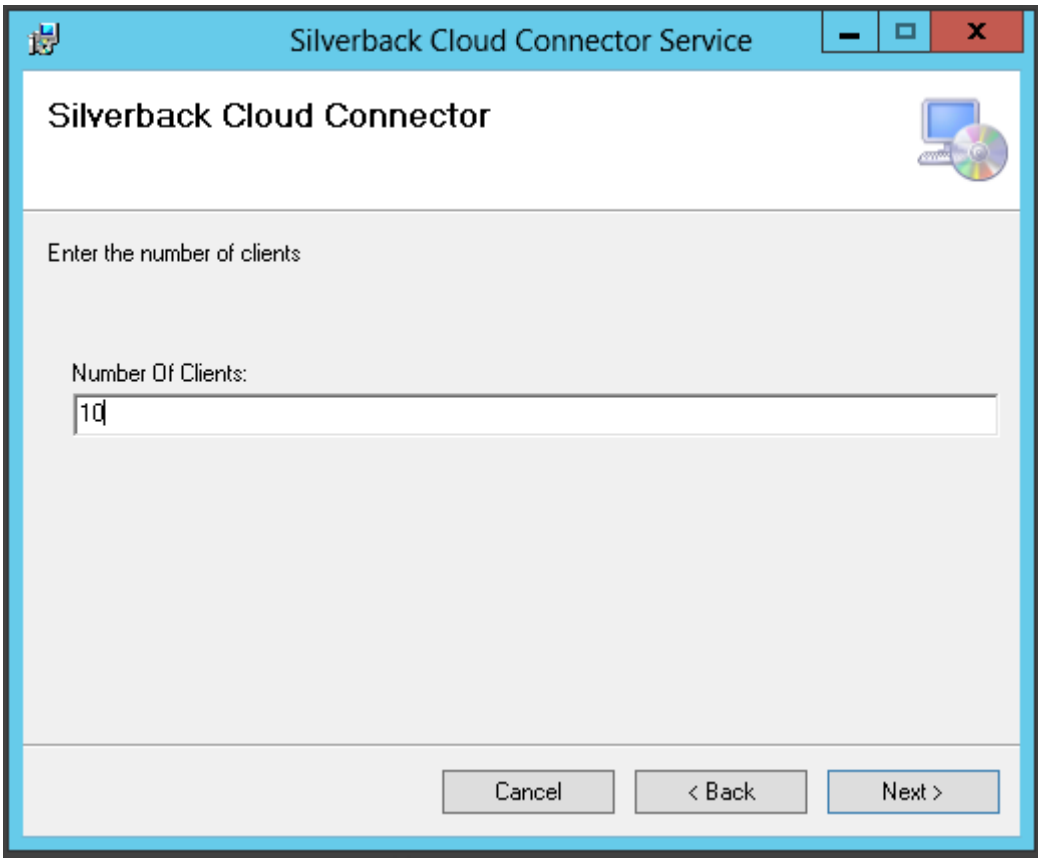
5.1.7. Select Install Location

Enter the destination folder, ensure “Everyone” is selected and click Next



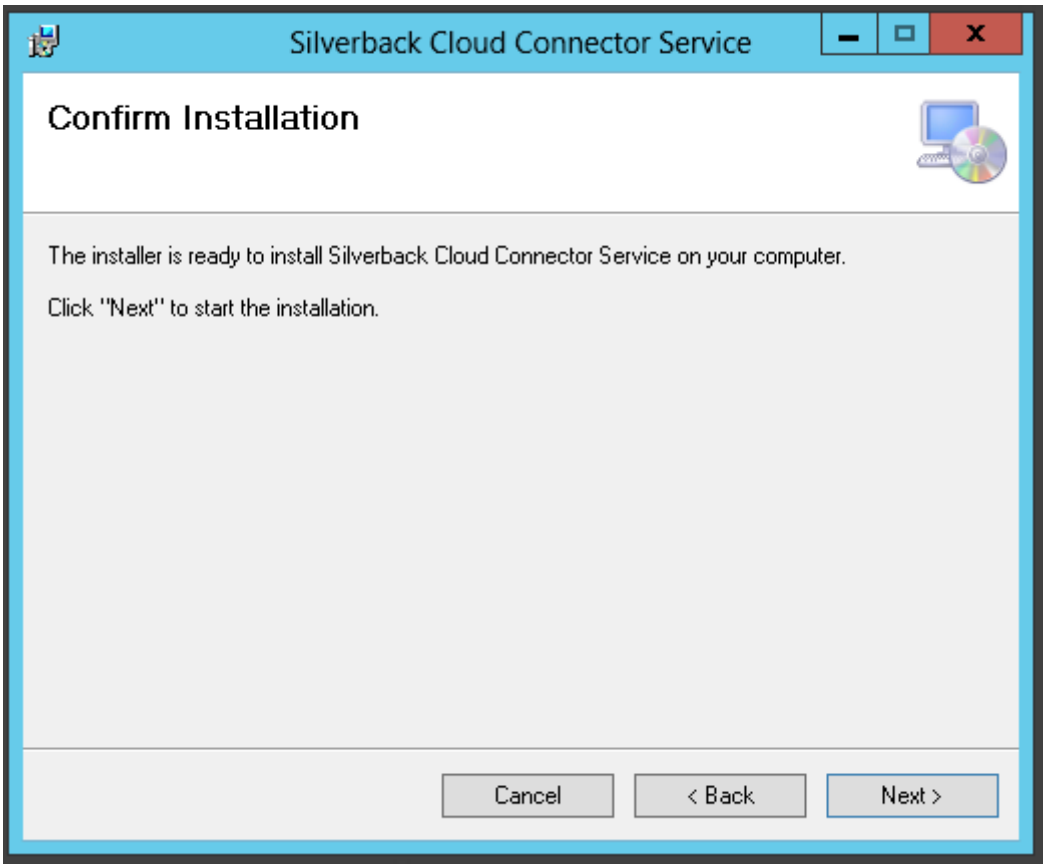
5.1.8. Enter the number of clients

You can have multiple Cloud Connector clients on the one machine to ensure redundancy. Each client will create a service on the local machine. Having more than one, ensures that if the service is to fail there will be another to take its place. Click Next

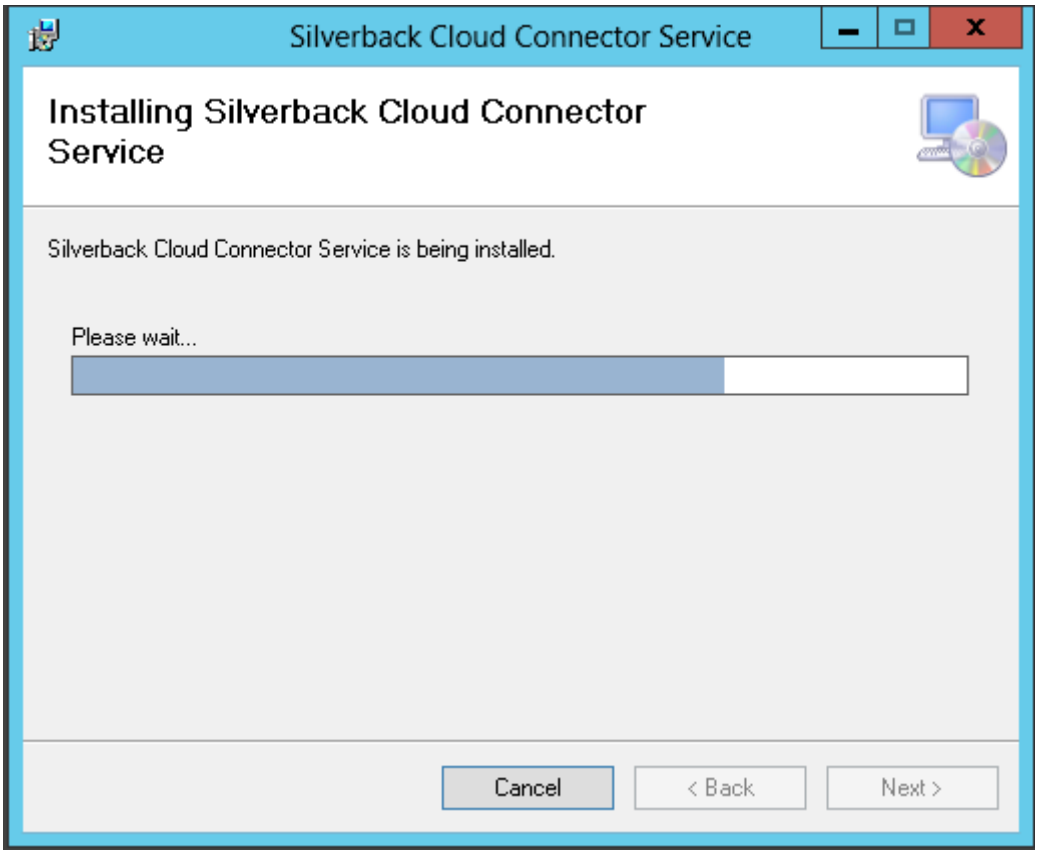


5.1.9. Confirm Installation

Click Next

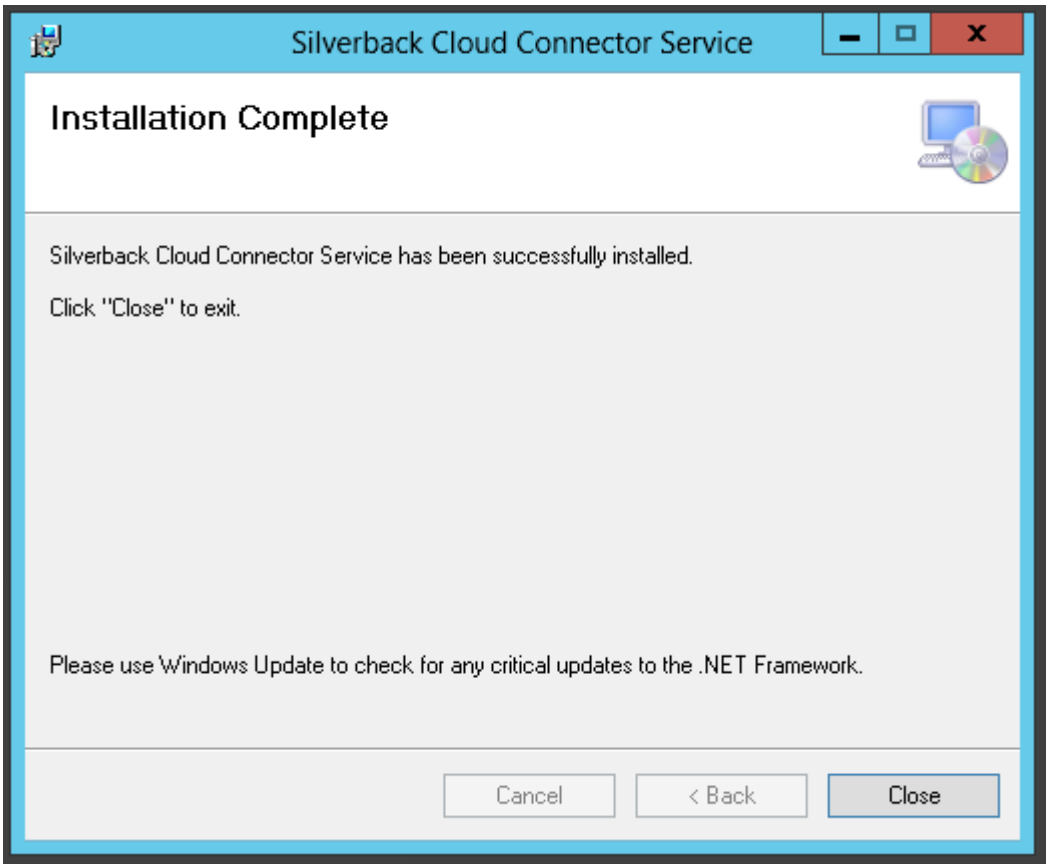


5.1.10. Wait for Installation to Complete



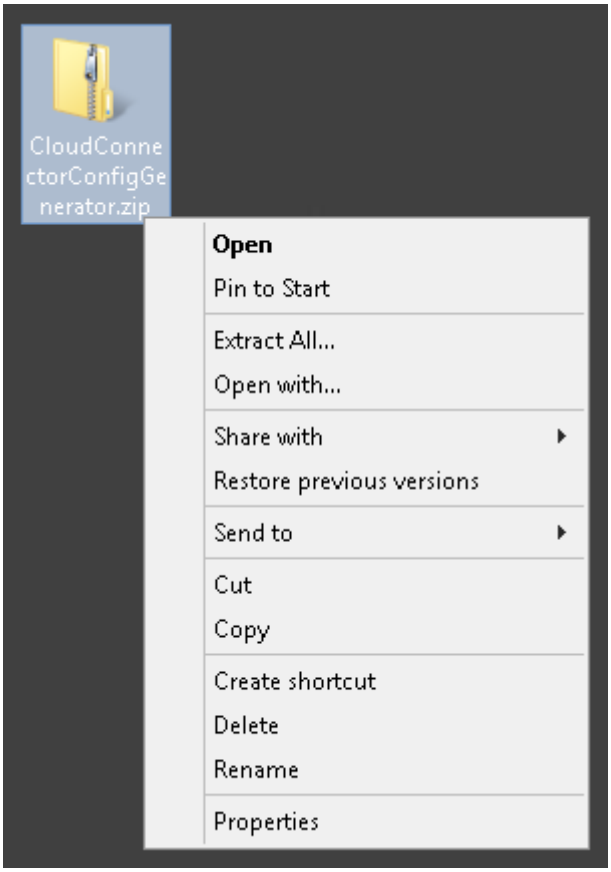
5.1.11. Complete Installation

Click Next



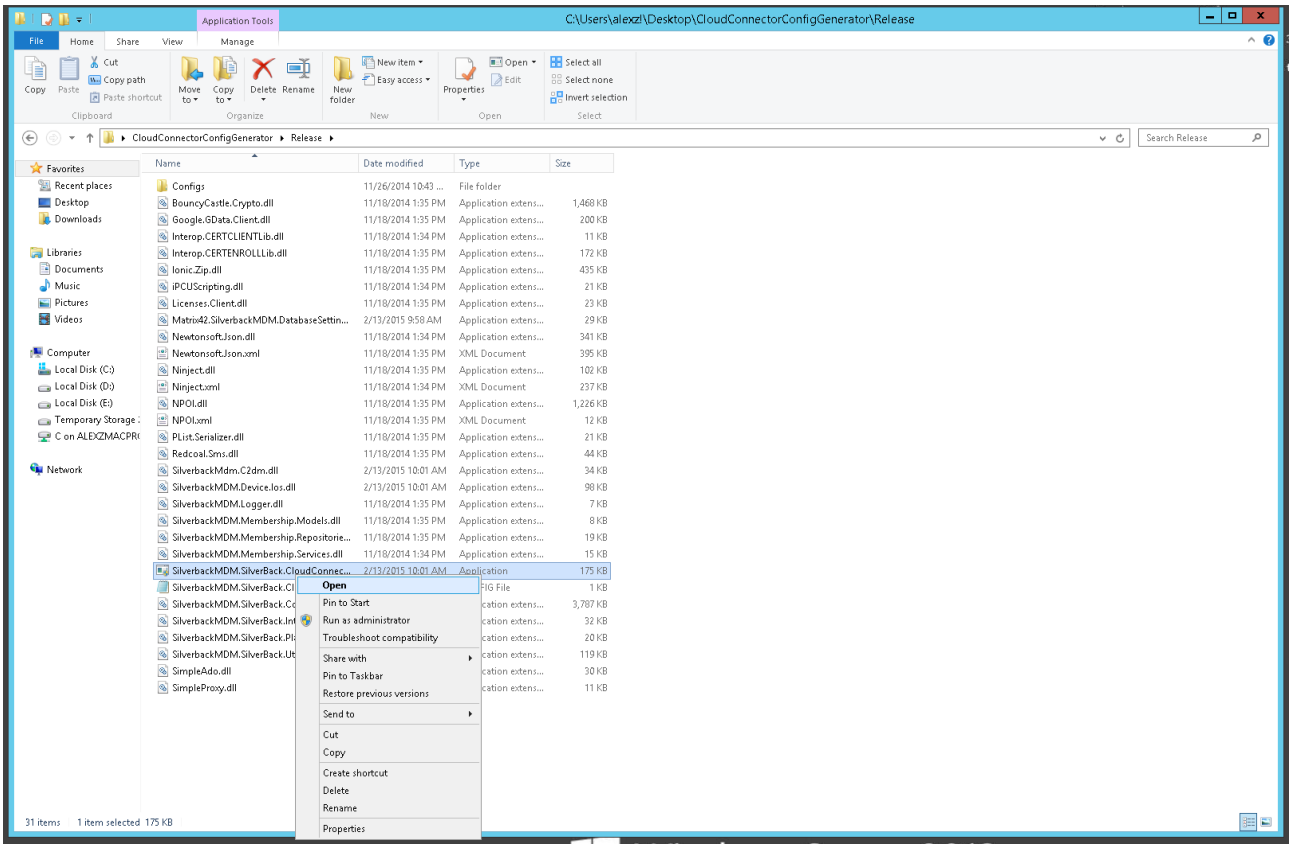
5.1.12. Extract Cloud Connector Configuration Generator Files

Provided with the setup are the Configuration Generator files. These are in an archive that should be extracted.



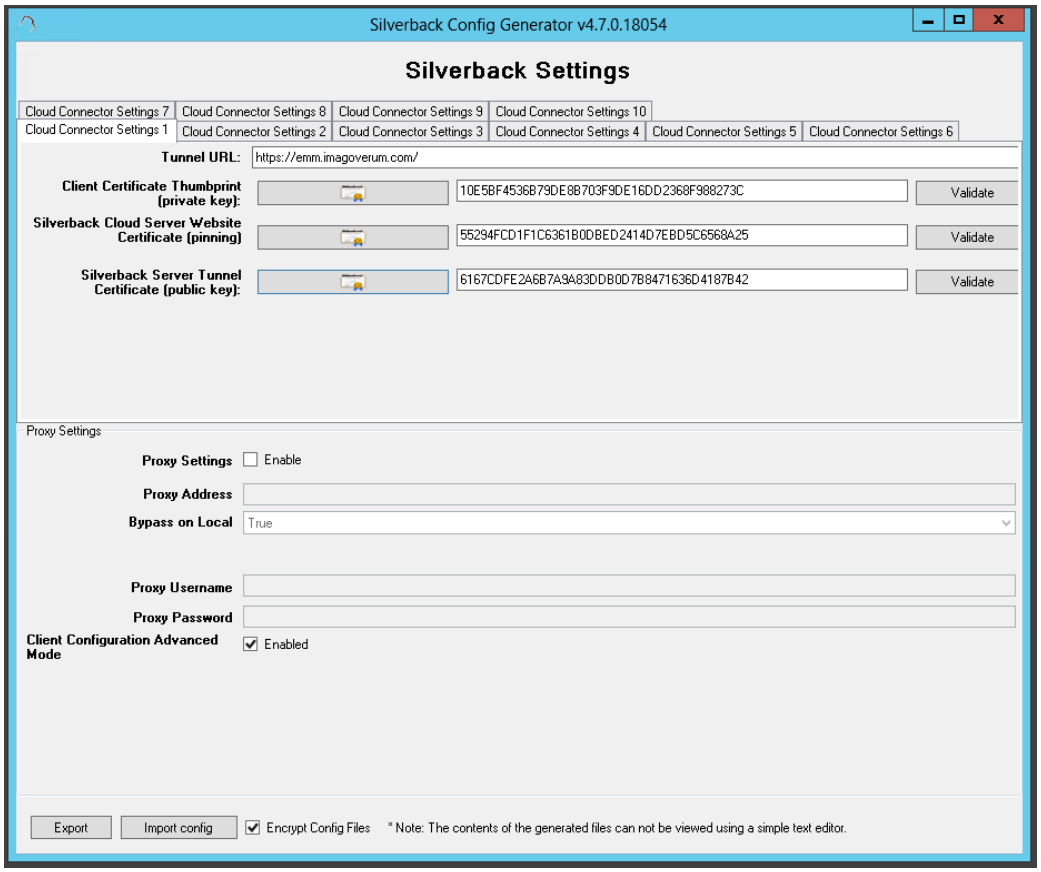
5.1.13. Launch the Configuration Generator

Navigate to where the extracted files were, and launch the executable



5.1.14. Configure the Individual Cloud Connector Clients

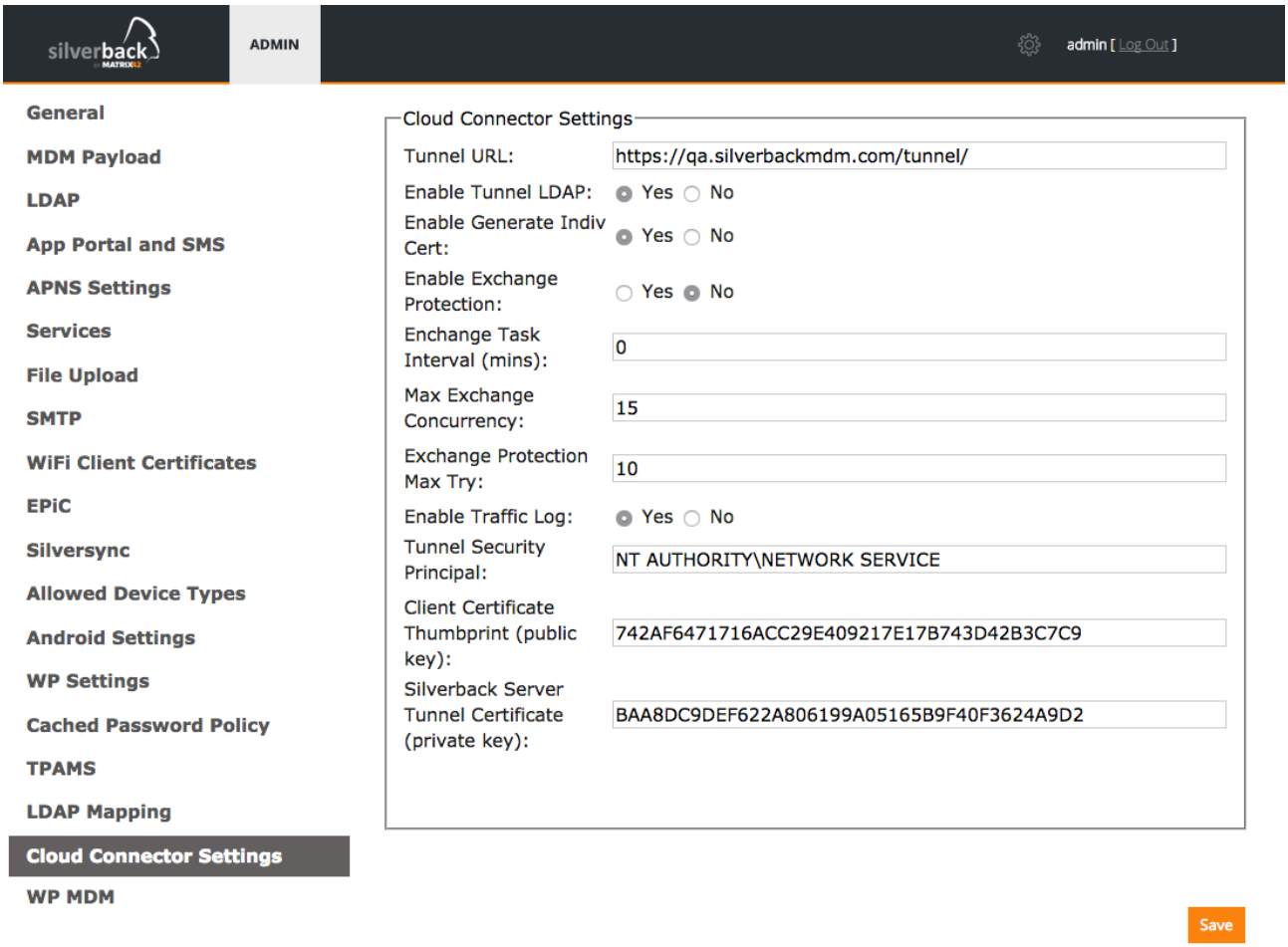
Each client required should be configured. The cloud connector uses a mutual authentication mechanism for it's connections. This means the server has a public/private key pair, and the client has a public/private key pair. The client should be configured to trust the server, and the server should be configured to trust the client. These settings need to be configured for each Cloud Connector Instance.



Field	Description
Tunnel URL	The Silverback Server URL
Client Certificate Thumbprint (Private Key)	The private key thumbprint for the CLIENT certificate
Silverback Cloud Server Website Certificate (pinning)	The thumbprint of the Silverback Server website SSL certificate. This is used to "pin" the client to only accept a certain server certificate to prevent man-in-the-middle attacks
Silverback Server Tunnel Certificate (public key)	This is the public key thumbprint for the Cloud Connector SERVER certificate. The client will use this to encrypt information so it's critical this matches the server Cloud Connector certificate.

5.1.15. Configure the server side

When the client is configured, you should then configure the server to accept connections from the client. Login to the admin console with a user belonging to the Settings Administrator Role.

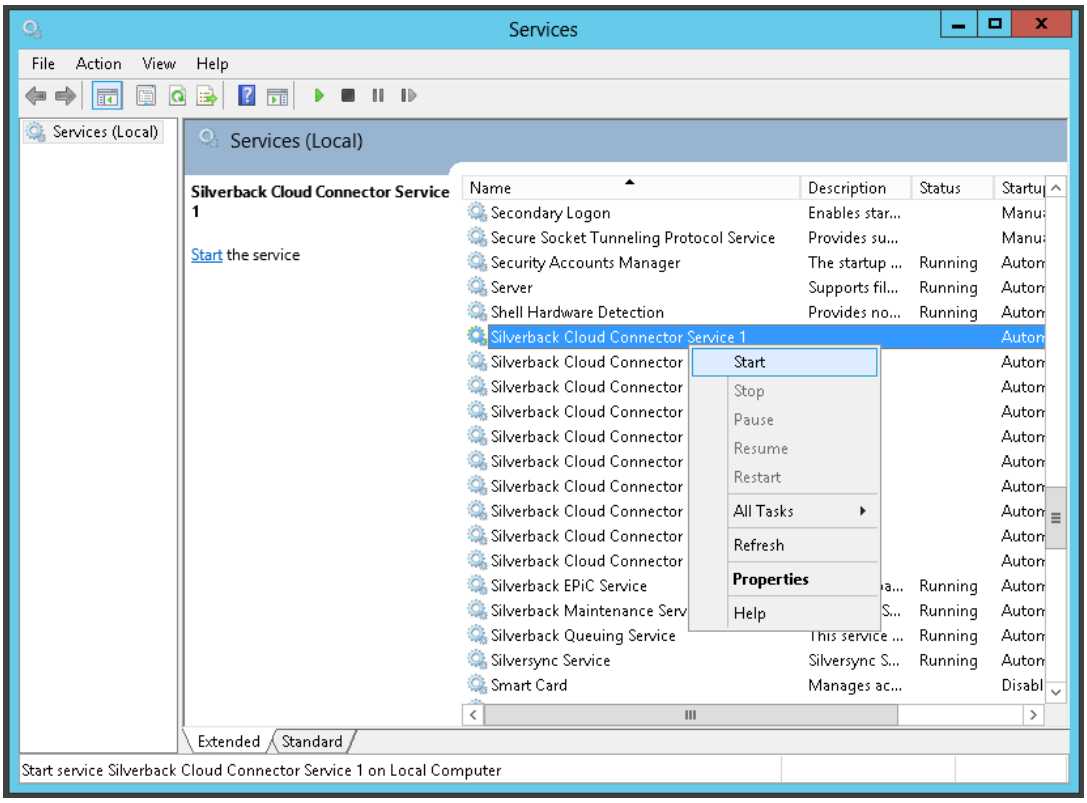


Field	Description
Tunnel URL	The tunnel end point the client connects to. This must match the Cloud Connector Client configuration
Enable Tunnel LDAP	Determines if LDAP traffic should go to the Cloud Connector or not
Enable Generate Indiv Cert	Determines if individual client certificates should be generated via the Cloud Connector
Enable Exchange Protection	Determines if Exchange Protection traffic should be sent via the Cloud Connector
Exchange Task Interval	How often the Exchange task should be

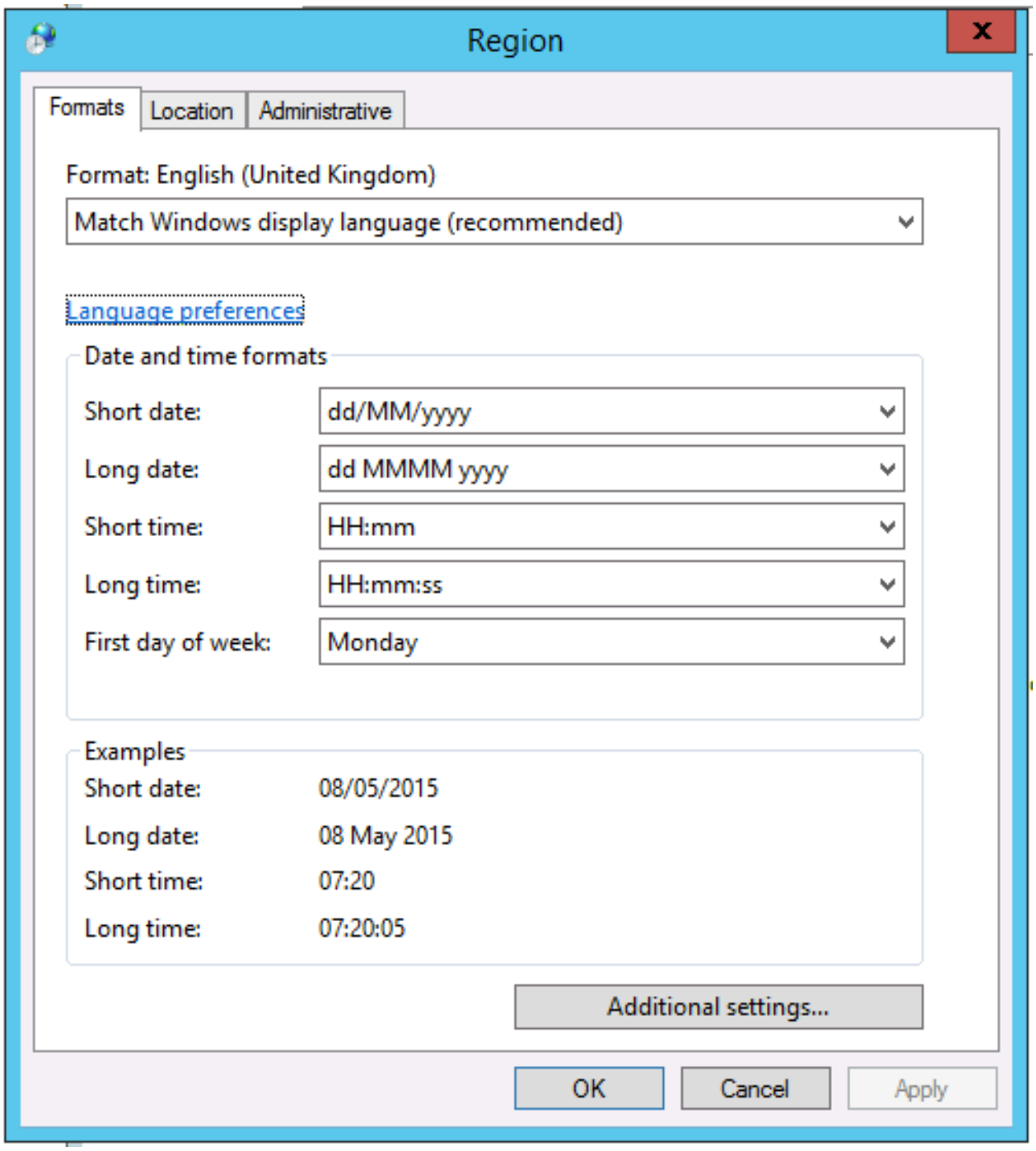
Field	Description
	executed
Max Exchange Concurrency	The number of connections to exchange allowed at a given time
Exchange Protection Max Try	The number of attempts before failing for Exchange Protection
Enable Traffic Log	Enables logging for the Cloud Connector Traffic, for troubleshooting
Tunnel Security Principal	The system account that is used for the Cloud Connector connections
Client Certificate Thumbprint (public key)	The thumbprint of the PUBLIC key of the Cloud Connector Client Certificate. The server will encrypt information meant for the client using this.
Silverback Server Tunnel Certificate (private key)	The thumbprint of the private key of the SERVER certificate. The server will decrypt information sent from the client using this.

5.1.16. Start the Cloud Connector Services

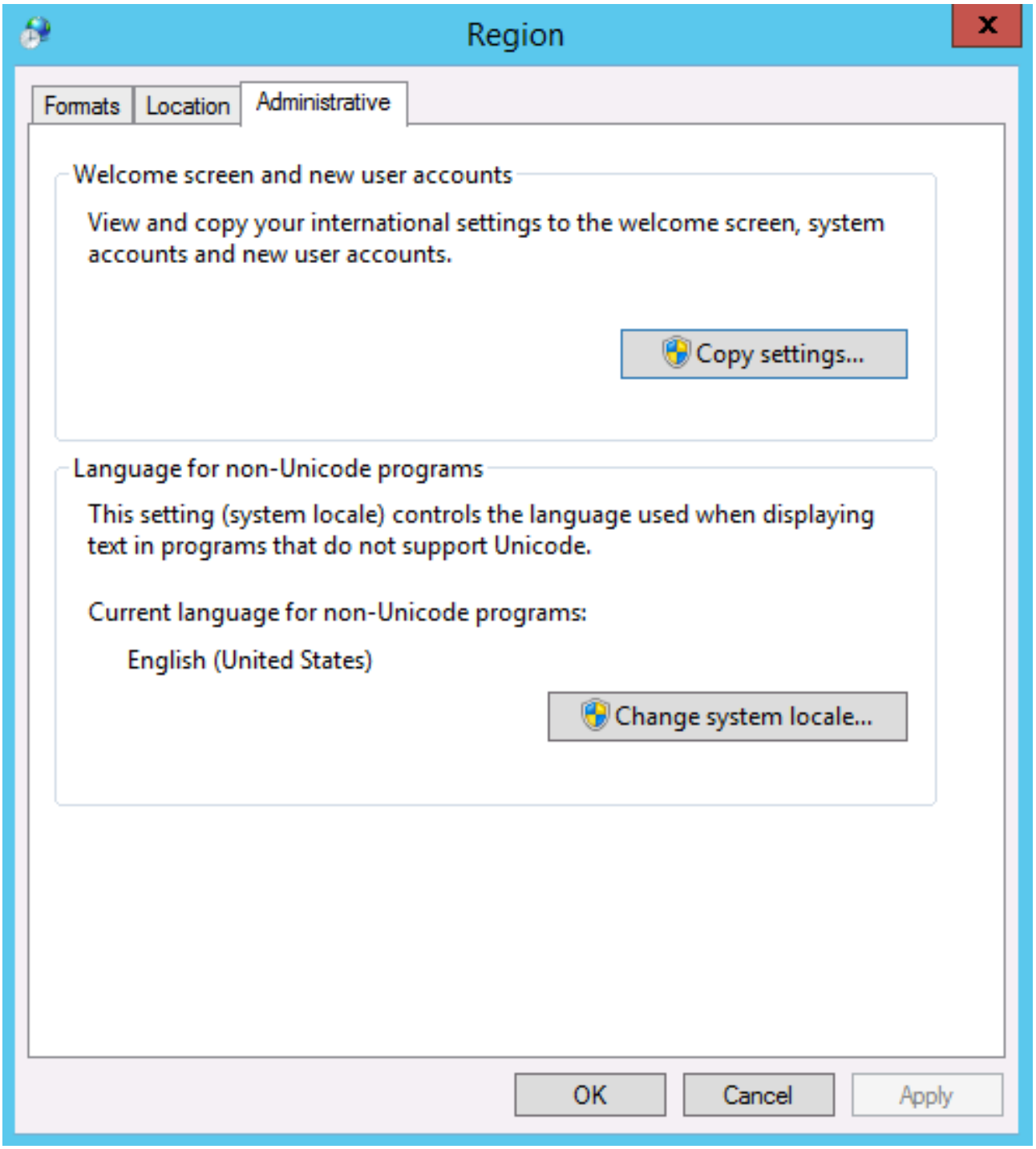
When everything is configured, you can start the Client Cloud Connector Services



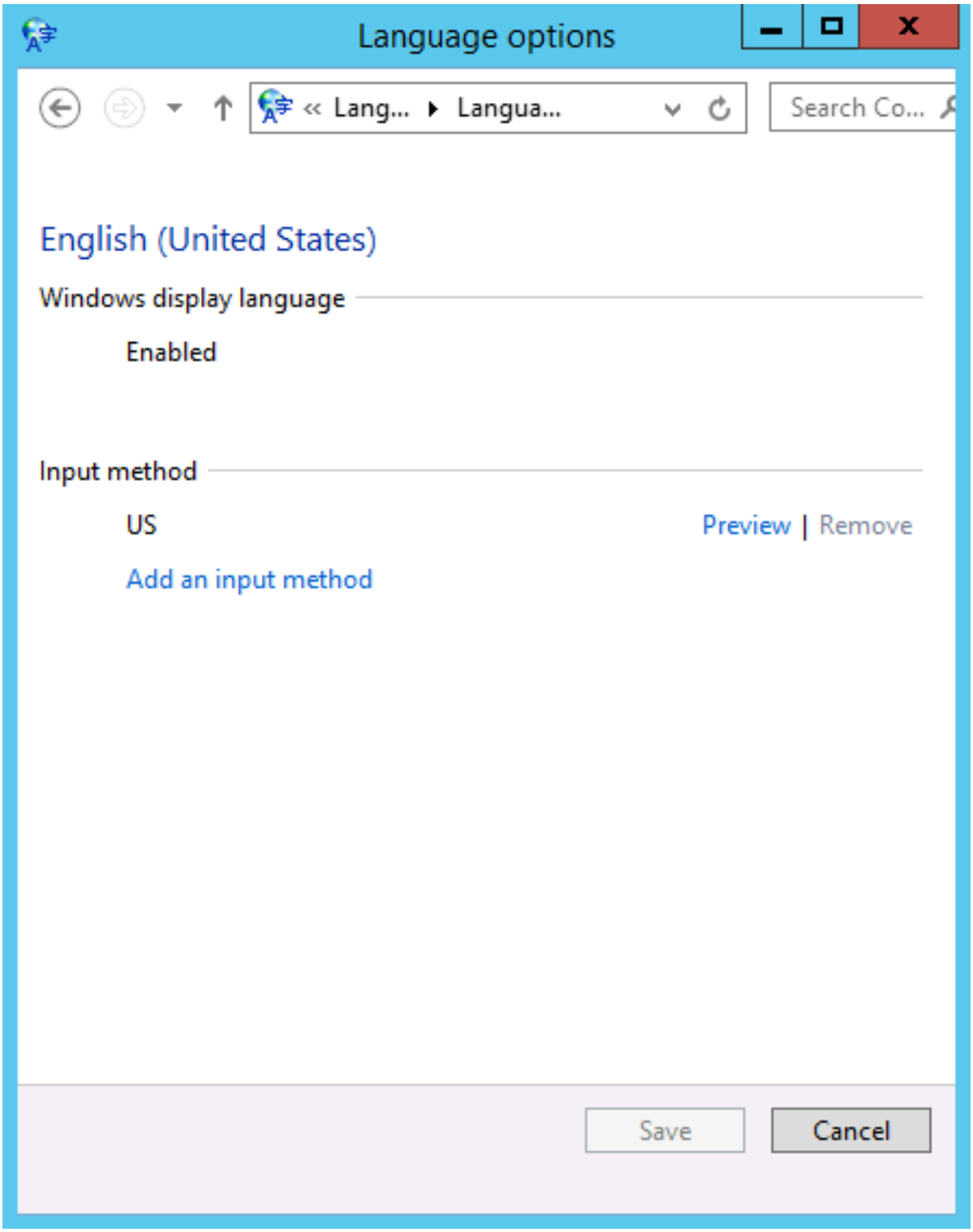
6. Appendix B – Example Region Format Screenshots



Installation Guide Version 5.1 U3



Installation Guide Version 5.1 U3



Author: Matrix42 Cloud & Mobile Management