MATRIX42
SMARTER WORKSPACE – BETTER LIFE

Silverback by Matrix42

Silversync 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 4
1.1. Overview 4
2. Preparation 5
2.1. System Requirements 5
2.2. Software Prerequisites 6
2.3. Account Requirements 8
2.4. Firewall Requirements 8
2.5. DNS Requirements 9
2.6. SSL Certificate Requirements 9
3. Installation and Configuration 10
3.1. Overview 10
3.2. Adding a Silversync Server 10
3.2.1. Create a new server in Silverback 10
3.3. Install Silversync 14
3.3.1. Configure the Silversync Server 18
3.3.2. Settings Tab 27
3.3.3. Service Mappings 28
3.3.4. Personal File Management 29
3.3.5. Logs 30
3.3.6. Binding Push 31
3.3.7. Assign Content to Tags 33
4. Appendix A – Example Region Format Screenshots 38
5. Appendix B – Configuring User Based Authentication Manually 41

Silversync Installation Guide Version 5.1 U3

1. Introduction

1.1. Overview

This document will guide you through a typical installation of the Silversync component 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 Silversync.

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.

The installation of Silversync has changed substantially as of the 5.0 Update 2 release, so even if you have experience installing Silversync, please ensure you follow this guide carefully.

Author: Matrix42 Cloud & Mobile Management

2. Preparation

2.1. System Requirements

Silverback generally requires the following for the Silversync server itself. In a production setup, this should be a separate server to the Silverback server:

- Windows Server 2012 R2 – Windows Server 2008 SP2 to R2 Standard 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 plus extra required for your Silversync content
- SCSI or SAS speed disks or equivalent SAS
- 1GB Network Interface Cards
- 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 A for example screenshots

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

It is possible to allocate users an amount of storage for their personal files on the server. Ensure that the server has sufficient space to accommodate files uploaded by users.

2.2. Software Prerequisites

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

- Silverlight
- Powershell
- Microsoft Access Database Engine x64 2010
- .NET 3.5
- .NET 4.0
- .NET 4.5
- .NET 4.5.1
- IIS 8
  - For IIS, the following IIS Role Services must be enabled:

- [-] Web Server (IIS)
  - [-] Web Server
    - [-] Common HTTP Features
      - [x] Default Document
      - [x] Directory Browsing
      - [x] HTTP Errors
      - [x] Static Content
      - [x] HTTP Redirection
      - [ ] WebDAV Publishing (Not installed)
    - [-] 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)
    - [-] Performance
      - [x] Static Content Compression
      - [ ] Dynamic Content Compression (Not installed)
    - [-] 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)

Silversync Installation Guide Version 5.1 U3

- [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)

2.3. Account Requirements

Silversync Server

To install the Silversync Server a domain account that is a member of the Local Administrators group is needed. If installing in a workgroup environment, a local administrator account is needed.

Silverback has two methods of access files for users. These are called Server Based and User Based.

- Server Based authentication means that the service account on the server will access the files on behalf of the user. This means only the service account for the Silversync server needs access to the files.
- User Based authentication means that the individual user's file permissions are used. This means that a user must be granted read permissions on a file before they will be able to sync it.

If you intend to use User Based Authentication, it is recommended run the installer as a Domain Administrator, as the system needs to configure permissions for the user to access the files. It is possible to perform this setup without a Domain Administrator account, and this is outlined later in the document, however this requires manual server changes for every content location so it's not recommended.

2.4. Firewall Requirements

As Silversync connects to external and internal systems, you need to ensure that the following connectivity items are configured.

Note that if you intend to use User Based authentication for file access, more ports may be required for KCD authentication depending on your AD specification and Forest Functional Level.

Traffic Source	Destination	Port/Protocol
Devices (External/Internal)	Silversync Server	443/tcp
Silversync	Silverback Server	443/tcp
Admin Workstation	Silversync Server	3389/tcp

2.5. DNS Requirements

The Silversync server requires devices to connect via DNS, The appropriate DNS entries should 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: **silversync.yourcompany.com.**

- The external DNS name for Silversync is **silversync.*yourcompany.com***
- The internal DNS name for Silversync is **silversync.*yourcompany.com***

An authoritative DNS aliases needs to be created for silversync.*yourcompany.com* and it must resolve to IP the external interface of the Silversync server (or DMZ Gateway)

An internal DNS aliases needs to be created for silversync.*yourcompany.com* and it must resolve to the Silversync server interface.

2.6. SSL Certificate Requirements

The Silversync solution allows users to securely synchronise content to their devices and requires an established trust relationship between the device and server.

The Silversync 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 the DNS section above

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

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

3. Installation and Configuration

3.1. Overview

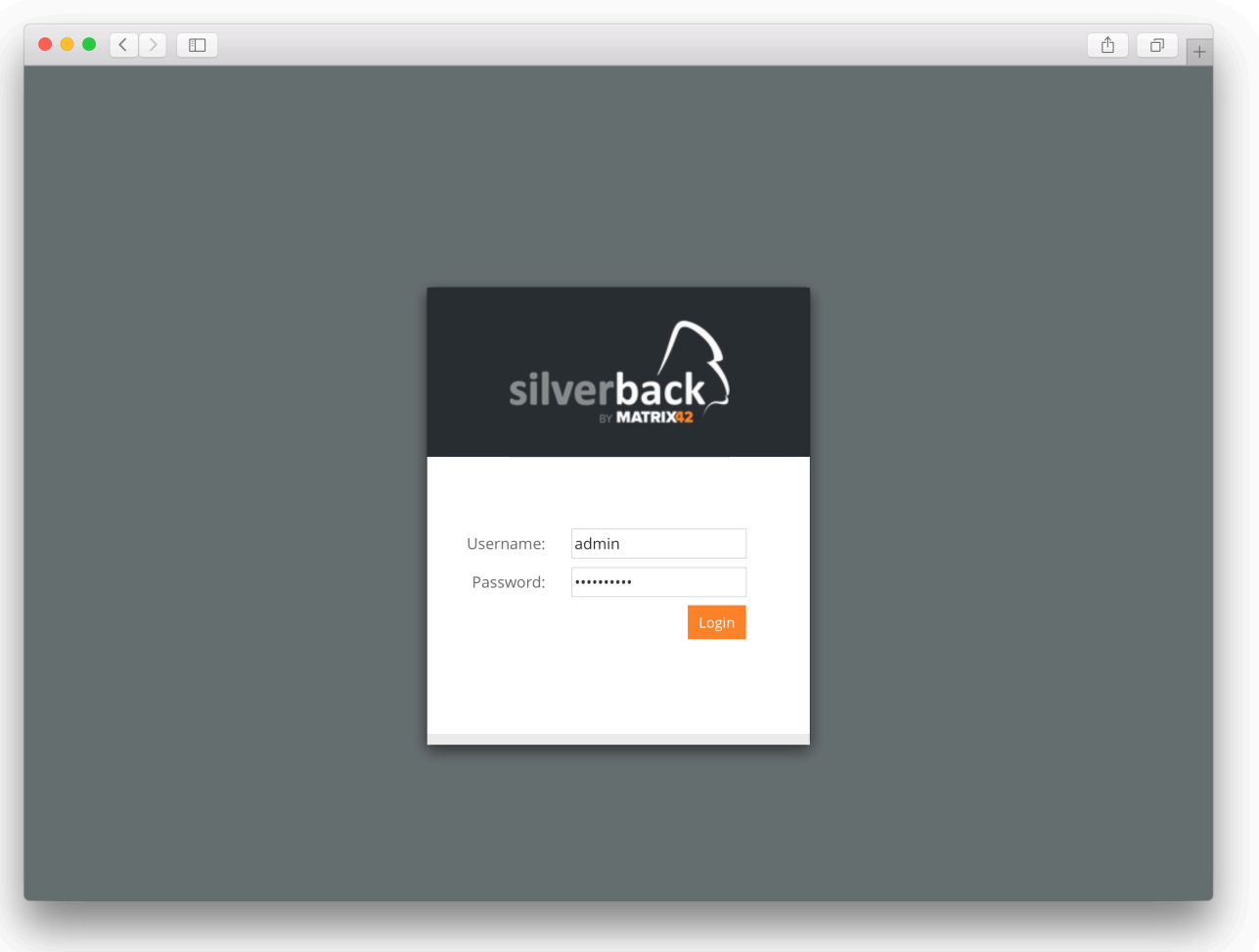
Before beginning the installation, ensure that you've confirmed all the items in Section 2.

Important: It is assumed the Silverback Installation Guide has been completed, and a working Silverback instance is configured before continuing with this section.

3.2. Adding a Silversync Server

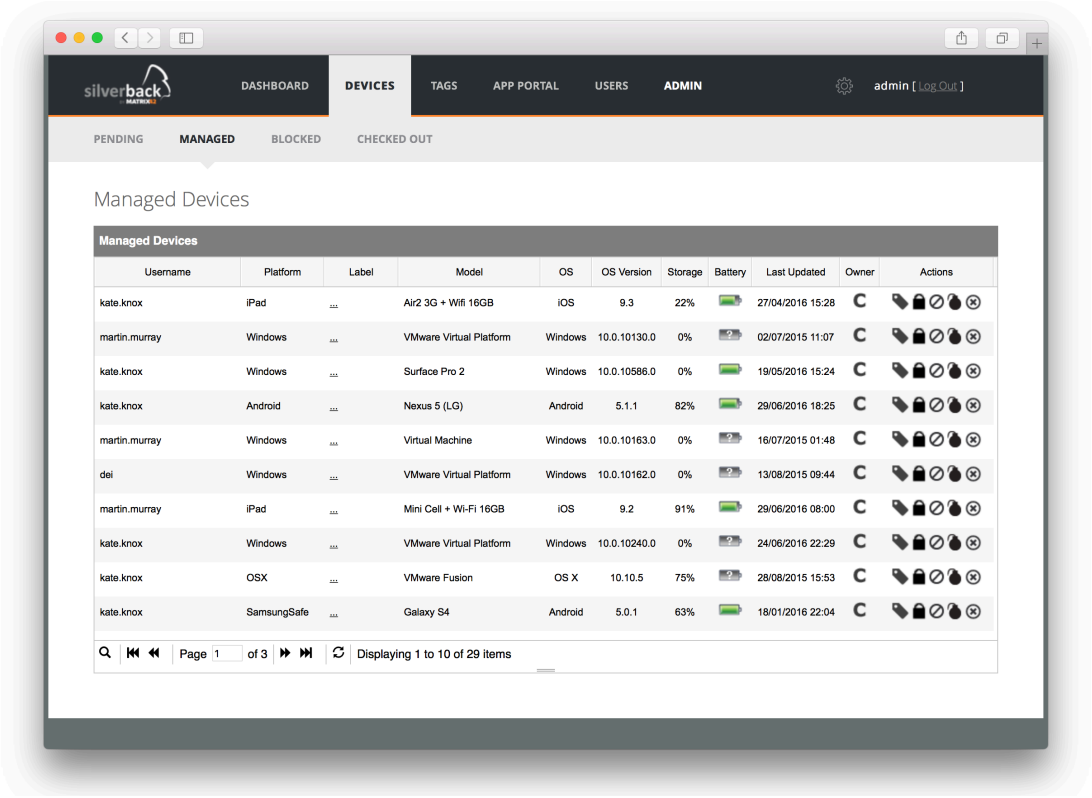
3.2.1. Create a new server in Silverback

Log in to your Silverback server admin console as a user with the Administrator role.

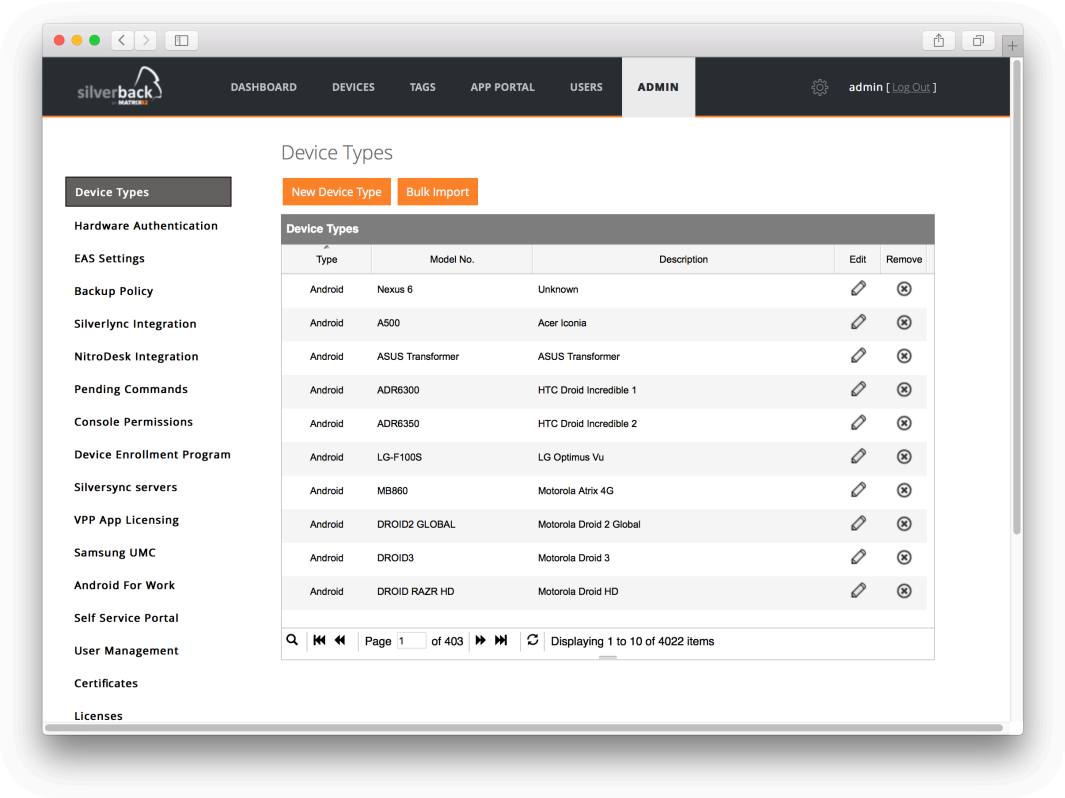


Silversync Installation Guide Version 5.1 U3

Click on the Admin Tab from the top navigation menu



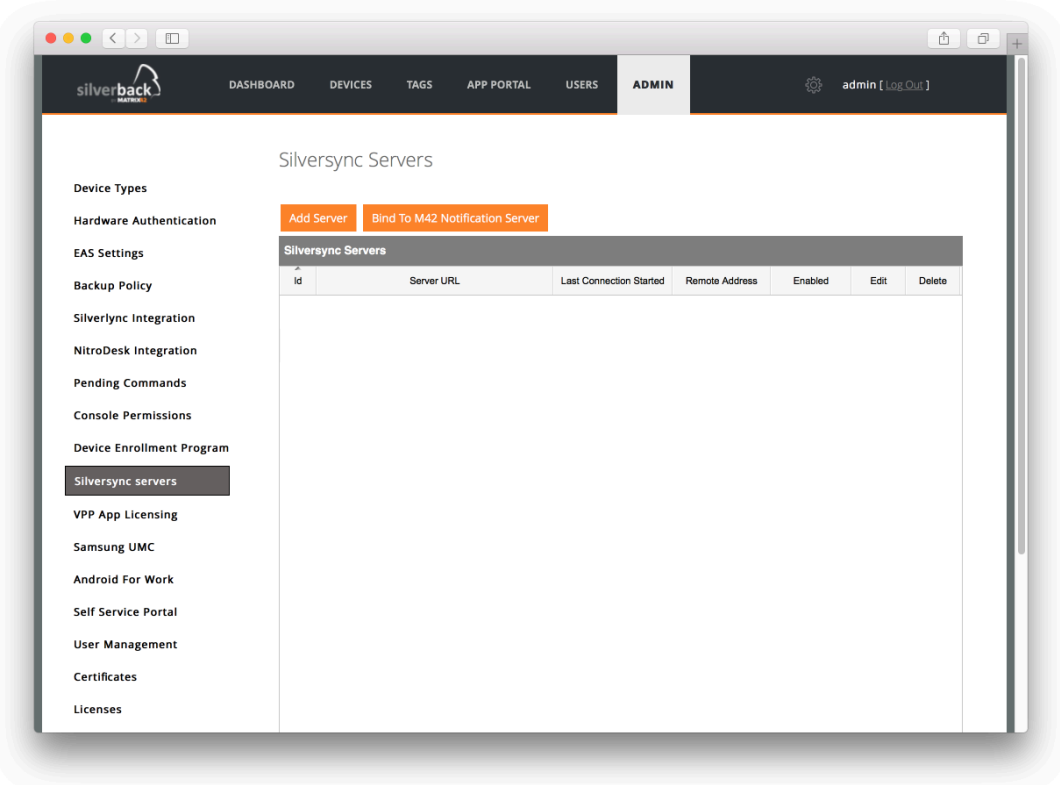
Click on Silversync Servers from the Admin Tab Left hand menu



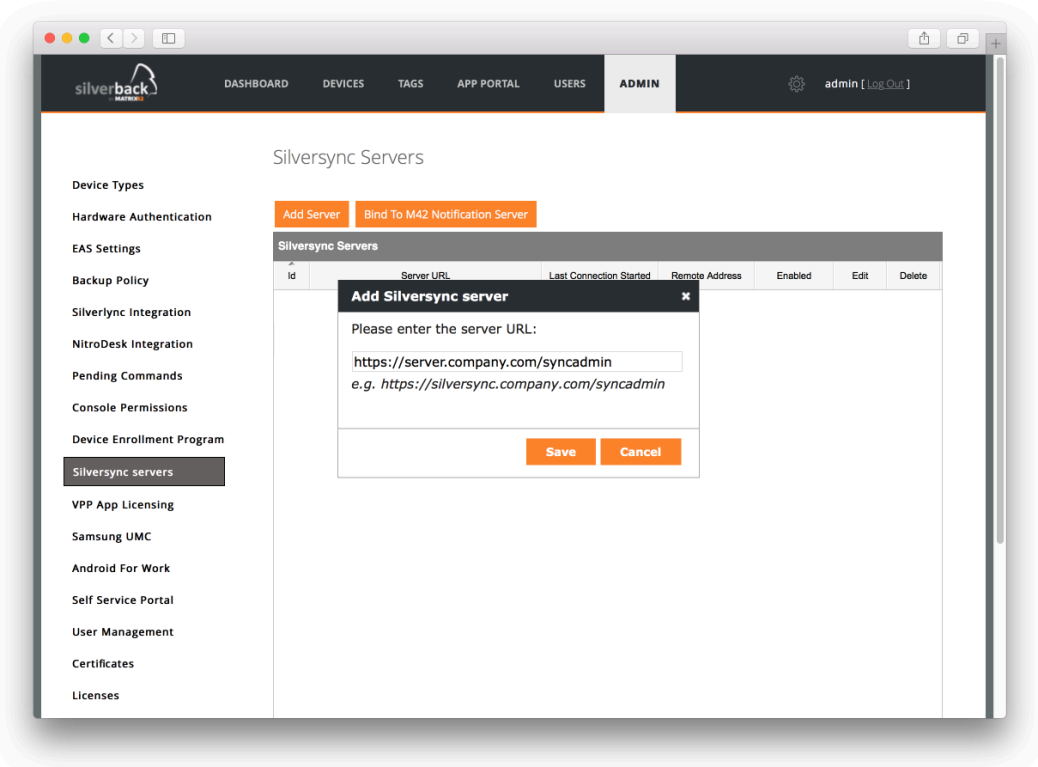
Author: Matrix42 Cloud & Mobile Management

Silversync Installation Guide Version 5.1 U3

Click Add Server

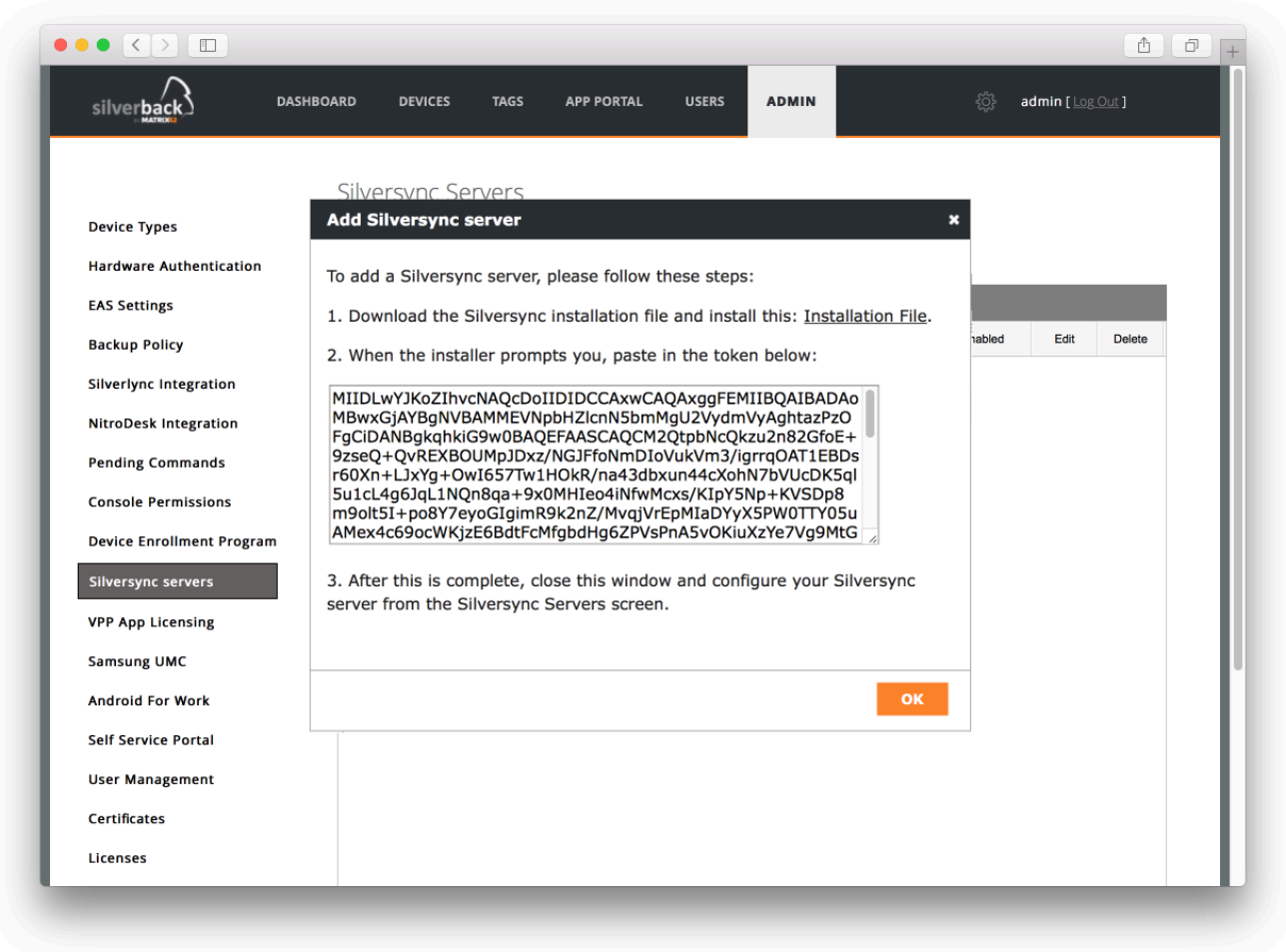


Enter your server URL and click Save. Note that this should match the DNS entry users will use to sync to your Silversync server. You should also ensure to enter https:// and add /syncadmin to the end of the URL.



Silversync Installation Guide Version 5.1 U3

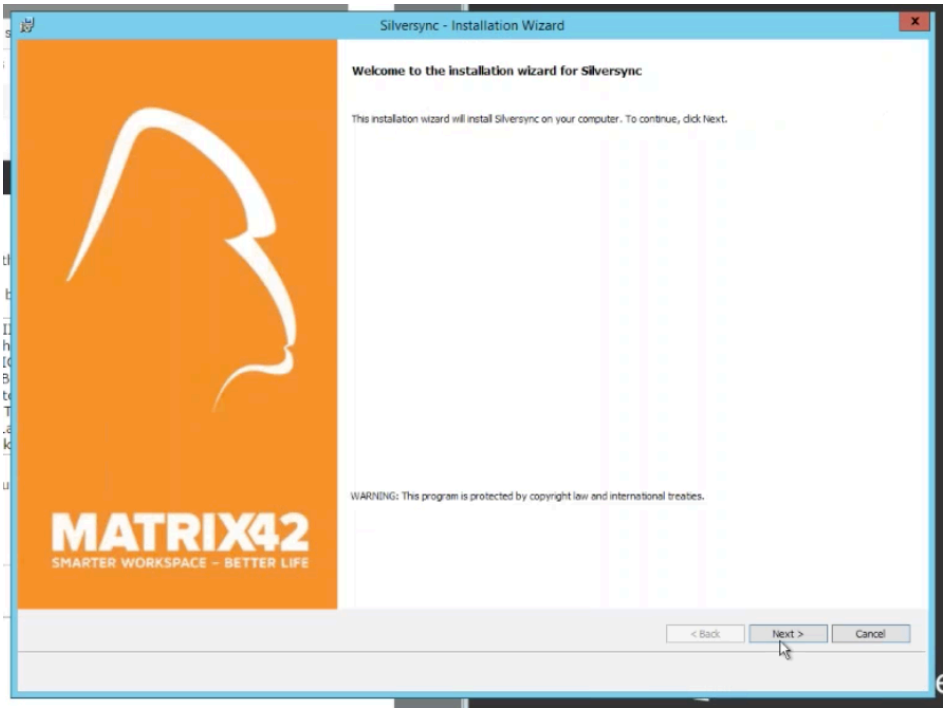
On the following prompt, click the Installation File link to download the Silversync installer. Copy this file to the intended Silversync server. Also while you have this page open, you should copy the token displayed in the text area. This token is used to bind your Silversync server to this Silverback server.



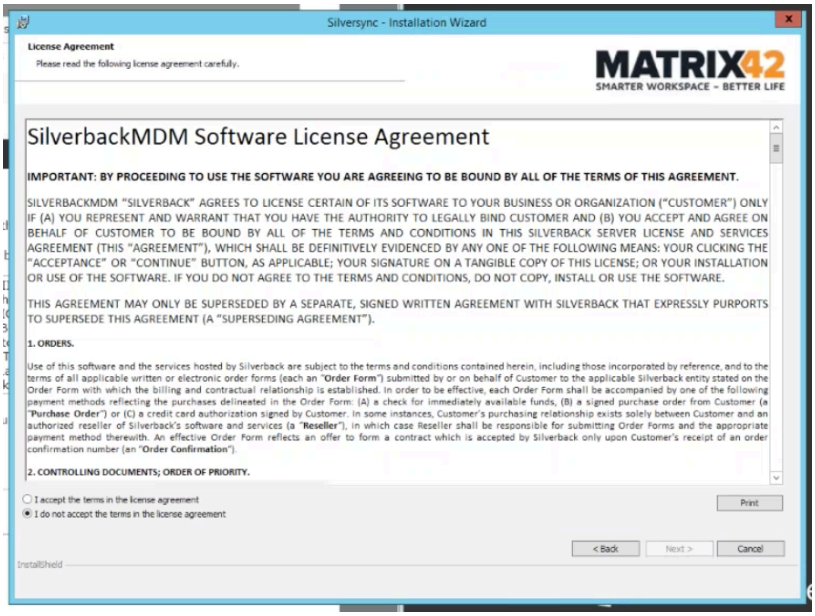
3.3. Install Silversync

After downloading the installation file from the Silverback console, launch the installer. This should be launched on the Silversync server as an account with local administrator privileges. It's also important that if you intend to use User Based authentication for syncing users, that you are a Domain Administrator account.

Launch the installer and click Next

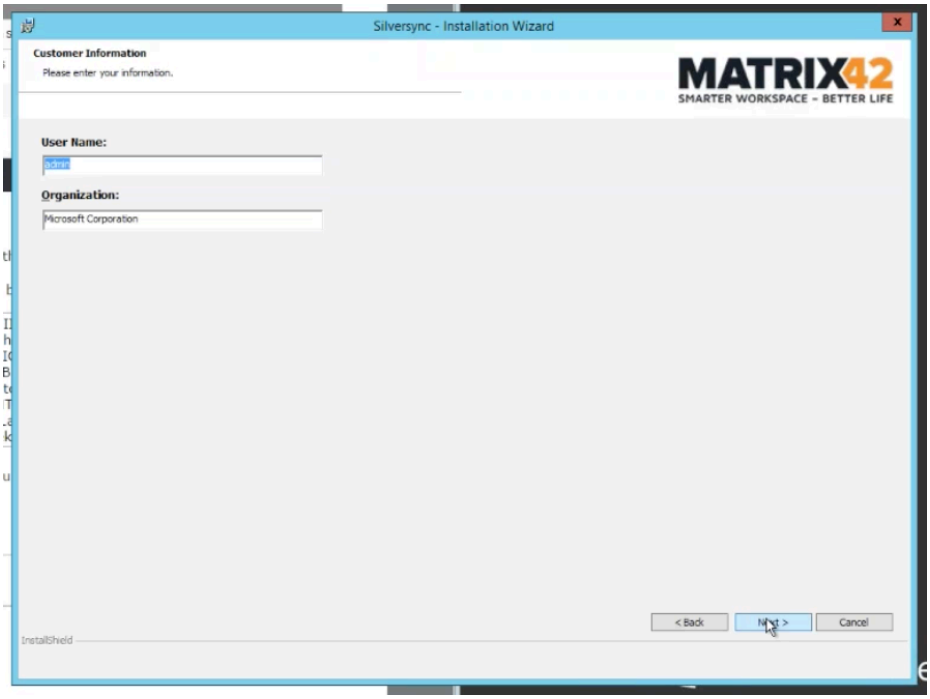


Accept the license agreement and click Next



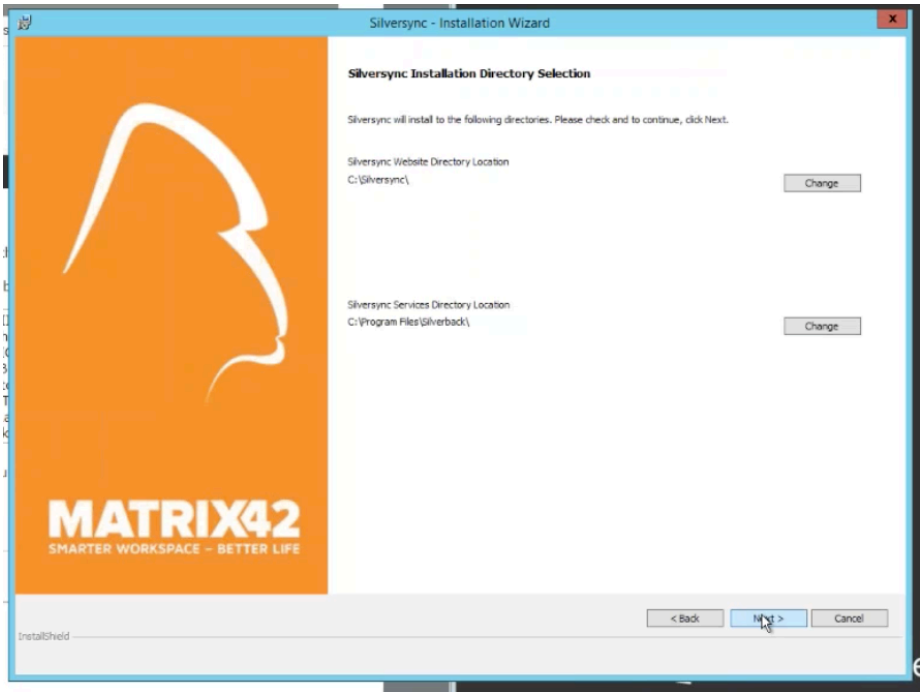
Silversync Installation Guide Version 5.1 U3

Enter your information. This information is only used for local installation information by Windows.



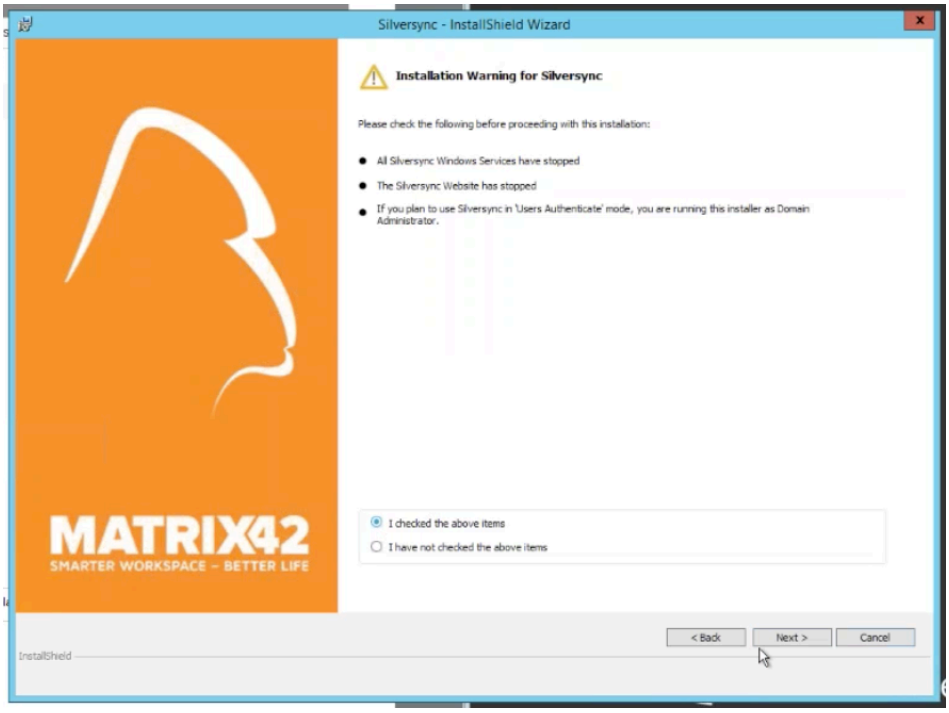
Modify the installation destination if needed, and click Next.

Note: If you are installing on the same machine as a Silverback server, select the same directory for the website.

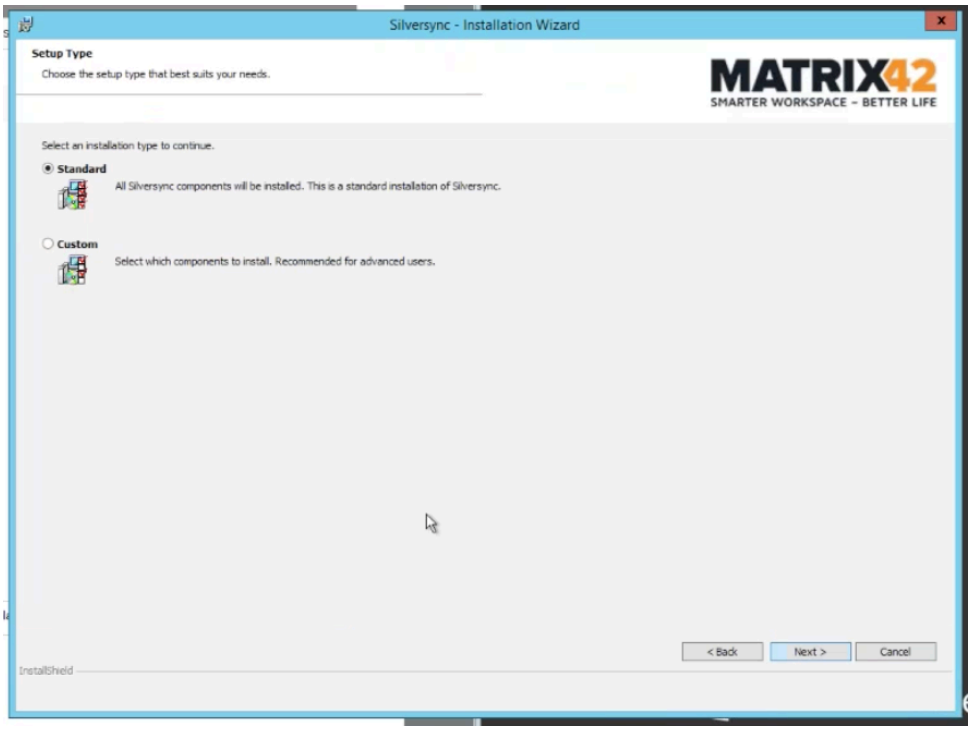


Silversync Installation Guide Version 5.1 U3

Check the items the installer mentions if they are applicable, and click Next.

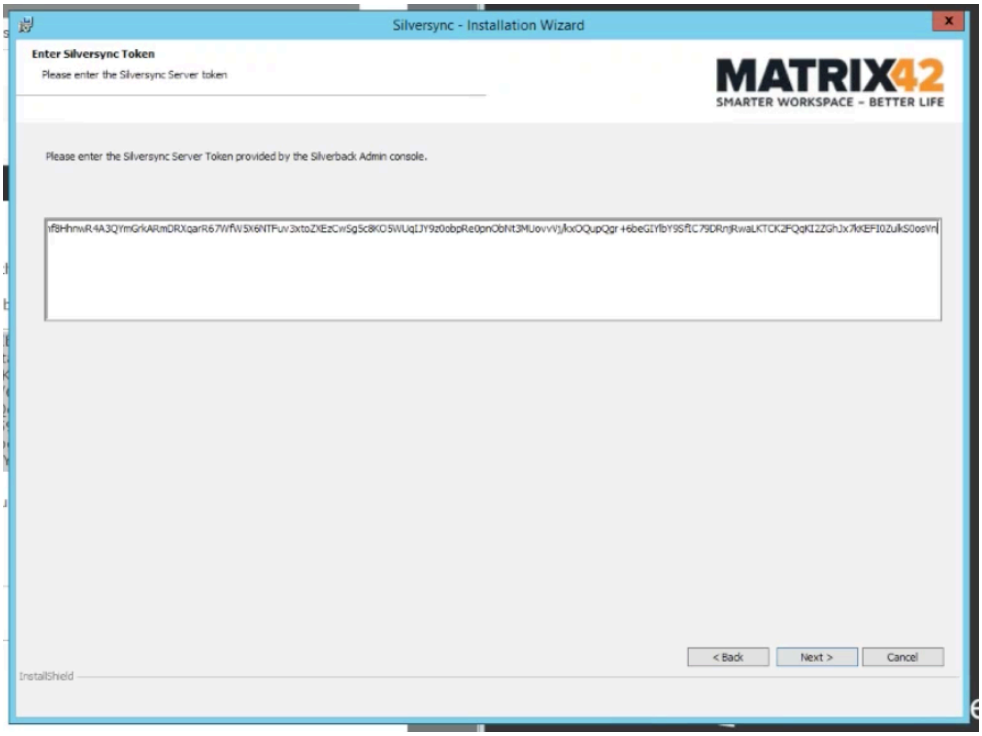


Choose Standard and click Next

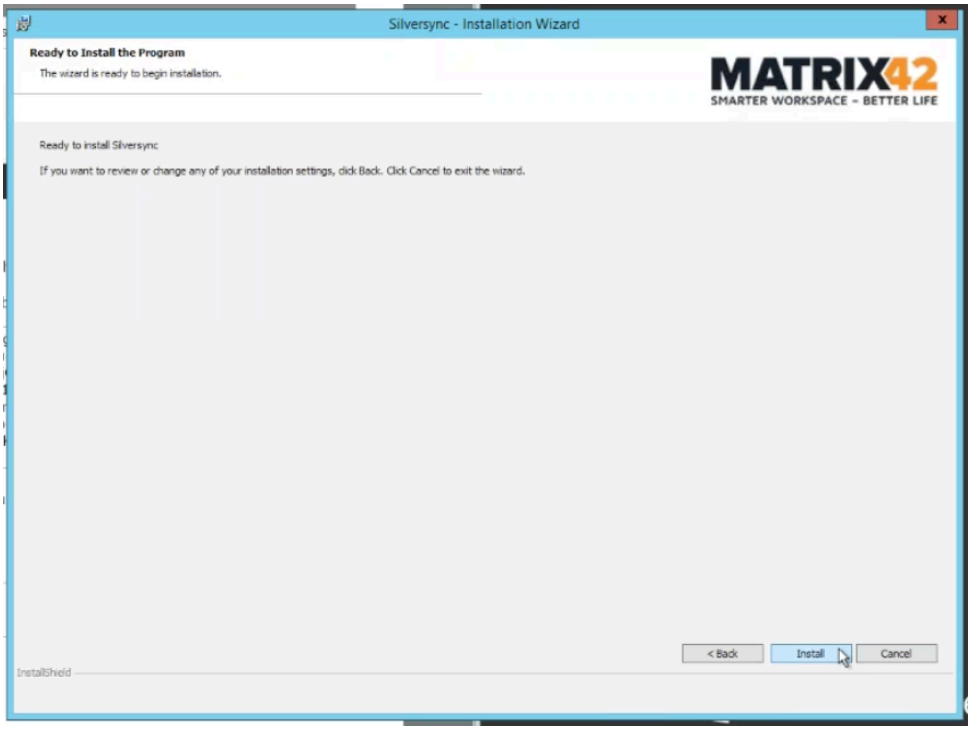


Silversync Installation Guide Version 5.1 U3

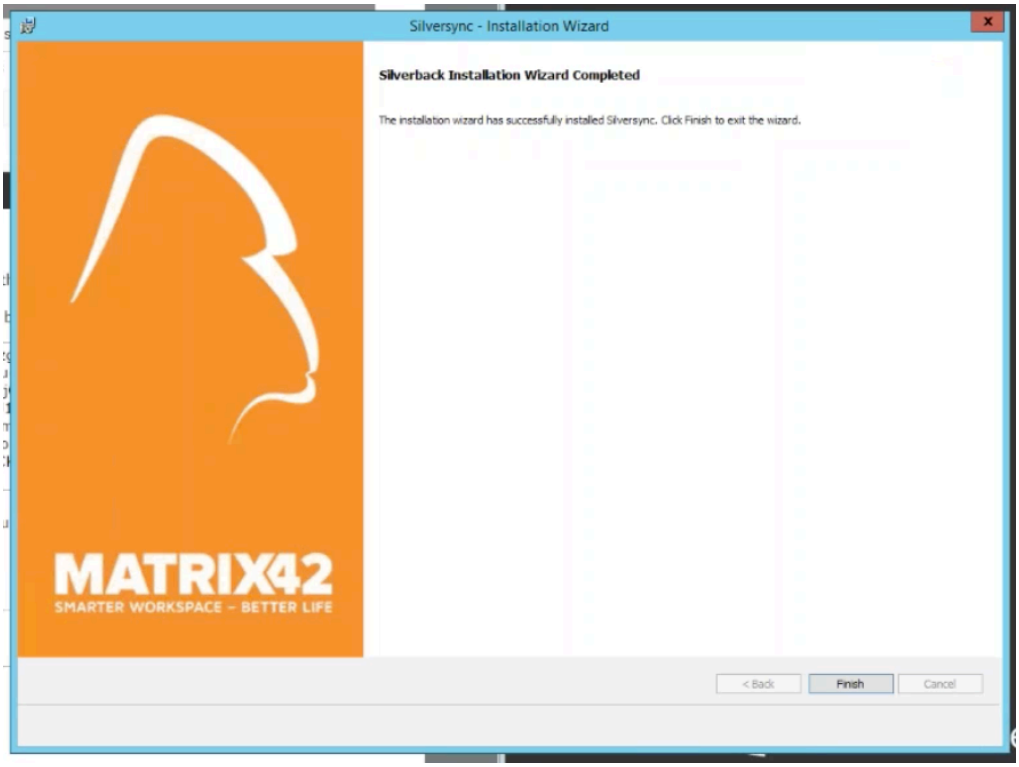
Paste in the token you copied from the Silverback website and click Next.



Click Install to start the process.



Wait for the installation to finish and then click Finish to complete the installation.

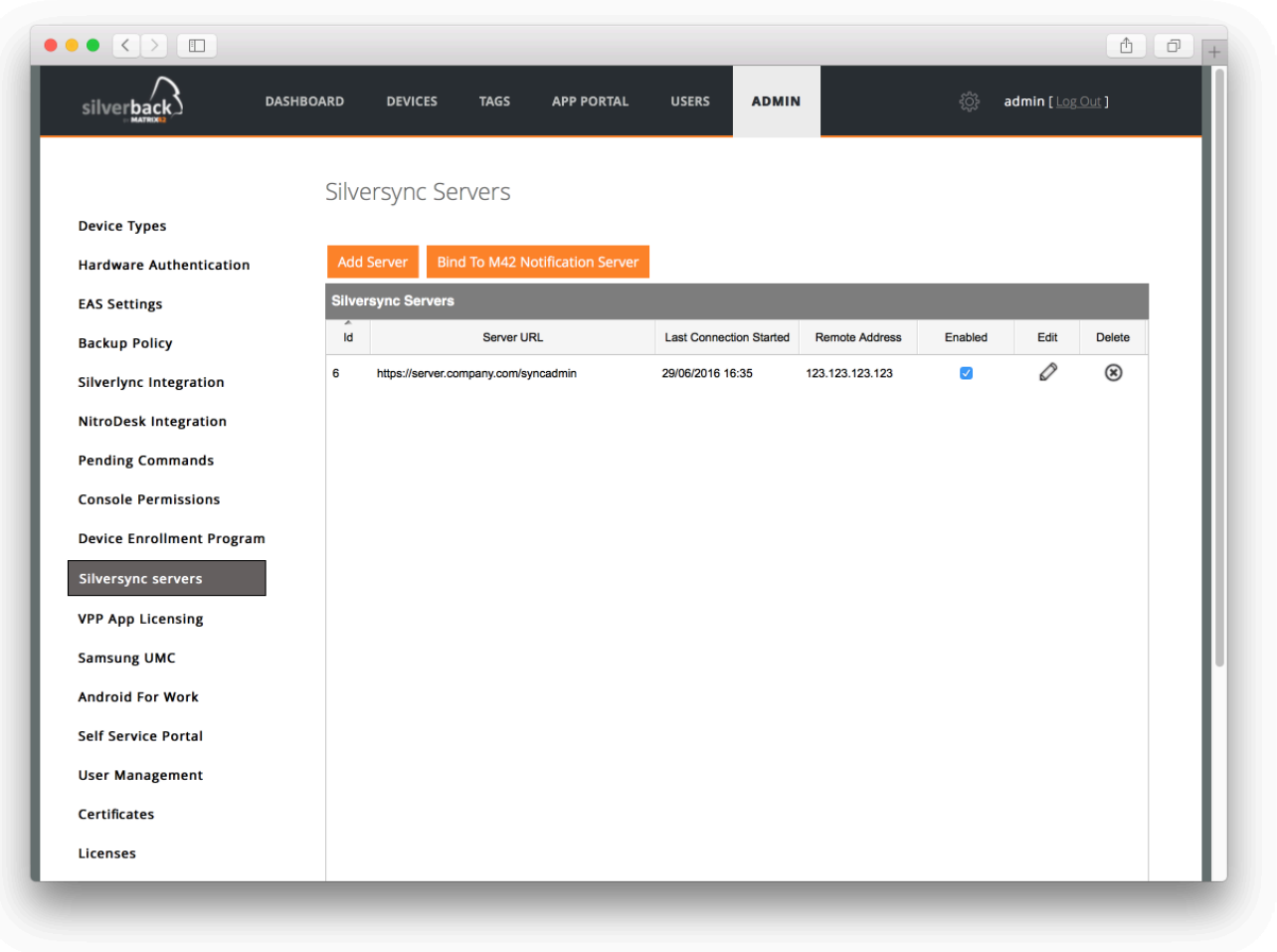


At this point, the Silversync server is already running and should be connected to your Silverback server. Return to the Silverback admin console for the next steps.

3.3.1. Configure the Silversync Server

Unlike previous versions of Silversync, all configuration is now handled via the Silverback admin console. If you navigate back to the Silversync Servers section of the admin console as per the above steps you should now see your Silversync server there and connected. If you don't see it, refresh the page.

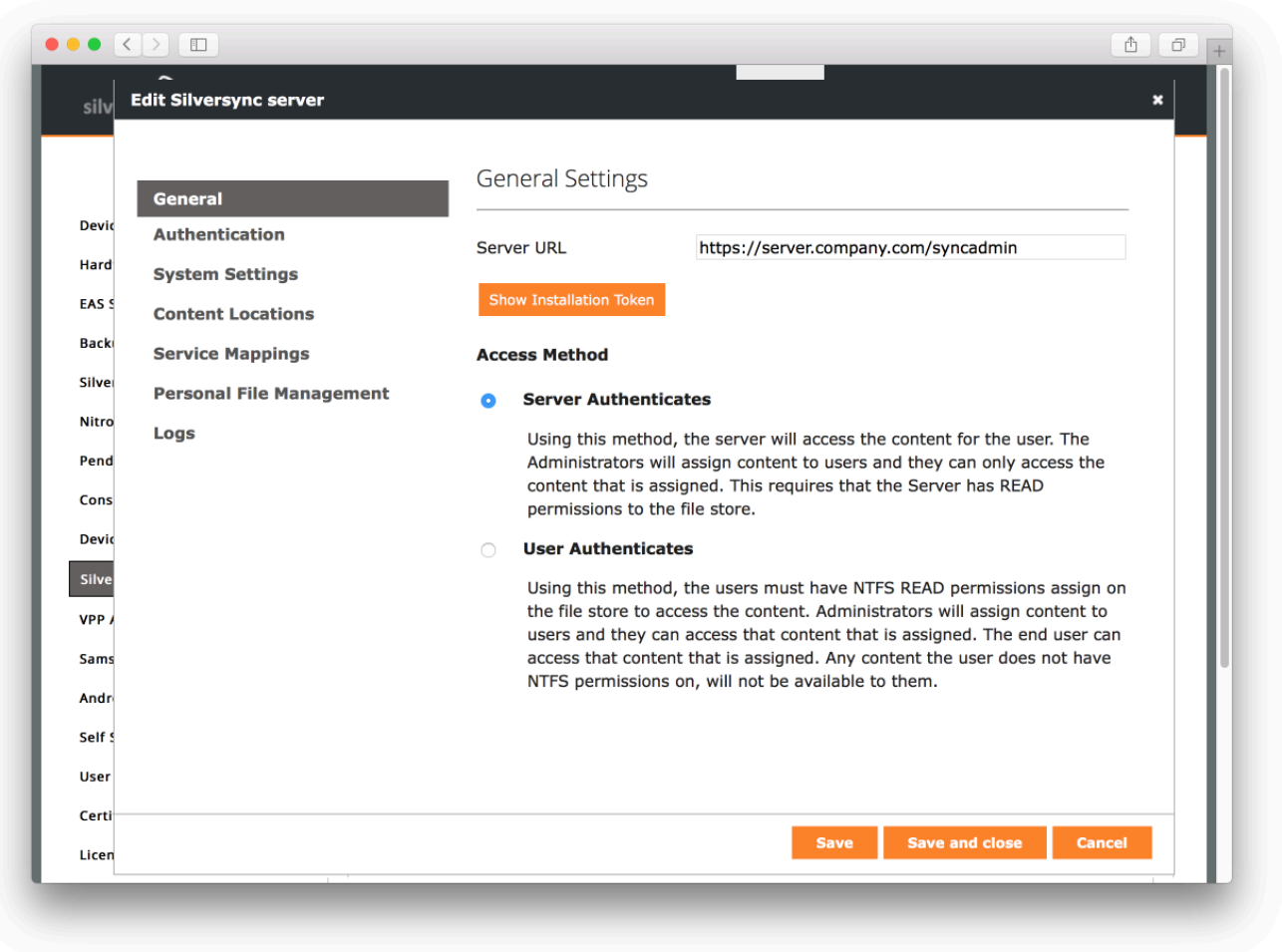
You should see your server, with a last connection time and IP Address:



Click Edit on the server to open the server properties.

On the General tab you need to specify the Access method. This determines how users will access files:

- Server Based authentication means that the service account on the server will access the files on behalf of the user. This means only the service account for the Silversync server needs access to the files.
- User Based authentication means that the individual user's file permissions are used. This means that a user must be granted read permissions on a file before they will be able to sync it.



The following two sections cover configuring both, you should only complete one of these, either server based or user based.

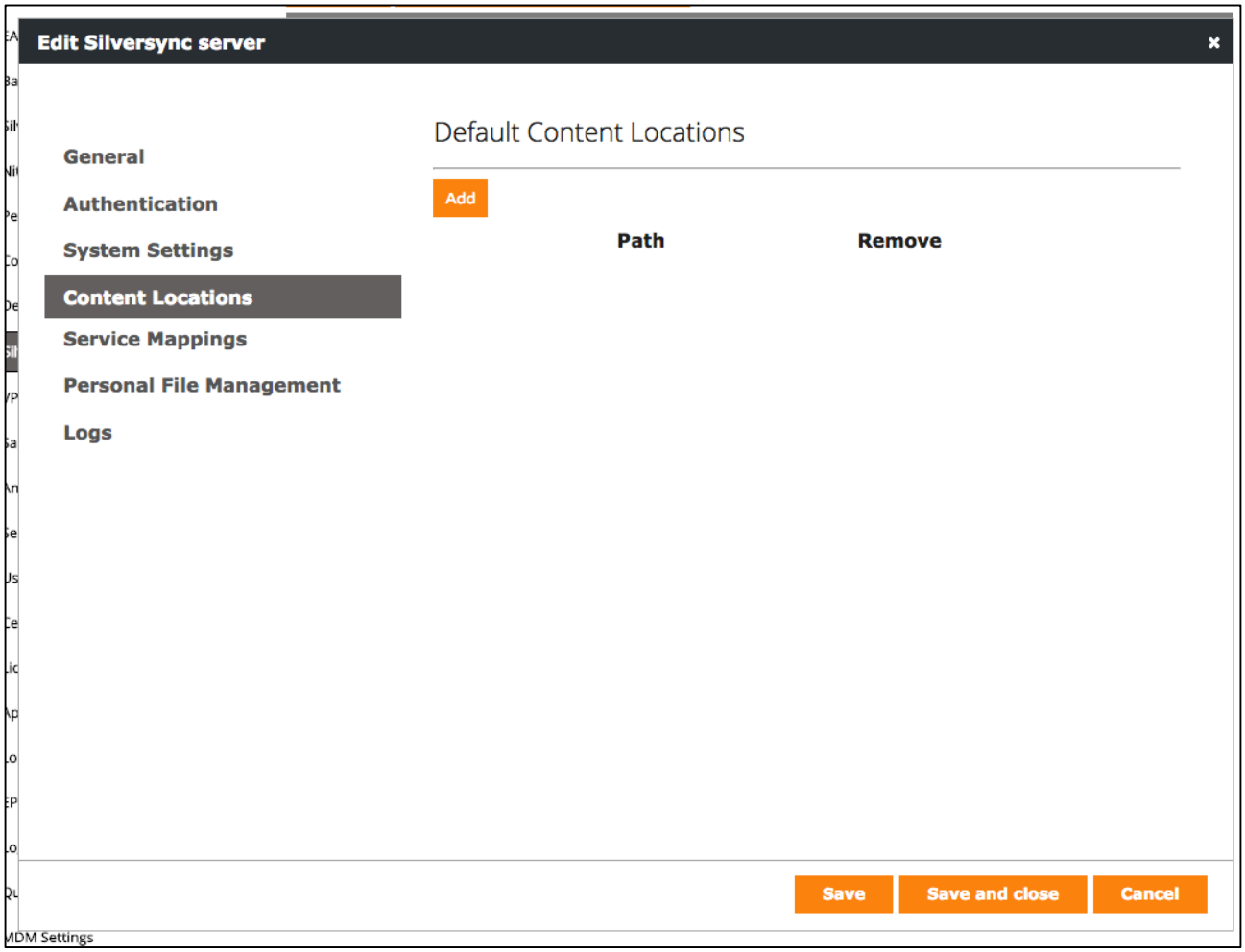
Note: If you do not see the "User Authenticates" option, this likely means that your Silversync server is not domain joined. This is a requirement for User based authentication.

3.3.1.1. Configuring Server Authenticates Endpoint

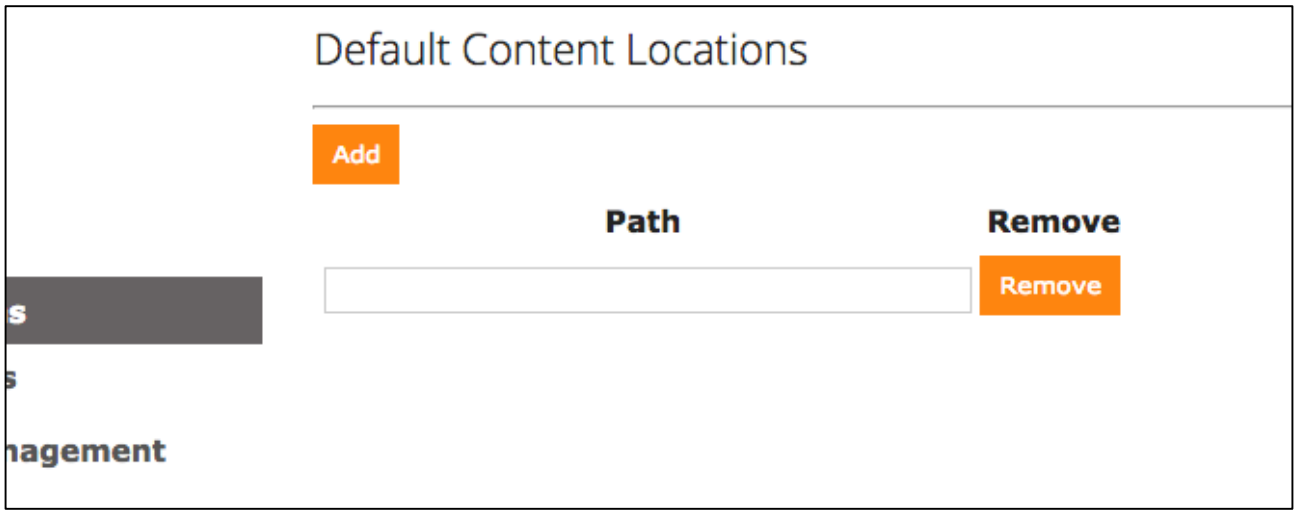
Server Authenticates is the functionality that the legacy Silversync system used. This means that the server has an account that needs permissions on all files users will synchronise, and access to the files is governed by Silverback and the Tags assigned to the user.

To configure this, first ensure that “Server Authenticates” is selected from the General Tab as in the screenshot above.

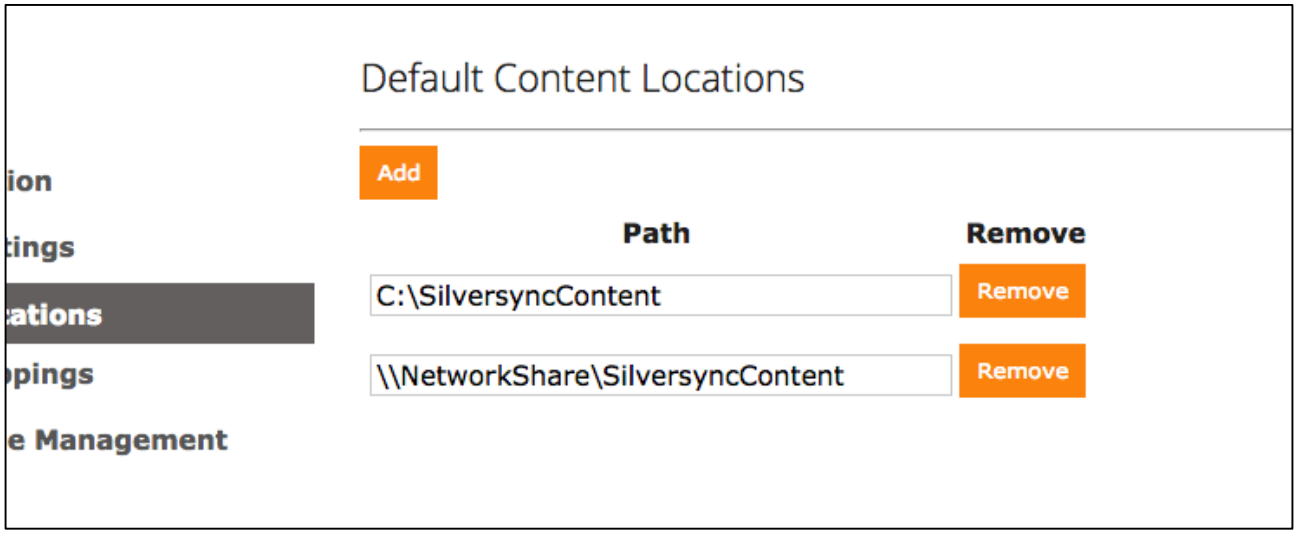
Next Navigate to the Content Locations section from the menu. You should see the following screen with no Content Locations entered:



Click the Add Button, and a new Content Location field will appear:



Enter in the file path for the Content Location, note that this can be either a local file path (e.g. “C:\Files”) or also a path to a network share (e.g. \\Share\Files):



When you have added the locations, click Save in the bottom right and wait for the progress indicator to finish.

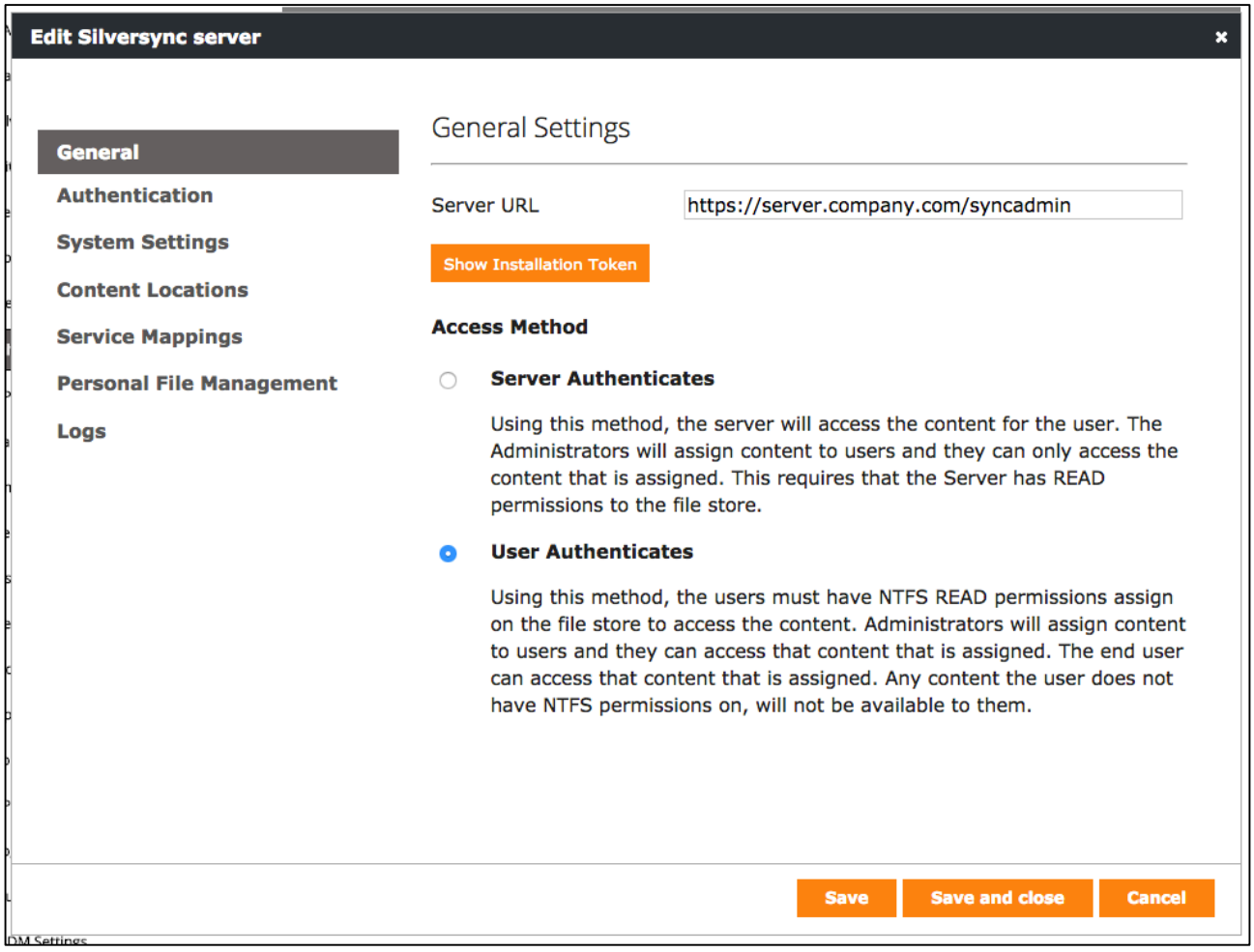
The Server Authenticates content locations are now configured.

3.3.1.2. Configuring User Authenticates Endpoint

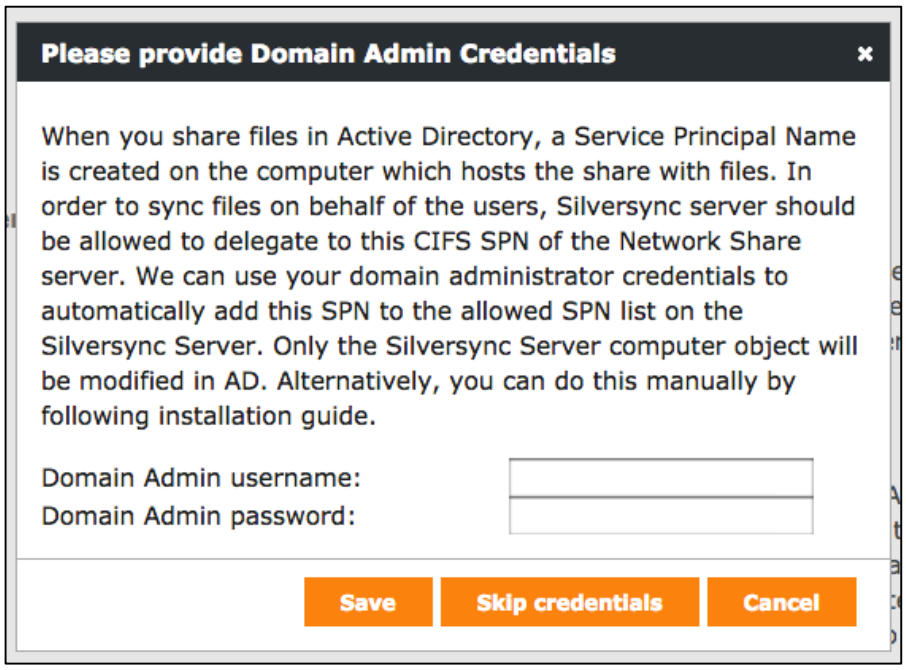
User Authenticates endpoints require that the user themselves have permissions on the file store. This means that access to the files is not managed by Silverback, but managed by the actual file permissions themselves. This means to grant users access to files you need to assign the file permissions separately.

Because Silverback doesn't store a user's password, the system needs to check file permissions on behalf of the user and this means that some extra steps are required to configure a Content Location for this method.

To configure this, first ensure that "User Authenticates" is selected from the General Tab:



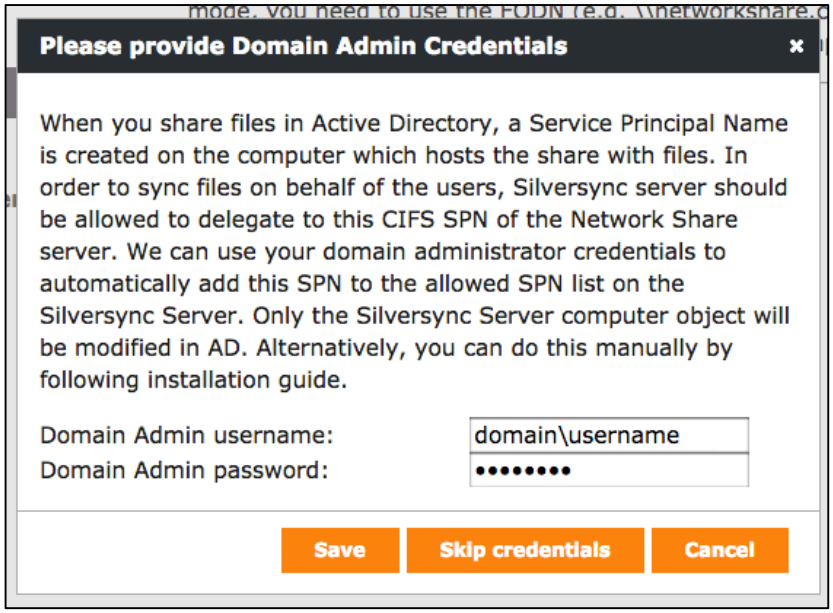
After selecting this, click Save to apply the change, and you should get the following prompt:



Please read the text on this page as it's important to understand why Domain Administrator credentials are needed. If you do not want to enter Domain Administrator credentials here, you will need to manually configure the Silversync server for file access for users.

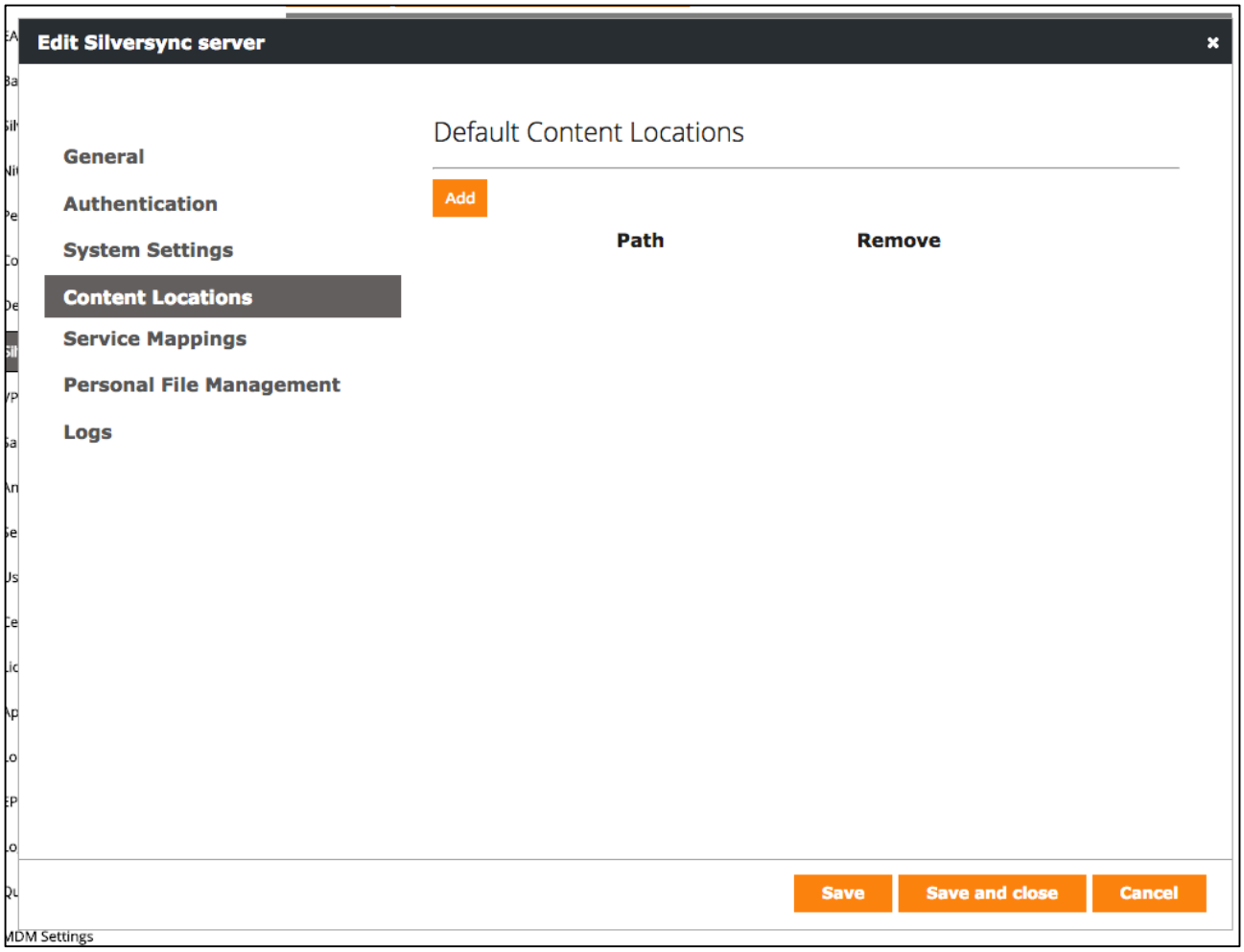
Note: Please see Appendix B at the end of this document if you wish to configure this manually.

Enter your Domain Administrator credentials and click Save. Ensure these are correct, because there will be no authentication error if you enter these incorrectly:

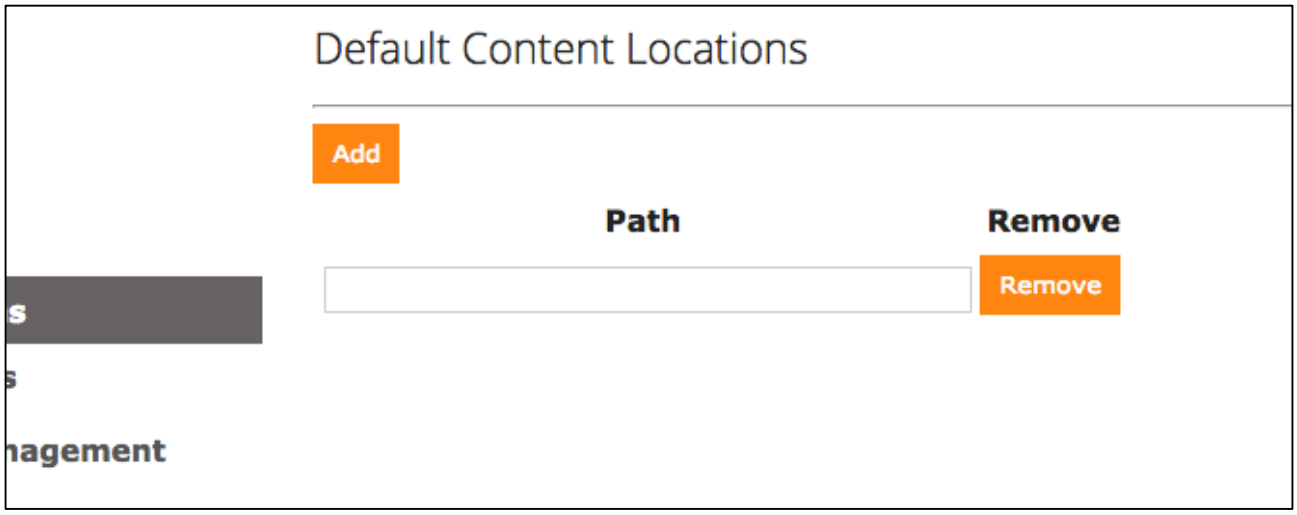


After this, the server is configured to allow creating connections to files for users, however we still need to add the content locations.

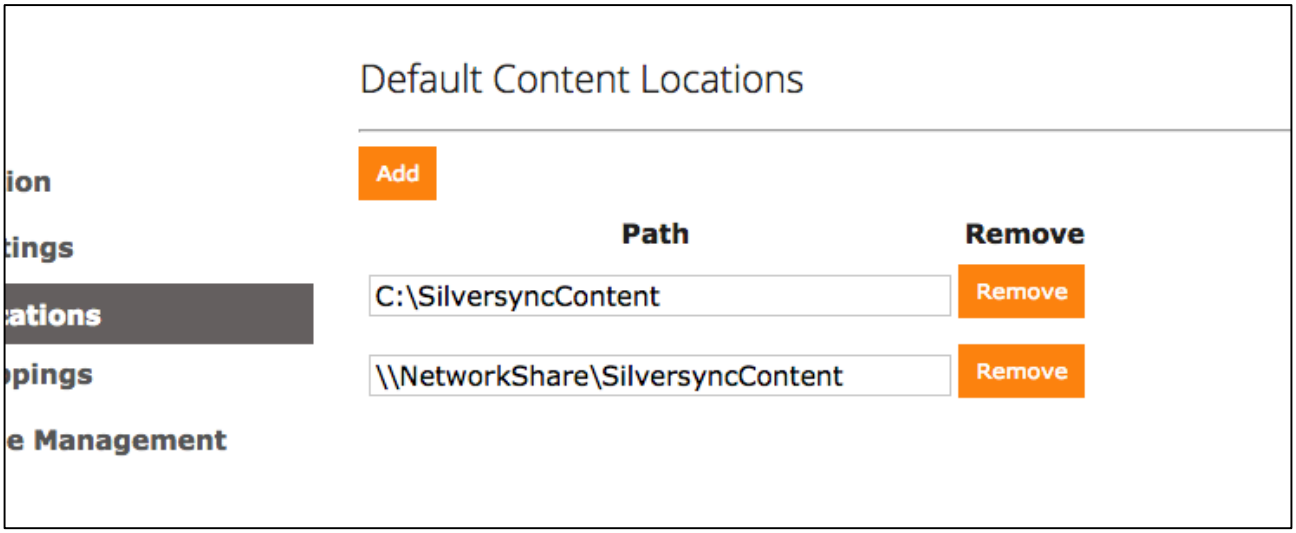
Next Navigate to the Content Locations section from the menu. You should see the following screen with no Content Locations entered:



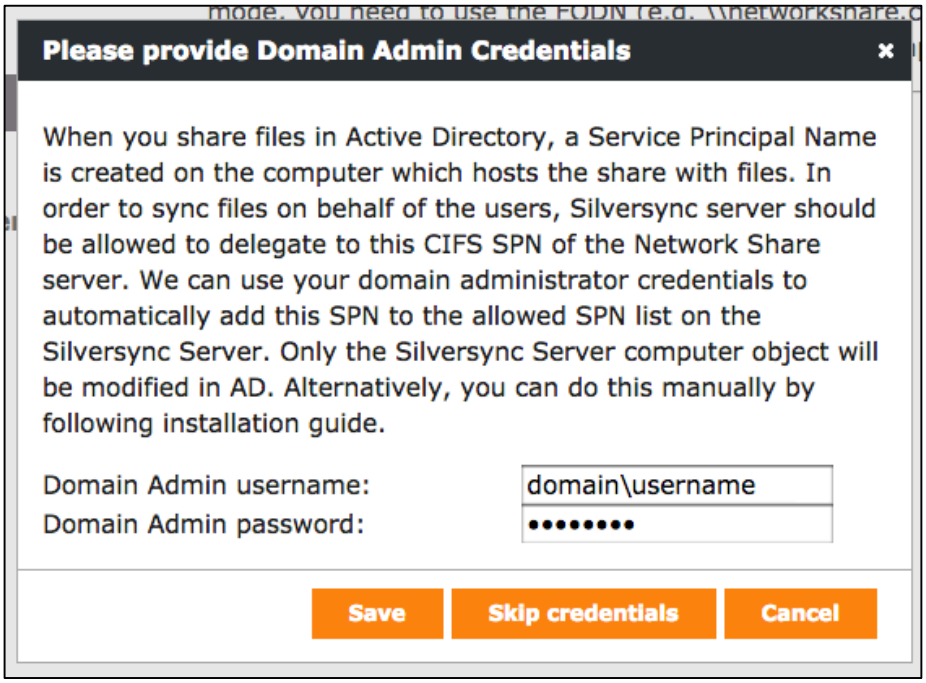
Click the Add Button, and a new Content Location field will appear:



Enter in the file path for the Content Location, note that this can be either a local file path (e.g. “C:\Files”) or also a path to a network share (e.g. \\Share\Files):



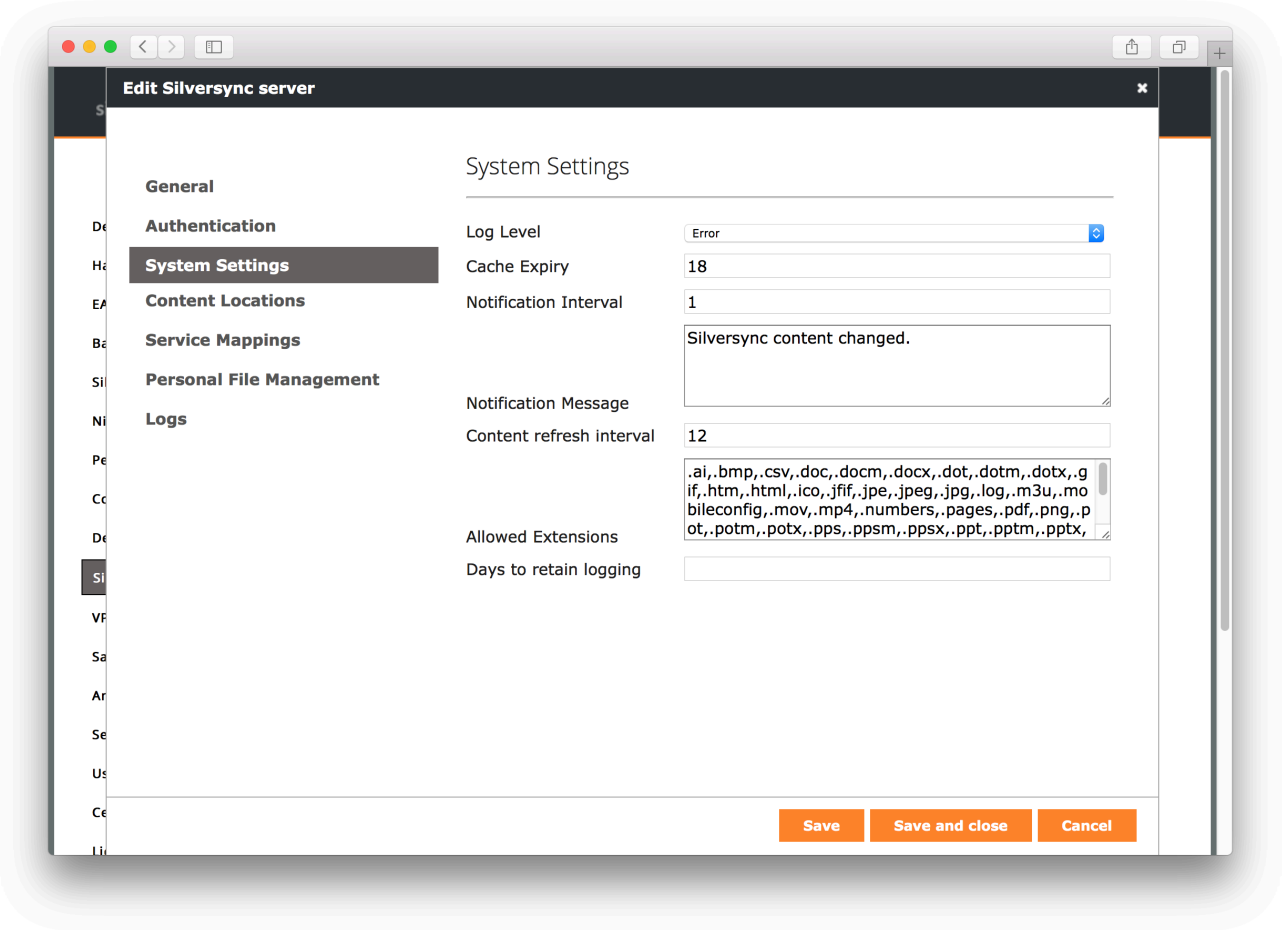
When you have added the locations, click Save in the bottom right. You will be prompted for the Domain Administrator credentials again. It’s important to note that the reason Silverback requires these credentials for every file path change is because we do not store the Domain Administrator credentials. This means we need to ask you each time. Because of this, it’s recommended to add all content locations at once before saving:



Wait for the progress indicator to finish and your User Authenticates endpoint is now configured.

3.3.2. Settings Tab

Next check the System Settings Tab settings for your system. Click on “System Settings”, and check the settings. In most cases this can be left as default.



The settings affect the system in the following way:

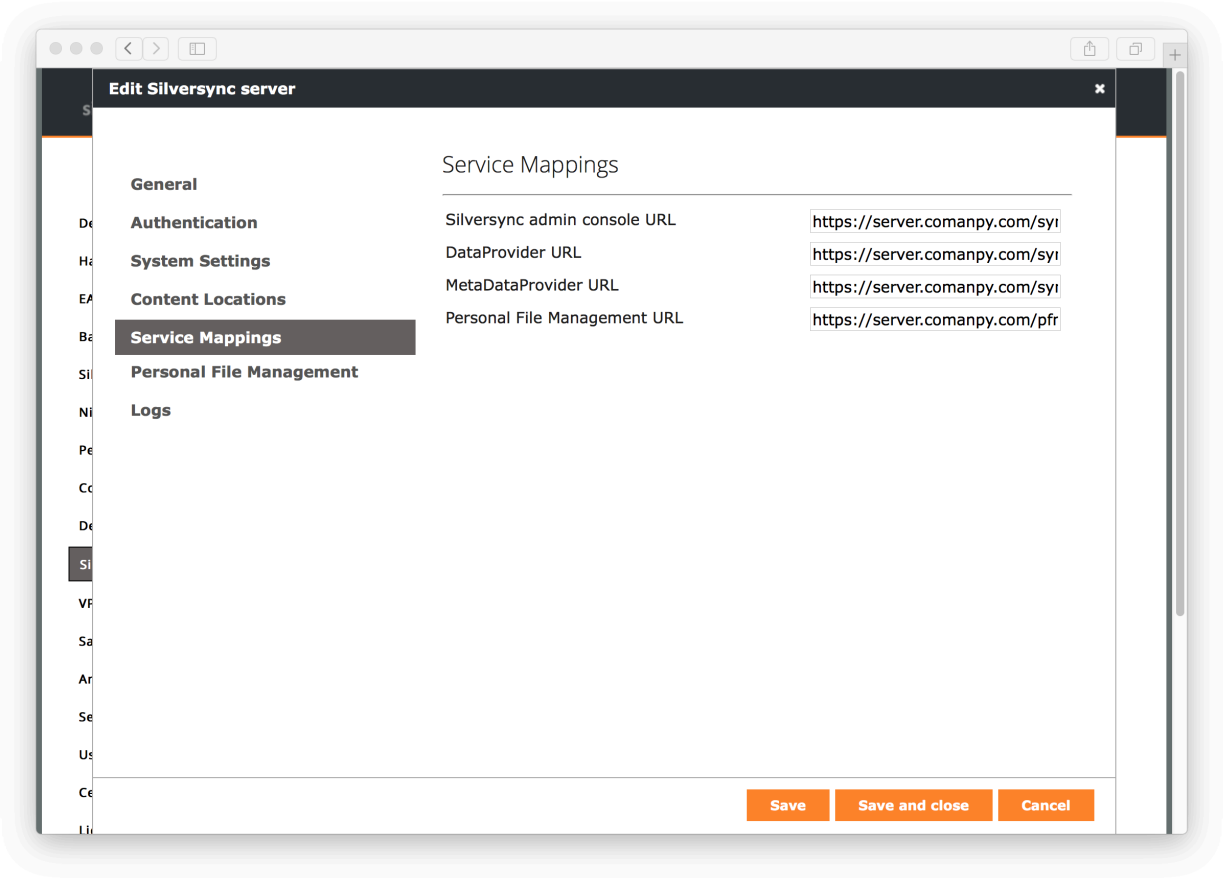
- Log Level – This is the amount of detail included in the logging, this should mainly be changed for troubleshooting purposes
- Cache Expiry – How long until the cached will be cleared. Caching the content helps speed up synchronization, but it should not last for a long time as it takes system resources to maintain.
- Notification Interval – How long in minutes the system should wait before sending another push to a user. This prevents the user from being notified multiple times when copying several files. This prevents the user from getting, for example five notifications instantly if you copy five files to the content location.
- Notification Message – This is the message that is sent to the user when content changes are detected
- Content Refresh Interval – How long until the system will refresh the entire content location for the users. In general, this can be left, as individual file changes are automatically detected.

- Allowed Extensions – This lets you determine what file types should be recognised by Silversync. Files not on this list will be excluded which is helpful for filtering out system files, or file types that users might not be able to open.
- Days to retain logging – How many days should the Silversync logging be kept before being removed.

After you've checked these settings click on the Service Mappings tab.

3.3.3. Service Mappings

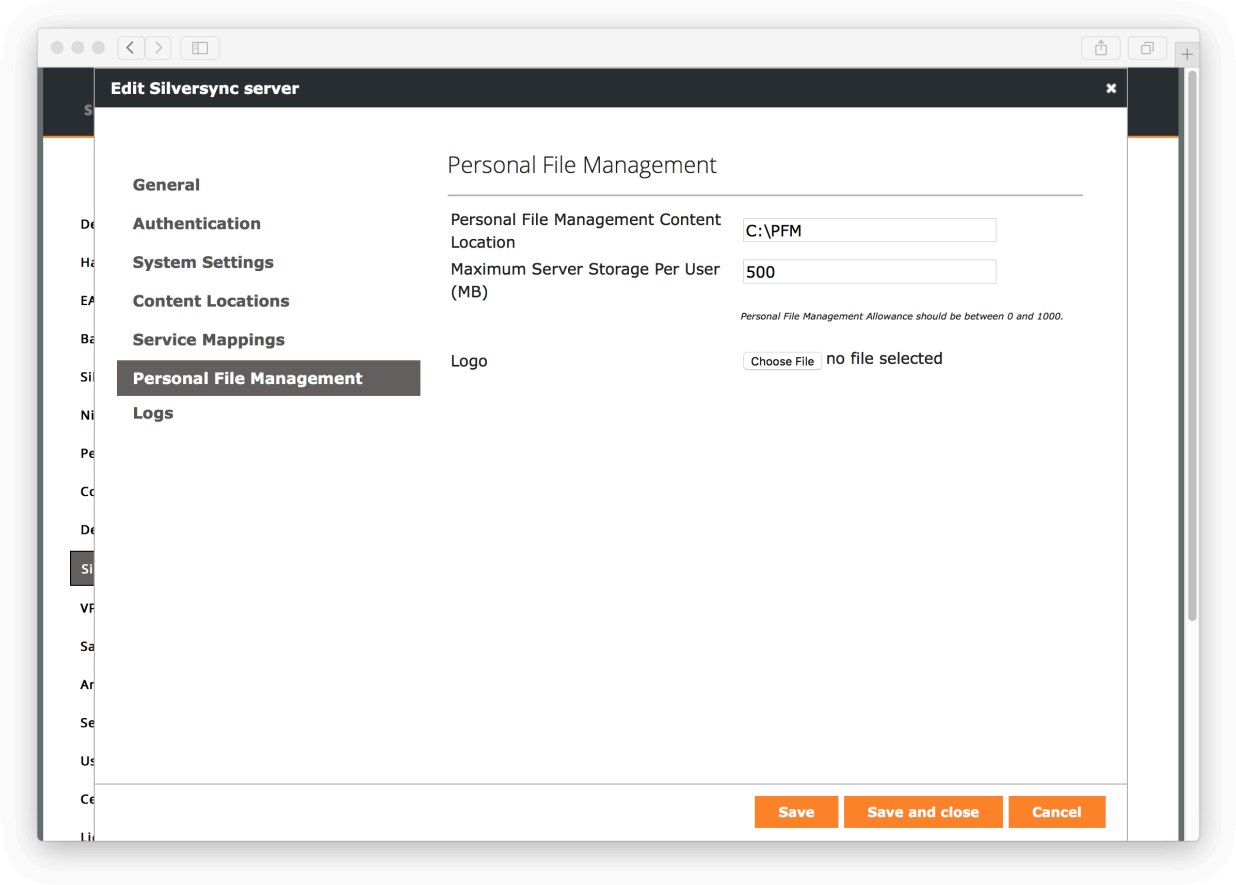
Service Mappings determine the location of web services for access by users and applications. It's recommended to leave these as default, but also ensure you check that it matches the DNS entry for your Silversync server. It should be automatically populated with your server URL:



After verifying the URLs are correct, click on Personal File Management

3.3.4. Personal File Management

This optional module lets users upload their own content into Silversync. Note that the files in normal Content Locations defined above are READ only. Personal File Management is a user's own personal storage space. The settings on this page let you configure the requirements for this.

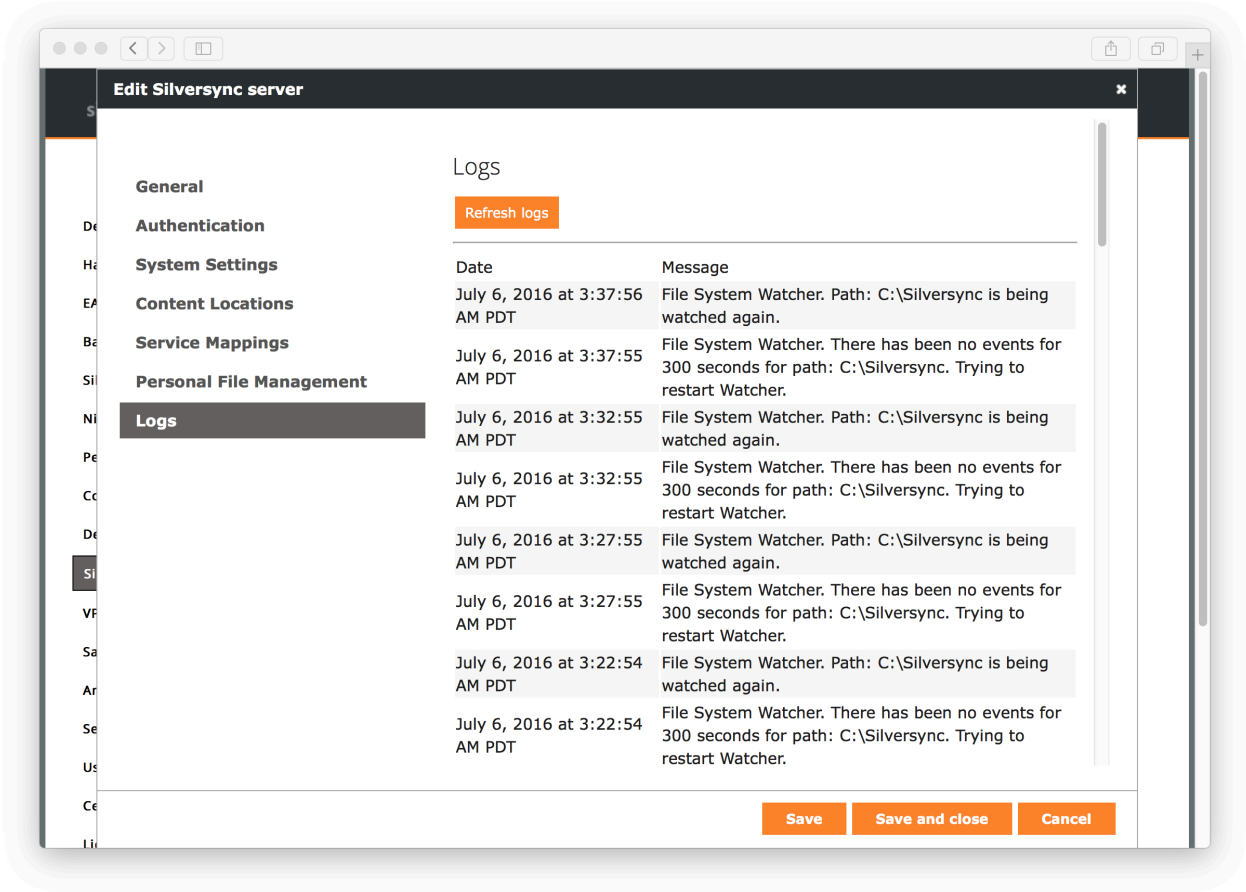


- Personal File Management Content Location – This is the location relative to the Silversync server to store Personal File Management uploads by users. Leave this blank if you do not wish to use PFM.
- Maximum Server Storage Per User – The maximum size in megabytes that a user is allowed to consume on the server. This is per user, so keep this in mind when planning available storage, that this number should multiply with every new user in the system.
- Logo – Lets you upload a logo file that will be shown to users in the PFM console. This helps with branding to give users a common feel with your other company pages.

Next, click on the Logs menu item.

3.3.5. Logs

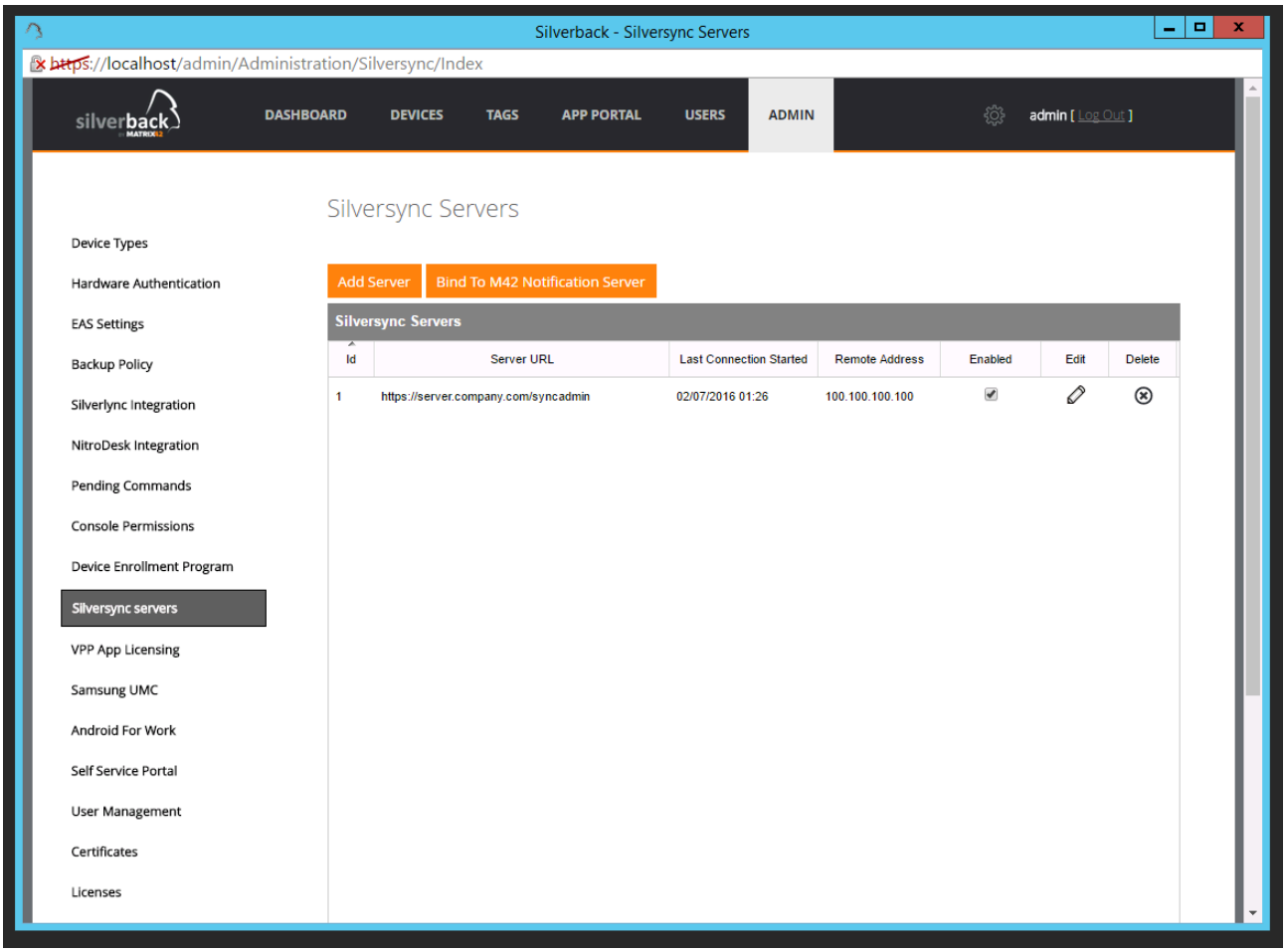
Logs doesn't require you to configure anything, but its useful to know how to access this page. This is where logging can be found for your Silversync server. If you need to troubleshoot a problem, or confirm that new content is being picked up, you can check this page.



3.3.6. Binding Push

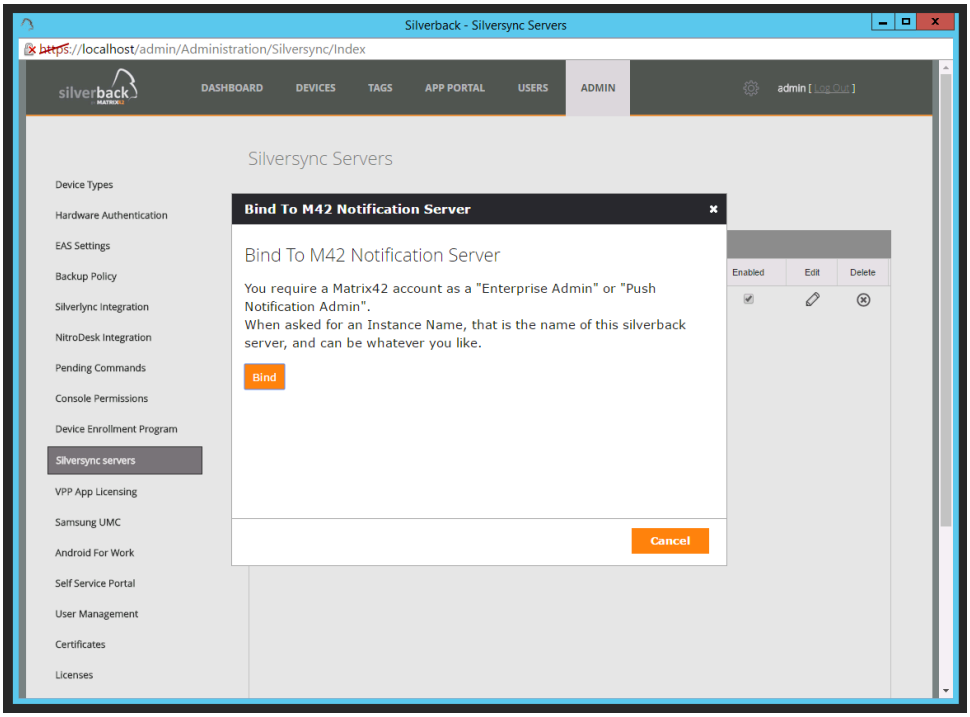
Previously Silversync used its own push certificate for notifying users of new content. In this version, Silverback connects to the Matrix42 push service for you to handle push notifications.

To enable this, you need to bind your server to the M42 Notification Server. This is done from the Admin console in the Silversync Servers menu item, by clicking “Bind to M42 Notification Server”.

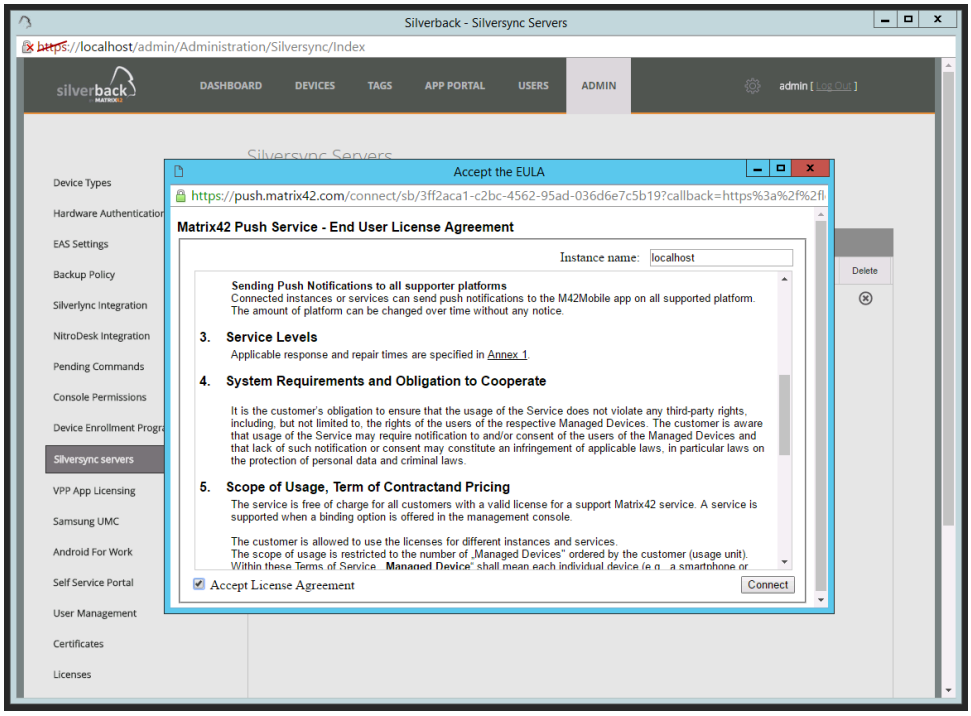


Silversync Installation Guide Version 5.1 U3

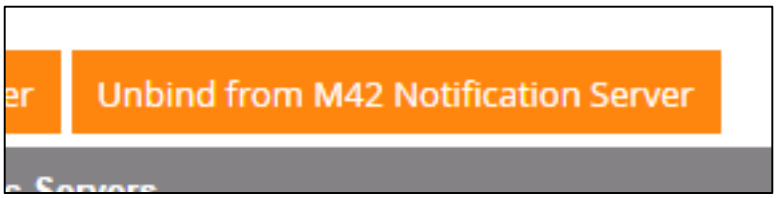
You will get a popup to complete the binding. Ensure you have a Matrix42 account that matches the requirements in the popup, and then click Bind:



Login with your Matrix42 account, accept the EULA and click Connect:



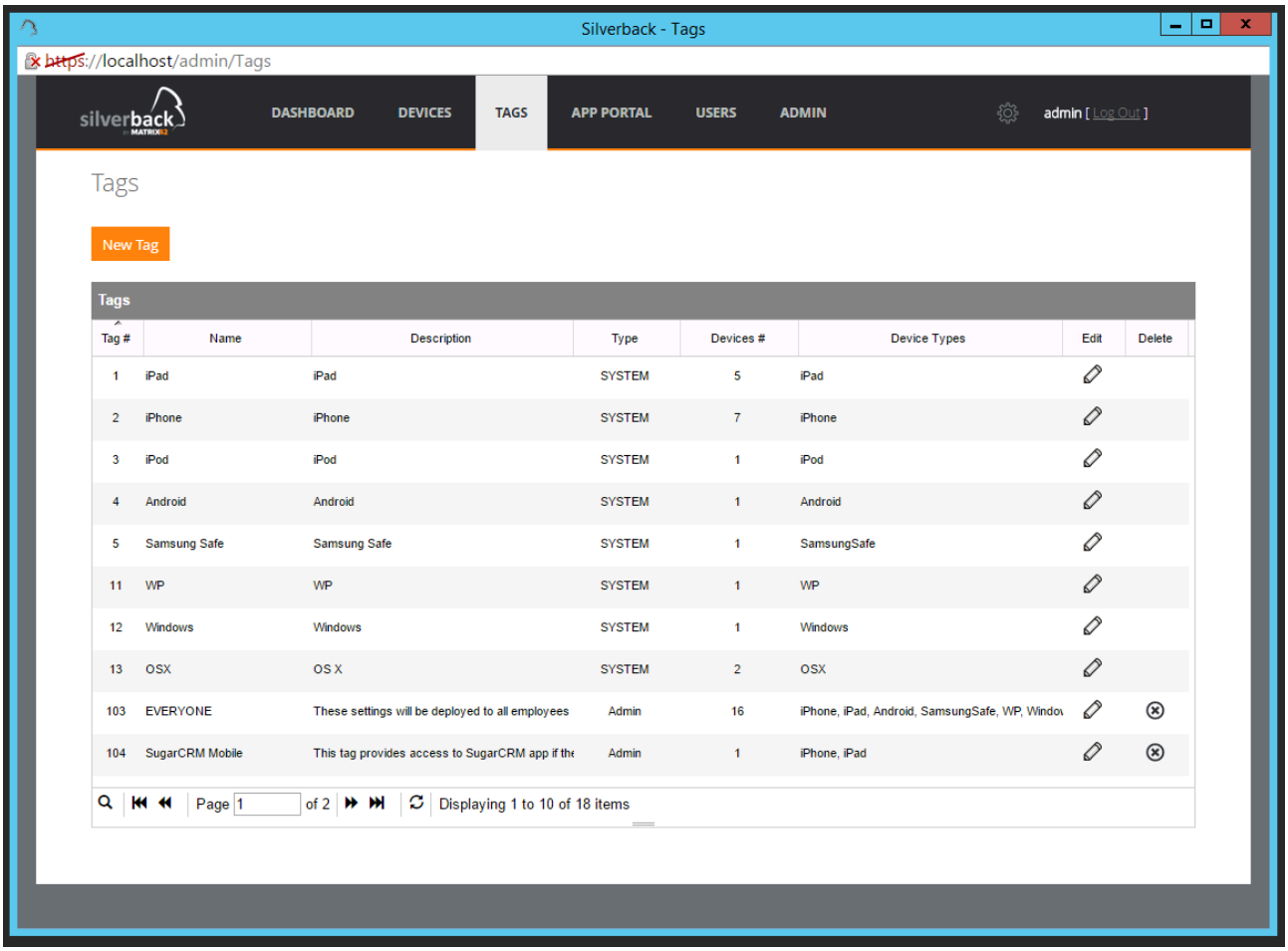
If this completed successfully, the button should change to “Unbind from M42 Notification Server”:



3.3.7. Assign Content to Tags

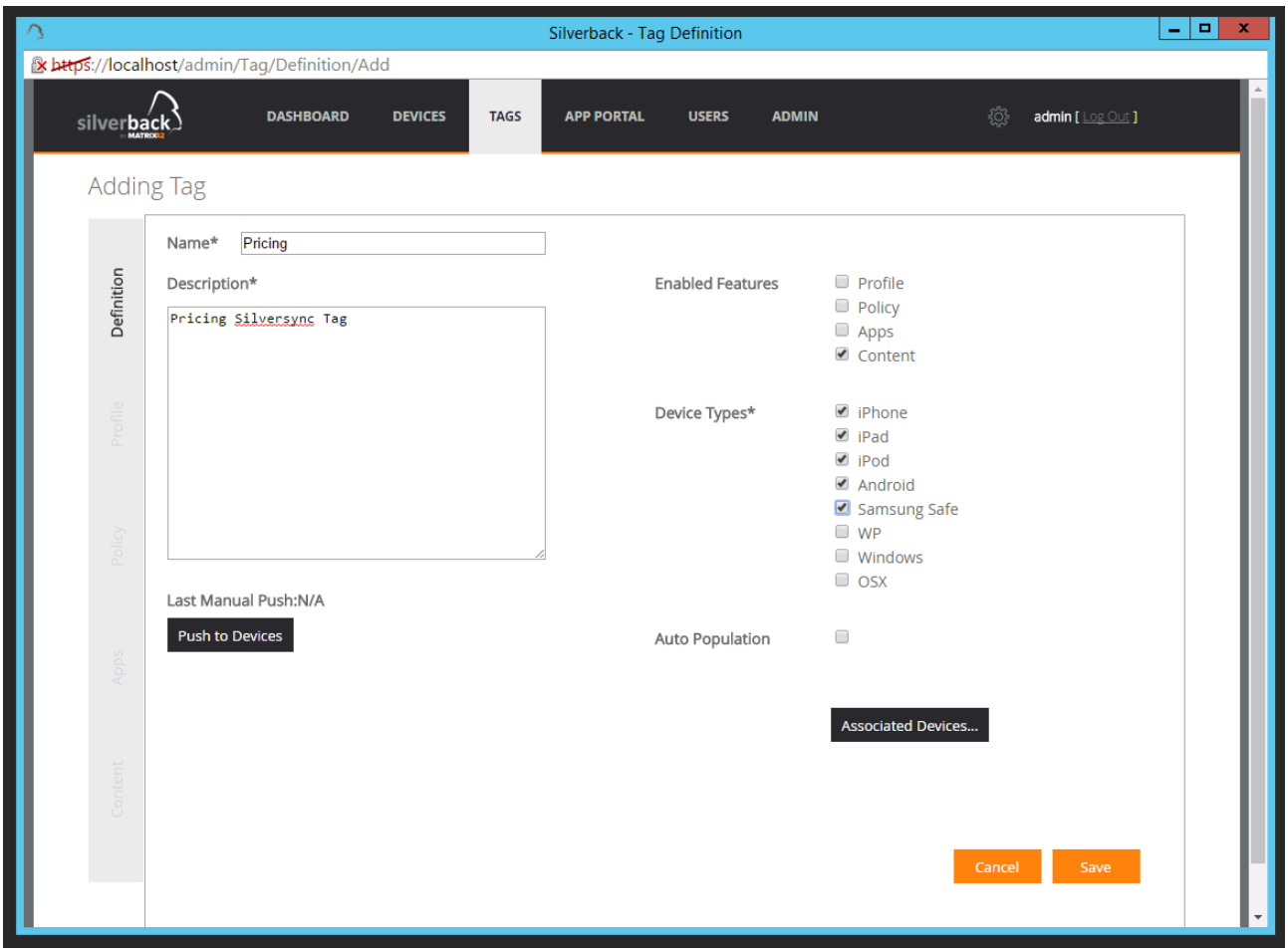
Now we will assign the content to Silverback Tags. Previously we’ve configured the server to run, but users still can’t synchronise any content. Note that with this step, you are free to create whatever Tags you would like, it’s not mandatory to use the Tag names and examples below:

Click the Tags upper menu item:



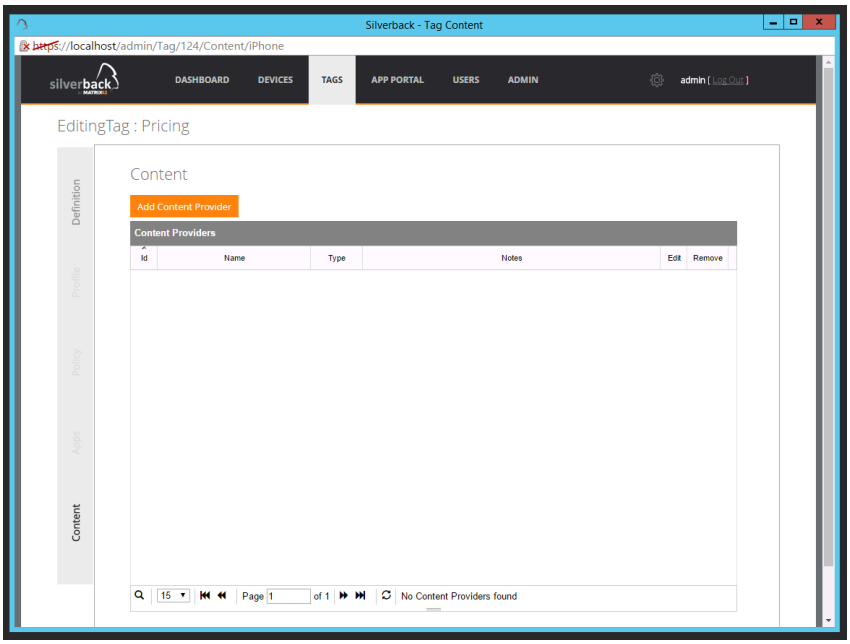
Then click “New Tag”:

On the New Tag page, enter the name of the Silversync Tag you want to create, make sure you enable the Content feature for the Tag and also enable the Device Types you want to allow access and click Save:



Silversync Installation Guide Version 5.1 U3

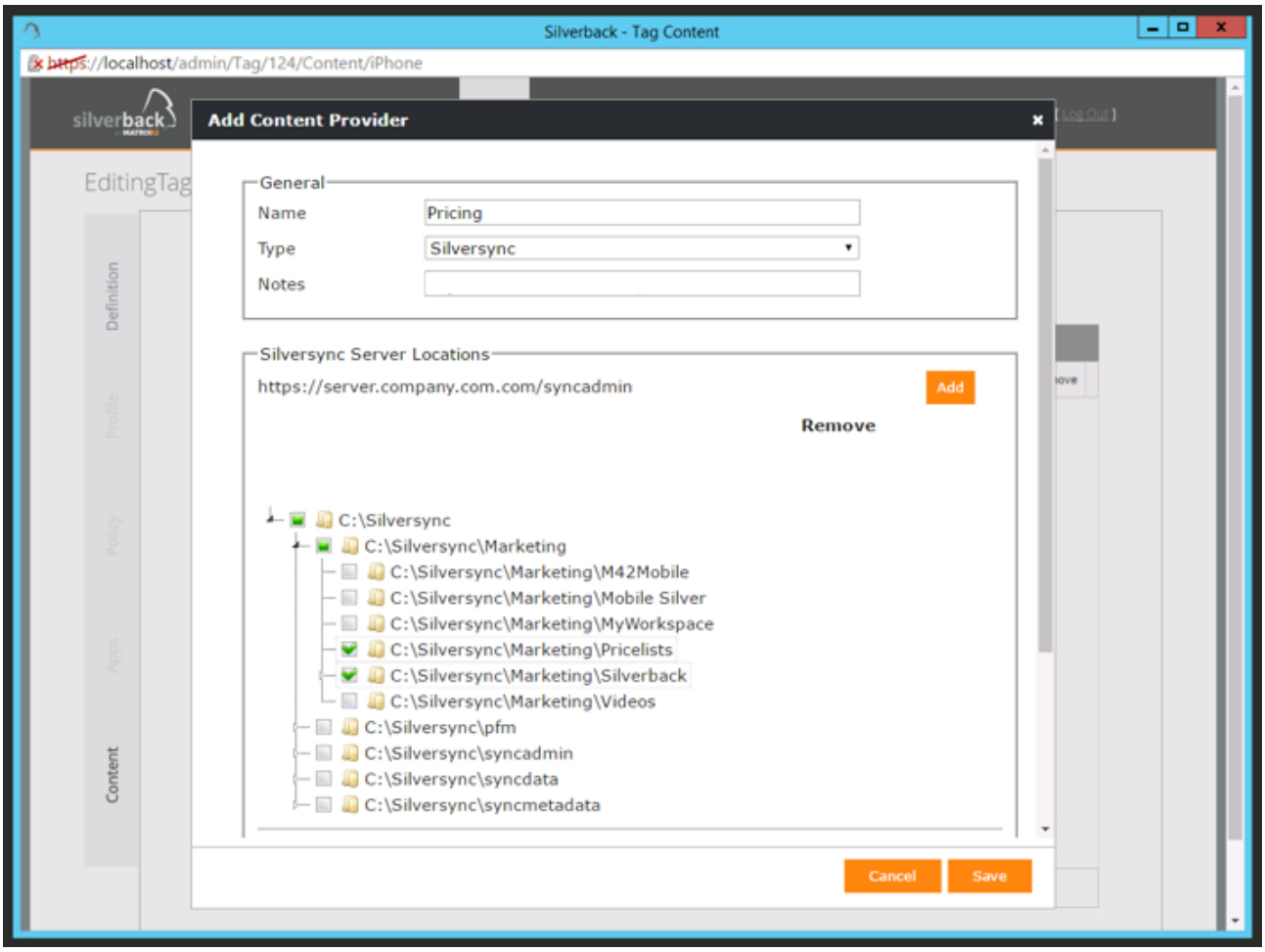
After saving, the “Content” Tab should be available from the left menu, click this to go to the Content Providers section:



Click Add Content Provider and you will be able to define the file paths. Give the settings a name and a note if required. It might be useful to use the note field to explain to other administrators what these settings are and what content they map to.

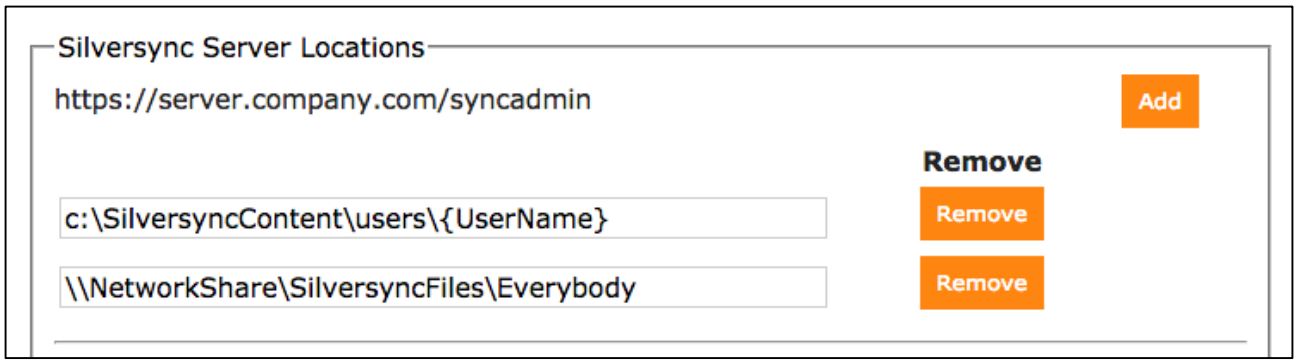
For assigning content, there are generally two ways to do this, either by selecting the folders from the Content Tree. You can expand and collapse folders if you want to assign content at a level down in the file system.

Silversync Installation Guide Version 5.1 U3



Note the Content Tree is only available for Server Based Authentication. If you are using User Based Authentication you will not be able to see this tree structure, and you must assign the content manually by typing in file paths.

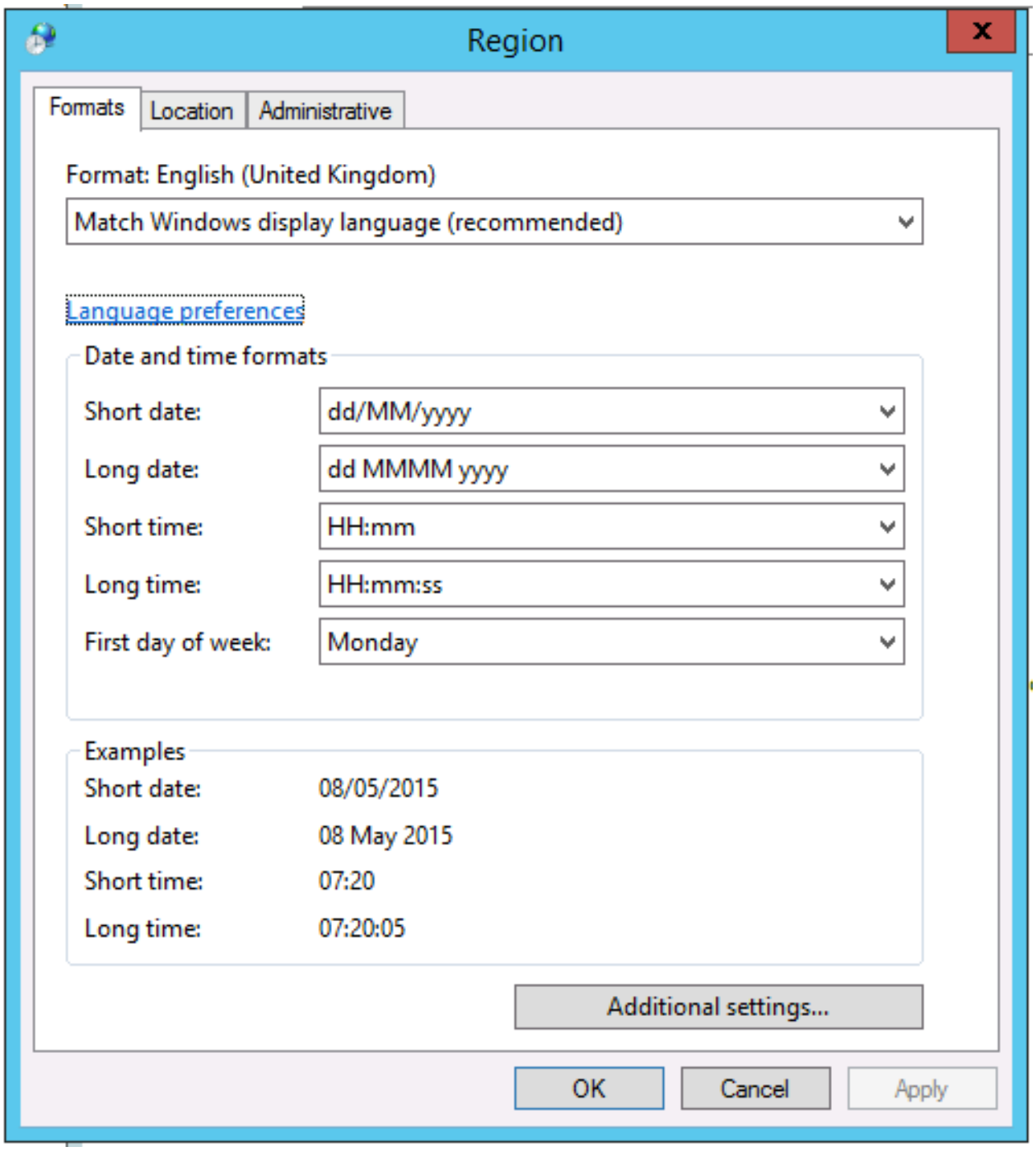
You can also assign content by clicking “Add” and typing a file path directly:

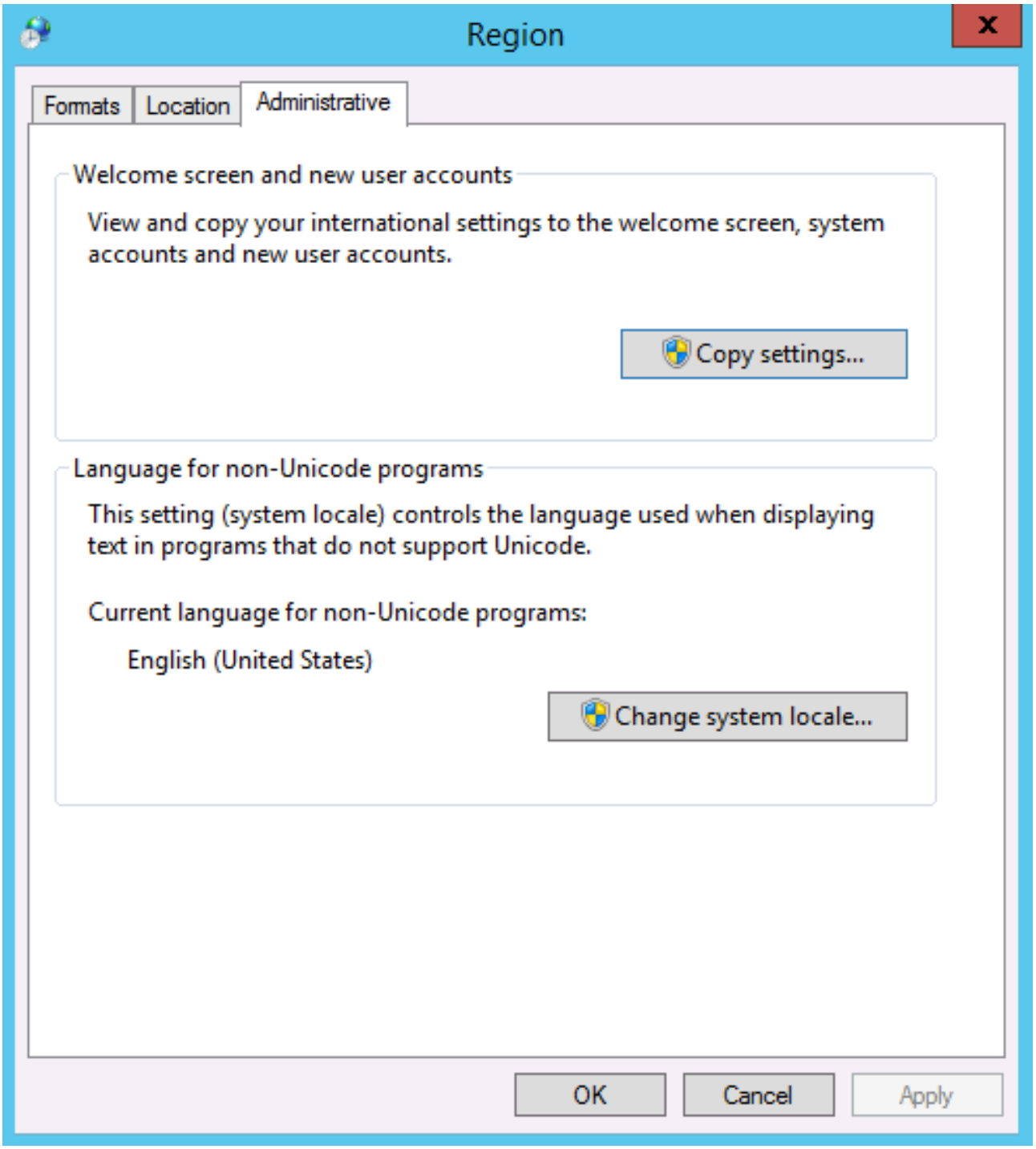


It’s important to note that these paths support system variables. In the example above “{UserName}” will be replaced with that unique user’s username. This is useful for mapping to a home drive network share for example.

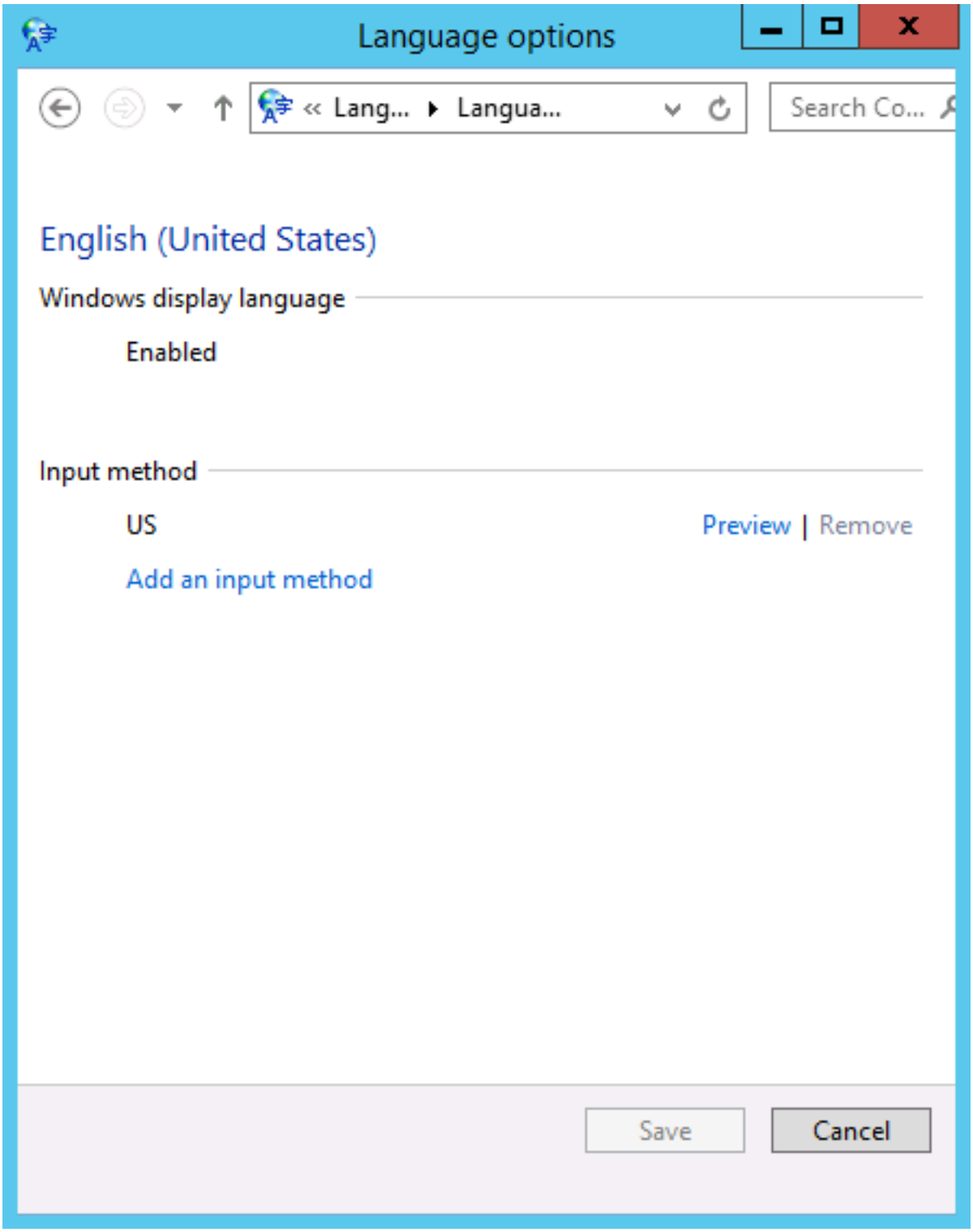
Repeat this section for any other Silversync Tags you want to create. You can add multiple file paths to one Tag if you would like, or create an individual Tag for every content location.

4. Appendix A – Example Region Format Screenshots




Region
Formats
Location
Administrative
Welcome screen and new user accounts
View and copy your international settings to the welcome screen, system accounts and new user accounts.
Copy settings...
Language for non-Unicode programs
This setting (system locale) controls the language used when displaying text in programs that do not support Unicode.
Current language for non-Unicode programs:
English (United States)
Change system locale...
OK
Cancel
Apply

Silversync Installation Guide Version 5.1 U3

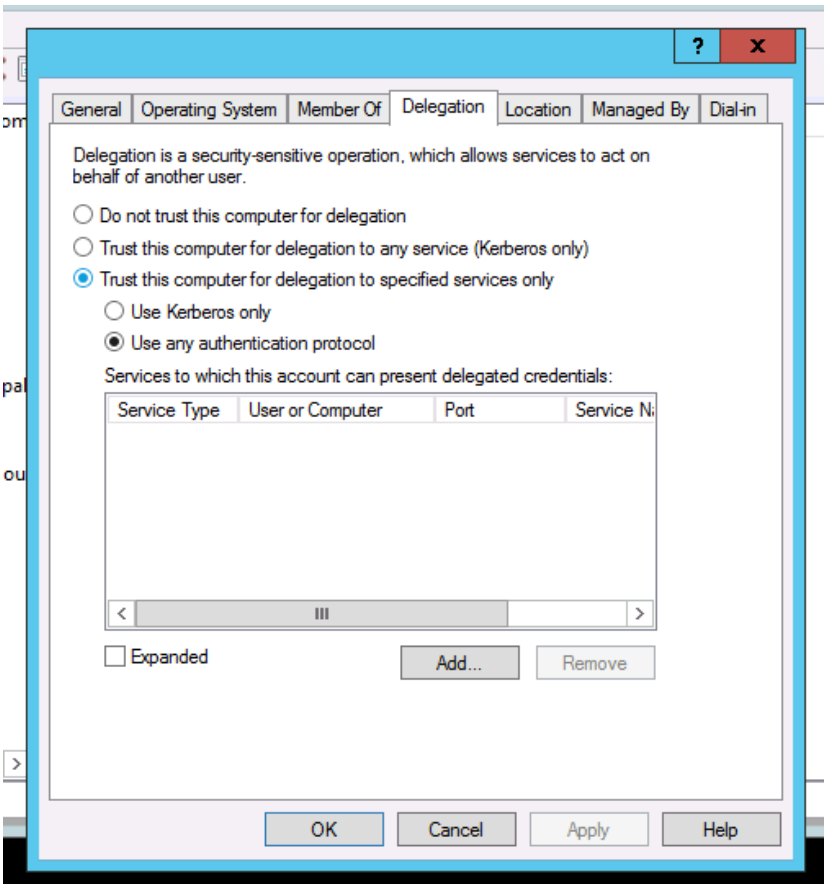


Author: Matrix42 Cloud & Mobile Management

5. Appendix B – Configuring User Based Authentication Manually

In some environments it might not be possible to enter domain administrator credentials into third party applications like Silverback. The system needs these permissions because it needs to established trusts in the Active Directory Domain so that the server is able to access files as the user. This lets Silverback determine if the user actually has permissions on the file.

To perform this process, you need to have someone with Domain Administrator privileges perform the following items for you. They will need to look at the properties in Active Directory Users and Computers for your Silversync server, and go to the Delegation Tab.



They need to ensure that like the above image, “Trust this computer for delegation to specified services only” is select, and beneath that “Use any authentication protocol”.

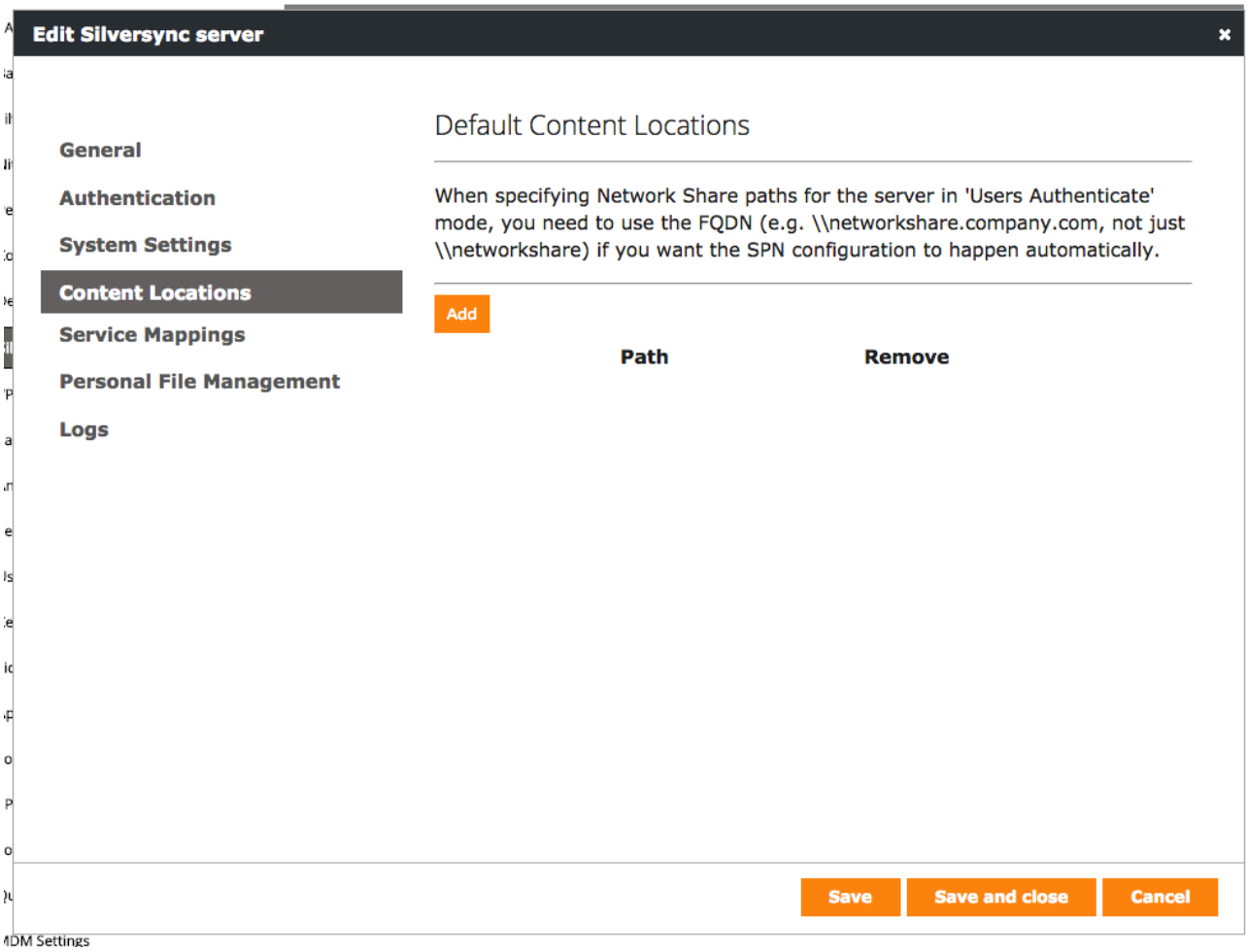
After they have applied these settings, we need to allow for the actually delegation of permissions.

There are two difference types of delegation we can add, one for local files to the Silversync server (e.g. “C:\Files”) and network shares (e.g. \\RemoteServer\Share). These require slightly different processes, and we will cover both in the examples below.

Silversync Installation Guide Version 5.1 U3

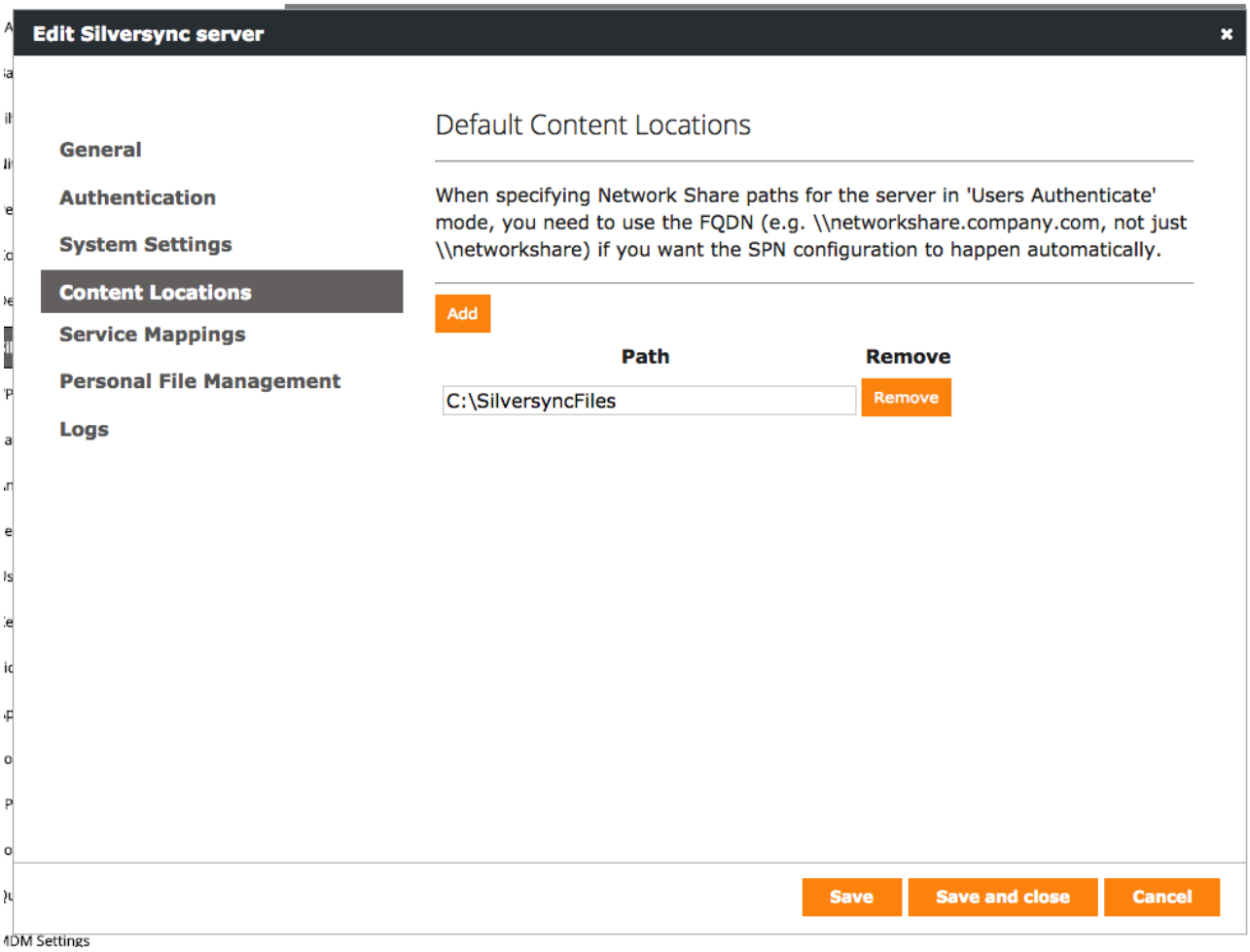
First we will add a local path, and then add the SPN to the server for this delegation.

Edit your Silversync server and go to the Content Locations Tab:

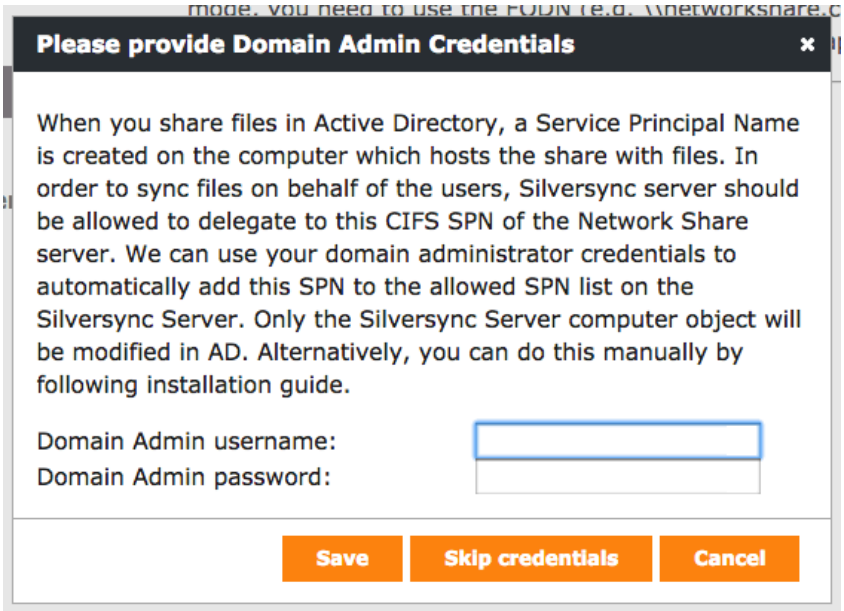


Silversync Installation Guide Version 5.1 U3

Click the “Add” button and enter your local file path:



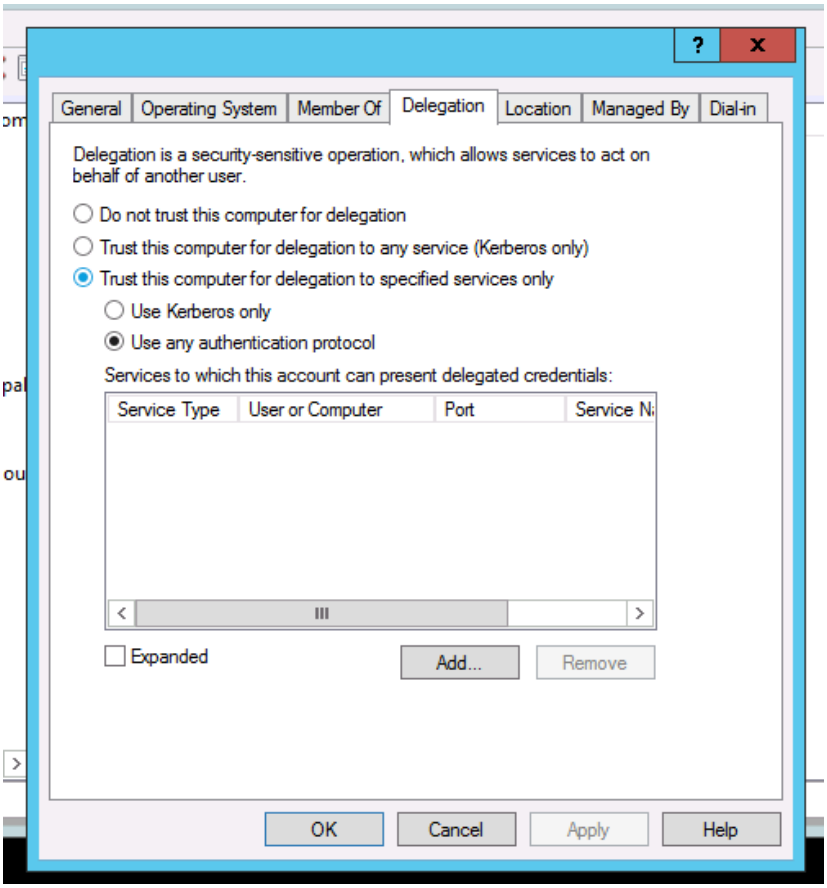
Click “Save” and when prompted, click “Skip Credentials”.



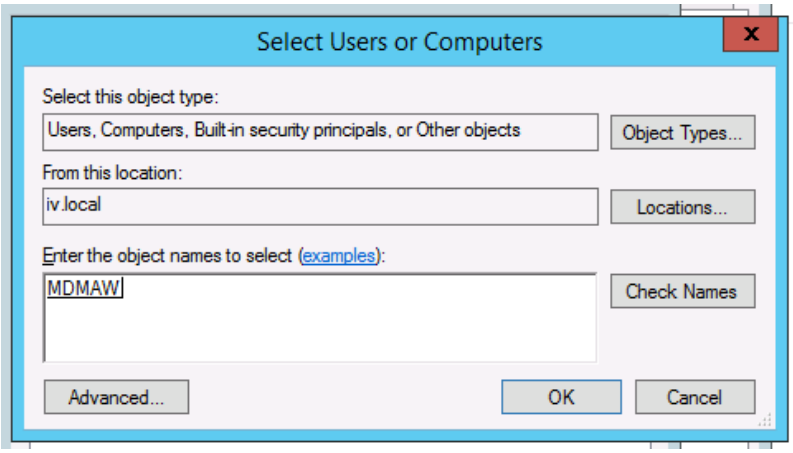
Silversync Installation Guide Version 5.1 U3

Now you need to instruct your Domain Administrator to add the “SPN” which will allow users to synchronise to this location. Tell them to open Active Directory Users and Computers and find your Silversync server computer object, right click and open Properties for it. Then navigate to the Delegation tab.

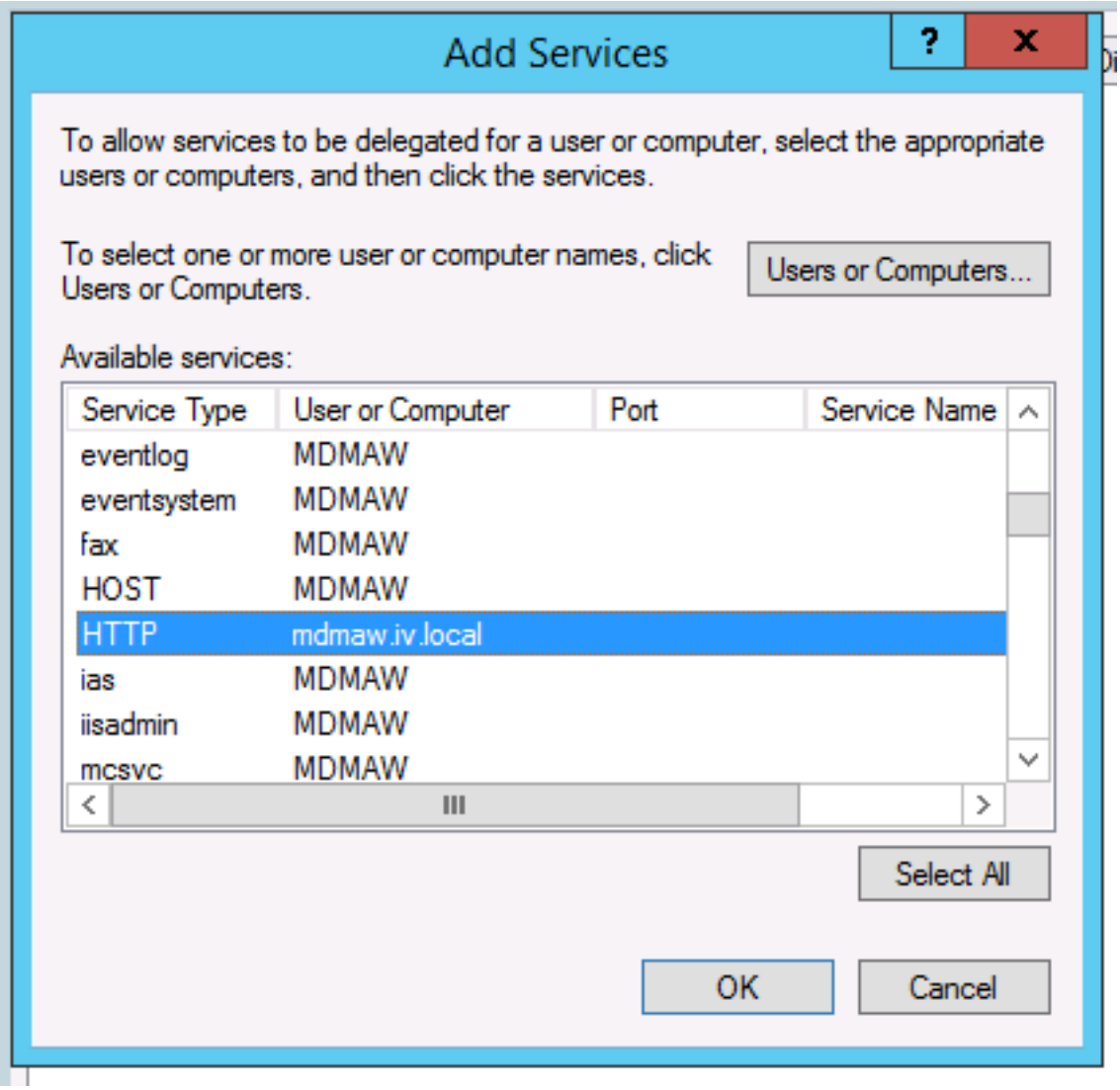
Click “Add”:



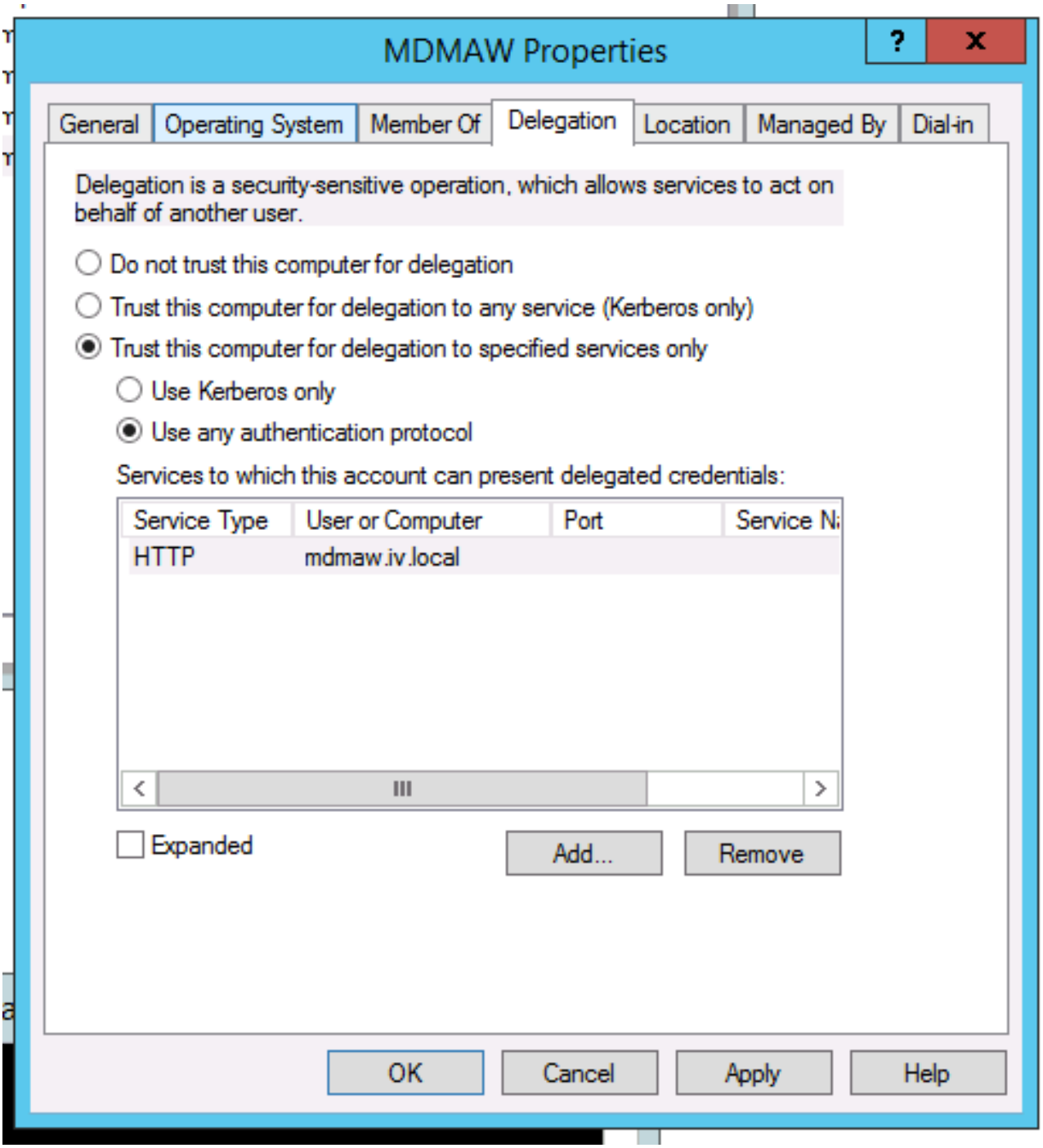
Find your Silversync server object and click OK:



Then on the Add Services screen, scroll down until you find “HTTP”, select it and click OK:

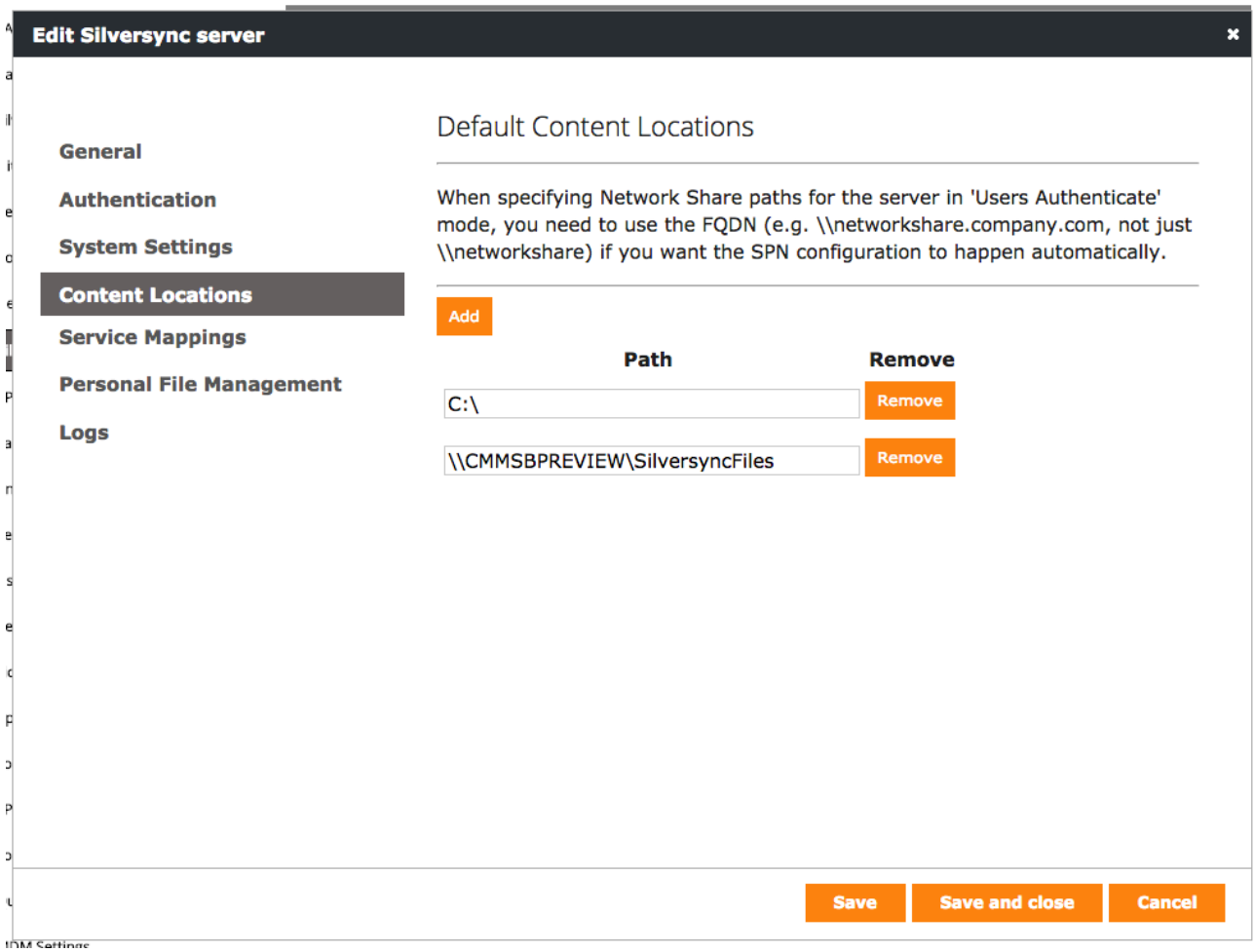


You should now have the HTTP service registered for this server:

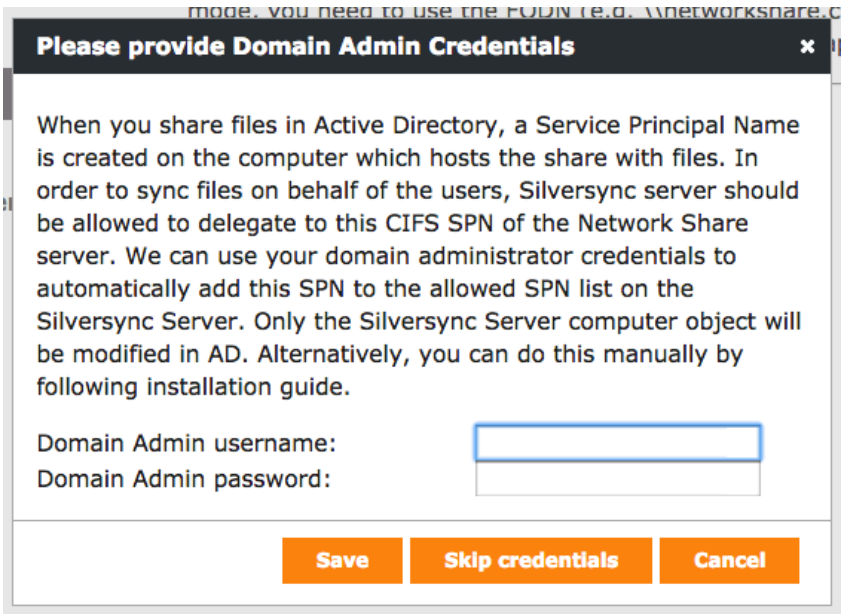


Silversync Installation Guide Version 5.1 U3

Next we will add a network path example. Navigate back to your Silversync server Content Location Settings, click “Add” and enter the network share location, for example:

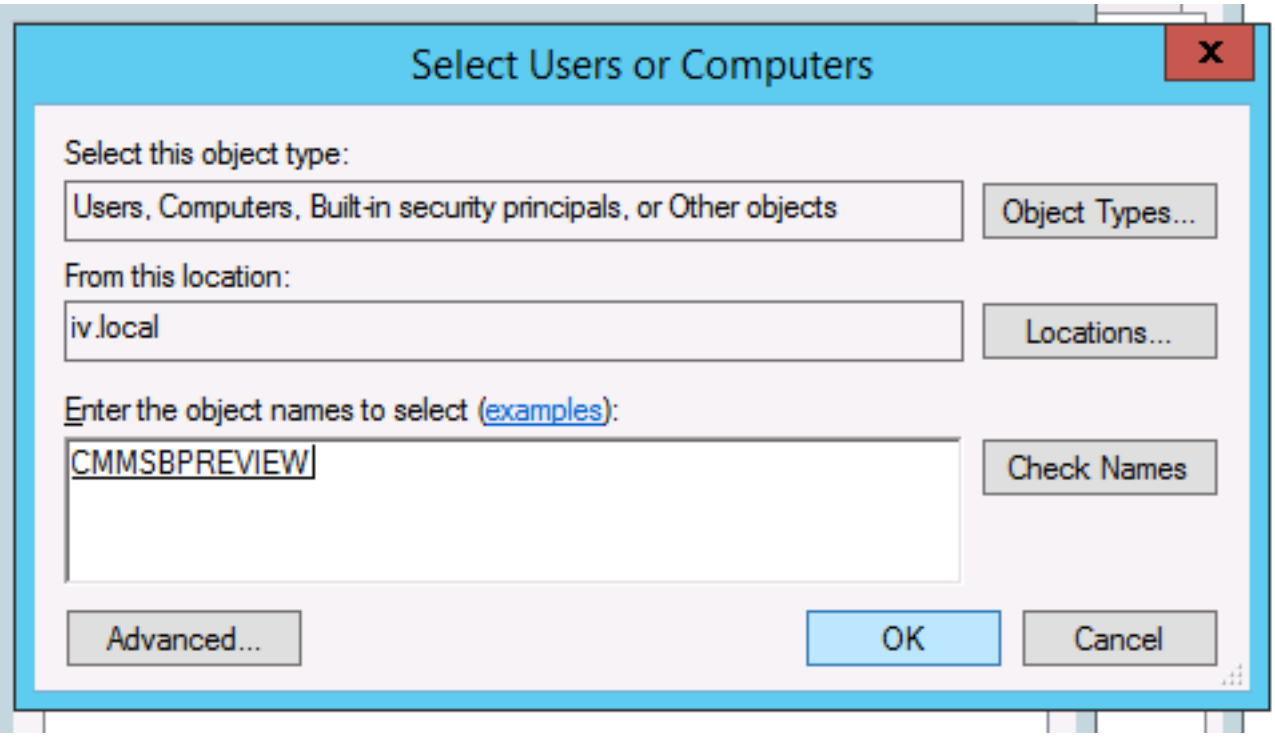


Click “Save” and when prompted, click “Skip Credentials”.



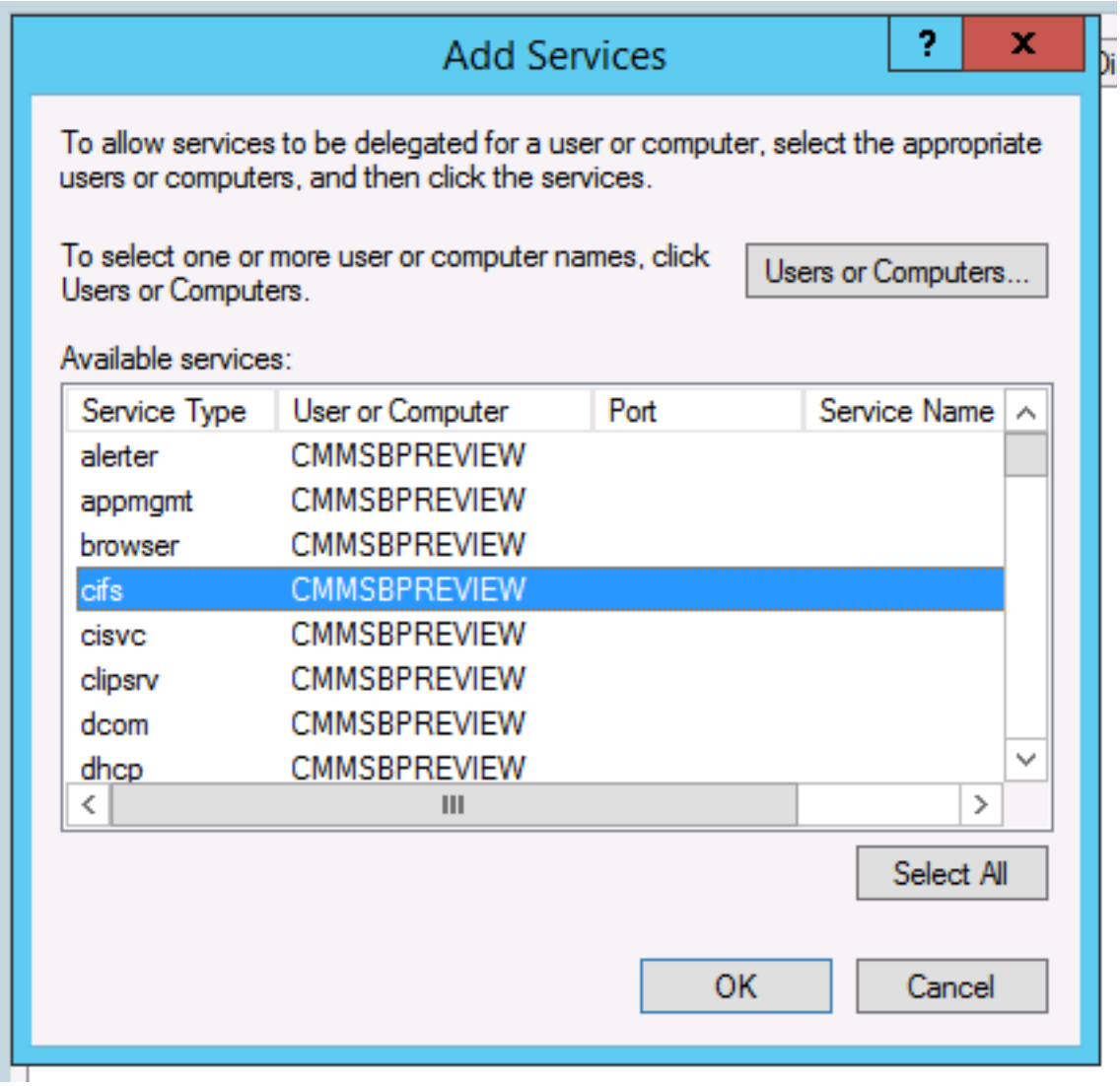
Now we need to add a different service to let users access this. Have your Domain Administrator edit the Properties of your server again, and under the Delegation Tab click “Add”.

Now we need to search for the remote server where the share is located. This will be a different server to the local one added previously:



Click OK, and then on the following screen, select the “cifs” entry and click OK. This will create the link between this server and the remote server for delegation.

NOTE: If you are directing users to a DFS share, you must add the delegation for ALL members of the DFS environment individually. Repeat these steps for all members.



Complete these steps for any more local or remote Content Locations, and then follow the Tag assignment steps listed earlier in the document to actually assign the content to users.