

Table of Contents

1 Microsoft ADFS 2 Integration.....	1
2 Overview.....	2
3 Updates.....	3
4 Prerequisites.....	4
5 How to Guide.....	5
5.1 Swivel Configuration Changes.....	5
5.2 Installing the Swivel ADFS Filter.....	5
5.3 Configuring the Swivel ADFS Filter.....	7
6 Additional Configuration Options.....	10
6.1 PINpad.....	10
6.2 Changing the Show TURING Button.....	10
7 Testing.....	11
8 Known Issues.....	12
9 Troubleshooting.....	13
10 Microsoft ADFS 3 Authentication.....	14
11 Microsoft ADFS 4 and 3 Authentication.....	15
12 Introduction.....	16
13 Requirements.....	17
13.1 Current Version Installer.....	17
13.2 Previous Versions.....	17
13.3 Version History.....	17
13.4 Networking Requirements.....	17
13.5 Configure Sentry Agent.....	17
14 Installation.....	19
15 Configuration.....	23
16 Using the Swivel Proxy.....	28
16.1 Proxy Configuration.....	28
16.2 Enabling the Proxy Web Application.....	29
17 Using the Authentication Provider.....	30
18 Advanced Features.....	34
18.1 Requiring Swivel Authentication for Single Applications.....	34
18.2 Customising the Login Page Look and Feel.....	35
19 Known Issues.....	36
19.1 Public Access to Swivel Server, Untrusted Certificates and TURING/Pinpad Images.....	36
19.2 Problems Registering the Authentication Provider.....	36
20 Uninstalling the Authentication Provider.....	37
21 Upgrading.....	38
22 Troubleshooting.....	39
23 Error Messages.....	40
24 Microsoft Office 365.....	41
25 Introduction.....	42
25.1 Video showing login to Office 365 using ADFS with PINpad.....	42
26 Prerequisites.....	43
26.1 Downloads.....	43
27 Baseline.....	44
28 Architecture.....	45
29 Installation.....	46
29.1 Configure The Swivel Server.....	46
29.2 Using additional attributes for authentication.....	47
29.3 ADFS Integration.....	47
29.4 Additional Installation Options.....	48
30 Testing the Installation.....	50
31 Uninstalling the Swivel Integration.....	51

Table of Contents

32 Troubleshooting.....	52
33 Known Issues and Limitations.....	53
34 Additional Information.....	54
35 Additional documentation.....	55
35.1 Swivel.....	55

1 Microsoft ADFS 2 Integration

2 Overview

This document describes how PINsafe authentication can be integrated with web-forms-based login for Active Directory Federation Services (ADFS). It works with ADFS web and ADFS proxy version 2. For ADFS version 3 see [Microsoft ADFS 3 Authentication](#).

3 Updates

NOTE: updated to version 1.2.1.15 to fix error in JavaScript when allowing unknown users.

The version linked to below is version 1.2.1 The following changes have been made from 1.1.5:

- Client DLL and web pages for Swivel image proxy etc. have been incorporated into the filter DLL
- More granular logging available

There were several minor updates between version 1.1 and 1.1.5: mainly bug fixes.

The following changes were made between versions 1.0 and 1.1:

- Fixed some bugs in the login page customisation
- More control over which features are available in the login page
- Ability to share configuration with other ADFS servers
- Ability to control logging of authentication attempts

4 Prerequisites

- ADFS version 2.0 or later, or ADFS 2.0 proxy.
- Swivel ADFS filter, downloadable from [here](#).

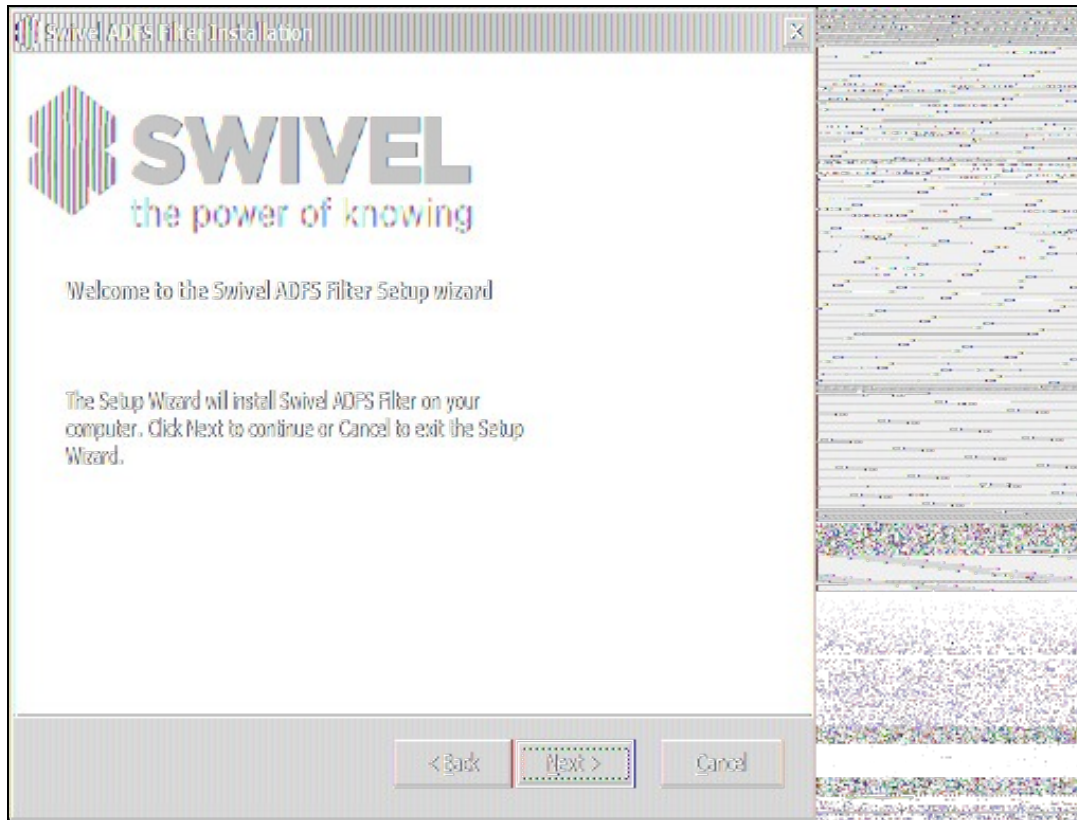
5 How to Guide

5.1 Swivel Configuration Changes

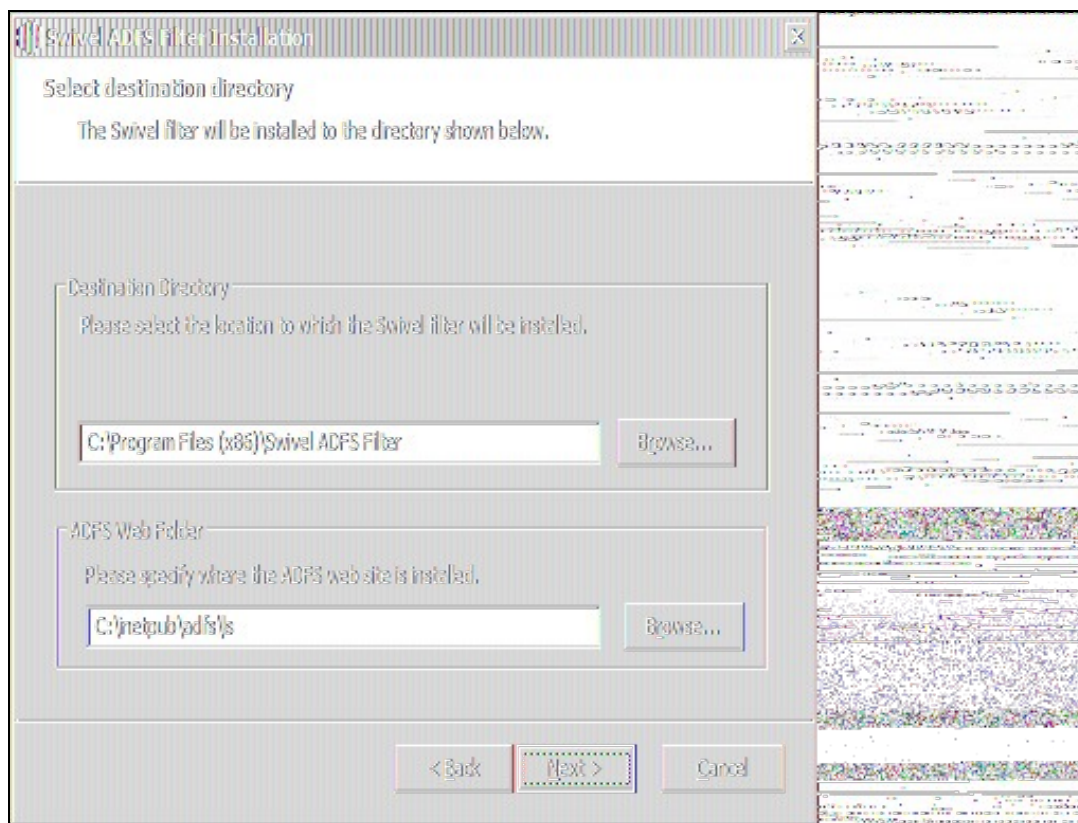
- Under Server -> Single Channel, ensure that ?Allow session start by username? is set to Yes.
- Under Server -> Agents, add the ADFS server as an Agent, and make a note of the secret you enter here.

5.2 Installing the Swivel ADFS Filter

Copy ADFSFilterInstaller.exe to the ADFS server and run it. Note that the program must be run as an administrator. You will see the following display:



Click Next to select the installation location:



You would normally accept the destination directory as default. Note, however, that if the ADFS Web folder is not in the default location, C:\inetpub\adfs\ls, then you should change the second location to match the correct location. Click Next when these values are correct.

The next screen allows you to specify the name for the Start Menu folder. You can also choose to install the menu for all users, rather than just the installer.

The next screen is a summary screen. Click Next to install the filter.

When installation is complete, you will see the following screen:



You will need to run the configuration utility program in order to complete the installation and configuration, so it is recommended that you leave the option to Launch Configuration Utility checked. Click Finish to complete the installation and optionally run the configuration program.

5.3 Configuring the Swivel ADFS Filter

The configuration program consists of four tabs:

The screenshot shows the 'PINsafe RDS Web Filter Configuration' dialog box with the 'PINsafe' tab selected. The 'PINsafe URL' field is set to 'https://pinsafe.swiveldev.local:8080/pinsafe'. There are checkboxes for 'Allow self-signed certificates' (unchecked), 'Allow non-PINsafe users' (unchecked), 'Ignore domain prefix' (checked), and 'Ignore domain suffix' (unchecked). The 'Agent Secret' and 'Confirm Secret' fields are masked with asterisks. 'Save' and 'Close' buttons are at the bottom.

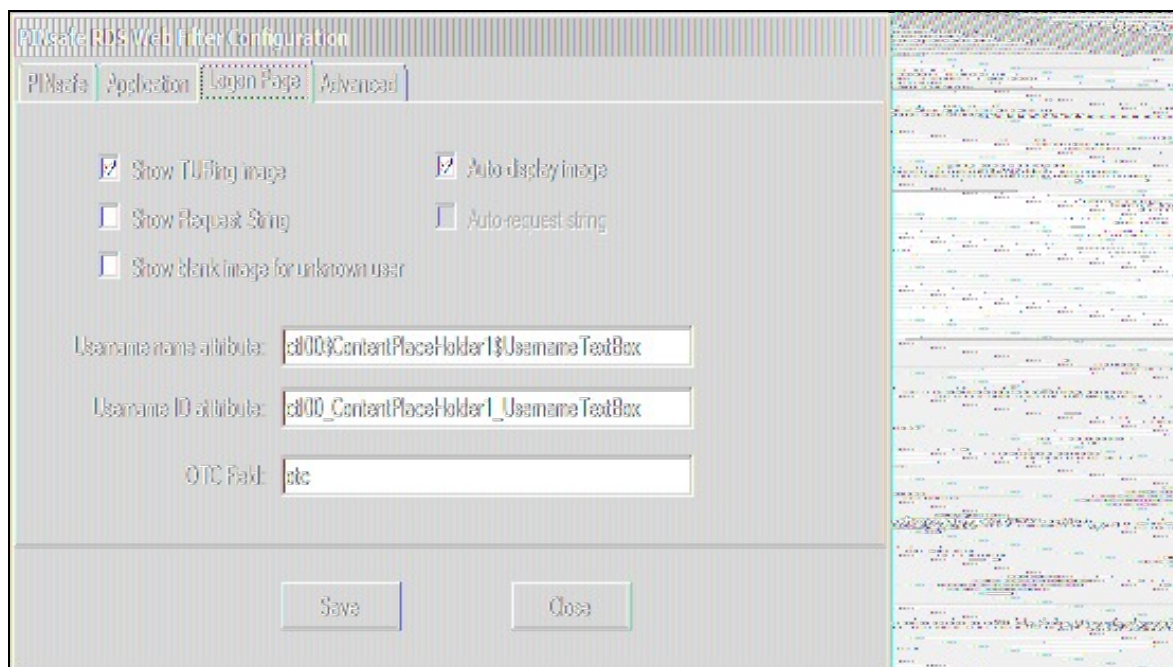
The PINsafe tab allows you to specify the details for the Swivel server. Most of these settings should be obvious. You should check the option **Allow self-signed certificates** if you are using https and your SSL certificate is not either a commercial certificate or one generated by an internal certificate authority which is Trusted by the ADFS server.

Note: For a Swivel appliance port 8080 is required to be used, rather than the 8443 proxy port.

The option to allow unknown users to authenticate without Swivel authentication only applies to users not known to Swivel at all. You cannot specify that it only applies to a group of users, and not to other users who are known to Swivel, but not in a particular group.

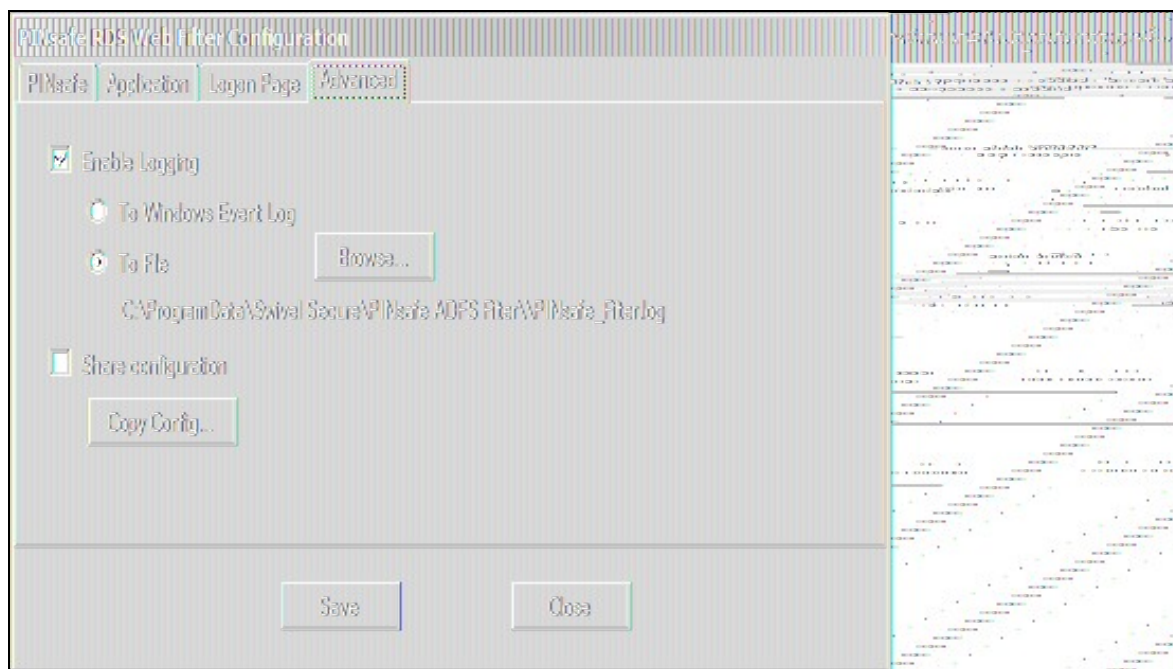
The screenshot shows the 'PINsafe RDS Web Filter Configuration' dialog box with the 'Application' tab selected. The 'Web Application Folder' is 'C:\inetpub\adfs\A'. The 'Login URL' is '/adfs/s'. The 'Logout URL' is '/adfs/s/Logout.aspx'. The 'Excluded URLs' list contains '/pinsafe_image.aspx', '/exists.aspx', and '/adfs/s/MasterPages/'. A 'Change...' button is next to the folder path. 'Save' and 'Close' buttons are at the bottom.

The second page shows details of the ADFS web application. You should not normally need to change any of these settings. Ensure that the Excluded URLs section includes all the names listed above.



The Logon Page tab shows details relating to the Swivel filter's integration with the ADFS logon page. The Username name and ID attributes should reflect the values of the name and id attributes of the username text input field as displayed to the web client. The default values are correct as of latest available information.

NOTE: the "Auto-display image" and "Auto-request string" options will perform the relevant action as soon as you enter the username, without having to click on a button. Only one of these options can be active.



The Advanced tab shows the logging and sharing options.

Logging enables you to record all attempts to authenticate via the PINsafe ADFS filter. By default, nothing is logged. You can choose to log to the Windows Event log, or to a file. Please note, however, that logging to the event log may fail, if the account running the ADFS web application does not have the right permissions. In this case, the log will be written to the default file location instead: C:\ProgramData\Swivel Secure\PINsafe ADFS Filter\PINsafe_Filter.log.

NOTE: this tab has changed slightly in version 1.2. Instead of a simple Yes/No, logging can be set to "None", "Error", "Info" and "Debug". The last option is only recommended for troubleshooting. Also, the default log method is to file: in order to log to the Windows Event log, you need to ensure that the account under which the ADFS web application is running has the relevant permissions.

If you have more than one ADFS server or proxy, you can save having to enter the settings twice. On the first installation (**Master**), configure the filter as required, and then check the "Share Configuration" checkbox. This will create a share on this server, containing the filter settings. On subsequent installations, click the "Copy Config" button and enter the name or IP address of the Master. The settings will be automatically copied from the Master.

server. Note that if you change any settings on the master, you will have to copy the configuration again on each slave server.

You are strongly advised to use this option if you have multiple servers, as the configuration includes a random value used to encrypt the authentication cookie. If you configure each server manually, this encryption value will be different, so if you authenticate to one server, and subsequently access another, the PINsafe authentication cookie will not be valid.

5.3.1 A Note on Versions

The first two versions of this application had no means of explicitly identifying the program version, other than right-clicking on the .exe or .dll and selecting Properties. However, you can identify version 1.0 of the program from the fact that it had only 3 tabs in the configuration application, whereas version 1.1 had 4.

From version 1.1.1 onwards, there is an "About..." button on the Advanced tab, which shows a pop-up dialog with version information. This, and the fact that the configuration program is forced to run as Administrator, is the only difference between 1.1 and 1.1.1.

6 Additional Configuration Options

6.1 PINpad

The single channel challenge "PINpad" is available for use. After the standard filter is installed replace the login page with the PINpad specific version, available [here](#).

Note that you need Swivel core version 3.9.2 or later to use this integration.

The zip file linked above also includes the necessary code to display individual Pinpad digits, and static images for the additional buttons required. All these buttons must be added to the list of files excluded from authentication.

Please note that some login page customisations are not available in the PINpad version. It is possible to implement them, but they must be made manually, and any changes to the configuration may result in the non-PINpad login page being restored. The next version of the filter will have the PINpad option integrated.

6.2 Changing the Show TURING Button

After applying the Swivel customisation, go to C:\inetpub\adfs\ls and edit as an Administrator the FormsSignIn.aspx. Look for "Show TURING" and alter it as appropriate.

7 Testing

8 Known Issues

9 Troubleshooting

10 Microsoft ADFS 3 Authentication

This article has been merged with the article for ADFS 4: [Microsoft ADFS 4 and 3 Authentication](#). Please see that article.

For ADFS version 2 see [Microsoft ADFS 2 Integration](#).

11 Microsoft ADFS 4 and 3 Authentication

12 Introduction

This article describes the Swivel Authentication Provider for ADFS versions 3 and 4, which is included as an option in all Microsoft Windows Server Operating Systems from 2012 R2. For ADFS version 2 see [Microsoft ADFS 2 Integration](#)

13 Requirements

This solution works with Windows Server 2012 R2 64-bit or higher (tested against all versions up to 2022), with the ADFS role installed. This should be installed and tested before installing the Swivel provider. It should also have the Microsoft.Net framework version 4.5 or higher installed.

The Swivel proxy component can be installed separately, either on the ADFS proxy or any other Windows PC with IIS and ASP.Net 4.5 installed, and exposed publicly, either directly or through a proxy.

13.1 Current Version Installer

Please note that the latest version is now 1.4.5, available from [here](#).

13.2 Previous Versions

- The installer for version 1.4.2 of the Swivel ADFS Authentication Provider can be found [here](#).
- The installer for version 1.3.1 of the Swivel ADFS Authentication Provider can be found [here](#).
- Version 1.0.6.1 can be found [here](#).

13.3 Version History

- 1.4.5.0 The shared secret is now stored in encrypted form.
- 1.4.4.0 Fixed some cosmetic problems with the configuration program.
- 1.4.3.0 Fixed problems with monitoring standby appliance. Option to hide OTC for PINpad. Faster PINpad when connecting to cloud instances.
- 1.4.2.0 Support for Push added. Support for a standby appliance added. Various bug fixes.
- 1.3.1.0 Bug fixes. Support for cross-origin resource policies. ADFS 4 compatible.
- 1.2.1.0 Some minor updates
- 1.2.0.0 Updated to support ADFS 4.0
- 1.1.0.0 Added the ability to customise the page style. Not released.
- 1.0.6.1 Added option not to show TURING or PINpad automatically
- 1.0.5.3 Fix for special characters in username
- 1.0.4.1 Various bug fixes and added logging
- 1.0.3.2 Advanced connections added. Fixed language strings configuration.
- 1.0.2.1 Bug fix: in certain circumstances, the first security string would not work and refresh was required to authenticate
- 1.0.1.2 Fix to work with secondary ADFS servers
- 1.0.0.0 Initial release

13.4 Networking Requirements

The following network connections are required in order for this product to work with ADFS. All connections use HTTP(S):

- Connection between the ADFS server and the Sentry appliance, or load balancer if used, on port 8080 if connecting directly to the Core Sentry application, or port 8443 if using the appliance proxy.
- If you are using a proxy for the TURING / PINpad images, you will need the same connections from the proxy to the appliance.

Note that it is possible to configure the appliance proxy to redirect to port 443, in which case you can use this port rather than port 8443.

13.5 Configure Sentry Agent

Log into your Sentry web administration. Select "Server" from the left-hand menu, then "Agents"

Click on the "New Entry" link at the bottom and enter your details as shown below.

- [Status](#)
- [Log Viewer](#)
- ▢ [Server](#)
 - [Name](#)
 - [Language](#)
 - [License](#)
 - [Jobs](#)
 - [SMTP](#)
 - [Agents](#)
 - [Peers](#)
 - [Single Channel](#)
 - [Dual Channel](#)
 - [Third Party Authentication](#)
 - [Voice Channel](#)
- ▢ [Policy](#)
- ▢ [Logging](#)
- ▢ [Messaging](#)
- ▢ [Database](#)
- ▢ [Mode](#)
- ▢ [Repository](#)
- ▢ [RADIUS](#)
- ▢ [Migration](#)
- ▢ [Windows GINA](#)
- ▢ [Appliance](#)
- ▢ [OATH](#)
- ▢ [Config Sync](#)
- ▢ [Reporting](#)
- [User Administration](#)
- [Save Configuration](#)
- [Upload Email Images](#)
- [Administration Guide](#)

Server>Agents

Please enter the details for any Sentry agents below. Agents are permitted to access

Agents:

☒ [Robin](#)

☒ [Swivel Wifi](#)

☒ [Local](#)

☐

Name:

ADFS

Hostname/IP:

fs.office365.swivelsecure.c

Shared secret:

vvvvvvvv

Group:

---ANY--- ▾

Authentication Modes:

ALL ▾

Check password with Repository:

No ▾

Check password for non-user:

No ▾

Username attribute for repository:

Allow alternative usernames:

No ▾

Alternative username attributes:

Can act as Repository:

No ▾

URL Check password:

Encryption/Decryption key:

The shared secret can be anything, but remember it, as you will need it for the Authentication Provider configuration

14 Installation

NOTE: If you are installing on the ADFS server(s) and one or more proxies (see below), you should install on the ADFS server(s) first.

NOTE: You must uninstall any old version before installing a new one. See the notes below on uninstalling - in particular, you need to remove the old provider from any authentication policies. Note that the settings are not deleted on uninstall, so when you install the new provider, the previous settings will still be there.

If you have more than one ADFS server, you should install on the primary first. The installer automatically detects whether or not the server is a primary ADFS server, and adjusts the installation actions accordingly. However, when installing the proxy only on a non-ADFS server, you must manually disable the Authentication Provider option.

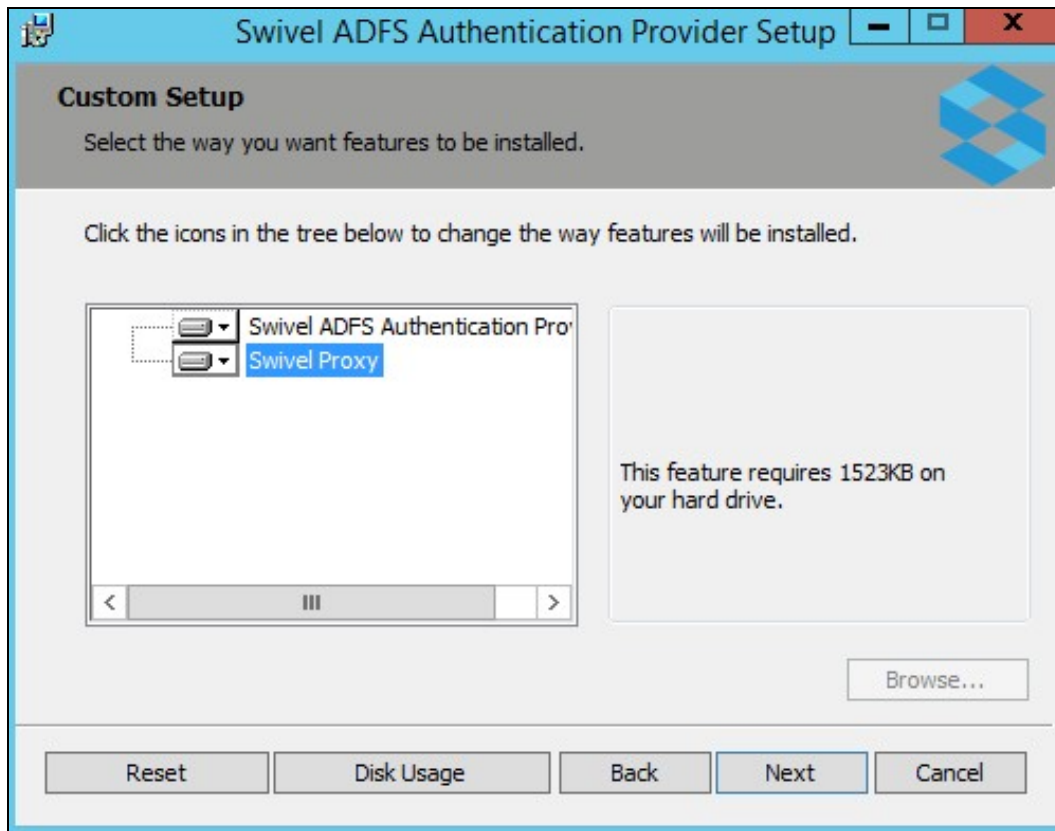
To install this product, simply unzip the file SwivelAuthProviderInstall.msi from the download and double-click it. Note that you must be logged in as an administrator to install this product. If you are not logged in as administrator, open a command prompt as administrator, switch to the directory containing the msi file, and run the following command:

```
msiexec /i SwivelAuthProviderInstall.msi
```

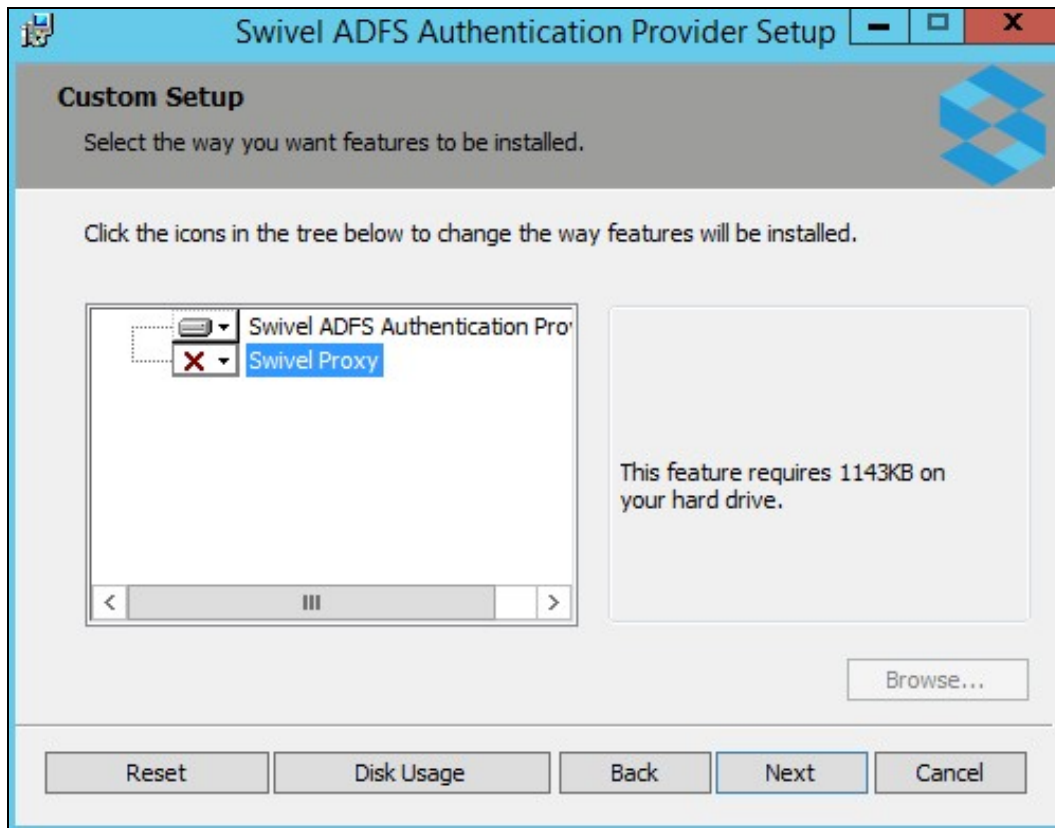


You will next be asked to choose whether to install the ADFS Authentication Provider, the Swivel proxy or both. There are a number of possible scenarios, summarized below.

- ADFS and IIS installed on the same public server, no proxy:
 - ◆ Install both components on this server.

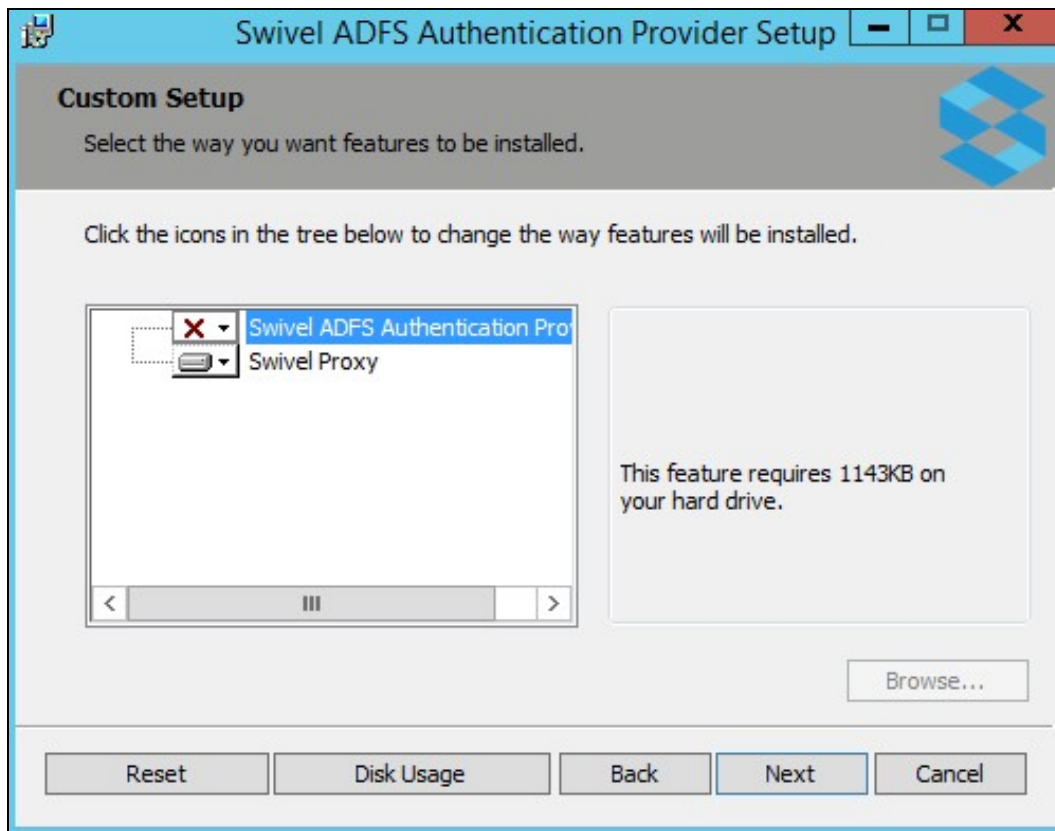


- Single ADFS server, no IIS:
 - ♦ Install Authentication provider only. For Swivel single channel, you will need to provide some other method to display the TURing or Pinpad.



- ADFS server and ADFS proxy, IIS installed on the proxy:

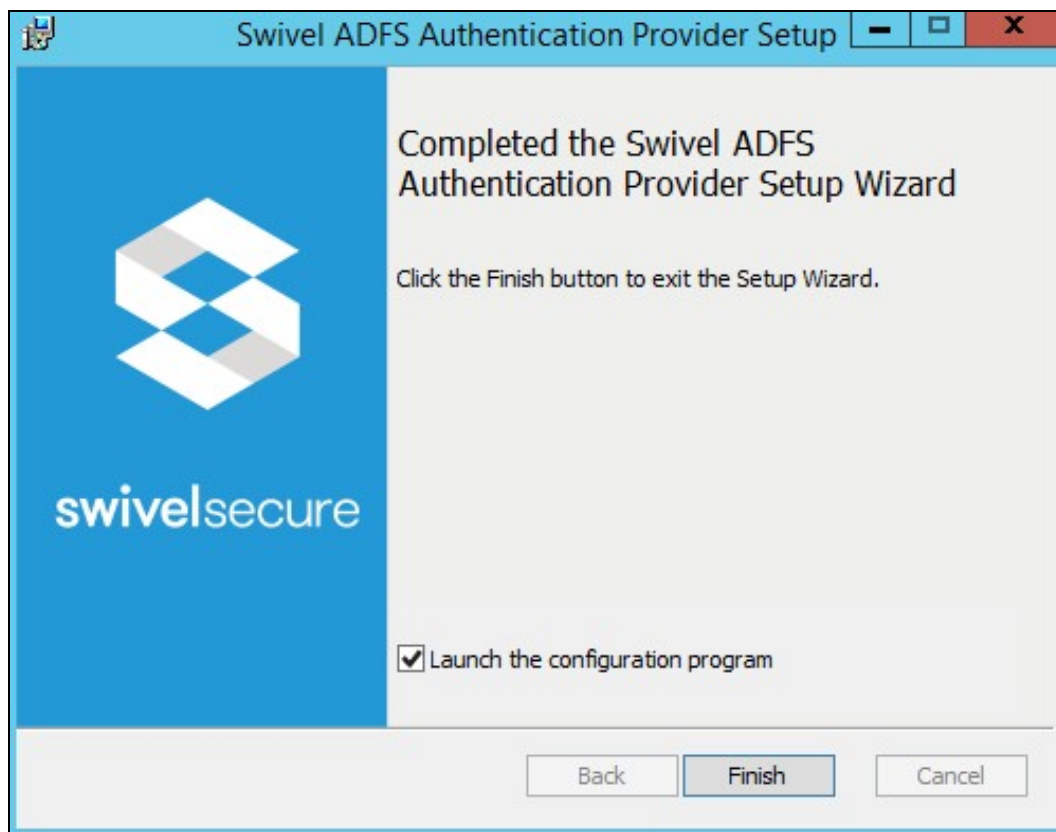
- ◆ Install Authentication provider only on the ADFS server.
- ◆ Install proxy component only on the ADFS proxy.



- ADFS server and ADFS proxy, IIS not installed on the proxy:
 - ◆ Install Authentication provider only on the ADFS server.
 - ◆ No additional components are required on the proxy.
 - ◆ Optionally, you can install the Swivel proxy on a third server with IIS installed, and proxy that through the ADFS proxy.

Note that, if you have not installed IIS (and ASP.Net 4.5) on the ADFS proxy, you do not need to install any components on the proxy. If you are using the ADFS proxy as a Swivel proxy, make sure that you only proxy the /adfs application through to the ADFS server, not the entire website.

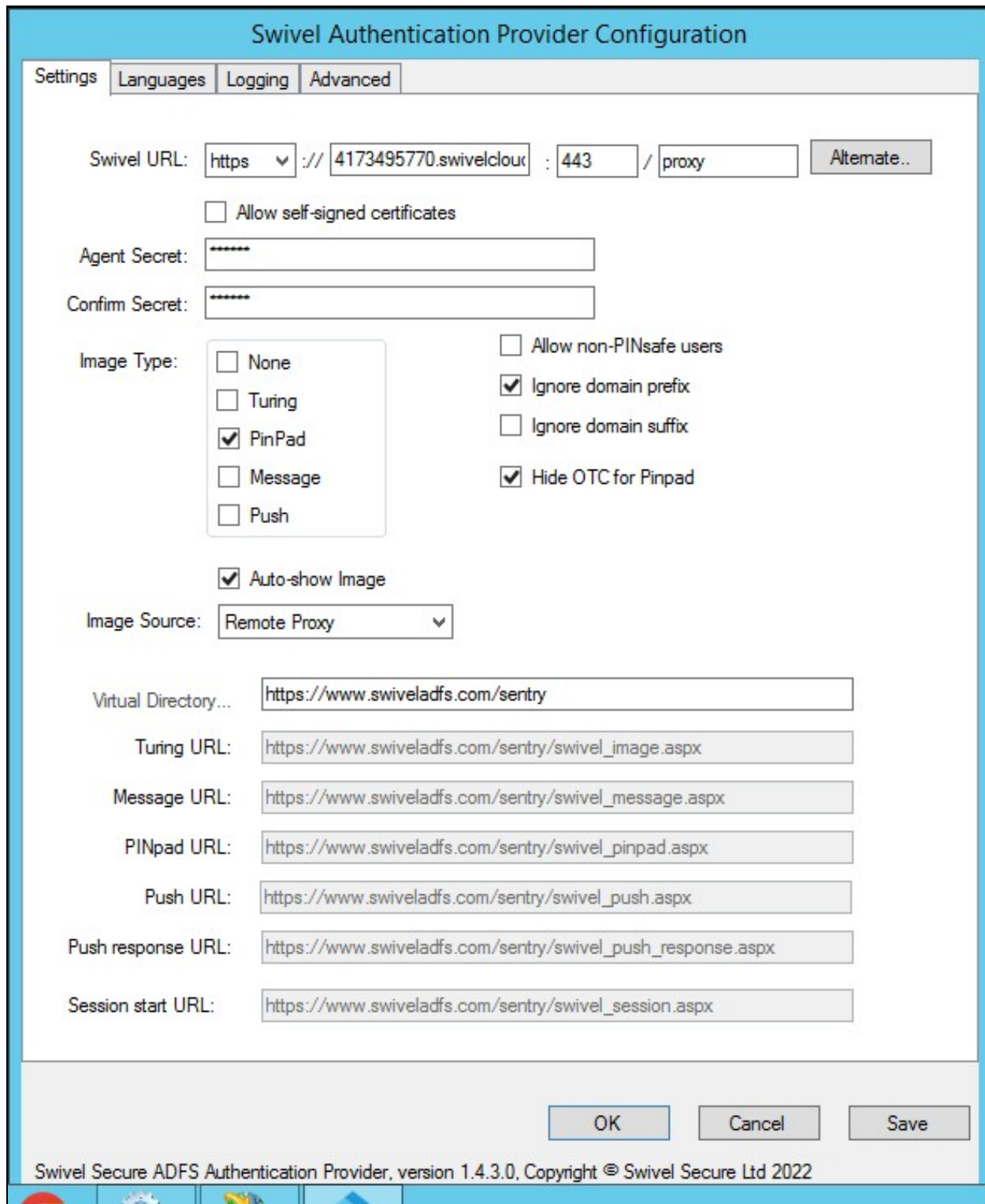
Please note that the Swivel Proxy component does not have to be installed on an ADFS Proxy server. It can be any Windows Server with IIS and ASP.Net installed with a public URL.



On the final screen, you will be prompted whether you want to run the filter configuration program.

15 Configuration

The configuration program for the authentication provider consists of 4 tabs, although typically you will only need to modify the first one. The Configuration program for the proxy is shown below.



The image shows a screenshot of the 'Swivel Authentication Provider Configuration' window. The window has a title bar and four tabs: 'Settings', 'Languages', 'Logging', and 'Advanced'. The 'Settings' tab is selected. The configuration fields are as follows:

- Swivel URL:** A text field containing 'https' (with a dropdown arrow), '://', '4173495770.swivelcloud', ':', '443', '/', 'proxy', and an 'Alternate..' button.
- Allow self-signed certificates:** An unchecked checkbox.
- Agent Secret:** A text field with masked characters (dots).
- Confirm Secret:** A text field with masked characters (dots).
- Image Type:** A group box containing five checkboxes: 'None' (unchecked), 'Turing' (unchecked), 'PinPad' (checked), 'Message' (unchecked), and 'Push' (unchecked).
- Allow non-PINsafe users:** An unchecked checkbox.
- Ignore domain prefix:** A checked checkbox.
- Ignore domain suffix:** An unchecked checkbox.
- Hide OTC for Pinpad:** A checked checkbox.
- Auto-show Image:** A checked checkbox.
- Image Source:** A dropdown menu showing 'Remote Proxy'.
- Virtual Directory...** A text field containing 'https://www.swiveladfs.com/sentry'.
- Turing URL:** A text field containing 'https://www.swiveladfs.com/sentry/swivel_image.aspx'.
- Message URL:** A text field containing 'https://www.swiveladfs.com/sentry/swivel_message.aspx'.
- PINpad URL:** A text field containing 'https://www.swiveladfs.com/sentry/swivel_pinpad.aspx'.
- Push URL:** A text field containing 'https://www.swiveladfs.com/sentry/swivel_push.aspx'.
- Push response URL:** A text field containing 'https://www.swiveladfs.com/sentry/swivel_push_response.aspx'.
- Session start URL:** A text field containing 'https://www.swiveladfs.com/sentry/swivel_session.aspx'.

At the bottom of the window, there are three buttons: 'OK', 'Cancel', and 'Save'. Below the buttons, the text 'Swivel Secure ADFS Authentication Provider, version 1.4.3.0, Copyright © Swivel Secure Ltd 2022' is displayed.

Enter the URL for the Sentry appliance that will be used to authenticate users. If you have 2 Sentry appliances with different URLs, you can specify a second URL by clicking the "Alternate.." button:

The screenshot shows a Windows-style dialog box titled "Alternative Sentry Server". Inside, there are three input fields: "Swivel URL:" with a dropdown set to "https", a text box containing "sentry.swiveladfs.com", a port field with "8080", and a path field with "sentry". Below these is a "Secret:" field with a masked password "*****". At the bottom are three buttons: "Save", "Remove", and "Cancel".

Enter the alternative URL on this form. The primary URL will be used by preference, but the authentication provider will remember if the primary was not available for the last attempt and will use the alternative first in this case.

If the Sentry appliance uses HTTPS and does not have a valid, trusted certificate, check the option to *Allow self-signed certificates* (but see [#Known Issues](#)).

Enter the Agent secret for the Swivel twice: you should have previously created an Agent on the Swivel server corresponding to this ADFS server, and you should use the same secret here as you entered on that.

Image Type: You can choose to display either a TURING image, a Pinpad or no Swivel image (if you are using dual channel). Alternatively, you can specify Message on-demand or Push authentication.

Select *Allow non-PINsafe users* if you want users that do not have Swivel accounts to be able to authenticate without having to enter additional credentials. Generally, it is easier to manage this using Authentication Policies on ADFS.

Select *Ignore domain prefix* or *Ignore domain suffix*, depending on your Swivel usernames: typically, you will always ignore the domain prefix, unless you configure your Swivel repository to automatically add a prefix. You will need to ignore domain suffix if you are using SAMAccountName as the Swivel username (the default), but not if you are using userPrincipalName.

Select *Hide OTC for PINpad* if you do not want the OTC to be displayed when using PINpad. If the image type is not PINpad, this option has no effect and the OTC will be displayed. The exception is for Push, when the OTC is never displayed, since it is not relevant.

Image Source:

There are 4 possible options for Image Source:

- Swivel direct: the image will be delivered directly from the Swivel server to the end user. In this case, the Swivel server must be publicly visible, and the URL for the image will be constructed from the Swivel URL.
- Local Proxy: the image will be delivered by the ADFS server or ADFS proxy, using the proxy component of the authentication provider. In this case, the proxy component must be installed either on the ADFS server or on a proxy with the same public URL as the ADFS server, which means that IIS must be installed on the appropriate server. Configuring the web application for the proxy is described in the Proxy section below.
- Remote Proxy: the image will be delivered by a web server that has the Swivel ADFS proxy application installed. See [below](#) for more details on using this option.
- Define manually: use this option if you have an alternative source for the TURING or Pinpad images. For example, if you have another Swivel integration, such as OWA, that provides an image proxy. This proxy must be to the same Swivel instance that is used for authentication, but does not have to be a direct connection. In this case, you must specify the full public URL for the image in the appropriate field below.

To directly access a Swivel appliance through a NAT etc, then the URL should be <https://URL:8443/proxy/SCImage>

IMPORTANT: if you choose either the Swivel direct or Define manually options, you will need to add some additional security headers to the ADFS. Use the following Powershell commands on the ADFS server:

```
Set-AdfsResponseHeaders -EnableCORS $true
Set-AdfsResponseHeaders -CORSTrustedOrigins https://proxyhost:port
Set-AdfsResponseHeaders -SetHeaderName "Content-Security-Policy" -SetHeaderValue "default-src 'self' https://proxyhost:port 'unsafe-inline' "
```

You should substitute your actual public hostname and port (if it isn't the default) in both cases above.

You may find you need the first two options for Remote Proxy as well, but you shouldn't need the third, as the proxy URL is automatically inserted into the response in this case.

Swivel Authentication Provider Configuration

Settings
Languages
Logging
Advanced

Locale ID: [default] ▼ New locale...

Phrase ID	Text
Friendly Name	Swivel Secure
Description	Swivel Secure Authentication Provider
Page Title	Swivel Secure Authentication
Otc	OTC
Continue	Continue
Unknown User	No further authentication required
Refresh	Refresh
Clear	Clear
Login Type	Login Type
None	None
Turing	Turing
Pin Pad	Pin Pad

OK
Cancel
Save

Swivel Secure ADFS Authentication Provider, version 1.4.2.0, Copyright © Swivel Secure Ltd 2022

The languages tab allows you to change the messages used for various parts of the login page. You can either enter a new locale ID if you know the locale ID for the language you want to use. See [here](#) for a list of Microsoft-assigned locale IDs. Alternatively, if you know that most of your users will be using a particular language, you can change the default messages.

Note that in ADFS 4.0, you must have a language defined for the locale of the ADFS service user, which will typically be the locale of the server operating system. To facilitate this, the installer automatically detects the locale of the service user and creates a set of phrases for that locale. Do not delete this locale, or ADFS will fail to authenticate.

When you create a new locale, or one is created for you automatically, all the phrases are copied from the English phrases. Swivel Secure does not currently provide messages for any other language.

Swivel Authentication Provider Configuration

SettingsLanguagesLoggingAdvanced

Logging Level: Debug

View Log For: 16 June 2022View

Remove logs more than 30 days old.Delete

OKCancelSave

Swivel Secure ADFS Authentication Provider, version 1.4.2.0, Copyright © Swivel Secure Ltd 2022

The Logging tab allows you to control how much information is logged by the provider, to view existing logs and to remove old logs. By default, nothing is logged.

Swivel Authentication Provider Configuration

SettingsLanguagesLoggingAdvanced

SSL Protocols

☐ SSL v3
☐ TLS 1.0
☐ TLS 1.1
☒ TLS 1.2

Web Proxy Settings

Automatic

▼

Proxy Server:

User Agent String:

Custom Headers:

OK

Cancel

Save

Swivel Secure ADFS Authentication Provider, version 1.4.2.0, Copyright © Swivel Secure Ltd 2022

The Advanced tab provides advanced settings for the Swivel server connection. You should normally only use this if you are having problems connecting.

SSL protocols: Typically, you should stick to using just TLS 1.2, since all earlier protocols are deprecated. However, we have seen problems in some instances where there are no common cipher suites available between the appliance and the ADFS server. In this case, you will have to enable TLS 1.1 on both the appliance and the ADFS authentication provider. You may also need to add cipher suites to the appliance to support TLS 1.1.

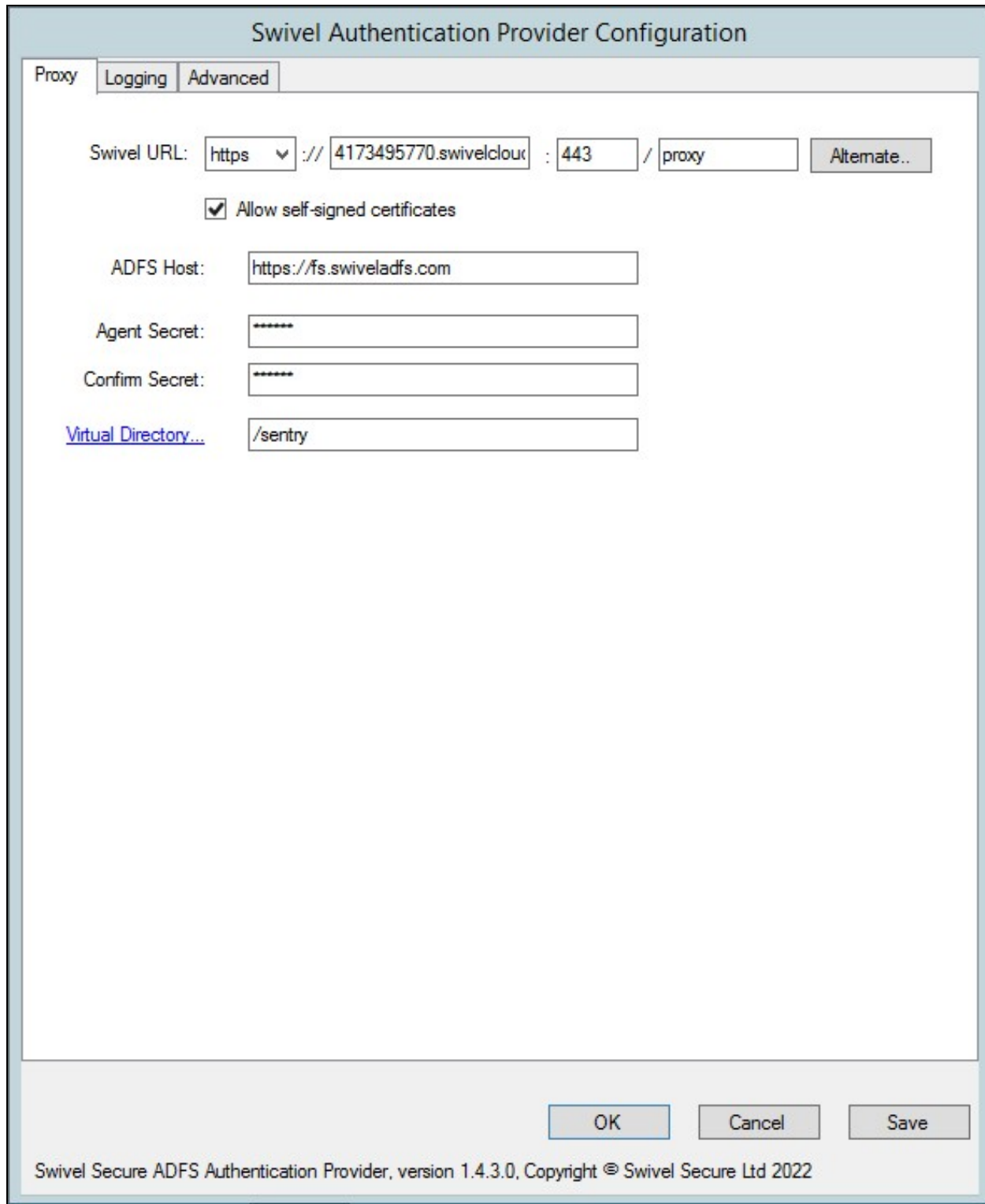
You can configure a web proxy to be used for the connection. By default, the Automatic option is selected, in which case the connection will use whichever proxy is configured for internet connections on the ADFS server. The other options are None, in which case no proxy is used, or Manual, in which case you can specify the URL of a proxy to use.

User Agent provides a custom user agent string to be sent with the request. You might want to alter this to try emulating a particular browser, if you have problems connecting.

Finally, you can specify other HTTP headers that will be sent with the request. Right click on the Headers list to add, delete or edit them.

16 Using the Swivel Proxy

16.1 Proxy Configuration



The image shows a 'Swivel Authentication Provider Configuration' dialog box with three tabs: 'Proxy', 'Logging', and 'Advanced'. The 'Proxy' tab is selected. It contains the following fields and controls:

- Swivel URL:** A text field with a dropdown menu set to 'https', followed by '://', a text box containing '4173495770.swivelcloud', a colon, a text box containing '443', a slash, and a text box containing 'proxy'. To the right is an 'Alternate..' button.
- Allow self-signed certificates:** A checked checkbox.
- ADFS Host:** A text box containing 'https://fs.swiveladfs.com'.
- Agent Secret:** A text box filled with asterisks.
- Confirm Secret:** A text box filled with asterisks.
- Virtual Directory...** A text box containing '/sentry'.

At the bottom right are three buttons: 'OK', 'Cancel', and 'Save'. At the bottom left is the text: 'Swivel Secure ADFS Authentication Provider, version 1.4.3.0, Copyright © Swivel Secure Ltd 2022'.

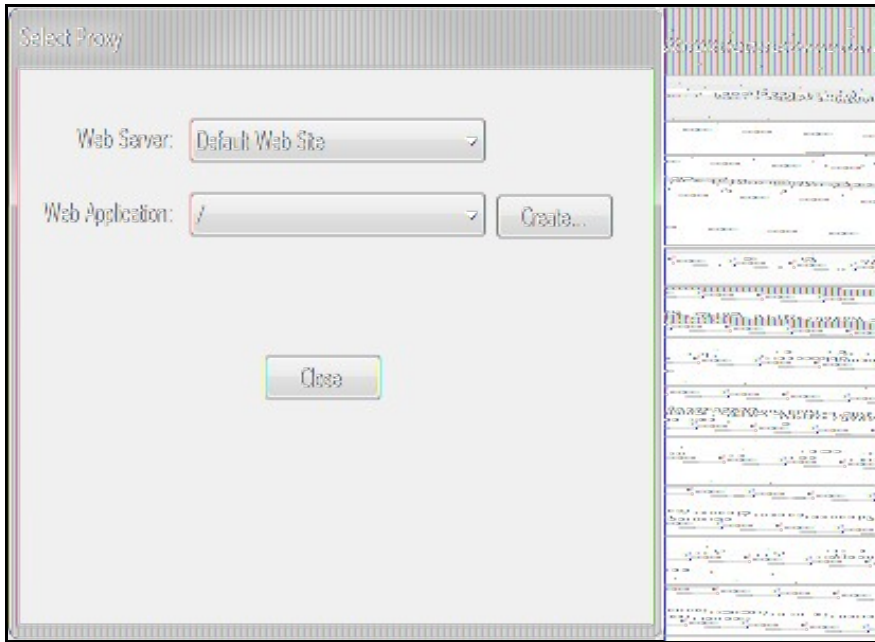
The proxy configuration program is largely a simplified version of the full configuration program, including just the Settings, Logging and Advanced tabs. However, there is one additional option to take note of:

ADFS Host: this must be the public URL for the ADFS appliance, including the "https://" prefix. It is essential that this is specified for the remote proxy, as it enables Cross-Origin Resource Sharing - so that images hosted by the proxy can be displayed on the ADFS login page. As of version 1.4.3, if the "https://" prefix is omitted, it will automatically be added.

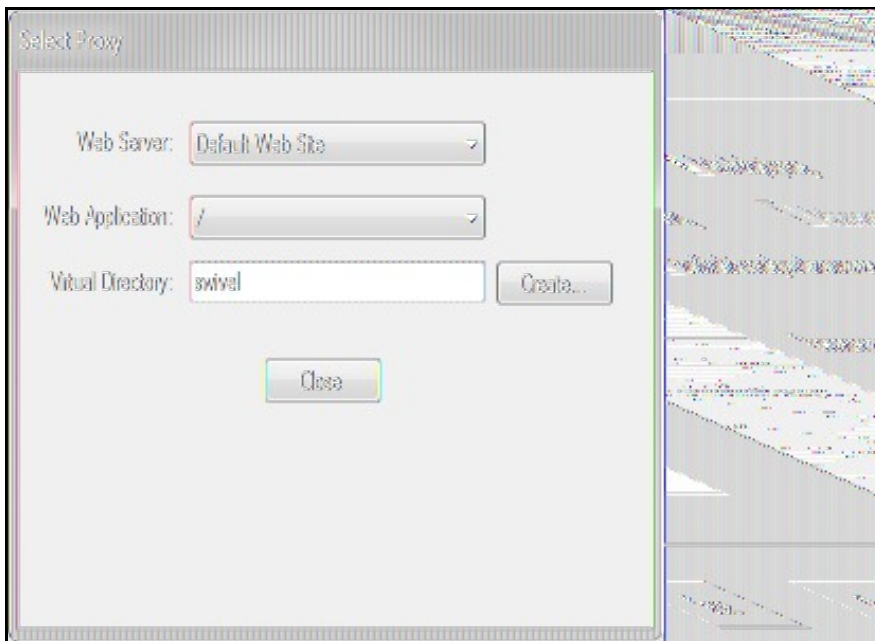
After making any changes to the proxy configuration, you should restart IIS to ensure the changes are registered.

16.2 Enabling the Proxy Web Application

This is required for both Local and Remote Proxy, and is accessed by clicking the **Virtual Directory** link.



Select the existing web application you want to install the proxy under (typically this will be the root application), and click **Create...** to show the following



Enter the name of the directory you want to use for the proxy - note you should *not* include a "/" prefix - and click **Create...** again. This will create a web application with the given name. This application contains links for the TURING and Pinpad images.

In order to use this proxy, you need to specify the same directory name - but this time *including* a "/" prefix - in the ADFS configuration.

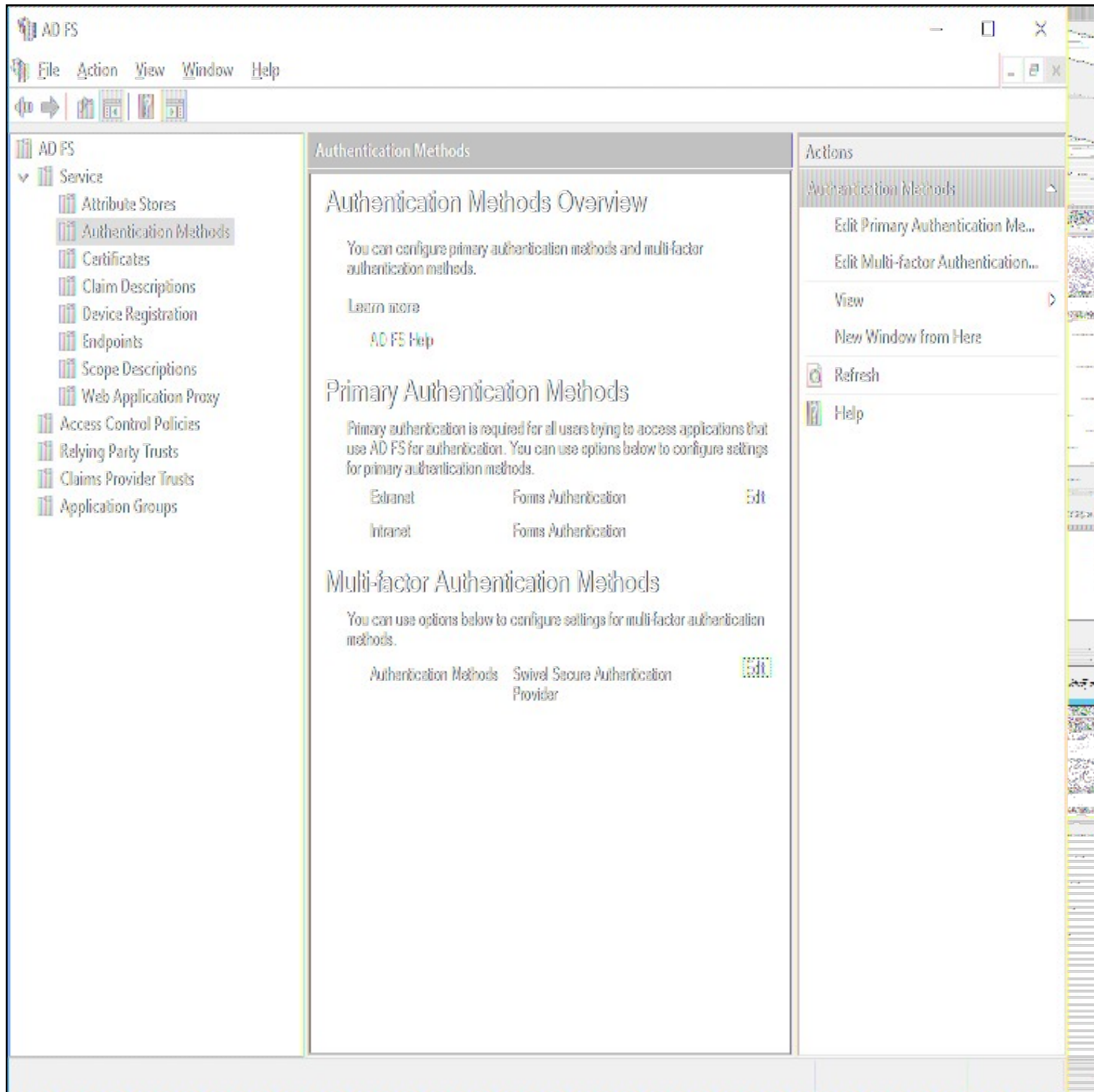
An additional menu option is provided to remove the virtual directory. This should normally be done before uninstalling the authentication provider.

17 Using the Authentication Provider

Note that the installer simply makes the Swivel Authentication Provider available for use: it does not actually enforce its use. To do so, you need to modify an Authentication Policy:

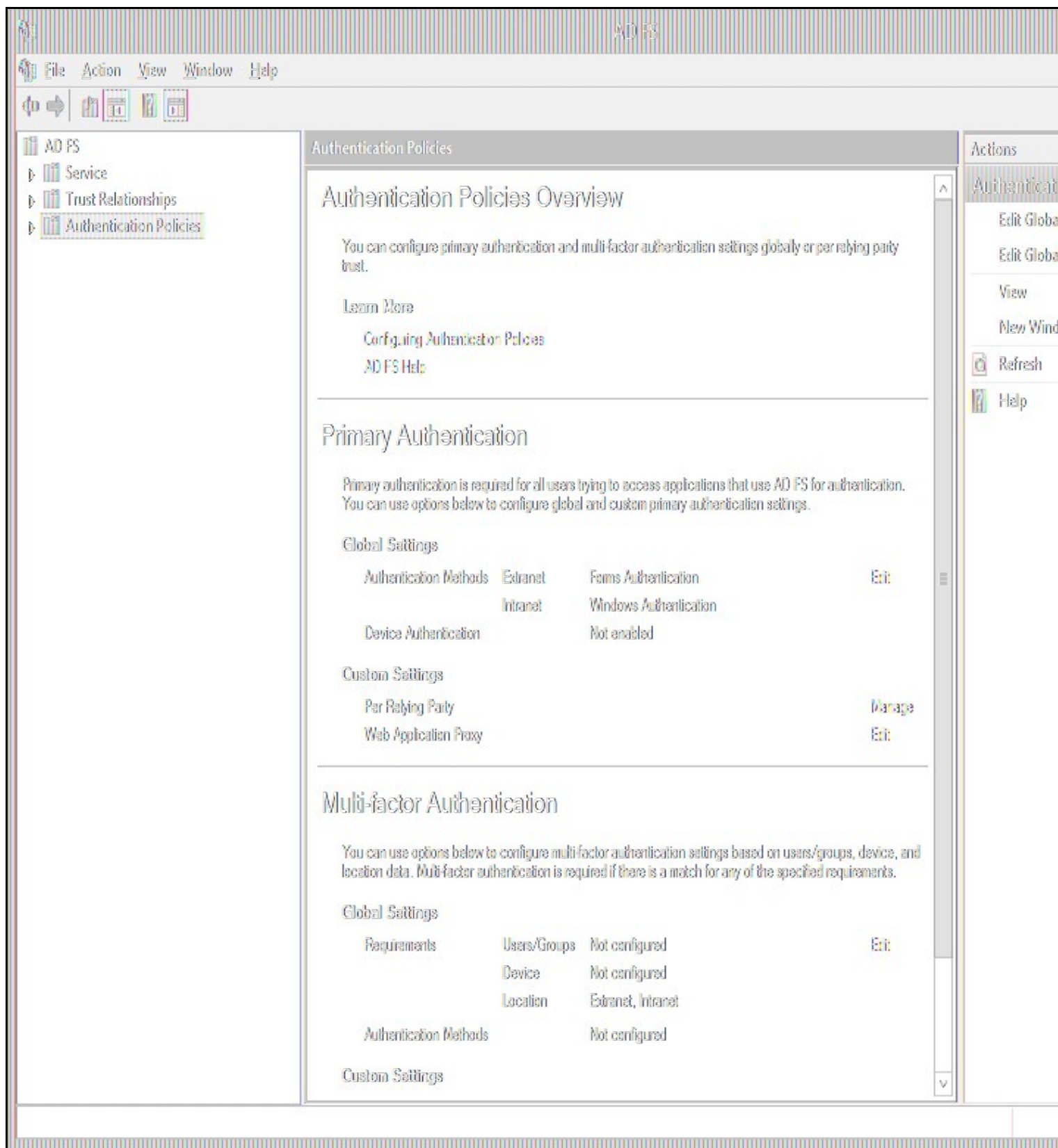
From *Administrative Tools*, select *AD FS Management*,

This is the dialog for ADFS 4:



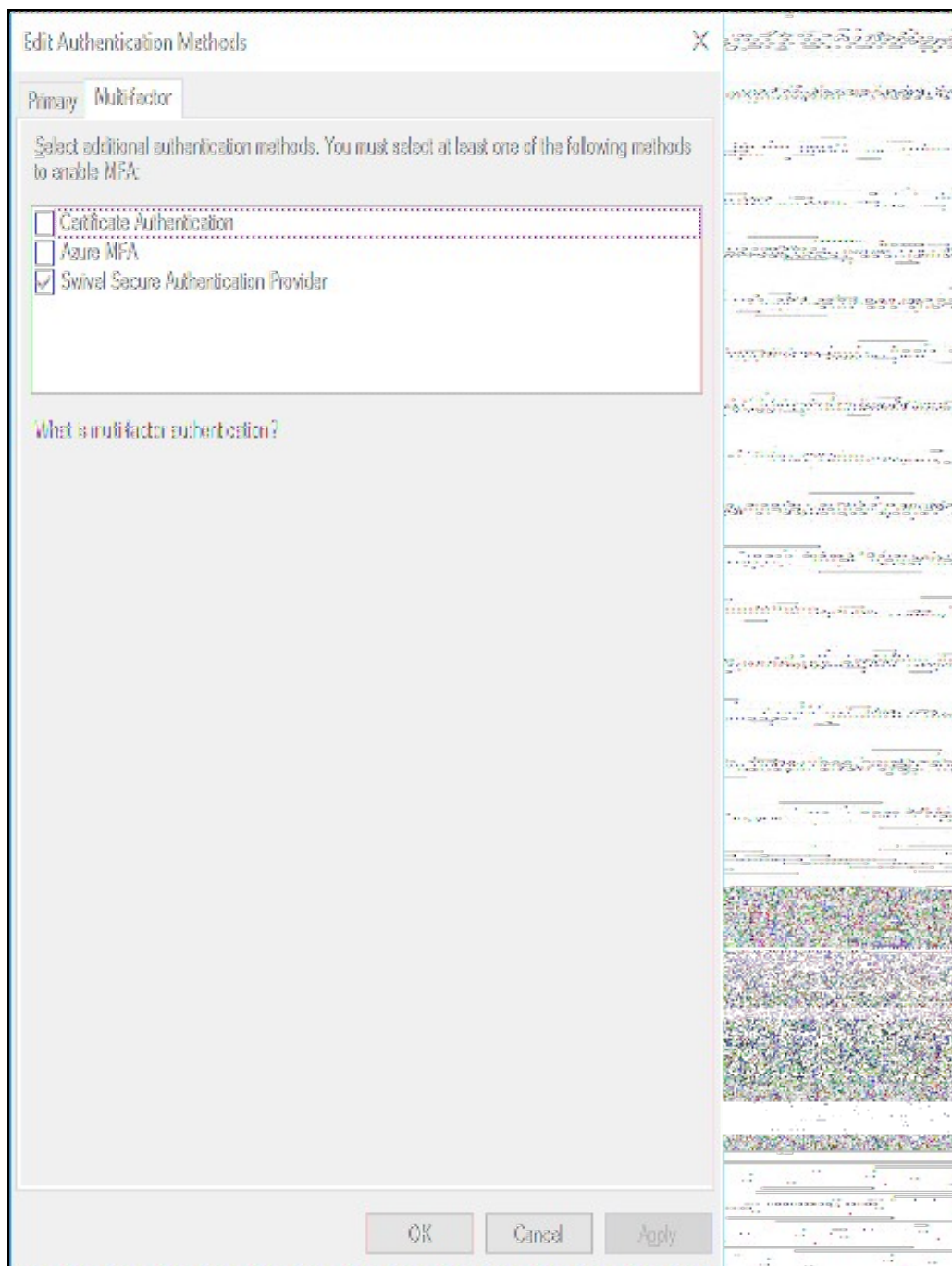
In ADFS 4.0, select *Service*, then *Authentication Methods*.

This is the dialog for ADFS 3:



In AD FS 3.0, choose *Authentication Policies*.

Under *Multi-factor Authentication*, click Edit.



In ADFS 3.0, this dialog looked different, but the principle is the same:

Edit Global Authentication Policy

Primary **Multi-factor**

Configure multi-factor authentication (MFA) settings.

Users/Groups
MFA is required for the following users and groups:

SWIWDEV\PinSafeUsers

Add... Remove

Devices
MFA is required for the following devices:

☐ Unregistered devices
☐ Registered devices

Locations
MFA is required when accessing applications from the following locations:

☒ Extranet
☒ Intranet

Select additional authentication methods. You must select at least one of the following methods to enable MFA:

☐ Certificate Authentication
☒ **Swivel Authentication Provider**

What is multi factor authentication?

OK Cancel Apply

You should see *Swivel Authentication Provider* as an additional authentication method at the bottom of the dialog. Check this to enable it. You will also need to choose which users or groups are required to use MFA, and where they need to use it from. This document does not describe how to configure ADFS Authentication Policies - you should read the appropriate Microsoft documentation for that.

Note that if you have multiple ADFS Servers and/or ADFS Proxies you must install the Authentication Provider component **every** server. To use single-channel authentication, you must install the Proxy component on every proxy server. You do not need to install anything on the proxies if you are only using dual-channel authentication methods.

Once you have enabled MFA for the Swivel Authentication Provider, the next time you go to a page that requires ADFS authentication, after you enter your usual AD credentials successfully, you will be prompted to enter a Swivel one-time code.

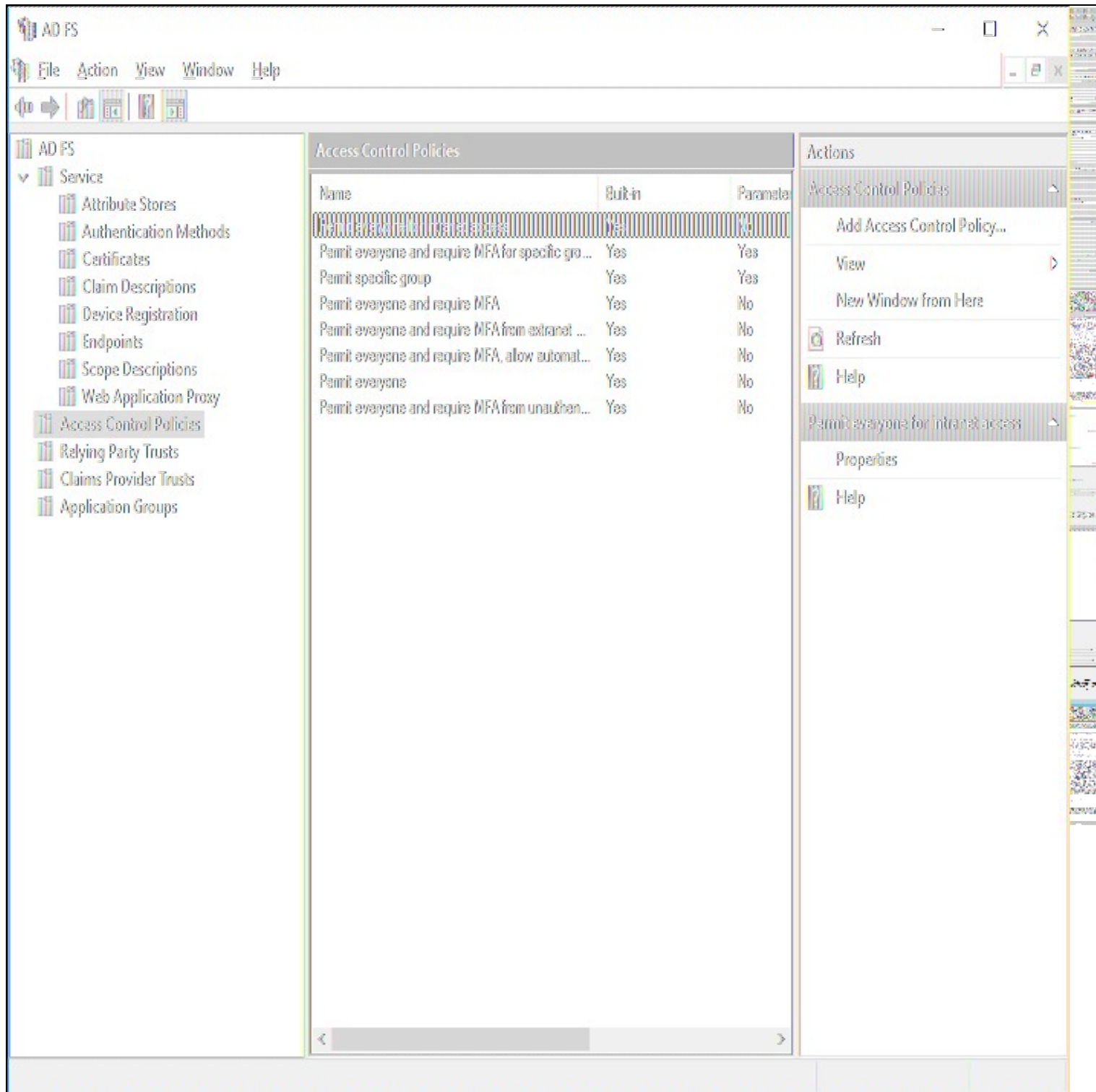
18 Advanced Features

18.1 Requiring Swivel Authentication for Single Applications

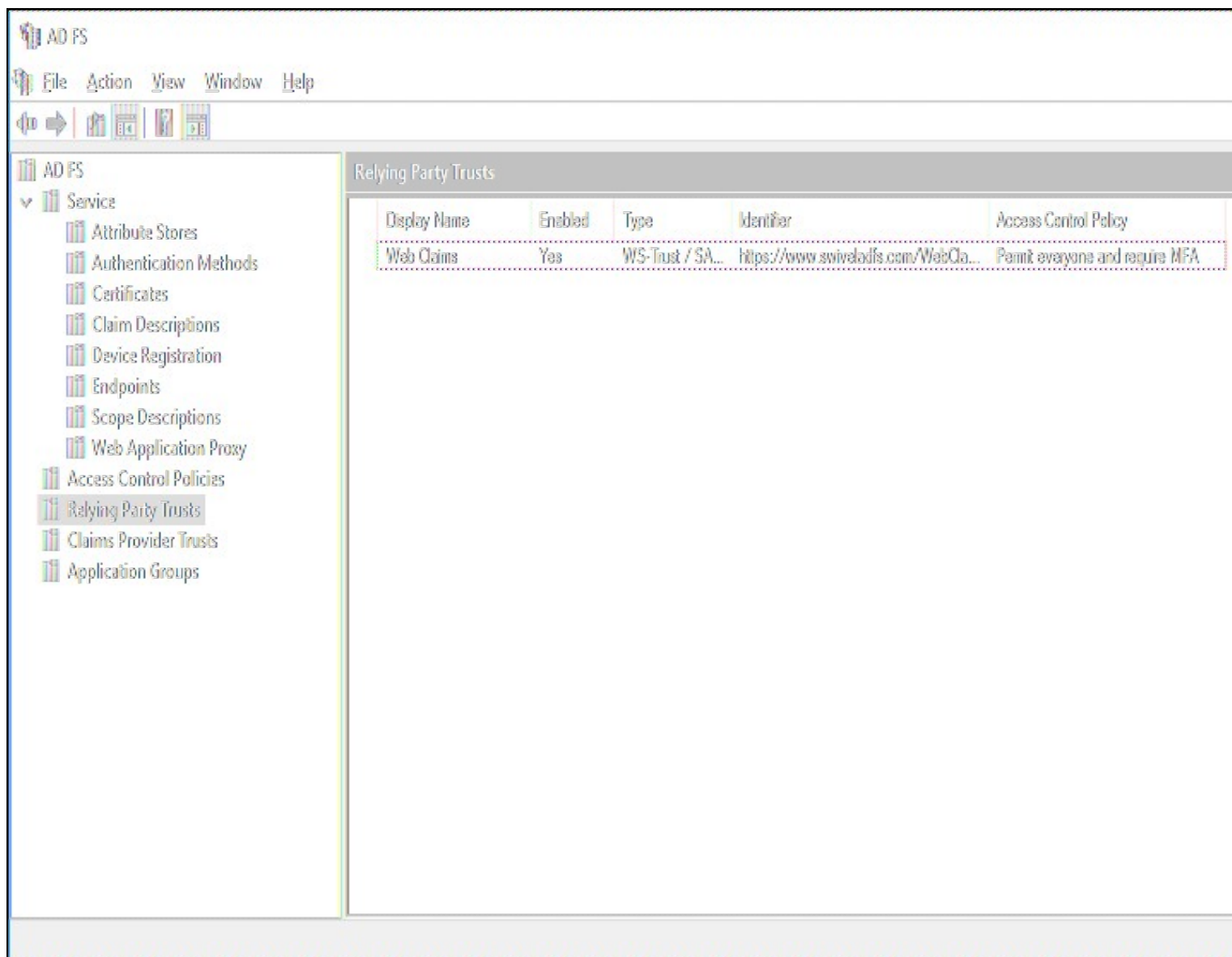
NOTE: these instructions are relevant to any ADFS Multi-Factor Authentication provider, not just Swivel, so are subject to the facilities provided by Microsoft. The way authentication is configured has changed considerably in ADFS 4.0, so we provide two separate sets of instructions.

It may be that you want to enable Swivel Authentication in ADFS for some applications but not others. It is possible to manage this, with certain limitations, as described below:

18.1.1 ADFS 4.0



A number of built-in access control policies are provided. It is possible to define new policies, but the only important feature to enable Swivel authentication is that Multi-Factor Authentication is required.



For each relying party, you can select an Access Control Policy from the list.

18.1.2 ADFS 3.0

Firstly, you must set up Global Multi-factor Authentication (MFA), and enable "Swivel Authentication Provider". However, DO NOT add any groups or check any devices or locations options. This will enable the Swivel authentication provider, but not require it for anything.

Secondly, got to Authentication Policies -> Per Relying Party Trust and select the relevant Trust (i.e. Application). Click Edit Custom Multi-factor Authentication for this application, and set the conditions under which you require MFA.

You will note that the MFA providers are not listed here. You can only enable or disable MFA: you can't specify which MFA provider to use. This is a limitation of ADFS, and not within Swivel's control. There are advanced methods to manage this, using claim rules, but this is beyond the scope of this article.

18.2 Customising the Login Page Look and Feel

It is possible to make minor adjustments to the Swivel login page. In order to do this, you must be familiar with Cascading Stylesheets (CSS).

The stylesheet used by the Swivel login page is stored under C:\ProgramData\Swivel Secure\Swivel ADFS Authentication Provider together with the provider configuration and logs. The file you need to modify is SwivelStyle.css. This is always delivered by the ADFS server, not the proxy. Also, you should restart the ADFS services after any changes you make. You can only make changes to existing styles within the CSS, as these are the only ones used. The style names should make it obvious what they affect.

19 Known Issues

19.1 Public Access to Swivel Server, Untrusted Certificates and TURING/Pinpad Images

As noted above, by default TURING images and Pinpad images are delivered directly from the Swivel server. This has two consequences:

- The Swivel Server must be published on the Internet
- If the Swivel server is running HTTPS, it must have a valid commercial SSL certificate

The best solution for this is to install the optional local proxy, but this requires IIS to be installed on the ADFS server, the ADFS proxy or a suitable alternative public server. Alternatively, you can proxy the image through a different public web server, but this has the same provisos as for delivering images directly from the Swivel appliance.

19.2 Problems Registering the Authentication Provider

Sometimes the authentication provider fails to register, usually because the installer didn't have the correct permissions. You can register it manually by opening Powershell as administrator, and entering the following command:

```
Register-AdfsAuthenticationProvider -Name SwivelAuthenticationProvider -TypeName "com.swivelsecure.authprovider.SwivelAuthProxy, SwivelAuthPr
```

Check that Version in the above command is set to the version of the authentication provider you are installing.

20 Uninstalling the Authentication Provider

As noted below, uninstalling the old version is also necessary for upgrading.

The procedure for uninstalling is as follows:

- Make sure that Swivel Authentication Provider is removed from ALL Authentication Policies. The simplest way to do that is to uncheck Swivel Authentication Provider as a permissible MFA authentication provider. If you do not do this, you will not be able to reinstall or upgrade to a newer version.
- Unregister the authentication provider using the following command from a PowerShell command prompt run as administrator:

```
Unregister-AdfsAuthenticationProvider -Name SwivelAuthenticationProvider
```

- If the above command fails, go back and check that it has been properly removed from MFA
- Restart the ADFS service. It is important to restart the service on all ADFS servers before attempting a new installation.
- The uninstallation procedure does not remove any web application for the image proxy. Typically, you should uninstall this, using the menu shortcut provided, before uninstalling, but if you are uninstalling in order to install a newer version, this is not necessary.
- If you want to completely remove the Swivel Authentication Provider, you will also need to remove the folder C:\ProgramData\Swivel Secure\Swivel Authentication Provider. This contains the filter configuration and logs. If you are upgrading, this is not necessary, and doing so will require you to reconfigure from scratch.
- Once you have completed the steps above, you can uninstall the Swivel Authentication Provider using the Add or Remove Programs dialog.

21 Upgrading

Currently, the filter installer does not permit direct upgrading from an earlier version, so it is necessary to uninstall the previous filter, including changing the ADFS authentication policy, before installing a new version, using the procedure above. However, the configuration is retained (unless you deleted it as above), and will be automatically applied to the new version. You will still have to re-enable the ADFS authentication policy, though.

22 Troubleshooting

Check to see if a connection can be made from the ADFS server to the Swivel server, for an appliance: <https://Swivel-URL:8080/pinsafe>

23 Error Messages

24 Microsoft Office 365

25 Introduction

This article describes how to manually integrate Swivel with Microsoft Office 365 to provide strong and two factor authentication. A more recent integration with a swivel installer and configuration program is available in the [Microsoft ADFS 2 Integration](#). For ADFS version 3 see [Microsoft ADFS 3 Authentication](#).

25.1 Video showing login to Office 365 using ADFS with PINpad

Swivel Authenticating Office365 using ADFS with PINpad from [Swivel Secure](#).

26 Prerequisites

Swivel authentication platform 3.x

ADFS Proxy 2.0, ADFS Proxy 2.1

Microsoft Office 365

26.1 Downloads

[ADFS Integration files](#)

27 Baseline

(The version tested with)

Swivel 3.9.5

ADFS Proxy 2.0, ADFS Proxy 2.1

Microsoft Office 365

28 Architecture

The process of the filter is quite simple and verifies the credentials against the Swivel server and, if correct, passes the user through to ADFS for issuing of the secure token. The filter plays no role in interpreting ADFS authentication requests or in generating responses.

29 Installation

29.1 Configure The Swivel Server

Configure a Swivel Agent (For standard XML Authentication)

1. On the Swivel Management Console select Server/Agent
2. Enter a name for the Agent
3. Enter the Exchange IP address
4. Enter the shared secret used above on the Exchange Filter
5. Click on Apply to save changes

Agents:	Name:	<input type="text" value="local"/>	
	Hostname/IP:	<input type="text" value="127.0.0.1"/>	
	Shared secret:	<input type="password" value="....."/>	
	Group:	<input type="text" value="---ANY---"/>	
	Authentication Modes:	<input type="text" value="ALL"/>	<input type="button" value="Delete"/>
	Name:	<input type="text" value="IIS"/>	
	Hostname/IP:	<input type="text" value="192.168.1.1"/>	
	Shared secret:	<input type="password" value="....."/>	
	Group:	<input type="text" value="---ANY---"/>	
	Authentication Modes:	<input type="text" value="ALL"/>	<input type="button" value="Delete"/>

Configure Single Channel Access

1. On the Swivel Management Console select Server/Single Channel
2. Ensure ?Allow session request by username? is set to YES

Server>Single Channel

Please specify how single channel security strings are delivered.

Image file:	<input type="text" value="turing.xml"/>
Rotate letters:	<input type="text" value="No"/>
Allow session request by username:	<input type="text" value="Yes"/>
Only use one font per image:	<input type="text" value="Yes"/>
Jiggle characters within slot:	<input type="text" value="No"/>
Add blank trailer frame to animated images:	<input type="text" value="Yes"/>
Text Alpha Value:	<input type="text" value="80"/>
Number of complete display cycles per image:	<input type="text" value="10"/>
Inter-frame delay (1/100s):	<input type="text" value="40"/>
Image Rendering:	<input type="text" value="Static"/>
Multiple Authentications per String:	<input type="text" value="No"/>
Generate animated images:	<input type="text" value="No"/>
Random glyph order when animating:	<input type="text" value="No"/>
No. Characters Visible:	<input type="text" value="1"/>
<input type="button" value="Apply"/> <input type="button" value="Reset"/>	

29.2 Using additional attributes for authentication

When using additional attributes for authentication see [User Attributes How To](#)

29.3 ADFS Integration

The Swivel integration needs to be made on the internet facing ADFS proxy server that customers use for their OWA login.

The following files are used for integration

- FormsSignIn.aspx ? example logon page
- Web.config ? example configuration file
- Pinsafe_image.aspx ? TURING image proxy web page
- Exists.aspx ? utility web page to check if a user exists
- Bin\PINsafeASPNetFilter.dll ? the PINsafe HTTP module that manages authentication
- Bin\PINsafeClient.dll ? manages PINsafe communication

29.3.1 Copy required files to the ADFS server

Copy *pinsafe_image.aspx* and *exists.aspx* to the *adfs\ls*

Copy the *PINsafeASPNetFilter.dll* and *PINsafeClient.dll* to *adfs\ls\bin* (you may need to create this folder).

29.3.2 Modify the ADFS login pages

The other two files, *FormsSignIn.aspx* and *web.config*, are example files only. You should examine these files, and copy the relevant parts to your existing versions of these files, modifying them as appropriate. Instructions are included in the files themselves. Each section that needs to be changed or inserted is prefixed by and ended by .

29.3.2.1 web.config options

PINsafeServer default: 192.168.78.103, The IP address or hostname of the Swivel server.

PINsafePort default: 8080, The port used to communicate with the Swivel server. This usually should be 8080 for appliance and software installations.

PINsafeContext default: pinsafe, The Swivel application installation name, usually *pinsafe*.

PINsafeSecure default: True, On the *PINsafePort* if the Swivel server is using SSL communication this should be set to Yes, if no SSL is used this should be set to False.

PINsafeSecret default: secret, This needs to be set to the same as that set on the Swivel server Agent.

PINsafeLogonPath default: /adfs/ls/, the logon path to be used.

PINsafeLogoffPath default: /adfs/ls/, the logoff path to be used.

PINsafeExcludedPaths default: /adfs/ls/MasterPages/;./pinsafe_image.aspx, Add any custom paths that need to be accessed during authentication here.

PINsafeIgnoreDomain default: true, If True it will strip off the domain name to get the PINsafe username, if False it will not alter the user login name.

PINsafeAcceptSelfSigned default: True, If set to True it will allow self signed and invalid certificates to be used on the Swivel server. If set to False, the certificate must be correct for that of the Swivel server.

PINsafePassword default: True"

PINsafeImage default: True, If True Display a single Channel authentication image, if False do not display an image.

PINsafeMessage default: False, If True send the user an dual channel message, if False do not send the user a message.

PINsafeCookieSecret default: will be generated randomly.

PINsafeldleTimeSecs default: 300

AllowNonPINsafeUsers default: False, If True allow non Swivel users to authenticate without Swivel authentication, if False do not permit non Swivel users to authenticate. the option to allow unknown users to authenticate without Swivel authentication only applies to users not known to Swivel at all. You cannot specify that it only applies to a group of users, and not to other users who are known to Swivel, but not in a particular group.

PINsafeFilterEnabled default: True, If true the Swivel ADFS filter is working, if False the Swivel ADFS filter is present but Swivel authentication is disabled.

PINsafeAuthenticationDomain default:

PINsafeUsernameField default: ctl00\$ContentPlaceHolder1\$UsernameTextBox

PINsafeOTCFIELD default: otc, The prompt displayed to users where the Swivel authentication details should be entered.

29.3.3 Restart IIS

Restart IIS on the ADFS server for the changes to take effect.

29.4 Additional Installation Options

29.4.1 Disabling or enabling the Automated TURING

If login methods other than the TURING are to be used such as SMS, Mobile Client or Token, then the automated TURING must be disabled. This is for Swivel ADFS filter version 1.2.

Backup then edit the file *C:\inetpub\adfs\FormsSignIn.aspx*

Find the line with only *showTuring()*; and comment out using as below. To re-enable remove the comments.

```
rowTuring.style.display = "";
showTuring();
{
```

to

```
rowTuring.style.display = "";
```

```
{
```

Reload the browser and verify that the login page is now correct.

29.4.2 Changing the Show TURING Button

After applying the Swivel customisation, go to C:\inetpub\adfs\ls and edit as an Administrator the FormsSignIn.aspx. Look for "Show TURING" and alter it as appropriate.

30 Testing the Installation

The next time you try to access the ADFS login page, there will be no apparent difference to the login page. However, after you enter the username, for an existing user, you should see an additional field for one-time code, and a button to request a TURING image. You should not be able to authenticate to ADFS without entering both the AD password AND the PINsafe one-time code.

31 Uninstalling the Swivel Integration

32 Troubleshooting

Check the Swivel logs

Check the ADFS server logs

33 Known Issues and Limitations

The ADFS proxy currently does not support a redirect if the user is required to Change their PIN.

34 Additional Information

35 Additional documentation

35.1 Swivel

Swivel ADFS and Office 365

High Level Overview Document