

Microsoft ADFS 4 and 3 Authentication

Contents

- 1 Introduction
- 2 Requirements
 - ◆ 2.1 Current Version Installer
 - ◆ 2.2 Previous Versions
 - ◆ 2.3 Version History
 - ◆ 2.4 Networking Requirements
 - ◆ 2.5 Configure Sentry Agent
- 3 Installation
- 4 Configuration
- 5 Using the Swivel Proxy
 - ◆ 5.1 Proxy Configuration
 - ◆ 5.2 Enabling the Proxy Web Application
- 6 Using the Authentication Provider
- 7 Advanced Features
 - ◆ 7.1 Requiring Swivel Authentication for Single Applications
 - ◇ 7.1.1 ADFS 4.0
 - ◇ 7.1.2 ADFS 3.0
 - ◆ 7.2 Customising the Login Page Look and Feel
- 8 Known Issues
 - ◆ 8.1 Public Access to Swivel Server, Untrusted Certificates and TURING/Pinpad Images
 - ◆ 8.2 Problems Registering the Authentication Provider
- 9 Uninstalling the Authentication Provider
- 10 Upgrading
- 11 Troubleshooting
- 12 Error Messages

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](#)

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.

Current Version Installer

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

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](#).

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

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.

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](#)

▢ [New Entry](#)

Name:

ADFS

Hostname/IP:

fs.office365.swivelsecure.c

Shared secret:

000000

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

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.

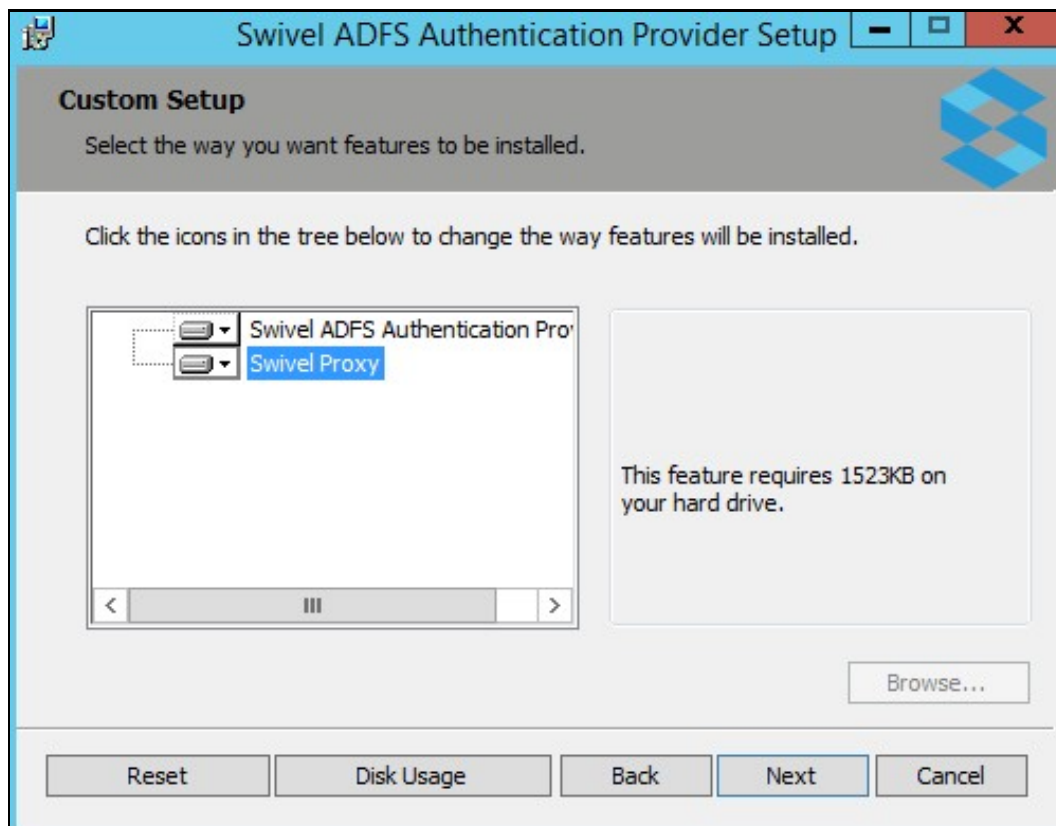
To install this product, simply unzip the file SwivelAuthProviderInstall.msi from the download and double-click it. Note that you must be logged in as an administrator to install this product. If you are not logged in as administrator, open a command prompt as administrator, switch to the directory containing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

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



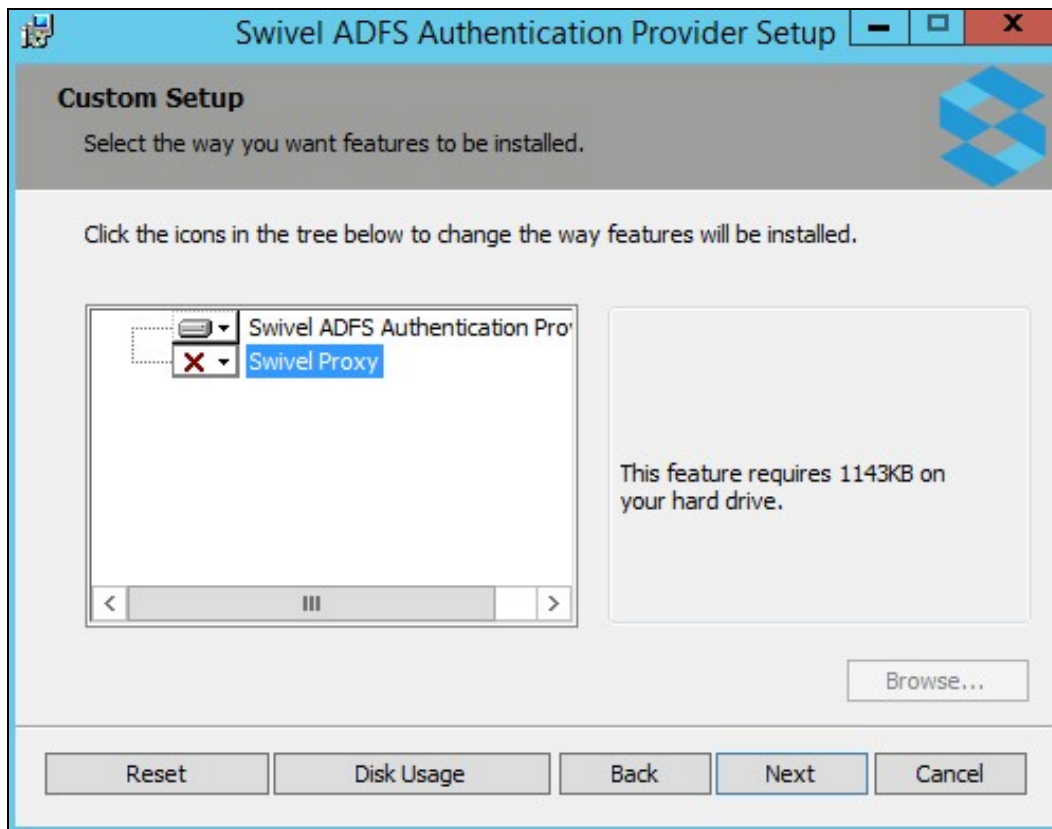
You will next be asked to choose whether to install the ADFS Authentication Provider, the Swivel proxy or both. There are a number of possible scenarios, summarized below.

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

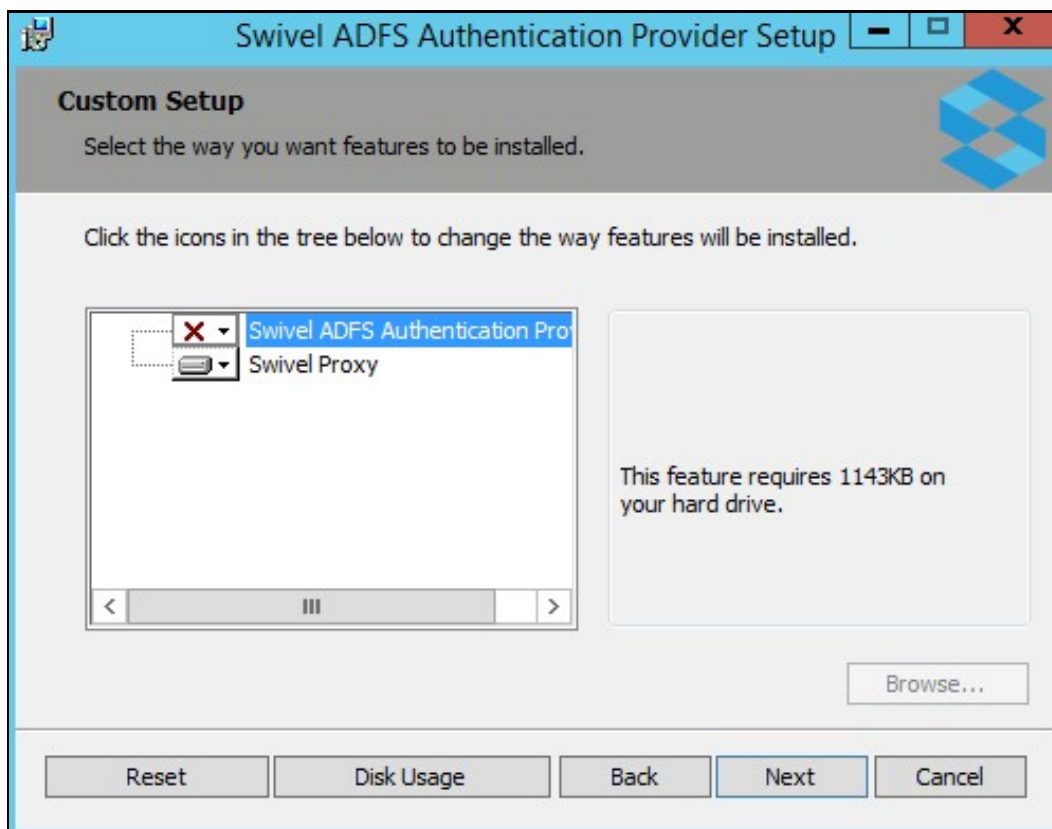


- Single ADFS server, no IIS:

- ◆ Install Authentication provider only. For Swivel single channel, you will need to provide some other method to display the TURING or Pinpad.



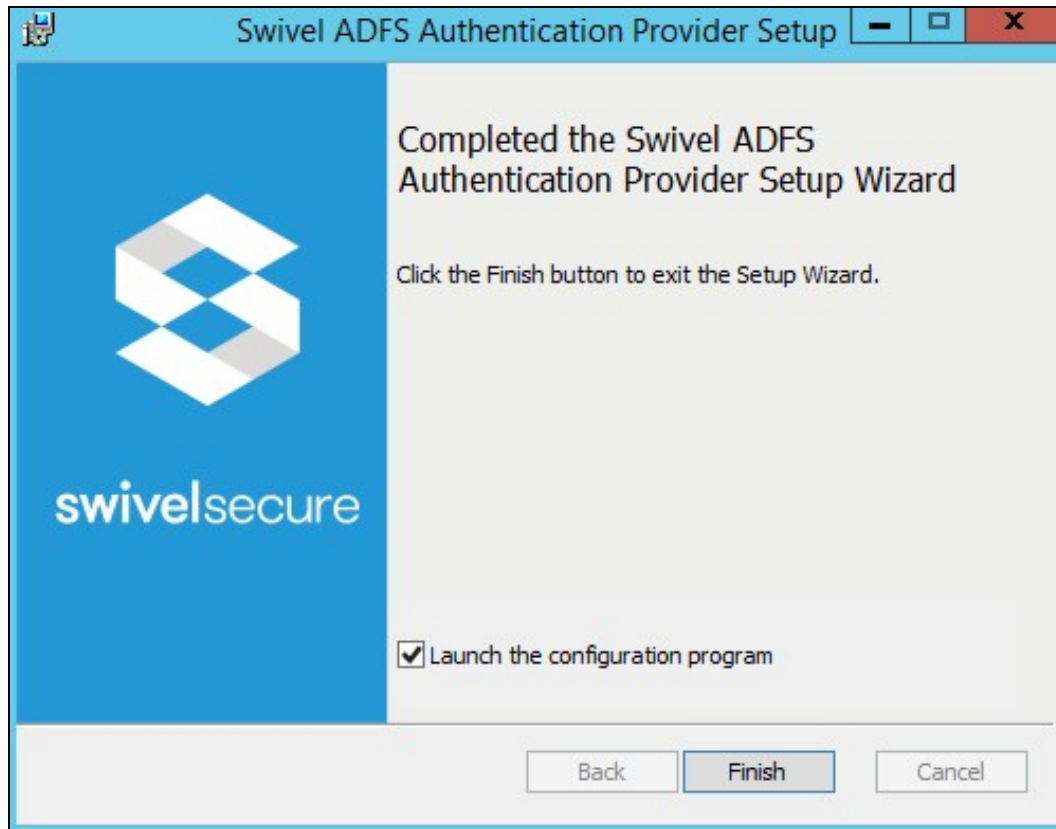
- ADFS server and ADFS proxy, IIS installed on the proxy:
 - ◆ Install Authentication provider only on the ADFS server.
 - ◆ Install proxy component only on the ADFS proxy.



- 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.

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.

Swivel Authentication Provider Configuration

Settings

Languages

Logging

Advanced

Swivel URL:

https

:

4173495770.swivelcloud

:

443

/

proxy

Alternate..

☐

Allow self-signed certificates

Agent Secret:

Confirm Secret:

Image Type:

☐ None

☐ Turing

☒ PinPad

☐ Message

☐ Push

☐ Allow non-PINsafe users

☒ Ignore domain prefix

☐ Ignore domain suffix

☒ Hide OTC for Pinpad

☒ Auto-show Image

Image Source:

Remote Proxy

Virtual Directory...

https://www.swiveladfs.com/sentry

Turing URL:

https://www.swiveladfs.com/sentry/swivel_image.aspx

Message URL:

https://www.swiveladfs.com/sentry/swivel_message.aspx

PINpad URL:

https://www.swiveladfs.com/sentry/swivel_pinpad.aspx

Push URL:

https://www.swiveladfs.com/sentry/swivel_push.aspx

Push response URL:

https://www.swiveladfs.com/sentry/swivel_push_response.aspx

Session start URL:

https://www.swiveladfs.com/sentry/swivel_session.aspx

OK

Cancel

Save

Swivel Secure ADFS Authentication Provider, version 1.4.3.0, Copyright © Swivel Secure Ltd 2022

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 is a "Swivel URL" field with a dropdown menu set to "https", followed by a text box containing "sentry.swiveladfs.com", a port field with "8080", and a path field with "sentry". Below this is a "Secret:" label followed by a masked text box. 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:

OKCancelSave

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.

Using the Swivel Proxy

Proxy Configuration

Swivel Authentication Provider Configuration

Proxy

Logging

Advanced

Swivel URL:

https

:

4173495770.swivelcloud

:

443

/

proxy

Alternate..

☒

Allow self-signed certificates

ADFS Host:

https://fs.swiveladfs.com

Agent Secret:

Confirm Secret:

[Virtual Directory...](#)

/sentry

OK

Cancel

Save

Swivel Secure ADFS Authentication Provider, version 1.4.3.0, Copyright © Swivel Secure Ltd 2022

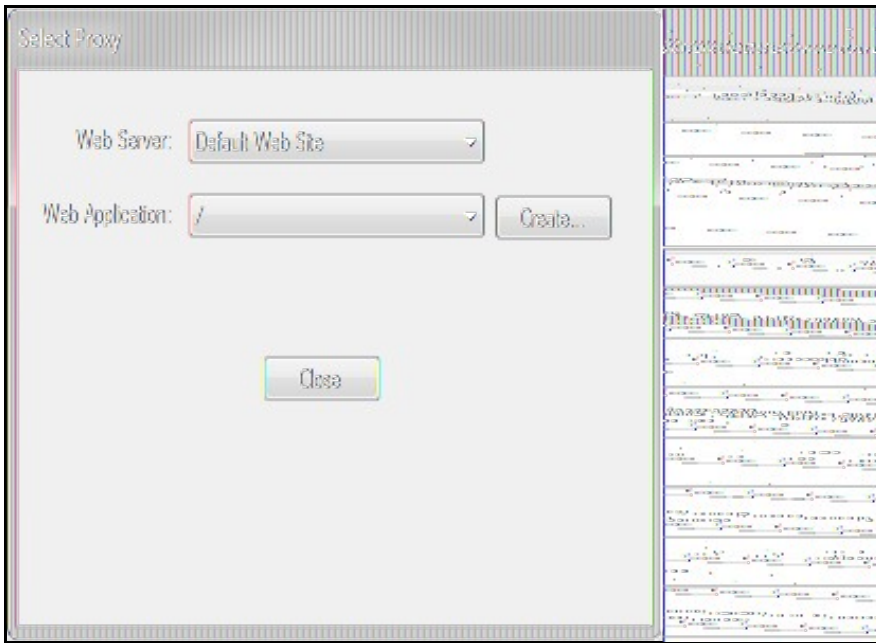
The proxy configuration program is largely a simplified version of the full configuration program, including just the Settings, Logging and Advanced tabs. However, there is one additional option to take note of:

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.

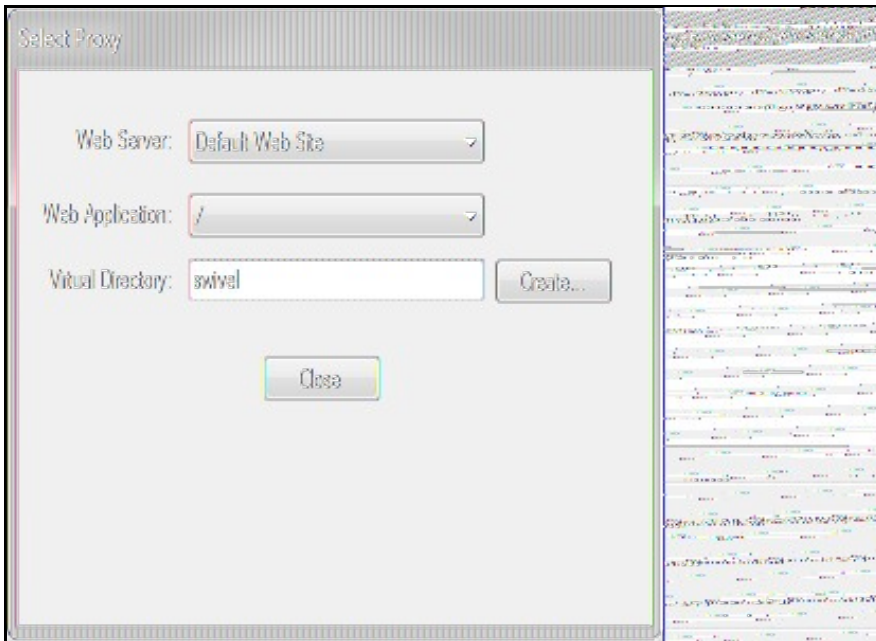
After making any changes to the proxy configuration, you should restart IIS to ensure the changes are registered.

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.

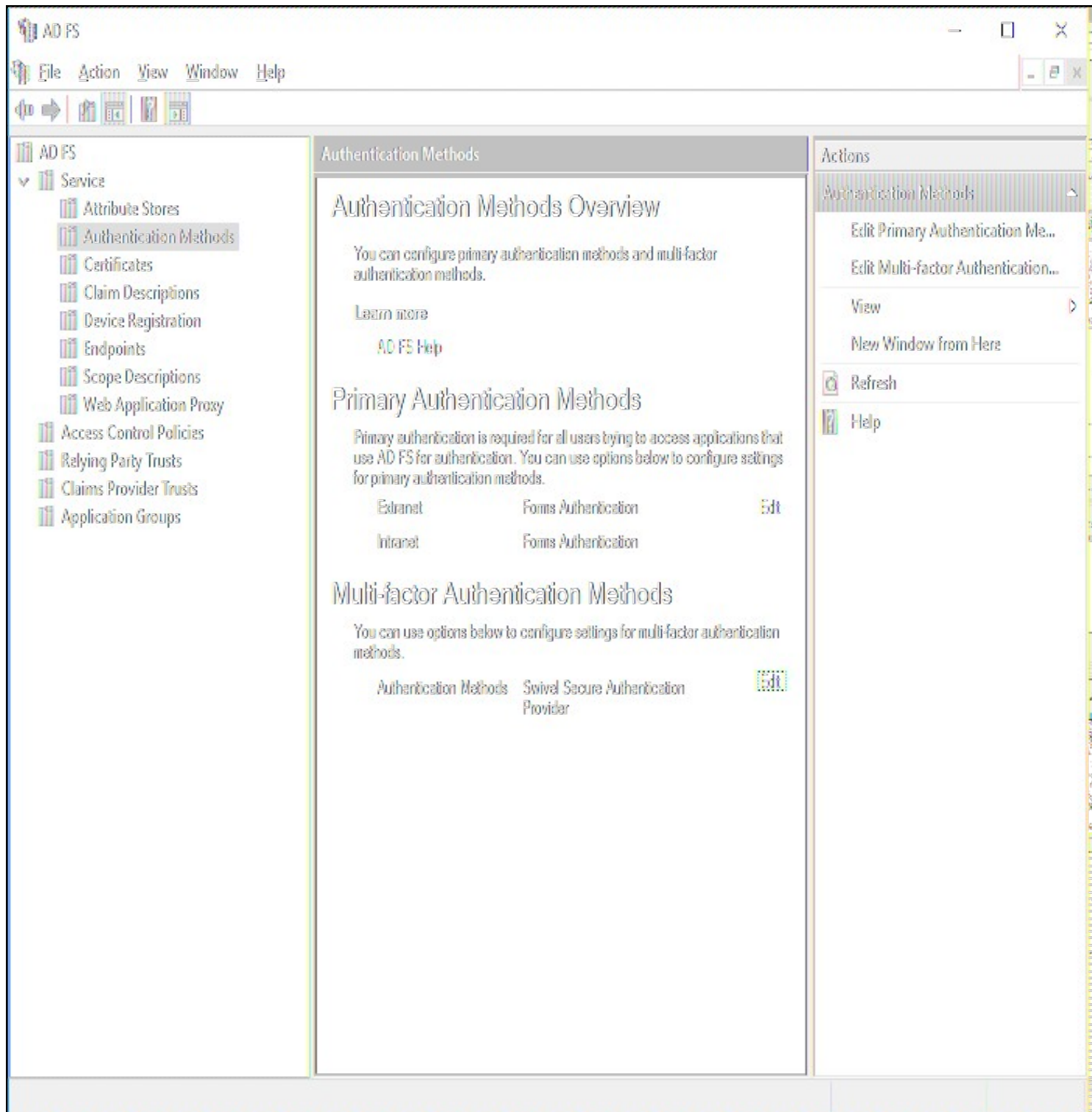
An additional menu option is provided to remove the virtual directory. This should normally be done before uninstalling the authentication provider.

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:

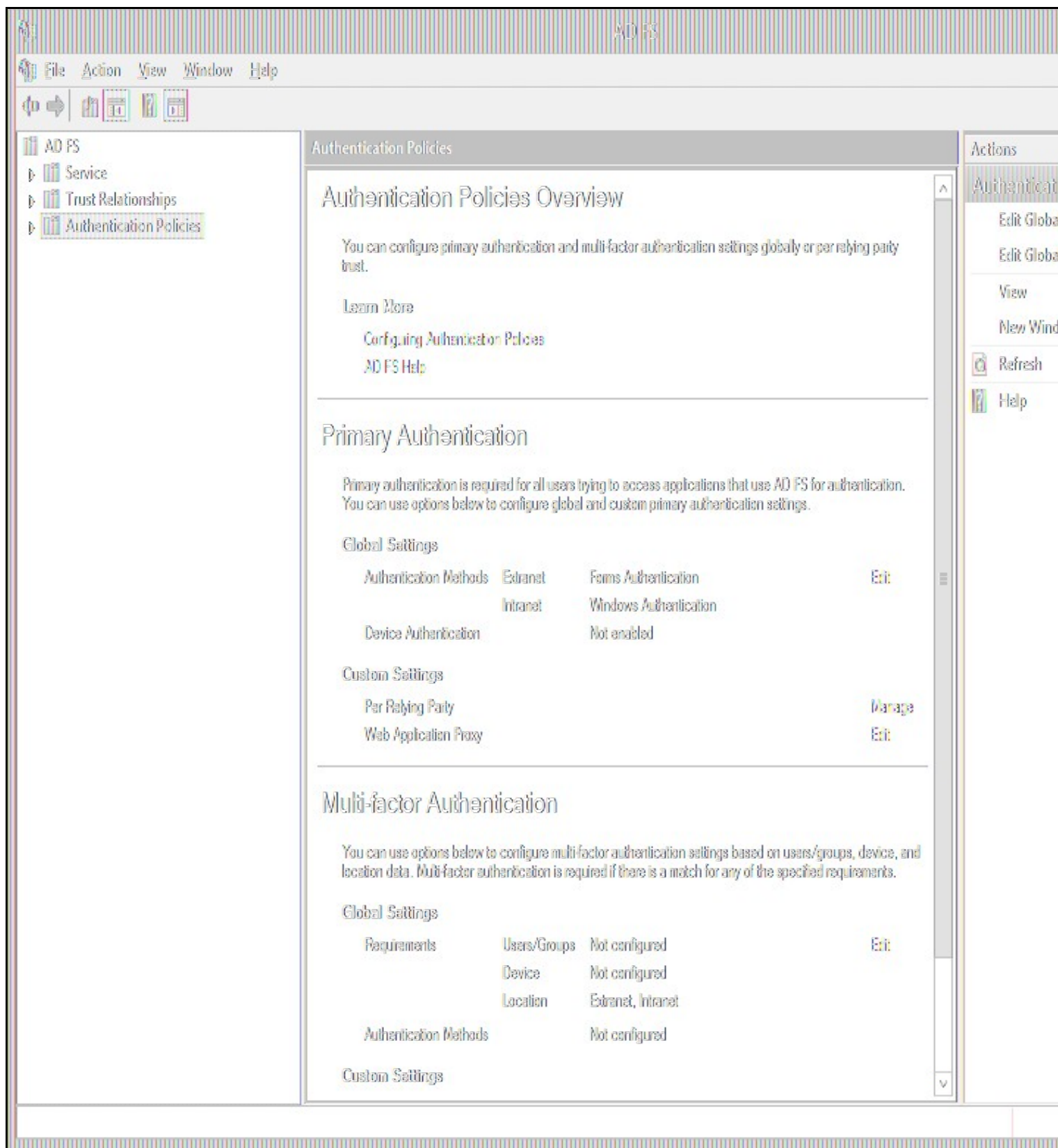
From *Administrative Tools*, select *AD FS Management*,

This is the dialog for ADFS 4:



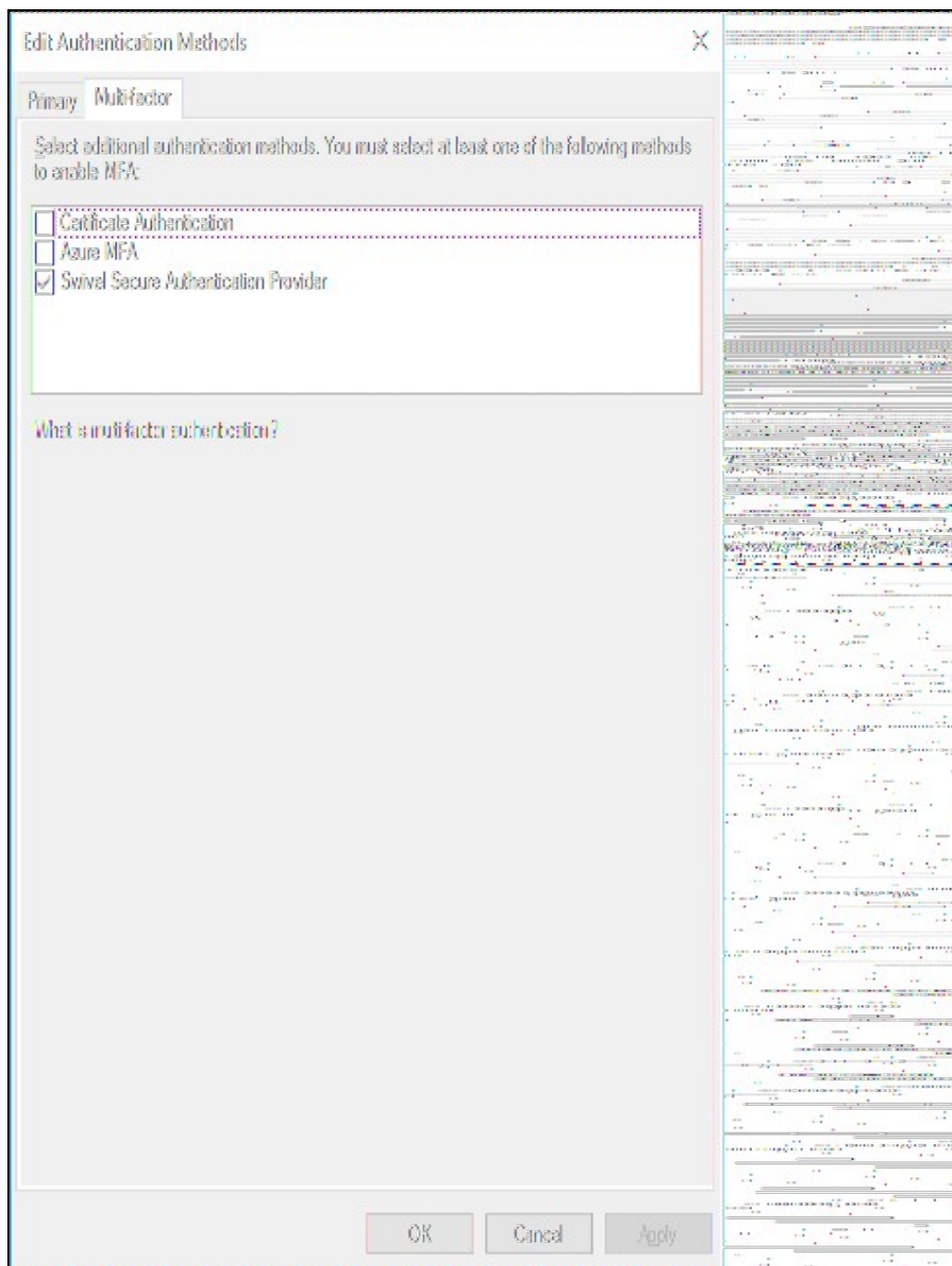
In ADFS 4.0, select *Service*, then *Authentication Methods*.

This is the dialog for ADFS 3:

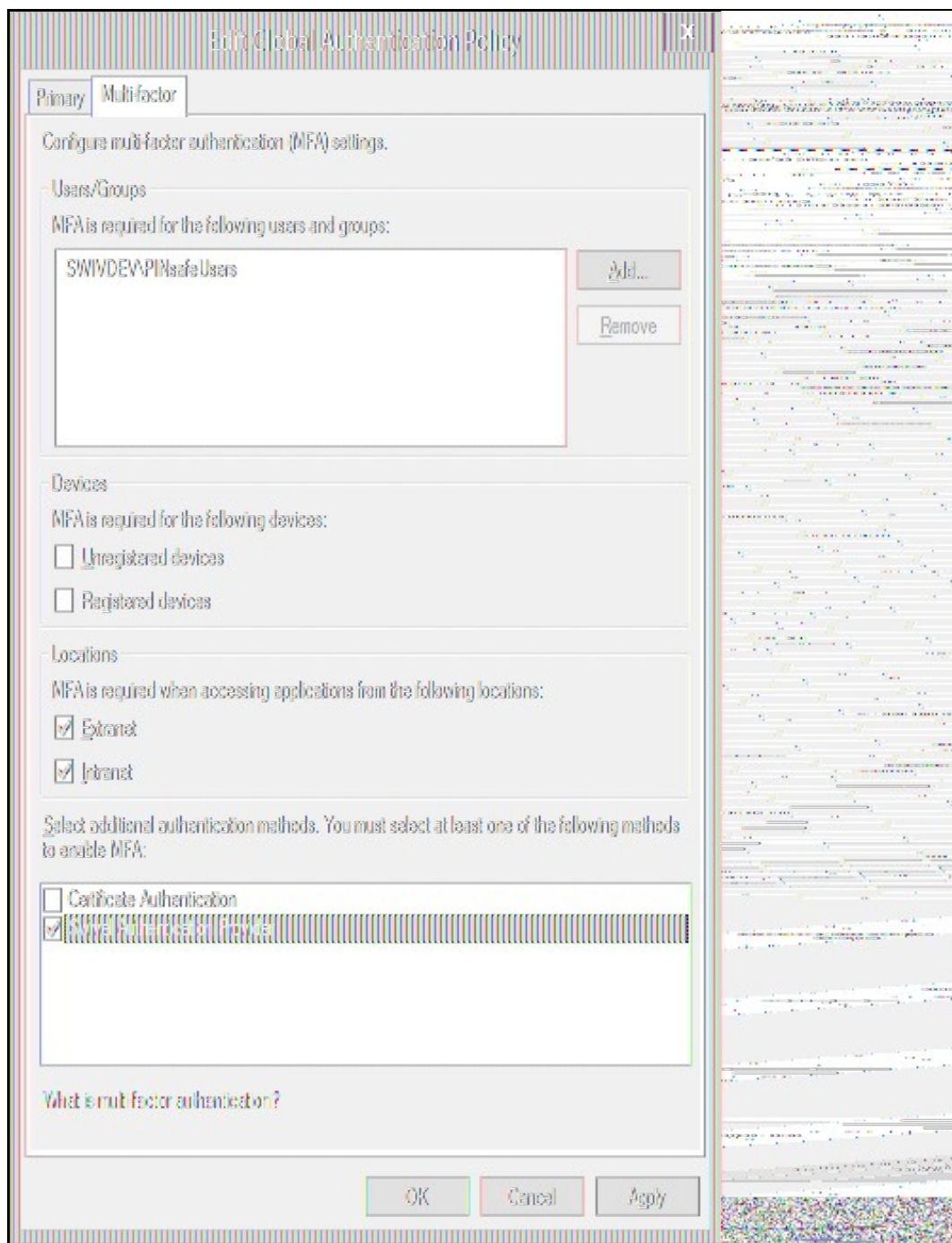


In AD FS 3.0, choose *Authentication Policies*.

Under *Multi-factor Authentication*, click Edit.



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



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.

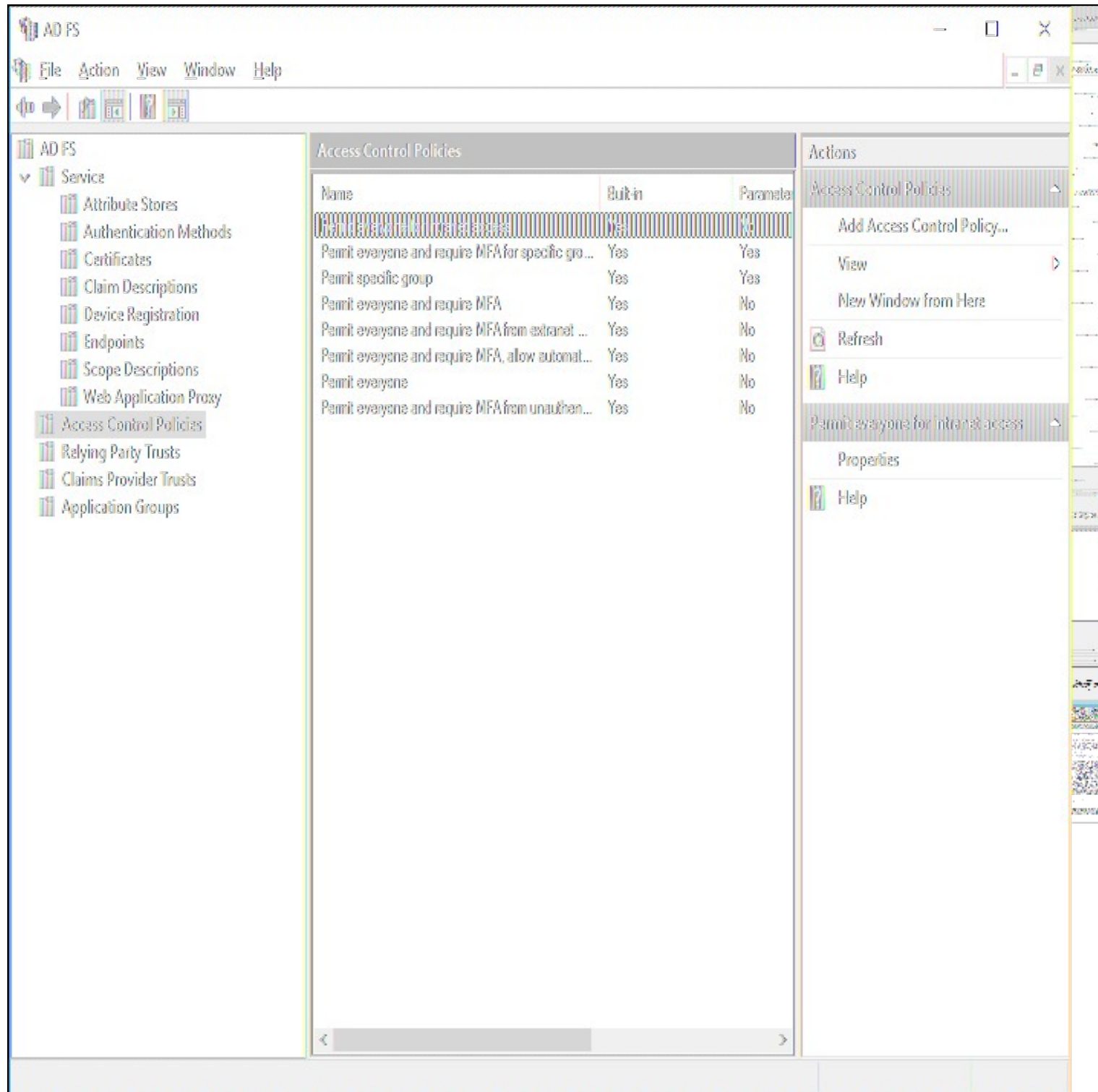
Advanced Features

Requiring Swivel Authentication for Single Applications

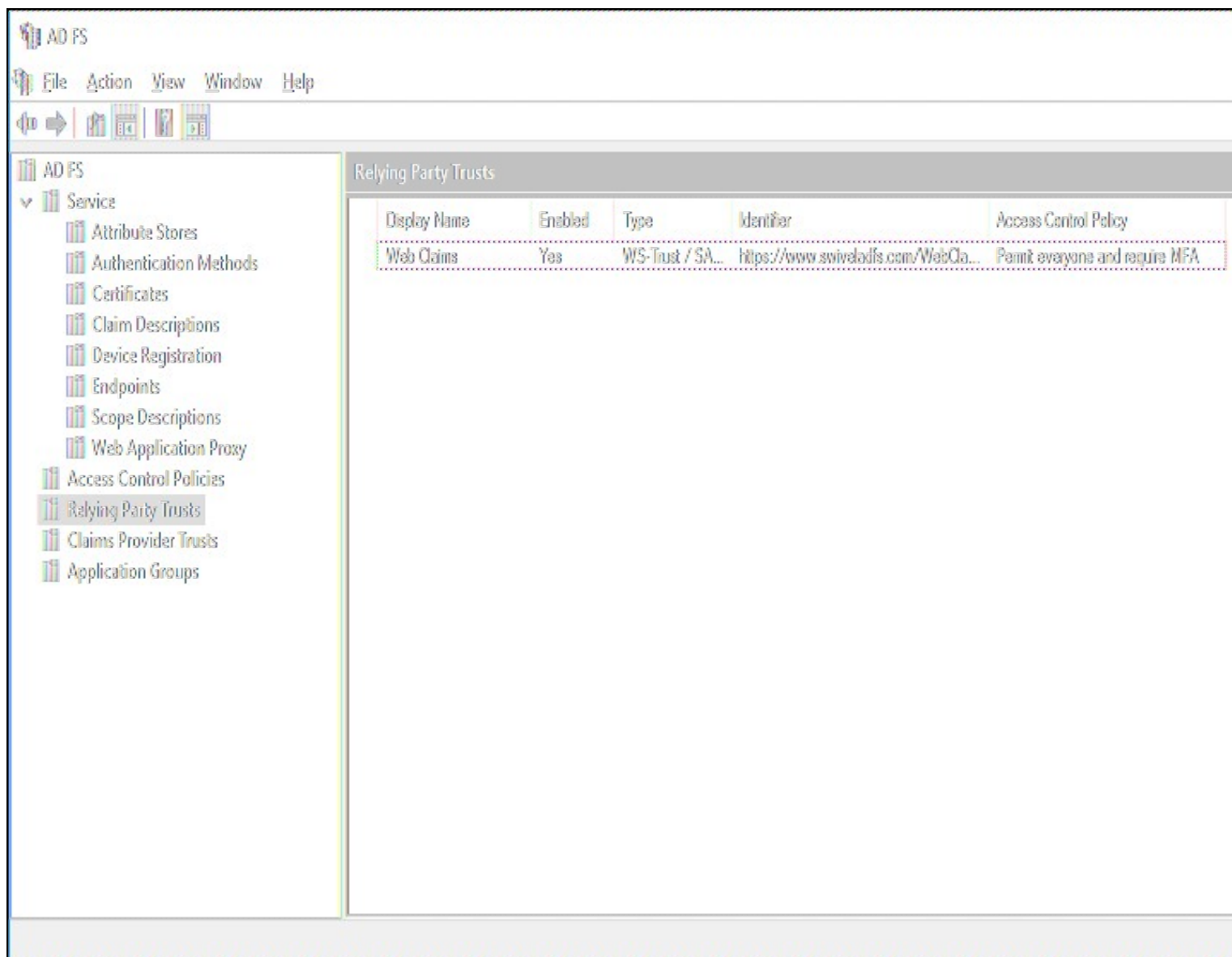
NOTE: these instructions are relevant to any ADFS Multi-Factor Authentication provider, not just Swivel, so are subject to the facilities provided by Microsoft. The way authentication is configured has changed considerably in ADFS 4.0, so we provide two separate sets of instructions.

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:

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.

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.

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.

Known Issues

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.

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.

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.

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.

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>

Error Messages