Microsoft ADFS 2 Integration

Contents

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.

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

Prerequisites

- ADFS version 2.0 or later, or ADFS 2.0 proxy.
- Swivel ADFS filter, downloadable from here.

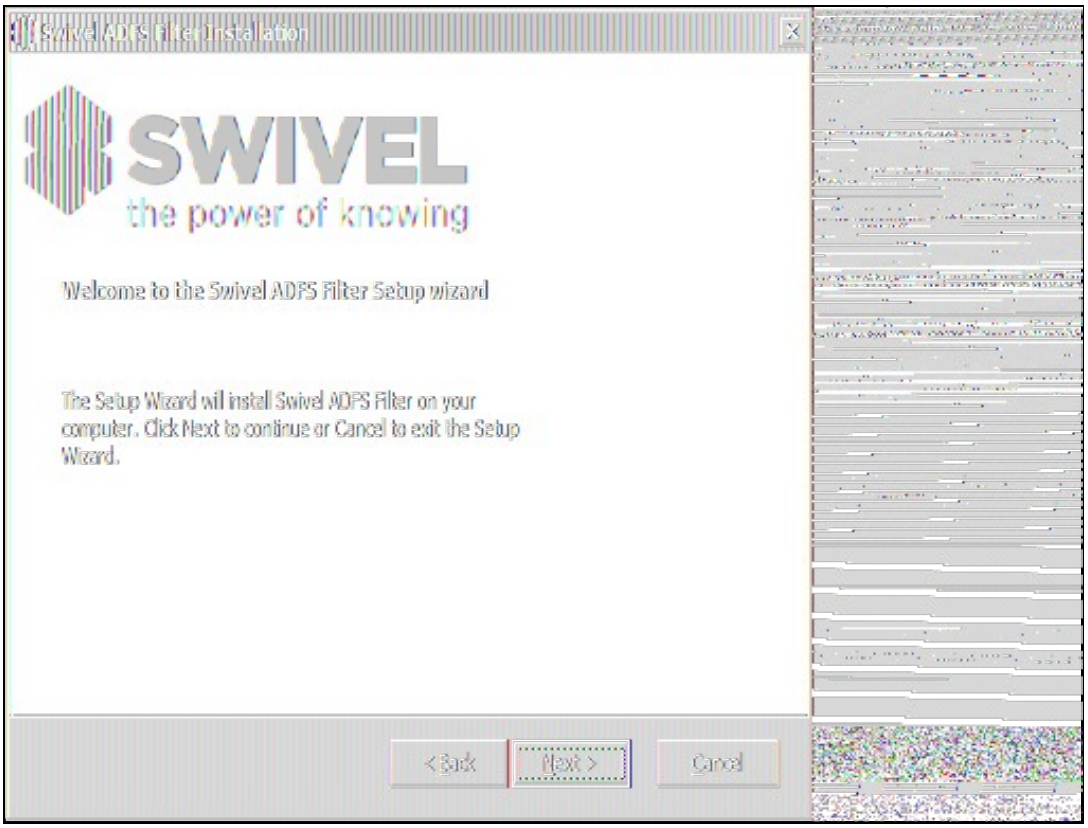
How to Guide

Swivel Configuration Changes

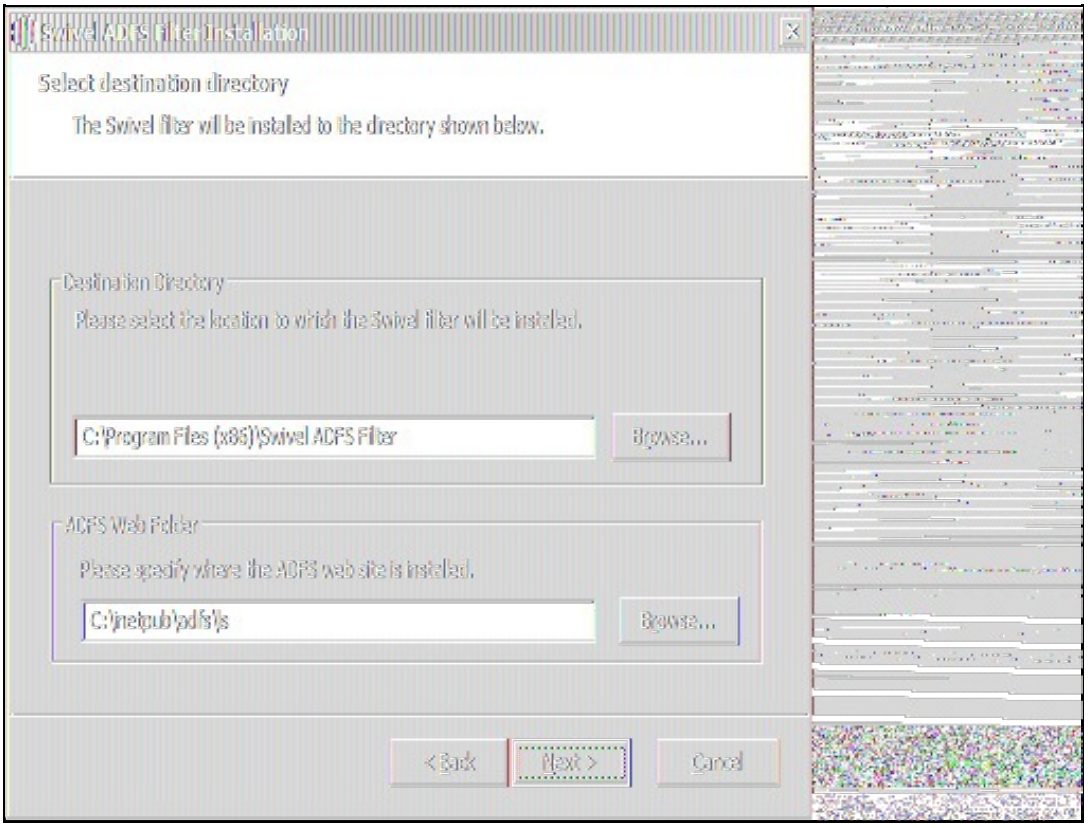
- Under Server -> Single Channel, ensure that ?Allow session start by username? is set to Yes.
- Under Server -> Agents, add the ADFS server as an Agent, and make a note of the secret you enter here.

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:

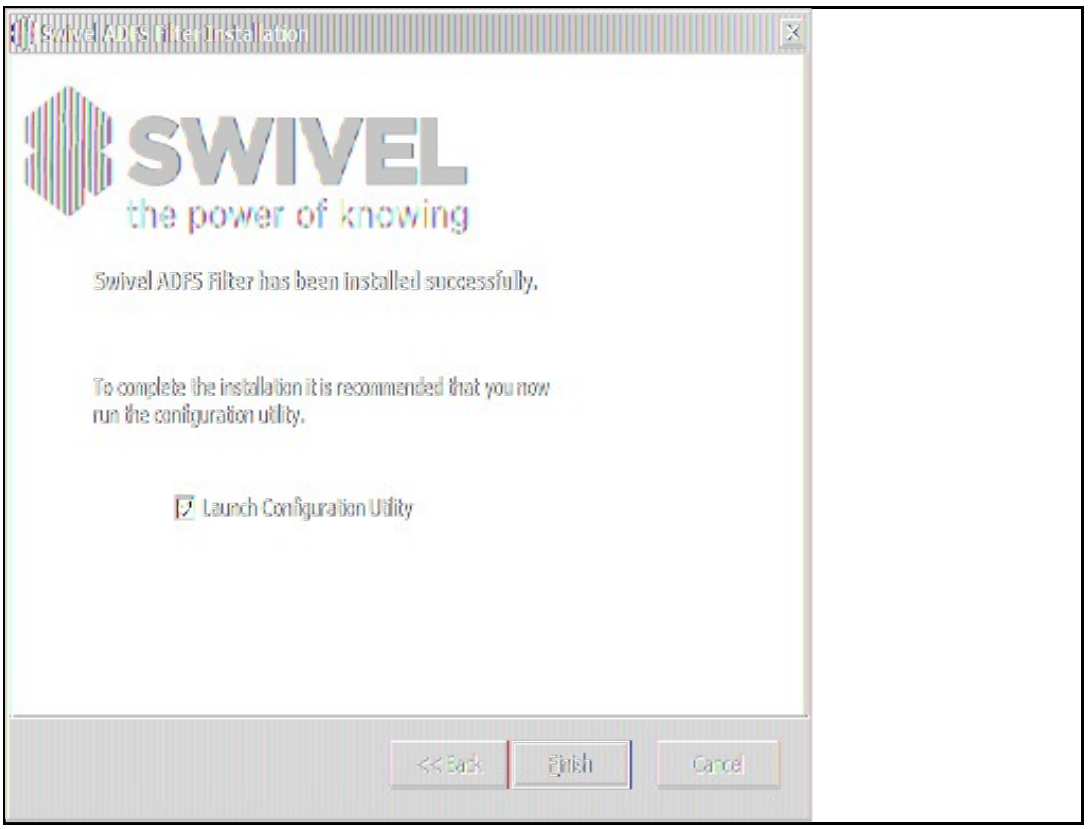


You would normally accept the destination directory as default. Note, however, that if the ADFS Web folder is not in the default location, C:\inetpub\adfs\ls, then you should change the second location to match the correct location. Click Next when these values are correct.

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.

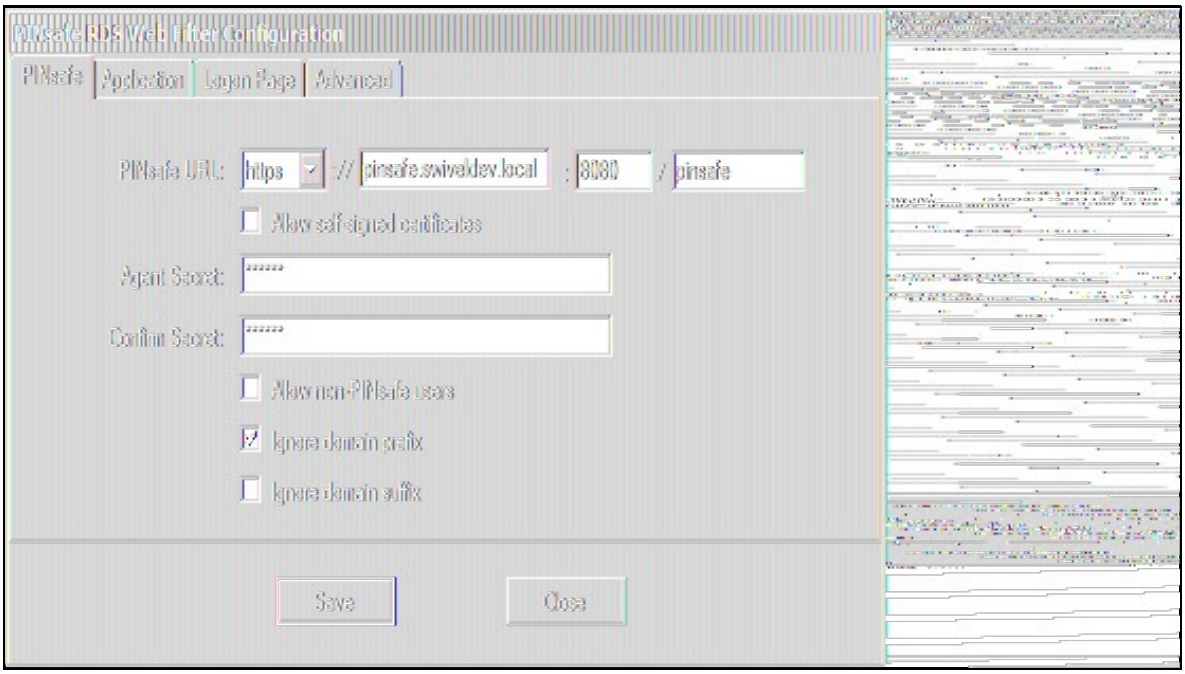
When installation is complete, you will see the following screen:



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.

Configuring the Swivel ADFS Filter

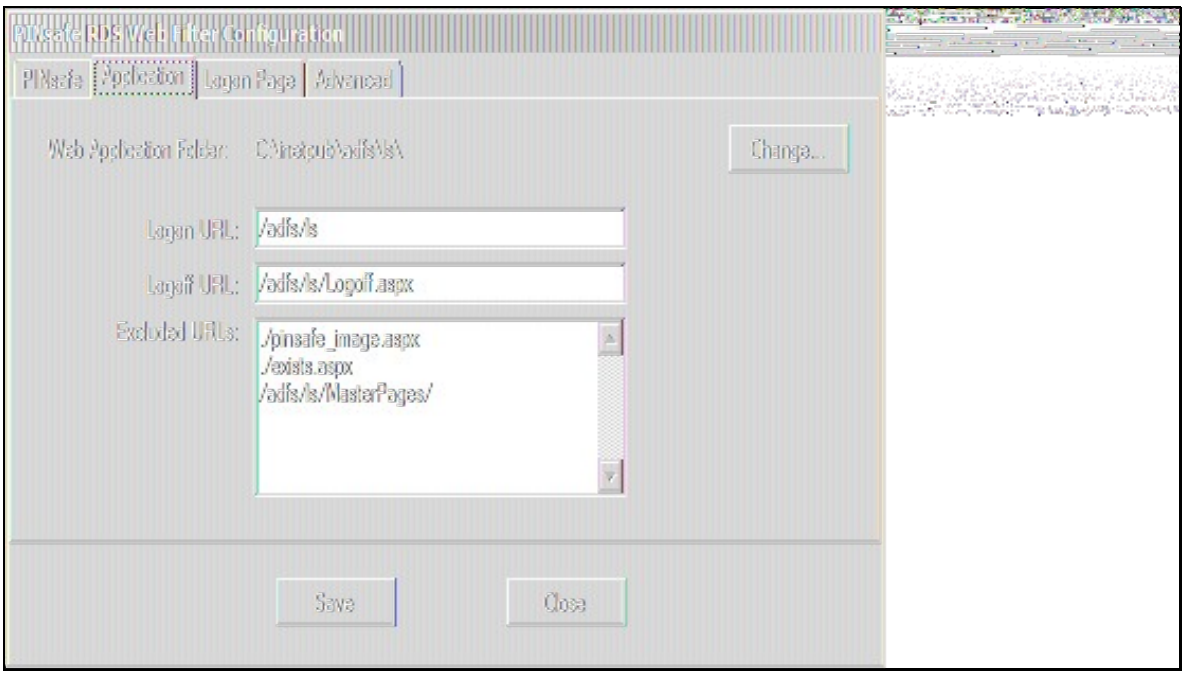
The configuration program consists of four tabs:



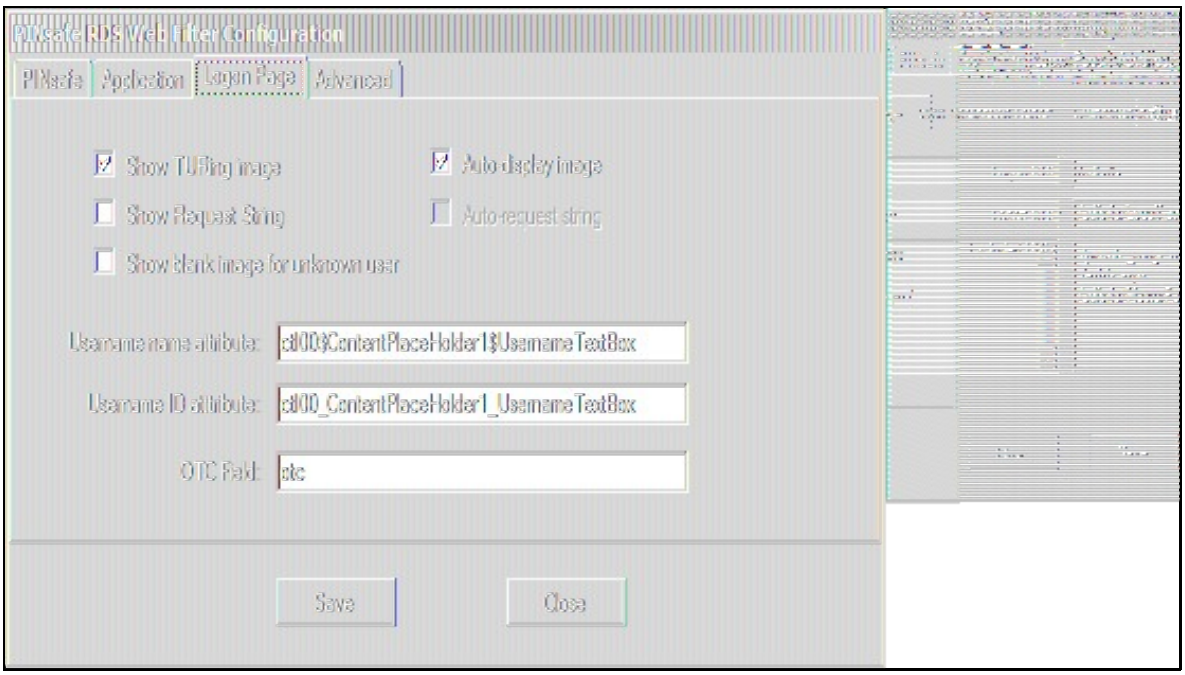
The PINsafe tab allows you to specify the details for the Swivel server. Most of these settings should be obvious. You should check the option **Allow self-signed certificates** if you are using https and your SSL certificate is not either a commercial certificate or one generated by an internal certificate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

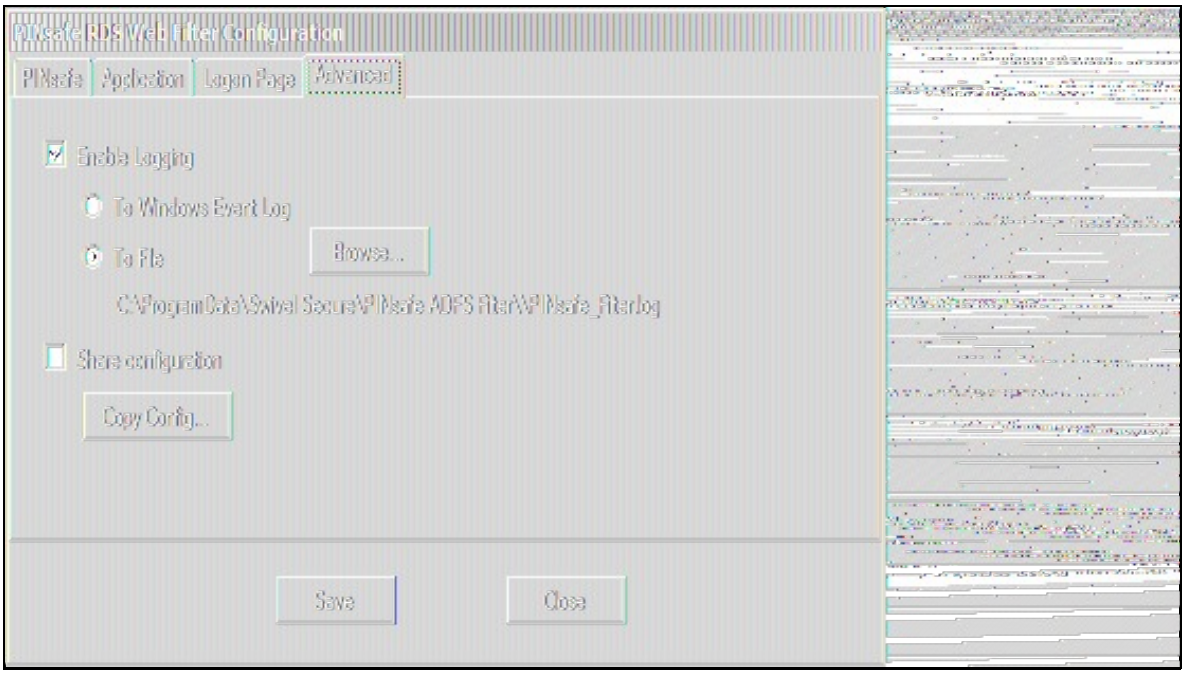


The second page shows details of the ADFS web application. You should not normally need to change any of these settings. Ensure that the Excluded URLs section includes all the names listed above.



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.

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.

Additional Configuration Options

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.

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.

Testing

Known Issues

Troubleshooting