Microsoft RD Web Access

Contents

Introduction

This filter allows you to protect Windows Remote Desktop Services (RDS) Web Access with Swivel authentication.

-

MS RD Web & TURing

-

MS RD Web & SMS / Mobile App.

Prerequisites

Swivel version 3.x or 4.x

Windows Server 2012 R2 or Windows Server 2016 with RDS Web Access already installed

Microsoft.Net Framework version 4.5, full edition (rather than client-only) installed

A version compatible with Windows Server 2008 is also available. This requires Microsoft.Net framework 4.0 only.

Swivel Server Configuration

The only configuration you need to do on the Swivel server is to ensure that the RDS server is configured as an Agent for Swivel (under Server -> Agents), and if you are using the TURing image or PINpad, that under Server -> Single Channel, the option Allow session request by username is set to Yes.
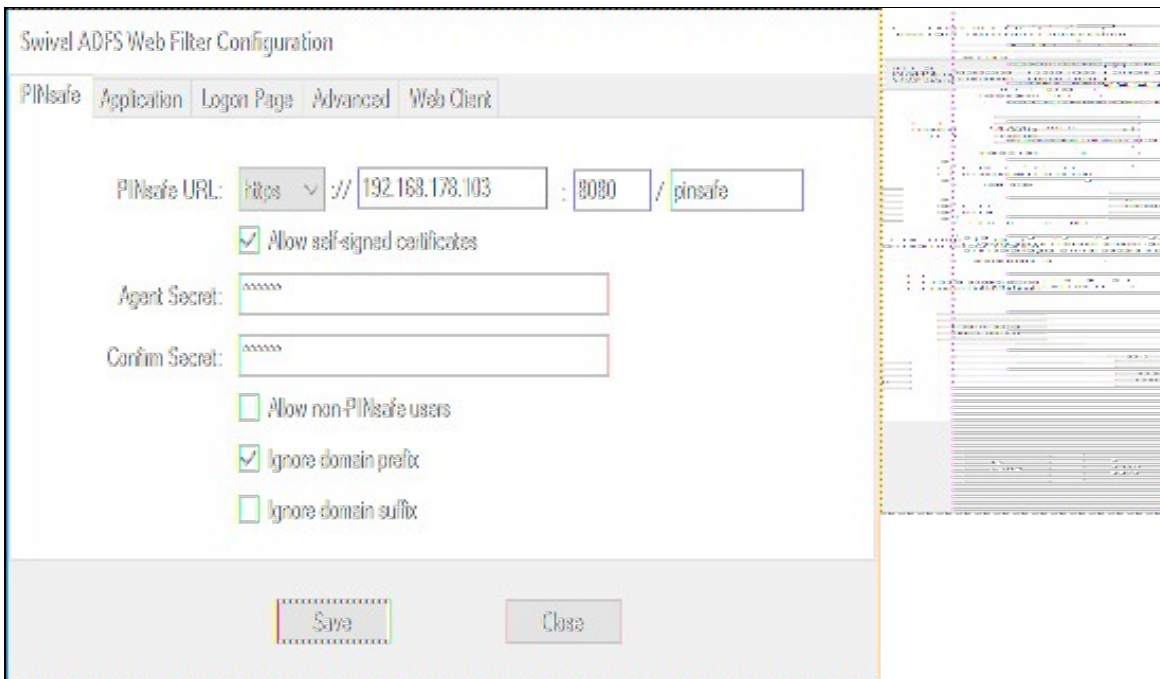
Installation

You can download the Windows Server 2019 filter from here, the Windows Server 2016 filter from here and the Windows Server 2012 R2 filter from here. The version compatible with Windows Server 2008 is available from here.

Installation consists of a single executable, RDSWebFilterInstaller.exe. In most cases you can accept the default settings during installation. When you get to the destination folder, make sure that the RDS web root folder is selected correctly. In most cases, C:\Windows\Web\RDWeb will be correct, but make sure if your configuration is not a default installation that the right folder is selected.
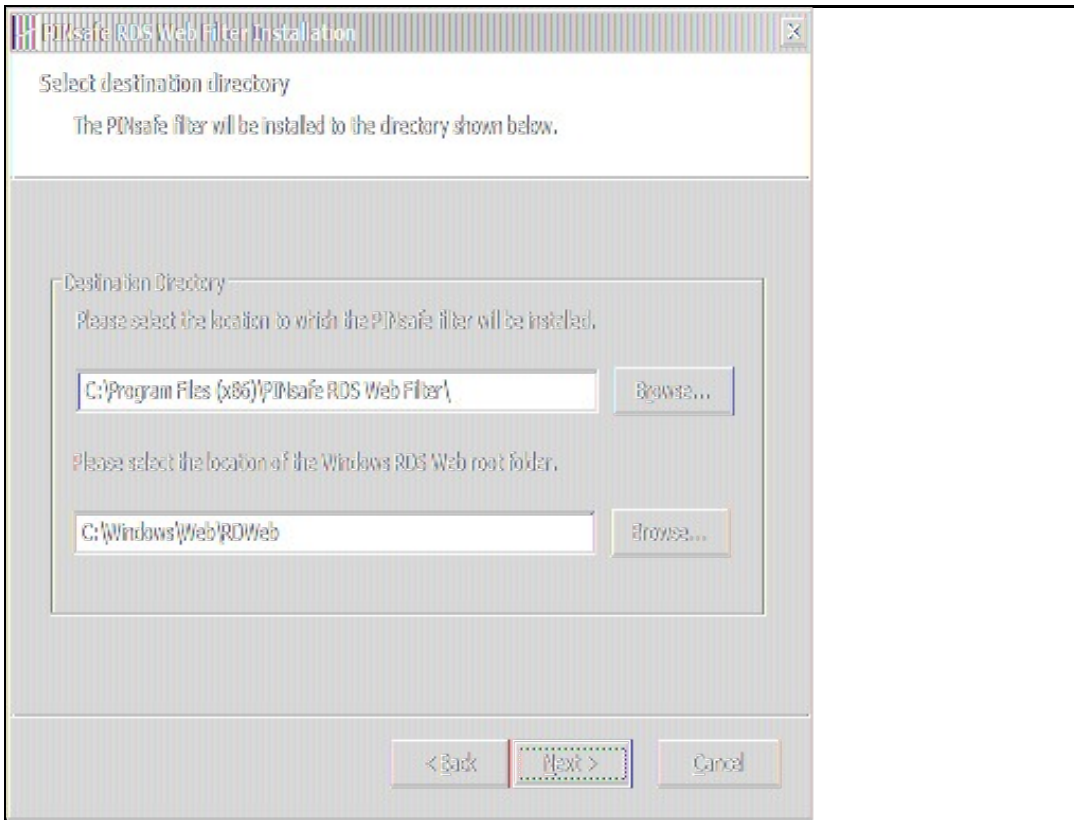
Configuration

When installation is completed, you will be presented by the configuration page, as shown here.

Configuration Options

PINsafe URL: select https or http, enter the Swivel IP or hostname. Use port 8080, unless you have a custom installation. The context will be "pinsafe" for version 3.x and "sentry" for version 4.x.

Note: do not use the ?:8443/proxy? URL, as that is not valid for authentication.

Allow self-signed certificates Check box, Check the box to ignore certificate errors

Agent Secret: and **Confirm Secret:** The shared secret entered on the Swivel instance under Server/Agents

Allow non-PINsafe Users if checked permits users that do not have PINsafe accounts to log in with just username and password.

Ignore domain prefix and **Ignore domain suffix** if checked remove the domain name before or after the username before passing to PINsafe. The fully-qualified name is always passed to Windows for authentication.
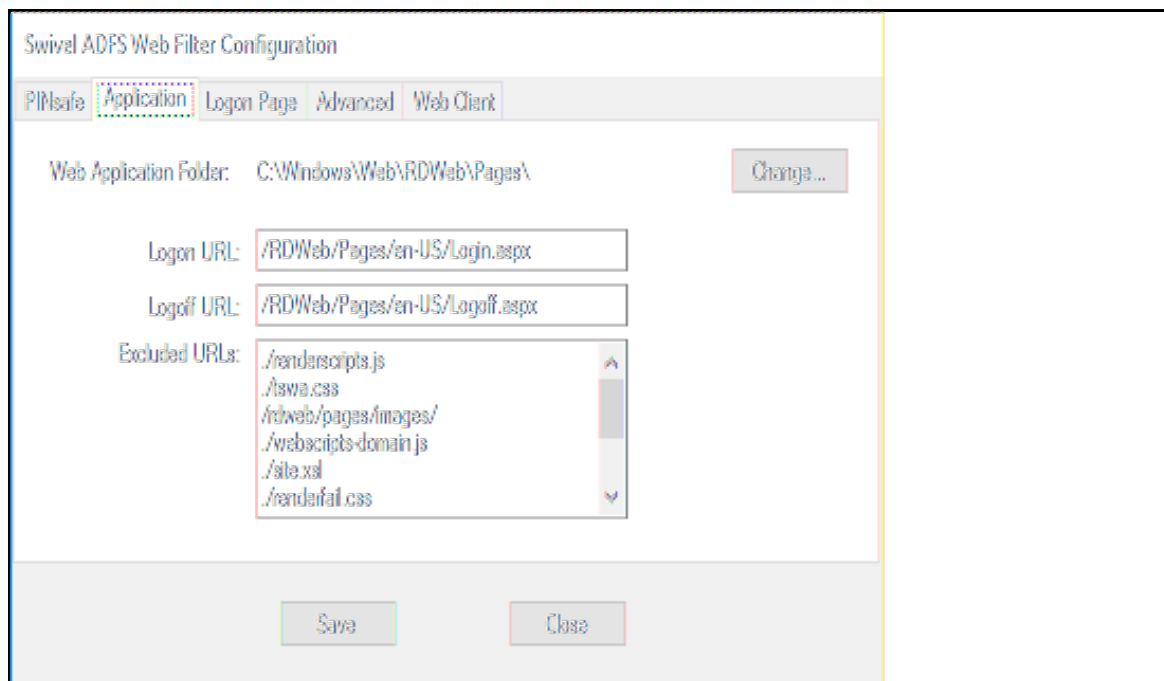

Web Application Folder: Change allows a new path to be specified

The following settings you will probably not need to change, unless you have customised your login page. In this case, make sure that any images, scripts or stylesheets you have added are listed under the Excluded URLs. An entry beginning with ?./? will match any path that ends with the remaining part of the path: for example, ?./renderscripts.js? will match the file renderscripts.js wherever it is in the web hierarchy. Any files not listed under Excluded URLs, or the logon or logoff path, will be blocked by the Swivel filter, until you have authenticated to Swivel.

Logon URL: default: /RDWeb/Pages/en-US/Login.aspx

Logoff URL: default: /RDWEB/Pages/en-US/Logoff.aspx

Excluded URLs: list of URLs for which authentication is excluded. NOTE: URLs must be entered one per line, but unfortunately, it is not possible to enter new lines into this box. To change it, you must therefore copy the current list into a text editor, make any changes required and then paste the new list back.
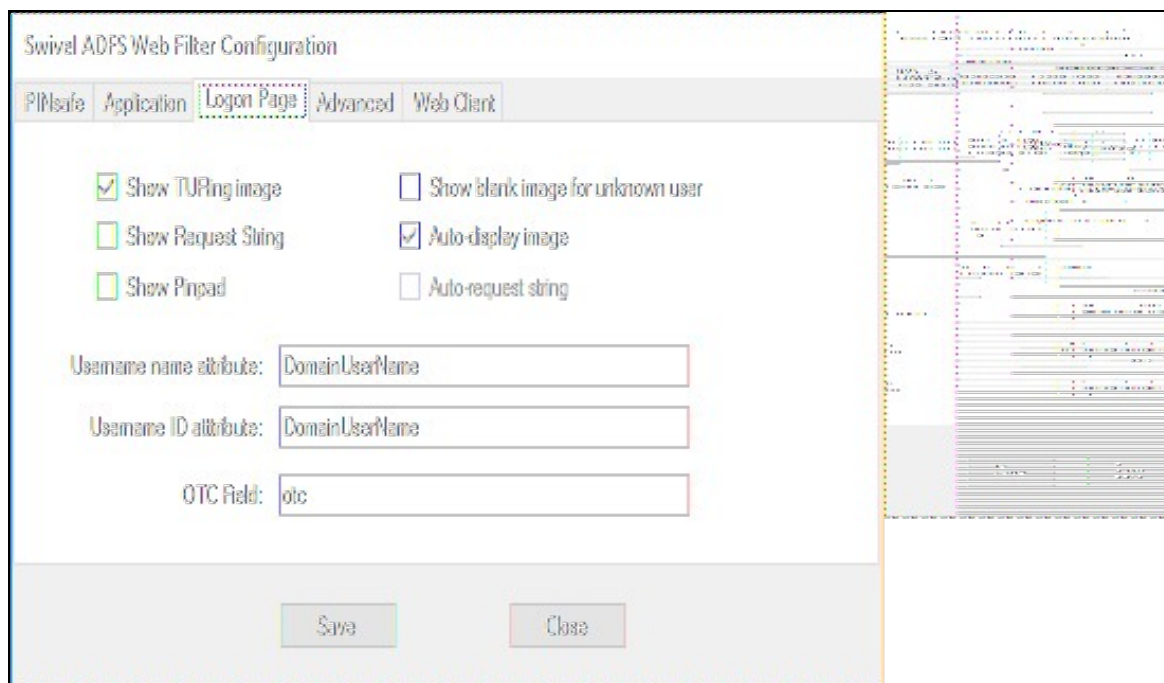
Show TURing image check to display the TURing image

Show Request String check to display a button to request the dual channel security string to send to the user

Show Pinpad check to display a Pinpad keypad

Show blank image for unknown user if checked, no image is shown if the user is not know. If unchecked, a random image is shown.

Auto-display image if checked, the TURing or Pinpad is automatically displayed after entering the username.

Auto-request string if checked, a security string is automatically requested after entering the username.

Username name attribute the HTML "name" attribute for the username field. Do not change this unless instructed.

Username ID attribute the HTML "id" attribute for the username field. Do not change this unless instructed.

OTC Field the HTML "name" attribute for the OTC field. Do not change this unless instructed.
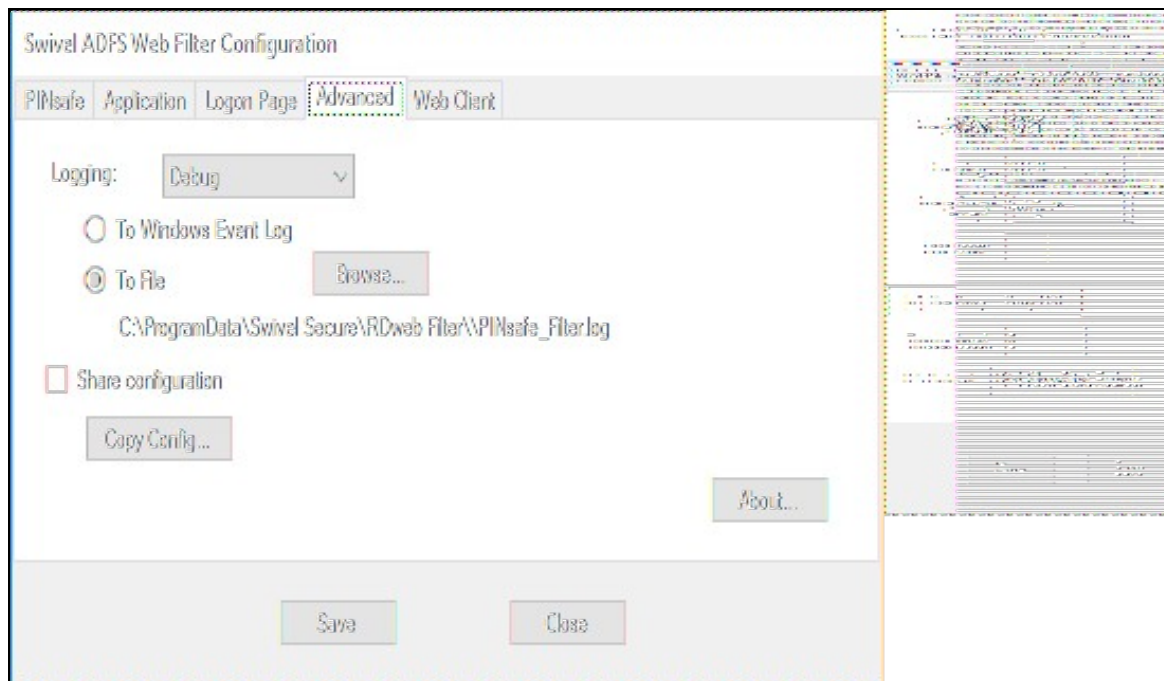
Logging enables the recording of certain information by the filter. The different levels indicate more detailed logs. Logs can either be written to the Windows Event Log, or to a chosen file. When writing to a file, make sure that the account used to run the RDWeb application has write access to the appropriate folder.

Share configuration allows you to export the configuration and import it to another RDWeb server.

About displays the version number and copyright information.
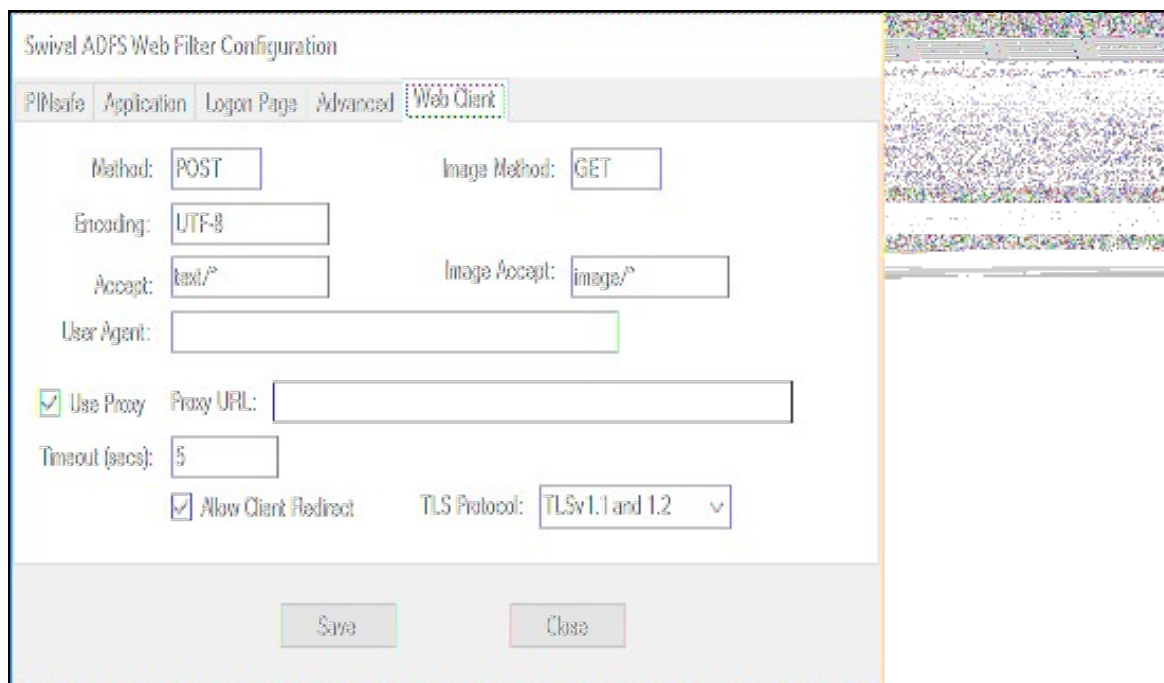
Most of the settings on this page should be left unchanged, unless instructed. The one exception is

TLS Protocol Version 2 Swivel appliances do not support TLS versions 1.1 or 1.2. Version 3 and 4 appliances do not support anything lower than TLS 1.1 unless specifically enabled, so unless you have a version 2 appliance, please ensure that you select "TLSv1.1 and 1.2".

If you need to change any of these settings later, a link to the configuration program is provided on the shortcut menu.

Changes to Existing Files

The installer will make modifications to three files within the RDS web hierarchy:

- Login.aspx from within the language folder. The appropriate buttons to display a TURing image are added if required. If you have significantly altered the login page, the installer may not be able to make its changes. Contact Swivel Secure for advice in this case.
- Renderscripts.js. A new function is added to display a TURing image, or to request a message on demand.
- Web.config. The Swivel filter is added as a new module, and the Swivel server details are stored under appSettings.

Additionally, the filter copies two DLLs to the bin folder of RDWeb/Pages: the filter itself and the Swivel client. It also copies a TURing image proxy, pinsafe_image.aspx, to the language folder.

Troubleshooting

We have seen in one instance, a problem whereby the TURing image could not be displayed even though the settings were correct, and the TURing image could be directly requested from the RDS Web server to the Swivel virtual or hardware appliance. The conclusion in this case was that the problem was due to permissions issues with the RDSWeb application pool account. Although we were unable to identify the exact problem, we resolved it by changing a setting on the application pool (under Advanced Settings) to enable Load User Profile.

Uninstalling

An uninstall program is provided, so you can either uninstall from the Windows Control Panel, or from the uninstall link on the shortcut menu.

The uninstall process requires that the files login.aspx.sav and renderscripts.js.sav, which are created when the appropriate files are modified, remain in their initial locations. These are the original files, without the PINsafe modifications. If these files do not exist, the filter cannot be properly uninstalled.