Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

1 Category:ADFS

2 Azure AD as a Data Source

3 Overview

This document describes how to use Azure AD as a Data Source.

4 Prerequisites

- Enable Azure AD Domain Services.
- Enable Secure LDAP.
- It is also necessary a connection between Swivel and Azure AD SLDAP

4.1 Implementation

You can follow the instructions on this article here.

Please have a read in this instructions on this article [1] and also [2]

5 Microsoft ADFS 2 Integration

6 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.

7 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

8 Prerequisites

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

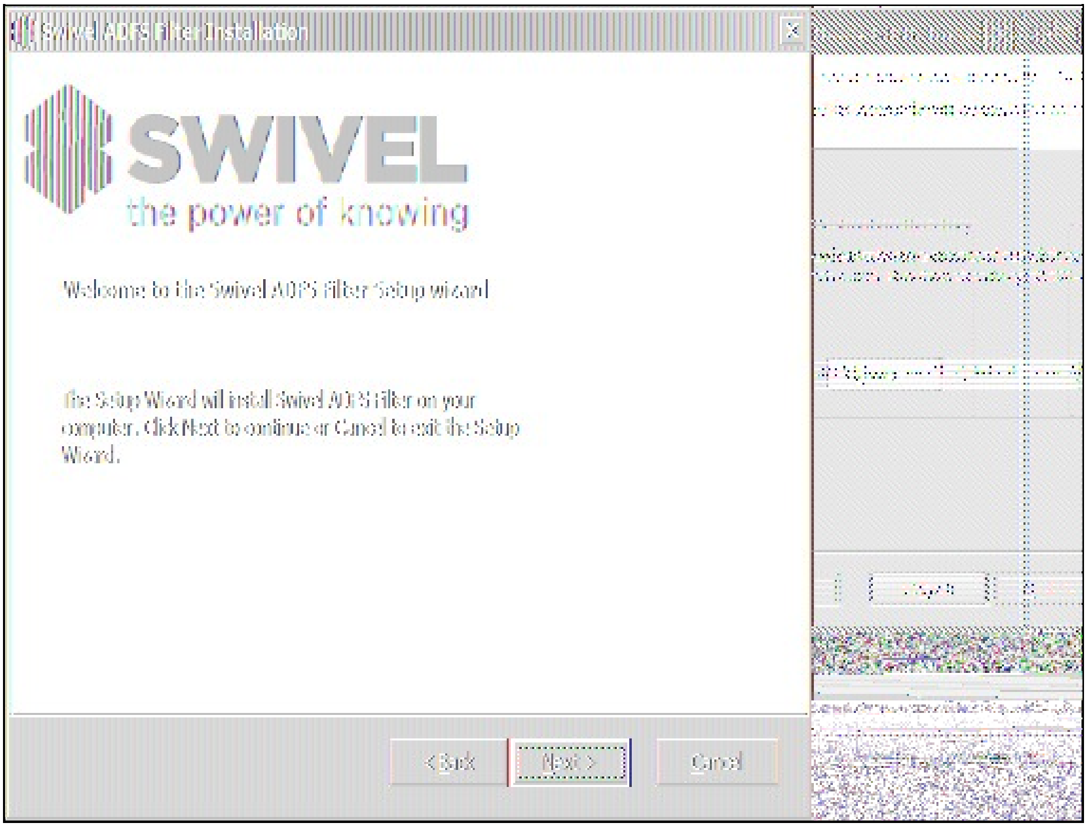
9 How to Guide

9.1 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.

9.2 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:

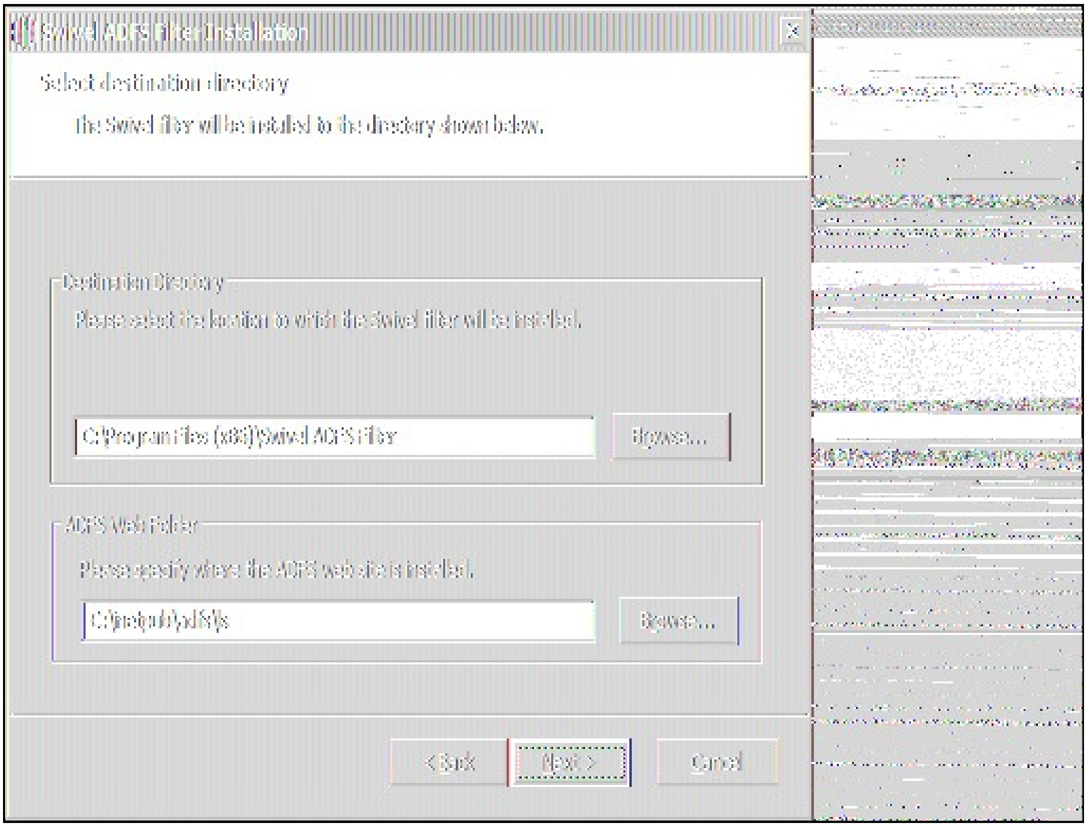


Swivel ADFS Filter Installation

Welcome to the Swivel ADFS Filter Setup wizard

The Setup Wizard will install Swivel ADFS Filter on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

Click Next to select the installation location:



Select destination directory

The Swivel filter will be installed to the directory shown below.

Destination Directory

Please select the location to which the Swivel filter will be installed.

C:\Program Files (x86)\Swivel ADFS Filter

ADFS Web Folder

Please specify where the ADFS web site is installed.

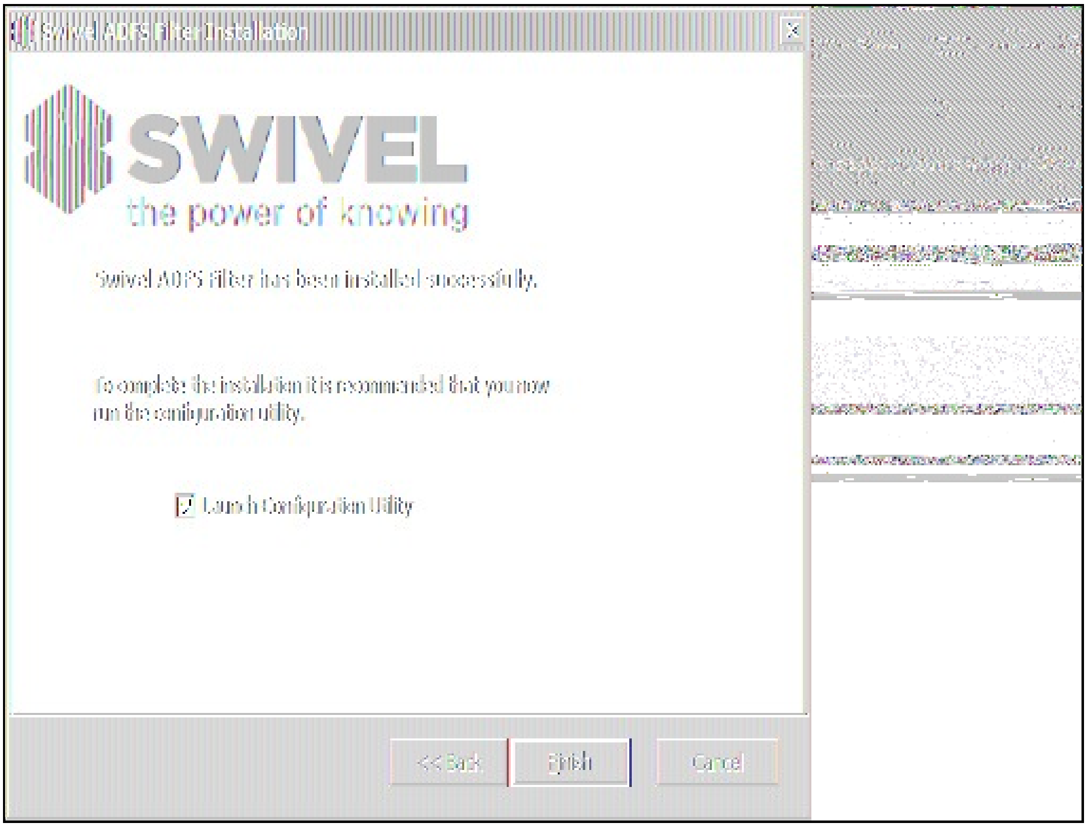
C:\inetpub\adfs\ls

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:



Swivel ADFS Filter has been installed successfully.

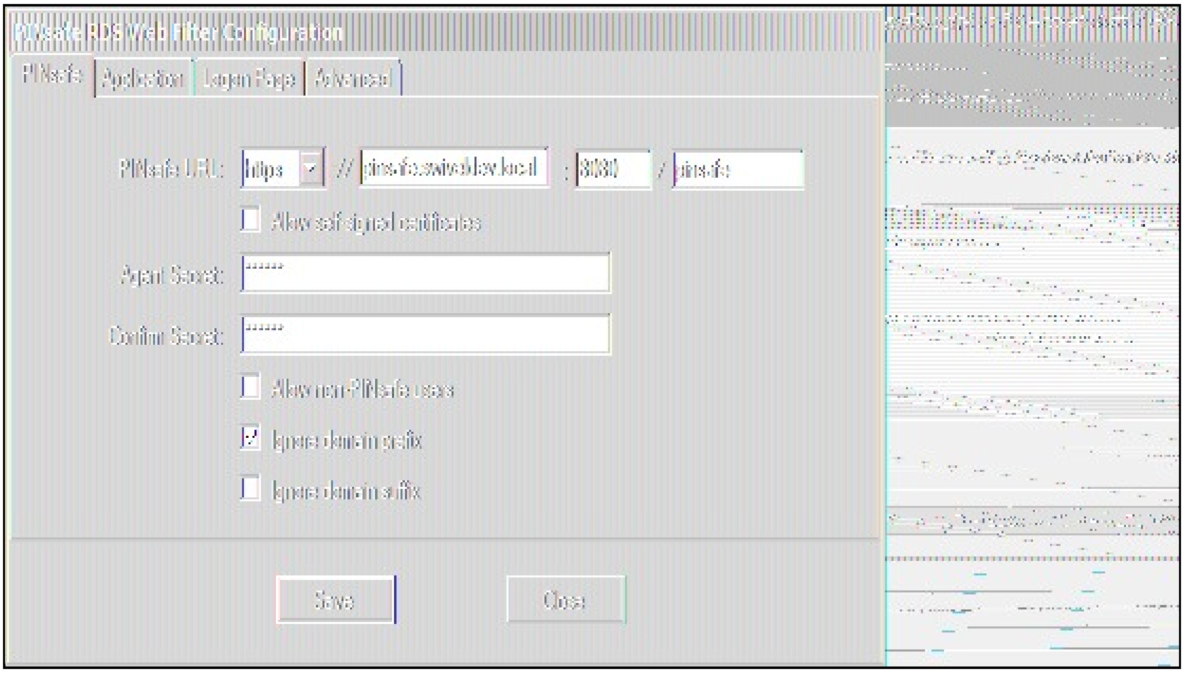
To complete the installation it is recommended that you now run the configuration utility.

☑ Launch Configuration Utility

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.

9.3 Configuring the Swivel ADFS Filter

The configuration program consists of four tabs:



PINsafe URL: https :// pinsafe.swiveldev.local : 8080 / pinsafe

☐ Allow self-signed certificates

Agent Secret: ******

Confirm Secret: ******

☐ Allow non-PINsafe users

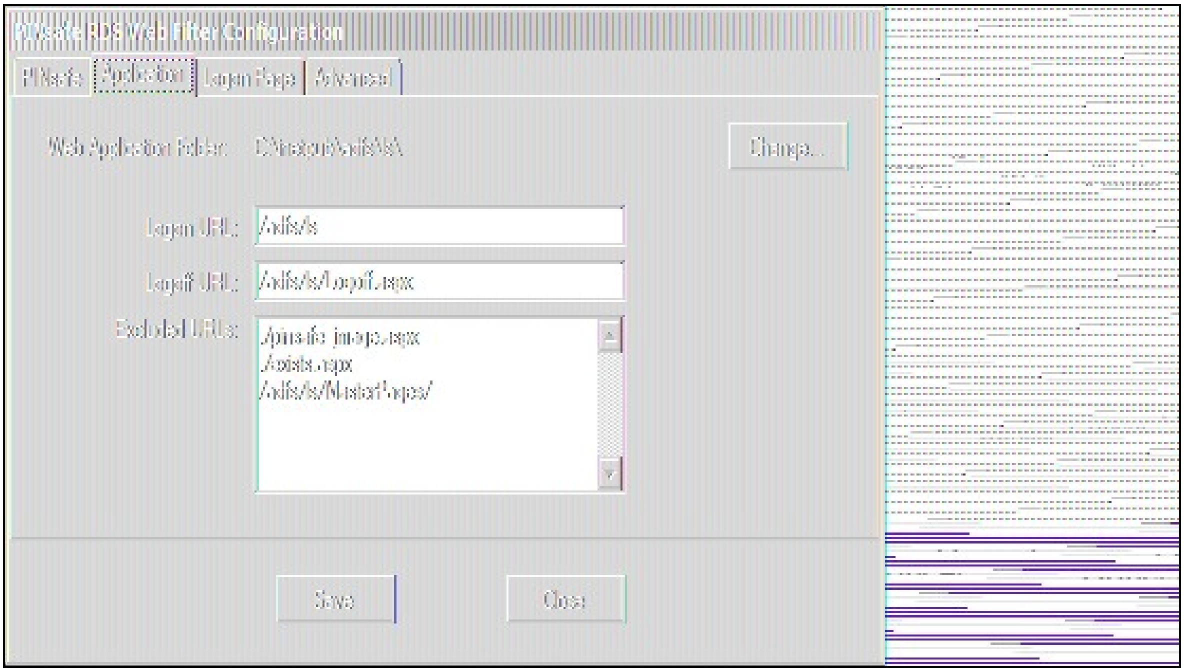
☑ Ignore domain prefix

☐ Ignore domain suffix

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.



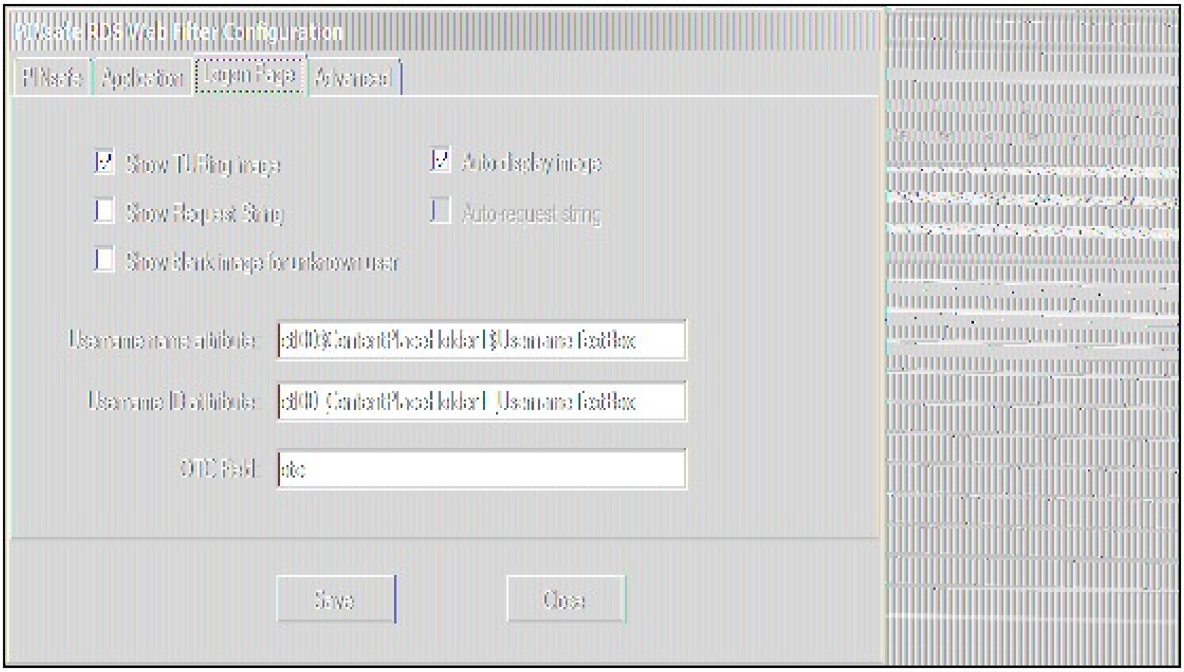
Web Application Folder: C:\inetpub\adfs\ls\

Logon URL: /adfs/ls

Logoff URL: /adfs/ls/Logoff.aspx

Excluded URLs:
/pinsafe_image.aspx
/exists.aspx
/adfs/ls/MasterPages/

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.



PINsafe RDS Web Filter Configuration

☑ Show TURing image

☑ Auto-display image

□ Show Request String

□ Auto-request string

□ Show blank image for unknown user

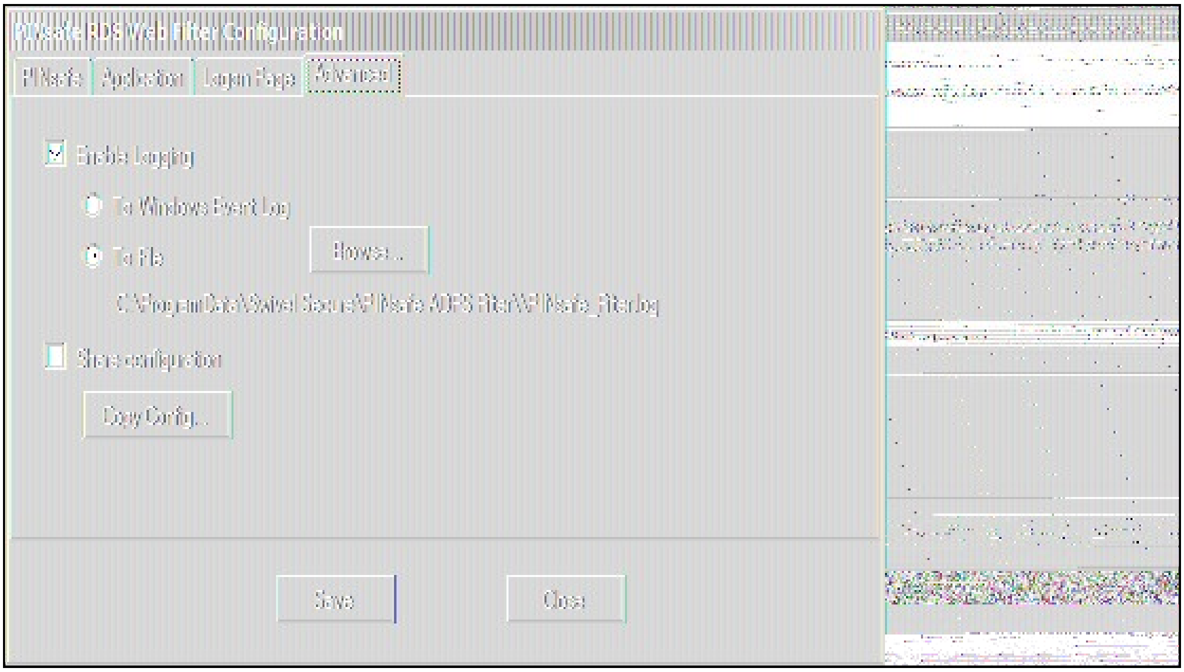
Username name attribute: ctl00$ContentPlaceHolder1$UsernameTextBox

Username ID attribute: ctl00_ContentPlaceHolder1_UsernameTextBox

OTC Field: otc

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.



PINsafe RDS Web Filter Configuration

☑ Enable Logging

○ To Windows Event Log

● To File

C:\ProgramData\Swivel Secure\PINsafe ADFS Filter\PINsafe_Filter.log

□ Share configuration

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.

9.3.1 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.

10 Additional Configuration Options

10.1 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.

10.2 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.

11 Testing

12 Known Issues

It has been observed that some browsers, noteably Chrome, will cause authentication to fail if the browser default language is not available in the filter. The filter is only provided with English. However, it is possible to add new languages in the configuration page, so please make sure you add any languages your users are likely to require.

13 Troubleshooting

14 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.

15 Microsoft ADFS 4 and 3 Authentication

16 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

17 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.

17.1 Current Version Installer

Please note that the latest version is now 1.4.5, available from here.

17.2 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.

17.3 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

17.4 Networking Requirements

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

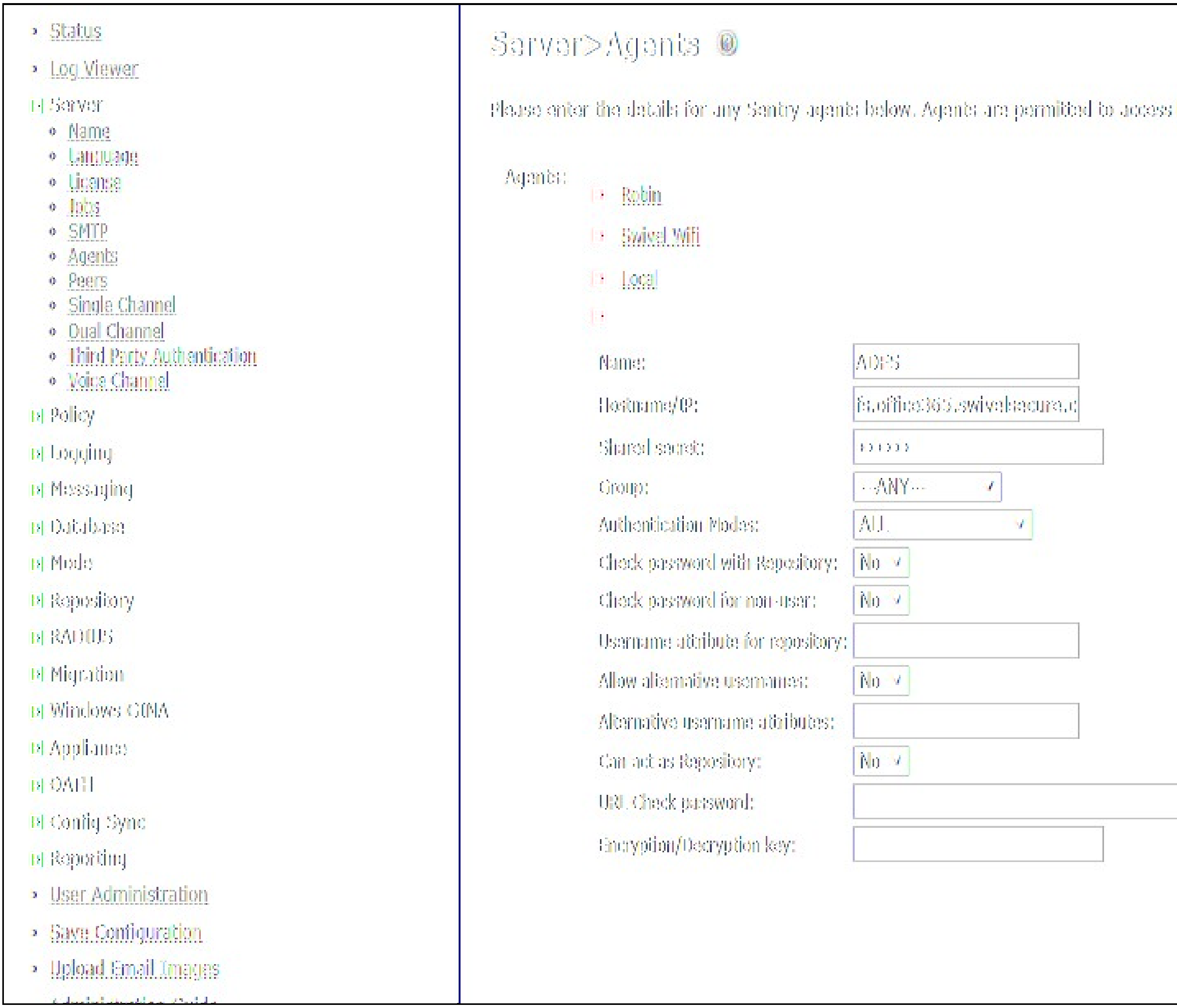
- Connection between the ADFS server and the Sentry appliance, or load balancer if used, on port 8080 if connecting directly to the Core Sentry application, or port 8443 if using the appliace proxy.
- If you are using a proxy for the TURing / PINpad images, you will need the same connections from the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

17.5 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.



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:	••••••
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

18 Installation

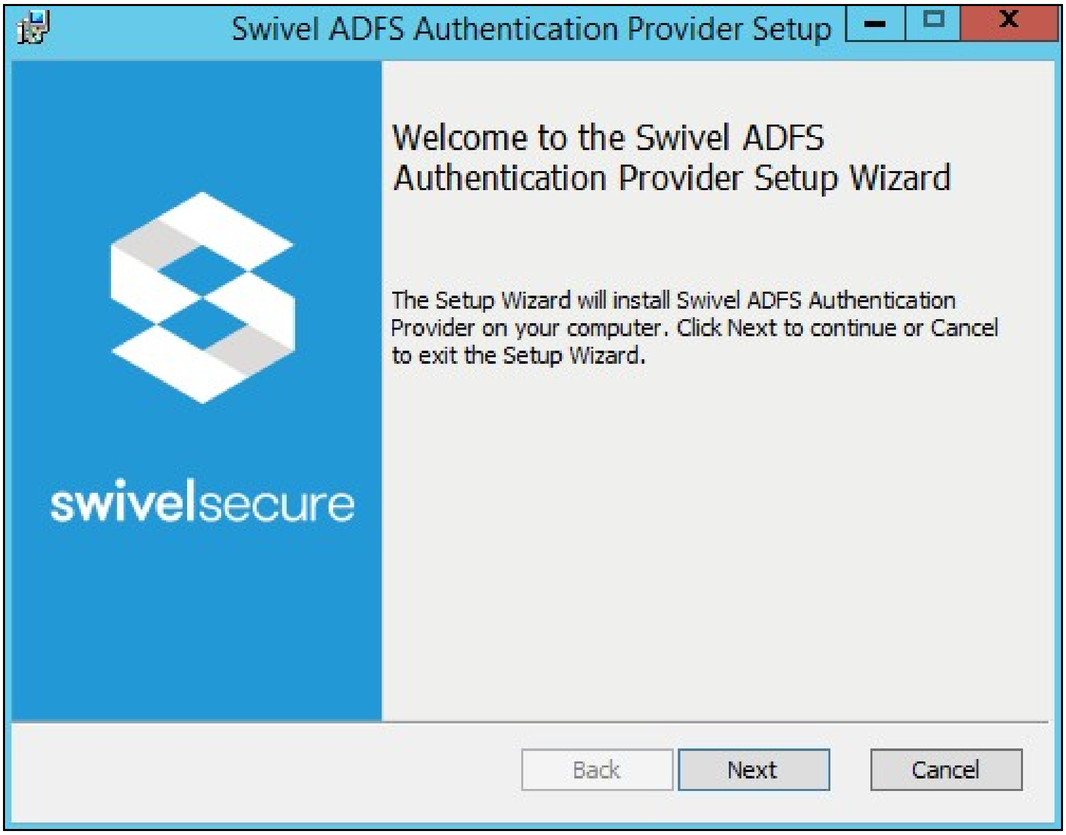
NOTE: If you are installing on the ADFS server(s) and one or more proxies (see below), you should install on the ADFS server(s) first.

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
```

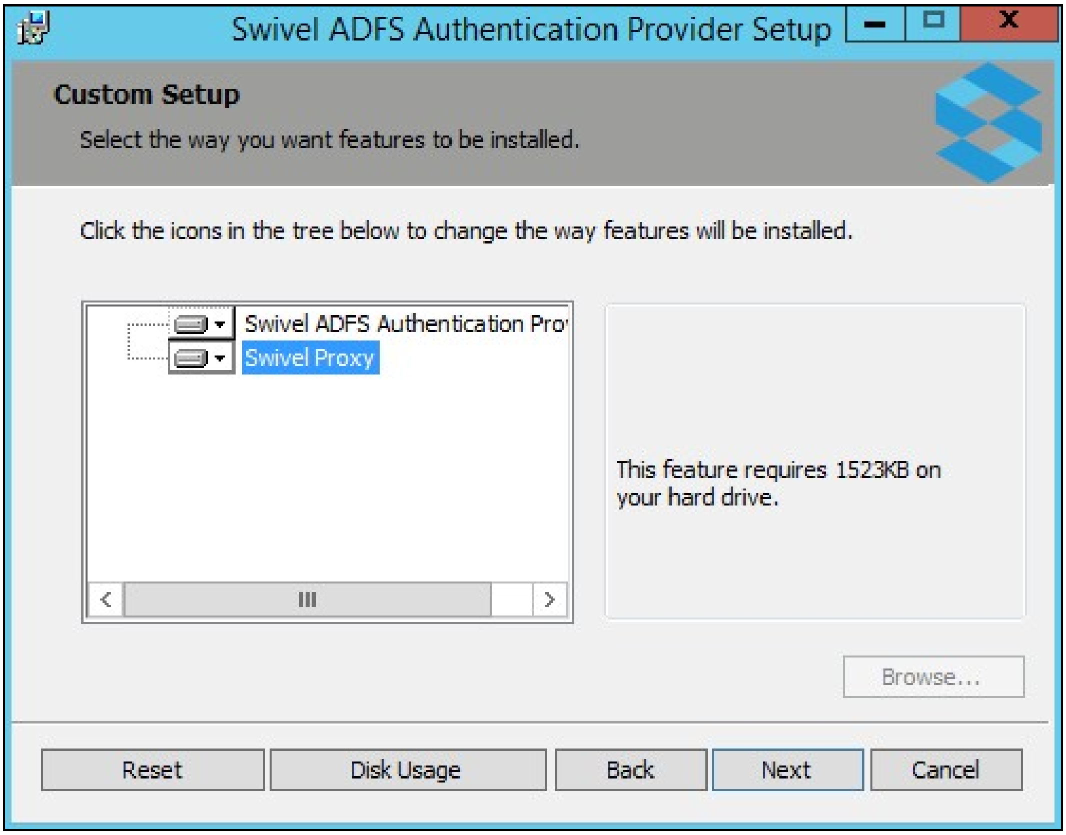


Welcome to the Swivel ADFS Authentication Provider Setup Wizard

The Setup Wizard will install Swivel ADFS Authentication Provider on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

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.



Swivel ADFS Authentication Provider Setup

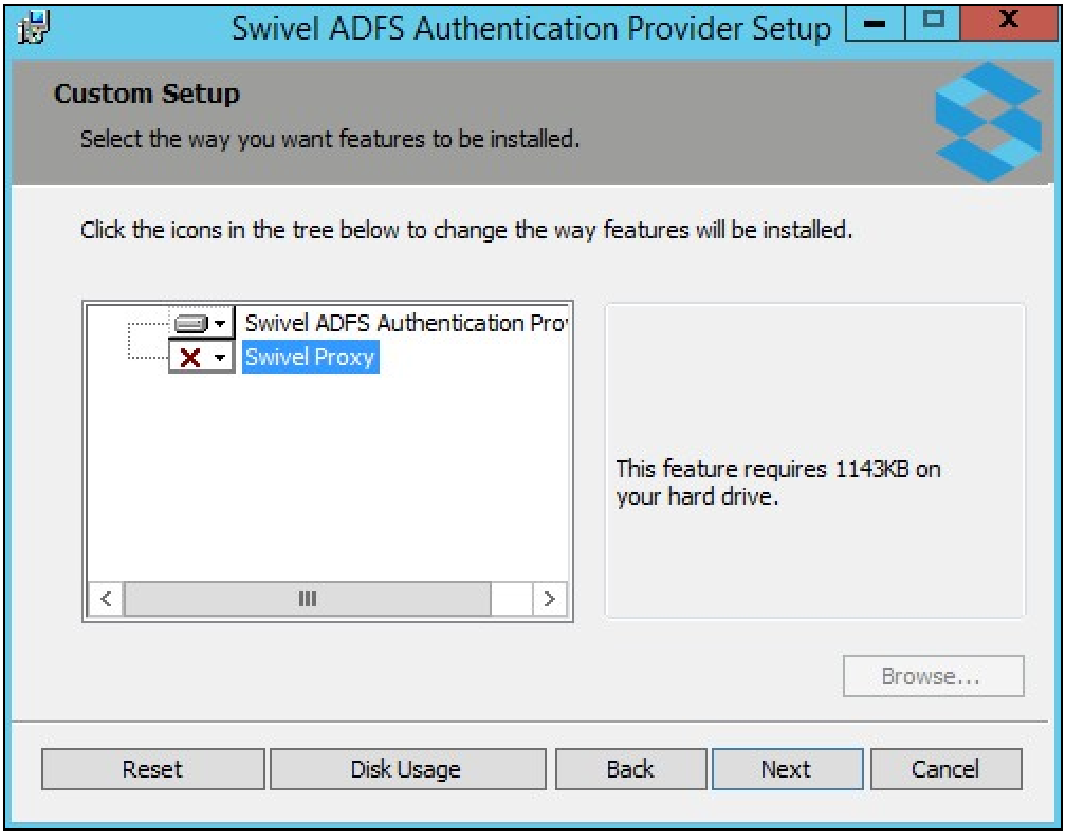
Custom Setup

Select the way you want features to be installed.

Click the icons in the tree below to change the way features will be installed.

This feature requires 1523KB on your hard drive.

- 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.



Swivel ADFS Authentication Provider Setup

Custom Setup

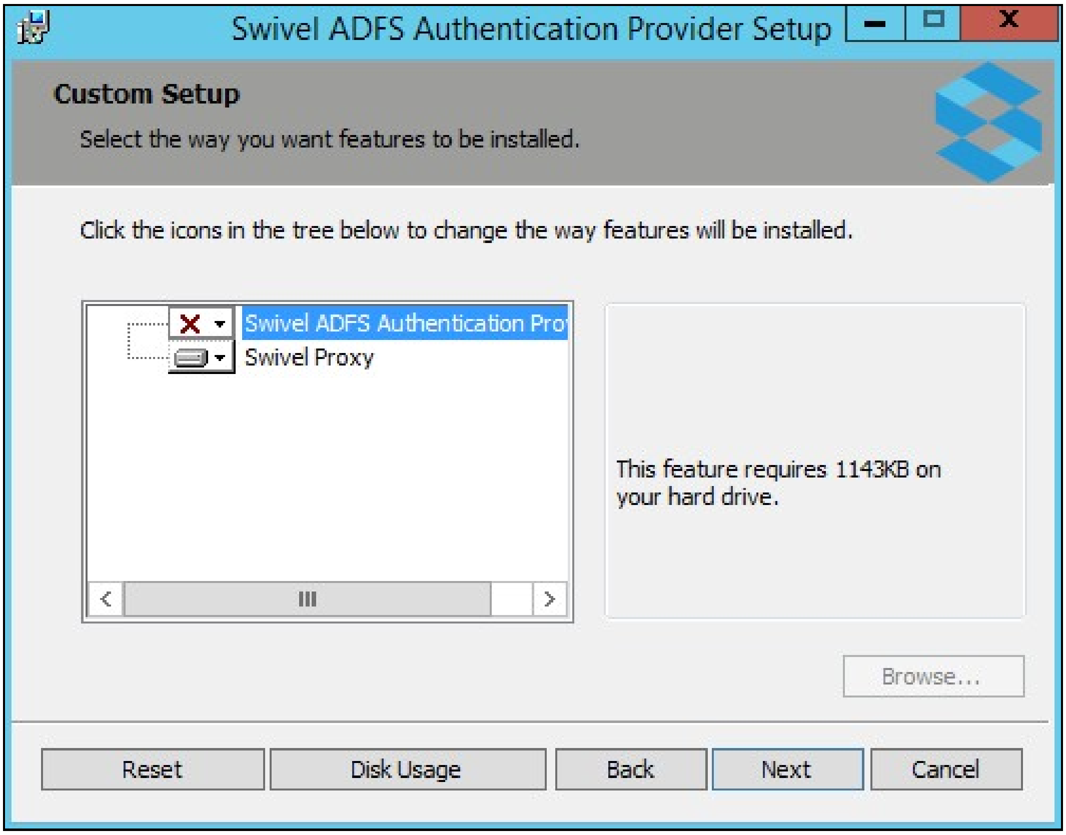
Select the way you want features to be installed.

Click the icons in the tree below to change the way features will be installed.

This feature requires 1143KB on your hard drive.

- 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.



Swivel ADFS Authentication Provider Setup

Custom Setup

Select the way you want features to be installed.

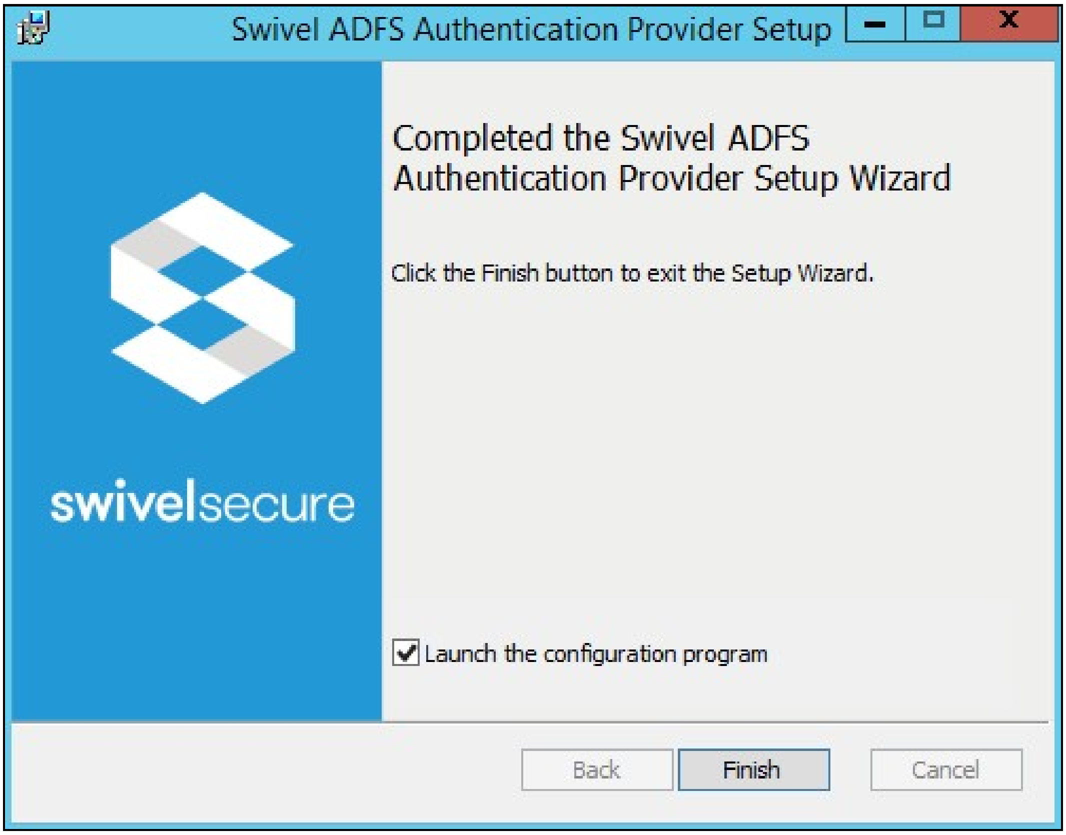
Click the icons in the tree below to change the way features will be installed.

This feature requires 1143KB on your hard drive.

- 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.



Swivel ADFS Authentication Provider Setup

Completed the Swivel ADFS Authentication Provider Setup Wizard

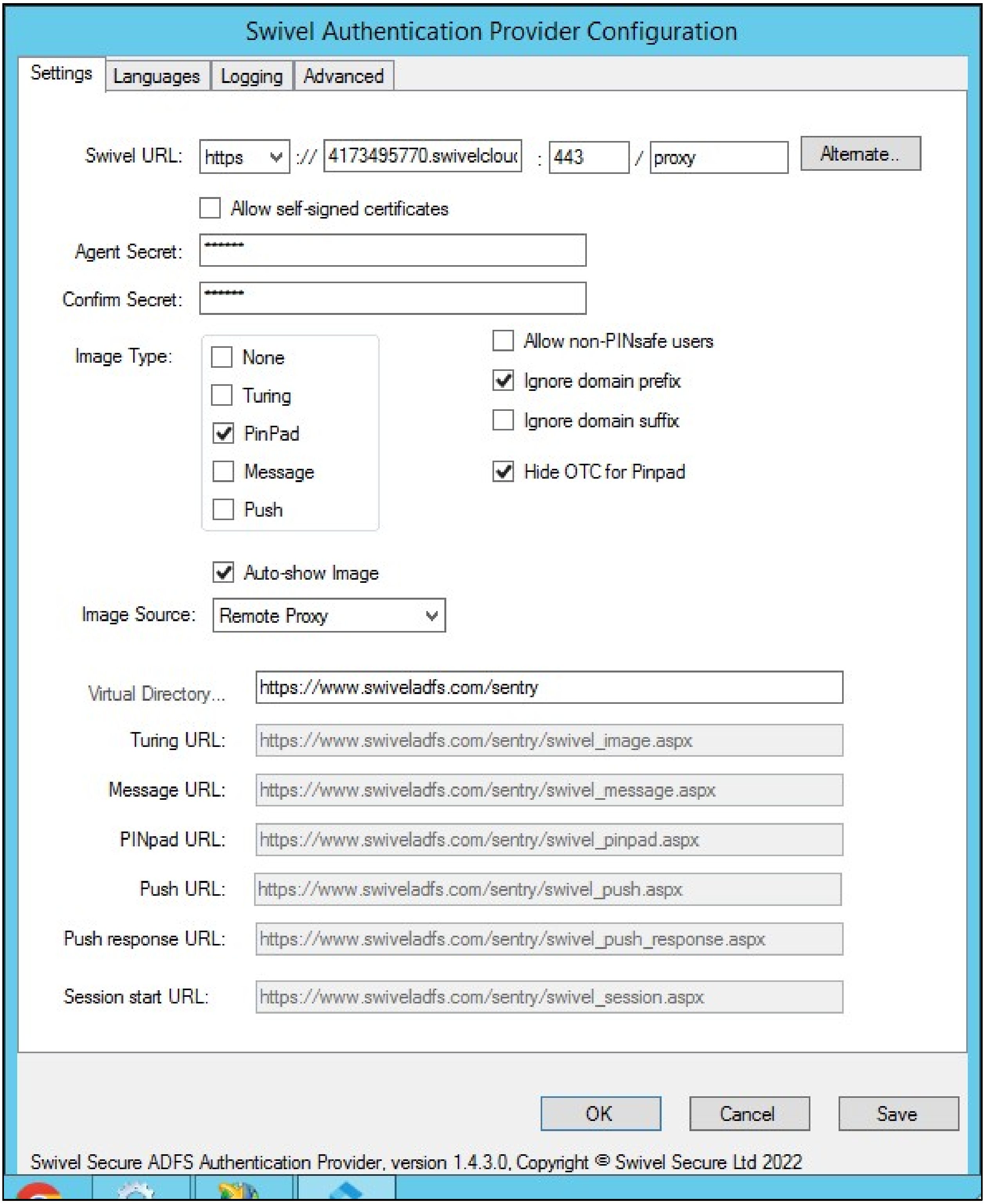
Click the Finish button to exit the Setup Wizard.

☑ Launch the configuration program

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

19 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.swivelclouc : 443 / proxy

□ 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

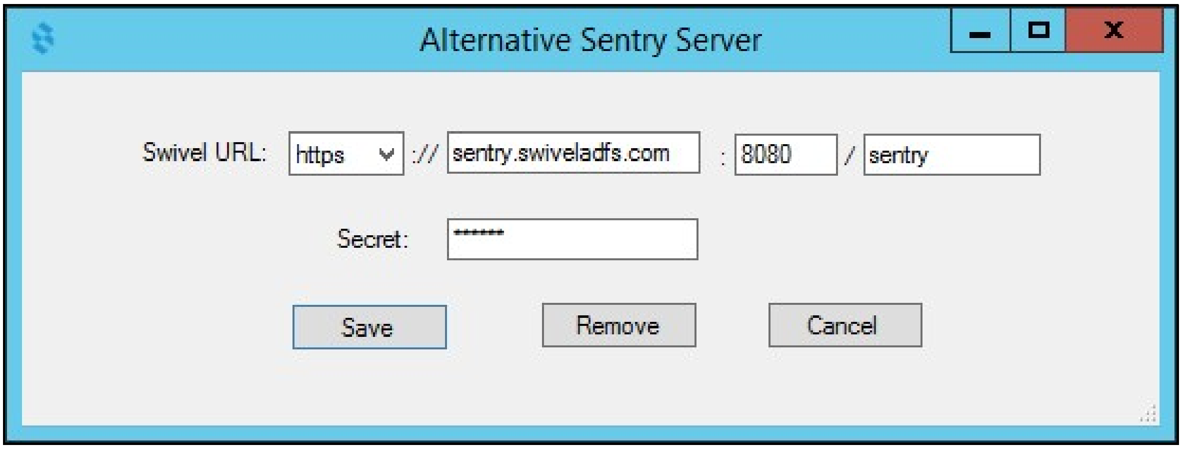
Push URL: https://www.swiveladfs.com/sentry/swivel_push.aspx

Push response URL: https://www.swiveladfs.com/sentry/swivel_push_response.aspx

Session start URL: https://www.swiveladfs.com/sentry/swivel_session.aspx

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:



Alternative Sentry Server

Swivel URL: https :// sentry.swiveladfs.com : 8080 / sentry

Secret: *******

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.

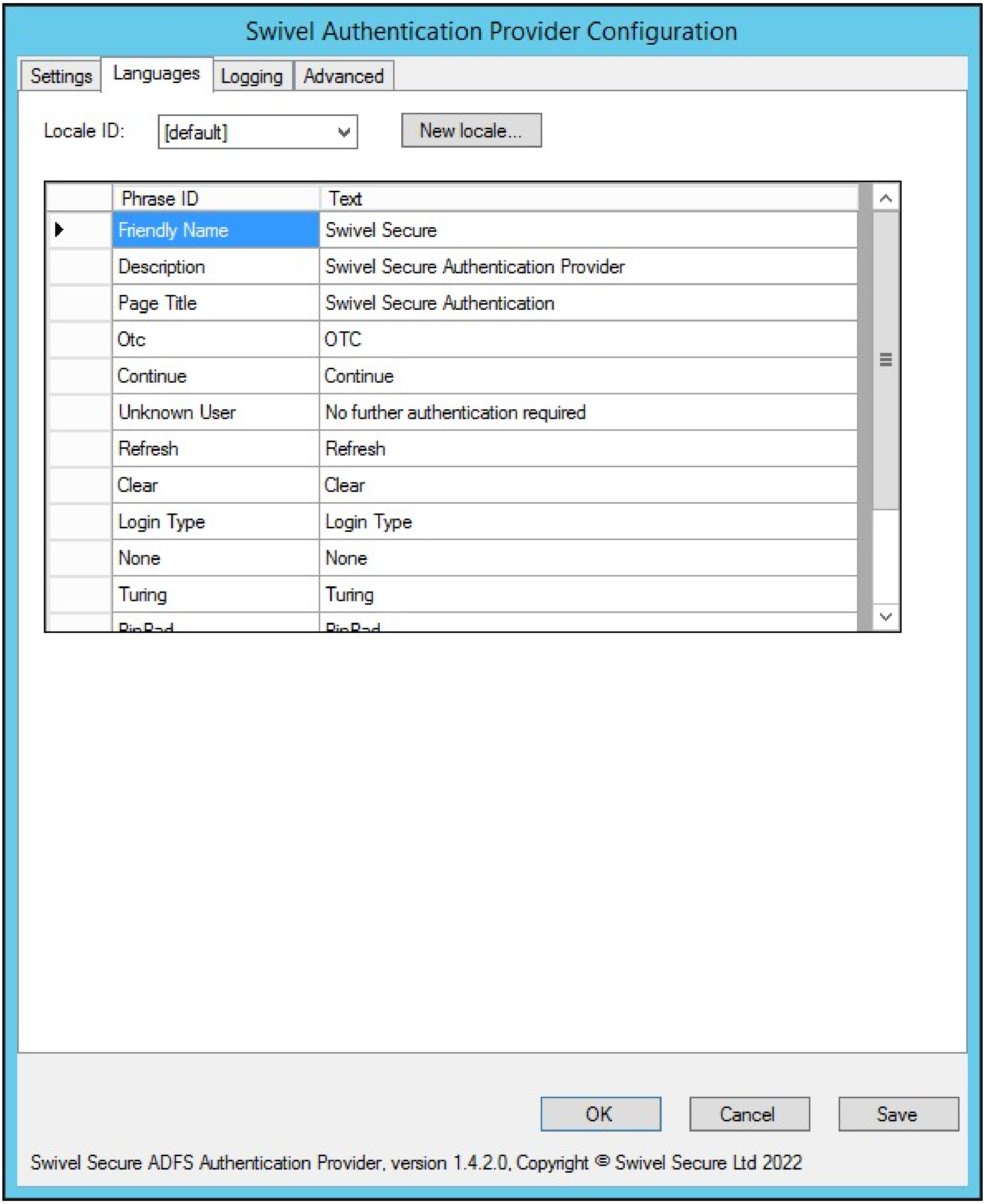
To directly access a Swivel appliance through a NAT etc, then the URL should be https://URL:8443/proxy/SCImage

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.



Locale ID: [default]

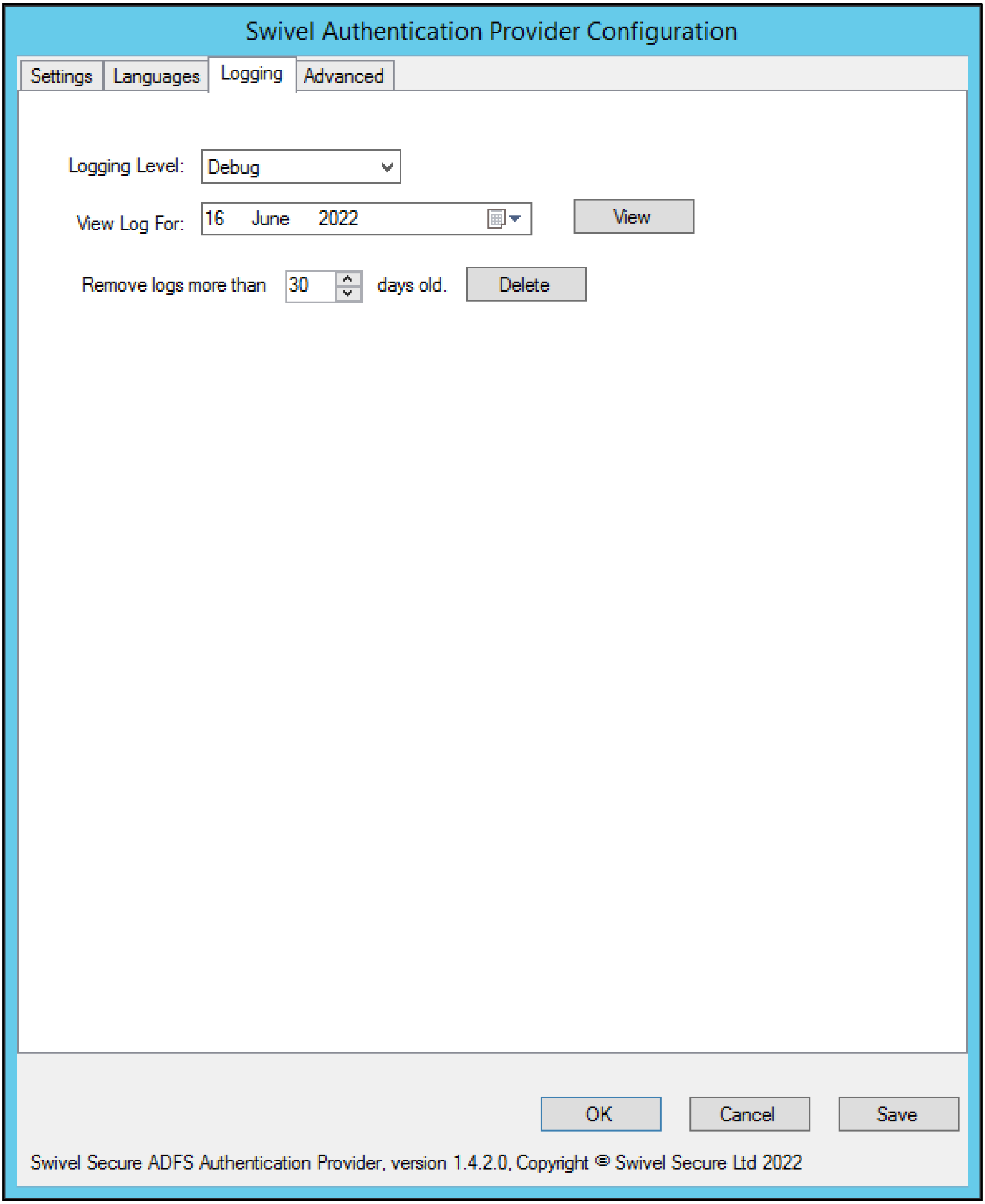
Phrase ID	Text
Friendly Name	Swivel Secure
Description	Swivel Secure Authentication Provider
Page Title	Swivel Secure Authentication
Otc	OTC
Continue	Continue
Unknown User	No further authentication required
Refresh	Refresh
Clear	Clear
Login Type	Login Type
None	None
Turing	Turing
PinPad	PinPad

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.



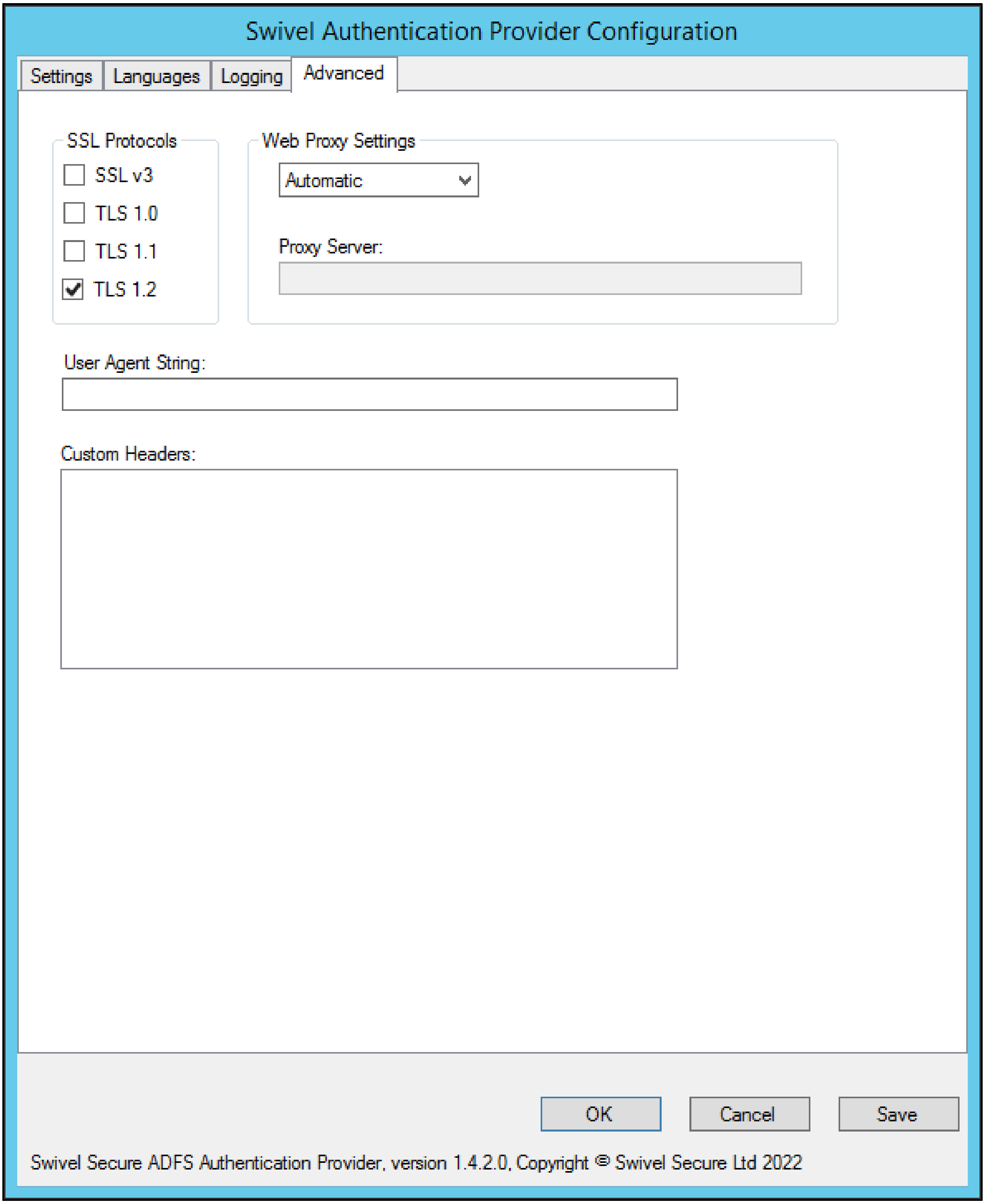
Logging Level: Debug

View Log For: 16 June 2022

Remove logs more than 30 days old.

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

SSL Protocols

□ SSL v3
□ TLS 1.0
□ TLS 1.1
☑ TLS 1.2

Web Proxy Settings

Automatic

Proxy Server:

User Agent String:

Custom Headers:

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.

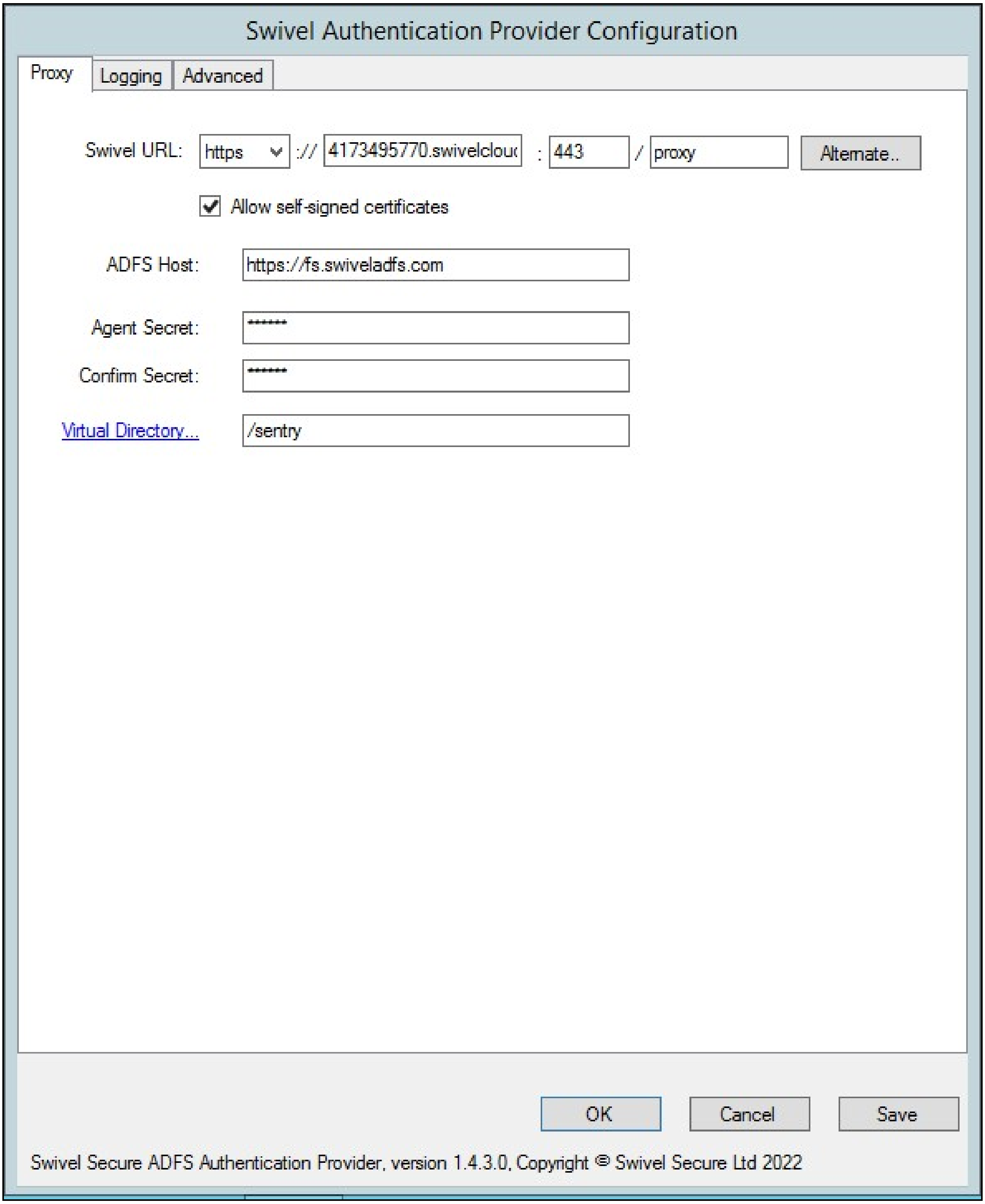
You can configure a web proxy to be used for the connection. By default, the Automatic option is selected, in which case the connection will use whichever proxy is configured for internet connections on the ADFS server. The other options are None, in which case no proxy is used, or Manual, in which case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

20 Using the Swivel Proxy

20.1 Proxy Configuration



Swivel Authentication Provider Configuration

Swivel URL: https :// 4173495770.swivelclou(: 443 / proxy

☑ Allow self-signed certificates

ADFS Host: https://fs.swiveladfs.com

Agent Secret: *******

Confirm Secret: *******

Virtual Directory... /sentry

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

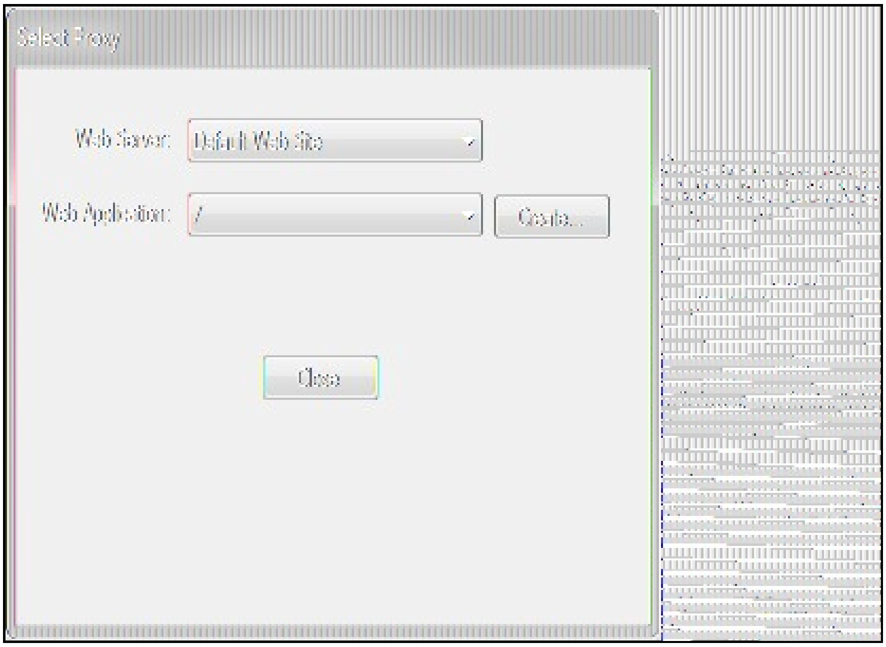
The proxy configuration program is largely a simplified version of the full configuration program, including just the Settings, Logging and Advanced tabs. However, there is one additional option to take note of:

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.

20.2 Enabling the Proxy Web Application

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

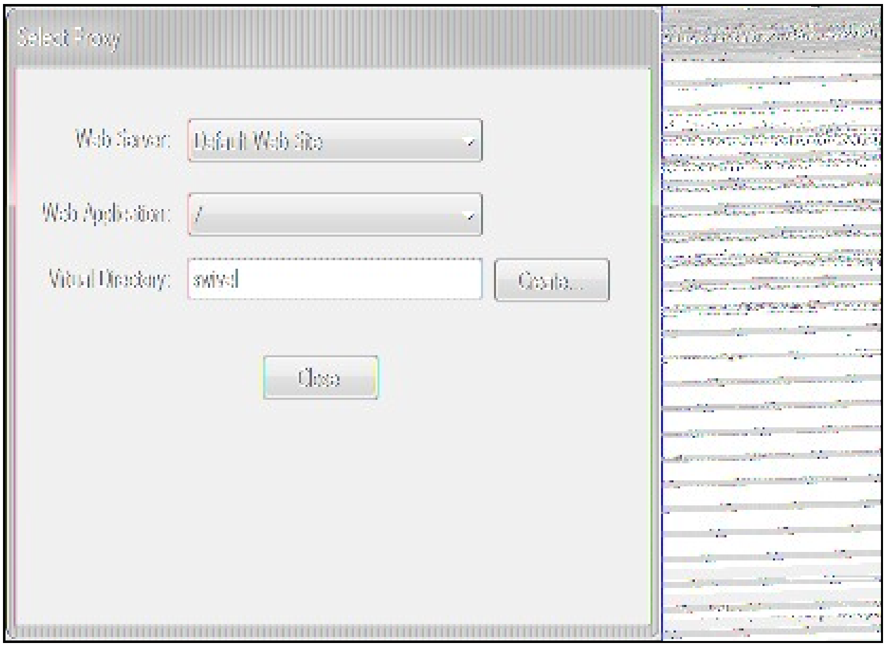


Select Proxy

Web Server: Default Web Site

Web Application: /

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



Select Proxy

Web Server: Default Web Site

Web Application: /

Virtual Directory: swivel

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.

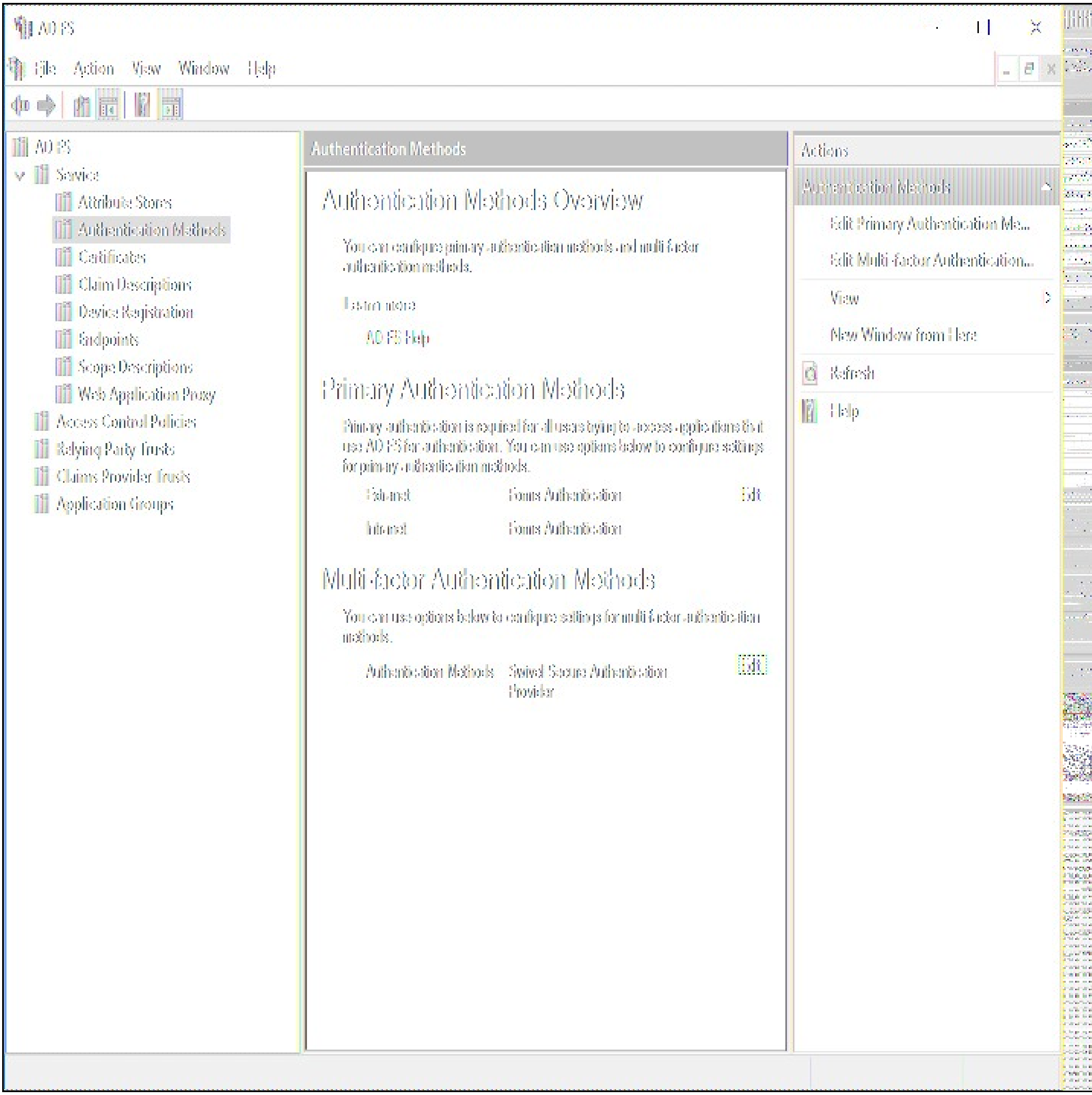
An additional menu option is provided to remove the virtual directory. This should normally be done before uninstalling the authentication provider.

21 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:



Authentication Methods Overview

You can configure primary authentication methods and multi factor authentication methods.

Learn more

AD FS Help

Primary Authentication Methods

Primary authentication is required for all users trying to access applications that use AD FS for authentication. You can use options below to configure settings for primary authentication methods.

Extranet	Forms Authentication	Edit
Intranet	Forms Authentication	

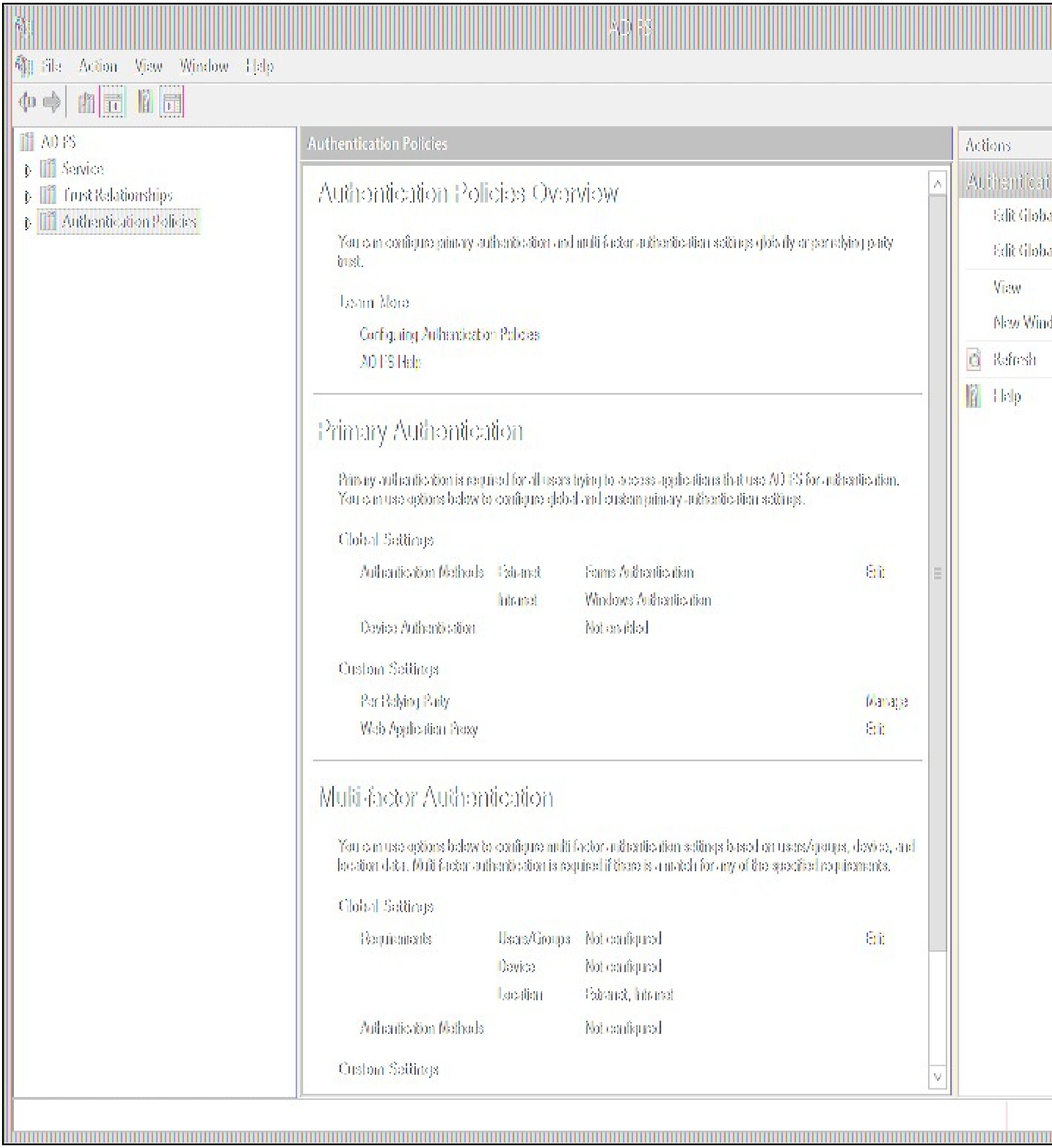
Multi-factor Authentication Methods

You can use options below to configure settings for multi-factor authentication methods.

Authentication Methods	Swivel Secure Authentication Provider	Edit

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

This is the dialog for ADFS 3:



Authentication Policies

Authentication Policies Overview

You can configure primary authentication and multi-factor authentication settings globally or per relying party trust.

Learn More

Configuring Authentication Policies

AD FS Help

Primary Authentication

Primary authentication is required for all users trying to access applications that use AD FS for authentication. You can use options below to configure global and custom primary authentication settings.

Global Settings

Authentication Methods	Extranet	Forms Authentication	Edit
	Intranet	Windows Authentication	
Device Authentication		Not enabled	

Custom Settings

Per Relying Party	Manage
Web Application Proxy	Edit

Multi-factor Authentication

You can use options below to configure multi-factor authentication settings based on users/groups, device, and location data. Multi-factor authentication is required if there is a match for any of the specified requirements.

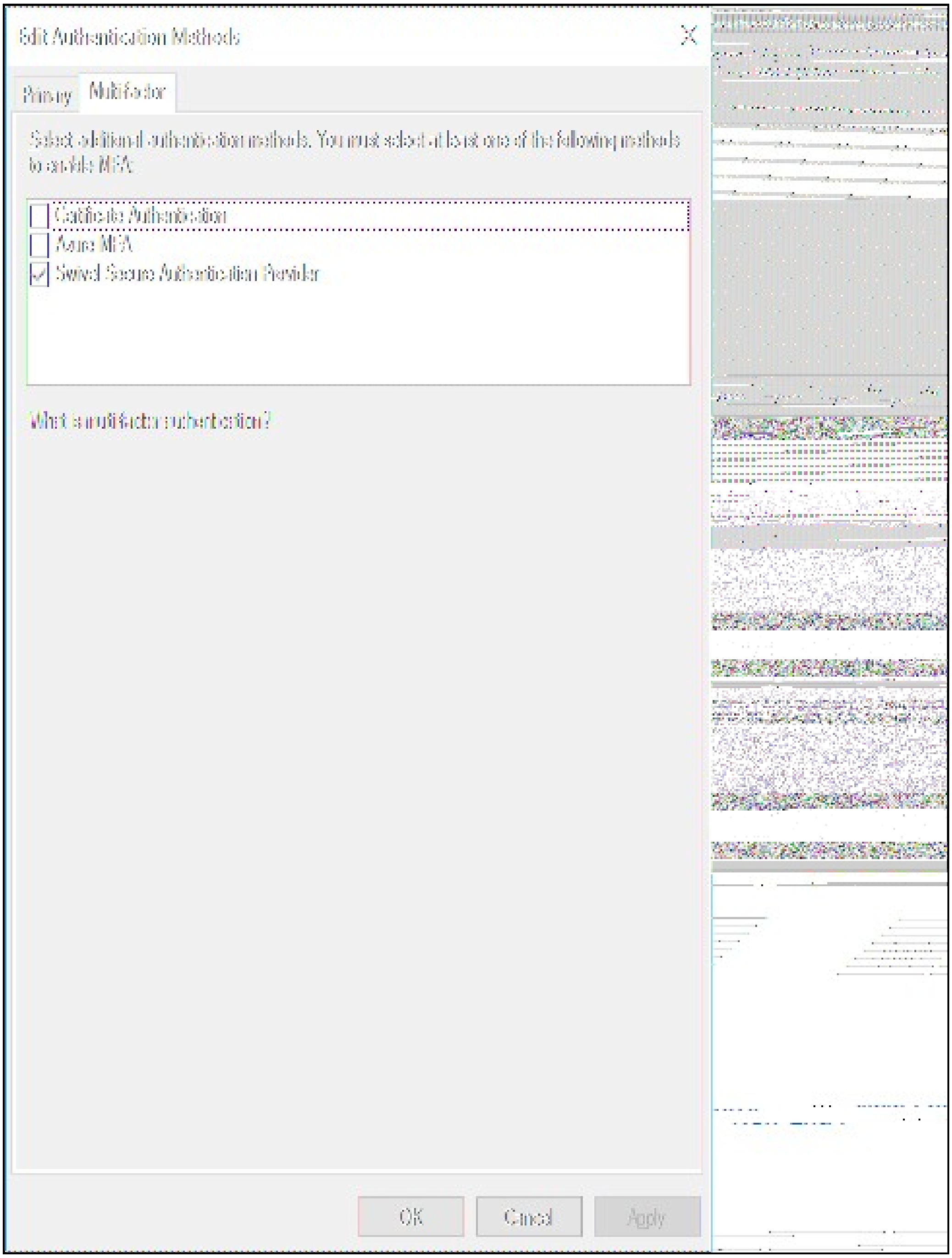
Global Settings

Requirements	Users/Groups	Not configured	Edit
	Device	Not configured	
	Location	Extranet, Intranet	
Authentication Methods		Not configured	

Custom Settings

`In ADFS 3.0, choose Authentication Policies.`

Under *Multi-factor Authentication*, click Edit.

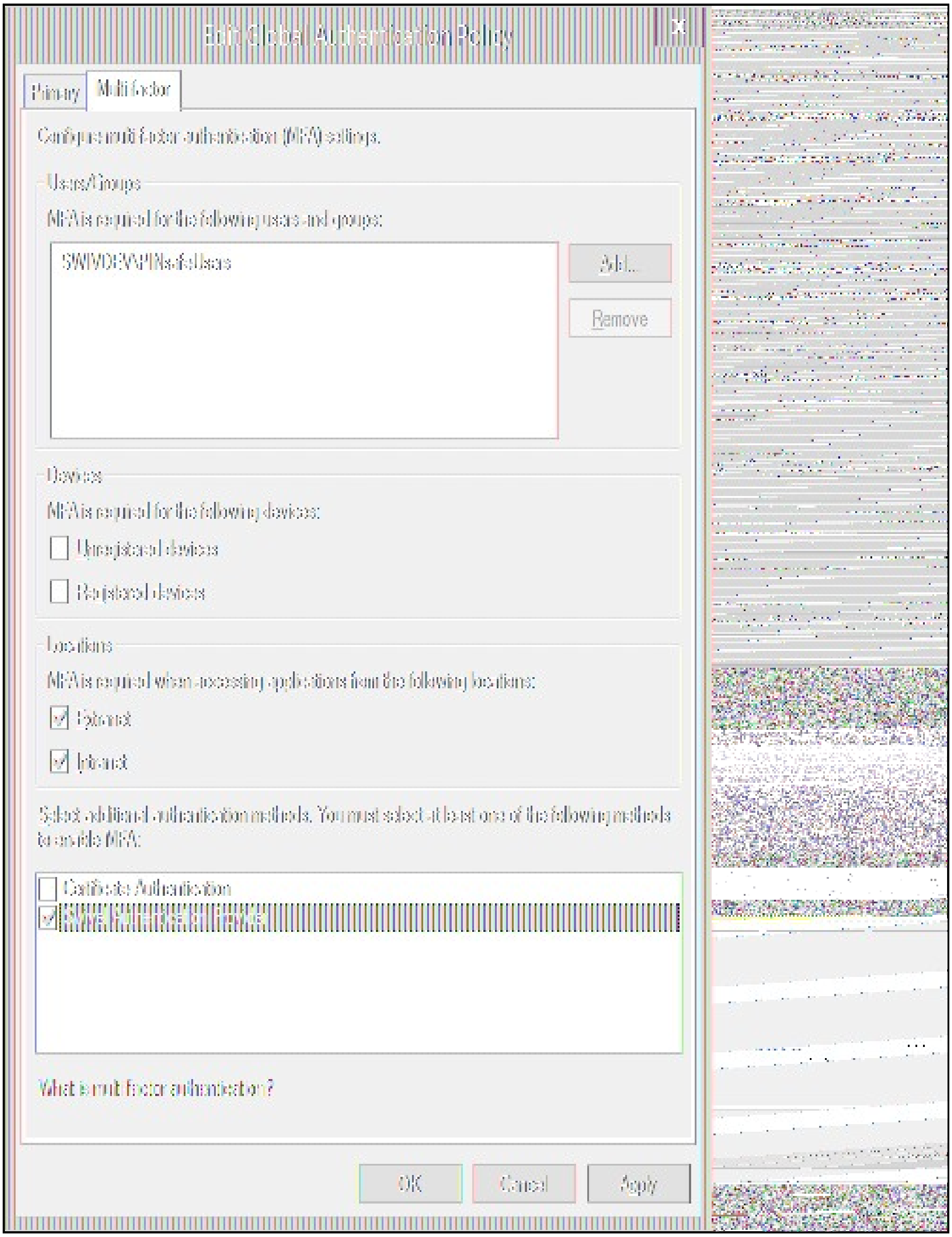


Select additional authentication methods. You must select at least one of the following methods to enable MFA:

- □ Certificate Authentication
- □ Azure MFA
- ☑ Swivel Secure Authentication Provider

What is multi-factor authentication?

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:

SWIVDEV\PINsafeUsers

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

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.

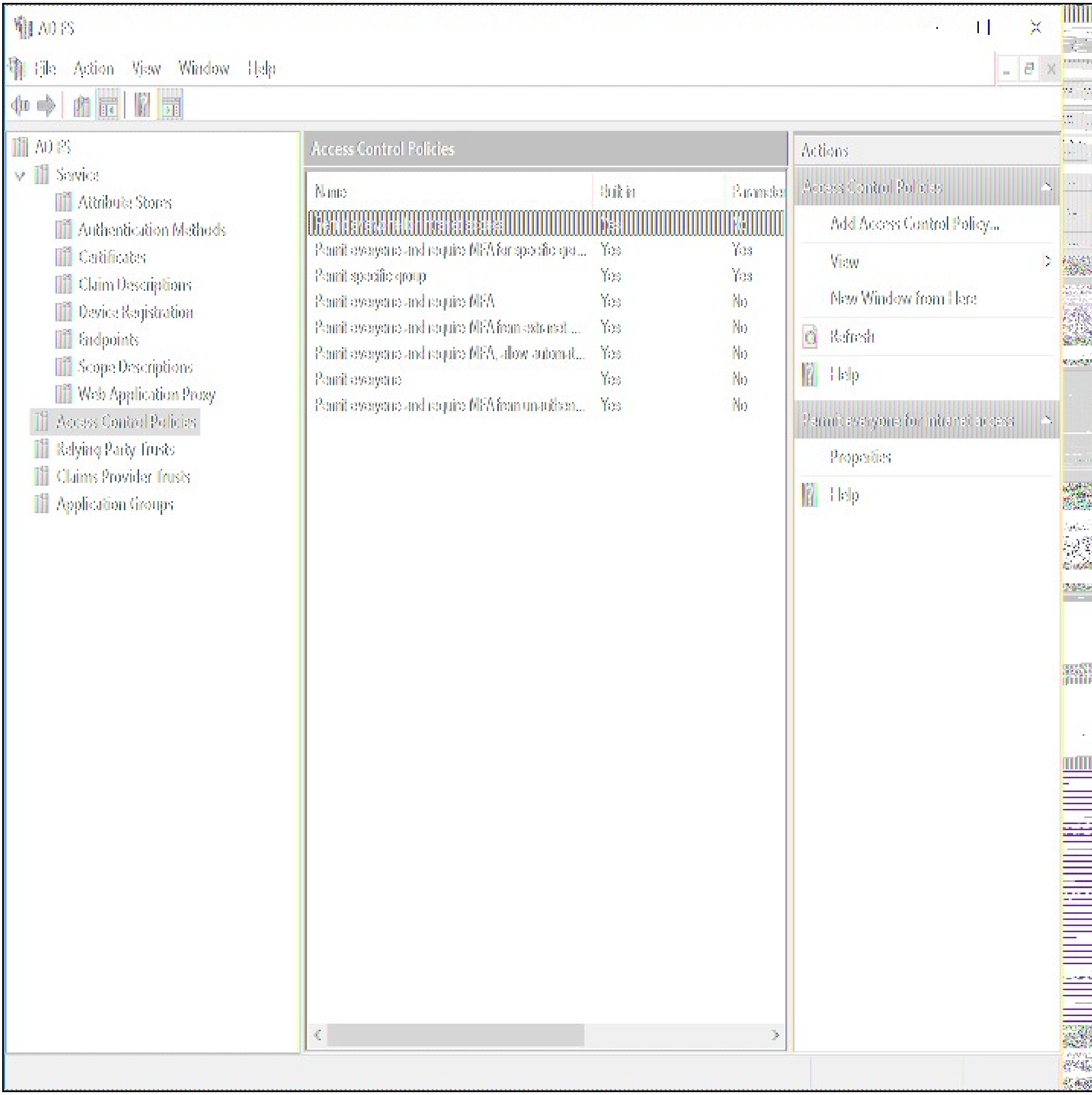
22 Advanced Features

22.1 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.

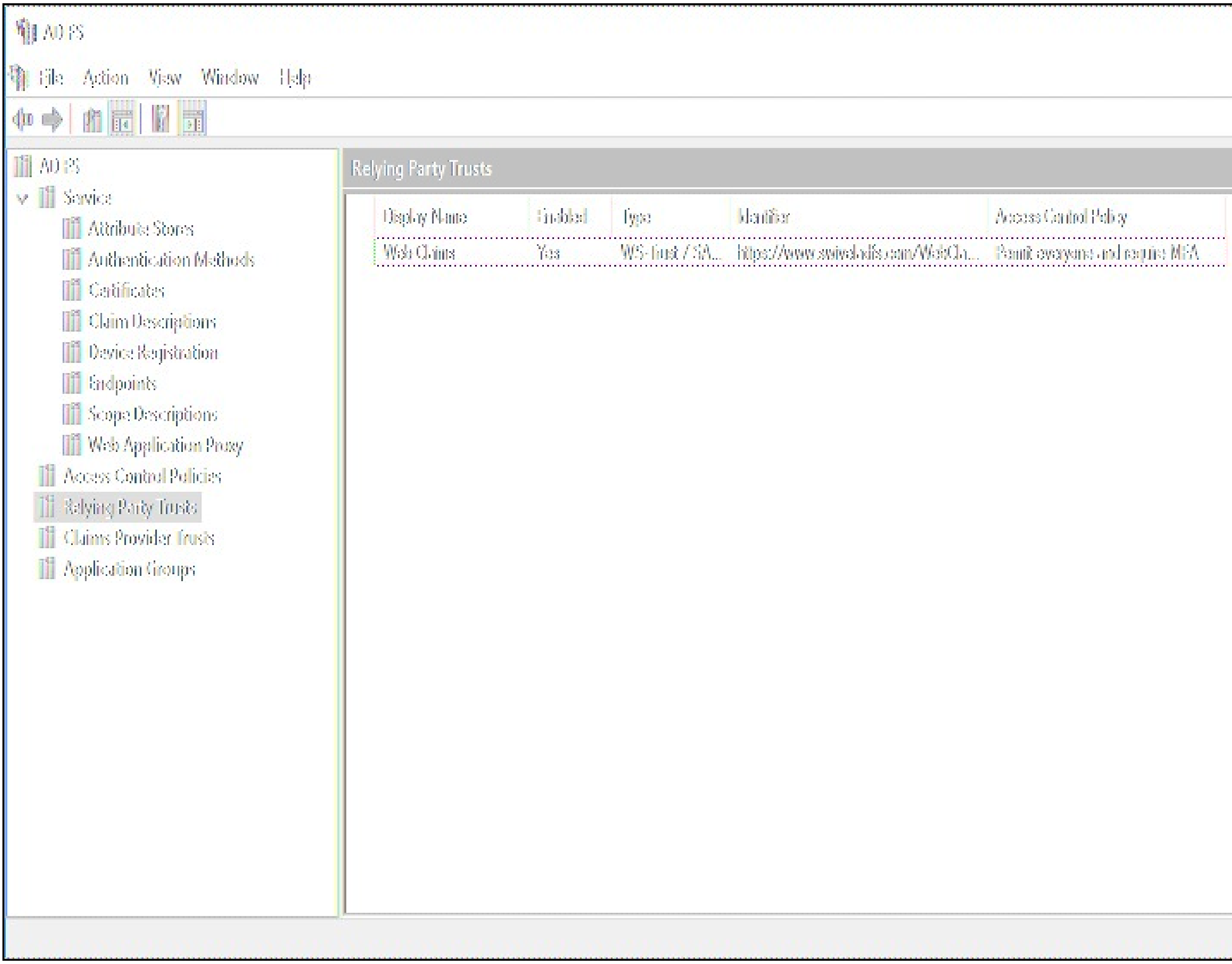
It may be that you want to enable Swivel Authentication in ADFS for some applications but not others. It is possible to manage this, with certain limitations, as described below:

22.1.1 ADFS 4.0



Name	Built in	Paramete
Permit everyone for intranet access	Yes	No
Permit everyone and require MFA for specific gro...	Yes	Yes
Permit specific group	Yes	Yes
Permit everyone and require MFA	Yes	No
Permit everyone and require MFA from extranet ...	Yes	No
Permit everyone and require MFA, allow automat...	Yes	No
Permit everyone	Yes	No
Permit everyone and require MFA from unauthen...	Yes	No

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.



Display Name	Enabled	Type	Identifier	Access Control Policy
Web Claims	Yes	WS-Trust / SA...	https://www.swiveladfs.com/WebCla...	Permit everyone and require MFA

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

22.1.2 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.

22.2 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.

23 Known Issues

23.1 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.

23.2 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.

24 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.

25 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.

26 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

27 Error Messages

28 AuthControl Desktop

29 Introduction

AuthControl Desktop is the brand name for Swivel Secure's custom Windows Credential Provider.

The detailed article can be found under Windows Credential Provider.

30 Deploy ACD using MS group policies

31 Introduction

These are the instructions to use the windows group policies to "deploy" the AuthControl Desktop (Credential Provider).

32 Steps

1 - Install the Credential Provider on a single machine. Configure it as required, then use File, Export Settings from the configuration program to create a settings file named acd.xml. Alternatively, if you have a pre-configured build, there is no need for this step.

2 - Create a network share that can be accessed by all computers. Copy both the credential provider MSI and acd.xml (if required) to that folder.

3 - From the domain controller, in Server Manager, select the Tools menu, then "Group Policy Management".

4 - Select the domain node on the left-hand window. Right-click and choose "Create a GPO in this domain and link it here".

5 - Give the GPO a name, such as "AuthControl Credential Provider", and click OK.

6 - Under Group Policy Objects, find the GPO you just created, right-click on it and click Edit.

7 - Choose Computer Configuration, Policies, Software Settings, Software installation. Right-click and select New -> Package.

8 - From the file browser, enter the location of the MSI. It must be entered as a network share, i.e. \\Computer\Share\AuthControlCredentialProvider.msi. Leave deployment method as "Assigned".

9 - Choose User Configuration, Policies, Software Settings, Software installation and repeat the last 2 steps, except this time, the deployment method should be "Published".

10 - Close the editor and left-click on the GPO. Under Scope you should see the domain name in the Links section. Right-click on it and check "Enforced". Note that this will install the CP on every computer in the domain. It should be possible to restrict the policy to a single Organisational Unit, by applying the GPO link to that OU. You can only apply policies to domains or OUs, not ordinary containers. You can also restrict the policy by creating a group of computers and adding that group to Security Filtering.

9a) Choose User Configuration, Policies, Software Settings, Software installation. Right-click and select New -> Package.

9b) From the file browser, enter the location of the MSI. It must be entered as a network share, i.e. \\Computer\Share\AuthControlCredentialProvider.msi. Set deployment method to "Published".

33 Notes

Our understanding is that steps 7 and 8 make the software available for network installation. This step installs the software automatically if it is not yet installed, the next time each user connects to the domain.

The notes on the final step suggest how you can restrict which computers have the WCP installed.

Check the link below for more details:

https://support.microsoft.com/en-gb/help/816102/how-to-use-group-policy-to-remotely-install-software-in-windows-server

34 Changing Settings

If you want to change the settings for computers that already have AuthControl Desktop installed, for example, to enable or disable test mode, currently the only way to do this is to change the registry settings directly.

All the settings are in the following registry key:

\\HKEY_LOCAL_MACHINE\SOFTWARE\Swivel Secure\AuthControl Desktop

You will need to know the names of the settings in the registry: please contact Swivel Secure support for specific requests. We will give an example below of enabling or disabling Test Mode, for which the setting name is "TestMode".

1. Open "Group Policy Management" from a Domain Controller.
2. Right-click on the domain, or an OU if you only want to apply the policy to a subset
3. Select "Create a GPO in this domain and link it here". Give the GPO a name.
4. Right-click on the GPO and select "Edit"
5. Expand the tree for "Computer Configuration" -> "Preferences" -> "Windows Settings" -> "Registry"
6. Right-click on "Registry" and select New -> Registry Item
7. Make sure that action is "Update" and Hive is "HKEY_LOCAL_MACHINE"
8. Enter Key Path as "SOFTWARE\Swivel Secure\AuthControl Desktop". Make sure you type this correctly, including the correct spacing
9. Enter the Value name as "TestMode". To change a different value, enter the name as given by Swivel Secure
10. Set the value type to REG_DWORD (this is for numeric or on/off settings - for text settings use REG_SZ)
11. Set the value data to 1 to enable TestMode, or 0 to disable it.
12. Click OK

Note two points:

- The settings are only applied when a computer is restarted
- The settings are not applied immediately, so it is possible that the first login after restart will still use the old settings.

35 Microsoft Windows Credential Provider Integration (Legacy OS)

36 Introduction

Microsoft Windows Credential Provider is used in the desktop operating systems Windows Vista, 7, 8 and 8.1, and in the server operating systems Windows Server 2008 and 2012, including Remote Desktop Gateway. For newer operating systems (Windows Vista and Server 2012 R2 onwards), see Windows Credential Provider. For integration with the older Windows GINA used in Windows 2000, 2003 and XP see Microsoft Windows GINA login.

Users can authenticate using the Swivel Credential Provider allowing 2FA (Two Factor Authentication), or strong authentication at the Windows Logon. Offline authentication is also supported for single Channel authentication, following at least one successful authentication against the Swivel server with Third Party Authentication configured.

For new features in recent releases of the Credential Provider, see below.

36.1 Swivel Credential Provider FAQ

Q). Does the Credential provider support offline authentication? A). Offline authentication is permissible for Swivel users who have previously authenticated to the device. Offline local authentication is always single channel, even if single channel is normally disabled.

Q). Do all users have to authenticate using Swivel? A). Swivel does have the option to *Allow Unknown Users*, users known to Swivel will be prompted for authentication in this instance.

Q). Is it possible to define users who do not have Swivel authentication? A). Only by using the *Allow Unknown Users* for non Swivel user authentication.

Q). Is it possible to login without AD password, A). No the AD password is required.

37 Prerequisites

Swivel 3.x Server

Connectivity to Swivel server during installation (with Third Party Authentication for GINA enabled)

Microsoft Windows Vista, 7 or 8 (including 8.1); Microsoft Windows 2008 or 2012 Server (including R2).

Microsoft.Net Framework version 4.

Swivel Windows Credential Provider 64 bit (version 4.6) or

Swivel Windows Credential Provider 32 bit (version 4.6) or

Both of the above files in a single zip

Documentation only

A separate Swivel Credential Provider license is not required, but the users authenticating to Swivel must be licensed.

User with AD account and valid password.

38 Baseline

Swivel 3.7

Windows 7, Windows 2008 Server R2

39 Architecture

Swivel is installed as a Windows Credential Provider, and when a Windows login is made, AD username and password is checked against AD and the username and Swivel OTC is sent to the Swivel server using XML authentication, or locally if offline authentication is enabled.

39.1 Offline Authentication

Swivel allows offline authentication using single channel but not dual channel authentication. For offline authentication the user attempting to authenticate must have made at least one successful authentication against the Swivel server while Offline Authentication has been enabled. Swivel caches a limited number of strings for authentication, and cycles through these so there is no limit on the number of authentications which can be made. Swivel Account lockout is disabled for Swivel offline authentication. ChangePIN will not function when the Swivel server is not contactable. Local authentication is always single channel, even if single channel is normally disabled.

40 Swivel Integration Configuration

40.1 Configure a Swivel Agent

1. On the Swivel Management Console select Server/Agent

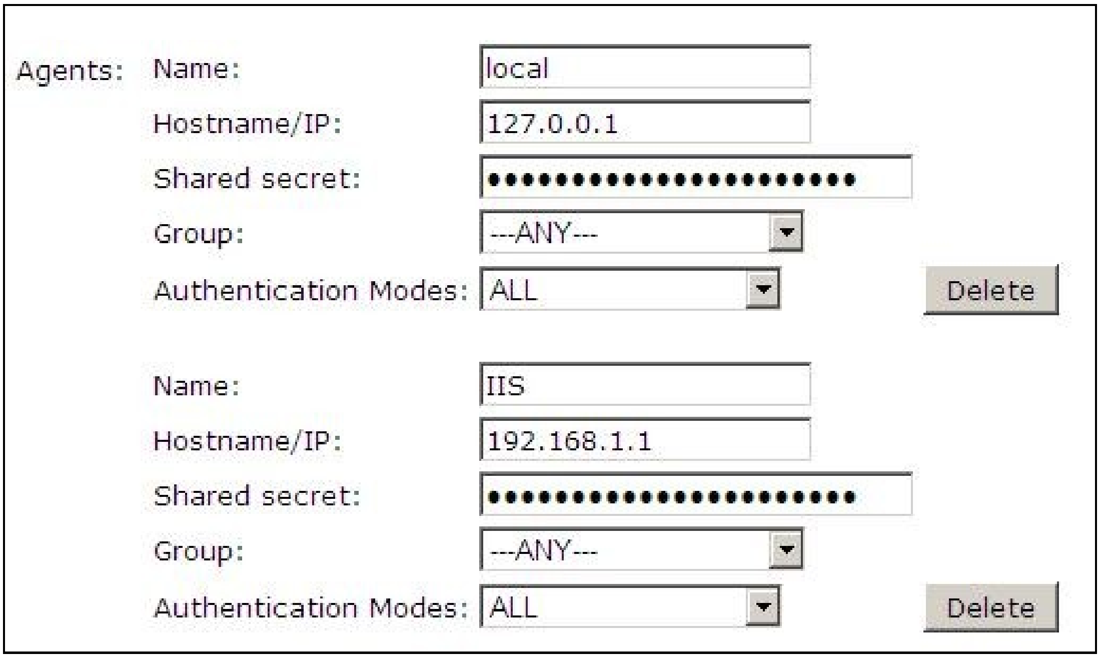
2. Enter a name for the Agent

3. Enter the Credential Provider IP address. You can limit the Agent IP to an IP address range like: 192.168.0.0/255.255.0.0 where the mask of 255 requires an exact match and 0 allows any value, so the previous example would allow any Agent in the range 192.168, or you can use an individual IP address for the Credential Provider.

4. Enter the shared secret used above on the Credential Provider

5. Enter a group, (Note in this instance ANY is not a valid group and will cause authentication to fail)

6. Click on Apply to save changes



Agents:
Name: local
Hostname/IP: 127.0.0.1
Shared secret: ••••••••••••••••••••••
Group: ---ANY---
Authentication Modes: ALL

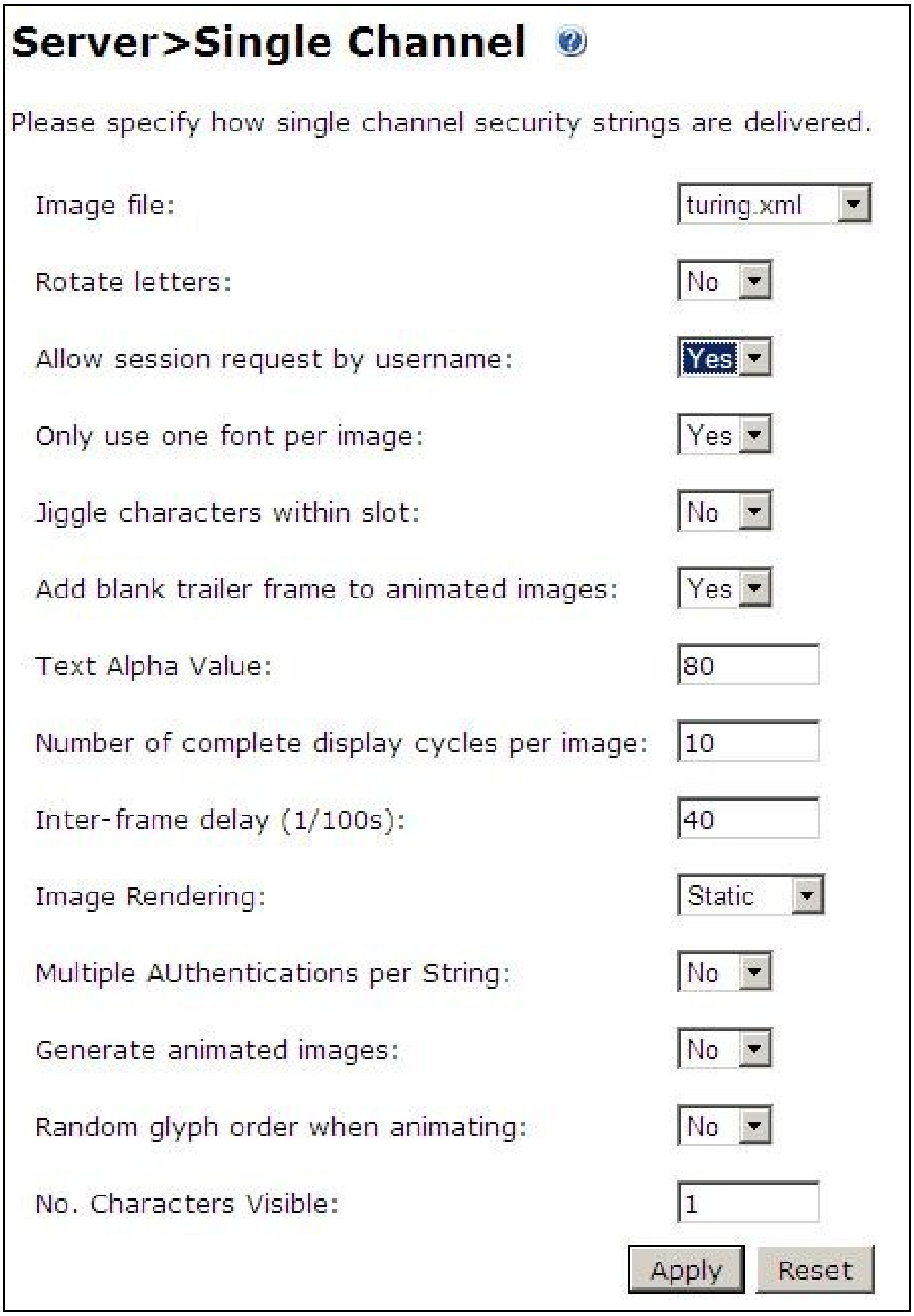
Name: IIS
Hostname/IP: 192.168.1.1
Shared secret: ••••••••••••••••••••••
Group: ---ANY---
Authentication Modes: ALL

Note that this creates a GINA menu item, but there are no configurable options, so is not selectable.

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

40.3 Create a Third Party Authentication

If offline authentication is to be allowed, a third party authentication must be created with an Identifier of WindowsGINA. (Even though the GINA is not part of Credential Provider the third party authentication module is still used and must be configured)

1. On the Swivel Management Console select Server/Third Party Authentication

2. For the Identifier Name enter: WindowsGINA (Even though the GINA is not used, this must be entered as WindowsGINA)

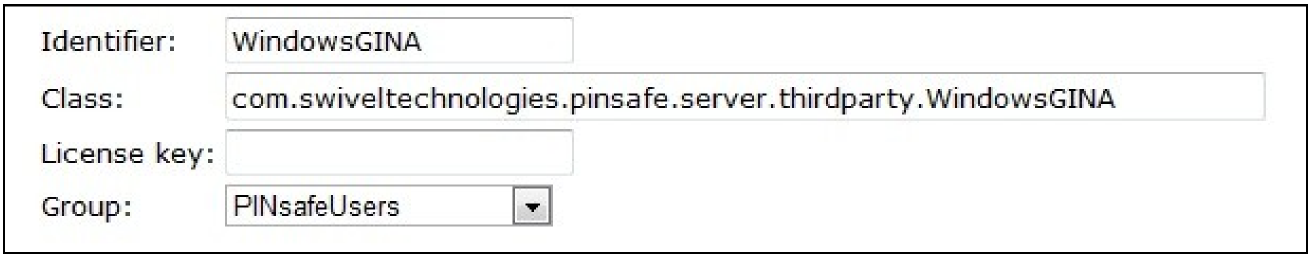
3. For the Class enter: com.swiveltechnologies.Swivel.server.thirdparty.WindowsGINA

4. For the License Key, leave this empty as it is not required

5. For the Group select a group of users (Note: the option Any cannot be selected)

6. Click Apply to save the settings

To allow offline authentication to be made a successful authentication must be made with the third party authentication in place.



Identifier:	WindowsGINA
Class:	com.swiveltechnologies.pinsafe.server.thirdparty.WindowsGINA
License key:	
Group:	PINsafeUsers

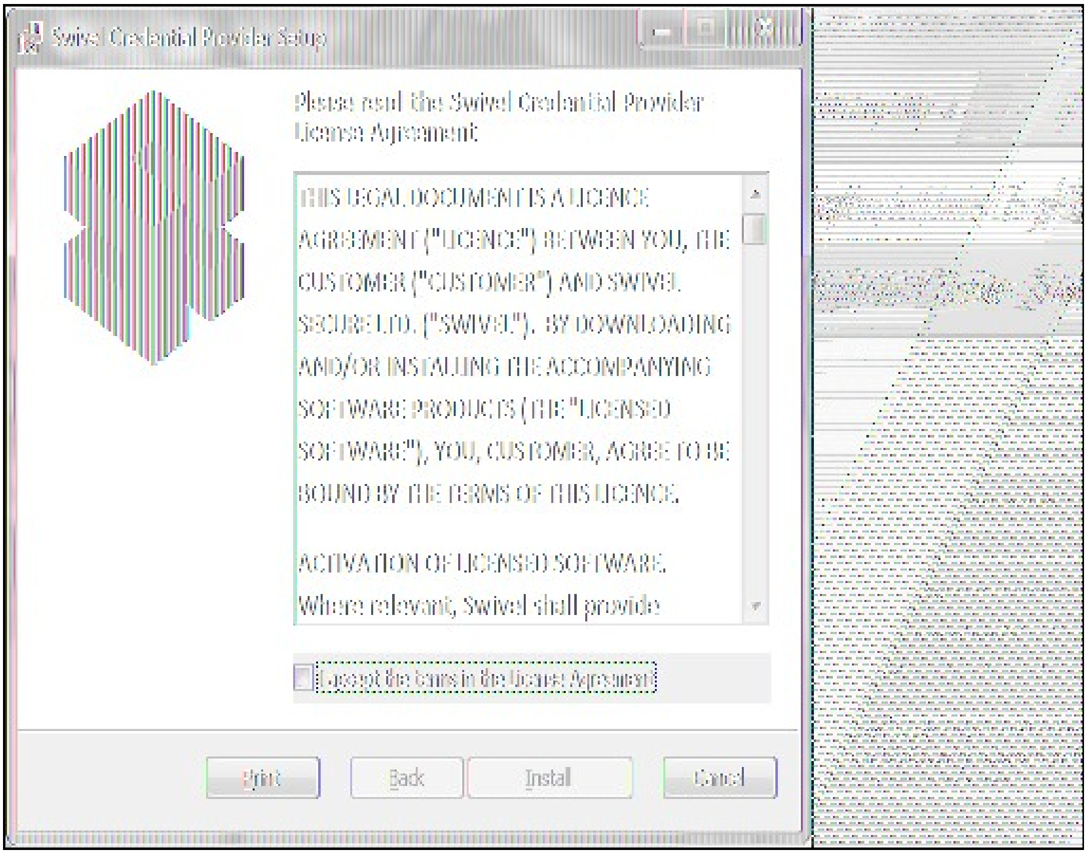
41 Microsoft Windows Swivel Credential Provider Installation

The Credential Provider is provided as a Microsoft Installer .msi file. You must run this as an administrator.

Ensure that the correct Swivel Windows Credential Provider is used: SwivelCredentialProvider_x86.msi for 32-bit or SwivelCredentialProvider_x64.msi for 64-bit.

Double-click the .msi file to run it. Alternatively, you can install from the command line, using the msiexec command.

The first page is the licence agreement:



Swivel Credential Provider Setup

Please read the Swivel Credential Provider License Agreement

THIS LEGAL DOCUMENT IS A LICENCE AGREEMENT ("LICENCE") BETWEEN YOU, THE CUSTOMER ("CUSTOMER") AND SWIVEL SECURE LTD. ("SWIVEL"). BY DOWNLOADING AND/OR INSTALLING THE ACCOMPANYING SOFTWARE PRODUCTS (THE "LICENSED SOFTWARE"), YOU, CUSTOMER, AGREE TO BE BOUND BY THE TERMS OF THIS LICENCE.

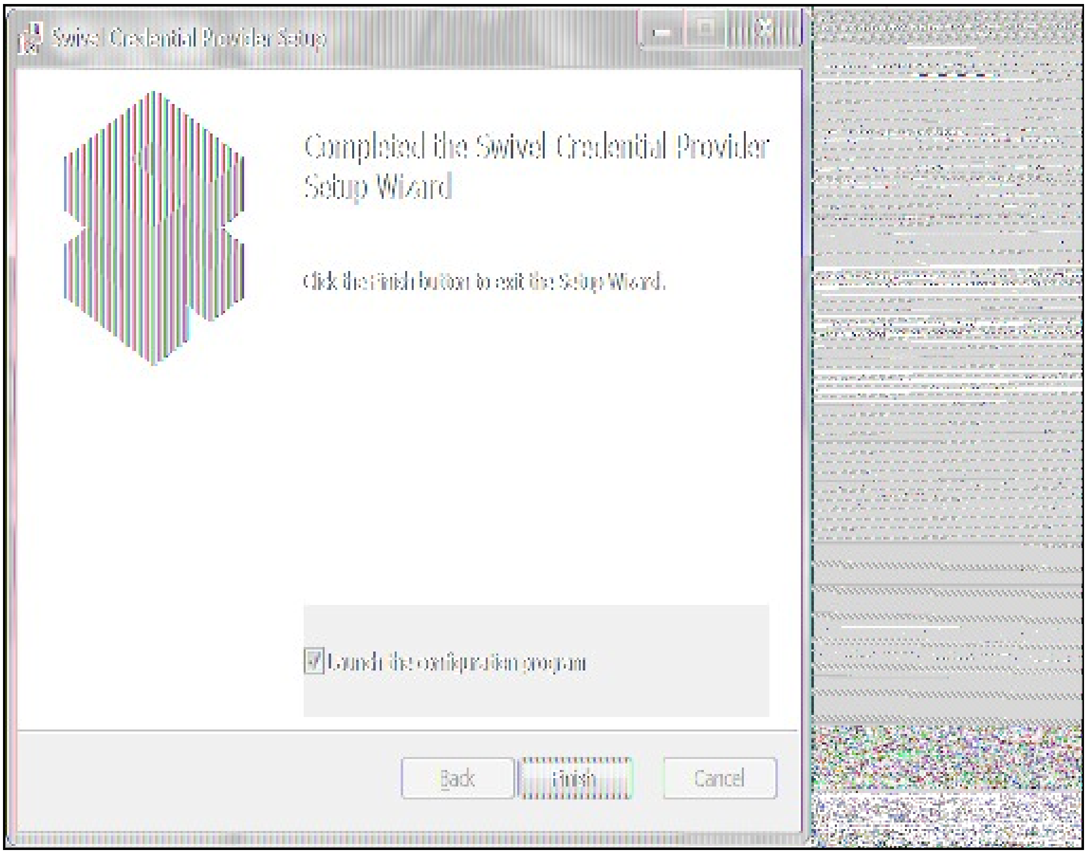
ACTIVATION OF LICENSED SOFTWARE.
Where relevant, Swivel shall provide

□ I accept the terms in the License Agreement

Read the licence agreement (yeah, right!), and check the box to acknowledge it. Click Next to continue.

The application will be installed to C:\Program Files\Swivel Secure\Swivel Credential Provider. If you have reconfigured the program files directory elsewhere, it will be installed there, but otherwise you cannot control where the application is installed.

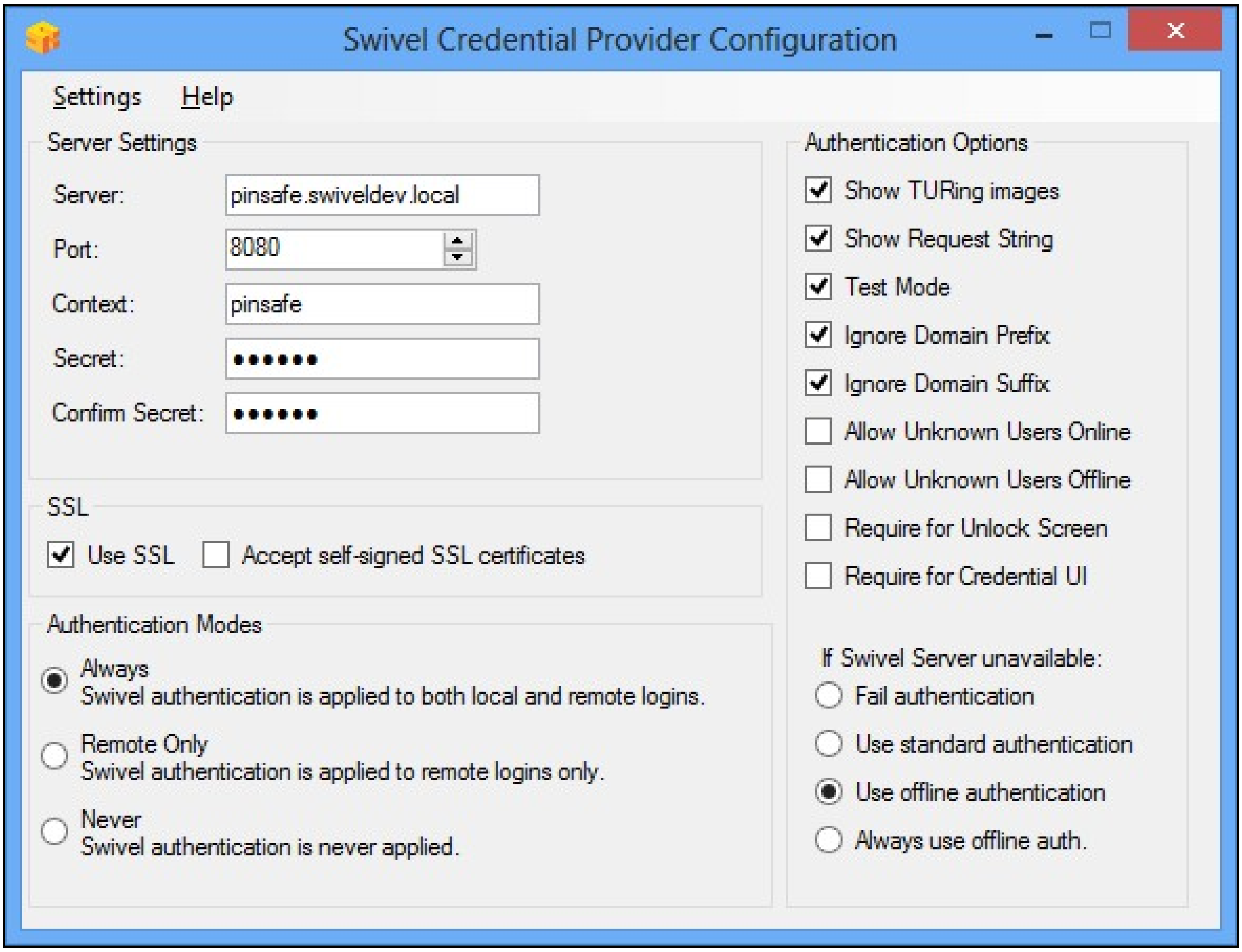
When the install has completed, the following dialog is shown:



Swivel Credential Provider Setup
Completed the Swivel Credential Provider Setup Wizard
Click the Finish button to exit the Setup Wizard.
☑ Launch the configuration program
Back
Finish
Cancel

Ensure that the tick box is checked for *Launch the configuration program* to configure the Swivel instance then click on Finish.

41.1 Windows Swivel Credential Provider configuration



Swivel Credential Provider Configuration

Server Settings

Server: pinsafe.swiveldev.local

Port: 8080

Context: pinsafe

Secret: ●●●●●●

Confirm Secret: ●●●●●●

SSL

☑ Use SSL ☐ Accept self-signed SSL certificates

Authentication Modes

● Always
Swivel authentication is applied to both local and remote logins.

○ Remote Only
Swivel authentication is applied to remote logins only.

○ Never
Swivel authentication is never applied.

Authentication Options

☑ Show TURing images

☑ Show Request String

☑ Test Mode

☑ Ignore Domain Prefix

☑ Ignore Domain Suffix

☐ Allow Unknown Users Online

☐ Allow Unknown Users Offline

☐ Require for Unlock Screen

☐ Require for Credential UI

If Swivel Server unavailable:

○ Fail authentication

○ Use standard authentication

● Use offline authentication

○ Always use offline auth.

The following options are available:

Server: The Swivel virtual or hardware appliance or server IP or hostname. To add resilience for use the VIP on a swivel virtual or hardware appliance, see VIP on PINsafe Appliances

NOTE: it has been observed in testing that DNS is not always available when logging on. It is therefore recommended that you use IP address, rather than host name in this section.

Port: The Swivel virtual or hardware appliance or server port

Context: The Swivel virtual or hardware appliance or server installation instance

Secret: and **Confirm Secret:** A shared secret which must be entered onto the Swivel virtual or hardware appliance or server

Use SSL The Swivel server or virtual or hardware appliance uses SSL communications

Accept self signed SSL certificates Check this box if Use SSL is enabled, and you do not have a commercial certificate on your Swivel server (or a certificate signed by an authority that the client machine trusts).

Authentication Mode, Always Swivel authentication is required for remote and local logins

Authentication Mode, Remote Only Swivel authentication is required for remote logins only

Authentication Mode, Never Swivel authentication is not used

Show TURing images Show TURing images if requested

Show Request String Show the Request string image to allow the user to obtain a new security string by dual channel

Test Mode With test mode the user can switch user to a standard authentication, see below

Ignore Domain Swivel will remove any domain prefix (domain\username) or suffix (username@domain) before matching username. This does not affect Windows authentication usernames.

Allow Unknown Users Online If the username is not recognized by Swivel, the user can authenticate using Windows credentials only. Any Swivel OTC entered will be ignored. If the user is known then they must authenticate using Swivel authentication.

Allow Unknown Users Offline If offline authentication is used, users that do not have credentials cached locally can authenticate using Windows credentials only. Any OTC entered will be ignored. If the user has previously authenticated in online mode, then they must enter the correct one-time code.

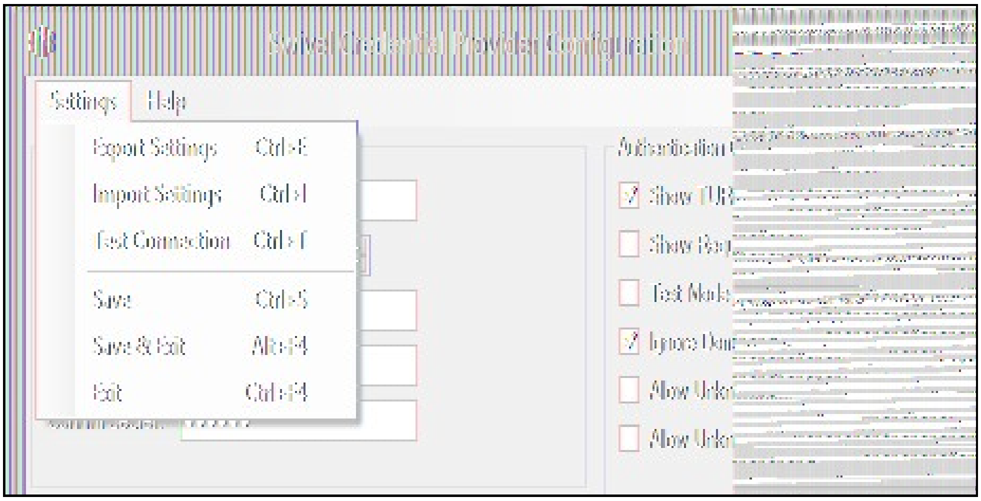
If Swivel unavailable, Fail authentication If the Swivel server cannot be contacted then authentication will fail

If Swivel unavailable, Use standard authentication If the Swivel server is unavailable use standard authentication, the OTC field is displayed but ignored.

If Swivel unavailable, Use offline authentication If the Swivel server cannot be contacted a locally generated Turing image can be used for authentication. If this option is enabled, users will be able to force offline mode using a checkbox on the login dialog.

Always use local auth A local Turing image is always used and the Swivel server is not contacted. All users must previously have authenticated using online authentication (unless the option "Allow unknown users offline" is enabled).

The remaining options are available from the Settings menu:

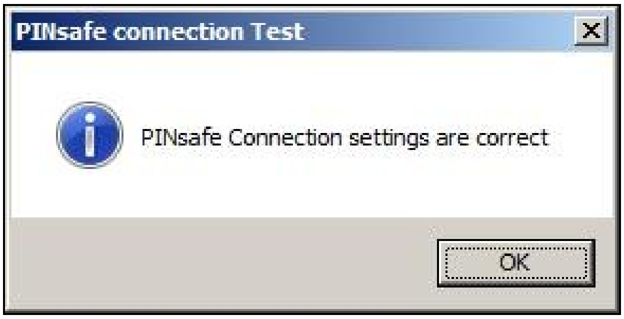


Export Settings Export settings as an XML file. These can be used to import settings elsewhere.

Import Settings Import settings from an XML file exported elsewhere.

Test Connection Tests link to Swivel server:

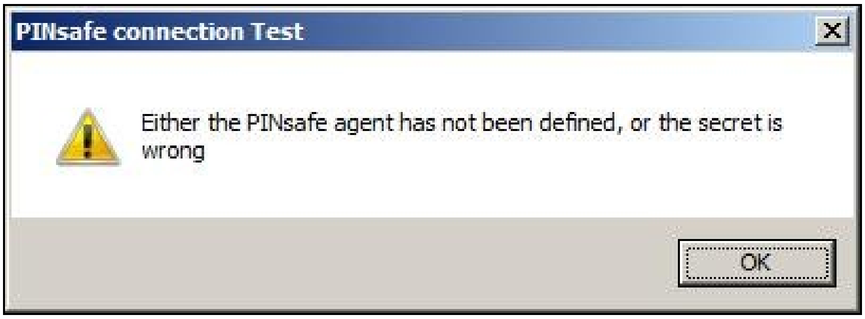
A correct configuration should produce a dialogue box with **Swivel Connection settings are correct.**



PINsafe connection Test

PINsafe Connection settings are correct

Incorrect settings will produce a dialogue box with **Either the Swivel agent has not been defined, or the secret is wrong**



PINsafe connection Test

Either the PINsafe agent has not been defined, or the secret is wrong

Save Save the current settings.

Save and Exit Save the current settings and close the program.

Exit Close the program without saving the settings. You will be prompted to confirm if any settings have been changed.

41.2 Additional Installation Options

41.2.1 Manually configuring the Swivel Login

NOTE: It is recommended to use the Swivel Login Configuration Tool where possible.

If it is not possible to use the configuration utility the Swivel Login settings may be edited manually in the registry. The following values found within the "HKEY_LOCAL_MACHINE\SOFTWARE\Swivel Secure\Swivel Credential Provider" key are used by the Login:

PINsafeServer - The name or IP of the Swivel server

PINsafePort - The Swivel server port

PINsafeContext - The Swivel server context

PINsafeSecret - The Swivel agent secret

PINsafeProtocol - 1 for https, 0 for http

PINsafeAllowSelfCert - 1 to allow SSL requests to a Swivel server with certificate errors, 0 not to

PINsafeLoginSelect - determines when Swivel authentication is required: always, remote or disabled.

PINsafeShowTURing - 1 to show the TURing request link, 0 not to

PINsafeRequestString - 1 to show the request string link, 0 not to

PINsafeAllowDefaultLogin - 1 to allow default login if Swivel unavailable, 0 not to

PINsafeUseLocalAuth - When to use local TURing authentication: always, fallback or never.

PINsafeDisableFilter - 1 to enable test mode, 0 to hide the standard authentication option

PINsafeAllowUnknownUsers - 1 to allow unknown users in online mode

PINsafeAllowUnknownOffline - 1 to allow unknown users in offline mode

PINsafeIgnoreDomain - 1 to ignore the domain prefix when checking Swivel users

The following values may be seen in this registry key also, but should not be changed:

PINsafeBackgroundsFolder

PINsafeFontsFolder

PINsafeResourceDLL

PINsafeHelpUrl

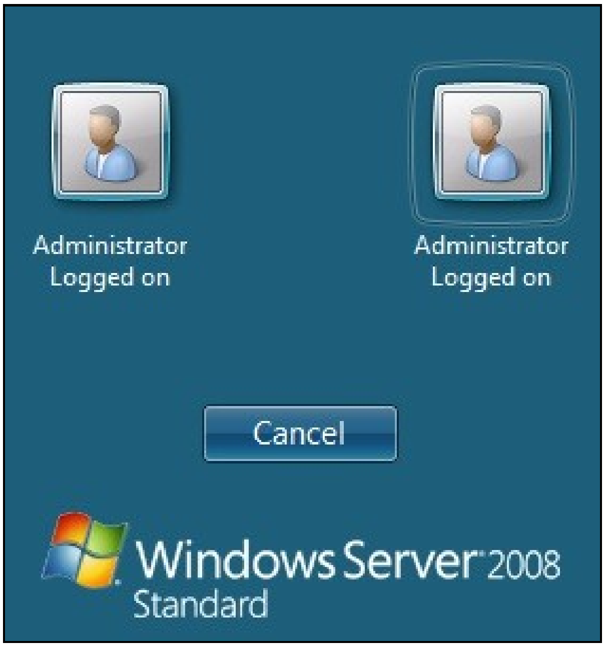
Directory

Uninstaller

Version

41.3 Test Mode

In Test Mode the Windows Credential Provider has an additional login that can be used as a standard user login. In test mode the last successful login will be selected for login.



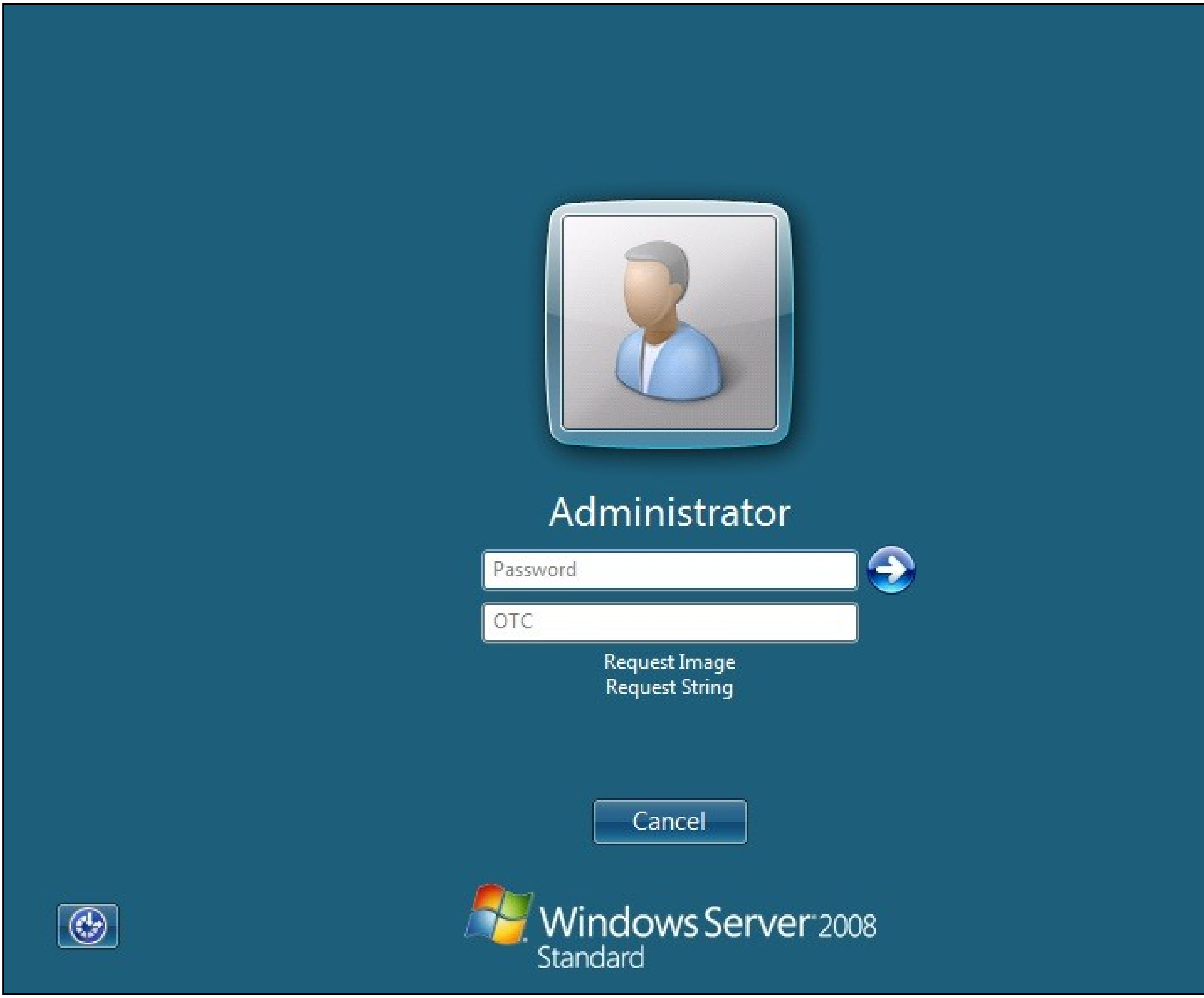
The Swivel credentials will always be on the left, the standard credentials on the right.

41.4 Importing Configurations

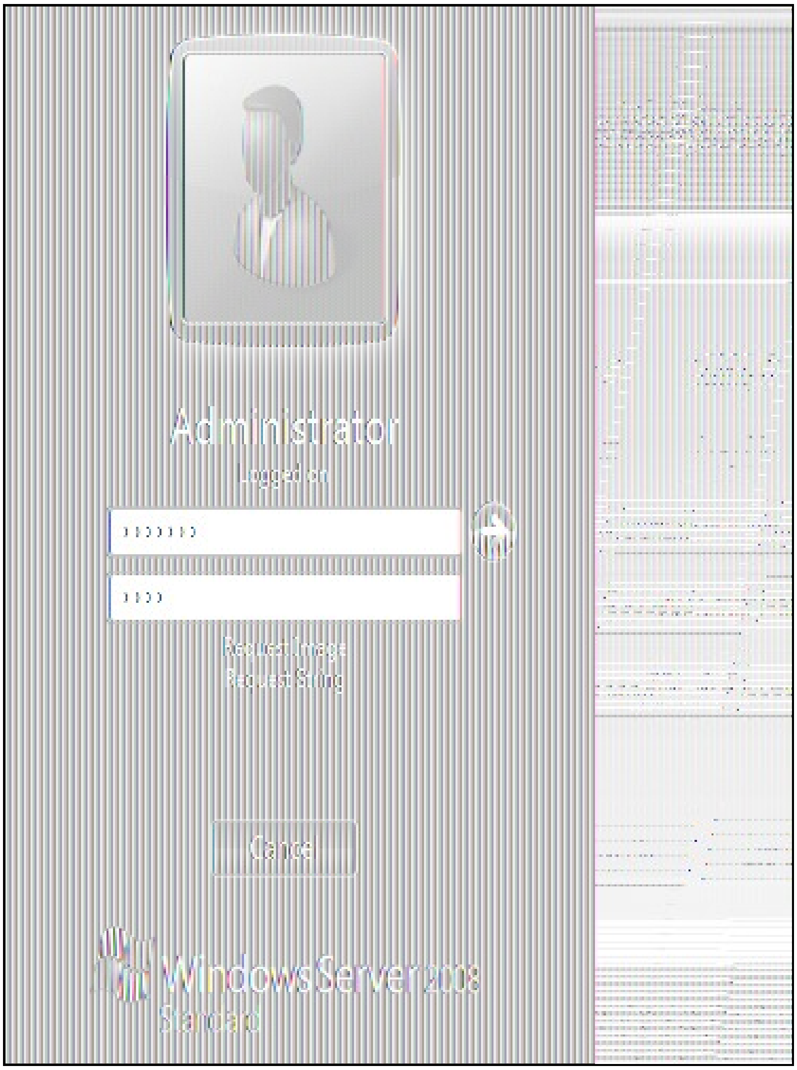
You can import credentials exported from other installations using the Import Settings menu item. Alternatively, if you need to install the Credential Provider on a large number of machines, you can modify the .msi file and replace the blank LoginSettings.xml file included with your own custom version. If you do not have the ability to modify MSI files, you can email your settings to support@swivelsecure.com and request a custom build.

42 Verifying the Installation

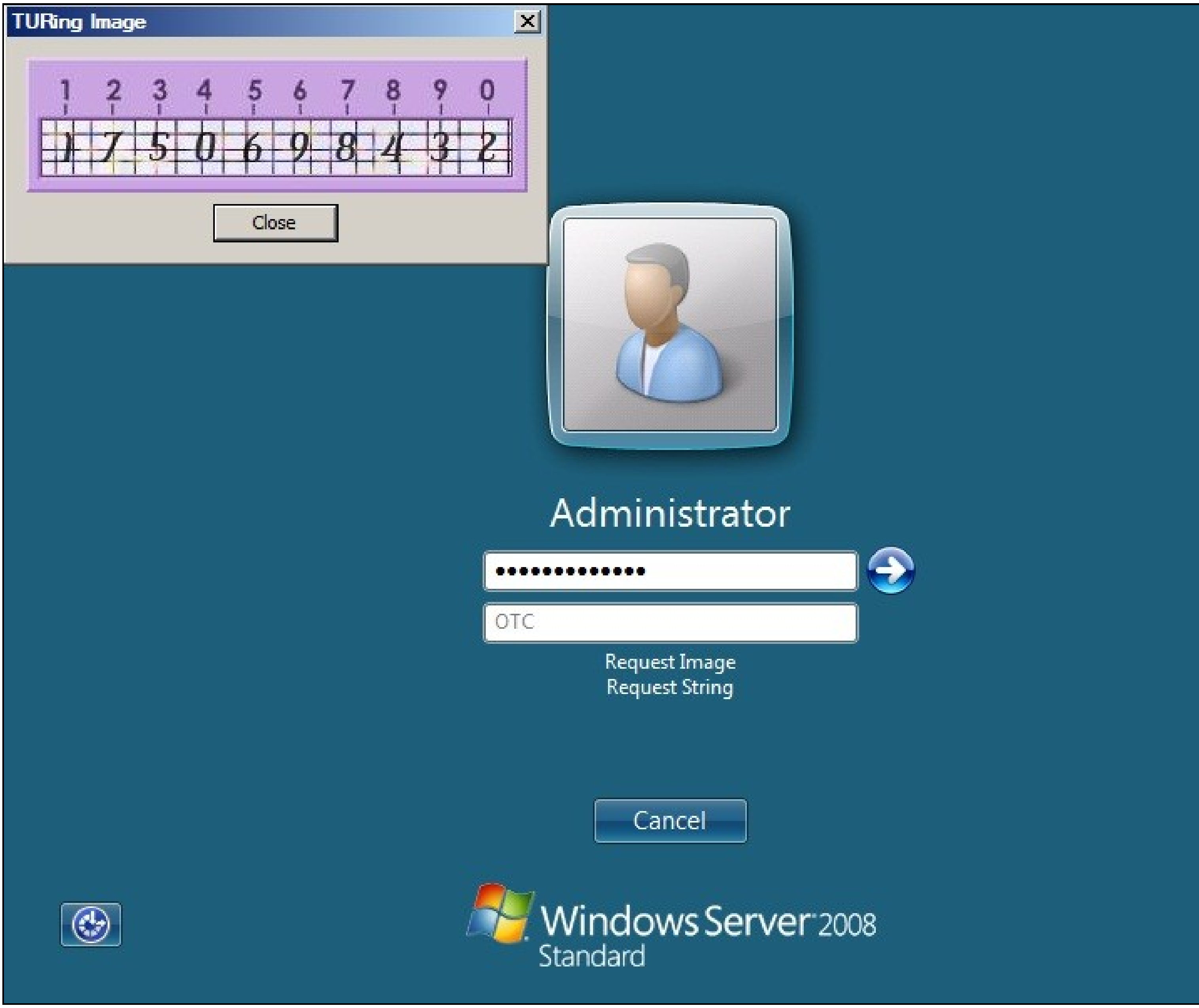
At the windows login a password and OTC login field should be available with Request Image and Request String options available.



If a Dual Channel login is made then the user should be able to enter their OTC. Note the Get Image should not be pressed, otherwise the log will be expecting a Single Channel login for the length of the session timeout (default 2 minutes).



Selecting the Request Image button should generate a Single channel Image for authentication. The Swivel log should show a session request message: *Session started for user: username.*



A successful login should appear in the Swivel log: *Login successful for user: username*

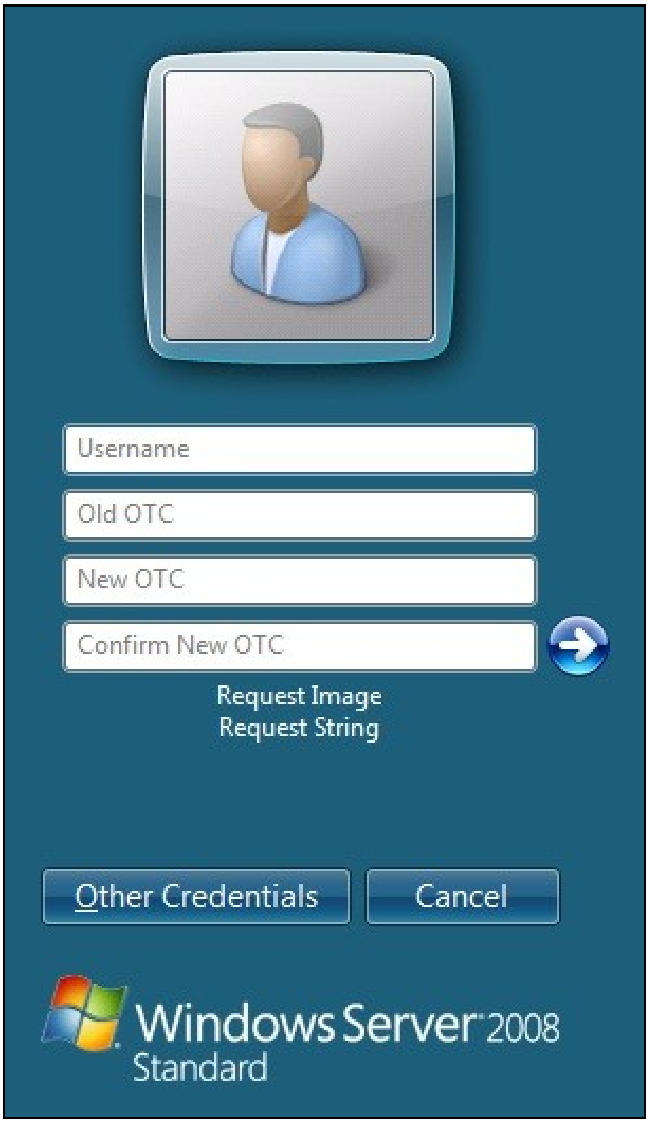
A failed login should not allow a login, and the following message should be displayed in the Swivel log: *Login failed for user: username*

43 ChangePIN

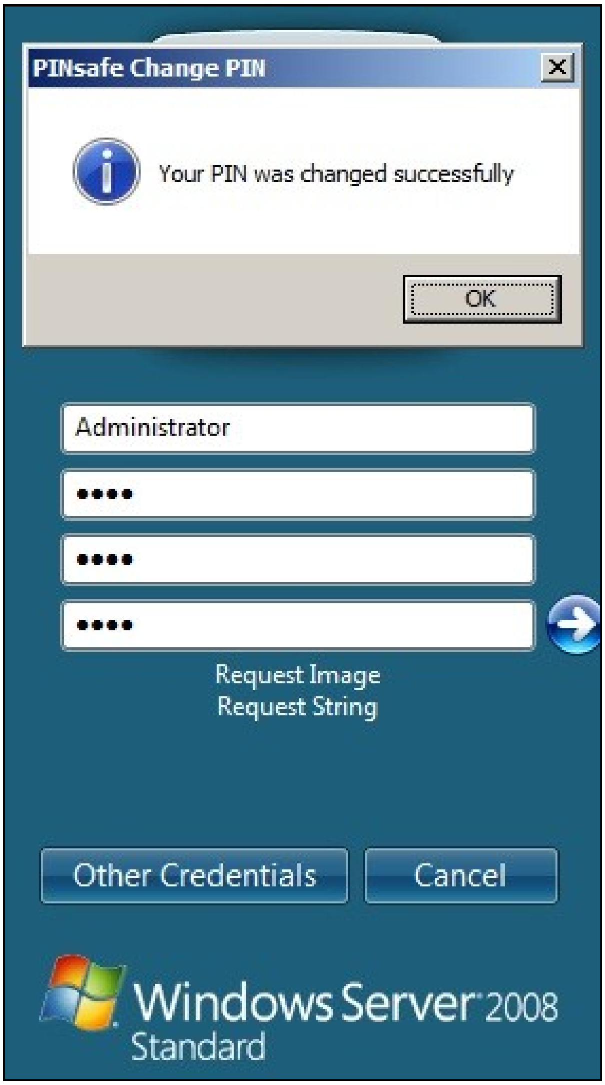
A user is usually able to change the password by using the Ctrl-Alt-Del keys (CTL-Alt-End for remote sessions). With the Windows Swivel Credential Provider installed, an additional option exists when the Change Password is selected, by clicking on the Other Credentials. This will not function for Offline authentication.

With Swivel authentication a user never changes enters PIN and this is true for ChangePIN. A user enters their current OTC, and then enters an OTC for what they wish their new PIN to be. PIN enforcement may be in place to the Swivel server to prevent the choosing of poor PIN numbers.

A user may use a single channel image or a dual channel security string to change their PIN.



A successful Change PIN will show the message **Your PIN was changed successfully**



PINsafe Change PIN

Your PIN was changed successfully

The Swivel server will also display in the logs a changePIN message **Change PIN successful for user: username**

44 Uninstalling the Swivel Integration

Use the Uninstall option from the Program menu, right click on the Windows Credentials provider and click on Uninstall. Note that uninstalling and reinstalling the Credential Provider will remove the settings, so if you need to reinstall at any point, make sure you have an exported settings file saved.

45 Troubleshooting

Test Mode enables you to login using the Standard Windows authentication and not Swivel authentication. If you disable Test Mode the additional logon users disappear and the machine will then be purely using Swivel.

If there is a problem then use Windows Safe Mode to login and enable Test Mode again. Safe Mode uses Standard Windows authentication.

Pressing Ctrl+Alt+Del reverts user back to login screen

A normal login may be attempted after a short period. This can occur as the Windows login screen may appear before a network connection has been made during boot. To prevent the login screen from not being accessible, enable the option in group policy to Wait until network is ready before user logon.

User must select the back button and select Other User to logon

This occurs when the system is running in Test mode. Disable the Test mode to allow normal login.

Change Pin is displayed instead of the logon screen

This has been seen on Dell laptops that have the *Dell Control Point Security Manager* installed. Remove this prior to the Windows Swivel Credential Provider installation.

FLUSHING_IMAGE_CACHE, ClientAbortException: java.net.SocketException: Connection reset

This error message can be seen in the Swivel log when a Windows login is attempting to use an animated gif. Turn off animated gifs and switch to 'Static', on Swivel - This is set under Server > Single Channel > Image Rendering.

Double User Entry at login, enforced test mode when test mode is disabled

Some fingerprint scanning software may cause this issue, this has been seen on an IBM Thinkpad. Check in the registry under the following

\\HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Authentication\Credential Provider Filters

look for keys which have values of: Fingerprint Logon Credential Provider Filter

and

\\HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers

look for keys which have values of: Fingerprint Logon Credential Provider

To test if these are the cause, on a test system, either remove the fingerprint software (disabling may still leave the registry keys) or backup the keys by exporting them, then remove them.

45.1 Disabling the Swivel Login

If the Swivel Login fails to load correctly it can be disabled using the following process:

Using the F8 boot menu start Windows in safe mode

Either run the Swivel Login Configuration and edit the settings or

Using regedit.exe remove the "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowNT\CurrentVersion\WinLogon\ginadll" registry value

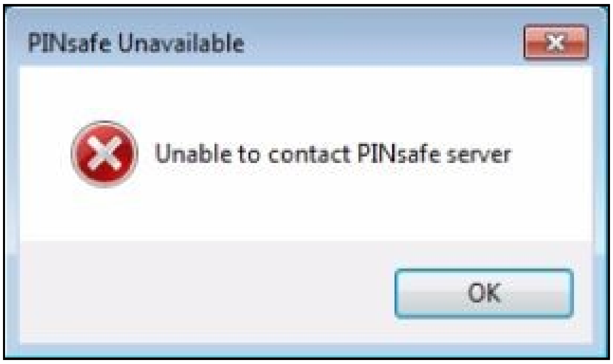
Reboot Windows

Following this process the standard Windows Login should be restored allowing access.

45.2 Error Messages

Unable to contact PINsafe server

Version 4.x only supports TLSv1 which means if you are running a version 3 Appliance, you must enable TLSv1 under Tomcat > SSL Protocols > Enable TLS1.0.


PINsafe Unavailable

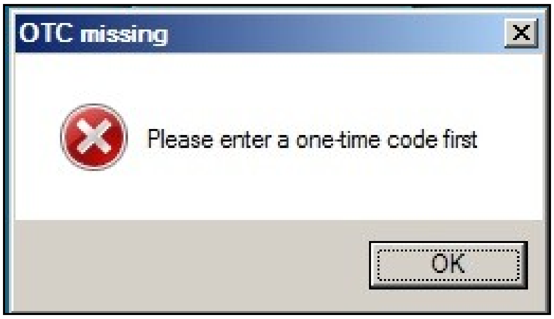
Unable to contact PINsafe server

Wrong Parameter or **Parameter is incorrect**

This message is displayed at the Windows login and can have several causes, check the Swivel logs for errors:

- The user must exist in AD and Swivel
- When an incorrect OTC is entered, when using local authentication. Unfortunately, local authentication will not work with the "Connect To" dialog. However, you should still get the remote desktop login displayed, and will be able to authenticate to this.
- The user account is locked in Swivel
- The Swivel Sever Agent has not been configured correctly

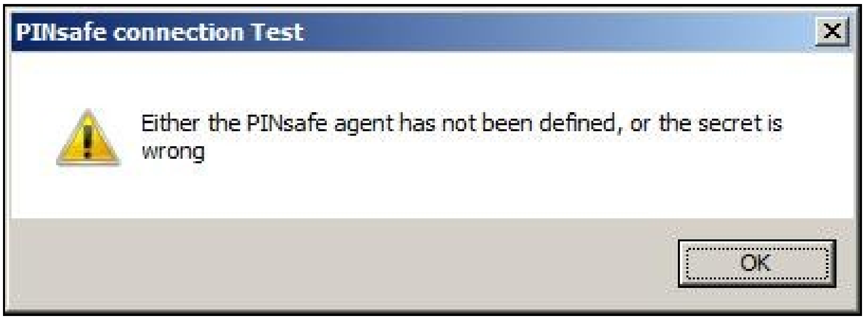
Please enter a one-time code first


OTC missing

Please enter a one-time code first

A One Time Code was not entered in the OTC field during login.

Either the Swivel agent has not been defined, or the shared secret is wrong

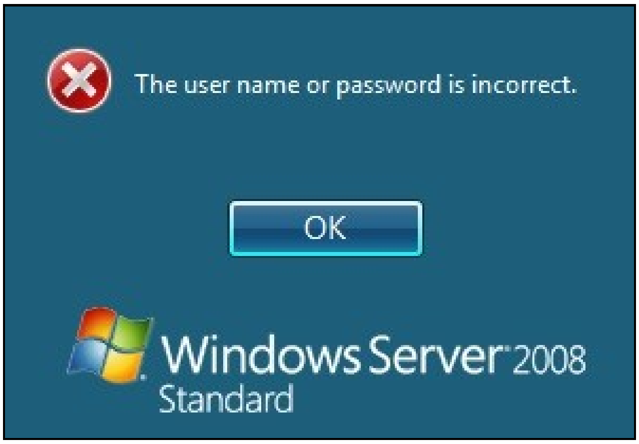

PINsafe connection Test

Either the PINsafe agent has not been defined, or the secret is wrong

AgentXML request failed, error: The agent is not authorised to access the server.

The credential Provider is not permitted to connect to the Swivel server. Add an Agent for communication.

The user name or password is incorrect.



The user name or password is incorrect.

Check Password with Repository: If this setting is enabled against the Agent, then you should disable it to prevent it attempting to check for a password against the repository. This is a potential cause when receiving "The user name or password is incorrect".

AgentXML request failed, error: No suitable authentication method for the user "Administrator" was found. The user may be missing from the user repository or a synchronisation has not yet occurred.

The user Administrator is not defined as a Swivel user

Session start failed for user: x, error: No Data for user was found. or **error: No data for the user was found**
The requested user does not exist in the database. If the user does exist in the repository (e.g. Active Directory) then Swivel needs to sync with that repository.

Dual channel message request failed, error: On-demand dual channel delivery is disabled.

A dual channel message request was made but the On-demand delivery is not enabled. If it should be enabled, on the Swivel Administration console select Server/Dual Channel, then set On-demand delivery to Yes.

AgentXML request contained third party data for a third party class that does not exist. Third Party Class ID: WindowsGINA.

and

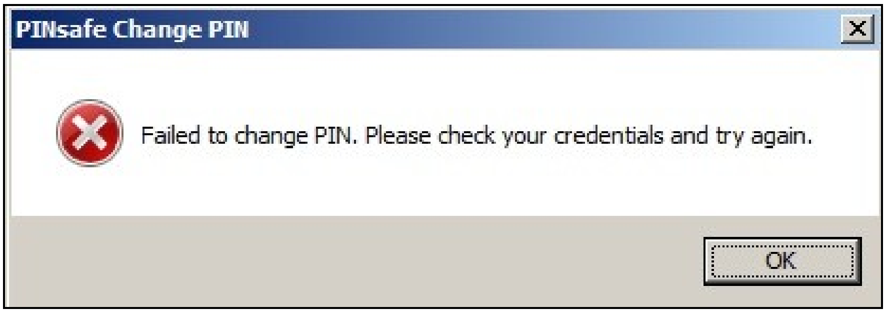
error: The third party class could not be found.

The Third Party Authentication class does not exist or has been created incorrectly. Create the class, see Create a Third Party Authentication

The third party class could not be found

This error can also be created when the Swivel Administration console Server/Agents, Group is set to Any. A group should be specified.

Failed to change PIN. Please check your credentials and try again.



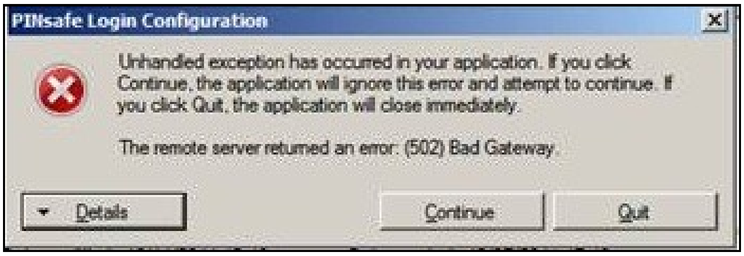
PINsafe Change PIN

Failed to change PIN. Please check your credentials and try again.

The user has failed to change the PIN number. This could occur if the Swivel server cannot be contacted.

Unhandled exception has occurred in your application. If you click Continue the application will ignore this error and attempt to continue. If you click Quit, the application will close immediately.

The remote Server returned an error: (502) Bad Gateway.


PINsafe Login Configuration

Unhandled exception has occurred in your application. If you click Continue, the application will ignore this error and attempt to continue. If you click Quit, the application will close immediately.

The remote server returned an error: (502) Bad Gateway.

This error has been seen when a Test Connection is made from the Credential Provider and can be caused by being unable to connect to the Swivel server. Check for network settings such as proxy settings on the local server, and if an SSL connection is required.

46 Release Notes

46.1 Release of Version 4.6

4.6.2.1, released 27th June 2016.

The main change in version 4.6 is that there is better support for offline authentication: it has been observed in previous versions that the strings ran out after a number of offline authentications. This has now been resolved.

There is a known issue with version 4.6, in that it requires Microsoft Update KB2999226 to have been applied. This should be applied automatically by Windows Update, but if you have a problem installing or running the program, check that this update has been applied.

46.2 Release of Version 4.5

4.5.4.1, released 4th February 2015.

Version 4.5 includes the following fixes and enhancements over previous versions:

- Swivel authentication is optionally applied to the Unlock screen as well as the login screen
- Swivel authentication may be disabled (and by default is disabled) when connecting to remote computers
- The image window resizes dynamically depending on the type of image. The scale option is on the Settings drop-down menu.

46.3 Release of Version 4.4

Version 4.4 includes the following fixes and enhancements over the previous releases:

- It is fully-compatible with Windows 8 and Windows 2012 Server.
- It switches to single-channel mode if local authentication is enabled and the Swivel server is not available.
- Unlike the previous beta, version 4.3, this version is compatible with ALL Windows Operating Systems from Windows Vista onwards.
- If the user's password has expired, they are correctly redirected to the change password page.
- A problem which occasionally caused crashes when entering the username has now been resolved.
- You can now import settings exported from other installations.
- The installer is now a standard Windows MSI file. This makes it possible to customise the installation to contain your company's settings file, if you have the tools to modify MSI files. Alternatively, you can send your exported settings to support@swivelsecure.com, who can create a custom installer for your organisation.

47 Known Issues and Limitations

This version of the Swivel Credential Provider is not compatible with the Swivel version 3 appliance. An update will be available shortly.

The Swivel Windows Credential Provider does not support the use of

- Pinpad
- Animated gifs

for Single Channel authentication.

It has been observed in testing that DNS is not always available when logging on. It is therefore recommended that you use IP address, rather than host name for the Swivel server.

Local authentication only works in single channel mode: the dual channel strings are not available offline. To use offline authentication, TURing image display must be enabled, even if normal authentication is dual channel.

If a Swivel server has been configured with a Single Channel login configuration that is not viewable, the following options are available to recover access:

- Login using dual channel
- Login using an image generated elsewhere such as on the Swivel Administration console or Taskbar on another server
- Alter the settings on the Swivel server to serve a permitted image
- Login offline if permitted
- Login to safe mode as described elsewhere

In Windows 8 and Windows Server 2012, the Credential Provider appears as a single key icon, which you must select before logging on. In some cases, where Windows should show the last used credential, you will need to click the back arrow and then select the Credential Provider. A similar problem occurs with the Unlock screen. An updated version, specific to Windows 8 and Windows Server 2012, will be released in due course.

By default, the credential provider assumes that administrator is the local administrator, rather than the domain administrator, so you have to explicitly state the domain name to logon as domain administrator. This is a feature of the default credential provider as well.

In the Swivel administration console, the Windows GINA menu item is present, but there are no configurable options, so is not selectable.

48 Swivel Windows Credential Provider

49 Introduction

Version 5 of the Credential Provider is now released. Documentation on it can be found at Windows Credential Provider. This documentation is out of date, and is not being maintained

This version has been tested on Windows 8, Windows 10 and Windows Server 2012 R2

The current version only works for 64 bit operating systems.

Swivel Windows Credential Provider is used in the desktop operating systems Windows 8 and 10 and the server operating system Windows Server 2012. For integration with Windows Vista and 7 and Server 2008, see Microsoft Windows Credential Provider Integration.

Users can authenticate using the Swivel Credential Provider allowing 2FA (Two Factor Authentication), or strong authentication at the Windows Logon. Offline authentication is also supported for single Channel authentication, following at least one successful authentication against the Swivel server with Third Party Authentication configured.

Supported methods are:

- **TURing** Lets the user sign into windows by using TURing.
- **PINpad** Lets the user sign into windows by using PINpad.
- **On Demand** Lets the user sign into windows by requesting a security string to their preferred method (SMS or email). More information.
- **Other Two Factor** Lets the user sign into windows by entering a one-time code based on a security string received previously or OATH token.

NOTE: One Touch is not currently supported.

49.1 Downloads

Swivel Windows Credential Provider 64 bit (version 5.1.0)

49.2 Swivel Credential Provider FAQ

Q). Does the Credential provider support offline authentication? A). Offline authentication is permissible for Swivel users who have previously authenticated to the device. Offline local authentication is always single channel, even if single channel is normally disabled.

Q). Do all users have to authenticate using Swivel? A). Swivel has the option to *Allow Unknown Users*, users known to Swivel will be prompted for authentication in this instance. There is also a "Trusted Users" list where specific users can be added.

Q). Is it possible to define users who do not have Swivel authentication? A). Yes either by the *Allow Unknown Users* for non Swivel user authentication or by adding the user to the "Trusted Users" list

Q). Is it possible to login without AD password, A). No the AD password is required.

50 Prerequisites

Swivel version 3.11.3 or later.

Connectivity to Swivel server during installation (with Third Party Authentication for GINA enabled).

Microsoft Windows 8 (including 8.1) and 10 or Windows Server 2012.

Microsoft.Net Framework version 4.

Swivel Windows Credential Provider 64 bit (version 5.1.0)

A separate Swivel Credential Provider license is not required, but the users authenticating to Swivel must be licensed.

User with AD account and valid password.

51 Baseline

Swivel 3.10.4

Windows 8, 10, Server 2012 R2.

52 Installation

52.1 Basic Installation

To install the Swivel Windows Credential Provider run the installer and follow the on-screen instructions. At the end of the on-screen instructions you will be given the option to launch the configuration program to customise the Credential Provider. This can normally be found in the start menu under "Swivel Secure" and in "C:\Program Files\Swivel Secure\Swivel Credential Provider".

After installation and configuration:

- On Windows 8, 8.1 and 10 the computer must be restarted.
- On Windows Server 2012 R2 the Administration account can be signed out rather than doing a full restart.

52.2 Multiple Installation

If a configured Swivel Windows Credential Provider has been set up then the settings can be imported automatically on new installations.

1. Extract the settings using the existing Credential Provider from the "File > Export Settings" option, keeping the default name.
2. Copy this file and the installation file onto the new computer, they must be in the same location (example both files on the desktop).
3. Run the installation as described above and the settings will be automatically loaded during installation.

53 Architecture

Swivel is installed as a Windows Credential Provider, and when a Windows login is made, AD username and password is checked against AD and the username and Swivel OTC is sent to the Swivel server using XML authentication, or locally if offline authentication is enabled.

53.1 Offline Authentication

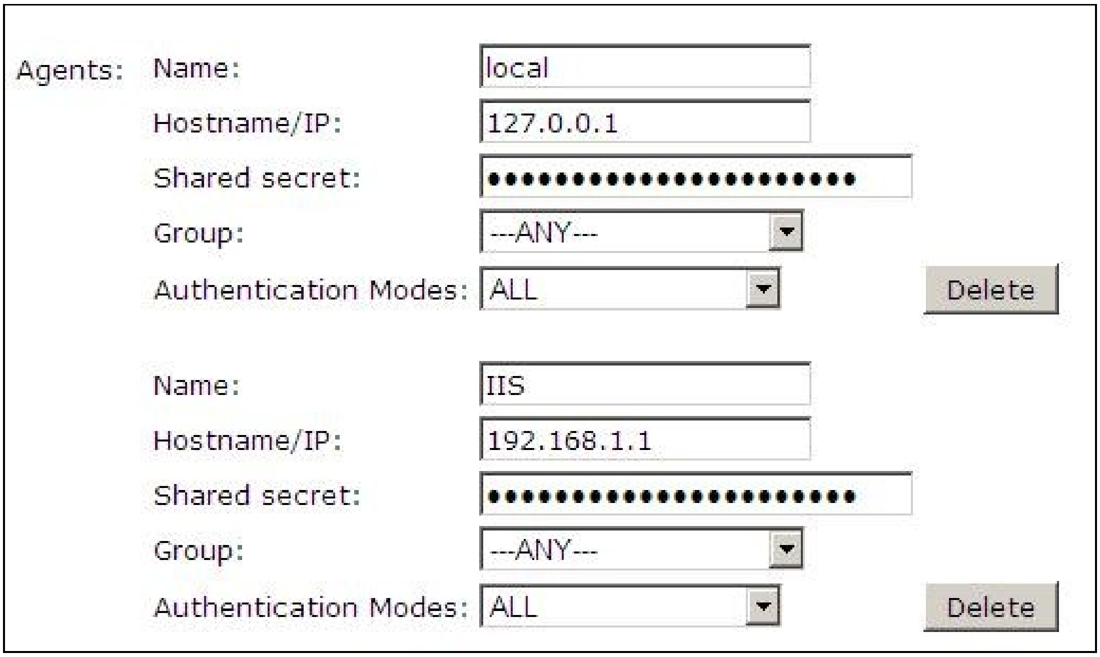
Swivel allows offline authentication using single channel but not dual channel authentication. For offline authentication the user attempting to authenticate must have made at least one successful authentication against the Swivel server while Offline Authentication has been enabled. Swivel caches a limited number of strings for authentication, when one is shown then it's classed as used and will not be re-shown, if the user makes a successful offline authentication then the number of strings will be replenished however if the user runs out of strings then they will need to authenticate online to get some more. Swivel Account lockout is disabled for Swivel offline authentication. ChangePIN will not function when the Swivel server is not contactable. Local authentication is always single channel, even if single channel is normally disabled.

Update: from version 5.4 onwards, offline is also supported for OATH tokens and for mobile app in OATH mode. This requires Sentry version 4.0.5 or later.

54 Swivel Integration Configuration

54.1 Configure a Swivel Agent

1. On the Swivel Management Console select Server/Agent.
2. Enter a name for the Agent.
3. Enter the Credential Provider IP address. You can limit the Agent IP to an IP address range like: 192.168.0.0/255.255.0.0 where the mask of 255 requires an exact match and 0 allows any value, so the previous example would allow any Agent in the range 192.168, or you can use an individual IP address for the Credential Provider.
4. Enter the shared secret used above on the Credential Provider.
5. Enter a group, (Note in this instance ANY is not a valid group and will cause authentication to fail).
6. Click on Apply to save changes.



Agents:

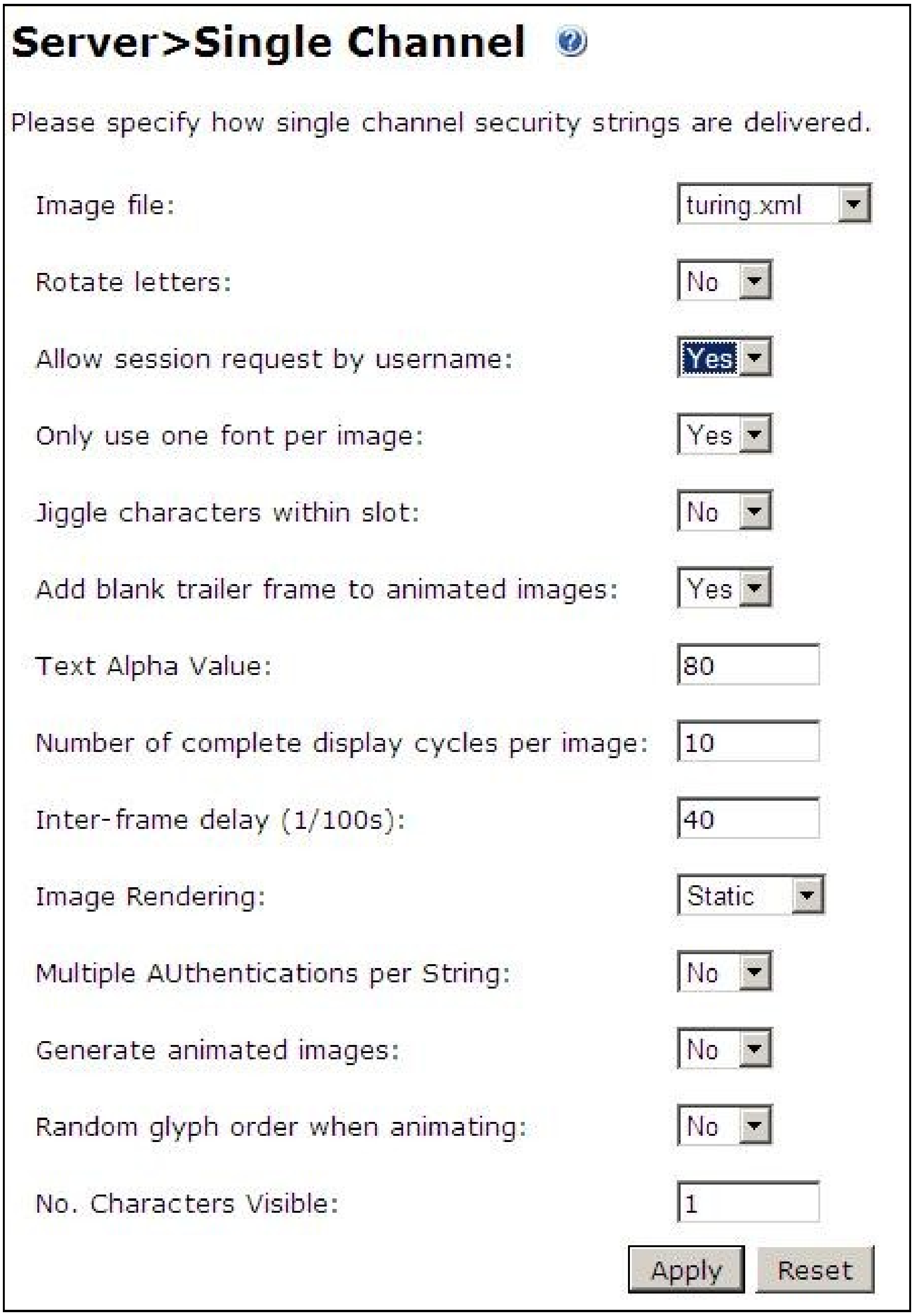
Name: local
Hostname/IP: 127.0.0.1
Shared secret: ●●●●●●●●●●●●●●●●●●●●●●●
Group: ---ANY---
Authentication Modes: ALL

Name: IIS
Hostname/IP: 192.168.1.1
Shared secret: ●●●●●●●●●●●●●●●●●●●●●●●
Group: ---ANY---
Authentication Modes: ALL

Note that this creates a GINA menu item, but there are no configurable options, so is not selectable.

54.2 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.

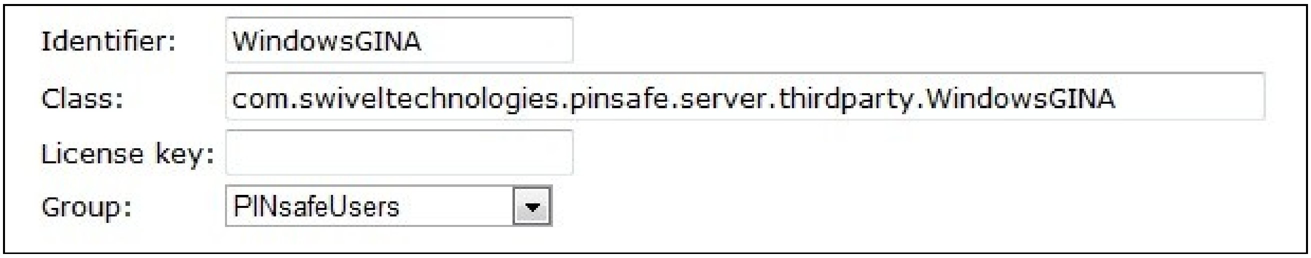
Image file:	turing.xml
Rotate letters:	No
Allow session request by username:	Yes
Only use one font per image:	Yes
Jiggle characters within slot:	No
Add blank trailer frame to animated images:	Yes
Text Alpha Value:	80
Number of complete display cycles per image:	10
Inter-frame delay (1/100s):	40
Image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

54.3 Create a Third Party Authentication

If offline authentication is to be allowed, a third party authentication must be created with an Identifier of WindowsGINA. (Even though the GINA is not part of Credential Provider the third party authentication module is still used and must be configured).

1. On the Swivel Management Console select Server/Third Party Authentication.
2. For the Identifier Name enter: WindowsGINA (Even though the GINA is not used, this must be entered as WindowsGINA).
3. For the Class enter: com.swiveltechnologies.Swivel.server.thirdparty.WindowsGINA.
4. For the License Key, leave this empty as it is not required.
5. For the Group select a group of users (Note: the option Any cannot be selected).
6. Click Apply to save the settings.

To allow offline authentication to be made a successful authentication must be made with the third party authentication in place.



Identifier: WindowsGINA

Class: com.swiveltechnologies.pinsafe.server.thirdparty.WindowsGINA

License key:

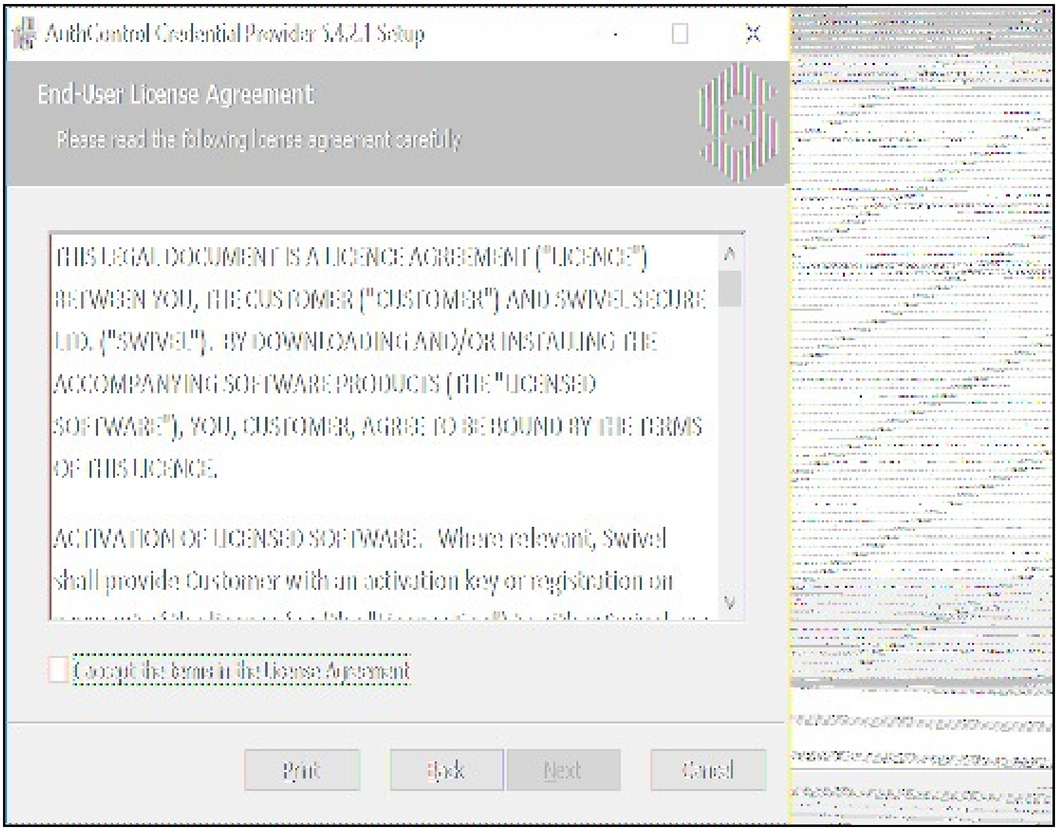
Group: PINsafeUsers

55 Microsoft Windows Swivel Credential Provider Installation

The Credential Provider is provided as a Microsoft Installer .msi file. You must run this as an administrator.

Double-click the .msi file to run it. Alternatively, you can install from the command line, using the msiexec command.

The first page is the licence agreement:



AuthControl Credential Provider 5.4.2.1 Setup
End-User License Agreement
Please read the following license agreement carefully
Print
Back
Next
Cancel

THIS LEGAL DOCUMENT IS A LICENCE AGREEMENT ("LICENCE") BETWEEN YOU, THE CUSTOMER ("CUSTOMER") AND SWIVEL SECURE LTD. ("SWIVEL"). BY DOWNLOADING AND/OR INSTALLING THE ACCOMPANYING SOFTWARE PRODUCTS (THE "LICENSED SOFTWARE"), YOU, CUSTOMER, AGREE TO BE BOUND BY THE TERMS OF THIS LICENCE.

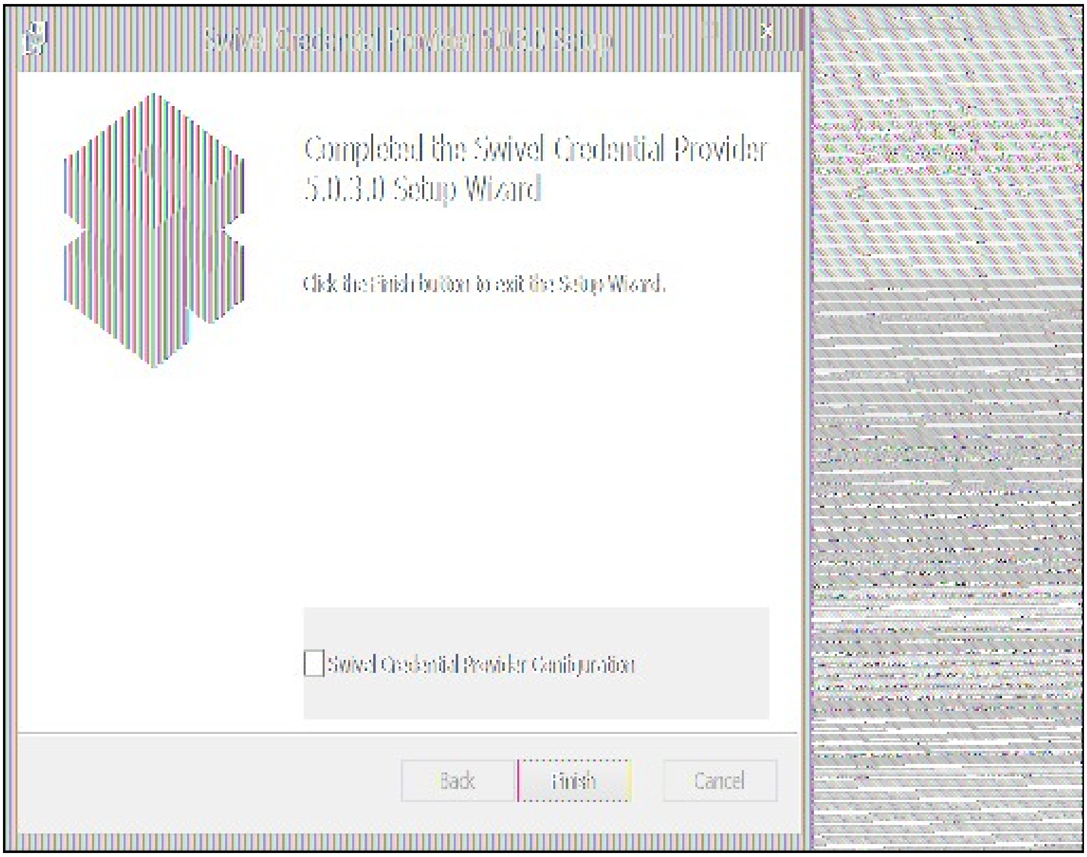
ACTIVATION OF LICENSED SOFTWARE. Where relevant, Swivel shall provide Customer with an activation key or registration on

□ I accept the terms in the License Agreement

Read the licence agreement (yeah, right!), and check the box to acknowledge it. Click Next to continue.

The application will be installed to C:\Program Files\Swivel Secure\Swivel Credential Provider. If you have reconfigured the program files directory elsewhere, it will be installed there, but otherwise you cannot control where the application is installed.

When the install has completed, the following dialog is shown:



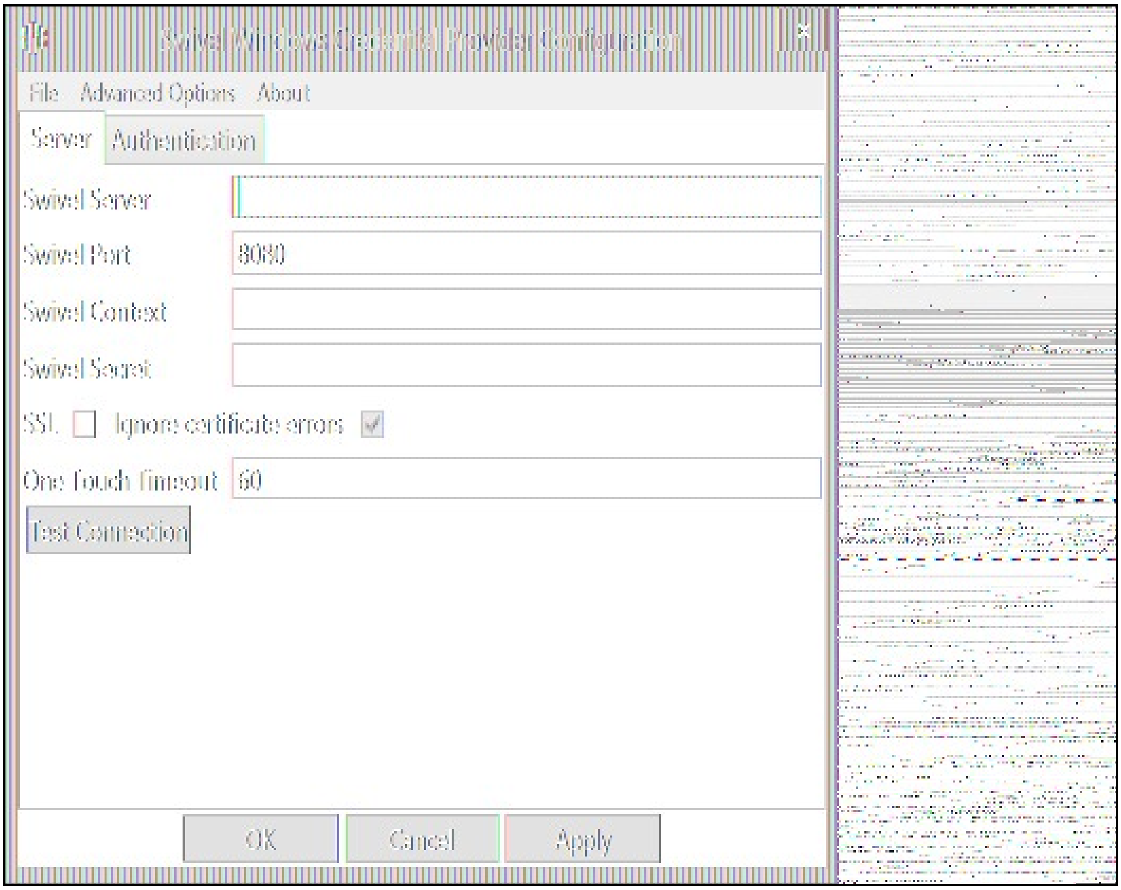
Completed the Swivel Credential Provider 5.0.3.0 Setup Wizard

Click the Finish button to exit the Setup Wizard.

□ Swivel Credential Provider Configuration

55.1 Windows Swivel Credential Provider configuration

55.1.1 Server



Swivel Server

Swivel Port 8080

Swivel Context

Swivel Secret

SSL □ Ignore certificate errors ☑

One Touch Timeout 60

Server: The Swivel virtual or hardware appliance or server IP or hostname. To add resilience, use the VIP on a swivel virtual or hardware appliance. See VIP on PINsafe Appliances.

NOTE: it has been observed in testing that DNS is not always available when logging on. It is therefore recommended that you use IP address, rather than host name in this section.

Port: The Swivel virtual or hardware appliance or server port.

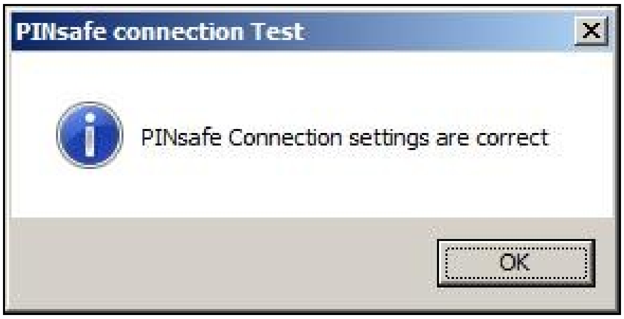
Context: The Swivel virtual or hardware appliance or server installation instance.

Secret: and **Confirm Secret:** A shared secret which must be entered onto the Swivel virtual or hardware appliance or server.

Use SSL The Swivel server or virtual or hardware appliance uses SSL communications.

Accept self signed SSL certificates Check this box if Use SSL is enabled, and you do not have a commercial certificate on your Swivel server (or a certificate signed by an authority that the client machine trusts). You should also check this box if you are using IP address rather than host name, as recommended above.

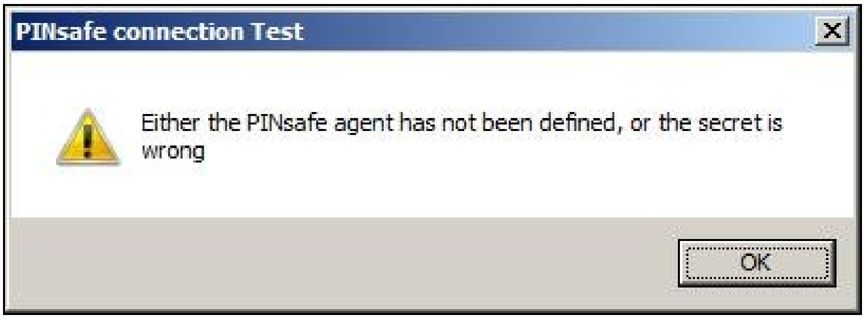
Test Connection Tests link to Swivel server. A correct configuration should produce a dialogue box with **Swivel Connection settings are correct.**



PINsafe connection Test

PINsafe Connection settings are correct

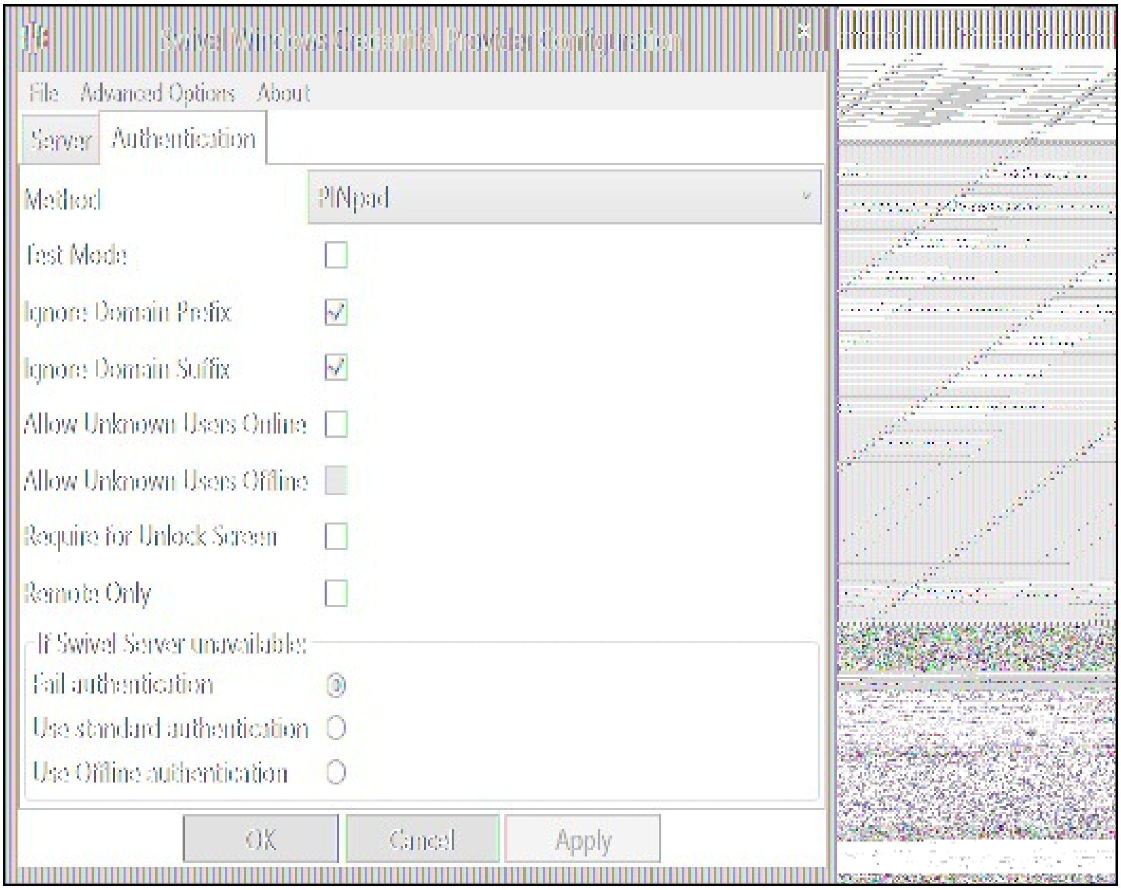
Incorrect settings will produce a dialogue box with **Either the Swivel agent has not been defined, or the secret is wrong**, Please check that the machine can contact Swivel and that the entered settings are correct.



PINsafe connection Test

Either the PINsafe agent has not been defined, or the secret is wrong

55.1.2 Authentication



Method: PINpad

Test Mode □

Ignore Domain Prefix ☑

Ignore Domain Suffix ☑

Allow Unknown Users Online □

Allow Unknown Users Offline □

Require for Unlock Screen □

Remote Only □

If Swivel Server unavailable:

Fail authentication ●

Use standard authentication ○

Use Offline authentication ○

Method Select the method of authenticating with Swivel, see above.

Test Mode With test mode the user can switch to a standard authentication, see below.

Ignore Domain Prefix Swivel will Remove any domain prefix (domain\username) before matching username. This does not affect Windows authentication usernames.

Ignore Domain Suffix Swivel will Remove any domain suffix (username@domain) before matching username. This does not affect Windows authentication usernames.

Allow Unknown Users Online If the username is not recognized by Swivel, the user can authenticate using Windows credentials only. Any Swivel OTC entered will be ignored. If the user is known then they must authenticate using Swivel authentication.

Allow Unknown Users Offline If Swivel is not found and the user has not authenticated with Swivel before then the user can authenticate using Windows credentials only.

Require for Unlock Screen Shows the selected authentication method on the unlock screen.

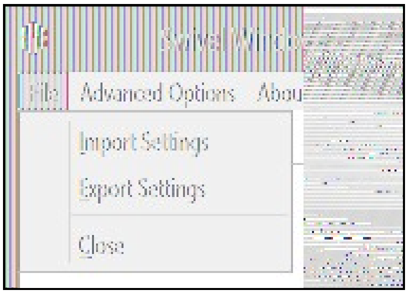
Remote Only The selected authentication method will only be shown for users logging into the machine remotely.

If Swivel unavailable, Fail authentication If the Swivel server cannot be contacted then authentication will fail.

If Swivel unavailable, Use standard authentication If the Swivel server is unavailable use standard authentication, the OTC field is displayed but ignored.

If Swivel unavailable, Use offline authentication If the Swivel server cannot be contacted a locally generated Turing image can be used for authentication. If this option is enabled, users will be able to force offline mode using a checkbox on the login dialog. (Only works for single channel authentication methods)

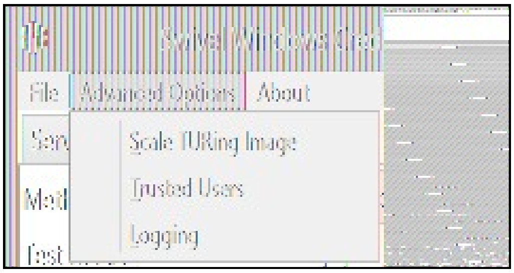
55.1.3 File menu



Export Settings Export settings as an XML file. These can be used to import settings elsewhere.

Import Settings Import settings from an XML file exported elsewhere.

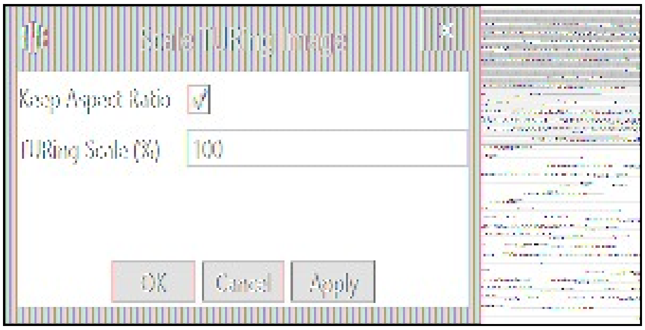
55.1.4 Advanced Options



55.1.4.1 Scale TURing Image

Scale TURing Image... Opens a dialog to let you scale the size of the TURing shown.

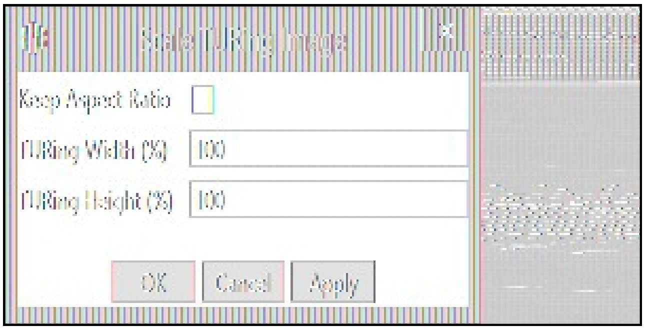
If **Keep Aspect Ratio** is selected then select the scale (%) of the TURing.



Keep Aspect Ratio ☑

TURing Scale (%) 100

If its not selected then you can select the width and hight independently.



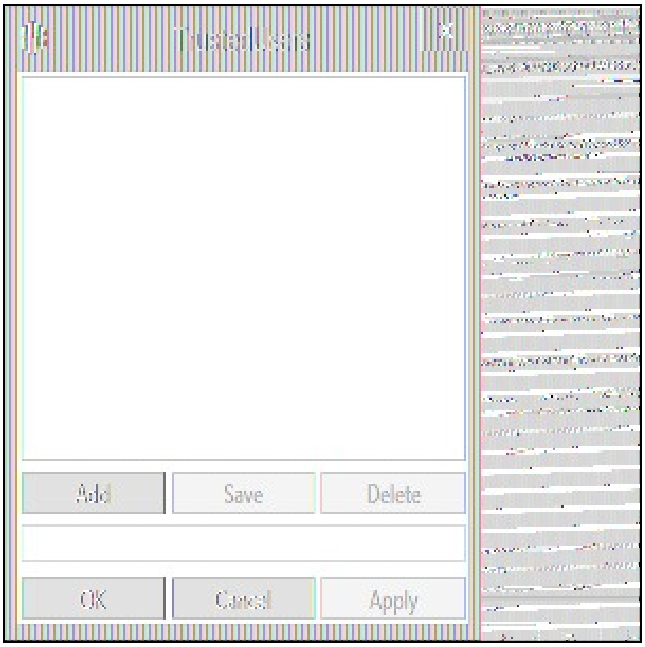
Keep Aspect Ratio □

TURing Width (%) 100

TURing Height (%) 100

55.1.4.2 Trusted Users

""Trusted Users"" Lets listed users Authenticate without Swivel.



To add a trusted user you must first click ""Add"" then enter the username in the text-box and click ""Save"", repeat these sets to add more users.

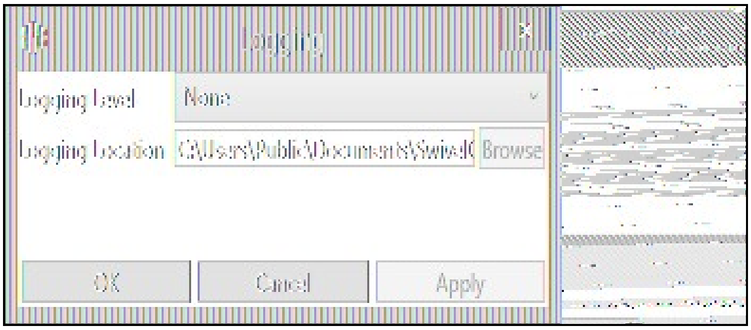
To edit a username select the username from the list, change the name in the text-box and click ""Save"".

To delete a username select the username from the list and press delete.

Make sure that the ""Apply"" or ""OK"" button to save these settings.

55.1.4.3 Logging

""Logging"" change settings relating to logging, recommended to be turned off unless problem are found.



Logging Level None

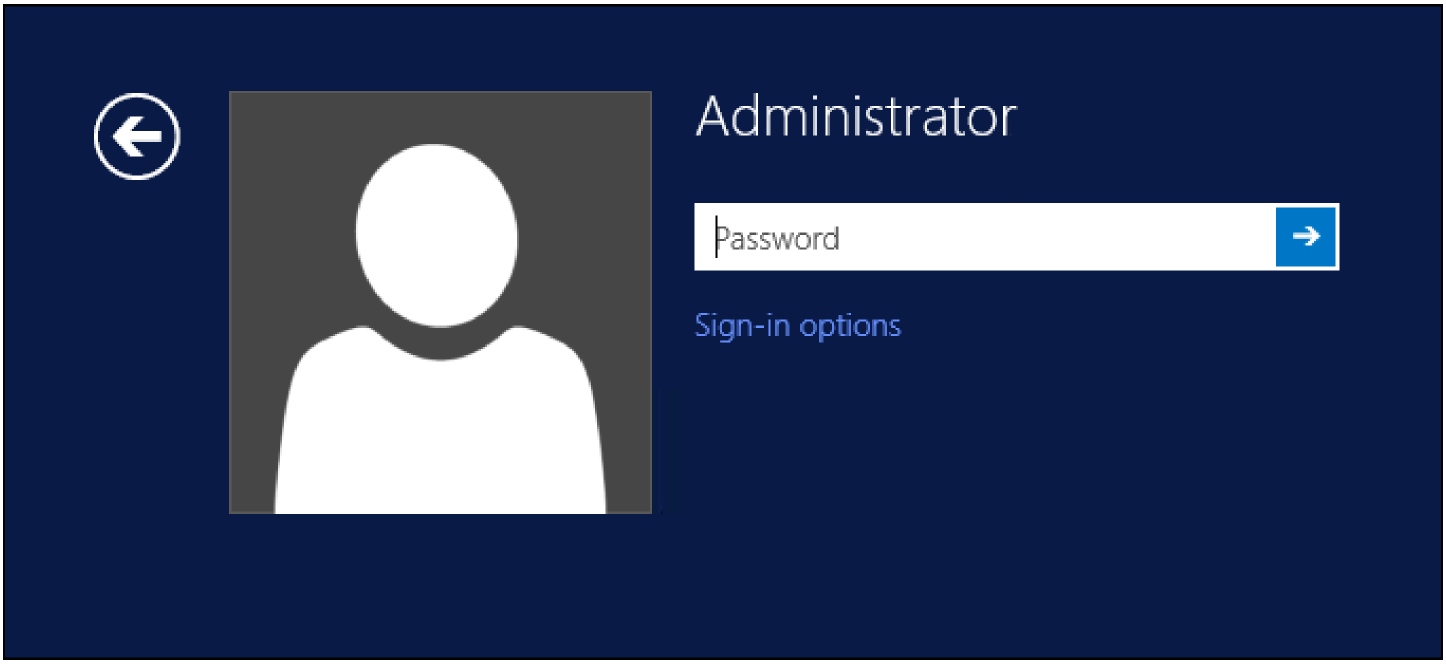
Logging Location C:\Users\Public\Documents\Swivel(

""Logging Level"" The account of message that will be logged.

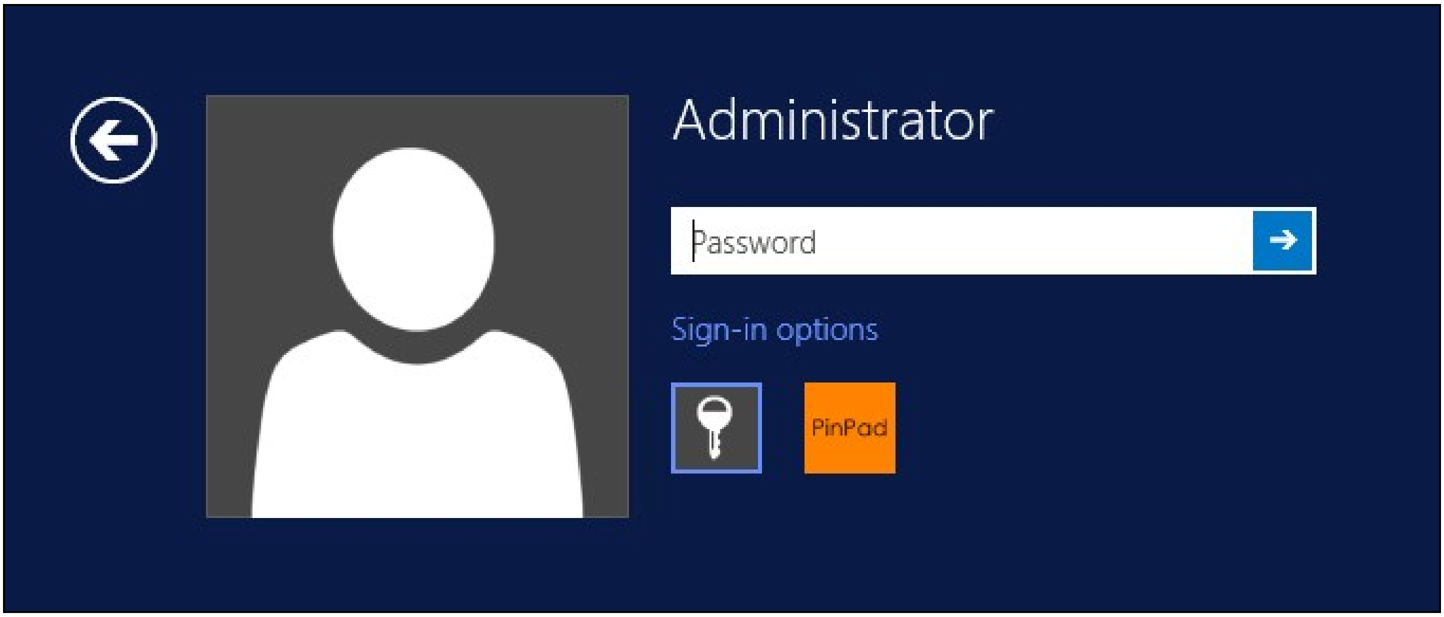
""Logging Location"" The location the logs will be created, this must be somewhere any account has access to.

55.2 Test Mode

With Test Mode enabled the user will be able to select how they will authenticate



The **Sign-in options** button is shown to let users select from the list which method they would like to use.



The last successful authentication method will be selected by default when the credential is loaded.

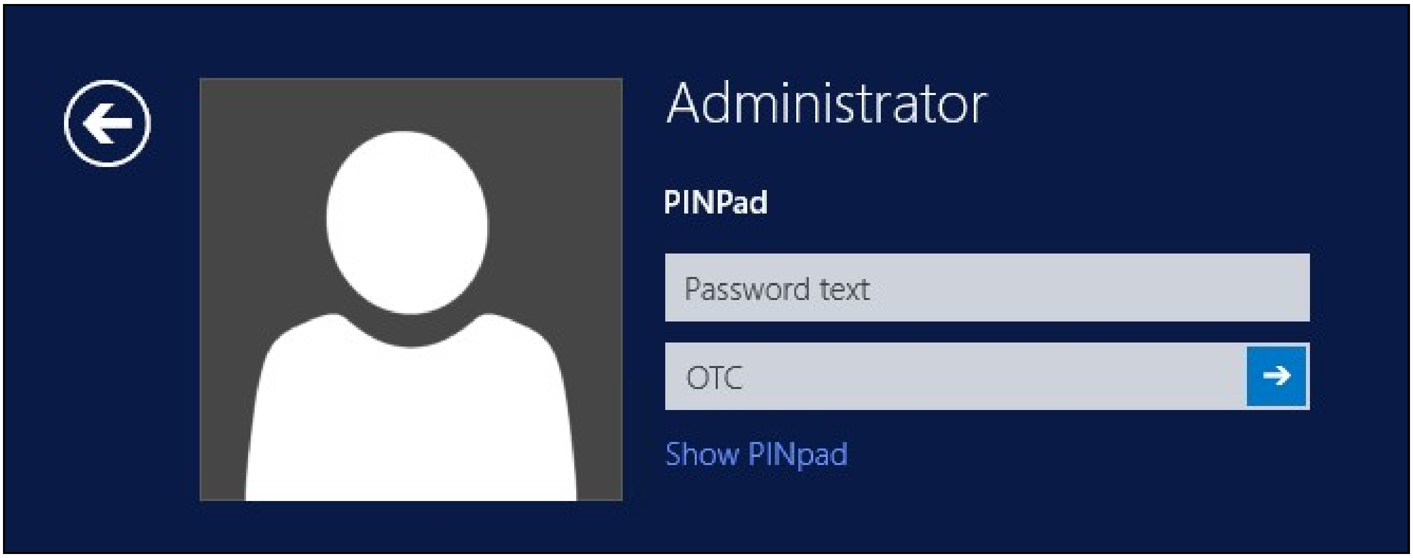
55.3 Importing Configurations

You can import credentials exported from other installations using the Import Settings menu item.

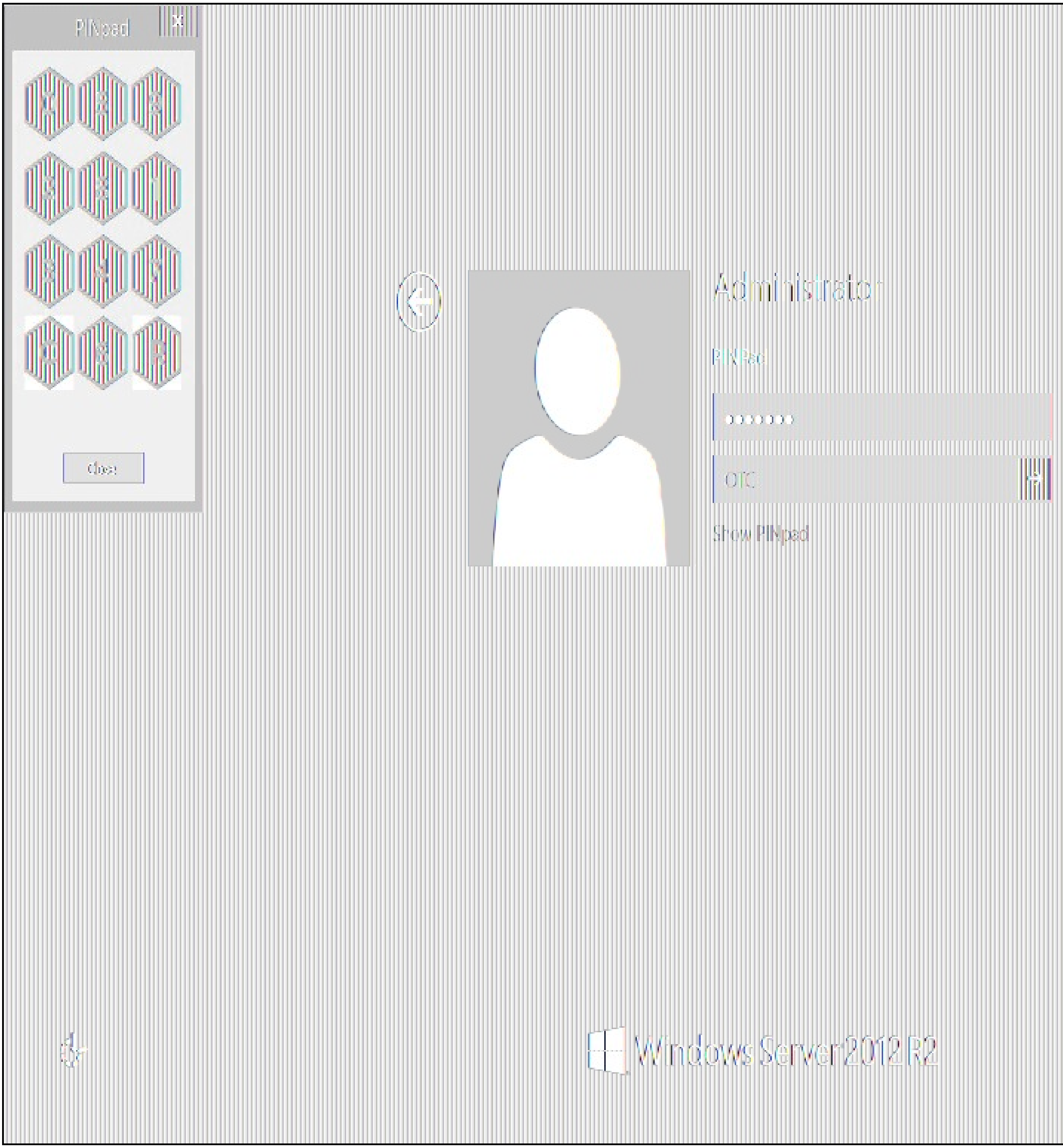
56 Verifying the Installation

This will be an example of one of the credentials.

At the windows login screen a password and OTC login field should be available with a "Show PINpad" Button.



Pressing the "Show PINpad" button will generate a PINpad image for authentication. The Swivel log should show a session request message: *Session started for user: username.*



A successful login should appear in the Swivel log: *Login successful for user: username*.

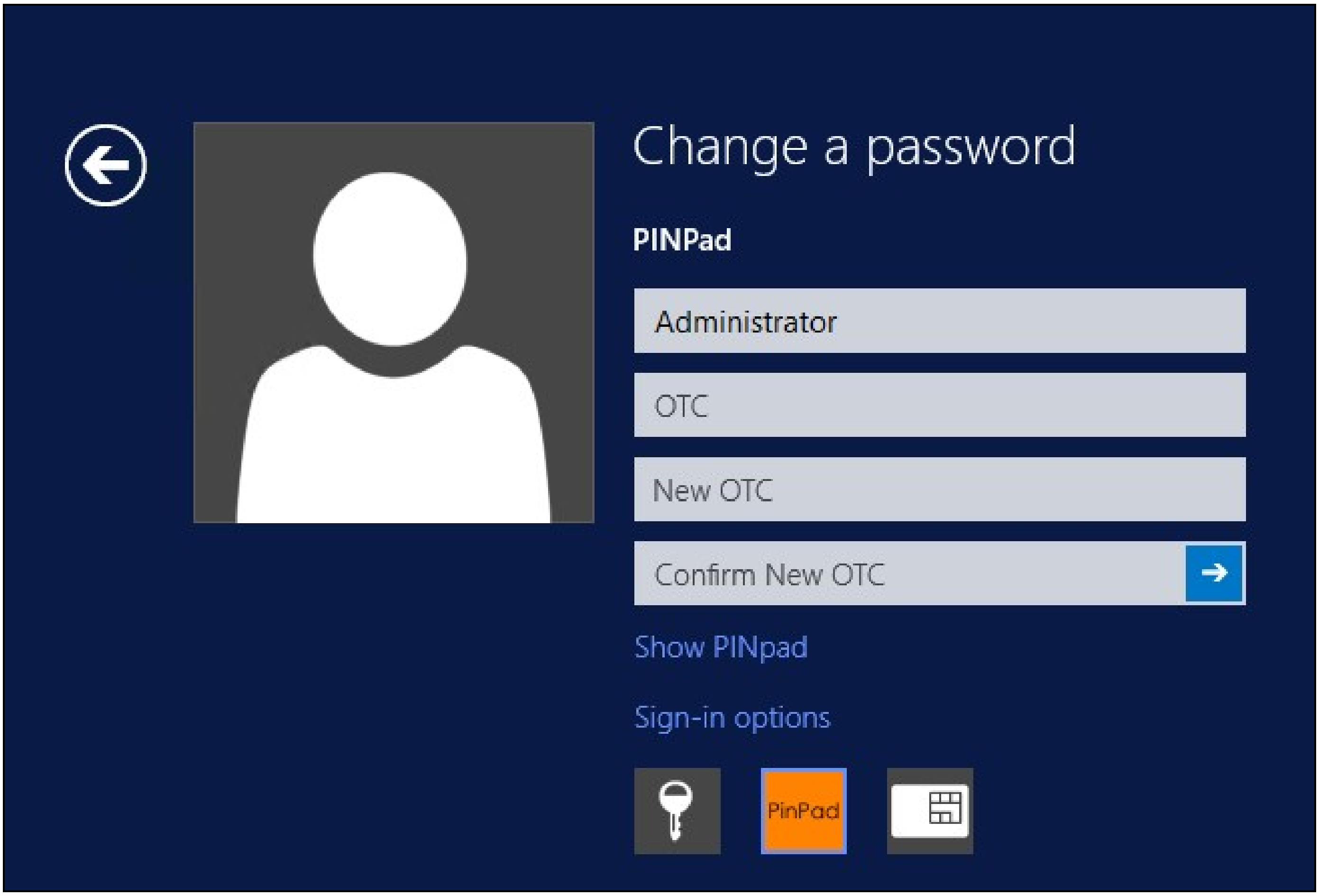
A failed login should not allow a login, and the following message should be displayed in the Swivel log: *Login failed for user: username*.

57 ChangePIN

A user is usually able to change the password by using the Ctrl-Alt-Del keys (Ctrl-Alt-End for remote sessions). With the Swivel Credential Provider installed, an additional option exists when the Change Password is selected, by clicking on the "Sign-in options" button and selecting the Swivel credential. This will not function for Offline authentication.

With Swivel authentication a user never changes enters PIN and this is true for ChangePIN. A user enters their current OTC, and then enters an OTC for what they wish their new PIN to be. PIN enforcement may be in place to the Swivel server to prevent the choosing of poor PIN numbers.

A user may use a single channel image or a dual channel security string to change their PIN.

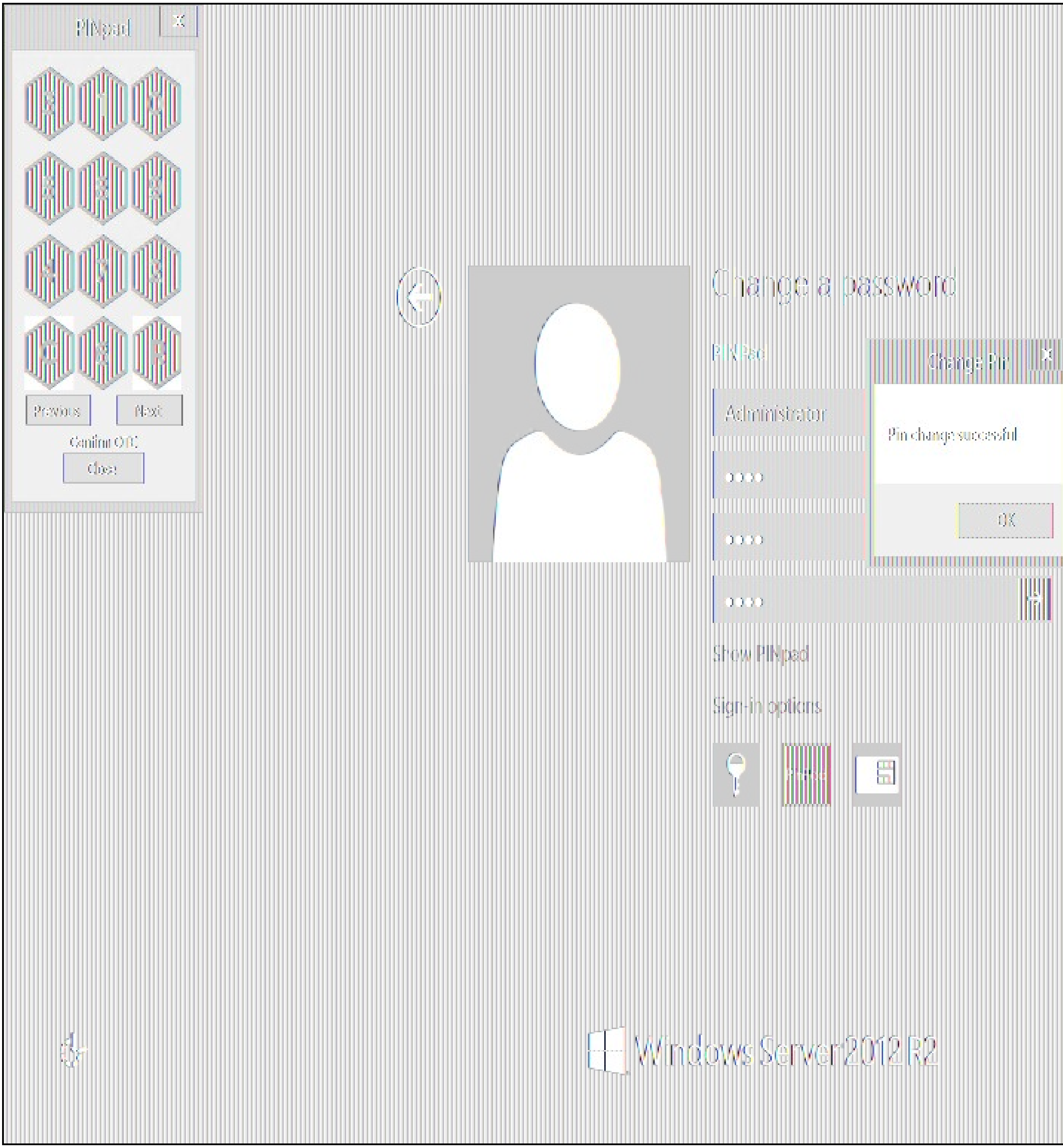


Change a password

PINPad

Administrator

A successful Change PIN will show the message **Your PIN was changed successfully**, the Swivel server will also display in the logs a changePIN message **Change PIN successful for user: username**.



Pin change successful

Other Changes to PINpad are that the PINpad dialog has buttons to select which text-box the numbers will be entered and text to show which text-box is currently selected.

58 Uninstalling the Swivel Integration

Use the Uninstall option from the Program menu, right click on the Windows Credentials provider and click on Uninstall. Note that uninstalling and reinstalling the Credential Provider will remove the settings, so if you need to reinstall at any point, make sure you have an exported settings file saved.

58.1 Disabling the Credential Provider

If the Credential Provider needs to be disabled temporarily, use the following procedure:

If the credential provider is preventing the machine starting normally, boot the machine into safe mode and log in as an administrator.

Try each of the following in turn. Only one of the following is required, so use the first one that works.

- Run the Swivel Login Configuration and edit the settings to disable the provider.
- Using regedit.exe, edit the following registry keys. Add a DWORD value named "disabled" to each one, set to 1. To re-enable it, you can set disabled to 0, rather than deleting the value.
    - "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers\{6AD69A51-00E9-4BE9-A3D6-9D26255DA4E1}"
    - "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Authentication\Credential Provider Filters\{6AD69A51-00E9-4BE9-A3D6-9D26255DA4E1}"
- Uninstall the Credential Provider.
- Using regedit.exe, remove the following registry keys:
    - "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers\{6AD69A51-00E9-4BE9-A3D6-9D26255DA4E1}"
    - "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Authentication\Credential Provider Filters\{6AD69A51-00E9-4BE9-A3D6-9D26255DA4E1}"
    - "HKEY_CLASSES_ROOT \CLSID\{6AD69A51-00E9-4BE9-A3D6-9D26255DA4E1}"

59 Known Issues and Limitations

- The Swivel Windows Credential Provider does not support the use of Animated gifs for Single Channel authentication.
- It has been observed in testing that DNS is not always available when logging on. It is therefore recommended that you use IP address, rather than host name for the Swivel server.
- Local authentication only works in single channel and OATH modes: the dual channel strings are not available offline.
- If the user gets an online TURing with a different scale then gets an offline TURing, the TURing is broken, the fix is to close the dialog and request an new TURing.
- If **Allow Unknown Users Offline** is enabled then users that have not previously authenticated to Swivel online can bypass Swivel by checking the offline box and authenticating with AD only.
- On Windows server 2012 R2 there is an update from Microsoft to fix an issue where dialogues will not be displayed, please ensure that windows update 2919355 is installed.
- Local authentication does not know if a users PIN has expired or even if the account is locked or deleted. Once a user has successfully authenticated they are allowed offline until their offline strings are deleted or the offline option is deselected.

60 Windows Credential Provider

61 Introduction

Swivel Secure AuthControl Desktop (formerly Windows Credential Provider) is used in the desktop operating systems Windows 8, 10 and 11 and the server operating system Windows Server 2012 and 2019. For integration with Windows Vista and 7 and Server 2008, use version 5.3 or later, or see Microsoft Windows Credential Provider Integration (Legacy OS).

Users can authenticate using the Swivel Credential Provider allowing 2FA (Two Factor Authentication), or strong authentication at the Windows Logon. Offline authentication is also supported for single Channel authentication, following at least one successful authentication against the Swivel server with Third Party Authentication configured.

Supported methods are:

- **TURing** Lets the user sign into windows by using TURing.
- **PINpad** Lets the user sign into windows by using PINpad.
- **On Demand** Lets the user sign into windows by requesting a security string to their preferred method (SMS or email). More information.
- **Other Two Factor** Lets the user sign into windows by entering a one-time code based on a security string received previously or OATH token.
- **Push** for Windows 8 and Server 2012 R2 onwards.
- **Fingerprint** (From v5.4.2 onwards and requires AuthControl Sentry v4.0.5) Lets the user sign into windows using Biometric Fingerprint.

61.1 Downloads

Latest Release Versions:

Swivel AuthControl Desktop 64-bit version MSI 5.7.42.1 NOTE: this is the latest release. Documentation has not yet been updated to reflect the changes in this version.

Swivel AuthControl Desktop 64-bit version MSI 5.7.31.1

Swivel AuthControl Desktop 64-bit version executable 5.7.31.1

Swivel AuthControl Desktop 32-bit version MSI 5.7.31.1

If you have difficulties downloading these files, please contact teamsupport@swivelsecure.com for an alternative method.

The two versions install identical products. The difference is that the executable will copy the current settings from version 5.x and reapply them after installation. The MSI will always overwrite the settings with either blank settings or the contents of acd.xml or scps.xml if provided (see later). As of 5.7, old settings are no longer removed on upgrade, but that only applies to the version that is uninstalled, so upgrading to 5.7 from an earlier version will still remove the old settings.

Settings from versions earlier than 5 cannot be imported automatically on upgrade: you will need to export the settings, uninstall the version 4 credential provider and then install the new version and import the settings.

Important: the Credential Provider requires Microsoft Visual Studio C++ redistributable to work. Recent operating systems already include this, but it will need to be installed on older operating systems if it has not already been installed. You can retrieve it from here. If you have already installed the credential provider, it is not necessary to uninstall it before installing the redistributable.

Note that this article has not yet been fully updated to reflect the changes in version 5.6 or 5.7. See below for release notes.

Older Versions:

Swivel AuthControl Desktop 64-bit version executable 5.6.10.1

NOTE: we discovered a bug in version 5.6.3.1 whereby the stored secret fails to be decrypted at unpredictable times. We therefore recommend using the following version, 5.6.10.1, which stores the secret unencrypted. This version also fixes a problem with Push authentication, which did not work in 5.6.3.1 or 5.6.9.1.

Swivel AuthControl Desktop 64-bit version MSI 5.6.10.1

Swivel AuthControl Desktop 64-bit version executable 5.5.11.1

Swivel AuthControl Desktop 64-bit version MSI 5.5.11.1

Swivel AuthControl Credential Provider 64 bit version 5.4.4.2

Swivel AuthControl Credential Provider 64 bit version 5.4.3.2

Swivel AuthControl Credential Provider 64 bit version 5.4.2.1

Swivel AuthControl Credential Provider 64 bit version 5.3.1.5

Swivel Windows Credential Provider 64 bit version 5.1.1

Swivel Windows Credential Provider 64 bits version 5.3.0.1

61.2 Swivel Credential Provider FAQ

Q). Does the Credential provider support offline authentication?
A). Offline authentication is permissible for Swivel users who have previously authenticated to the device. Offline local authentication is a

Q). Do all users have to authenticate using Swivel?
A). Swivel has the option to *Allow Unknown Users*. Users known to Swivel will be prompted for authentication in this instance. There is also a

Q). Is it possible to define users who do not have Swivel authentication?
A). Yes either by the *Allow Unknown Users* for non Swivel user authentication or by adding the user to the "Trusted Users" list

Q). Is it possible to login without AD password?
A). Yes, there is an option to log in without the AD password, but you must previously have logged in with the AD password.

62 Prerequisites

Swivel version 3.11.3 or later. For password caching, version 4.0.4 or later is required.

Connectivity to Swivel server during installation (with Third Party Authentication for GINA enabled).

Microsoft Windows 8 (including 8.1), 10 and 11 or Windows Server 2012 (including R2) and Windows Server 2019. Version 5.3 and later have backward support for Windows Vista or later, and Windows Server 2008 or later.

Microsoft.Net Framework version 4.5.

AuthControl Windows Credential Provider 64-bit - see above for links.

A separate Swivel Credential Provider license is not required, but the users authenticating to Swivel must be licensed.

User with AD account and valid password.

63 Baseline

Swivel 3.11.3

Windows 8, 10, 11 Server 2012 R2, Server 2019.

64 Installation

64.1 Basic Installation

To install the Swivel Windows Credential Provider run the installer and follow the on-screen instructions. At the end of the on-screen instructions you will be given the option to launch the configuration program to customise the Credential Provider. This can normally be found in the start menu under "Swivel Secure" and in "C:\Program Files\Swivel Secure\Swivel Credential Provider".

After installation and configuration:

- On Desktop Windows versions the computer must be restarted.
- On Windows Server versions the Administration account can be signed out rather than doing a full restart.

64.2 Multiple Installation

If a configured Swivel Windows Credential Provider has been set up then the settings can be imported automatically on new installations.

1. Extract the settings using the existing Credential Provider from the "File > Export Settings" option, naming the output file either "acd.xml" or "scps.xml". Alternatively, you can export the settings as encrypted and name the file "acd.enc". Note that for the file to be imported automatically you must not specify a password (the default password will be used).
2. Copy this file and the installation file onto the new computer. They must be in the same location (for example both files on the desktop).
3. Run the installation as described above and the settings will be automatically loaded during installation.

NOTE: in version 5.6.9.1 and later builds, the configuration file can be named "acd.xml" instead of "scps.xml". The latter will be used by preference if both files exist.

Alternatively, you can build an pre-configured installer executable. Please contact Swivel Secure support to get the necessary build script.

1. Extract the files from the zip link above into a folder
2. Extract the settings using the existing Credential Provider from the "File > Export Settings" option, naming the output file "acd_in.xml".
3. Replace acd_in.xml in the extracted folder with your customised one
4. Compile the executable using ACDInstall.nsi with Nullsoft installation system. If you don't have a copy of Nullsoft, it can be downloaded from here.

65 Release Notes

65.1 AuthControl Desktop 5.7

65.1.1 New Features

65.1.1.1 Generate offline strings outside ACD

The credential manager application allows you to authenticate to Sentry and to download offline security strings. These strings can then be exported to another machine and used there to authenticate users offline

65.1.1.2 All displayed text is customisable

The configuration program allows you to customise the text displayed in the Windows credential. Additionally, you can copy the customised text to the same folder as the ACD installer and it will be imported to the target machine on installation. Currently, only one set of strings is possible per installation, but it is hoped in the future to support multiple languages.

65.1.1.3 Proxy for Sentry connections

You can optionally specify an HTTP proxy for connecting to the Sentry server.

65.1.1.4 Enhancements to Import and Export Settings

Version 5.6 introduced encrypted settings files using a password. Version 5.7 expands on this by allowing for a fixed password, used automatically if encryption is selected but no password is given. Automatic import of settings on installation works with encrypted settings, provided the fixed password is used for encryption. Automatic import of settings will look for the following file names, in this order:

- scps.xml (previously the only name that worked)
- acd.xml
- scps.enc ? assumes the settings are encrypted using the default password
- acd.enc ? as above

Note that the MSI installation no longer deletes the old settings on uninstallation. However, this only applies to upgrading FROM 5.7 or reinstalling. Since the settings are deleted by uninstalling the old version, upgrading from a version older than 5.7 will still remove the old settings.

65.1.1.5 Change PIN for locked users

Previously, if a user attempted to log in and the account was locked due to PIN expiry, authentication would fail. Now, the PIN change screen is shown. It should be noted that in order to change a PIN when the account is locked, you need Sentry version 4.1.4 or later.

65.1.1.6 Optionally, OTC field is not shown initially for Other User

It is possible to specify that the OTC field is not initially shown for the ?Other User? credential. This is the credential that is shown with an empty username field. In the case where users unknown to Sentry are permitted to log on without MFA, it might be preferable not to show the OTC field, in case it is not required. If a user logs in with username and password, and it is subsequently discovered that an OTC is required, the login form is redisplayed with the OTC field.

65.1.1.7 Offline OATH works with On Demand credential

Previously, offline OATH only worked if the authentication method was set to ?Other Two-Factor? (and that not reliably ? see bug fixes). Now it also works with ?On Demand?.

65.1.2 Bug Fixes / Improvements

65.1.2.1 Error messages displayed for PIN change errors

Previously, if an error occurred in the PIN change screen, no message was displayed. The screen was simply redisplayed with no additional information. Now, an error is displayed on the screen indicating why the PIN change failed.

65.1.2.2 Improved configuration for Single Sign-On

In 5.6 and earlier, the use of Single Sign-On (SSO) to check if MFA is required was indicated simply by providing a port and context for SSO. This could result in the settings being entered when they were not really needed, just because the fields are there. Version 5.7 shows a check-box to indicate that SSO is active. Activating SSO will display a pop-up dialog requesting the SSO settings, which includes a host name as well as port and context, so the SSO server does not have to be the same as the Sentry Core.

65.1.2.3 Push authentication not working

Version 5.6 (prior to 5.6.10.1) did not support Push authentication due to incompatible changes in the code. Version 5.7 now supports Push correctly.

65.1.2.4 Offline OATH not working

Version 5.6 did not always work for OATH if the token details were stored locally. This was due to an error in the encryption code that affected several features. This has now been corrected.

65.1.2.5 Fixed problems with Secret not encrypting/decrypting on occasions

This problem was caused by the same encryption issue as the previous one. As a workaround, versions 5.6.9.1 and 5.6.10.1 were released with the secret being stored unencrypted, as it was in version 5.5 and earlier. Now that the encryption issue has been resolved, the secret is once again stored in encrypted format, although the encryption is not backward-compatible with 5.6, so copying the secret registry entry from 5.6 to 5.7 will not work. Exporting and importing will work, provided the secret is not encrypted in the export file.

65.1.2.6 Allow unknown users online

It was discovered that version 5.6 did not correctly handle the situation where users were not known to Sentry but could authenticate with password only. This has now been fixed.

66 Architecture

Swivel is installed as a Windows Credential Provider. When a Windows login is made, AD username and password is checked against AD and the username and Swivel OTC is sent to the Swivel server using XML authentication, or locally if offline authentication is enabled.

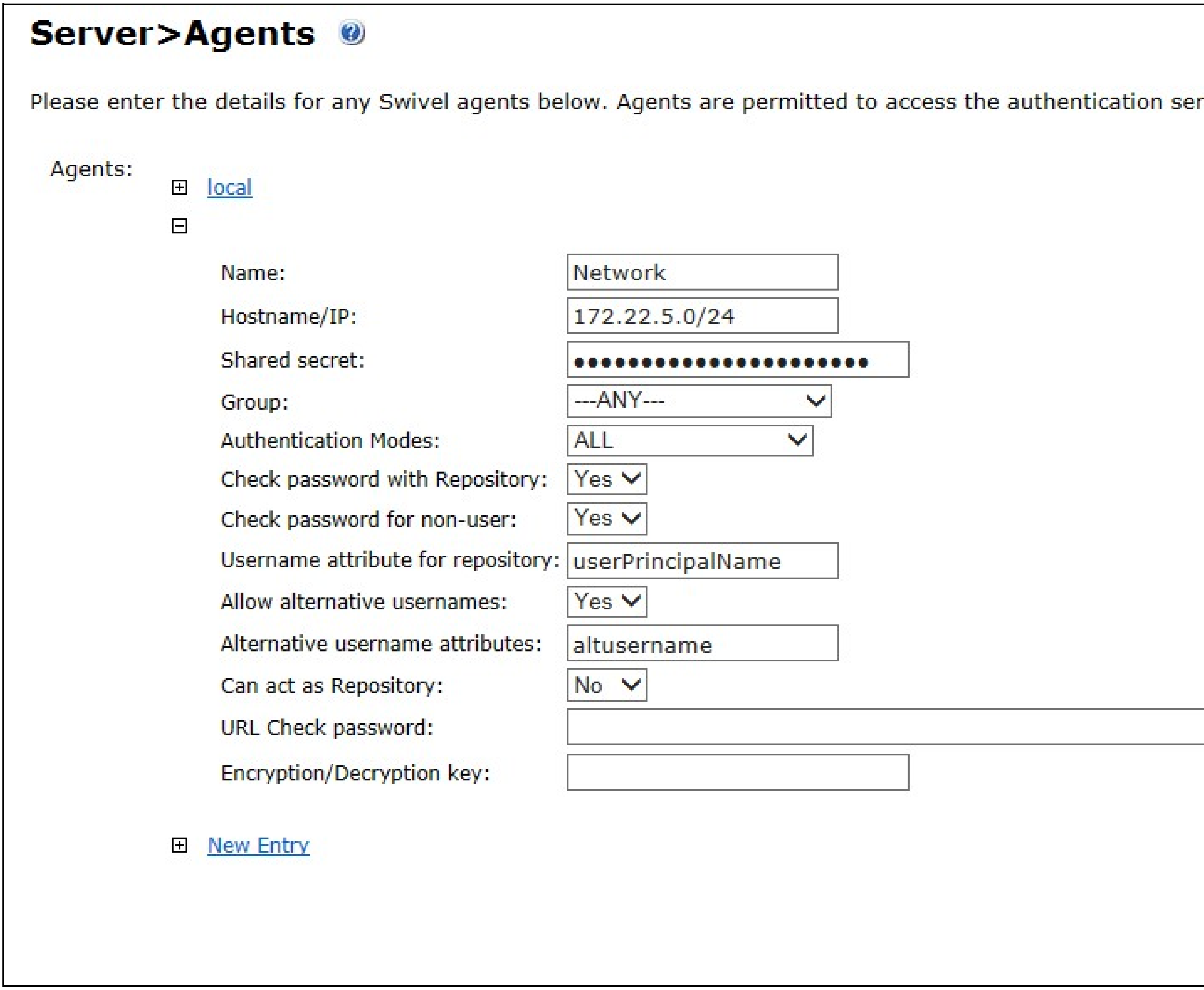
66.1 Offline Authentication

Swivel allows offline authentication using single channel or OATH, but not dual channel authentication. For offline authentication the user attempting to authenticate must have made at least one successful authentication against the Swivel server while Offline Authentication has been enabled. Swivel caches a limited number of strings for authentication: when one is shown then it's classed as used and will not be re-shown. If the user makes a successful offline authentication then the number of strings will be replenished: however if the user runs out of strings then they will need to authenticate online to get some more. Swivel Account lockout is disabled for Swivel offline authentication. ChangePIN will not function when the Swivel server is not contactable. Local authentication is always single channel, even if single channel is normally disabled. The exception is that OATH authentication is also supported offline, provided the user has previously authenticated online using the same token.

67 Swivel Integration Configuration

67.1 Configure a Swivel Agent

1. On the Swivel Management Console select Server/Agent.
2. Enter a name for the Agent.
3. Enter the Credential Provider IP address. You can use an individual IP address for the Credential Provider, such as 192.168.0.99, or you can specify an IP address range like 192.168.0.0/24, which means the first 24 bits, or 3 numbers, are significant or you (i.e. 192.168.0.x).
4. Enter the shared secret used above on the Credential Provider.
5. Select a group, or leave it as "Any" to allow all users to authenticate.
6. Click on Apply to save changes.



Server>Agents

Please enter the details for any Swivel agents below. Agents are permitted to access the authentication ser

Agents:

⊞ local

⊟

Name:	Network
Hostname/IP:	172.22.5.0/24
Shared secret:	••••••••••••••••••••••
Group:	---ANY---
Authentication Modes:	ALL
Check password with Repository:	Yes
Check password for non-user:	Yes
Username attribute for repository:	userPrincipalName
Allow alternative usernames:	Yes
Alternative username attributes:	altusername
Can act as Repository:	No
URL Check password:	
Encryption/Decryption key:	

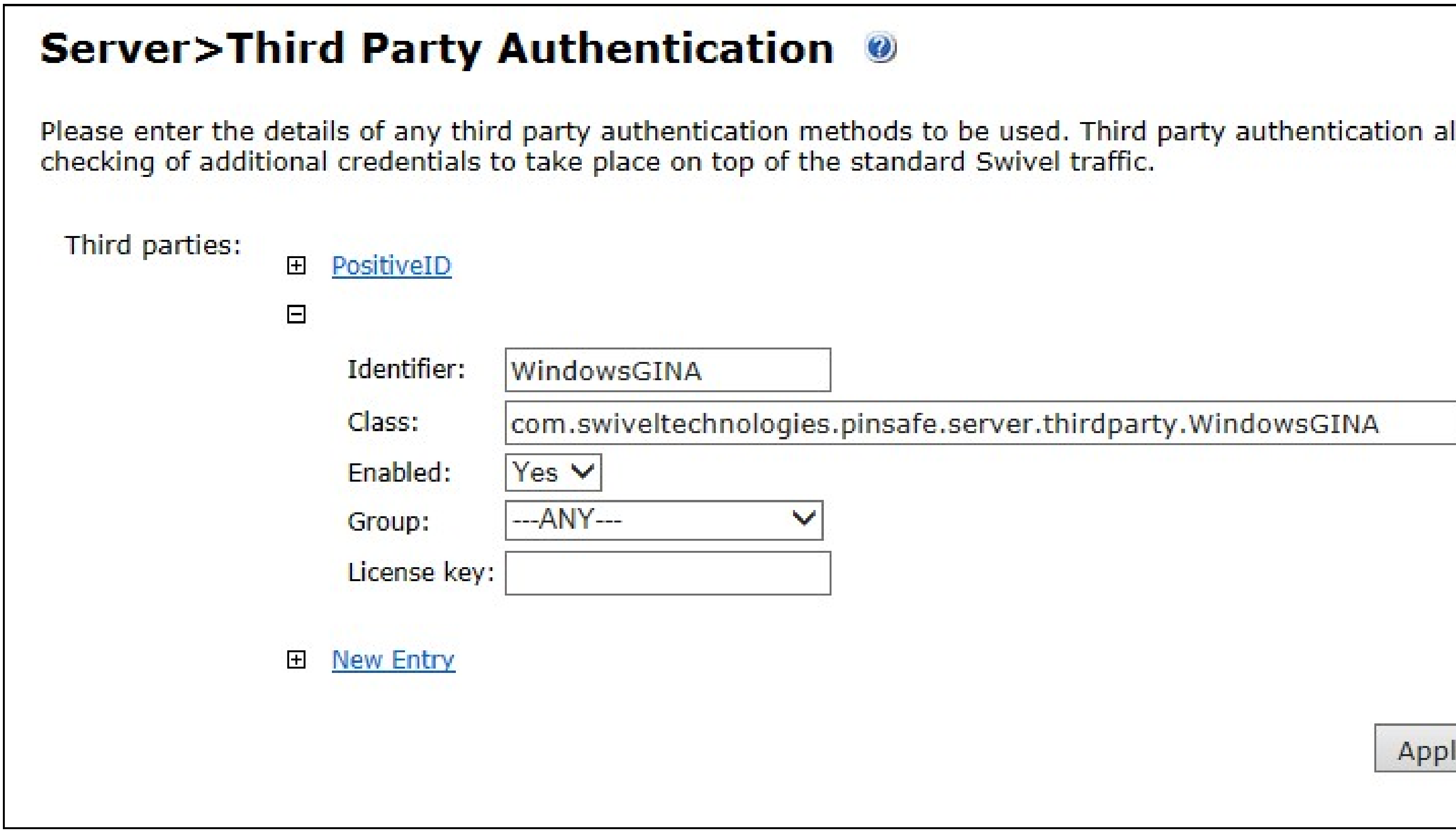
⊞ New Entry

Note that this creates a GINA menu item, but there are no configurable options, so is not selectable.

67.2 Create a Third Party Authentication

If offline authentication is to be allowed, a third party authentication must be created with an Identifier of WindowsGINA. The name must be exactly as shown. This entry should already exist, but check that the settings are as shown.

1. On the Swivel Management Console select Server/Third Party Authentication.
2. For the Identifier Name: WindowsGINA.
3. For the Class: com.swiveltechnologies.Swivel.server.thirdparty.WindowsGINA.
4. Ensure that Enabled is set to Yes.
5. For the Group select a group of users, or Any to allow any users to authenticate using this third party.
6. For the License Key, leave this empty as it is not required.
7. Click Apply to save the settings.



Server>Third Party Authentication

Please enter the details of any third party authentication methods to be used. Third party authentication al
checking of additional credentials to take place on top of the standard Swivel traffic.

Third parties:

⊞ PositiveID

⊟

Identifier: WindowsGINA

Class: com.swiveltechnologies.pinsafe.server.thirdparty.WindowsGINA

Enabled: Yes

Group: ---ANY---

License key:

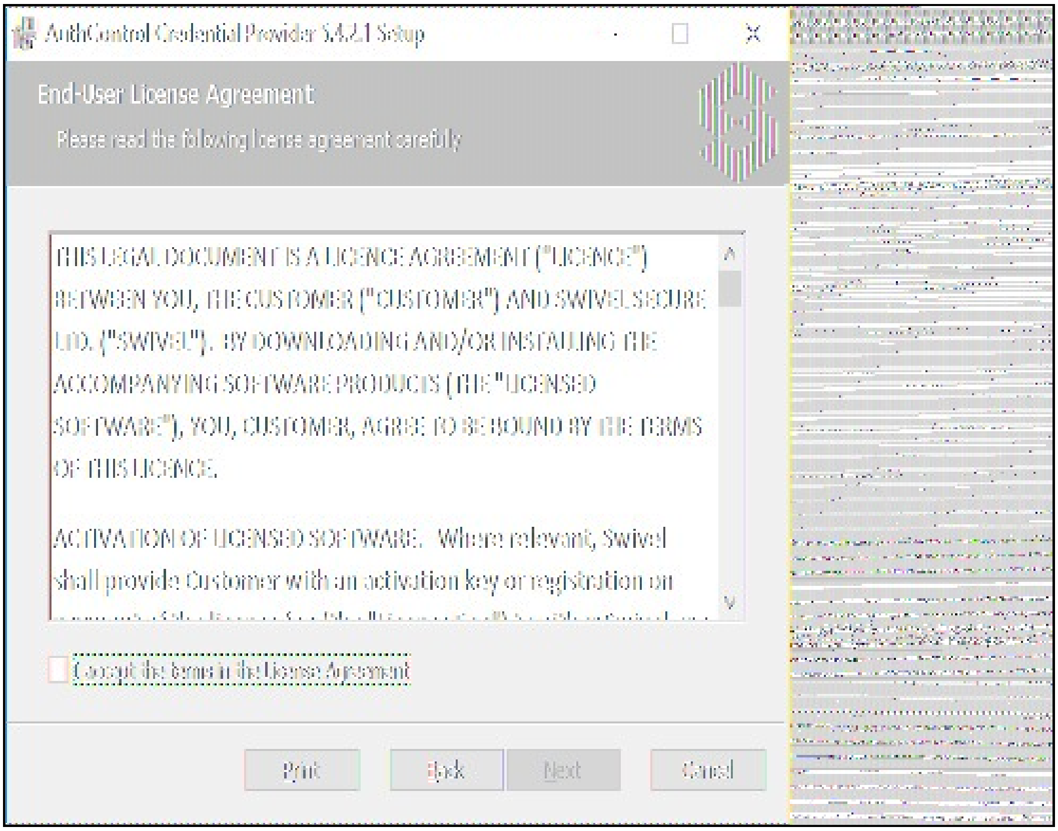
⊞ New Entry

68 Microsoft Windows AuthControl Credential Provider Installation

The Credential Provider is provided as a Microsoft Installer .msi file. You must run this as an administrator.

Double-click the .msi file to run it. Alternatively, you can install from the command line, using the msiexec command.

The first page is the licence agreement:



AuthControl Credential Provider 5.4.2.1 Setup
End-User License Agreement
Please read the following license agreement carefully
Print
Back
Next
Cancel

THIS LEGAL DOCUMENT IS A LICENCE AGREEMENT ("LICENCE") BETWEEN YOU, THE CUSTOMER ("CUSTOMER") AND SWIVEL SECURE LTD. ("SWIVEL"). BY DOWNLOADING AND/OR INSTALLING THE ACCOMPANYING SOFTWARE PRODUCTS (THE "LICENSED SOFTWARE"), YOU, CUSTOMER, AGREE TO BE BOUND BY THE TERMS OF THIS LICENCE.

ACTIVATION OF LICENSED SOFTWARE. Where relevant, Swivel shall provide Customer with an activation key or registration on

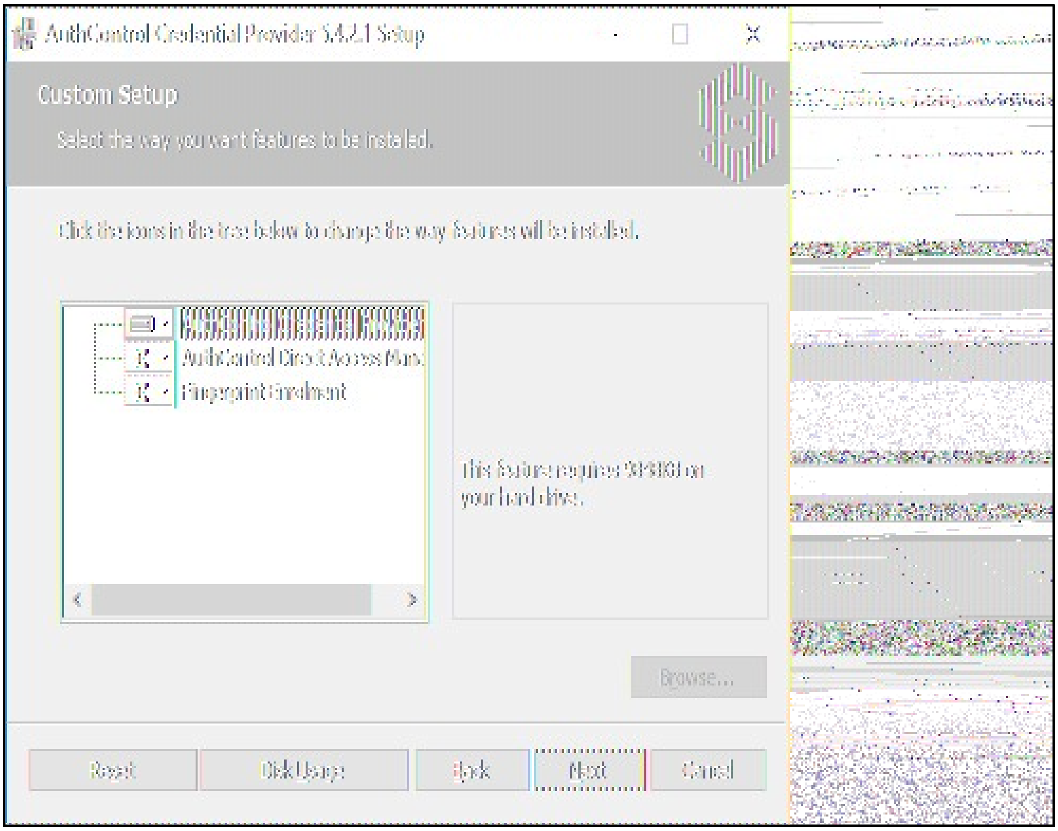
□ I accept the terms in the License Agreement

Read the licence agreement (yeah, right!), and check the box to acknowledge it. Click Next to continue.

Select the neccessary addons:

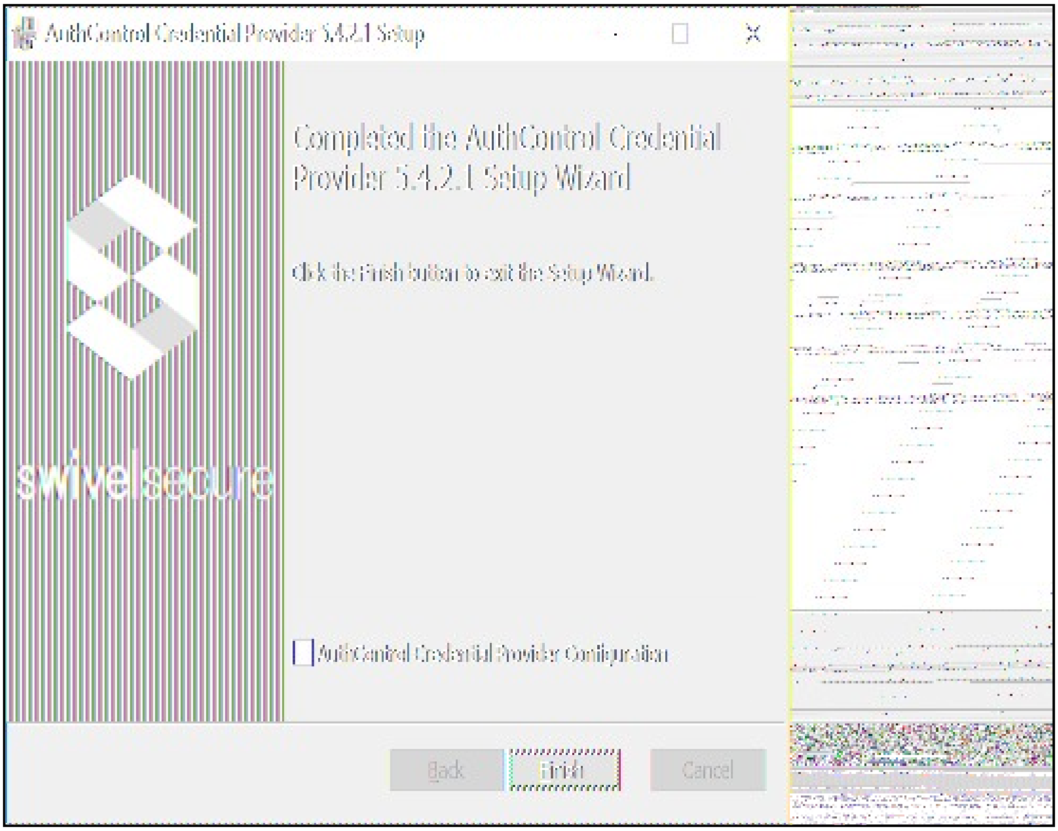
AuthControl Direct Access Manager - for integration with Direct Access

Fingerprint Enrolment - for Biometric Fingerprint enrolment and use Biometric authentication


AuthControl Credential Provider 5.4.2.1 Setup
Custom Setup
Select the way you want features to be installed.
Click the icons in the tree below to change the way features will be installed.
AuthControl Direct Access Man
Fingerprint Enrolment
This feature requires [illegible] on your hard drive.
Browse...
Reset
Disk Usage
Back
Next
Cancel

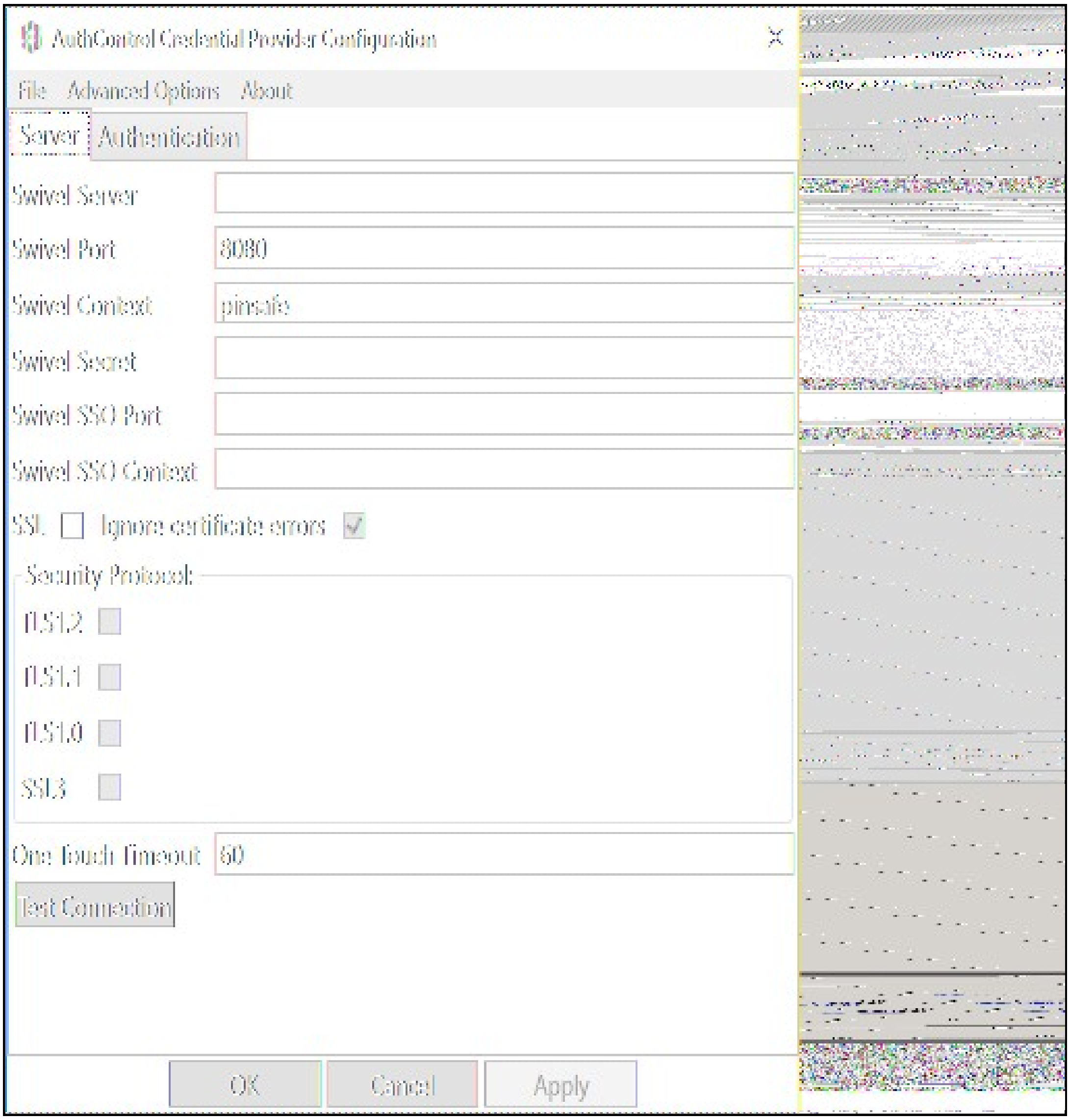
The application will be installed to C:\Program Files\Swivel Secure\Swivel Credential Provider. If you have reconfigured the program files directory elsewhere, it will be installed there, but otherwise you cannot control where the application is installed.

When the install has completed, the following dialog is shown:


AuthControl Credential Provider 5.4.2.1 Setup
swivelsecure
Completed the AuthControl Credential Provider 5.4.2.1 Setup Wizard
Click the Finish button to exit the Setup Wizard.
□ AuthControl Credential Provider Configuration
Back
Finish
Cancel

68.1 AuthControl Credential Provider configuration

68.1.1 Server



Swivel Server
Swivel Port 8080
Swivel Context pinsafe
Swivel Secret
Swivel SSO Port
Swivel SSO Context
SSL □ Ignore certificate errors ☑
Security Protocol
TLS1.2 □
TLS1.1 □
TLS1.0 □
SSL3 □
One Touch Timeout 60

Server: The Swivel virtual or hardware appliance or server IP or hostname. To add resilience, use the VIP on a swivel virtual or hardware appliance. See VIP on PINsafe Appliances.

NOTE: it has been observed in testing that DNS is not always available when logging on. It is therefore recommended that you use IP address, rather than host name in this section.

Port: The Swivel virtual or hardware appliance or server port.

Context: The Swivel virtual or hardware appliance or server installation instance.

Secret: and **Confirm Secret:** A shared secret which must be entered onto the Swivel virtual or hardware appliance or server.

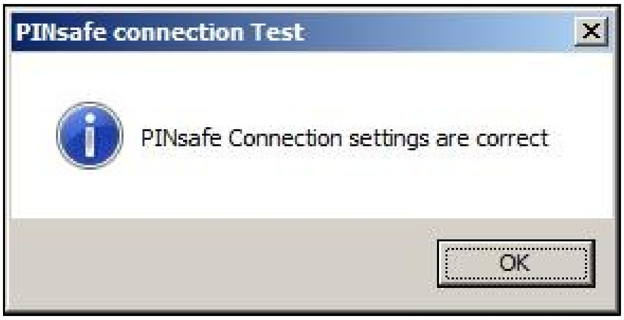
SSO Port: (Sentry v4.0.5 required) The AuthControl Sentry SSO port to allow RBA usage. (ex: 8443)

SSO Context: (Sentry v4.0.5 required) The AuthControl Sentry SSO context to allow RBA usage. (ex: sentry)

Use SSL The Swivel server or virtual or hardware appliance uses SSL communications.

Accept self signed SSL certificates Check this box if Use SSL is enabled, and you do not have a commercial certificate on your Swivel server (or a certificate signed by an authority that the client machine trusts). You should also check this box if you are using IP address rather than host name, as recommended above.

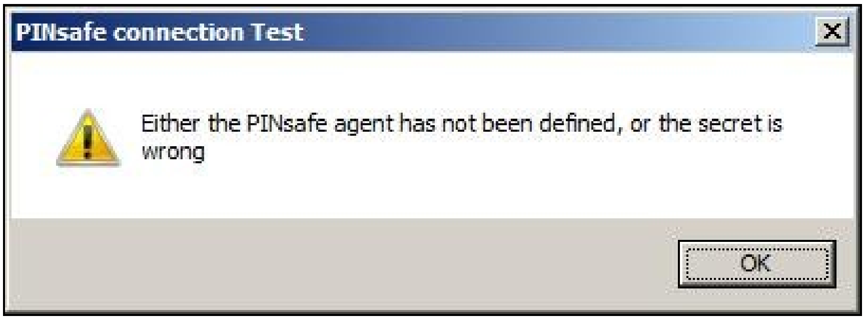
Test Connection Tests link to Swivel server. A correct configuration should produce a dialogue box with **Swivel Connection settings are correct.**



PINsafe connection Test

PINsafe Connection settings are correct

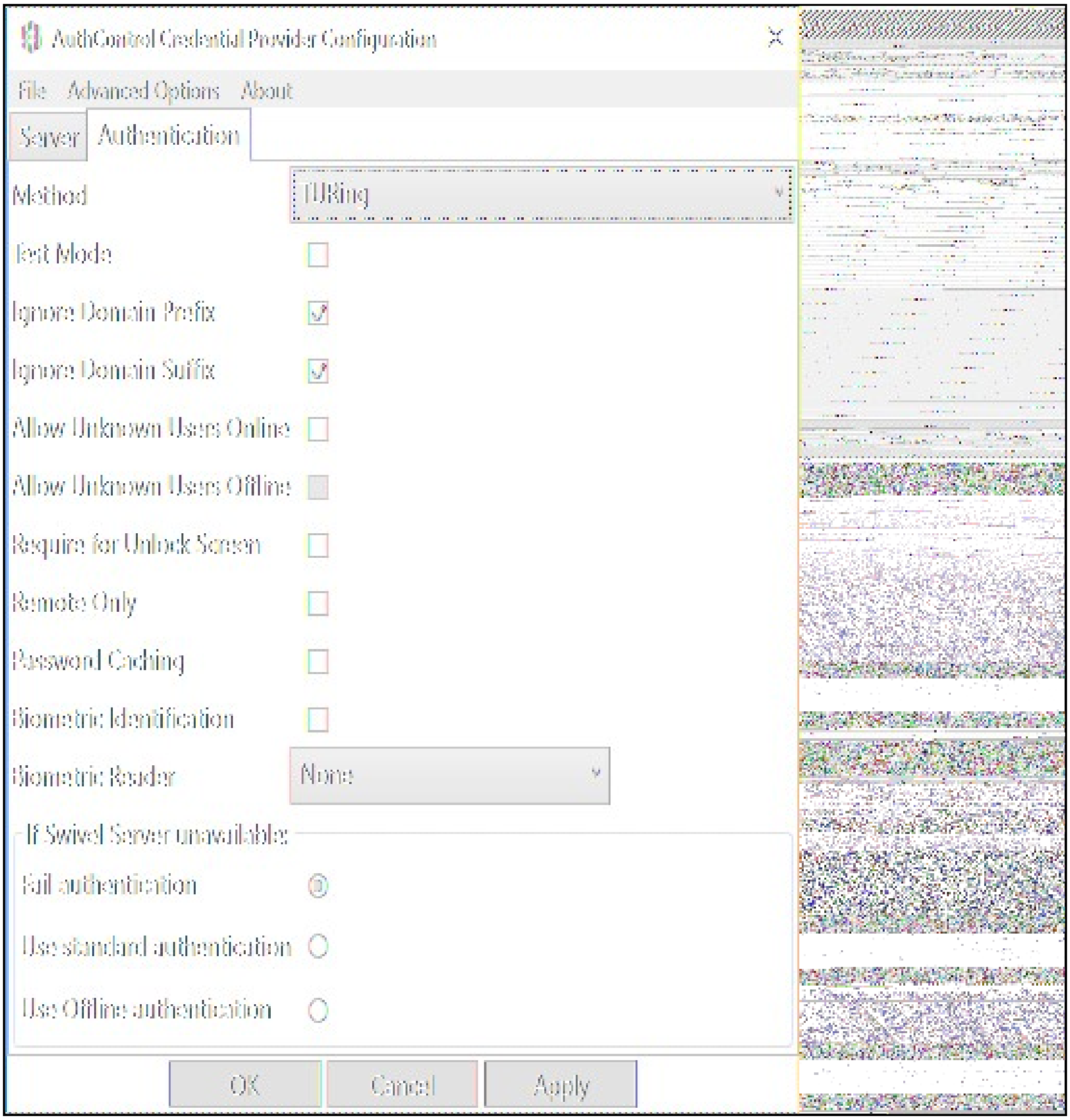
Incorrect settings will produce a dialogue box with **Either the Swivel agent has not been defined, or the secret is wrong**, Please check that the machine can contact Swivel and that the entered settings are correct.



PINsafe connection Test

Either the PINsafe agent has not been defined, or the secret is wrong

68.1.2 Authentication



AuthControl Credential Provider Configuration

Method: TURing

Test Mode ☐

Ignore Domain Prefix ☑

Ignore Domain Suffix ☑

Allow Unknown Users Online ☐

Allow Unknown Users Offline ☐

Require for Unlock Screen ☐

Remote Only ☐

Password Caching ☐

Biometric Identification ☐

Biometric Reader: None

If Swivel Server unavailable:

Fail authentication ●

Use standard authentication ○

Use Offline authentication ○

Method Select the method of authenticating with Swivel, see above.

Test Mode With test mode the user can switch to a standard authentication, see below.

Ignore Domain Prefix Swivel will Remove any domain prefix (domain\username) before matching username. This does not affect Windows authentication usernames.

Ignore Domain Suffix Swivel will Remove any domain suffix (username@domain) before matching username. This does not affect Windows authentication usernames.

Allow Unknown Users Online If the username is not recognized by Swivel, the user can authenticate using Windows credentials only. Any Swivel OTC entered will be ignored. If the user is known then they must authenticate using Swivel authentication.

Allow Unknown Users Offline If Swivel is not found and the user has not authenticated with Swivel before then the user can authenticate using Windows credentials only.

Require for Unlock Screen Shows the selected authentication method on the unlock screen.

Remote Only The selected authentication method will only be shown for users logging into the machine remotely.

Password Caching Allows to cache the password and login using only 2fa. This option only works online.

Biometric Identification Allows to use the Biometric Reader to obtain the username.

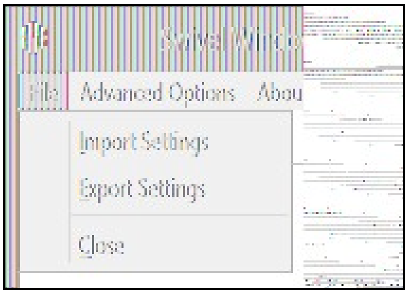
Biometric Reader The type of Biometric Reader: Nitgen or Native Laptop.

If Swivel unavailable, Fail authentication If the Swivel server cannot be contacted then authentication will fail.

If Swivel unavailable, Use standard authentication If the Swivel server is unavailable use standard authentication, the OTC field is displayed but ignored.

If Swivel unavailable, Use offline authentication If the Swivel server cannot be contacted a locally generated Turing image can be used for authentication. If this option is enabled, users will be able to force offline mode using a checkbox on the login dialog. (Only works for single channel authentication methods)

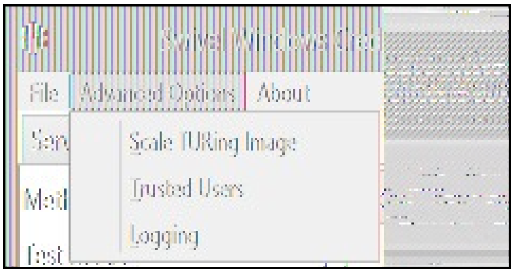
68.1.3 File menu



Export Settings Export settings as an XML file. These can be used to import settings elsewhere.

Import Settings Import settings from an XML file exported elsewhere.

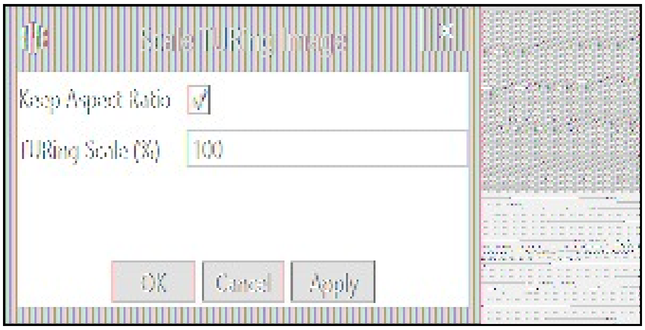
68.1.4 Advanced Options



68.1.4.1 Scale TURing Image

Scale TURing Image... Opens a dialog to let you scale the size of the TURing shown.

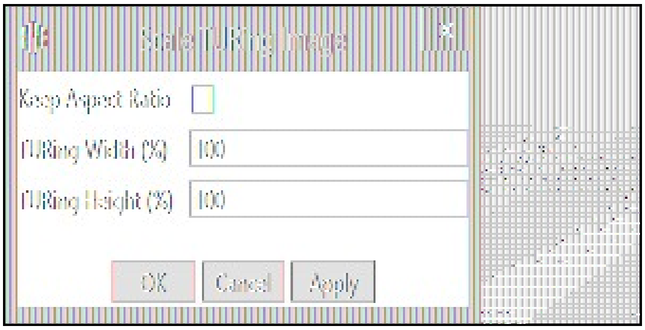
If **Keep Aspect Ratio** is selected then select the scale (%) of the TURing.



Keep Aspect Ratio ☑

TURing Scale (%) 100

If its not selected then you can select the width and hight independently.



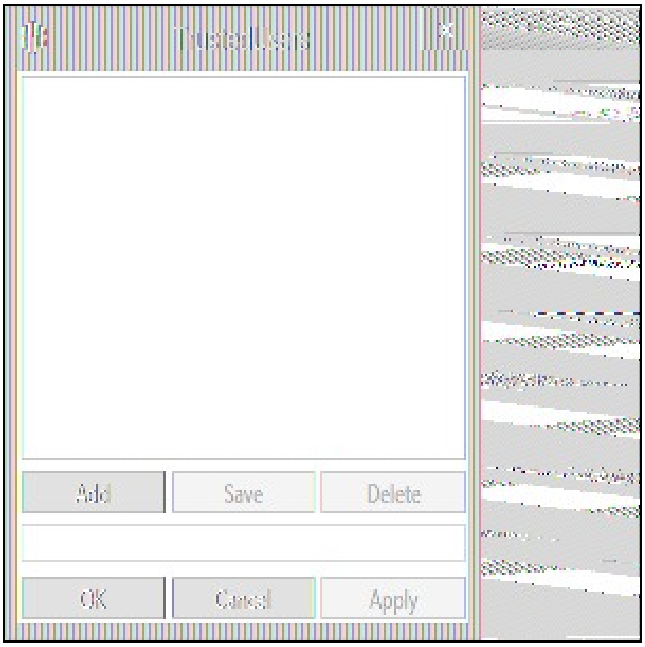
Keep Aspect Ratio □

TURing Width (%) 100

TURing Height (%) 100

68.1.4.2 Trusted Users

""Trusted Users"" Lets listed users Authenticate without Swivel.



To add a trusted user you must first click ""Add"" then enter the username in the text-box and click ""Save"", repeat these sets to add more users.

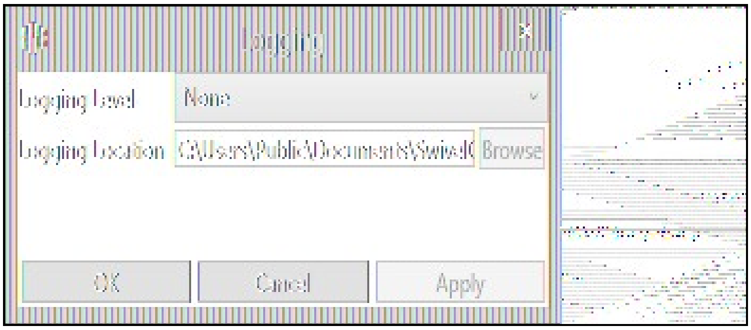
To edit a username select the username from the list, change the name in the text-box and click ""Save"".

To delete a username select the username from the list and press delete.

Make sure that the ""Apply"" or ""OK"" button to save these settings.

68.1.4.3 Logging

""Logging"" change settings relating to logging, recommended to be turned off unless problem are found.



Logging Level: None

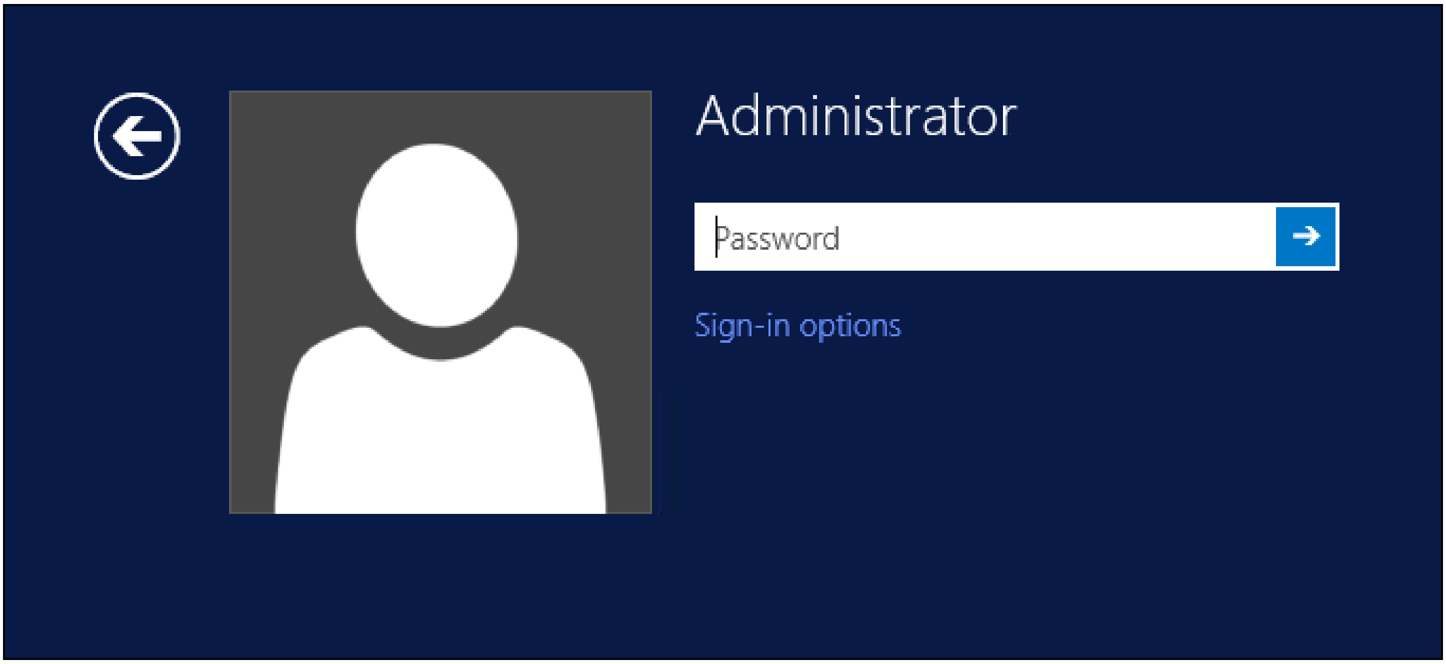
Logging Location: C:\Users\Public\Documents\Swivel(

""Logging Level"" The account of message that will be logged.

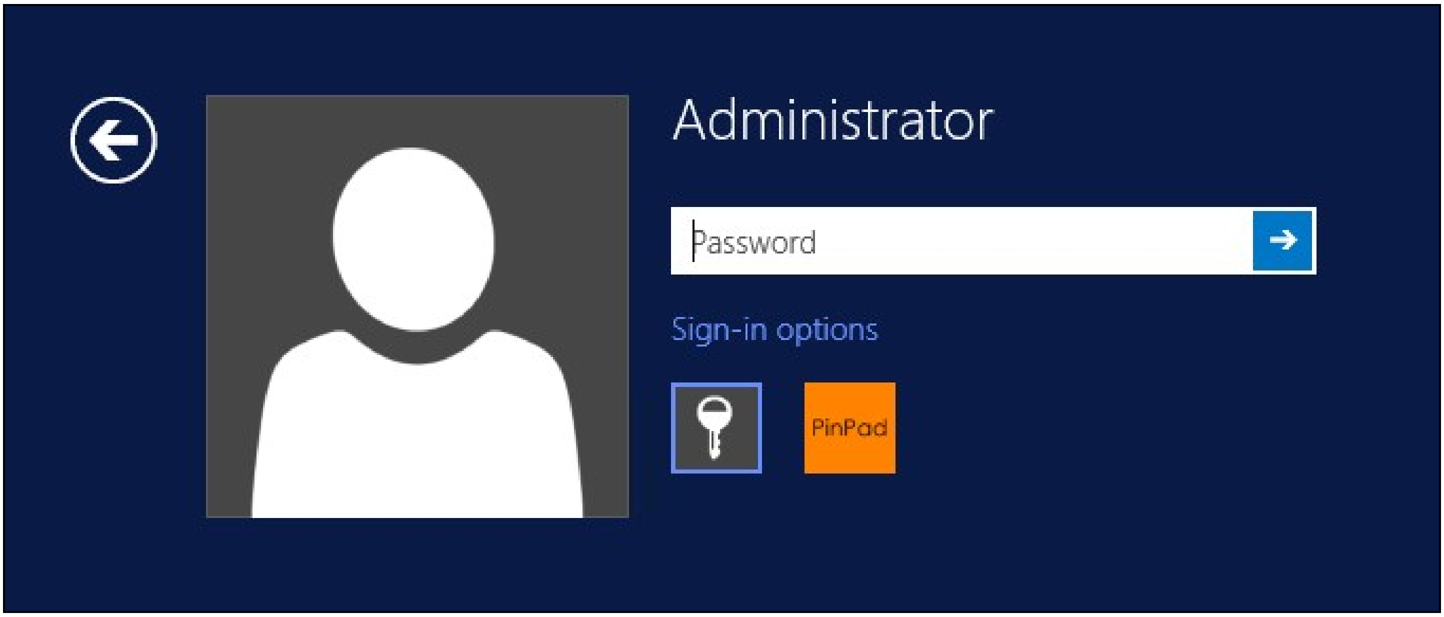
""Logging Location"" The location the logs will be created, this must be somewhere any account has access to.

68.2 Test Mode

With Test Mode enabled the user will be able to select how they will authenticate



The **Sign-in options** button is shown to let users select from the list which method they would like to use.



The last successful authentication method will be selected by default when the credential is loaded.

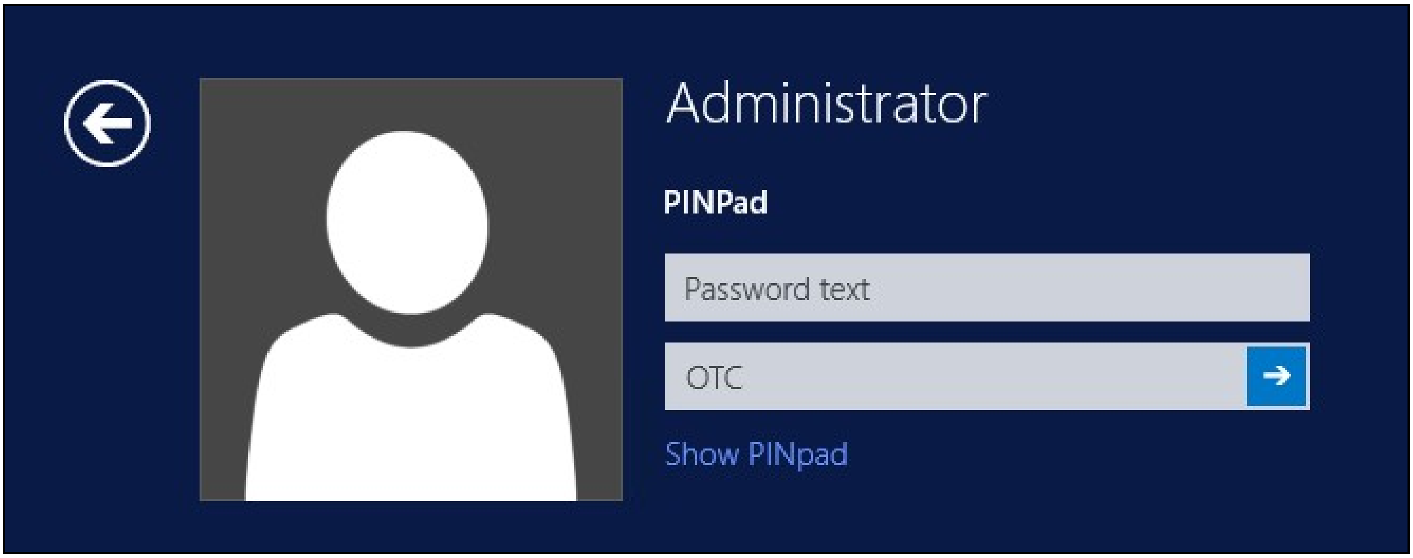
68.3 Importing Configurations

You can import credentials exported from other installations using the Import Settings menu item.

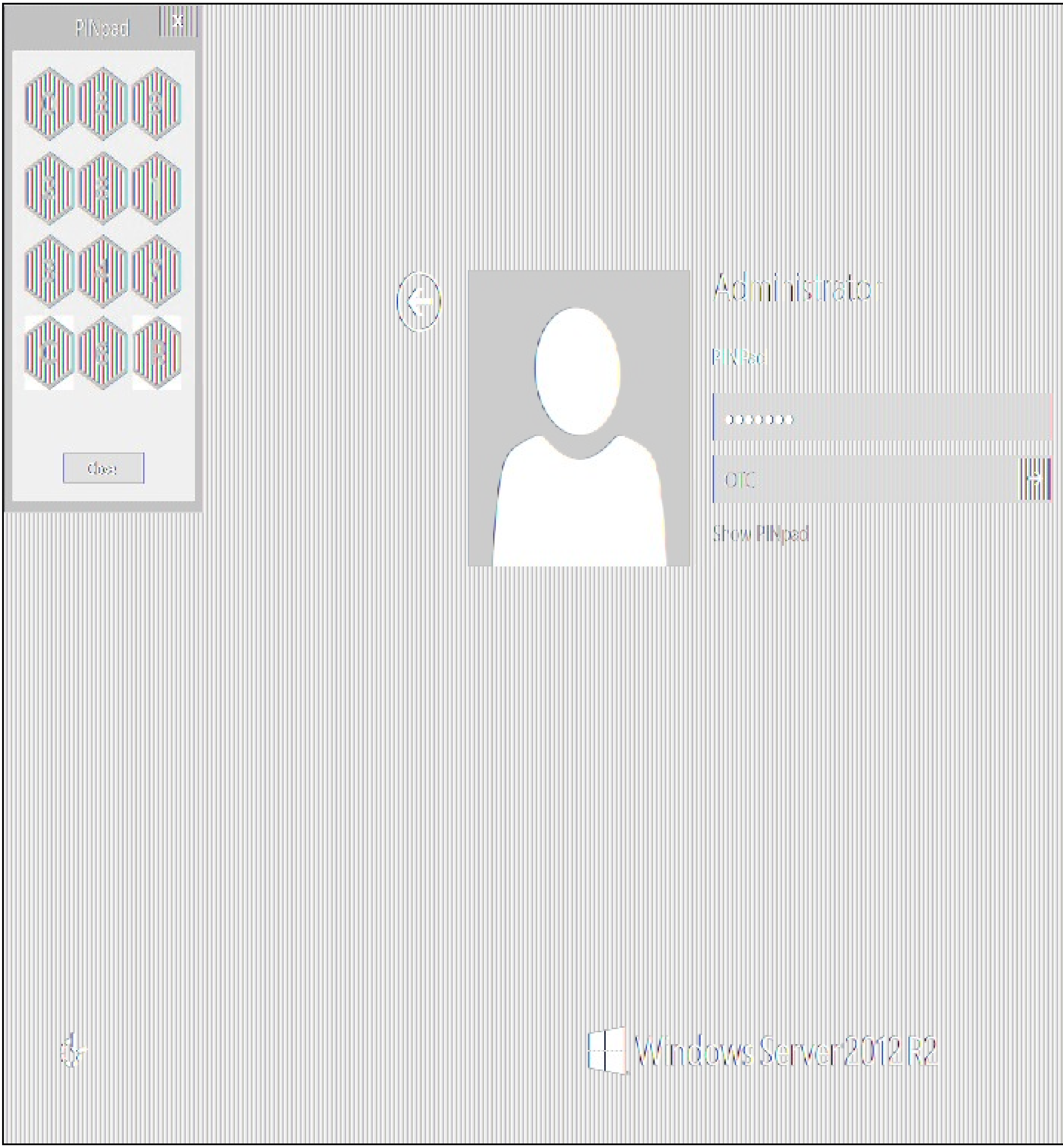
69 Verifying the Installation

This will be an example of one of the credentials.

At the windows login screen a password and OTC login field should be available with a "Show PINpad" Button.



Pressing the "Show PINpad" button will generate a PINpad image for authentication. The Swivel log should show a session request message: *Session started for user: username.*



A successful login should appear in the Swivel log: *Login successful for user: username*.

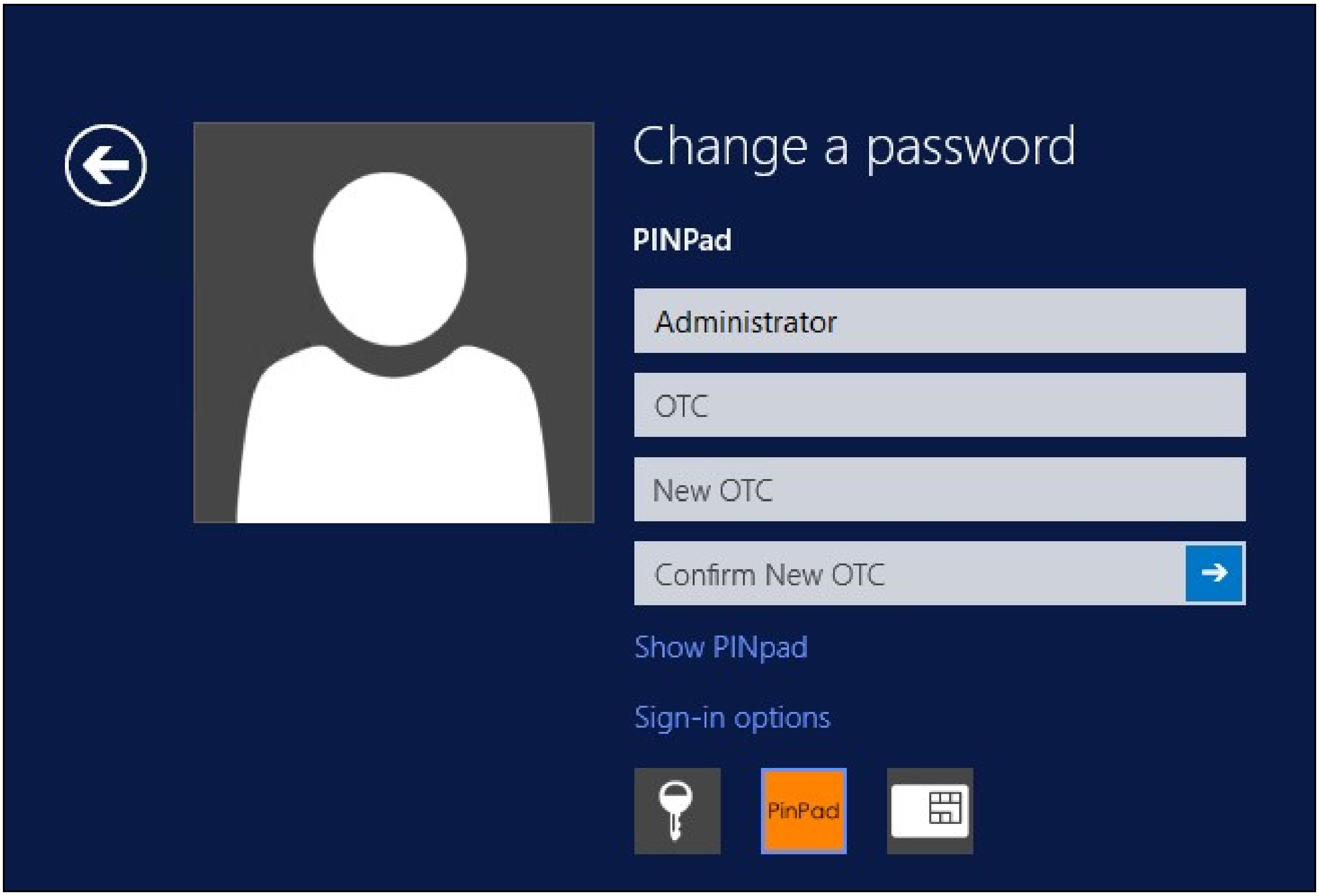
A failed login should not allow a login, and the following message should be displayed in the Swivel log: *Login failed for user: username*.

70 ChangePIN

A user is usually able to change the password by using the Ctrl-Alt-Del keys (Ctrl-Alt-End for remote sessions). With the Swivel Credential Provider installed, an additional option exists when the Change Password is selected, by clicking on the "Sign-in options" button and selecting the Swivel credential. This will not function for Offline authentication.

With Swivel authentication a user never changes enters PIN and this is true for ChangePIN. A user enters their current OTC, and then enters an OTC for what they wish their new PIN to be. PIN enforcement may be in place to the Swivel server to prevent the choosing of poor PIN numbers.

A user may use a single channel image or a dual channel security string to change their PIN.

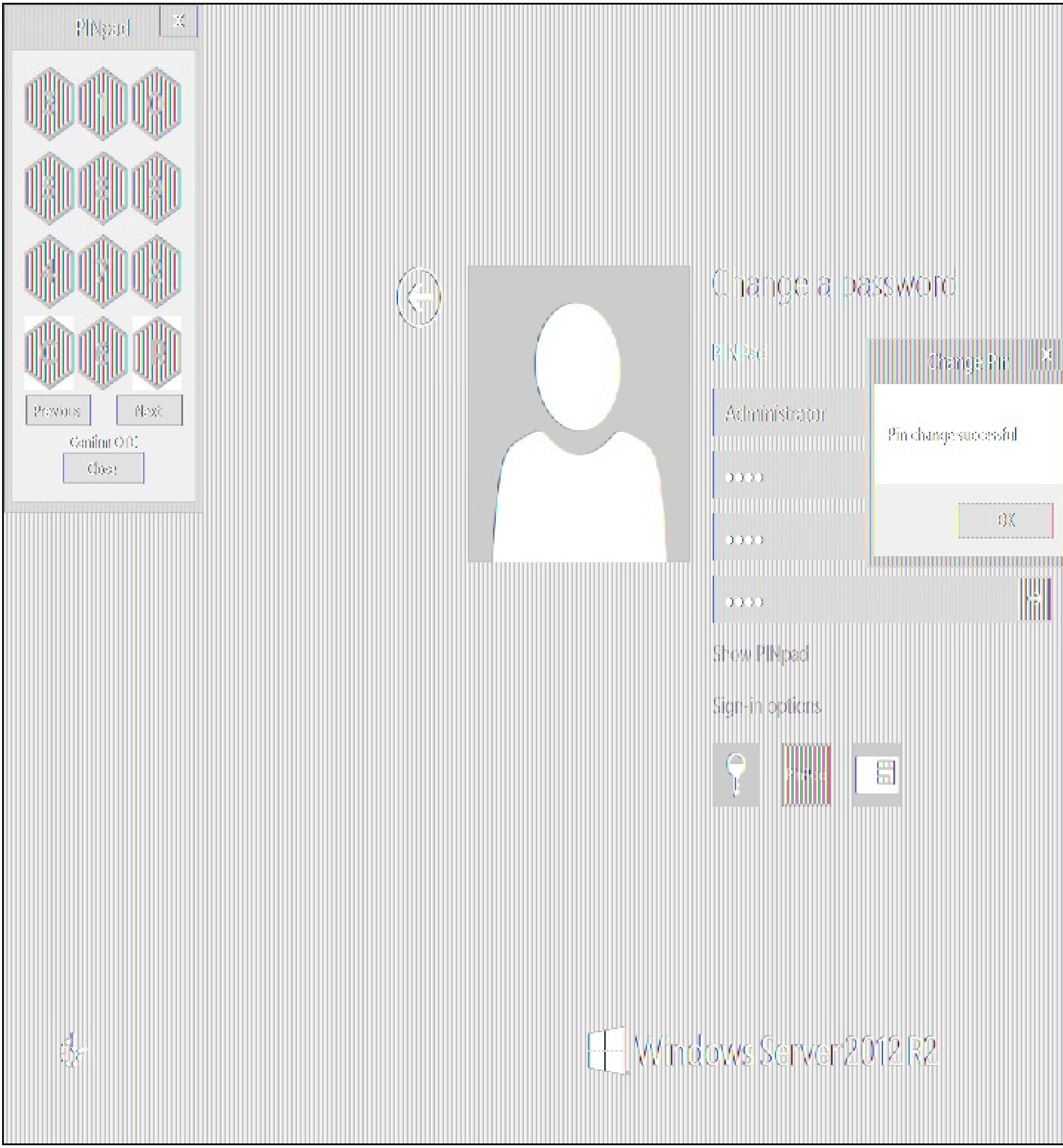


Change a password

PINPad

Administrator

A successful Change PIN will show the message **Your PIN was changed successfully**, the Swivel server will also display in the logs a changePIN message **Change PIN successful for user: username**.



Pin change successful

Other Changes to PINpad are that the PINpad dialog has buttons to select which text-box the numbers will be entered and text to show which text-box is currently selected.

71 Uninstalling the Swivel Integration

Use the Uninstall option from the Program menu, right click on the Windows Credentials provider and click on Uninstall. Note that uninstalling and reinstalling the Credential Provider will remove the settings, so if you need to reinstall at any point, make sure you have an exported settings file saved.

71.1 Disabling the Credential Provider

If the Credential Provider fails to load correctly it can be disabled using the following process:

Boot the machine into safe mode and log in as an administrator.

Try each of the following in turn. Only one of the following is required, so use the first one that works. Experience suggests that the first two options do not work in Windows 10.

- Run the Swivel Login Configuration and edit the settings to disable the provider.
- Uninstall the Credential Provider.
- Using regedit.exe add or alter the following registry values:
    - "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers\{6AD69A51-00E9-4BE9-A3D6-9D26255DA4E1}\Disabled=1"
    - "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Authentication\Credential Provider Filters\{6AD69A51-00E9-4BE9-A3D6-9D26255DA4E1}\Disabled=1"
- Using regedit.exe remove the following registry keys:
    - "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers\{6AD69A51-00E9-4BE9-A3D6-9D26255DA4E1}"
    - "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Authentication\Credential Provider Filters\{6AD69A51-00E9-4BE9-A3D6-9D26255DA4E1}"
    - "HKEY_CLASSES_ROOT \CLSID\{6AD69A51-00E9-4BE9-A3D6-9D26255DA4E1}"

The third option disables the credential provider, whereas the others actually remove it.

71.2 Temporarily Disabling the Credential Provider Remotely

If there is a problem with the Swivel Secure appliance, and you need to disable the AuthControl Credential Provider on a number of machines temporarily, you can do this using a PowerShell script.

71.2.1 Enabling Powershell Remoting

In order to be able to run PowerShell scripts on remote machines, you need to enable the WinRM service on both the target machines and the machine running the script. This article provides a step-by-step guide on setting up PowerShell remoting.

71.2.2 Setting up a List of Computers

The first step is to get a list of computers that you want to disable. This article suggests three alternative methods: hard-code the list in your script, read it from a file, or query the Active Directory. The last is only useful if you want to run the script on every computer on your domain. We will use the second method in our example, so assume there is a list of computer names, one per line, in "CPComputers.txt". This also assumes that the list is in the directory from which you are running the script, so you might want to use a full path in your script.

71.2.3 Setting up Credentials

For completeness, we will describe how to set up credentials to connect to the remote machines. If you are able simply to use the current logged-in user credentials on all remote PCs, then you can ignore this part.

To initialize a credential for use on the remote computers, use the following PowerShell command:

```
$cred = Get-Credential domain\adminuser
```

Replace "domain\adminuser" with the qualified name of the user whose credentials you will be using: note that you must include the domain. You will be prompted for the user's password.

If you are using the current user's credentials, leave off -Credential $cred from the Enter-PSSession command below.

71.2.4 The Script

Here is an example script for disabling the Credential Provider on a number of remote computers:

```
$cred = Get-Credential domain\adminuser
$computers = Get-Content -Path ".\CPComputers.txt"
foreach ($pc in $computers) {
 Enter-PSSession -ComputerName $pc -Credential $cred
 $filterPath = "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Provider Filters\{6AD69A51-00E9-4BE9-A3D6-9D26255DA
 if (Test-Path $filterPath) { Set-ItemProperty -Path $filterPath -Name Disabled -Value 1 }
 $credPath = "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers\{6AD69A51-00E9-4BE9-A3D6-9D26255DA4E1}"
 if (Test-Path $credPath) { Set-ItemProperty -Path $credPath -Name Disabled -Value 1 }
 Exit-PSSession
}
```

71.2.5 Known Limitations

Be aware that running this script may not immediately disable the Credential Provider. You may need to wait a few minutes, or restart the computer, for the change to take effect.

71.2.6 Re-enabling the Credential Provider

To re-enable the Credential Provider, use the same script, but change the Disabled Value to 0 in two lines. So the script between Enter-PSSession and Exit-PSSession becomes

```
 $filterPath = "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Provider Filters\{6AD69A51-00E9-4BE9-A3D6-9D26255DA
```

```
if (Test-Path $filterPath) { Set-ItemProperty -Path $filterPath -Name Disabled -Value 0 }
$credPath = "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers\{6AD69A51-00E9-4BE9-A3D6-9D26255DA4E1}"
if (Test-Path $credPath) { Set-ItemProperty -Path $credPath -Name Disabled -Value 0 }
```

72 Known Issues and Limitations

- The Swivel Windows Credential Provider does not support the use of Animated gifs for Single Channel authentication.
- It has been observed in testing that DNS is not always available when logging on. It is therefore recommended that you use IP address, rather than host name for the Swivel server.
- Local (offline) authentication only works in single channel and OATH modes: the dual channel strings are not available offline.
- If the user gets an online TURing with a different scale then gets an offline TURing, the TURing is broken, the fix is to close the dialog and request an new TURing.
- If **Allow Unknown Users Offline** is enabled then users that have not previously authenticated to Swivel online can bypass Swivel by checking the offline box and authenticating with AD only.
- On Windows server 2012 R2 there is an update from Microsoft to fix an issue where dialogues will not be displayed, please ensure that windows update 2919355 is installed.
- Local authentication does not know if a users PIN has expired or even if the account is locked or deleted. Once a user has successfully authenticated they are allowed offline until their offline strings are deleted or the offline option is deselected.

73 Windows Credential Provider with RBA

74 Introduction

From AuthControl Sentry v4.0.5, you can use your RBA rules with AuthControl Credential Provider to disable 2fa in case the user has enough points.

75 Prerequisites

AuthControl Credential Provider v5.4.2

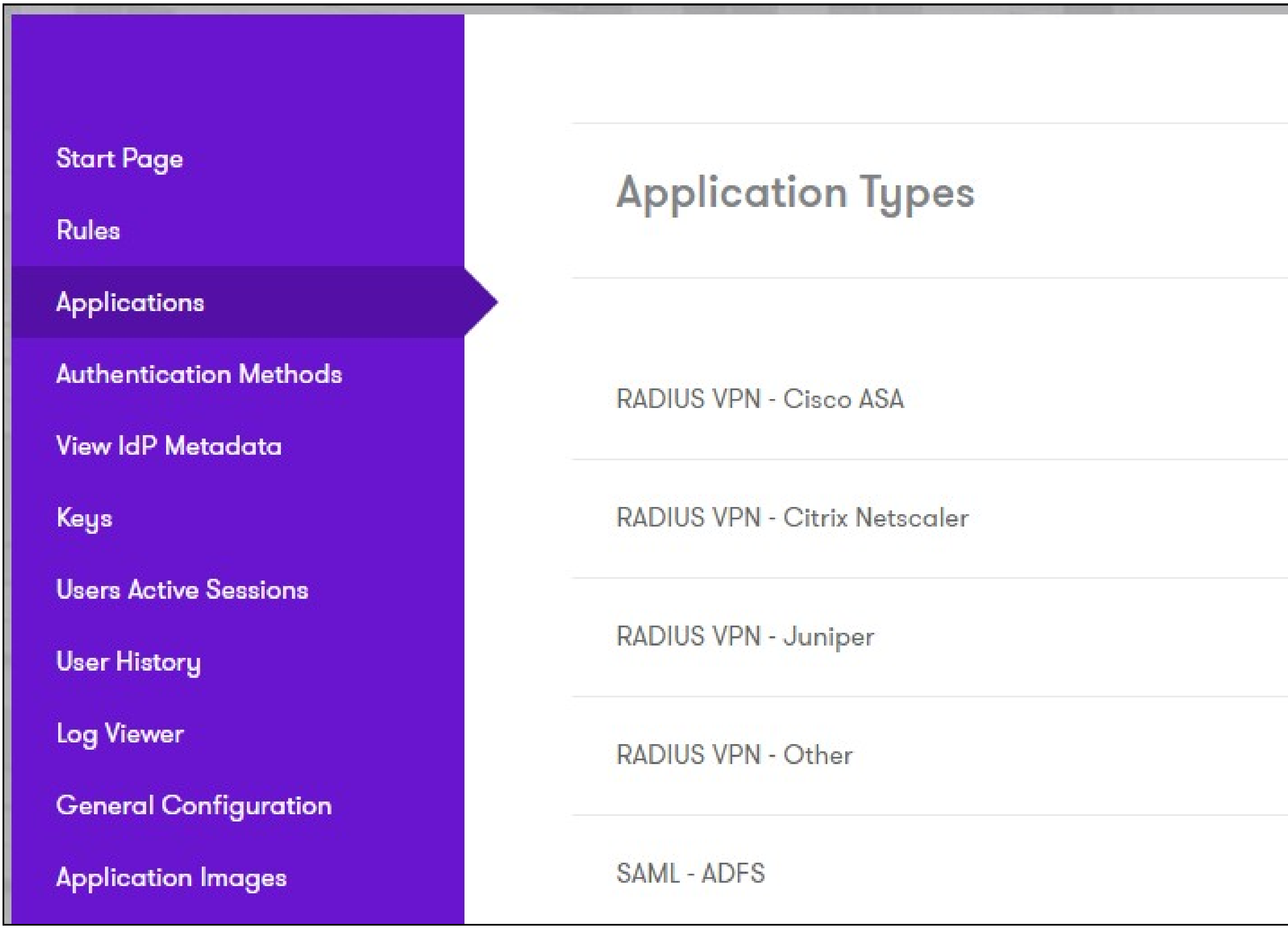
AuthControl Sentry v4.0.5

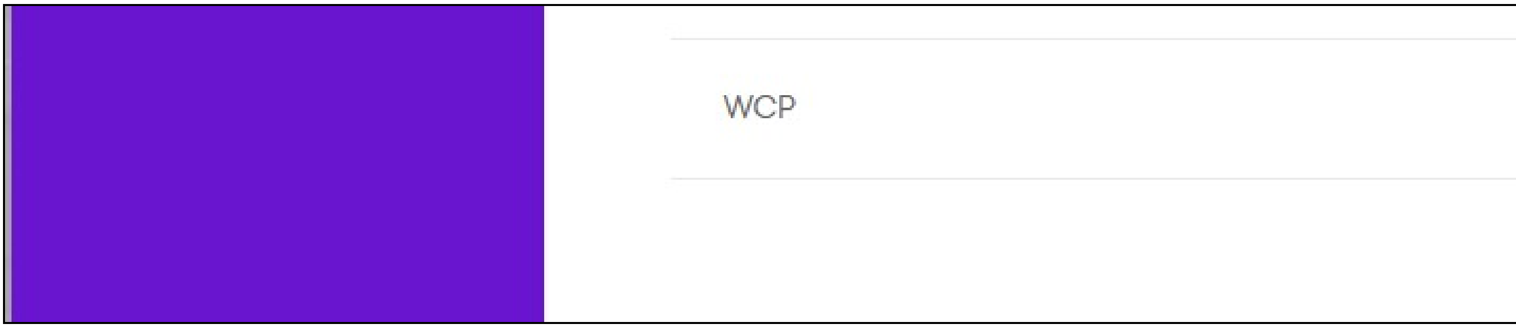
76 Limitations

Certificate rule does not work with WCP

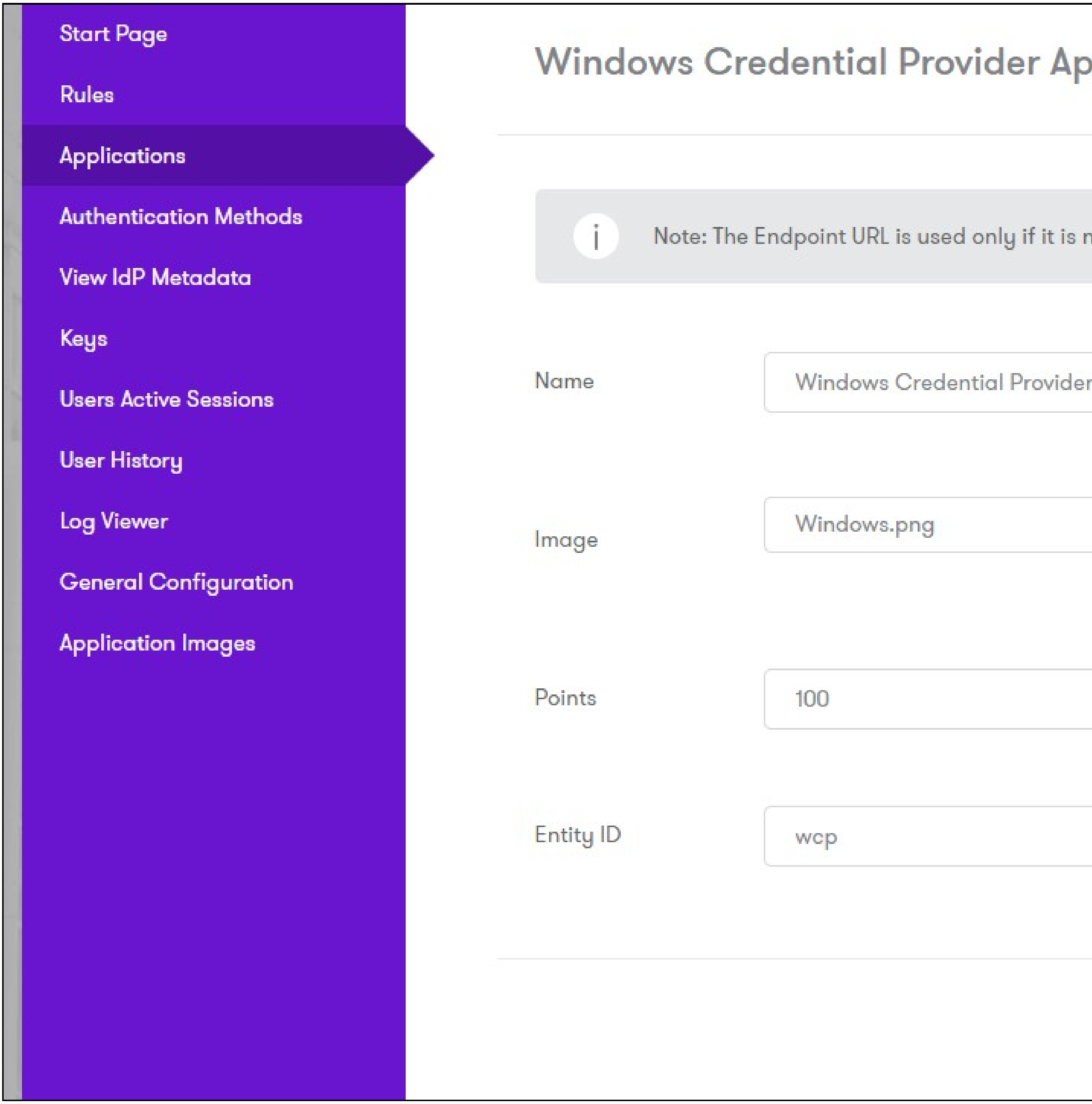
77 RBA Configuration

In AuthControl Sentry SSO administration page you have a new application type WCP. Add a new application.





Select WCP.



Windows Credential Provider Ap

Note: The Endpoint URL is used only if it is n

Name: Windows Credential Provider

Image: Windows.png

Points: 100

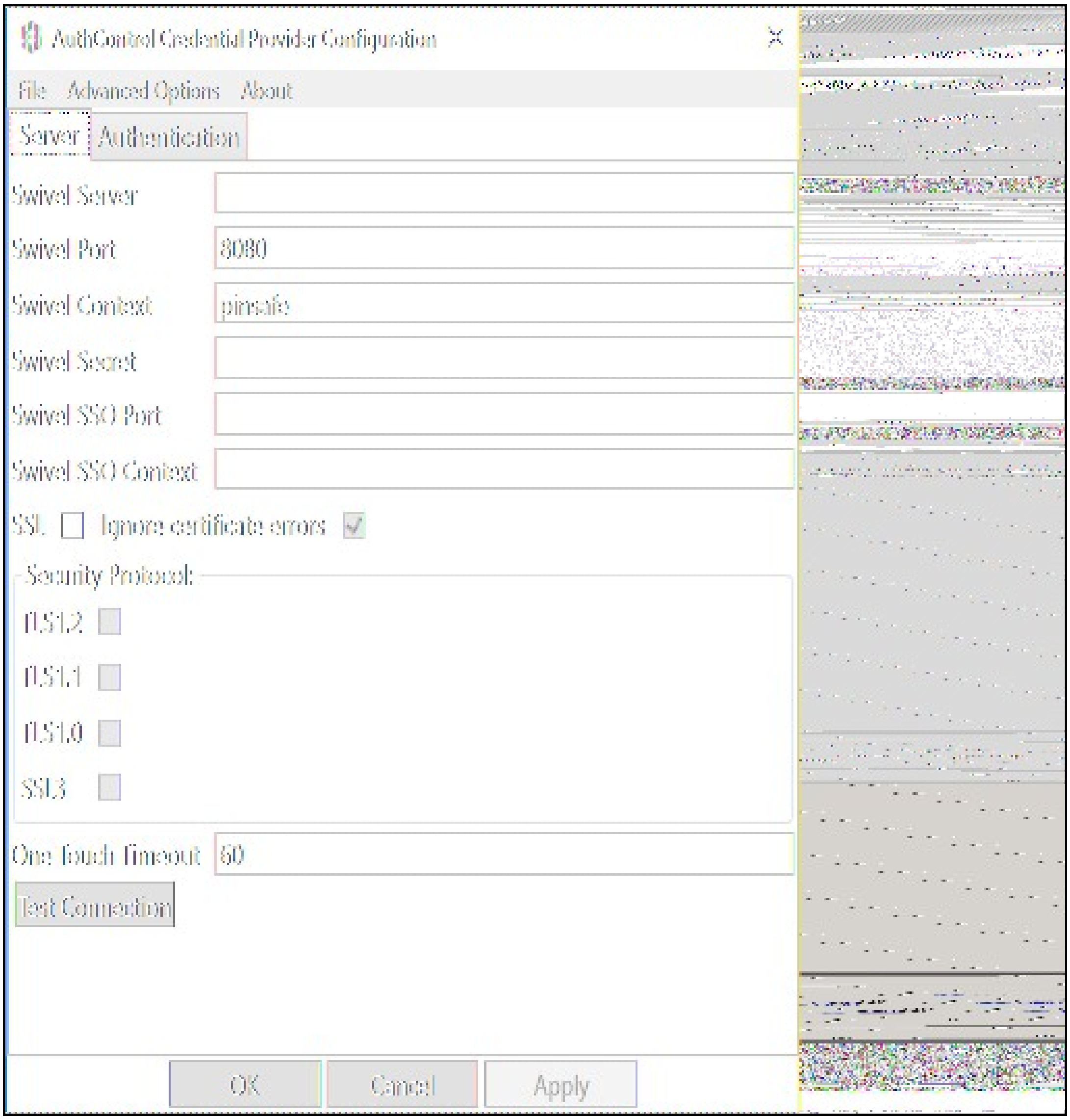
Entity ID: wcp

Enter a name, the required points for authentication without 2fa, **the entity ID must be wcp** and click Save.

If you haven't configure any rules, please look at Authcontrol v4 Sentry SSO and Adaptive Authentication.

78 WCP Configuration

Open AuthControl Credential Provider Configuration



Swivel Server

Swivel Port: 8080

Swivel Context: pinsafe

Swivel Secret

Swivel SSO Port

Swivel SSO Context

SSL □ Ignore certificate errors ☑

Security Protocol

TLS1.2 □

TLS1.1 □

TLS1.0 □

SSL3 □

One Touch Timeout: 60

enter the Swivel SSO Port as 8443 and Swivel SSO Context as sentry. This will enable the check for RBA rules in WCP.

79 Authenticating

When you try to login now it will check for the rules. If the user has enough points, it will allow authentication without using 2fa.

80 RBA with fingerprint

If you have Biometric Identification active, you can use this to give more points to RBA and disable 2fa.

81 Microsoft Direct Access Integration

82 Introduction

Microsoft Direct Access allows a VPN connection to be brought up when a user requires access to an organisations internal resources. PINsafe can authenticate a user accessing those internal resources using Dual channel authentication such as SMS, Mobile Phone Client and the Taskbar utility Taskbar How to Guide and Token.

83 Prerequisites

Microsoft Direct Access fully configured

Microsoft CA server for OTP authentication

PINsafe 3.x

84 Baseline

Microsoft UAG SP1 with Direct access configured

PINsafe 3.8

85 Architecture

When a Direct Access connection is made, a pop up appears for the user prompting them to enter their One Time Code. This is then checked by the UAG against PINsafe using RADIUS authentication.

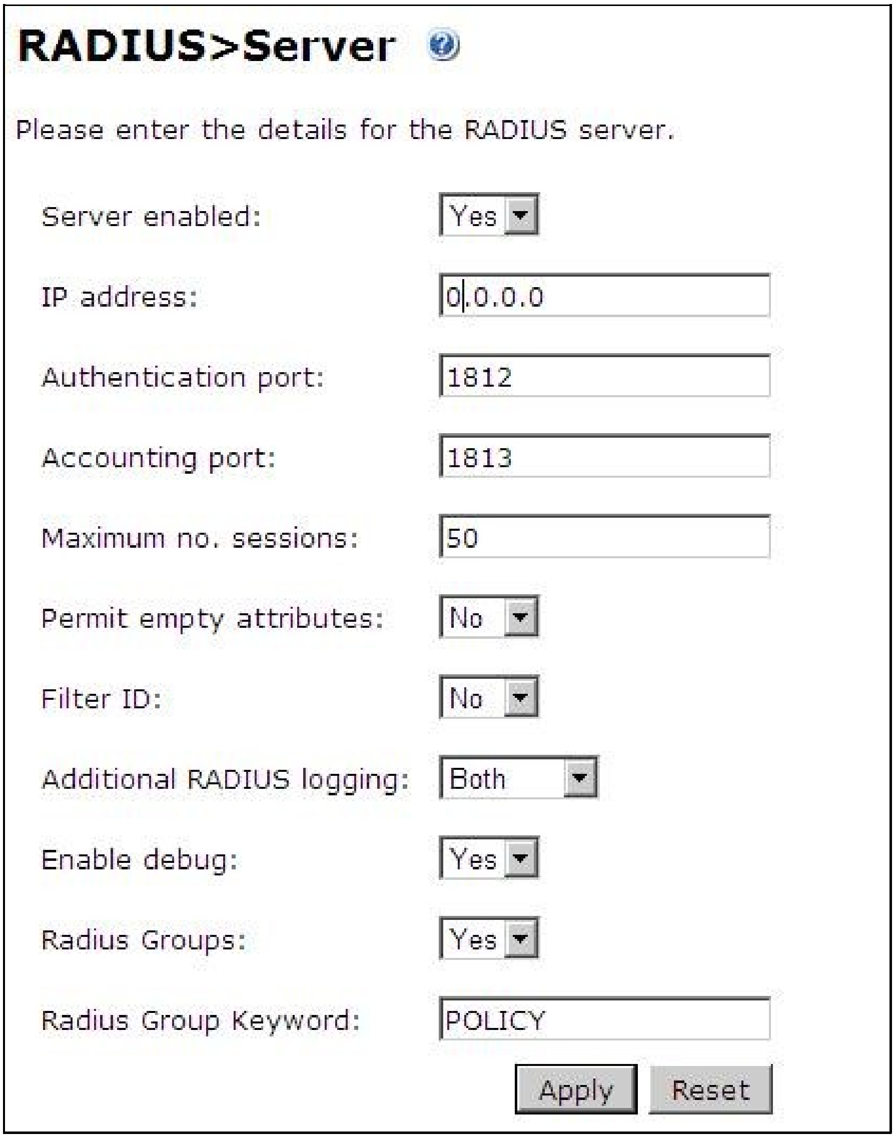
86 Installation

86.1 PINsafe Configuration

86.1.1 Configuring the RADIUS server

Configure the RADIUS settings using the RADIUS configuration page in the PINsafe Administration console. In this example (see diagram below) the RADIUS Mode is set to ?Enabled? and the HOST IP (the PINsafe server) is set to 0.0.0.0. (leaving the field empty has the same result). This means that the server will answer all RADIUS requests received by the server regardless of the IP address that they were sent to.

Note: for appliances, the PINsafe VIP should not be used as the server IP address, see VIP on PINsafe Appliances



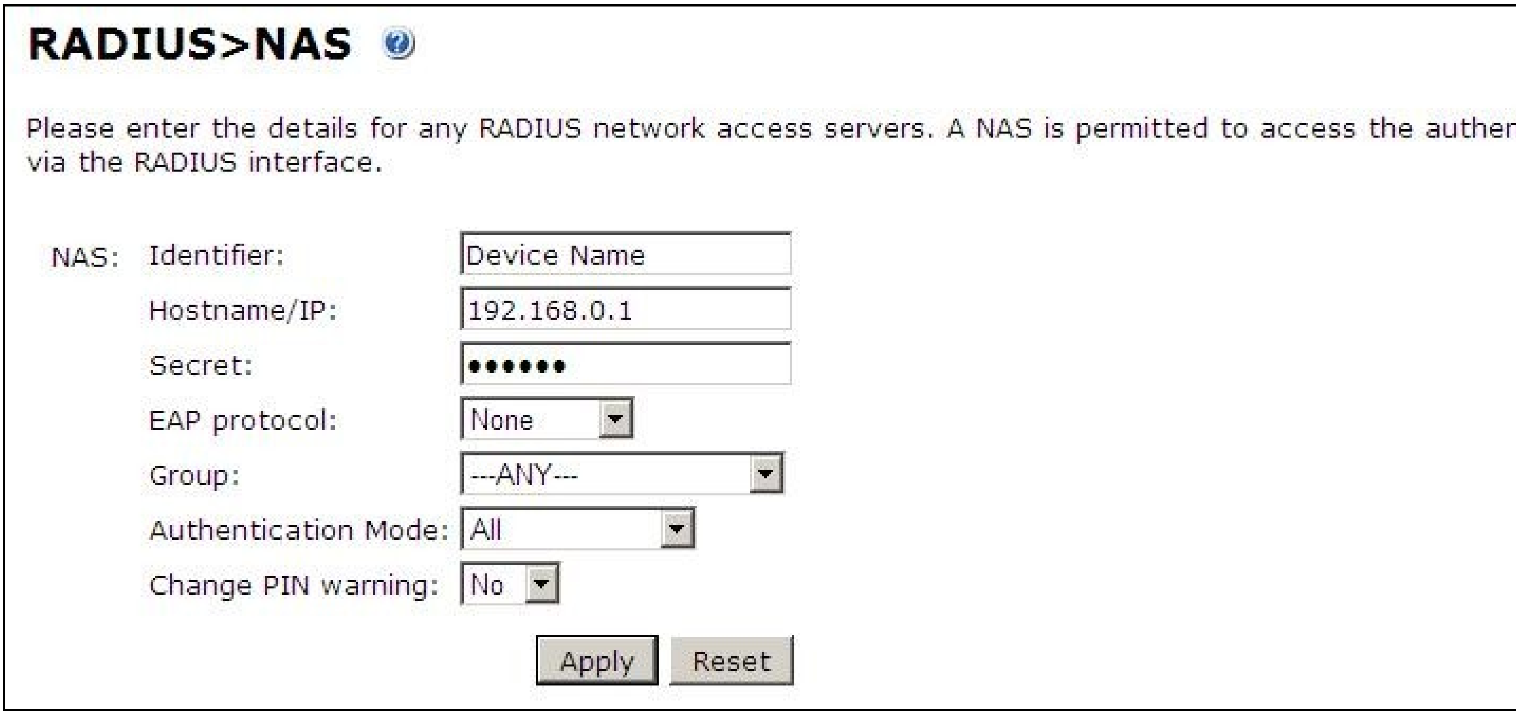
RADIUS>Server

Please enter the details for the RADIUS server.

Server enabled:	Yes
IP address:	0.0.0.0
Authentication port:	1812
Accounting port:	1813
Maximum no. sessions:	50
Permit empty attributes:	No
Filter ID:	No
Additional RADIUS logging:	Both
Enable debug:	Yes
Radius Groups:	Yes
Radius Group Keyword:	POLICY

86.1.2 Setting up the RADIUS NAS

Set up the NAS using the Network Access Servers page in the PINsafe Administration console. Enter a name for the VPN server. The IP address has been set to the IP of the VPN appliance, and the secret ?secret? assigned that will be used on both the PINsafe server and VPN RADIUS configuration.



RADIUS>NAS

Please enter the details for any RADIUS network access servers. A NAS is permitted to access the auther via the RADIUS interface.

NAS:	Identifier:	Device Name
	Hostname/IP:	192.168.0.1
	Secret:	••••••
	EAP protocol:	None
	Group:	---ANY---
	Authentication Mode:	All
	Change PIN warning:	No

You can specify an EAP protocol if required, others CHAP, PAP and MSCHAP will be supported. All users will be able to authenticate via this NAS unless to restrict authentication to a specific repository group.

86.1.3 Enabling Session creation with username

PINsafe can be configured to use the Taskbar to present a TURing image to users when prompted for authentication by Direct Access. See Taskbar How to Guide

To allow Single Channel authentication on PINsafe follow the below steps.

Go to the ?Single Channel? Admin page and set ?Allow Session creation with Username:? to YES.

To test your configuration you can use the following URL using a valid PINsafe username:

Appliance

https://PINsafe_server_IP:8443/proxy/SCImage?username=testuser

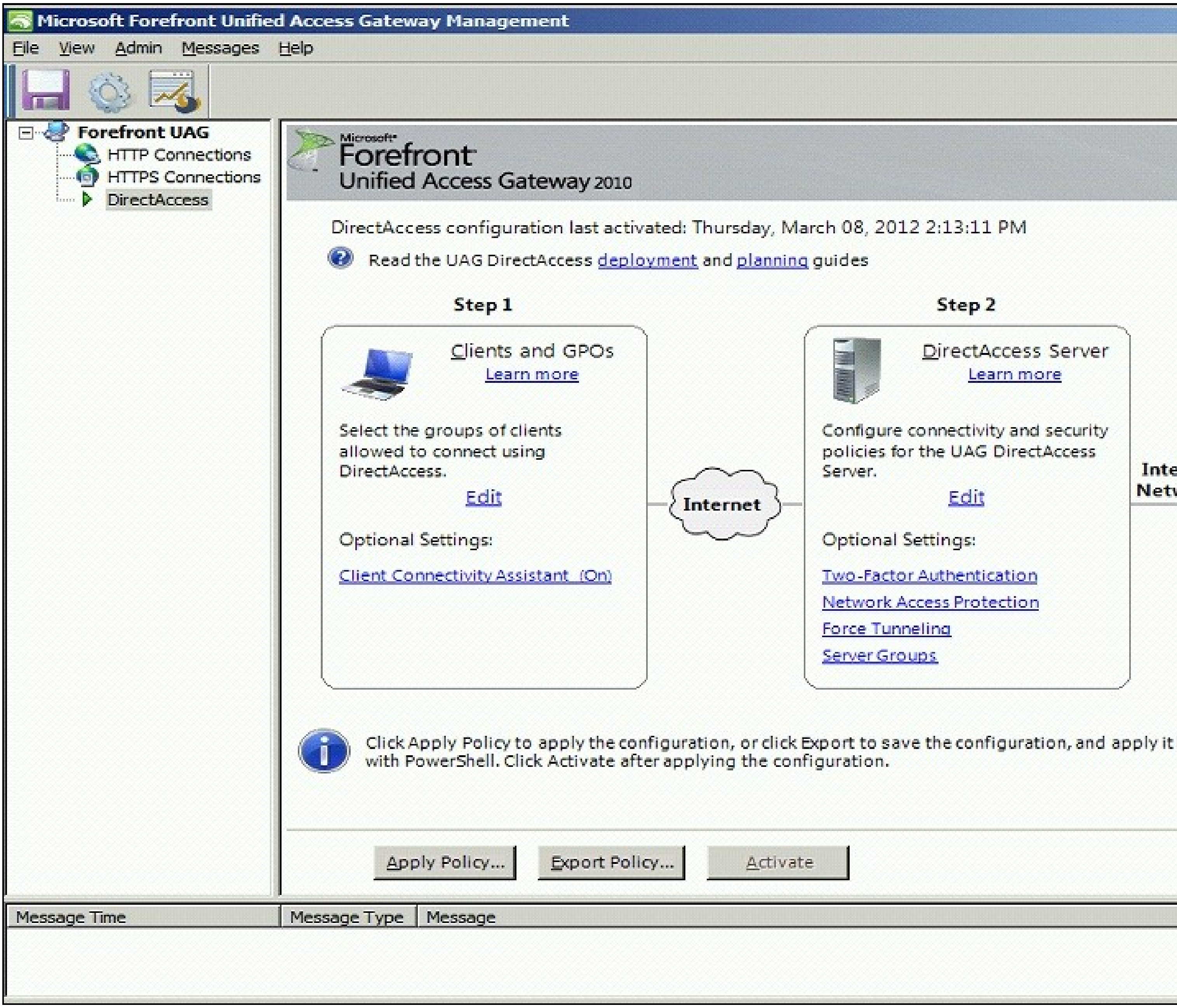
For a software only install see Software Only Installation

86.2 Microsoft Direct Access Integration

Ensure that the Microsoft Direct Access is fully working and tested before startigng the PINsafe integration.

86.2.1 Enable Two Factor Authentication

On the Forefront UAG Direct Access configuration page select under Step 2 Optional Settings the link for *Two-Factor Authentication*


Microsoft Forefront Unified Access Gateway Management
File View Admin Messages Help
Forefront UAG
HTTP Connections
HTTPS Connections
DirectAccess
Microsoft Forefront
Unified Access Gateway 2010

DirectAccess configuration last activated: Thursday, March 08, 2012 2:13:11 PM

Read the UAG DirectAccess deployment and planning guides

Step 1

Clients and GPOs

Learn more

Select the groups of clients allowed to connect using DirectAccess.

Edit

Optional Settings:

Client Connectivity Assistant (On)

Internet

Step 2

DirectAccess Server

Learn more

Configure connectivity and security policies for the UAG DirectAccess Server.

Edit

Optional Settings:

Two-Factor Authentication

Network Access Protection

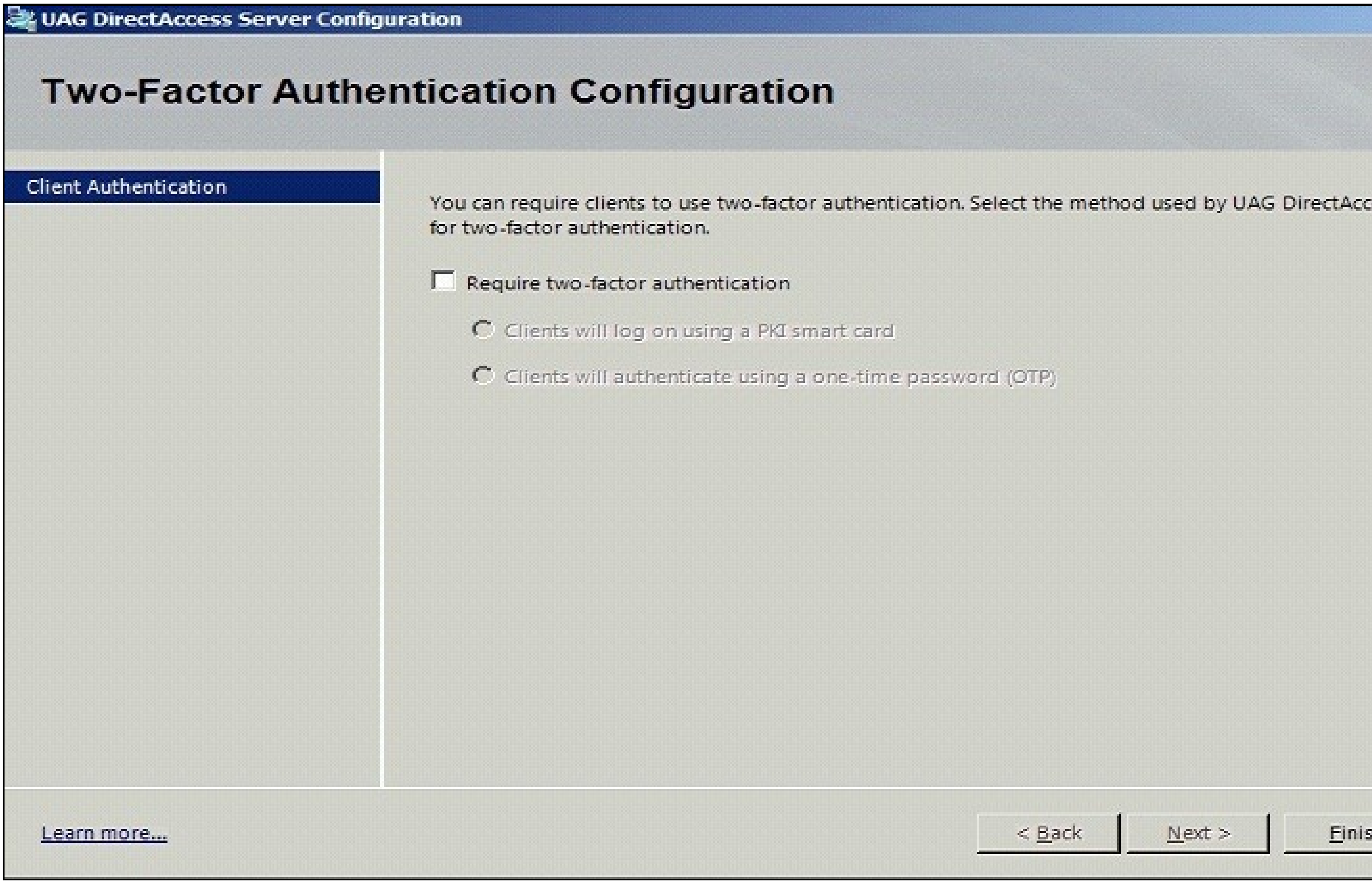
Force Tunneling

Server Groups

Inte
Netw

Click Apply Policy to apply the configuration, or click Export to save the configuration, and apply it with PowerShell. Click Activate after applying the configuration.

Click on *Require two-factor authentication*



UAG DirectAccess Server Configuration

Two-Factor Authentication Configuration

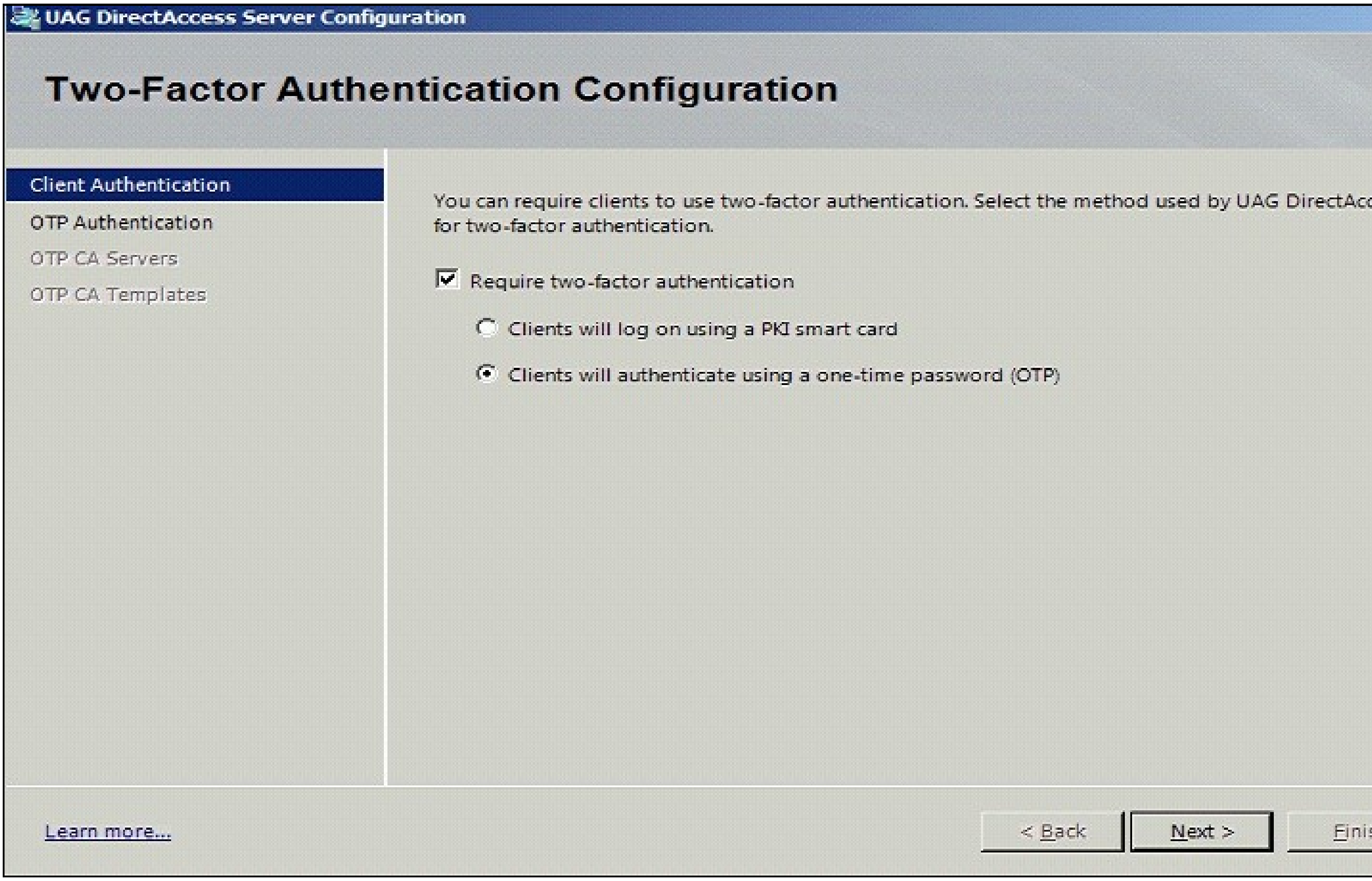
You can require clients to use two-factor authentication. Select the method used by UAG DirectAcc
for two-factor authentication.

□ Require two-factor authentication

○ Clients will log on using a PKI smart card

○ Clients will authenticate using a one-time password (OTP)

Click on *Clients will authenticate using a one-time password (OTP)*



UAG DirectAccess Server Configuration

Two-Factor Authentication Configuration

You can require clients to use two-factor authentication. Select the method used by UAG DirectAcc
for two-factor authentication.

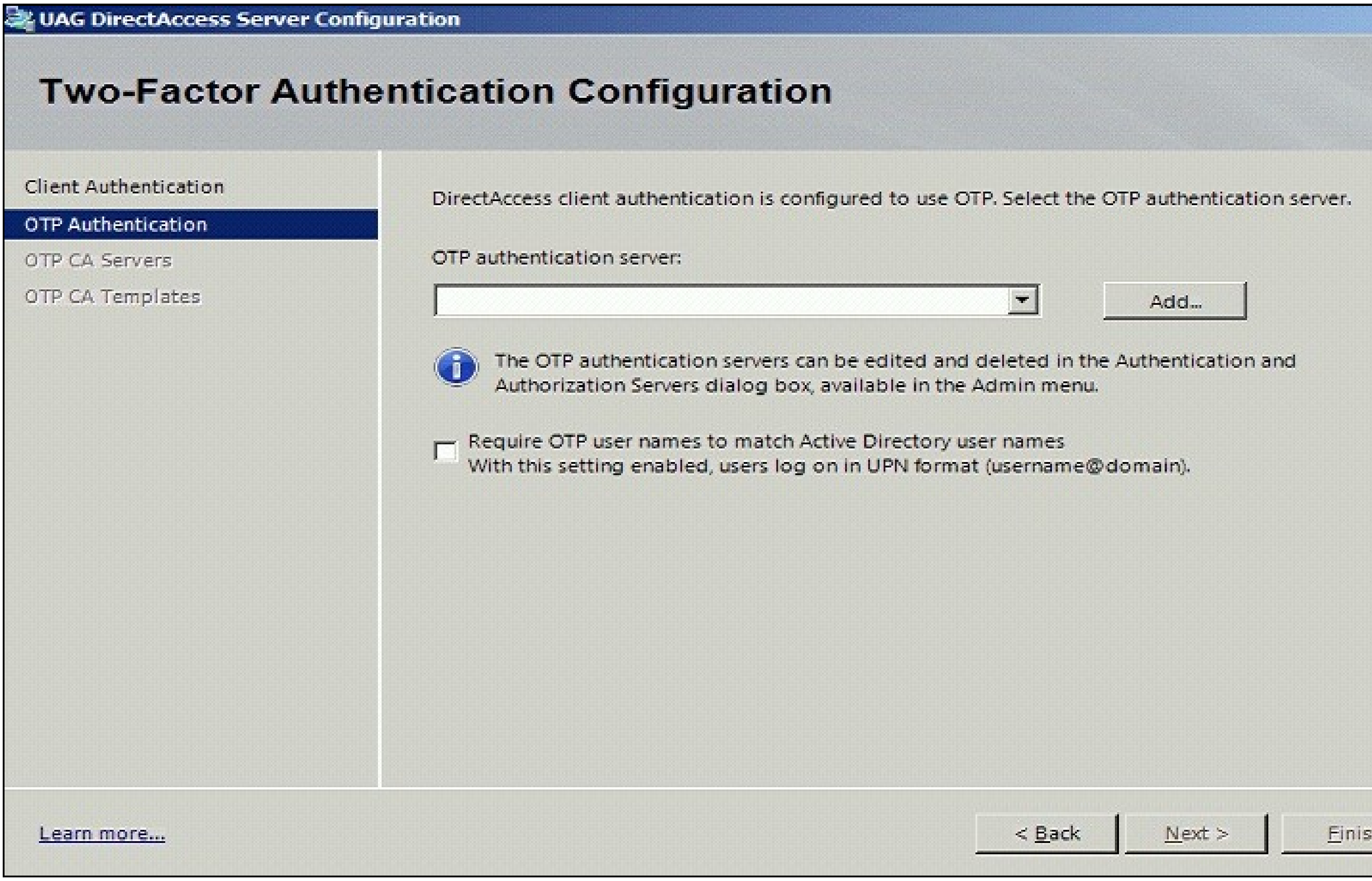
☑ Require two-factor authentication

○ Clients will log on using a PKI smart card

● Clients will authenticate using a one-time password (OTP)

86.2.2 Configure OTP Authentication Server

On the OTP Authentication tab click Add



UAG DirectAccess Server Configuration

Two-Factor Authentication Configuration

DirectAccess client authentication is configured to use OTP. Select the OTP authentication server.

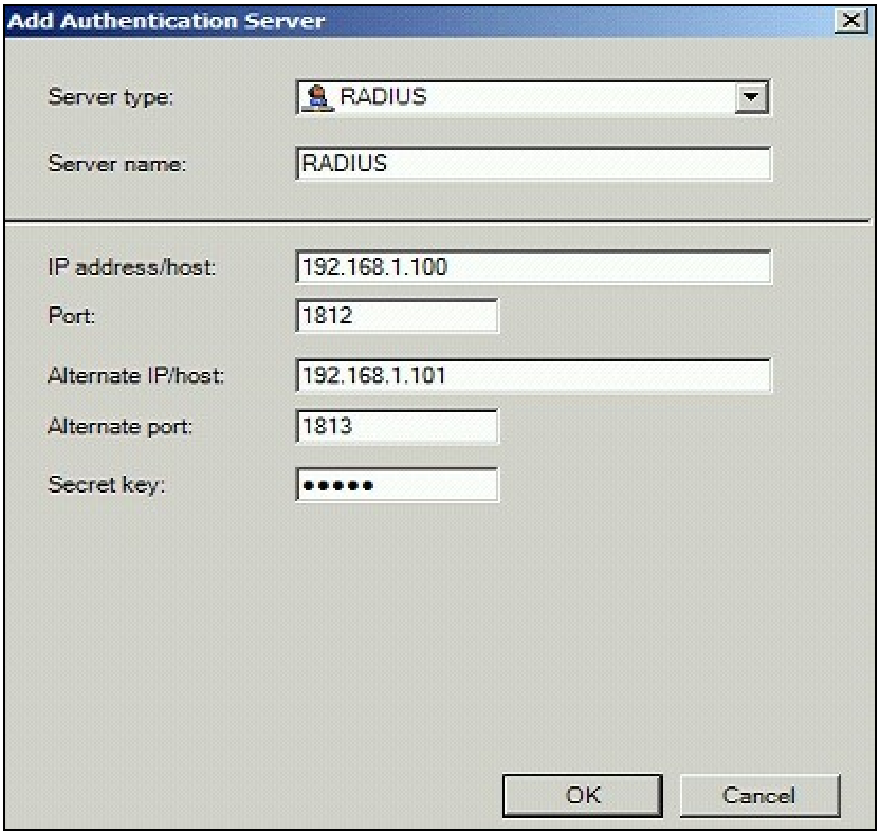
OTP authentication server:

The OTP authentication servers can be edited and deleted in the Authentication and Authorization Servers dialog box, available in the Admin menu.

□ Require OTP user names to match Active Directory user names
With this setting enabled, users log on in UPN format (username@domain).

Select Server Type RADIUS and enter the following information:

- Server Name: A descriptive name for the RADIUS server
- Port: RADIUS port used by the Swivel server, usually 1812
- IP address/host: The Swivel RADIUS server
- Alternate IP/host: A secondary Swivel RADIUS server
- Alternate port: The port used by the secondary Swivel server, usually 1812
- Secret Key: A shared secret entered on the Swivel servers.



Server type: RADIUS

Server name: RADIUS

IP address/host: 192.168.1.100

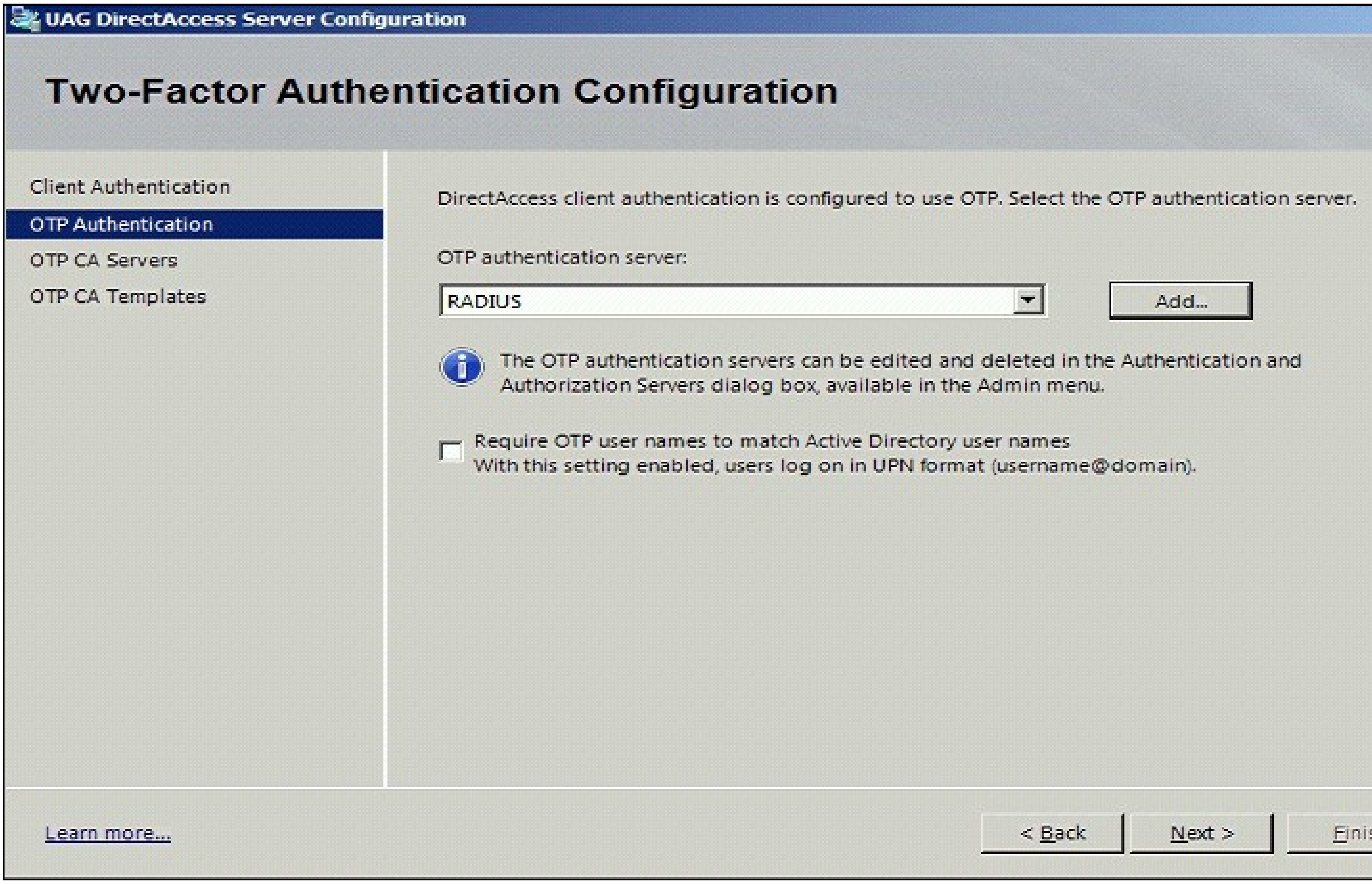
Port: 1812

Alternate IP/host: 192.168.1.101

Alternate port: 1813

Secret key: ●●●●●

Ensure that the new Swivel server is selected. Optionally select *Require OTP user names to match Active Directory user names with this setting enabled, users log on in UPN format (username@domain).* then the user name will be automatically populated at the direct access login.



DirectAccess client authentication is configured to use OTP. Select the OTP authentication server.

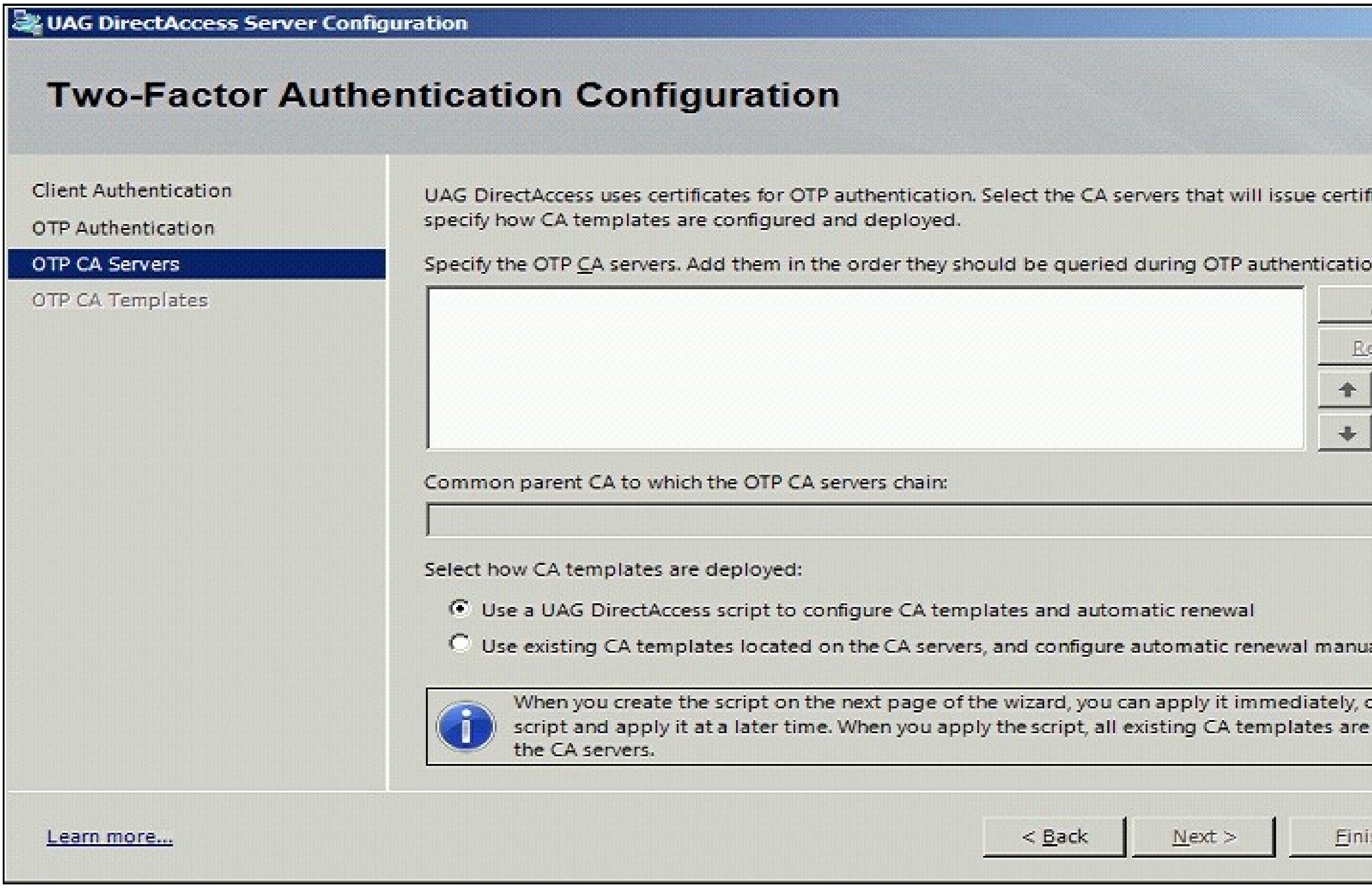
OTP authentication server: RADIUS

The OTP authentication servers can be edited and deleted in the Authentication and Authorization Servers dialog box, available in the Admin menu.

□ Require OTP user names to match Active Directory user names
With this setting enabled, users log on in UPN format (username@domain).

86.2.3 CA Server Configuration

Under OTP CA Servers click on Add and select the OTP CA Server.



UAG DirectAccess Server Configuration

Two-Factor Authentication Configuration

UAG DirectAccess uses certificates for OTP authentication. Select the CA servers that will issue certif
specify how CA templates are configured and deployed.

Specify the OTP CA servers. Add them in the order they should be queried during OTP authenticatio

Common parent CA to which the OTP CA servers chain:

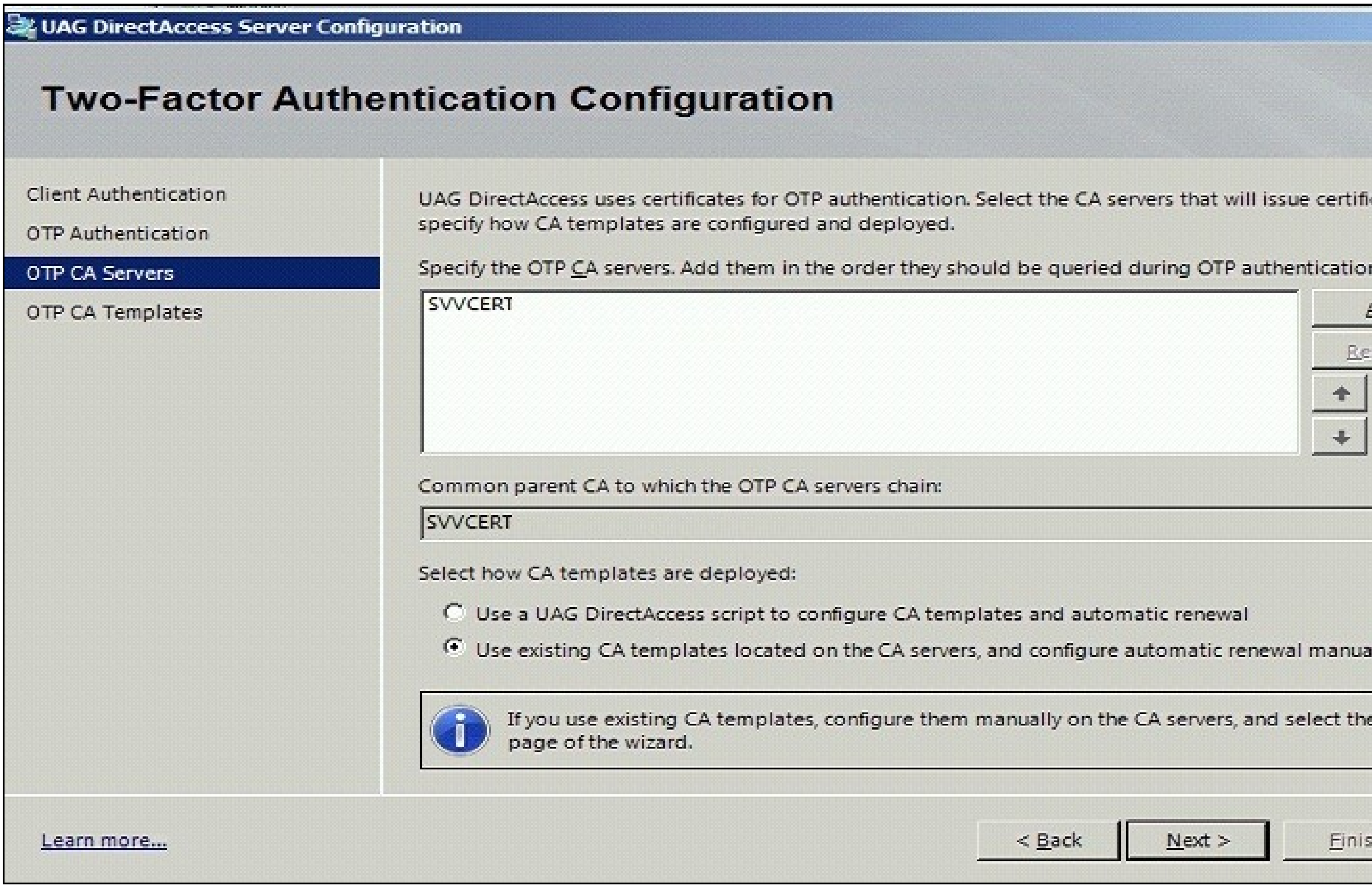
Select how CA templates are deployed:

● Use a UAG DirectAccess script to configure CA templates and automatic renewal

○ Use existing CA templates located on the CA servers, and configure automatic renewal manu

When you create the script on the next page of the wizard, you can apply it immediately, c
script and apply it at a later time. When you apply the script, all existing CA templates are
the CA servers.

This example is configured to use existing CA templates.



Two-Factor Authentication Configuration

UAG DirectAccess uses certificates for OTP authentication. Select the CA servers that will issue certifi
specify how CA templates are configured and deployed.

Specify the OTP CA servers. Add them in the order they should be queried during OTP authenticatio

SVVCERT

Common parent CA to which the OTP CA servers chain:

SVVCERT

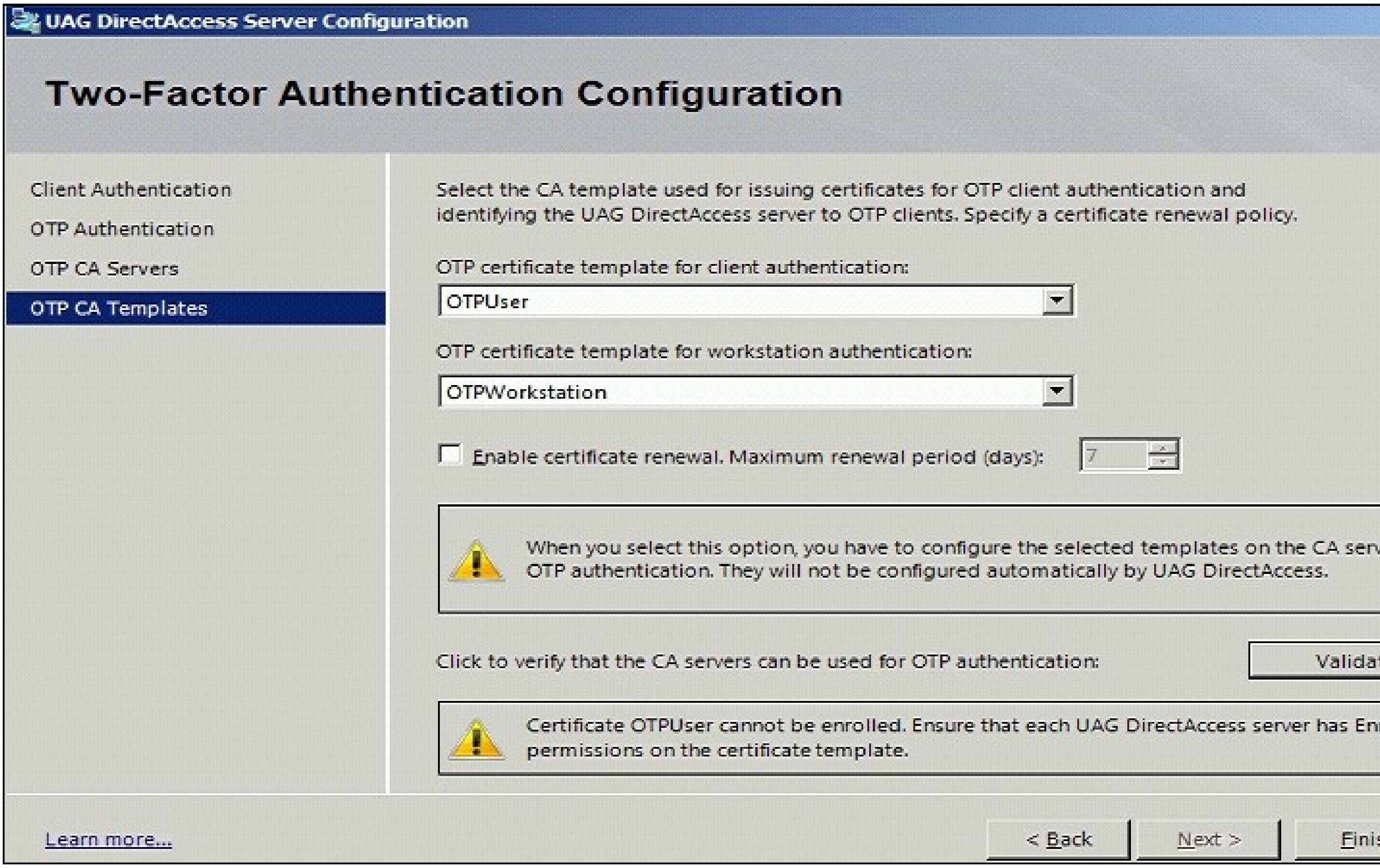
Select how CA templates are deployed:

○ Use a UAG DirectAccess script to configure CA templates and automatic renewal

● Use existing CA templates located on the CA servers, and configure automatic renewal manua

If you use existing CA templates, configure them manually on the CA servers, and select the
page of the wizard.

Select the required templates



UAG DirectAccess Server Configuration

Two-Factor Authentication Configuration

Select the CA template used for issuing certificates for OTP client authentication and identifying the UAG DirectAccess server to OTP clients. Specify a certificate renewal policy.

OTP certificate template for client authentication: OTPUser

OTP certificate template for workstation authentication: OTPWorkstation

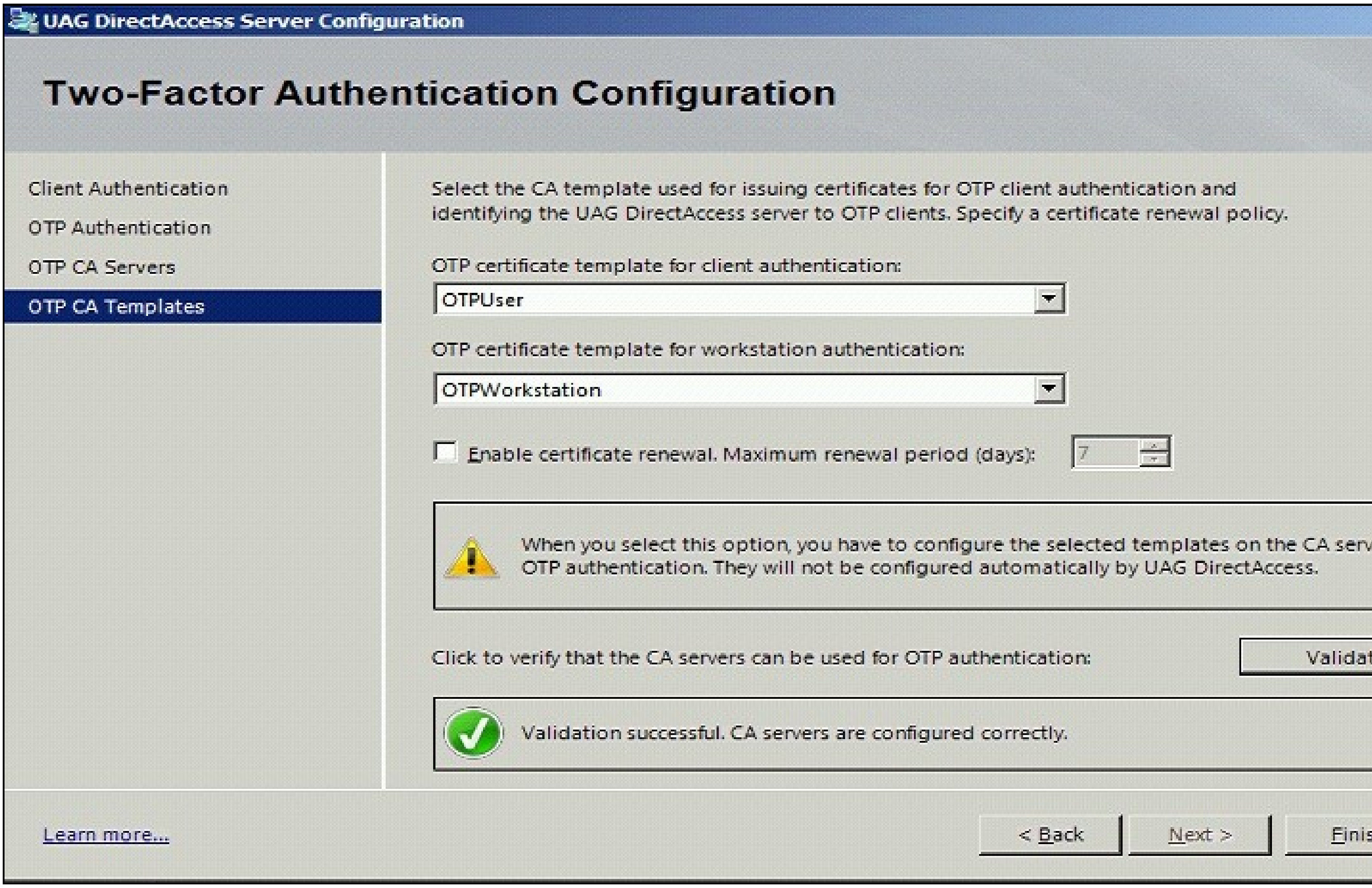
□ Enable certificate renewal. Maximum renewal period (days): 7

When you select this option, you have to configure the selected templates on the CA serv OTP authentication. They will not be configured automatically by UAG DirectAccess.

Click to verify that the CA servers can be used for OTP authentication: Validat

Certificate OTPUser cannot be enrolled. Ensure that each UAG DirectAccess server has En permissions on the certificate template.

Validate the CA templates



UAG DirectAccess Server Configuration

Two-Factor Authentication Configuration

Select the CA template used for issuing certificates for OTP client authentication and identifying the UAG DirectAccess server to OTP clients. Specify a certificate renewal policy.

OTP certificate template for client authentication: OTPUser

OTP certificate template for workstation authentication: OTPWorkstation

□ Enable certificate renewal. Maximum renewal period (days): 7

When you select this option, you have to configure the selected templates on the CA serv
OTP authentication. They will not be configured automatically by UAG DirectAccess.

Click to verify that the CA servers can be used for OTP authentication:

Validation successful. CA servers are configured correctly.

86.3 Additional Installation Options

87 Verifying the Installation

Access with the Direct Access client entering username, AD password and One Time Code. If the option to *Require OTP user names to match Active Directory user names* then the user name will be automatically populated.

Check the UAG and PINsafe logs for authentication messages.

88 Uninstalling the PINsafe Integration

89 Troubleshooting

90 Known Issues and Limitations

91 Additional Information

Microsoft DirectAccess

92 Microsoft Windows GINA login

93 Introduction

Windows GINA (graphical identification and authentication) is the login for Windows 2000 Server, 2003 Server and XP. Also available is the Windows GINA login User Guide.

The Winlogon GINA has been replaced in Vista, 2008 Server, Windows 7 and Windows 8, by the Windows Credential Provider, See Microsoft Windows Credential Provider Integration

The PINsafe GINA supports the use of Dual Channel (in advance, not on-demand) and Single Channel authentication for Terminal Services using Windows 2000 and 2003 server. It does not support an offline authentication mode, whereas the Windows Credential provider does, thus the PINsafe GINA should only be used for networked machines or for Terminal Services.

This version of the PINsafe GINA supersedes an earlier version which would overwrite the AD password. The current version of the PINsafe GINA does not overwrite the AD password.

94 Prerequisites

PINsafe 3.x

Recommended platform is Windows 2003 with Microsoft.Net Framework 2 and Terminal Services

A separate PINsafe GINA license is not required, but the users authenticating to PINsafe must be licensed.

Microsoft Visual C++ 2010 SP1 redistributable. For the 32-bit version of the GINA, the x86 redistributable is required. For the 64-bit version, **both** the x86 redistributable **and** the x64 redistributable are required. These must be installed before the GINA, as they are required by the installer.

PINsafe GINA 32 bit software

PINsafe GINA 64 bit software

NOTE: the latest version is version 3.6.1. This adds support for dual-channel message on-demand and allowing unknown users to authenticate without Swivel credentials.

95 Baseline

96 Architecture

The 64-bit GINA is the same as the (32-bit) Terminal Services GINA, except built for 64-bit operating systems.

97 Swivel Configuration

97.1 Configure a Swivel Agent

1. On the Swivel Management Console select Server/Agent

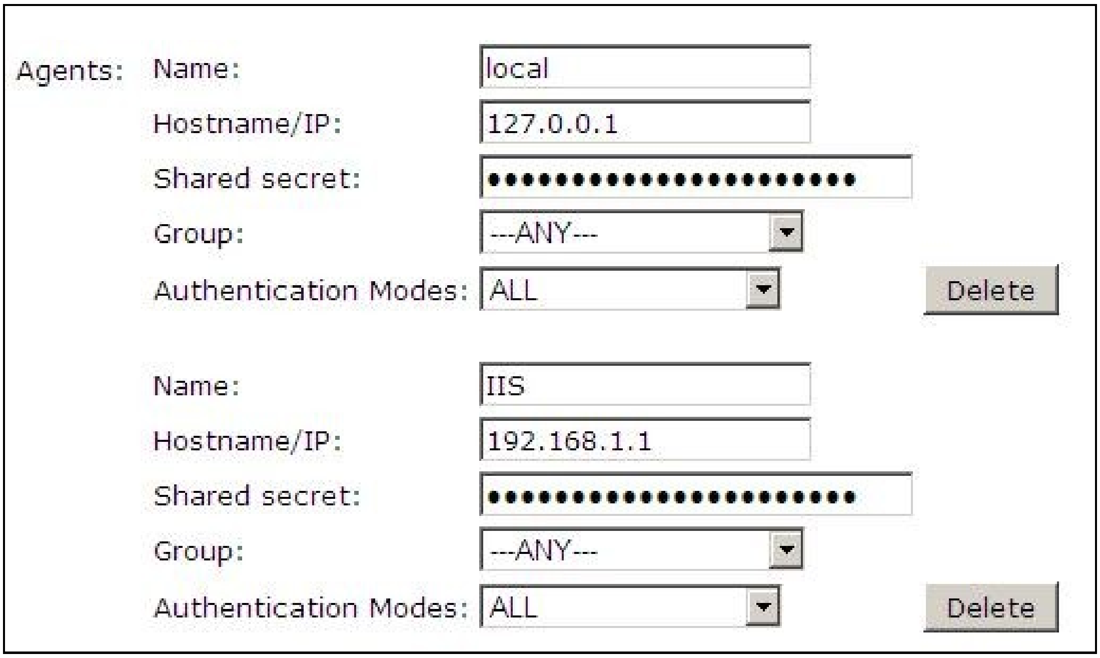
2. Enter a name for the Agent

3. Enter the GINA IP address. You can limit the Agent IP to an IP address range like: 192.168.0.0/255.255.0.0 where the mask of 255 requires an exact match and 0 allows any value, so the previous example would allow any Agent in the range 192.168, or you can use an individual IP address for the Credential Provider.

4. Enter the shared secret used above on the GINA

5. Enter a group, (Note in this instance ANY is not a valid group and will cause authentication to fail)

6. Click on Apply to save changes

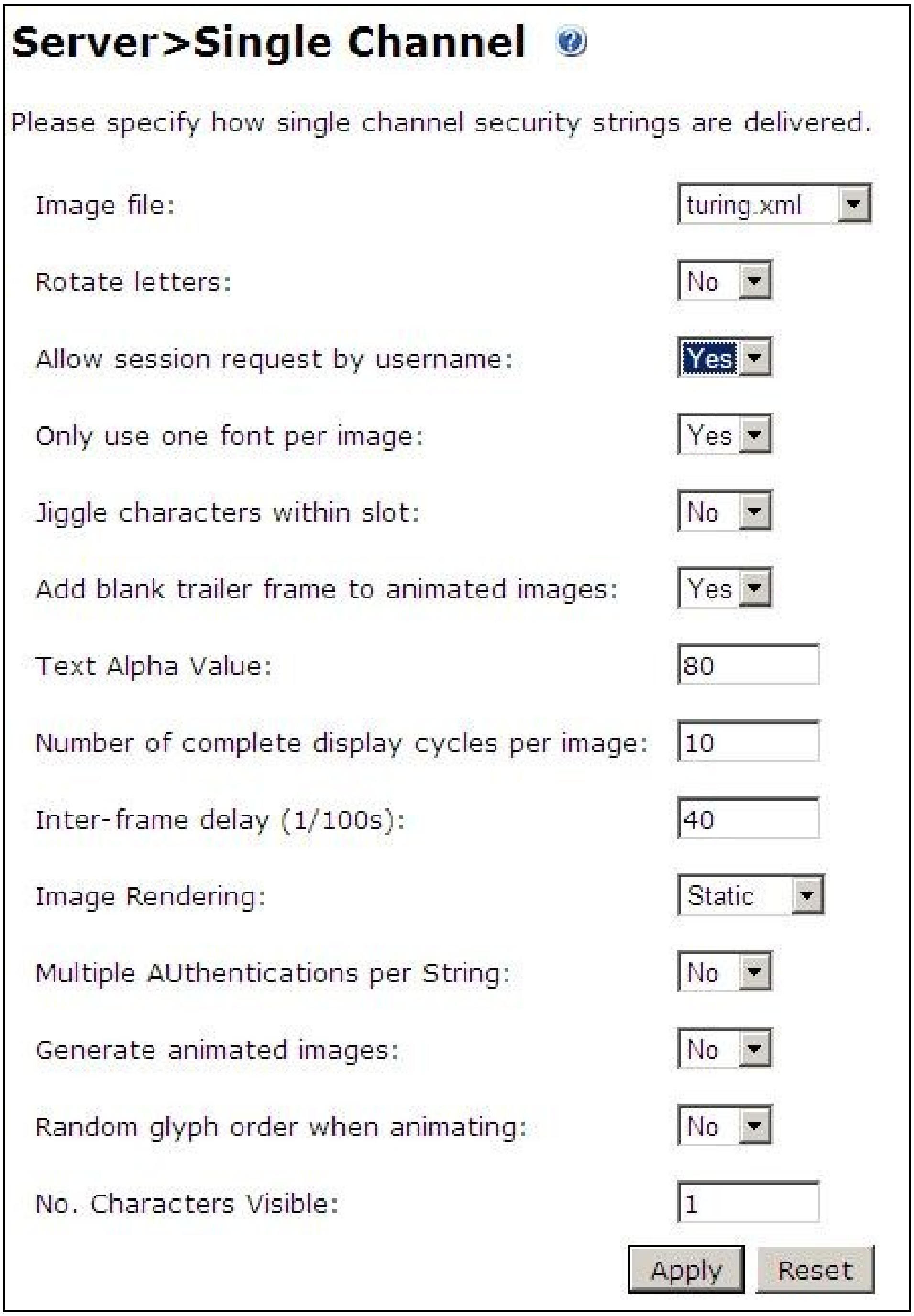


Agents:	Name:	local	
	Hostname/IP:	127.0.0.1	
	Shared secret:	••••••••••••••••••••••	
	Group:	---ANY---	
	Authentication Modes:	ALL	Delete
	Name:	IIS	
	Hostname/IP:	192.168.1.1	
	Shared secret:	••••••••••••••••••••••	
	Group:	---ANY---	
	Authentication Modes:	ALL	Delete

Configure Single Channel Access

1. On the PINsafe Management Console select Server/Single Channel

2. Ensure ?Allow session request by username? is set to YES



Server>Single Channel

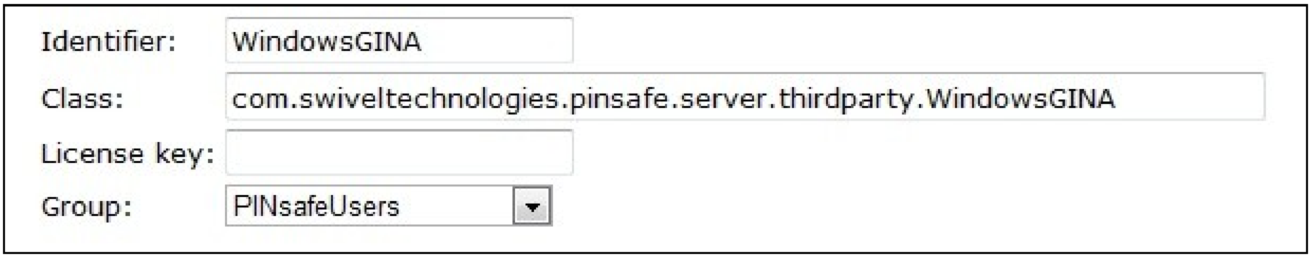
Please specify how single channel security strings are delivered.

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

97.2 Create a Third Party Authentication

A third party authentication must be created with an Identifier of WindowsGINA.

1. On the PINsafe Management Console select Server/Third Party Authentication
2. For the Identifier Name enter: WindowsGINA
3. For the Class enter: com.swiveltechnologies.pinsafe.server.thirdparty.WindowsGINA
4. For the License Key, leave this empty as it is not required
5. For the Group select a group of users
6. Click Apply to save the settings



Identifier:	WindowsGINA
Class:	com.swiveltechnologies.pinsafe.server.thirdparty.WindowsGINA
License key:	
Group:	PINsafeUsers

Note that this creates a GINA menu item, but there are no configurable options, so is not selectable.

98 Terminal Services GINA Integration

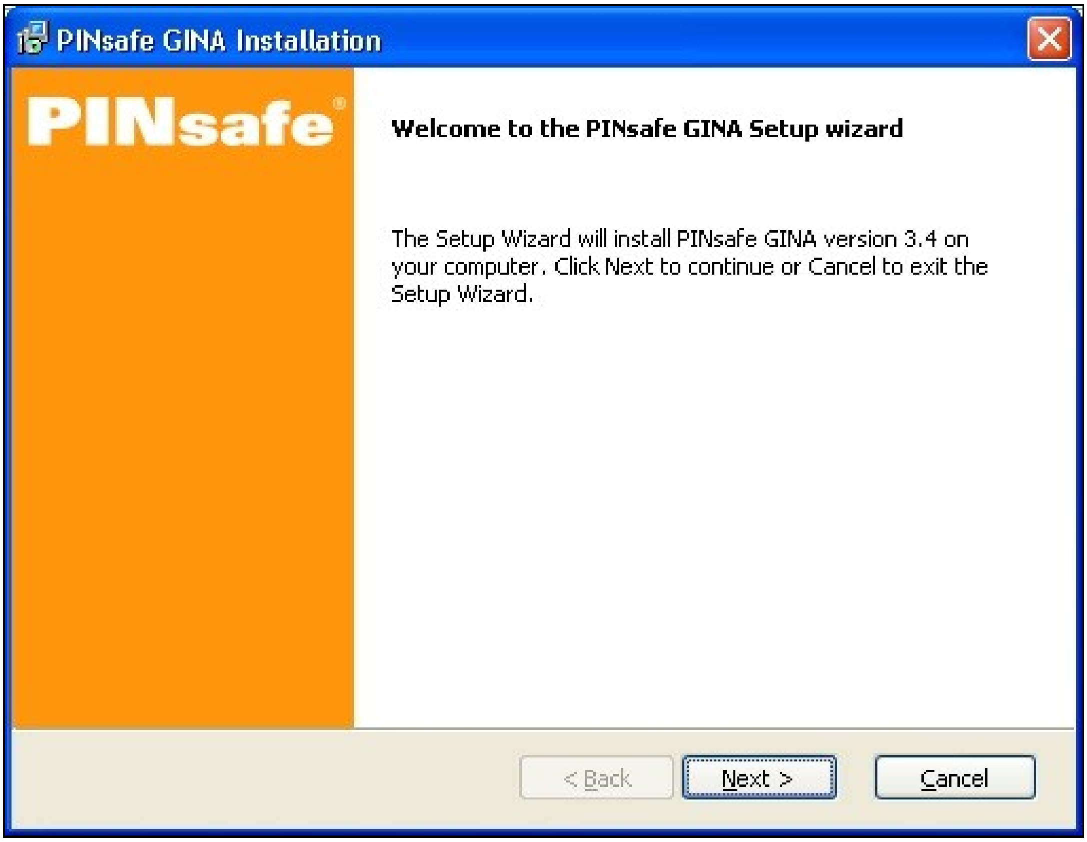
The PINsafe GINA Configuration utility provides a convenient means of configuring the installed PINsafe GINA.

Microsoft.Net 2 is only required for the configuration application. The GINA will work without .Net 2, but you will have to configure it manually. If your system does not meet the requirements, when you click "Next", you will see a dialog showing what components are missing. You can still install, but with the provisos mentioned above.

Install the GINA software on the Windows Terminal Server.

98.1 Terminal Services GINA Installation

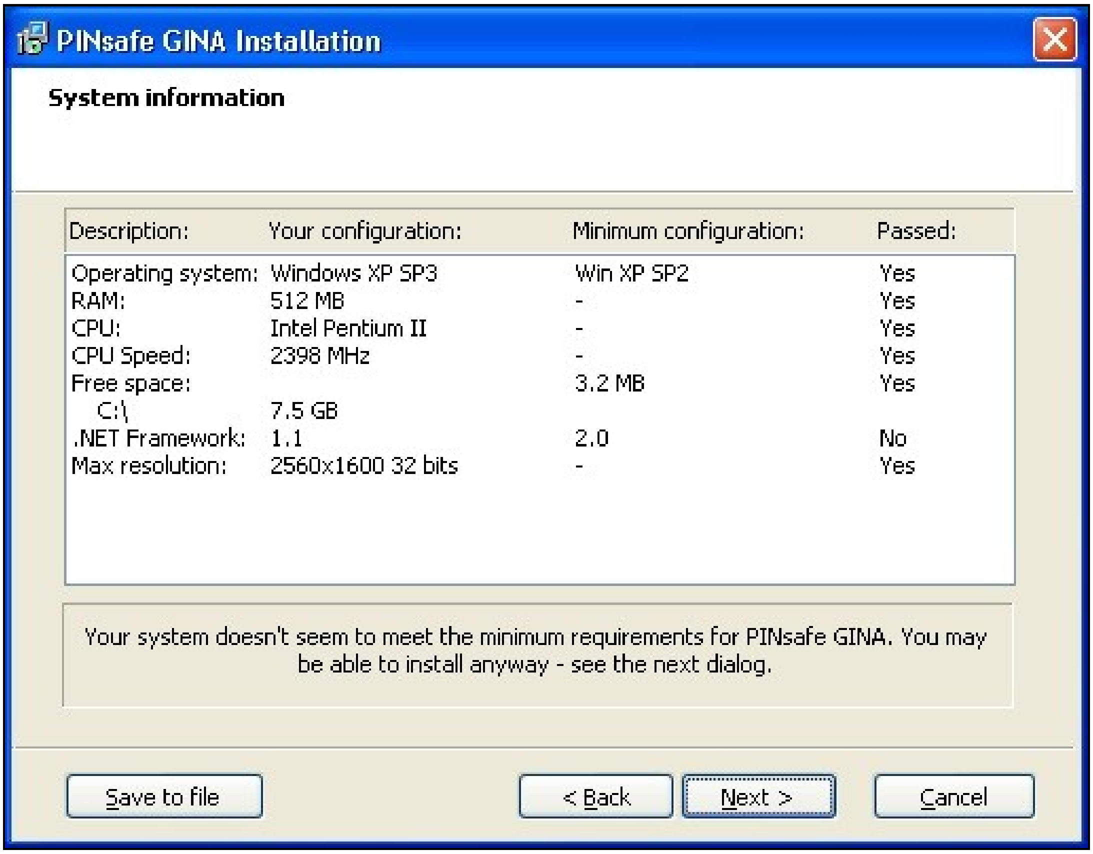
Start the PINsafe installation Wizard



Welcome to the PINsafe GINA Setup wizard

The Setup Wizard will install PINsafe GINA version 3.4 on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

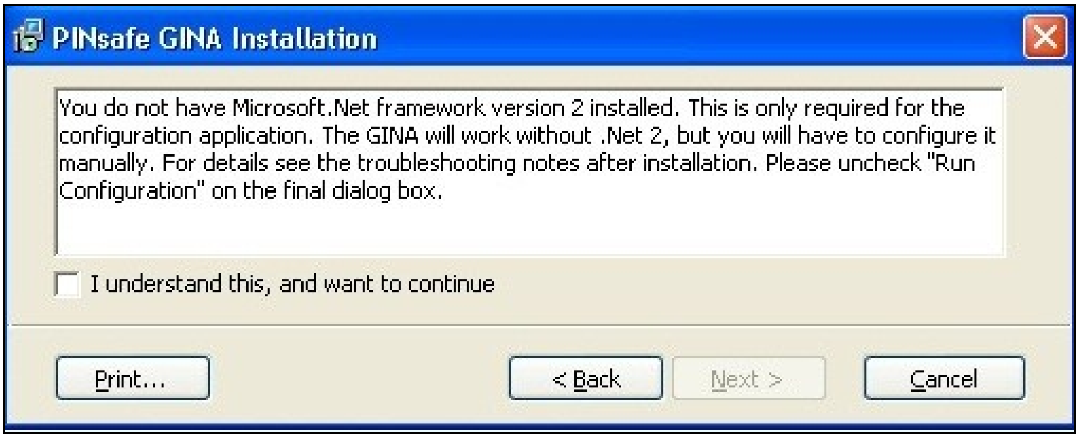
The system summary will report on any requirements which are not met, in this example .Net



```
Description:       Your configuration:     Minimum configuration:   Passed:
Operating system:  Windows XP SP3          Win XP SP2               Yes
RAM:               512 MB                  -                        Yes
CPU:               Intel Pentium II        -                        Yes
CPU Speed:         2398 MHz                -                        Yes
Free space:                                3.2 MB                   Yes
   C:\             7.5 GB
.NET Framework:    1.1                     2.0                      No
Max resolution:    2560x1600 32 bits       -                        Yes
```

Your system doesn't seem to meet the minimum requirements for PINsafe GINA. You may be able to install anyway - see the next dialog.

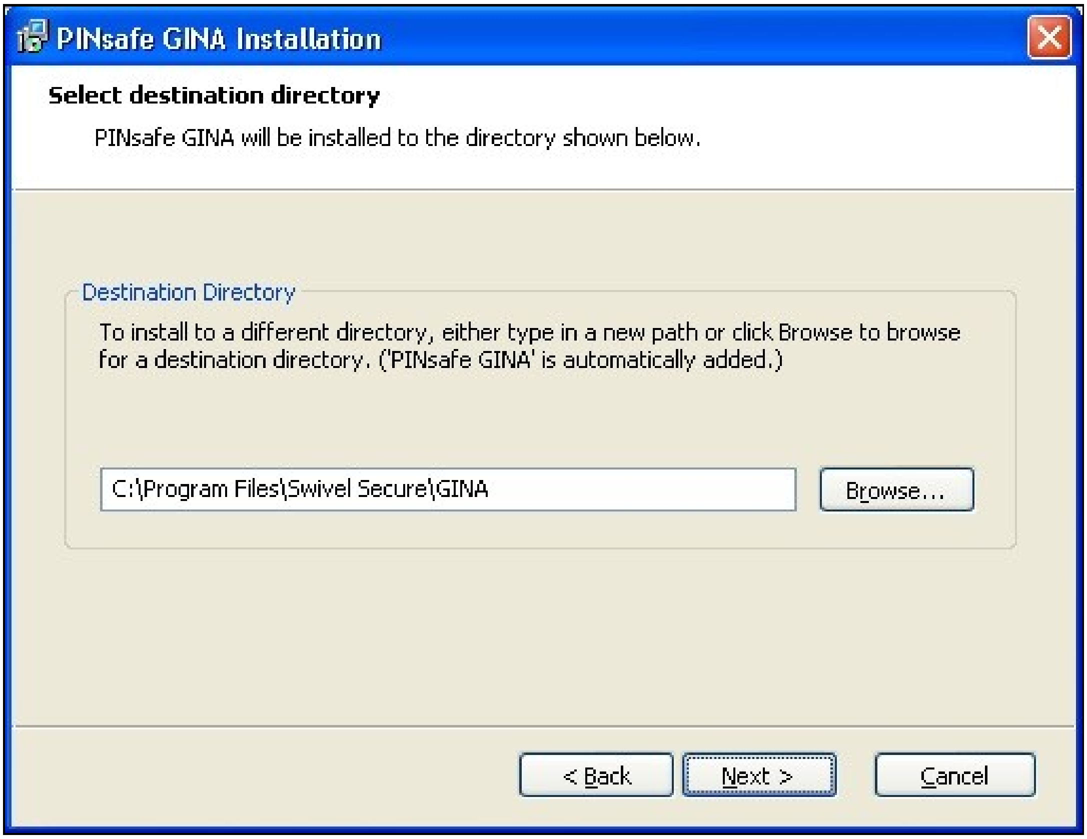
The PINsafe GINA may optionally be installed without .Net, the PINsafe GINA configuration utility requires .Net to install, but may be configured manually



You do not have Microsoft.Net framework version 2 installed. This is only required for the configuration application. The GINA will work without .Net 2, but you will have to configure it manually. For details see the troubleshooting notes after installation. Please uncheck "Run Configuration" on the final dialog box.

☐ I understand this, and want to continue

Select the install directory



PINsafe GINA Installation

Select destination directory

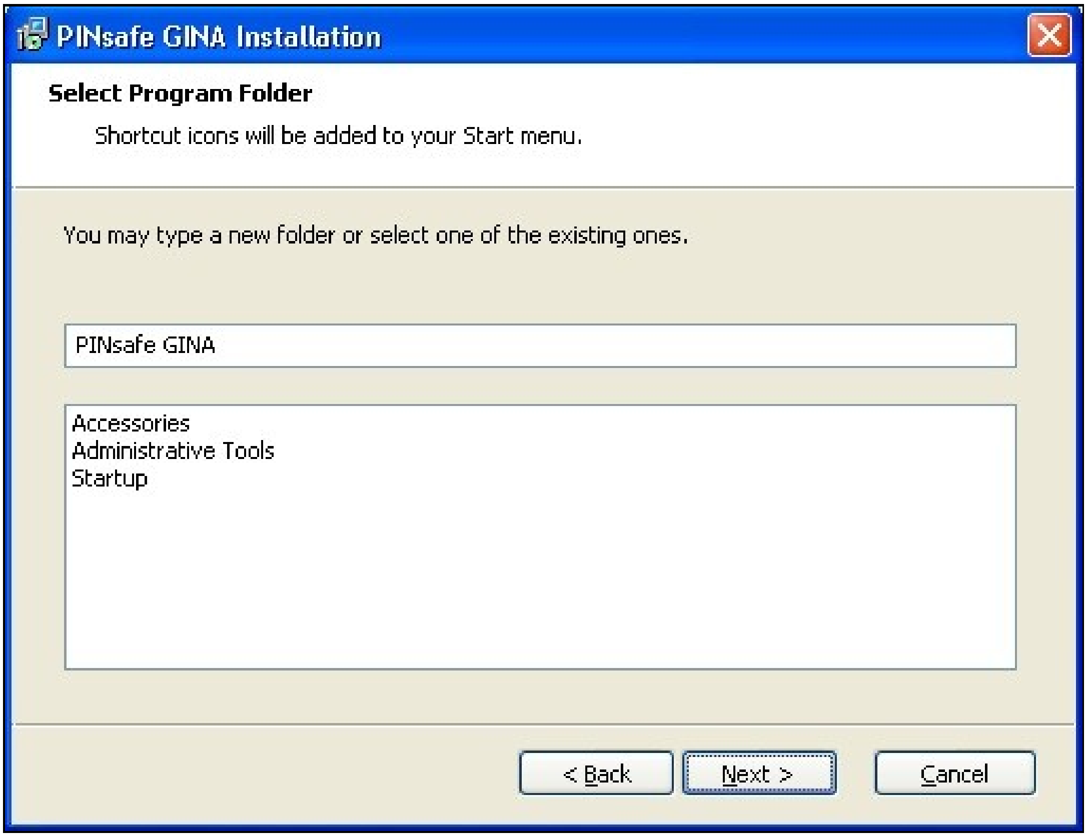
PINsafe GINA will be installed to the directory shown below.

Destination Directory

To install to a different directory, either type in a new path or click Browse to browse for a destination directory. ('PINsafe GINA' is automatically added.)

C:\Program Files\Swivel Secure\GINA

Select the Start Program files group



PINsafe GINA Installation

Select Program Folder

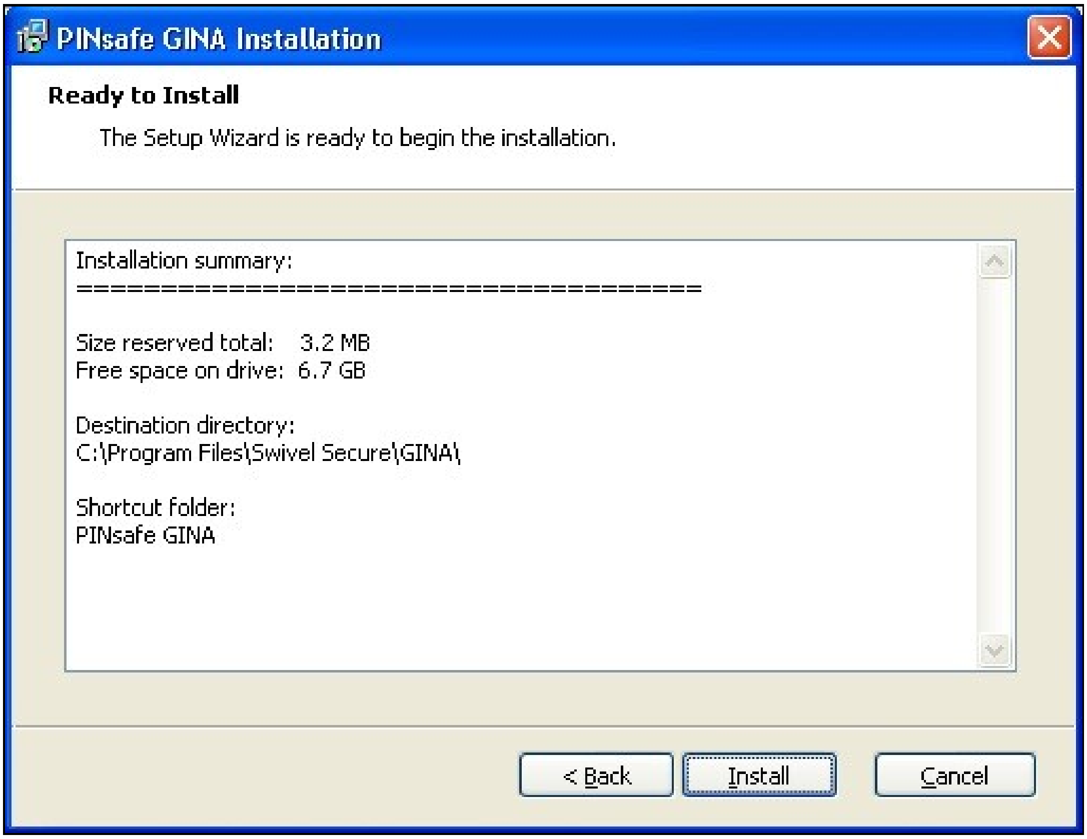
Shortcut icons will be added to your Start menu.

You may type a new folder or select one of the existing ones.

PINsafe GINA

Accessories
Administrative Tools
Startup

Check the installation details


PINsafe GINA Installation

Ready to Install

The Setup Wizard is ready to begin the installation.

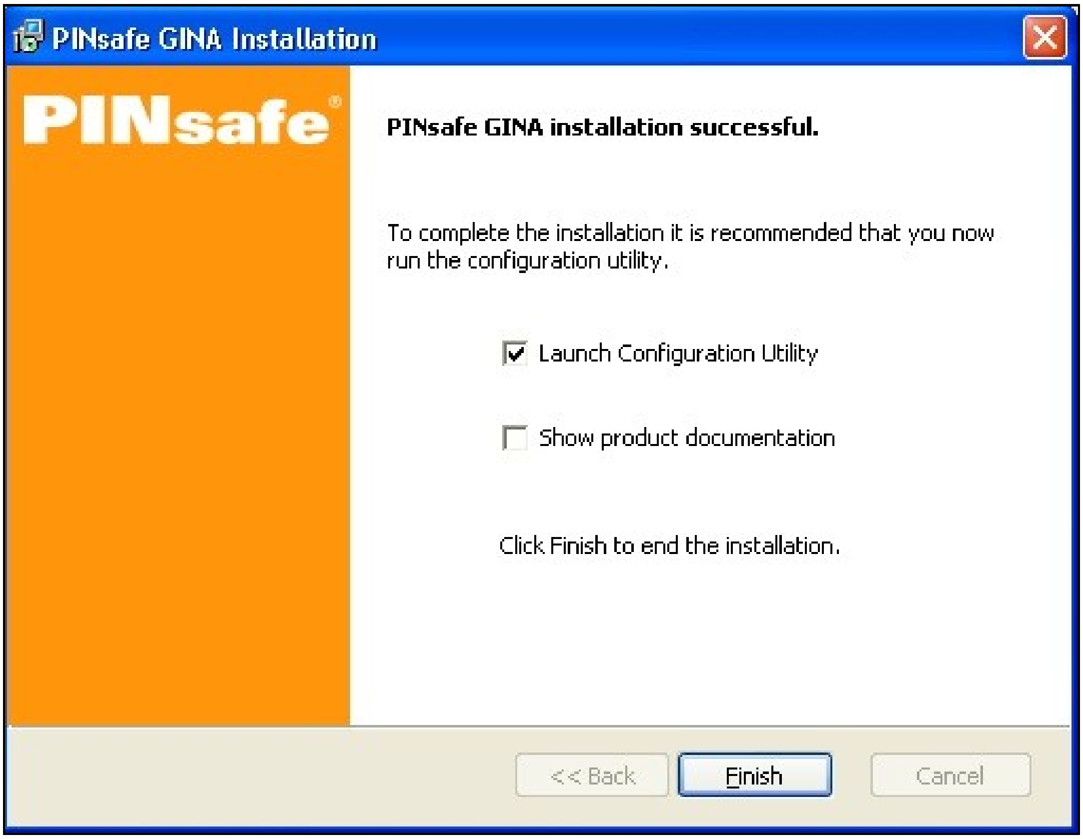
```
Installation summary:
=======================================

Size reserved total:    3.2 MB
Free space on drive:  6.7 GB

Destination directory:
C:\Program Files\Swivel Secure\GINA\

Shortcut folder:
PINsafe GINA
```

The PINsafe GINA installation reports when it is complete and allows the configuration utility to be run


PINsafe GINA Installation

PINsafe GINA installation successful.

To complete the installation it is recommended that you now run the configuration utility.

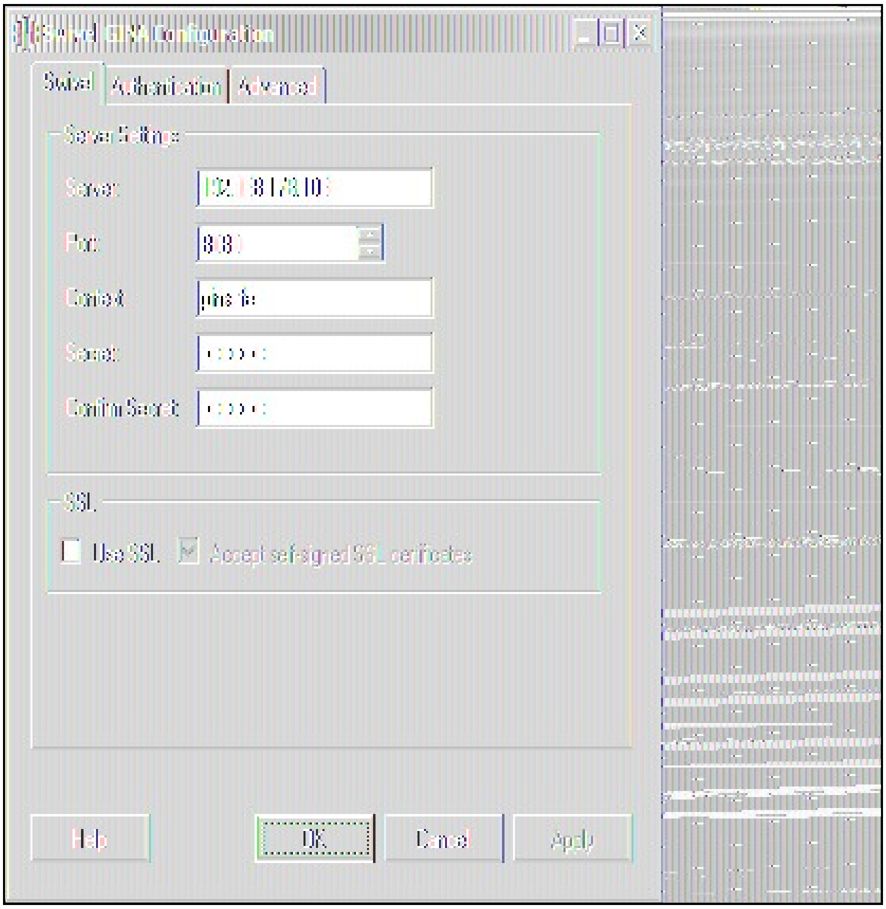
☑ Launch Configuration Utility

□ Show product documentation

Click Finish to end the installation.

98.2 Terminal Services GINA Configuration

98.2.1 Server Settings



Server Settings

Server: 192.168.178.100

Port: 8080

Context: pinsafe

Secret: ******

Confirm Secret: ******

SSL

□ Use SSL ☑ Accept self-signed SSL certificates

Server The IP address or hostname of the PINsafe server to use for authentication.

Port The TCP/IP port used by the PINsafe server. Commonly "8080" or "8443" if SSL is enabled.

Context The web application context used by the PINsafe server. Commonly "pinsafe" for standard installations.

Secret The shared secret configured for the GINA agent.

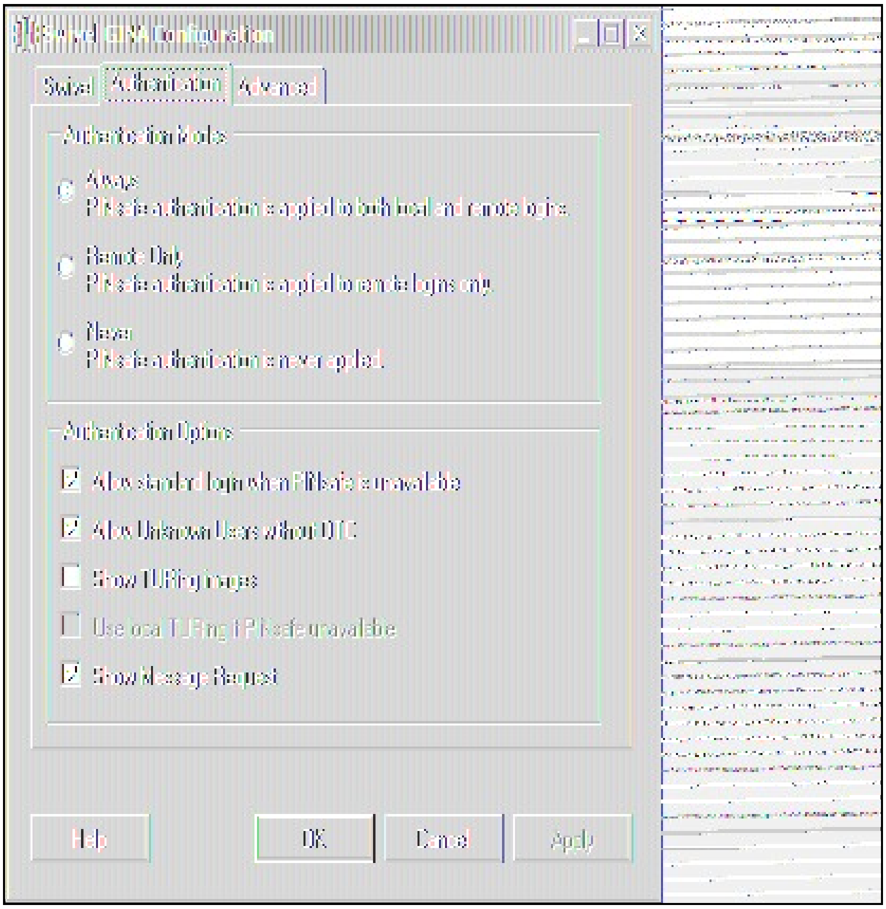
Confirm Secret Repeat the shared secret to ensure it has been entered correctly.

SSL

Use SSL Enable the use of SSL when communication with the PINsafe server. In order to use this option SSL must have been configured on the PINsafe server with an appropriate certificate.

Allow self-signed SSL certificates Accept an SSL certificate from the PINsafe server that has not been signed by a recognised certificate authority.

98.2.2 Authentication Settings



Swivel GINA Configuration

Swivel | Authentication | Advanced

Authentication Modes

● Always
PINsafe authentication is applied to both local and remote logins.

○ Remote Only
PINsafe authentication is applied to remote logins only.

○ Never
PINsafe authentication is never applied.

Authentication Options

☑ Allow standard login when PINsafe is unavailable

☑ Allow Unknown Users without OTC

□ Show TURing images

□ Use local TURing if PINsafe unavailable

☑ Show Message Request

Always Selecting this mode enables PINsafe authentication for local and remote logins.

Remote Only Selecting this mode enables PINsafe authentication for remote logins only. Local logins continue to only require a standard Windows username and password combination.

Never Selecting this mode disables the use of PINsafe authentication by the GINA.

Authentication Options

Allow standard login when PINsafe is unavailable When enabled this option temporarily disables PINsafe authentication if the GINA determines that the PINsafe server is not available for authentication.

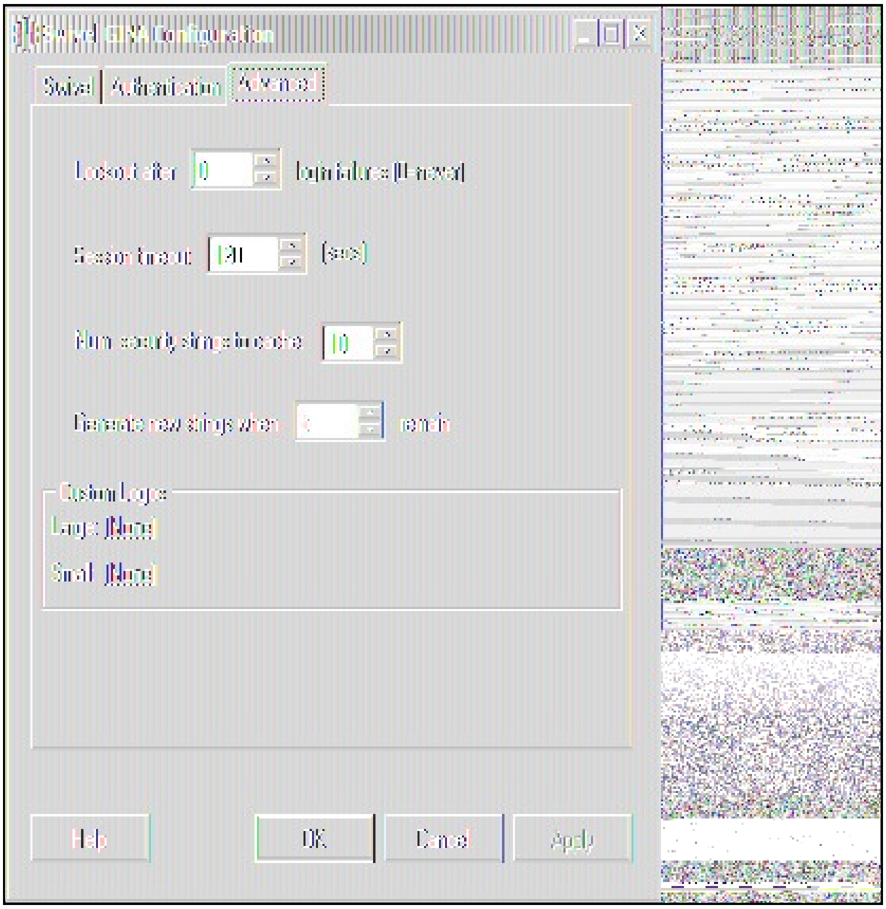
Allow unknown users without OTC When enabled, if a user is not known to PINsafe, they are not required to enter a one-time code to authenticate. There is no visible indication that the user is not known to PINsafe.

Show TURing images Enable the ability for users to request a single-channel TURing image from the PINsafe server.

Use local TURing if PINsafe unavailable When enabled, if the GINA is unable to connect to PINsafe, it will display a locally-generated TURing image to users who have previously authenticated to this computer. Users who have not previously authenticated on-line will not be able to authenticate.

Show Message Request When enabled, a button is shown to request a new security string to be sent to the user's designated transport (email or SMS). This cannot be selected together with TURing: disable TURing to use this option.

98.2.3 Advanced Settings



Swivel GINA Configuration

Swivel | Authentication | Advanced

Lockout after 0 login failures (0=never)

Session timeout: 120 (secs)

Num. security strings to cache 10

Generate new strings when [illegible] remain

Custom Logos

Large: (None)

Small: (None)

Lockout after # failures The number of authentication failures before a user is locked out. This only applies to local authentication: Swivel authentication is managed by policies on the Swivel Server.

Session timeout The length of time to wait before closing the login dialog.

Num. security strings to cache The number of security strings to request from the Swivel server for local authentication.

Generate new strings when # remain Controls the minimum number of cached local security strings.

Custom logos This allows you to re-brand the GINA with your own logos. The large logo is displayed when the GINA is first displayed, and must be 413 by 88 pixels. The small logo is displayed at the top of the login screen, and must be 413 by 72 pixels.

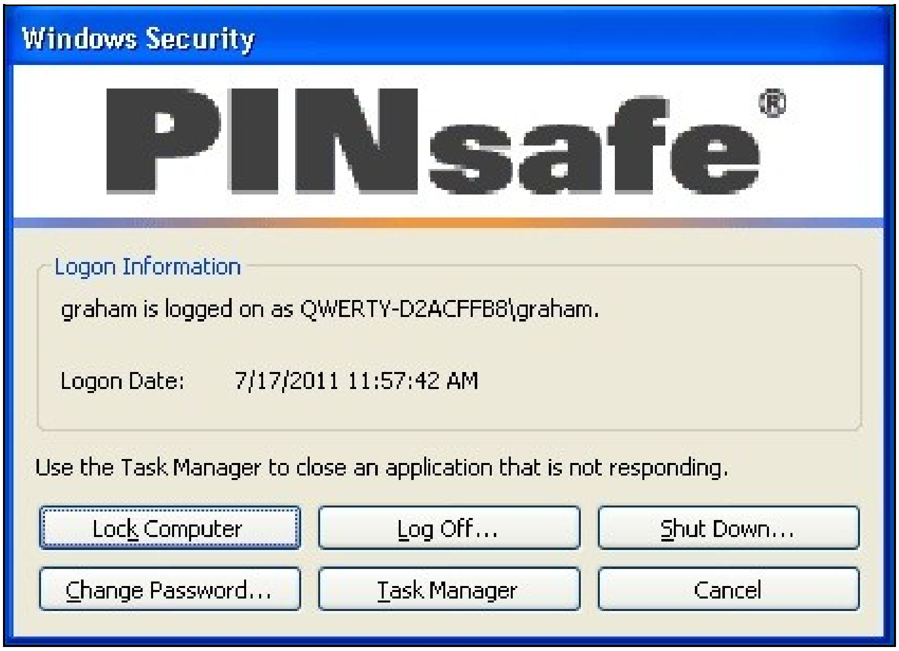
99 ChangePIN

Users may change their PIN using the Change Password option, or if automatically directed at login time.

Remember that to use ChangePIN, a user does not enter their PIN, but uses an OTC and generates a OTC for which they want the new PIN to be. Dual channel and mobile Phone Clients may be used with the ChangePIN as well as the TURing image.

99.1 User Requested ChangePIN using Change Password

From the Windows menu select Ctrl-Alt-Delete



Windows Security

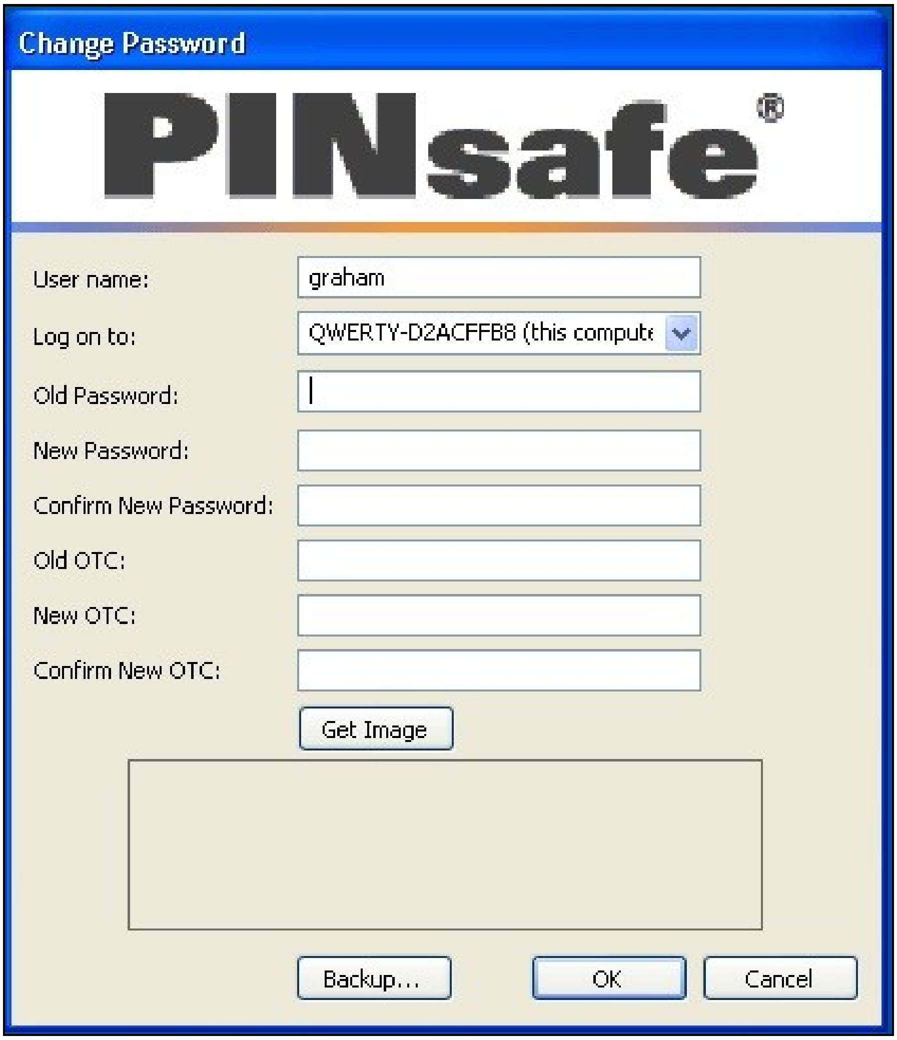
Logon Information

graham is logged on as QWERTY-D2ACFFB8\graham.

Logon Date: 7/17/2011 11:57:42 AM

Use the Task Manager to close an application that is not responding.

The user may change their PIN and or password. To ChangePIN, password details can be left blank.



Change Password

User name: graham

Log on to: QWERTY-D2ACFFB8 (this compute

Old Password:

New Password:

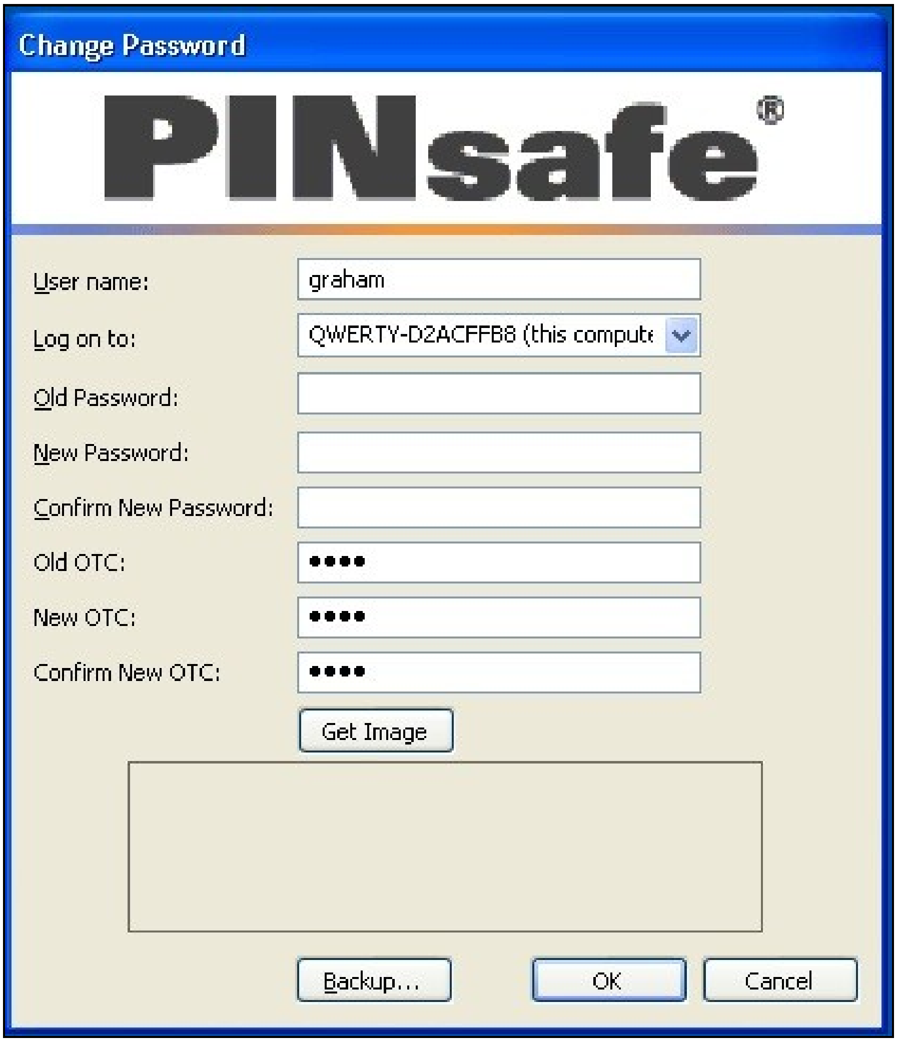
Confirm New Password:

Old OTC:

New OTC:

Confirm New OTC:

ChangePIN using dual channel or mobile phone client



Change Password

User name: graham

Log on to: QWERTY-D2ACFFB8 (this compute

Old Password:

New Password:

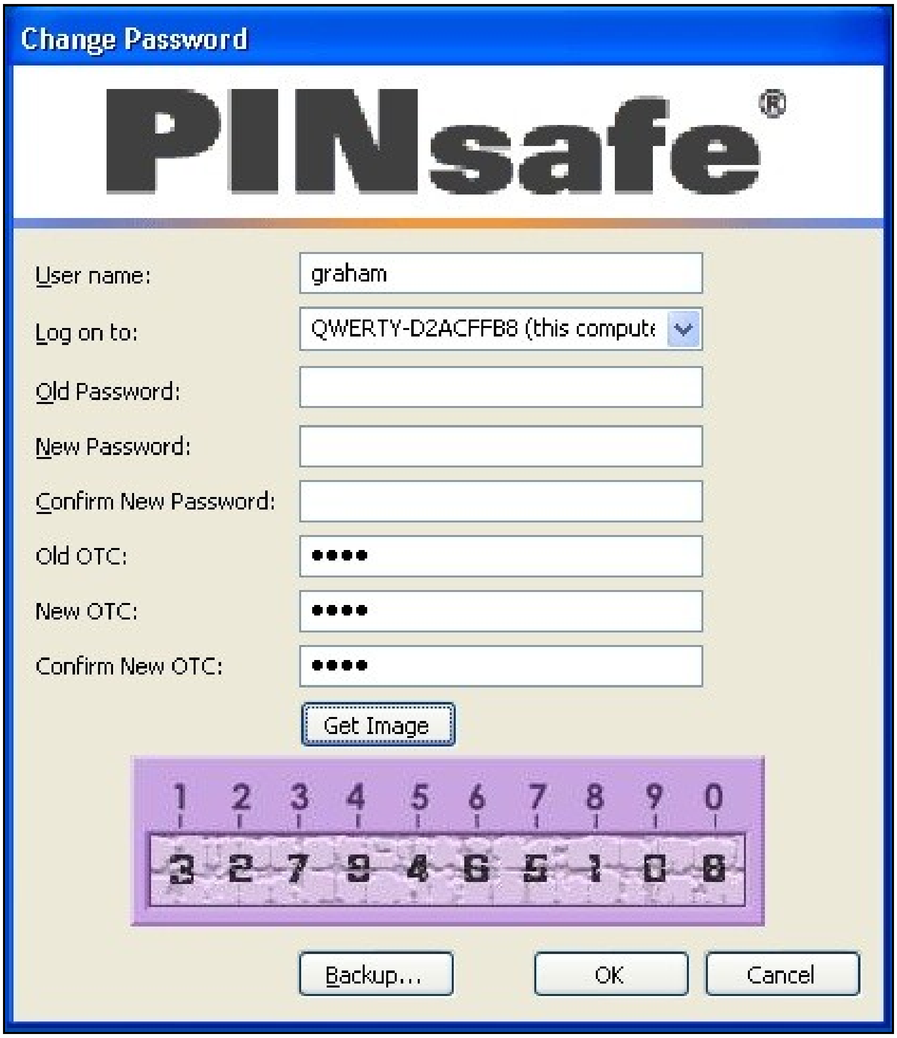
Confirm New Password:

Old OTC: ●●●●

New OTC: ●●●●

Confirm New OTC: ●●●●

ChangePIN using TURing



Change Password

User name: graham

Log on to: QWERTY-D2ACFFB8 (this comput

Old Password:

New Password:

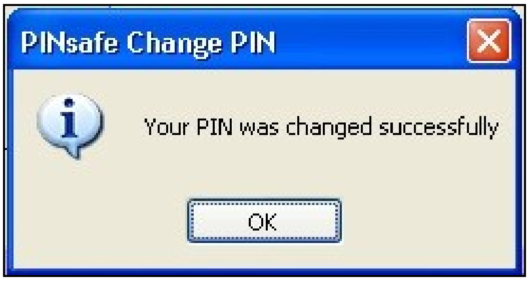
Confirm New Password:

Old OTC: ●●●●

New OTC: ●●●●

Confirm New OTC: ●●●●

ChangePIN successful

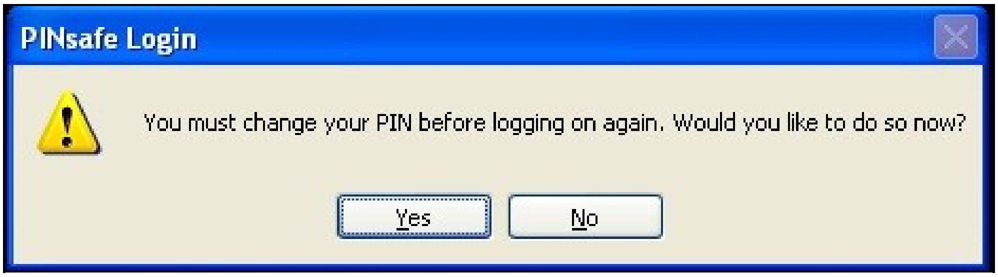


PINsafe Change PIN

Your PIN was changed successfully

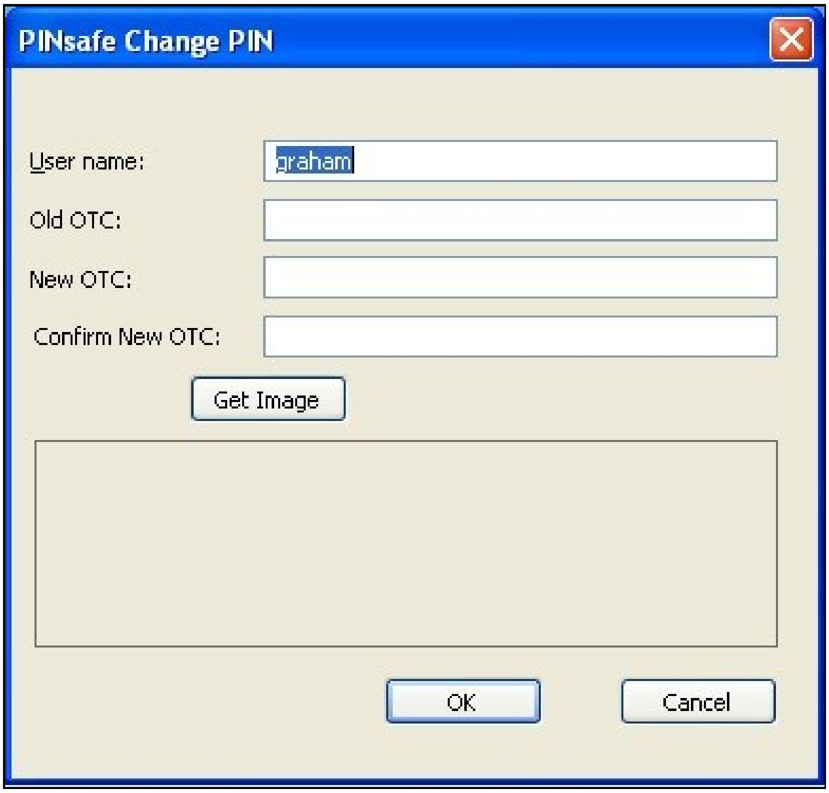
99.2 ChangePIN redirect at login

Where the user is required to ChangePIN the user is redirected at login.



PINsafe Login

You must change your PIN before logging on again. Would you like to do so now?



PINsafe Change PIN

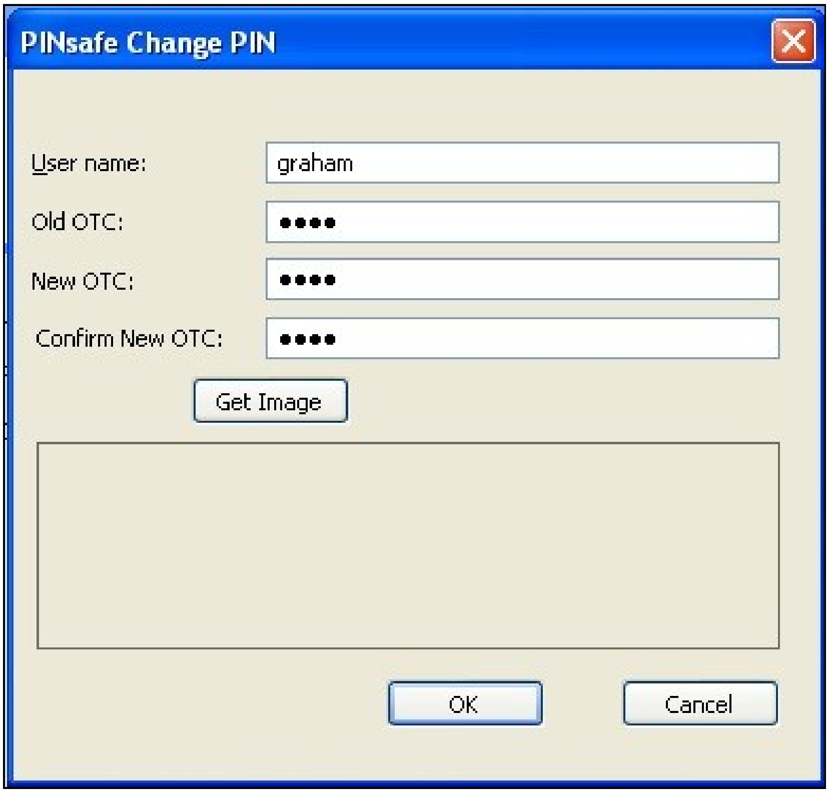
User name: graham

Old OTC:

New OTC:

Confirm New OTC:

ChangePIN using dual channel or mobile phone client



PINsafe Change PIN

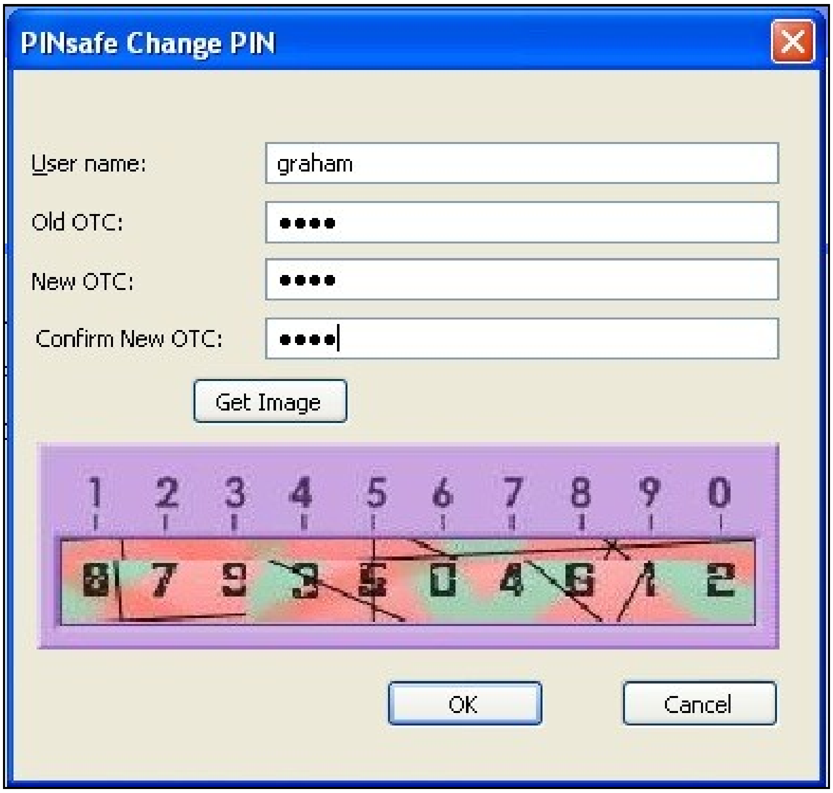
User name: graham

Old OTC: ●●●●

New OTC: ●●●●

Confirm New OTC: ●●●●

ChangePIN using TURing



PINsafe Change PIN

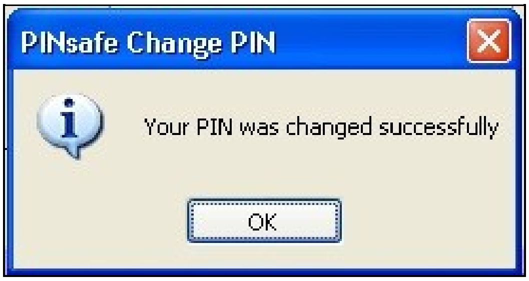
User name: graham

Old OTC: ●●●●

New OTC: ●●●●

Confirm New OTC: ●●●●

ChangePIN successful



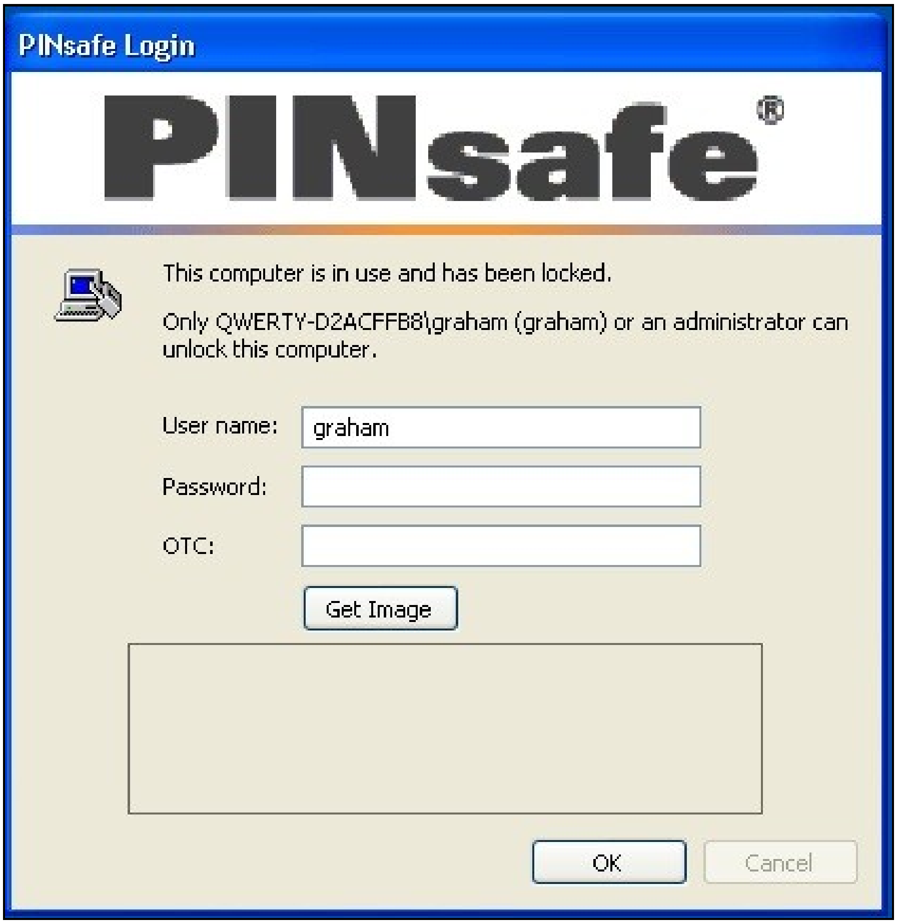
PINsafe Change PIN

Your PIN was changed successfully

100 Additional Installation Options

101 Verifying the Installation

When a user logs out they should be prompted for PINsafe authentication



PINsafe Login

This computer is in use and has been locked.

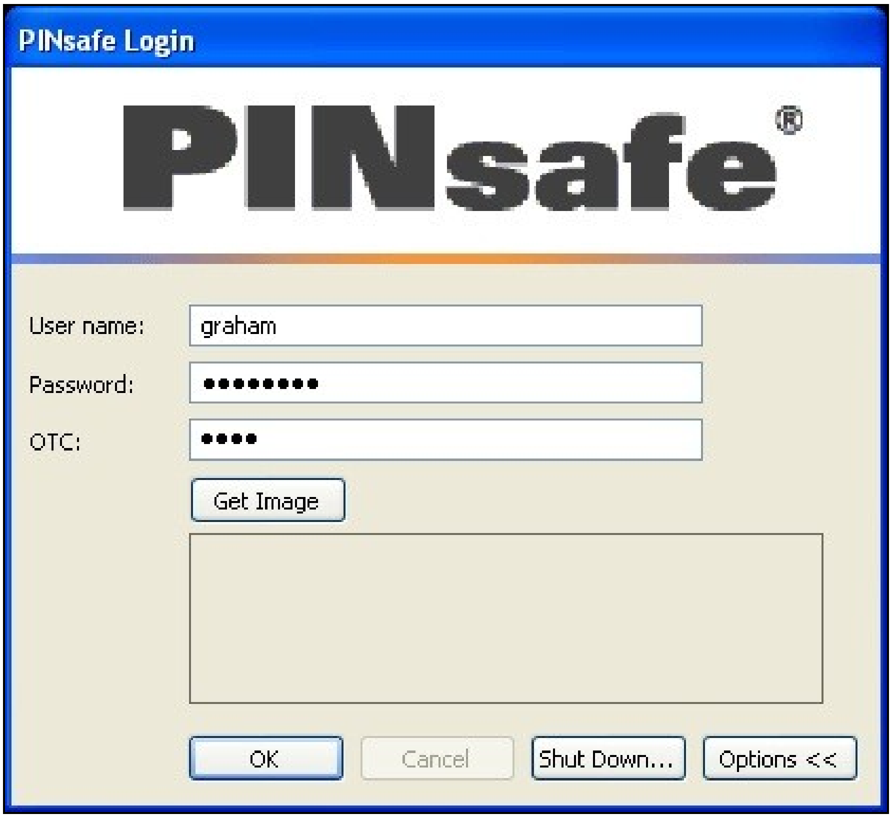
Only QWERTY-D2ACFFB8\graham (graham) or an administrator can unlock this computer.

User name: graham

Password:

OTC:

A user may use dual channel authentication to login by entering AD password and One Time Code.



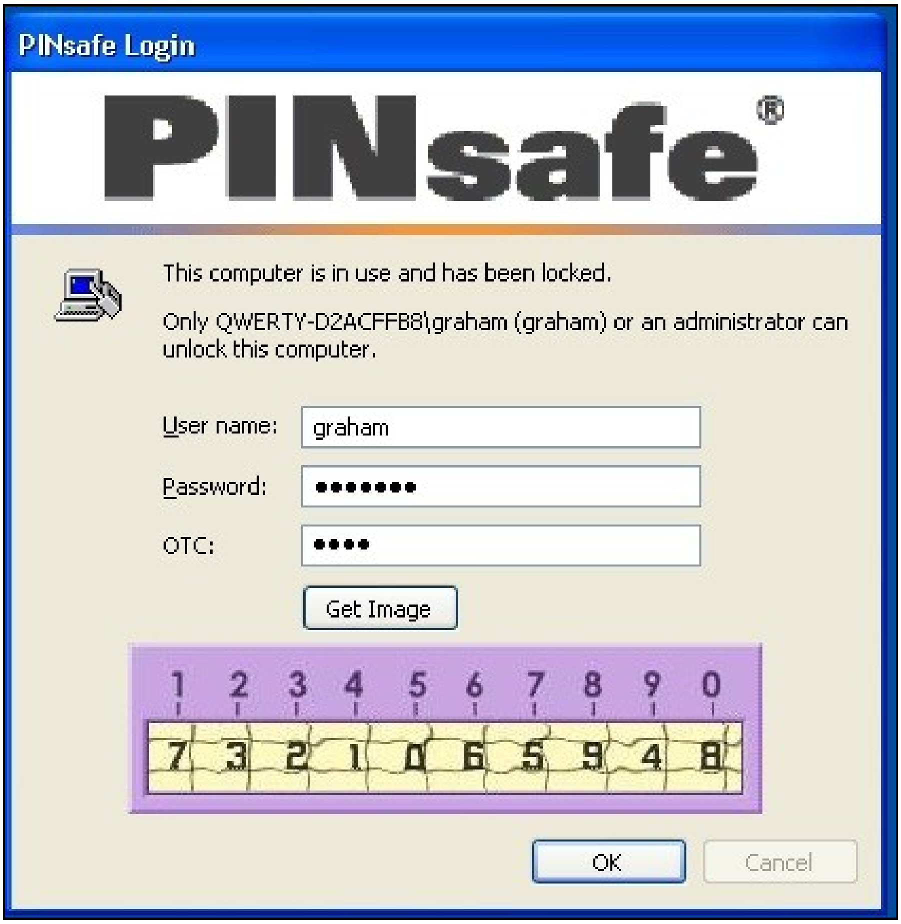
PINsafe Login

User name: graham

Password: •••••••••

OTC: ••••

A user can also authenticate using single channel by generating a TURing image.


PINsafe Login

This computer is in use and has been locked.

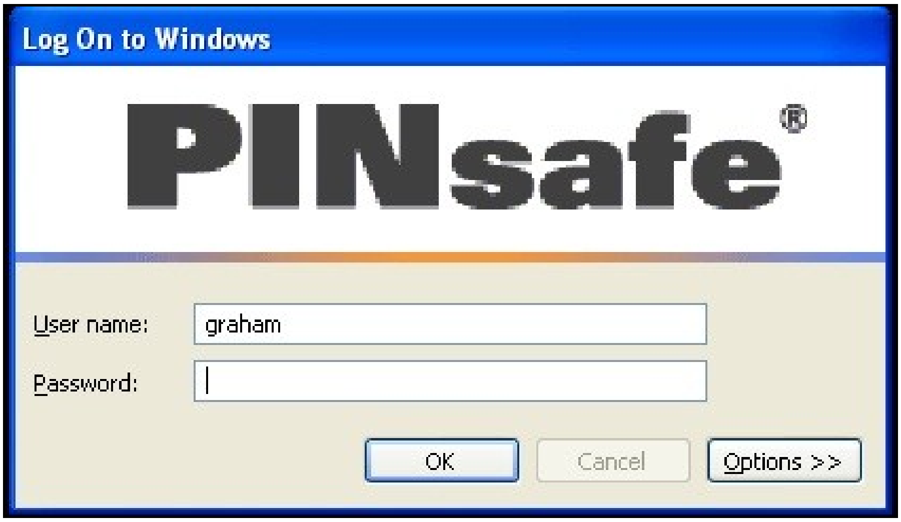
Only QWERTY-D2ACFFB8\graham (graham) or an administrator can unlock this computer.

User name: graham

Password: ●●●●●●●●

OTC: ●●●●

Standard authentication when the PINsafe server cannot be contacted.


Log On to Windows

User name: graham

Password:

102 Uninstalling the PINsafe Integration

To uninstall the PINsafe GINA select Start, Programs, PINsafe GINA, PINsafe GINA Uninstaller or Start, Control panel, Add or Remove Programs, select PINsafe GINA then remove.

Follow the instructions to remove the PINsafe installation.

103 Troubleshooting

PINsafe login options not displayed

If the "Allow standard login when PINsafe is unavailable" is enabled then the GINA will only display PINsafe login options if it is able to contact the PINsafe server. If PINsafe options are not displayed check the server settings and connectivity to the PINsafe server.

Manually configuring the PINsafe GINA

If it is not possible to use the configuration utility the PINsafe GINA settings may be edited manually in the registry. The following values found within the "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowNT\CurrentVersion\WinLogon" key are used by the GINA:

PINsafeServer

PINsafePort

PINsafeContext

PINsafeSecret

PINsafeProtocol

PINsafeLoginSelect

PINsafeShowTURing

PINsafeAllowDefaultLogin

PINsafeAllowSelfCert

Disabling the PINsafe GINA

If the PINsafe GINA fails to load correctly it can be disabled using the following process:

Using the F8 boot menu start Windows in safe mode

Using regedit.exe remove the "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowNT\CurrentVersion\WinLogon\ginadll" registry value

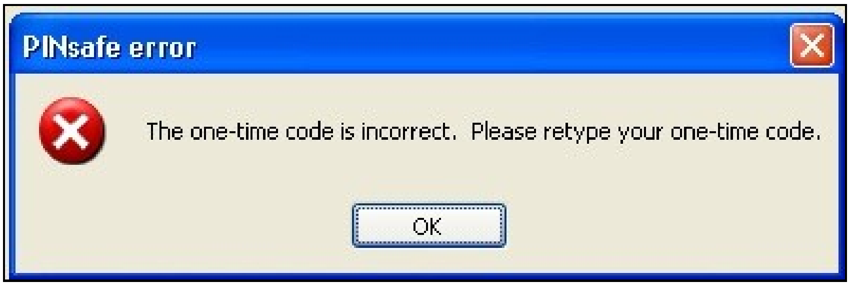
Reboot Windows

Following this process the standard Windows GINA should be restored allowing access.

103.1 Error Messages

The one-time code is incorrect. Please retype your one-time code

The One Time Code is incorrect

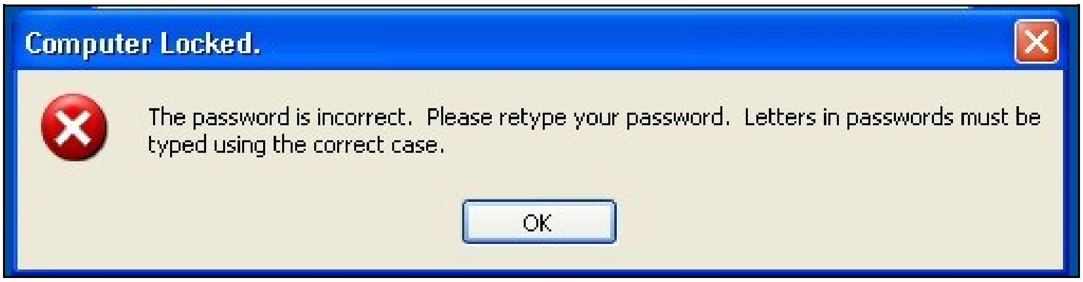


PINsafe error

The one-time code is incorrect. Please retype your one-time code.

The password is incorrect. Please retype your password. Letters in passwords must be typed using the correct case.

The Active Directory Password is incorrect

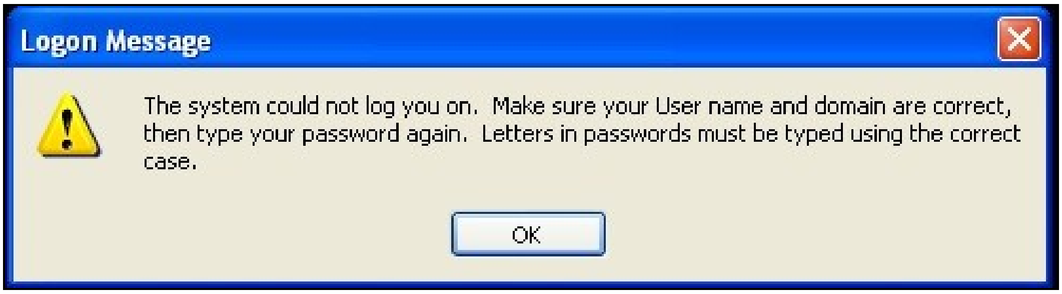


Computer Locked.

The password is incorrect. Please retype your password. Letters in passwords must be typed using the correct case.

The system could not log you on. Make sure your username and domain are correct, then type your password again. Letters in passwords must be typed using the correct case.

The PINsafe account may be locked contact the PINsafe system Administrator



Logon Message

The system could not log you on. Make sure your User name and domain are correct, then type your password again. Letters in passwords must be typed using the correct case.

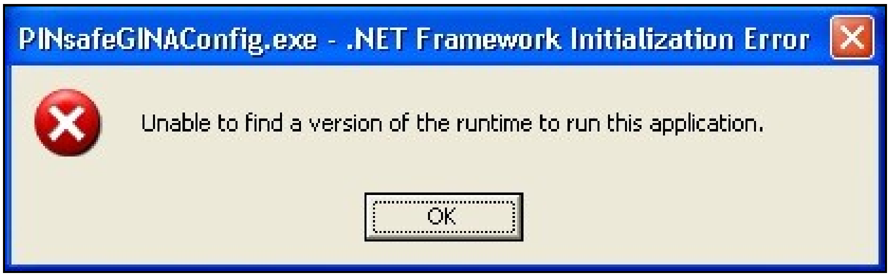
To recover a locked system protected by PINsafe see PINsafe GINA

Installing without Microsoft.Net Framework 2.0

The GINA itself does not require the .Net Framework - only the configuration utility. Therefore, if you are unwilling to install Microsoft.Net 2.0, you can ignore the warning about this being missing and install GINA anyway. However, you will have to configure the application manually, as described below.

Unable to find a runtime of the runtime to run this application

The PINsafe configuration utility is being un without the .Net version 2.0



PINsafeGINAConfig.exe - .NET Framework Initialization Error

Unable to find a version of the runtime to run this application.

FLUSHING_IMAGE_CACHE, ClientAbortException: java.net.SocketException: Connection reset

This error message can be seen in the PINsafe log when a Windows login is attempting to use an animated gif. Turn off animated gifs and switch to 'Static', on Swivel - This is set under Server > Single Channel > Image Rendering.

The third party class could not be found

This error can also be created when the Swivel Administration console Server/Agents, Group is set to Any. A group should be specified.

104 Known Issues and Limitations

Installation on a Windows 2003 server without Terminal Services, will only provide administrator logon, and only 3 simultaneous logins (including the console session).

Installation on Windows XP will work, but only one user can log on at a time, and then only if no-one is logged on directly to the machine.

There is a usability issue with Windows 2000: it takes about 20 seconds to display a TURing image. For this reason, we are not supporting Windows 2000 in this release, and recommend that if you absolutely have to use it, you should use Dual Channel only.

The following are not supported for Single Channel Authentication when using the Windows GINA:

- BUTton
- PATtern
- Animated Gifs

Dual channel on-demand is not supported.

The Windows GINA menu item is present, but there are no configurable options, so is not selectable.

105 Additional Information

106 Category:IAG

107 Category:IIS

108 Category:ISA

109 Microsoft IAG Integration

109.1 Introduction

This document covers the integration of PINsafe with the Microsoft Intelligent Application Gateway.

109.2 Prerequisites

PINsafe 3.x

Microsoft IAG

The IAG integration guide can be found here: IAG SP1 Integration Guide and here SP2 Integration Guide

109.3 Baseline

109.4 Architecture

109.5 Installation

109.5.1 PINsafe Integration Configuration

109.5.2 Access Device or Application Integration

109.5.3 Additional Installation Options

109.6 Verifying the Installation

109.7 Uninstalling the PINsafe Integration

109.8 Troubleshooting

109.9 Known Issues and Limitations

109.10 Additional Information

110 Microsoft IAG Multiple Authentication

110.1 PINsafe and IAG/UAG Integration using multiple repositories

This article explains how to use PINsafe with Microsoft IAG/UAG so that different applications are available to users depending on how they authenticated.

These notes are based on IAG Version 3.7 and PINsafe Version 3.6

This article shows the approach required to add this functionality to a standard IAG/UAG and PINsafe integration. Standard integration notes are available from the Microsoft IAG Integration guide and should also be referred to.

110.2 Approach

The approach is to create two different repositories on the IAG. One repository will use Agent-XML for authentication the other will use RADIUS.

One repository will be associated with single channel authentication, the other with dual channel authentication.

The login page will determine which repository the user is authenticating based on whether the user has requested a single channel (TURing) image or not.

The IAG will be configured to allow access to specific applications based on the repository a user has authenticated to.\

On the PINsafe server the NAS or Agent associated with the IAG Dual channel repository will be set to accept dual channel authentication only.

110.3 Implementation

The names used for repositories etc are just examples, but sometimes names are important, eg the repository of type "other" needs to have the same name as the associated .inc file and needs to reflected in the checkradio() function in PinsafeLogin.asp

110.3.1 PINsafe Configuration

In this example radius will be used for dual channel authentications only so on the PINsafe server

Enable RADIUS server

Create a NAS entry for the IAG

Set ip address and shared secret as required

Set mode to dual channel only for the NAS

Create an Agent entry for the IAG

Set ip address and shared secret as required

110.3.2 IAG Repository Configuration

Copy images.asp to von\IntnernalSite\Images\CustomUpdate

Ensure that it is the version that can also handle index images and ensure that the IP addresses etc match the PINsafe server

```
if request.querystring("index") <> "" then
  Set objWinHttp = Server.CreateObject("WinHttp.WinHttpRequest.5")
  objWinHttp.Open "GET", "http://127.0.0.1:8080/pinsafe/DCIndexImage?username="&request.querystring("username"), false
else
  Set objWinHttp = Server.CreateObject("WinHttp.WinHttpRequest.5")
  objWinHttp.Open "GET", "http://127.0.0.1:8080/pinsafe/SCImage?username="&request.querystring("username"), false
end if
```

Create a new Repository called pinsafe of type other.

Copy the pinsafe.inc file to von\InternalSite\inc\CustomUpdate

Edit pinsafe.inc so that the secret (m_secret), ip address and port matches that of the PINsafe server

```
function checkswivelpwd (userName, password)
LIGHT_TRACE "checkswivelpwd entered for " & userName
LIGHT_TRACE "SWIVEL - lets check if the password is right"
Dim strHTML
m_secret = "secret"
Dim objWinHttp
m_request = "<?xml version=""1.0"" ?><SASRequest><Version>1.0</Version><Action>login</Action><Username>" & username & "</Username><OTC>" & pa
& m_secret & "</Secret></SASRequest>"
Set objWinHttp = Server.CreateObject("WinHttp.WinHttpRequest.5")
objWinHttp.Open "GET", "http://<ipaddress>:8080/pinsafe/AgentXML?xml=" & m_request, false
```

Create a new Repository called pinsaferadius or type RADIUS.

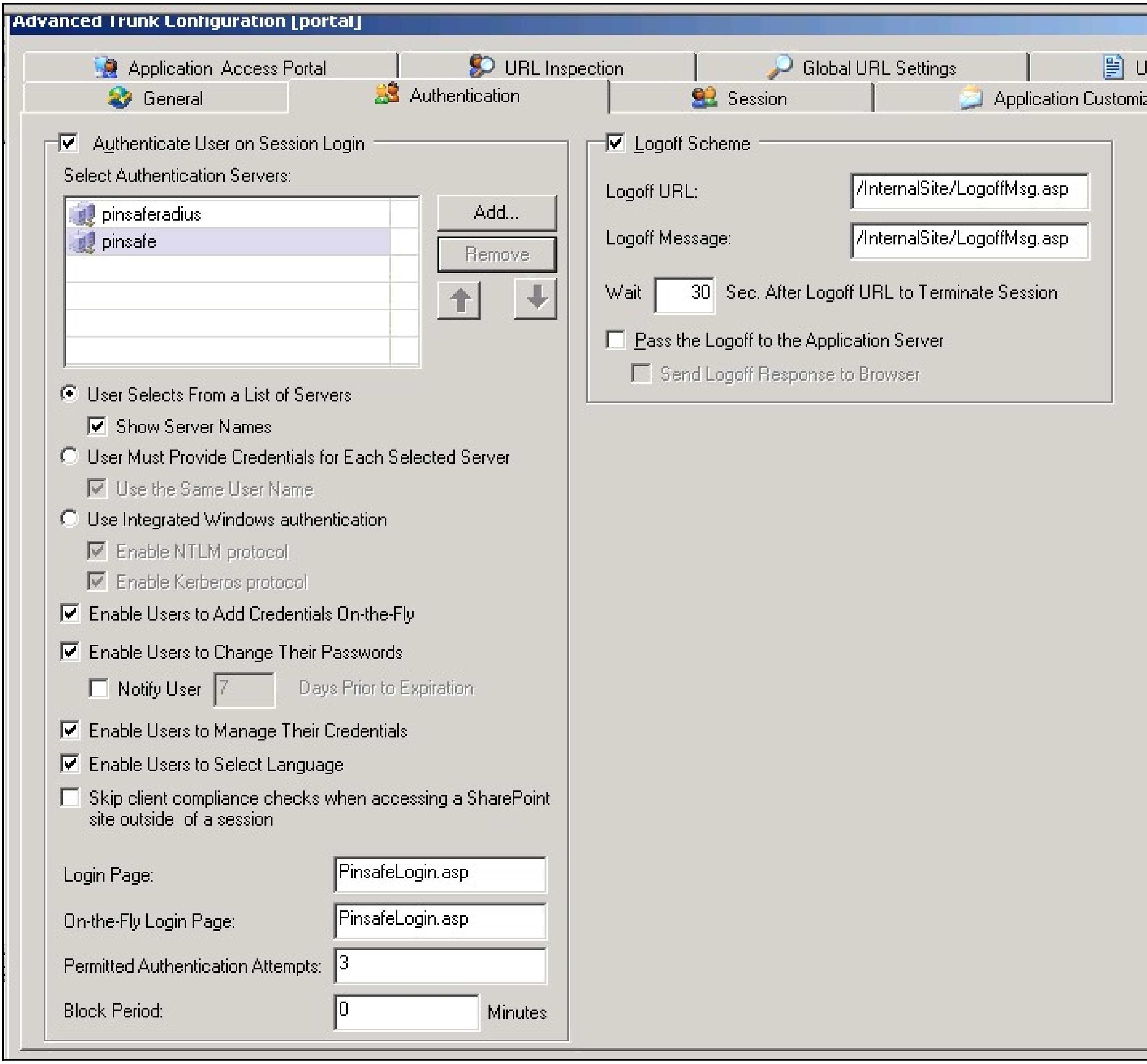
Enter the details of the PINsafe RADIUS server on the config screen.

110.3.3 Trunk Configuration

For the trunk you are using eg portal, ensure that both pinsafe and pinsaferadius repositories are associatd with the page

Also ensure that the option User Selects from A List of Servers is set

Set the login pages to be PINsafeLogin.jsp



☑ Authenticate User on Session Login

Select Authentication Servers:

- pinsaferadius
- pinsafe

● User Selects From a List of Servers

☑ Show Server Names

○ User Must Provide Credentials for Each Selected Server

☑ Use the Same User Name

○ Use Integrated Windows authentication

☑ Enable NTLM protocol

☑ Enable Kerberos protocol

☑ Enable Users to Add Credentials On-the-Fly

☑ Enable Users to Change Their Passwords

□ Notify User 7 Days Prior to Expiration

☑ Enable Users to Manage Their Credentials

☑ Enable Users to Select Language

□ Skip client compliance checks when accessing a SharePoint site outside of a session

Login Page: PinsafeLogin.asp

On-the-Fly Login Page: PinsafeLogin.asp

Permitted Authentication Attempts: 3

Block Period: 0 Minutes

☑ Logoff Scheme

Logoff URL: /InternalSite/LogoffMsg.asp

Logoff Message: /InternalSite/LogoffMsg.asp

Wait 30 Sec. After Logoff URL to Terminate Session

□ Pass the Logoff to the Application Server

□ Send Logoff Response to Browser

Now copy the PINsafeLogin.jsp to von\InternalSite

Edit the PINsafeLogin.jsp to ensure that the repository names match those that you are using and that the dual channel and single channel authentication are matched to the correct repository.

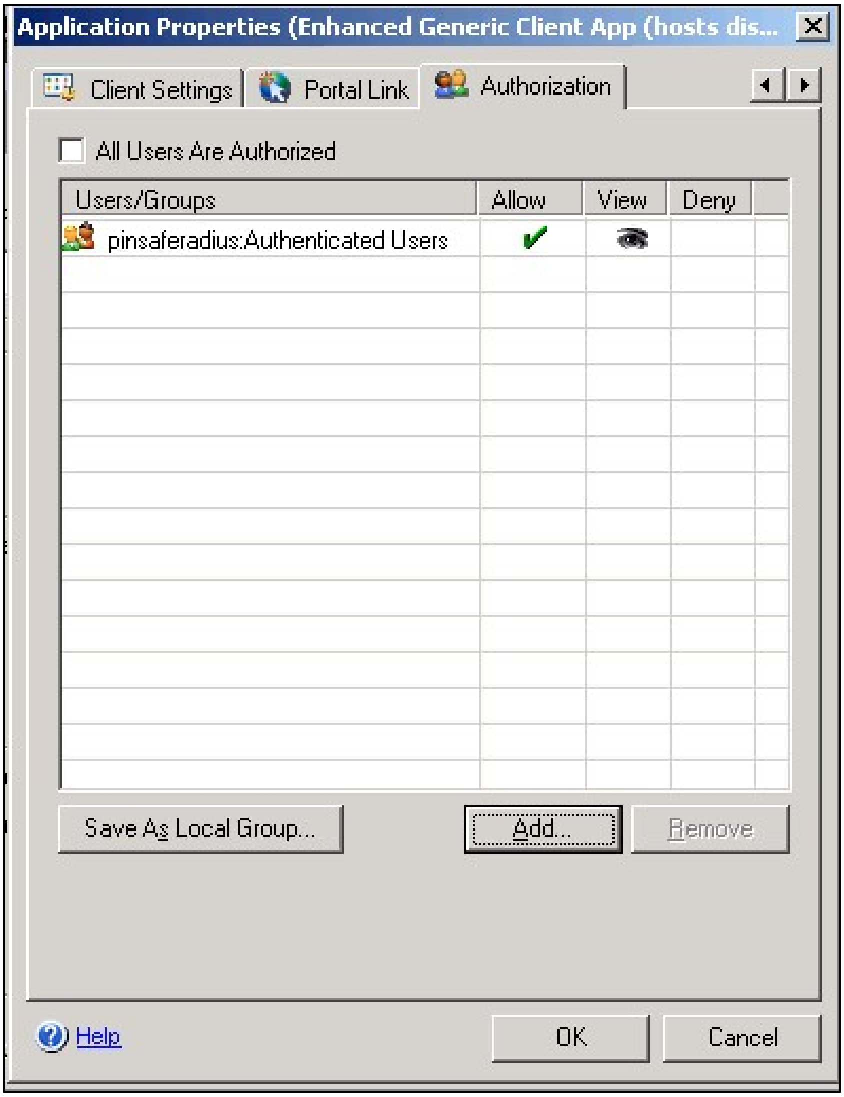
```
function checkradio()
{
  var radiovalue = eval(document.form1.swivel[1].checked);
  var r = document.getElementById("repository");
  if (radiovalue == true)
  {
  //alert("turing");
  //TURing selected, therefore refresh TURing image
  updateotp();
  //repository for TURing is pinsafe
  r.value = "pinsafe"
  } else{
 //alert("sms");
 updateindex(); //if we are using multi-sms update index will display required index
 r.value = "pinsaferadius"
 //repository for TURing is pinsaferadius
 }
```

}

110.3.4 Application Authorization

With different repositories aligned to different authentication methods, it is possible then to make some applications only accessible when a user has authenticated using the dual channel method.

To do this restrict access to applications to the pinsaferadius group on the Trunk->Applications-.Authorization tab



□ All Users Are Authorized

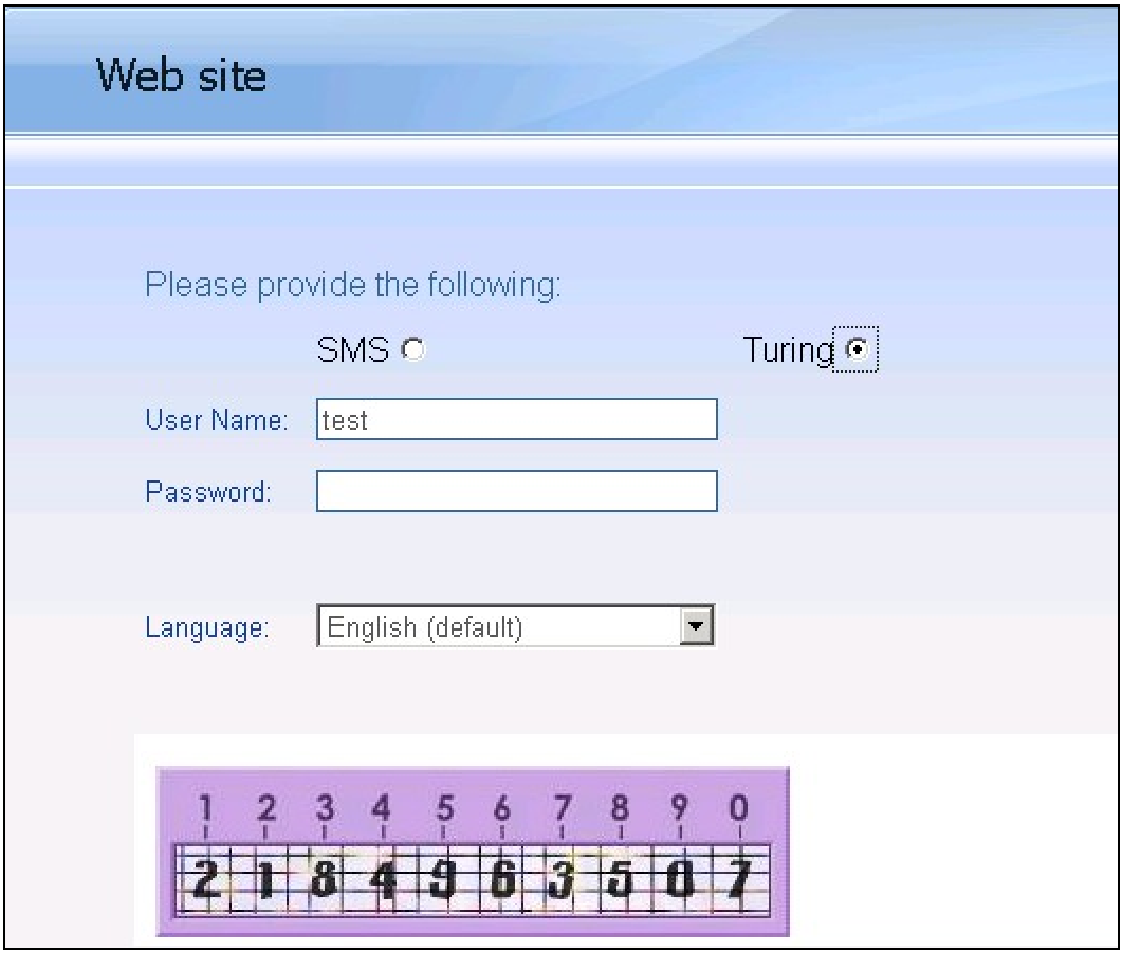
Users/Groups	Allow	View	Deny
pinsaferadius:Authenticated Users	✓	👁	

110.4 User Experience

The user is presented with the option of authenticating via SMS or TURing.

To authenticate the user enters their username and then clicks on the authentication method they wish to use.

If they select TURing and TURing image is displayed.



Web site

Please provide the following:

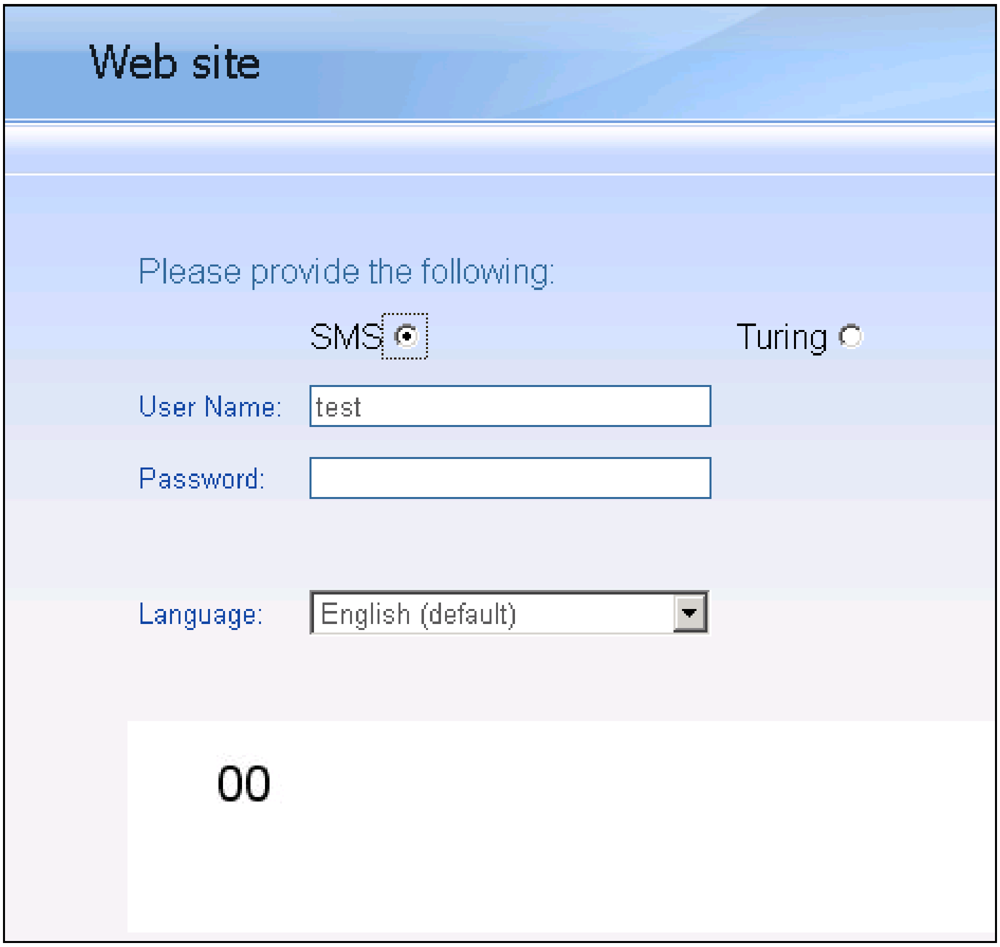
SMS ○ Turing ●

User Name: test

Password:

Language: English (default)

If they select SMS (and multi-SMS is being used) the index of the security string that they need to use is displayed.



Web site

Please provide the following:

SMS ● Turing ○

User Name: test

Password:

Language: English (default)

00

(If they have no valid SMS strings, -1 is shown)

When they make their selection the login page automatically associates them with the correct repository.

After authentication they will only have access to applications appropriate to their method of authentication.

111 Microsoft IAG SMS login video

111.1 Microsoft IAG SMS login Video

PINsafe_IAG_SMS_login.swf

112 Microsoft IAG Turing login video

112.1 Microsoft IAG TURing login Video

PINsafe_IAG_Turing_login.swf?

113 Microsoft IIS version 6 Integration

113.1 Overview

This document outlines the steps required to integrate the Internet Information Server (IIS) with PINsafe using dual or single channel authentication. The PINsafe install requires configuring an agent on the PINsafe server and setting up a shared secret with the IIS server to allow communication for authentication. An ISAPI filter installed on the IIS server allows access to protected resources through the PINsafe authentication.

NOTE: This document refers to the version of the filter numbered 1.1.0.1, and the configuration application with the same version number.

32 bit and 64 bit versions of the filter are available.

If Windows 2008 Server server is being used, or only ASP.Net applications are being protected an alternative authentication is available, see Microsoft IIS version 7 ASP.NET Integration. However, this filter will still work in these situations if you prefer.

113.2 Prerequisites

Internet Information Server on Windows server 2000, 2003, 2008

PINsafe server

The appropriate PINsafe ISAPI filter software can be downloaded from here, depending on your operating system:

- 32-bit ISAPI Filter
- 64-bit ISAPI Filter

These links refer to the latest version of the filter: 1.3.8.

The previous version (1.2) is provided here:

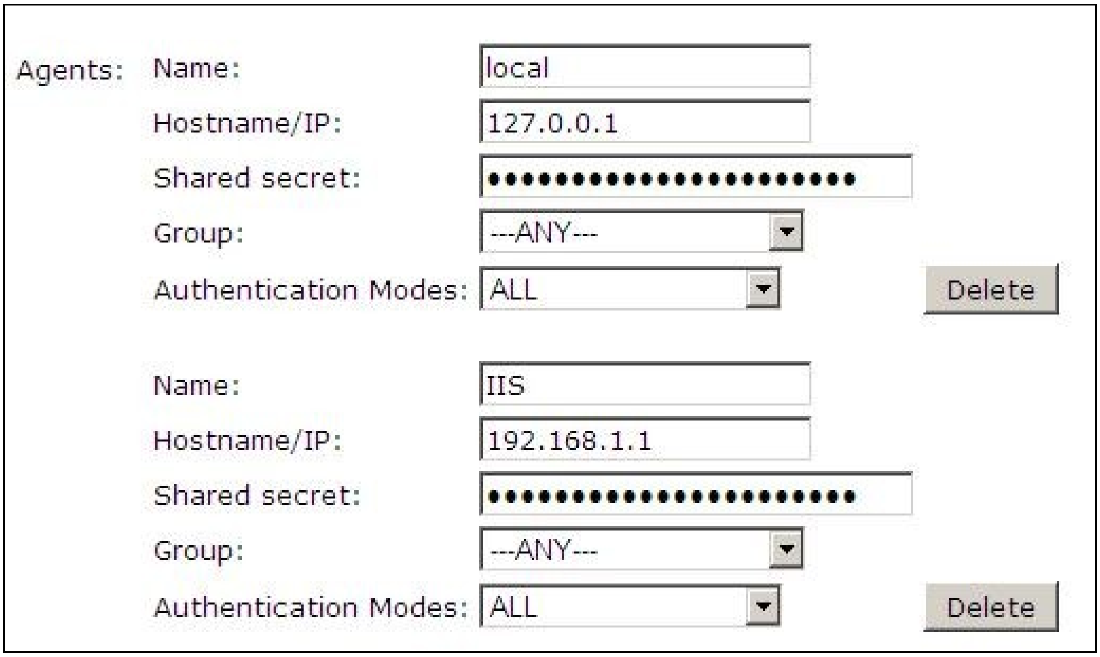
- 32-bit ISAPI Filter
- 64-bit ISAPI Filter

113.3 PINsafe Configuration

On the PINsafe server configure the agent that is permitted to request authentication. On the PINsafe Administration Console select from the server menu Agents and enter the details of the IIS server IP address and a shared key, then click on apply.

Example:

```
Name : IIS server 1,
Hostname/IP : 192.168.1.1,
shared secret : secret
```

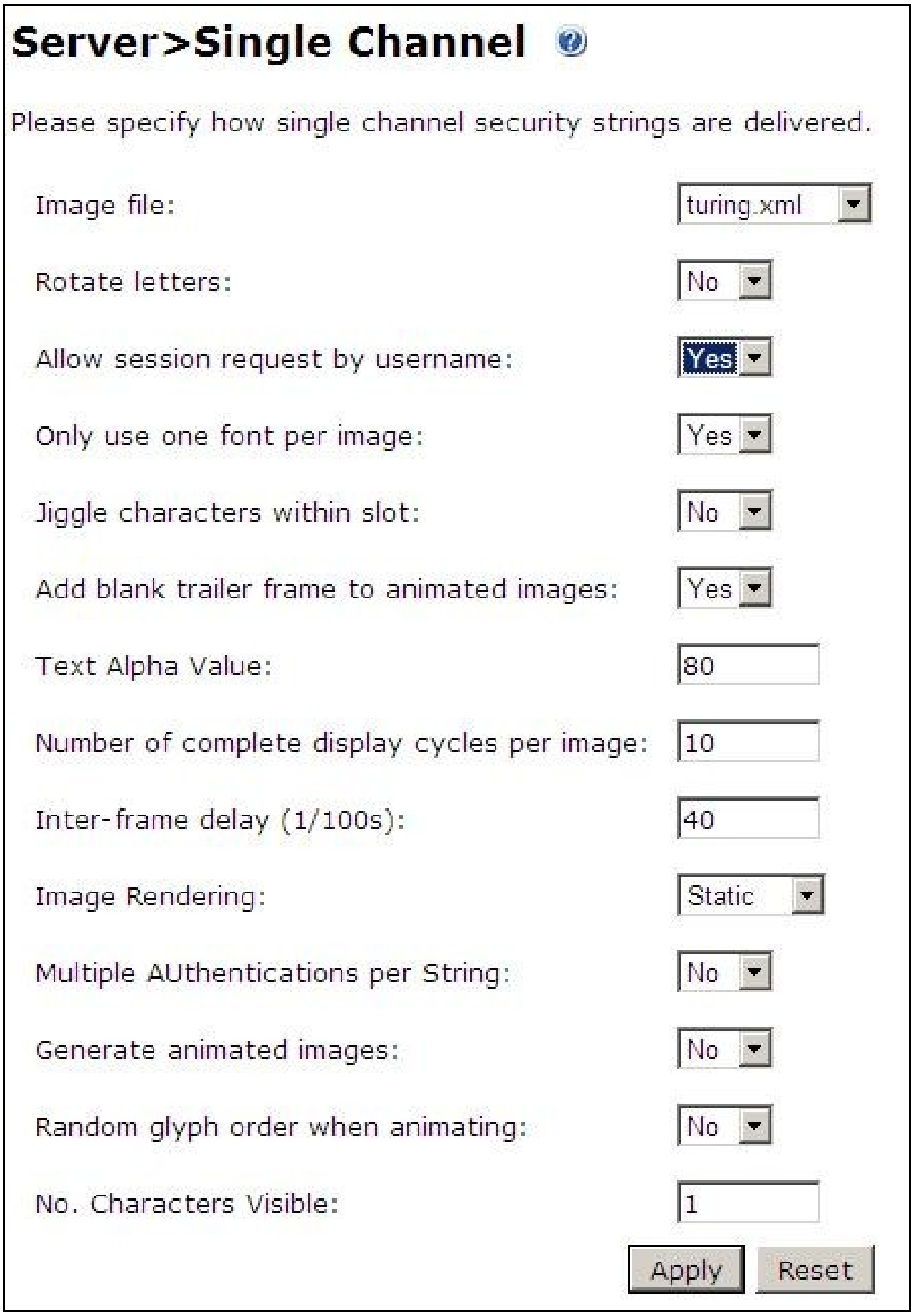


Agents:

Name: local
Hostname/IP: 127.0.0.1
Shared secret: ●●●●●●●●●●●●●●●●●●●●●●
Group: ---ANY---
Authentication Modes: ALL

Name: IIS
Hostname/IP: 192.168.1.1
Shared secret: ●●●●●●●●●●●●●●●●●●●●●●
Group: ---ANY---
Authentication Modes: ALL

If Single Channel communication is to be used, select from the PINsafe Administration Console Single Channel, and set the Allow image request by username to Yes then click on apply.



Server>Single Channel

Please specify how single channel security strings are delivered.

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

113.4 Configuring the IIS Server

113.4.1 Install the PINsafeIISFilter.exe

1. On the IIS server run the PINsafeIISFilter.exe. The IIS filter may need to be run as an Administrator user (The filter needs to be installed by IIS running as Administrator user but it can run as a normal user).

2. Choose the Path to Install to - the default is as C:\Program Files\Swivel Secure\Swivel IIS Filter

3. Select Start Menu Folder

4. When details are correct click on Install

5. If the error ?Incorrect Command Line Parameters? is seen click on OK

NOTE: you will see that there are two installation options: "Filter" and "Configuration". Typically, you would install both on the web server, but the configuration program requires Microsoft.Net Framework 4.0 or higher installed. If your web server doesn't have this, and you prefer not to install it, then you can install the configuration program on a separate machine. You would then need to create the configuration file locally, and copy it to the web server.

113.4.2 Configure the ISAPI filter

When the installation is completed, you will be presented with the configuration program. See below for details on using this.

113.4.3 Create a PINsafe virtual directory

1. On the Internet Information Services Manager right click on the website and select New, Virtual Directory

2. Create an Alias called PINsafe

3. Point the path to the PINsafe directory Web folder, by default C:\Program Files\Swivel Secure\Swivel IIS Filter\Web.

4. Set the permissions to Read and Run Scripts

5. Right-click on the newly-created virtual directory and choose Properties. On the Virtual Directory tab, click the Remove button next to Application name and then click OK.

113.4.4 Install The IIS ISAPI filter

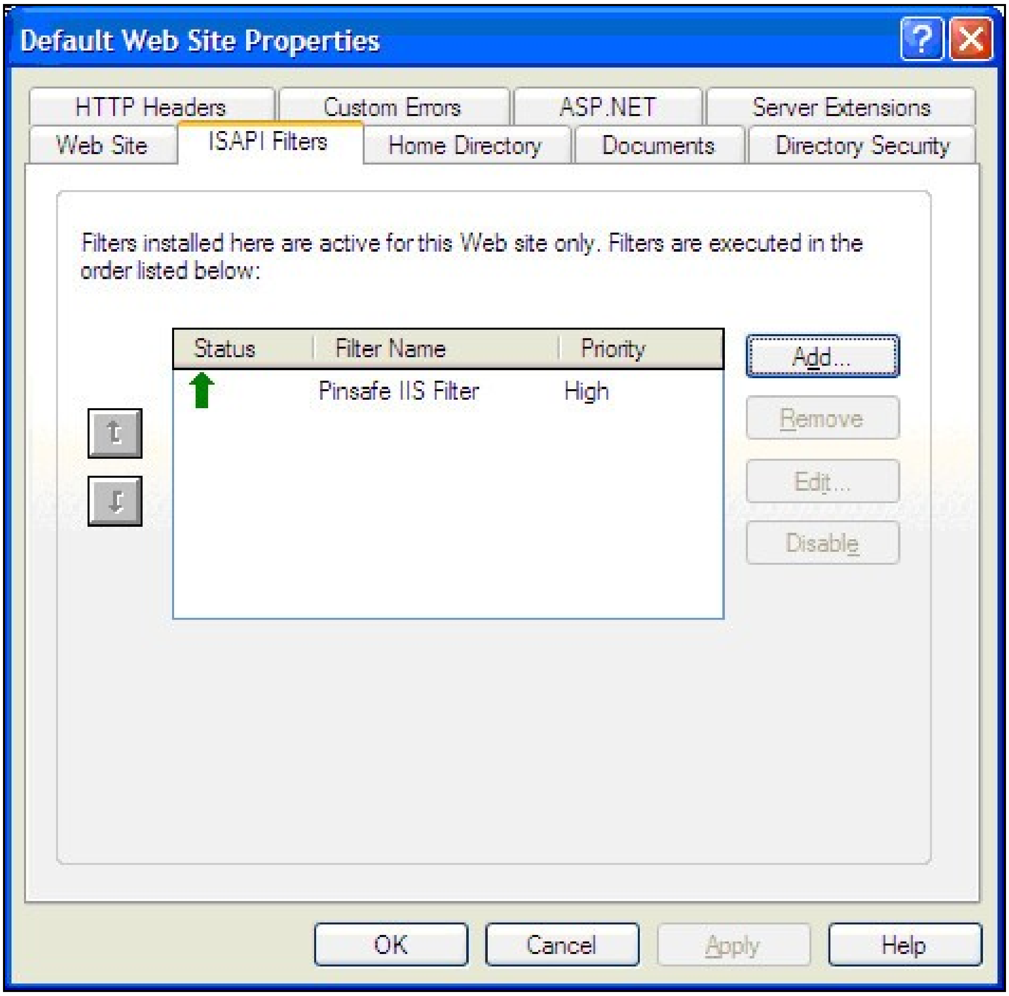
1. On the Internet Information Services Manager Select the Properties for the website

2. Select ISAPI filters

3. Select Add ISAPI filter

4. Select the Path to the PINsafe ISAPI filter. Note that the actual file you require will be PINsafeIISFilter.dll, located in the installation folder.

5. Ensure PINsafe ISAPI filter is top filter then click on OK

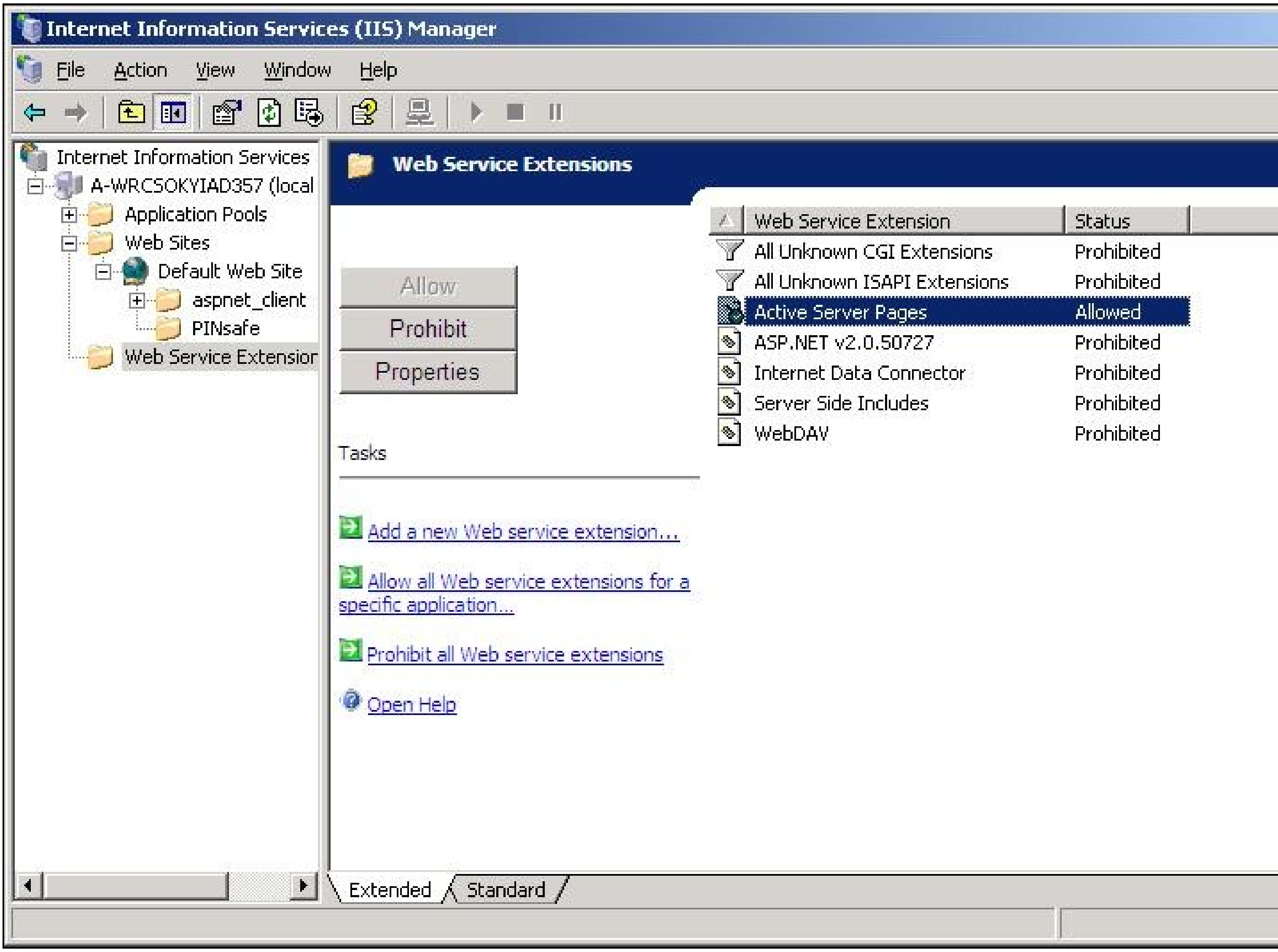


Filters installed here are active for this Web site only. Filters are executed in the order listed below:

Status	Filter Name	Priority
↑	Pinsafe IIS Filter	High

From the Services application, usually found from the Control Panel Administrative Tools, restart the World Wide Web Publishing Services.

Allow Active Server Pages: to verify this, select the Internet Information Services Manager expand the required server then click on Web Service Extension.

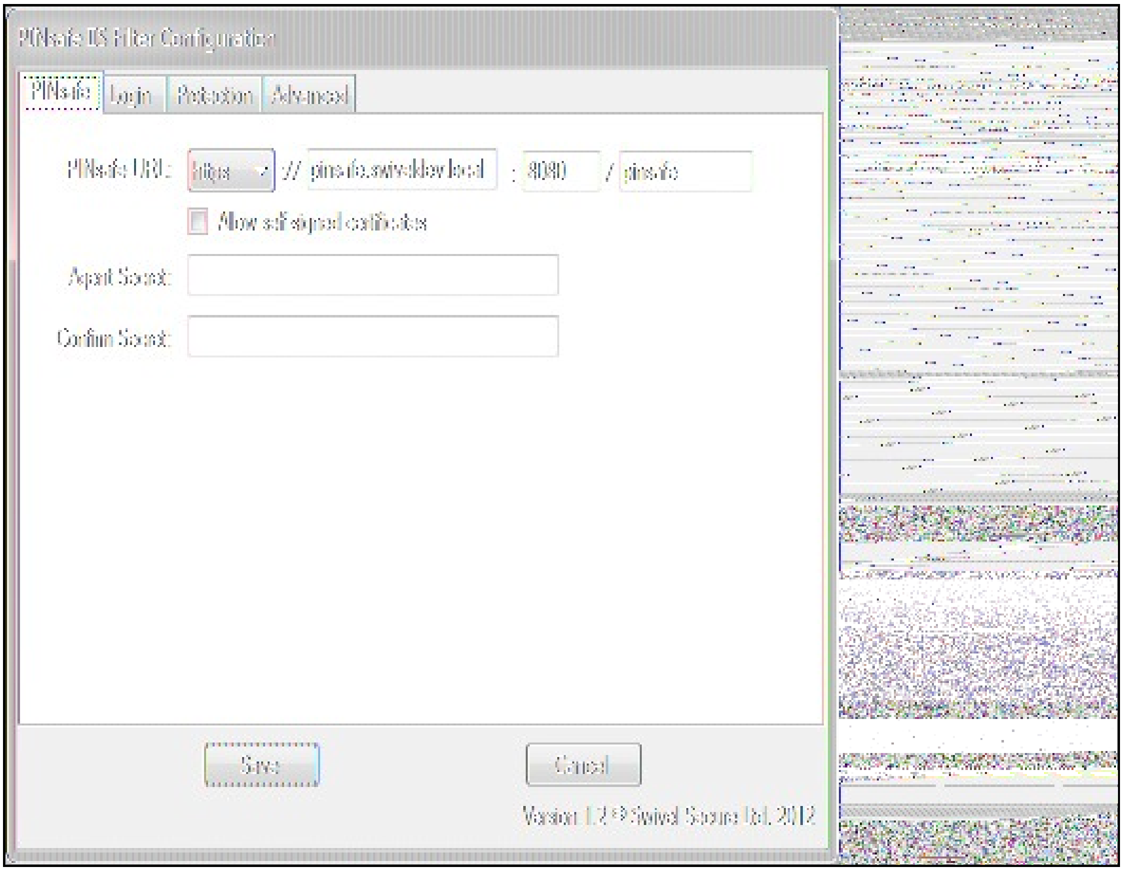


Web Service Extension	Status
All Unknown CGI Extensions	Prohibited
All Unknown ISAPI Extensions	Prohibited
Active Server Pages	Allowed
ASP.NET v2.0.50727	Prohibited
Internet Data Connector	Prohibited
Server Side Includes	Prohibited
WebDAV	Prohibited

113.5 Configure the ISAPI Filter

This documentation refers to version 1.2 of the configuration program. If you are still using an older version, see the next section for a description of the configuration program.

113.5.1 PINsafe Server Settings


PINsafe IIS Filter Configuration
PINsafe
Login
Protection
Advanced
Save
Cancel
Version 1.2 © Swivel Secure Ltd. 2012

PINsafe URL: https :// pinsafe.swiveldev.local : 8080 / pinsafe

□ Allow self-signed certificates

Agent Secret:

Confirm Secret:

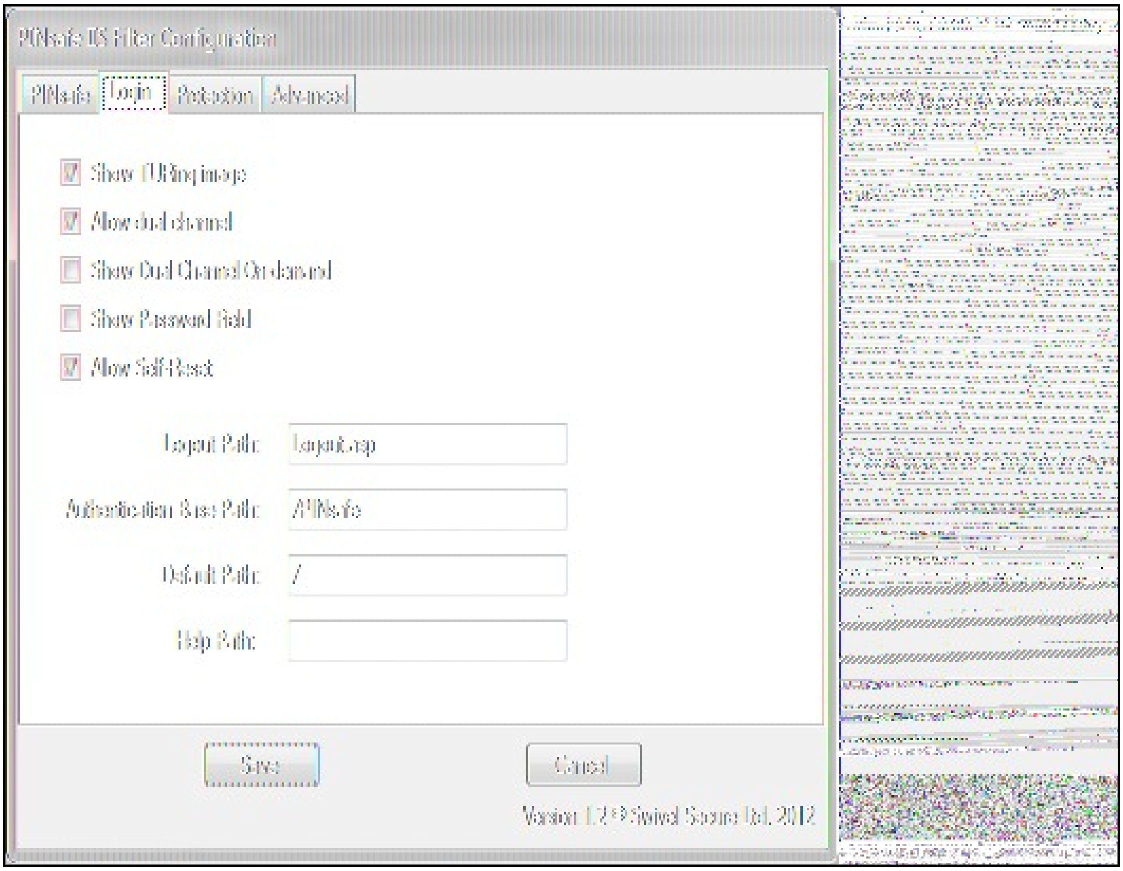
This page defines the connection to the PINsafe server.

In the first line, enter the URL for the PINsafe server. As you will see, it is entered in several parts: http/https, the server host name or IP address, port number and context.

The check box on the second line indicates whether self-signed SSL certificates are allowed for https. This actually ignores all SSL certificate errors, including incorrect host name and expired certificates. You should only use this option if the connection is internal only, and you are confident that the PINsafe server settings are correct.

The final option on this page is the shared Agent secret. This should be the same as the secret entered for the Agent entry on the PINsafe configuration. It is not normally displayed, and you should only enter a value if you wish to change it: a blank entry will result in no change. You need to enter the same value twice to ensure it is entered correctly.

113.5.2 Login Page Settings



☑ Show TURing image

☑ Allow dual channel

□ Show Dual Channel On-demand

□ Show Password Field

☑ Allow Self-Reset

Logout Path: logout.asp

Authentication Base Path: /PINsafe

Default Path: /

Help Path:

Version 1.2 © Swivel Secure Ltd. 2012

This page defines how the login page is displayed, and what happens on login.

The first 5 checkboxes enable or disable features on the page:

Show TURing image: displays a button to show a TURing image.

Allow dual channel: has no obvious effect - dual channel authentication is always allowed if PINsafe policy permits it.

Show Dual Channel On-demand: displays a button to request an on-demand security string.

Show Password Field: requests a PINsafe password as well as the one-time code. This will also enable repository (e.g. AD) password if the Agent has "Check Repository Password" enabled.

Allow Self-Reset: shows a link on the page to the self-reset page, in case the user has forgotten their one-time code.

The four paths are:

Logout Path: if the filter detects this path, the PINsafe authentication cookie is removed, so the user must log in again.

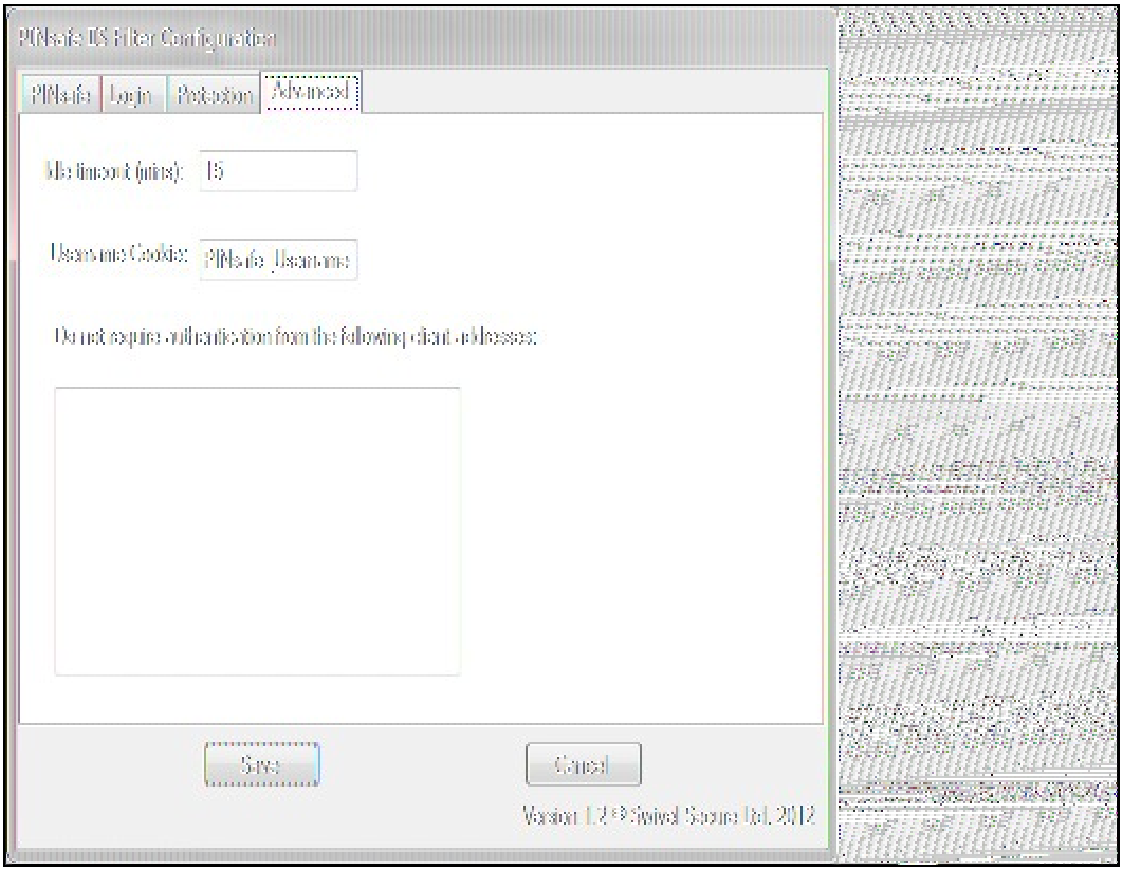
Authentication Base Path: the virtual path containing the PINsafe authentication pages.

Default Path: if a user navigates directly to the PINsafe login page, rather than being redirected by the filter, this is the path the user will be redirected to on successful authentication.

Help Path: if present, a link will be displayed to this path if the user requires help. This must be provided by the customer: Swivel does not provide any help pages.

113.5.3 Advanced Settings

Let us take the last tab out of order, as the Protection tab is the most complicated one:


PINsafe IIS Filter Configuration
PINsafe
Login
Protection
Advanced

Idle timeout (mins): 15

Username Cookie: PINsafe_Username

Do not require authentication from the following client addresses:

Save
Cancel
Version 1.2 © Swivel Secure Ltd. 2012

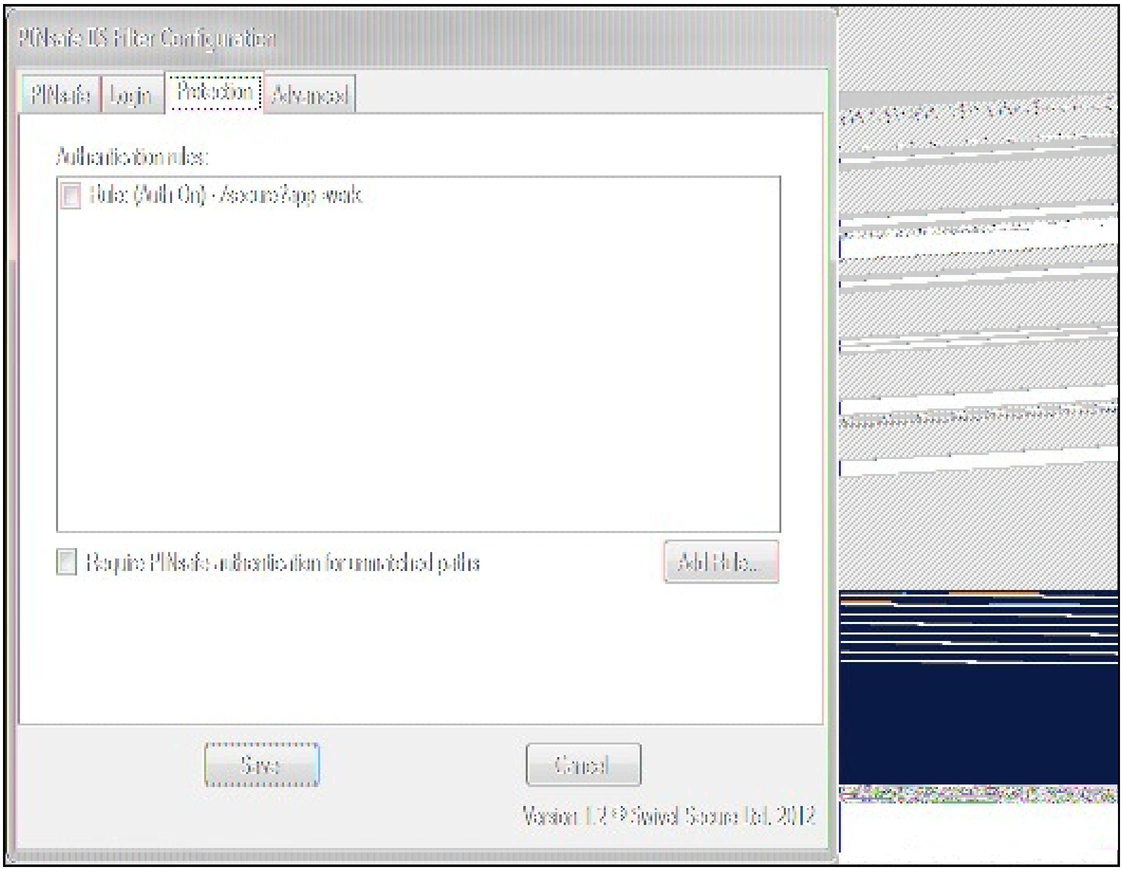
Idle timeout is the time (in minutes) that the user can leave a page open without refreshing it or navigating to another page: in other words, the lifetime of the authentication cookie. However, if the user requests a new page (or refreshes the current one) within that time, the cookie expiration time is updated.

Username cookie, if entered, specifies the name of a cookie that will contain the name of the authenticated user. Other applications can make use of this cookie if they are written to read it.

The final option on this page allows you to specify a list of source addresses that are not required to authenticate to PINsafe. Typically, these will be internal addresses.

113.5.4 Protection Settings

This tab replaces the Included and Excluded paths of the older filter:



PINsafe IIS Filter Configuration

PINsafe | Login | Protection | Advanced

Authentication rules:

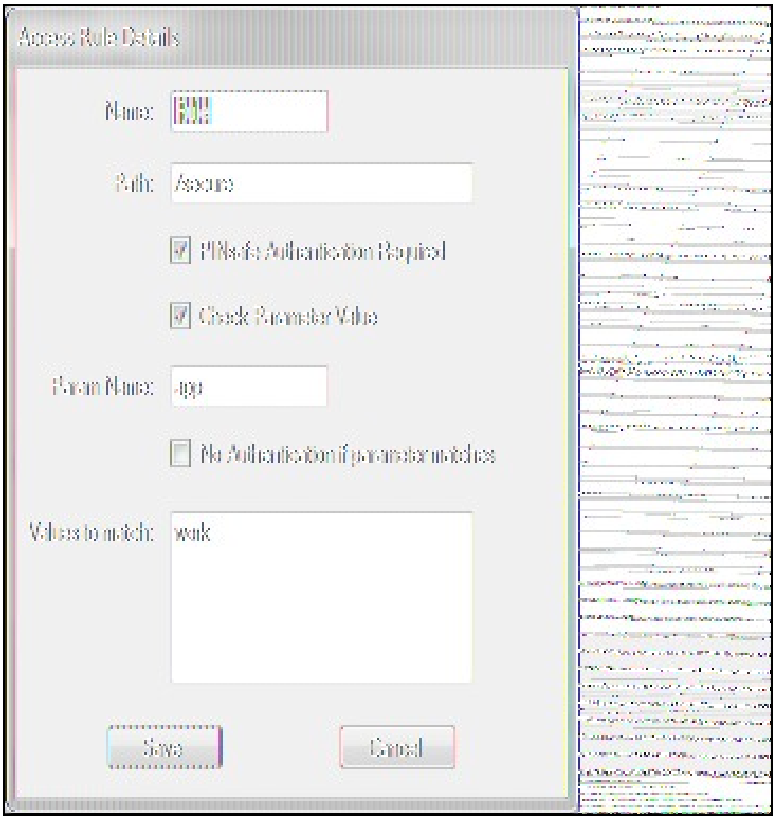
□ Rule: (Auth On) - /secure?app=work

□ Require PINsafe authentication for unmatched paths

Version 1.2 © Swivel Secure Ltd. 2012

In order to define which paths PINsafe protects, you need to define rules. The main part of this tab summarises the current list of rules.

To add a new rule, click "Add Rule...", and you will see the following page.



Access Rule Details

Name: Rule

Path: /secure

☑ PINsafe Authentication Required

☑ Check Parameter Value

Param Name: app

□ No Authentication if parameter matches

Values to match: work

The rule name is just a means of identifying the rule: it doesn't affect how the rule works.

The path is the URL that must match the URL entered for the rule to apply. The path must start at the slash immediately after the host name (and port if given). The match is case-insensitive, and the entire entered URL does not have to match the path: it just has to match as far as the path is specified. So, for example, if the path is "/secure", it will match "/secure/default.aspx", or even "/securepage", but not "/somewhere/secure".

The next checkbox indicates what happens if the path is matched. If it is checked, PINsafe authentication is required, and if no PINsafe cookie is found, the user is redirected to the login page. If this box is unchecked, the user is permitted to continue without authenticating, and no further rules are tested.

The remainder of the rule allows you to restrict PINsafe authentication according to the value of a particular parameter in the query string. Check the "Check Parameter Value" checkbox to enable this option.

Param Name is the name of the parameter that must be matched. Values to match allows you to specify a list of values that are accepted. The parameter must match one of these values.

The final checkbox defines how PINsafe authentication is affected depending on the value of this parameter. Normally, PINsafe authentication is applied if any of the values match. Checking this box reverses the logic, so PINsafe authentication is applied only if the parameter DOESN'T match any of these values.

Note that the parameter value only affects whether or not PINsafe authentication is applied, not whether or not the rule matches. Rule matching is done by path only.

Note also that parameter matching only applies to HTTP GET requests, i.e. when the query string is part of the URL. It cannot handle POST requests, when the parameters are in the body of the request.

So, using the example rule above: if the URL entered is "/secure/default.aspx?app=work", then PINsafe authentication is required. If the path is "/secure/default.aspx?app=play", or "/secure/default.aspx" (i.e. no parameter), then PINsafe authentication is NOT required.

NOTE: all comparisons, of path, parameter name and parameter value are case-insensitive.

The filter works by checking each rule in the order given. The first rule that matches determines whether or not PINsafe authentication is required for that URL.

You can change the order of the rules by right-clicking on the list. There are options to move sets of rules to the top or bottom, to move individual rules up or down the list, or to delete rules. You also use this menu to modify an existing rule. The dialog displayed is the same as above.

Finally, you can specify what happens if the entered URL doesn't match any rules: by default, no PINsafe authentication is required. If you check the final checkbox, PINsafe authentication will be required for all URLs that don't match any explicit rules.

113.5.5 Special Consideration for Windows Server 2003 / Windows XP

The settings are saved to the Windows common data folder. In Windows Server 2008 / Windows 7 and later, this is usually **C:\ProgramData**. In Windows Server 2003 and Windows XP or earlier, it is **C:\Documents and Settings\All Users\Application Data**.

The configuration program, and the filter itself, automatically select the correct folder. However, the web page **settings.asp** has the path hard-coded. If you are using Windows Server 2003 or earlier, or if you have changed the common data folder for some reason, you need to edit settings.asp to set the correct folder for config.xml. Edit the file **C:\Program Files\Swivel Secure\Swivel IIS Filter\Web\settings.asp** and look for the following line:

```
configDoc.load("C:\ProgramData\Swivel Secure\IIS Filter\config.xml")
```

Change the file path to the correct path for your environment.

113.5.6 Reading and Saving Configurations Elsewhere

The File menu on the configuration program allows you to save a copy of the configuration elsewhere, or to read a configuration file from elsewhere. This is useful if you are configuring the filter from a different machine, or if you have multiple configurations.

Additionally, you may find that you are unable to save the configuration to the default location (C:\ProgramData\Swivel Secure\IIS Filter\). You may find that the program appears to save it, but when you check, it has not been saved there. In this case, save a copy of the configuration file (config.xml) to a different location, and then copy it to the correct location.

You will also need to do this if you have installed the configuration program on a separate computer.

113.6 Configure the ISAPI filter (Version 1.0-1.1)

This documentation applies to the older version of the filter.

1. Select Start Programs/PINsafe IIS Filter/Filter Configuration. This will look for the location of config.xml, this will be created when first used and this must be located in web/bin.

2. You will be asked to select the location of the configuration file. It is important that you select the right location. It should be in the same folder as the ISAPI filter. Initially, this file will not exist, but will be created as a result of running this configuration application.

113.6.1 PINsafeIISFilter Options

PINsafeServer: The PINsafe Server tab contains settings which define the PINsafe server which will be used to authenticate users.

Hostname/IP: The name or IP address of the PINsafe server.

Port: The port number used by the PINsafe server (normally 8080).

Context: The context (i.e. web application name) of the PINsafe instance on that server

Secret: The common secret used to communicate with the PINsafe server. This value must be the same as the secret defined for the PINsafe agent configured earlier.

SSL enabled: Tick this box to require SSL (HTTPS) communication with the PINsafe server.

Permit self-signed certificates: Tick this box to allow SSL certificates to be self-signed. This also ignores other certificate errors, such as site names not matching.

Authentication: The Authentication tab contains the following settings:

Idle time (s): The time (in seconds) for which the authentication cookie will be valid if the web page is not used.

Username header: The name of a cookie which will pass the username of the authenticated PINsafe user. If this value is blank, no cookie will be provided.

Single: Indicates that single channel security strings (i.e. TURing image) are permitted.

Dual: Indicates that dual channel security strings (i.e. via e-mail, SMS) are permitted.

On-demand dual: Indicates that the login page should display a button to request dual-channel security strings.

Display password fields: Indicates that the login page should show a field for PINsafe password as well as OTC.

Permit self-reset: Indicates that the user self-reset page should be enabled.

Exclusions and Inclusions: Use the inclusion and exclusion tabs to enter which paths should be protected by PINsafe:

Included paths: This is a list of paths within the current website which require PINsafe authentication. If this list is empty, the entire website will be protected except as indicated by the Exclusions tab. Paths should be one per line.

Excluded paths: This is a list of paths within the current website which should be exempt from PINsafe authentication. This is only relevant if the included paths list is empty, in which case all paths not on this list will be protected by PINsafe.

Excluded addresses: This is a list of IP addresses which are exempt from PINsafe authentication. All requests from these addresses are passed through without authentication.

Misc: On the Misc tab, edit any custom paths as follows:

Default path: This is the path to which authenticated requests are directed if the login page is targeted directly. If a user tries to access a protected page, she is redirected to the login page, and after authentication, back to the page she was trying to access. If the user requests the login page directly, she will be redirected to this location after authentication.

Logout path: Requesting this path will result in the user being logged out. Subsequent requests will require re-authentication, if relevant. If this path is empty, users can only be logged out by closing the browser, or if the authentication times out. Note: The logout path must be an included file location.

Virtual web path: This is the path to the PINsafe authentication pages. See the next section for details on setting this up. You should normally set this to be ?/pinsafe?, unless you have a particular reason not to.

Help URL: The URL for PINsafe IIS filter help. The filter does not come with help pages as standard, so this should only be filled in if help pages have been provided by the reseller or end user.

113.7 Installing the Filter on Multiple Websites

Most of the instructions above assume that you are installing the IIS filter on the single default website of a web server. However, if you want to use the filter on multiple websites on the same server, you need to carry out a few extra steps. Firstly, if all the settings on all the websites are exactly the same, you can configure it once, and then carry out the same steps to activate the filter on each website. In this case, simply save the settings to all the relevant locations.

If, however, you need different settings for each website, you will need to do the following for all except the first website:

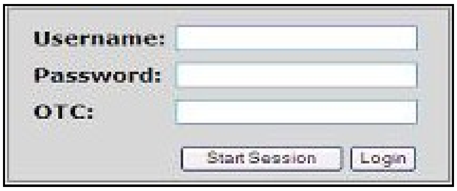
1. Make a copy of the entire Web folder, including the bin sub-folder. You can copy it as a sub-folder of PINsafe IIS filter, with a different name, or you can put it somewhere completely different. It is important, however, that you keep the structure the same ? all the .asp files must remain intact, and the filter DLL must be in a sub-folder called ?bin?. You do not, however, have to copy the FilterConfig.exe file (but it does no harm if you do).

2. When you come to configure each filter, navigate to the bin sub-folder of the copy you have just made. Otherwise, configuration is exactly as before.

3. When selecting the IIS filter to install, and also when defining the virtual directory for PINsafe web pages, you should use the copy you have just created, rather than the original. This is important, as both the filter and the web pages look for the configuration file relative to their own location.

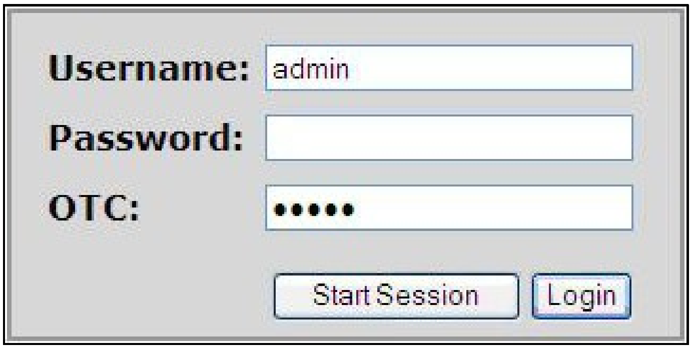
113.8 Testing

Browse to a web page that has been configured for protection. This should display a PINsafe login dialog:



Enter the Username.

For dual channel, enter the One Time Code:

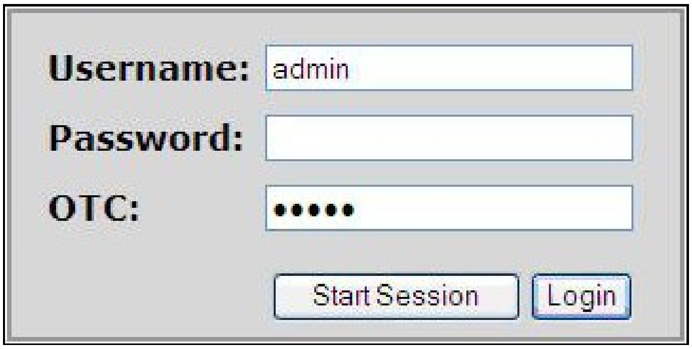


Username: admin

Password:

OTC: •••••

Or click start session to enter a single channel OTC. The PINsafe log will record that a single channel session has started.

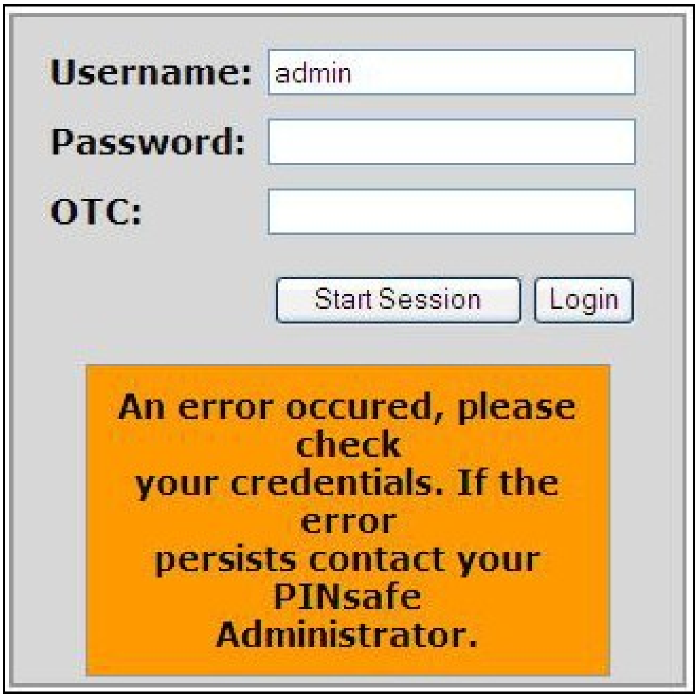


Username: admin

Password:

OTC: •••••

If authentication is successful it should redirect to the login page. If failed an error message will appear. The PINsafe log will record any successful log attempt for the agent.



Username: admin

Password:

OTC:

An error occured, please check your credentials. If the error persists contact your PINsafe Administrator.

113.9 Troubleshooting

Verify the correct filter version has been installed for the operating system i.e. 32 bit or 64 bit.

Check for error messages in the PINsafe log

Check the IIS log messages

Filter Install issues: The IIS service needs to run as an administrator in order to install the filter. Once the filter is installed, it will run as the normal user. Open the Services applet and locate World Wide Web Publishing. Select properties, then go to the Log On tab. Assuming you are logged in as an administrator, select Local System account. Then restart the service. Hopefully, this will start the filter. You can then switch back to the default account and restart again.

If you are not redirected to the PINsafe login page when trying to access a protected page, open IIS manager and check that the ISAPI filter is installed and has loaded properly (there should be a green arrow next to it, and the priority should be ?High?). If this is not the case, restart IIS, if you have not already done so, and try again. The filter doesn't try to install until you try to access a web page from that website, so try that before assuming it hasn't worked.

If the filter is listed, but showing a red cross, then it failed to start. In this case, check the error messages in the event log showing.

If the filter shows as green, with priority unknown, it may not be installed. In this case, you need to check. You can do this with a debug viewer, such as the one supplied by SysInternals (http://technet.microsoft.com/en-us/sysinternals/bb896647.aspx). Download this and run it (there's no need to install it) on the server, then restart IIS. If you don't see any messages relating to the PINsafe IIS filter, then it's not installed properly.

If the page is still not redirected, try the following:

1. Check which application pool your web application is running as, then go to the properties page for that application pool.

2. On the Identity tab, change the user to ?Local System?. You will be warned that this is a potential security risk, but don?t worry ? it won?t be left like this.

3. Restart IIS.

4. Try accessing a protected page again. Hopefully this time you will be redirected.

5. You can now go back to the application pool and change the identity back to what it was originally: it would appear that it is only necessary to run as an administrator to get the filter to register initially.

If you do not see a Turing image when using start session then in a web browser test the following link from the IIS server. If an image is not seen, then there is a problem either with communicating with the PINsafe server or the Allow Image request by username may be set to No.

For an virtual or hardware appliance Install

https://<pinsafe_server_ip>:8443/proxy/SCImage?username=<username>

For a software only install see Software Only Installation

If the web page is redirected to the /PINsafe/login.asp page but an error message appears then ensure that the Active Server Pages are allowed. To verify this select the Internet Information Services Manager expand the required server then click on Web Service Extension.

113.9.1 Error Messages

AgentXML request failed, error: The agent is not authorised to access the server

User fails to authenticate with the above error message in the PINsafe log. An Agent on PINsafe server has not been defined for the IIS server. Go to Server/Agents in the PINsafe admin console, and add a new entry, using the IP address of the IIS server. Make sure the agent secret is the same as on the IIS filter configuration.

This installation package is not supported on this processor type. Contact your product vendor

The 32 bit version is being attempted to be installed on a 64 bit OS or the 64 bit version is being attempted to be installed on a 32 bit OS. Verify the OS version and install the correct PINsafe software version.

114 Microsoft IIS version 7 ASP.NET Forms Integration

114.1 Introduction

Swivel allows ASP.NET application authentication using Agent-XML for IIS 7 and IIS 6 ASP.NET

NOTE: the method listed here uses standard ASP.Net forms-based authentication to authenticate to PINsafe. We now have an alternative solution that uses a HTTP module. This might be an easier solution than the manual method described below, as all installation and configuration is done using provided applications. Documentation for this solution can be found here.

114.2 Prerequisites

PINsafe

ASP.NET application

ASP.NET Server

114.3 Baseline

PINsafe 3.7

IIS6 and IIS7

114.4 Architecture

The ASP.NET application makes authentication requests against the PINsafe server by Agent-XML.

114.5 ASP.NET Sample Files

ASP.NET Sample File is available here: ASP.NET Sample File

ASP.NET Sample file for 2008 server is available here: ASP.NET for 2008 Server

The pinsafe folder contains an example login page, plus aspx pages which render a TURing image or request a dual channel image.

114.6 PINsafe Configuration

114.6.1 Configure a PINsafe Agent

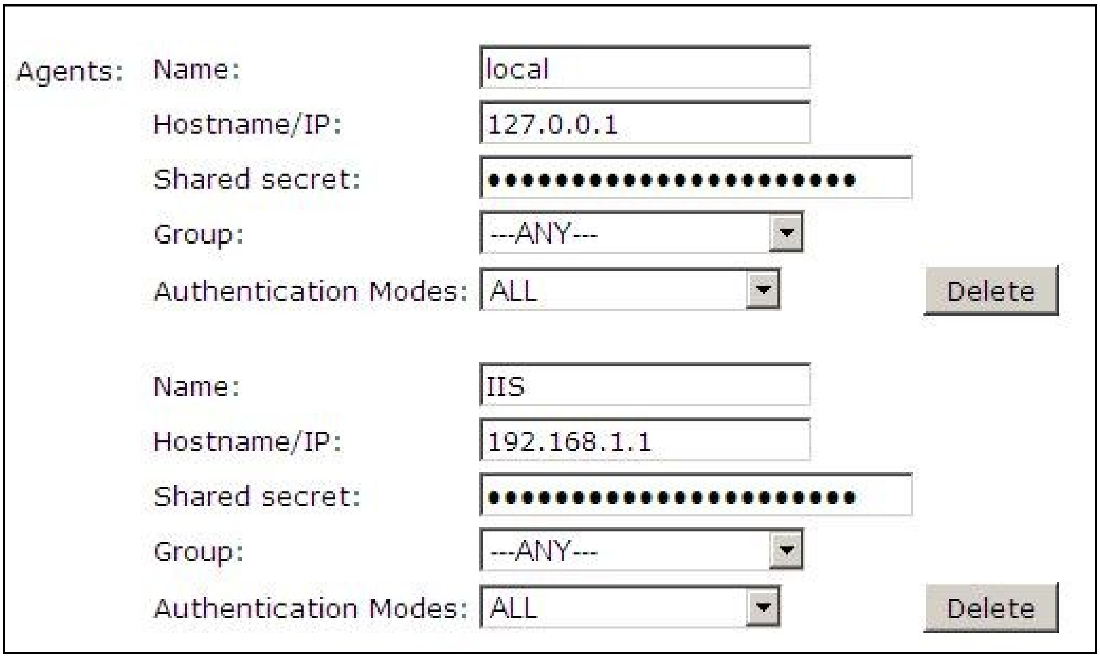
1. On the PINsafe Management Console select Server/Agent

2. Enter a descriptive name for the Agent

3. Enter the IP address or hostname of the server on which the ASP.NET will be running

4. Enter the shared secret used above on the ASP.NET

5. Click on Apply to save changes



Agents:

Name: local
Hostname/IP: 127.0.0.1
Shared secret: ••••••••••••••••••••••
Group: ---ANY---
Authentication Modes: ALL

Name: IIS
Hostname/IP: 192.168.1.1
Shared secret: ••••••••••••••••••••••
Group: ---ANY---
Authentication Modes: ALL

Note: Session creation by username is not required for this integration as PINsafe can use session ID.

114.7 ASP.NET Configuration

114.7.1 Integrating the ASP.NET

First of all, extract the sample zip file to a temporary location. There should be 2 folders:

- App_Code
- pinsafe

and one file:

- web.config.

Copy the pinsafe folder and its contents into the ASP.NET application you want to protect or the root of the website to protect the entire website. It is important that the folder is contained within the application, and is not an application in its own right. You will need to set IIS (or other ASP.NET server) to allow anonymous access to the pinsafe folder, and you may need to modify permissions on the files to ensure that the default IIS (or other ASP.NET server) user has read access.

Copy the contents of the App_Code folder into the App_Code folder of the application or create one if it doesn't already have one.

Edit the web.config file for the application, and add the contents of the enclosed web.config in the appropriate locations. You will need to change the PINsafe server settings as appropriate.

114.7.2 Configure the web.config file

This file contains the information for communication with the PINsafe server. The options are displayed below:

PINsafeServer: The IP address or hostname of the PINsafe server or appliance

PINsafePort: The port used for communication, usually 8080

PINsafeContext: The install name of pinsafe, usually pinsafe

PINsafeSecret: The shared secret key, which must be the same as that entered on the PINsafe server

PINsafeSecure: This is if the connection to the PINsafe server is https for SSL or http. The default value is true, which is for https

PINsafePassword: This is to display the password field, the default value of false will not display a password field

PINsafeImage: This is to display a button to generate a Single Channel Image of the security string

PINsafeMessage: This is to display a button to generate a Dual Channel security string to be sent to the user

PINsafeAcceptSelfSigned: If self signed certificates are accepted, defualt is yes

NOTE: As the requests are made using Agent-XML, they must be made to the pinsafe appliance on port 8080 and the context of pinsafe and not the proxy port of 8443. Security is usually provided by the IIS server proxying the request to the PINsafe server.

Default Settings, suitable for a software install of PINsafe are:

```
<add key="PINsafeServer" value="pinsafe_server" />
<add key="PINsafePort" value="8080" />
<add key="PINsafeContext" value="pinsafe" />
<add key="PINsafeSecret" value="secret" />
<add key="PINsafeSecure" value="true" />
<add key="PINsafePassword" value="false" />
<add key="PINsafeImage" value="true" />
<add key="PINsafeMessage" value="false" />
<add key="PINsafeAcceptSelfSigned" value="true" />
```

Appliance settings are likely to be:

```
<add key="PINsafeServer" value="pinsafe_server" />
<add key="PINsafePort" value="8080" />
<add key="PINsafeContext" value="pinsafe" />
<add key="PINsafeSecret" value="secret" />
<add key="PINsafeSecure" value="true" />
<add key="PINsafePassword" value="false" />
<add key="PINsafeImage" value="true" />
<add key="PINsafeMessage" value="false" />
<add key="PINsafeAcceptSelfSigned" value="true" />
```

114.7.3 Additional web.config file IIS7 Options

The loginUrl setting assumes that you are protecting the entire website. If you are only protecting an application, add the path for that application to this URL. For example, to protect an application with URL "/secure", loginUrl="/secure/pinsafe/Login.aspx".

The <modules> section is not relevant if you are protecting an application that is ASP.NET only. These changes allow ASP.NET authentication to be used for static web pages as well as .aspx pages. This is a new feature of IIS7.

114.7.4 Enabling Authentication

For IIS, open the IIS manager, locate the website or application that you are protecting, and double-click the Authentication icon. Make sure that anonymous authentication is disabled, and that forms authentication is enabled, and the URL is as set earlier. Go to the pinsafe sub-folder, select Authentication under there, and make sure anonymous authentication is enabled (you need to be able to access the login pages anonymously).

114.8 Additional Configuration Options

114.9 Testing

Navigate to the login page. Attempting to login with a correct username and password but no one time code should result in failure. Only when a correct PINsafe one time code is entered should the user be logged in. If the Single Channel button is displayed then an image should appear.

114.10 Troubleshooting

To verify the Single Channel Image works, on the ASP.NET server enter the following into a web browser, which should display a Turing image if the sever is functioning correctly:

For a PINsafe appliance install:

https://<pinsafe_server_ip>:8080/pinsafe/SCImage?username=test

For a software only install see Software Only Installation

114.11 Known Issues and Limitations

Requesting a Security String Index would require modification of the login page for an existing button. See also Multiple Security Strings How To Guide

114.12 Additional Information

For assistance in the PINsafe installation and configuration please firstly contact your reseller and then email Swivel Secure support at support@swivelsecure.com

115 Microsoft IIS version 7 ASP.NET Integration

115.1 Introduction

This solution uses ASP.Net technology, specifically an HTTP Module, to protect specified web pages using Swivel authentication.

NOTE: the method listed elsewhere uses standard ASP.Net forms-based authentication to authenticate to PINsafe. The solution described on this page is simpler to install and maintain, but if you are familiar with forms-based authentication and want more control over the look and feel of the login page, you may prefer the alternative solution.

115.2 Prerequisites

PINsafe server version 3.6 or later

ASP.NET application running on Microsoft IIS version 7 (or later). The latest release is compatible with Server 2012 R2 IIS 8.5 and with Server 2016 IIS 10.0. Testing on Windows Server 2019 pending.

Versions: Latest Version 2.3.2.0 available from here. This version fixes several reported vulnerabilities relating to redirecting after login and same-site cookies. It requires Microsoft.Net framework 4.8 or later, and ASP.Net 4.0.

Version 2.2.1.1 available from here. This version is compatible with the Microsoft.Net framework version 4.5 or later, and ASP.Net 4.0.

Version, 2.1.1.1, available from here. This version is compatible with Microsoft.Net framework version 4.0 or later, but does not support TLS versions higher than 1.0, so should only be used in Windows Server 2008 R1, which doesn't have native TLS 1.1/1.2 support.

115.3 Architecture

A HTTP module is installed into a specific ASP.Net application, where it checks all incoming requests. Any request requiring PINsafe authentication will be redirected to the Swivel login page, unless the user has already been authenticated to PINsafe.

115.4 PINsafe Configuration

115.4.1 Configure a PINsafe Agent

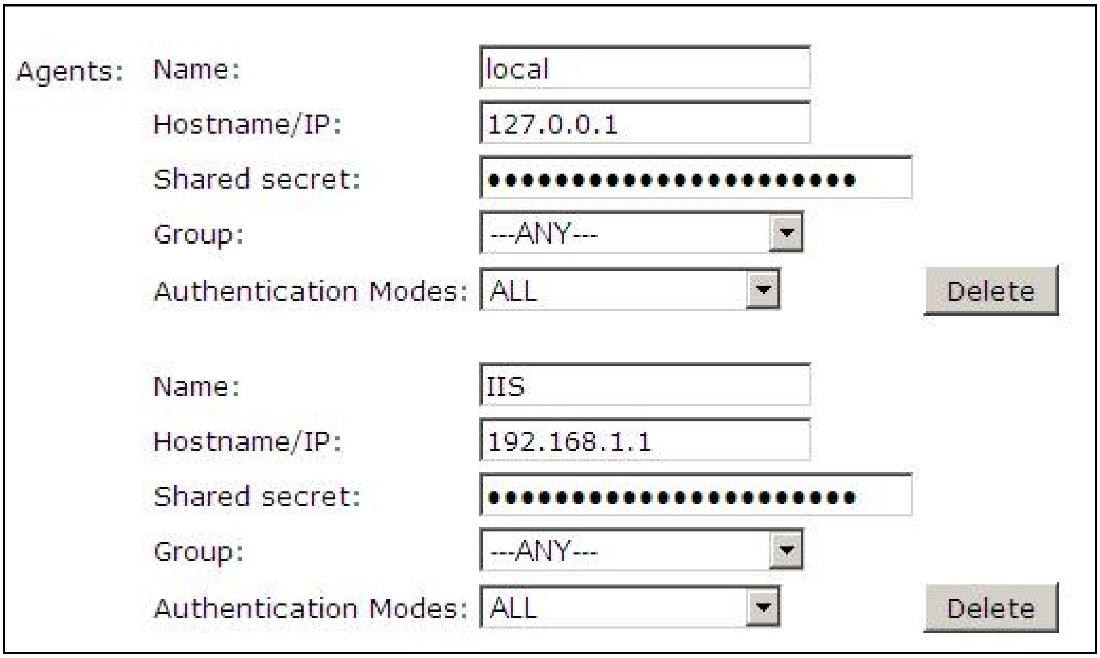
1. On the PINsafe Management Console select Server/Agent

2. Enter a descriptive name for the Agent

3. Enter the IP address or hostname of the server on which the ASP.NET will be running

4. Enter the shared secret used above on the ASP.NET

5. Click on Apply to save changes



Agents:

Name: local

Hostname/IP: 127.0.0.1

Shared secret: ••••••••••••••••••••••

Group: ---ANY---

Authentication Modes: ALL

Name: IIS

Hostname/IP: 192.168.1.1

Shared secret: ••••••••••••••••••••••

Group: ---ANY---

Authentication Modes: ALL

Note: Session creation by username is not required for this integration as PINsafe can use session ID.

115.5 Filter Installation

To install the filter, simply run the executable program found in the downloadable zip file. You can generally accept the default recommendations, unless you have reason to change them.

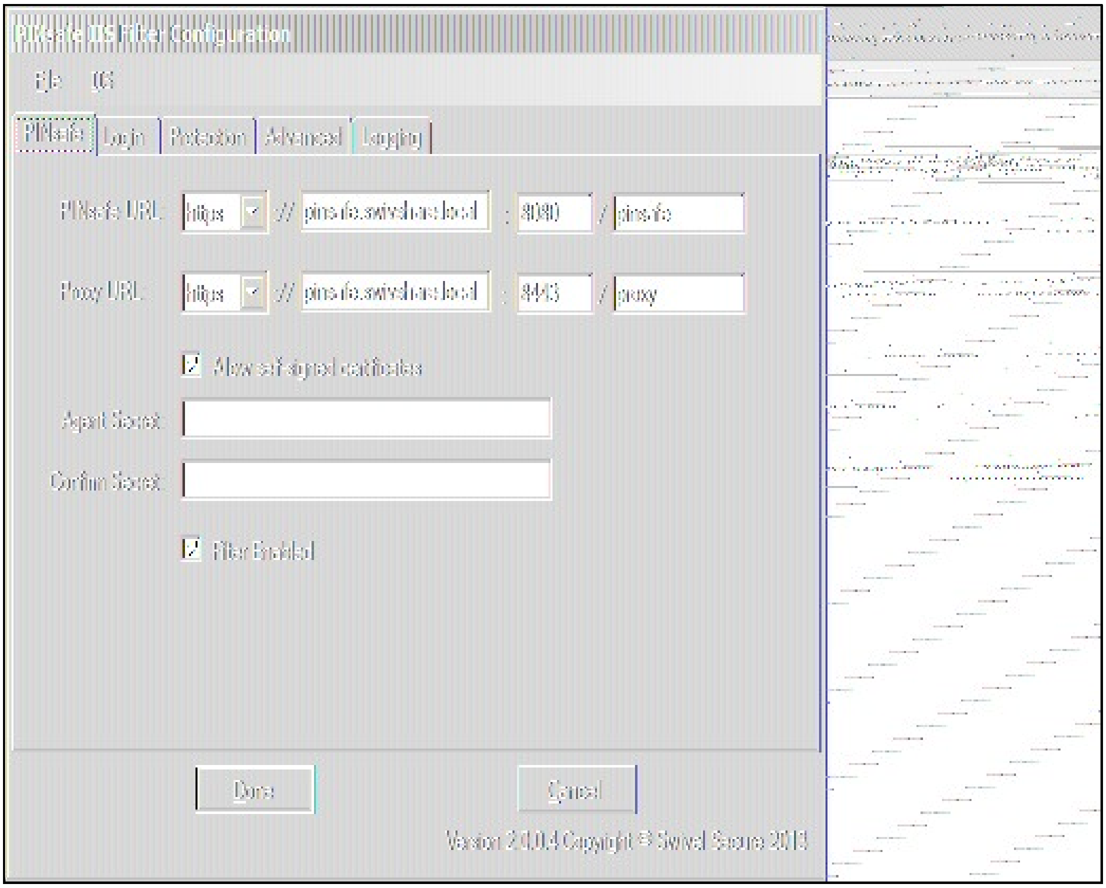
Once the filter is installed, you will be taken to the configuration program (unless you choose not to do so yet).

115.6 Filter Configuration

The filter configuration program enables you to set up which PINsafe server to use for authentication, and also the rules governing which URLs need PINsafe authentication.

The program displays a form with multiple tabs. The tabs are described in separate sections below.

115.6.1 PINsafe Tab


PINsafe IIS Filter Configuration
File
OK
PINsafe
Login
Protection
Advanced
Logging
Done
Cancel
Version 2.0.0.4 Copyright © Swivel Secure 2013

PINsafe URL: https :// pinsafe.swivelsecure.local : 8080 / pinsafe

Proxy URL: https :// pinsafe.swivelsecure.local : 8443 / proxy

☑ Allow self-signed certificates

Agent Secret:

Confirm Secret:

☑ Filter Enabled

On this page, you define the PINsafe server settings used for authentication.

Firstly, you define the URL for the PINsafe server, as used to authenticate users.

Secondly, you define the URL for the proxy server, used to deliver single channel images (TURing or PINpad) or dual channel on-demand messages. This may be the same as the PINsafe URL - typically the host name or IP address will be the same. However, if you have an virtual or hardware appliance running PINsafe 3.8 or earlier, PINpad is not available directly from PINsafe. You need to install a recent version of the proxy application, in which case the port and context should be ":8443/proxy", rather than the usual ":8080/pinsafe". These settings will always work for any version of the virtual or hardware appliance. If you have a PINsafe version 3.9 or newer, or are not using PINpad, you can safely use ":8080/pinsafe" for both.

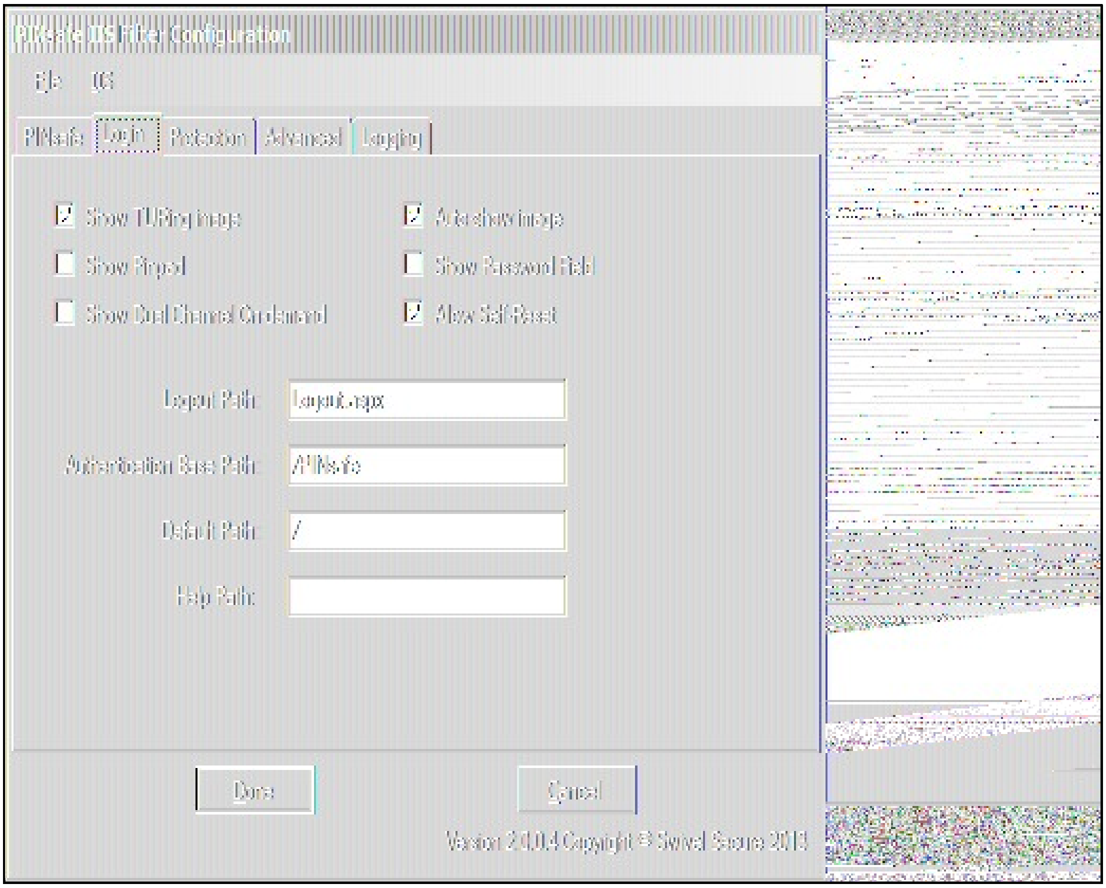
Note that the URLs only need to be resolvable and accessible from the web server. Direct access for the end user to the PINsafe server is not required - the filter proxies all requests.

The next option is "Allow self-signed certificates". If you are using https (recommended), and have specified an IP address for the PINsafe server (not recommended), or have a self-signed or untrusted SSL certificate (not recommended), you need to check this option. For production use, it is recommended that you install a certificate on the Swivel virtual or hardware appliance with the fully-qualified name that you are using to connect to it. If the Swivel virtual or hardware appliance is not visible externally, the certificate can be self-signed or signed by an internal certificate authority, and you can install the signing authority certificate as a trusted certificate on the web server. This is the recommended solution for production use.

Next, you need to enter the Agent secret, which you entered on the PINsafe Agent definition earlier. Enter it twice to confirm it.

The final option on this tab enables or disables the filter. Should you wish to disable the filter temporarily for any reason, you can do this for all websites on this server using this checkbox.

115.6.2 Login Tab


PINsafe IIS Filter Configuration
File
OK
PINsafe
Login
Protection
Advanced
Logging
Done
Cancel
Version 2.0.0.4 Copyright © Swivel Secure 2013

☑ Show TURing image
☑ Auto show image
□ Show Pinpad
□ Show Password Field
□ Show Dual Channel On demand
☑ Allow Self-Reset

Logout Path: Logout.aspx

Authentication Base Path: /PINsafe

Default Path: /

Help Path:

This tab allows you to control the login page used to authenticate to PINsafe.

The 3 checkboxes on the left-hand side allow you to display TURing image, PINpad or a dual-channel on-demand button. You can't have both TURing and PINpad at the same time, but either one can be combined with dual-channel on-demand.

Auto-show image, if checked, will display the TURing image or Pinpad as soon as the username has been entered and the focus moves away from it. This doesn't affect dual-channel on-demand - you always need to click the button for this.

Show Password Field, if checked, will display a password field as well as the OTC field. You only need this if PINsafe passwords are enabled, or the Agent is configured to check the repository password.

Allow self-reset, if checked, will display a link for the self-reset page on the login page. **NOT IMPLEMENTED IN THIS VERSION**.

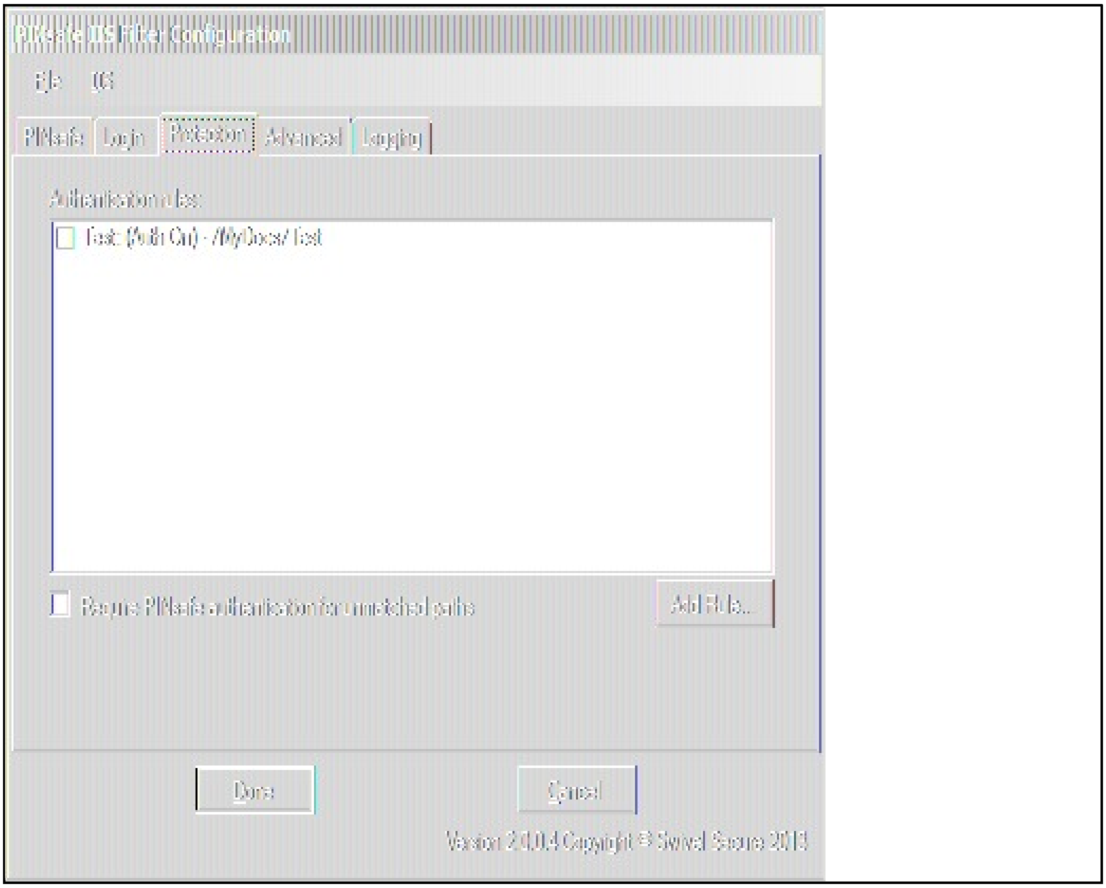
Logout path is the full path used to log out from PINsafe. Typically, this will be /PINsafe/Logout.aspx. If this is detected in the URL, the PINsafe authentication cookie will be removed, and users must re-authenticate to access protected URLs.

Authentication Base Path is the path containing the PINsafe login pages. It will be used when deploying to a web application as the virtual directory. The default is "/PINsafe", and typically you should not need to change this.

Default Path is the path to which the user is redirected after authentication if no source path is provided - for example, if the user navigates directly to the login page. Typically, the user attempts to access a page directly, and is redirected to the login page, with the intended page as the source path.

Help Path is a path to a help file describing how to authenticate to PINsafe. Swivel do not provide such a page, but if the customer wishes to do so, they can enter it here, and a link will be provided on the login page. **NOT IMPLEMENTED IN THIS VERSION**.

115.6.3 Protection Tab



Authentication rules:

□ Test: (Auth On) - /MyDocs/Test

□ Require PINsafe authentication for unmatched paths

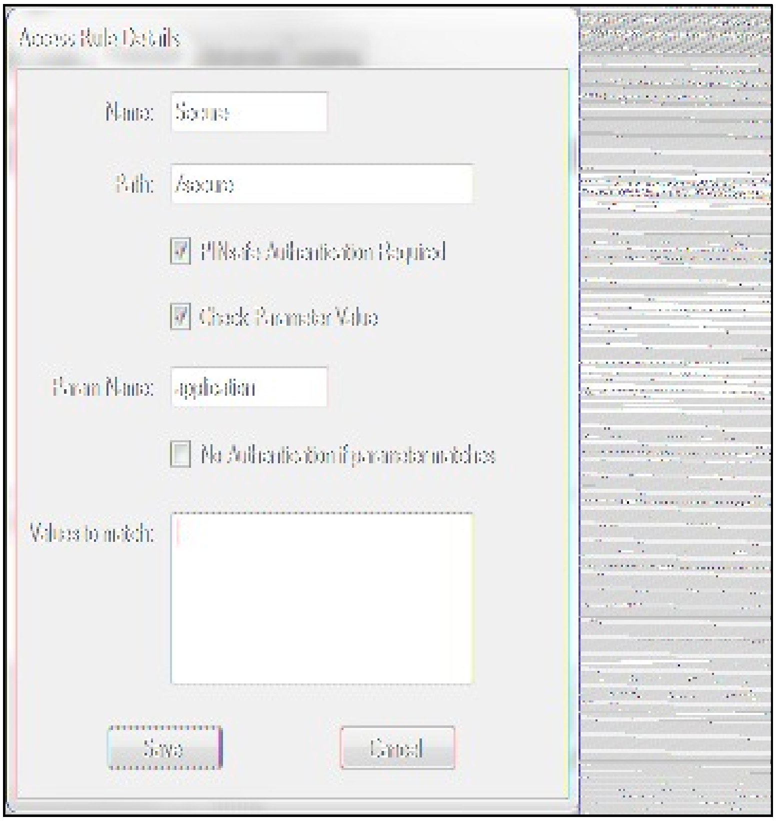
Version 2.0.0.4 Copyright © Swivel Secure 2013

On this page, you specify which paths should require PINsafe authentication. You do this by defining a list of rules. Each rule is a path to be matched, with a flag indicating whether or not PINsafe authentication is required. The filter runs through the rules in order until it matches one, and determines whether or not to check for PINsafe authentication according to that rule.

If no rules match, the default rule can either specify that PINsafe authentication is required or is not required.

NOTE: if you specify the default rule to require PINsafe authentication, make sure that any paths used by the login page are excluded. In particular, you will need a rule for the authentication base path (e.g. "/PINsafe") that does NOT require PINsafe authentication. This is not necessary if the default rule does not require PINsafe authentication.

You can create new rules by clicking the "Add Rule" button. The following dialog appears:



Access Rule Details

Name: Secure

Path: /secure

☑ PINsafe Authentication Required

☑ Check Parameter Value

Param Name: application

□ No Authentication if parameter matches

Values to match:

The name is just a label for the rule - it has no intrinsic meaning.

Path is the path that must be matched. By default, the path specified must match the **START** of the request path, so must start with "/": for example, "/secure" will match "/secure/default.aspx" or "/secure/subite/default.aspx", but not "/home/secure/default.aspx". However, if you start the path with a "*", it will match the **END** of the request path: for example "*/default.aspx" will match any page called "default.aspx" anywhere in the website.

"PINsafe Authentication Required" indicates whether or not this rule requires PINsafe authentication.

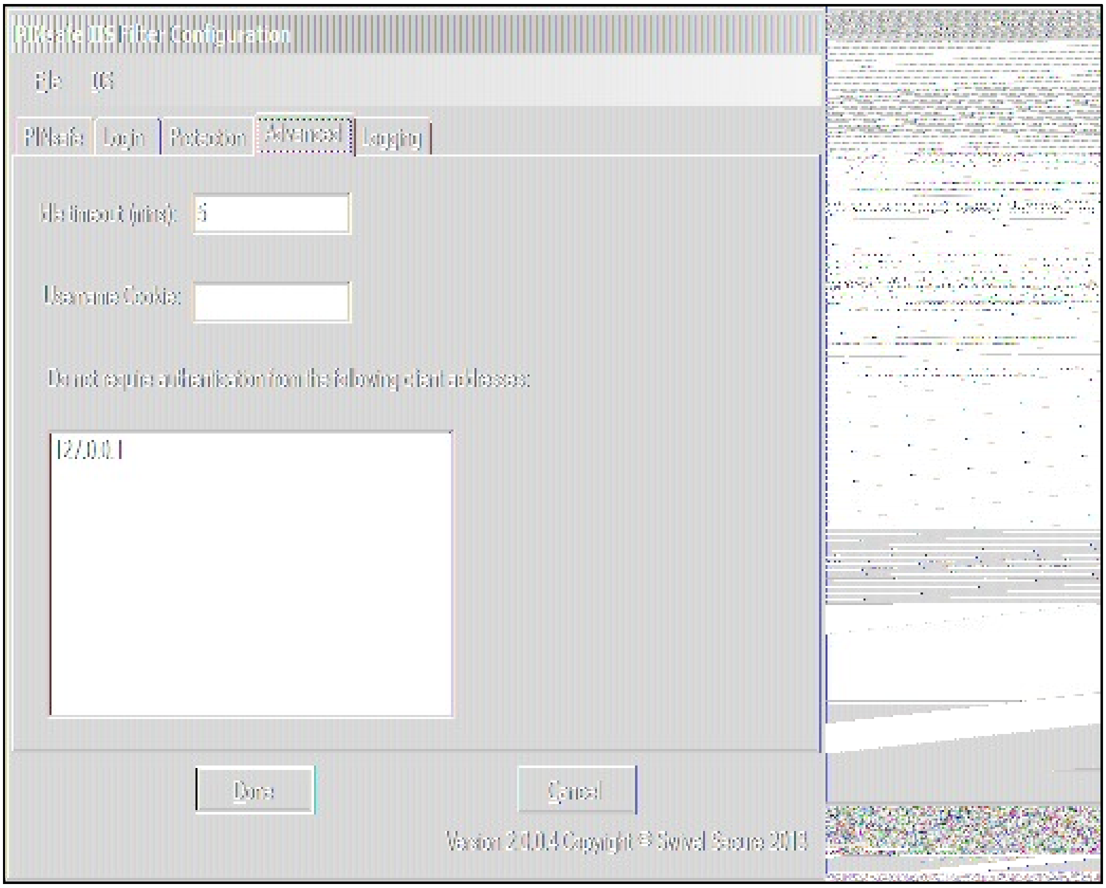
"Check Parameter Value" allows finer control over PINsafe authentication. When checked, you can specify the name of a single query parameter that is checked to determine whether or not PINsafe authentication is required. You can specify a list of possible values for the parameter, but if you specify no values, the presence or absence of the parameter determines whether or not to require authentication.

The final control on this page, "No Authentication if parameter matches", allows you to reverse the parameter check. So for example, if the rule requires authentication, but this option is enabled, PINsafe authentication is required UNLESS the parameter value matches one of the specified values.

A final note of clarification: the rule is matched purely on the path, not on the parameters. Specifying "Check Parameter Value" only allows you to change whether or not authentication is required.

Going back to the main form and the list of rules, to change a rule, change the order of rules, or delete rules, check the rules you want to move/change/delete and right-click to bring up a context menu.

115.6.4 Advanced Tab



PINsafe IIS Filter Configuration

Idle timeout (mins): 5

Username Cookie:

Do not expire authentication from the following client addresses:

127.0.0.1

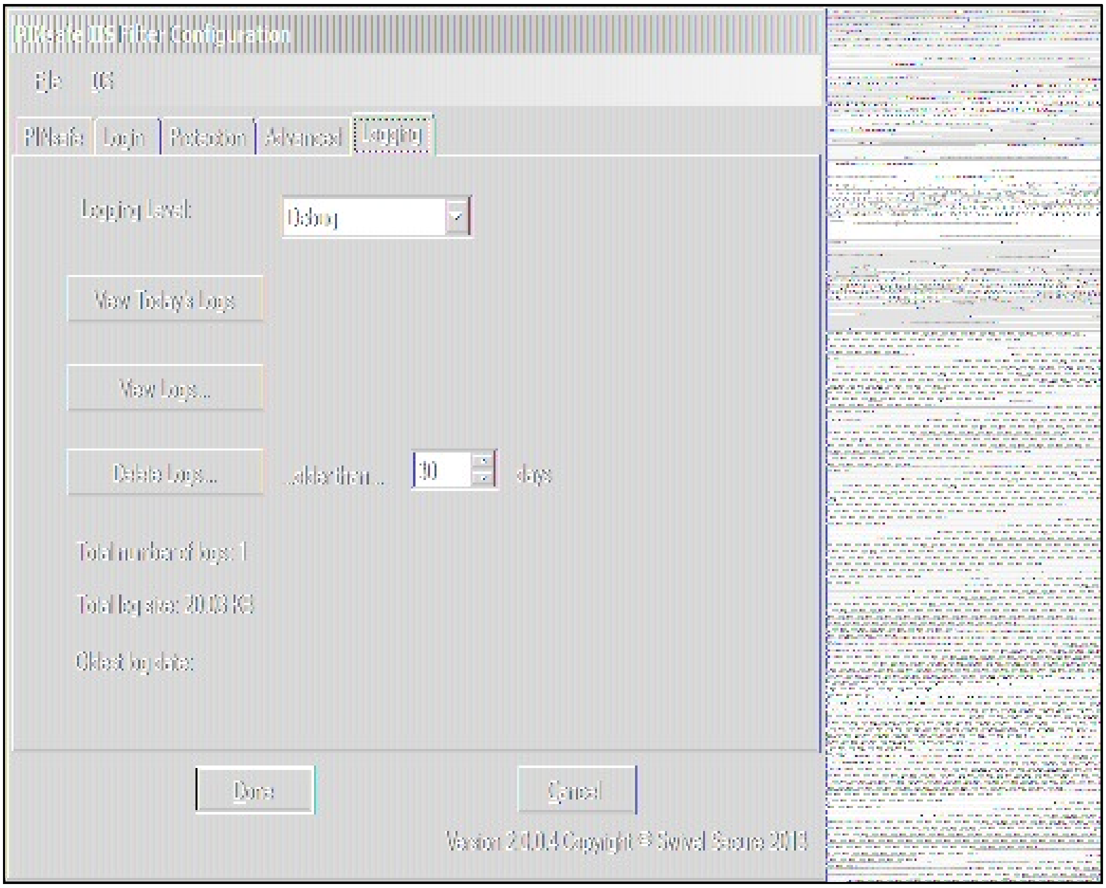
There are 3 settings on this tab:

Idle timeout: this specifies how long the PINsafe authentication cookie is valid if the web page is not refreshed. The default is 5 minutes. If the page is idle for more than 5 minutes, you will need to re-authenticate. You can make this longer if you wish. Note that this doesn't mean that you have to reauthenticate after every 5 minutes - only if you do not refresh the page (or view a different page). Every time a request is made to the website, the timeout resets.

Username cookie: this is provided for additional web development. If you specify a name here, the filter will provide a cookie with the name of the authenticated PINsafe user. **NOT IMPLEMENTED IN THIS VERSION**.

Excluded clients: the final option allows you to specify that PINsafe authentication is not required if the request comes from specified client IP addresses.

115.6.5 Logging Tab



Logging Level: Debug

...older than... 30 days

Total number of logs: 1

Total log size: 20.03 KB

Oldest log date:

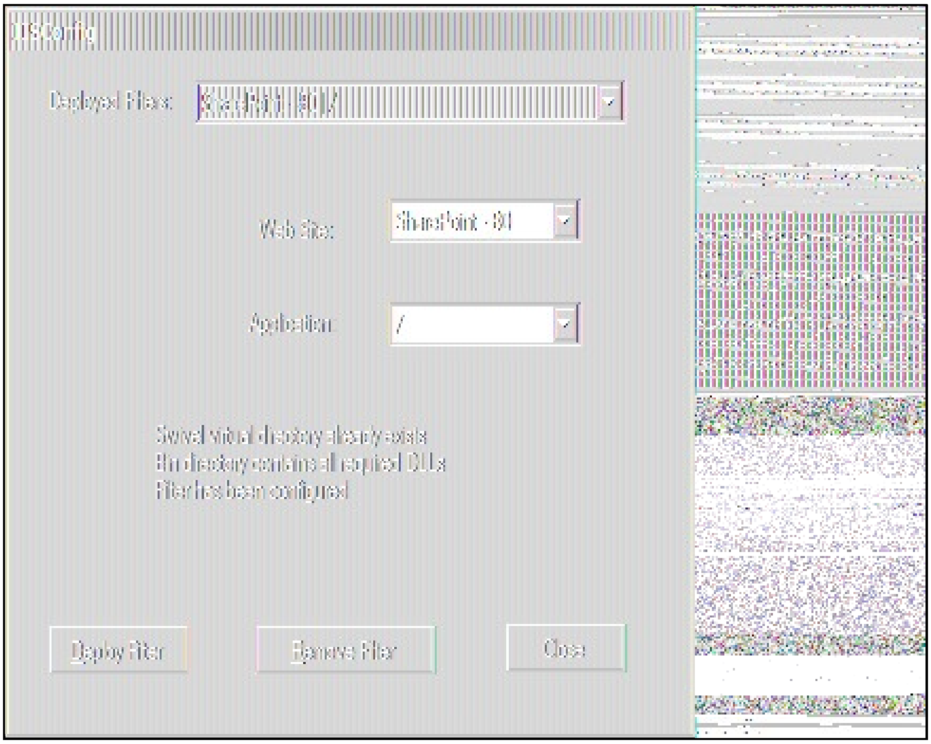
Version 2.0.0.4 Copyright © Swivel Secure 2013

This page allows you to specify what logging the filter does, and to view or delete logs.

There are 4 logging levels: Debug, Info, Error and None. The most verbose, Debug, logs all activity, and all pages checked. Info logs only when a redirect to the login page occurs. Error only logs error events. None disables all logging.

115.6.6 IIS Configuration

None of the option specified above have any effect on any website until the filter is deployed to the website. To do this, Select the IIS menu option, then the Configure sub-menu. The following dialog is displayed:



Deployed Filters: SharePoint | 80 | /

Web Site: SharePoint - 80

Application: /

Swivel virtual directory already exists
Bin directory contains all required DLLs
Filter has been configured

The first drop-down lists all websites where the filter has been deployed. Initially, therefore, it is empty. If you have already deployed to a website, you can select it to check the status.

The second drop-down lists all websites on the current server. Select one to enable the application drop-down.

The third drop-down list all web applications on the selected website. Select one to check, deploy or remove the filter.

One you have selected a web application, you can choose to deploy or remove the Swivel filter.

115.7 Additional Configuration Options

115.8 Testing

Navigate to the login page. Attempting to login with a correct username and password but no one time code should result in failure. Only when a correct PINsafe one time code is entered should the user be logged in. If the Single Channel button is displayed then an image should appear.

115.9 Troubleshooting

To verify the Single Channel Image works, on the ASP.NET server enter the following into a web browser, which should display a Turing image if the sever is functioning correctly:

For a PINsafe virtual or hardware appliance installs:

https://<pinsafe_server_ip>:8080/pinsafe/SCImage?username=test

For a software only install see Software Only Installation

115.10 Known Issues and Limitations

Requesting a Security String Index would require modification of the login page for an existing button. See also Multiple Security Strings How To Guide

115.11 Additional Information

For assistance in the PINsafe installation and configuration please firstly contact your reseller and then email Swivel Secure support at support@swivelsecure.com

116 Microsoft IIS version 7 Integration

116.1 Overview

This document outlines the steps required to integrate the Internet Information Server (IIS) with Swivel using dual or single channel authentication. The Swivel install requires configuring an agent on the Swivel server and setting up a shared secret with the IIS server to allow communication for authentication. An ISAPI filter installed on the IIS server allows access to protected resources through the Swivel authentication.

NOTE: This document refers to the version of the filter numbered 1.2, and the configuration application with the same version number. 32-bit and 64-bit versions of the filter are available. Version 1.3.4, with PINpad support, is available for 64-bit only.

If Windows 2008 Server server is being used, or only ASP.Net applications are being protected an alternative authentication is available, see Microsoft IIS version 7 ASP.NET Integration

116.2 Prerequisites

Internet Information Server on Windows server 2008, 32-bit or 64-bit operating system.

Swivel server

The appropriate Swivel ISAPI filter software can be downloaded from here, depending on your operating system:

The latest release is version 1.3.9. Support for PINpad is included from 1.3.0 onwards. Version 1.3.4 adds PINpad support for change PIN as well:

- 64-bit ISAPI Filter
- 32-bit ISAPI Filter

These links refer to version 1.2 of the filter, provided for legacy purposes.

- 32-bit ISAPI Filter
- 64-bit ISAPI Filter

116.3 IIS Filter Version History

1.2 32 bit and 64 bit

1.3.3 (64-bit only): PINpad support added

1.3.4 (64-bit only): added PINpad support for ChangePIN

1.3.5 (64-bit only): enhancements to ChangePIN support

1.3.6 (64-bit only): added a default logout page

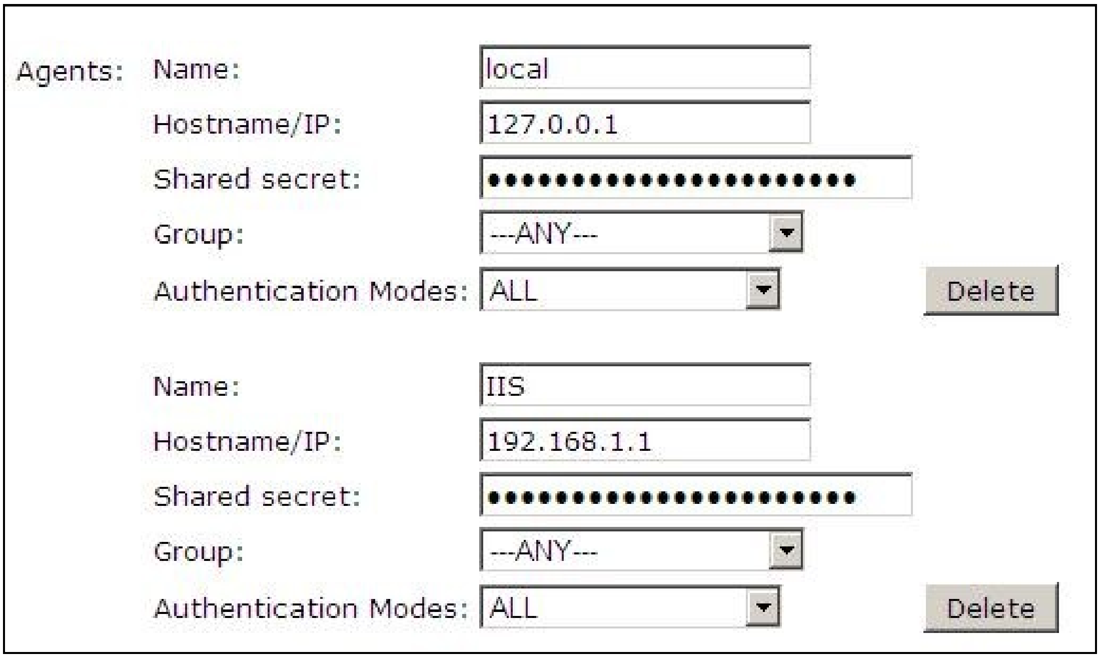
1.3.7-9: various bug fixes

116.4 Swivel Configuration

On the Swivel server configure the agent that is permitted to request authentication. On the Swivel Administration Console select from the server menu Agents and enter the details of the IIS server IP address and a shared key, then click on apply.

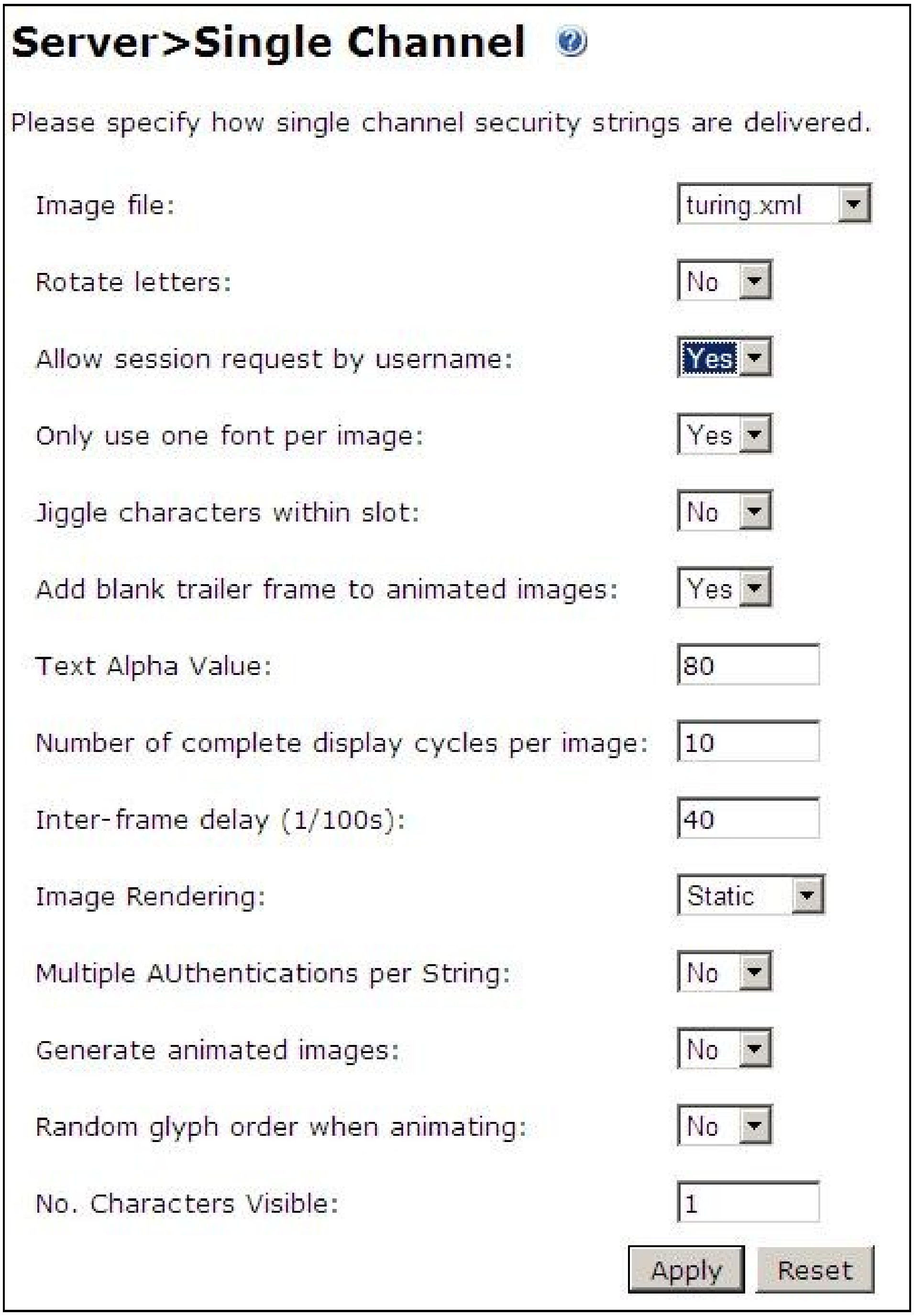
Example:

```
Name : IIS server 1,
Hostname/IP : 192.168.1.1,
shared secret : secret
```



Agents:	Name:	local	
	Hostname/IP:	127.0.0.1	
	Shared secret:	●●●●●●●●●●●●●●●●●●●●●●	
	Group:	---ANY---	
	Authentication Modes:	ALL	Delete
	Name:	IIS	
	Hostname/IP:	192.168.1.1	
	Shared secret:	●●●●●●●●●●●●●●●●●●●●●●	
	Group:	---ANY---	
	Authentication Modes:	ALL	Delete

If Single Channel communication is to be used, select from the Swivel Administration Console Single Channel, and set the Allow image request by username to Yes then click on apply.



Server>Single Channel

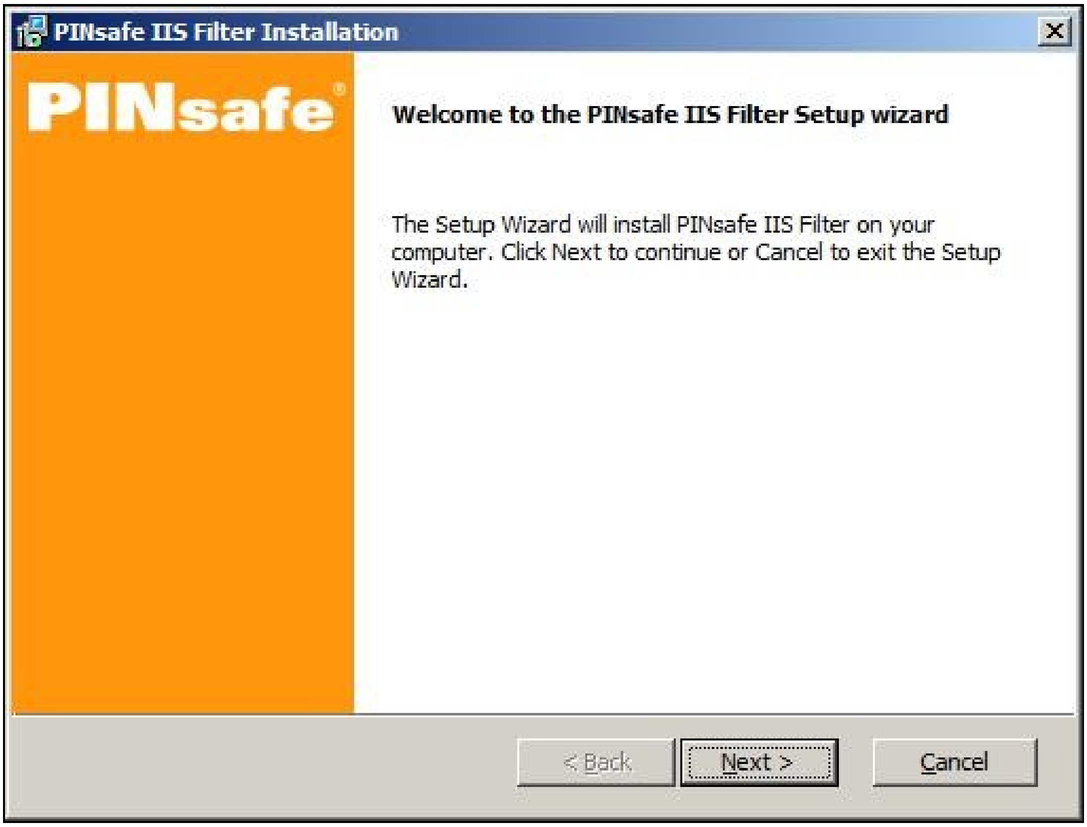
Please specify how single channel security strings are delivered.

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

116.5 Configuring the IIS Server

116.5.1 Install the Swivel Filter

1. On the IIS server run the PINsafeIISFilter.exe. The IIS filter may need to be run as an Administrator user (The filter needs to be installed by IIS running as Administrator user but it can run as a normal user).

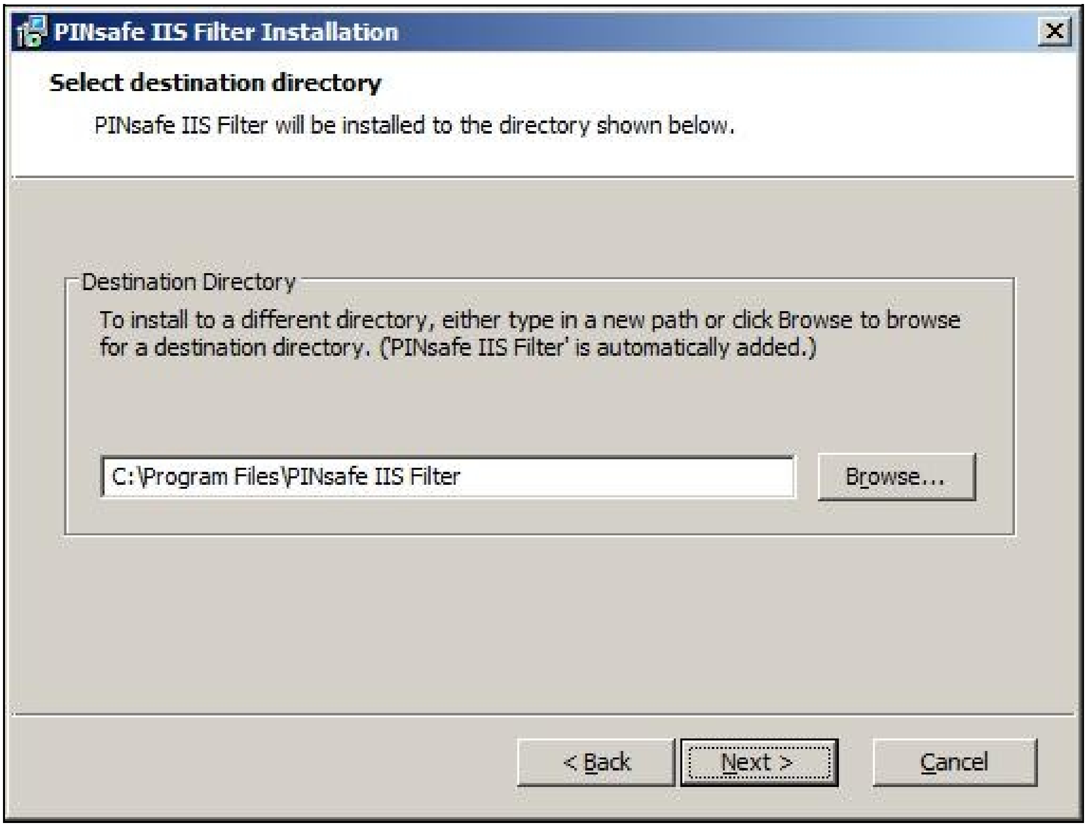


PINsafe IIS Filter Installation

Welcome to the PINsafe IIS Filter Setup wizard

The Setup Wizard will install PINsafe IIS Filter on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

2. Choose the Path to Install to such as C:\Program Files\PINsafe IIS Filter



PINsafe IIS Filter Installation

Select destination directory

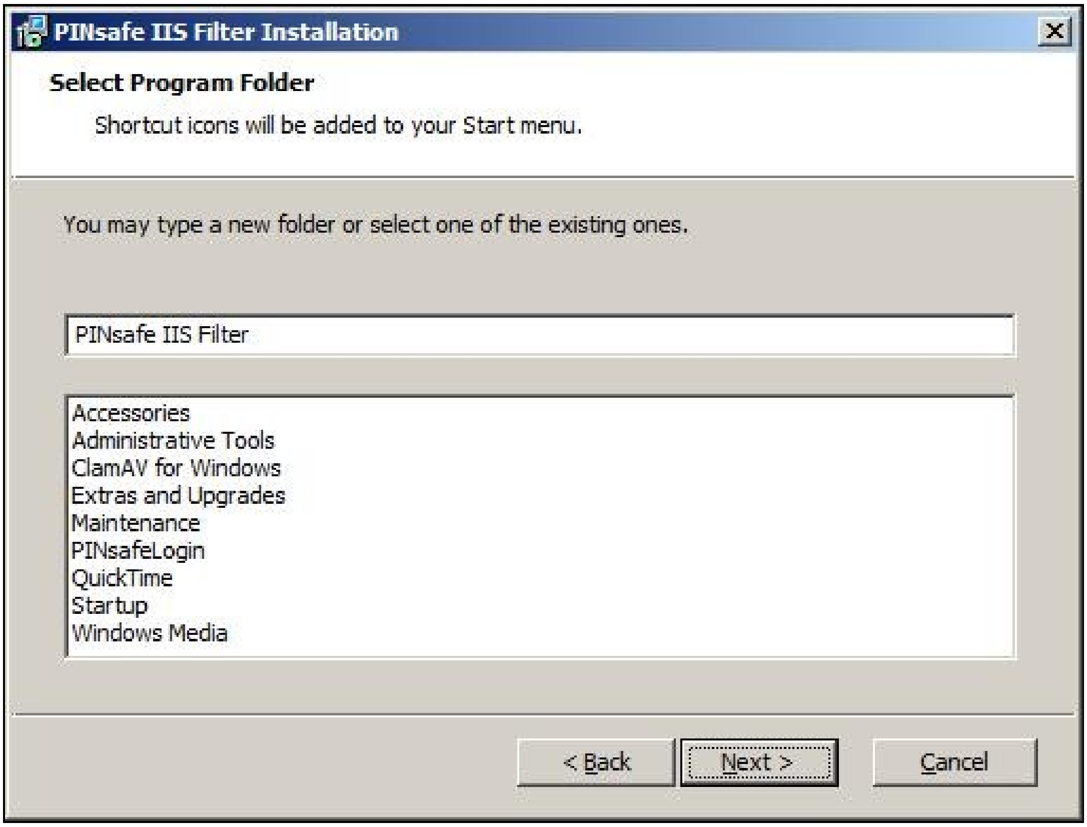
PINsafe IIS Filter will be installed to the directory shown below.

Destination Directory

To install to a different directory, either type in a new path or click Browse to browse for a destination directory. ('PINsafe IIS Filter' is automatically added.)

C:\Program Files\PINsafe IIS Filter

3. Select Start Menu Folder


PINsafe IIS Filter Installation

Select Program Folder

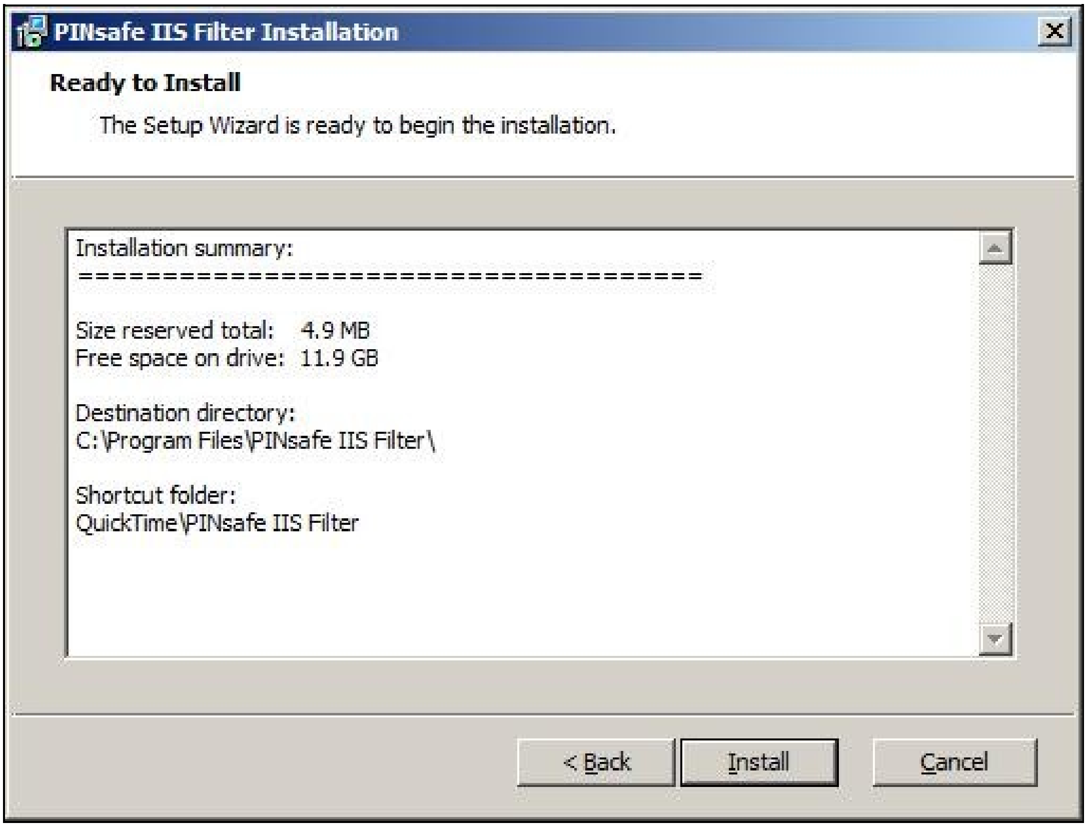
Shortcut icons will be added to your Start menu.

You may type a new folder or select one of the existing ones.

PINsafe IIS Filter

Accessories
Administrative Tools
ClamAV for Windows
Extras and Upgrades
Maintenance
PINsafeLogin
QuickTime
Startup
Windows Media

4. When details are correct click on Install


PINsafe IIS Filter Installation

Ready to Install

The Setup Wizard is ready to begin the installation.

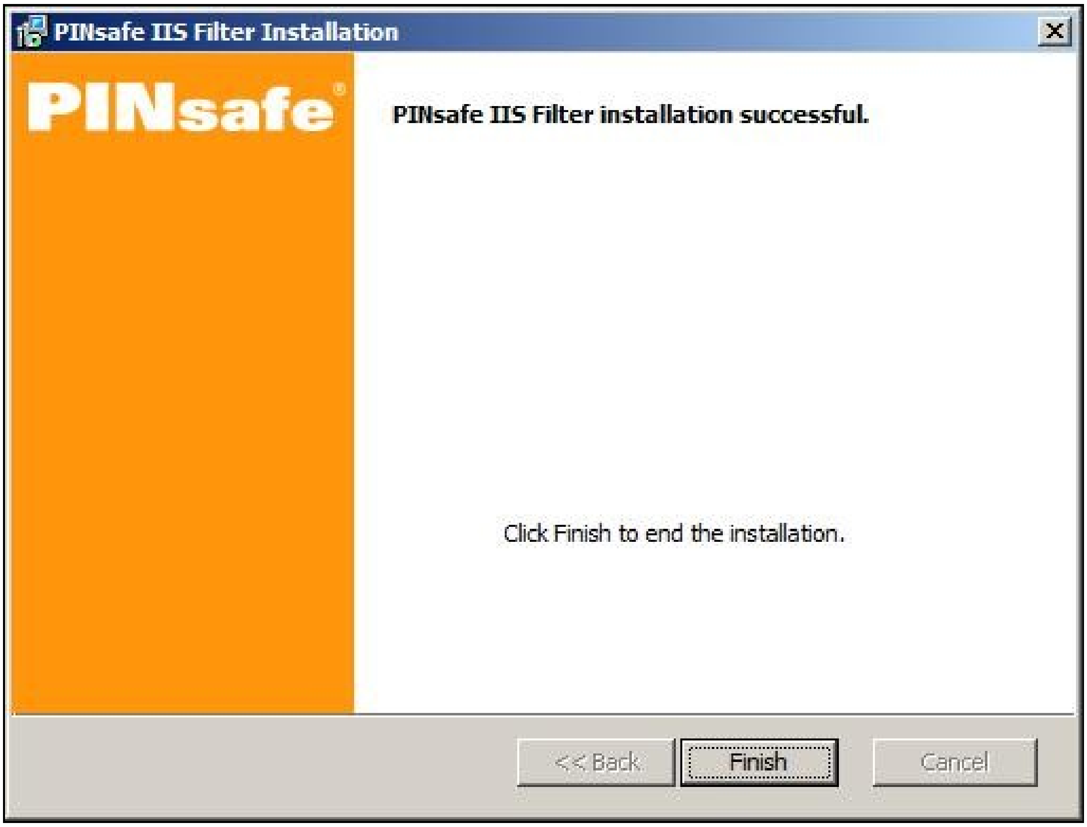
```
Installation summary:
=====================================

Size reserved total:    4.9 MB
Free space on drive:  11.9 GB

Destination directory:
C:\Program Files\PINsafe IIS Filter\

Shortcut folder:
QuickTime\PINsafe IIS Filter
```

5. If the error ?Incorrect Command Line Parameters? is seen click on OK

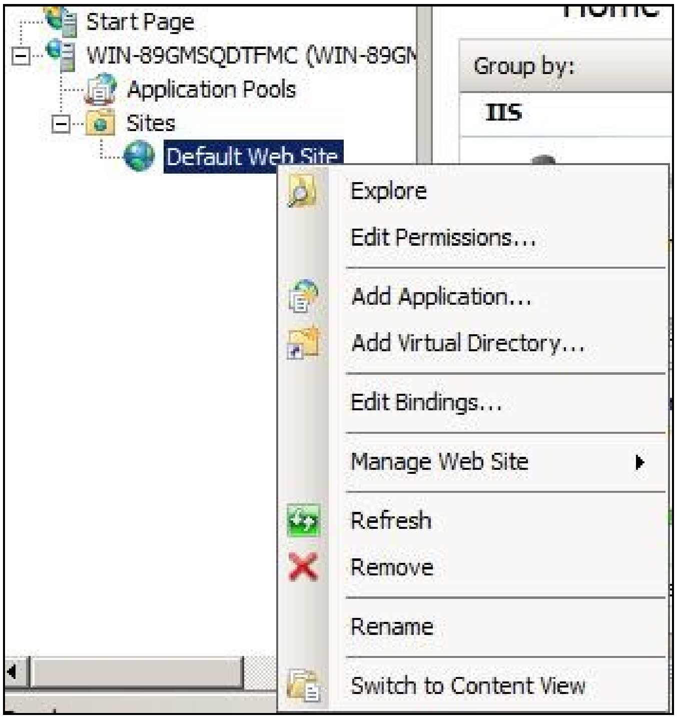

PINsafe IIS Filter Installation

PINsafe IIS Filter installation successful.

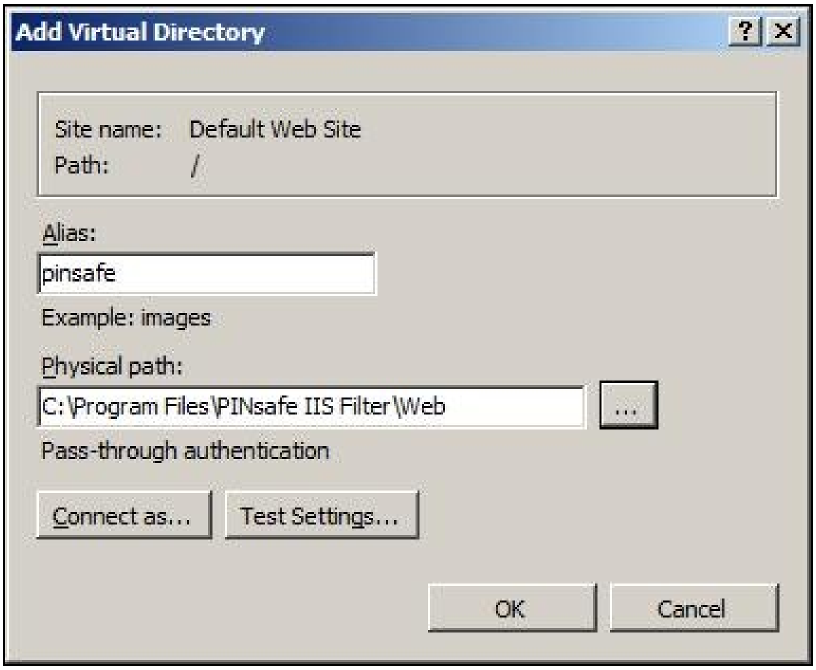
Click Finish to end the installation.

Create a PINsafe virtual directory

1. On the Internet Information Services Manager right click on the website and select Add Virtual Directory



2. Create an Alias called PINsafe



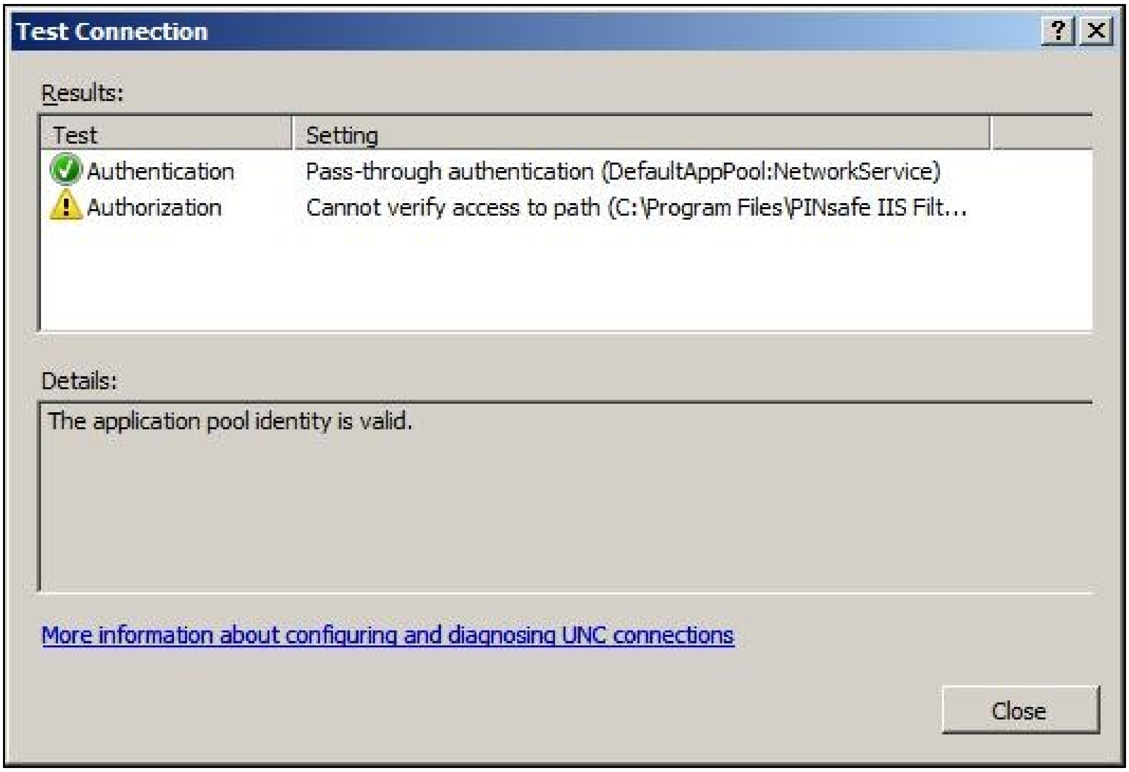
Add Virtual Directory

Site name: Default Web Site
Path: /

Alias: pinsafe
Example: images

Physical path: C:\Program Files\PINsafe IIS Filter\Web
Pass-through authentication

3. Point the path to the PINsafe directory Web folder, by default C:\Program Files\PINsafe IIS Filter\Web. Test Connection verifies the path, and Connect As allows Application User for pass through authentication.



Test Connection

Results:

Test	Setting
✓ Authentication	Pass-through authentication (DefaultAppPool:NetworkService)
⚠ Authorization	Cannot verify access to path (C:\Program Files\PINsafe IIS Filt...

Details:

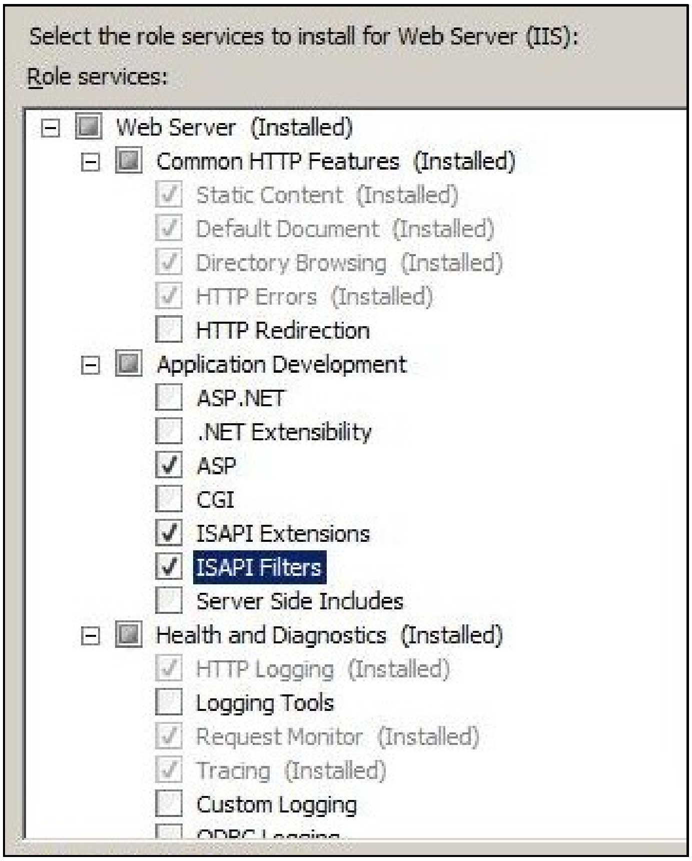
The application pool identity is valid.

More information about configuring and diagnosing UNC connections

4. Set the permissions to Read and Run Scripts

116.5.2 Installing the ISAPI Filters, extensions and ASP on IIS

This requires the ISAPI filters, ISAPI extensions and ASP to be installed. To verify or install these, for Windows 2008, on the IIS server start the Server Manager by selecting Start/Administrative Tools/Server Manager then expand the tab for Roles, click on the Web Server (IIS), then look under Role Services to ensure that the *ISAPI Filters*, *ISAPI Extensions* and ASP are installed. If it is not click on Add Role Services and add them.



Select the role services to install for Web Server (IIS):

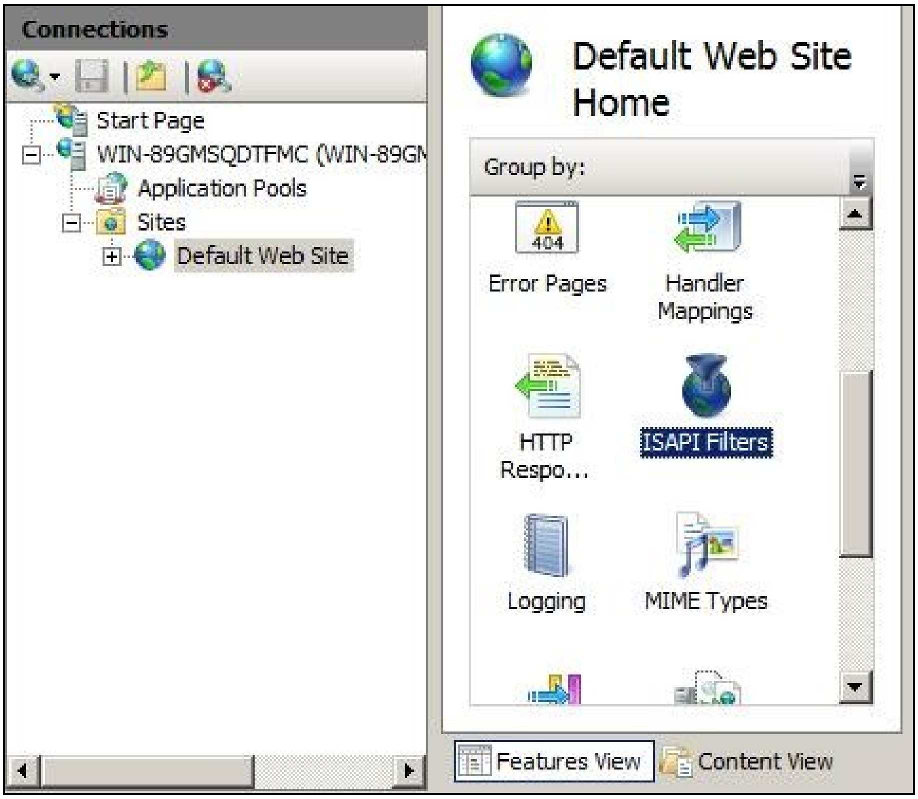
Role services:

- ▣ Web Server (Installed)
  - ▣ Common HTTP Features (Installed)
    - ☑ Static Content (Installed)
    - ☑ Default Document (Installed)
    - ☑ Directory Browsing (Installed)
    - ☑ HTTP Errors (Installed)
    - □ HTTP Redirection
  - ▣ Application Development
    - □ ASP.NET
    - □ .NET Extensibility
    - ☑ ASP
    - □ CGI
    - ☑ ISAPI Extensions
    - ☑ ISAPI Filters
    - □ Server Side Includes
  - ▣ Health and Diagnostics (Installed)
    - ☑ HTTP Logging (Installed)
    - □ Logging Tools
    - ☑ Request Monitor (Installed)
    - ☑ Tracing (Installed)
    - □ Custom Logging
    - □ ODBC Logging

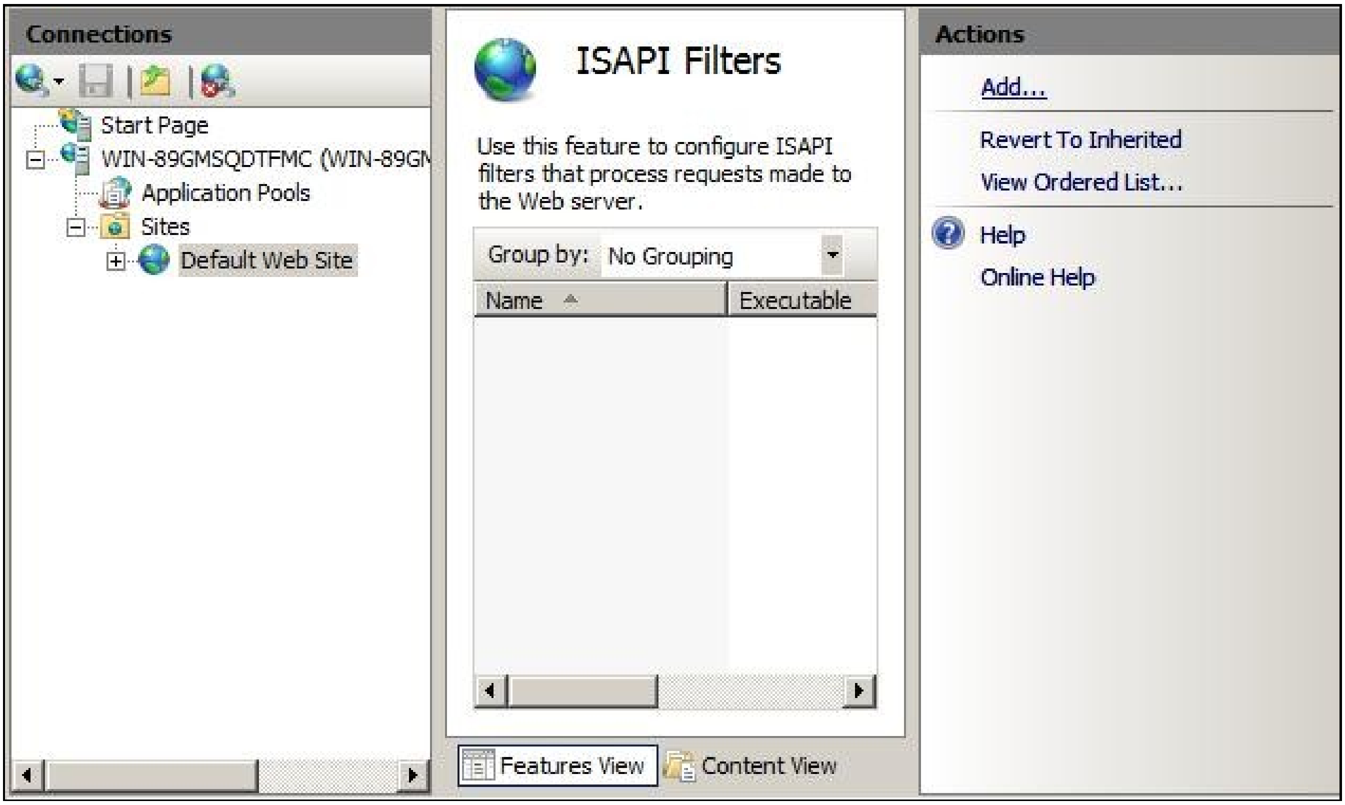
116.5.3 Install the Swivel ISAPI Filter

1. On the Internet Information Services Manager Select the website

2. Select ISAPI filters by double clicking on the ISAPI filters icon

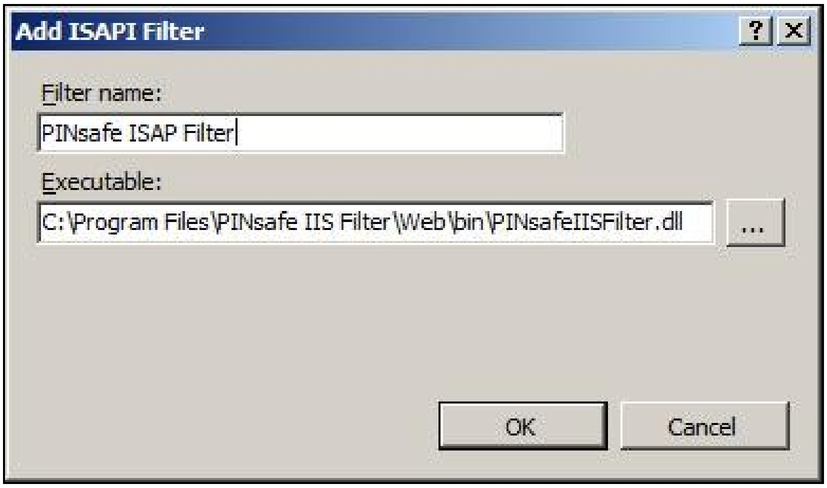


3. Under Actions select Add



Use this feature to configure ISAPI filters that process requests made to the Web server.

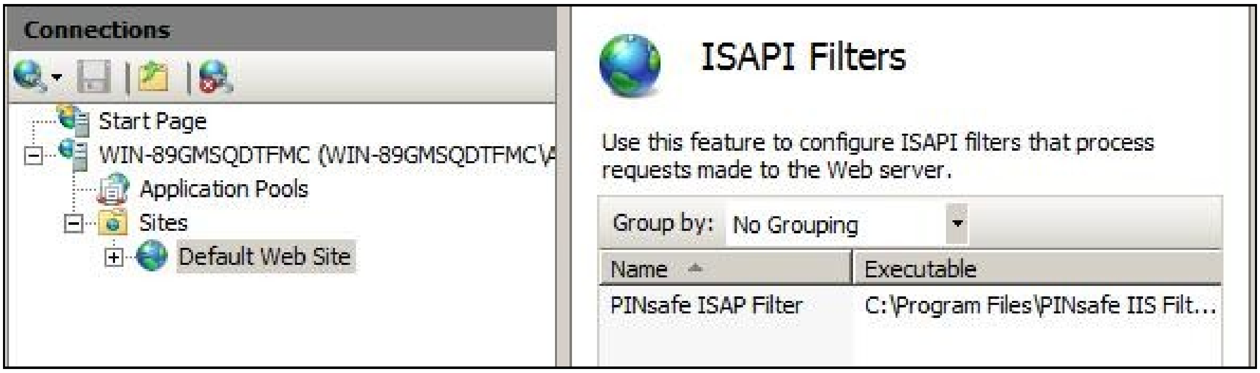
4. Select the Path to the Swivel ISAPI filter. Note that the actual file you require will be PINsafeIISFilter.dll, located in the sub-folder Web\bin of the installation folder. Enter a name for the Filter such as *PINsafe ISAPI Filter*. When information is complete click on Ok.



Filter name: PINsafe ISAP Filter

Executable: C:\Program Files\PINsafe IIS Filter\Web\bin\PINsafeIISFilter.dll

5. Ensure the Swivel ISAPI filter is the top filter by selecting the 'View Ordered List...'



Connections

Start Page

WIN-89GMSQDTFMC (WIN-89GMSQDTFMC\A

Application Pools

Sites

Default Web Site

ISAPI Filters

Use this feature to configure ISAPI filters that process requests made to the Web server.

Group by: No Grouping

Name	Executable
PINsafe ISAP Filter	C:\Program Files\PINsafe IIS Filt...

116.5.4 Configure the ISAPI filter

1. Select Start Programs/PINsafe IIS Filter/Filter Configuration. This will look for the location of config.xml, this will be created when first used and this must be located in web/bin.

Note: If the Swivel Filter Configuration does not exist in the Start Menu, it can be started by running it from its install location. The default install location is C:\Program Files\PINsafe IIS Filter\Web\bin\ConfigApp.exe

2. You will be asked to select the location of the configuration file. It is important that you select the right location. It should be in the same folder as the ISAPI filter. Initially, this file will not exist, but will be created as a result of running this configuration application.

PINsafeIISFilter Options

PINsafeServer: The PINsafe Server tab contains settings which define the Swivel server which will be used to authenticate users.

Hostname/IP: The name or IP address of the Swivel server.

Port: The port number used by the Swivel server (normally 8080, or 8443 for HTTPS).

Context: The context (i.e. web application name) of the Swivel instance on that server

Secret: The common secret used to communicate with the Swivel server. This value must be the same as the secret defined for the Swivel agent configured earlier.

SSL enabled: Tick this box to require SSL (HTTPS) communication with the Swivel server.

Permit self-signed certificates: Tick this box to allow SSL certificates to be self-signed. This also ignores other certificate errors, such as site names not matching.

Authentication: The Authentication tab contains the following settings:

Idle time (s): The time (in seconds) for which the authentication cookie will be valid if the web page is not used.

Username header: The name of a cookie which will pass the username of the authenticated Swivel user. If this value is blank, no cookie will be provided.

Single: Indicates that single channel security strings (i.e. TURing image) are permitted.

Dual: Indicates that dual channel security strings (i.e. via e-mail, SMS) are permitted.

On-demand dual: Indicates that the login page should display a button to request dual-channel security strings.

Display password fields: Indicates that the login page should show a field for Swivel password as well as OTC.

Permit self-reset: Indicates that the user self-reset page should be enabled.

Exclusions and Inclusions: Use the inclusion and exclusion tabs to enter which paths should be protected by Swivel:

Included paths: This is a list of paths within the current website which require Swivel authentication. If this list is empty, the entire website will be protected except as indicated by the Exclusions tab. Paths should be one per line.

Excluded paths: This is a list of paths within the current website which should be exempt from Swivel authentication. This is only relevant if the included paths list is empty, in which case all paths not on this list will be protected by Swivel.

Excluded addresses: This is a list of IP addresses which are exempt from Swivel authentication. All requests from these addresses are passed through without authentication.

Misc: On the Misc tab, edit any custom paths as follows:

Default path: This is the path to which authenticated requests are directed if the login page is targeted directly. If a user tries to access a protected page, she is redirected to the login page, and after authentication, back to the page she was trying to access. If the user requests the login page directly, she will be redirected to this location after authentication.

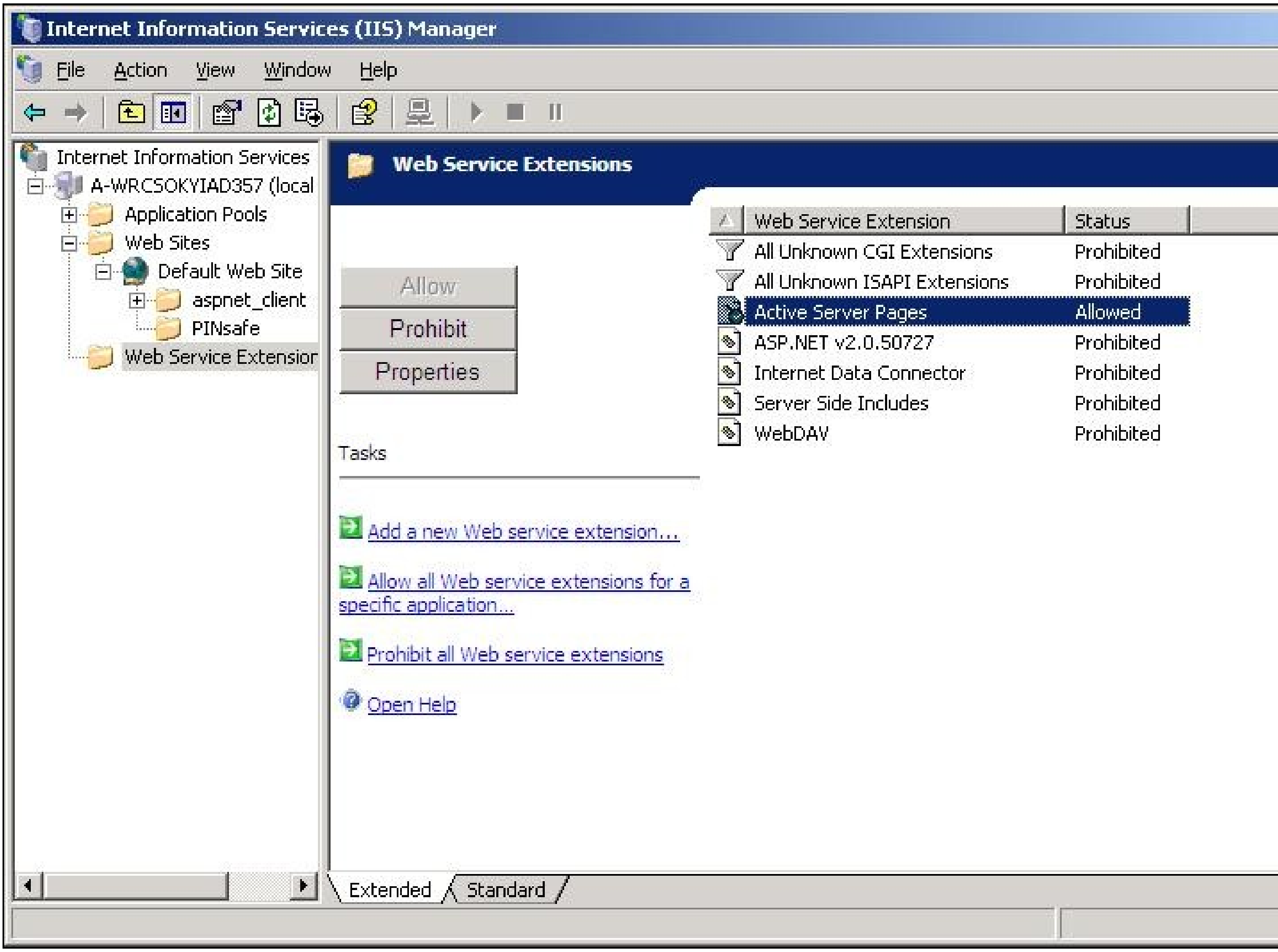
Logout path: Requesting this path will result in the user being logged out. Subsequent requests will require re-authentication, if relevant. If this path is empty, users can only be logged out by closing the browser, or if the authentication times out. Note: The logout path must be an included file location.

Virtual web path: This is the path to the Swivel authentication pages. See the next section for details on setting this up. You should normally set this to be ?/pinsafe?, unless you have a particular reason not to.

Help URL: The URL for Swivel IIS filter help. The filter does not come with help pages as standard, so this should only be filled in if help pages have been provided by the reseller or end user.

After configuration is complete Apply the settings and restart the World Wide Web Publishing Services.

Allow Active Server Pages: to verify this, select the Internet Information Services Manager expand the required server then click on Web Service Extension.



Web Service Extension	Status
All Unknown CGI Extensions	Prohibited
All Unknown ISAPI Extensions	Prohibited
Active Server Pages	Allowed
ASP.NET v2.0.50727	Prohibited
Internet Data Connector	Prohibited
Server Side Includes	Prohibited
WebDAV	Prohibited

116.6 Installing the Filter on Multiple Websites

Most of the instructions above assume that you are installing the IIS filter on the single default website of a web server. However, if you want to use the filter on multiple websites on the same server, you need to carry out a few extra steps.

Firstly, if all the settings on all the websites are exactly the same, you can configure it once, and then carry out the same steps to activate the filter on each website.

If, however, you need different settings for each website, you will need to do the following for all except the first website:

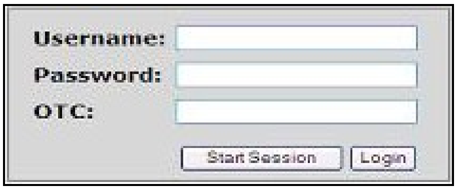
1. Make a copy of the entire Web folder, including the bin sub-folder. You can copy it as a sub-folder of Swivel IIS filter, with a different name, or you can put it somewhere completely different. It is important, however, that you keep the structure the same ? all the .asp files must remain intact, and the filter DLL must be in a sub-folder called ?bin?.

2. When you come to configure each filter, navigate to the bin sub-folder of the copy you have just made. Otherwise, configuration is exactly as before.

3. When selecting the IIS filter to install, and also when defining the virtual directory for Swivel web pages, you should use the copy you have just created, rather than the original. This is important, as both the filter and the web pages look for the configuration file relative to their own location.

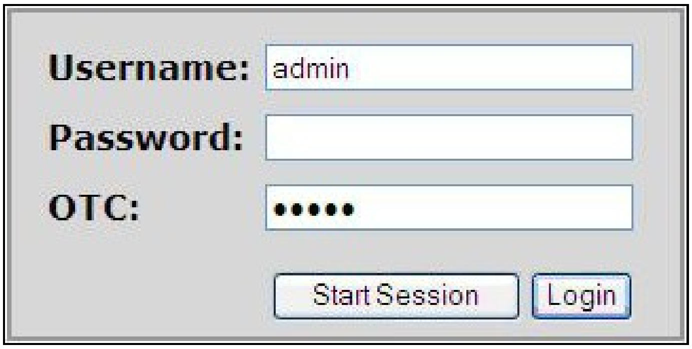
116.7 Testing

Browse to a web page that has been configured for protection. This should display a Swivel login dialogue:



Enter the Username.

For dual channel, enter the One Time Code:

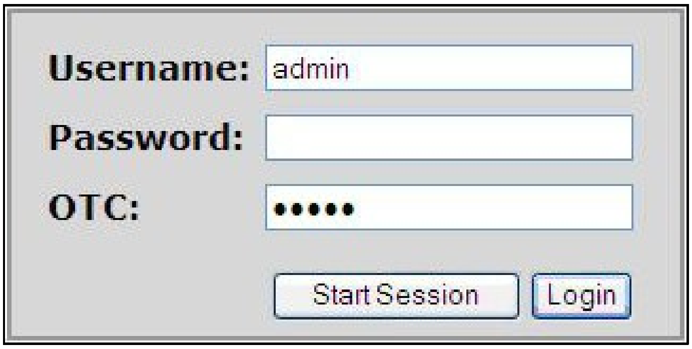


Username: admin

Password:

OTC: •••••

Or click start session to enter a single channel OTC. The Swivel log will record that a single channel session has started.

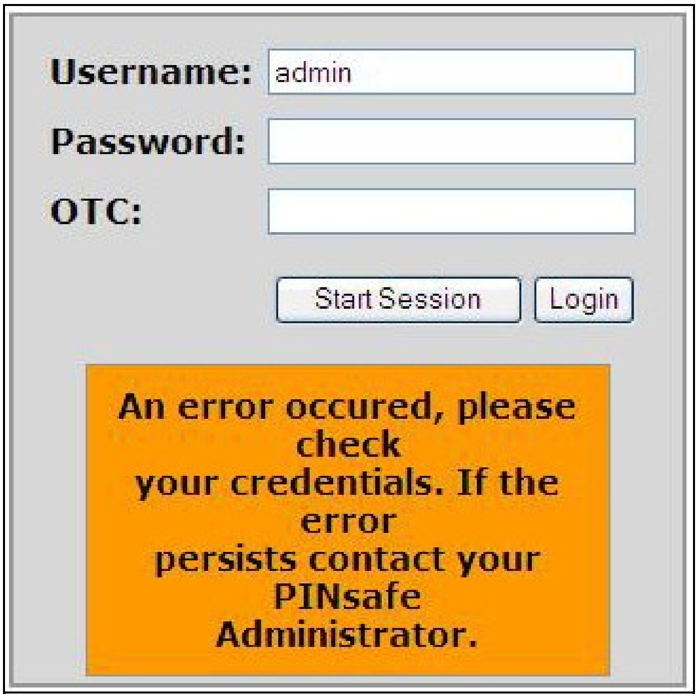


Username: admin

Password:

OTC: •••••

If authentication is successful it should redirect to the login page. If failed an error message will appear. The Swivel log will record any successful log attempt for the agent.



Username: admin

Password:

OTC:

An error occured, please check
your credentials. If the error
persists contact your PINsafe Administrator.

116.8 Uninstalling the filter

To remove the Filter, remove role services that are not required by other applications, to do this for Windows 2008, on the IIS server start the Server Manager by selecting Start/Administrative Tools/Server Manager then expand the tab for Roles, click on the Web Server (IIS), then look under Role Services to remove the *ISAPI Filters*, *ISAPI Extensions* and ASP are installed. The system will require a restart to complete.

From the IIS Manager right click on the Swivel Virtual Directory, then select Remove, Click on Yes to Confirm.

To uninstall the Swivel IIS Filter, choose Start/All Programs/PINsafe IIS Filter/PINsafe IIS Filter Uninstaller, then click Yes on the confirmation to uninstall.

The Swivel Filter config may be left after uninstalling, so to completely remove this, remove the folder Program Files\PINsafe IIS Filter.

116.9 Troubleshooting

Verify the correct filter version has been installed for the operating system i.e. 32 bit or 64 bit.

Check for error messages in the Swivel log

Check the IIS log messages

Filter Install issues: The IIS service needs to run as an administrator in order to install the filter. Once the filter is installed, it will run as the normal user. Open the Services applet and locate World Wide Web Publishing. Select properties, then go to the Log On tab. Assuming you are logged in as an administrator, select Local System account. Then restart the service. Hopefully, this will start the filter. You can then switch back to the default account and restart again.

If you are not redirected to the Swivel login page when trying to access a protected page, open IIS manager and check that the ISAPI filter is installed and has loaded properly (there should be a green arrow next to it, and the priority should be ?High?). If this is not the case, restart IIS, if you have not already done so, and try again. The filter doesn't try to install until you try to access a web page from that website, so try that before assuming it hasn't worked.

If the filter is listed, but showing a red cross, then it failed to start. In this case, check the error messages in the event log showing.

If the filter shows as green, with priority unknown, it may not be installed. In this case, you need to check. You can do this with a debug viewer, such as the one supplied by SysInternals (http://technet.microsoft.com/en-us/sysinternals/bb896647.aspx). Download this and run it (there's no need to install it) on the server, then restart IIS. If you don't see any messages relating to the Swivel IIS filter, then it's not installed properly.

If the page is still not redirected, try the following:

1. Check which application pool your web application is running as, then go to the properties page for that application pool.

2. On the Identity tab, change the user to ?Local System?. You will be warned that this is a potential security risk, but don?t worry ? it won?t be left like this.

3. Restart IIS.

4. Try accessing a protected page again. Hopefully this time you will be redirected.

5. You can now go back to the application pool and change the identity back to what it was originally: it would appear that it is only necessary to run as an administrator to get the filter to register initially.

If you do not see a Turing image when using start session then in a web browser test the following link from the IIS server. If an image is not seen, then there is a problem either with communicating with the Swivel server or the Allow Image request by username may be set to No.

For a virtual or hardware appliance Install

https://<pinsafe_server_ip>:8443/proxy/SCImage?username=<username>

For a software only install see Software Only Installation

If the web page is redirected to the /PINsafe/login.asp page but an error message appears then ensure that the Active Server Pages are allowed. To verify this select the Internet Information Services Manager expand the required server then click on Web Service Extension.

No authentication on main page

Open IIS Manager and disable Anonymous authentication for the root folder. Refresh the browser to prevent caching and try again.

You may need to ensure that Anonymous authentication is enabled for the PINsafe folder, though, so you don't run into problems showing the TURing image.

Authentication working internally but not externally

If it is working internally, but not externally, ensure that there is no caching by openine a new browser. Also specify the default redirect URL as "/default.htm", rather than "./default.htm". The latter will redirect to default.htm within the pinsafe folder.

116.9.1 Error Messages

AgentXML request failed, error: The agent is not authorised to access the server

User fails to authenticate with the above error message in the Swivel log. An Agent on Swivel server has not been defined for the IIS server. Go to Server/Agents in the Swivel admin console, and add a new entry, using the IP address of the IIS server. Make sure the agent secret is the same as on the IIS filter configuration.

This installation package is not supported on this processor type. Contact your product vendor

117 Microsoft ISA 2006 Cluster Integration

117.1 ISA 2006 Cluster Integration

117.2 Overview

In an ISA cluster, the Swivel filter needs to be registered with the cluster on the storage server and on each member of the cluster.

If all the ISA Servers are installed on 32-bit operating systems, then you can use version 1.2 of the PINsafe ISA filter, which manages filter registration as part of the login process. You must install on the configuration storage server first, and then on each member server. See the standard ISA filter integration guide (link below) for further instructions.

If you are running ISA Server on a 64-bit operating system, the reference above will not work. Instead, you will have to use the older 64-bit version together with installation scripts.

Refer to the ISA 2006 integration guide for additional steps, for both versions of the filter. Microsoft_ISA_2006_Integration

117.3 Prerequisites

These are required in addition to the ISA 2006 Integration prerequisites

- RegisterFilter.vbs
- RegisterFilterMember.vbs

These files can be downloaded from here: File:PINsafe_ISA_2006_Cluster_Registration.zip

117.4 ISA 2006 Cluster Installation Steps

117.4.1 Install the PINsafe filter

Run the setup.exe file on each of the ISA servers ignoring errors relating to registration of the PINsafeISAFIlter

117.4.2 Ensure the PINsafe Filter is on each ISA server

Ensure that the PINsafeISAFilter.dll is installed on C:\Program Files\Microsoft ISA Server on all ISA servers.

117.4.3 ISA Cluster Storage Server Filter Registration

On the configuration storage server copy RegisterFilter.vbs to C:\Program Files\Microsoft ISA Server and run it.

You may have to run it from the command prompt, specifying the fully-qualified name of the configuration storage server, if that is not the server you are running it from.

117.4.4 ISA Cluster Member Filter Registration

Copy RegisterFilterMember.vbs to C:\Program Files\Microsoft ISA Server on each member server, and run. Once you have done this, check that it appears in the list of web filters for the server.

when manually registering a web filter .dll, from the command prompt you need to be in the SAME directory as the .DLL, otherwise you will get an error:

Error: The Web Filter referenced by Server xxxxxx does not exist The error occurred on object ?xxxxxx? of class ?Server? in the scope of array ?Learning-ISA?

117.4.5 Configure the ISA Filter

Configure the ISA filter using the configuration tool provided. Each ISA server in the cluster will need to be configured. To start is select Start/Programs/PINsafe ISA Filter/Configuration.

118 Microsoft ISA 2006 Integration

119 Microsoft Internet Security and Acceleration Server (ISA) Integration Notes

120 Introduction

This document outlines the necessary steps to integrate Swivel authentication into either Outlook Web Access (OWA) 2003 or Sharepoint Forms-based Authentication (FBA) provided with Microsoft ISA Server 2006. Additionally the login page can be further customised, for further information see: Microsoft ISA 2006 web page customisation How to Guide. If the ISA server is part of a cluster then the filter needs to be installed on each cluster, the 32 bit installer handles cluster registration, for further information and manual registration see Microsoft ISA 2006 Cluster Integration

Note that with the release of version 1.2 of the Swivel ISA filter, filter registration is part of the configuration process. See below for more information. This also means that the same installer can be used for Enterprise and Standard ISA Server. Unfortunately, version 1.2 supports 32-bit operating systems only. However, there is a 64-bit version for Microsoft Forefront Threat Management Gateway. The documentation for this is now available from a separate page here.

121 Prerequisites

This installation guide assumes that publication of the relevant service has already been configured in ISA Server, following the relevant instructions. In addition a working Swivel server version 3.1 or later is required.

If the option to check a user is a Swivel user and issue a OTC field is to be used, this requires Swivel 3.4 or later.

The Swivel Configuration utility requires .Net version 2 or higher. This is not supplied above and must be downloaded and installed if you do not already have it.

The ISA server and its configuration should be fully backed up prior to the Swivel integration.

Allow around 1 hour downtime per ISA server for the integration, and the integration will require a restart of the ISA Firewall Services.

121.1 ISA 2006 Filter

The installer can be downloaded from here.

121.2 TMG Filter

The TMG version can be found here. NOTE: this is version 1.4.0 of the TMG filter, released 23/8/12, which includes a number of enhancements over previous versions. See the included documentation.

122 Baseline

Swivel 3.4 or later (3.6 or later preferred)

Microsoft ISA Server 2006 or Microsoft Forefront TMG

Web-based server, typically Microsoft IIS-based, to be protected, such as OWA or SharePoint.

123 Architecture

The ISA server makes authentication requests against the Swivel server by XML or RADIUS. Some of the additional features are only available in the XML authentication. For security reasons Sharepoint authentication should be configured using RADIUS. The Swivel installation creates a separate custom login.

The default install path for the standard OWA login page is:

C:\Program Files\Microsoft ISA Server\CookieAuthTemplates\Exchange\HTML

The standard install path for PINsafe OWA authentication page is:

C:\Program Files\Microsoft ISA Server\CookieAuthTemplates\PINsafeOWA\HTML

124 Swivel Configuration

124.1 Configure a Swivel Agent For XML Authentication

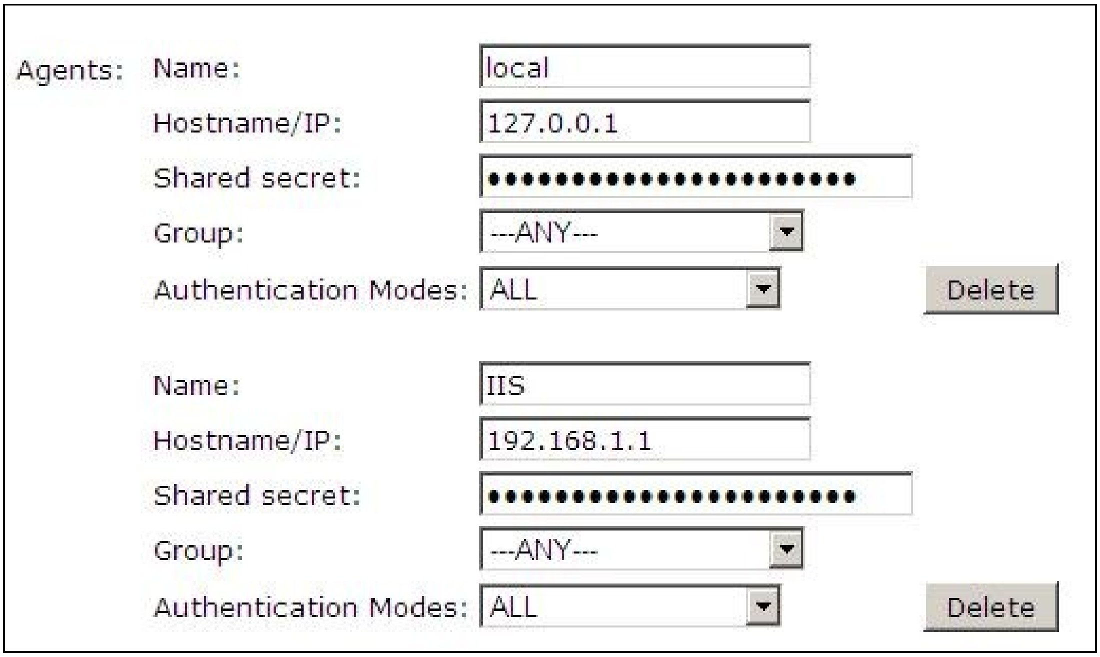
1. On the Swivel Management Console select Server/Agent

2. Enter a name for the Agent

3. Enter the ISA internal IP address

4. Enter the shared secret

5. Click on Apply to save changes



Agents:

Name: local

Hostname/IP: 127.0.0.1

Shared secret: ••••••••••••••••••••••

Group: ---ANY---

Authentication Modes: ALL

Name: IIS

Hostname/IP: 192.168.1.1

Shared secret: •••••••••••••••••••••••

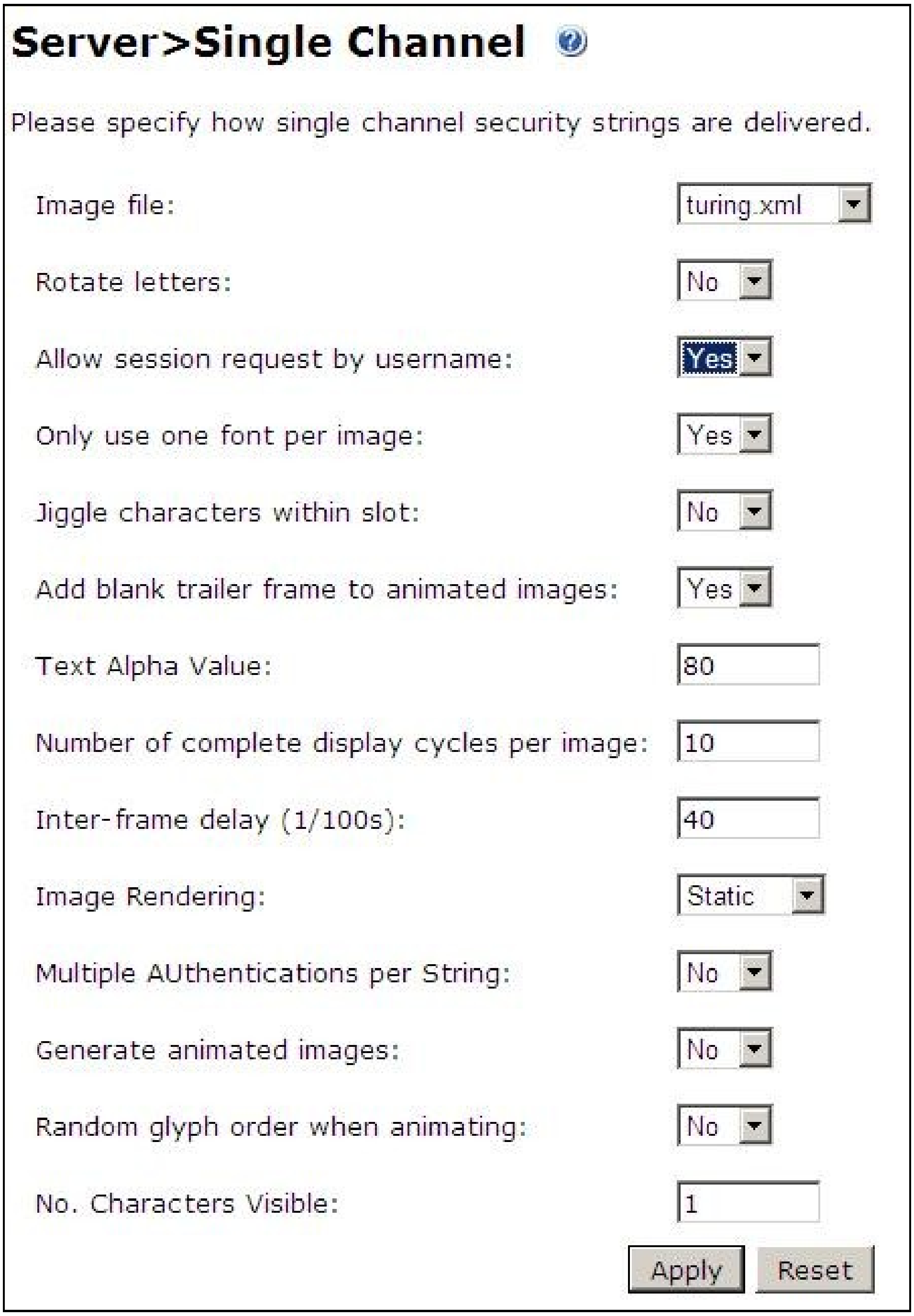
Group: ---ANY---

Authentication Modes: ALL

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

124.3 Configure a RADIUS NAS entry for Sharepoint authentication

NOTE: this is only required if you wish to use RADIUS authentication with Swivel. This is recommended for SharePoint integration and optional for other solutions.

1. Ensure the RADIUS server is running on Swivel

2. On the Swivel Management Console select RADIUS NAS

3. Enter a name for the NAS

4. Enter the ISA internal IP address

5. Enter the shared secret

6. Click on Apply to save changes

125 ISA Installation

The following steps should be carried out on the ISA server. No configuration changes need to be performed on the Exchange server or Sharepoint server. For Additional Sharepoint configuration see the Special Considerations for Sharepoint below.

125.1 Publish OWA or Sharepoint

Publish Outlook Web Access, Sharepoint or your website as described in the ISA Server documentation, if you have not already done so. Ensure that they are working as expected.

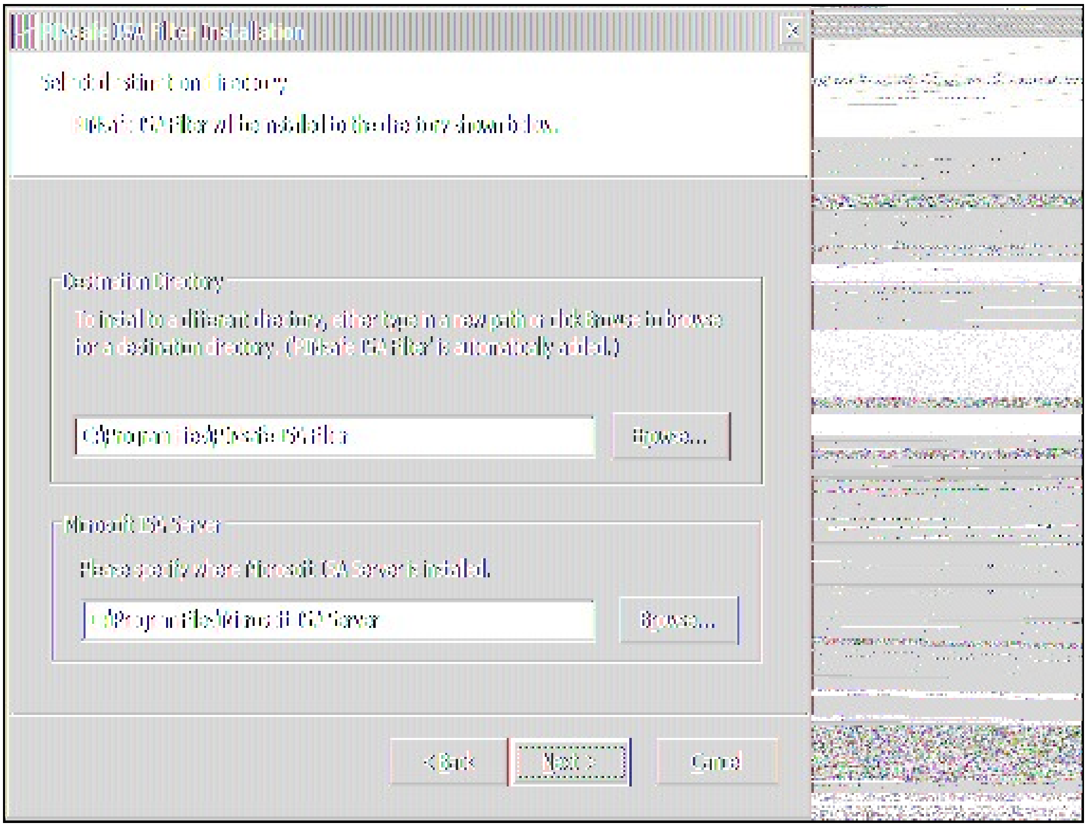
125.1.1 Configure ISA firewall rules

Create an access rule permitting HTTP access from the ISA Server to the correct port (commonly 8080) on the Swivel server. To do this, you will need to create a new protocol for outbound TCP on the appropriate port.

125.1.2 Install the ISA server software

NOTE: if you are installing in an Enterprise environment, you should always install on the Configuration Storage server first, and then on each array member. Be aware that the firewall service on member servers will stop when they try to synchronise with the configuration storage server, if that has the Swivel filter installed and the member does not. Once the filter is installed on the member server, you will be able to restart the firewall service.

Run PINsafeISAFilter.exe to install the filter DLL. You will be prompted for the location in which to install the filter configuration, and also for the location of Microsoft ISA Server, usually C:\Program Files\Microsoft ISA Server.



PINsafe ISA Filter Installation

Select Installation Directory

PINsafe ISA Filter will be installed to the directory shown below.

Destination Directory

To install to a different directory, either type in a new path or click Browse to browse for a destination directory. ('PINsafe ISA Filter' is automatically added.)

C:\Program Files\PINsafe ISA Filter

Microsoft ISA Server

Please specify where Microsoft ISA Server is installed.

C:\Program Files\Microsoft ISA Server

Note that the installation process will include installation of Microsoft Visual C++ 2010 runtime libraries, if they are not already installed.

125.2 Register the ISA Filter

When installation is complete, you have the option to run the configuration program. Assuming you elect to do so, you will first be prompted to register the filter with Swivel. You have a choice of registration types:

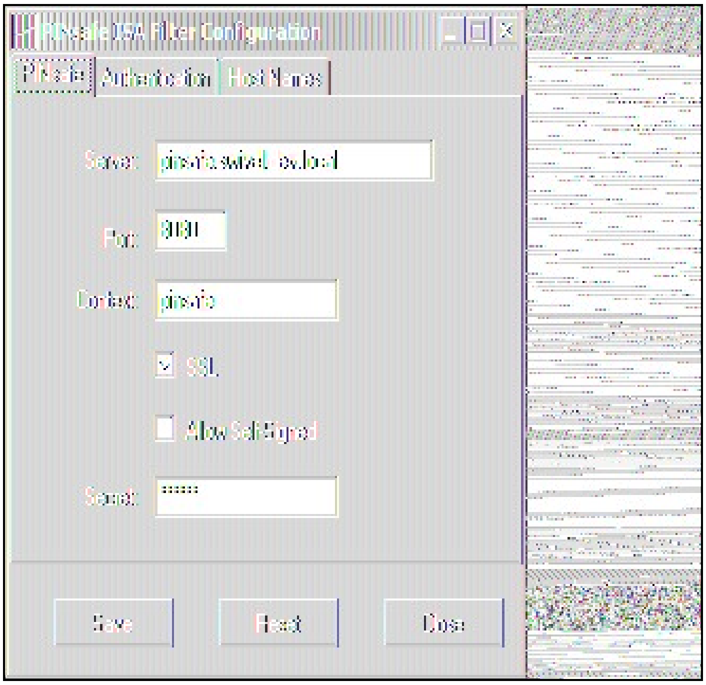
[[Image: Register_Filter.PNG]]

Select the right option for your requirements. The last option is required if you are installing on the Configuration Storage server and the same server is also a member of the ISA server array.

125.2.1 Configure the ISA server

Configure the ISA filter using the configuration tool provided. This will optionally run immediately after installation. To start subsequently, select Start/Programs/PINsafe ISA Filter/Configuration.

PINsafe configuration tab:



PINsafe ISA Filter Configuration

Server: pinsafe.swivel.dev.local

Port: 8080

Context: pinsafe

☑ SSL

☐ Allow Self Signed

Secret: ******

Server: is the name or IP address of the Swivel server (Hint: Use hostname to avoid problems with SSL certificates)

Port: is the port on which Tomcat is running. PINsafe virtual or hardware appliances require the use of XML authentication on port 8080 and the 8443 proxy port should not be used when integrating with ISA. (Hint: Use port 8080)

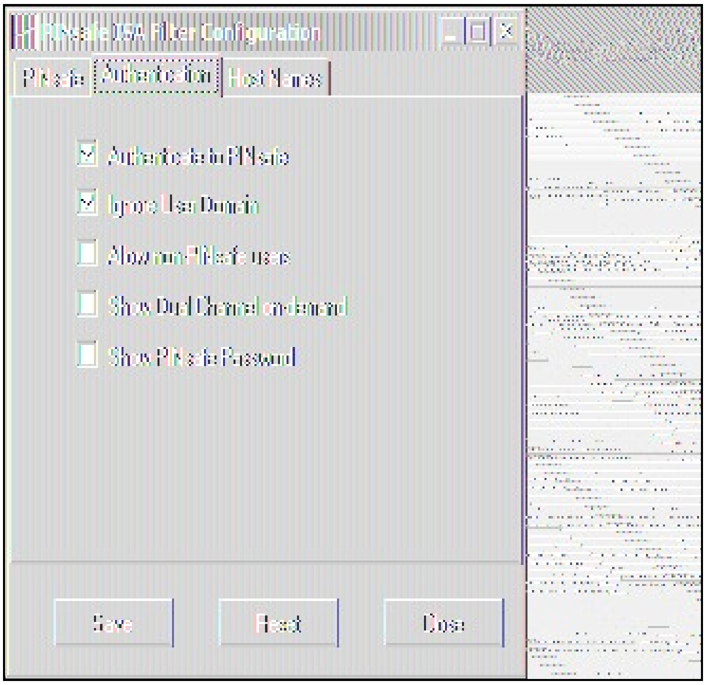
Context: is the name of the Swivel web application, usually ?pinsafe?. Note when using a Swivel virtual or hardware appliance where the proxy port is available, the path pinsafe using port 8080 should still be used, the ISA proxy provides security.

SSL: will, if checked, send requests to the Swivel server using https, rather than http.

Allow self-signed: when checked, causes SSL certificate errors from the PINsafe server to be ignored.

Secret: is the shared secret for the Swivel agent for the ISA Server, and needs to be the same as that on the Swivel server. After you enter this value, you will be prompted to enter it again, to confirm that it is correct.

Authentication configuration tab:



☑ Authenticate to PINsafe

☑ Ignore User Domain

□ Allow non-PINsafe users

□ Show Dual Channel on demand

□ Show PINsafe Password

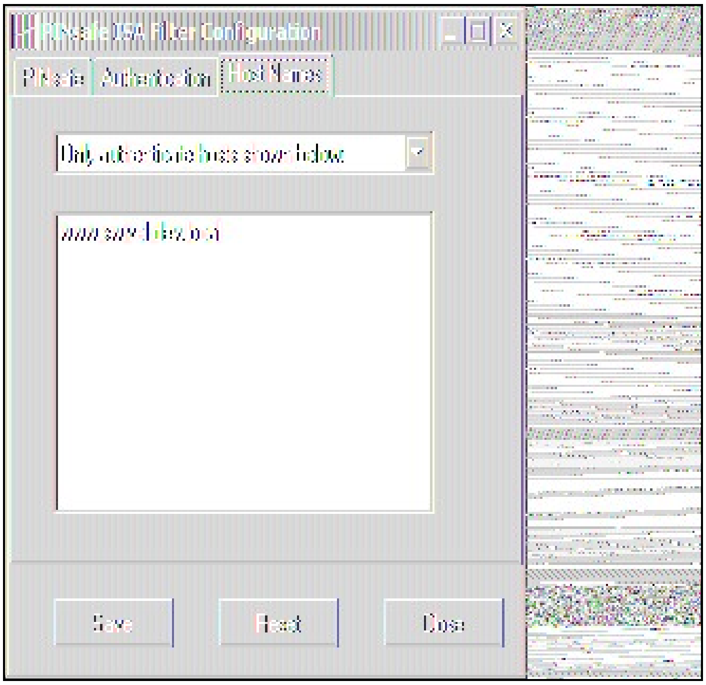
Authenticate to PINsafe: should be checked to use standard Swivel authentication. You should uncheck this if you are using the ISA filter to protect a Sharepoint website, as described in the ?Special Considerations for Sharepoint? section below. If you uncheck it, Swivel will not directly authenticate the login request. In this case, you should enable RADIUS authentication instead.

Ignore user domain: This will remove the AD domain of users, and when Swivel is using the SAM account name it should normally be checked, in this case, if you enter ?domain\user? as the logon username, only ?user? will be sent to Swivel. If it is not checked the full name will be sent to Active Directory and should be used when Swivel uses the User Principle Name.

Allow non-PINsafe users: when checked, users not known to Swivel may authenticate using only their AD credentials. This feature is useful for transition to Swivel, where not all users have Swivel accounts. If checked, the OTC field is not shown initially, only when the username is checked and found to exist in Swivel. Note that this feature is not compatible with RADIUS authentication.

The last two options on this tab should not be used - they do not work, and are there for future enhancement.

Hosts configuration tab:



Only authenticate hosts shown below

www.swiveldev.local

This feature is new to version 1.2. Previously, when installed, the PINsafe ISA filter would affect all authentication requests through the ISA Server. This option allows you to apply PINsafe authentication per host name. It can either be configured to authenticate all host names except those specified, or to authenticate only those hosts specified, and to ignore all others.

125.3 Confirm that the filter has been registered correctly

Once completed the filter will appear in the ISA Server Management Web Filters section. If the filter does not appear in the list of available filters check the Windows system event log for errors. The 32 bit installer handles cluster registration, for further information and manual registration see Microsoft_ISA_2006_Cluster_Integration

125.4 Modify the Listener

Modify the Listener used to publish OWA or Sharepoint as follows: On the relevant firewall rule, right-click and select properties, select Listener, then click Properties. On the Forms tab, tick the check box labelled ?Use customized HTML forms instead of the default?. For the form set directory, type:

?PINsafeOWA? for Outlook Web Access

and ?PINsafeWeb? or ?PINsafeRadius? for Sharepoint or other websites (?PINsafeISA? for TMG).

You should always use PINsafeRadius for Sharepoint, for reasons described below. You may use either set of forms for standard websites. Note that the TMG filter does not require a different set of custom pages for RADIUS.

Modify the properties for the relevant policy rule.

Then select Apply, and click Ok. Then select the Application Settings tab and UNCHECK the option to use customized HTML. Note that if you have customized your original OWA or Sharepoint login pages, you will need to apply the same customisation to the new Swivel pages. Please consult Swivel support for details of this.

Once you have configured everything, restart the Microsoft Firewall Service on the ISA server. It can take a long time to restart this service, and if you are connecting to the ISA Server via remote desktop, you may be temporarily disconnected from it.

126 SSL Certificate Considerations

There would appear to be an issue with a recent security update for ISA Server which prevents HTTP POST requests over SSL unless the target server certificate is fully trusted. This has consequences for the PINsafe ISA Server integration.

If you are not using SSL on your Swivel server, this issue will not affect you.

If you are using SSL, you must have a valid certificate on the Swivel server. This means:

- The certificate date must be current (i.e. not expired)
- The certificate must be issued by a trusted CA (see below for ways of managing this)
- The certificate subject must match the host name used by the ISA Server to connect to the Swivel server. In particular, this means that you must reference the Swivel server by name, not by IP address.

One way to manage this is to get a commercial certificate for the Swivel server. However, this costs money, and if your PINsafe server is not internet facing, is not necessary. A second option is if you have an internal certificate authority, you can use that to issue a certificate for the Swivel server (Windows Servers, for example, can optionally be configured as certificate authorities). If you do this, you need to make sure that the certificate authority server certificate is added to the trusted root certificates on the ISA Server, if it is not already. The third option is simply to generate a self-signed certificate on the Swivel server, with the correct host name, and to install that directly into the ISA Server trusted root store (see below).

For more detail, refer to the relevant knowledgebase documentation on generating SSL certificates if you are using a Swivel virtual or hardware appliance. Otherwise, refer to the relevant documentation for your operating system.

126.1 Installing a Self Signed Certificate into the ISA trusted root store

If you want to do is to trust the Swivel server certificate the following steps may be carried out:

1. Copy /home/swivel/.keystore to a suitable machine (it doesn?t have to be the ISA server).

2. Open the file in Keystore Explorer.

3. Right-click on the certificate (if there is more than one, it will probably be called ?swivel?). Select ?Export?, then ?Export key pair?.

4. Enter a password for the exported certificate. I recommend using ?lockbox?, but anything will do.

5. Select the export path. It doesn?t actually matter what the extension is.

6. Copy the exported certificate to the ISA Server. The remaining commands are done on the ISA Server.

7. Open ?mmc? from the Run dialog.

8. Select File -> Add/Remove Snap-in.

9. From the dialog, select ?Certificates? and click ?Add?.

10. Select ?Computer account?, then ?Local computer?.

11. Click OK.

12. Go to Certificates -> -> Trusted Root Certificate Authorities.

13. Right-click, then ?All Tasks?, ?Import?.

14. Select the exported certificate. You will need to enter the password. We recommend marking the key as exportable. Make sure the certificate is imported into the -> Trusted Root Certificate Authorities.

15. If you look under Certificates -> Personal -> Certificates, you should see the new certificate.

16. You may need to restart the Microsoft Firewall service before it shows the new certificate.

127 Special Considerations for Sharepoint

A security hole has been discovered when using earlier versions of the ISA filter for Sharepoint authentication. It was possible to open a Sharepoint document from within Word (for example) and only provide the standard Active Directory credentials.

The new solution avoids this problem by using RADIUS to authenticate to Swivel, rather than using the ISA filter directly. One minor inconvenience with this is that users must authenticate through the Sharepoint web page before they can access any documents.

Note that if you disable Swivel authentication for Sharepoint, it is also disabled for all other websites. Therefore, if you want to use Swivel authentication on multiple websites for a single ISA Server, they must all use the standard Swivel authentication, or all use RADIUS.

1. On the ISA filter configuration application, uncheck the Authenticate option. This means that Swivel will not authenticate the logon request directly. Instead, you should use RADIUS to perform Swivel authentication, as described below.

2. On the Authentication tab you should check the option ?Collect additional credentials in the form?. This will require you to select ?RADIUS OTP? as the authentication validation method. Click the ?Configure Validation Servers? button, and add the Swivel server as a RADIUS server. Make a note of the shared secret you set for the server.

3. In order for users to be able to open documents from other, non-browser applications once they have authenticated, you must enable persistent cookies. On the Forms tab, click the Advanced button. It is recommended that you select persistent cookies for private computers only. This means that users on public computers will have to open documents from the Sharepoint web site.

4. On the ISA server, create a rule to allow RADIUS authentication from the ISA server to the Swivel server

5. On the Swivel server, enable the RADIUS server (on the RADIUS > Server page). On the RADIUS > NAS page, add the ISA Server as a new NAS, and enter the shared secret you set on the ISA Server. If you wish to restrict access to a particular group of users, select that group, otherwise leave the Group drop-down as ?ANY?.

6. On the policy rule, on the Authentication Delegation tab, select ?NTLM Authentication?.

Once you have configured everything, reboot the ISA server.

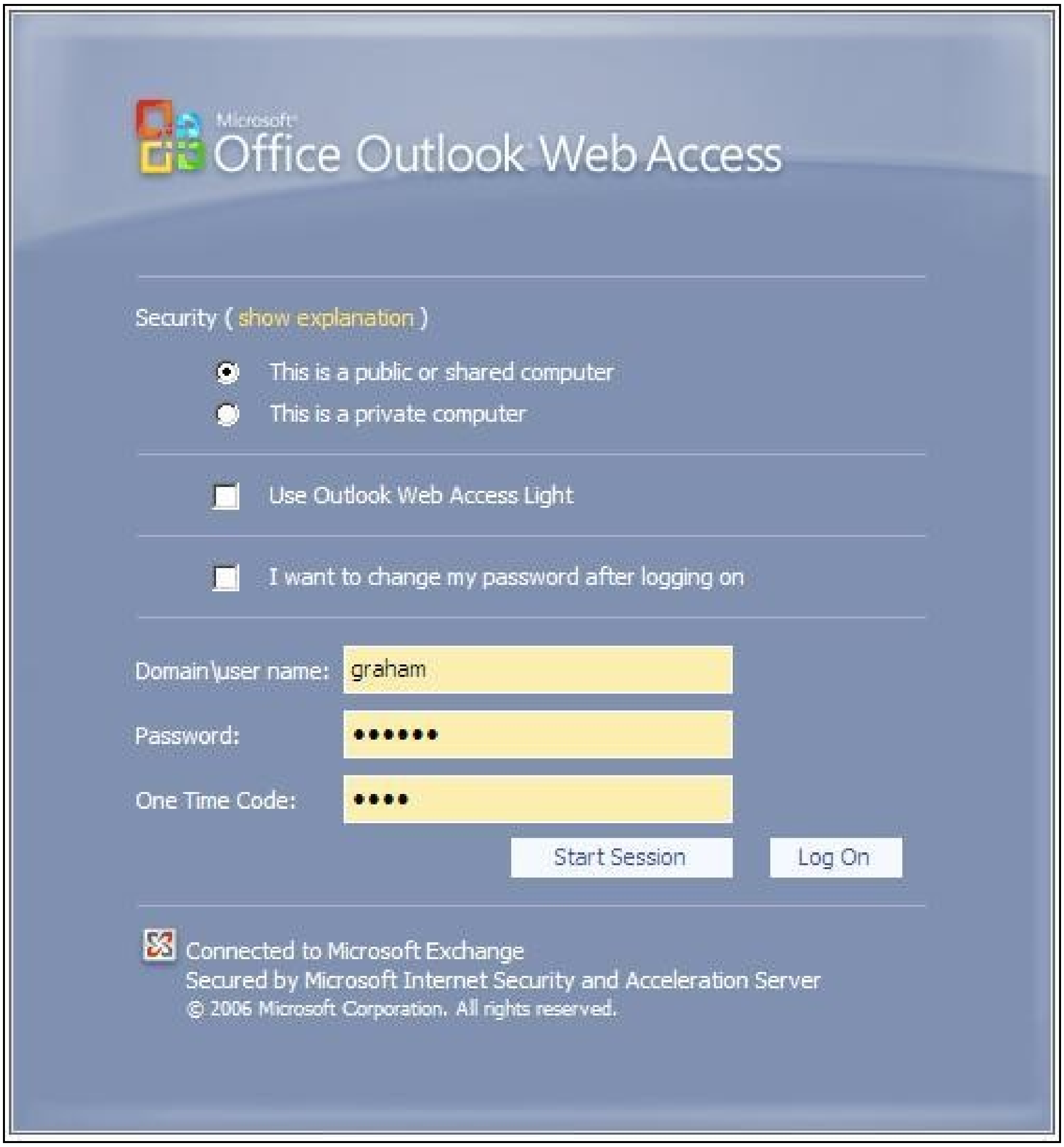
128 Verifying Installation

128.1 Outlook Web Access

Navigate to the URL on which ISA Server publishes OWA. The customisation is visible in the addition of a One Time Code field and a Start Session button. Attempting to login with a correct username and password but no one time code should result in failure. Only when a correct Swivel one time code is entered in addition to the Exchange or Sharepoint credentials should the user be logged into OWA.

Note that if a username is entered in the form Domain\username, the Domain\ portion of the username will be stripped before being passed to the Swivel server. This permits the use of sAMAccountName as the username attribute for synchronisation between Swivel and Active Directory.

Dual Channel Login



Microsoft Office Outlook Web Access

Security (show explanation)

● This is a public or shared computer

○ This is a private computer

□ Use Outlook Web Access Light

□ I want to change my password after logging on

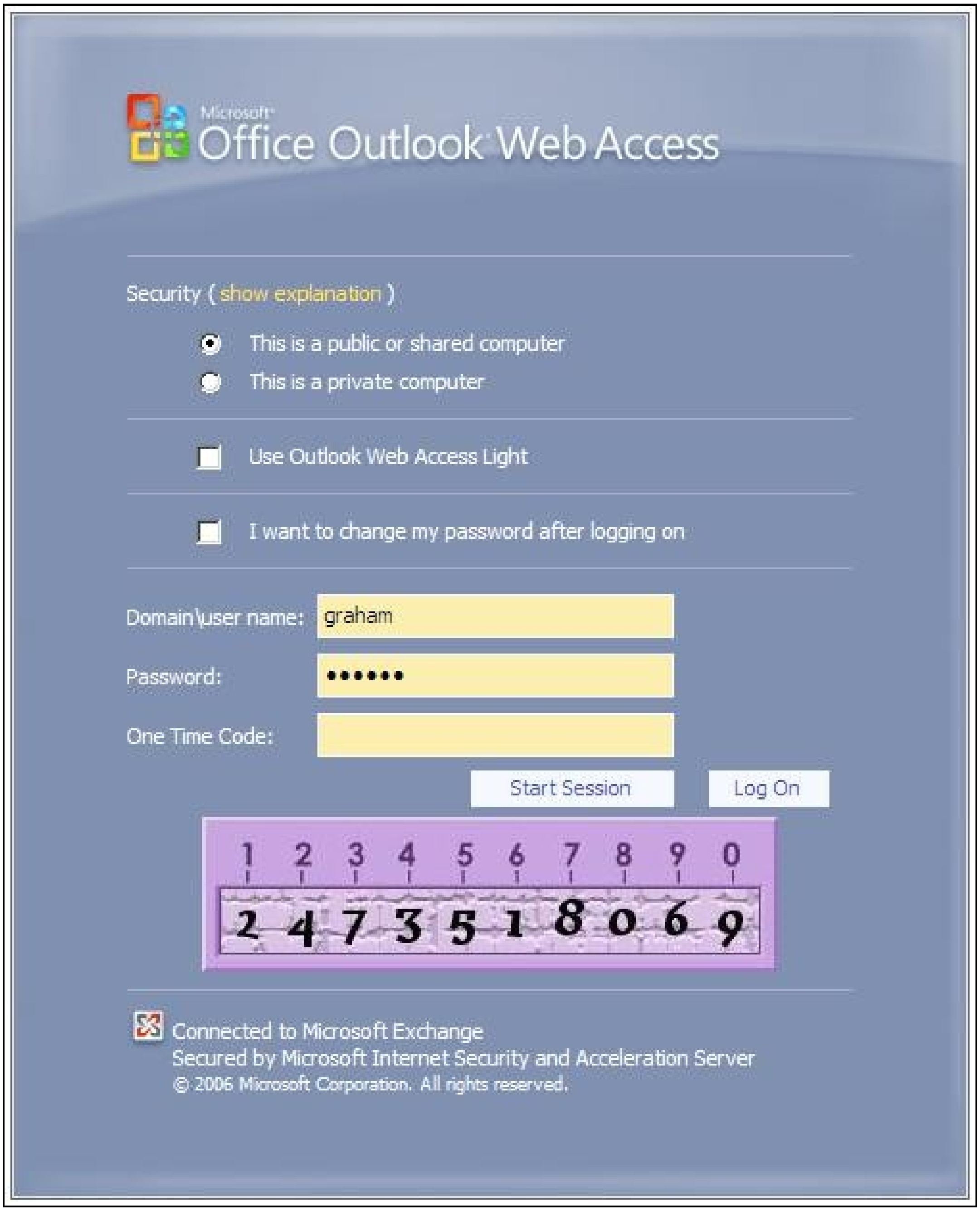
Domain\user name: graham

Password: ••••••

One Time Code: ••••

Connected to Microsoft Exchange
Secured by Microsoft Internet Security and Acceleration Server
© 2006 Microsoft Corporation. All rights reserved.

Single Channel Login



Security (show explanation)

● This is a public or shared computer
○ This is a private computer

□ Use Outlook Web Access Light

□ I want to change my password after logging on

Domain\user name: graham
Password: ••••••
One Time Code:

1	2	3	4	5	6	7	8	9	0
2	4	7	3	5	1	8	0	6	9

Connected to Microsoft Exchange
Secured by Microsoft Internet Security and Acceleration Server
© 2006 Microsoft Corporation. All rights reserved.

128.2 Sharepoint

Navigate to the URL on which ISA Server publishes Sharepoint. You will notice that there are two sets of credentials to enter. The Swivel credentials are entered in the top part, and the Active Directory credentials in the lower part. Enter the username in the first box as domain\user. Click the Start Session button to get a TURing image. Enter the Swivel password and one-time code in the next two boxes. (NOTE: the Swivel password and one-time code are actually concatenated and submitted as a single value. You can, if you prefer, enter them that way in the Passcode field ? password first).

In the final box, enter your Active Directory password, and click submit.

(NOTE: you actually have to enter different usernames for Swivel and Active Directory ? with the domain prefix for AD and without for Swivel. However, this is handled automatically for you. You will notice, if you fail login, that the Swivel username has changed, and the AD username has been inserted in the lower set of credentials.)

129 Additional Options

129.1 RADIUS Authentication

Set the Swivel server as the RADIUS server (and add the ISA Server as a NAS on Swivel). If you want to use the TURing image, then the Swivel ISA filter is required, but disable authentication in the filter configuration. PINsafeRADIUS custom login pages provided with the filter can be used.

129.2 Turning off Automated Security Strings

When a user enters their username and then their AD password, they will usually generate a single channel TURing image or for Dual channel On Demand authentication, automatically send an SMS message. This option is for the the integration using the OWA filter and will stop the automated display of single channel TURing images and the automated sending of SMS security strings.

The automation can be disabled by disabled by editing C:\Program Files\Microsoft ISA Server\CookieAuthTemplates\PINsafe\OWA\HTML\usr_pwd.htm (Exact path may vary depending upon installation).

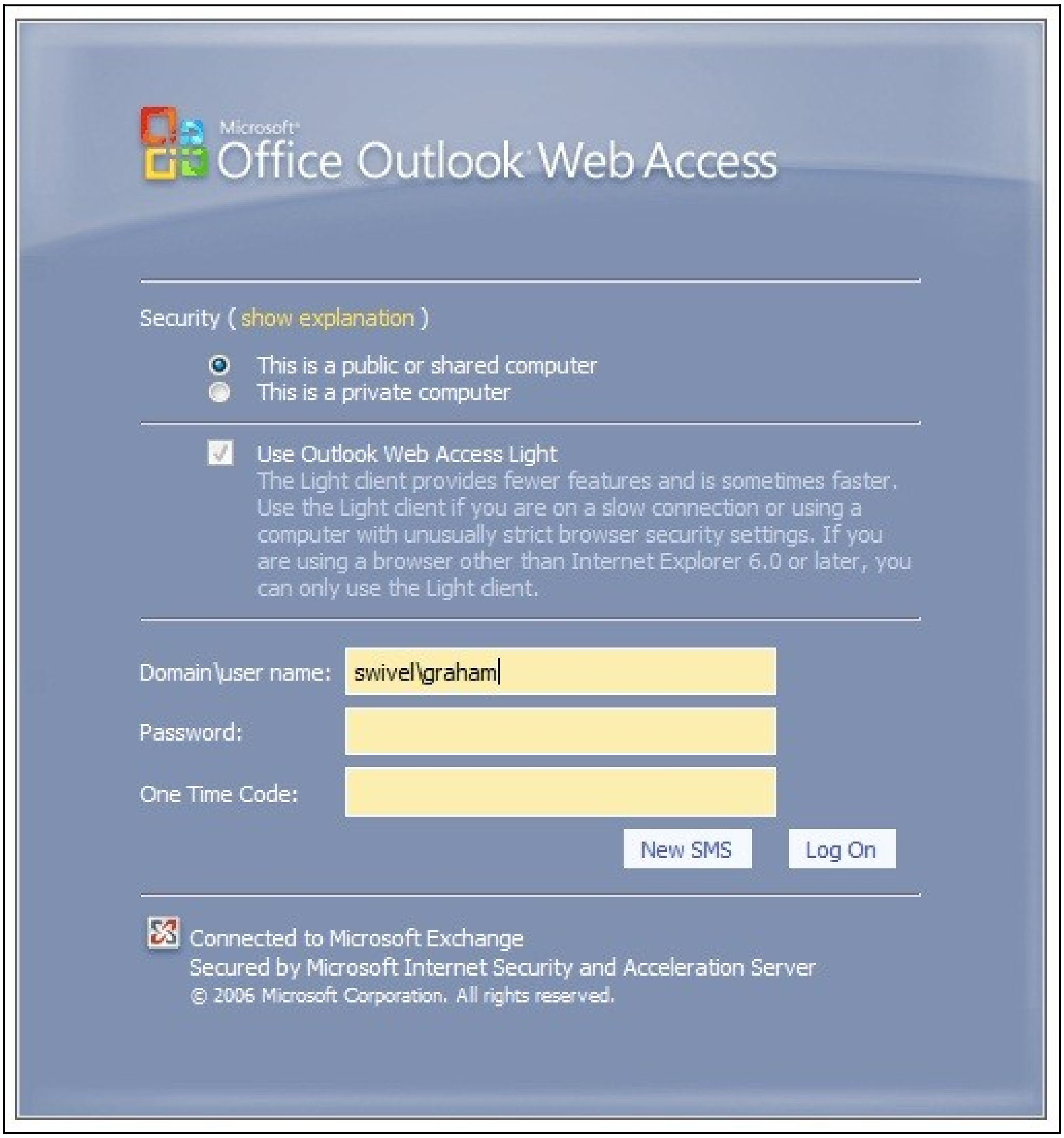
First Make a backup copy of the file

Edit the file in a text editor

Locate the setUserExists function

below this locate and remove the entire line ShowTuring();

Modified login page showing SMS on request



Security (show explanation)

● This is a public or shared computer
○ This is a private computer

☑ Use Outlook Web Access Light
The Light client provides fewer features and is sometimes faster. Use the Light client if you are on a slow connection or using a computer with unusually strict browser security settings. If you are using a browser other than Internet Explorer 6.0 or later, you can only use the Light client.

Domain\user name: swivel\graham

Password:

One Time Code:

Connected to Microsoft Exchange
Secured by Microsoft Internet Security and Acceleration Server
© 2006 Microsoft Corporation. All rights reserved.

129.3 Editing the Security String Request Buttons

The message request buttons can be edited to display different messages.

The default International English language version is located in the the following file:

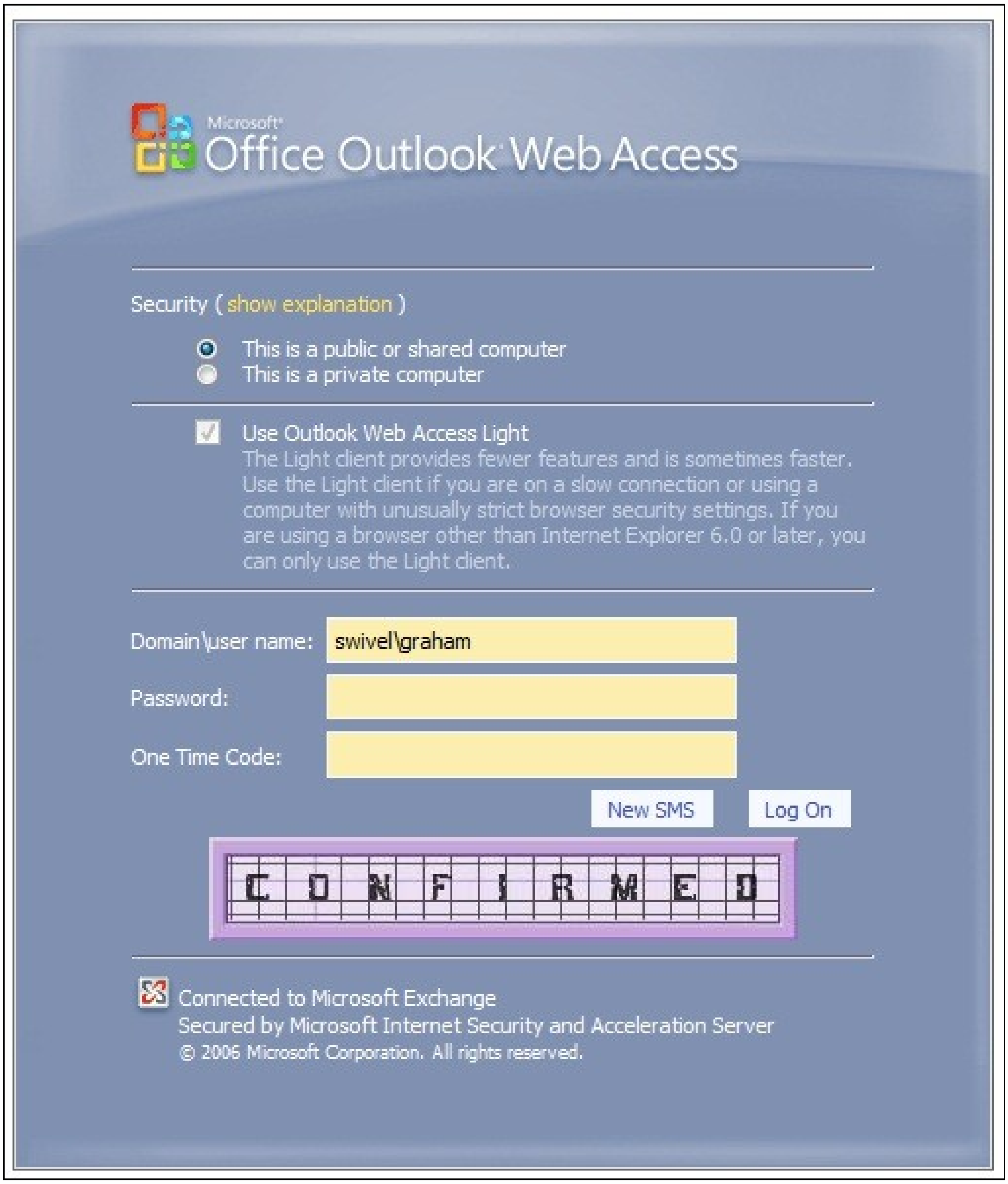
C:\Program Files\Microsoft ISA Server\CookieAuthTemplates\PINsafeOWA\HTML\nls\en\strings.txt (Path may vary with installation, and different language files may also be edited)

First Make a backup copy of the file

Edit the file in a text editor

Find the line L_StartSession_Text="Get Image" (May also be L_StartSession_Text="Start Session" or L_StartSession_Text="Refresh Image")

Modified login page



Security (show explanation)

● This is a public or shared computer
○ This is a private computer

☑ Use Outlook Web Access Light
The Light client provides fewer features and is sometimes faster. Use the Light client if you are on a slow connection or using a computer with unusually strict browser security settings. If you are using a browser other than Internet Explorer 6.0 or later, you can only use the Light client.

Domain\user name: swivel\graham

Password:

One Time Code:

Connected to Microsoft Exchange
Secured by Microsoft Internet Security and Acceleration Server
© 2006 Microsoft Corporation. All rights reserved.

130 Uninstalling

130.1 Modify the Listener

Modify the Listener used to remove OWA or Sharepoint as follows: On the relevant firewall rule, right-click and select properties, select Listener, then click Properties. On the Forms tab, remove the tick the check box labelled ?Use customized HTML forms instead of the default?. For the form set directory, remove:

?PINsafeOWA? for Outlook Web Access

Modify the properties for the relevant policy rule.

Then select Apply, and click Ok. Then select the Application Settings tab and CHECK the option to use customized HTML.

Uninstall the Swivel software using the Remove Programs.

reboot the ISA server

131 Known Issues

132 Troubleshooting

NOTE: After any changes are made, always restart the Microsoft Firewall service

The Swivel authentication filter logs its activity to the standard Windows debug log. This can be accessed using a tool such Sysinternals DebugView available as freeware from:

Sysinternals DebugView

To include logging of output from the filter the option Capture Global Win32 must be enabled in the Capture menu.

With regard to the Single Channel TURing image, the ISA server login page does not use SCImage, the image request comes through the filter, so that the the Swivel server noes not need to be accessed directly from the internet. If the filter is not working, then no image will appear.

Single Channel image does not appear:

- Check Swivel ISA filter settings
- Check the Firewall service is started
- Check the ISA server logs for any error messages
- Use a fully qualified hostname instead of IP address for the Swivel server
- Is an SSL connection being used
- Is a self signed cert being used, if so try without SSL using http or install a valid public certificate
- Check the Swivel ISA filter is correctly installed. On the ISA Server Management: under Configuration, Add-ins for the server, "PINsafe Authentication Filter" should be enabled
- From the ISA server check a Single Channel image can be generated in a web browser connecting to the Swivel server using:

Swivel virtual or hardware appliance

https://<PINsafe server IP>:8080/pinsafe/SCImage?username=test

For a software only install see Software Only Installation

- If you see a red cross where the Single Channel Image should be right click on it and select properties. Copy the Address (URL) which should look something like: https://<ISA URL>/PINsafeISAFilter.dll?username=graham&random=197405. Copy this line and paste into the URL bar of the web browser and see if a Single Channel Image is generated.

If a user is able to login without the One Time Code, then the ISA filter may not be installed.

If IP addresses, rather than host names is used, with SSL enabled, you must check the option to "permit self-signed certificates". This option actually means to ignore all certificate errors, as you will get when referencing a server by the IP address, rather than the name.

The following error can be seen when trying to install the Swivel ISA Filter on an ISA cluster:

```
Error 1904. Module C:\Program Files\Microsoft ISA Server\PINsafeISAFIlter.dll failed to register. HRESULT -2147024891. Contact your support

For more information, see Help and Support Center at http://go.microsoft.com/fwlink/events.asp.

The "PINSafe Authentication Filter" then does not appear in the Web Filters tab.
```

See Microsoft ISA 2006 Cluster Integration

The ISA 2006 filter will not work with ISA 2004.

See also: troubleshooting OWA 2007 publishing rules on ISA Server 2006

133 Additional Information

133.1 Note on Activesync and RADIUS authentication

If you are using the same listener for ActiveSync etc, then don't use the RADIUS (or RADIUS OTP) option, as this will affect authentication for the other types as well. Since using the AgentXML approach only affects forms authentication, it shouldn't affect ActiveSync, which doesn't use FBA.

133.2 ISA and OWA

Information regarding the configuration of ISA Server to publish OWA or Sharepoint may be found in the ISA Server help under Firewall policy.

134 Microsoft ISA 2006 web page customisation How to Guide

134.1 Microsoft ISA 2006 web page customisation How to Guide

NOTE: if you need to be able to support pass-through support for non-PINsafe users, the following article is insufficient. The current recommendation is to start with the files provided with the PINsafe ISA filter, and to customise them as required. Please contact support@swivelsecure.com for more details. Use the following article only if you do not need support for non-PINsafe users.

134.2 Overview

This is a brief outline of how to go about customising your forms-based authentication web pages in ISA server to support PINsafe authentication. It is assumed that you are reasonably familiar with modifying HTML pages.

134.3 Web Page Customisation

134.3.1 Install the ISA filter

First of all, you should install the latest version of the PINsafe ISA filter for ISA Server 2006, see Microsoft_ISA_2006_Integration. This includes customised pages for Outlook Web Access (OWA) and for general web access (the documentation specifically references Sharepoint, but it will work for other web applications).

You should only need to use this document if you wish to customise these pages further, or if you already have customised authentication pages to which you wish to add PINsafe functionality.

134.3.2 Obtain the ISA login pages

If you have not already got a customised set of ISA login pages, the simplest way is to make a copy of the entire contents of C:\Program Files\Microsoft ISA Server\CookieAuthTemplates\ISA. This folder contains 3 sub-folders: HTML, cHTML and xHTML. The latter two are for mobile standards, which PINsafe does not currently support, principally because those standards do not support JPEG images, which is the format that TURing images are generated in, so only the HTML folder is of interest. The copy should be made into a folder under C:\Program Files\Microsoft ISA Server\CookieAuthTemplates. The name of the folder should correspond to the name you enter in the custom form name in the listener properties. Within this folder, 4 files potentially need to be modified: strings.txt, usr_pcode.htm, usr_pwd.htm and usr_pwd_pcode.htm. Additionally, if international support is required, other strings.txt files will need to be modified. These files are under the nls sub-folder, one for each language. Note that, for international characters to be displayed correctly, the strings.txt file must contain Unicode characters, so you will need to use a text editor that supports reading and saving Unicode files (e.g. NOT Notepad).

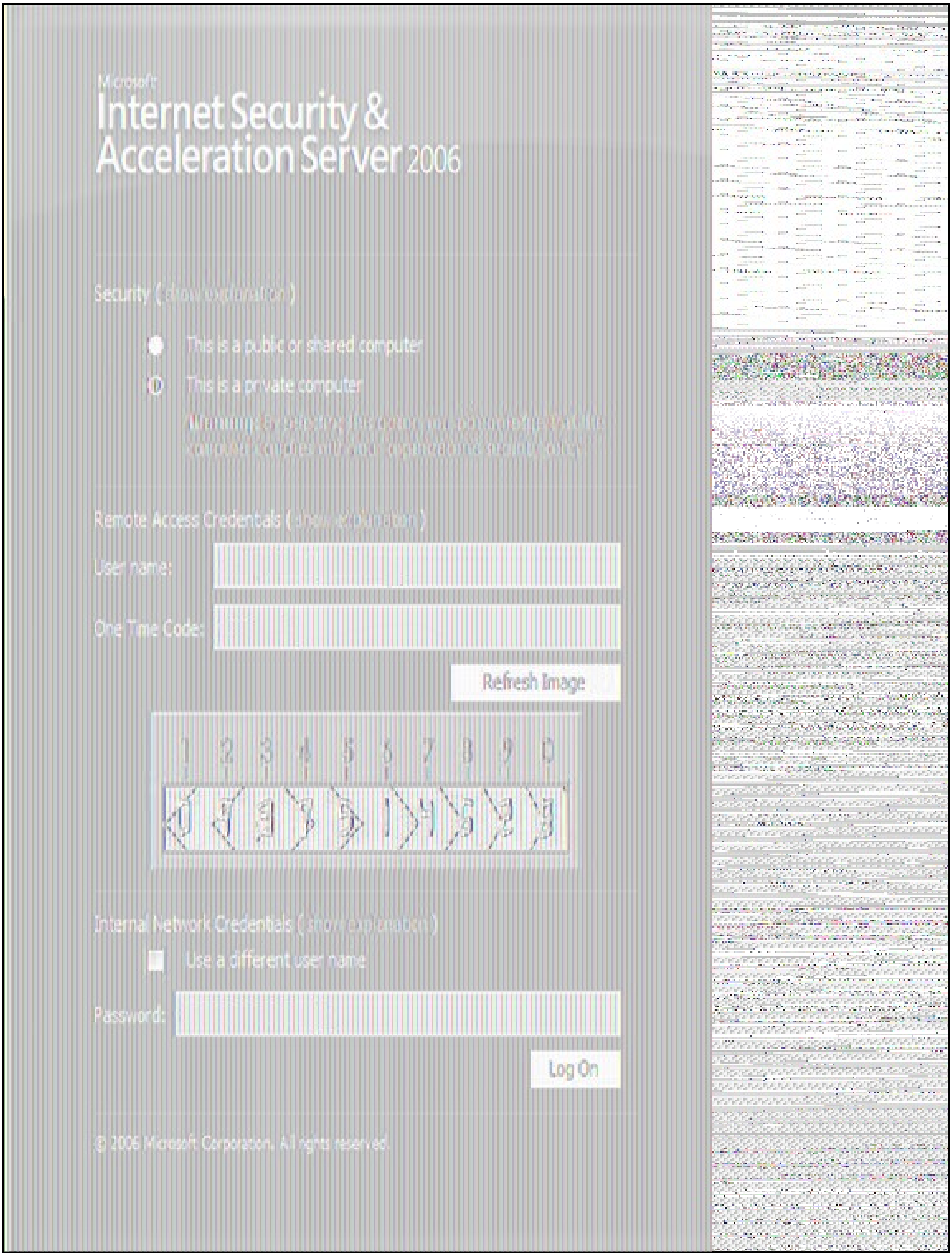
The strings.txt file supplied in the pinsafeWeb (or pinsafeOWA) folder of the PINsafe ISA filter installation should be sufficient for your needs, unless you have added other customised strings to your web pages.

Note also that if you have added custom images and/or stylesheets, you will need to include them in the new custom folder.

134.3.3 Customising the web pages

134.3.3.1 Change the Banner Logo

It is possible to change the logo displayed at the top of the login page. The page may look like this:



Microsoft®
Internet Security & Acceleration Server 2006

Security (show explanation)

● This is a public or shared computer

○ This is a private computer

Warning: By selecting this option, you confirm that this computer complies with your organization's security policy.

Remote Access Credentials (show explanation)

User name:

One Time Code:

Internal Network Credentials (show explanation)

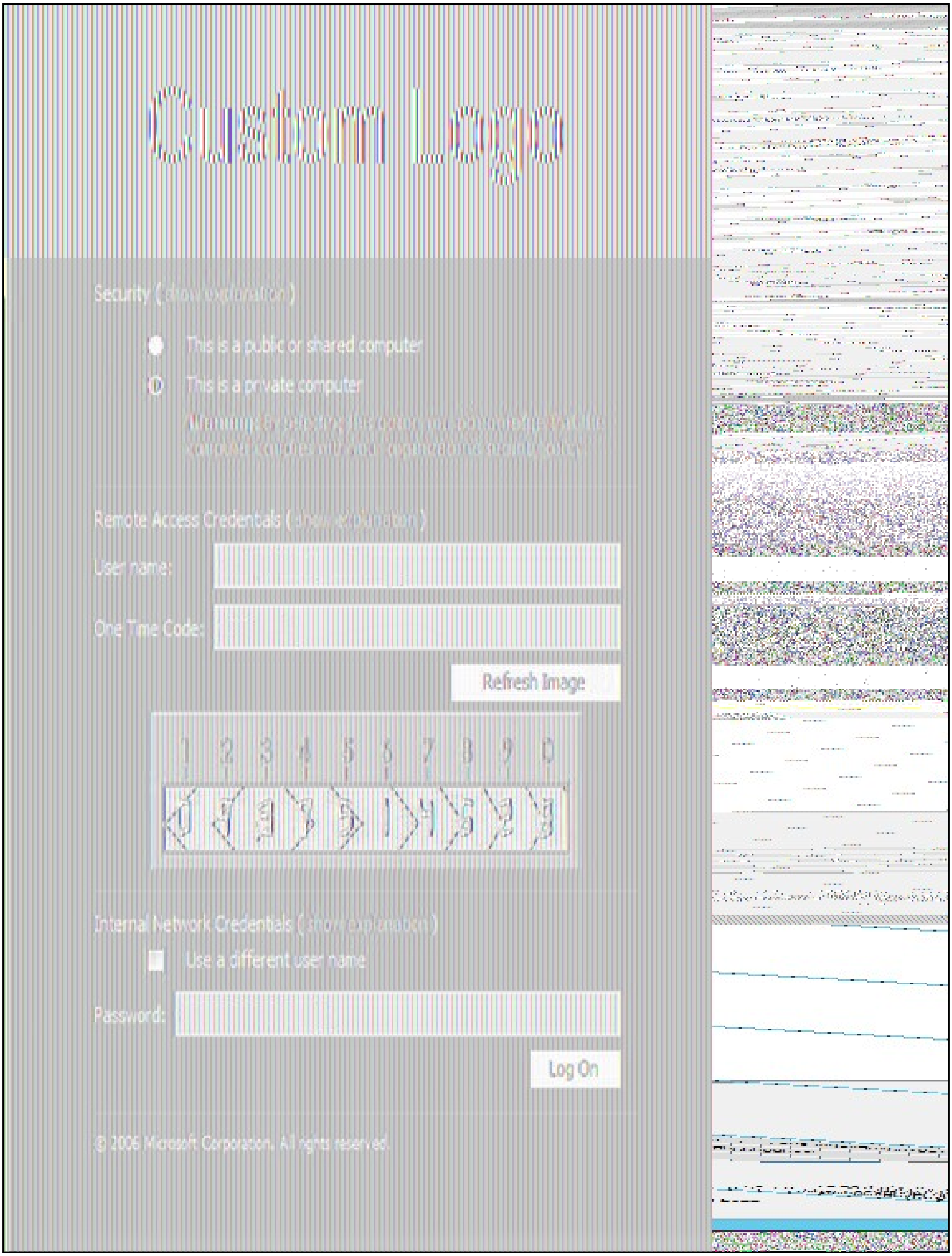
□ Use a different user name

Password:

© 2006 Microsoft Corporation. All rights reserved.

The image shown here at the top is in GIF format and is 500x115 pixels. On a 32-bit machine the picture can be found in "C:\Program Files\Microsoft ISA Server\CookieAuthTemplates\PINSafeOWA\HTML" - if the ISA server was installed to a non-standard location then this will not be the location. The file name of the logo is lgnTop.gif.

In order to update the picture for display you can simply substitute a new logo of exactly the same format and size then restart the ISA service to complete the installation of the new logo. This should then display the next time the page is accessed. The end result should look like this:



Custom Logo

Security (show explanation)

● This is a public or shared computer

○ This is a private computer

Warning: By selecting this option, you acknowledge that the computer complies with your organization's security policy.

Remote Access Credentials (show explanation)

User name:

One Time Code:

Refresh Image

Internal Network Credentials (show explanation)

□ Use a different user name

Password:

Log On

© 2006 Microsoft Corporation. All rights reserved.

134.3.3.1.1 Troubleshooting

If the page is requested by a refresh it is possible that the browser will display a cached version of the site. Clearing the cache within your browser may fix this.

If the logo is not of the same format (GIF) or of the same size (500x115pixels) then it may fail to display correctly.

If the name of the new image differs in case to the original then it may fail to load correctly.

When swapping the images it is recommended that you rename the old picture file and add the extension ".old". This will allow you to easily revert the image should the need arise.

134.3.3.2 Edit the strings.txt file

The entries added for PINsafe are:

L_OTC_Text = ?One Time Code:?

L_StartSession_Text = ?Start Session?

These are respectively the labels used for the one-time code text box and the TURing image request button. You can change these values (to the right of the = sign) to match your requirements, but ensure that the labels (to the left of the = sign) are as shown.

If you need to customise your pages for other languages, look in the nls sub-folder and find the sub-folder matching the language you need to use. Add strings with the same names as those shown above to the strings section. As noted above, please ensure that the files are saved as Unicode text.

Depending on what authentication method you are using, you may not need to modify all three of the login pages, as explained here:

- usr_pwd.htm is used for Active Directory plus PINsafe AgentXML authentication.
- usr_pcode.htm is used for RADIUS authentication as the ONLY form of authentication (i.e. when no Active Directory authentication is required).
- usr_pwd_pcode.htm is used when Active Directory authentication is used in conjunction with PINsafe RADIUS authentication.

The other 3 pages all need very similar modifications: they need a text box for the one-time code, a button to display the TURing image, a place to display the TURing image and the JavaScript necessary to display the image.

Starting with the last item, the following JavaScript should be sufficient:

```
function onClickStartSession()
{
    img = document.getElementById("PINsafeImage");
    username = document.getElementById("username");

    if ((img != null) && (username != null) && (username.value != ""))
    {
        var usernameValue;

        psn = username.value.indexOf("\\");
        if (psn != -1)
            usernameValue = username.value.slice(psn + 1);
        else
            usernameValue = username.value;

        img.src = "/PINsafeISAFilter.dll?username=" + usernameValue +
                  "&random=" + Math.round(Math.random()*1000000);
        img.style.display = "block";
    }
}
```

Note that, for usr_pwd_pcode.htm only, the fourth line should read

```
    username = document.getElementById("userid");
```

For the one-time code text box, both the id and the name attributes of the input field should be set to ?otc?:

```
<input id="otc" type="password" name="otc" />
```

For its label, use the value @@L_OTC_Text as the label text. This will be replaced by the label you defined in strings.txt:

```
<label for="otc">@@L_OTC_Text</label>
```

The button to display a TURing image should have an onclick event of ?onClickStartSession();?, and a value (label) of ?@@L_StartSession_Text?:

```
<input id="StartSession" type="button" value="@@L_StartSession_Text" name="StartSession" onclick="onClickStartSession();"/>
```

Finally, the placeholder for the TURing image should have an id of ?PINsafeImage?, and initially set to be invisible:

```
<img id="PINsafeImage" style="display:none;" />
```

135 Microsoft Office 365

136 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.

136.1 Video showing login to Office 365 using ADFS with PINpad

Swivel Authenticating Office365 using ADFS with PINpad from Swivel Secure.

137 Prerequisites

Swivel authentication platform 3.x

ADFS Proxy 2.0, ADFS Proxy 2.1

Microsoft Office 365

137.1 Downloads

ADFS Integration files

138 Baseline

(The version tested with)

Swivel 3.9.5

ADFS Proxy 2.0, ADFS Proxy 2.1

Microsoft Office 365

139 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.

140 Installation

140.1 Configure The Swivel Server

Configure a Swivel Agent (For standard XML Authentication)

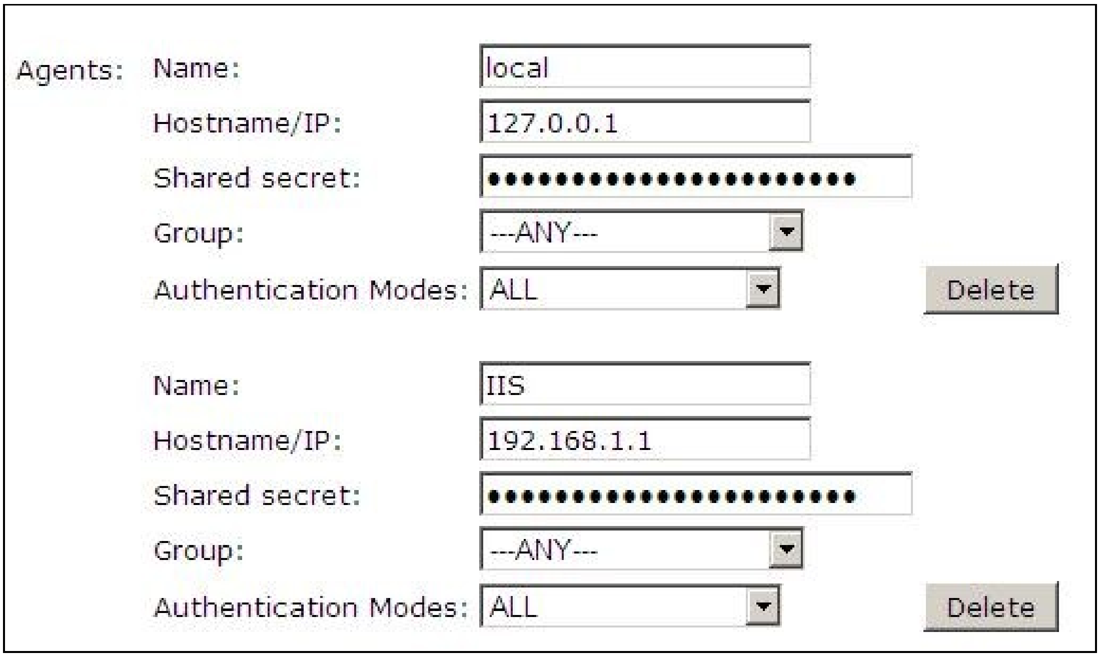
1. On the Swivel Management Console select Server/Agent

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: local

Hostname/IP: 127.0.0.1

Shared secret: ●●●●●●●●●●●●●●●●●●●●●●●

Group: ---ANY---

Authentication Modes: ALL

Name: IIS

Hostname/IP: 192.168.1.1

Shared secret: ●●●●●●●●●●●●●●●●●●●●●●●

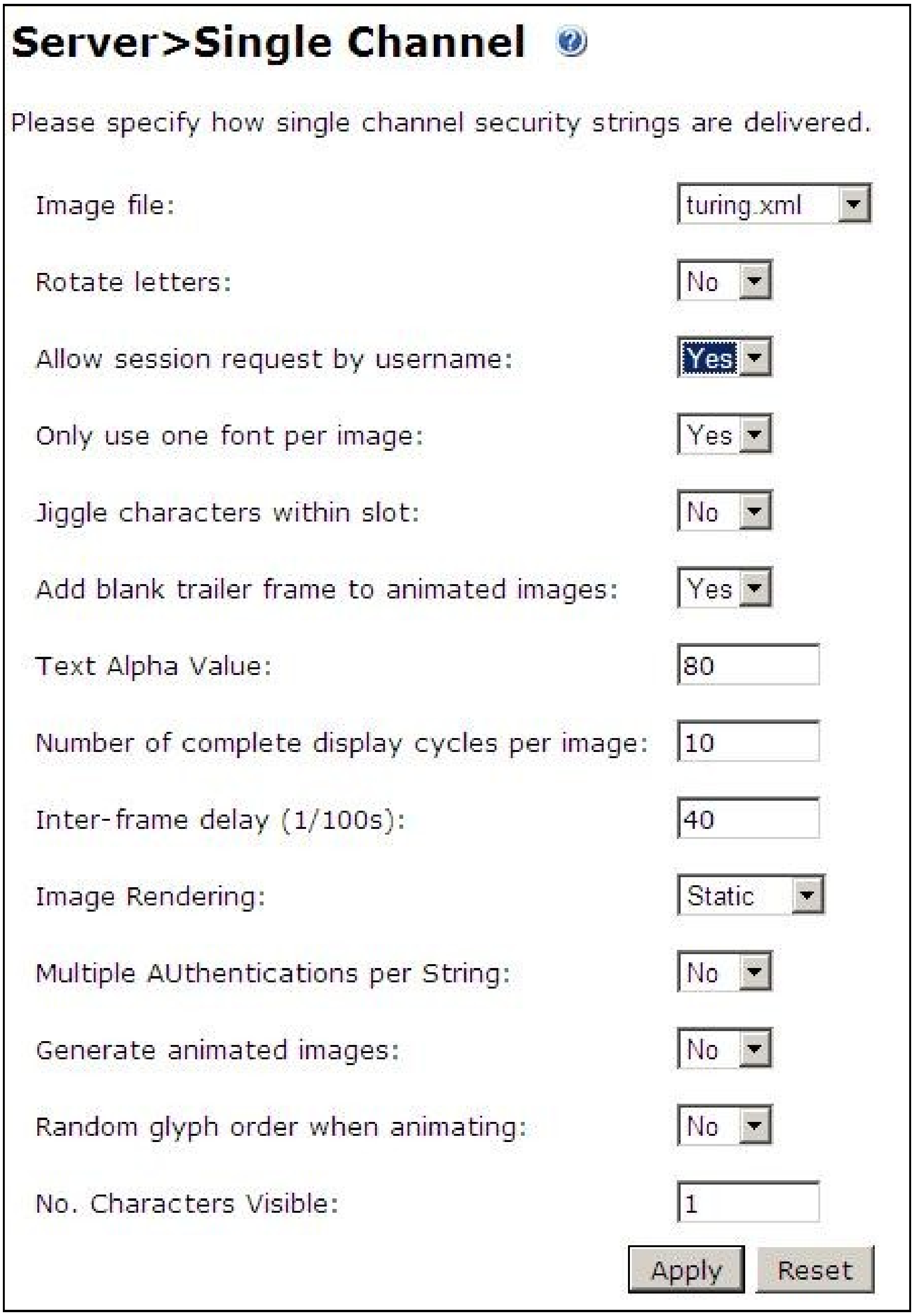
Group: ---ANY---

Authentication Modes: ALL

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: turing.xml

Rotate letters: No

Allow session request by username: Yes

Only use one font per image: Yes

Jiggle characters within slot: No

Add blank trailer frame to animated images: Yes

Text Alpha Value: 80

Number of complete display cycles per image: 10

Inter-frame delay (1/100s): 40

Image Rendering: Static

Multiple AUthentications per String: No

Generate animated images: No

Random glyph order when animating: No

No. Characters Visible: 1

140.2 Using additional attributes for authentication

When using additional attributes for authentication see User Attributes How To

140.3 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

140.3.1 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).

140.3.2 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 .

140.3.2.1 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.

PINsafeIdleTimeSecs 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.

140.3.3 Restart IIS

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

140.4 Additional Installation Options

140.4.1 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.

140.4.2 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.

141 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.

142 Uninstalling the Swivel Integration

143 Troubleshooting

Check the Swivel logs

Check the ADFS server logs

144 Known Issues and Limitations

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

145 Additional Information

146 Additional documentation

146.1 Swivel

Swivel ADFS and Office 365

High Level Overview Document

147 Microsoft OWA 2003 IIS Integration

147.1 Introduction

PINsafe allows users to authenticate users of Outlook Web Access (OWA) on Microsoft Exchange Server 2003. An ISAPI filter installed on the Exchange server allows access to protected resources through the PINsafe authentication. NOTE: This document refers to the version of the filter numbered 1.2.0.0, and the configuration application with the same version number.

147.2 Prerequisites

Microsoft Exchange 2003 with OWA. It should be configured as a front-end server for MS Exchange, with forms-based authentication enabled.

Microsoft 2003 Server

PINsafe server: Requires PINsafe 3.x. PINsafe does not need to be installed on the same machine, but the target server must be able to connect to a PINsafe server without any authentication except that provided by PINsafe.

Users are able to login using standard OWA

IIS Filter for OWA 2003

147.3 Baseline

Microsoft Exchange 2003 with OWA using IIS 6.0

Microsoft 2003 Server

PINsafe 3.7

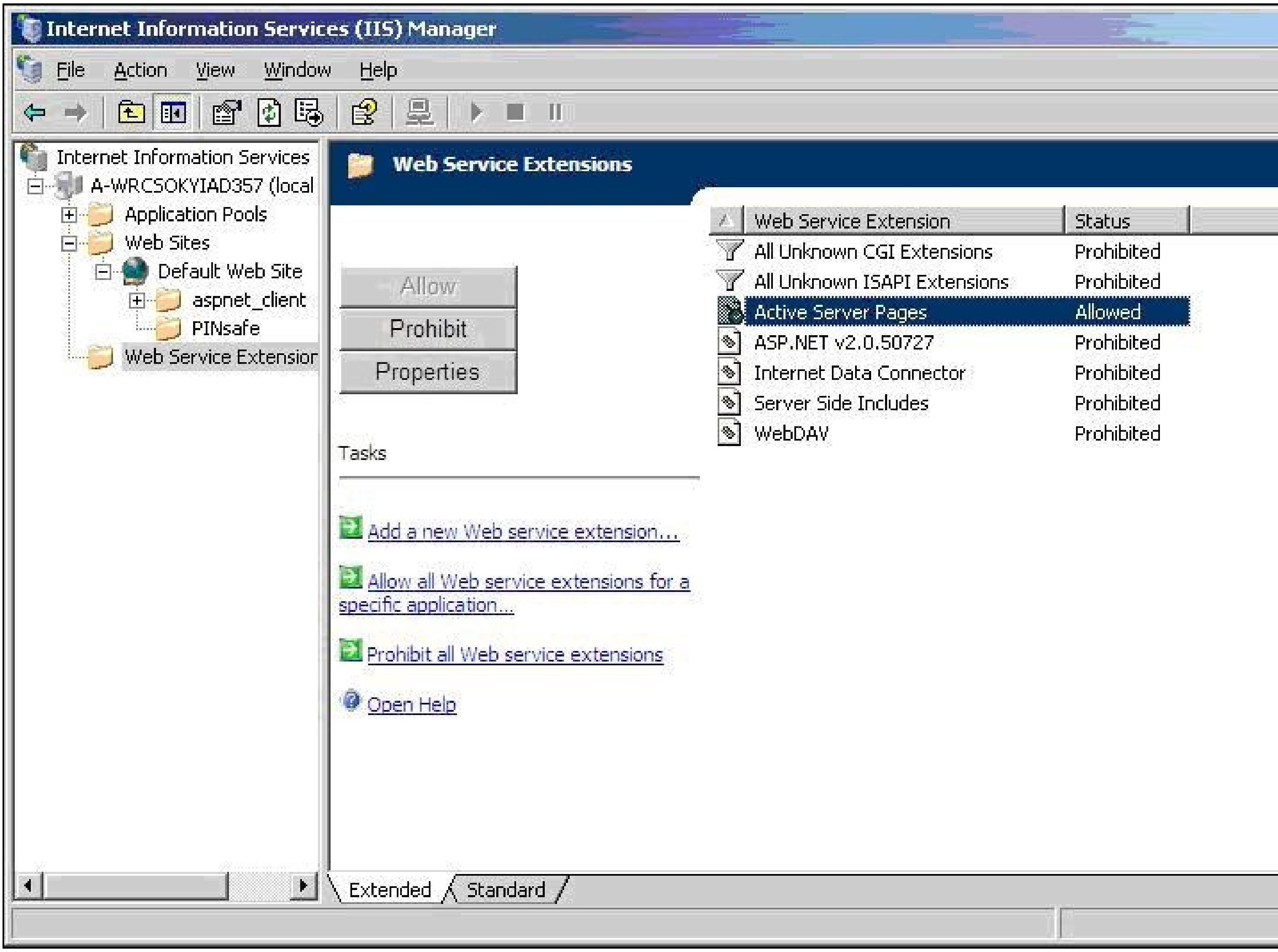
147.4 Architecture

The Exchange server makes authentication requests against the PINsafe server by XML authentication

147.5 Installation

147.5.1 Ensure Active Server Pages are Allowed

Allow Active Server Pages: to verify this, select the Internet Information Services Manager expand the required server then click on Web Service Extension.



Web Service Extension	Status
All Unknown CGI Extensions	Prohibited
All Unknown ISAPI Extensions	Prohibited
Active Server Pages	Allowed
ASP.NET v2.0.50727	Prohibited
Internet Data Connector	Prohibited
Server Side Includes	Prohibited
WebDAV	Prohibited

147.5.2 Software Installation

On the Exchange server run the PINsafeIISFilter.exe. The filter must be installed in the Exchange Server authentication web folder, which by default is C:\Program Files\Exchsrvr\exchweb\bin\auth. If this is not correct, change the target folder before installation. Select Start Menu Folder. When details are correct click on Install. If the error ?Incorrect Command Line Parameters? is seen click on OK.

147.5.3 Configuration of the IIS Filter

The Filter Configuration should start after installation or can be started through the Start Menu.

- PINsafe Server tab contains settings which define the PINsafe server which will be used to authenticate users.

Hostname/IP: The name or IP address of the PINsafe server.

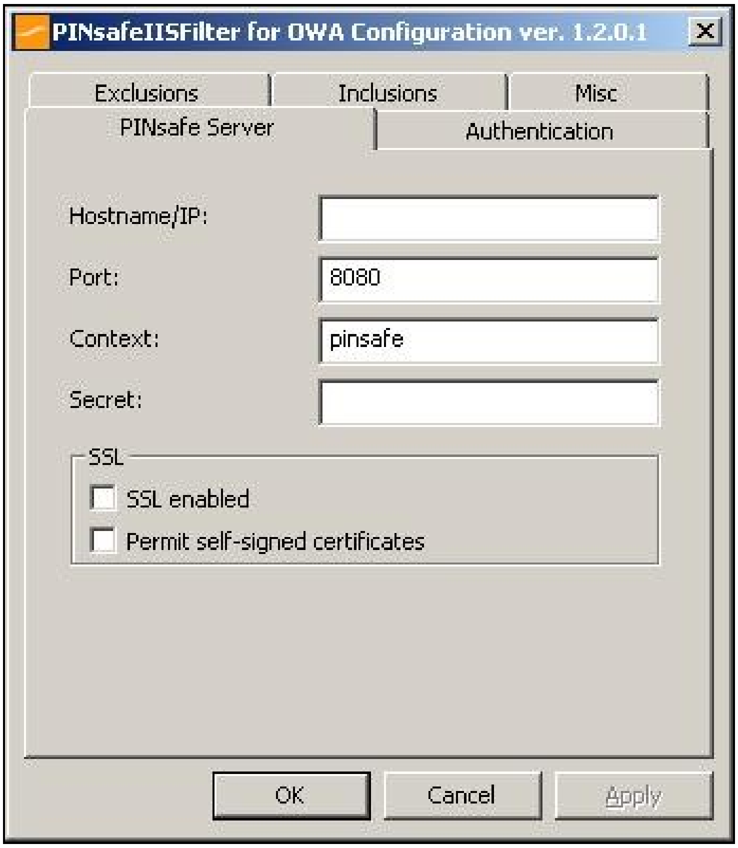
Port: The port number used by the PINsafe server, 8080 for a software install or PINsafe virtual or hardware appliance (do not use 8443)

Context: The PINsafe install name usually pinsafe, or for a PINsafe virtual or hardware appliance proxy.

Secret: The common secret used to communicate with the PINsafe server. This value must be the same as the secret defined for the PINsafe agent.

SSL enabled Tick this box to require SSL (HTTPS) communication with the PINsafe server, for a PINsafe virtual or hardware appliance ensure the box is ticked.

Permit self-signed certificates Tick this box to allow SSL certificates to be self-signed. This also ignores other certificate errors, such as site names not matching. For a PINsafe virtual or hardware appliance tick this box until a valid certificate is applied.



PINsafeIISFilter for OWA Configuration ver. 1.2.0.1

Hostname/IP:

Port: 8080

Context: pinsafe

Secret:

SSL

□ SSL enabled

□ Permit self-signed certificates

- The Authentication tab contains the following settings:

Idle time (s): The length of time in seconds that the authentication cookie is valid, provided you make no OWA requests in that time. If you do, the cookie is refreshed and the countdown starts again.

Username header: The name of a cookie which will pass the username of the authenticated PINsafe user. If this value is blank, no cookie will be provided.

Single Indicates that single channel security strings (i.e. TURing image) are permitted.

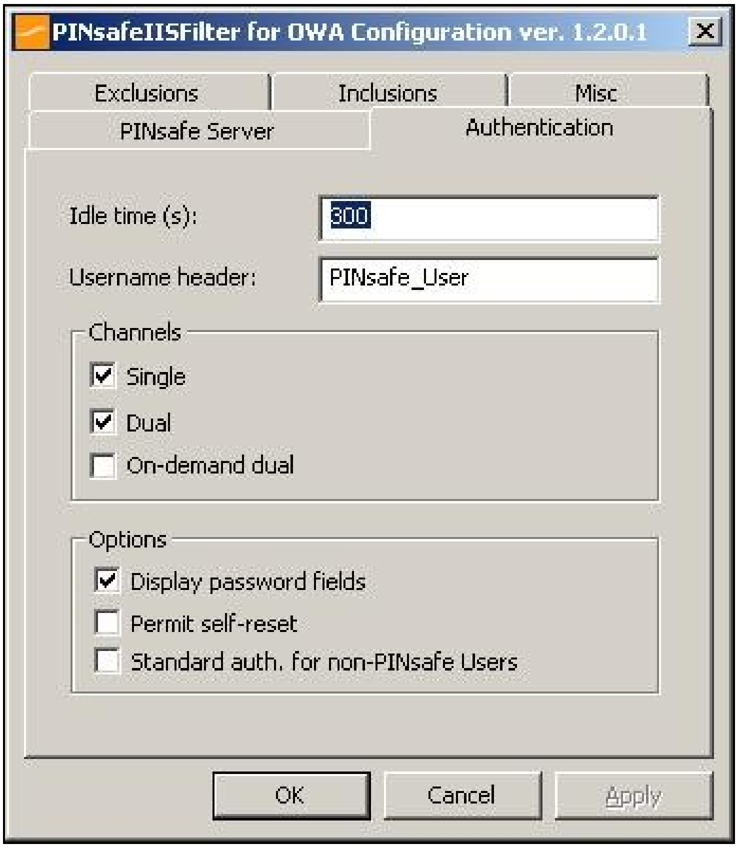
Dual Indicates that dual channel security strings (i.e. via e-mail, SMS) are permitted.

On-demand dual Indicates that the login page should display a button to request dual-channel security strings.

Display password fields Indicates that the login page should show a field for PINsafe password as well as OTC.

Permit self-reset Indicates that the user self-reset page should be enabled.

Standard auth. for non-PINsafe Users If enabled, users that PINsafe does not recognise will be allowed to authenticate using standard Active Directory methods. Note that this option requires PINsafe 3.5 or later. 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.



PINsafeIISFilter for OWA Configuration ver. 1.2.0.1

Idle time (s): 300

Username header: PINsafe_User

Channels

☑ Single

☑ Dual

□ On-demand dual

Options

☑ Display password fields

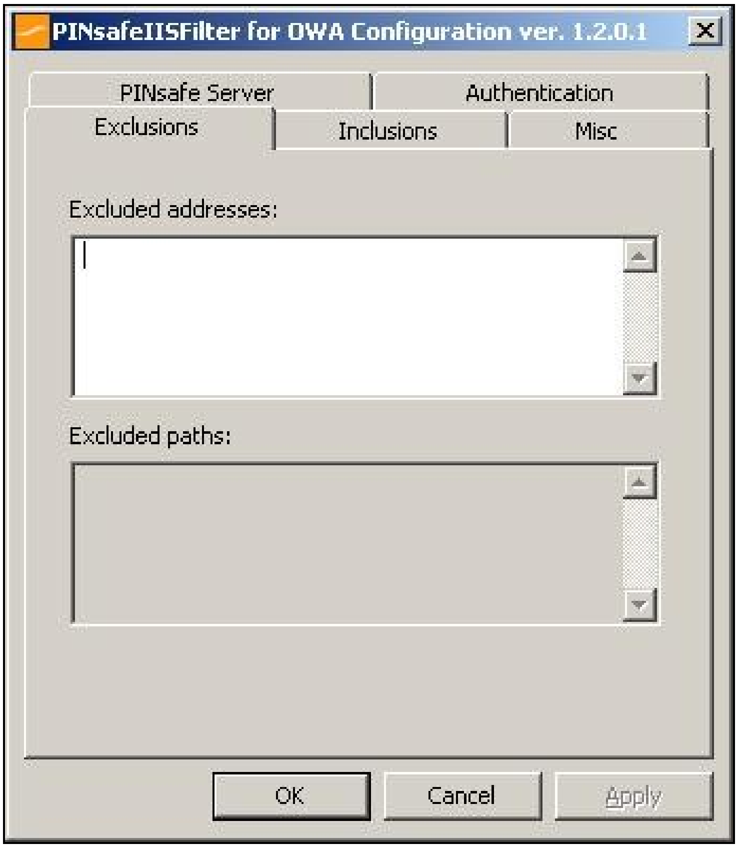
□ Permit self-reset

□ Standard auth. for non-PINsafe Users

- Exclusions

Excluded Paths: This is a list of paths within the current website which should be exempt from PINsafe authentication. This is only relevant if the included paths list is empty, in which case all paths not on this list will be protected by PINsafe.

Excluded addresses: This is a list of IP addresses which are exempt from PINsafe authentication. All requests from these addresses are passed through without authentication.



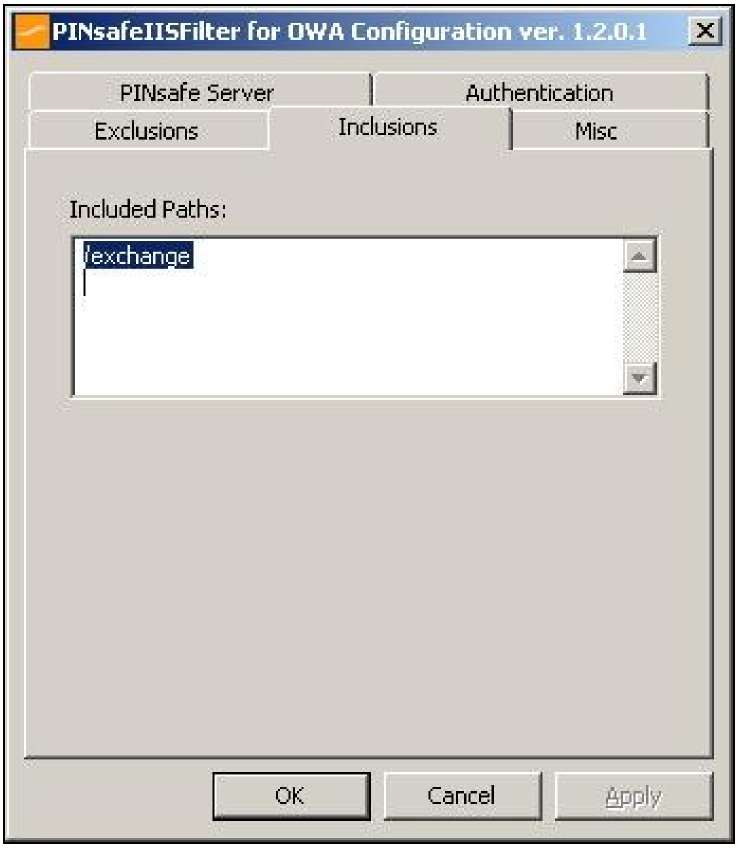
PINsafeIISFilter for OWA Configuration ver. 1.2.0.1

Excluded addresses:

Excluded paths:

- Inclusions

Included Paths This is a list of paths within the current website which require PINsafe authentication. If this list is empty, the entire website will be protected except as indicated by the Exclusions tab. Paths should be one per line. You should at least ensure that the virtual folder ?/exchange? is listed.



Included Paths:

/exchange

- Misc Tab

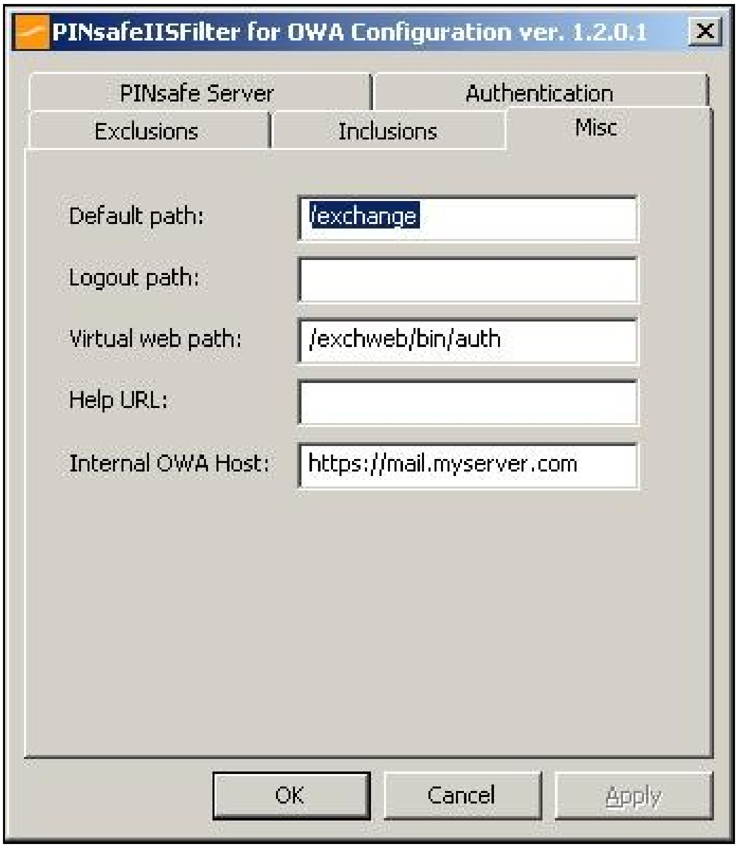
Default path: This is the path to which authenticated requests are directed if the login page is targeted directly. For this particular version of the filter, it should be ?/exchange?. If a user tries to access a protected page, she is redirected to the login page, and after authentication, back to the page she was trying to access. If the user requests the login page directly, she will be redirected to this location after authentication.

Logout path: Requesting this path will result in the user being logged out. Subsequent requests will require re-authentication, if relevant. If this path is empty, users can only be logged out by closing the browser, or if the authentication times out.

Virtual web path: This is the path to the PINsafe authentication pages. The default for this version of the filter is ?/exchweb/bin/auth?. You should only change this if your Exchange server has an unusual configuration.

Help URL: The URL for PINsafe IIS filter help. The filter does not come with help pages as standard, so this should only be filled in if help pages have been provided by the reseller or end user.

Internal OWA Host: This should be set to the URL of the OWA Exchange server, for example https://mail.myserver.com. Since this URL is called from the server itself, you could use https://localhost, but if you do that, make sure that you check the option to accept self-signed certificates, as the server certificate will not match the name ?localhost?.



PINsafeIISFilter for OWA Configuration ver. 1.2.0.1

Default path: /exchange

Logout path:

Virtual web path: /exchweb/bin/auth

Help URL:

Internal OWA Host: https://mail.myserver.com

147.5.4 Modifying the OWA Authentication Pages

The installation process replaces the existing owalogon.asp file with one customised for PINsafe. The existing file is renamed to owalogon.asp.old. Note that if you have customised the OWA logon page, other than simply replacing images or text messages, then you will not be able to use the customised pages as they are. You will need to combine your own customisations with those necessary for PINsafe authentication. For help with this, please contact your reseller, or Swivel Secure.

147.5.5 Modifying the login Page to stop the Single Channel Image automatically appearing

By default the single channel authentication will appear when the username and AD password is entered and the user selects the OTC field. As a single channel session has started the PINsafe server is expecting an OTC to be entered from the Single Channel TURing image. If dual channel authentication is required then the automatic display of the Single Channel Turing image needs to be turned off. This can be done by modifying the login.asp file which by default is located in C:\Program Files\Exchsrvr\exchweb\bin\auth. The following needs to be removed from the username attribute field:

```
onblur=?checkUser()?
```

147.5.6 Modifying the login Page to allow Dual Channel On Demand Delivery

If you want to use only dual-channel on-demand and no other method, then you can manage this by a simple change to image.asp (under /exchweb/bin/auth). Edit this file, search for "SCImage" and replace it with "DCMessage". Leave the onblur attribute as it was. Dual channel authentication for the user and also On Demand Delivery should be enabled on the PINsafe Administration console under Server/Dual Channel.

147.5.7 International OWA login Pages

If you want to use an internationalized version of the logon page, you will need to modify the installed files by hand, as follows:

1. Open an Explorer window on the OWA authentication folder (by default C:\Program Files\Exchsrvr\exchweb\bin\auth).

2. Copy all of the files in the authentication folder except owalogon.asp.old and owaauth.dll to the language-specific folder you intend to use (if you need to support multiple languages, you will need to copy all of them to each folder).

3. Rename owalogon.asp.old back to owalogon.asp.

4. In each folder, make a backup copy of logon.asp (which was in the folder before), and copy all the lines beginning ?CONST? from the beginning of the original logon.asp file to the copy of owalogon.asp you have just created, replacing similar lines in that file. You will also need to change the strings labelled ?CONST L_OTC_Text? and ?CONST L_StartSession_Text? with appropriate translations of the English strings ?OTC? and ?Show TURing?. Finally, rename owalogon.asp to logon.asp.

NOTE: Unlike previous versions of the PINsafe ISAPI filter (both standard and OWA), the PINsafe customisation is not visible immediately. Once you enter a username, the OTC field will appear, as will a TURing image. This means that it is no longer necessary to click a button to get a TURing image.

However, a button is provided should you wish to refresh the image (if the first one is too difficult to read, for example). Note that if you enable the option to allow standard authentication for non-PINsafe users, and the user is not recognised, no OTC field or TURing image will be displayed. Note also in this case there may be a small delay while the user is checked.

147.5.8 Applying Settings

After the changes have been made click apply and from the Services application, usually found from the Control Panel Administrative Tools, restart the World Wide Web Publishing Services.

147.5.9 Activating the ISAPI filter

1. On the Internet Information Services Manager Select the Properties for the website

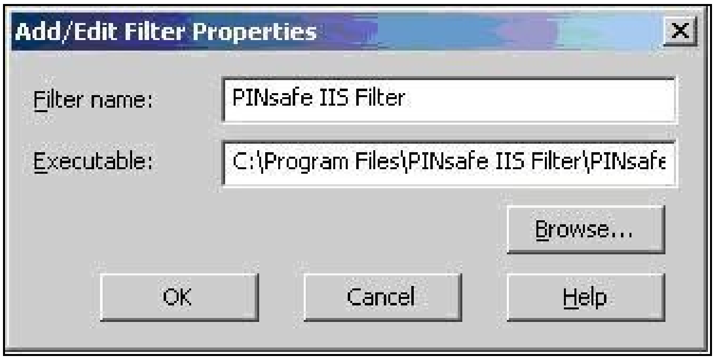
2. Select ISAPI filters

3. Select Add ISAPI filter

4. Select the Path to the PINsafe ISAPI filter. Note that the actual file you require will be PINsafeIISFilter.dll, located in the sub-folder bin of the installation folder.

Default: c:\Program Files\Exchsrvr\exchweb\bin\auth\bin\

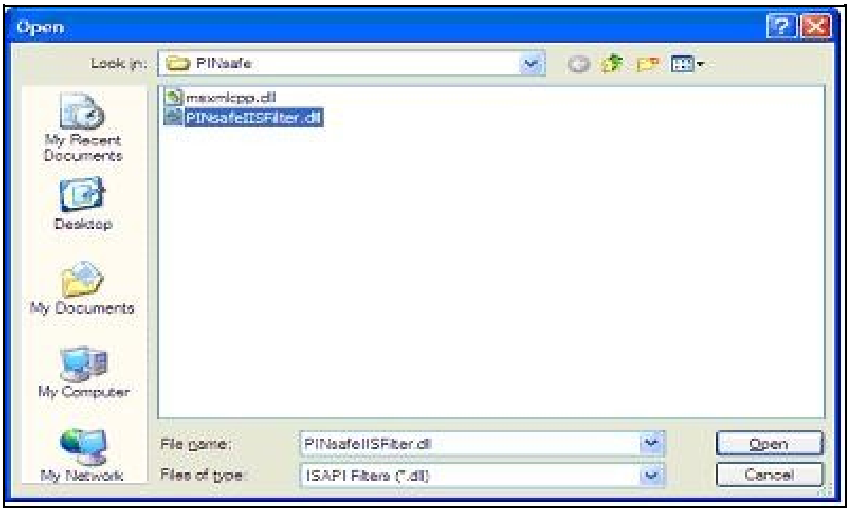
5. Ensure PINsafe ISAPI filter is top filter then click on OK



Add/Edit Filter Properties

Filter name: PINsafe IIS Filter

Executable: C:\Program Files\PINsafe IIS Filter\PINsafe



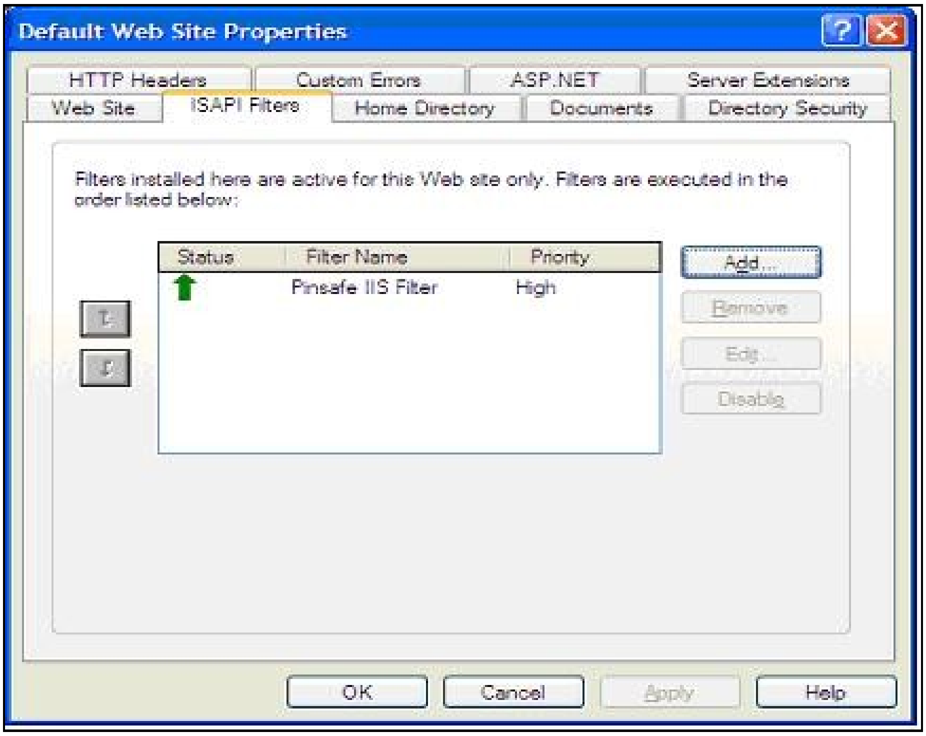
Open

Look in: PINsafe

maxmlcpp.dll
PINsafeIISFilter.dll

File name: PINsafeIISFilter.dll

Files of type: ISAPI Filters (*.dll)



Filters installed here are active for this Web site only. Filters are executed in the order listed below:

Status	Filter Name	Priority
⬆	Pinsafe IIS Filter	High

147.5.10 Configure The PINsafe Server

Configure a PINsafe Agent (For standard XML Authentication)

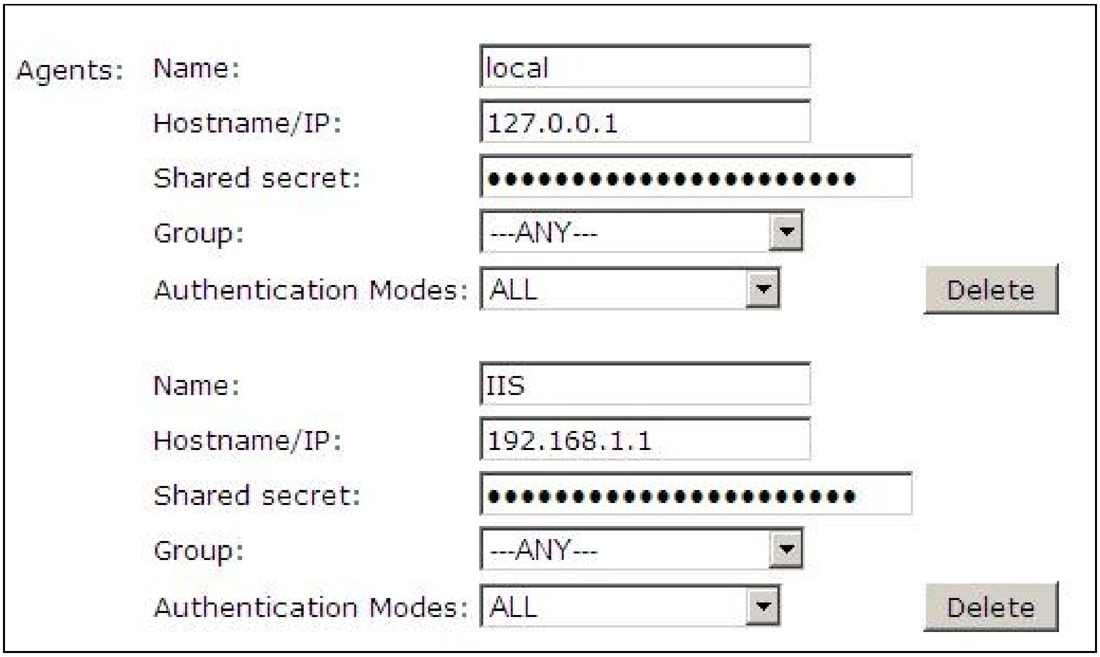
1. On the PINsafe Management Console select Server/Agent

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

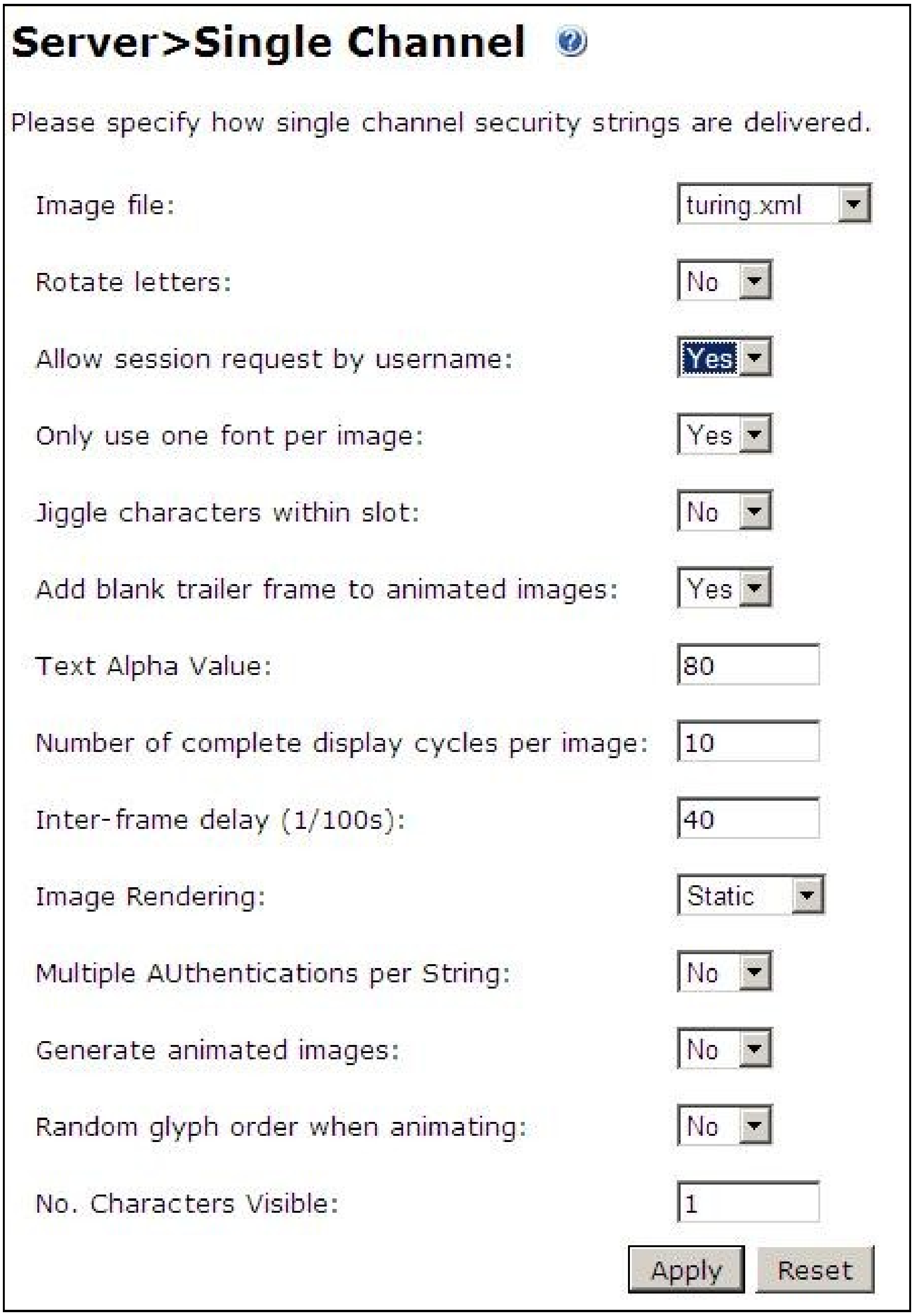


Agents:	Name:	local
	Hostname/IP:	127.0.0.1
	Shared secret:	●●●●●●●●●●●●●●●●●●●●●●●
	Group:	---ANY---
	Authentication Modes:	ALL
	Name:	IIS
	Hostname/IP:	192.168.1.1
	Shared secret:	●●●●●●●●●●●●●●●●●●●●●●●
	Group:	---ANY---
	Authentication Modes:	ALL

Configure Single Channel Access

1. On the PINsafe 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: turing.xml

Rotate letters: No

Allow session request by username: Yes

Only use one font per image: Yes

Jiggle characters within slot: No

Add blank trailer frame to animated images: Yes

Text Alpha Value: 80

Number of complete display cycles per image: 10

Inter-frame delay (1/100s): 40

Image Rendering: Static

Multiple AUthentications per String: No

Generate animated images: No

Random glyph order when animating: No

No. Characters Visible: 1

147.6 Verifying the Installation

To test the modifications, simply attempt to connect to Outlook Web Access. You should see the usual OWA authentication page, with two additions. Firstly, a third text box, for you to enter your PINsafe one-time code, and secondly, a new button labelled ?Show TURing? (or the equivalent if you have changed the language). To log on, enter your username (including domain if required) and click the ?Show TURing? button, if you are using TURing images. Enter your domain password and one-time code. Note that you should NOT use PINsafe passwords in this case. The authentication mechanism assumes that you have no PINsafe password, so will fail if you have. Now click ?Log On?, and if your credentials are correct, you should see the OWA interface as before.

147.7 Uninstalling the PINsafe Integration

Uninstall the PINsafe IIS filter then, the original Logon.aspx must be restored by renaming Logon.asp.old to Logon.aspx.

Note that the installation creates a new Logon.aspx file in /owa/auth, and renames the original to Logon.asp.old. To complete uninstallation this file must be copied back again.

147.8 Troubleshooting

147.8.1 General Errors

Check the PINsafe and Windows server logs, and the IIS log C:\Windows\System32\LogFiles\W3SVC1 (the last directory may be different if you have more than one website on the same server).

Add an entry to the hosts file on the OWA server (C:\Windows\System32\drivers\etc\hosts). Add a new line to the file containing the following:

127.0.0.1 <owaserver.domain>

Replace <owaserver.domain> with the full external host name used to access the OWA server (not including https://). Then change the internal OWA host name on the PINsafe configuration to https://owaserver.domain (replacing owaserver.domain as before).

Reboot the Exchange server if it has not been started

Check the AD User is not required to Change their Password

Check the AD User account is not locked

User regularly times out after a short interval

The session is kept open by user activity. If this is insufficient then increase the cookie idle timeout value.

Turing image appears but user cannot authenticate.

Verify that the OWA is configured to use port 8080 and context pinsafe. port 8443 and context proxy will cause problems with authenticating users but allow the Turing image to be displayed.

147.8.2 No Login Page Errors

No login page, check the Exchange version

Check to see if an International version of OWA is being used

147.8.3 Single Channel (Turing) Image issues

Red Cross instead of Turing image, right click on red cross and look at its properties. Ensure PINsafe server is running.

If you do not see a Turing image when using start session then in a web browser test the following link from the IIS server. If an image is not seen, then there is a problem either with communicating with the PINsafe server or the Allow Image request by username may be set to No.

For PINsafe software and virtual or hardware appliance installs:

http://<pinsafe_server_ip>:8080/pinsafe/SCImage?username=<username>

147.8.4 Active Server Pages Errors

If the web page is redirected to the owalogon.asp page but an error message appears, then ensure that the Active Server Pages are allowed. To verify this select the Internet Information Services Manager, expand the required server then click on Web Service Extensions.

147.8.5 ISAPI Filter Issues

NOTE: after the first time you authenticate to OWA, you should check that the ISAPI filter is loaded and running properly. Go to the web site properties dialog and locate the ISAPI filters tab. If the PINsafe filter doesn?t have a green arrow next to it, or the priority shows as ?Unknown?, then it is not working properly. You will still get redirected to the login page, and the built-in OWA security will handle that, but without the filter, it is possible for a knowledgeable person to authenticate with just the username and password, and bypass PINsafe.

The following procedure should ensure that the filter is loaded correctly:

1. Check which application pool your web application is running as, then go to the properties page for that application pool.

2. On the Identity tab, change the user to ?Local System?. You will be warned that this is a potential security risk, but don?t worry ? it won?t be left like this.

3. Restart IIS.

4. Authenticate to OWA. This should ensure that the filter is loaded: go back and check it.

5. You can now go back to the application pool and change the identity back to what it was originally: it would appear that it is only necessary to run as an administrator to get the filter to register initially.

147.8.6 Name resolution issue

The Exchange server may be looking for exchange.company.com from the internal network but cannot resolve it. Edit the hosts file mapping the name to 127.0.0.1.

147.9 Known Issues and Limitations

PINsafe requires Forms Based Authentication (FBA), whereas iPhone and other Smart Phones (plus Outlook Anywhere) will require Non Forms Based Authentication (NFBA). You cannot have FBA and NFBA running on the same front end Exchange server. You would have to create a new Exchange server as a front end to the existing Exchange server and put the PINsafe OWA filter on that. You should be able to maintain services to the existing Exchange server whilst creating a new Exchange front end. Eventually you should be able to disable access to the old OWA, but maintain NFBA authentication to your other services.

To check if FBA is enabled, in the exchange manager, go to the server, select protocols, http and choose properties.

Microsoft have published a workaround for this issue, see Microsoft OWA with OMA on Exchange 2003

147.10 Useful Links

HTTP to HTTPS Redirect [1]

147.11 Additional Information

For assistance in the PINsafe installation and configuration please firstly contact your reseller and then email Swivel Secure support at support@swivelsecure.com

148 Microsoft OWA 2007 IIS Integration

149 Introduction

PINsafe allows users to authenticate users of Outlook Web Access (OWA) using Microsoft Exchange Server 2007.

Active Sync users are able to receive email without PINsafe authentication as this uses a separate URL.

150 Prerequisites

Microsoft Exchange 2007 with OWA

Microsoft 2003/8 server

Microsoft .Net Framework version 3.5

PINsafe 3.x

Users are able to login using standard OWA

IIS Filter for OWA 2007 version 2.7. This uses a different authentication mechanism from 2.6, which resolves problems reported by some users. Also some cosmetic fixes: in particular, Pinpad images are correctly sent as PNG format, rather than JPG.

Older versions:

IIS Filter for OWA 2007 version 2.6, including support for Pinpad and Change PIN

IIS Filter for OWA 2007 version 2.3

IIS Filter for OWA 2007 version 2.0

Login page for OWA 2007 8.2.301 (not necessary for version 2.6).

151 Baseline

For version 2.3 or later:

- Microsoft Exchange 2007 service Pack 3 with OWA using IIS
- Microsoft 2008 server
- PINsafe 3.7 or later

For version 2.0

- Microsoft Exchange 2007 service Pack 1 with OWA using IIS
- Microsoft 2003 server
- PINsafe 3.7 or later

152 Architecture

The Exchange server makes authentication requests against the PINsafe server by XML authentication

153 Installation

153.1 Software Installation

Run the executable to install it on the Exchange Server. If your Exchange Server instance is not installed in the default location (C:\Program Files\Microsoft\Exchange Server\V14), you will need to modify the installation path. The installation path should be <ExchangeServerRoot>\ClientAccess\OWA

153.2 Configuration of the IIS Filter

After installation modify the settings. The Filter Configuration should start after installation or can be started through the Start Menu. If the Exchange Server installation is not in the default location, select the OWA directory as above in which to modify the web.config file.

153.2.1 Swivel Settings

Server Name/IP: The Swivel server IP address or hostname

Port: Swivel server port, for a Swivel virtual or hardware appliance use **8080** (**not 8443**)

Context: Swivel install name, for a Swivel virtual or hardware appliance use Swivel (not proxy)

Use SSL Select tick box if SSL is used, for a Swivel virtual or hardware appliance tick this box. This also ignores other certificate errors, such as site names not matching.

Secret: The shared secret that must be entered also on the Swivel server Administration Console under Server/Agents

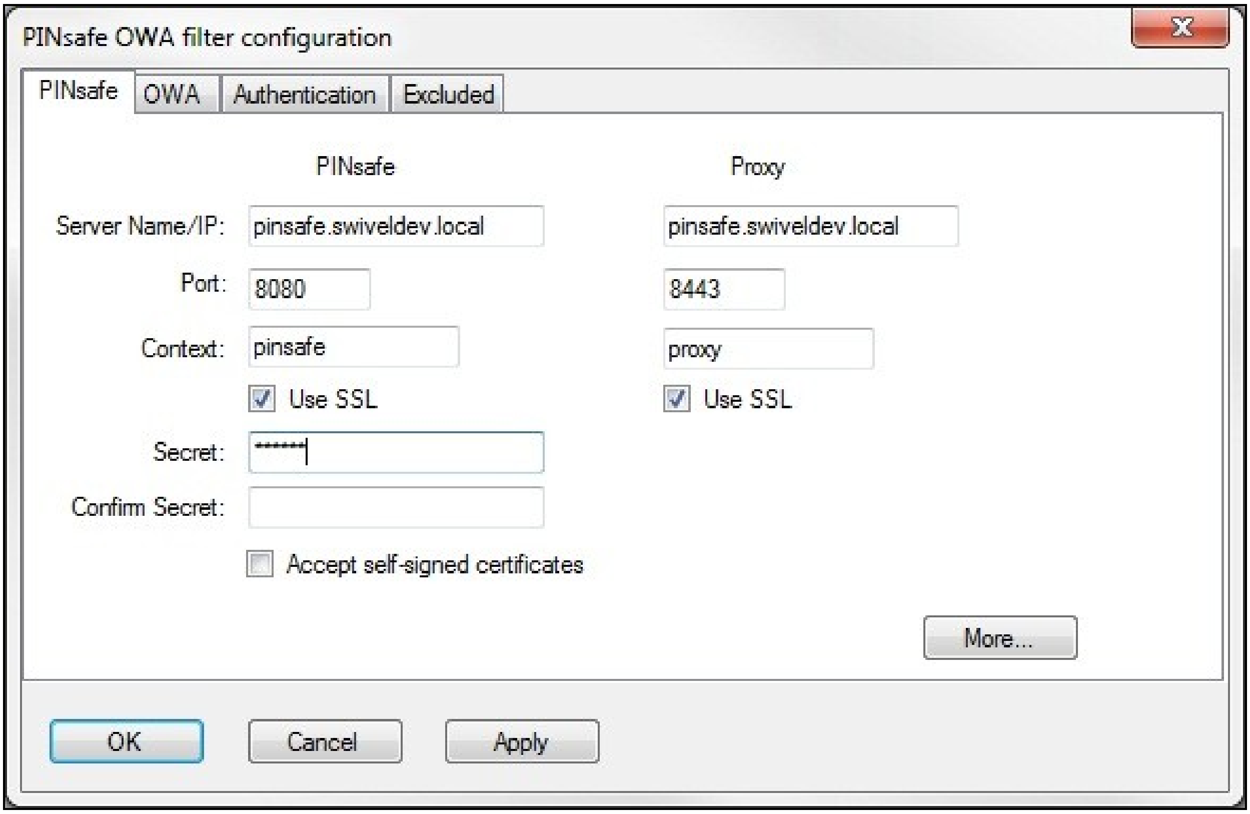
Accept self-signed certificates Where SSL is used with self signed certificates, for a Swivel virtual or hardware appliance tick this box until a valid certificate is installed.

Proxy Server These are used to retrieve TURing or PINpad images. If you are using a version of Swivel that does not support Pinpad natively (3.9 or earlier), you will need the special version of the virtual or hardware appliance proxy that does support Pinpad. If you are not using Pinpad, you can set these to be the same as the first set of values: if you are not using an virtual or hardware appliance, you MUST set them to be the same.

Proxy Port: Swivel server port, for a Swivel virtual or hardware appliance use **8443**

Proxy Context: Swivel install name, for a Swivel virtual or hardware appliance use proxy

Proxy Use SSL Select tick box if SSL is used, for a Swivel virtual or hardware appliance tick this box. This also ignores other certificate errors, such as site names not matching.



	PINsafe	Proxy
Server Name/IP:	pinsafe.swiveldev.local	pinsafe.swiveldev.local
Port:	8080	8443
Context:	pinsafe	proxy
	☑ Use SSL	☑ Use SSL
Secret:	******	
Confirm Secret:		
	☐ Accept self-signed certificates	

153.2.2 OWA Settings

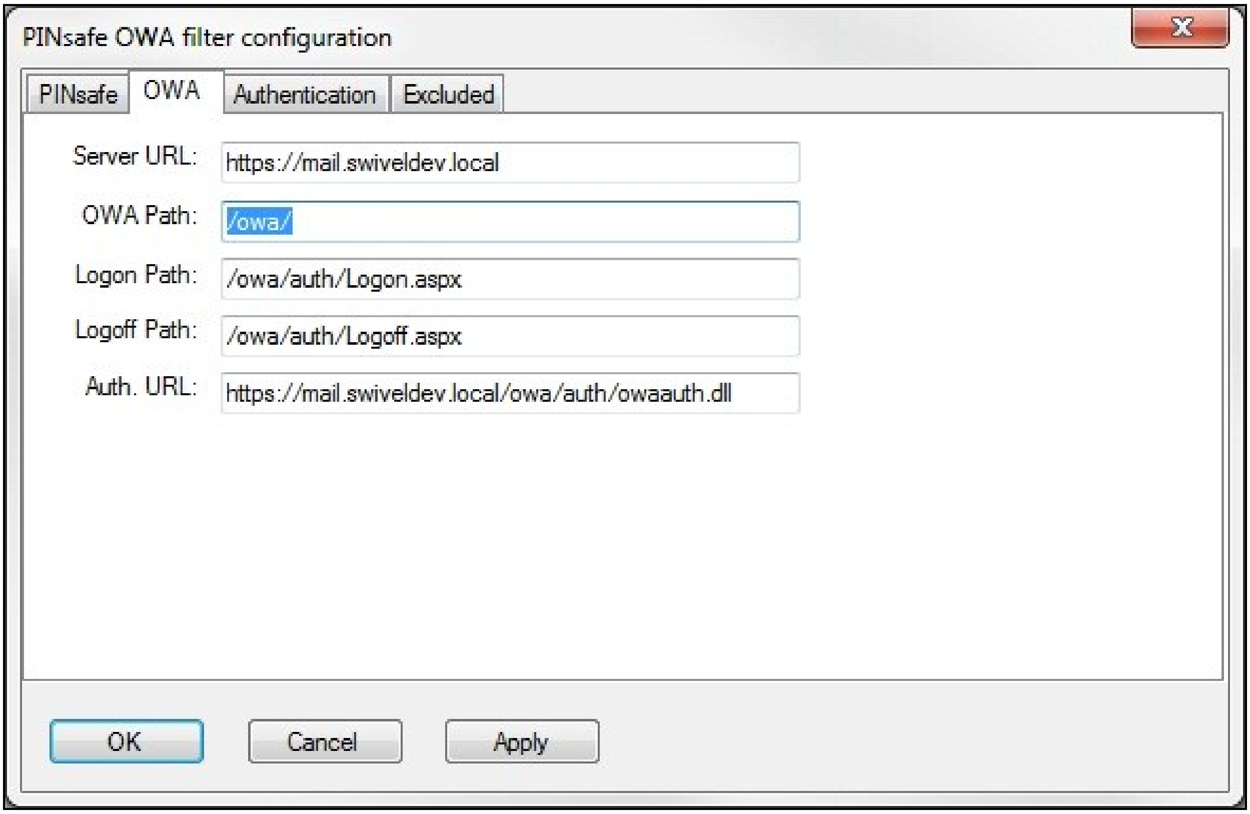
Server URL: Exchange Server URL, Example: https://<exchange.mycompany.com>

OWA Path: OWA path, usually /owa, unless this has been explicitly changed

Logon Path: Logon path Usually /owa/Logon.aspx

Logoff Path: Logoff path /owa/Logoff.aspx

Auth. URL: This is the URL for OWA authentication and is usually https://<exchange.mycompany.com>/owa/auth/owaauth.dll



PINsafe OWA filter configuration

Server URL: https://mail.swiveldev.local

OWA Path: /owa/

Logon Path: /owa/auth/Logon.aspx

Logoff Path: /owa/auth/Logoff.aspx

Auth. URL: https://mail.swiveldev.local/owa/auth/owaauth.dll

153.2.3 Authentication Settings

Cookie Secret Change: This is an experimental setting, which increases security by changing the secret used to encrypt the authentication cookie at a specified interval. It is recommended that you leave this at 0, i.e. never change it. In particular, do not change this if you have multiple OWA servers, as it will cause problems.

Idle Time: The length of time in seconds that the authentication cookie is valid, provided you make no OWA requests in that time. If you do, the cookie is refreshed and the countdown starts again.

Allow non-PINsafe Users If this option is ticked, non Swivel users are allowed to authenticate using standard OWA authentication. This requires Swivel 3.5 or higher. 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.

Filter Enabled The filter enabled option is mainly for testing, but also to handle situations such as enabling mobile access to the same Exchange Server i.e. ActiveSync and Windows Mobile Device Center. If the filter is disabled, you still need to authenticate through Swivel if you use the standard login page, but it is possible to authenticate using only AD credentials if you have a way to call the AD authentication filter directly.

Ignore Domain Prefix If this option is ticked, any prefixed domain (i.e. anything before the '\' character) is removed before sending the username to PINsafe. The full username is sent to OWA.

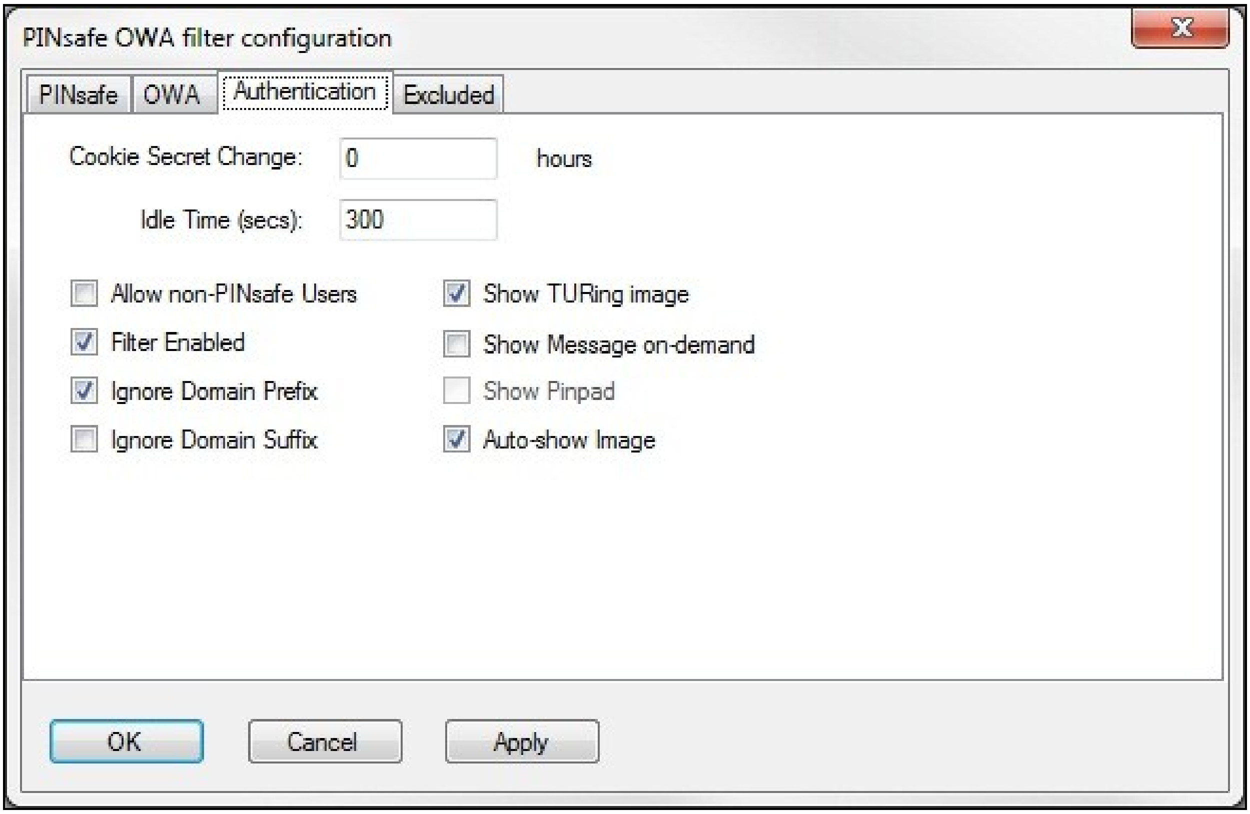
Ignore Domain Suffix If this option is ticked, any suffixed domain (i.e. anything after the '@' character) is removed before sending the username to PINsafe. The full username is sent to OWA.

Show TURing image If this option is ticked, a TURing image is shown to authenticate users.

Show Message on-demand If this option is ticked, a button is displayed to request a security string to be sent via SMS or email.

Show Pinpad If this option is ticked, an Pinpad button array is shown to authenticate users. You cannot have both TURing and Pinpad enabled.

Auto-show image If this option is ticked, the TURing or Pinpad image is requested as soon as the user enters the username and tabs away from it. If this option is not ticked, the user must click a button to show the image.



PINsafe OWA filter configuration

Cookie Secret Change: 0 hours

Idle Time (secs): 300

□ Allow non-PINsafe Users

☑ Filter Enabled

☑ Ignore Domain Prefix

□ Ignore Domain Suffix

☑ Show TURing image

□ Show Message on-demand

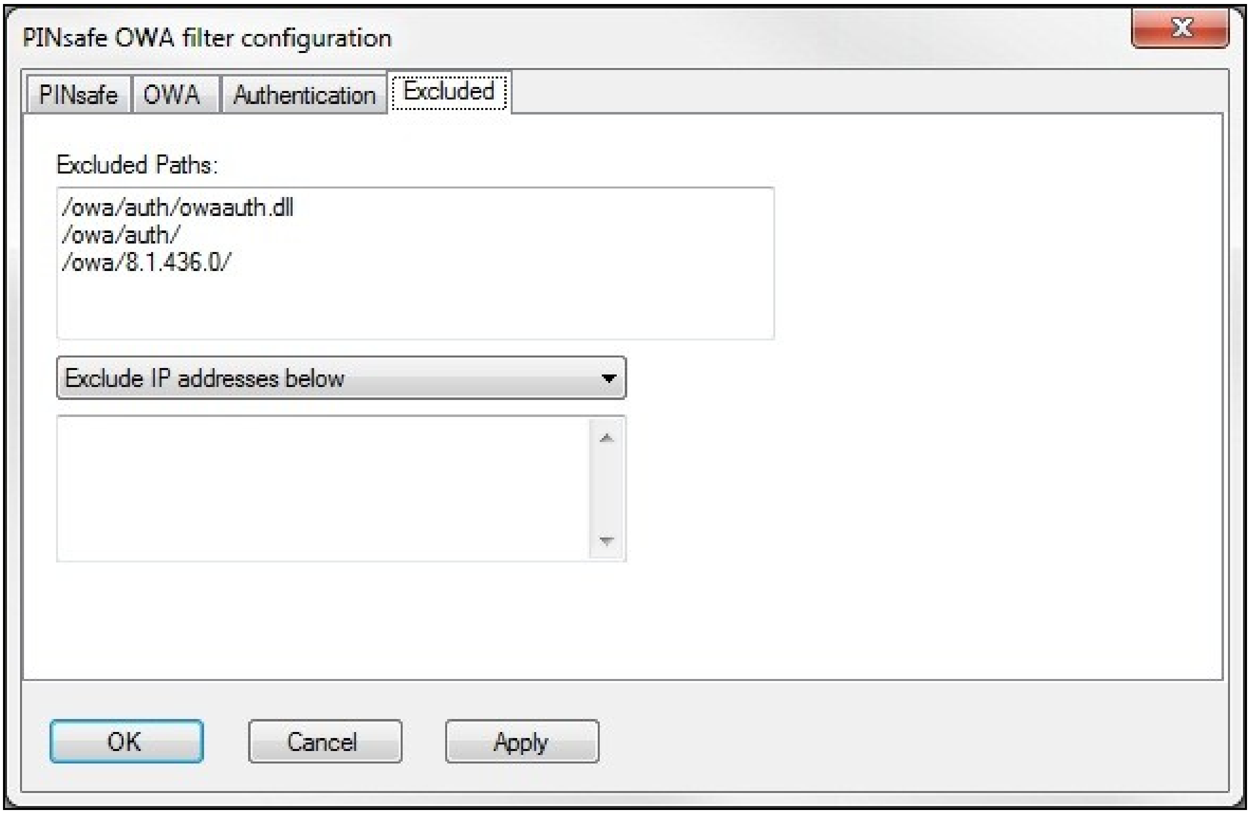
□ Show Pinpad

☑ Auto-show Image

153.2.4 Excluded Settings

Excluded Paths: This allows paths to be set for which authentication is not required to reach them. The paths shown on the display are added by default. The configuration program automatically detects the current build of OWA and includes that.

Excluded/Included IP addresses: You can choose to enable PINsafe authentication only for certain source IP addresses. Typically, you will do this if you wish to allow internal access to OWA without PINsafe authentication. Selecting "Exclude IP addresses below" will exclude the listed addresses from PINsafe authentication, while "Only include IP addresses below" will apply PINsafe authentication only to those IP addresses listed. For example, if you know that all external requests will come via a firewall at 192.168.0.99, you can select ?Only include IP addresses below?, and enter the single IP address as the address to include. Note that you can enter IP address ranges here using CIDR notation, for example 192.168.0.0/24 or 192.168.0.0/255.255.255.0. PINsafe will always display addresses using the latter format, irrespective of how they are entered. IPv6 addresses are not currently supported.



Excluded Paths:

```
/owa/auth/owaauth.dll
/owa/auth/
/owa/8.1.436.0/
```

Exclude IP addresses below

153.3 Configure The PINsafe Server

153.3.1 Configure a PINsafe Agent (For standard XML Authentication)

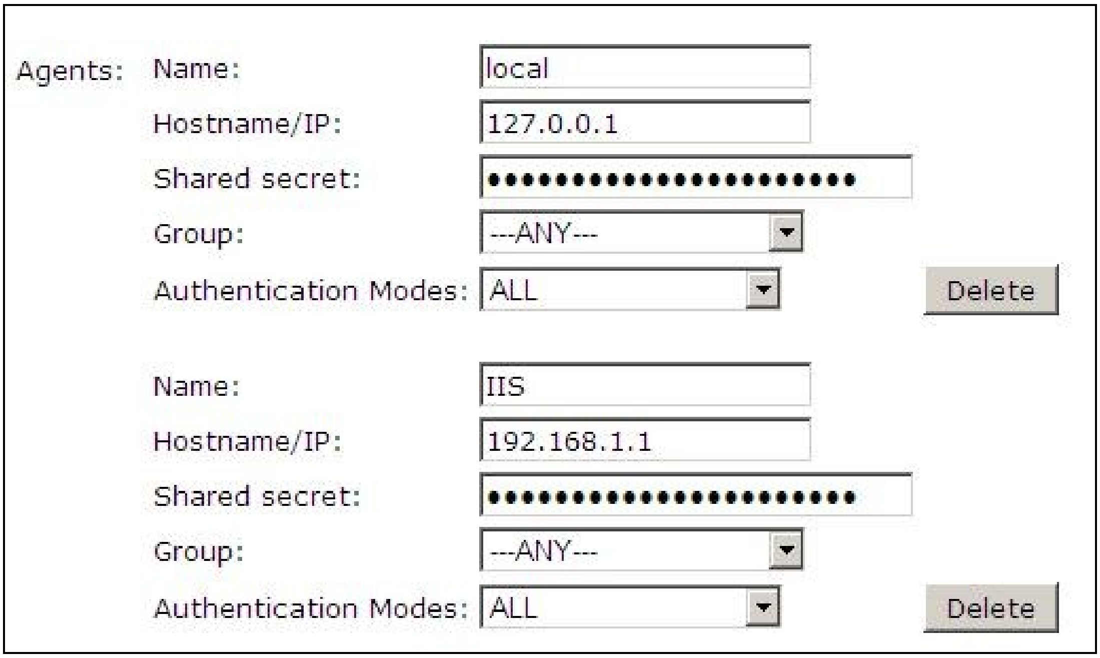
1. On the PINsafe Management Console select Server/Agent

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:

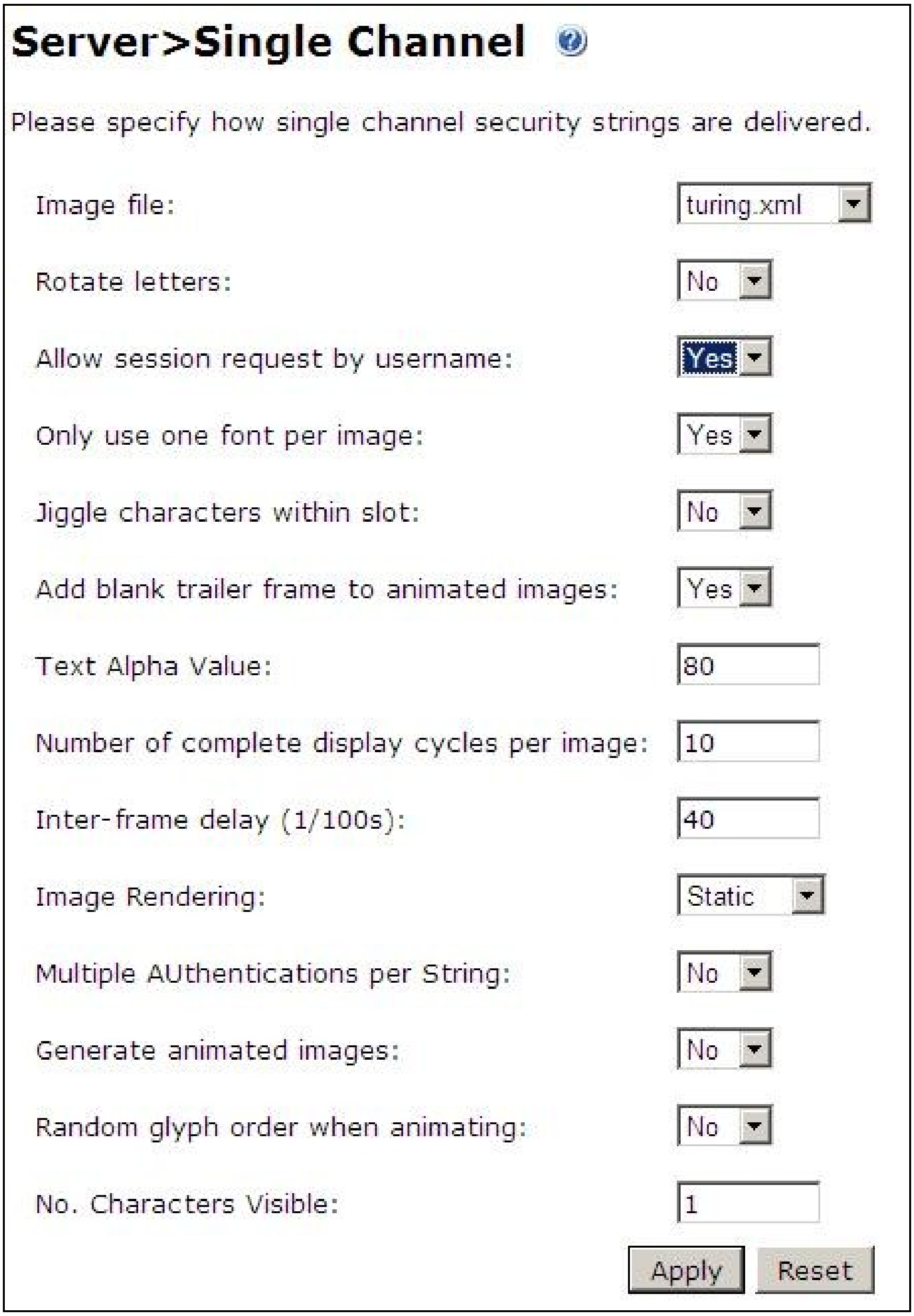
Name: local
Hostname/IP: 127.0.0.1
Shared secret: ●●●●●●●●●●●●●●●●●●●●●●●
Group: ---ANY---
Authentication Modes: ALL

Name: IIS
Hostname/IP: 192.168.1.1
Shared secret: ●●●●●●●●●●●●●●●●●●●●●●●
Group: ---ANY---
Authentication Modes: ALL

153.3.2 Configure Single Channel Access

1. On the PINsafe 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:	turing.xml
Rotate letters:	No
Allow session request by username:	Yes
Only use one font per image:	Yes
Jiggle characters within slot:	No
Add blank trailer frame to animated images:	Yes
Text Alpha Value:	80
Number of complete display cycles per image:	10
Inter-frame delay (1/100s):	40
Image Rendering:	Static
Multiple AUthentications per String:	No
Generate animated images:	No
Random glyph order when animating:	No
No. Characters Visible:	1

154 Additional Installation Options

154.1 Modifying the login Page to stop the Single Channel Image automatically appearing

NOTE: this section refers to earlier versions of the filter. In version 2.6 or later, this can be set using the configuration program.

By default the single channel authentication will appear when the username and AD password is entered and the user selects the OTC field. As a single channel session has started the PINsafe server is expecting an OTC to be entered from the Single Channel TURing image. If dual channel authentication is required then the automatic display of the Single Channel Turing image needs to be turned off. This can be done by modifying the login.asp file which by default is located in C:\Program Files\Exchsrvr\exchweb\bin\auth. The following needs to be removed from the username attribute field:

```
onblur=?checkUser()?
```

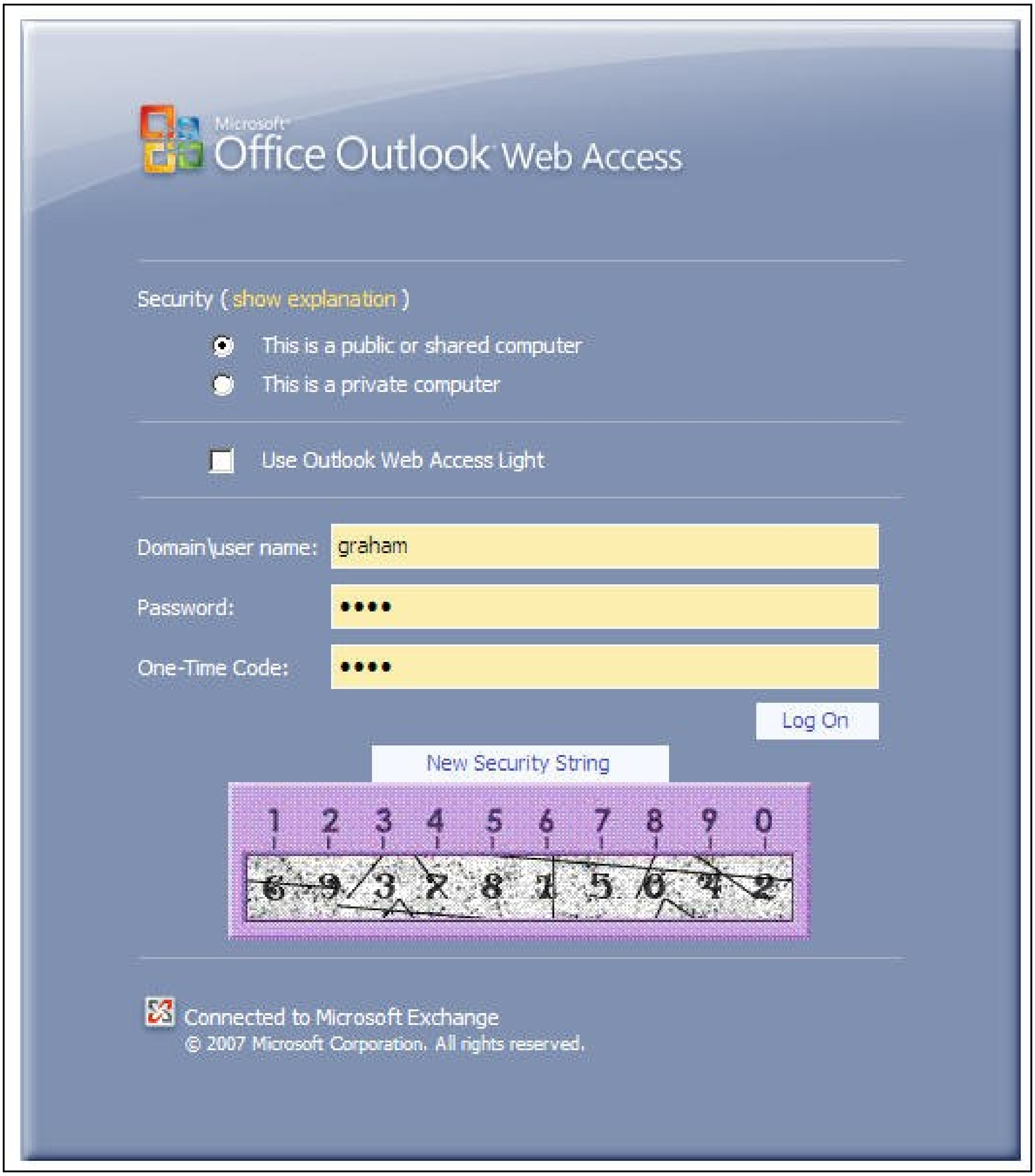
154.2 Modifying the login Page to allow Dual Channel On Demand Delivery

If you want to use only dual-channel on-demand and no other method, then you can manage this by a simple change to image.asp (under /exchweb/bin/auth). Edit this file, search for "SCImage" and replace it with "DCMessage". Leave the onblur attribute as it was. Dual channel authentication for the user and also On Demand Delivery should be enabled on the PINsafe Administration console under Server/Dual Channel.

155 Verifying the Installation

Enter a username and AD password then the PINsafe OTC for dual channel authentication. For single channel authentication enter the username, AD password then click on the button to generate a Single Channel Turing Security String, enter the OTC and login.

NOTE: if you have checked the option to allow non-PINsafe users, the OTC field and TURing button/image will not be displayed until you enter a username. If the username is not known to PINsafe, these elements will not appear. Similarly, if you have restricted the IP addresses to which PINsafe applies, the additional fields will not be displayed if PINsafe authentication is not required.



Security (show explanation)

● This is a public or shared computer

○ This is a private computer

□ Use Outlook Web Access Light

Domain\user name: graham

Password: ••••

One-Time Code: ••••

1 2 3 4 5 6 7 8 9 0

6 9 3 7 8 1 5 0 4 2

Connected to Microsoft Exchange

© 2007 Microsoft Corporation. All rights reserved.

156 Uninstalling the PINsafe Integration

Uninstall the PINsafe IIS filter then, the original Logon.aspx must be restored by renaming Logon.asp.old to Logon.aspx.

Note that the installation creates a new Logon.aspx file in ClientAccess\owa\auth\, and renames the original to login.aspx.sav. To complete uninstallation this file must be copied back again.

157 Troubleshooting

Check the PINsafe and 2007 server logs

Logon page takes a long time to load. The first time the OWA modification is started, the PINsafe page may take a while to load.

No login page, check the Exchange version in <path to Exchange>\ClientAccess\Owa

Look for folders consisting of 4 numbers separated by dots, for example "8.3.213.0". The first number will always be "8" for OWA 2007. You will need to ensure that the highest such folder is included in the list of excluded paths. In version 2.6 or higher, this should be handled automatically.

In version 2.0 of the filter, the file login.aspx needs to be modified so that it references the correct exchange install version. A program to automatically modify the login page is here. In versions 2.3 and higher, logon page modification is automatic.

1. Unzip and copy to <path to Exchange>\ClientAccess\Owa\auth.

2. Rename logon.aspx logon.aspx.current, rename logon.aspx.bk logon.aspx.

3. Open a command prompt and change directory to <path to Exchange>\ClientAccess\Owa\auth and run the OWAModifyLogonfor IIS program from in command line specifying logon.aspx i.e. *OWAModifylogonforIIS.exe logon.aspx*. If the option to allow authentication for non PINsafe users is being used then use the option switch *true*, e.g. *OWAModifylogonforIIS.exe logon.aspx true*. Using the option switch *false* will stop non PINsafe user authentication.

4. Check the file has been modified by the datestamp which should have changed for logon.aspx.

5. On the PINsafe IIS Filter Update the PINsafe filter under the Excluded path using the highest OWA version.

Red Cross instead of Turing image, right click on red cross and look at its properties. Ensure PINsafe server is running.

If you do not see a Turing image when using start session then in a web browser test the following link from the IIS server. If an image is not seen, then there is a problem either with communicating with the PINsafe server or the Allow Image request by username may be set to No.

For Swivel virtual or hardware appliances:

https://<pinsafe_server_ip>:8443/proxy/SCImage?username=<username>

For a software only install see Software Only Installation

Blank page after an authentication. A login page may be displayed on the Exchange server. Verify the settings on the PINsafe filter point to the DNS name:

Server URL: Exchange Server URL, Example: https://<exchange.mycompany.com>

Auth. URL: This is the URL for OWA authentication and the is usually https://<exchange.mycompany.com>/owa/auth/owaauth.dll

User regularly times out after a short interval

The session is kept open by user activity. If this is insufficient then increase the cookie idle timeout value.

157.1 Name resolution issue

The Exchange server may be looking for exchange.company.com from the internal network but cannot resolve it. Edit the hosts file mapping the name to 127.0.0.1. Note that because of security restrictions in OWA, the OWA server must be referred to by name, not by IP address, and the SSL certificate must be valid, and must be for the named host.

158 Known Issues and Limitations

Updates to the OWA 2007 server may require changes to the Excluded paths. You will also probably need to reapply the logon page changes.

If you wish to use the PINsafe filter with dual channel authentication, on demand or in advance, the logon page will need to be manually modified. Please contact Swivel support (support@swivelsecure.com) for more information.

159 Additional Information

For assistance in the PINsafe installation and configuration please firstly contact your reseller and then email Swivel Secure support at support@swivelsecure.com

160 Microsoft OWA 2010 IIS Integration

161 Introduction

Swivel allows users to authenticate users of Outlook Web Access (OWA) 2010 with Microsoft Exchange Server running on Microsoft 2008 server. Active Sync users are able to receive email without Swivel authentication as this uses a separate URL. This article describes how to integrate Swivel with OWA 2010.

162 Compatibility

Microsoft Exchange Version and update release	Build Version	Compatibility Status
Exchange Server 2010	14.0.639.21	Compatible (old release only)
Exchange Server 2010 SP1	14.1.218.15	Compatible
Update Rollup 1 for Exchange Server 2010 SP1	14.1.255.2	Compatible
Update Rollup 2 for Exchange Server 2010 SP1	14.1.270.1	Compatible
Update Rollup 3 for Exchange Server 2010 SP1	14.1.289.7	Compatible
Update Rollup 4 for Exchange Server 2010 SP1	14.1.323.6	Compatible
Update Rollup 5 for Exchange Server 2010 SP1	14.1.339.1	TBC
Update Rollup 6 for Exchange Server 2010 SP1	14.1.355.2	Compatible
Update Rollup 7 for Exchange Server 2010 SP1	14.1.421.2	Compatible
Exchange Server 2010 SP2	14.2.247.5	Compatible
Update Rollup 1 for Exchange Server 2010 SP2	14.2.283.3	TBC
Update Rollup 2 for Exchange Server 2010 SP2	14.2.298.4	TBC
Update Rollup 3 for Exchange Server 2010 SP2	14.2.309.2	TBC
Update Rollup 4 for Exchange Server 2010 SP2	14.2.318.4	TBC
Update Rollup 5 for Exchange Server 2010 SP2	14.2.328.5	Compatible
Update Rollup 5-v2 for Exchange Server 2010 SP2	14.2.328.10	Compatible
Update Rollup 6 for Exchange Server 2010 SP2	14.2.342.3	Compatible
Exchange Server 2010 SP3	14.3.123.3	Compatible
Update Rollup 7 for Exchange Server 2010 SP3	14.3.210.2	Compatible
Update Rollup 8 (v2) for Exchange Server 2010 SP3	14.3.224.2	Compatible

Note: Updates may result in the login page customisation being removed. In this case, you must select the option "Reapply Logon Page Changes" from the Swivel filter start menu. Updates to the 2010 server may also require changes to the Excluded paths. See the **Troubleshooting** and **Known Issues and Limitations** sections before updating.

163 Prerequisites

- Microsoft Exchange 2010 with OWA using IIS7
- Microsoft 2008 Server
- Swivel version 3.7 or later
- Users are able to login using standard OWA forms-based authentication.
- As the OWA server proxies the image request for Single channel TURing images and Pinpad, the Swivel server does not need a NAT.

The following is the latest release. Use this unless you have no Exchange service packs installed, in which case you need to use the older version, below. If you need a copy of an intermediate release for any reason, please contact support@swivelsecure.com.

163.1 Additional Prerequisites for Version 2.9

- Swivel Appliance version 3
- Microsoft .Net Framework 4.5 or later

NOTE: See notes below for additional installation requirements. Because of these additional requirements, it is recommended that you only upgrade to version 2.9 if you have a version 3 Swivel appliance.

164 File Downloads

Download links:

- Version 2.8
- Version 2.9

164.1 OWA Filter Change History

Recent changes:

- 2.9.0
    - ♦ Support for TLS 1.1 and 1.2. See notes below for additional requirements.
- 2.8.6
    - ♦ "Reapply Logon Page Changes" also updates default exclusions.
- 2.8.5
    - ♦ Fixed so that "/" is treated as a domain delimiter.
- 2.8.4
    - ♦ Change PIN page modified to show one field at a time.
- 2.8.3
    - ♦ Added hidden option to use previous authentication method.
    - ♦ Prevent Pinpad sessions being cached.
- 2.8.2
    - ♦ Fixed problem with names containing apostrophes.
- 2.8.1
    - ♦ Now supports direct upgrading - no need to uninstall a previous version before installing the new one. This only applies to upgrading from version 2.7 or later.
    - ♦ Change PIN Pinpad page selection of OTC field made more intuitive
    - ♦ Fix for bug introduced by changes in 2.7.7 when not using alternative usernames
- 2.7.7
    - ♦ Allow alternative usernames to work with versions of Swivel prior to 3.10 - see below.
    - ♦ Fixed some issues with Change PIN using Pinpad
- 2.7.6
    - ♦ Fixed problems with public/private flag
    - ♦ Changed Pinpad login to use session ID rather than username
- 2.7.1
    - ♦ Uses a slightly different authentication mechanism, since some users have reported problems with version 2.6.

Version 2.6 - if the new authentication mechanism causes problems with earlier service packs.

(Older release for OWA 2010 no service pack)

165 Architecture

The Exchange server makes authentication requests against the Swivel server by XML authentication

166 Installation

NOTE: it is only necessary (or indeed possible) to install on Microsoft Exchange Client Access Servers. No installation is required on back end servers.

166.1 Preparation for Installing Version 2.9

As noted above, you should only upgrade to version 2.9 if your Swivel appliance requires TLS 1.1 or 1.2, i.e. you have appliance version 3 or higher. Note that it is possible to enable support for TLS 1.0 on version 3 appliances, in order to support legacy applications, but for security reasons it is recommended that you do not do this.

Support for TLS protocol versions 1.1 and 1.2 require Microsoft.Net Framework version 4.5 or later and ASP.Net version 4.0. If your Microsoft Exchange server is running on Windows Server 2012 or later, you may already have this, but Server 2008 does not have the requsite .Net Framework installed by default.

Note that the following procedure will require that the Exchange web server is restarted, so a small amount of down time is expected.

Download and install the requisite framework from the Microsoft website, ensuring that ASP.Net support is enabled.

Open IIS manager, and go to Application Pools. Select each MSExchange... application pool, click Basic Settings and change the .Net Framework version to v4.0.30319 (the last number may be different).

Once you have updated all the MSExchange application pools to ASP.Net version 4, restart IIS.

166.2 Upgrading to Version 2.9

Version 2.9 uses a different installation mechanism from previous versions. For this reason, it is not possible to upgrade to 2.9 without uninstalling previous versions first. However, it is possible to keep the settings from the previous version as follows:

Under C:\Program Files\Microsoft\Exchange Server\V14\Owa\PINsafeConfig, locate and run ForceUninstall.exe as Administrator. If this program does not exist, you will need to use the alternative mechanism below. Type "yes" to confirm removal, then "n" to prevent the settings being removed. Note that this technique does not remove the program from Programs and Features. You should attempt to remove it from here also, and when you get a warning that the program cannot be removed, accept the option to remove it from the list.

If the ForceUninstall program does not exist, you can use the following manual method:

Under C:\Program Files\Microsoft\Exchange Server\V14\Owa, edit web.config. Search for "PINsafe settings". Copy everything from this line down to "End of PINsafe settings" into a new file and save it. Now uninstall as normal. After installing version 2.9, the configuration program will appear, with blank settings. Cancel this program, then edit web.config as before. You should have default settings for the Swivel filter installed. Remove these and replace with the saved settings. Now run the configuration program again and make any changes as necessary.

166.3 Software Installation

Run the executable to install it on the Exchange Server. If your Exchange Server instance is not installed in the default location (C:\Program Files\Microsoft\Exchange Server\V14), you will need to modify the installation path. The installation path should be the root Exchange path.

NOTE: it is not necessary to uninstall the previous filter before installing version 2.7.x or 2.8.x, as long as the previous filter is version 2.7 or later.

166.4 Configuration of the IIS Filter

After installation modify the settings. The Filter Configuration should start after installation or can be started through the Start Menu. If the Exchange Server installation is not in the default location, select the OWA directory as above in which to modify the web.config file.

166.4.1 Swivel Settings

Server Name/IP: The Swivel server IP address or hostname

Port: Swivel server port, for a Swivel virtual or hardware appliance use 8080 (not 8443)

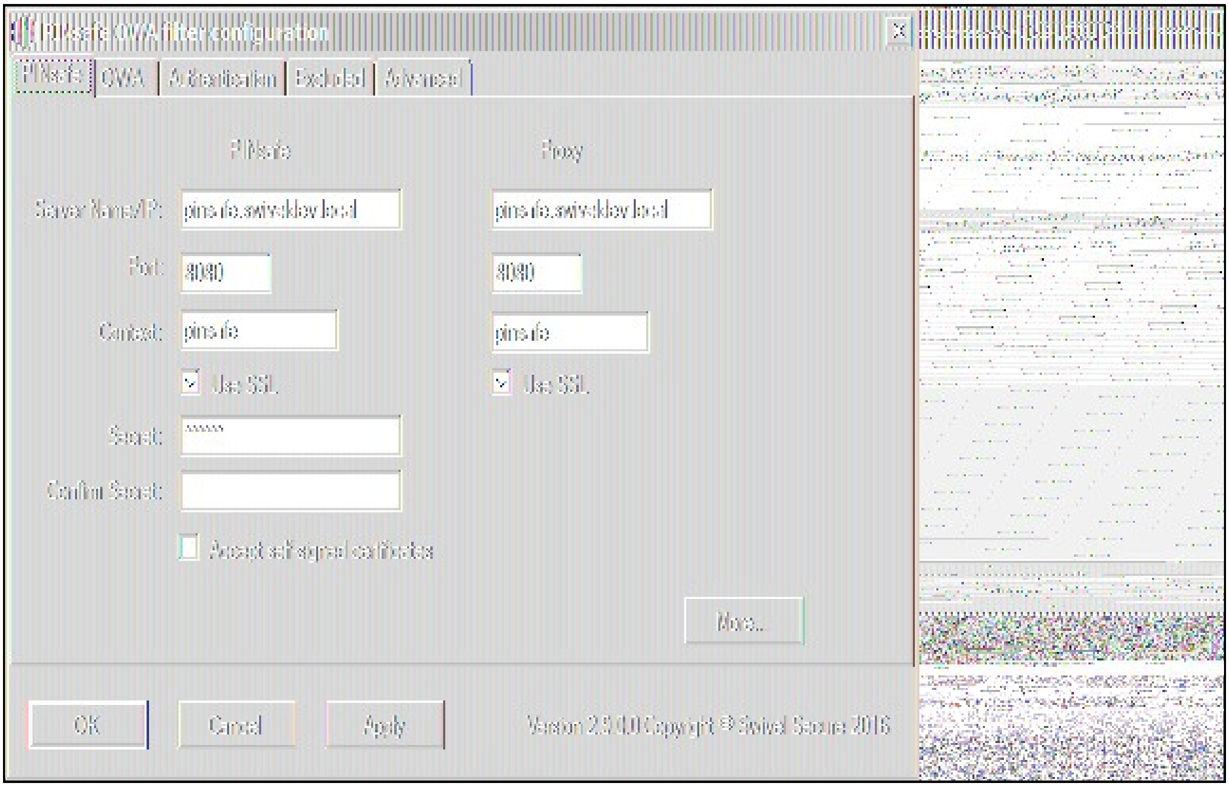
Context: Swivel install name, for a Swivel virtual or hardware appliance use pinsafe (not proxy)

Use SSL Select tick box if SSL is used, for a Swivel virtual or hardware appliance tick this box. This also ignores other certificate errors, such as site names not matching.

Secret: The shared secret that must be entered also on the Swivel server Administration Console under Server/Agents

Accept self-signed certificates Where SSL is used with self signed certificates, for a Swivel virtual or hardware appliance tick this box until a valid certificate is installed.

Proxy Server, Port, Context, Use SSL These are used to retrieve TURing or Pinpad images. If you are using a version of PINsafe that does not support Pinpad natively (3.9 or earlier), you will need the special version of the virtual or hardware appliance proxy that does support Pinpad. If you are not using Pinpad, you can set these to be the same as the first set of values: if you are not using a virtual or hardware appliance, you MUST set them to be the same.



PINsafe — Proxy

Server Name/IP: pinsafe.swivelkiev.local — pinsafe.swivelkiev.local

Port: 8080 — 8080

Context: pinsafe — pinsafe

☑ Use SSL — ☑ Use SSL

Secret: *****

Confirm Secret:

□ Accept self signed certificates

Version 2.5.0.0 Copyright © Swivel Secure 2016

166.4.2 OWA Settings

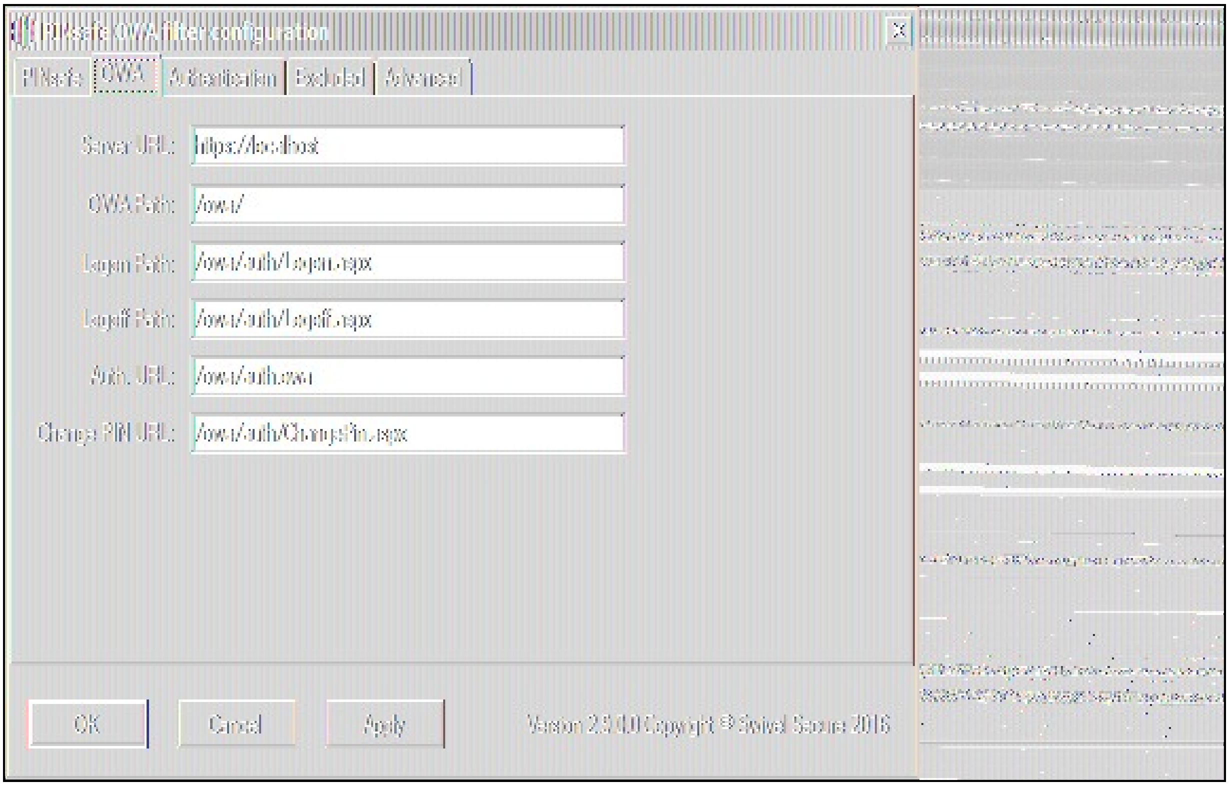
Server URL: Exchange Server URL, Example: https://<exchange.mycompany.com>

OWA Path: OWA path, usually /owa, unless this has been explicitly changed

Logon Path: Logon path Usually /owa/auth/Logon.aspx

Logoff Path: Logoff path /owa/auth/Logoff.aspx

Auth. URL: This is the URL for OWA authentication and is usually https://<exchange.mycompany.com>/owa/auth/auth.owa



Server URL: https://localhost

OWA Path: /owa/

Logon Path: /owa/auth/Logon.aspx

Logoff Path: /owa/auth/Logoff.aspx

Auth. URL: /owa/auth.owa

Change PIN URL: /owa/auth/ChangePin.aspx

Version 2.5.0.0 Copyright © Swivel Secure 2016

166.4.3 Authentication Settings

Cookie Secret Change: This is an experimental setting, which increases security by changing the secret used to encrypt the authentication cookie at a specified interval. It is recommended that you leave this at 0, i.e. never change it. In particular, do not change this if you have multiple OWA servers, as it will cause problems.

Idle Time: The length of time in seconds that the authentication cookie is valid, provided you make no OWA requests in that time. If you do, the cookie is refreshed and the countdown starts again. If users are being prompted for authentication after short time periods then this value may need to be increased.

Allow non-PINsafe Users If this option is ticked, non Swivel users are allowed to authenticate using standard OWA authentication. This requires Swivel 3.5 or higher. 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.

Filter Enabled The filter enabled option is mainly for testing, but also to handle situations such as enabling mobile access to the same Exchange Server i.e. ActiveSync and Windows Mobile Device Center. If the filter is disabled, you still need to authenticate through Swivel if you use the standard login page, but it is possible to authenticate using only AD credentials if you have a way to call the AD authentication filter directly.

Ignore Domain Prefix If this option is ticked, any prefixed domain (i.e. anything before the '\' character) is removed before sending the username to PINsafe. The full username is sent to OWA.

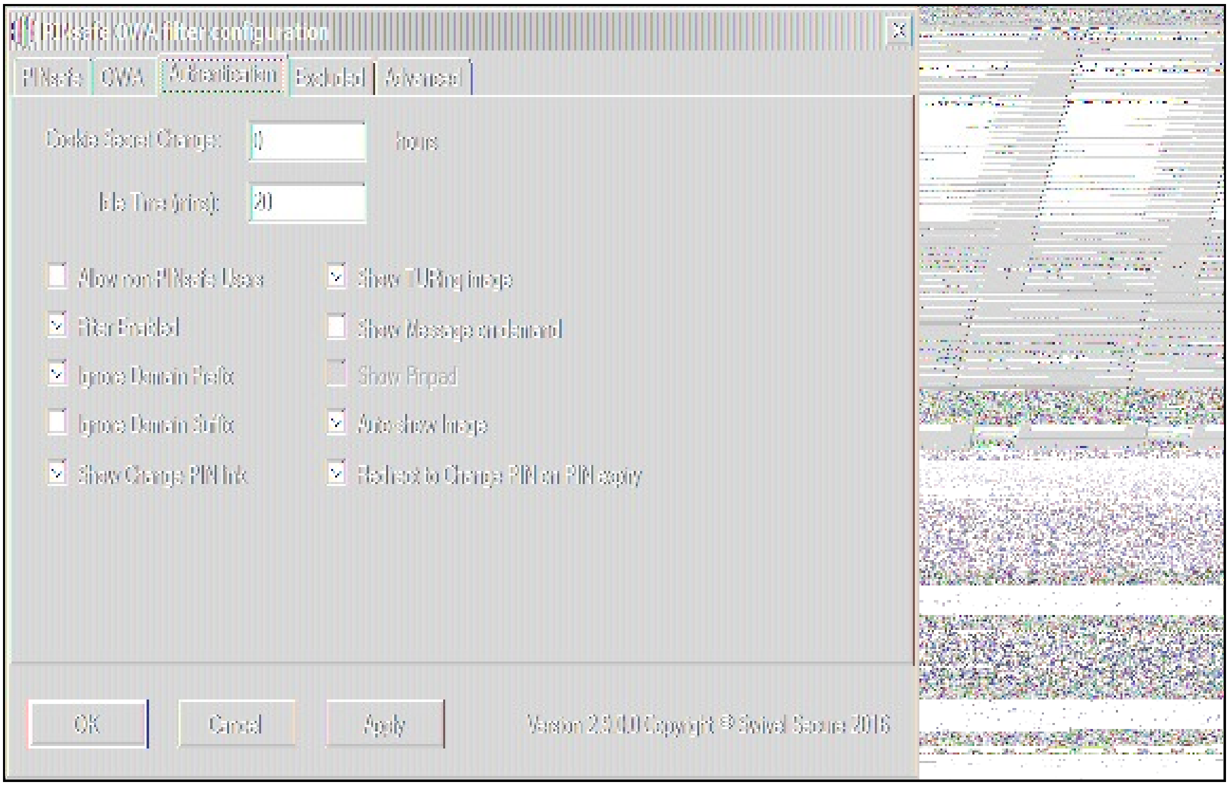
Ignore Domain Suffix If this option is ticked, any suffixed domain (i.e. anything after the '@' character) is removed before sending the username to PINsafe. The full username is sent to OWA.

Show TURing image If this option is ticked, a TURing image is shown to authenticate users.

Show Message on-demand If this option is ticked, a button is displayed to request a security string to be sent via SMS or email.

Show Pinpad If this option is ticked, an Pinpad button array is shown to authenticate users. You cannot have both TURing and Pinpad enabled.

Auto-show image If this option is ticked, the TURing or Pinpad image is requested as soon as the user enters the username and tabs away from it. If this option is not ticked, the user must click a button to show the image.



Cookie Secret Change: 0 hours

Idle Time (mins): 20

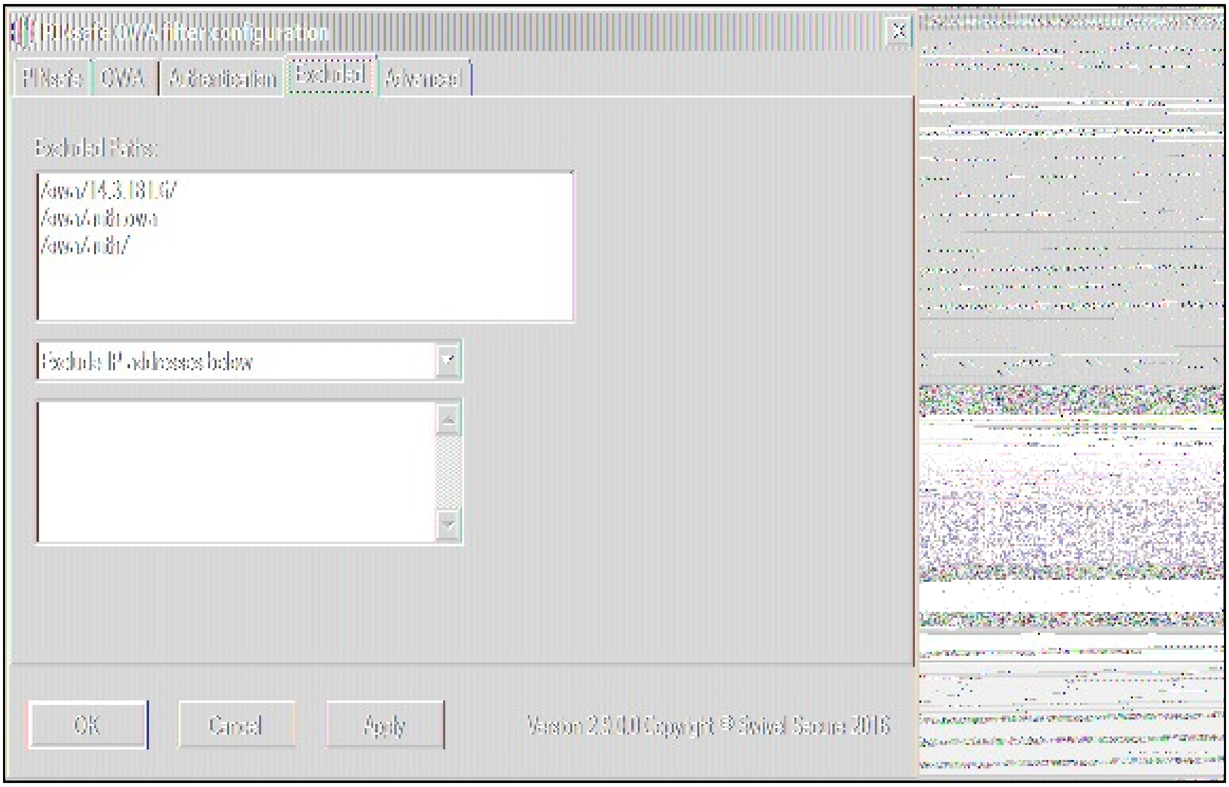
□ Allow non-PINsafe Users
☑ Filter Enabled
☑ Ignore Domain Prefix
□ Ignore Domain Suffix
☑ Show Change PIN link
☑ Show TURing image
□ Show Message on-demand
□ Show Pinpad
☑ Auto-show Image
☑ Redirect to Change PIN on PIN expiry

Version 2.5.4.0 Copyright © Swivel Secure 2016

166.4.4 Excluded Settings

Excluded Paths: This allows paths to be set for which authentication is not required to reach them. The paths shown on the display are added by default. The configuration program automatically detects the current build of OWA and includes that.

Excluded/Included IP addresses: You can choose to enable PINsafe authentication only for certain source IP addresses. Typically, you will do this if you wish to allow internal access to OWA without PINsafe authentication. Selecting "Exclude IP addresses below" will exclude the listed addresses from PINsafe authentication, while "Only include IP addresses below" will apply PINsafe authentication only to those IP addresses listed. For example, if you know that all external requests will come via a firewall at 192.168.0.99, you can select ?Only include IP addresses below?, and enter the single IP address as the address to include. Note that you can enter IP address ranges here using CIDR notation, for example 192.168.0.0/24 or 192.168.0.0/255.255.255.0. PINsafe will always display addresses using the latter format, irrespective of how they are entered. IPv6 addresses are not currently supported.



Excluded Paths:

/owa/14.3.181.6/
/owa/auth.owa
/owa/auth/

Exclude IP addresses below

Version 2.5.0.0 Copyright © Swivel Secure 2016

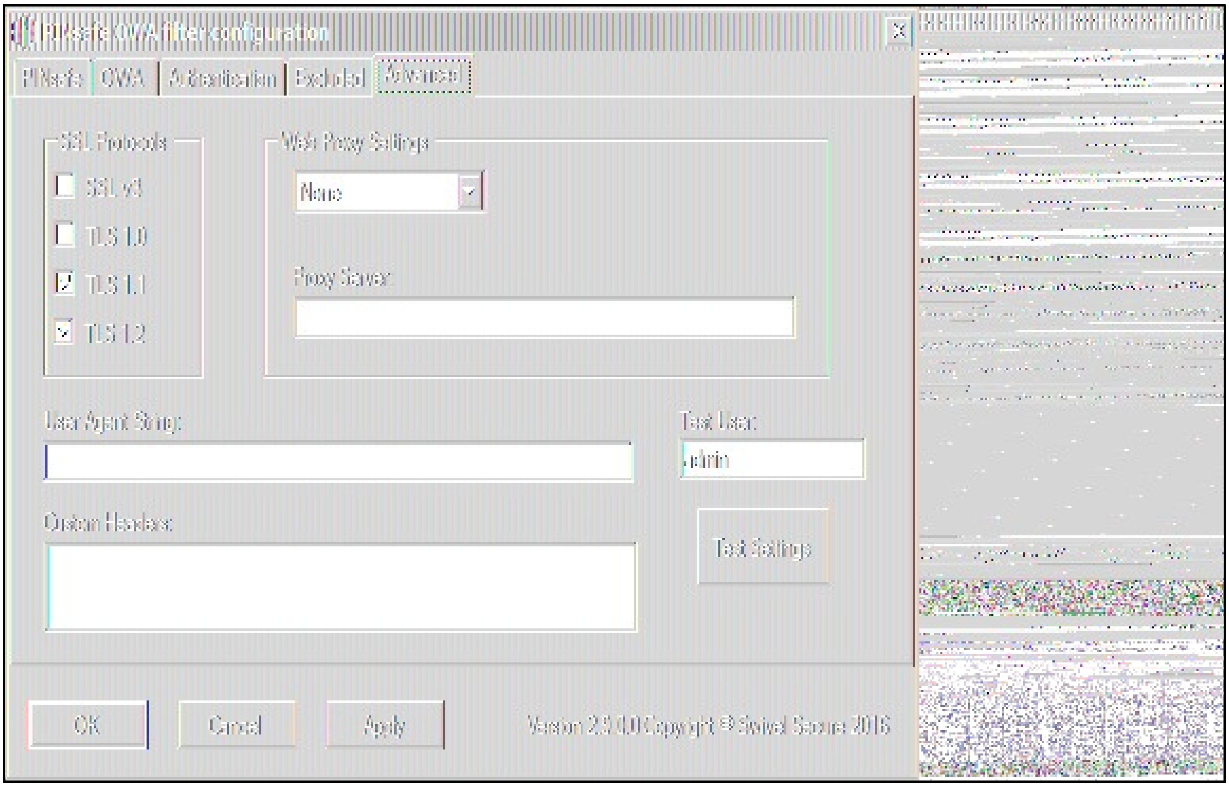
166.4.5 Advanced Settings

SSL Protocols: This indicates which protocols can be used for https communication with the Swivel server. The default allows SSLv3 and TLSv1, but the recommended setting for appliance version 3 is TLSv1.1 and TLSv1.2.

Web Proxy Settings: If the Exchange server needs to connect to a proxy server to access the Swivel server, you should specify the details here. Unless you are aware of such details, leave these as "None".

User Agent string: and **Custom headers:** These settings modify the http request sent to the Swivel server. Typically, you will not need to use these, but you may be aware of firewall rules between the servers which require such settings.

Test User: and **Test Settings** In order to test the settings, the configuration program will send a session start request on behalf of a user. You should enter a username that exists in the Swivel database (the default is 'admin'), then click Test Settings to confirm that the connection between the OWA Server and the Swivel server is correctly configured.


PINsafe OWA filter configuration

SSL Protocols

- □ SSL v3
- □ TLS 1.0
- ☑ TLS 1.1
- ☑ TLS 1.2

Web Proxy Settings: None

Proxy Server:

User Agent String:

Test User: admin

Custom Headers:

Version 2.8.0.0 Copyright © Swivel Secure 2016

166.5 Configure The Swivel Server

Configure a Swivel Agent (For standard XML Authentication)

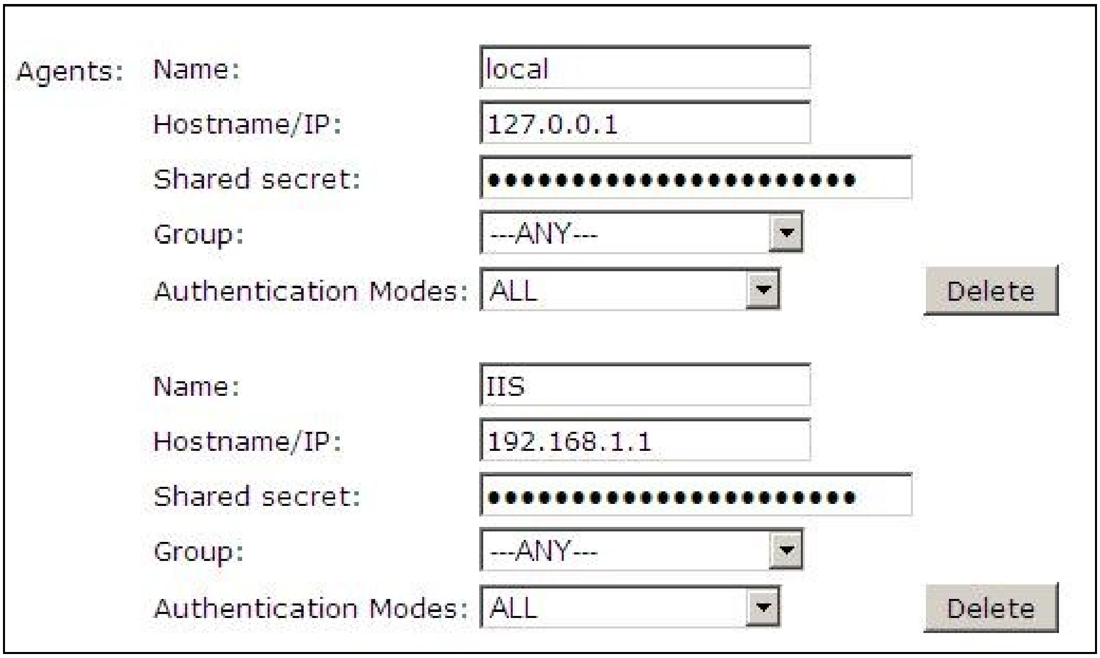
1. On the Swivel Management Console select Server/Agent

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

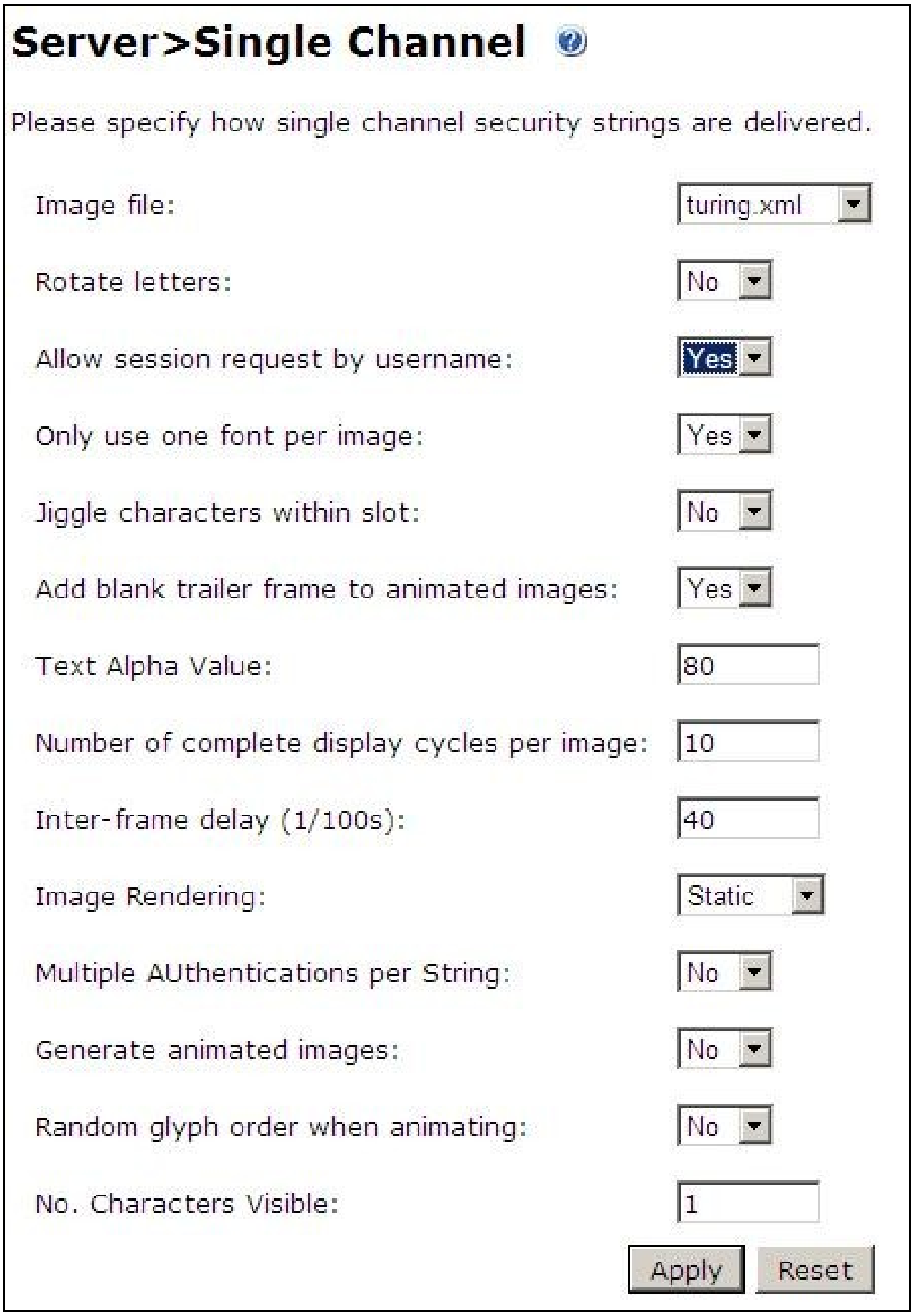

Agents:

Name:	local
Hostname/IP:	127.0.0.1
Shared secret:	••••••••••••••••••••••
Group:	---ANY---
Authentication Modes:	ALL
Name:	IIS
Hostname/IP:	192.168.1.1
Shared secret:	••••••••••••••••••••••
Group:	---ANY---
Authentication Modes:	ALL

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

166.6 Using additional attributes for authentication

When using additional attributes for authentication see User Attributes How To

167 Additional Installation Options

167.1 Modifying the login Page to stop the Single Channel Image automatically appearing

NOTE: this refers to older versions of the filter. In versions 2.5 and higher, this is set in the configuration program.

By default the single channel authentication will appear when the username and AD password is entered and the user selects the OTC field. As a single channel session has started the Swivel server is expecting an OTC to be entered from the Single Channel TURing image. If dual channel authentication is required then the automatic display of the Single Channel Turing image needs to be turned off. This can be done by modifying the login.asp file which by default is located in C:\Program Files\Exchsrvr\exchweb\bin\auth. The following needs to be removed from the username attribute field:

```
onblur=?checkUser()?
```

167.2 Modifying the login Page to allow Dual Channel On Demand Delivery

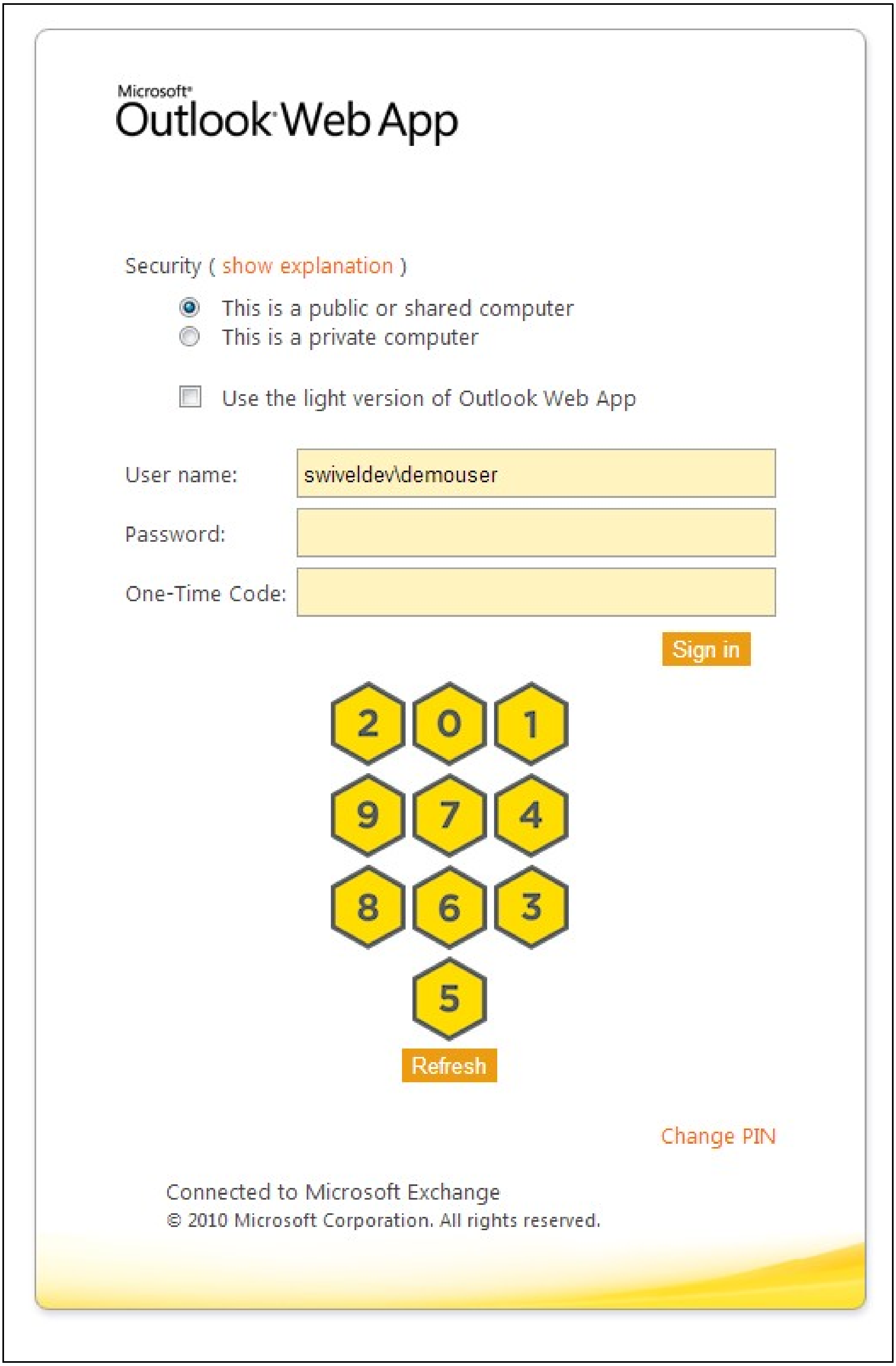
NOTE: this refers to older versions of the filter. In versions 2.5 and higher, this is set in the configuration program.

If you want to use only dual-channel on-demand and no other method, then you can manage this by a simple change to image.asp (under /exchweb/bin/auth). Edit this file, search for "SCImage" and replace it with "DCMessage". Leave the onblur attribute as it was. Dual channel authentication for the user and also On Demand Delivery should be enabled on the Swivel Administration console under Server/Dual Channel.

168 Verifying the Installation

Enter a username and AD password then the Swivel OTC for dual channel authentication. For single channel authentication enter the username, AD password then click on the button to generate a Single Channel Turing Security String, enter the OTC and login.

The below image shows the login page with PINpad.



Security (show explanation)

● This is a public or shared computer

○ This is a private computer

□ Use the light version of Outlook Web App

User name: swiveldev\demouser

Password:

One-Time Code:

Connected to Microsoft Exchange
© 2010 Microsoft Corporation. All rights reserved.

169 Uninstalling the Swivel Integration

Uninstall the Swivel IIS filter, this should restore all the original files. If it does not work then find the file Logon.aspx.sav located in ClientAccess\owa\auth\ which can be restored to the original Login.aspx.

WARNING: In versions of the filter earlier than 2.5, the login page customisation program did not check if the customisation was already done. This could cause the file Logon.aspx.sav to be overwritten with a customised page. In this case, you will need to locate another copy of the original file, or contact support@swivelsecure.com for assistance.

169.1 Uninstalling Manually

NOTE: This procedure should only be undertaken if uninstalling using the menu option (or Programs and Features) fails. For safety, you are advised to make copies of all modified or removed files to a safe location outside the Exchange Server installation.

Firstly, locate the OWA folder. The default location for this is C:\Program Files\Microsoft\Exchange Server\V14\ClientAccess\Owa.

Edit web.config in this folder: note that you may need to open your editor as Administrator in order to be able to change it. Search for the <modules> section. Within this, there should be a line such as the following:

```
 <add type="com.swivelsecure.owafilter.PINsafeOWAFilter, PINsafeOWAFilter, Version=2.8.5.1, Culture=neutral, PublicKeyToken=xxxx" name="PINsa
```

The Version number and PublicKeyToken may vary. Remove this line, making sure not to remove anything else.

Locate the section beginning with

and ending with

Remove everything within this section. If you intend to reinstall the filter later, you might want to copy these settings somewhere for later reference. Alternatively, make a backup of the entire web.config.

Save the modified web.config.

Restart IIS to release the Swivel filter.

Delete the folder "PINsafeConfig" and all its contents.

Go into the "Bin" subfolder and delete the 3 DLLs beginning with "PINsafe": PINsafeClient.dll, PINsafeLogin.dll and PINsafeOWAFilter.dll.

Go into the "auth" subfolder and delete the following files:

- ChangePIN.aspx
- CheckClient.aspx
- CheckUser.aspx
- pinpadBlank.png
- pinpadClear.png
- pinpadNext.png
- pinpadPrev.png
- pinpadRefresh.png
- pinsafe.js
- pinsafe_cp.js
- PINsafeLogon.aspx
- SCImage.aspx
- SCPinpad.aspx
- SessionStart.aspx
- turingBlank.jpg
- Logon.aspx.old

Depending on which version of the filter you have, you may not have all of these files.

The final step is to restore the original logon page. You should have a file named Logon.aspx.sav. If this file does not exist, please contact support@swivelsecure.com for help. Delete the file Logon.aspx, and rename Logon.aspx.sav to Logon.aspx.

Now test that your OWA logon works without Swivel. Some older versions of the filter would apply the logon page modification multiple times, which means that Logon.aspx.sav also had the Swivel modifications. If you find that the Logon page still has Swivel modifications, then please contact support@swivelsecure.com to request advice on restoring the original Logon page.

170 Change PIN

The OWA filter includes a page for the user to change their PIN. It can be configured to redirect to the change PIN page automatically if the user's PIN has expired, and you can also include a link to the Change PIN page on the login page.

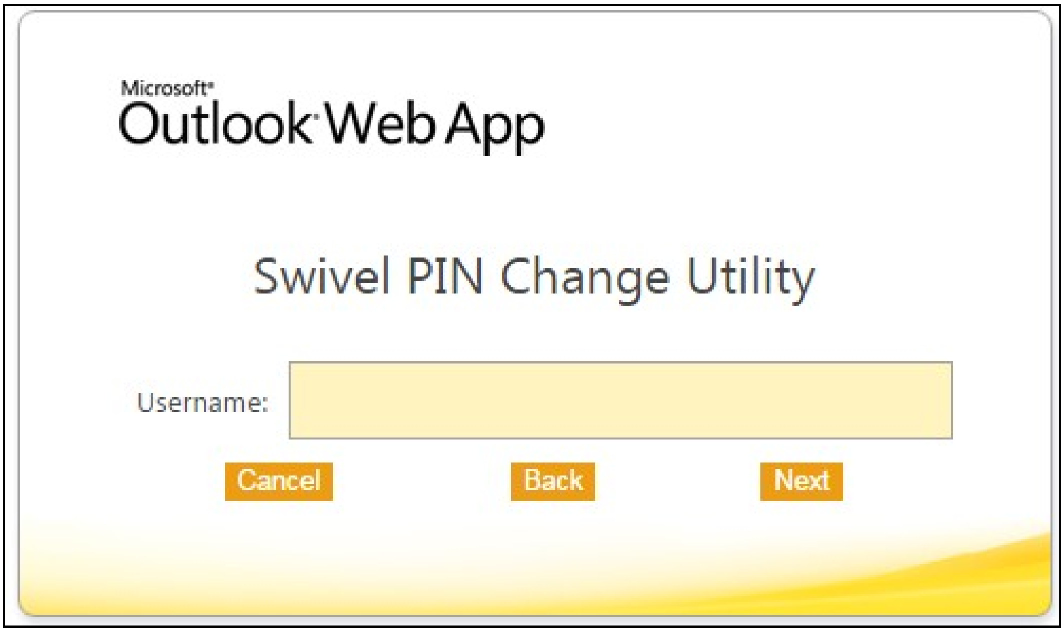
If you selected the Change PIN page in error, and want to return to the login page, then click the "Cancel" button ("Skip" button before 2.8.4) to return without changing your PIN.

NOTE: from version 2.8.4 onwards, the fields are shown one at a time. Click "Next" or press Tab to show the next field, or "Back" to go back and correct a field. See the Pinpad section below for example screen shots.

170.1 Change PIN with PinPad

The following instructions refer to the Change PIN page from version 2.8.4 onwards. See the following section for older versions.

The initial screen (with or without Pinpad) looks like this:

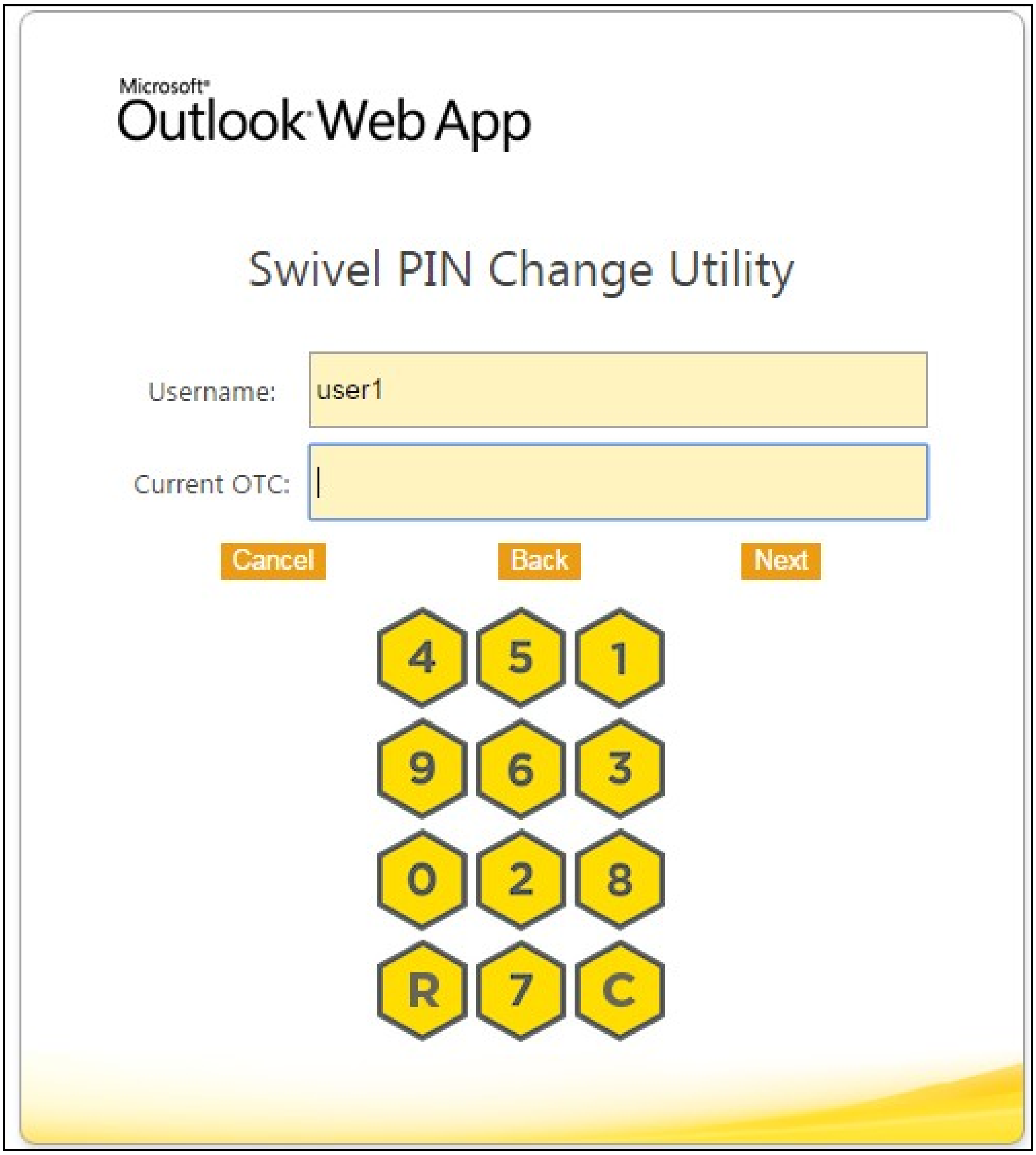


Microsoft® Outlook Web App

Swivel PIN Change Utility

Username:

Enter your username and click "Next" or press Tab to show the next field and the Pinpad:

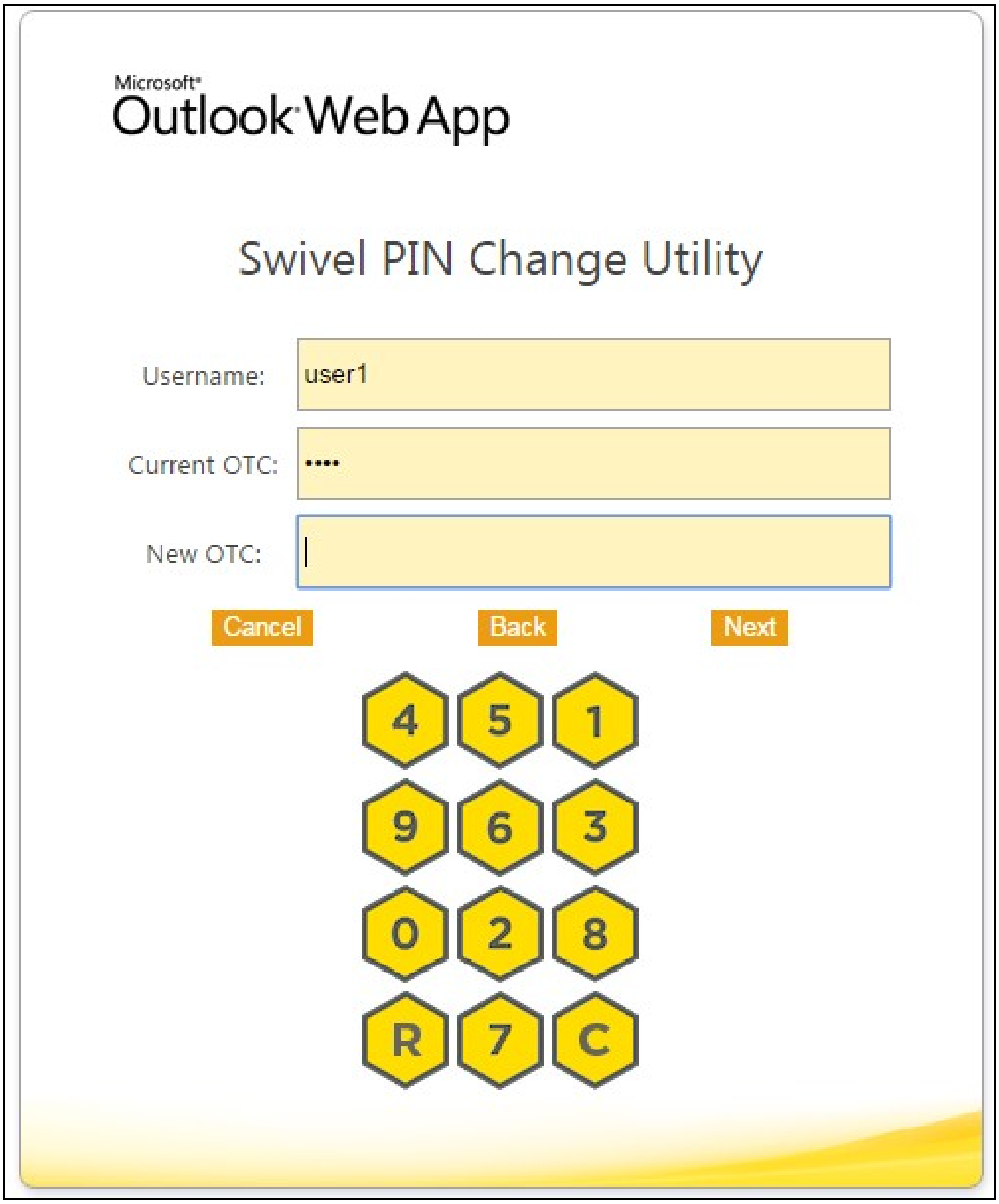


Swivel PIN Change Utility

Username: user1

Current OTC:

Click the buttons corresponding to the digits of your current PIN and then "Next":



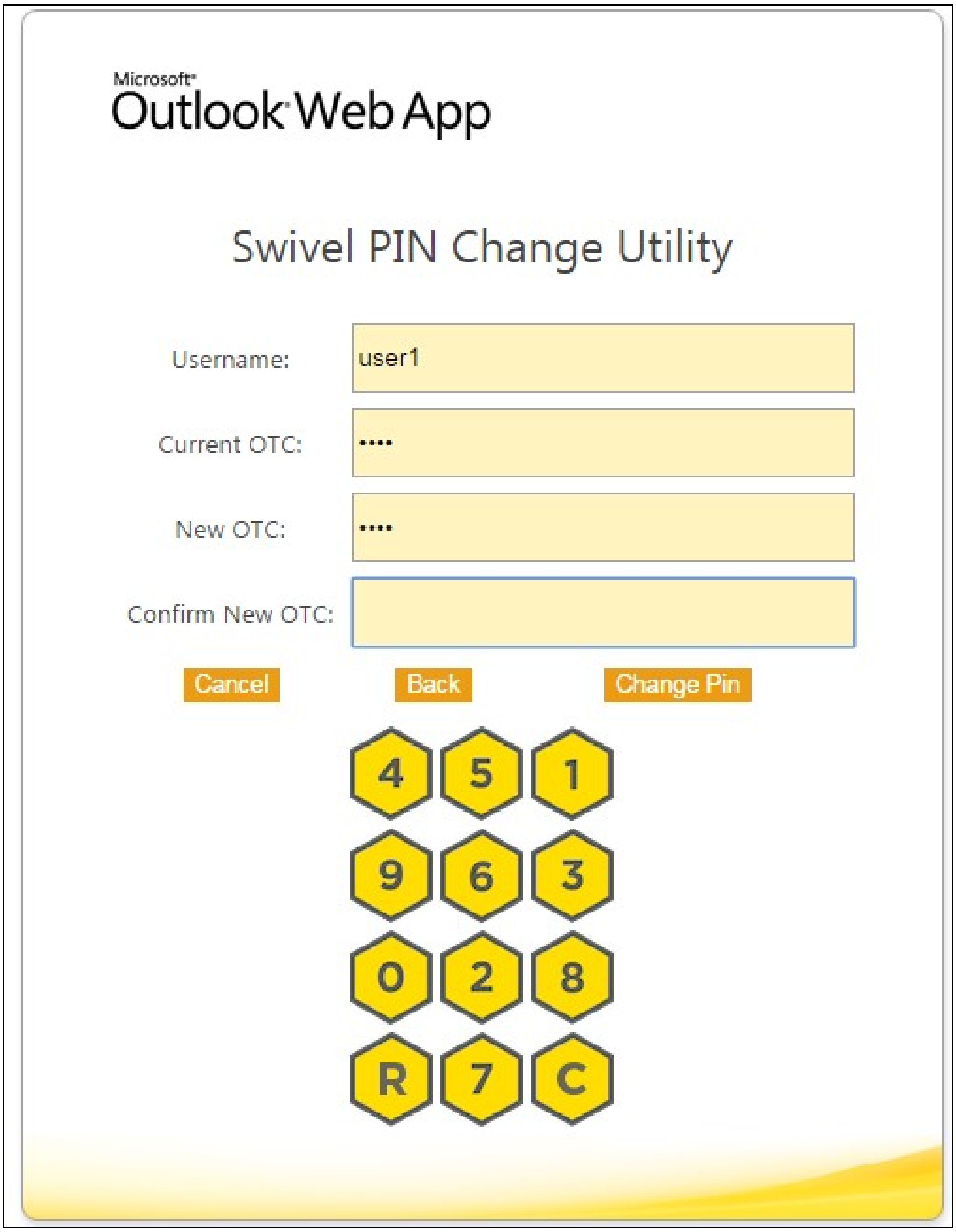
Swivel PIN Change Utility

Username: user1

Current OTC: ••••

New OTC:

Click the buttons corresponding to the digits of your new PIN and then "Next":



Swivel PIN Change Utility

Username: user1

Current OTC: ••••

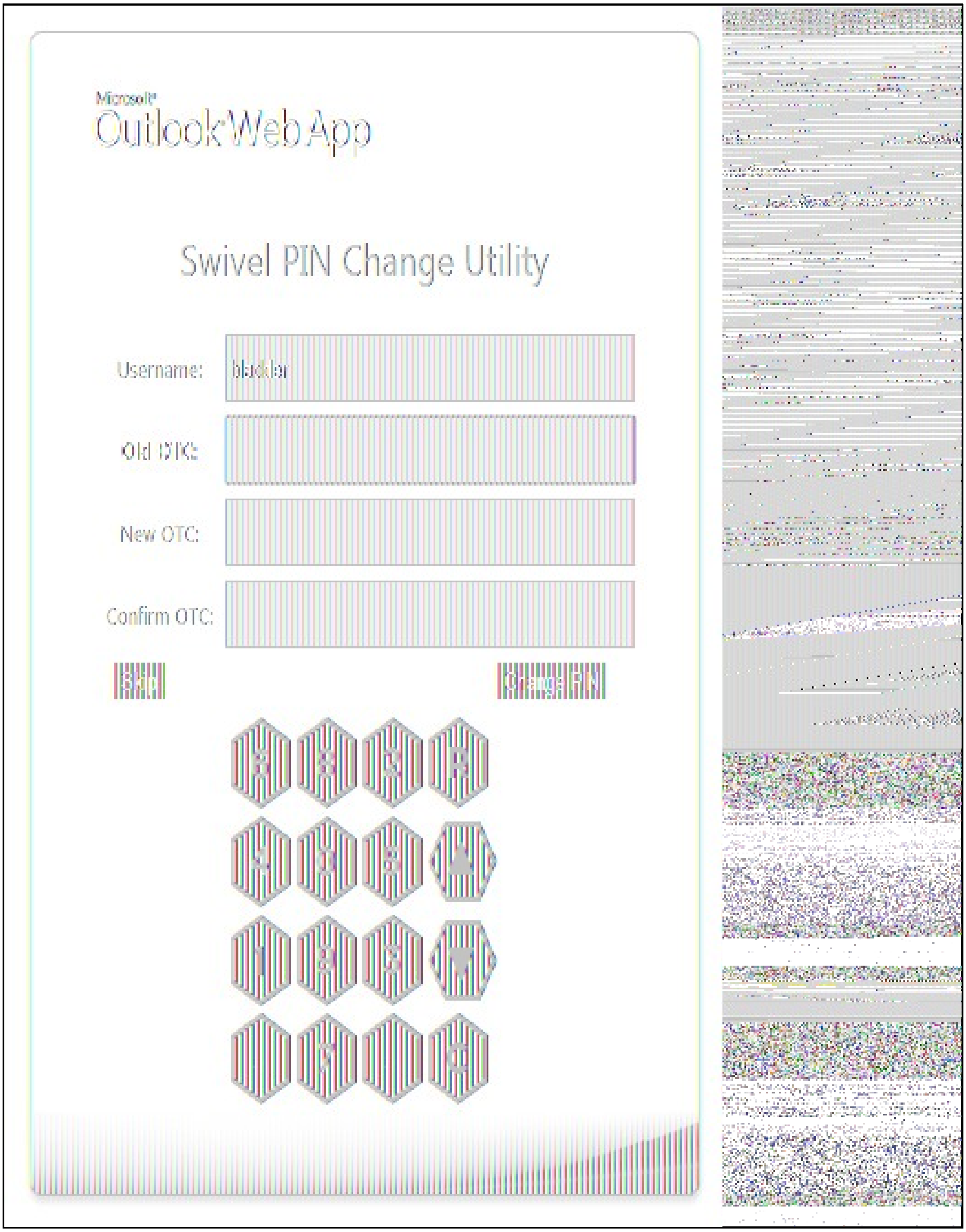
New OTC: ••••

Confirm New OTC:

Enter your new PIN again, to confirm, and then click "Change Pin".

170.1.1 PinPad prior to Version 2.8.4

When PinPad is enabled, there are 3 OTC fields, all of which can potentially use the Pinpad. For this reason, additional buttons are provided to select the field which is the target of the Pinpad:



Swivel PIN Change Utility

Username: blacker

Old OTC:

New OTC:

Confirm OTC:

You will notice that the current OTC field is highlighted in green. To select the next field, click on the down arrow button, or to go back to the previous field, click the up arrow button. You can also select an OTC field simply by clicking on it, or its label.

The "R" button will refresh the Pinpad (i.e. show a new pad), and the "C" button will clear the selected OTC field.

171 Troubleshooting

Check the Swivel and OWA server logs

No login page, check the Exchange version. The filter needs to match the Exchange version number, and the file login.aspx needs to be modified so that it references the correct exchange install version.

Red Cross instead of Turing image, right click on red cross and look at its properties. Ensure Swivel server is running.

If you do not see a Turing image when using start session then in a web browser test the following link from the OWA server. If an image is not seen, then there is a problem either with communicating with the Swivel server or the Allow Image request by username may be set to No.

For Swivel virtual or hardware appliances and software installs:

http(s)://<pinsafe_server_ip>:8080/pinsafe/SCImage?username=<username>

171.1 Enabling debug logging

Additional logging can be configured for troubleshooting, and will log from the time it was enabled.

edit C:\Program Files\Microsoft\Exchange Server\v14\ClientAccess\OWA\web.config

Locate

<add key="PINsafeEnableDebug" value="true" /> <add key="PINsafeDebugLocation" value="C:\Users\Public\Documents\PINsafeOWAFilter.log" />

171.2 User regularly times out after a short interval

The session is kept open by user activity. If this is insufficient then increase the cookie idle timeout value.

171.3 Turing image appears but user cannot authenticate

Verify that the OWA is configured to use port 8080 and context pinsafe. Port 8443 and context proxy will cause problems with authenticating users but allow the Turing image to be displayed. Note that this refers to the main PINsafe settings (for version 2.6 or higher) - the proxy settings SHOULD have these values if required.

171.4 User Authenticates Successfully to Swivel but OWA Login Page is Redisplayed

If you have entered the correct credentials, and the Swivel logs show successful authentication, but you are still redirected to the login page, the problem might be related to host names and/or SSL certificates.

First of all, if you connect to OWA using the IP address, or "localhost" from the OWA server itself, the Swivel filter will redirect you to the host name configured in the filter. This may result in the authentication cookie being lost, because the domain name doesn't match. In this case, attempting to authenticate a second time, with the correct host name, should succeed.

The second possibility is that the SSL certificate on the OWA Server doesn't match the host name used by the OWA filter, or the certificate has expired or is not trusted. This will result in authentication to OWA, from the Swivel filter, failing.

The solution for a production server is to ensure that the Exchange Server has a commercial SSL certificate, and that the Swivel OWA filter uses the host name that matches this.

For a development environment, you can generate a self-signed certificate with the correct host name, and add this to the list of trusted certificates on both the OWA server itself and the client (the latter might not be necessary). You might also need to add the host name to the hosts file on one or both of these.

NOTE: Version 2.7 or later of the filter should eliminate most of these problems. If you are still having problems of this nature with 2.7, please contact support@swivelsecure.com.

171.5 Name resolution issue

The Exchange server may be looking for exchange.company.com from the internal network but cannot resolve it. Edit the hosts file mapping the name to 127.0.0.1. Also ensure that the internal CA certificate is trusted by the OWA server.

Again, this problem is no longer relevant in version 2.7 onwards.

172 Known Issues and Limitations

172.1 Known Issues with Version 2.9

It has been observed that the first time the website is accessed after installing the 2.9 filter, an error page is seen. This disappears after refreshing the page, and does not appear to recur.

172.1.1 Problems With Connection Settings

We have experienced problems with installations of the filter when Exchange 2010 is installed on Windows Server 2012, or when certain security updates are installed in Windows Server 2008. While the exact cause is not yet known, it seems to be related to SSL connection settings. We have found success in making adjustments to the SSL settings and User Agent string.

There is a beta release of version 2.8.7 available from here which allows you to adjust these settings.

172.1.2 Default Exclusions Not Applied

There is a known issue with versions up to 2.8.5 that if you apply an update to Exchange that causes the Exchange version number to change, the folder containing the latest version of images etc. is not automatically added to the list of exclusions. Even though it is shown in the configuration program, it isn't saved.

The recommended solution is to update to 2.8.6. Here, if you reapply the logon changes after an update, it will also update the version-specific inclusions.

The workaround for this is to alter another configuration item, then save the configuration. You can subsequently change the other item back again, but making another change will force the exclusions to be updated.

172.1.3 One-time Code Not Shown

There is a known issue if you are using the option to allow unknown users to log on without Swivel credentials. With certain versions of the core, users are not recognised, even though they are known to exist in the Swivel database.

Another problem, Swivel may not recognise email addresses if the Swivel username is not the email address.

Both of these problems can be resolved by the same solution: you need to use a hidden option:

Edit the OWA web.config file (by default in C:\Program Files\Microsoft\Exchange Server\V14\ClientAccess\Owa). Note that you will probably need to open your text editor as Administrator in order to save changes.

Locate the following line:

```
<add key="PINsafeMultiUsername" value="False" />
```

If the above line is found, change value to "True".

If you cannot find the above line, search for

Insert the following line before the above line:

```
<add key="PINsafeMultiUsername" value="True" />
```

Note that this option will not work with versions of PINsafe earlier than 3.8.

172.1.4 Private Computer Option Doesn't Stay Selected

If your login page always defaults to Public computer and you have to select Private every time you log in, please upgrade to the latest version of the filter.

172.1.5 Swivel Customisation Lost

Updates may result in the login page customisation being removed. In this case, you must select the option "Reapply Logon Page Changes" from the Swivel filter start menu. IMPORTANT: in versions earlier than 2.5, make sure you do not use this option on a page that has already been customised. This will cause the page to become corrupted, and will also overwrite the backed up, unmodified file.

Updates to the 2010 server may also require changes to the Excluded paths. In version 2.8.6 or later, running "Reapply Logon Page Changes" fixes this too. In version 2.5 or later, the updates are handled by the configuration program, but if you do not change any other settings, the update will not be applied.

172.1.6 Later Versions of the Filter Not Working With Service Pack 1

We have had reports of the latest filter not working with Exchange Server Service Pack 1. The recommended solution is to upgrade to the latest service pack, but you might like to try the following (version 2.8.3 or later):

Insert the following line in web.config (see description above):

```
<add key="PINsafeUseOldAuthentication" value="True" />
```

This option reverts to the authentication mechanism used in version 2.6 and earlier. It is not known whether this is the cause of the problems seen, but it has been shown to work in some installations.

172.1.7 Logging

By default, the filter does not record any audit information, but it may be useful to do so for monitoring and debugging purposes. You can enable logging by adding the following line in web.config:

```
<add key="PINsafeEnableDebug" value="True" />
```

This writes logs to C:\Users\Public\Documents\PINsafeOWAFilter.log. You can change the file location with the following option:

```
<add key="PINsafeDebugLocation" value="FullFilePath" />
```

Replace *FullFilePath* above with the full path of the file to write to. Make sure that the account that OWA is running as has write permissions to that file/folder. </nowiki>

173 Multiple Swivel Servers

Versions 2.5 and later include the option to add multiple Swivel servers. Then, if the first one is unavailable, the filter will try the other servers in the order listed. The filter will always remember the last Swivel server successfully contacted and try that one first.

To support multiple servers, there is an additional button on the Swivel tab of the configuration program, which brings up a secondary dialogue containing a list of available servers. Use this to add or delete Swivel servers, and to select one to modify (the details are modified on the main dialogue).

174 Additional Information

For assistance in the Swivel installation and configuration please firstly contact your reseller and then email Swivel Secure support at support@swivelsecure.com.

175 Microsoft OWA 2013 IIS Integration

176 Introduction

Swivel allows users to authenticate users of Outlook Web Access (OWA) 2013 with Microsoft Exchange Server running on Microsoft 2012 server. Active Sync users are able to receive email without Swivel authentication as this uses a separate URL. This article describes how to integrate Swivel with OWA 2013.

So far as the Swivel integration is concerned, there are no significant differences between OWA 2013 and 2016 or 2019. Therefore, the OWA 2013 filter should work with OWA 2016 and 2019 as well.

177 Compatibility

Microsoft Exchange Version and update release	Build Version	Compatibility Status
Exchange Server 2013	15.0.516.32	Compatible
Exchange Server 2013 CU 3	15.0.775.38	Compatible
Exchange Server 2016	15.1.225.42	Compatible
Exchange Server 2019	15.2.858.5	Compatible

Note: Updates may result in the login page customisation being removed. In this case, you must select the option "Reapply Logon Page Changes" from the Swivel filter start menu. Updates to the 2013 server may also require changes to the Excluded paths. See the **Troubleshooting** and **Known Issues and Limitations** sections before updating.

178 Prerequisites

- Microsoft Exchange 2013 or 2016 with OWA
- Microsoft 2012 Server R2
- Microsoft.Net Framework version 4.5
- Swivel 3.7 or later
- Users are able to login using standard OWA forms-based authentication.
- * As the OWA server proxies the image request for Single channel TURing images and Pinpad, the Swivel server does not need a NAT.

NOTE: above is the test environment used for the filter. It will probably work with earlier versions of the Operating System (e.g. 2008), as long as version 4.5 of the .Net framework is installed.

179 File Downloads

- Version 2.12. Changes:
    - Settings are retained on upgrade of this product or of OWA: the settings are now saved to a location outside the OWA folder (C:\ProgramData\Swivel Secure\OWA Filter). Note that this doesn't apply to upgrade from a version earlier than 2.12.
    - Support for logging within the configuration program. Logs are written to C:\ProgramData\Swivel Secure\OWA Filter.
    - Version 2.12.3 ensure that data folder exists before trying to read from it.
    - Version 2.12.2: Bug in program to re-apply logon page changes after OWA upgrade now fixed.
    - Version 2.12.2: control over which attributes are checked for unknown users
    - Version 2.12.2: more control over logging
    - Version 2.12.2: fixed issue with Cookie encryption
- Version 2.11. The main change here is support for Push authentication. Due to technical issues, this version is available from a server that does not have https support. For this reason, you cannot simply click on the link in most browsers. Instead, you must right-click on it, copy the link address and open it in a new tab.
- Version 2.10. This is largely a rebranding of version 2.9. It also uses default settings that are more relevant for newer versions of Sentry, and references OWA 2016 and 2019. One notable change is that the reference to proxy server has been removed, as it is no longer necessary.

NOTE: We apologise that the original installer for version 2.10 was missing a file. This has now been corrected, but if you installed the original version and don't want to reinstall, you can simply unzip ChangePIN.aspx and place it in the swivel folder of the OWA web site. The usual location for this is C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\swivel.

- Version 2.9. This version includes support for TLS version 1.1 and 1.2. It is only necessary to upgrade to this version if you have a Swivel appliance version 3. Version 2 appliances work fine with version 2.8, and no other new features have been added.
- Version 2.8.7. Some minor updates copied from OWA 2010 filter, plus bug fix for images not displaying in certain circumstances. Now supports upgrading without uninstalling.

180 Architecture

The Exchange server makes authentication requests against the Swivel server by XML authentication

181 Installation

181.1 Software Installation

Run the executable to install it on the Exchange Server. If your Exchange Server instance is not installed in the default location (C:\Program Files\Microsoft\Exchange Server\V15), you will need to modify the installation path. The installation path should be the root Exchange path.

181.2 Configuration of the IIS Filter

After installation modify the settings. The Filter Configuration should start after installation or can be started through the Start Menu. If the Exchange Server installation is not in the default location, select the OWA directory as above in which to modify the web.config file.

181.2.1 Swivel Settings

Server Name/IP: The Swivel server IP address or hostname

Port: Swivel server port, for a Swivel appliance use 8080 (not 8443)

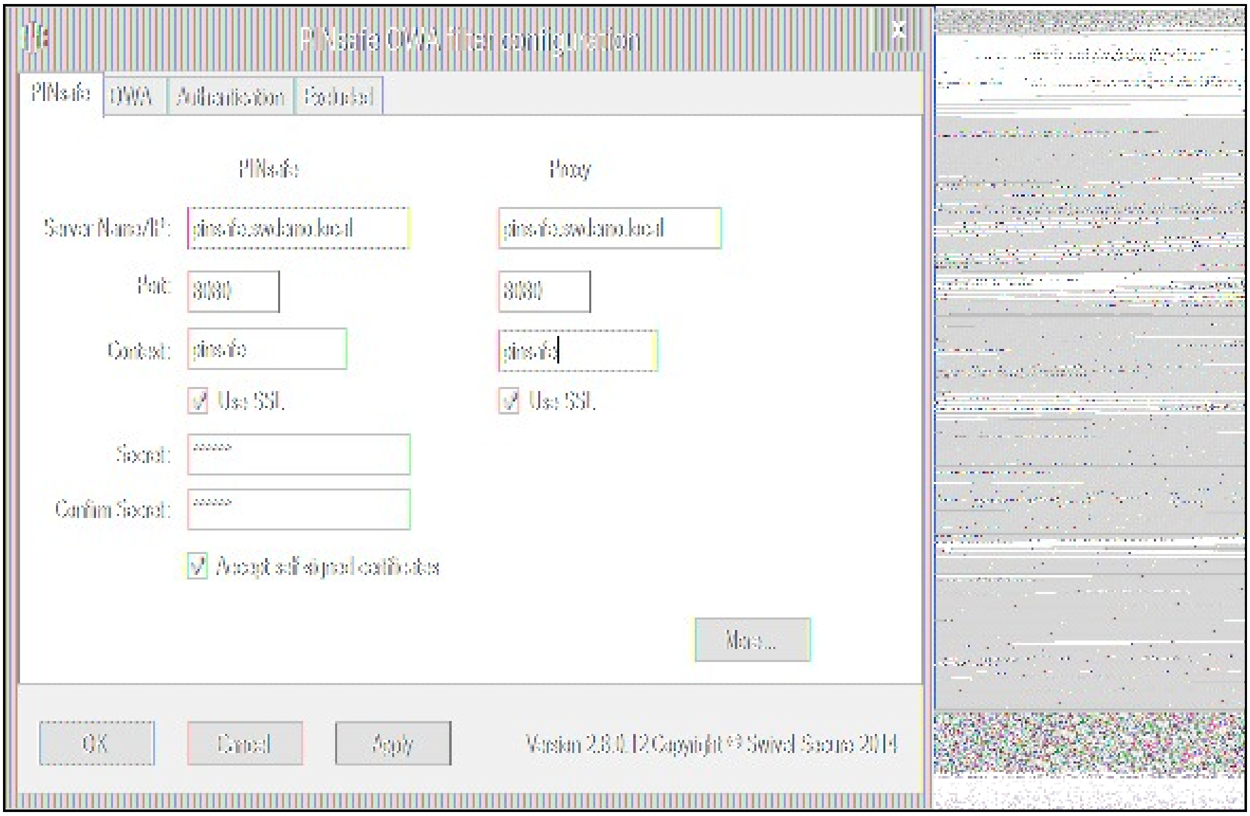
Context: Swivel install name, for a Swivel appliance use Swivel (not proxy)

Use SSL Select tick box if SSL is used, for a Swivel appliance tick this box. This also ignores other certificate errors, such as site names not matching.

Secret: The shared secret that must be entered also on the Swivel server Administration Console under Server/Agents

Accept self-signed certificates Where SSL is used with self signed certificates, for a Swivel appliance tick this box until a valid certificate is installed.

Proxy Server, Port, Context, Use SSL These are used to retrieve TURing or Pinpad images. If you are using a version of PINsafe that does not support Pinpad natively (3.9 or earlier), you will need the special version of the appliance proxy that does support Pinpad. If you are not using Pinpad, you can set these to be the same as the first set of values: if you are not using an appliance, you MUST set them to be the same. Version 2.10 removes the proxy settings altogether.



PINsafe

Server Name/IP: pinsafe.swlano.local

Port: 8080

Context: pinsafe

☑ Use SSL

Secret: ******

Confirm Secret: ******

☑ Accept self-signed certificates

Proxy

Server Name/IP: pinsafe.swlano.local

Port: 8080

Context: pinsafe

☑ Use SSL

Version 2.8.0.12 Copyright © Swivel Secure 2014

181.2.2 OWA Settings

Server URL: Exchange Server URL, Example: https://<exchange.mycompany.com>

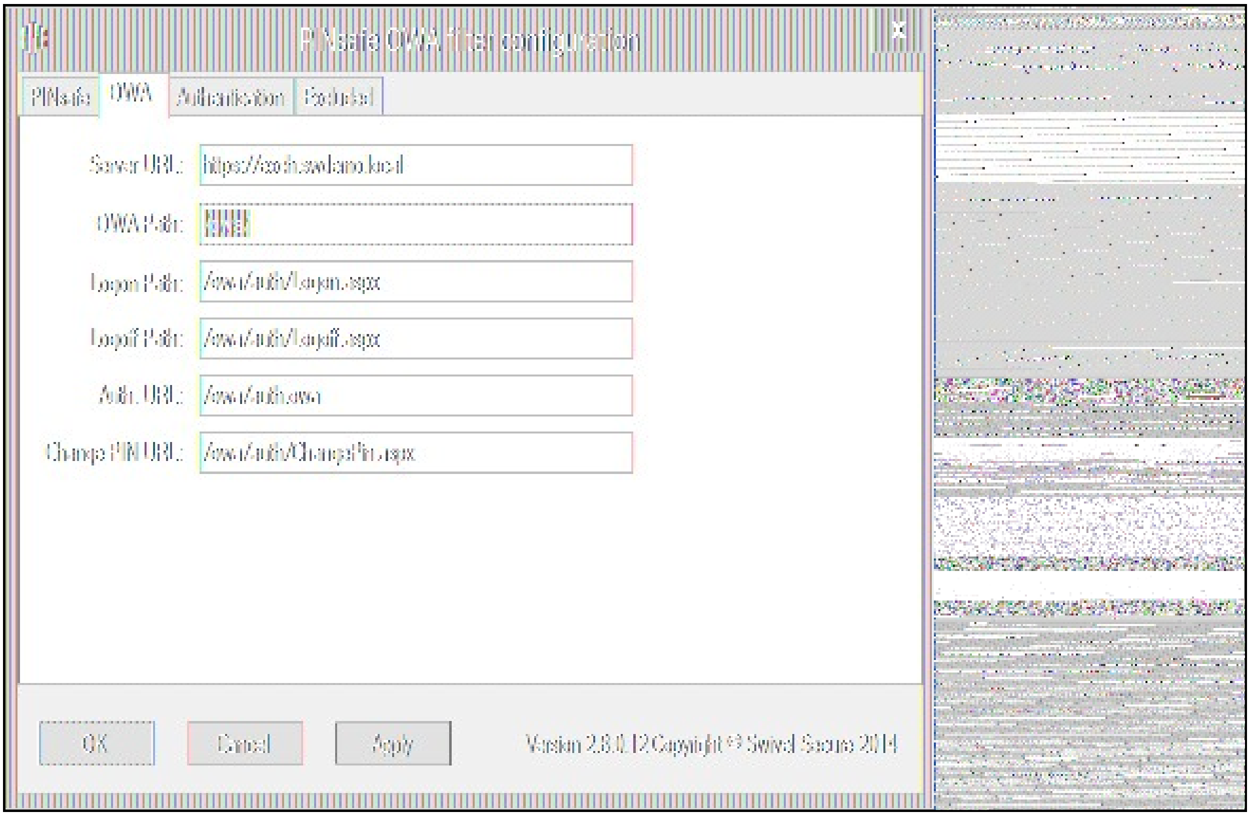
OWA Path: OWA path, usually /owa, unless this has been explicitly changed

Logon Path: Logon path Usually /owa/auth/Logon.aspx

Logoff Path: Logoff path /owa/auth/Logoff.aspx

Auth. URL: This is the URL for OWA authentication and is usually /owa/auth/auth.owa

Change PIN URL: This is the URL for the Change PIN page. Note that the default URL is actually incorrect, but this value is currently ignored anyway.



Server URL: https://auth.swlano.local

OWA Path: [illegible]

Logon Path: /owa/auth/Logon.aspx

Logoff Path: /owa/auth/Logoff.aspx

Auth. URL: /owa/auth.owa

Change PIN URL: /owa/auth/ChangePin.aspx

Version 2.8.0.12 Copyright © Swivel Secure 2014

181.2.3 Authentication Settings

Cookie Secret Change: This is an experimental setting, which increases security by changing the secret used to encrypt the authentication cookie at a specified interval. It is recommended that you leave this at 0, i.e. never change it. In particular, do not change this if you have multiple OWA servers, as it will cause problems.

Idle Time: The length of time in seconds that the authentication cookie is valid, provided you make no OWA requests in that time. If you do, the cookie is refreshed and the countdown starts again. If users are being prompted for authentication after short time periods then this value may need to be increased. The idle time on the Swivel OWA filter is in addition to the session timeout built into OWA. The Swivel timeout will never increase the OWA timeout, only reduce it. Therefore, it will not compromise the security of the public computer settings.

Allow non-PINsafe Users If this option is ticked, non Swivel users are allowed to authenticate using standard OWA authentication. This requires Swivel 3.5 or higher. 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.

Filter Enabled The filter enabled option is mainly for testing, but also to handle situations such as enabling mobile access to the same Exchange Server i.e. ActiveSync and Windows Mobile Device Center. If the filter is disabled, you still need to authenticate through Swivel if you use the standard login page, but it is possible to authenticate using only AD credentials if you have a way to call the AD authentication filter directly.

Ignore Domain Prefix If this option is ticked, any prefixed domain (i.e. anything before the '\' character) is removed before sending the username to PINsafe. The full username is sent to OWA.

Ignore Domain Suffix If this option is ticked, any suffixed domain (i.e. anything after the '@' character) is removed before sending the username to PINsafe. The full username is sent to OWA.

Show TURing image If this option is ticked, a TURing image is shown to authenticate users.

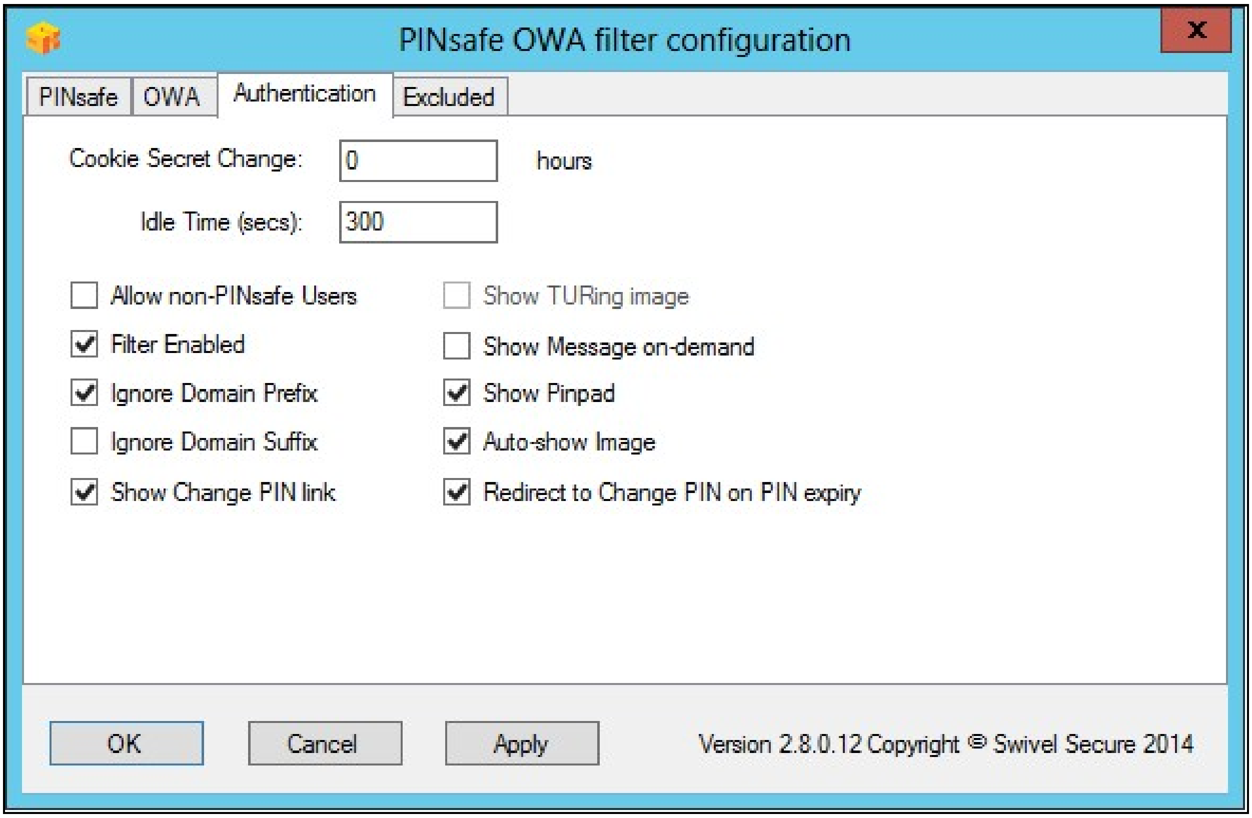
Show Message on-demand If this option is ticked, a button is displayed to request a security string to be sent via SMS or email.

Show Pinpad If this option is ticked, an Pinpad button array is shown to authenticate users. You cannot have both TURing and Pinpad enabled.

Auto-show image If this option is ticked, the TURing or Pinpad image is requested as soon as the user enters the username and tabs away from it. If this option is not ticked, the user must click a button to show the image.

Show Change PIN link If this option is ticked, a link to the Change PIN page will be shown on the login page.

Redirect to Change PIN on PIN expiry If this option is ticked, users are automatically redirected after successful login to the Change PIN page, if their PIN has expired.



Cookie Secret Change: 0 hours

Idle Time (secs): 300

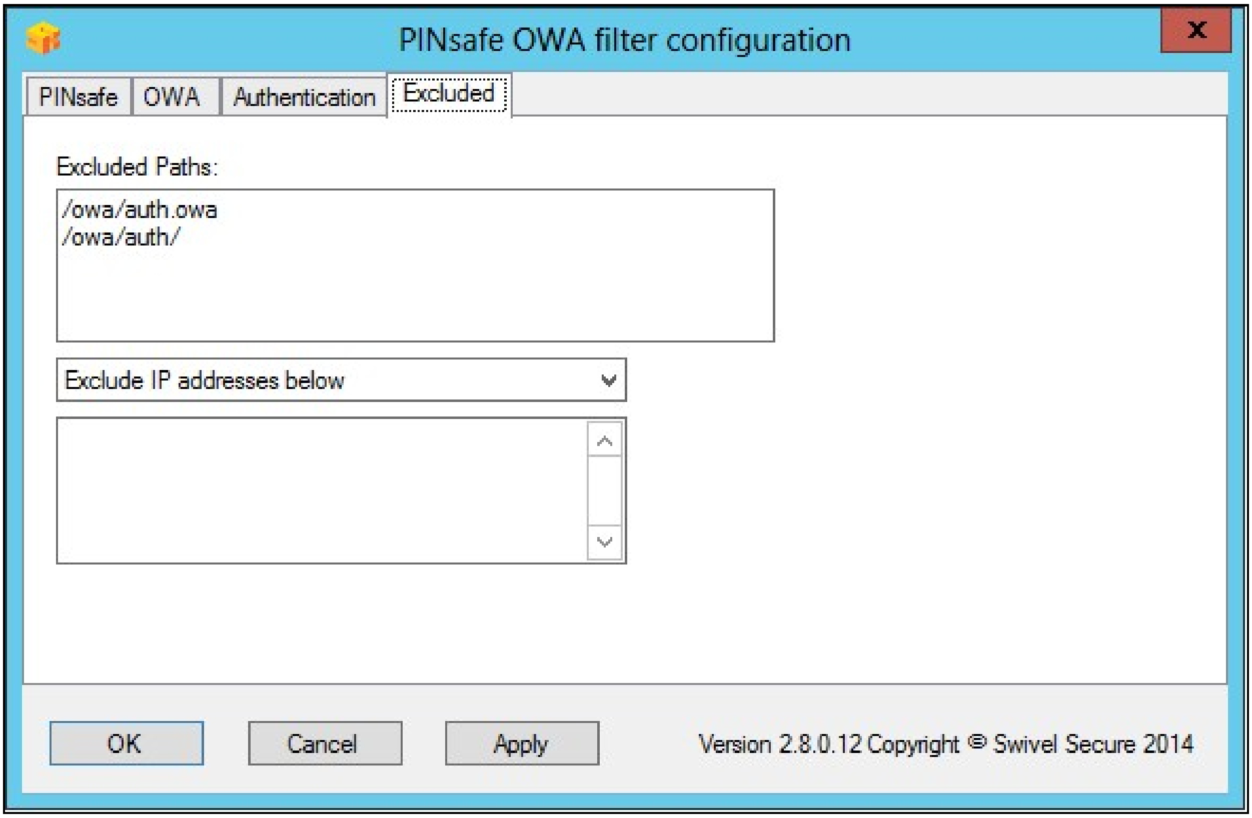
- □ Allow non-PINsafe Users
- ☑ Filter Enabled
- ☑ Ignore Domain Prefix
- □ Ignore Domain Suffix
- ☑ Show Change PIN link
- □ Show TURing image
- □ Show Message on-demand
- ☑ Show Pinpad
- ☑ Auto-show Image
- ☑ Redirect to Change PIN on PIN expiry

Version 2.8.0.12 Copyright © Swivel Secure 2014

181.2.4 Excluded Settings

Excluded Paths: This allows paths to be set for which authentication is not required to reach them. The paths shown on the display are added by default.

Excluded/Included IP addresses: You can choose to enable PINsafe authentication only for certain source IP addresses. Typically, you will do this if you wish to allow internal access to OWA without PINsafe authentication. Selecting "Exclude IP addresses below" will exclude the listed addresses from PINsafe authentication, while "Only include IP addresses below" will apply PINsafe authentication only to those IP addresses listed. For example, if you know that all external requests will come via a firewall at 192.168.0.99, you can select ?Only include IP addresses below?, and enter the single IP address as the address to include. Note that you can enter IP address ranges here using CIDR notation, for example 192.168.0.0/24 or 192.168.0.0/255.255.255.0. PINsafe will always display addresses using the latter format, irrespective of how they are entered. IPv6 addresses are not currently supported. To add multiple addresses, enter them into a text editor, one per line then copy and paste all entries, into the excluded field.



PINsafe OWA filter configuration

Excluded Paths:

```
/owa/auth.owa
/owa/auth/
```

Exclude IP addresses below

Version 2.8.0.12 Copyright © Swivel Secure 2014

181.2.4.1 External/Internal User Authentication

Using the above excluded IP addresses it is possible to configure a range of IP addresses for users, such as internal users, that will not be required to use Swivel authentication.

181.3 Configure The Swivel Server

181.3.1 Configuring Swivel for Agent XML Authentication

To allow communication from the OWA server to the Swivel server we need to configure an agent, see Agents How to Guide

181.3.2 Configuring Swivel for Single Channel Images

If Swivel Single Channel images are to be used for authentication, then the following guide can be used.

Single Channel How To Guide

181.3.3 Configuring Swivel for Dual Channel Authentication

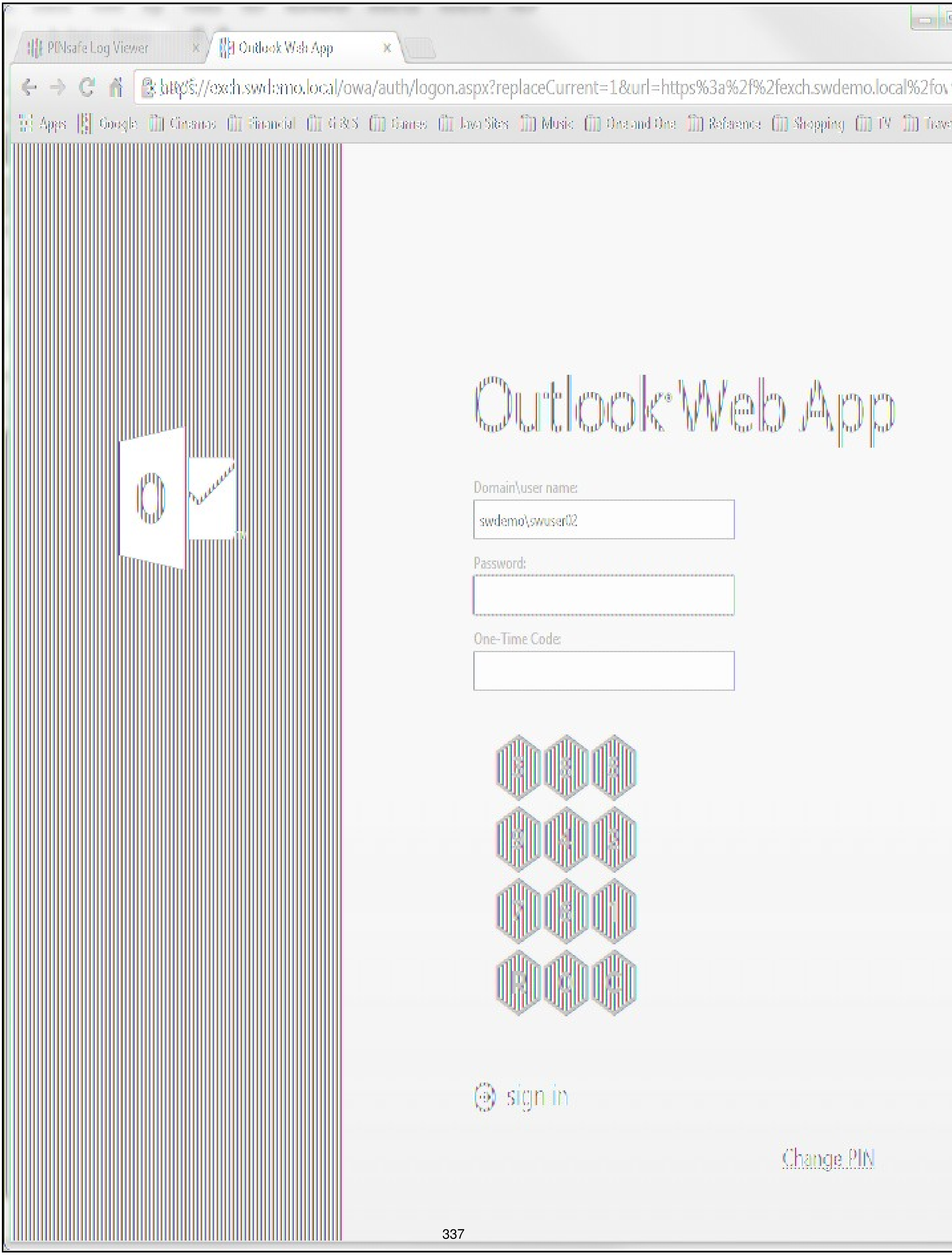
If Swivel Dual Channel authentication methods are to be used, refer to the following guide:

Transport Configuration

182 Verifying the Installation

Enter a username and AD password then the Swivel OTC for dual channel authentication. For single channel authentication enter the username, AD password then click on the button to generate a Single Channel Turing Security String, enter the OTC and login.

The below image shows the login page with PINpad.



Outlook Web App

Domain\user name: swdemo\swuser02

Password:

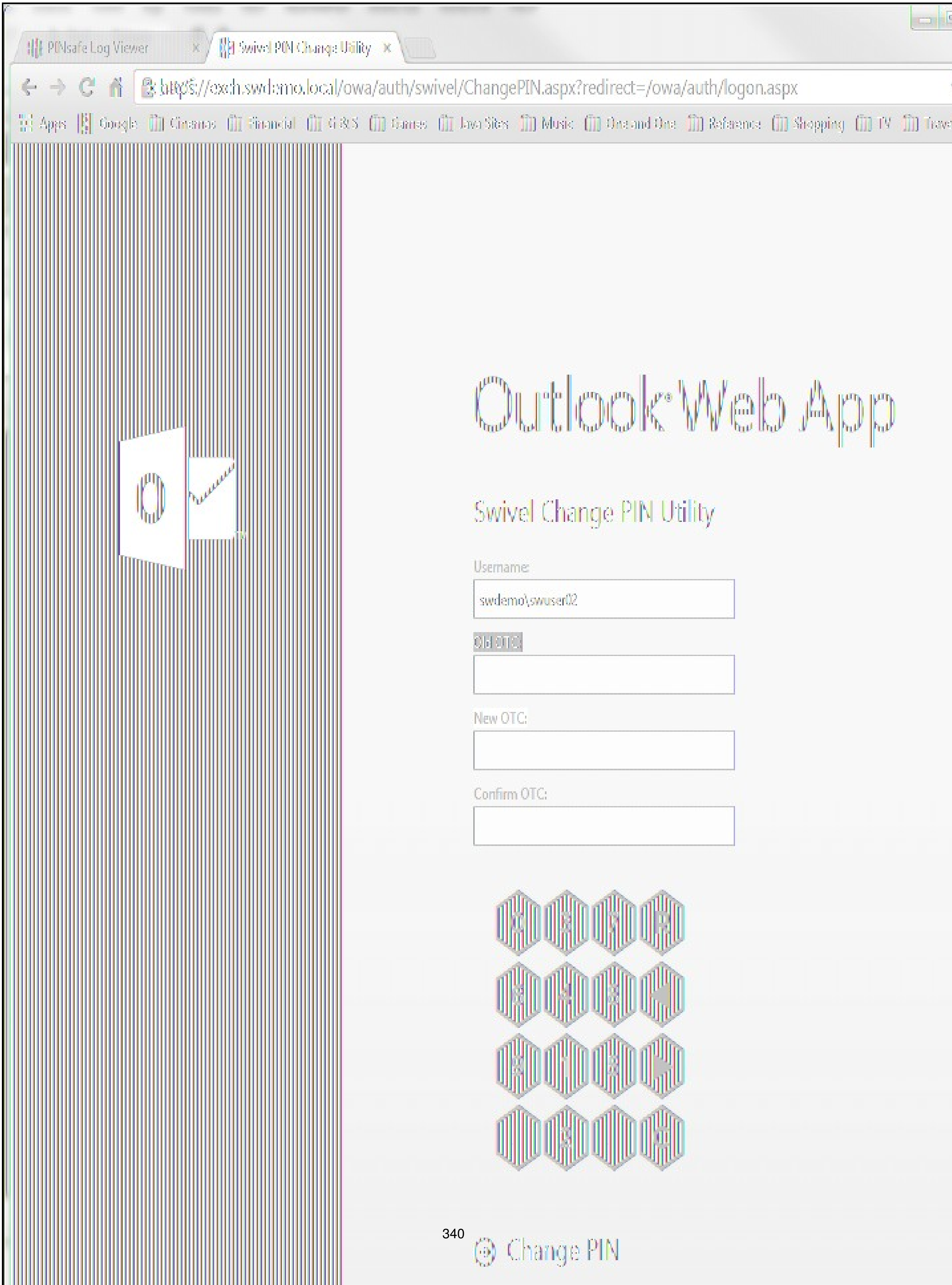
One-Time Code:

183 Change PIN

The Change PIN page is reasonably self-explanatory, but using Pinpad with change PIN may need some clarification.

You will notice on the screen shot that "Old OTC:" is highlighted. This means that clicking on the Pinpad digits will enter the corresponding digit into that field. To change the active field, either click on the field itself, or click the arrow keys in the Pinpad display.

The **R** key will refresh the Pinpad display (i.e. display a new security string), and the **C** key will clear the currently-active field.



Swivel Change PIN Utility

Username: swdemo\swuser02

Old OTC:

New OTC:

Confirm OTC:

184 Uninstalling the Swivel Integration

Uninstall the Swivel IIS filter, this should restore all the original files. If it does not work then find the file Logon.aspx.sav located in the Exchange Server folder (default is C:\Program Files\Microsoft\Exchange Server\V15) under the sub-folder FrontEnd\HttpProxy\owa\auth\. Rename this to restore the original Login.aspx.

185 Troubleshooting

Check the Swivel and OWA server logs

No login page, check the Exchange version. The filter needs to match the Exchange version number, and the file login.aspx needs to be modified so that it references the correct exchange install version.

Red Cross instead of Turing image, right click on red cross and look at its properties. Ensure Swivel server is running.

If you do not see a Turing image when using start session then in a web browser test the following link from the OWA server. If an image is not seen, then there is a problem either with communicating with the Swivel server or the Allow Image request by username may be set to No.

For Swivel appliances and software installs:

http(s)://<pinsafe_server_ip>:8080/pinsafe/SCImage?username=<username>

185.1 Enabling debug logging

Additional logging can be configured for troubleshooting, and will log from the time it was enabled.

edit C:\Program Files\Microsoft\Exchange Server\v15\FrontEnd\HttpProxy\owa\web.config

Locate

<add key="PINsafeEnableDebug" value="true" /> <add key="PINsafeDebugLocation" value="C:\Users\Public\Documents\PINsafeOWAFilter.log" />

185.2 User regularly times out after a short interval

The session is kept open by user activity. If this is insufficient then increase the cookie idle timeout value.

185.3 Turing image appears but user cannot authenticate

Verify that the OWA is configured to use port 8080 and context pinsafe. Port 8443 and context proxy will cause problems with authenticating users but allow the Turing image to be displayed. Note that this refers to the main PINsafe settings (for version 2.6 or higher) - the proxy settings SHOULD have these values if required.

185.4 User Authenticates Successfully to Swivel but OWA Login Page is Redisplayed

If you have entered the correct credentials, and the Swivel logs show successful authentication, but you are still redirected to the login page, the problem might be related to host names and/or SSL certificates.

First of all, if you connect to OWA using the IP address, or "localhost" from the OWA server itself, the Swivel filter will redirect you to the host name configured in the filter. This may result in the authentication cookie being lost, because the domain name doesn't match. In this case, attempting to authenticate a second time, with the correct host name, should succeed.

The second possibility is that the SSL certificate on the OWA Server doesn't match the host name used by the OWA filter, or the certificate has expired or is not trusted. This will result in authentication to OWA, from the Swivel filter, failing.

The solution for a production server is to ensure that the Exchange Server has a commercial SSL certificate, and that the Swivel OWA filter uses the host name that matches this.

For a development environment, you can generate a self-signed certificate with the correct host name, and add this to the list of trusted certificates on both the OWA server itself and the client (the latter might not be necessary). You might also need to add the host name to the hosts file on one or both of these.

185.5 Name resolution issue

The Exchange server may be looking for exchange.company.com from the internal network but cannot resolve it. Edit the hosts file mapping the name to 127.0.0.1. Also ensure that the internal CA certificate is trusted by the OWA server.

186 Known Issues and Limitations

Updates may result in the login page customisation being removed. In this case, you must select the option "Reapply Logon Page Changes" from the Swivel filter start menu.

There appears to be a problem locating the correct folder for OWA in some cases. We are investigating the cause of this, but meanwhile, if you are prompted to select the OWA folder, you should use the following:

C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HTTPProxy\owa

If Exchange Server is installed in a non-standard location, adjust the path accordingly, but the last part (FrontEnd\HTTPProxy\owa) should be the same.

186.1 TLS 1.2 Support

We have observed problems recently with the filter not working if TLS 1.2 only is enabled. We believe the problem is that the TLS 1.2 ciphers supported by Windows Server and the version of Java on our appliances do not overlap. If you are unable to connect the OWA filter to your Sentry appliance, it may be necessary to re-enable TLS 1.1 support on both the OWA filter and the appliance, and to enable the following cipher suite on the appliance: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA. In order to add this cipher suite, you will need command line access, so you will need assistance from Swivel Secure support.

186.2 Themes Support

The filter has been written and tested using the default theme (as seen in the screen shots). The screens may not look right (although they should still work) if the theme is changed. However, it should only be necessary to change the stylesheet in order to correct this. Please contact support@swivelsecure.com if you have difficulties getting the display looking right. In particular, the Change PIN page will only work with the default theme, and with the OWA 2013 versions listed above.

187 Multiple Swivel Servers

Versions 2.5 and later include the option to add multiple Swivel servers. Then, if the first one is unavailable, the filter will try the other servers in the order listed. The filter will always remember the last Swivel server successfully contacted and try that one first.

To support multiple servers, there is an additional button on the Swivel tab of the configuration program, which brings up a secondary dialogue containing a list of available servers. Use this to add or delete Swivel servers, and to select one to modify (the details are modified on the main dialogue).

188 Additional Information

For assistance in the Swivel installation and configuration please firstly contact your reseller and then email Swivel Secure support at supportdesk@swivelsecure.com.

189 Microsoft OWA with OMA on Exchange 2003

189.1 OWA and OMA on Exchange 2003 Integration Notes

the following Microsoft knowledge base article might be of interest:

http://support.microsoft.com/kb/817379

189.2 Article Summary

When you try to access a Microsoft Exchange Server 2003 computer by using Microsoft Office Outlook Mobile Access or Exchange ActiveSync, you may experience connection or synchronization problems. These issues can occur if either of the following conditions is true:

The Exchange virtual directory on an Exchange back-end server is configured to require SSL.

Forms-based authentication is enabled.

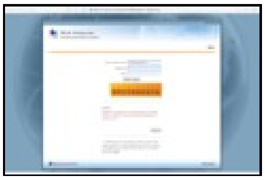
However, these issues do not occur if these same conditions are true on the Exchange virtual directory on a front-end server.

190 Category:OWA

191 Microsoft RD Web Access

192 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.

193 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.

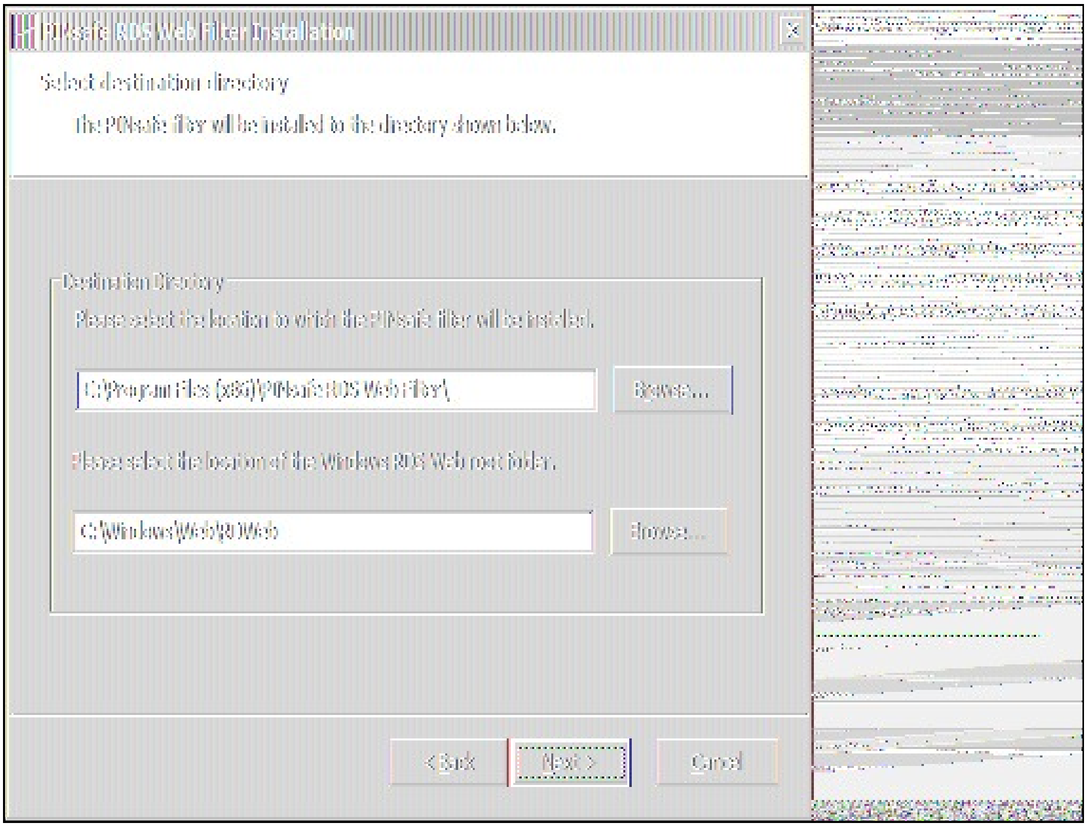
194 Swivel Server Configuration

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.

195 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.



PINsafe RDS Web Filter Installation

Select destination directory

The PINsafe filter will be installed to the directory shown below.

Destination Directory

Please select the location to which the PINsafe filter will be installed.

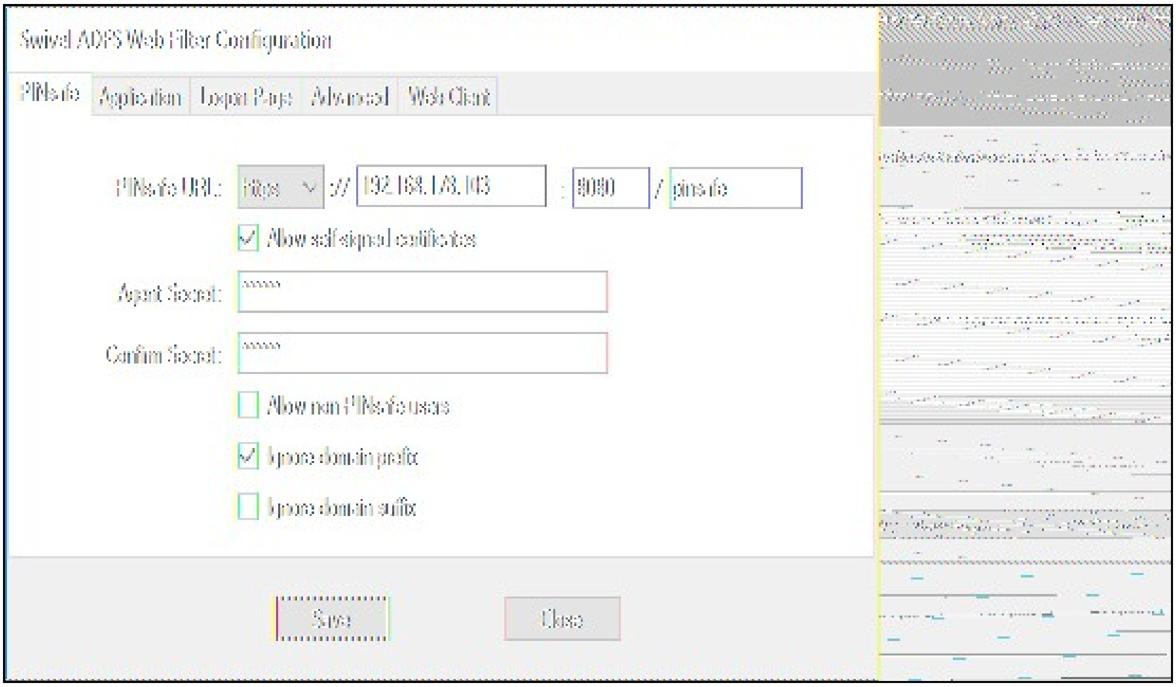
C:\Program Files (x86)\PINsafe RDS Web Filter\

Please select the location of the Windows RDS Web root folder.

C:\Windows\Web\RDWeb

196 Configuration

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



Swivel ADFS Web Filter Configuration

PINsafe URL: https :// 192.168.178.103 : 8080 / pinsafe

☑ Allow self-signed certificates

Agent Secret: ******

Confirm Secret: ******

□ Allow non PINsafe users

☑ Ignore domain prefix

□ Ignore domain suffix

196.1 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.

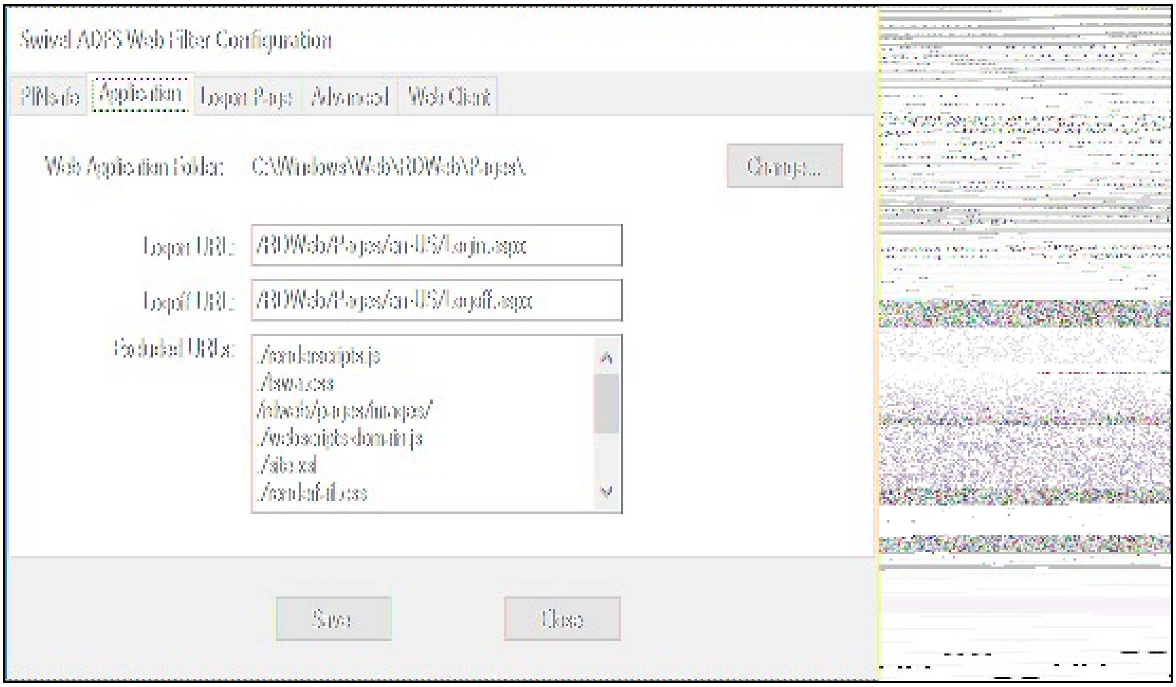
Note: do not use the ?:8443/proxy? URL, as that is not valid for authentication.

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.



Swivel ADFS Web Filter Configuration

Web Application Folder: C:\Windows\Web\RDWeb\Pages\

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

Logoff URL: /RDWeb/Pages/en-US/Logoff.aspx

Excluded URLs:
/renderscripts.js
/tswa.css
/rdweb/pages/images/
/webscripts-domain.js
/site.xsl
/renderfail.css

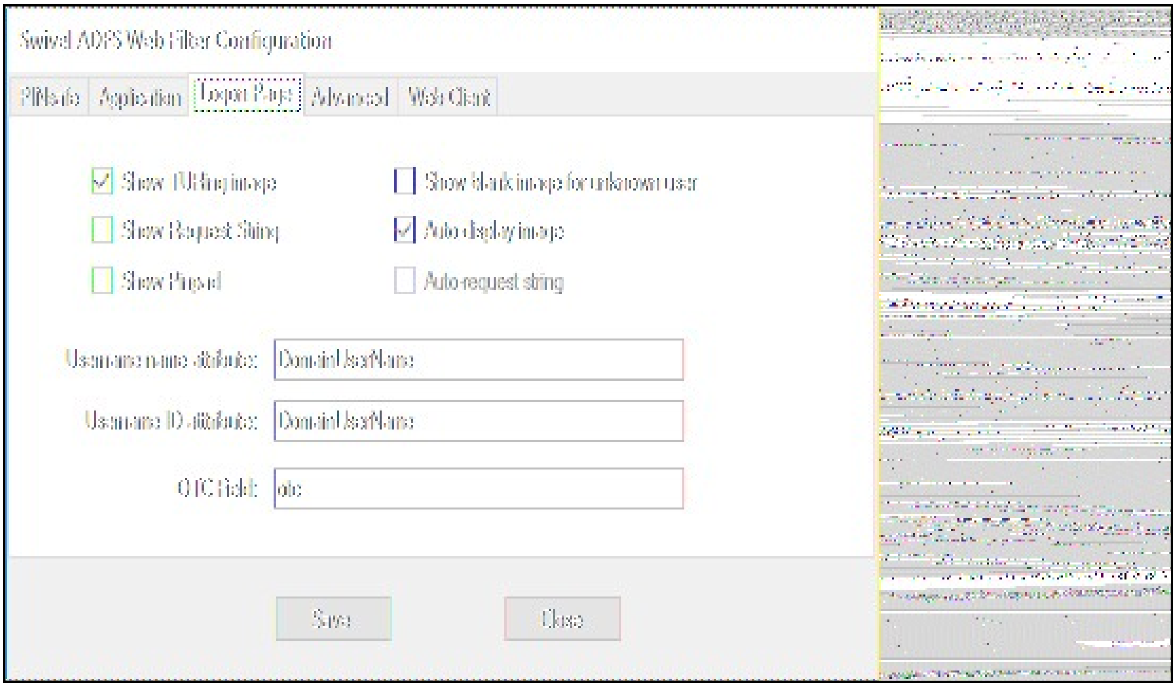
Web Application Folder: Change allows a new path to be specified

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.



Swivel ADFS Web Filter Configuration

☑ Show TURing image

□ Show Request String

□ Show Pinpad

□ Show blank image for unknown user

☑ Auto display image

□ Auto-request string

Username name attribute: DomainUserName

Username ID attribute: DomainUserName

OTC Field: otc

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.

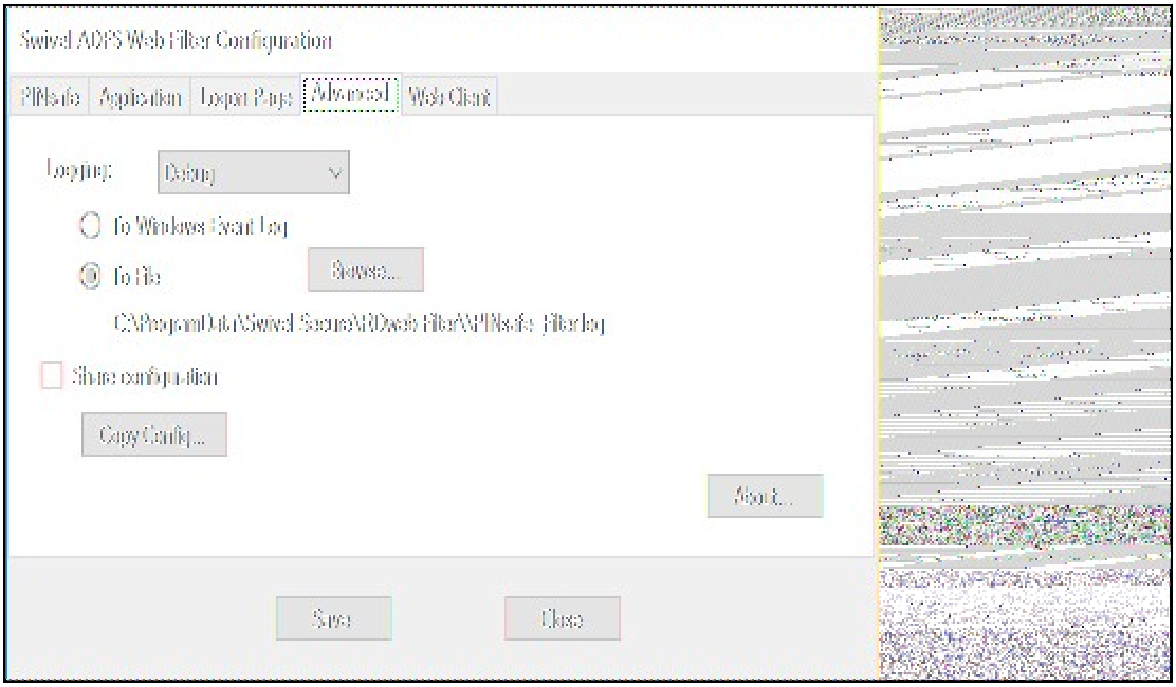
Auto-display image if checked, the TURing or Pinpad is automatically displayed after entering the username.

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.



Swivel ADFS Web Filter Configuration

Logging: Debug

○ To Windows Event Log

● To File

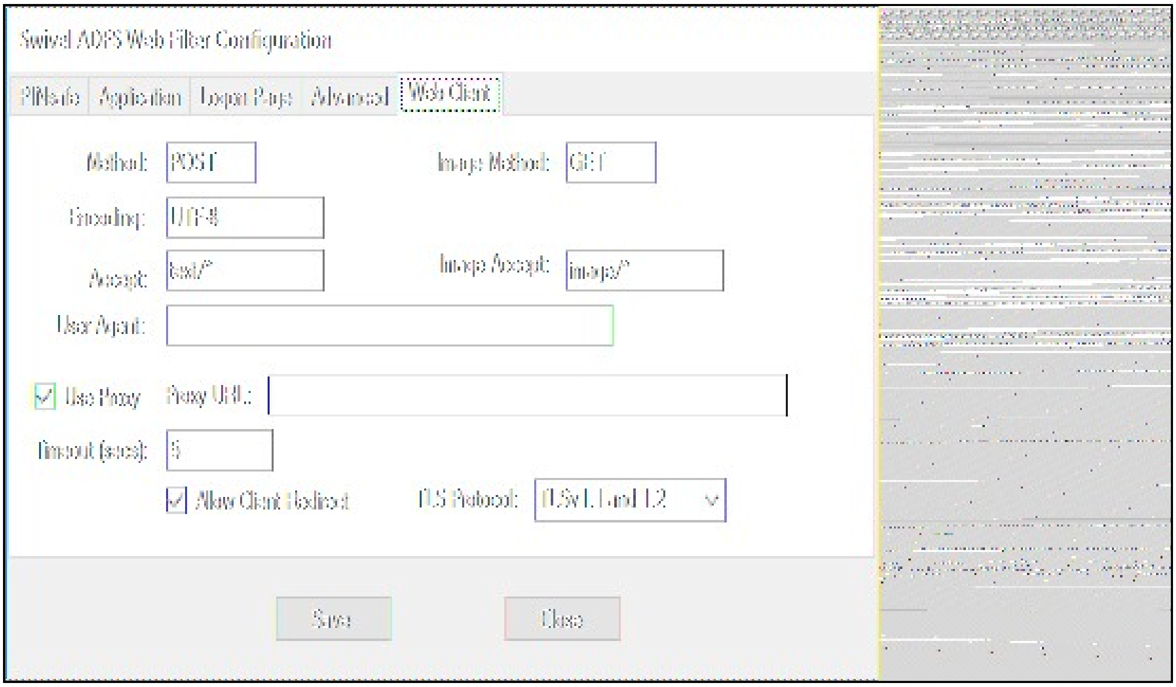
C:\ProgramData\Swivel Secure\RDweb Filter\PINsafe_Filter.log

□ Share configuration

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.



Swivel ADFS Web Filter Configuration

Method: POST

Image Method: GET

Encoding: UTF-8

Accept: text/*

Image Accept: image/*

User Agent:

☑ Use Proxy

Proxy URL:

Timeout (secs): 5

☑ Allow Client Redirect

TLS Protocol: TLSv1.1 and 1.2

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.

197 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.

198 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.

199 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.

200 Microsoft Sharepoint 2010 Integration

200.1 Overview

The solution described here is for SharePoint 2010 only, as it relies on claims-based authentication features introduced in that version. A similar solution is also available for SharePoint 2013.

For earlier versions of SharePoint, see this article.

200.2 Downloading the Filter

The latest solution for PINsafe SharePoint 2010 filter is version 1.5.3. It can be found here. Full instructions for installing the filter and configuring SharePoint to support it are included in the zip file.

200.3 Upgrading the Swivel SharePoint Filter

It is recommended to uninstall the old filter and then reinstall the new filter in order to remove the previous filter from the assembly cache. Choose the appropriate upgrade option when installing the new version.

200.4 Uninstalling the Swivel SharePoint filter

To uninstall the filter select the Add/Remove Programs on the SharePoint server then uninstall. The settings are not removed in the uninstall process.

200.5 SharePoint PINsafe FAQ

200.5.1 Can the Swivel SharePoint filter Manage the AD Credentials

Yes, version 1.4 or later of the SharePoint filter has the ability to set the AD password. See documentation included in the download for more information.

200.5.2 Can the filter detect an expired AD password

Yes, version 1.4 or later of the filter will detect if the AD password has expired, and will redirect to a page suitable for changing the AD password. See documentation included in the download for more information.

200.5.3 Can the filter allow users to reset a forgotten AD password

Yes, version 1.5 or later of the SharePoint filter has the ability to reset forgotten AD passwords as well as PINs. See included documentation for more information.

Note that the password reset feature requires version 3.9.6 or later of the Swivel Core server. However, if you do not wish to upgrade, a patch is available for version 3.8, from here, to add the required feature. If you want to use this feature, please contact support@swivelsecure.com to check if your version of PINsafe can be upgraded to support this feature. Please also contact support@swivelsecure.com for help in installing this patch.

200.5.4 Can the filter work with Membership Providers other than Active Directory

Yes, version 1.5.2 or later will work with other membership providers. However, the AD password management facilities must be disabled. These only work with the AD membership provider, and authentication with other membership providers will fail if this feature is enabled.

200.6 Troubleshooting

200.6.1 TURing image does not appear

A red cross may be present where the TURing image should appear. The usual causes are:

Incorrect path to PINsafe appliance

Self Signed Certificate is used, but the allow self signed certificate option has not been selected

Firewall blocking access to PINsafe server

Network issue

HTTP request against the PINsafe running HTTPS

200.6.2 Error Messages

502 - Bad Gateway

This has been seen where the SharePoint cannot connect to the PINsafe server. Check the above, particularly the settings for SSL or HTTP access.

Authentication provider not found

PINsafe cannot be accessed by the SharePoint server, verify connectivity settings.

201 Microsoft Sharepoint 2013 Integration

201.1 Overview

The solution described here is for SharePoint 2013 only. A similar solution is available for SharePoint 2010. Do not use version 1.6 of the filter for SharePoint 2010, and do not use earlier versions for SharePoint 2013.

For earlier versions of SharePoint, see this article.

201.2 Downloading the Filter

The latest solution for PINsafe SharePoint 2013 filter is version 1.6.1. It can be found here. The only change from 1.6.0 is that removing the domain prefix and/or suffix from usernames is now optional. In 1.6.0, they were always removed.

Full instructions for installing the filter and configuring SharePoint to support it are included in the zip file, or you can download it separately from here.

The previous version, 1.6.0, can be found here.

201.3 Upgrading the Swivel SharePoint Filter

It is recommended to uninstall the old filter and then reinstall the new filter in order to remove the previous filter from the assembly cache. You should then choose the appropriate upgrade option when prompted. Note that upgrading from a SharePoint 2010 filter has not been tested, but as the technology is very similar, no problems are anticipated. If you do have a problem when upgrading an existing SharePoint 2010 filter to SharePoint 2013, it is recommended that you uninstall and treat it as a new installation.

201.4 Uninstalling the Swivel SharePoint filter

To uninstall the filter select the Add/Remove Programs on the SharePoint server then uninstall. The settings are not removed in the uninstall process.

201.5 SharePoint PINsafe FAQ

201.5.1 Can the Swivel SharePoint filter Manage the AD Credentials

Yes, version 1.4 or later of the SharePoint filter has the ability to set the AD password. See documentation included in the download for more information.

201.5.2 Can the filter detect an expired AD password

Yes, version 1.4 or later of the filter will detect if the AD password has expired, and will redirect to a page suitable for changing the AD password. See documentation included in the download for more information.

201.5.3 Can the filter allow users to reset a forgotten AD password

Yes, version 1.5 or later of the SharePoint filter has the ability to reset forgotten AD passwords as well as PINs. See included documentation for more information.

However, the password reset feature requires version 3.9.6 or later of the Swivel Core server, which at the time of writing had not been released. However, a patch is available for version 3.8, from here, to add the required feature. If you want to use this feature, please contact support@swivelsecure.com to check if your version of PINsafe can be upgraded to support this feature. Please also contact support@swivelsecure.com for help in installing this patch.

201.5.4 Can the filter work with Membership Providers other than Active Directory

Yes, version 1.5.2 or later will work with other membership providers. However, the AD password management facilities must be disabled. These only work with the AD membership provider, and authentication with other membership providers will fail if this feature is enabled.

201.6 Troubleshooting

201.6.1 TURing image does not appear

A red cross may be present where the TURing image should appear. The usual causes are:

Incorrect path to PINsafe appliance

Self Signed Certificate is used, but the allow self signed certificate option has not been selected

Firewall blocking access to PINsafe server

Network issue

HTTP request against the PINsafe running HTTPS

201.6.2 Error Messages

502 - Bad Gateway

This has been seen where the SharePoint cannot connect to the PINsafe server. Check the above, particularly the settings for SSL or HTTP access.

Authentication provider not found

PINsafe cannot be accessed by the SharePoint server, verify connectivity settings.

202 Microsoft Sharepoint 2019 Integration

202.1 Overview

NOTE: this solution is based on the SharePoint 2013 solution. As such, it has had limited testing on SharePoint 2019, but it appears to be working successfully.

The solution described here is for SharePoint 2019 only. Similar solutions are available for SharePoint 2013 and SharePoint 2010. Do not use version 1.8 of the filter for previous versions of SharePoint, and do not use earlier versions for SharePoint 2019.

Please note that the illustrations in this article are from the SharePoint 2013 integration. The forms will looks slightly different in 2019, but functionality is essentially the same. There may also be some outdated references to SharePoint 2013. This article will be updated in due course.

202.2 Downloading the Filter

The latest solution for PINsafe SharePoint 2019 filter is version 1.8.0. It can be found here.

Full instructions for installing the filter and configuring SharePoint to support it can be downloaded from here. This article refers to version 1.6 for SharePoint 2013, but the instructions are unchanged.

202.3 Upgrading the Swivel SharePoint Filter

It is recommended to uninstall the old filter and then reinstall the new filter in order to remove the previous filter from the assembly cache. You should then choose the appropriate upgrade option when prompted. Note that upgrading from a SharePoint 2010 filter has not been tested, but as the technology is very similar, no problems are anticipated. If you do have a problem when upgrading an existing SharePoint 2010 filter to SharePoint 2013, it is recommended that you uninstall and treat it as a new installation.

202.4 Uninstalling the Swivel SharePoint filter

To uninstall the filter select the Add/Remove Programs on the SharePoint server then uninstall. The settings are not removed in the uninstall process.

202.5 SharePoint PINsafe FAQ

202.5.1 Can the Swivel SharePoint filter Manage the AD Credentials

Yes, version 1.4 or later of the SharePoint filter has the ability to set the AD password. See documentation included in the download for more information.

202.5.2 Can the filter detect an expired AD password

Yes, version 1.4 or later of the filter will detect if the AD password has expired, and will redirect to a page suitable for changing the AD password. See documentation included in the download for more information.

202.5.3 Can the filter allow users to reset a forgotten AD password

Yes, version 1.5 or later of the SharePoint filter has the ability to reset forgotten AD passwords as well as PINs. See included documentation for more information.

However, the password reset feature requires version 3.9.6 or later of the Swivel Core server, which at the time of writing had not been released. However, a patch is available for version 3.8, from here, to add the required feature. If you want to use this feature, please contact support@swivelsecure.com to check if your version of PINsafe can be upgraded to support this feature. Please also contact support@swivelsecure.com for help in installing this patch.

202.5.4 Can the filter work with Membership Providers other than Active Directory

Yes, version 1.5.2 or later will work with other membership providers. However, the AD password management facilities must be disabled. These only work with the AD membership provider, and authentication with other membership providers will fail if this feature is enabled.

202.6 Troubleshooting

202.6.1 TURing image does not appear

A red cross may be present where the TURing image should appear. The usual causes are:

Incorrect path to PINsafe appliance

Self Signed Certificate is used, but the allow self signed certificate option has not been selected

Firewall blocking access to PINsafe server

Network issue

HTTP request against the PINsafe running HTTPS

202.6.2 Error Messages

502 - Bad Gateway

This has been seen where the SharePoint cannot connect to the PINsafe server. Check the above, particularly the settings for SSL or HTTP access.

Authentication provider not found

PINsafe cannot be accessed by the SharePoint server, verify connectivity settings.

203 Microsoft Sharepoint Integration Methods

203.1 Overview

This document describes methods of integrating Swivel authentication with earlier versions of SharePoint that do not support claims-based authentication. Although these methods will work with later versions of SharePoint, it is recommended that you use the appropriate dedicated filters for SharePoint 2010 and 2013, in the following links:

SharePoint 2010

SharePoint 2013

203.2 Integration Using TMG or ISA

Our recommended solution for earlier versions of SharePoint is to use Microsoft TMG integration with RADIUS authentication (see here or here), or Microsoft ISA Server with RADIUS authentication (see Microsoft ISA 2006 Integration). However, the following article shows how to integrate with SharePoint as a 2-stage authentication process.

203.3 Authenticating to Earlier Versions of SharePoint as a 2-Stage Process

The solution is to use the PINsafe IIS7 filter. Install as per the included instructions.

The result should be that you will need to authenticate first to the Active Directory domain, if you are not already logged in. Subsequently, you will be redirected to the PINsafe login page to complete the second part of the authentication process, before being finally redirected to the SharePoint home page.

One issue which is not addressed by the IIS filter documentation, which might cause problems, particularly in Windows 2008 Server, is that the Windows account running the SharePoint application (normally Network Service) needs to have read and execute permission on the pinsafe virtual directory.

204 Microsoft Windows Small Business Server 2011

205 Introduction

Built on Windows Server 2008 R2, Windows SBS 2011 Standard includes Microsoft Exchange Server 2010 SP1, Microsoft SharePoint Foundation 2010 and Windows Software Update Services.

This configuration document outlines how to integrate Swivel with Microsoft Small Business Server 2011 authentication in addition to the Swivel authentication.

206 Prerequisites

Microsoft Small Business Server 2011

Swivel 3.x server

Swivel Small Business Software.

207 Baseline

Swivel 3.9

208 Architecture

The SBS makes authentication requests against the Swivel server by XML.

209 Installation

209.1 Configure The Swivel Server

Configure a Swivel Agent (For standard XML Authentication)

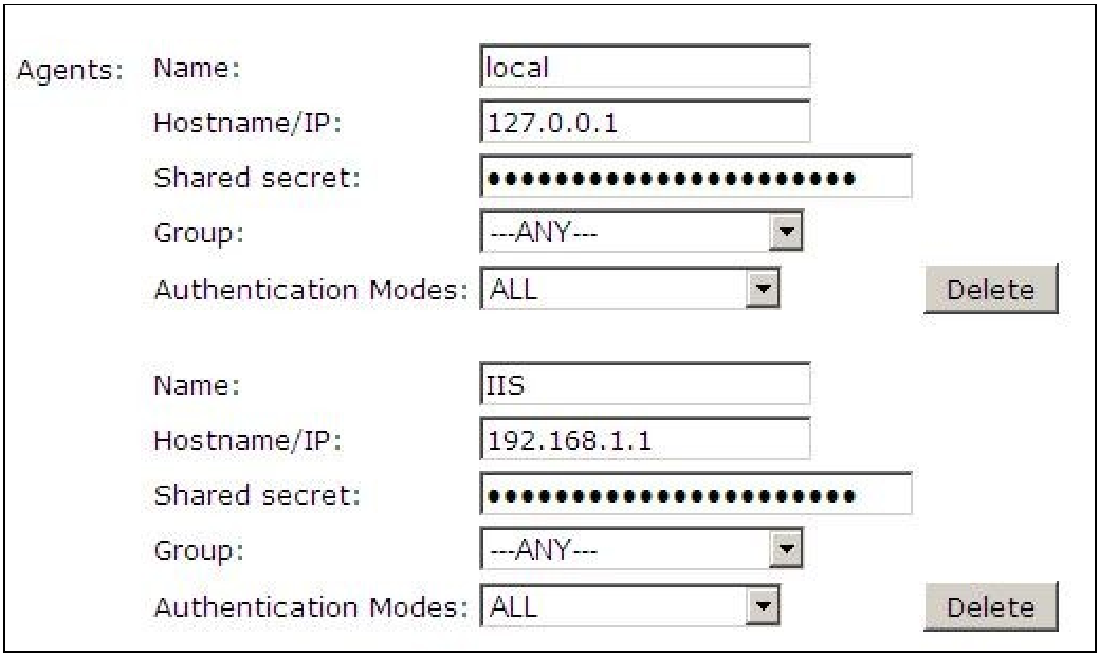
1. On the Swivel Management Console select Server/Agent

2. Enter a name for the Agent

3. Enter the Exchange IP address

4. Enter the shared secret used above on the SBS

5. Click on Apply to save changes



Agents:

Name: local

Hostname/IP: 127.0.0.1

Shared secret: ●●●●●●●●●●●●●●●●●●●●●●

Group: ---ANY---

Authentication Modes: ALL

Name: IIS

Hostname/IP: 192.168.1.1

Shared secret: ●●●●●●●●●●●●●●●●●●●●●●

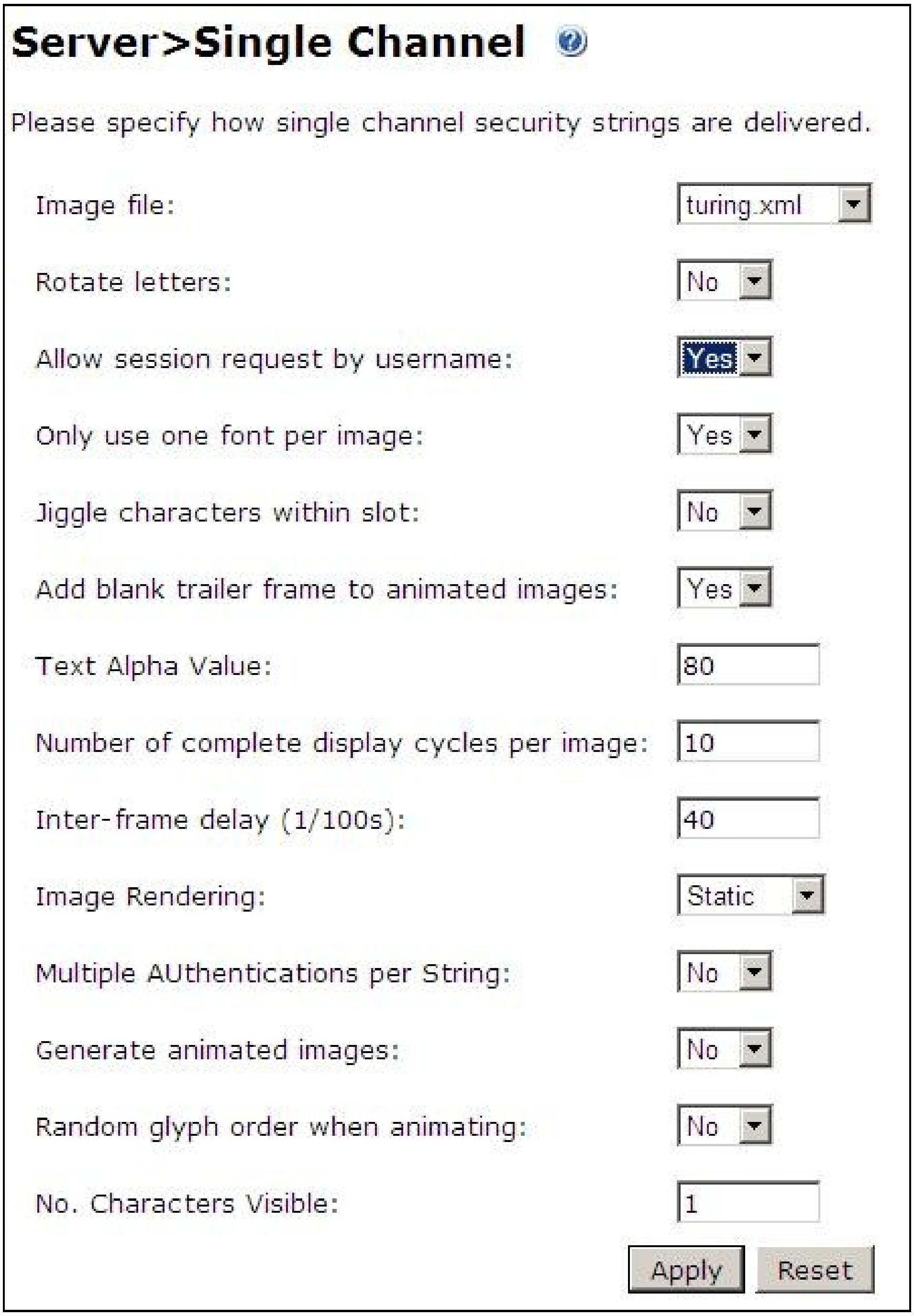
Group: ---ANY---

Authentication Modes: ALL

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

209.2 Configure the SBS 2011

1. Extract the files from the zip folder

2. Copy all the DLLs from the Bin folder to the Bin folder of the SBS application (by default C:\Program Files\Windows Small Business Server\Bin\WebApp\RemoteAccess).

3. Copy pinsafe_image.aspx from the AccountPage folder of the zip to the AccountPage folder of the SBS application.

4. Backup the existing SBS server Logon.aspx. Modify the existing Logon.aspx on the SBS server by locating the relevant sections in the customised Swivel Logon.aspx and copying to the SBS server Logon.aspx. Search for "Swivel Customisation Start". There are three separate sections. Copy each section into the existing Logon.aspx file (the end of the section is marked by "Swivel Customisation End"). It should be clear from the original file where the sections should go.

5. Backup the existing SBS server web.config. Modify the existing web.config on the SBS server by locating the relevant sections in the customised Swivel web.config and copying to the SBS server web.config. There are three sections to change, marked as before. The first one adds the Swivel filter as a HTTP module. The second adds an exclusion to default authorization, so that the TURing image can be displayed without having to authenticate. The third is the list of settings for the PINsafe server. You may find you have to create the <appSettings> section as well as inserting the settings, or you may find that there is a single, empty <appSettings /> entry. In the latter case, replace that with the entire <appSettings> section in the custom file. You will need to change the value="" entries to match the PINsafe settings for your local environment.

6. Finally, restart IIS (this may not be strictly necessary, but it's always best to make sure).

210 Verifying the Installation

211 Troubleshooting

212 Additional Configuration Options

213 Known Issues and Limitations

214 Additional Information

For assistance in the Swivel installation and configuration please firstly contact your reseller and then email Swivel Secure support at support@swivelsecure.com

215 Category:SharePoint

216 Microsoft Terminal Services Integration

216.1 Overview

PINsafe integrates with the Microsoft Windows GINA to allow authentication through Terminal Services. For further information see Microsoft Windows GINA login

217 Microsoft TMG 2010 Integration

217.1 Microsoft Forefront Threat Management Gateway (TMG) Integration Notes

217.2 Introduction

This document outlines the necessary steps to integrate Swivel authentication into Microsoft TMG Server 2010 for use with Swivel for Dual Channel authentication using SMS, Mobile Phone Clients and Single Channel using TURing, PINpad and the Taskbar. If the TMG server is part of a cluster then the filter needs to be installed on each server in the cluster.

217.3 Prerequisites

This installation guide assumes that publication of the relevant service has already been configured in TMG Server, following the relevant instructions. In addition a working Swivel server version 3.1 or later is required. Certain features of the filter require later versions of Swivel:

- If the option to allow unknown users is required, this requires Swivel 3.4 or later.
- If the option to use Pinpad is required, the Swivel version must be 3.9.2 or higher, or a version of the appliance proxy from 2012.

The Swivel Configuration utility requires .Net version 2 or higher. This is not supplied above and must be downloaded and installed if you do not already have it.

The TMG server and its configuration should be fully backed up prior to the Swivel integration.

Allow around 1 hour downtime per TMG server for the integration, and the integration will require a restart of the TMG Firewall Services. If you are replacing an older version of the Swivel filter, you must uninstall that version first. The filter configuration will not be lost. You will need to stop the TMG firewall service before uninstalling the old filter, or else you will be prompted to restart the server to complete uninstallation.

217.3.1 Swivel TMG 2010 Filter

The filter can be downloaded from here. NOTE: this is version 1.4.4 of the TMG filter, released 1/11/13. Version 1.4.4 fixes a bug found by some customers, whereby the login page was not detected in some circumstances, allowing authentication by password only. The same bug could also cause other failures, such as occasionally failing to show a TURing image. This version also adds better control over logging. See the included documentation for more details.

Version 1.4.3 was never released, but made detection of the required URLs case-insensitive.

Version 1.4.2 includes some bug fixes and enhancements, in particular:

- Redirecting to the login page after an incorrect one-time code now works correctly. This means that an error message is displayed if the one-time code is incorrect. It is also expected that this will resolve issues experienced by some customers whereby, having logged in once, users do not always have to re-enter their one-time code.
- The firewall service is restarted automatically after making configuration changes and before uninstalling the filter.

Version 1.4.1 fixes some bugs present in version 1.4.0. Version 1.4 includes a number of enhancements over previous versions. See the included documentation.

NOTE: if you are using this filter with RADIUS authentication, be aware that there are some errors in the file usr_pwd_pcode.htm. These need to be fixed manually - contact support@swivelsecure.com for details. An update with the correct script will be released shortly.

217.4 Baseline

Swivel 3.1 or later (3.6 or later preferred)

Microsoft Forefront TMG 2010

Web-based server, typically Microsoft IIS-based, to be protected, such as OWA or SharePoint.

217.5 Architecture

The TMG server makes authentication requests against the Swivel server by XML or RADIUS. Some of the additional features are only available in the XML authentication. For security reasons Sharepoint authentication should be configured using RADIUS. The Swivel installation creates a separate custom login.

217.6 Swivel Configuration

217.6.1 Configure a Swivel Agent For XML Authentication

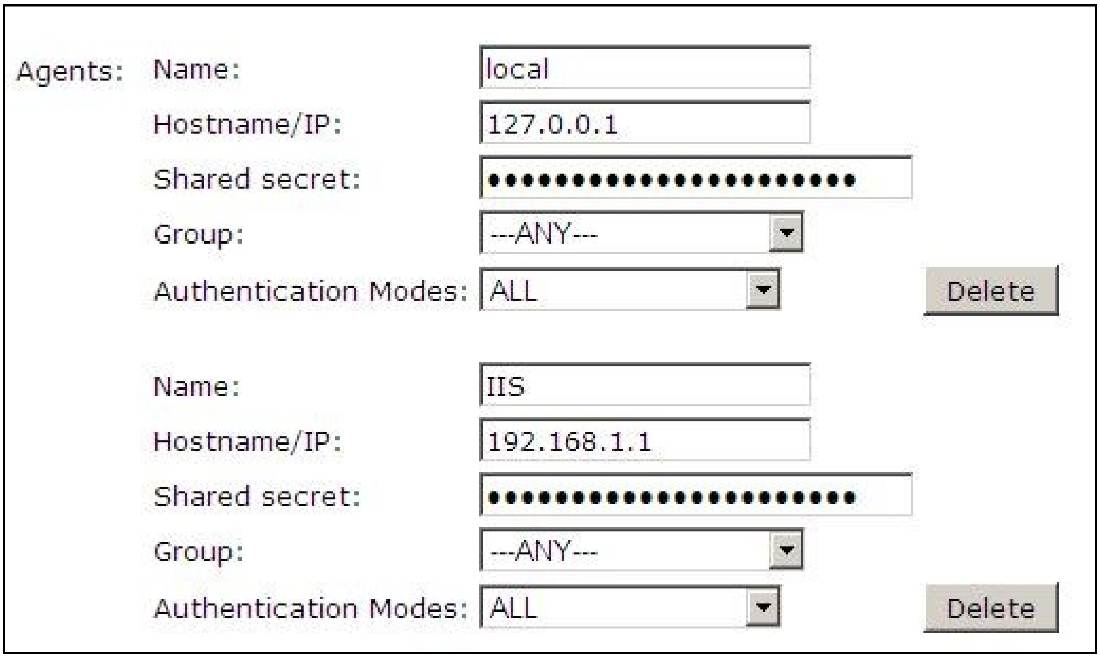
1. On the Swivel Management Console select Server/Agent

2. Enter a name for the Agent

3. Enter the TMG internal IP address

4. Enter the shared secret

5. Click on Apply to save changes



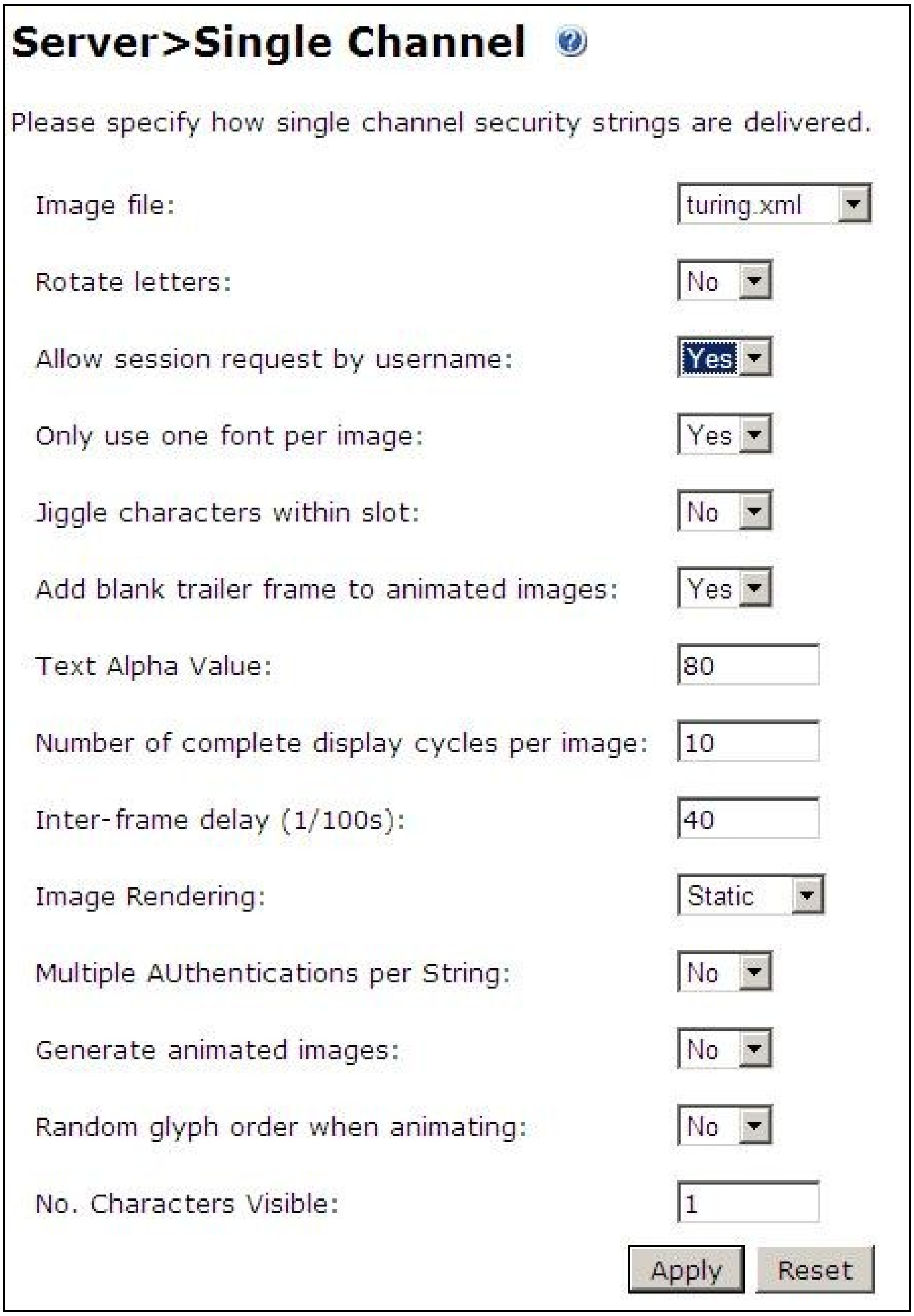
Agents: Name: local
Hostname/IP: 127.0.0.1
Shared secret: ●●●●●●●●●●●●●●●●●●●●●●
Group: ---ANY---
Authentication Modes: ALL

Name: IIS
Hostname/IP: 192.168.1.1
Shared secret: ●●●●●●●●●●●●●●●●●●●●●●
Group: ---ANY---
Authentication Modes: ALL

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

217.6.3 Configure a RADIUS NAS entry for Sharepoint authentication

NOTE: this is only required if you wish to use RADIUS authentication with Swivel. This is recommended for SharePoint integration and optional for other solutions.

1. Ensure the RADIUS server is running on Swivel

2. On the Swivel Management Console select RADIUS NAS

3. Enter a name for the NAS

4. Enter the TMG internal IP address

5. Enter the shared secret

6. Click on Apply to save changes

217.7 Swivel TMG Filter Upgrade

If an existing filter is installed then installing the new filter will first uninstall the existing filter.

217.8 Swivel TMG Filter Installation

The following steps should be carried out on the TMG server. No configuration changes need to be performed on the Exchange server or Sharepoint server. For Additional Sharepoint configuration see the Special Considerations for Sharepoint below. To upgrade or reinstall the filter, first remove the existing Swivel TMG filter.

217.8.1 Publish OWA or Sharepoint

Publish Outlook Web Access, Sharepoint or your website as described in the TMG Server documentation, if you have not already done so. Ensure that they are working as expected without Swivel authentication before attempting to install the Swivel filter.

For OWA, TMG should be configured to redirect to /owa automatically, otherwise a failure in the Swivel authentication will redirect to the root path, which will give an error. This external link shows how to configure this: Setting up an OWA redirect in Forefront TMG 2010 the easy way

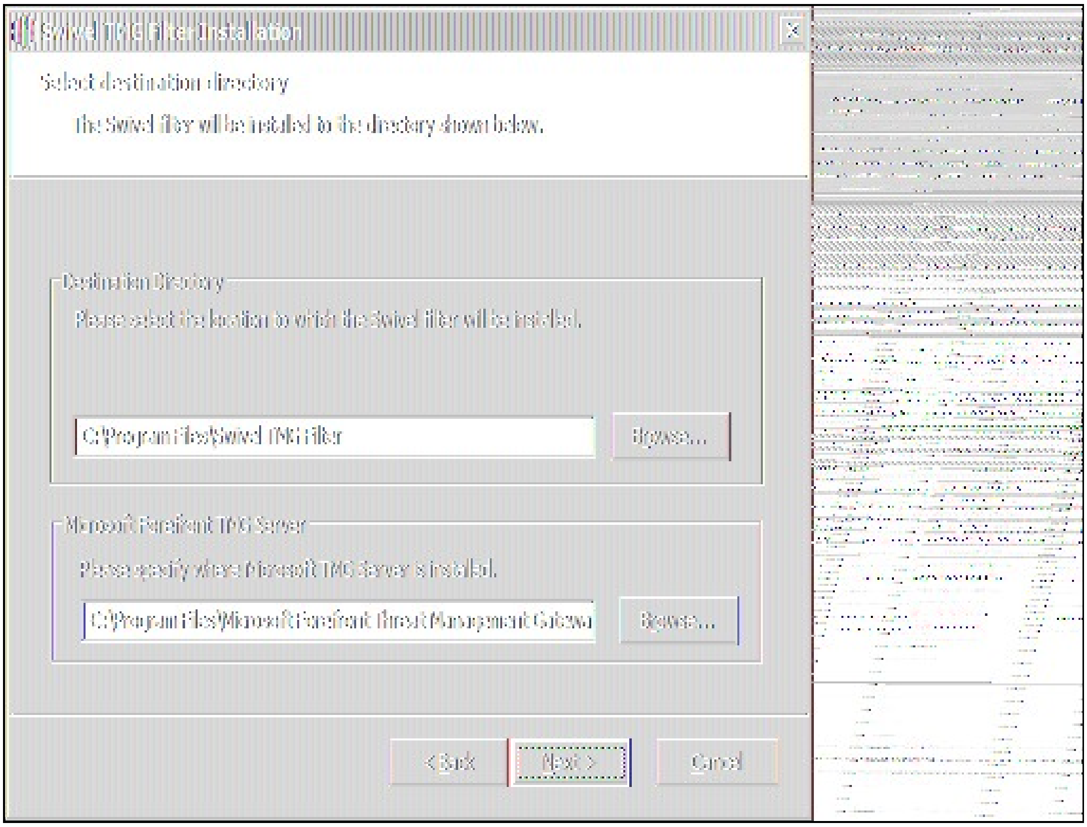
217.8.2 Configure TMG firewall rules

Create an access rule permitting HTTP access from the TMG Server to the correct port (commonly 8080) on the Swivel server. To do this, you will need to create a new protocol for outbound TCP on the appropriate port.

217.8.3 Install the TMG server software

NOTE: if you are installing in an Enterprise environment, you should always install on the Configuration Storage server first, and then on each array member. Be aware that the firewall service on member servers will stop when they try to synchronise with the configuration storage server, if that has the Swivel filter installed and the member does not. Once the filter is installed on the member server, you will be able to restart the firewall service.

Run PINsafeTMGFilter.exe to install the filter DLL. You will be prompted for the location in which to install the filter configuration, and also for the location of Microsoft TMG Server, usually C:\Program Files\Microsoft Forefront Threat Management Gateway.



Swivel TMG Filter Installation

Select destination directory

The Swivel filter will be installed to the directory shown below.

Destination Directory

Please select the location to which the Swivel filter will be installed.

C:\Program Files\Swivel TMG Filter

Microsoft Forefront TMG Server

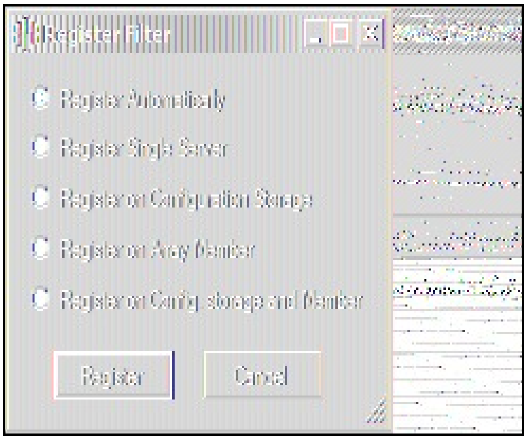
Please specify where Microsoft TMG Server is installed.

C:\Program Files\Microsoft Forefront Threat Management Gatewa

Note that the installation process will include installation of Microsoft Visual C++ 2010 runtime libraries, if they are not already installed.

217.8.4 Register the Swivel TMG Filter

When installation is complete, you have the option to run the configuration program. Assuming you elect to do so, you will first be prompted to register the filter with TMG. You have a choice of registration types:

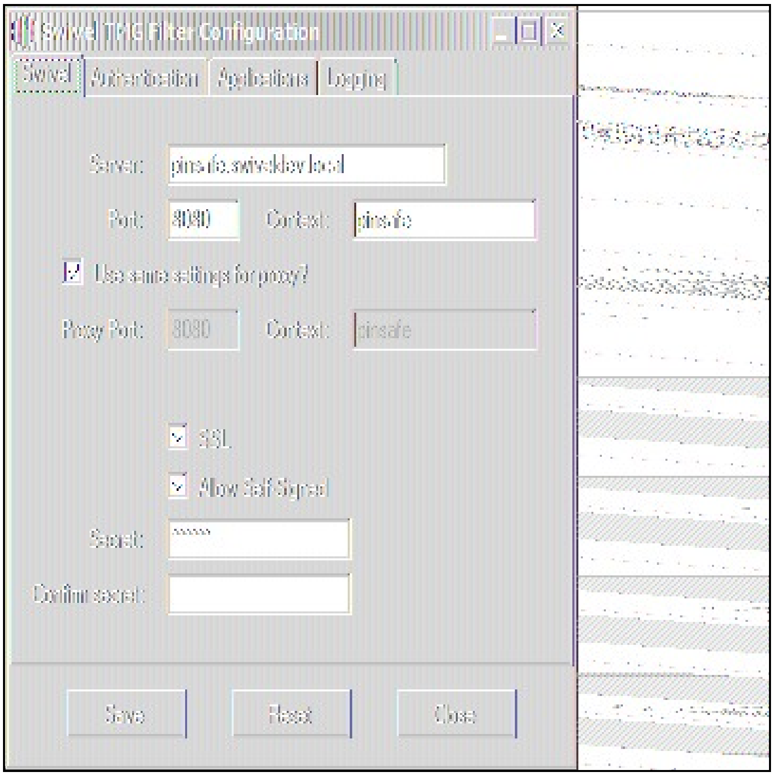

Register Filter
○ Register Automatically
○ Register Single Server
○ Register on Configuration Storage
○ Register on Array Member
○ Register on Config. storage and Member
Register
Cancel

The Automatic registration option should work in most situations. Only try the other options if automatic registration fails.

217.8.5 Configure the TMG filter

Configure the ISA filter using the configuration tool provided. This will optionally run immediately after installation. To start subsequently, select Start/Programs/Swivel TMG Filter/Configuration.

217.8.5.1 Swivel configuration tab



Server: pinsafe.swiveldev.local

Port: 8080 Context: pinsafe

☑ Use same settings for proxy?

Proxy Port: 8080 Context: pinsafe

☑ SSL

☑ Allow Self Signed

Secret: ******

Confirm secret:

Server: is the name or IP address of the Swivel server (Hint: Use hostname to avoid problems with SSL certificates)

Port: is the port on which Tomcat is running. Swivel appliances require the use of XML authentication on port 8080 and the 8443 proxy port should not be used when integrating with TMG. (Hint: Use port 8080)

Context: is the name of the Swivel web application, usually ?pinsafe?. Note when using a Swivel appliance where the proxy port is available, the path Swivel using port 8080 should still be used, the TMG proxy provides security.

Proxy port and **Proxy context** may be required if you are using Pinpad together with an appliance that has the a proxy application that supports Pinpad, but does not have a version of Swivel that supports it directly. In this case, you should use proxy port 8443 and proxy context "proxy". You can still use these values if you are not using Pinpad, but you are using a Swivel appliance.

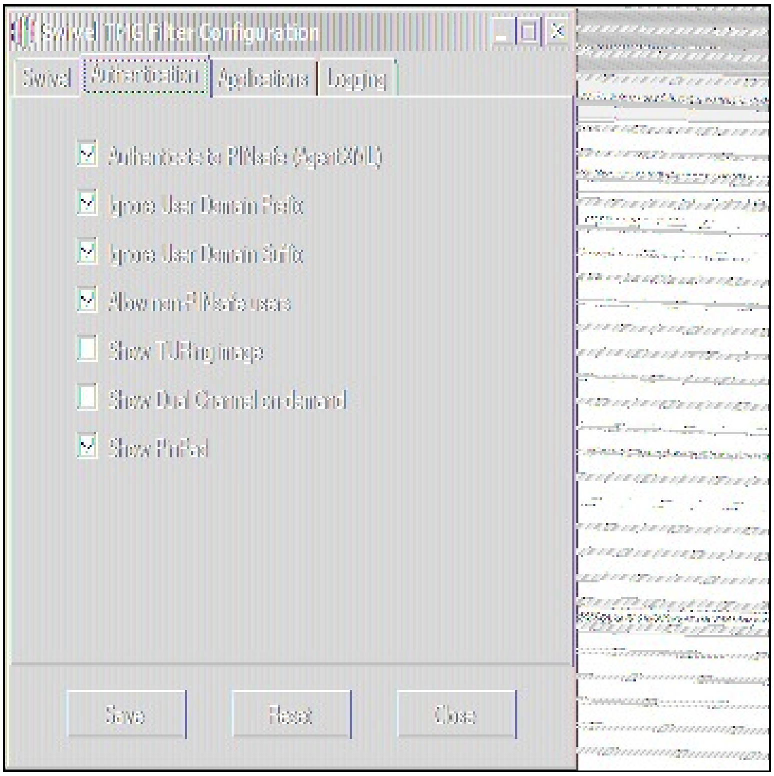
To clarify: the filter will use the proxy port and proxy context to retrieve TURing and Pinpad images (and message on-demand), but will use port and context to authenticate the user.

SSL: will, if checked, send requests to the Swivel server using https, rather than http. This applies to proxy as well: the current filter does not support connecting to one port on HTTP and the other on HTTPS.

Allow self-signed: when checked, causes SSL certificate errors from the Swivel server to be ignored.

Secret: is the shared secret for the Swivel agent for the ISA Server, and needs to be the same as that on the Swivel server. If you change this value, you must enter it twice to confirm the change.

217.8.5.2 Authentication configuration tab



☑ Authenticate to PINsafe (AgentXML)

☑ Ignore User Domain Prefix

☑ Ignore User Domain Suffix

☑ Allow non-PINsafe users

□ Show TURing image

□ Show Dual Channel on demand

☑ Show PinPad

Authenticate to PINsafe (AgentXML): should be checked to use standard Swivel authentication. You should uncheck this if you are using the filter to protect a SharePoint website, as described in the ?Special Considerations for SharePoint? section below. If you uncheck it, Swivel will not directly authenticate the login request. In this case, you should enable RADIUS authentication instead.

Ignore user domain prefix: This will remove the AD domain prefix for users (anything before the '\' symbol), and when Swivel is using the SAM account name it should normally be checked. In this case, if you enter ?domain\user? as the logon username, only ?user? will be sent to Swivel. If it is not checked the prefix will be sent as part of the name to Swivel. If you use the domain prefix option in Swivel, you should uncheck this option.

Ignore user domain suffix: This will remove the AD domain suffix for users (anything after the '@' symbol). You should normally check this if you use sAMAccountName as the username for Swivel, but uncheck if you use userPrincipalName.

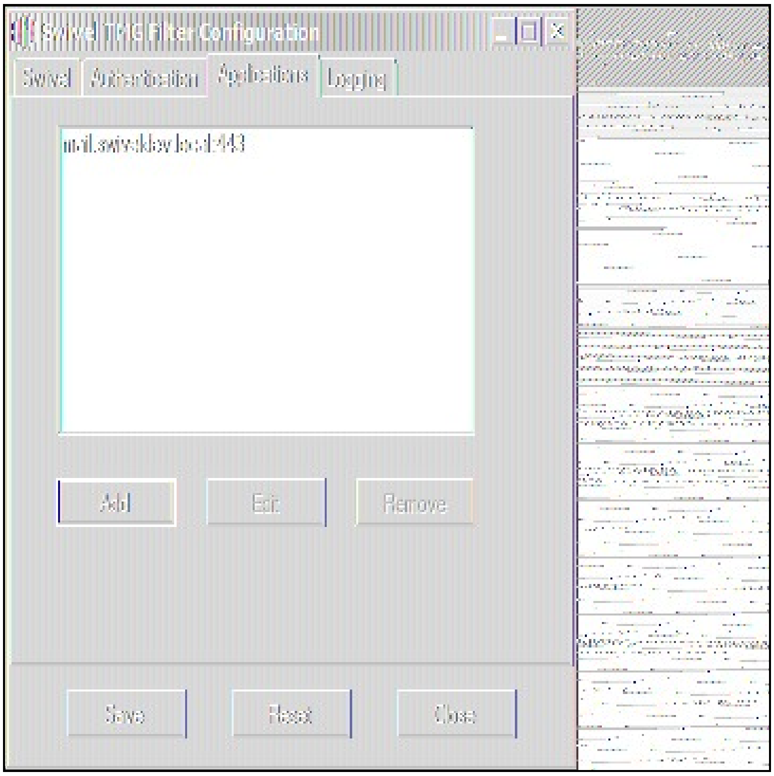
Allow non-PINsafe users: when checked, users not known to Swivel may authenticate using only their AD credentials. This feature is useful for transition to Swivel, where not all users have Swivel accounts. If checked, the OTC field is not shown initially, only when the username is checked and found to exist in Swivel. Note that this feature is not compatible with RADIUS authentication.

Show TURing image: when checked, entering a username or clicking the Start Session button on the login screen will display a TURing image for that user. It is not possible to prevent automatic display of the TURing image (i.e. only display when the button is clicked) from the configuration program, but this can be managed with a simple modification of the login page. Please contact Swivel for more information.

Show Dual Channel on-demand: when checked, a button is displayed allowing the user to request a security string via SMS or email (depending on how the strings transport is configured in Swivel). This option can be used together with the TURing or Pinpad option if required.

Show Pinpad: when checked, a Pinpad display is used to enter the one-time code. This option cannot be used with the TURing option, and requires that you have a version of Swivel or the appliance proxy that supports it.

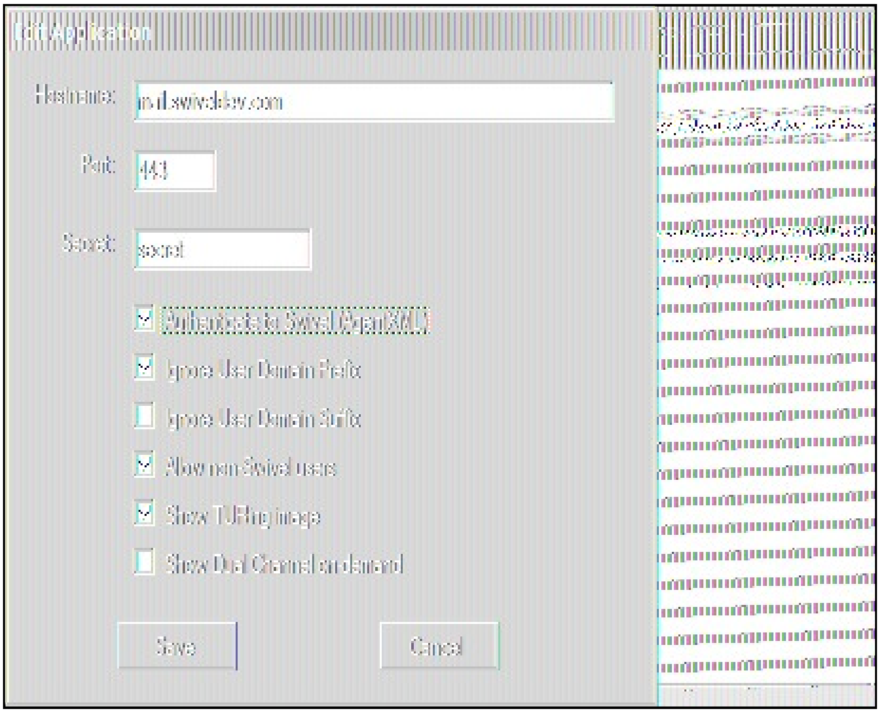
217.8.5.3 Hosts configuration tab



mail.swiveldev.local:443

This feature allows you to configure the filter to behave differently for different host names or ports on the TMG. It is only relevant if you are using the TMG to protect multiple websites.

If you add a new host, you will see the following form:



Hostname: mail.swiveldev.com

Port: 443

Secret: secret

☑ Authenticate to Swivel (AgentXML)

☑ Ignore User Domain Prefix

□ Ignore User Domain Suffix

☑ Allow non Swivel users

☑ Show TURing image

□ Show Dual Channel on demand

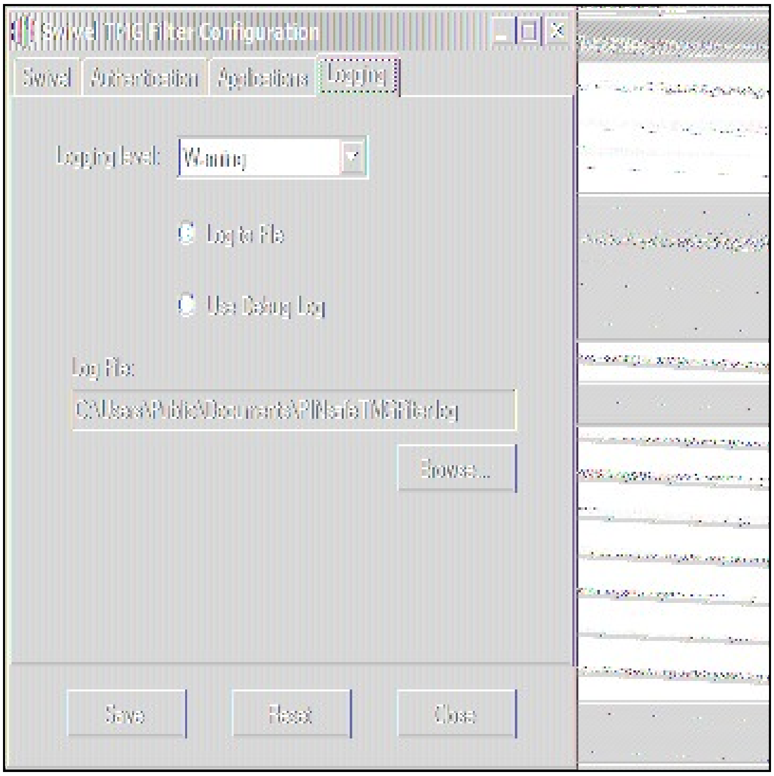
Specify the host name and port that this configuration should apply to. If you leave either one blank, it will apply to all host names on a given port, or all ports for a given host name.

You can specify a different secret from the default here. This allows you to use different Agents in Swivel, so for example, restrict authentication by groups. Swivel supports multiple agents for the same server, provided that the secret is different.

The remaining options override the default options for those particular settings. In particular, if you uncheck "Authenticate to Swivel", you can specify that certain host names do not require Swivel authentication.

If a request comes in that does not match any host name/port combination in this list, the default settings will apply.

217.8.5.4 Logging Configuration tab



Logging level: Warning

○ Log to File

○ Use Debug Log

Log File:
C:\Users\Public\Documents\PINsafeTMGFilter.log

Logging level controls how much data is logged: the levels are Debug, Info, Warning, Errors and None. The last option disables logging entirely. The most verbose level is Debug, and logs every single request received by the filter. It should only be used for troubleshooting.

You can choose to log to a file, or to a debug logger. The latter is provided for backward compatibility only ? you will need to have a debug logger installed to make use of it.

If you choose to log to a file, the default name is C:\Users\Public\Documents\PINsafeTMGFilter.log. Note that the log file does not roll over, but continues to fill up, so depending on what level of logging you use, you will need to back up or delete the log file regularly.

217.8.6 Confirm that the filter has been registered correctly

Once completed the filter will appear in the ISA Server Management Web Filters section. If the filter does not appear in the list of available filters check the Windows system event log for errors.

217.8.7 Modify the Listener

Modify the Listener used to publish OWA or Sharepoint as follows: On the relevant firewall rule, right-click and select properties, select Listener, then click Properties. On the Forms tab, tick the check box labelled ?Use customized HTML forms instead of the default?. For the form set directory, type:

?PINsafeExchange? for Outlook Web Access

and ?PINsafeISA? for Sharepoint or other websites.

Modify the properties for the relevant policy rule, then select Apply, and click OK. Then select the Application Settings tab and UNCHECK the option to use customized HTML. Note that if you have customized your original OWA or Sharepoint login pages, you will need to apply the same customisation to the new Swivel pages. Please consult Swivel support for details of this.

Once you have configured everything, restart the Microsoft Firewall Service on the TMG Server (not just activating TMG). It can take a long time to restart this service, and if you are connecting to the TMG Server via remote desktop, you may be temporarily disconnected from it.

217.9 SSL Certificate Considerations

There would appear to be an issue with certain security updates for TMG Server which prevents HTTP POST requests over SSL unless the target server certificate is fully trusted. This has consequences for the Swivel TMG Filter integration.

If you are not using SSL on your Swivel server, this issue will not affect you.

If you are using SSL, you must have a valid certificate on the Swivel server. This means:

- The certificate date must be current (i.e. not expired)
- The certificate must be issued by a trusted CA (see below for ways of managing this)
- The certificate subject must match the host name used by the TMG Server to connect to the Swivel server. In particular, this means that you must reference the Swivel server by name, not by IP address.

One way to manage this is to get a commercial certificate for the Swivel server. However, this costs money, and if your Swivel server is not internet facing, is not necessary. A second option is if you have an internal certificate authority, you can use that to issue a certificate for the Swivel server (Windows Servers, for example, can optionally be configured as certificate authorities). If you do this, you need to make sure that the certificate authority server certificate is added to the trusted root certificates on the TMG Server, if it is not already. The third option is simply to generate a self-signed certificate on the Swivel server, with the correct host name, and to install that directly into the TMG Server trusted root store.

For more detail, refer to the relevant knowledgebase documentation on generating SSL certificates if you are using a Swivel appliance. Otherwise, refer to the relevant documentation for your operating system.

217.10 Special Considerations for Sharepoint

A security hole has been discovered when using earlier versions of the ISA filter for Sharepoint authentication. It was possible to open a Sharepoint document from within Word (for example) and only provide the standard Active Directory credentials.

The new solution avoids this problem by using RADIUS to authenticate to Swivel, rather than using the ISA filter directly. One minor inconvenience with this is that users must authenticate through the Sharepoint web page before they can access any documents.

Note that if you disable Swivel authentication for Sharepoint, it is also disabled for all other websites. Therefore, if you want to use Swivel authentication on multiple websites for a single ISA Server, they must all use the standard Swivel authentication, or all use RADIUS.

1. On the ISA filter configuration application, uncheck the Authenticate option. This means that Swivel will not authenticate the logon request directly. Instead, you should use RADIUS to perform Swivel authentication, as described below.

2. On the Authentication tab you should check the option ?Collect additional credentials in the form?. This will require you to select ?RADIUS OTP? as the authentication validation method. Click the ?Configure Validation Servers? button, and add the Swivel server as a RADIUS server. Make a note of the shared secret you set for the server.

3. In order for users to be able to open documents from other, non-browser applications once they have authenticated, you must enable persistent cookies. On the Forms tab, click the Advanced button. It is recommended that you select persistent cookies for private computers only. This means that users on public computers will have to open documents from the Sharepoint web site.

4. On the ISA server, create a rule to allow RADIUS authentication from the ISA server to the Swivel server

5. On the Swivel server, enable the RADIUS server (on the RADIUS > Server page). On the RADIUS > NAS page, add the ISA Server as a new NAS, and enter the shared secret you set on the ISA Server. If you wish to restrict access to a particular group of users, select that group, otherwise leave the Group drop-down as ?ANY?.

6. On the policy rule, on the Authentication Delegation tab, select ?NTLM Authentication?.

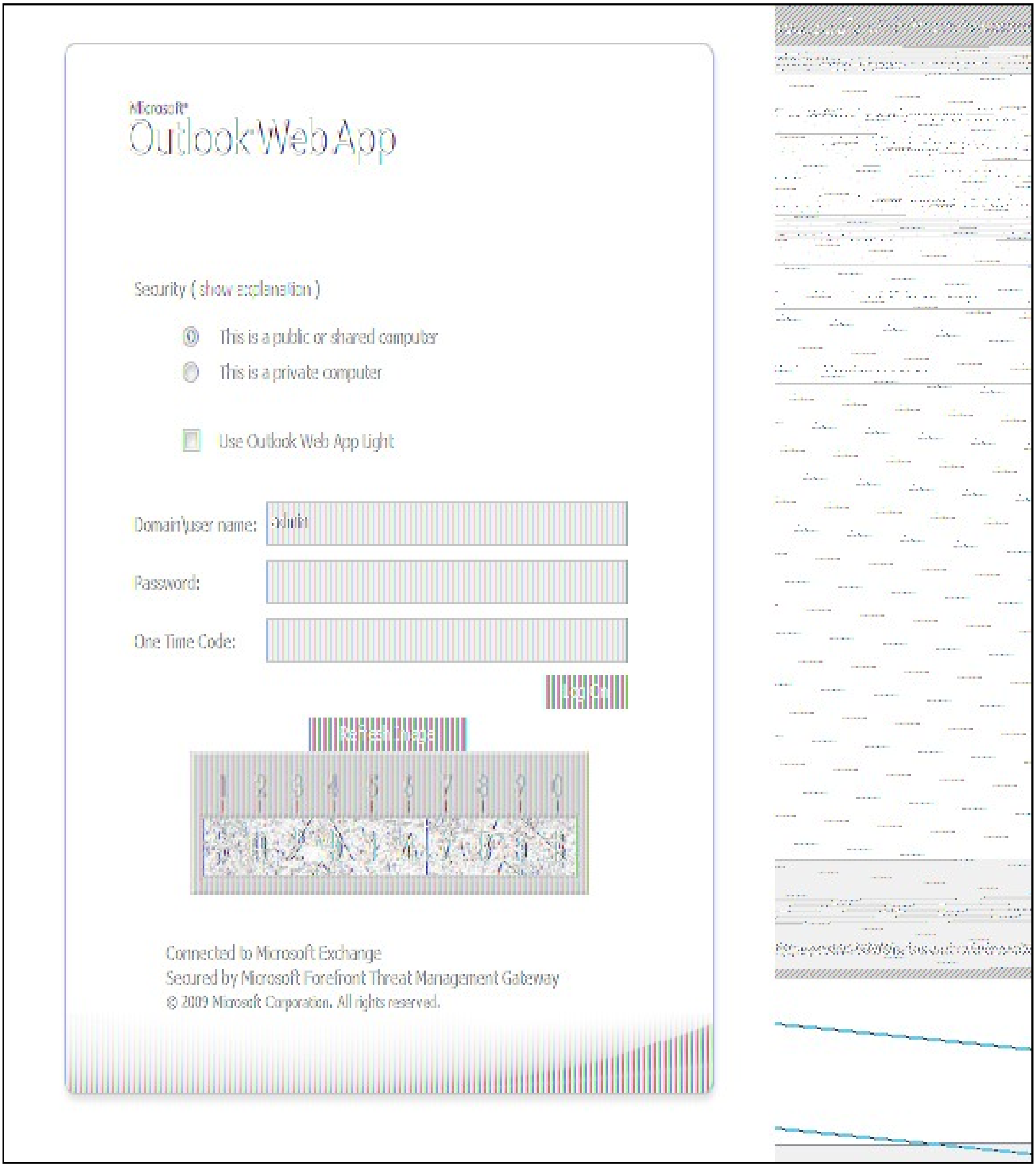
Once you have configured everything, reboot the ISA server.

217.11 Verifying Installation

217.11.1 Outlook Web Access

Navigate to the URL on which TMG Server publishes OWA. The customisation is visible in the addition of a One Time Code field and a Start Session button. Attempting to login with a correct username and password but no one time code should result in failure. Only when a correct Swivel one time code is entered in addition to the Exchange or Sharepoint credentials should the user be logged into OWA.

If you have enabled the option to allow non-Swivel users, then no Swivel customisation will be evident until after you enter the username and move to a different screen. The Swivel additional fields will then appear:



Microsoft®

Outlook Web App

Security (show explanation)

● This is a public or shared computer

○ This is a private computer

□ Use Outlook Web App Light

Domain\user name: admin

Password:

One Time Code:

Connected to Microsoft Exchange
Secured by Microsoft Forefront Threat Management Gateway
© 2009 Microsoft Corporation. All rights reserved.

217.11.2 Sharepoint

Navigate to the URL on which ISA Server publishes Sharepoint. You will notice that there are two sets of credentials to enter. The Swivel credentials are entered in the top part, and the Active Directory credentials in the lower part. Enter the username in the first box as domain\user. Click the Start Session button to get a TURing image. Enter the Swivel password and one-time code in the next two boxes. (NOTE: the Swivel password and one-time code are actually concatenated and submitted as a single value. You can, if you prefer, enter them that way in the Passcode field ? password first).

In the final box, enter your Active Directory password, and click submit.

(NOTE: you actually have to enter different usernames for Swivel and Active Directory ? with the domain prefix for AD and without for Swivel. However, this is handled automatically for you. You will notice, if you fail login, that the Swivel username has changed, and the AD username has been inserted in the lower set of credentials.)

217.12 Additional Options

217.12.1 RADIUS Authentication

Set the Swivel server as the RADIUS server (and add the ISA Server as a NAS on Swivel). If you want to use the TURing image, then the Swivel ISA filter is required, but disable authentication in the filter configuration. Swivel RADIUS custom login pages provided with the filter can be used.

217.12.2 Automatic sending of SMS

The login page can be configured to automatically send the user an SMS message when they have entered the username and proceed to the next field. On a default installation, edit the file "C:\Program Files\Microsoft Threat Management Gateway\Templates\CookieAuthTemplates\PINsafeExchange\HTML\usr_pwd.htm".locate the following lines:

locate the following

function setUserExists(attribute)

Approximately 20 lines below this, you should find the following section:

```
if (btnMessage) {
if (showMessage) {
btnMessage.style.display = "";
} else {
btnMessage.style.display = "none";
}
}
```

Insert a new line, as follows:

```
if (btnMessage) {
if (showMessage) {
btnMessage.style.display = "";
ShowMessage();
} else {
btnMessage.style.display = "none";
}
}
```

Once you have made this change and saved the file, you have to restart the Microsoft Gateway service for the change to take effect. Also, be aware that you need to make the same change on all TMG servers in the farm.

These instructions assume you have the latest version of the TMG filter.

217.12.3 Removing the OTC button

If you don't want the button to appear at all, on a default installation, edit the file "C:\Program Files\Microsoft Threat Management Gateway\Templates\CookieAuthTemplates\PINsafeExchange\HTML\usr_pwd.htm". Locate the following lines:

<input class="btn" id="btnImage" type="button" value="@@L_StartSession_Text" onclick="ShowTuring();" />

<input class="btn" id="btnMessage" type="button" value="@@L_SendMessage_Text" onclick="ShowMessage();" />

and delete them.

Once you have made this change and saved the file, you have to restart the Microsoft Gateway service for the change to take effect. Also, be aware that you need to make the same change on all TMG servers in the farm.

These instructions assume you have the latest version of the TMG filter.

217.12.4 Disabling the Auto TURing feature

When a TURing image is generated it expects the user to authenticate with that image for the length of the Session Cleanup.

When using the XML authentication the automatic display of the TURing image can be prevented by editing the file: "C:\Program Files\Microsoft Threat Management Gateway\Templates\CookieAuthTemplates\PINsafeExchange\HTML\usr_pwd.htm". Delete the line *ShowTuring();* within the function *setUserExists(attribute)*.

217.13 Uninstalling

217.13.1 Modify the Listener

Modify the Listener used to remove OWA or Sharepoint as follows: On the relevant firewall rule, right-click and select properties, select Listener, then click Properties. On the Forms tab, remove the tick the check box labelled ?Use customized HTML forms instead of the default?. For the form set directory, remove:

?PINsafeOWA? for Outlook Web Access

Modify the properties for the relevant policy rule.

Then select Apply, and click Ok. Then select the Application Settings tab and CHECK the option to use customized HTML.

Uninstall the Swivel software using the Remove Programs.

reboot the ISA server

217.14 Known Issues

217.15 Troubleshooting

NOTE: After any changes are made, always restart the Microsoft Firewall service

With regard to the Single Channel TURing image, the TMG server login page does not use SCImage directly: the image request comes through the filter, so that the the Swivel server does not need to be accessed directly from the internet. If the filter is not working, then no image will appear.

217.15.1 Filter status Check

This should be made in a web browser against the TMG login.

https://<path_to_TMG server>/PINsafeTMGFilter.dll?usepinsafe

This should return a series of 0s and 1s, Example: 10100110, the order can show the status as below:

1 - Show one-time code field

2 ? Allow unknown users

3 ? Show TURing image

4 ? Show Message on demand

5 - Show Pinpad

6 ? Ignore domain prefix

7 ? Ignore domain suffix

If it cannot contact the Swivel server, or if the filter is disabled, the first digit will be 0. NOTE: for versions of the TMG earlier than 1.4, the PINpad flag is not present.

217.15.2 Enabling Swivel logging

The Swivel authentication filter can optionally log its activity to a file. By default, no logging takes place, but you can enable logging by editing the filter registry key directly, using Regedit. The key to edit is

\\HKEY_LOCAL_MACHINE\Software\Swivel Secure\PINsafeTMGFilter

Create a DWORD value named "LogOptions". Set it to 2 to enable logging to a file. Set it to 1 to enable logging to the Windows debug log (see below), or 3 to enable both. Setting it to 0, or omitting it entirely, results in no logging.

The default log file is

C:\Users\Public\Documents\PINsafeTMGFilter.log

If you want to log to a different file, create a String registry value in the filter key named "LogFile", and set the value to the full path of the log file.

Older versions of the filter always log activity to the standard Windows debug log. Newer versions can optionally do this as well. This can be accessed using a tool such Sysinternals DebugView available as freeware from:

Sysinternals DebugView

To include logging of output from the filter the option Capture Global Win32 must be enabled in the Capture menu.

217.15.3 Single Channel image does not appear

- Check Swivel TMG filter settings
- Use a fully qualified hostname instead of IP address for the Swivel server
- Is an SSL connection being used
- Is a self signed cert being used, if so try without SSL using http or install a valid public certificate
- Is the certificate using the internal hostname or the external hostname? The hostname used by Swivel must match the certificate hostname.
- Check the Swivel TMG filter is correctly installed. On the TMG Server Management: under System, on the Web Filters tab, "Swivel Authentication Filter" should be enabled
- From the TMG server check a Single Channel image can be generated in a web browser connecting to the Swivel server using:

Swivel appliance

https://<PINsafe server IP>:8080/pinsafe/SCImage?username=test

or

https://<PINsafe server IP>:8443/proxy/SCImage?username=test

For a software only install see Software Only Installation

- If you see a red cross where the Single Channel Image should be right click on it and select properties. Copy the Address (URL) which should look something like: https://<ISA URL>/PINsafeISAFilter.dll?username=graham&random=197405. Copy this line and paste into the URL bar of the web browser and see if a Single Channel Image is generated.

If a user is able to login without the One Time Code, then the TMG filter may not be installed.

If IP addresses, rather than host names is used, with SSL enabled, you must check the option to "permit self-signed certificates". This option actually means to ignore all certificate errors, as you will get when referencing a server by the IP address, rather than the name.

217.15.4 Page fails to display after failed login

An **Access Forbidden message** is displayed. After a login failure, the user is redirected to https://hostname/, rather than https://hostname/owa. You can configure the TMG firewall rule to automatically redirect to /owa. This external link shows how to configure this redirect: Setting up an OWA redirect in Forefront TMG 2010 the easy way

217.15.5 Adding Swivel authentication stops other pages appearing

You can specify that PINsafe authentication only applies to certain host names, in which case the others are ignored. On the Swivel TMG filter disable Swivel authentication in the default configuration, then add an application with the host name that DOES require authentication, and set Swivel authentication ON for that one only, or if you want to be explicit, add all three host names, and disable Swivel authentication for the ones you don't want.

217.16 Additional Information

Information regarding the configuration of TMG Server to publish OWA or Sharepoint may be found in the TMG Server help under Firewall policy.

For assistance in Swivel installation and configuration please contact your reseller.

218 Microsoft TMG RADIUS Integration

219 Microsoft Threat Management Gateway Integration

This guide describes how to integrate Swivel with Microsoft Forefront Threat Management Gateway using RADIUS authentication. No additional software is required.

If you want more control over authentication, with support for restricting Swivel to certain hostnames and allowing non-Swivel users to authenticate, see the TMG filter documentation for more information.

219.1 Configuring Swivel

- Log on to the Swivel Admin Console
- Under RADIUS -> Server, make sure that the server is enabled. All the other settings can be left as default.
- Under RADIUS -> NAS, enter a name in the blank identifier box (e.g. ?TMG?). Enter the name or IP address of the TMG server, and a chosen secret. Remember what you enter in the Secret box, as you will need it later.
- Click Apply.

219.2 Configuring Firewall Rules

It is assumed that you already have a firewall rule set up to support the website you need to protect. If not, use the appropriate wizard under Firewall Policy Tasks to set up the rule.

219.2.1 Modifying the Website Access Rule

To support Swivel authentication, all you need to do is to right-click on the Listener for the rule and select Properties. On the Authentication tab, select HTML Form Authentication, if it is not already selected.

Under most circumstances, you will need to authenticate to Windows Active Directory as well as to Swivel. Configure both AD and Swivel as authentication servers. To use Windows and Swivel authentication, check the box marked ?Collect additional delegation credentials in the form?. Make sure ?RADIUS OTP? is selected in the lower box, then click on ?Configure Validation Servers?. On the RADIUS Servers tab, click Add. Enter the IP or name of the Swivel server and the shared secret that you entered earlier for the Swivel NAS.

If you only want to use Swivel to authenticate, and no other method, then leave the option for additional delegation credentials unchecked and select either RADIUS or RADIUS OTP. You can only select RADIUS OTP if the Authentication Delegation option on the main rule is No Delegation.

NOTE: As described below, you may choose to create a new set of custom login pages, rather than replacing the existing ones. If you do, you will need to check the option to use custom HTML forms (on the Forms tab), and enter the name of the custom forms set.

219.2.2 Proxying the TURing Image

In order to allow Swivel to deliver a TURing image to the end user without exposing the Swivel server to the internet, it is necessary to create a firewall rule to proxy it. If you are using dual channel only, except for dual channel on demand, you can skip this step.

- Click on Publish Web Sites.
- Call the rule Swivel Image, or as required.
- Accept the defaults for the first few steps.
- Under internal site name, enter the name of the Swivel server. Note that this name must match the name of the SSL certificate on the Swivel server, since SSL requests through this rule must not generate any errors. Alternatively, you can configure Swivel not to use HTTPS.
- For Path, enter /proxy/SCImage (assuming this is an appliance, or /pinsafe/SCImage if not). For dual channel on demand, change SCImage to DCMessage.
- Select Any domain name.
- Create a new Listener. Call it TURing, or whatever you like.
- Require SSL (if you don't have an SSL certificate installed, select non-SSL)
- Select External networks only
- Select an SSL certificate if required
- Select No Authentication
- The remaining Listener options do not require configuration
- Back on the publishing wizard, accept the defaults for the remaining options.
- Once the rule is complete, right-click and select Properties
- On the Bridging tab, choose to redirect to port 8443 for context /proxy, or 8080 for context /pinsafe.

219.3 Customising Login Pages

If you are using dual channel authentication in Swivel, and do not require an embedded TURing image in your login page, you do not need to customise the login pages. This does not apply to dual-channel on-demand, for which the customisation IS required.

You can choose either to customise the default login pages, or to create a custom set of pages. If you are not using Swivel for all authentication rules on this TMG, you must create a custom set.

To create a custom set of rules:

- In Explorer, go to the TMG root folder: under a default installation, this is C:\Program Files\Microsoft Forefront Threat Management Gateway.
- Select the Templates sub-folder
- Select the CookieAuthTemplates sub-folder.
- Make a copy of one of the folders you find underneath here: for an Exchange firewall rule, select Exchange, and for other rules select ISA.
- Give the folder an appropriate name. NOTE: remember to change the custom forms option on the listener to specify the name of this folder.

If you choose to replace the existing login pages, select the CookieAuthTemplates folder as described above, then select either the ISA sub-folder, or the Exchange sub-folder, depending on whether or not you are customising Exchange access. If you have created a custom set, select that. Select the HTML sub-folder.

NOTE: if you are replacing existing standard login pages, make sure you take backup copies of any files you replace.

There are 3 files you might need to replace, depending on which authentication option you selected:

- For RADIUS authentication only, replace usr_pwd.htm
- For RADIUS OTP authentication only, replace usr_pcode.htm
- For dual Windows and RADIUS OTP authentication, replace usr_pwd_pcode.htm

The custom pages can be found here.

You will need to edit the file(s), and change the value of imageUrl to the appropriate external URL for the TURing image, as determined by the firewall rule you created earlier.

219.3.1 Changing the OTC button text

To change the OTC label, edit the following file:

C:\Program Files\Microsoft Forefront Threat Management Gateway\Templates\CookieAuthTemplates\PINsafeExchange\HTML\usr_pwd.htm.

Search for OTC as a whole word. You should find the following line:

```
                  <td class="nowrap"><label for="otc">OTC</label></td>
```

Change the prompt as required, and restart the firewall service.

219.3.2 Automatic sending of SMS

The login page can be configured to automatically send the user an SMS message when they have entered the username and proceed to the next field. On a default installation, edit the file "C:\Program Files\Microsoft Threat Management Gateway\Templates\CookieAuthTemplates\PINsafeExchange\HTML\usr_pwd.htm".locate the following lines:

locate the following

function setUserExists(attribute)

Approximately 20 lines below this, you should find the following section:

```
if (btnMessage) {
if (showMessage) {
btnMessage.style.display = "";
} else {
btnMessage.style.display = "none";
}
}
```

Insert a new line, as follows:

```
if (btnMessage) {
if (showMessage) {
btnMessage.style.display = "";
ShowMessage();
} else {
btnMessage.style.display = "none";
}
}
```

Once you have made this change and saved the file, you have to restart the Microsoft Gateway service for the change to take effect. Also, be aware that you need to make the same change on all TMG servers in the farm.

These instructions assume you have the latest version of the TMG filter.

219.3.3 Removing the OTC button

If you don't want the button to appear at all, on a default installation, edit the file "C:\Program Files\Microsoft Threat Management Gateway\Templates\CookieAuthTemplates\PINsafeExchange\HTML\usr_pwd.htm".locate the following lines:

<input class="btn" id="btnImage" type="button" value="@@L_StartSession_Text" onclick="ShowTuring();" />

<input class="btn" id="btnMessage" type="button" value="@@L_SendMessage_Text" onclick="ShowMessage();" />

and delete them.

Once you have made this change and saved the file, you have to restart the Microsoft Gateway service for the change to take effect. Also, be aware that you need to make the same change on all TMG servers in the farm.

These instructions assume you have the latest version of the TMG filter.

219.4 Troubleshooting

The thing you are most likely to have problems with in this integration is SSL certificates. When linking to a server that requires SSL, the TMG will fail if there are any errors in SSL handshaking. The guidelines here should help.

NOTE: to import a certificate from a Swivel appliance into a TMG to use as a proxy for the Swivel server, you must generate the private key with the argument -keyalg RSA. This is NOT the default when using the CMI options, so the certificate must be generated from the command line.

If you create SSL certificates using an internal Windows certificate authority, and generate the certificate request from the web interface, be aware that certificates generated using the Web Server template are not exportable. You need to create a new template for exportable web server certificates, as detailed here. Also, TMG does not support CNG / Windows 2008 certificates, so when creating the new template, make sure you select Windows 2003 compatibility. For the same reason, if you generate a new certificate request using the certificates MMC plug-in (details not given here), make sure you select Legacy rather than CNG. Our recommendation, however, is to use Keystore Explorer (see SSL Solutions) and to generate the certificate request with that.

As a last resort, particularly if the Swivel Appliance is not to be visible on the internet, you can simply disable HTTPS on the Swivel server. See the appliance documentation for details on this. Note that if you do disable https, you must alter the TURing Listener to match the settings.

If users are allowed to authenticate without Swivel authentication ensure 'Require all users to authenticate' option is checked.

220 Category:TMG

221 Microsoft UAG Integration

221.1 Introduction

This configuration document outlines how to integrate Swivel with Microsoft Forefront Unified Access Gateway using Active Directory authentication in addition to the Swivel authentication.

If installing Swivel on the UAG appliance it may be required to install Swivel to use a different port than the default 8080.

221.2 Prerequisites

Microsoft Forefront Unified Access Gateway

UAG and URL rewriting documentation

Swivel 3.x server with ChangePIN

ChangePIN configuration document

The following files are required to be uploaded to the UAG

images.asp

login.asp (Rename loginturingsms.asp as login.asp)

Portalname1postpostvalidate.inc

Token.inc

The files can be downloaded from here: UAG Files

UAG Update 1 requires a modified login page, this additional file can be downloaded here: UAG Update 1 Files

UAG SP1 through to SP4 requires modified login pages, the complete set of files can be downloaded here: UAG SP1 Files

UAG SP1 through to SP4 SMS only request button login also UAG SP1 through to SP4 TURing only request button login

RADIUS ChangePIN for UAG, backup then replace the file LoginContinue.asp

221.3 Baseline

Microsoft Forefront Unified Access Gateway 1.0.1101.0

Swivel 3.5

221.4 Architecture

The UAG makes authentication requests against the Swivel server by RADIUS or XML.

221.5 Installation

221.5.1 Configure The Swivel Server

221.5.1.1 Configure a RADIUS NAS entry

1. Ensure the RADIUS server is running on Swivel

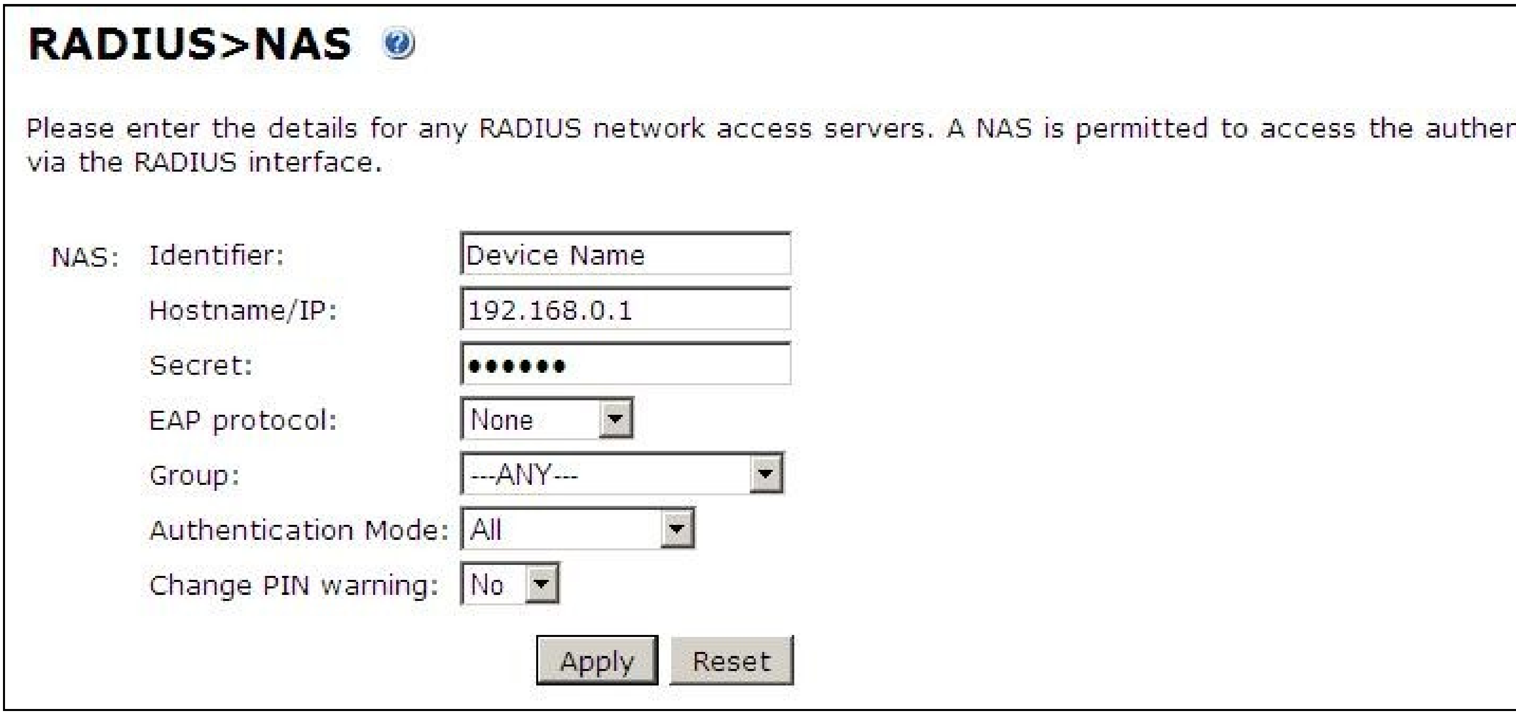
2. On the Swivel administration Console select RADIUS NAS

3. Enter a name for the NAS

4. Enter the UAG internal IP address

5. Enter the shared secret

6. Click on Apply to save changes



RADIUS>NAS

Please enter the details for any RADIUS network access servers. A NAS is permitted to access the auther
via the RADIUS interface.

NAS: Identifier: Device Name

Hostname/IP: 192.168.0.1

Secret: ●●●●●●

EAP protocol: None

Group: ---ANY---

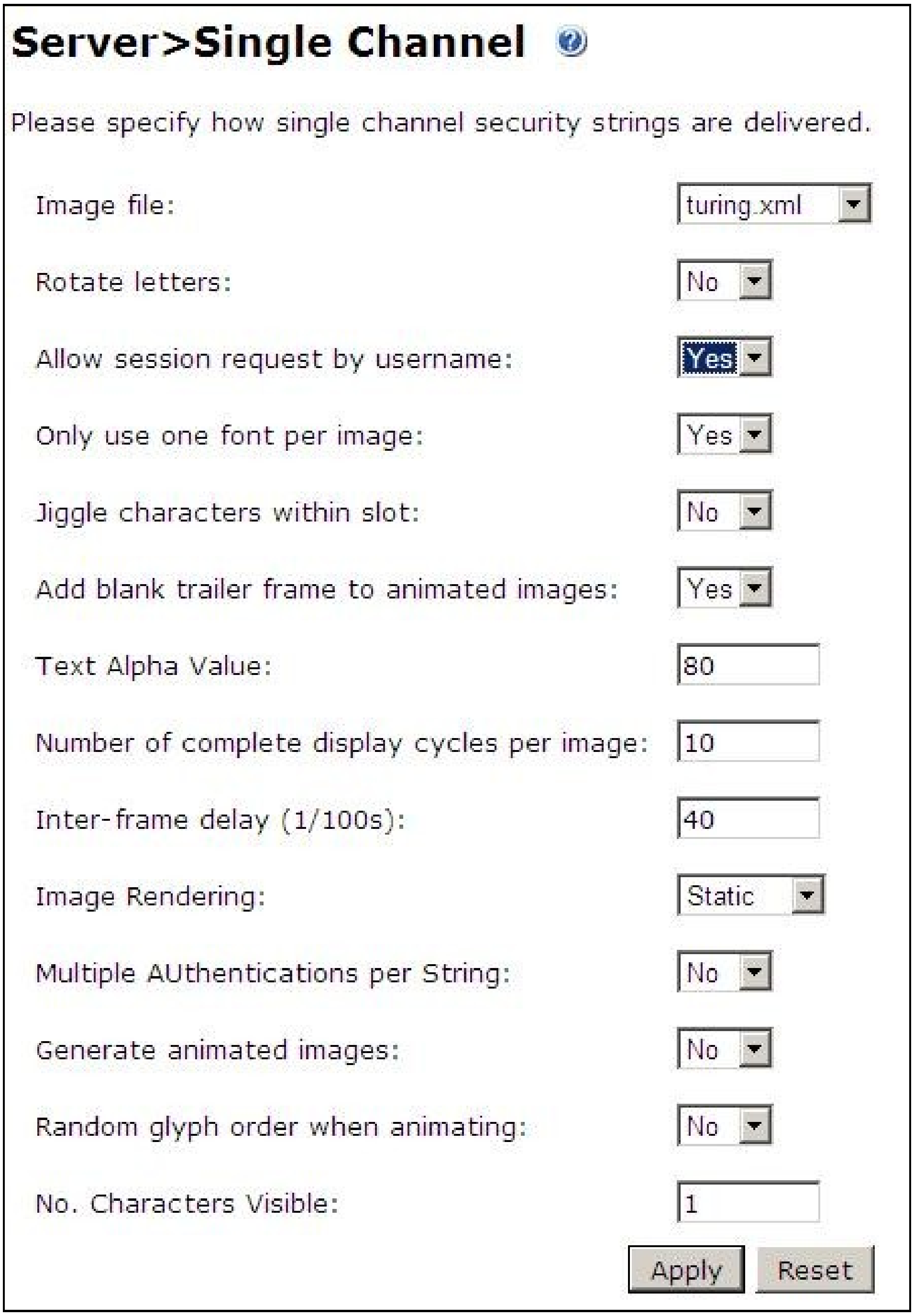
Authentication Mode: All

Change PIN warning: No

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

221.5.2 Configure the UAG

221.5.2.1 Edit the UAG Configuration Files

Edit the file images.asp with the below URL to represent the Swivel server IP address and Swivel install name:

```
objWinHttp.Open "GET", "https://<hostname_of_pinsafe>:8443/proxy/SCImage?username=" & request.querystring("username"),false
```

Where <hostname_of_pinsafe> is your Swivel server hostname.

Then edit Token.inc with the required shared secret:

```
m_secret = "<secret>"
```

Where <secret> is your secret (do not enter the angle brackets).

221.5.2.2 Copy the Configuration files

Note: Ensure any existing files are backed up first.

1. Copy Token.inc and Portalname1postpostvalidate.inc to: <path to UAG install>\von\InternalSite\inc\CustomUpdate

2. Copy login.asp file to: <path to UAG install>\von\InternalSite\CustomUpdate

3. Copy images.asp to: <path to UAG install>\von\InternalSite\Images\CustomUpdate

221.5.2.3 Configure the TMG

Create a Threat Management Gateway rule to allow access from the UAG to the Swivel server

On the TMG configuration select New Access Rule and create a rule to allow traffic from the UAG to the Swivel server.

Port 8443 (or port 8080 for software installs, older virtual or hardware appliances and when using XML authentication)

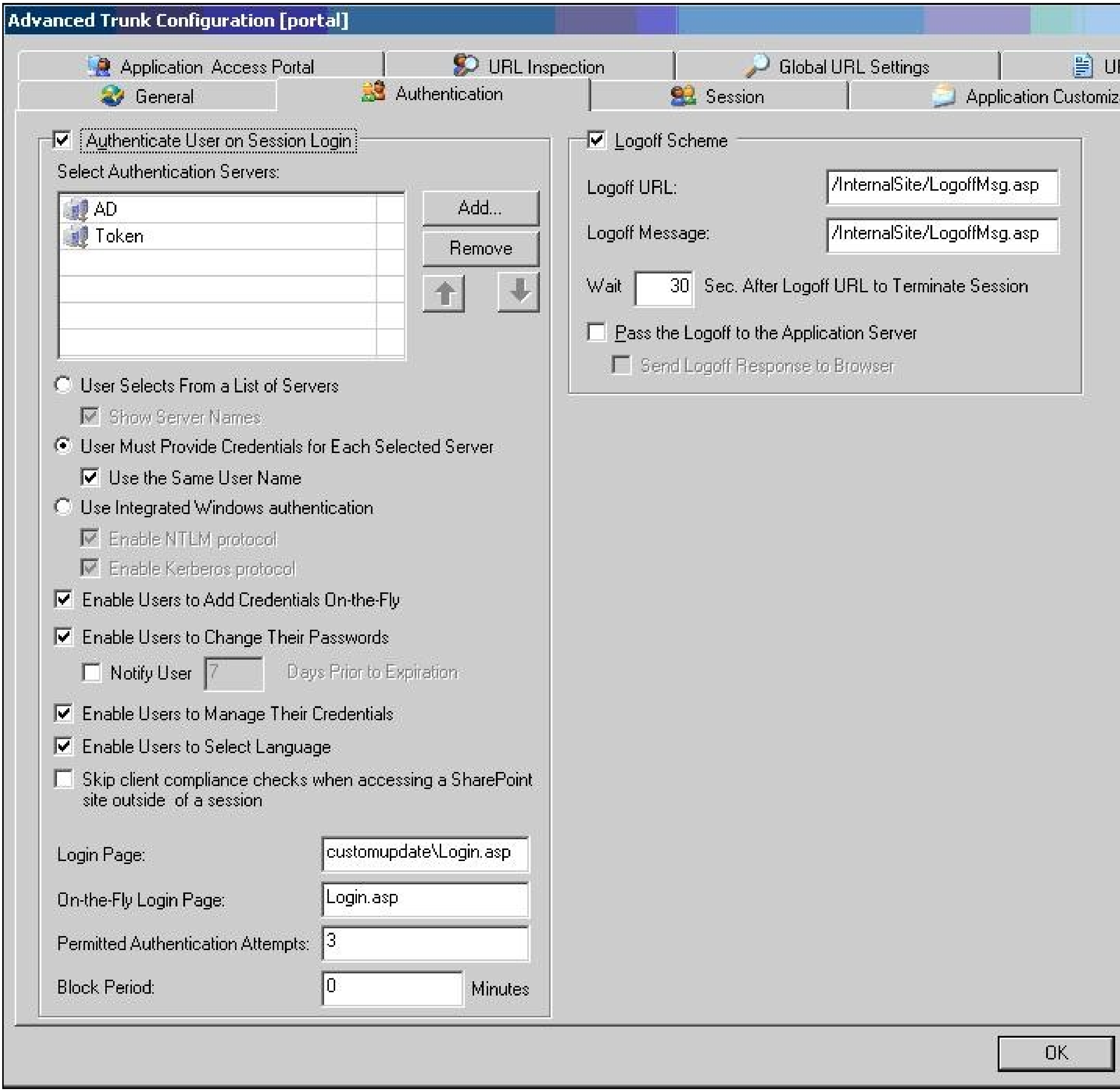
From Local Host (i.e. the UAG)

To Swivel Server (or Internal Network)

Outbound Traffic

221.5.2.4 Configure Login Page

Select the UAG Configuration GUI, From the Advanced Trunk Configuration select Authentication and set the Login Page to customupdate\Login.asp. This can be changed to reflect a different install location or trunk.



☑ Authenticate User on Session Login

Select Authentication Servers:

AD
Token

○ User Selects From a List of Servers

☑ Show Server Names

● User Must Provide Credentials for Each Selected Server

☑ Use the Same User Name

○ Use Integrated Windows authentication

☑ Enable NTLM protocol

☑ Enable Kerberos protocol

☑ Enable Users to Add Credentials On-the-Fly

☑ Enable Users to Change Their Passwords

□ Notify User 7 Days Prior to Expiration

☑ Enable Users to Manage Their Credentials

☑ Enable Users to Select Language

□ Skip client compliance checks when accessing a SharePoint site outside of a session

Login Page: customupdate\Login.asp

On-the-Fly Login Page: Login.asp

Permitted Authentication Attempts: 3

Block Period: 0 Minutes

☑ Logoff Scheme

Logoff URL: /InternalSite/LogoffMsg.asp

Logoff Message: /InternalSite/LogoffMsg.asp

Wait 30 Sec. After Logoff URL to Terminate Session

□ Pass the Logoff to the Application Server

□ Send Logoff Response to Browser

221.5.2.5 RADIUS authentication Configuration

Swivel can be configured as the Primary authentication server or more usually is configured as a secondary authentication server. When using Swivel as a secondary authentication such as with Active Directory, ensure that the options for secondary authentication are selected.

To enable RADIUS authentication create a repository of type ?RADIUS? on the UAG configuration.

To use RADIUS do the following-

1. Access the UAG configuration GUI.

2. Click on Admin Authentication Users/Group repository

3. Select New to create a new repository

4. In the drop down menu, select ?RADIUS? and in the Name field enter Swivel RADIUS

5. Enter the IP of the Swivel server. Note, when using a Swivel HA pair, do not use the VIP address for RADIUS authentication, but use the real IP address.

6. Enter port 1812

7. If required enter a second IP/port

8. Enter a shared secret key of the same value as the Swivel server

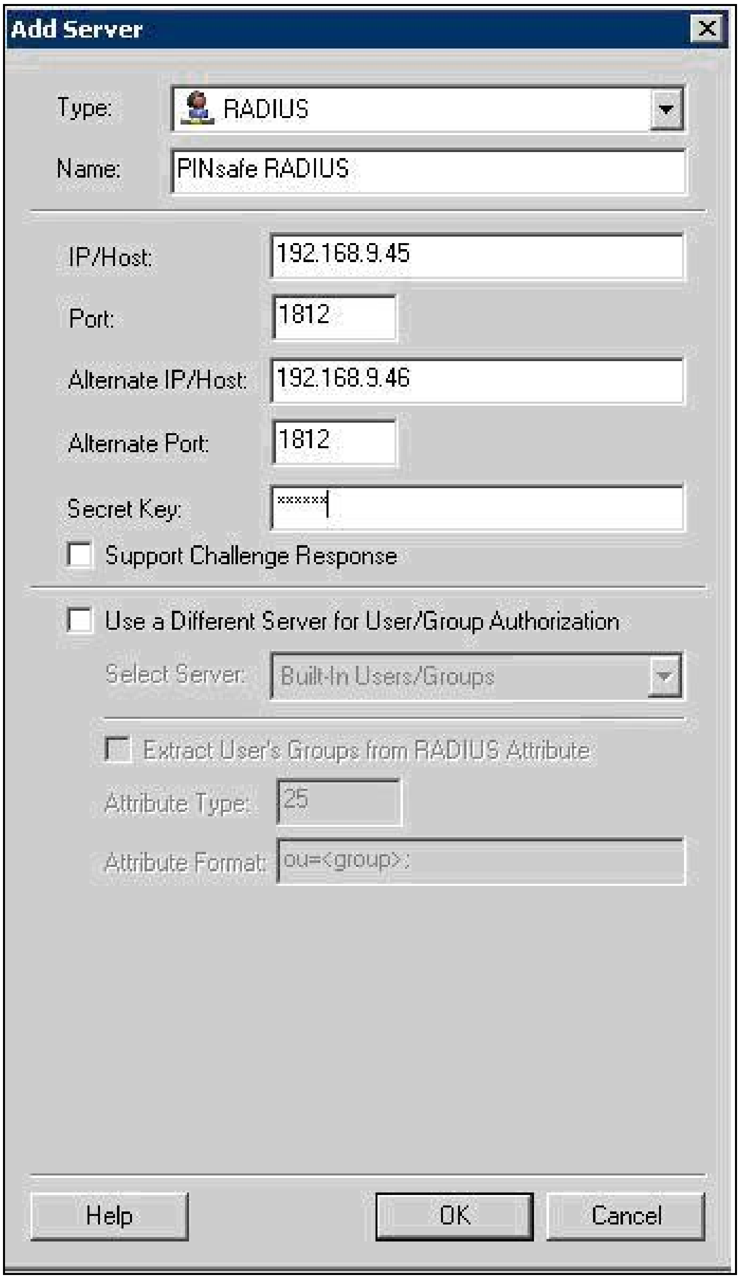
9. Click on Add and apply this repository to the relevant trunk.

10. Ensure User must enter credentials for each server is selected.

11. If AD password is to be entered ensure that an AD authentication server is specified.

12. Activate the configuration

13. Configure Swivel as a RADIUS server



Add Server

Type: RADIUS

Name: PINsafe RADIUS

IP/Host: 192.168.9.45

Port: 1812

Alternate IP/Host: 192.168.9.46

Alternate Port: 1812

Secret Key: ******

□ Support Challenge Response

□ Use a Different Server for User/Group Authorization

Select Server: Built-In Users/Groups

□ Extract User's Groups from RADIUS Attribute

Attribute Type: 25

Attribute Format: ou=<group>;

221.5.2.6 Configuring the URL rewriting rules

To allow access to the images.asp

1. Select the required Trunk

2. Select Configure from the Advanced Trunk Configuration

3. Select the ?URL Set? Tab

4. Add a rule to permit access to the images.asp

InternalSite_Rule100

Note: This must be named InternalSite_Rule, example: InternalSite_Rule100 (use a high number to prevent it being overwritten by updates)

With parameters of:

Action: Accept

URL: /internalsite/images/customupdate/images.asp

Note: You can use /internalsite/images/customupdate/* for testing, and add additional rules to check the input.

Parameter: Handle (i.e. handle any parameters. For troubleshooting it may be useful to set this to ignore).

Method: Get

To Allow access to Swivel specific parameters:

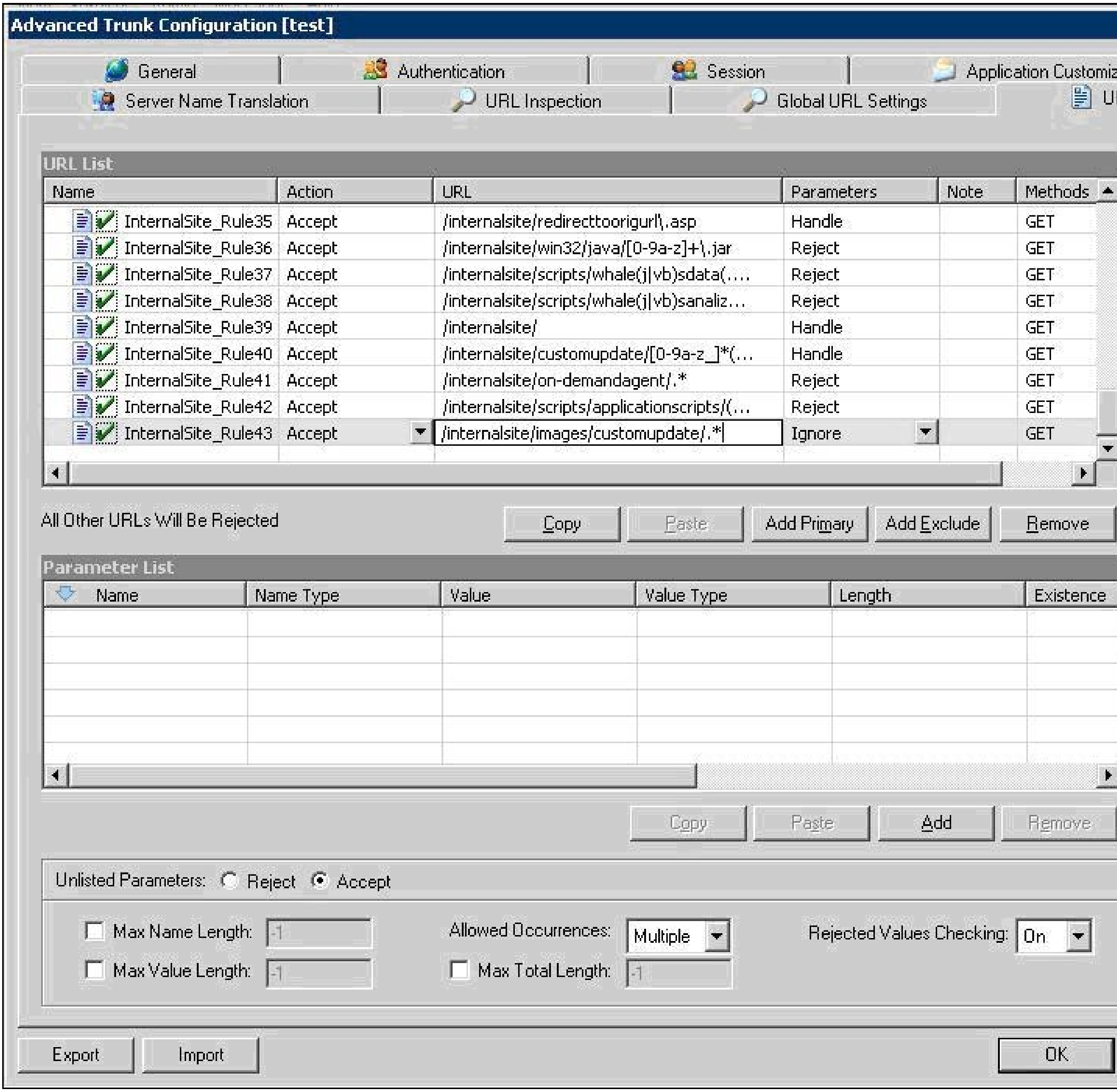
Under Parameters select Add, add the following values:

Parameter 1:

- Name: username
- Name Type: String
- Value: ?[a-z0-9]+? (this is a basic regex and may need changing depending on the users username policy)
- Value Type: String
- Length: 1:100 (may need to up 100 depending on customer username length)
- Existence: Mandatory
- Occurrences: Single
- Max total length: -1
- Rejected values checking: on

Parameter 2:

- Name: random
- Name Type: String
- Value Type: Integer
- Existence: Optional
- Occurrences: Single
- Max total length: -1
- Rejected values checking: on



Name	Action	URL	Parameters	Note	Methods
InternalSite_Rule35	Accept	/internalsite/redirecttoorigurl\.asp	Handle		GET
InternalSite_Rule36	Accept	/internalsite/win32/java/[0-9a-z]+\.jar	Reject		GET
InternalSite_Rule37	Accept	/internalsite/scripts/whale(j|vb)sdata(....	Reject		GET
InternalSite_Rule38	Accept	/internalsite/scripts/whale(j|vb)sanaliz...	Reject		GET
InternalSite_Rule39	Accept	/internalsite/	Handle		GET
InternalSite_Rule40	Accept	/internalsite/customupdate/[0-9a-z_]*(...	Handle		GET
InternalSite_Rule41	Accept	/internalsite/on-demandagent/.*	Reject		GET
InternalSite_Rule42	Accept	/internalsite/scripts/applicationscripts/(...	Reject		GET
InternalSite_Rule43	Accept	/internalsite/images/customupdate/.*	Ignore		GET

All Other URLs Will Be Rejected

Name	Name Type	Value	Value Type	Length	Existence

Unlisted Parameters: ○ Reject ● Accept

□ Max Name Length: -1

Allowed Occurrences: Multiple

Rejected Values Checking: On

□ Max Value Length: -1

□ Max Total Length: -1

Edit Rule to allow Access to the validate.asp

1. Select the validate.asp rule (Usually Internal_Rule2)

2. Under Parameters select Ignore

Alternatively add the following to the parameters list:

Turing

SMS

To Allow access to Swivel specific parameters:

Select the InternalSite_Rule2

Under Parameters select Add, add the following values:

Name: swivel

Name Type: String

Value:

Value Type: String

Length: 1:100

Existence: Optional

Occurrences: Multiple

Max total length: -1

Rejected values checking: on

Also add a Parameter with the following values:

Name: orig_url

Name Type: String

Value:

Value Type: String

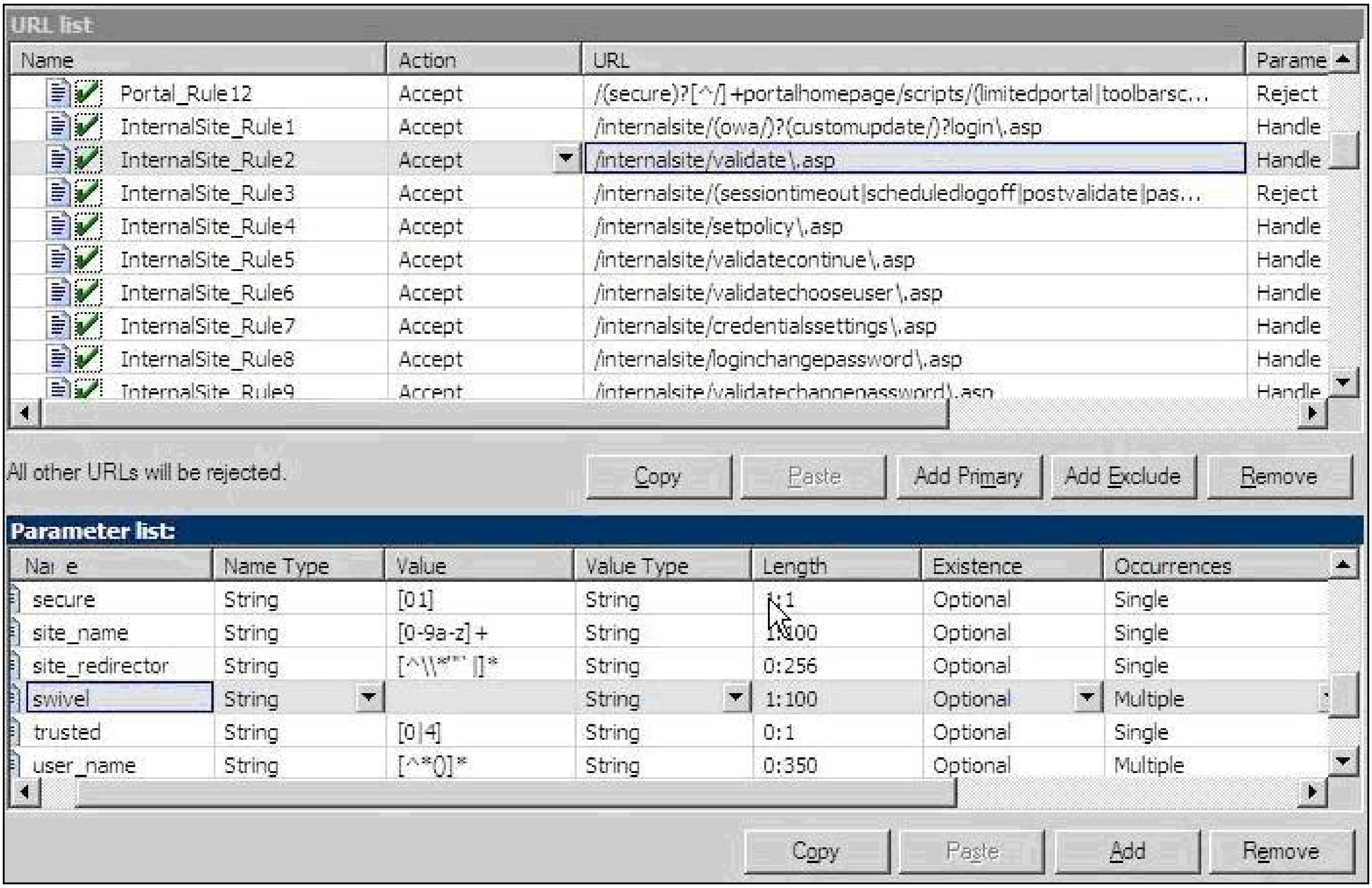
Length: 1:200

Existence: Optional

Occurrences: Multiple

Max total length: -1

Rejected values checking: on



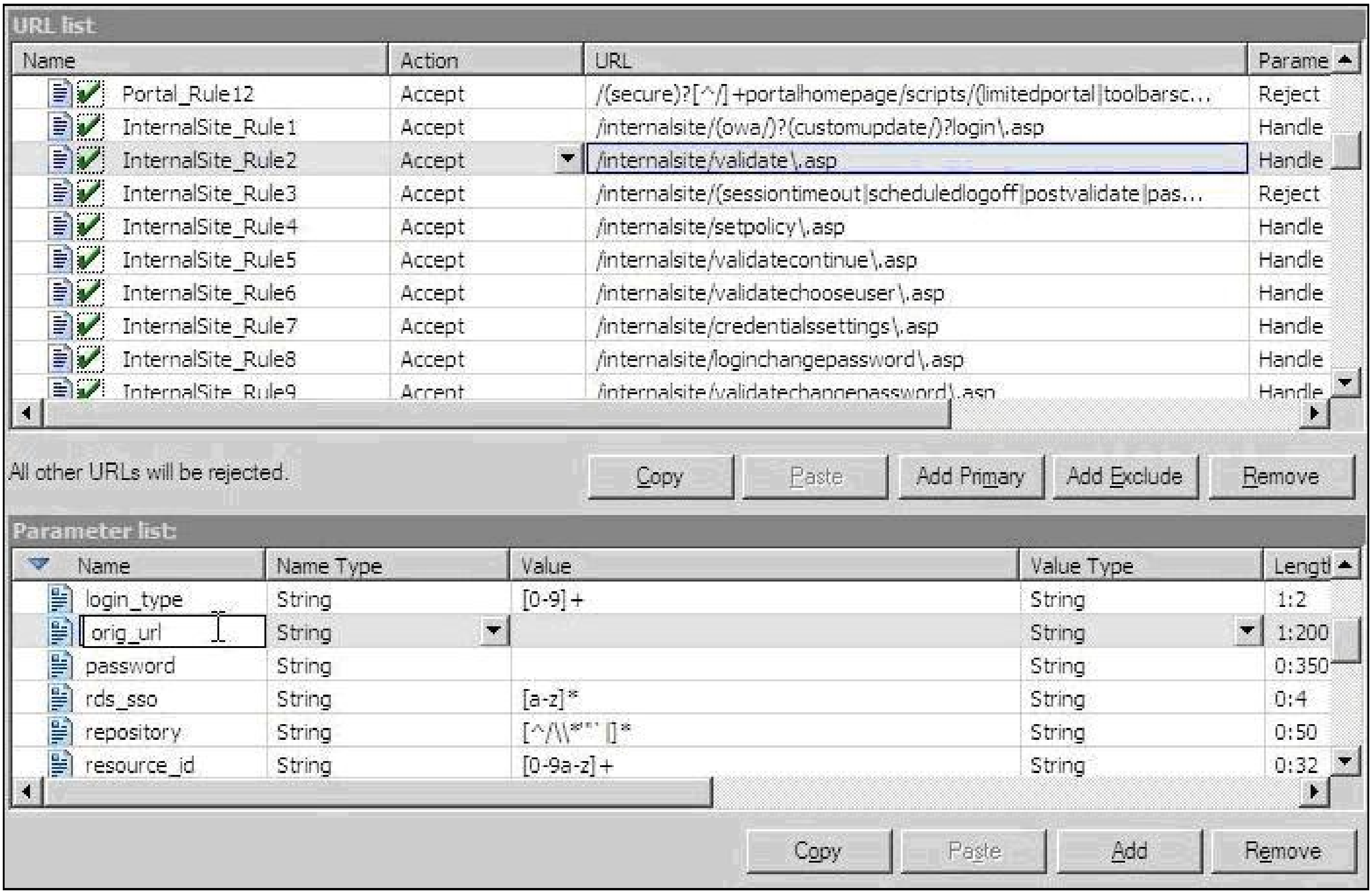
URL list

Name	Action	URL	Parame
Portal_Rule12	Accept	/(secure)?[^/] +portalhomepage/scripts/(limitedportal|toolbarsc…	Reject
InternalSite_Rule1	Accept	/internalsite/(owa/)?(customupdate/)?login\.asp	Handle
InternalSite_Rule2	Accept	/internalsite/validate\.asp	Handle
InternalSite_Rule3	Accept	/internalsite/(sessiontimeout|scheduledlogoff|postvalidate|pas…	Reject
InternalSite_Rule4	Accept	/internalsite/setpolicy\.asp	Handle
InternalSite_Rule5	Accept	/internalsite/validatecontinue\.asp	Handle
InternalSite_Rule6	Accept	/internalsite/validatechooseuser\.asp	Handle
InternalSite_Rule7	Accept	/internalsite/credentialssettings\.asp	Handle
InternalSite_Rule8	Accept	/internalsite/loginchangepassword\.asp	Handle
InternalSite_Rule9	Accept	/internalsite/validatechangepassword\.asp	Handle

All other URLs will be rejected.

Parameter list:

Nai e	Name Type	Value	Value Type	Length	Existence	Occurrences
secure	String	[01]	String	1:1	Optional	Single
site_name	String	[0-9a-z]+	String	1:100	Optional	Single
site_redirector	String	[^*"']*	String	0:256	Optional	Single
swivel	String		String	1:100	Optional	Multiple
trusted	String	[0|4]	String	0:1	Optional	Single
user_name	String	[^*()]*	String	0:350	Optional	Multiple



URL list

Name	Action	URL	Parame
Portal_Rule12	Accept	/(secure)?[^/]+portalhomepage/scripts/(limitedportal|toolbarsc...	Reject
InternalSite_Rule1	Accept	/internalsite/(owa/)?(customupdate/)?login\.asp	Handle
InternalSite_Rule2	Accept	/internalsite/validate\.asp	Handle
InternalSite_Rule3	Accept	/internalsite/(sessiontimeout|scheduledlogoff|postvalidate|pas...	Reject
InternalSite_Rule4	Accept	/internalsite/setpolicy\.asp	Handle
InternalSite_Rule5	Accept	/internalsite/validatecontinue\.asp	Handle
InternalSite_Rule6	Accept	/internalsite/validatechooseuser\.asp	Handle
InternalSite_Rule7	Accept	/internalsite/credentialssettings\.asp	Handle
InternalSite_Rule8	Accept	/internalsite/loginchangepassword\.asp	Handle
InternalSite_Rule9	Accept	/internalsite/validatechangepassword\.asp	Handle

All other URLs will be rejected.

Parameter list:

Name	Name Type	Value	Value Type	Lengt
login_type	String	[0-9]+	String	1:2
orig_url	String		String	1:200
password	String		String	0:350
rds_sso	String	[a-z]*	String	0:4
repository	String	[^/*"' []*	String	0:50
resource_id	String	[0-9a-z]+	String	0:32

To allow access to the ChangePIN application

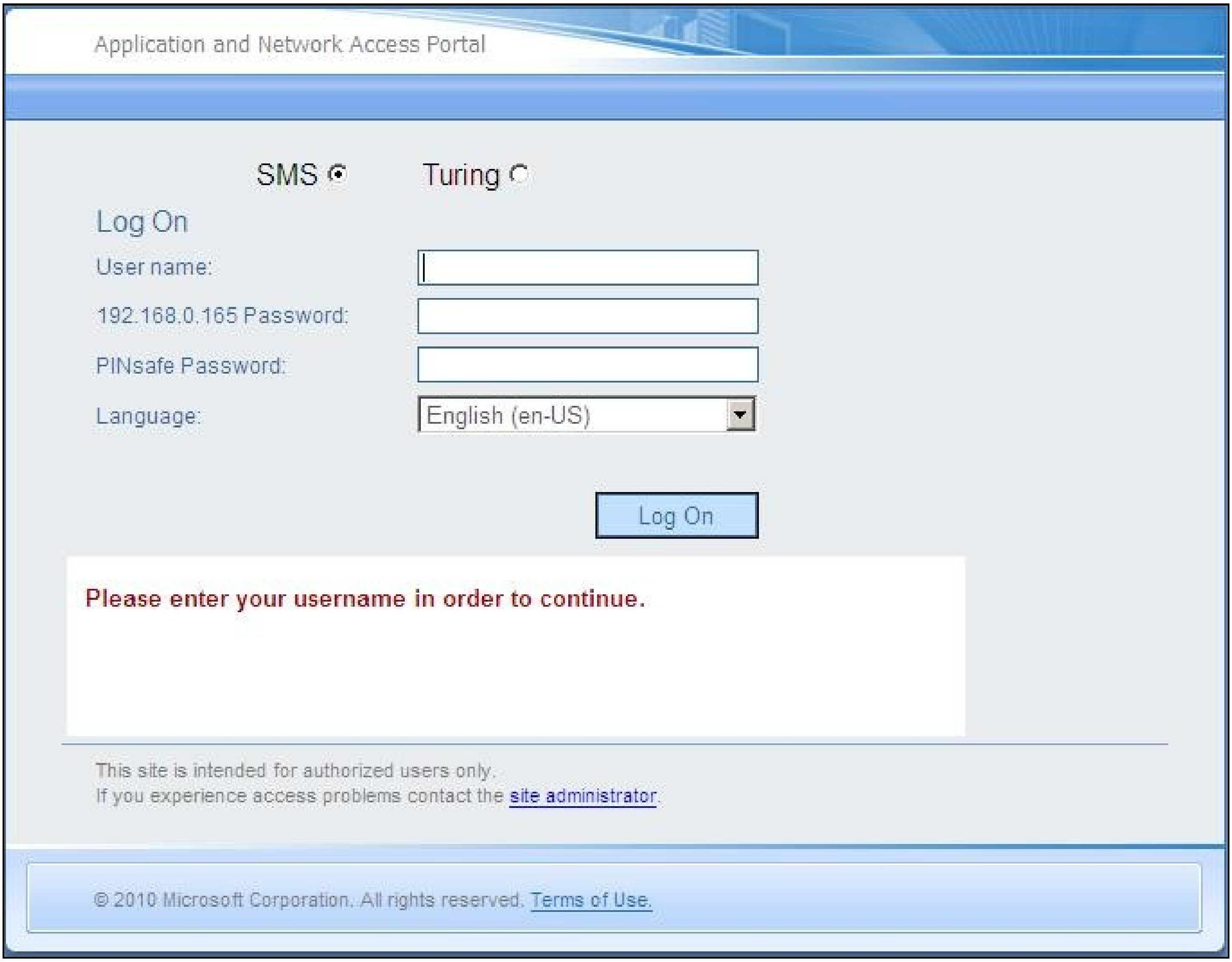
- Select the required Trunk
- Under Applications select Add
- Click the Web Applications Radio App and Generic Web App then Next
- Enter Application name ChangePIN and Application Type: pinsafe then Next
- Enter the ChangePIN IP address, and under path the location of the ChangePIN install (normally changepin), set the port to 8443, then Next
- Select Next
- Check details are correct, specifically https://<IP Address>:8443/changepin and then Finish

NOTE: If changing the IP address then change the IP address in the Application Properties on the Web Servers and the Portal Applications tabs.

221.6 Verifying the Installation

Browse to the login page, select TURing and enter a username, the Turing image should appear. Test using the SMS option. Check for requests on the Swivel server.

UAG Login Page



SMS ● Turing ○

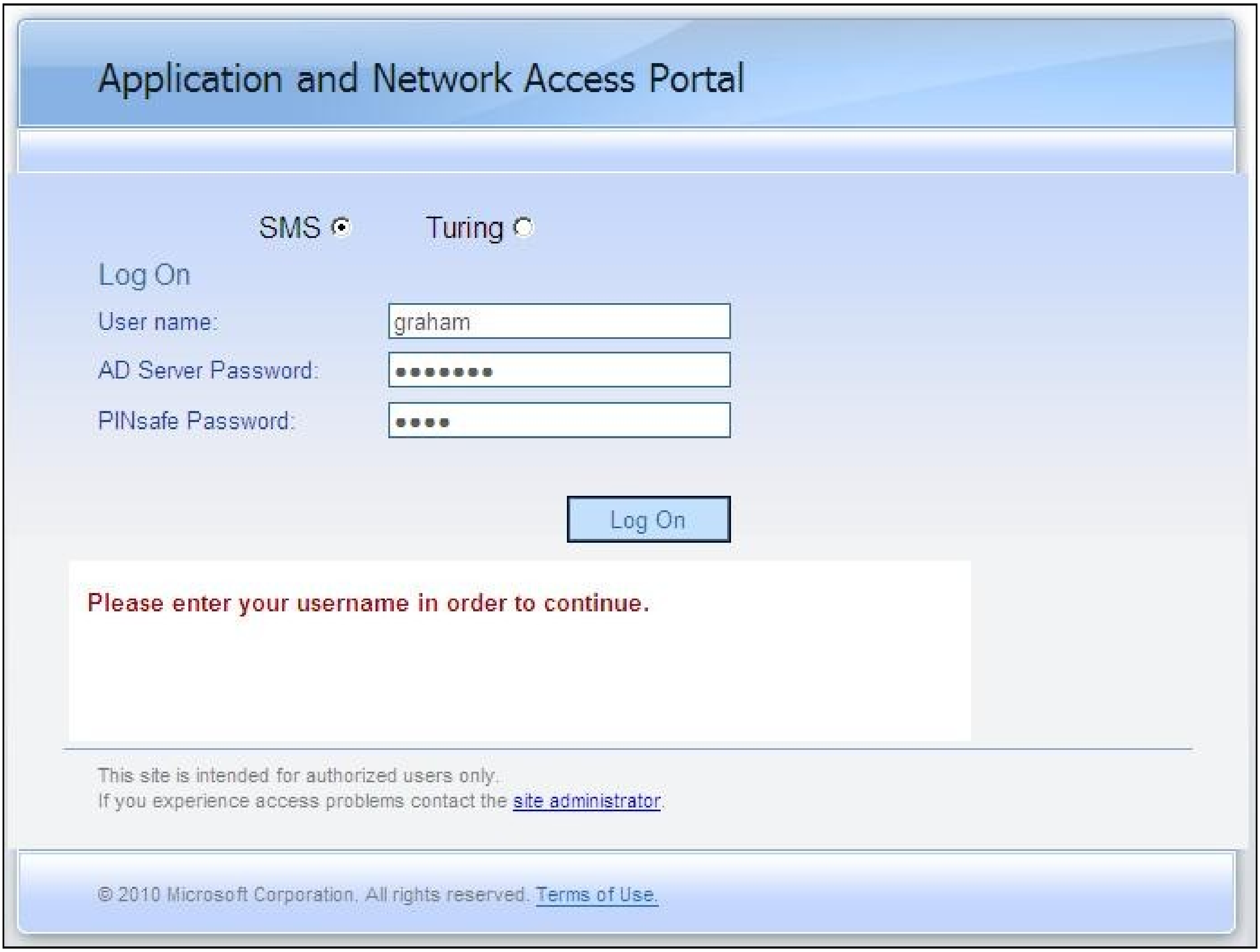
Language: English (en-US)

Please enter your username in order to continue.

This site is intended for authorized users only.
If you experience access problems contact the site administrator.

© 2010 Microsoft Corporation. All rights reserved. Terms of Use.

UAG login using SMS



Application and Network Access Portal

SMS ● Turing ○

Log On

User name: graham

AD Server Password: ••••••••

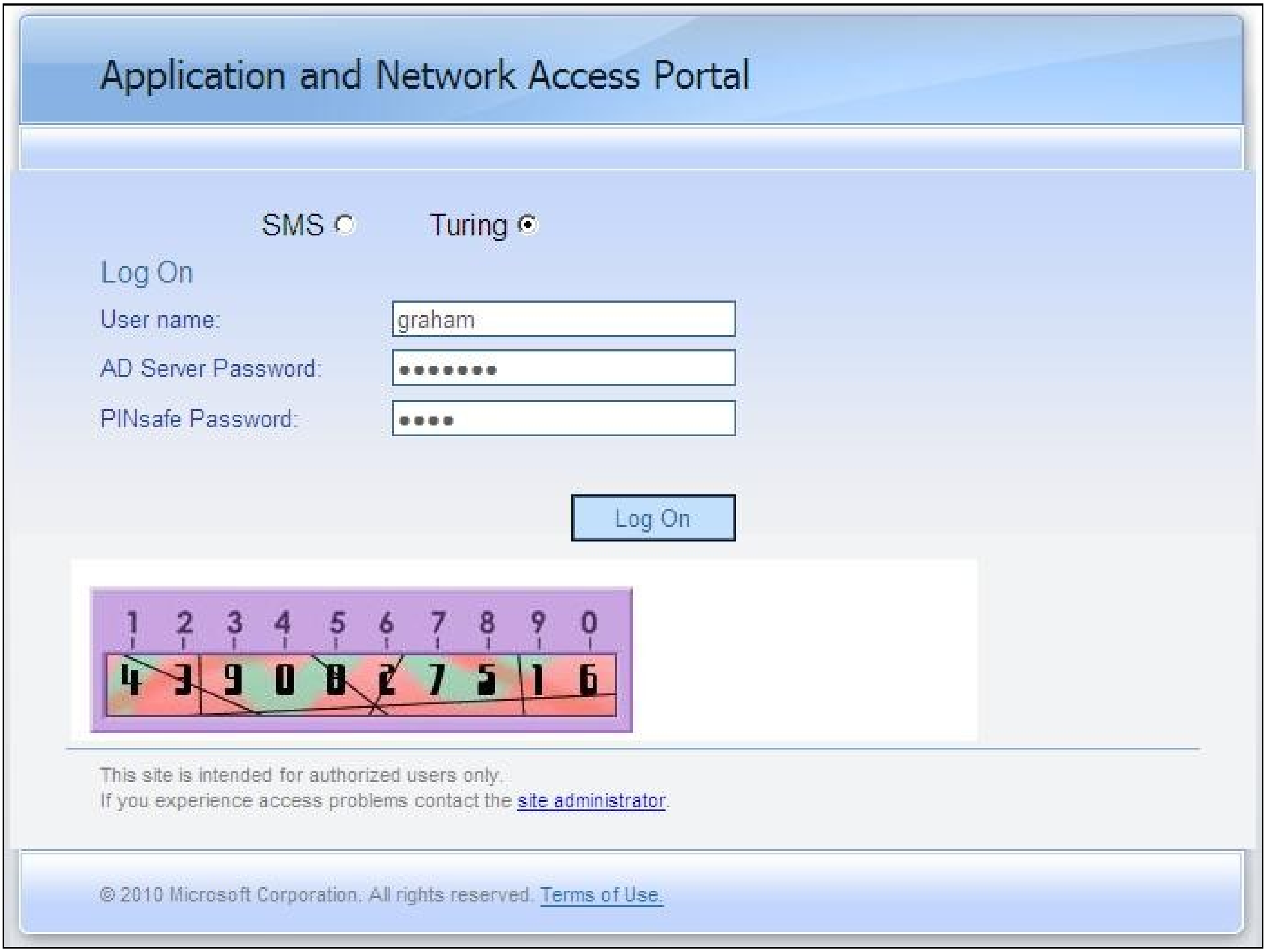
PINsafe Password: ••••

Please enter your username in order to continue.

This site is intended for authorized users only.
If you experience access problems contact the site administrator.

© 2010 Microsoft Corporation. All rights reserved. Terms of Use.

UAG login using Turing Single Channel Image



Application and Network Access Portal

SMS ○ Turing ●

Log On

User name: graham

AD Server Password: ••••••••

PINsafe Password: ••••

Log On

This site is intended for authorized users only.
If you experience access problems contact the site administrator.

© 2010 Microsoft Corporation. All rights reserved. Terms of Use.

Successful RADIUS authentication

The following user logged into trunk "test" (secure=0): User: admin; Source IP: 192.168.9.87; Authentication Server: PINsafe RADIUS; Session: B9FCC62A-B073-445D-9AAE-2FB1109EE5E6.

221.7 Troubleshooting

Check the Swivel server logs and system event logs for any errors or lack of communication as well as the UAG logs. Attempt a login and if required the TURing image, to generate an event then view it under under Admin/Web Monitor/Event Viewer/Security. Check the ISA server logs.

From a web browser on the UAG check to see if it is possible to generate a Turing image https://<IP address of Swivel server>:8443/proxy/SCImage?username=test

If the changes made in the UAG are not reflected in the login page, allow sufficient time for the rules to be written on the TMG (wait 10 minutes).

Request failed, the URL contains an illegal path. Trunk: test; Secure=0; Application Name: Whale Internal Site; Application Type: InternalSite; Rule: Default rule; Source IP: 192.168.9.87; Method: GET; URL: /InternalSite/Images/customupdate/images.asp?username=admin

URL blocking by the UAG. Check that the image can be rendered and that the URL rewriting rules are correct

The URL /internalsite/images/customupdate/images*.asp contains an illegal path. The rule applied is Default rule. The method is GET.

When the message *The rule applied is Default rule* is seen, it means that no rule has been matched and by default the URL is blocked. In the above example the path is incorrect to images.asp.

Http 500 error

If you get an http 500 error when using xml based integration you may need to edit the token.inc file so that

```
Set objWinHttp = Server.CreateObject("WinHttp.WinHttpRequest.5")
```

is replaced with

```
Set objWinHttp = Server.CreateObject("WinHttp.WinHttpRequest.5.1")
```

Ensure that the UAG can resolve the Swivel server name when hostname is used for connecting by RADIUS. Try with the IP address of the Swivel server.

221.8 Additional Configuration Options

221.8.1 RADIUS Challenge and Response

The UAG and Swivel supports the use of Challenge and Response authentication.

On the Swivel Administration Console ensure two-stage authentication is set to "Yes" for the RADIUS NAS definition. Secondly, under Server -> Dual Channel, ensure On demand authentication is set to "Yes".

In order to use two-stage authentication on Swivel, all users have to have a password defined. There are two ways to manage this: either set a password for each user under user administration, or enable the option to check password with repository (under Policy -> Password), in which case Swivel uses the AD password. Either way, you need to enter the password for Swivel as well as the AD password. (It might be possible, using the repository password option, to have a custom page that copies the AD password to the Swivel password, but this has not been tested).

If the Swivel password is entered correctly, you will be sent a security string, and a second login page will be displayed, to enter your one-time code.

221.8.2 PINpad Integration

PINpad integration can be accomplished using these files, and a slight modification to the installation procedure. Please note that this zip file reflects the relative locations of the 3 files included, starting from "InternalSite". The login page goes into /InternalSite/customupdate and the other two into /InternalSite/images/customupdate.

Please ensure that you have Pinpad enabled on your Swivel virtual or hardware appliance, following the instructions here.

Use pinpad.asp instead of images.asp from the original integration, and edit this in a similar way, replacing the internal URL for the Swivel appliance. Keep everything from "/proxy/SCPinPad" as it is. You will also need to make a similar change to StartSession.asp. One important difference to recognise with this solution is that it makes a session start request explicitly. Therefore, you cannot use the /proxy application. Instead, you must use port 8080 and context /pinsafe on a virtual or hardware appliance. This also means that you must have PINsafe version 3.9.2 or later, since earlier versions do not support PINpad natively. Make sure that the firewall rule is configured appropriately. If you have an earlier version of PINsafe, either upgrade, or use this older solution. If you use the older solution, note the differences below, and ignore any references to StartSession.asp.

Use /customupdate/loginpinpad.asp as the login page.

When configuring the URL rewriting rules, you will need to include pinpad.asp and StartSession.asp in /images/CustomUpdate as accepted pages, unless you have allowed all pages in /images/CustomUpdate. Either set "ignore" for all parameters for these pages, or else permit the following parameters:

- pinpad.asp:
    - sessionid (or username for the old solution)
    - padno
- StartSession.asp
    - username
    - random

NOTE: this login page assumes that PINsafe is the primary authentication. If it is the secondary, you need to edit the login page (loginpinpad.asp) and change the following line

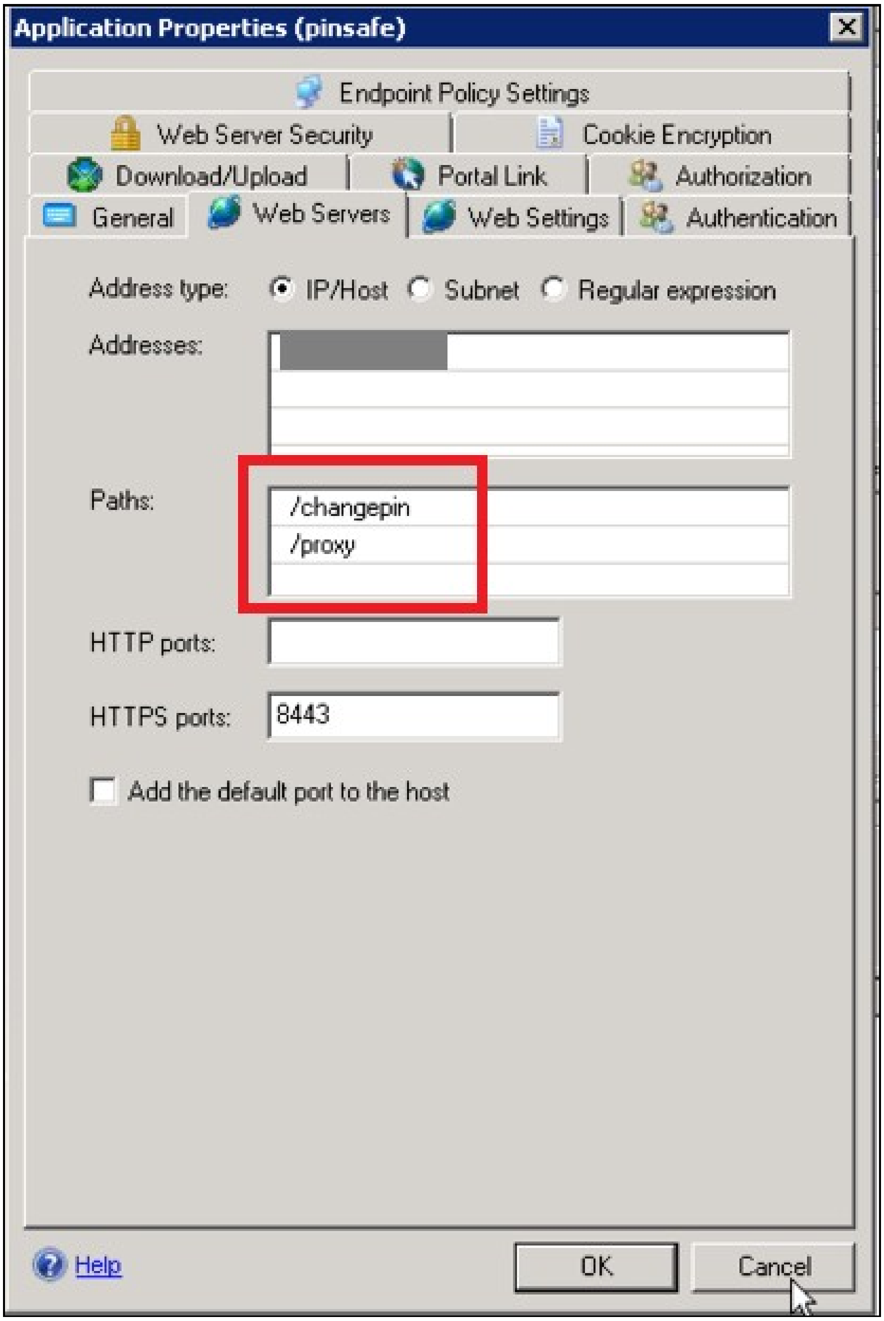
```
 var PINSAFE_PASSWORD_INDEX = 0;
```

to this:

```
 var PINSAFE_PASSWORD_INDEX = 1;
```

221.8.3 ChangePINpad Integration

When publishing access to ChangePINpad, ensure that you enable the following paths during creation:



Address type: ● IP/Host ○ Subnet ○ Regular expression

Addresses: [redacted]

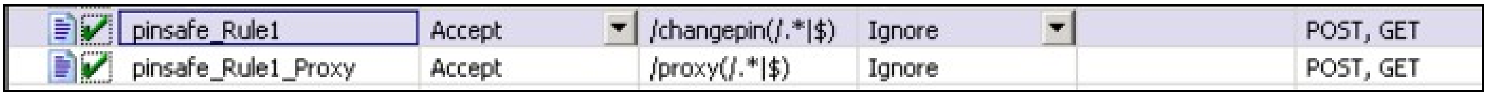
Paths:
/changepin
/proxy

HTTP ports:

HTTPS ports: 8443

□ Add the default port to the host

This should in turn create the following rules:



pinsafe_Rule1	Accept	/changepin(/.*|$)	Ignore		POST, GET
pinsafe_Rule1_Proxy	Accept	/proxy(/.*|$)	Ignore		POST, GET

Beware that if you add paths to the published application afterwards, the rules for these paths will not be created. So ensure that you enter the paths at creation time.

221.8.4 Button size and aspect ratio

The Button size and aspect ratio is controlled by the settings in the login page:

document.all.otp.innerHTML = '<img src="/InternalSite/customupdate/FetchTuring.asp? username=' + otpusername +'" height="81" width="300">'; }

change the height and width settings to the value that is appropriate.

221.8.5 XML Authentication

Configuring XML authentication (when not using RADIUS)

XML authentication has not been tested with the current version of UAG and is supplied for reference if required, RADIUS authentication is the preferred method of authentication.

Note that when using a Swivel virtual or hardware appliance with a proxy configured, the XML requests need to be made to the https://<IP>:8080/pinsafe address rather than the proxy address. This applies currently to all Swivel virtual or hardware appliance versions.

This step is not required when RADIUS authentication is used. RADIUS authentication is the preferred method of authentication. To enable the token.inc file, create a repository of type ?Other? on the UAG configuration. The repository you create must match the name of the file (ie, if the inc file is called Token.inc, the repository must be named Token).

Configure a Swivel Agent (For XML Authentication)

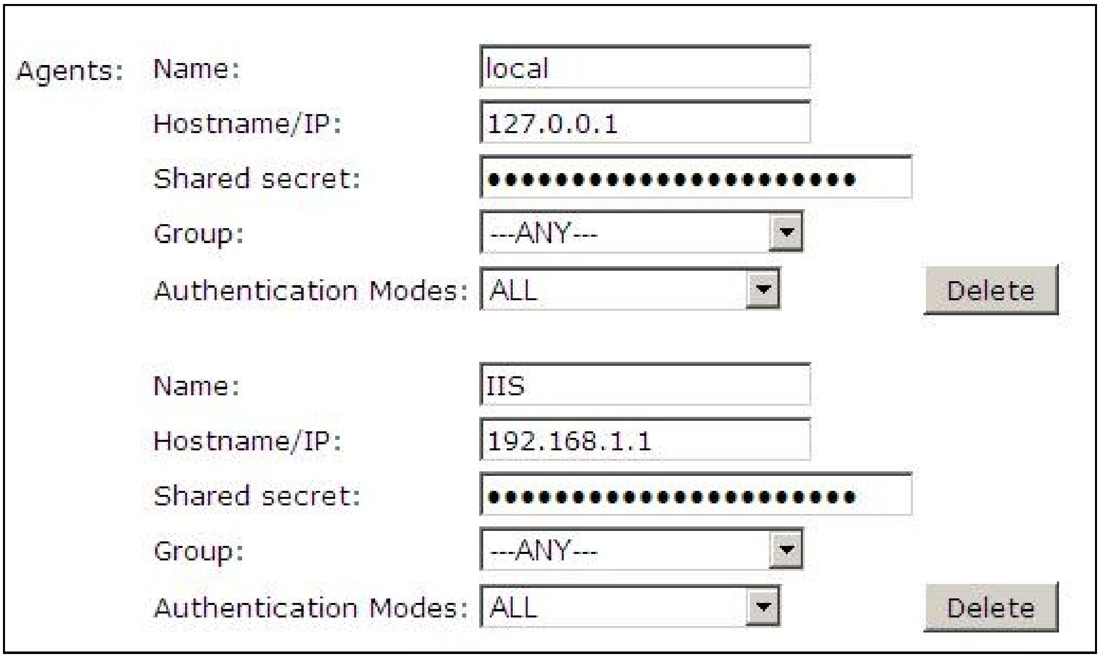
1. On the Swivel Administration Console select Server/Agent

2. Enter a name for the Agent

3. Enter the UAG internal IP address

4. Enter the shared secret

5. Click on Apply to save changes



Agents: Name: local

Hostname/IP: 127.0.0.1

Shared secret: ●●●●●●●●●●●●●●●●●●●●●●●

Group: ---ANY---

Authentication Modes: ALL

Name: IIS

Hostname/IP: 192.168.1.1

Shared secret: ●●●●●●●●●●●●●●●●●●●●●●●

Group: ---ANY---

Authentication Modes: ALL

To create the repository, do the following-

1. Access the UAG configuration GUI.

2. Click on Admin Authentication Users/Group repository

3. Select New to create a new repository

4. In the drop down menu, select ?Other? and in the Name field type in the name of the inc file (See screen shot below)

5. Click on Add and apply this repository to the relevant trunk.

6. Activate the configuration

Edit the file Token.inc with the required shared secret and to represent the Swivel server IP address and Swivel install name, Note for all Swivel installs this needs to point to the PINsafe server on port 8080 and not the proxy port 8443.

```
m_secret = "secret"
```

```
objWinHttp.Open "GET", "https://192.168.1.1:8080/pinsafe/AgentXML?xml=" & m_request, false
```

Note If you get an http 500 error when using xml based integration you may need to edit the token.inc file so that

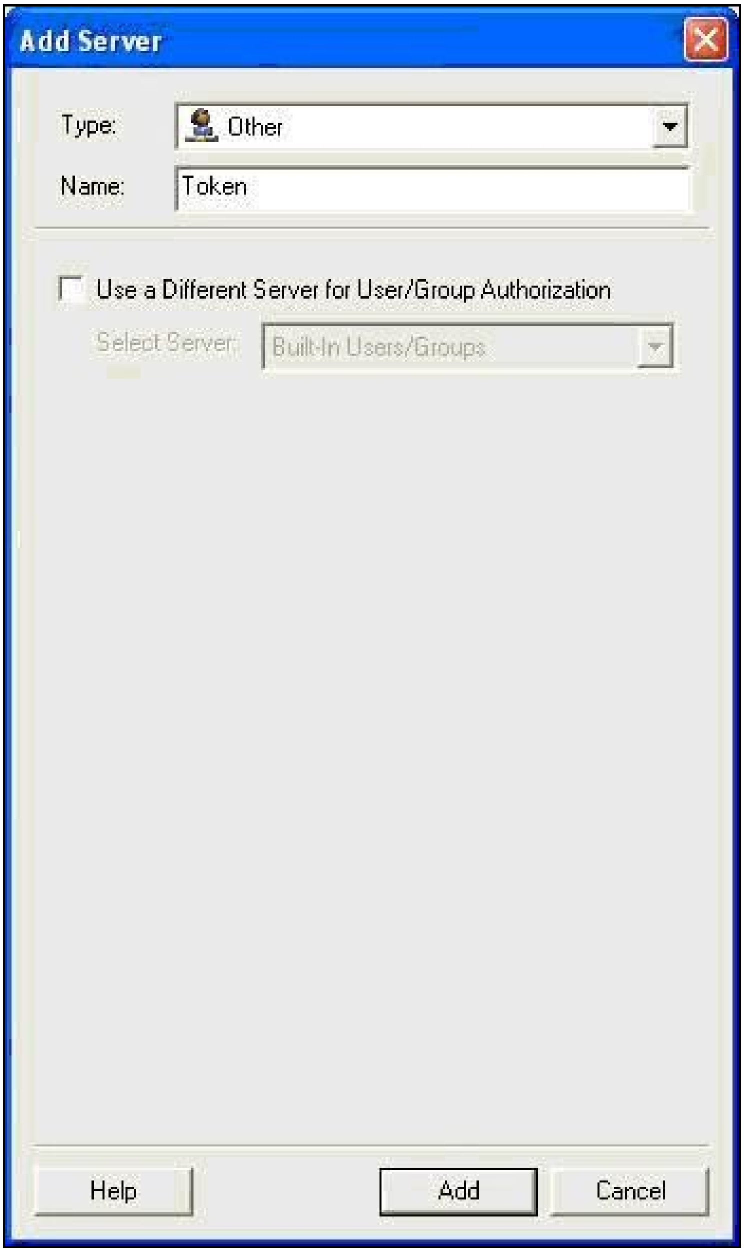
```
Set objWinHttp = Server.CreateObject("WinHttp.WinHttpRequest.5")
```

is replaced with

```
Set objWinHttp = Server.CreateObject("WinHttp.WinHttpRequest.5.1")
```

Edit the file Portalname1postpostvalidate.inc to represent the PINsafe server IP address and changePIN install name:

```
'response.redirect "https://192.168.1.1:8443/changepin"
g_orig_url = "https://192.168.1.1:8443/changepin"
```



221.9 Known Issues and Limitations

If upgrading the UAG to a higher service pack, the configuration files, particularly login.asp may be overwritten. Verify the files after an upgrade. Also note that the URL rewriting rules may differ from version to version, so these should also be verified.

Upgrading from RTM Update 2, to SP1 will cause the InternalSite rules, on the UAG to be removed, or changed back to defaults.

If the login page is viewed incorrectly as a mobile page then this workaround will allow the correct page to be displayed, and works with Windows 7 and Windows 8.

221.10 Additional Information

For assistance in the Swivel installation and configuration please firstly contact your reseller and then email Swivel Secure support at support@swivelsecure.com

222 Category:UAG