Microsoft OWA 2010 IIS Integration

Contents

- 1 Introduction
- 2 Compatibility
- 3 Prerequisites
  - 3.1 Additional Prerequisites for Version 2.9
- 4 File Downloads
  - 4.1 OWA Filter Change History
- 5 Architecture
- 6 Installation
  - 6.1 Preparation for Installing Version 2.9
  - 6.2 Upgrading to Version 2.9
  - 6.3 Software Installation
  - 6.4 Configuration of the IIS Filter
    - 6.4.1 Swivel Settings
    - 6.4.2 OWA Settings
    - 6.4.3 Authentication Settings
    - 6.4.4 Excluded Settings
    - 6.4.5 Advanced Settings
  - 6.5 Configure The Swivel Server
  - 6.6 Using additional attributes for authentication
- 7 Additional Installation Options
  - 7.1 Modifying the login Page to stop the Single Channel Image automatically appearing
  - 7.2 Modifying the login Page to allow Dual Channel On Demand Delivery
- 8 Verifying the Installation
- 9 Uninstalling the Swivel Integration
  - 9.1 Uninstalling Manually
- 10 Change PIN
  - 10.1 Change PIN with PinPad
    - 10.1.1 PinPad prior to Version 2.8.4
- 11 Troubleshooting
  - 11.1 Enabling debug logging
  - 11.2 User regularly times out after a short interval
  - 11.3 Turing image appears but user cannot authenticate
  - 11.4 User Authenticates Successfully to Swivel but OWA Login Page is Redisplayed
  - 11.5 Name resolution issue
- 12 Known Issues and Limitations
  - 12.1 Known Issues with Version 2.9
  - 12.2 Problems With Connection Settings
  - 12.3 Default Exclusions Not Applied
  - 12.4 One-time Code Not Shown
  - 12.5 Private Computer Option Doesn't Stay Selected
  - 12.6 Swivel Customisation Lost
  - 12.7 Later Versions of the Filter Not Working With Service Pack 1
  - 12.8 Logging
- 13 Multiple Swivel Servers
- 14 Additional Information

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.

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.

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.

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.

File Downloads

Download links:

- Version 2.8
- Version 2.9

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)

Architecture

The Exchange server makes authentication requests against the Swivel server by XML authentication

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.

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.

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.

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.

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.

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)

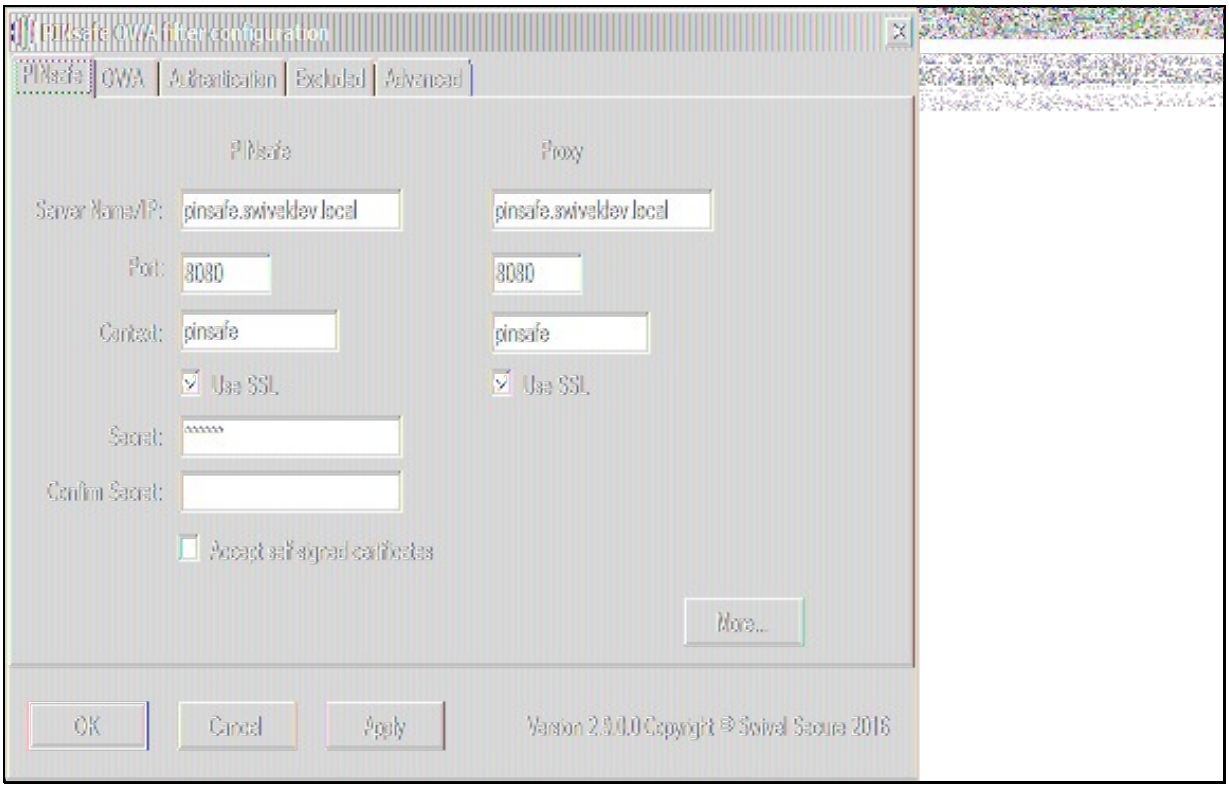
Context: Swivel install name, for a Swivel virtual or hardware appliance use pinsafe (not proxy)

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.



OWA Settings

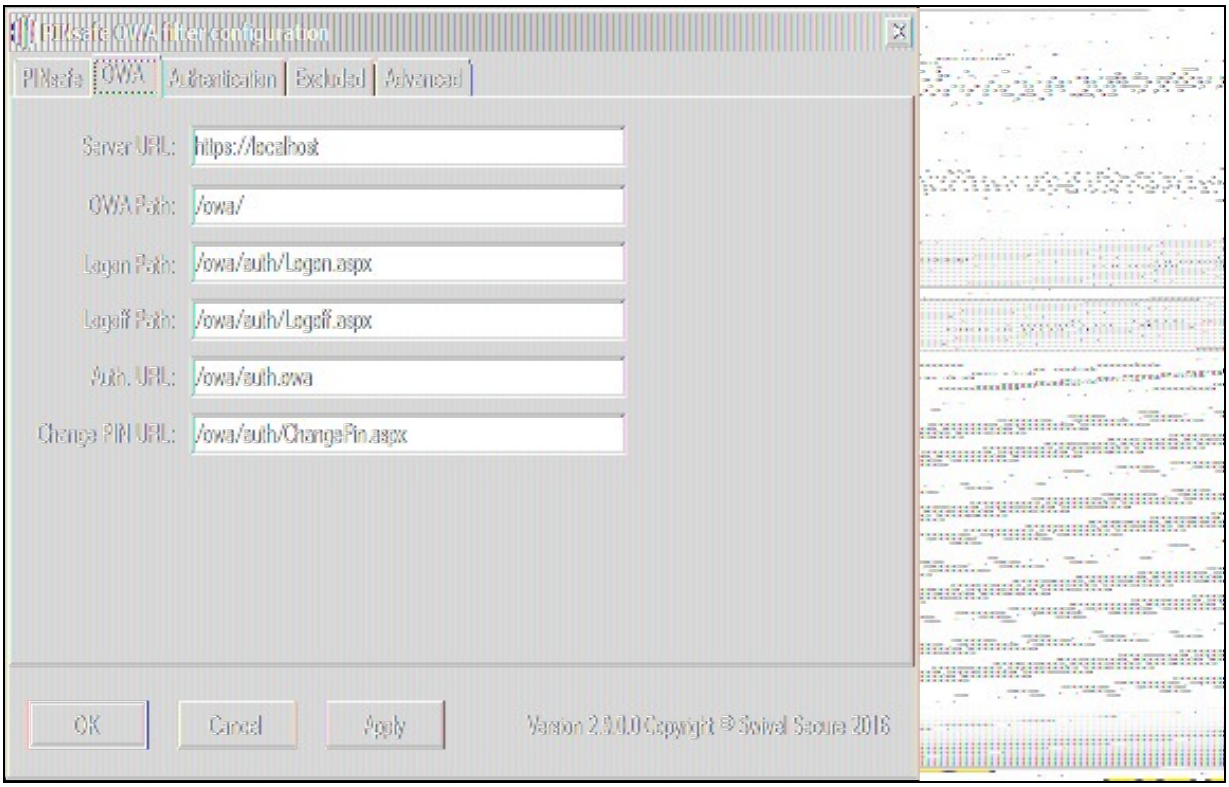
Server URL: Exchange Server URL, Example: https://<exchange.mycompany.com>

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



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.

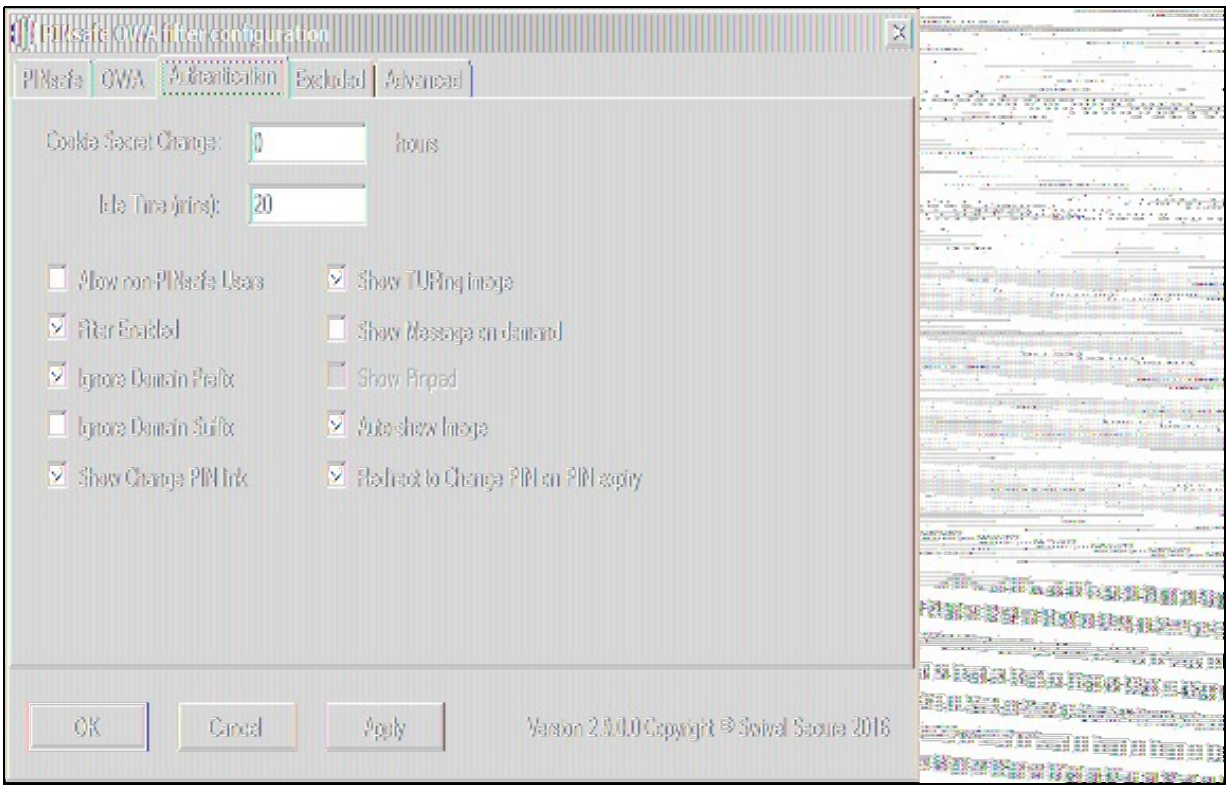
Ignore Domain Suffix If this option is ticked, any suffixed domain (i.e. anything after the '@' character) is removed before sending the username to PINsafe. The full username is sent to OWA.

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.

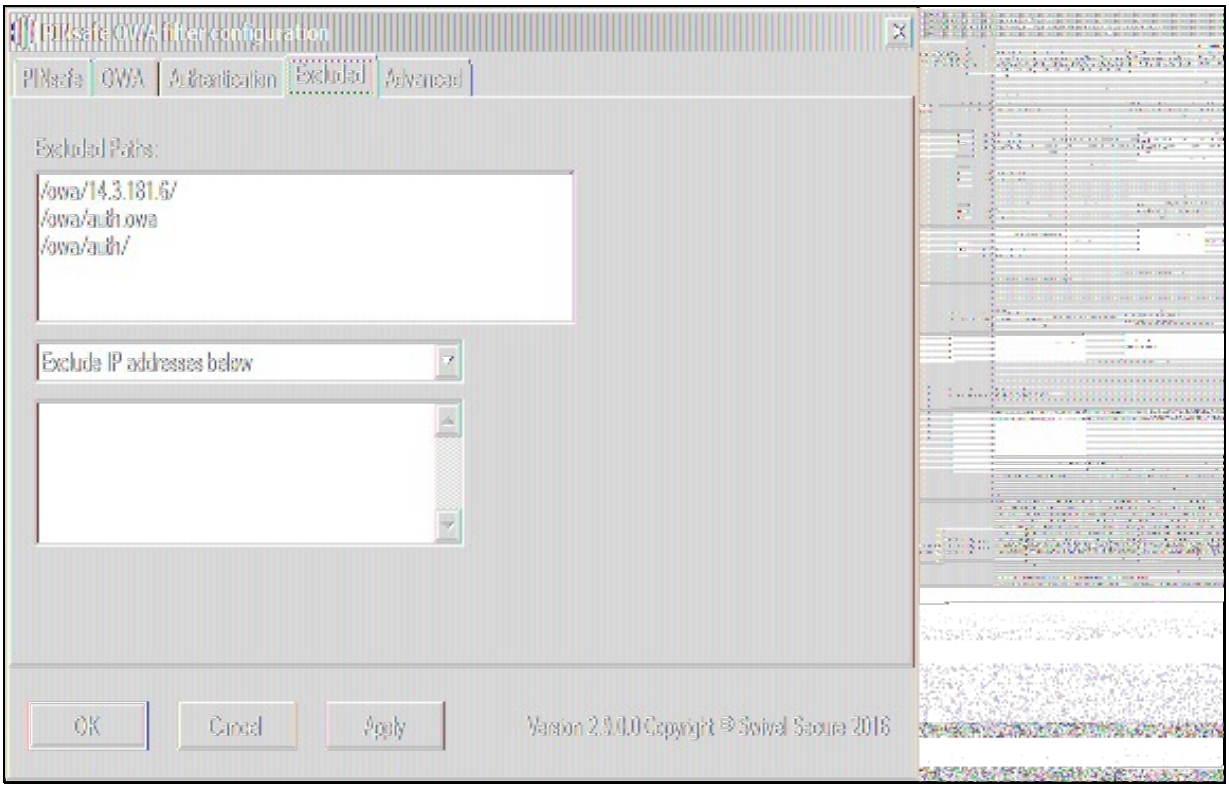
Auto-show image If this option is ticked, the TURing or Pinpad image is requested as soon as the user enters the username and tabs away from it. If this option is not ticked, the user must click a button to show the image.



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.



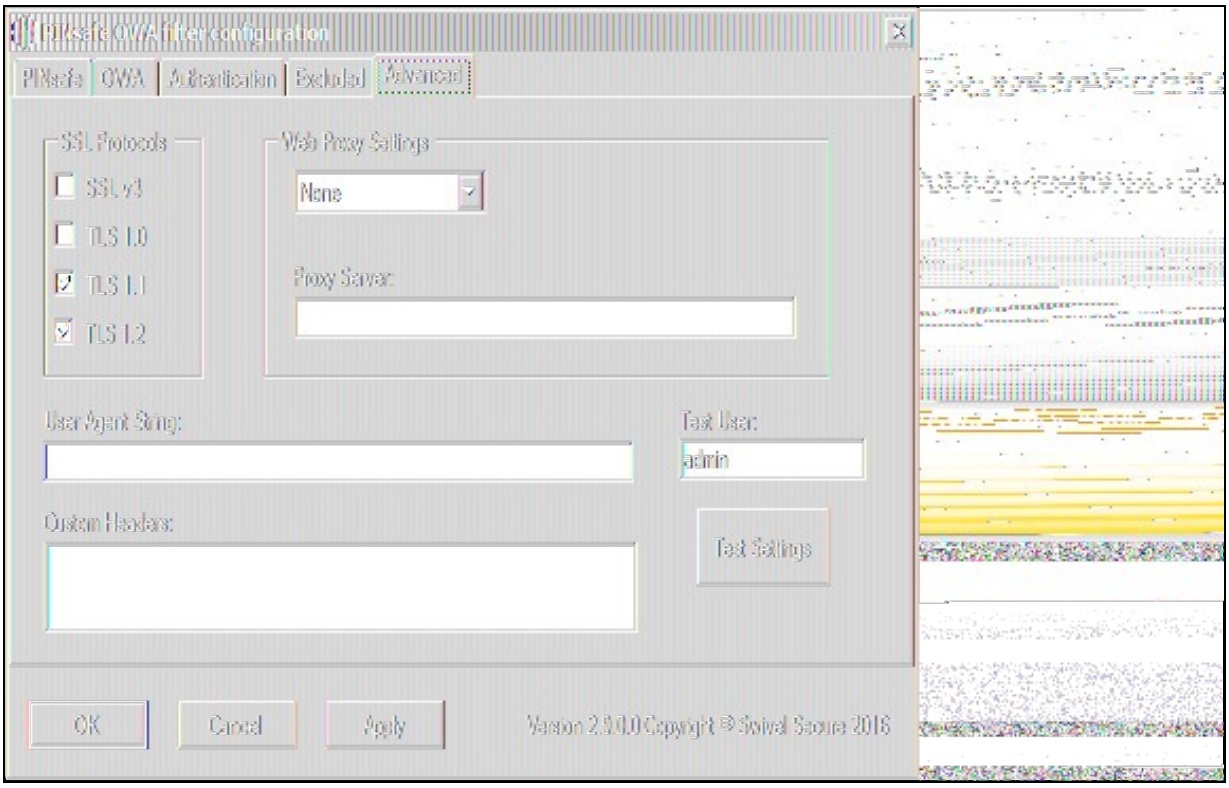
Advanced Settings

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.

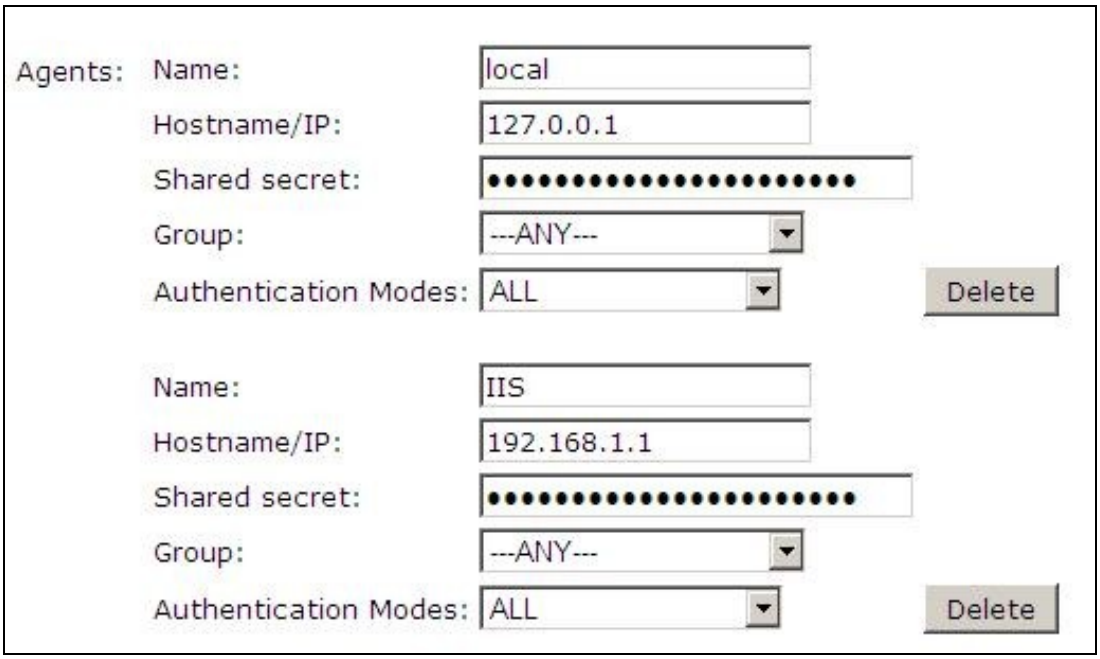
Test User: and **Test Settings** In order to test the settings, the configuration program will send a session start request on behalf of a user. You should enter a username that exists in the Swivel database (the default is 'admin'), then click Test Settings to confirm that the connection between the OWA Server and the Swivel server is correctly configured.



Configure The Swivel Server

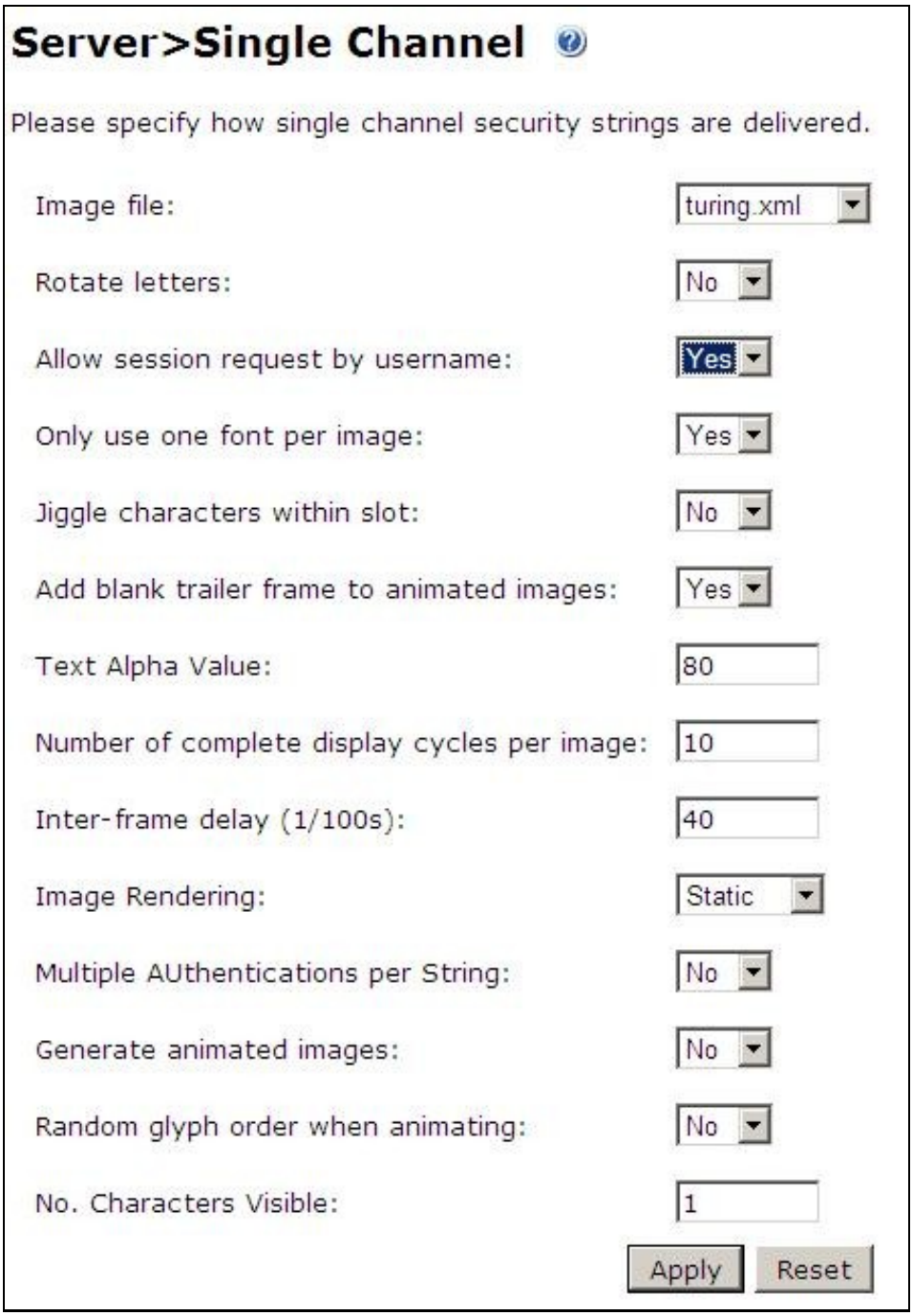
Configure a Swivel Agent (For standard XML Authentication)

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



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



Using additional attributes for authentication

When using additional attributes for authentication see User Attributes How To

Additional Installation Options

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()?
```

Modifying the login Page to allow Dual Channel On Demand Delivery

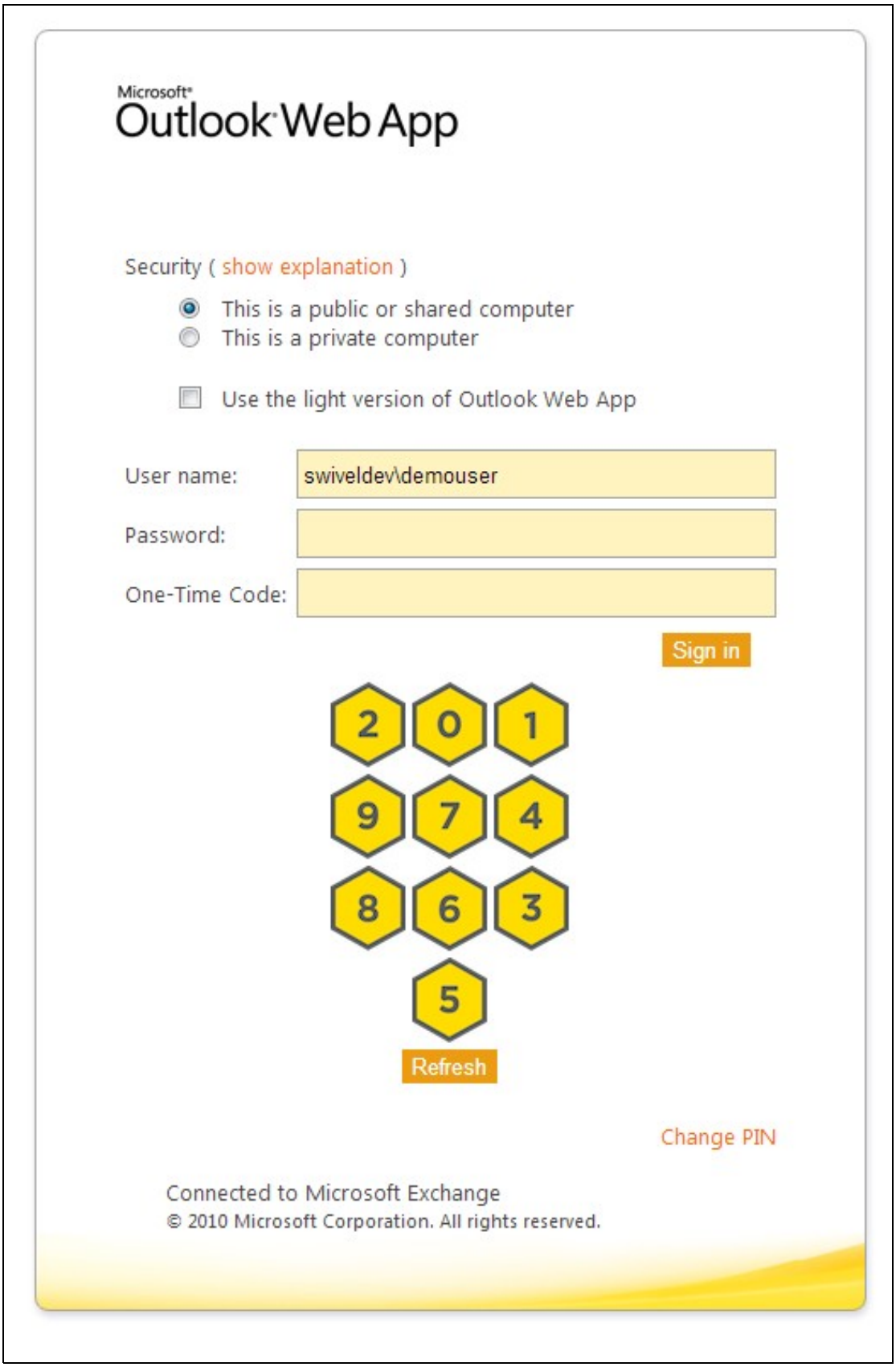
NOTE: this refers to older versions of the filter. In versions 2.5 and higher, this is set in the configuration program.

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.

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.



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.

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.

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.

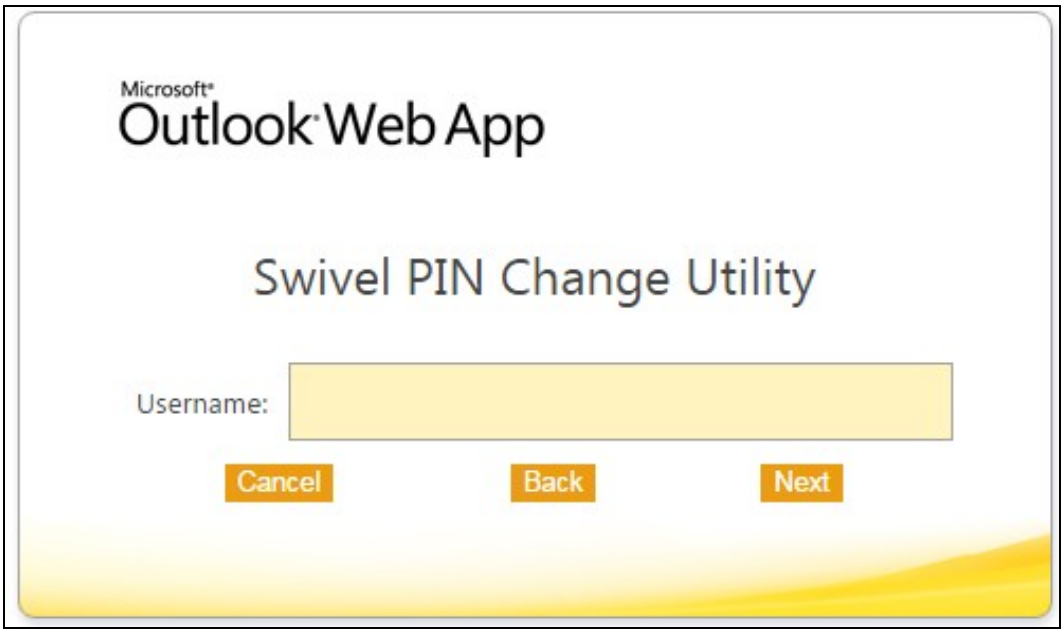
If you selected the Change PIN page in error, and want to return to the login page, then click the "Cancel" button ("Skip" button before 2.8.4) to return without changing your PIN.

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.

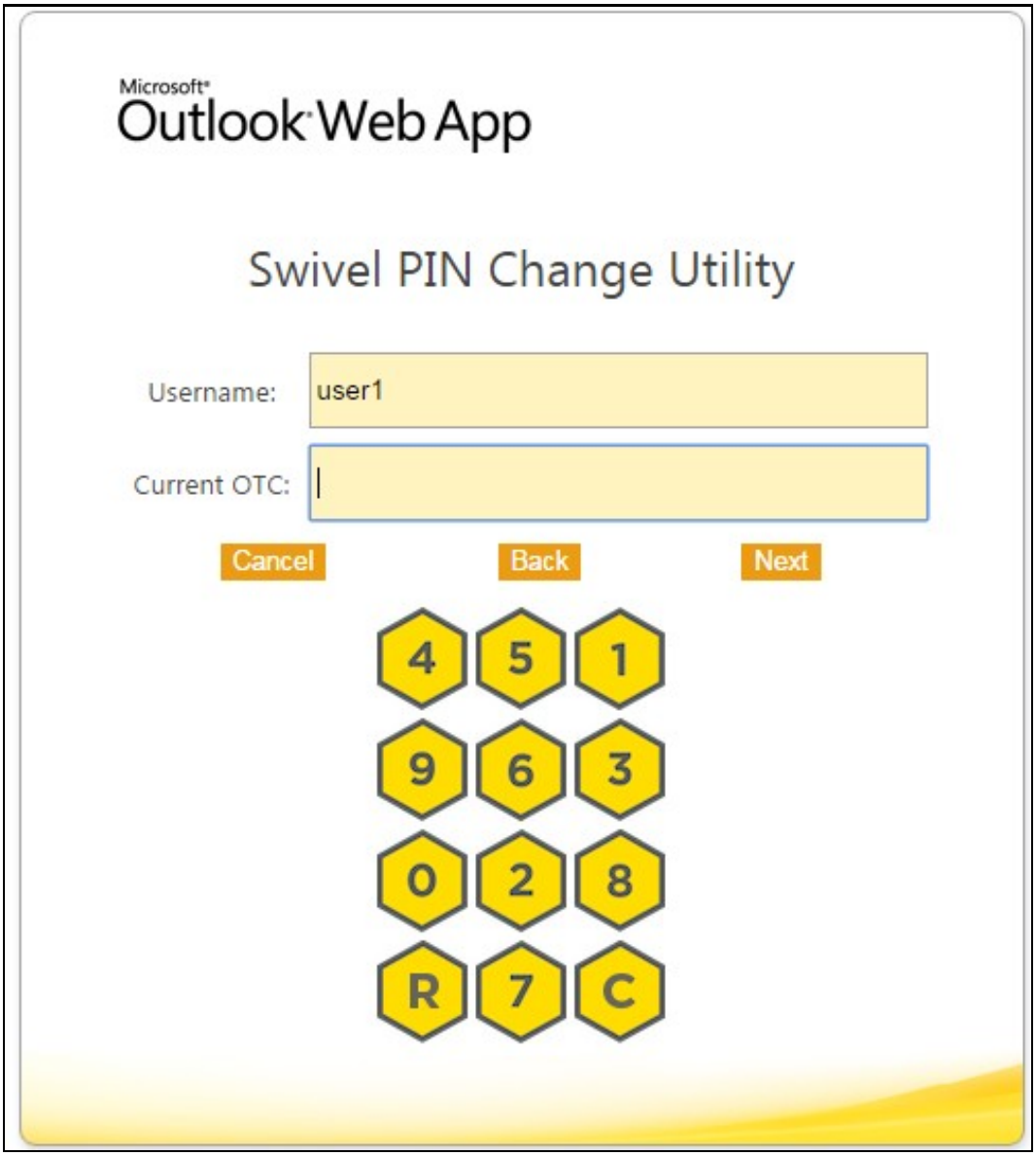
Change PIN with PinPad

The following instructions refer to the Change PIN page from version 2.8.4 onwards. See the following section for older versions.

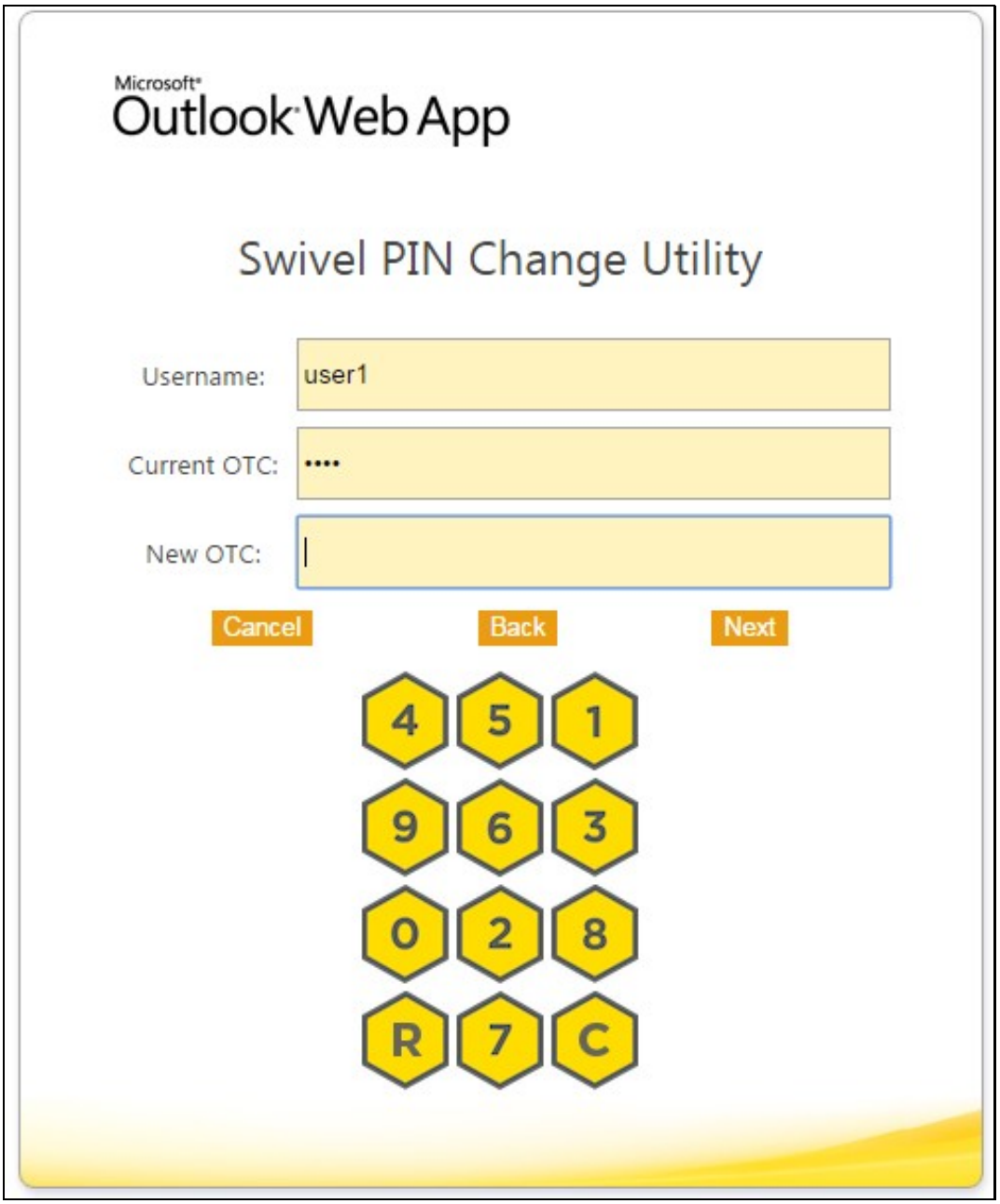
The initial screen (with or without Pinpad) looks like this:



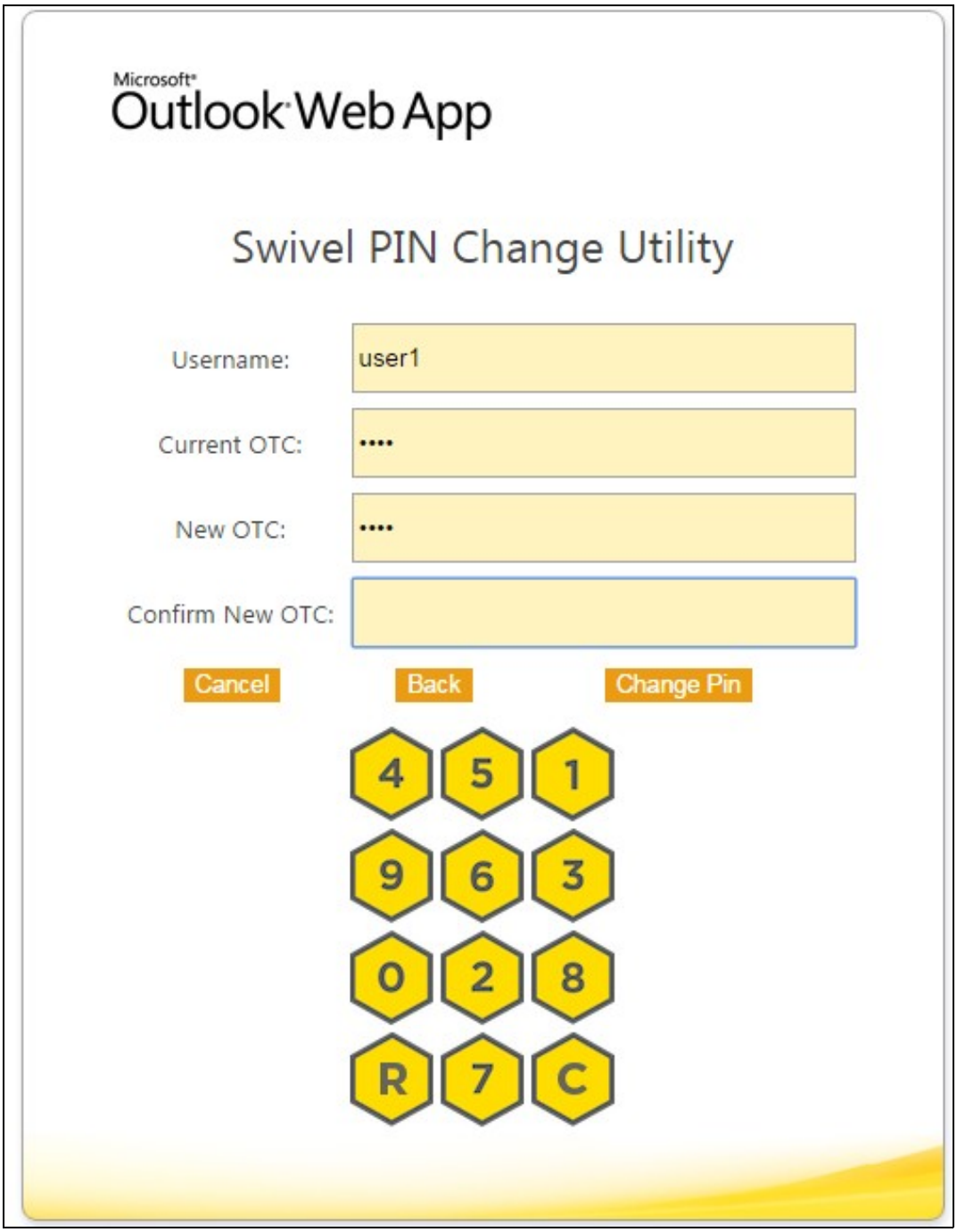
Enter your username and click "Next" or press Tab to show the next field and the Pinpad:



Click the buttons corresponding to the digits of your current PIN and then "Next":



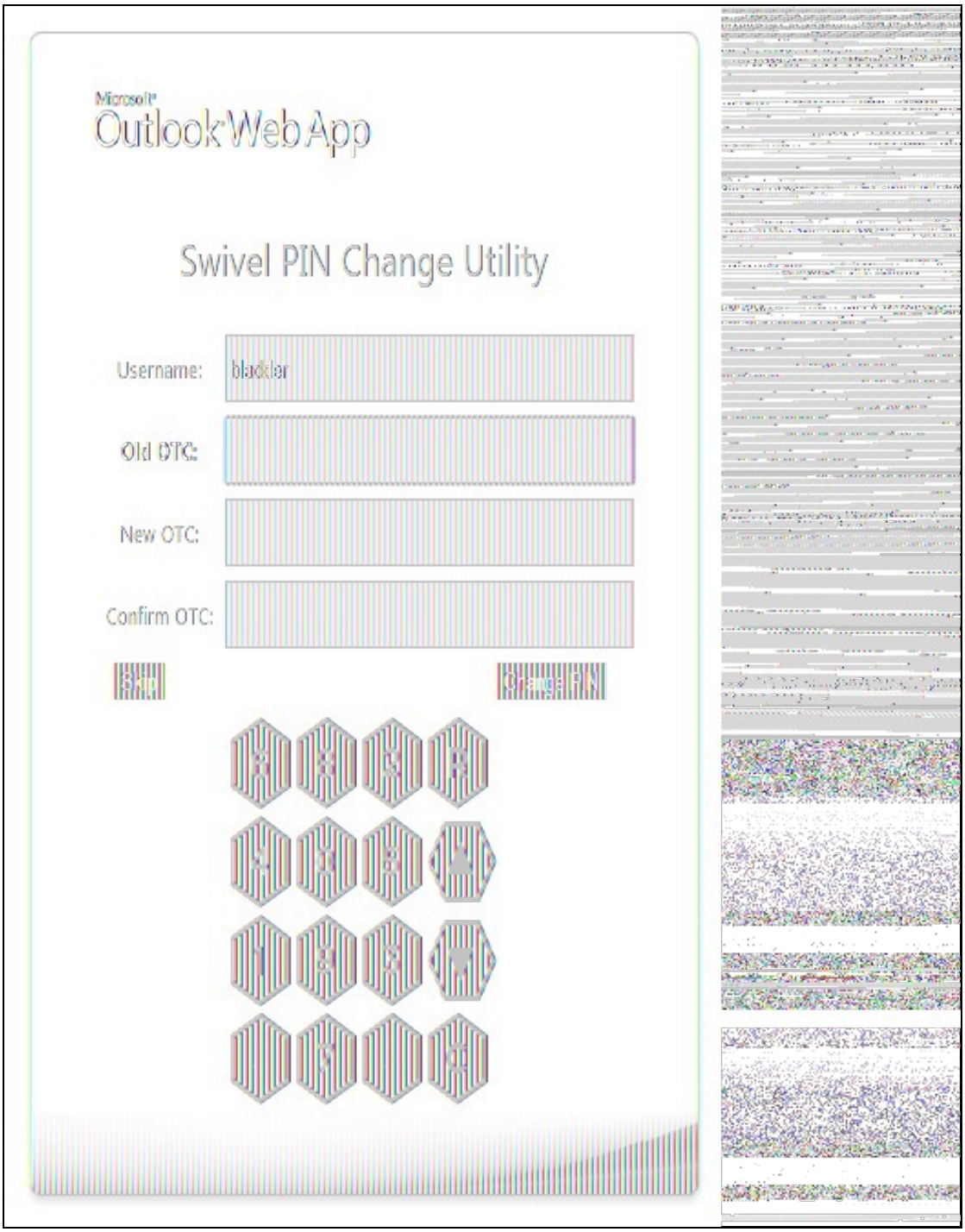
Click the buttons corresponding to the digits of your new PIN and then "Next":



Enter your new PIN again, to confirm, and then click "Change Pin".

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:



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.

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>

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" />

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. Note that this refers to the main PINsafe settings (for version 2.6 or higher) - the proxy settings SHOULD have these values if required.

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.

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.

Known Issues and Limitations

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.

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.

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.

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.

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.

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.

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.

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>

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).

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.