Table of Contents

Table of Contents

1 Microsoft OWA 2003 IIS Integration

1.1 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.

1.2 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

1.3 Baseline

Microsoft Exchange 2003 with OWA using IIS 6.0

Microsoft 2003 Server

PINsafe 3.7

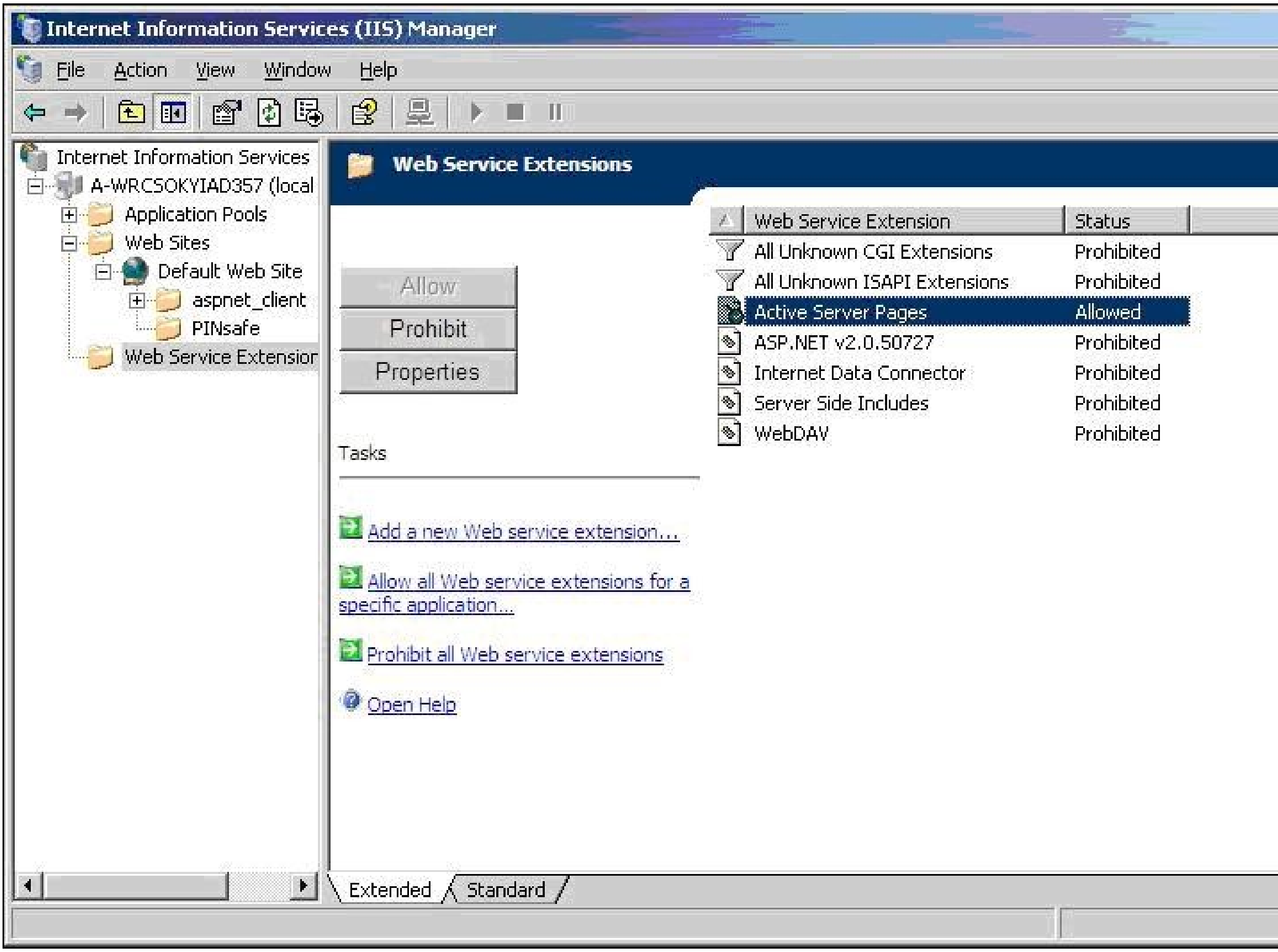
1.4 Architecture

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

1.5 Installation

1.5.1 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

1.5.2 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.

1.5.3 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.

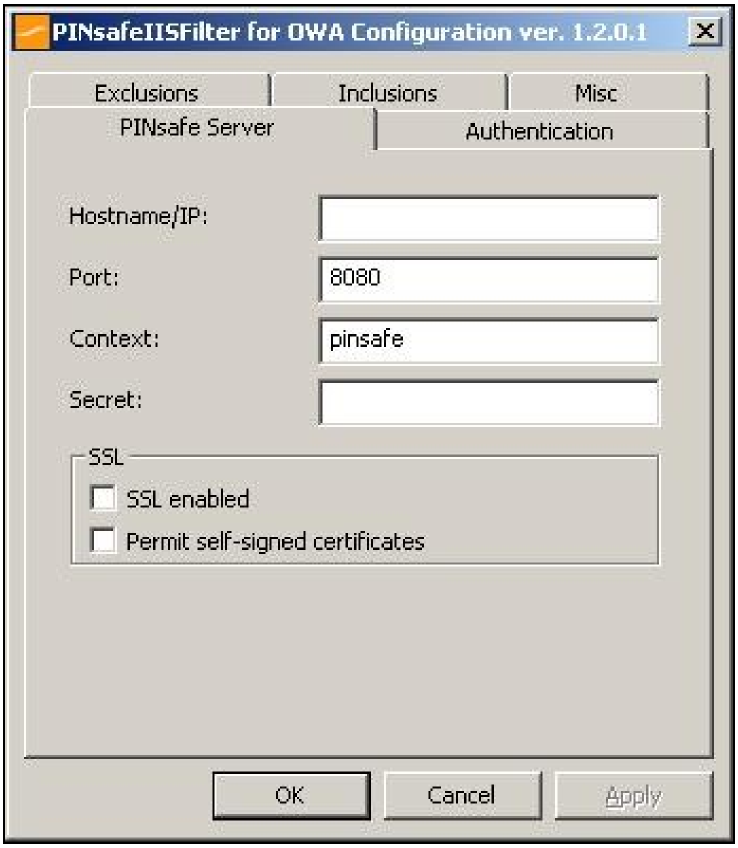
Port: The port number used by the PINsafe server, 8080 for a software install or PINsafe virtual or hardware appliance (do not use 8443)

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.



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.

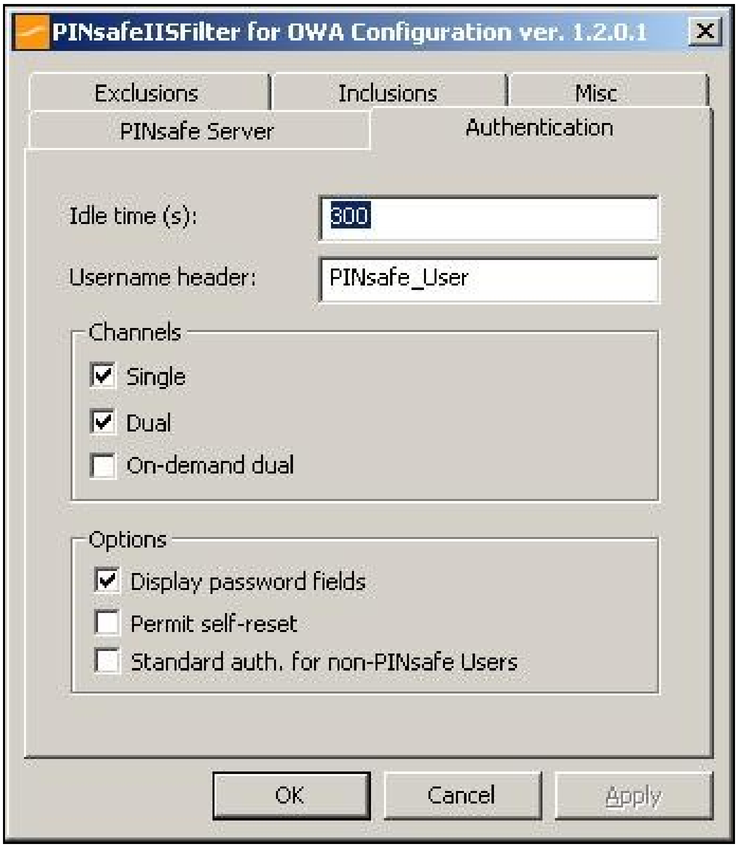
Dual Indicates that dual channel security strings (i.e. via e-mail, SMS) are permitted.

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

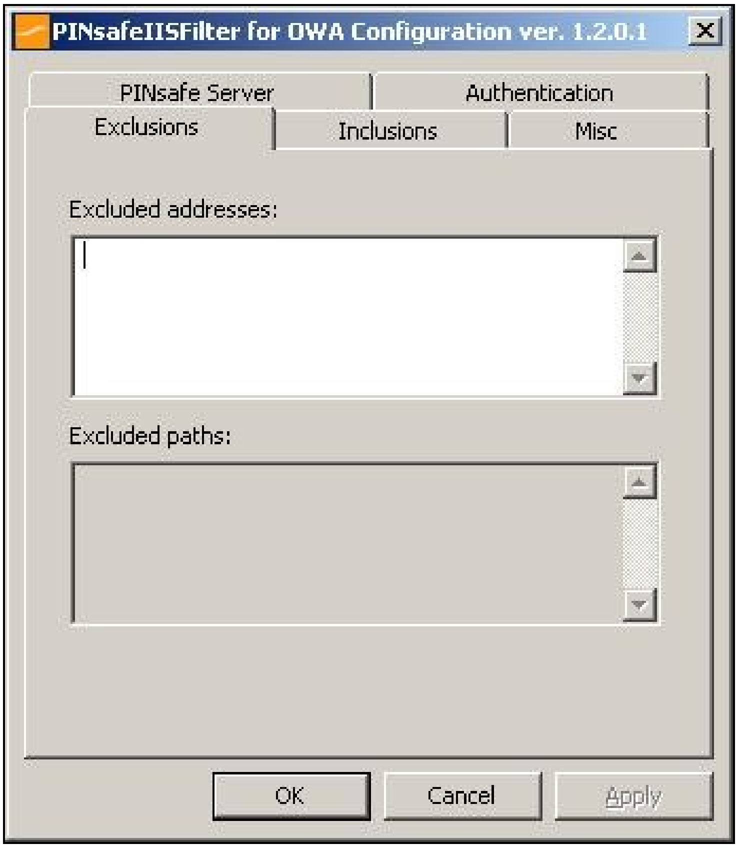
□ Permit self-reset

□ 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.

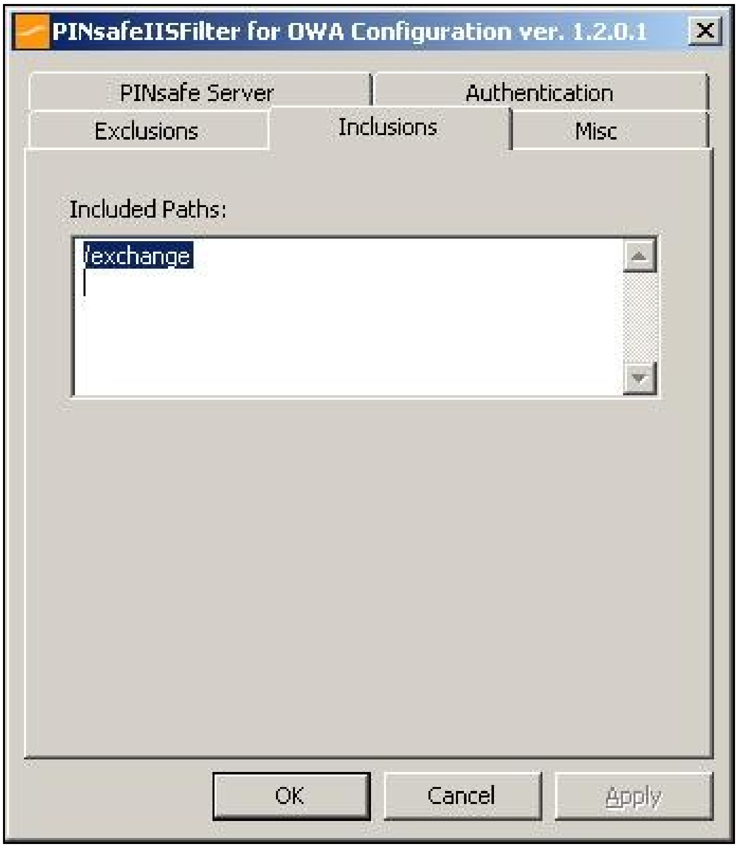

PINsafeIISFilter for OWA Configuration ver. 1.2.0.1

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

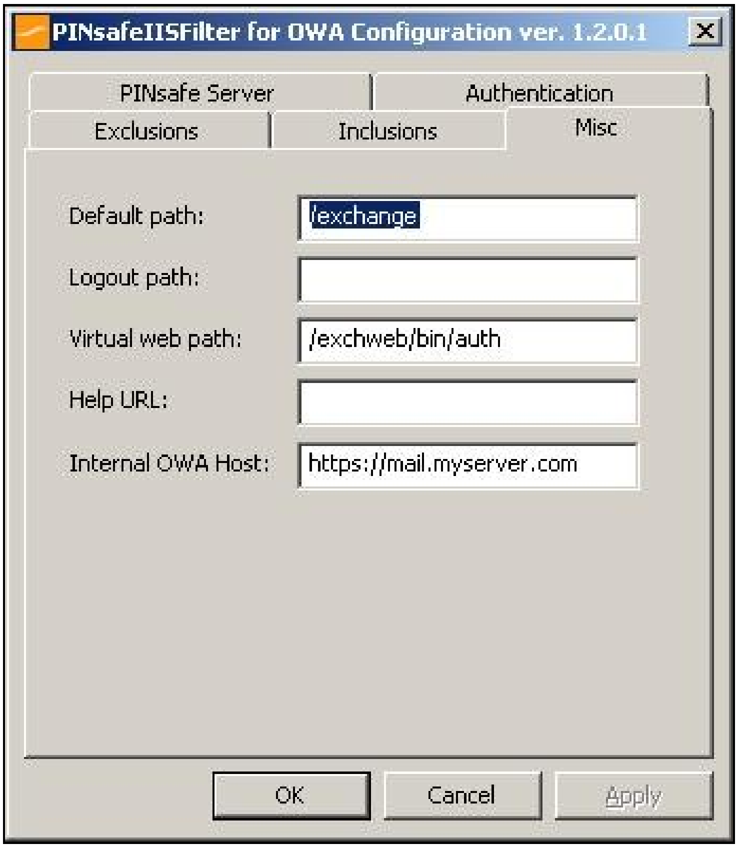
Default path: This is the path to which authenticated requests are directed if the login page is targeted directly. For this particular version of the filter, it should be ?/exchange?. If a user tries to access a protected page, she is redirected to the login page, and after authentication, back to the 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?.



Default path: /exchange

Logout path:

Virtual web path: /exchweb/bin/auth

Help URL:

Internal OWA Host: https://mail.myserver.com

1.5.4 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.

1.5.5 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()?
```

1.5.6 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.

1.5.7 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.

1.5.8 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.

1.5.9 Activating the ISAPI filter

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

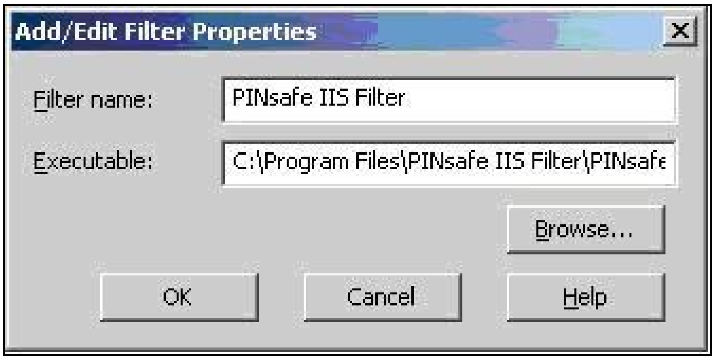
2. Select ISAPI filters

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\

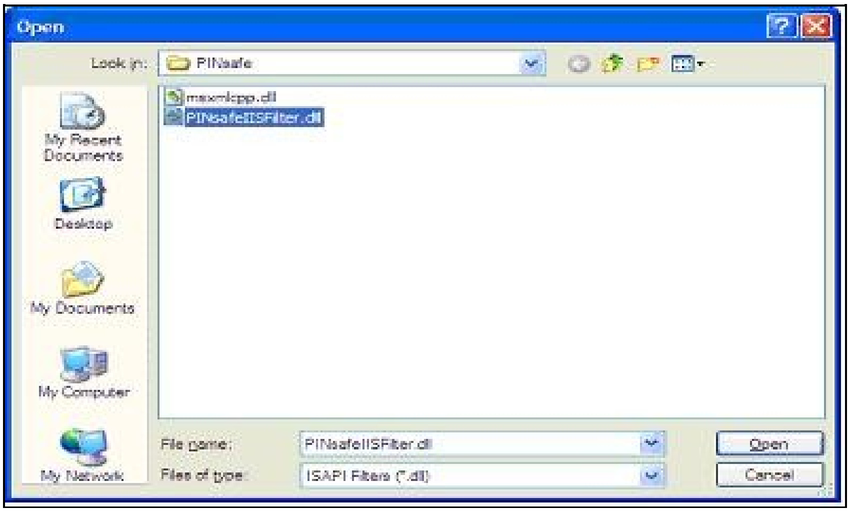
5. Ensure PINsafe ISAPI filter is top filter then click on OK



Add/Edit Filter Properties

Filter name: PINsafe IIS Filter

Executable: C:\Program Files\PINsafe IIS Filter\PINsafe



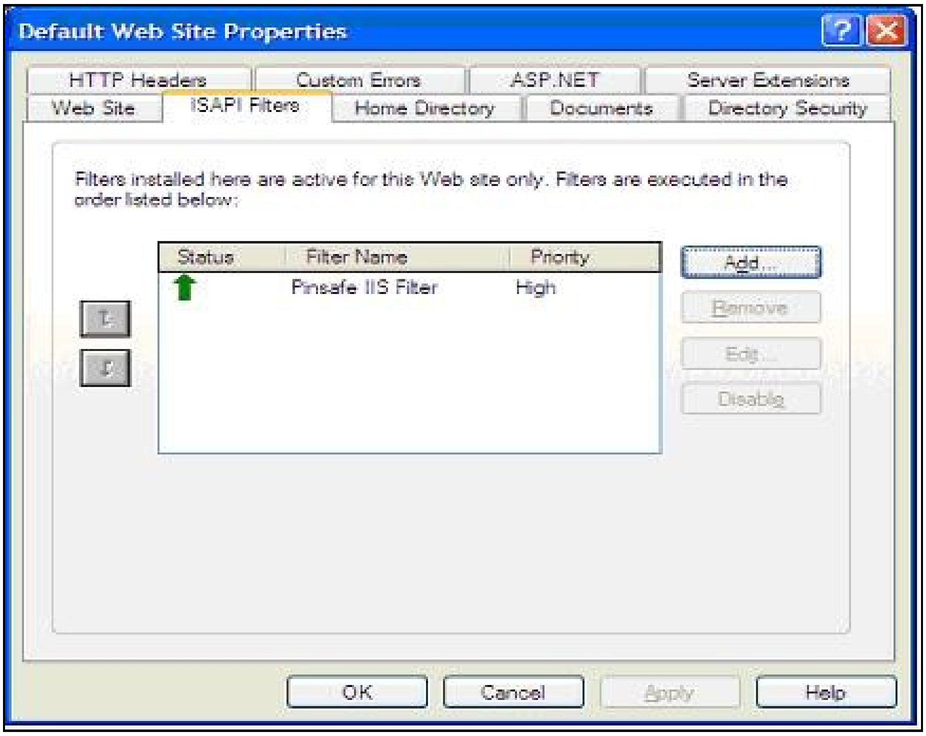
Open

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

1.5.10 Configure The PINsafe Server

Configure a PINsafe Agent (For standard XML Authentication)

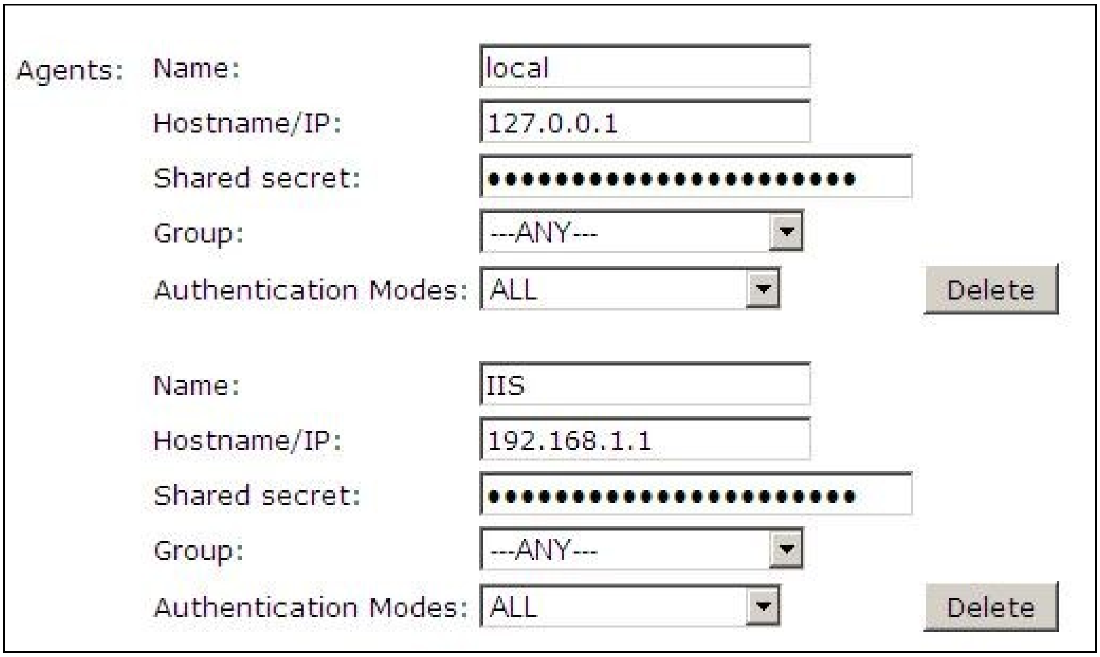
1. On the PINsafe Management Console select Server/Agent

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



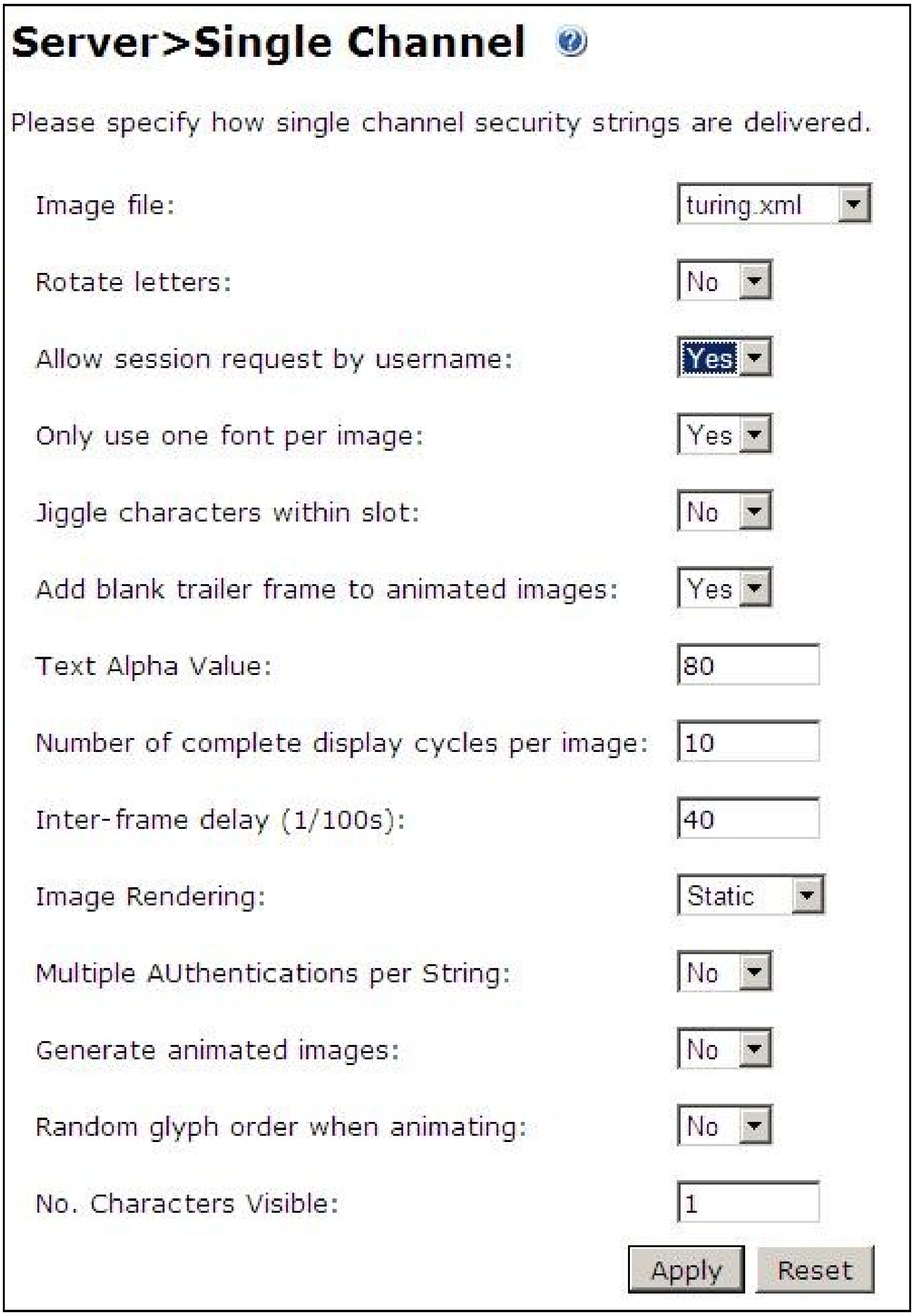
Agents: Name: local
Hostname/IP: 127.0.0.1
Shared secret: ●●●●●●●●●●●●●●●●●●●●●●●
Group: ---ANY---
Authentication Modes: ALL

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

1.6 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.

1.7 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.

1.8 Troubleshooting

1.8.1 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.

1.8.2 No Login Page Errors

No login page, check the Exchange version

Check to see if an International version of OWA is being used

1.8.3 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>

1.8.4 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.

1.8.5 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.

1.8.6 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.

1.9 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

1.10 Useful Links

HTTP to HTTPS Redirect [1]

1.11 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

2 Microsoft OWA 2007 IIS Integration

3 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.

4 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).

5 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

6 Architecture

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

7 Installation

7.1 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

7.2 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.

7.2.1 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

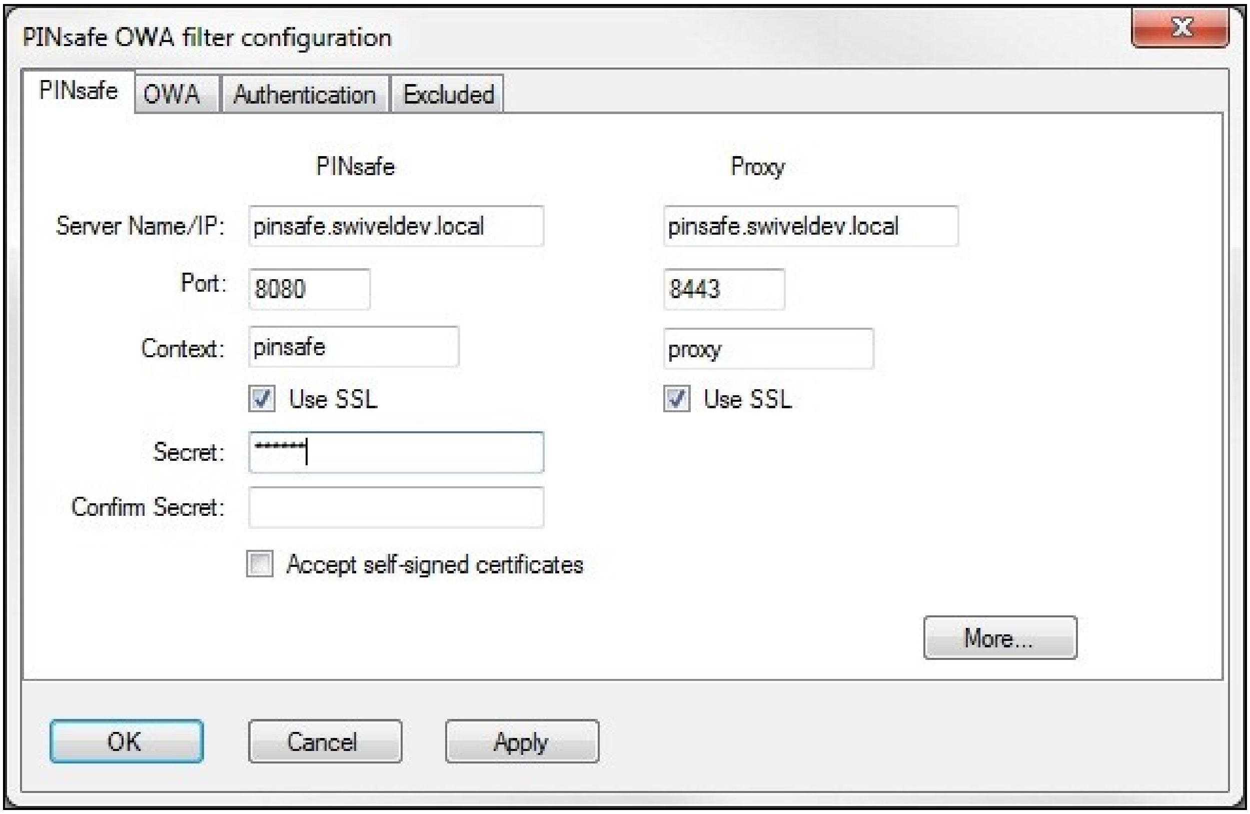
Accept self-signed certificates Where SSL is used with self signed certificates, for a Swivel virtual or hardware appliance tick this box until a valid certificate is installed.

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	

7.2.2 OWA Settings

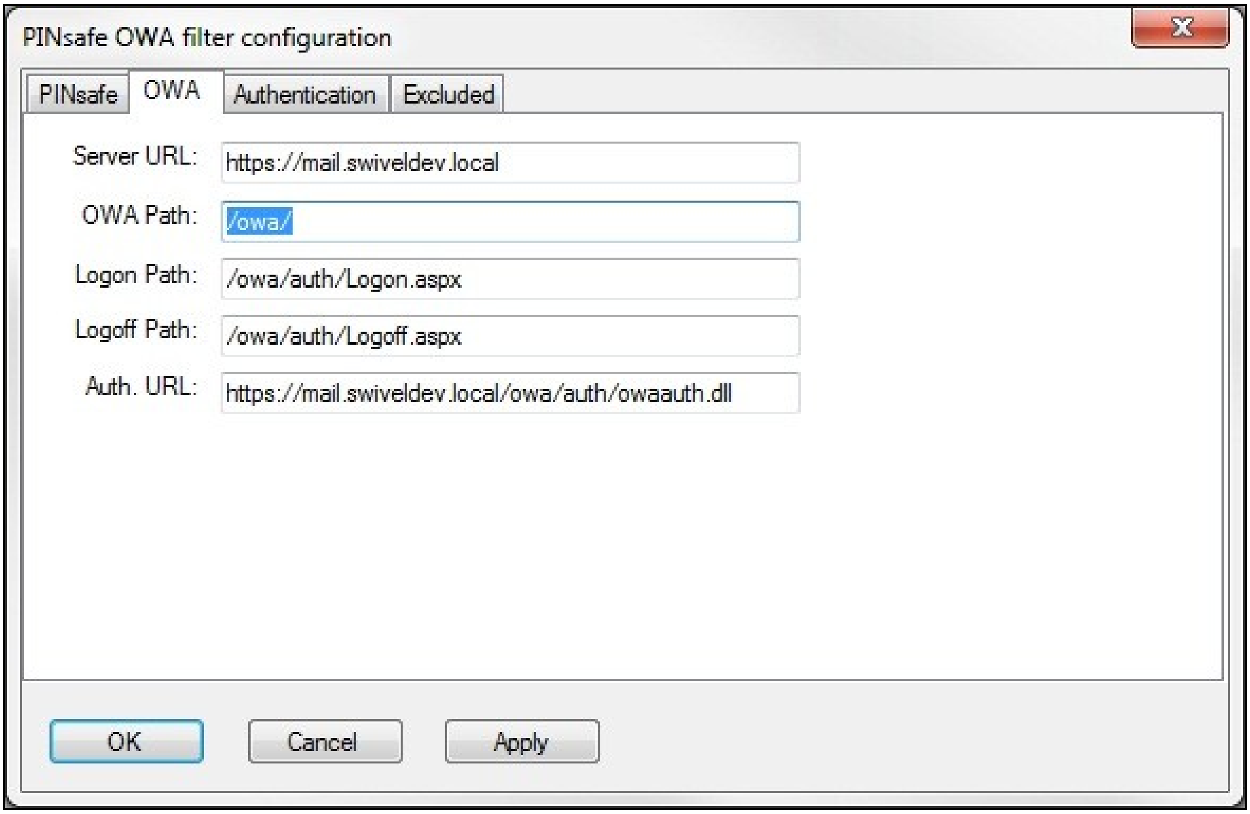
Server URL: Exchange Server URL, Example: https://<exchange.mycompany.com>

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



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

7.2.3 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.

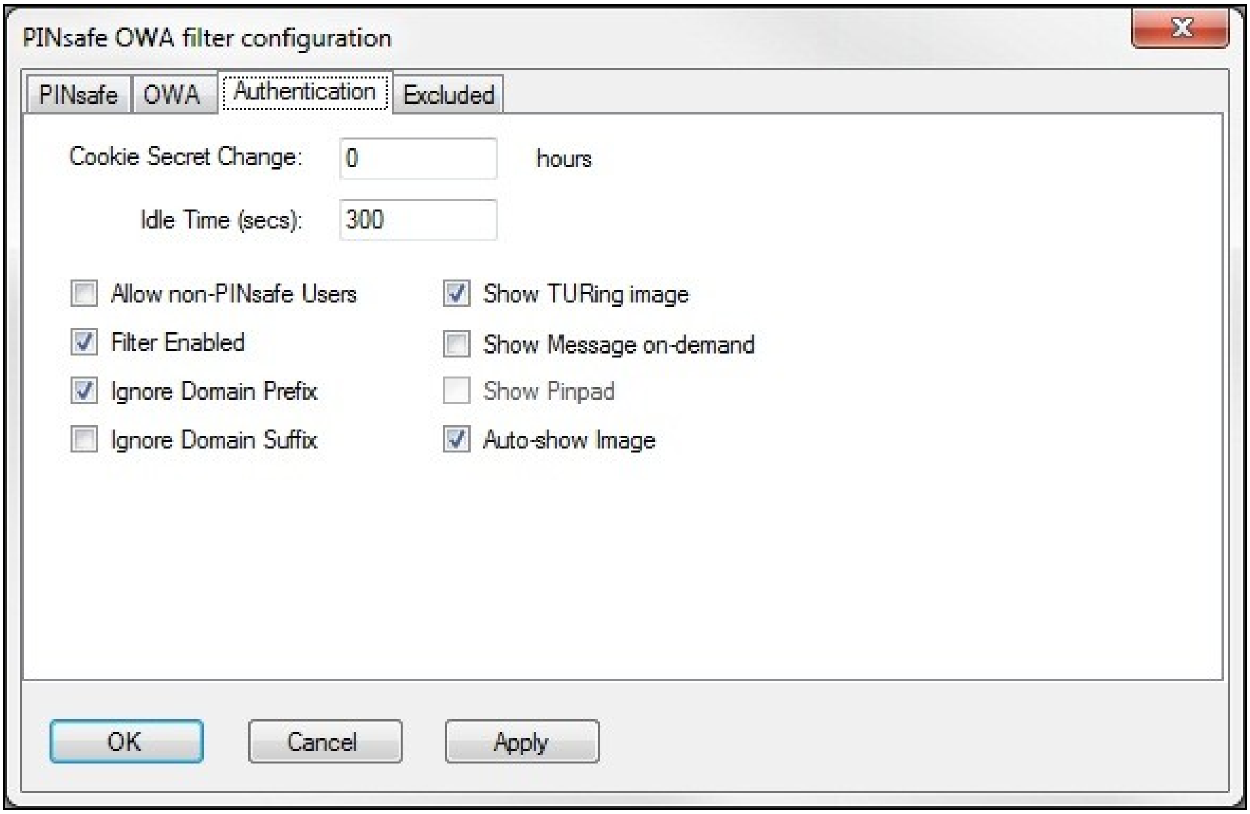
Ignore Domain Suffix If this option is ticked, any suffixed domain (i.e. anything after the '@' character) is removed before sending the username to PINsafe. The full username is sent to OWA.

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

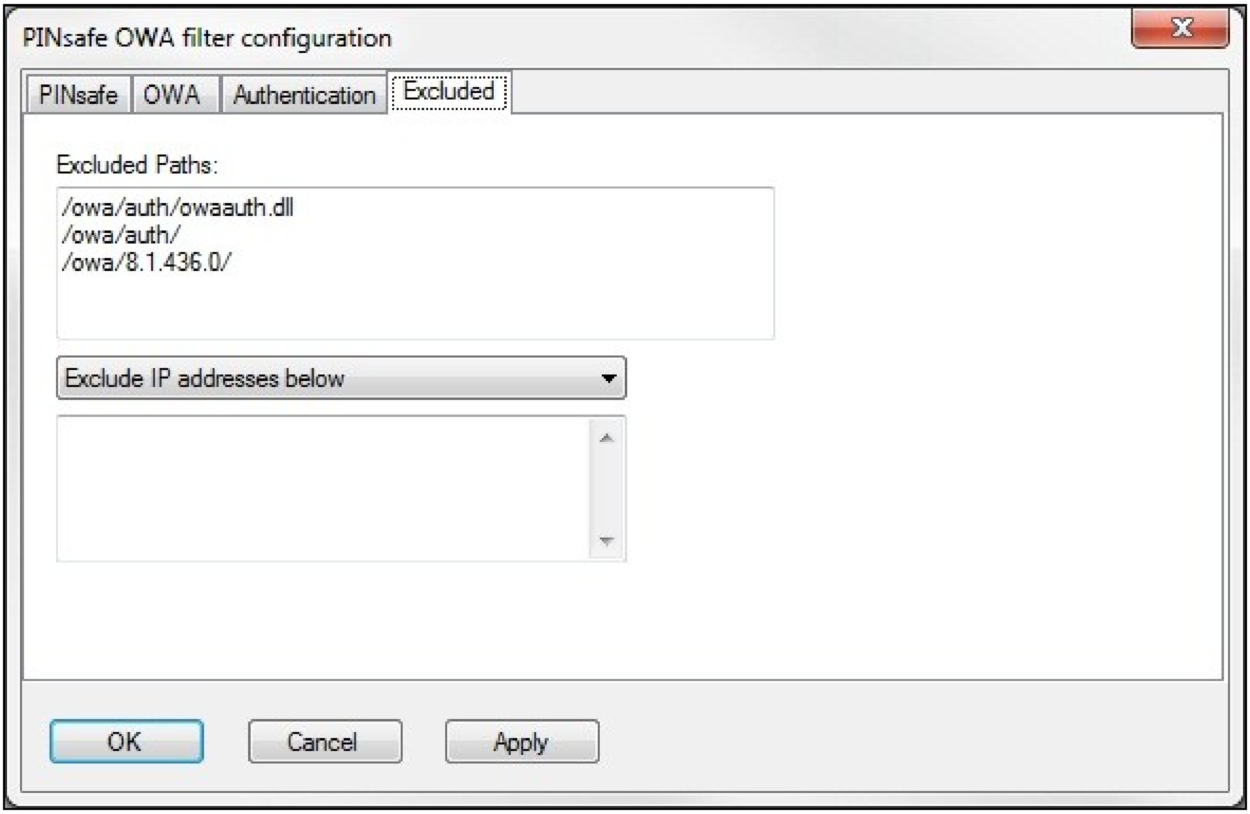
☐ Show Pinpad

☑ Auto-show Image

7.2.4 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

7.3 Configure The PINsafe Server

7.3.1 Configure a PINsafe Agent (For standard XML Authentication)

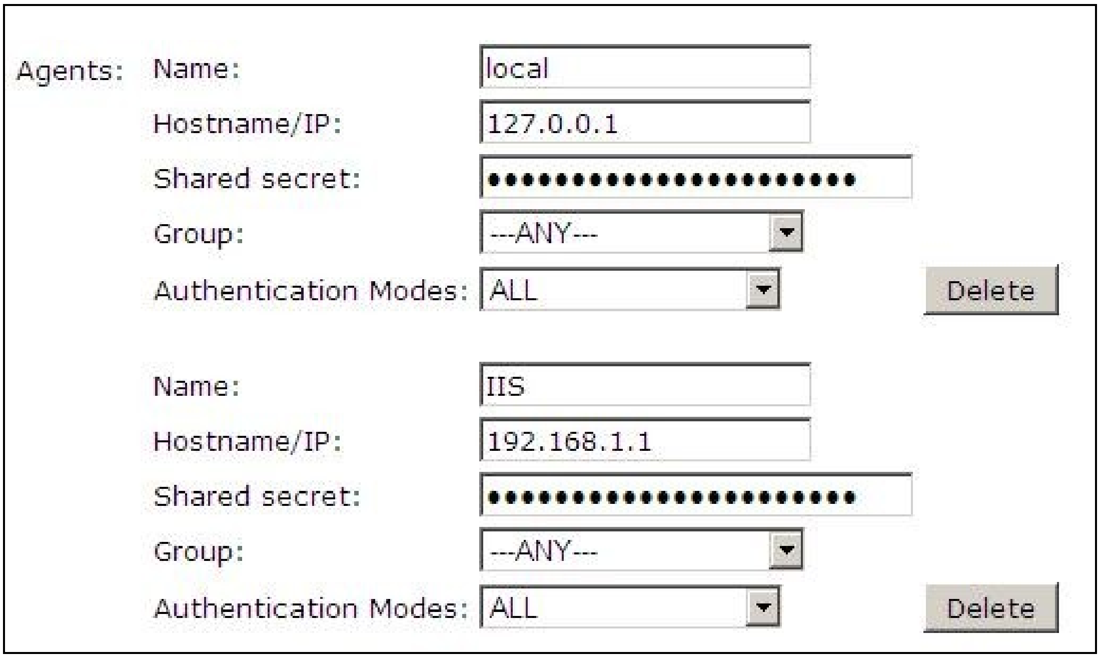
1. On the PINsafe Management Console select Server/Agent

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



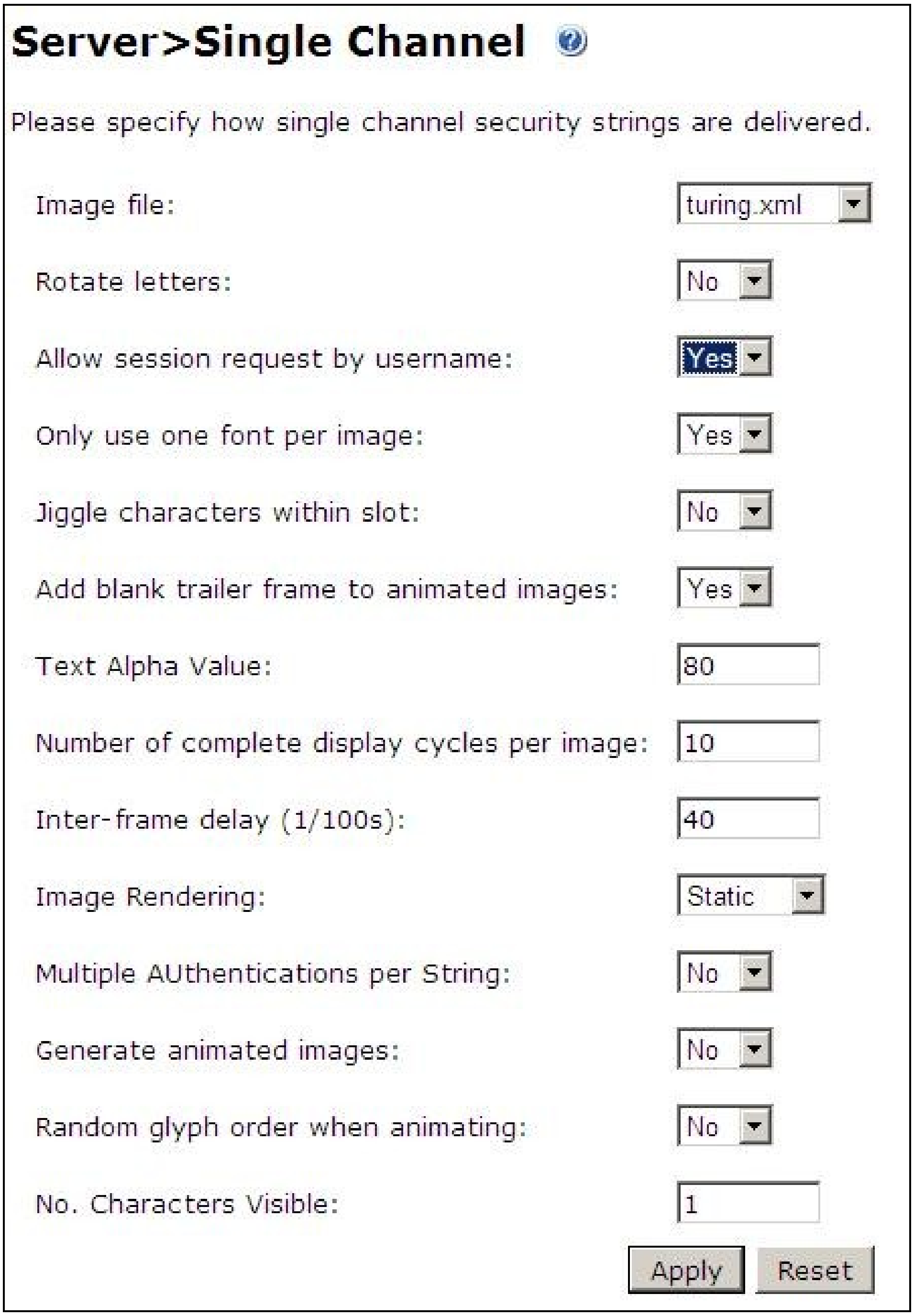
Agents:

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

7.3.2 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

8 Additional Installation Options

8.1 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()?
```

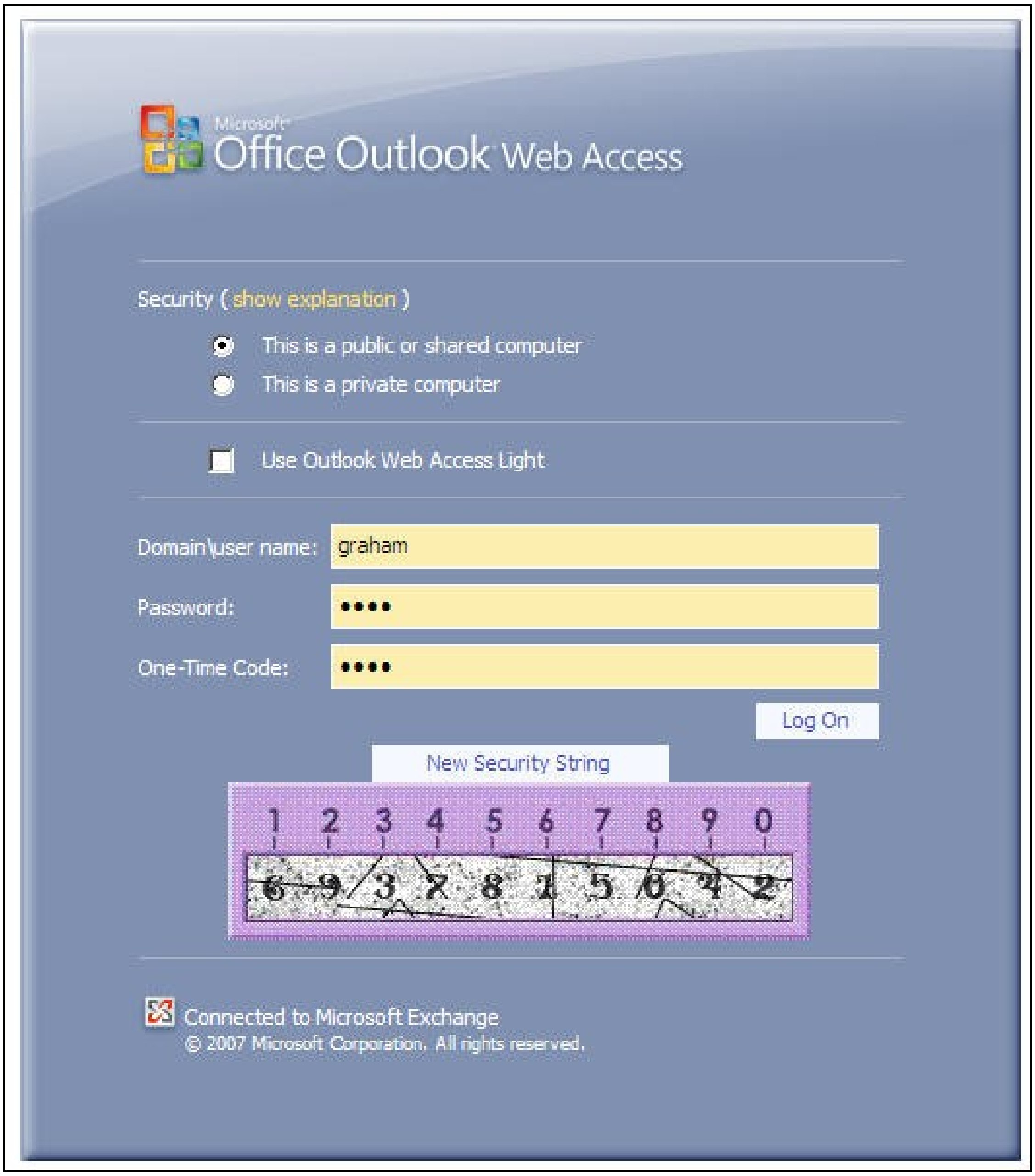
8.2 Modifying the login Page to allow Dual Channel On Demand Delivery

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.

9 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: ••••

Connected to Microsoft Exchange
© 2007 Microsoft Corporation. All rights reserved.

10 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.

11 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.

11.1 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.

12 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.

13 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

14 Microsoft OWA 2010 IIS Integration

15 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.

16 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.

17 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.

17.1 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.

18 File Downloads

Download links:

- Version 2.8
- Version 2.9

18.1 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)

19 Architecture

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

20 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.

20.1 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.

20.2 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.

20.3 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.

20.4 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.

20.4.1 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)

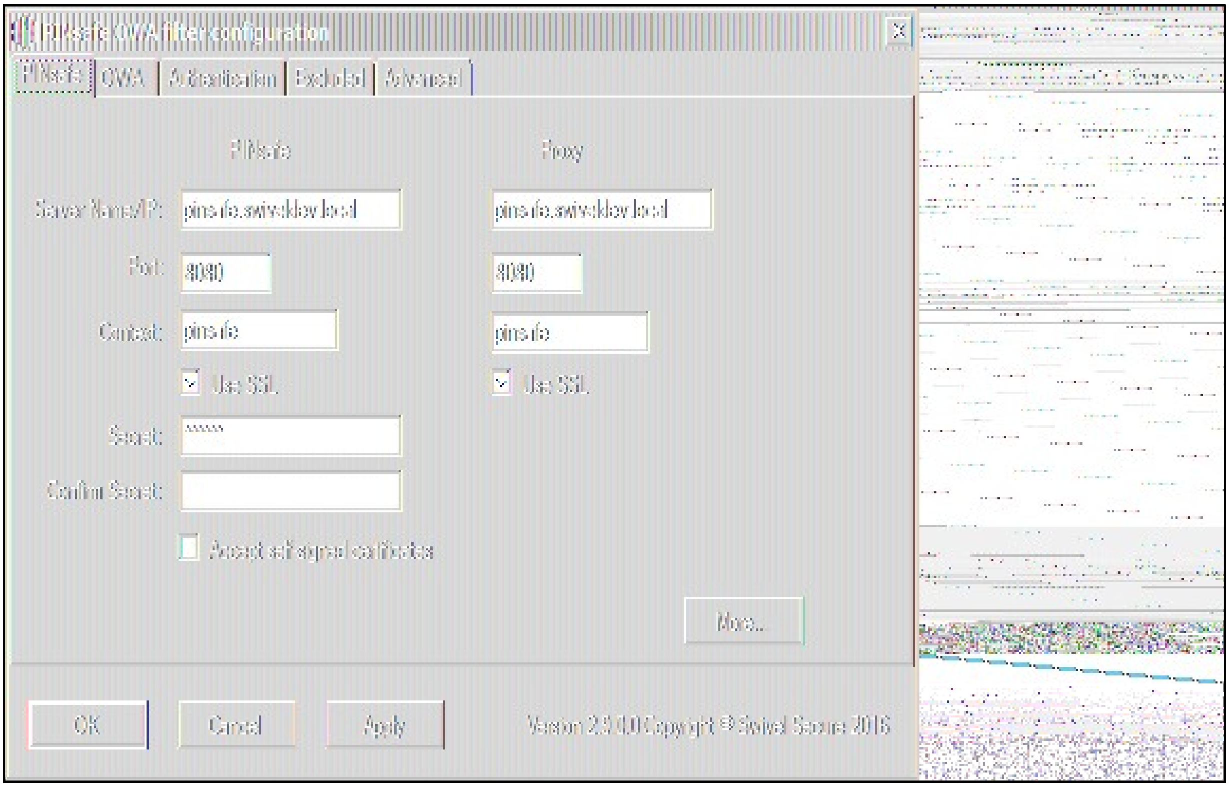
Context: Swivel install name, for a Swivel virtual or hardware appliance use pinsafe (not proxy)

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 OWA filter configuration

PINsafe / Proxy

Server Name/IP: pinsafe.swivelkdev.local / pinsafe.swivelkdev.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

20.4.2 OWA Settings

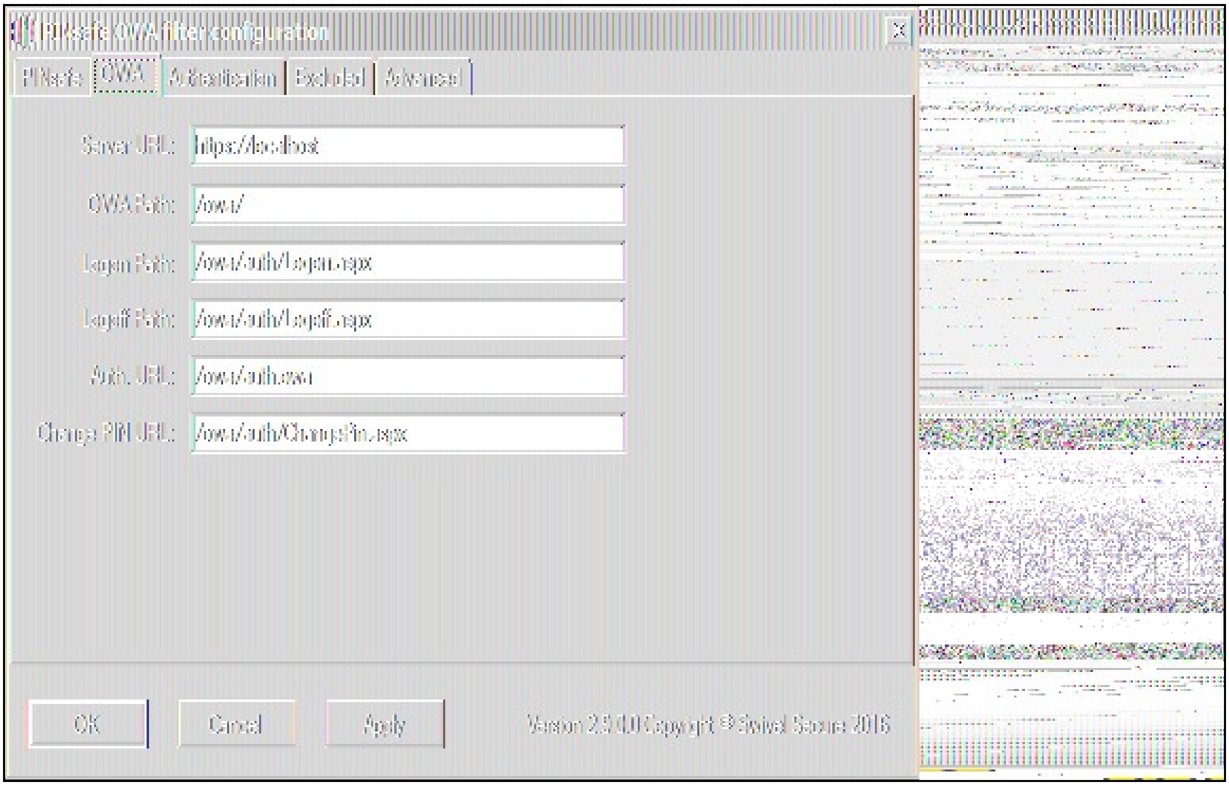
Server URL: Exchange Server URL, Example: https://<exchange.mycompany.com>

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



PINsafe OWA filter configuration

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

20.4.3 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.

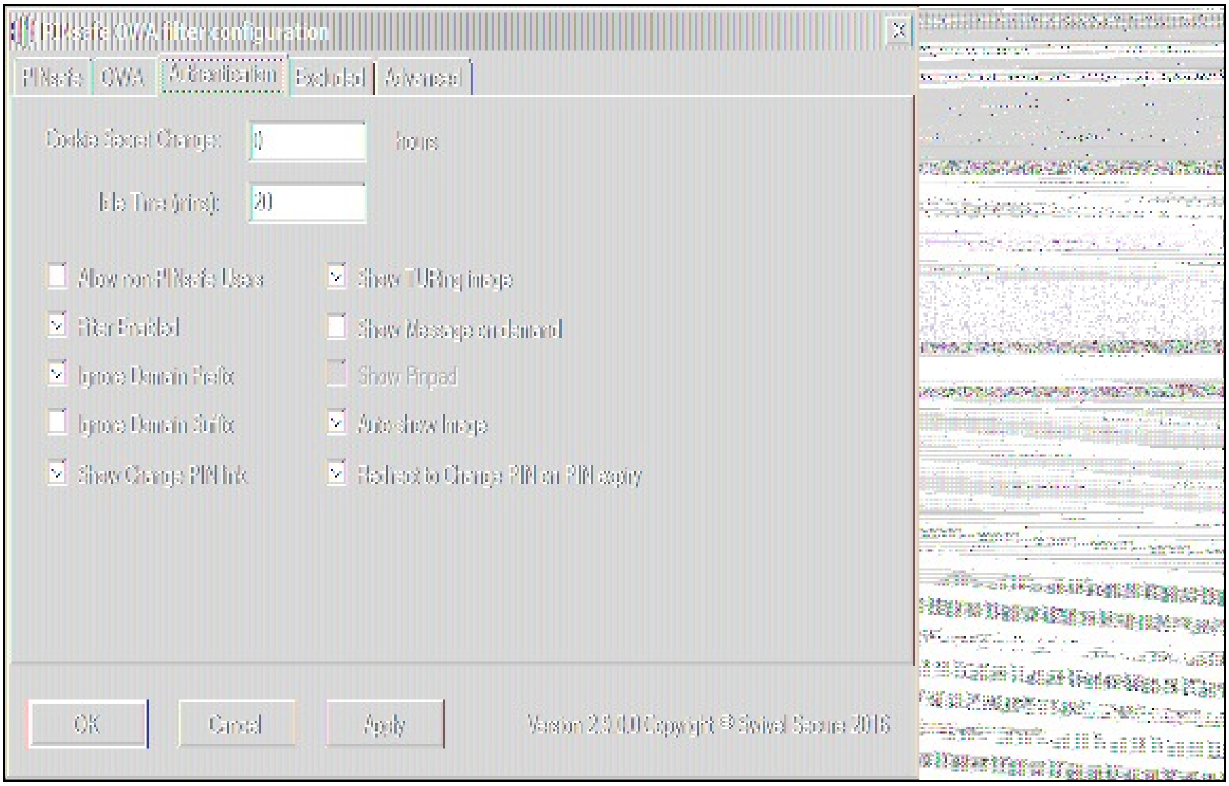
Ignore Domain Suffix If this option is ticked, any suffixed domain (i.e. anything after the '@' character) is removed before sending the username to PINsafe. The full username is sent to OWA.

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.


PINsafe OWA filter configuration
PINsafe
OWA
Authentication
Excluded
Advanced
OK
Cancel
Apply
Version 2.5.0.0 Copyright © Swivel Secure 2016

Cookie Secret Change: 0 hours

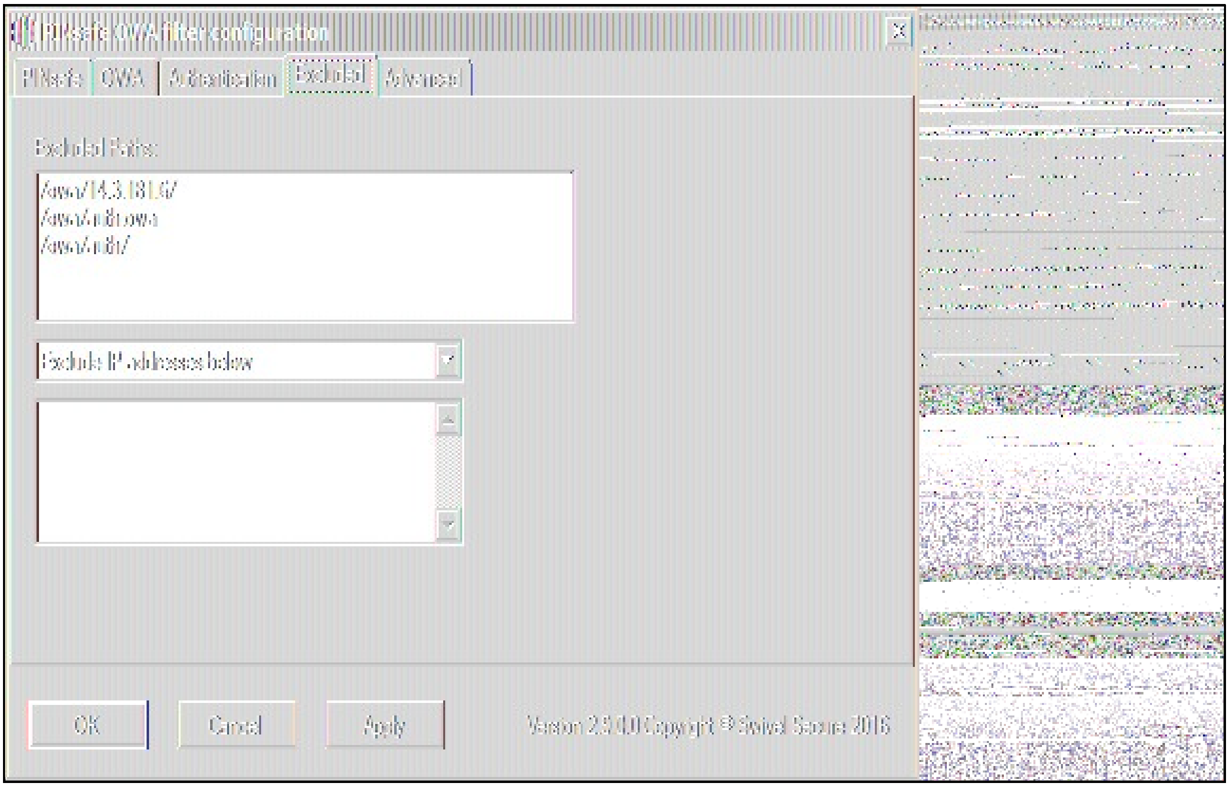
Idle Time (mins): 20

□ 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

20.4.4 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

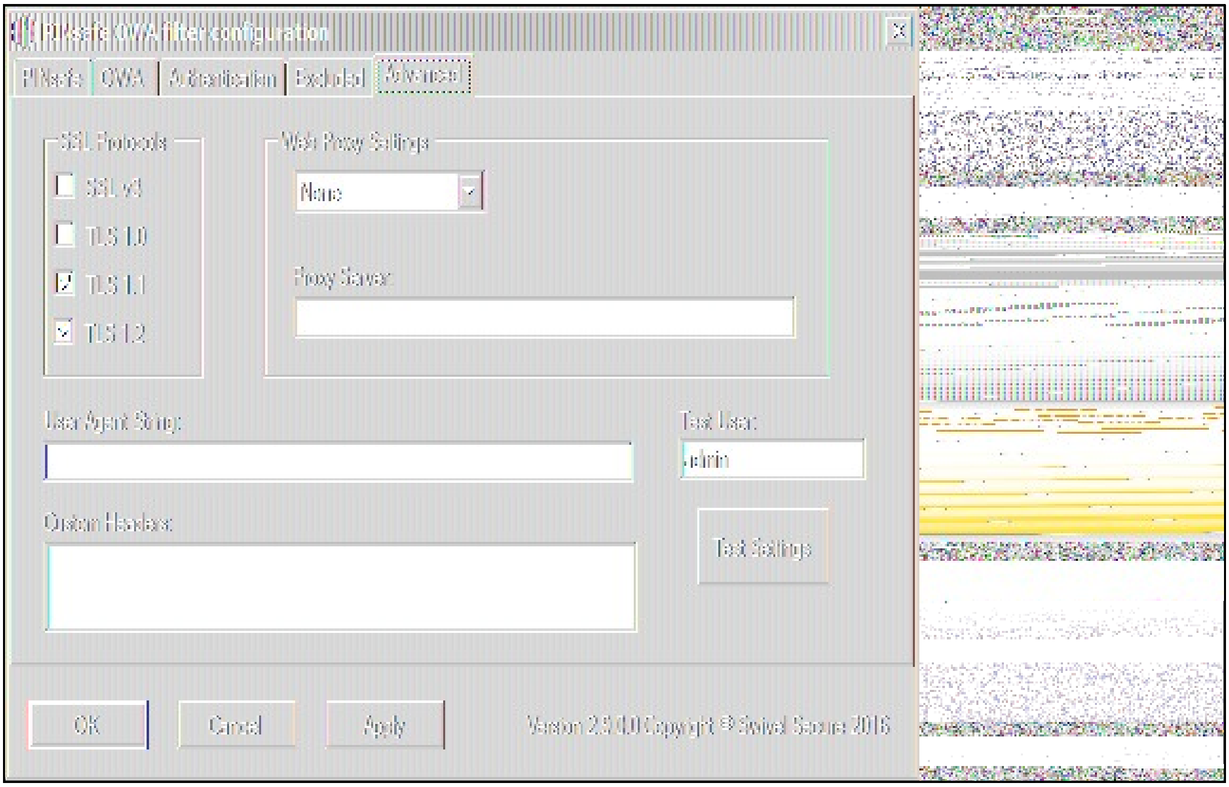
20.4.5 Advanced Settings

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 2.5.0.0 Copyright © Swivel Secure 2016

20.5 Configure The Swivel Server

Configure a Swivel Agent (For standard XML Authentication)

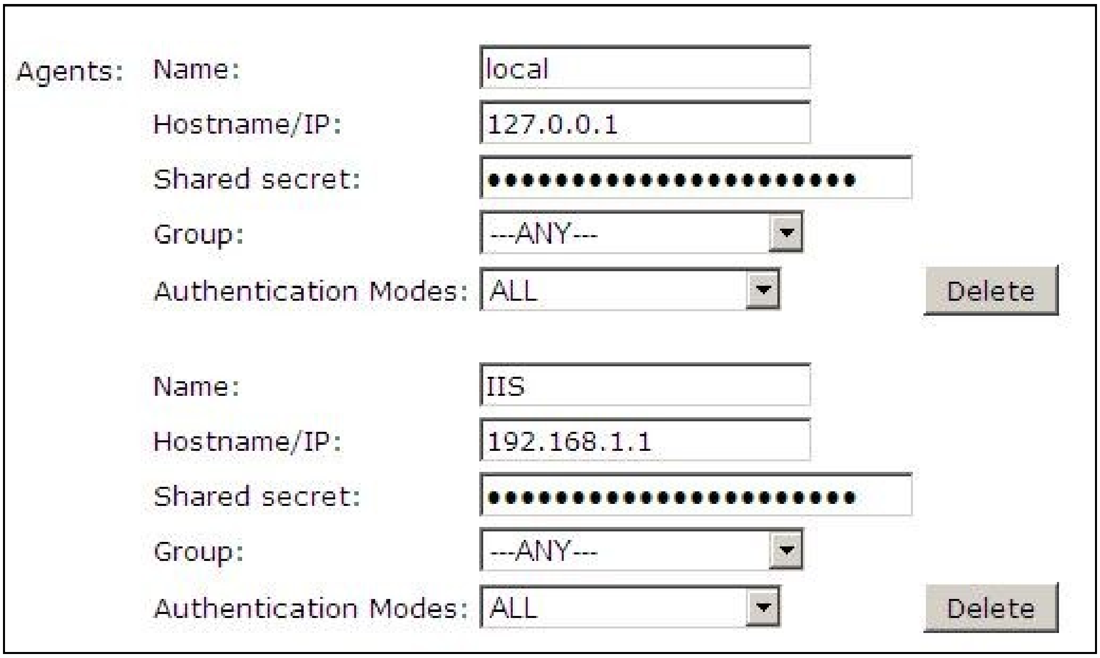
1. On the Swivel Management Console select Server/Agent

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



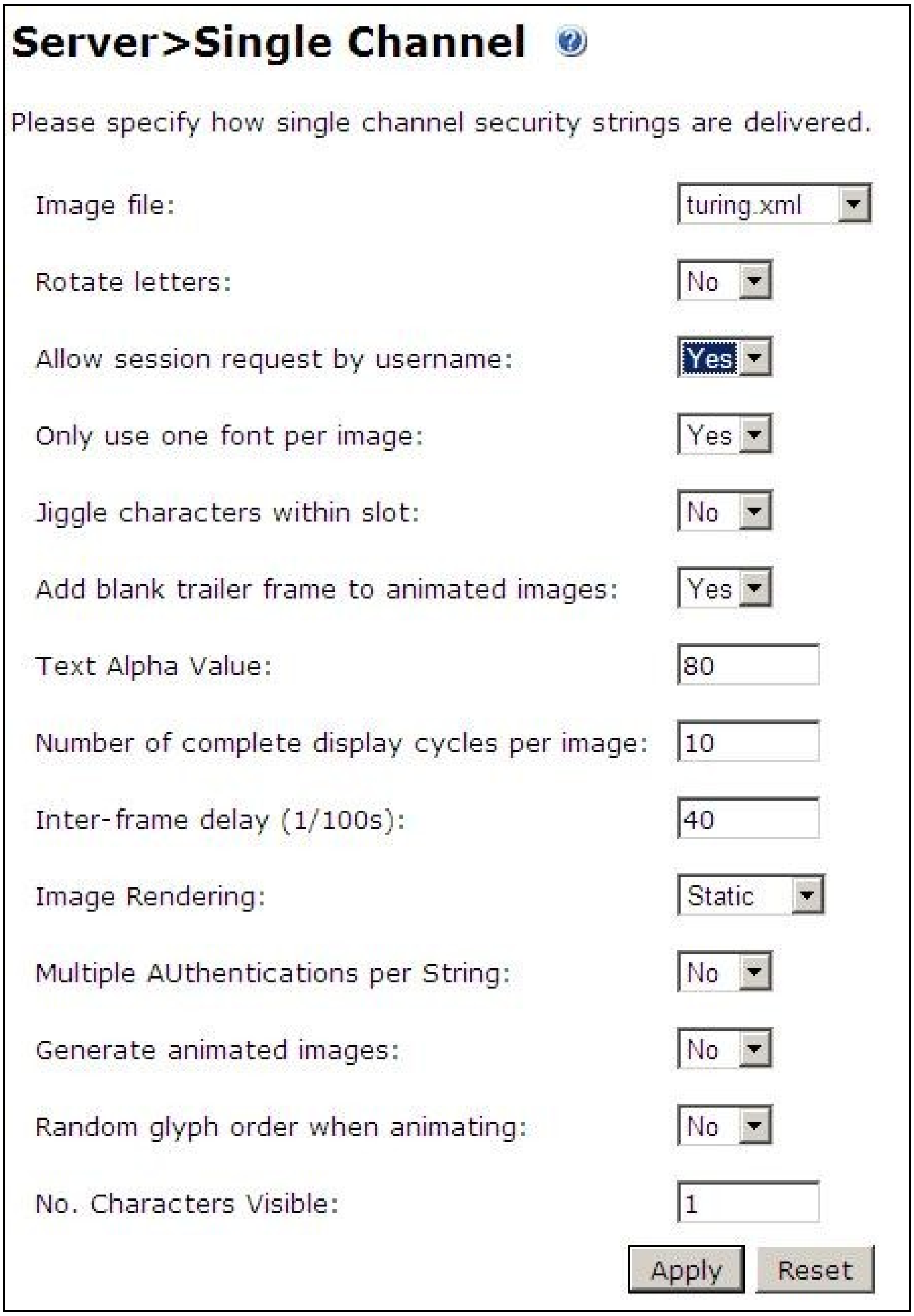
Agents:

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

20.6 Using additional attributes for authentication

When using additional attributes for authentication see User Attributes How To

21 Additional Installation Options

21.1 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()?
```

21.2 Modifying the login Page to allow Dual Channel On Demand Delivery

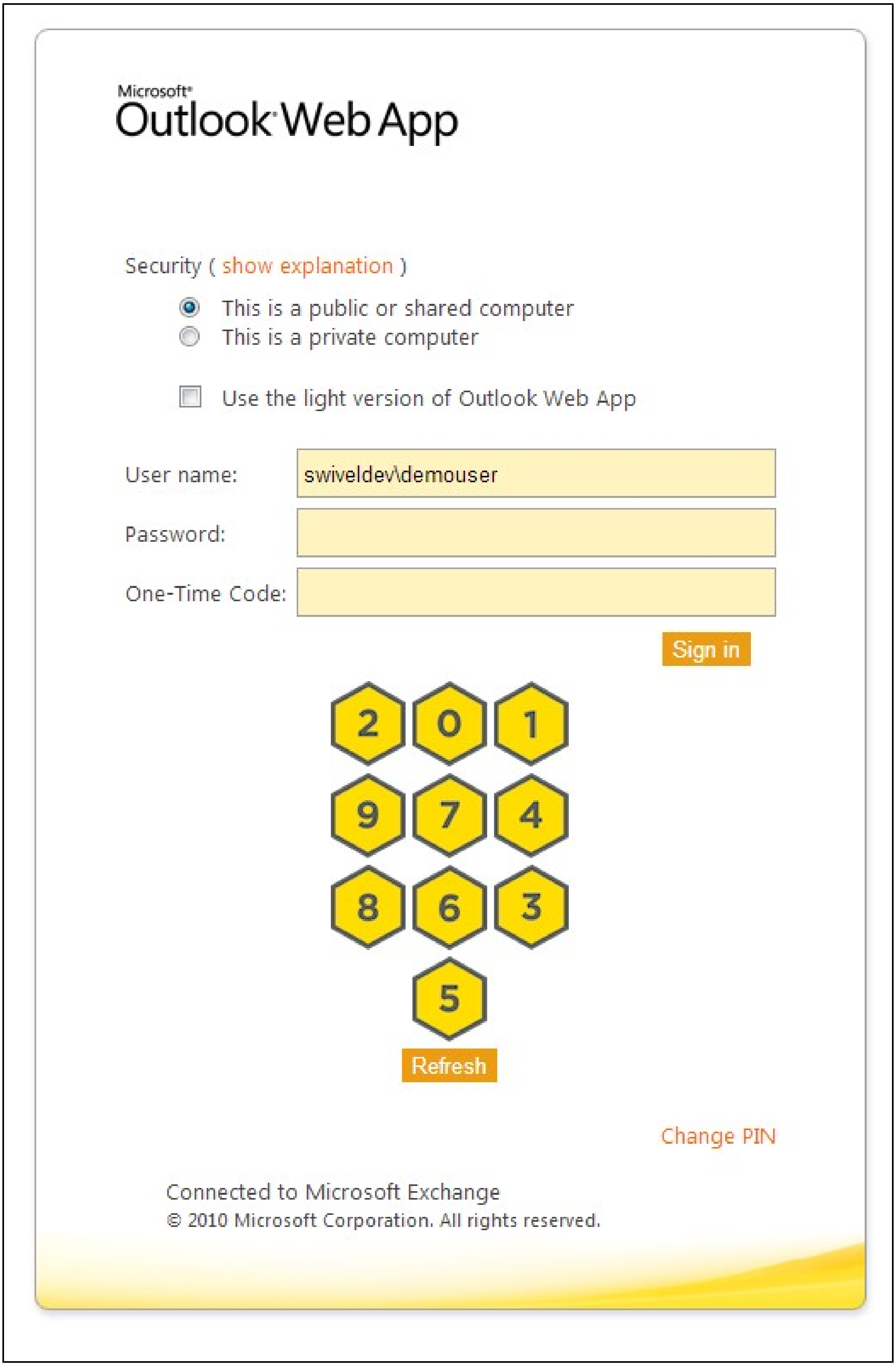
NOTE: this refers to older versions of the filter. In versions 2.5 and higher, this is set in the configuration program.

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.

22 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.



Microsoft® Outlook Web App

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.

23 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.

23.1 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.

24 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.

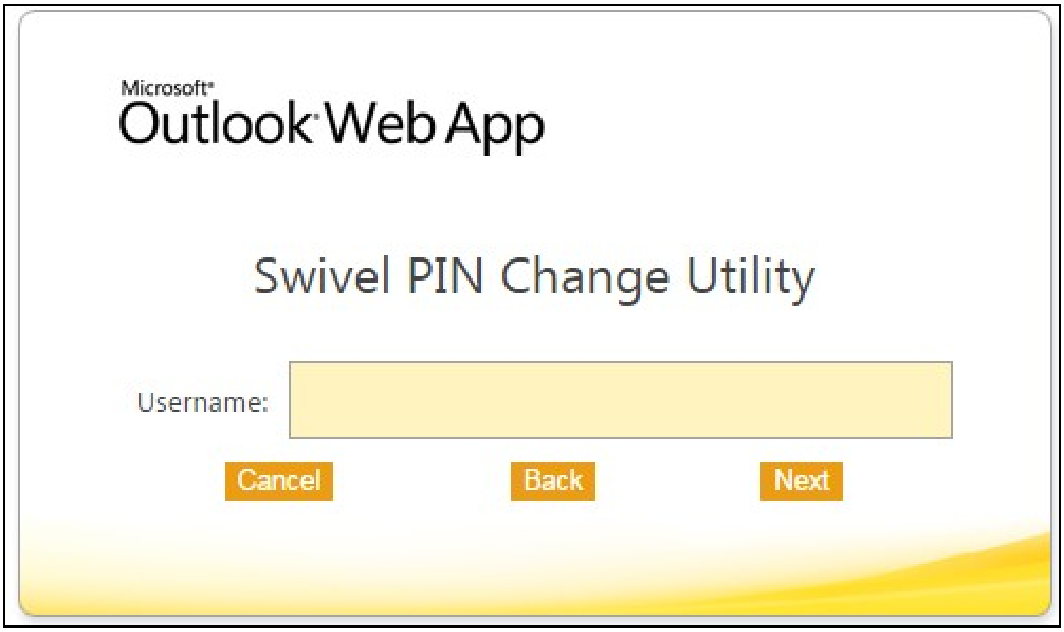
If you selected the Change PIN page in error, and want to return to the login page, then click the "Cancel" button ("Skip" button before 2.8.4) to return without changing your PIN.

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.

24.1 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.

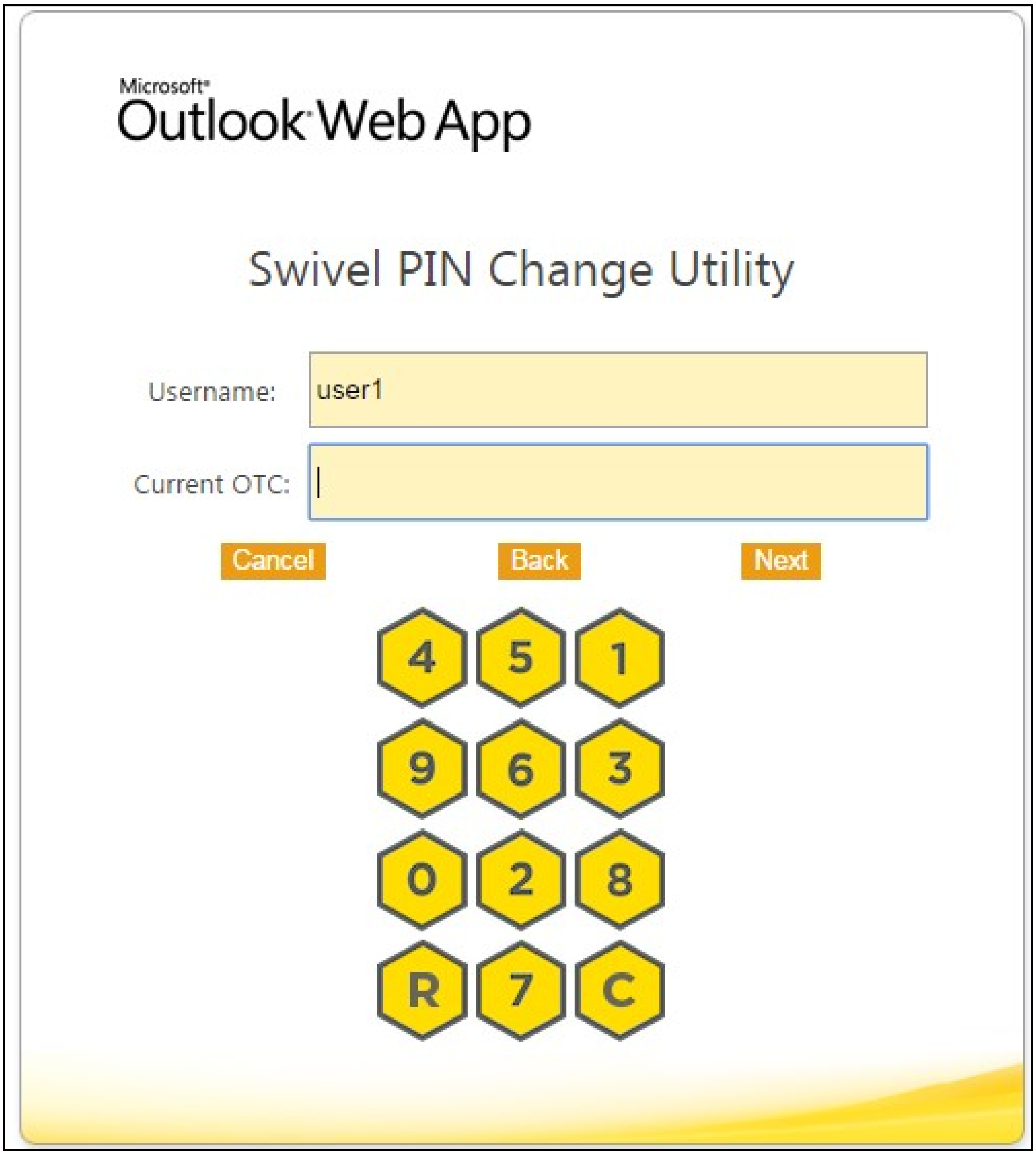
The initial screen (with or without Pinpad) looks like this:



Swivel PIN Change Utility

Username:

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

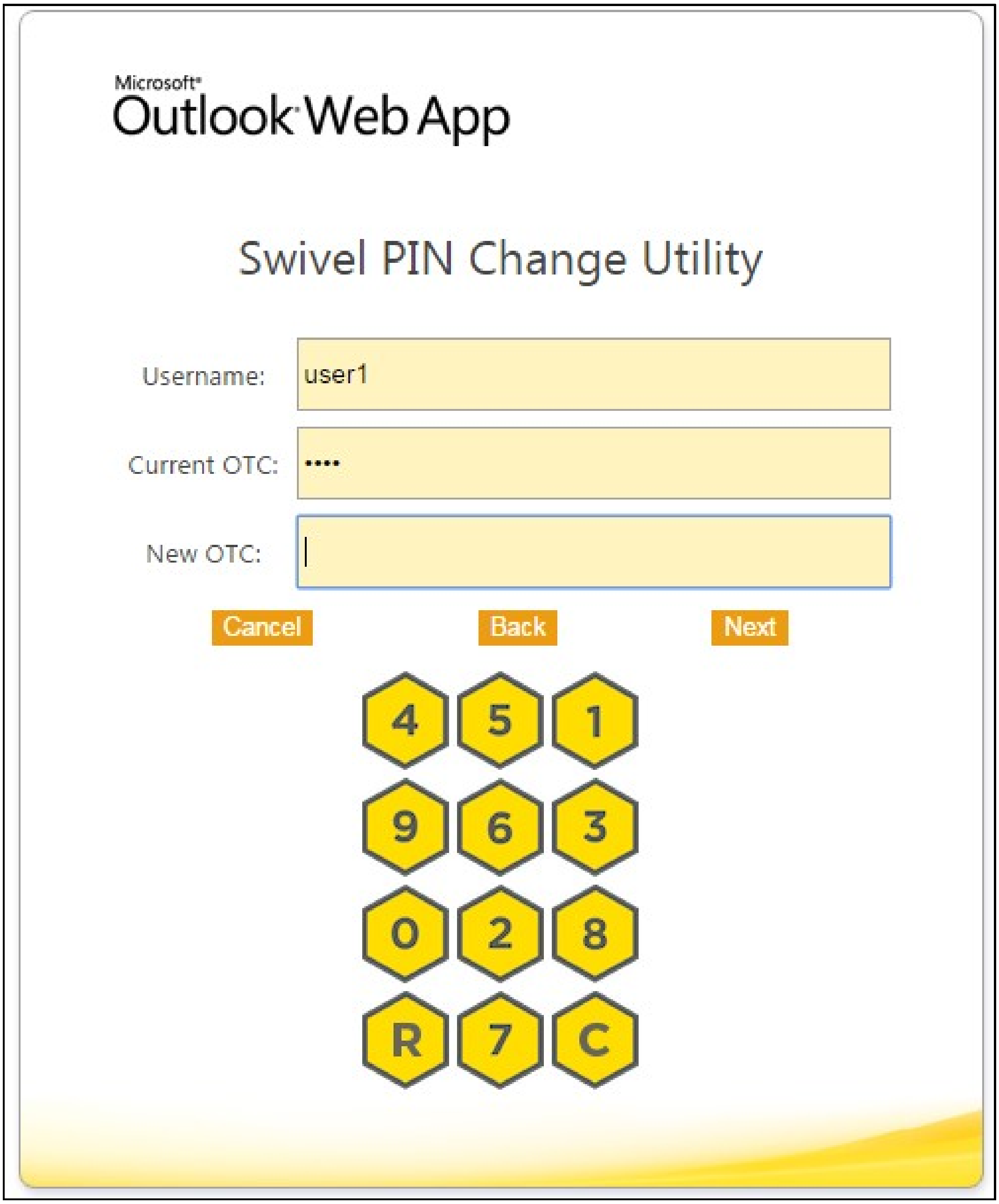


Swivel PIN Change Utility

Username: user1

Current OTC:

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



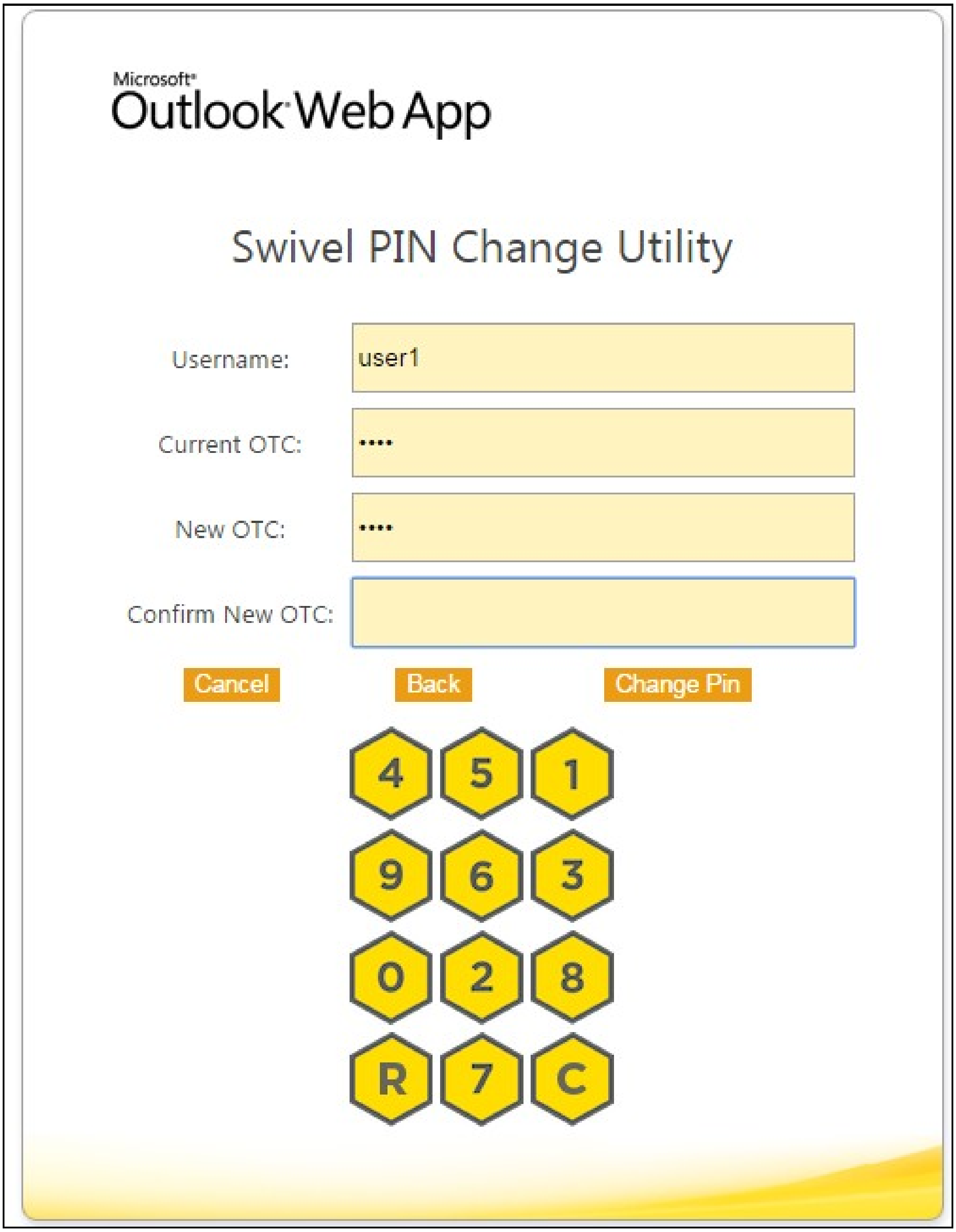
Swivel PIN Change Utility

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: ••••

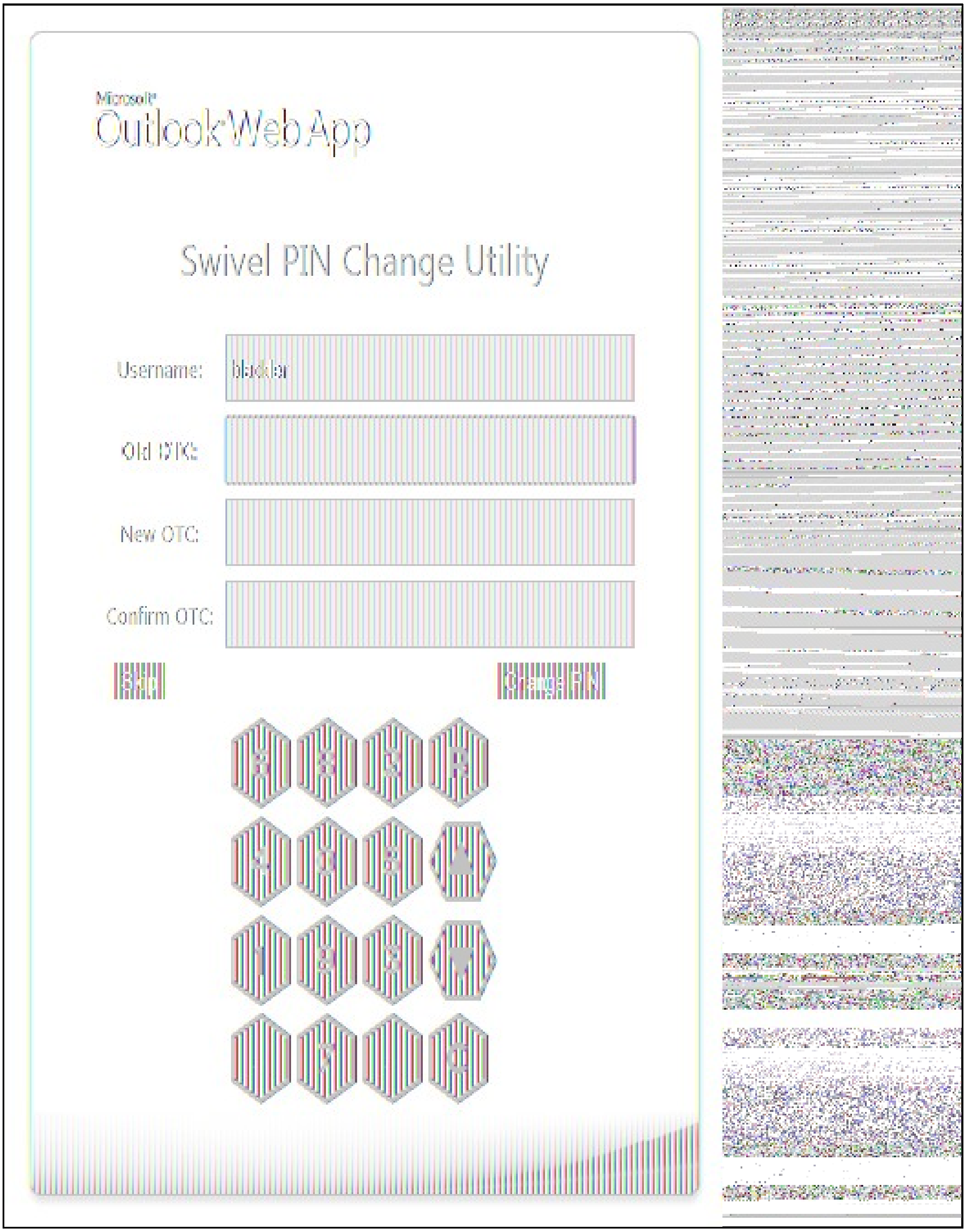
New OTC: ••••

Confirm New OTC:

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

24.1.1 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:



Username: blackler

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.

25 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>

25.1 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" />

25.2 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.

25.3 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.

25.4 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.

25.5 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.

26 Known Issues and Limitations

26.1 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.

26.1.1 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.

26.1.2 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.

26.1.3 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.

26.1.4 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.

26.1.5 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.

26.1.6 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.

26.1.7 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>

27 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).

28 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.

29 Microsoft OWA 2013 IIS Integration

30 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.

31 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.

32 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.

33 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.

34 Architecture

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

35 Installation

35.1 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.

35.2 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.

35.2.1 Swivel Settings

Server Name/IP: The Swivel server IP address or hostname

Port: Swivel server port, for a Swivel appliance use 8080 (not 8443)

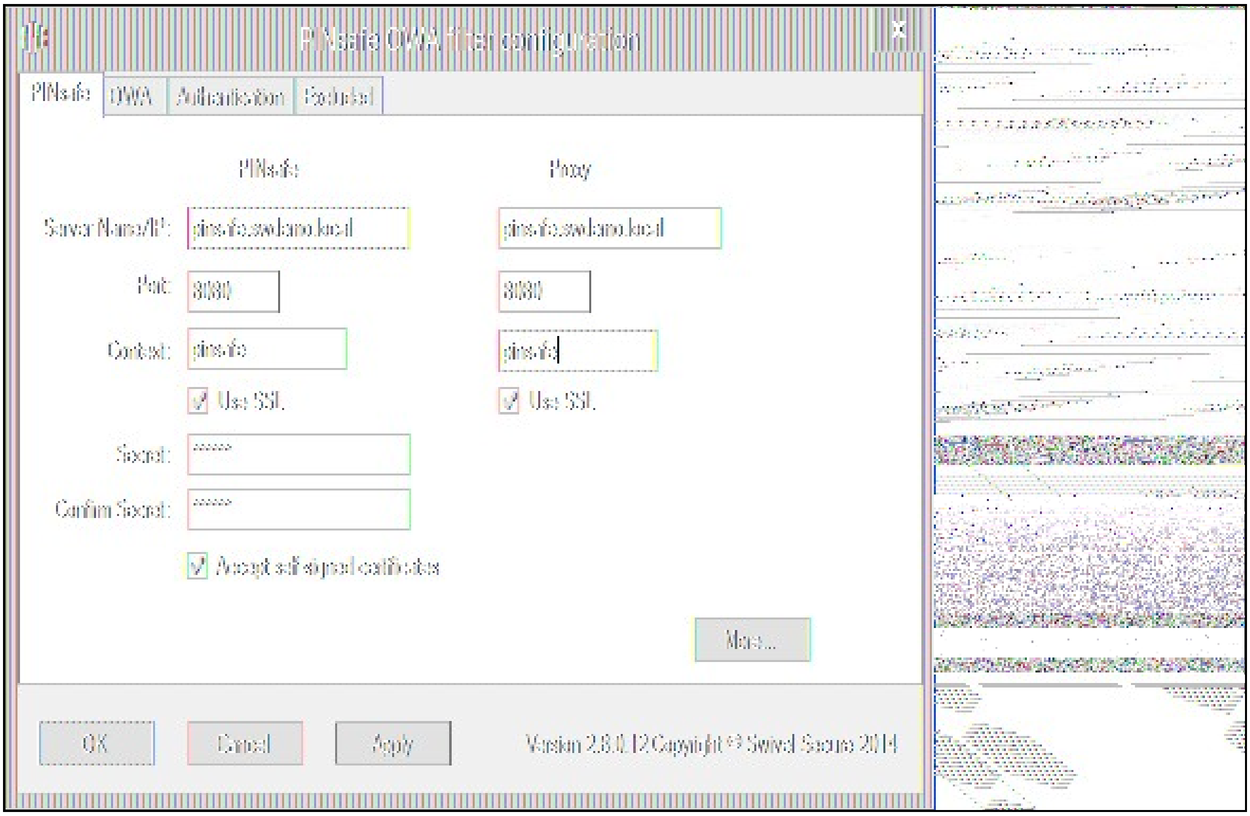
Context: Swivel install name, for a Swivel appliance use Swivel (not proxy)

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	Proxy
Server Name/IP:	pinsafe.swlano.local	pinsafe.swlano.local
Port:	8080	8080
Context:	pinsafe	pinsafe
	☑ Use SSL	☑ Use SSL
Secret:	******	
Confirm Secret:	******	
	☑ Accept self-signed certificates	

Version 2.8.0.12 Copyright © Swivel Secure 2014

35.2.2 OWA Settings

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

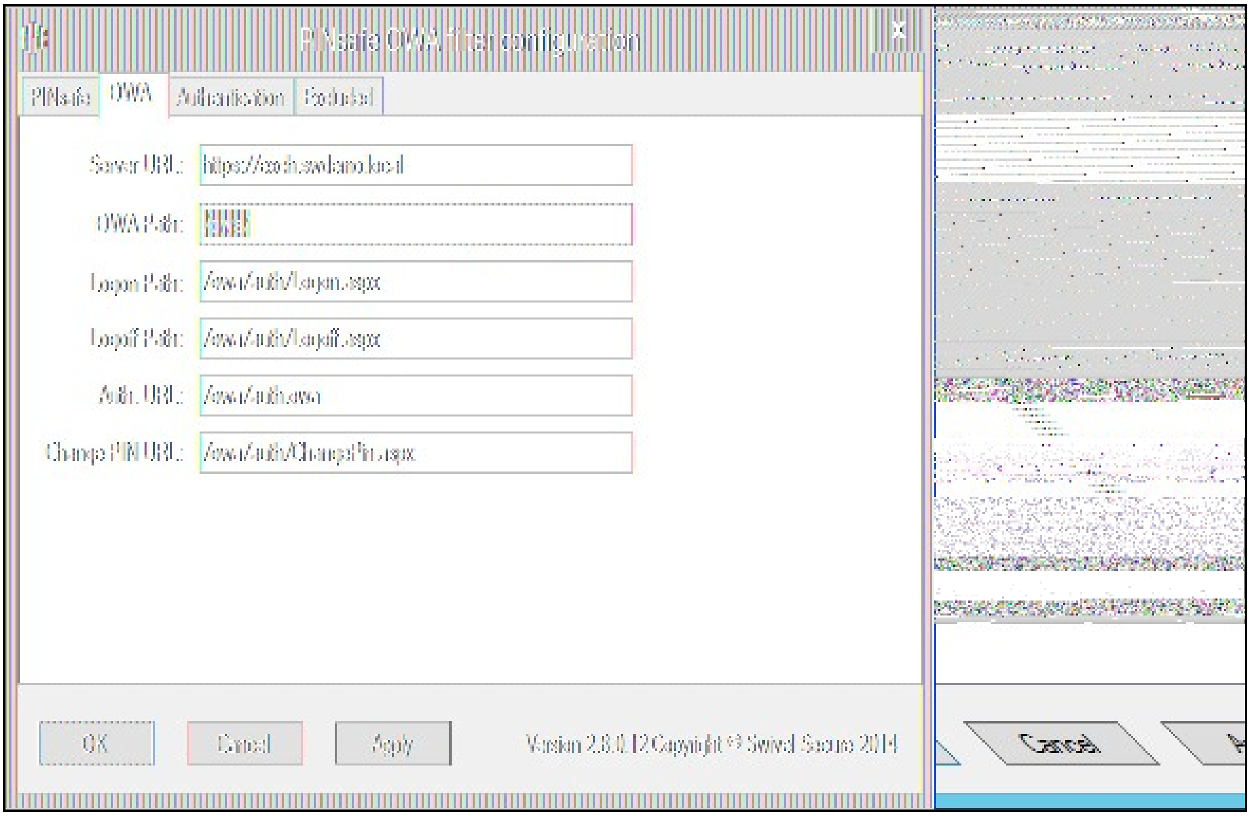
OWA Path: OWA path, usually /owa, unless this has been explicitly changed

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://ooth.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

35.2.3 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.

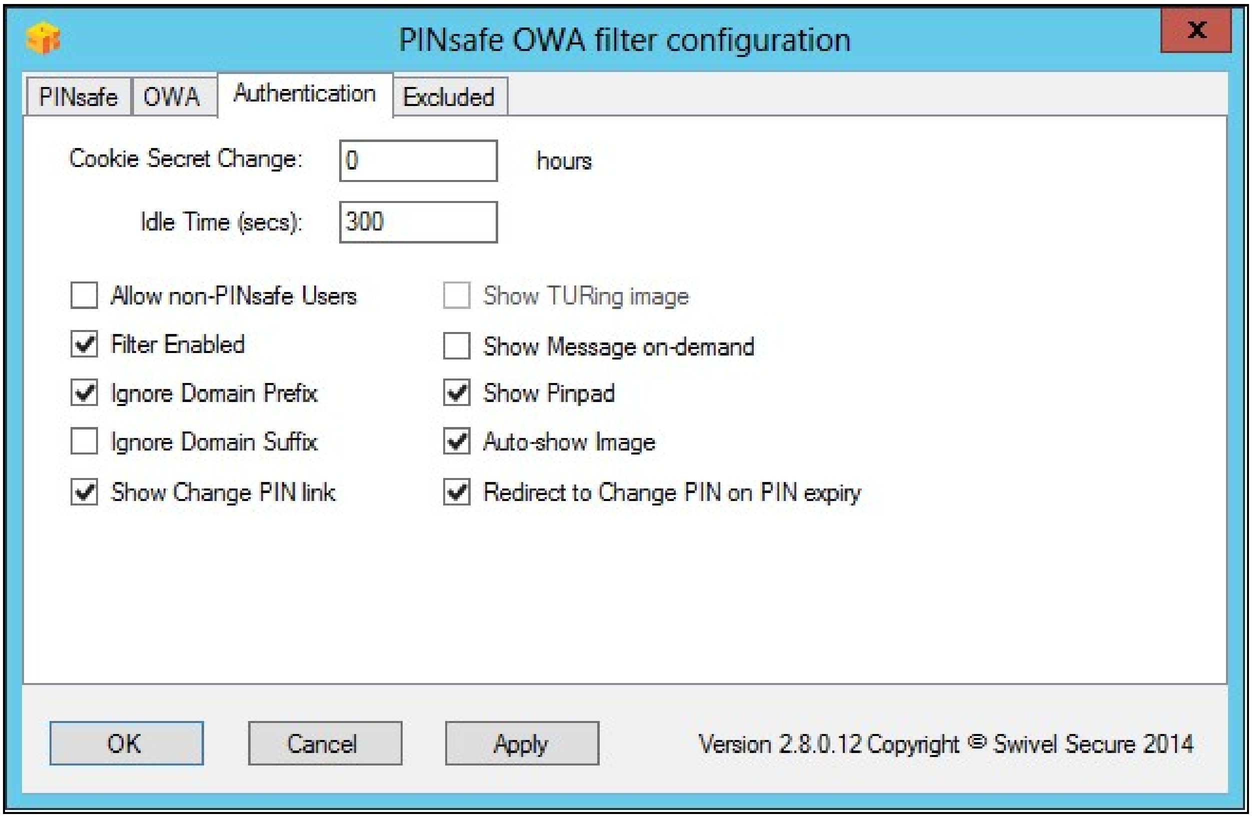
Show Message on-demand If this option is ticked, a button is displayed to request a security string to be sent via SMS or email.

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.



PINsafe OWA filter configuration

Cookie Secret Change: 0 hours

Idle Time (secs): 300

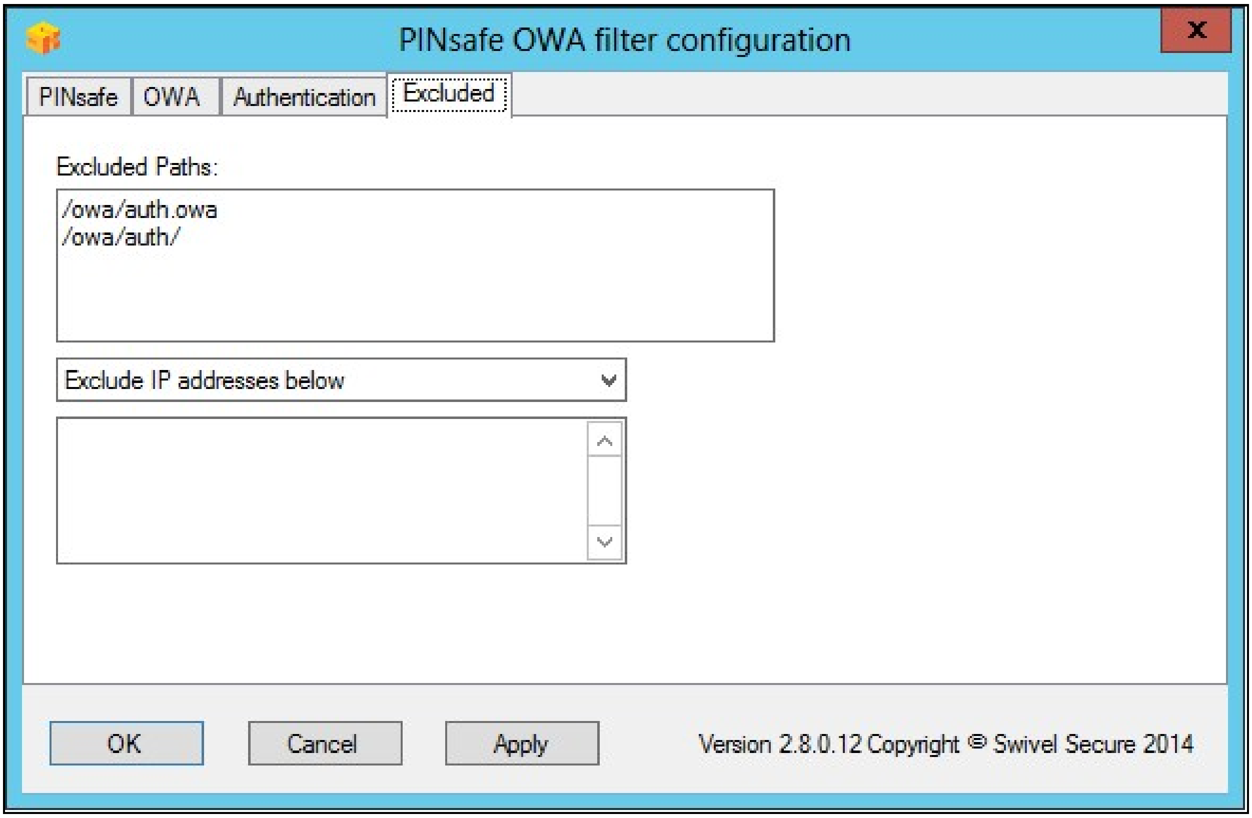
- □ Allow non-PINsafe Users
- ☑ Filter Enabled
- ☑ Ignore Domain Prefix
- □ Ignore Domain Suffix
- ☑ Show Change PIN link
- □ Show TURing image
- □ Show Message on-demand
- ☑ Show Pinpad
- ☑ Auto-show Image
- ☑ Redirect to Change PIN on PIN expiry

Version 2.8.0.12 Copyright © Swivel Secure 2014

35.2.4 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

35.2.4.1 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.

35.3 Configure The Swivel Server

35.3.1 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

35.3.2 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

35.3.3 Configuring Swivel for Dual Channel Authentication

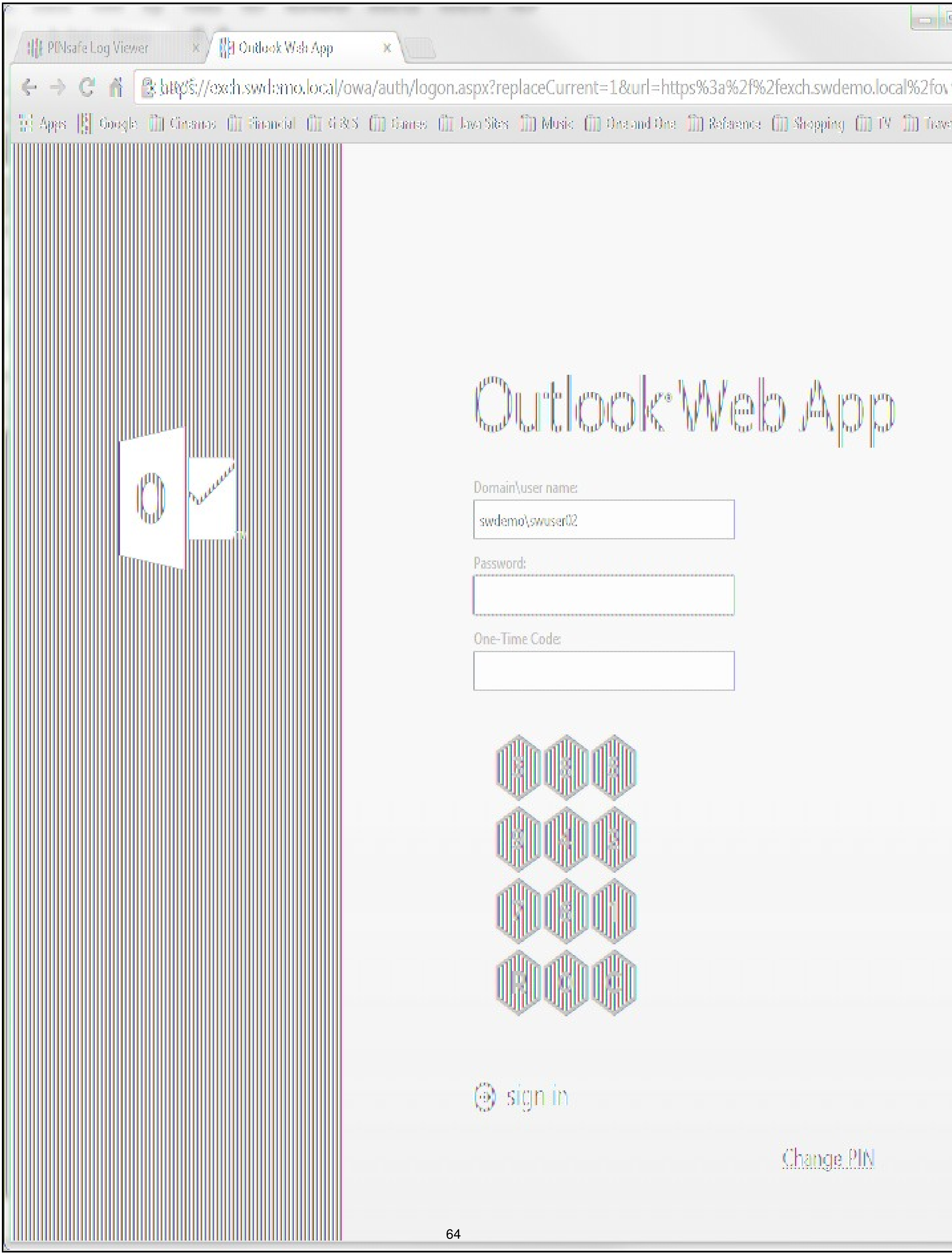
If Swivel Dual Channel authentication methods are to be used, refer to the following guide:

Transport Configuration

36 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:

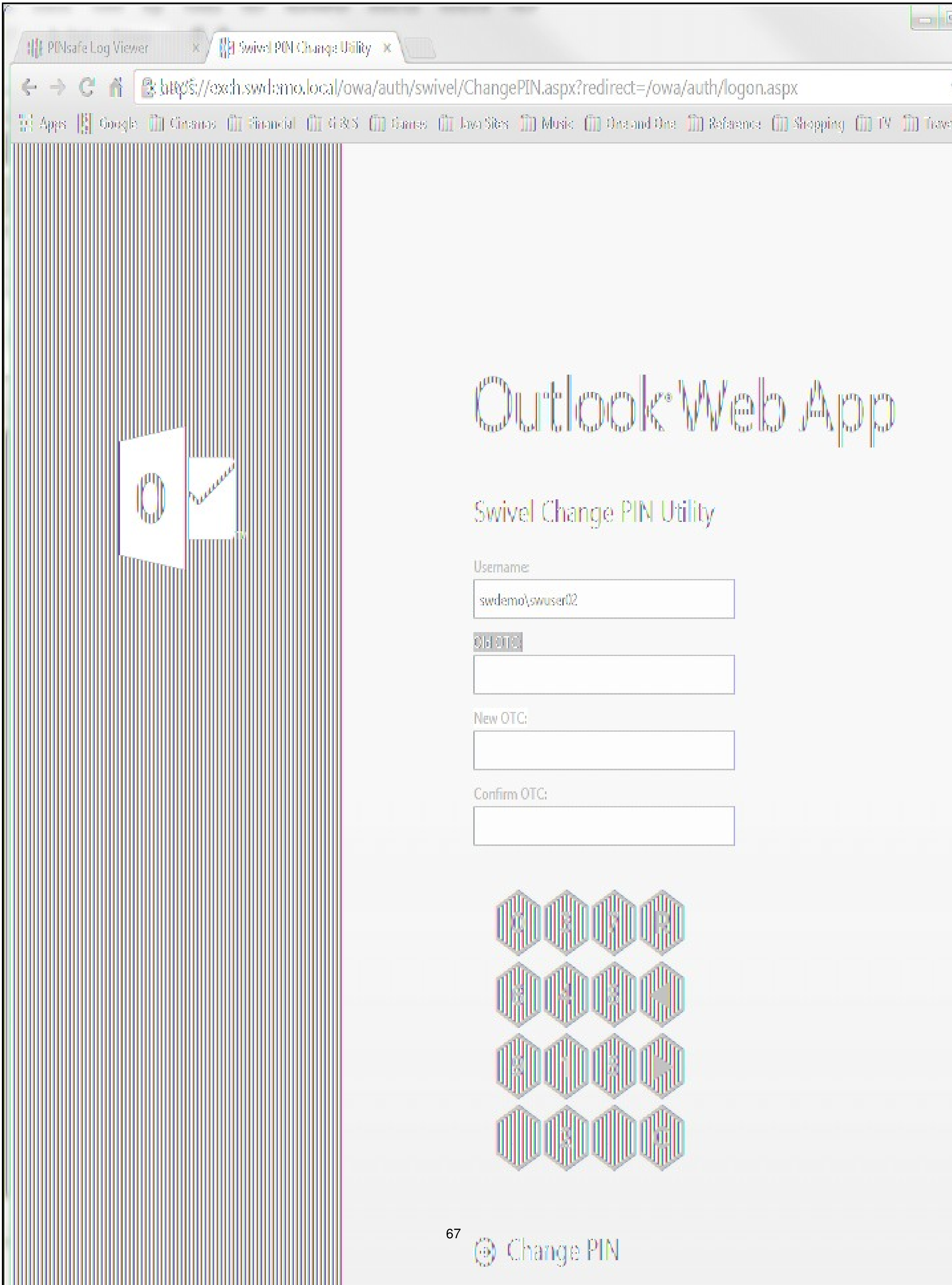
One-Time Code:

37 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.



https://exch.swdemo.local/owa/auth/swivel/ChangePIN.aspx?redirect=/owa/auth/logon.aspx

Outlook® Web App

Swivel Change PIN Utility

Username:
swdemo\swuser02

Old OTC:

New OTC:

Confirm OTC:

38 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.

39 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>

39.1 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" />

39.2 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.

39.3 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.

39.4 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.

39.5 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.

40 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.

40.1 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.

40.2 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.

41 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).

42 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.

43 Microsoft OWA with OMA on Exchange 2003

43.1 OWA and OMA on Exchange 2003 Integration Notes

the following Microsoft knowledge base article might be of interest:

http://support.microsoft.com/kb/817379

43.2 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.