

Microsoft OWA 2013 IIS Integration

Contents

- 1 Introduction
- 2 Compatibility
- 3 Prerequisites
- 4 File Downloads
- 5 Architecture
- 6 Installation
 - ◆ 6.1 Software Installation
 - ◆ 6.2 Configuration of the IIS Filter
 - ◇ 6.2.1 Swivel Settings
 - ◇ 6.2.2 OWA Settings
 - ◇ 6.2.3 Authentication Settings
 - ◇ 6.2.4 Excluded Settings
 - 6.2.4.1 External/Internal User Authentication
 - ◆ 6.3 Configure The Swivel Server
 - ◇ 6.3.1 Configuring Swivel for Agent XML Authentication
 - ◇ 6.3.2 Configuring Swivel for Single Channel Images
 - ◇ 6.3.3 Configuring Swivel for Dual Channel Authentication
- 7 Verifying the Installation
- 8 Change PIN
- 9 Uninstalling the Swivel Integration
- 10 Troubleshooting
 - ◆ 10.1 Enabling debug logging
 - ◆ 10.2 User regularly times out after a short interval
 - ◆ 10.3 Turing image appears but user cannot authenticate
 - ◆ 10.4 User Authenticates Successfully to Swivel but OWA Login Page is Redisplayed
 - ◆ 10.5 Name resolution issue
- 11 Known Issues and Limitations
 - ◆ 11.1 TLS 1.2 Support
 - ◆ 11.2 Themes Support
- 12 Multiple Swivel Servers
- 13 Additional Information

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.

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.

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.

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.

Architecture

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

Installation

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.

Configuration of the IIS Filter

After installation modify the settings. The Filter Configuration should start after installation or can be started through the Start Menu. If the Exchange Server installation is not in the default location, select the OWA directory as above in which to modify the web.config file.

Swivel Settings

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

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

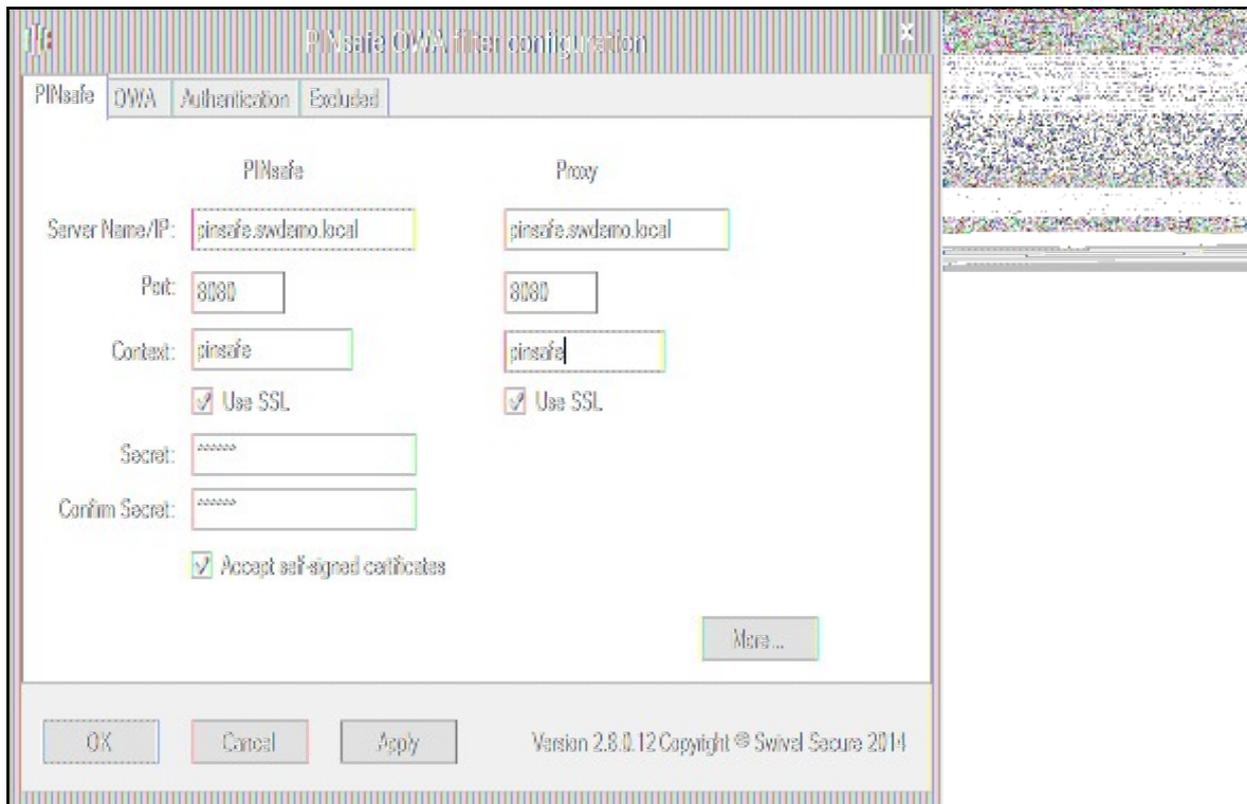
Context: Swivel install name, for a Swivel appliance use Swivel (not proxy)

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.



OWA Settings

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

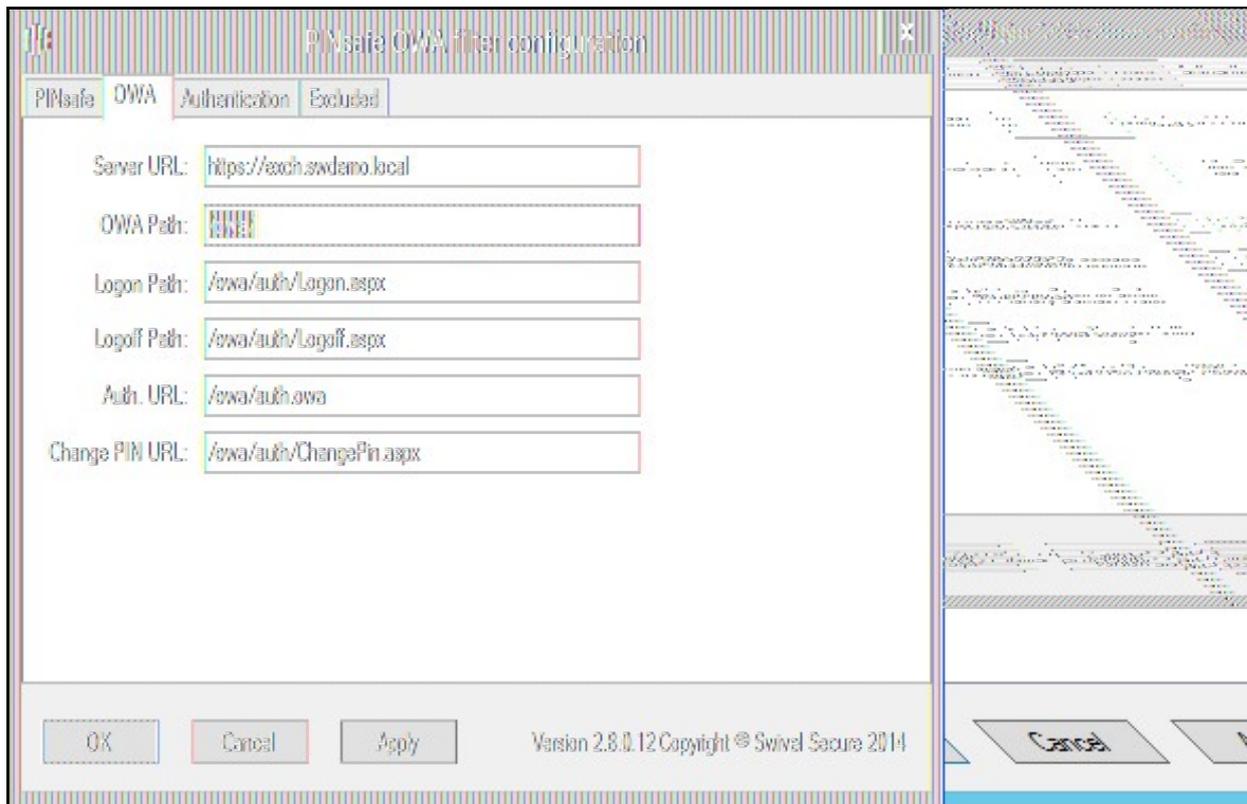
OWA Path: OWA path, usually /owa, unless this has been explicitly changed

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.



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.

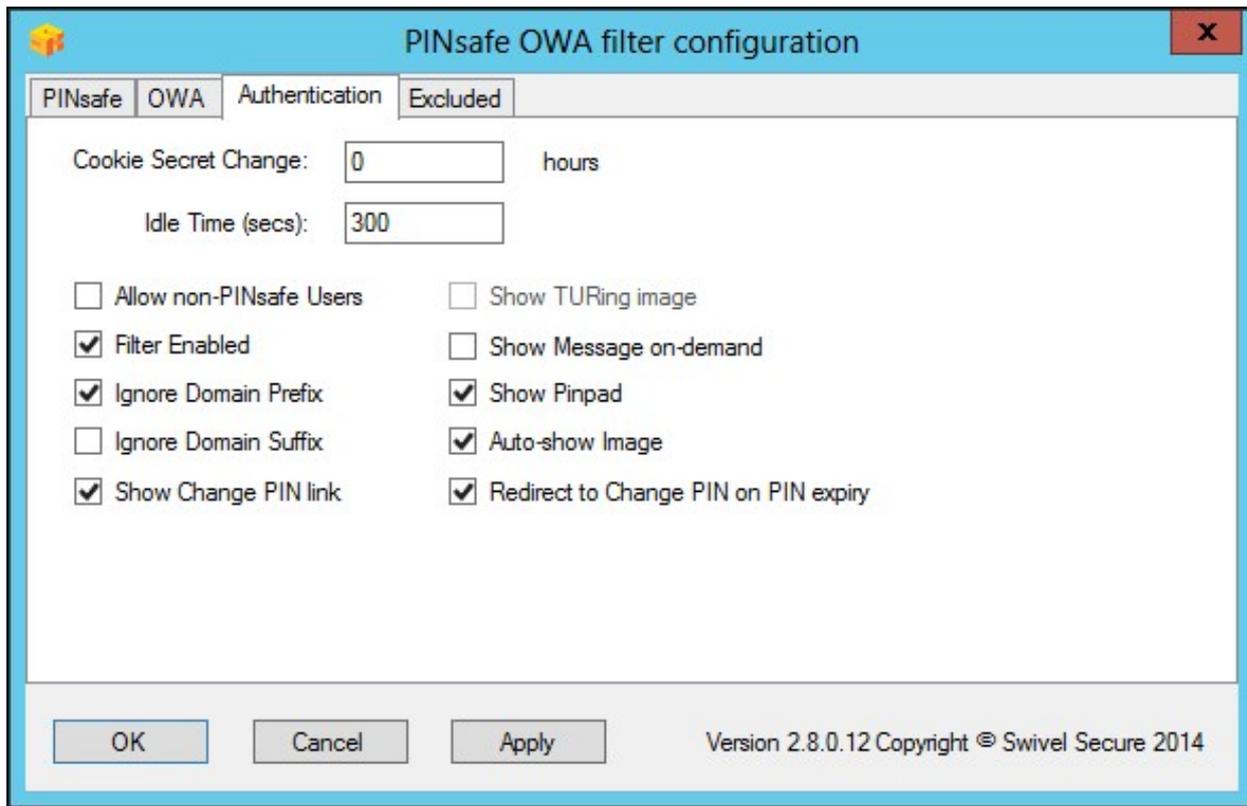
Show Message on-demand If this option is ticked, a button is displayed to request a security string to be sent via SMS or email.

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.

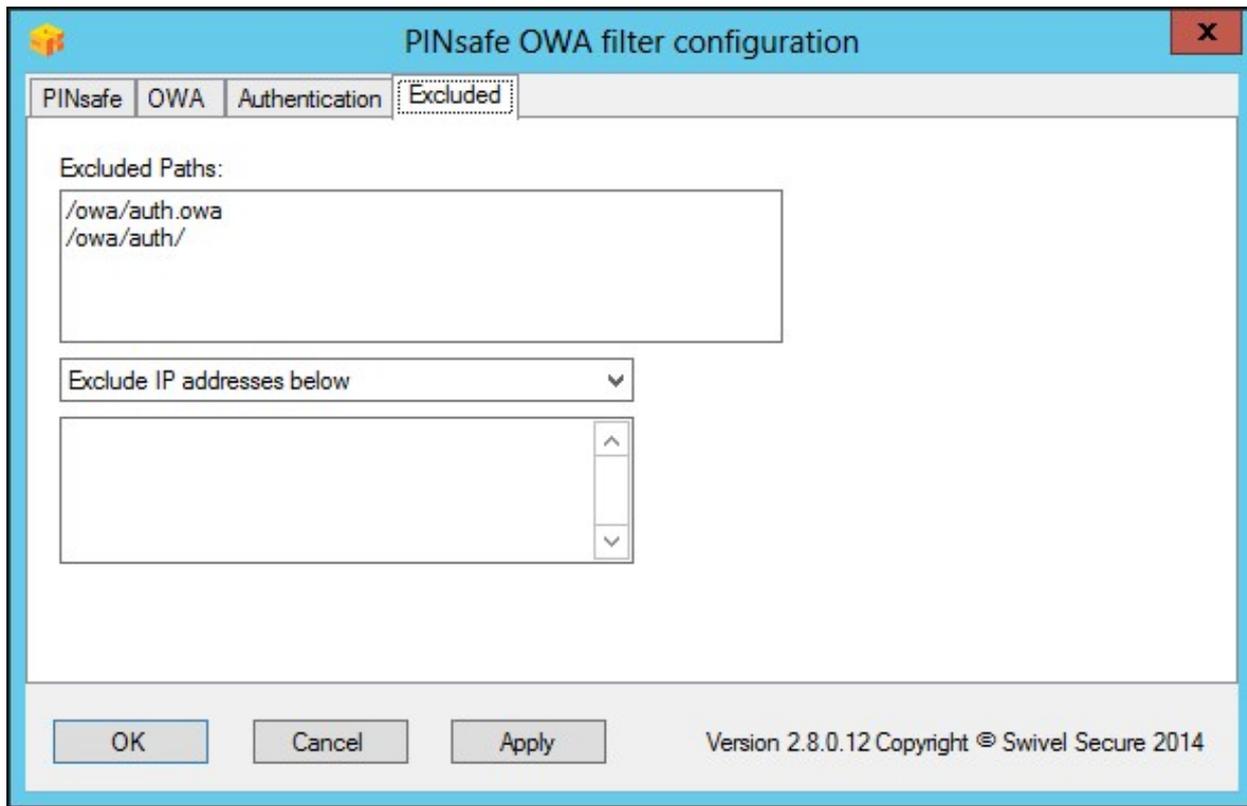
Redirect to Change PIN on PIN expiry If this option is ticked, users are automatically redirected after successful login to the Change PIN page, if their PIN has expired.



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.



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.

Configure The Swivel Server

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](#)

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](#)

Configuring Swivel for Dual Channel Authentication

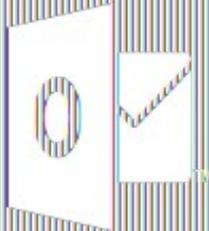
If Swivel Dual Channel authentication methods are to be used, refer to the following guide:

[Transport Configuration](#)

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:

Password:

One-Time Code:



 sign in

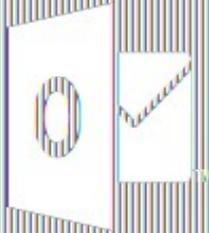
[Change PIN](#)

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.



Outlook® Web App

Swivel Change PIN Utility

Username:

Old OTC:

New OTC:

Confirm OTC:



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\15) under the sub-folder FrontEnd\HttpProxy\owa\auth\. Rename this to restore the original Login.aspx.

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>
```

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\15\FrontEnd\HttpProxy\owa\web.config
```

Locate

```
<add key="PINsafeEnableDebug" value="true" /> <add key="PINsafeDebugLocation" value="C:\Users\Public\Documents\PINsafeOWAFilter.log" />
```

User regularly times out after a short interval

The session is kept open by user activity. If this is insufficient then increase the cookie idle timeout value.

Turing image appears but user cannot authenticate

Verify that the OWA is configured to use port 8080 and context pinsafe. Port 8443 and context proxy will cause problems with authenticating users but allow the Turing image to be displayed. Note that this refers to the main PINsafe settings (for version 2.6 or higher) - the proxy settings SHOULD have these values if required.

User Authenticates Successfully to Swivel but OWA Login Page is Redisplayed

If you have entered the correct credentials, and the Swivel logs show successful authentication, but you are still redirected to the login page, the problem might be related to host names and/or SSL certificates.

First of all, if you connect to OWA using the IP address, or "localhost" from the OWA server itself, the Swivel filter will redirect you to the host name configured in the filter. This may result in the authentication cookie being lost, because the domain name doesn't match. In this case, attempting to authenticate a second time, with the correct host name, should succeed.

The second possibility is that the SSL certificate on the OWA Server doesn't match the host name used by the OWA filter, or the certificate has expired or is not trusted. This will result in authentication to OWA, from the Swivel filter, failing.

The solution for a production server is to ensure that the Exchange Server has a commercial SSL certificate, and that the Swivel OWA filter uses the host name that matches this.

For a development environment, you can generate a self-signed certificate with the correct host name, and add this to the list of trusted certificates on both the OWA server itself and the client (the latter might not be necessary). You might also need to add the host name to the hosts file on one or both of these.

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.

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.

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.

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.

Multiple Swivel Servers

Versions 2.5 and later include the option to add multiple Swivel servers. Then, if the first one is unavailable, the filter will try the other servers in the order listed. The filter will always remember the last Swivel server successfully contacted and try that one first.

To support multiple servers, there is an additional button on the Swivel tab of the configuration program, which brings up a secondary dialogue containing a list of available servers. Use this to add or delete Swivel servers, and to select one to modify (the details are modified on the main dialogue).

Additional Information

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