Microsoft ISA 2006 Integration

Contents

Microsoft Internet Security and Acceleration Server (ISA) Integration Notes

Introduction

This document outlines the necessary steps to integrate Swivel authentication into either Outlook Web Access (OWA) 2003 or Sharepoint Forms-based Authentication (FBA) provided with Microsoft ISA Server 2006. Additionally the login page can be further customised, for further information see: Microsoft ISA 2006 web page customisation How to Guide. If the ISA server is part of a cluster then the filter needs to be installed on each cluster, the 32 bit installer handles cluster registration, for further information and manual registration see Microsoft ISA 2006 Cluster Integration

Note that with the release of version 1.2 of the Swivel ISA filter, filter registration is part of the configuration process. See below for more information. This also means that the same installer can be used for Enterprise and Standard ISA Server. Unfortunately, version 1.2 supports 32-bit operating systems only. However, there is a 64-bit version for Microsoft Forefront Threat Management Gateway. The documentation for this is now available from a separate page here.

Prerequisites

This installation guide assumes that publication of the relevant service has already been configured in ISA Server, following the relevant instructions. In addition a working Swivel server version 3.1 or later is required.

If the option to check a user is a Swivel user and issue a OTC field is to be used, this requires Swivel 3.4 or later.

The Swivel Configuration utility requires .Net version 2 or higher. This is not supplied above and must be downloaded and installed if you do not already have it.

The ISA server and its configuration should be fully backed up prior to the Swivel integration.

Allow around 1 hour downtime per ISA server for the integration, and the integration will require a restart of the ISA Firewall Services.

ISA 2006 Filter

The installer can be downloaded from here.

TMG Filter

The TMG version can be found here. NOTE: this is version 1.4.0 of the TMG filter, released 23/8/12, which includes a number of enhancements over previous versions. See the included documentation.

Baseline

Swivel 3.4 or later (3.6 or later preferred)

Microsoft ISA Server 2006 or Microsoft Forefront TMG

Web-based server, typically Microsoft IIS-based, to be protected, such as OWA or SharePoint.

Architecture

The ISA server makes authentication requests against the Swivel server by XML or RADIUS. Some of the additional features are only available in the XML authentication. For security reasons Sharepoint authentication should be configured using RADIUS. The Swivel installation creates a separate custom login.

The default install path for the standard OWA login page is:

C:\Program Files\Microsoft ISA Server\CookieAuthTemplates\Exchange\HTML

The standard install path for PINsafe OWA authentication page is:

C:\Program Files\Microsoft ISA Server\CookieAuthTemplates\PINsafeOWA\HTML

Swivel Configuration

Configure a Swivel Agent For XML Authentication

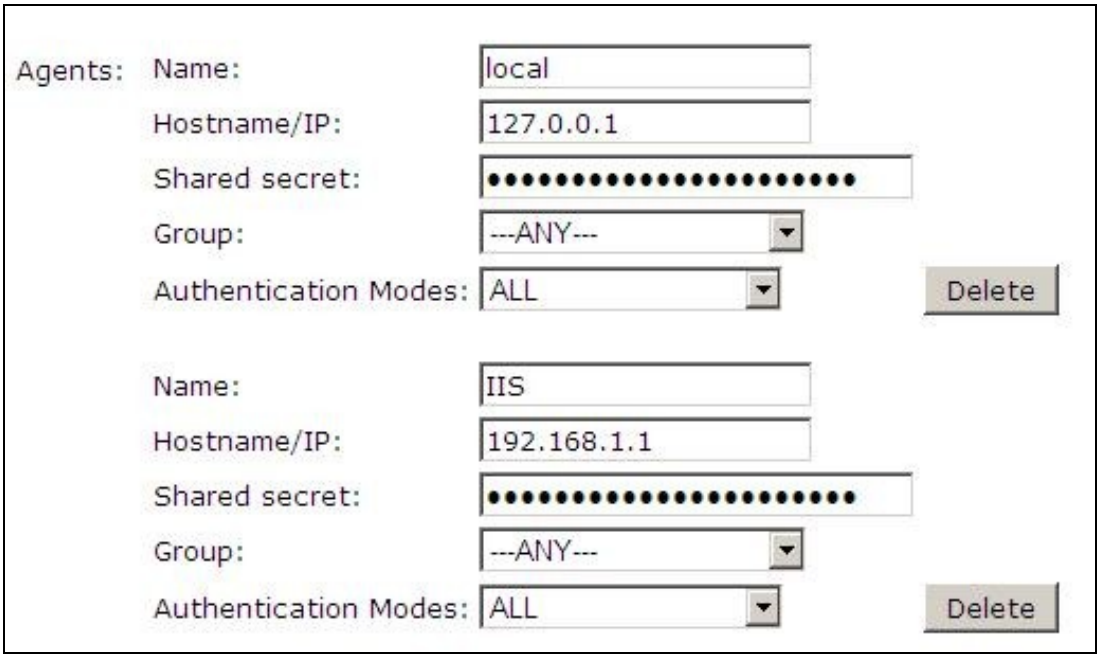
1. On the Swivel Management Console select Server/Agent

2. Enter a name for the Agent

3. Enter the ISA internal IP address

4. Enter the shared secret

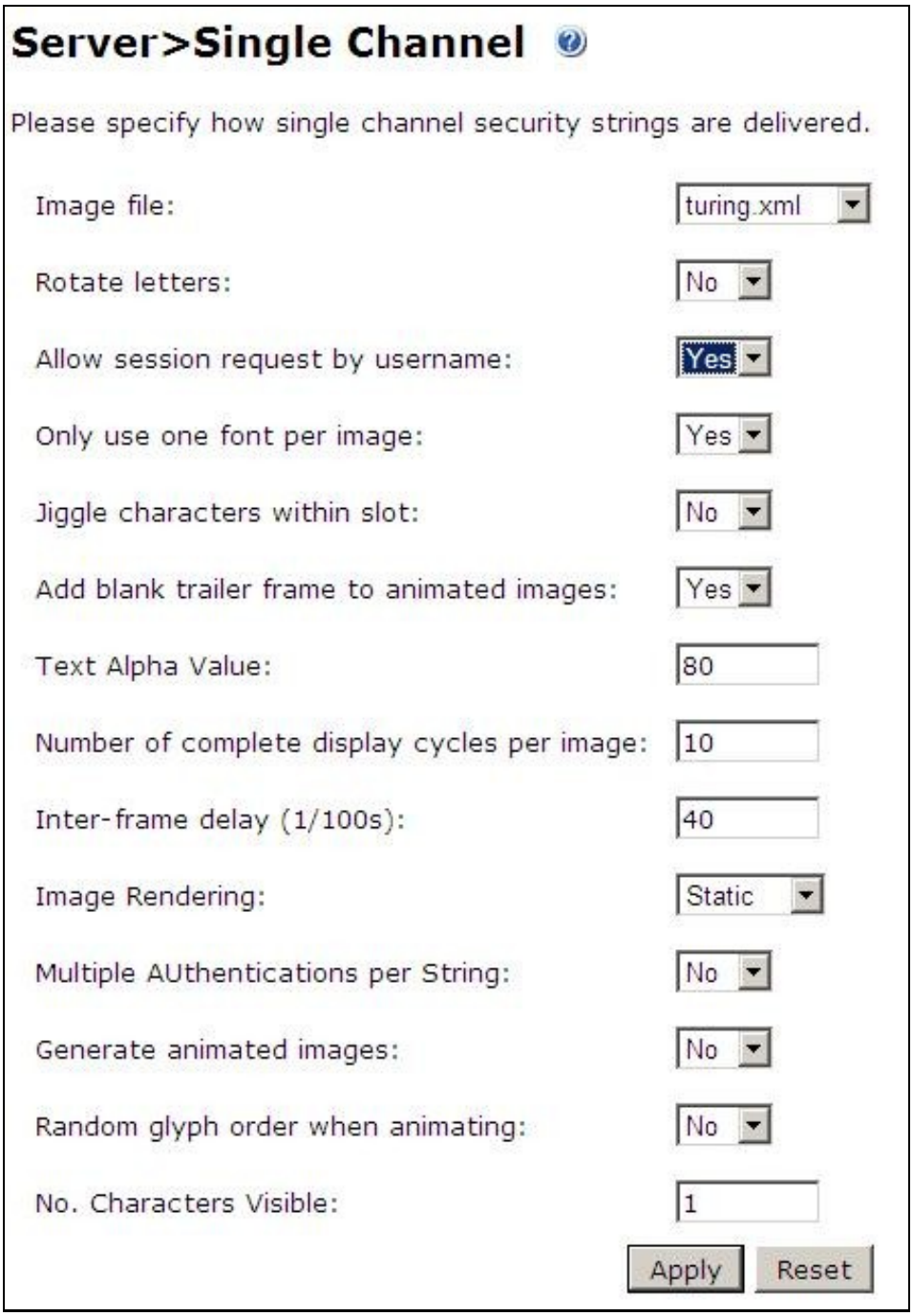
5. Click on Apply to save changes



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



Configure a RADIUS NAS entry for Sharepoint authentication

NOTE: this is only required if you wish to use RADIUS authentication with Swivel. This is recommended for SharePoint integration and optional for other solutions.

1. Ensure the RADIUS server is running on Swivel
2. On the Swivel Management Console select RADIUS NAS
3. Enter a name for the NAS
4. Enter the ISA internal IP address
5. Enter the shared secret
6. Click on Apply to save changes

ISA Installation

The following steps should be carried out on the ISA server. No configuration changes need to be performed on the Exchange server or Sharepoint server. For Additional Sharepoint configuration see the Special Considerations for Sharepoint below.

Publish OWA or Sharepoint

Publish Outlook Web Access, Sharepoint or your website as described in the ISA Server documentation, if you have not already done so. Ensure that they are working as expected.

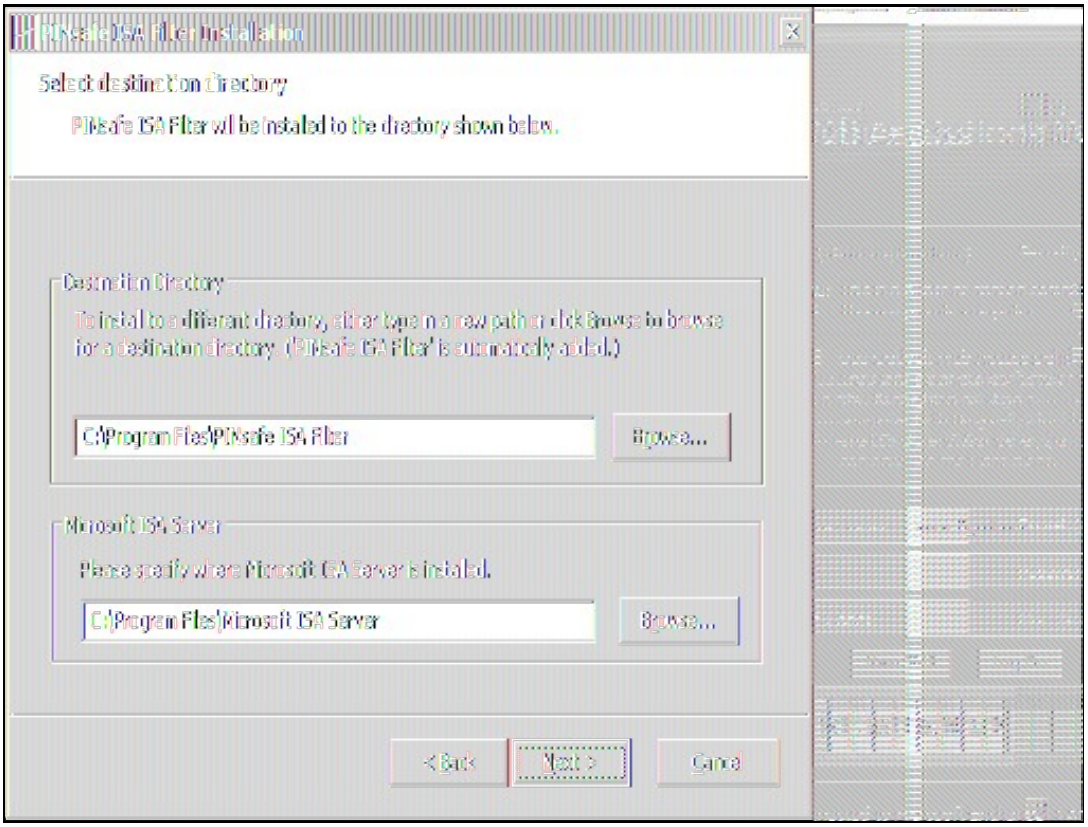
Configure ISA firewall rules

Create an access rule permitting HTTP access from the ISA Server to the correct port (commonly 8080) on the Swivel server. To do this, you will need to create a new protocol for outbound TCP on the appropriate port.

Install the ISA server software

NOTE: if you are installing in an Enterprise environment, you should always install on the Configuration Storage server first, and then on each array member. Be aware that the firewall service on member servers will stop when they try to synchronise with the configuration storage server, if that has the Swivel filter installed and the member does not. Once the filter is installed on the member server, you will be able to restart the firewall service.

Run PINsafeISAFilter.exe to install the filter DLL. You will be prompted for the location in which to install the filter configuration, and also for the location of Microsoft ISA Server, usually C:\Program Files\Microsoft ISA Server.



Note that the installation process will include installation of Microsoft Visual C++ 2010 runtime libraries, if they are not already installed.

Register the ISA Filter

When installation is complete, you have the option to run the configuration program. Assuming you elect to do so, you will first be prompted to register the filter with Swivel. You have a choice of registration types:

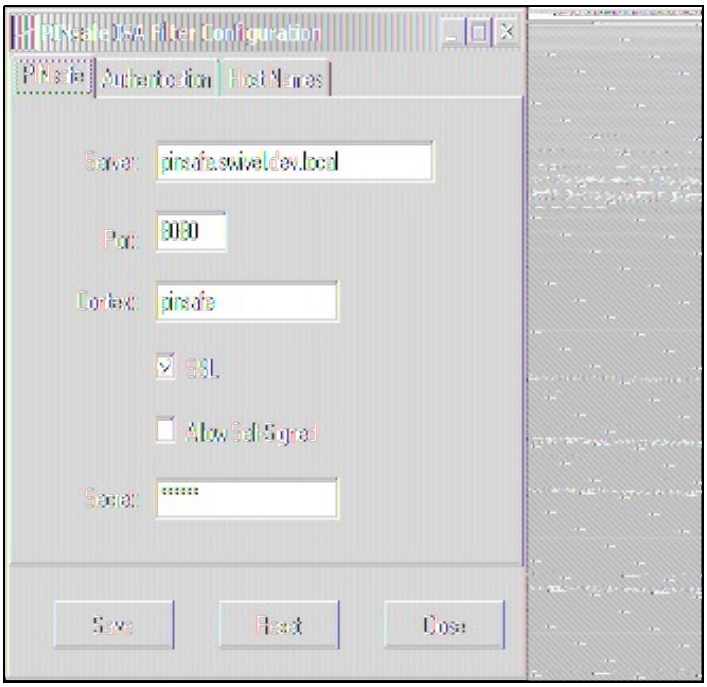
[[Image: Register_Filter.PNG]]

Select the right option for your requirements. The last option is required if you are installing on the Configuration Storage server and the same server is also a member of the ISA server array.

Configure the ISA server

Configure the ISA filter using the configuration tool provided. This will optionally run immediately after installation. To start subsequently, select Start/Programs/PINsafe ISA Filter/Configuration.

PINsafe configuration tab:



Server: is the name or IP address of the Swivel server (Hint: Use hostname to avoid problems with SSL certificates)

Port: is the port on which Tomcat is running. PINsafe virtual or hardware appliances require the use of XML authentication on port 8080 and the 8443 proxy port should not be used when integrating with ISA. (Hint: Use port 8080)

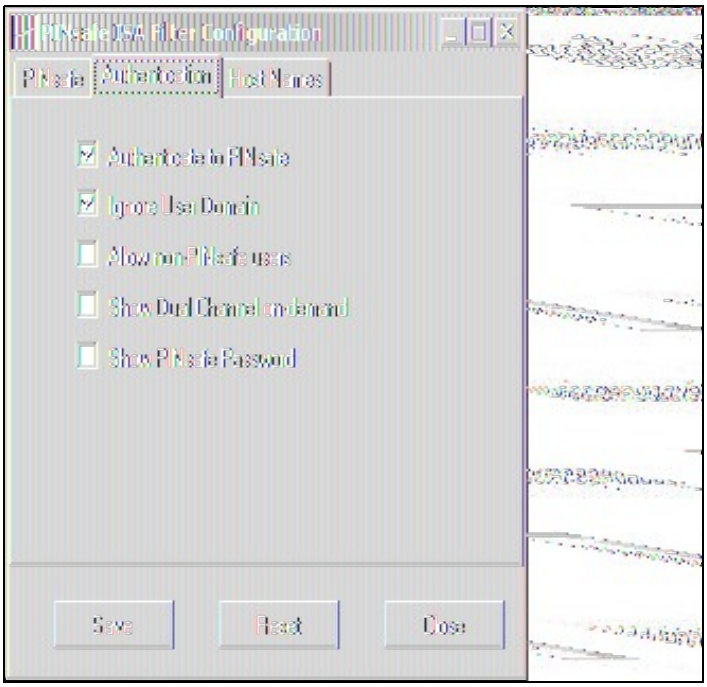
Context: is the name of the Swivel web application, usually ?pinsafe?. Note when using a Swivel virtual or hardware appliance where the proxy port is available, the path pinsafe using port 8080 should still be used, the ISA proxy provides security.

SSL: will, if checked, send requests to the Swivel server using https, rather than http.

Allow self-signed: when checked, causes SSL certificate errors from the PINsafe server to be ignored.

Secret: is the shared secret for the Swivel agent for the ISA Server, and needs to be the same as that on the Swivel server. After you enter this value, you will be prompted to enter it again, to confirm that it is correct.

Authentication configuration tab:



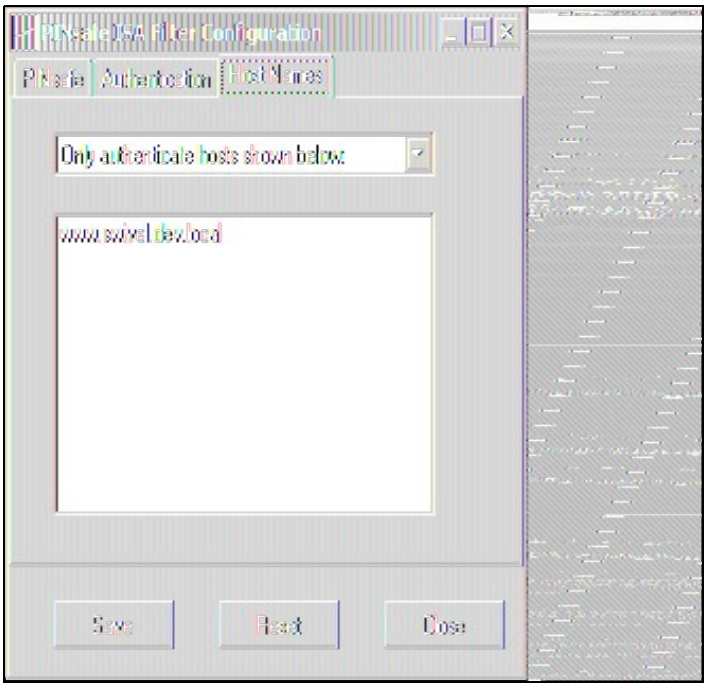
Authenticate to PINsafe: should be checked to use standard Swivel authentication. You should uncheck this if you are using the ISA filter to protect a Sharepoint website, as described in the ?Special Considerations for Sharepoint? section below. If you uncheck it, Swivel will not directly authenticate the login request. In this case, you should enable RADIUS authentication instead.

Ignore user domain: This will remove the AD domain of users, and when Swivel is using the SAM account name it should normally be checked, in this case, if you enter ?domain\user? as the logon username, only ?user? will be sent to Swivel. If it is not checked the full name will be sent to Active Directory and should be used when Swivel uses the User Principle Name.

Allow non-PINsafe users: when checked, users not known to Swivel may authenticate using only their AD credentials. This feature is useful for transition to Swivel, where not all users have Swivel accounts. If checked, the OTC field is not shown initially, only when the username is checked and found to exist in Swivel. Note that this feature is not compatible with RADIUS authentication.

The last two options on this tab should not be used - they do not work, and are there for future enhancement.

Hosts configuration tab:



This feature is new to version 1.2. Previously, when installed, the PINsafe ISA filter would affect all authentication requests through the ISA Server. This option allows you to apply PINsafe authentication per host name. It can either be configured to authenticate all host names except those specified, or to authenticate only those hosts specified, and to ignore all others.

Confirm that the filter has been registered correctly

Once completed the filter will appear in the ISA Server Management Web Filters section. If the filter does not appear in the list of available filters check the Windows system event log for errors. The 32 bit installer handles cluster registration, for further information and manual registration see Microsoft_ISA_2006_Cluster_Integration

Modify the Listener

Modify the Listener used to publish OWA or Sharepoint as follows: On the relevant firewall rule, right-click and select properties, select Listener, then click Properties. On the Forms tab, tick the check box labelled ?Use customized HTML forms instead of the default?. For the form set directory, type:

?PINsafeOWA? for Outlook Web Access

and ?PINsafeWeb? or ?PINsafeRadius? for Sharepoint or other websites (?PINsafeISA? for TMG).

You should always use PINsafeRadius for Sharepoint, for reasons described below. You may use either set of forms for standard websites. Note that the TMG filter does not require a different set of custom pages for RADIUS.

Modify the properties for the relevant policy rule.

Then select Apply, and click Ok. Then select the Application Settings tab and UNCHECK the option to use customized HTML. Note that if you have customized your original OWA or Sharepoint login pages, you will need to apply the same customisation to the new Swivel pages. Please consult Swivel support for details of this.

Once you have configured everything, restart the Microsoft Firewall Service on the ISA server. It can take a long time to restart this service, and if you are connecting to the ISA Server via remote desktop, you may be temporarily disconnected from it.

SSL Certificate Considerations

There would appear to be an issue with a recent security update for ISA Server which prevents HTTP POST requests over SSL unless the target server certificate is fully trusted. This has consequences for the PINsafe ISA Server integration.

If you are not using SSL on your Swivel server, this issue will not affect you.

If you are using SSL, you must have a valid certificate on the Swivel server. This means:

- The certificate date must be current (i.e. not expired)
- The certificate must be issued by a trusted CA (see below for ways of managing this)
- The certificate subject must match the host name used by the ISA Server to connect to the Swivel server. In particular, this means that you must reference the Swivel server by name, not by IP address.

One way to manage this is to get a commercial certificate for the Swivel server. However, this costs money, and if your PINsafe server is not internet facing, is not necessary. A second option is if you have an internal certificate authority, you can use that to issue a certificate for the Swivel server (Windows Servers, for example, can optionally be configured as certificate authorities). If you do this, you need to make sure that the certificate authority server certificate is added to the trusted root certificates on the ISA Server, if it is not already. The third option is simply to generate a self-signed certificate on the Swivel server, with the correct host name, and to install that directly into the ISA Server trusted root store (see below).

For more detail, refer to the relevant knowledgebase documentation on generating SSL certificates if you are using a Swivel virtual or hardware appliance. Otherwise, refer to the relevant documentation for your operating system.

Installing a Self Signed Certificate into the ISA trusted root store

If you want to do is to trust the Swivel server certificate the following steps may be carried out:

1. Copy /home/swivel/.keystore to a suitable machine (it doesn?t have to be the ISA server).

2. Open the file in Keystore Explorer.

3. Right-click on the certificate (if there is more than one, it will probably be called ?swivel?). Select ?Export?, then ?Export key pair?.

4. Enter a password for the exported certificate. I recommend using ?lockbox?, but anything will do.

5. Select the export path. It doesn?t actually matter what the extension is.

6. Copy the exported certificate to the ISA Server. The remaining commands are done on the ISA Server.

7. Open ?mmc? from the Run dialog.

8. Select File -> Add/Remove Snap-in.

9. From the dialog, select ?Certificates? and click ?Add?.

10. Select ?Computer account?, then ?Local computer?.

11. Click OK.

12. Go to Certificates -> -> Trusted Root Certificate Authorities.

13. Right-click, then ?All Tasks?, ?Import?.

14. Select the exported certificate. You will need to enter the password. We recommend marking the key as exportable. Make sure the certificate is imported into the -> Trusted Root Certificate Authorities.

15. If you look under Certificates -> Personal -> Certificates, you should see the new certificate.

16. You may need to restart the Microsoft Firewall service before it shows the new certificate.

Special Considerations for Sharepoint

A security hole has been discovered when using earlier versions of the ISA filter for Sharepoint authentication. It was possible to open a Sharepoint document from within Word (for example) and only provide the standard Active Directory credentials.

The new solution avoids this problem by using RADIUS to authenticate to Swivel, rather than using the ISA filter directly. One minor inconvenience with this is that users must authenticate through the Sharepoint web page before they can access any documents.

Note that if you disable Swivel authentication for Sharepoint, it is also disabled for all other websites. Therefore, if you want to use Swivel authentication on multiple websites for a single ISA Server, they must all use the standard Swivel authentication, or all use RADIUS.

1. On the ISA filter configuration application, uncheck the Authenticate option. This means that Swivel will not authenticate the logon request directly. Instead, you should use RADIUS to perform Swivel authentication, as described below.

2. On the Authentication tab you should check the option ?Collect additional credentials in the form?. This will require you to select ?RADIUS OTP? as the authentication validation method. Click the ?Configure Validation Servers? button, and add the Swivel server as a RADIUS server. Make a note of the shared secret you set for the server.

3. In order for users to be able to open documents from other, non-browser applications once they have authenticated, you must enable persistent cookies. On the Forms tab, click the Advanced button. It is recommended that you select persistent cookies for private computers only. This means that users on public computers will have to open documents from the Sharepoint web site.

4. On the ISA server, create a rule to allow RADIUS authentication from the ISA server to the Swivel server

5. On the Swivel server, enable the RADIUS server (on the RADIUS > Server page). On the RADIUS > NAS page, add the ISA Server as a new NAS, and enter the shared secret you set on the ISA Server. If you wish to restrict access to a particular group of users, select that group, otherwise leave the Group drop-down as ?ANY?.

6. On the policy rule, on the Authentication Delegation tab, select ?NTLM Authentication?.

Once you have configured everything, reboot the ISA server.

Verifying Installation

Outlook Web Access

Navigate to the URL on which ISA Server publishes OWA. The customisation is visible in the addition of a One Time Code field and a Start Session button. Attempting to login with a correct username and password but no one time code should result in failure. Only when a correct Swivel one time code is entered in addition to the Exchange or Sharepoint credentials should the user be logged into OWA.

Note that if a username is entered in the form Domain\username, the Domain\ portion of the username will be stripped before being passed to the Swivel server. This permits the use of sAMAccountName as the username attribute for synchronisation between Swivel and Active Directory.

Dual Channel Login

Single Channel Login

Sharepoint

Navigate to the URL on which ISA Server publishes Sharepoint. You will notice that there are two sets of credentials to enter. The Swivel credentials are entered in the top part, and the Active Directory credentials in the lower part. Enter the username in the first box as domain\user. Click the Start Session button to get a TURing image. Enter the Swivel password and one-time code in the next two boxes. (NOTE: the Swivel password and one-time code are actually concatenated and submitted as a single value. You can, if you prefer, enter them that way in the Passcode field ? password first).

In the final box, enter your Active Directory password, and click submit.

(NOTE: you actually have to enter different usernames for Swivel and Active Directory ? with the domain prefix for AD and without for Swivel. However, this is handled automatically for you. You will notice, if you fail login, that the Swivel username has changed, and the AD username has been inserted in the lower set of credentials.)

Additional Options

RADIUS Authentication

Set the Swivel server as the RADIUS server (and add the ISA Server as a NAS on Swivel). If you want to use the TURing image, then the Swivel ISA filter is required, but disable authentication in the filter configuration. PINsafeRADIUS custom login pages provided with the filter can be used.

Turning off Automated Security Strings

When a user enters their username and then their AD password, they will usually generate a single channel TURing image or for Dual channel On Demand authentication, automatically send an SMS message. This option is for the the integration using the OWA filter and will stop the automated display of single channel TURing images and the automated sending of SMS security strings.

The automation can be disabled by disabled by editing C:\Program Files\Microsoft ISA Server\CookieAuthTemplates\PINsafe\OWA\HTML\usr_pwd.htm (Exact path may vary depending upon installation).

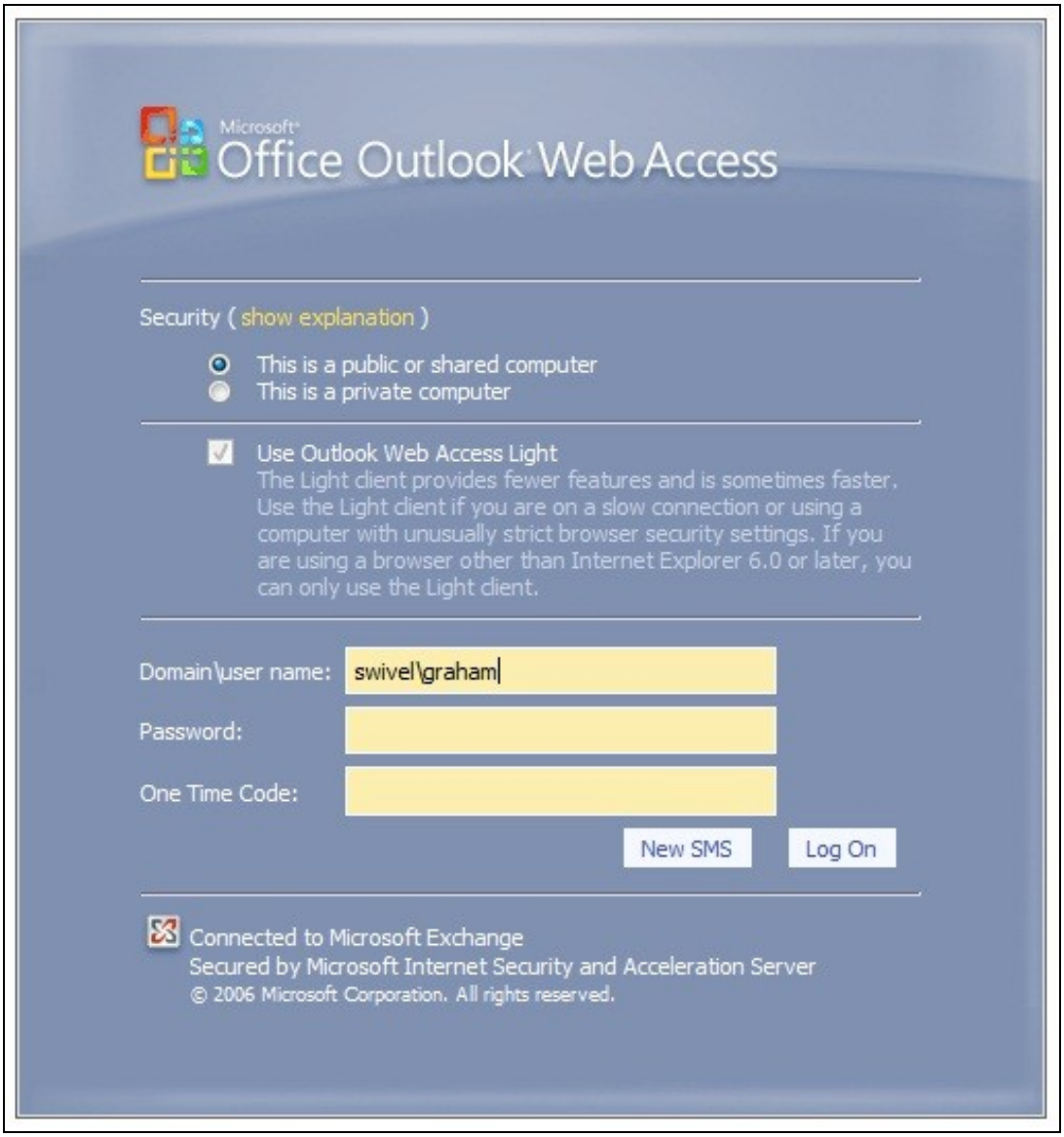
First Make a backup copy of the file

Edit the file in a text editor

Locate the setUserExists function

below this locate and remove the entire line ShowTuring();

Modified login page showing SMS on request



Editing the Security String Request Buttons

The message request buttons can be edited to display different messages.

The default International English language version is located in the the following file:

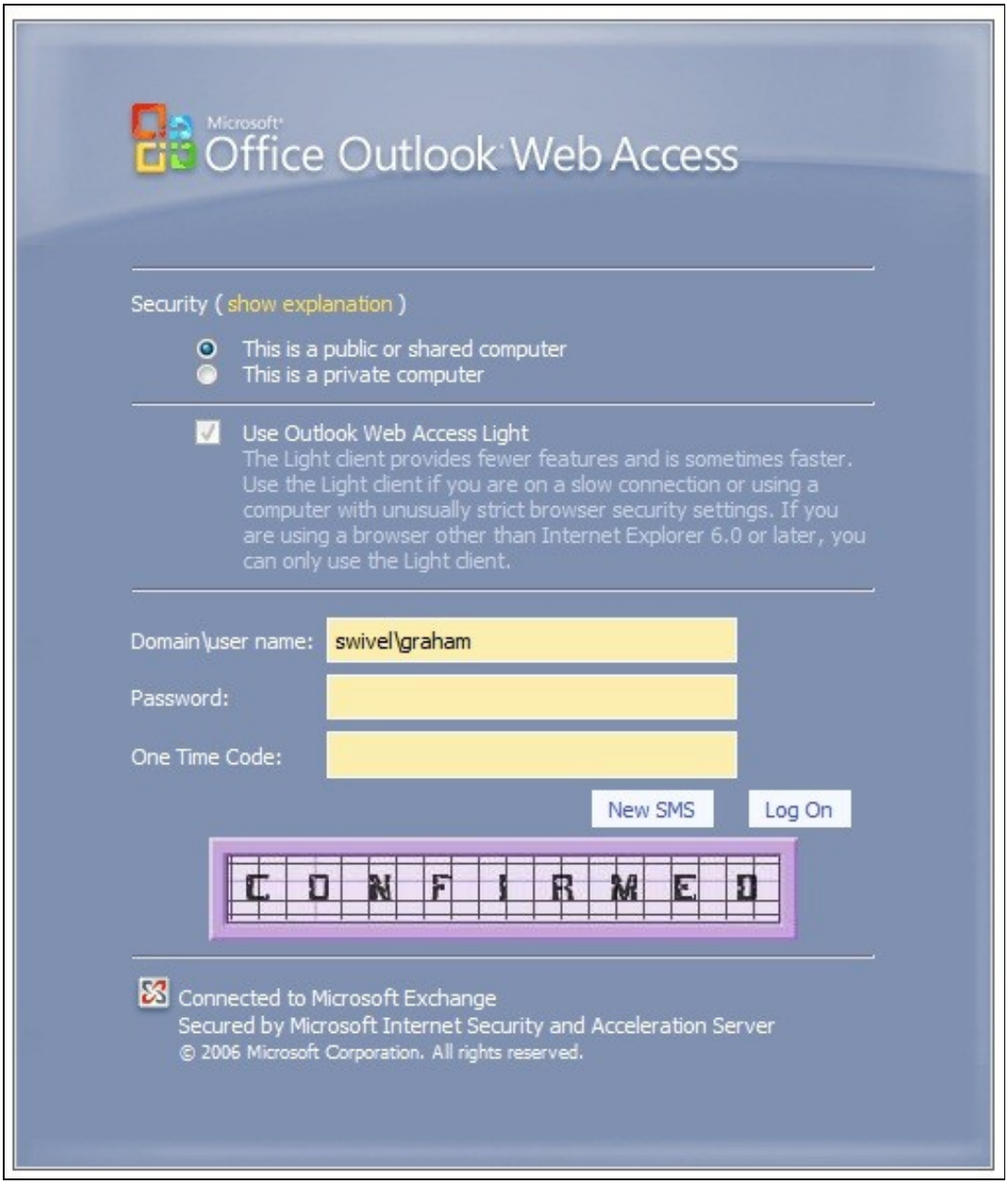
C:\Program Files\Microsoft ISA Server\CookieAuthTemplates\PINsafeOWA\HTML\nls\en\strings.txt (Path may vary with installation, and different language files may also be edited)

First Make a backup copy of the file

Edit the file in a text editor

Find the line L_StartSession_Text="Get Image" (May also be L_StartSession_Text="Start Session" or L_StartSession_Text="Refresh Image")

Modified login page



Uninstalling

Modify the Listener

Modify the Listener used to remove OWA or Sharepoint as follows: On the relevant firewall rule, right-click and select properties, select Listener, then click Properties. On the Forms tab, remove the tick the check box labelled ?Use customized HTML forms instead of the default?. For the form set directory, remove:

?PINsafeOWA? for Outlook Web Access

Modify the properties for the relevant policy rule.

Then select Apply, and click Ok. Then select the Application Settings tab and CHECK the option to use customized HTML.

Uninstall the Swivel software using the Remove Programs.

reboot the ISA server

Known Issues

Troubleshooting

NOTE: After any changes are made, always restart the Microsoft Firewall service

The Swivel authentication filter logs its activity to the standard Windows debug log. This can be accessed using a tool such Sysinternals DebugView available as freeware from:

Sysinternals DebugView

To include logging of output from the filter the option Capture Global Win32 must be enabled in the Capture menu.

With regard to the Single Channel TURing image, the ISA server login page does not use SCImage, the image request comes through the filter, so that the the Swivel server noes not need to be accessed directly from the internet. If the filter is not working, then no image will appear.

Single Channel image does not appear:

- Check Swivel ISA filter settings
- Check the Firewall service is started
- Check the ISA server logs for any error messages
- Use a fully qualified hostname instead of IP address for the Swivel server
- Is an SSL connection being used
- Is a self signed cert being used, if so try without SSL using http or install a valid public certificate
- Check the Swivel ISA filter is correctly installed. On the ISA Server Management: under Configuration, Add-ins for the server, "PINsafe Authentication Filter" should be enabled
- From the ISA server check a Single Channel image can be generated in a web browser connecting to the Swivel server using:

Swivel virtual or hardware appliance

https://<PINsafe server IP>:8080/pinsafe/SCImage?username=test

For a software only install see Software Only Installation

- If you see a red cross where the Single Channel Image should be right click on it and select properties. Copy the Address (URL) which should look something like: https://<ISA URL>/PINsafeISAFilter.dll?username=graham&random=197405. Copy this line and paste into the URL bar of the web browser and see if a Single Channel Image is generated.

If a user is able to login without the One Time Code, then the ISA filter may not be installed.

If IP addresses, rather than host names is used, with SSL enabled, you must check the option to "permit self-signed certificates". This option actually means to ignore all certificate errors, as you will get when referencing a server by the IP address, rather than the name.

The following error can be seen when trying to install the Swivel ISA Filter on an ISA cluster:

```
Error 1904. Module C:\Program Files\Microsoft ISA Server\PINsafeISAFIlter.dll failed to register. HRESULT -2147024891. Contact your support
For more information, see Help and Support Center at http://go.microsoft.com/fwlink/events.asp.
The "PINSafe Authentication Filter" then does not appear in the Web Filters tab.
```

See Microsoft ISA 2006 Cluster Integration

The ISA 2006 filter will not work with ISA 2004.

See also: troubleshooting OWA 2007 publishing rules on ISA Server 2006

Additional Information

Note on Activesync and RADIUS authentication

If you are using the same listener for ActiveSync etc, then don't use the RADIUS (or RADIUS OTP) option, as this will affect authentication for the other types as well. Since using the AgentXML approach only affects forms authentication, it shouldn't affect ActiveSync, which doesn't use FBA.

ISA and OWA

Information regarding the configuration of ISA Server to publish OWA or Sharepoint may be found in the ISA Server help under Firewall policy.