Table of Contents

1 Microsoft TMG 2010 Integration

1.1 Microsoft Forefront Threat Management Gateway (TMG) Integration Notes

1.2 Introduction

This document outlines the necessary steps to integrate Swivel authentication into Microsoft TMG Server 2010 for use with Swivel for Dual Channel authentication using SMS, Mobile Phone Clients and Single Channel using TURing, PINpad and the Taskbar. If the TMG server is part of a cluster then the filter needs to be installed on each server in the cluster.

1.3 Prerequisites

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

- If the option to allow unknown users is required, this requires Swivel 3.4 or later.
- If the option to use Pinpad is required, the Swivel version must be 3.9.2 or higher, or a version of the appliance proxy from 2012.

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

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

Allow around 1 hour downtime per TMG server for the integration, and the integration will require a restart of the TMG Firewall Services. If you are replacing an older version of the Swivel filter, you must uninstall that version first. The filter configuration will not be lost. You will need to stop the TMG firewall service before uninstalling the old filter, or else you will be prompted to restart the server to complete uninstallation.

1.3.1 Swivel TMG 2010 Filter

The filter can be downloaded from here. NOTE: this is version 1.4.4 of the TMG filter, released 1/11/13. Version 1.4.4 fixes a bug found by some customers, whereby the login page was not detected in some circumstances, allowing authentication by password only. The same bug could also cause other failures, such as occasionally failing to show a TURing image. This version also adds better control over logging. See the included documentation for more details.

Version 1.4.3 was never released, but made detection of the required URLs case-insensitive.

Version 1.4.2 includes some bug fixes and enhancements, in particular:

- Redirecting to the login page after an incorrect one-time code now works correctly. This means that an error message is displayed if the one-time code is incorrect. It is also expected that this will resolve issues experienced by some customers whereby, having logged in once, users do not always have to re-enter their one-time code.
- The firewall service is restarted automatically after making configuration changes and before uninstalling the filter.

Version 1.4.1 fixes some bugs present in version 1.4.0. Version 1.4 includes a number of enhancements over previous versions. See the included documentation.

NOTE: if you are using this filter with RADIUS authentication, be aware that there are some errors in the file usr_pwd_pcode.htm. These need to be fixed manually - contact support@swivelsecure.com for details. An update with the correct script will be released shortly.

1.4 Baseline

Swivel 3.1 or later (3.6 or later preferred)

Microsoft Forefront TMG 2010

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

1.5 Architecture

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

1.6 Swivel Configuration

1.6.1 Configure a Swivel Agent For XML Authentication

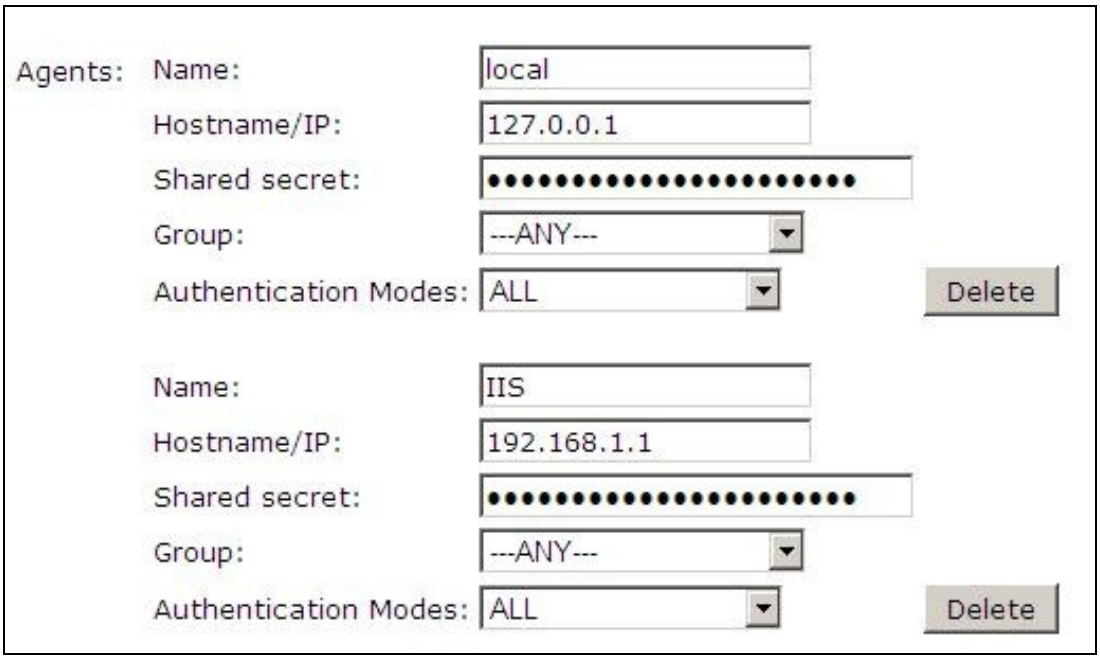
1. On the Swivel Management Console select Server/Agent

2. Enter a name for the Agent

3. Enter the TMG internal IP address

4. Enter the shared secret

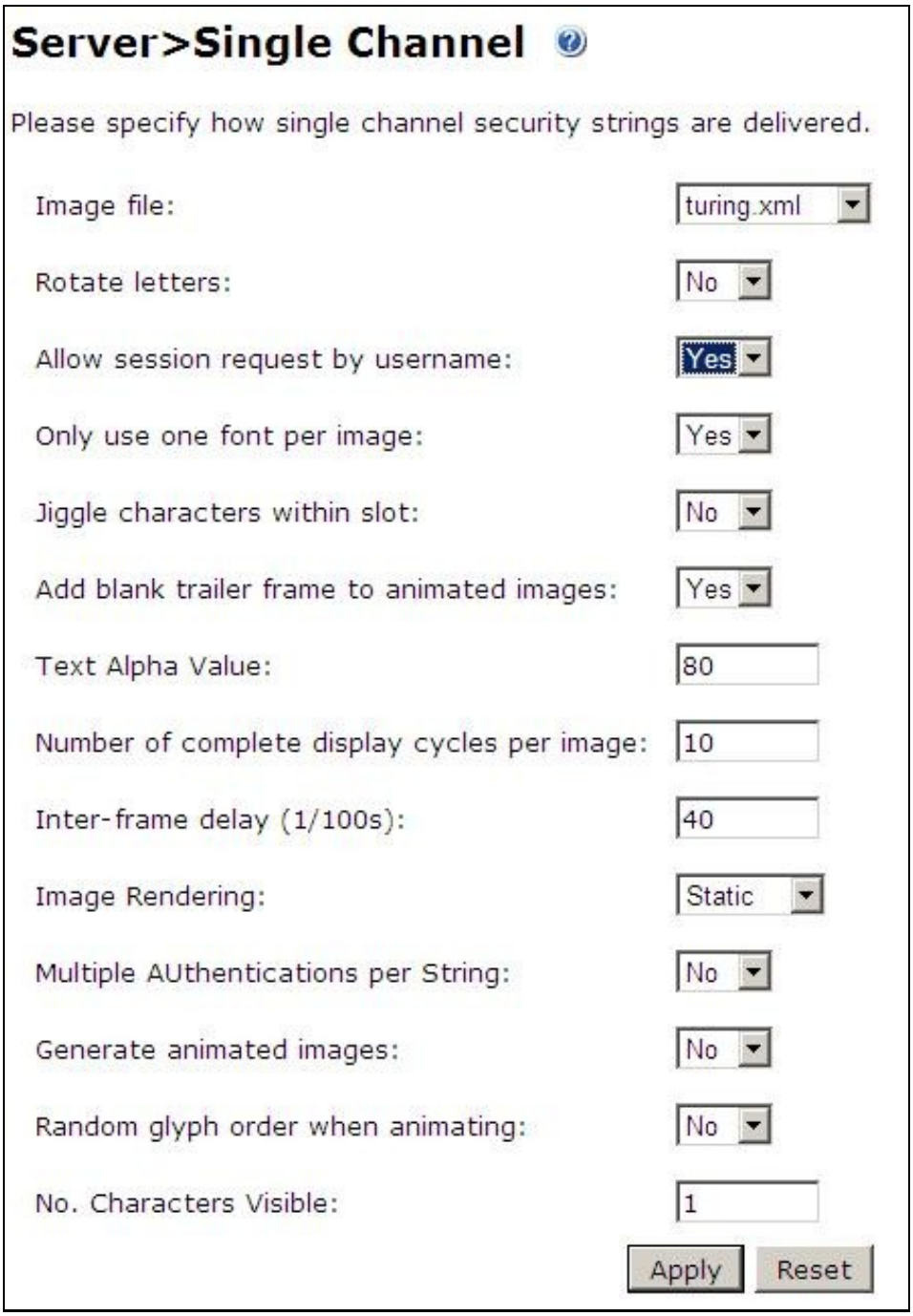
5. Click on Apply to save changes



1.6.2 Configure Single Channel Access

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

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



1.6.3 Configure a RADIUS NAS entry for Sharepoint authentication

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

1. Ensure the RADIUS server is running on Swivel

2. On the Swivel Management Console select RADIUS NAS

3. Enter a name for the NAS

4. Enter the TMG internal IP address

5. Enter the shared secret

6. Click on Apply to save changes

1.7 Swivel TMG Filter Upgrade

If an existing filter is installed then installing the new filter will first uninstall the existing filter.

1.8 Swivel TMG Filter Installation

The following steps should be carried out on the TMG server. No configuration changes need to be performed on the Exchange server or Sharepoint server. For Additional Sharepoint configuration see the Special Considerations for Sharepoint below. To upgrade or reinstall the filter, first remove the existing Swivel TMG filter.

1.8.1 Publish OWA or Sharepoint

Publish Outlook Web Access, Sharepoint or your website as described in the TMG Server documentation, if you have not already done so. Ensure that they are working as expected without Swivel authentication before attempting to install the Swivel filter.

For OWA, TMG should be configured to redirect to /owa automatically, otherwise a failure in the Swivel authentication will redirect to the root path, which will give an error. This external link shows how to configure this: Setting up an OWA redirect in Forefront TMG 2010 the easy way

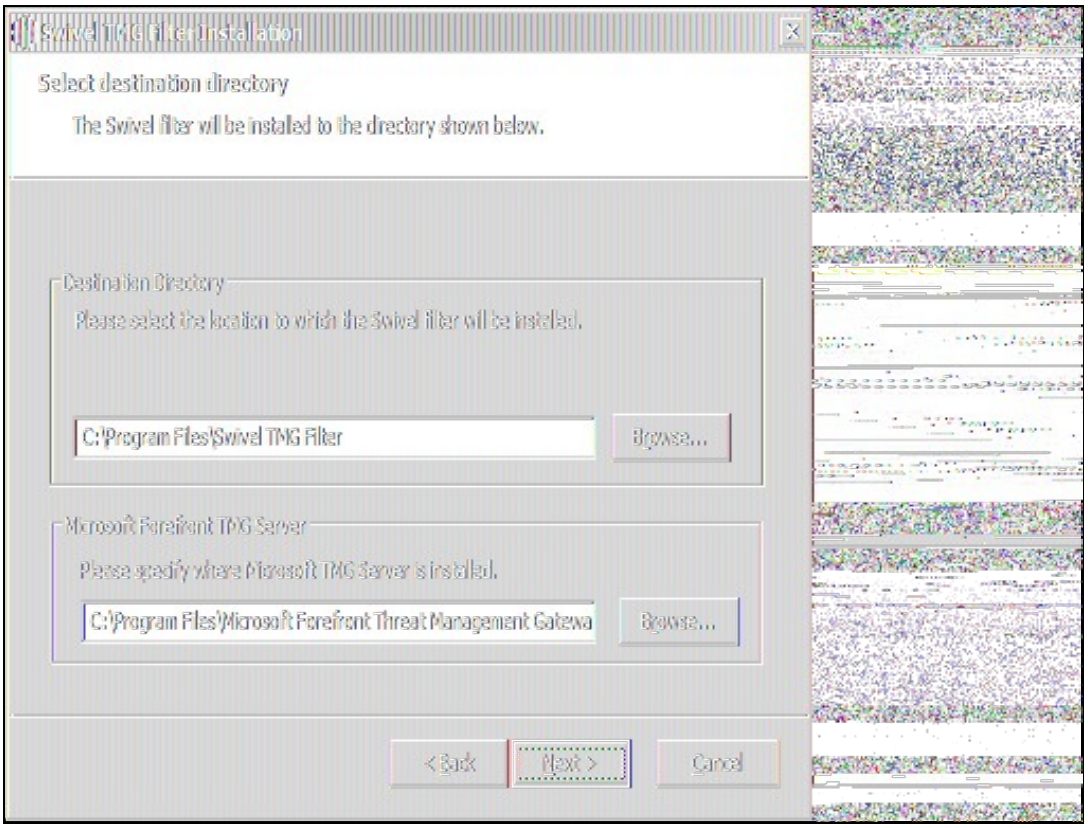
1.8.2 Configure TMG firewall rules

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

1.8.3 Install the TMG server software

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

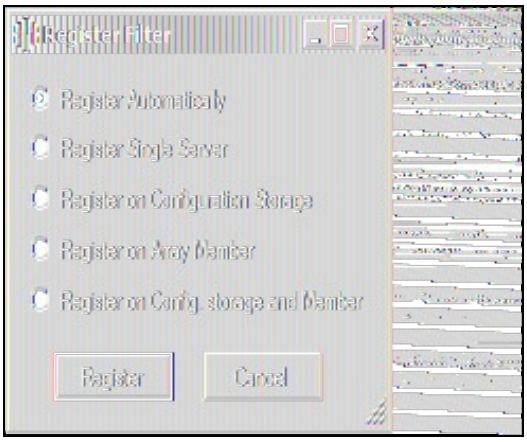
Run PINsafeTMGFilter.exe to install the filter DLL. You will be prompted for the location in which to install the filter configuration, and also for the location of Microsoft TMG Server, usually C:\Program Files\Microsoft Forefront Threat Management Gateway.



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

1.8.4 Register the Swivel TMG Filter

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

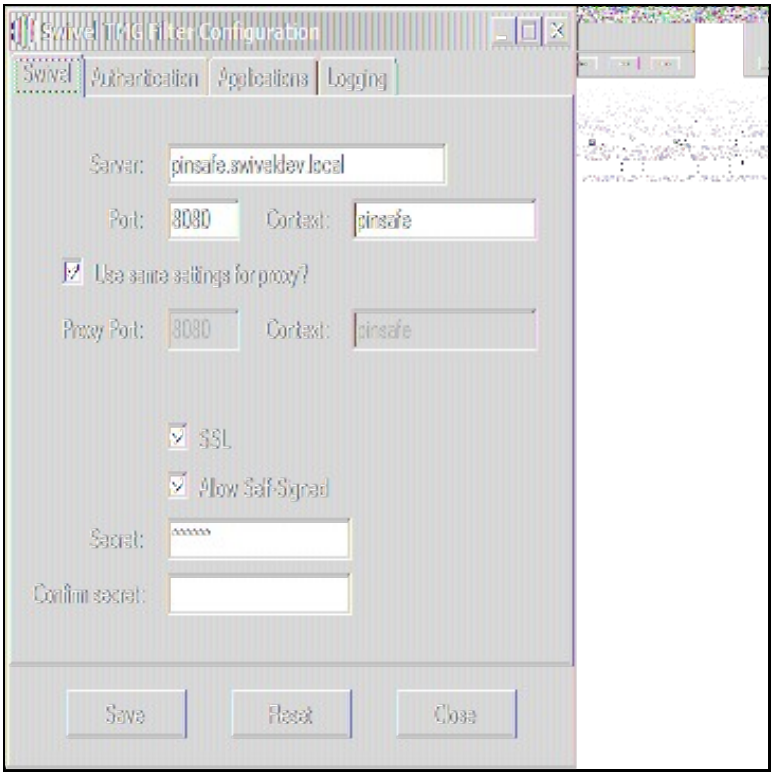


The Automatic registration option should work in most situations. Only try the other options if automatic registration fails.

1.8.5 Configure the TMG filter

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

1.8.5.1 Swivel 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. Swivel appliances require the use of XML authentication on port 8080 and the 8443 proxy port should not be used when integrating with TMG. (Hint: Use port 8080)

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

Proxy port and **Proxy context** may be required if you are using Pinpad together with an appliance that has the a proxy application that supports Pinpad, but does not have a version of Swivel that supports it directly. In this case, you should use proxy port 8443 and proxy context "proxy". You can still use these values if you are not using Pinpad, but you are using a Swivel appliance.

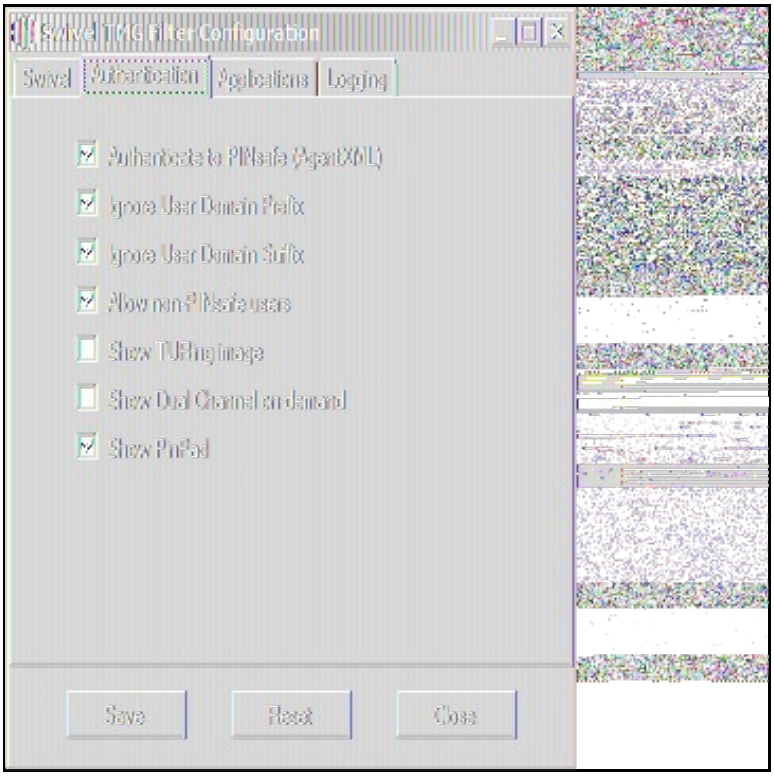
To clarify: the filter will use the proxy port and proxy context to retrieve TURing and Pinpad images (and message on-demand), but will use port and context to authenticate the user.

SSL: will, if checked, send requests to the Swivel server using https, rather than http. This applies to proxy as well: the current filter does not support connecting to one port on HTTP and the other on HTTPS.

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

Secret: is the shared secret for the Swivel agent for the ISA Server, and needs to be the same as that on the Swivel server. If you change this value, you must enter it twice to confirm the change.

1.8.5.2 Authentication configuration tab



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

Ignore user domain prefix: This will remove the AD domain prefix for users (anything before the '\' symbol), and when Swivel is using the SAM account name it should normally be checked. In this case, if you enter ?domain\user? as the logon username, only ?user? will be sent to Swivel. If it is not checked the prefix will be sent as part of the name to Swivel. If you use the domain prefix option in Swivel, you should uncheck this option.

Ignore user domain suffix: This will remove the AD domain suffix for users (anything after the '@' symbol). You should normally check this if you use sAMAccountName as the username for Swivel, but uncheck if you use userPrincipalName.

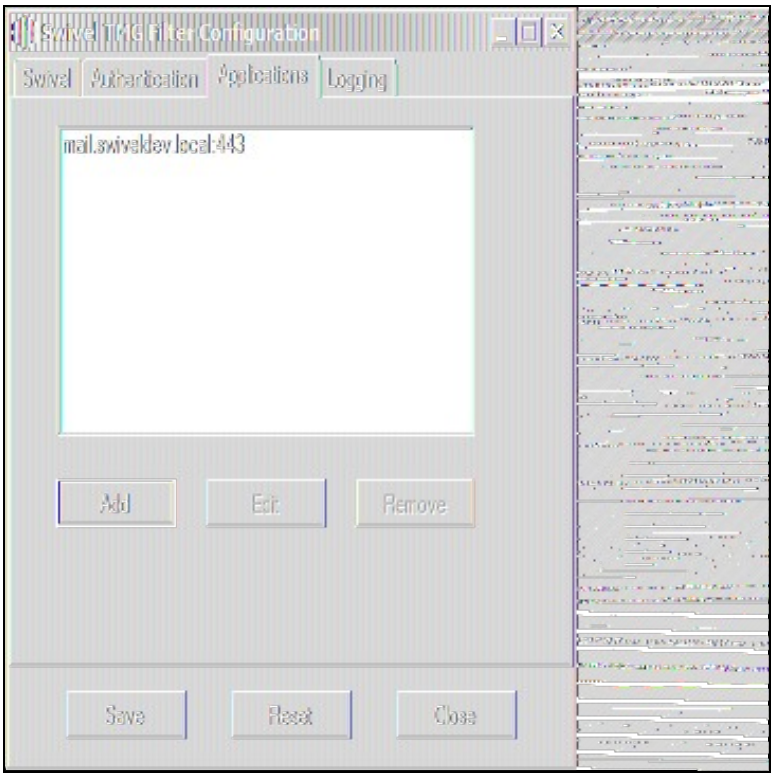
Allow non-PINsafe users: when checked, users not known to Swivel may authenticate using only their AD credentials. This feature is useful for transition to Swivel, where not all users have Swivel accounts. If checked, the OTC field is not shown initially, only when the username is checked and found to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

Show TURing image: when checked, entering a username or clicking the Start Session button on the login screen will display a TURing image for that user. It is not possible to prevent automatic display of the TURing image (i.e. only display when the button is clicked) from the configuration program, but this can be managed with a simple modification of the login page. Please contact Swivel for more information.

Show Dual Channel on-demand: when checked, a button is displayed allowing the user to request a security string via SMS or email (depending on how the strings transport is configured in Swivel). This option can be used together with the TURing or Pinpad option if required.

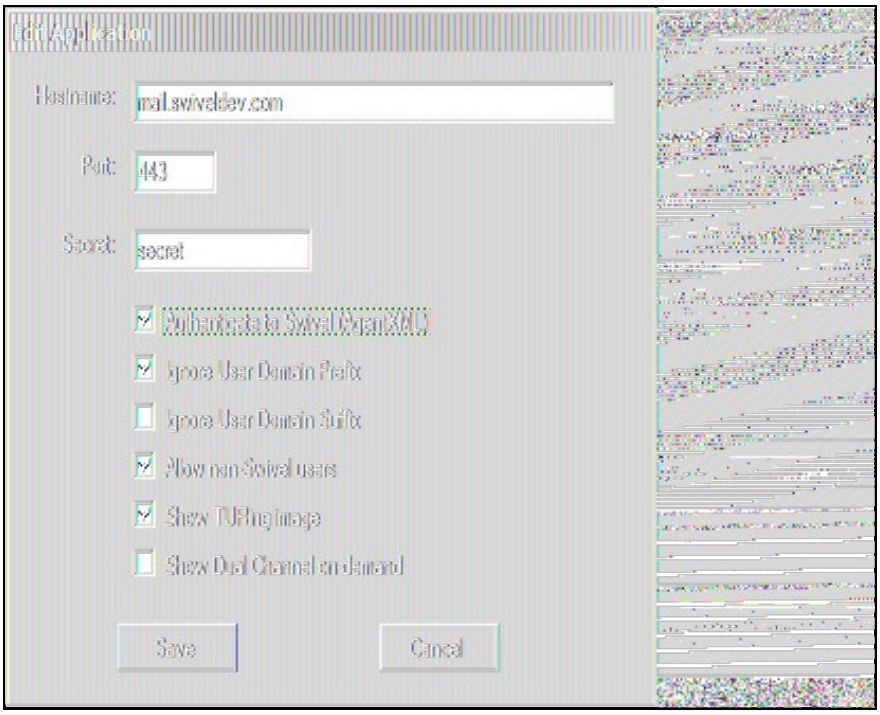
Show Pinpad: when checked, a Pinpad display is used to enter the one-time code. This option cannot be used with the TURing option, and requires that you have a version of Swivel or the appliance proxy that supports it.

1.8.5.3 Hosts configuration tab



This feature allows you to configure the filter to behave differently for different host names or ports on the TMG. It is only relevant if you are using the TMG to protect multiple websites.

If you add a new host, you will see the following form:



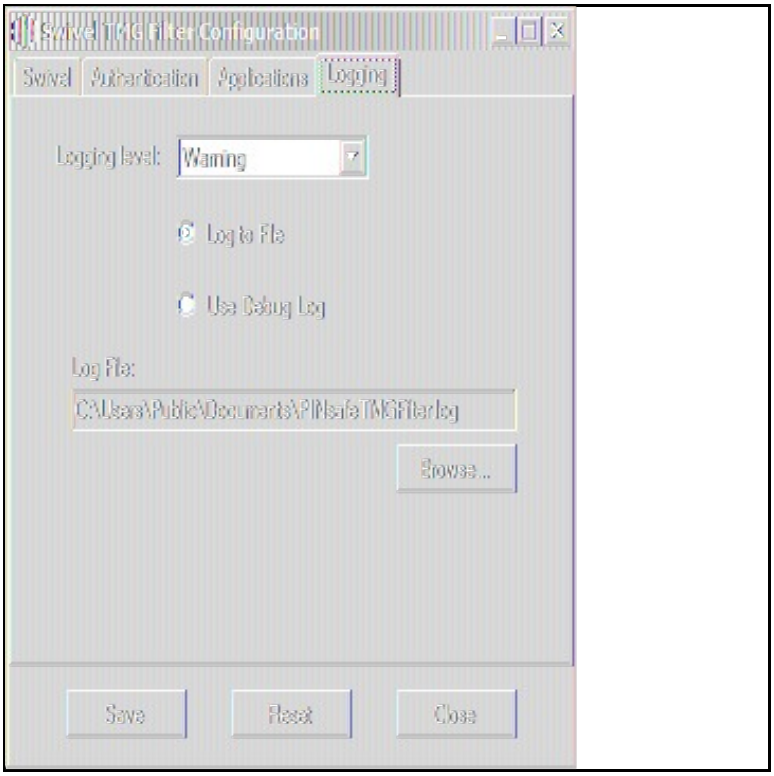
Specify the host name and port that this configuration should apply to. If you leave either one blank, it will apply to all host names on a given port, or all ports for a given host name.

You can specify a different secret from the default here. This allows you to use different Agents in Swivel, so for example, restrict authentication by groups. Swivel supports multiple agents for the same server, provided that the secret is different.

The remaining options override the default options for those particular settings. In particular, if you uncheck "Authenticate to Swivel", you can specify that certain host names do not require Swivel authentication.

If a request comes in that does not match any host name/port combination in this list, the default settings will apply.

1.8.5.4 Logging Configuration tab



Logging level controls how much data is logged: the levels are Debug, Info, Warning, Errors and None. The last option disables logging entirely. The most verbose level is Debug, and logs every single request received by the filter. It should only be used for troubleshooting.

You can choose to log to a file, or to a debug logger. The latter is provided for backward compatibility only ? you will need to have a debug logger installed to make use of it.

If you choose to log to a file, the default name is C:\Users\Public\Documents\PINsafeTMGFilter.log. Note that the log file does not roll over, but continues to fill up, so depending on what level of logging you use, you will need to back up or delete the log file regularly.

1.8.6 Confirm that the filter has been registered correctly

Once completed the filter will appear in the ISA Server Management Web Filters section. If the filter does not appear in the list of available filters check the Windows system event log for errors.

1.8.7 Modify the Listener

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

?PINsafeExchange? for Outlook Web Access

and ?PINsafeISA? for Sharepoint or other websites.

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

Once you have configured everything, restart the Microsoft Firewall Service on the TMG Server (not just activating TMG). It can take a long time to restart this service, and if you are connecting to the TMG Server via remote desktop, you may be temporarily disconnected from it.

1.9 SSL Certificate Considerations

There would appear to be an issue with certain security updates for TMG Server which prevents HTTP POST requests over SSL unless the target server certificate is fully trusted. This has consequences for the Swivel TMG Filter integration.

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

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

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

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

certificate on the Swivel server, with the correct host name, and to install that directly into the TMG Server trusted root store.

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

1.10 Special Considerations for Sharepoint

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

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

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

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

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

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

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

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

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

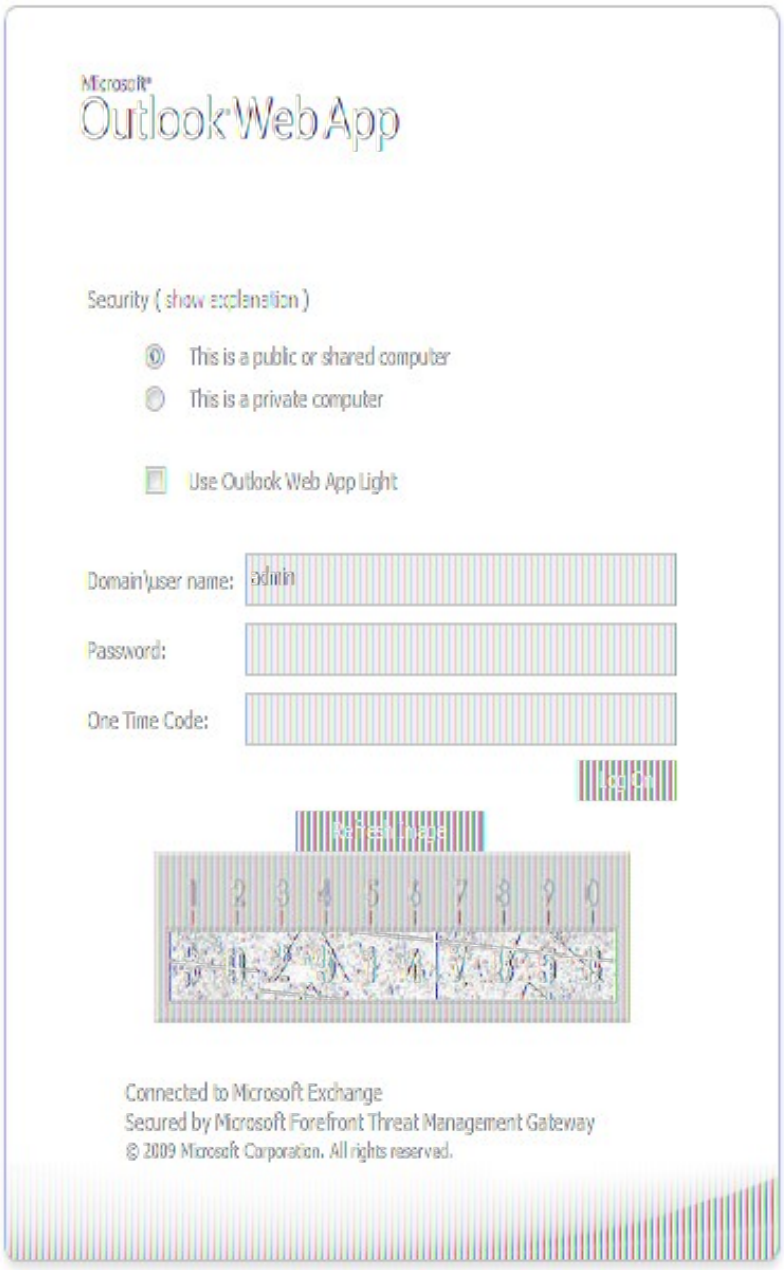
Once you have configured everything, reboot the ISA server.

1.11 Verifying Installation

1.11.1 Outlook Web Access

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

If you have enabled the option to allow non-Swivel users, then no Swivel customisation will be evident until after you enter the username and move to a different screen. The Swivel additional fields will then appear:



1.11.2 Sharepoint

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

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

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

1.12 Additional Options

1.12.1 RADIUS Authentication

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

1.12.2 Automatic sending of SMS

The login page can be configured to automatically send the user an SMS message when they have entered the username and proceed to the next field. On a default installation, edit the file "C:\Program Files\Microsoft Threat Management Gateway\Templates\CookieAuthTemplates\PINsafeExchange\HTML\usr_pwd.htm".locate the following lines:

locate the following

function setUserExists(attribute)

Approximately 20 lines below this, you should find the following section:

```
if (btnMessage) {
if (showMessage) {
btnMessage.style.display = "";
} else {
btnMessage.style.display = "none";
}
}
```

Insert a new line, as follows:

```
if (btnMessage) {
if (showMessage) {
btnMessage.style.display = "";
ShowMessage();
} else {
btnMessage.style.display = "none";
}
}
```

Once you have made this change and saved the file, you have to restart the Microsoft Gateway service for the change to take effect. Also, be aware that you need to make the same change on all TMG servers in the farm.

These instructions assume you have the latest version of the TMG filter.

1.12.3 Removing the OTC button

If you don't want the button to appear at all, on a default installation, edit the file "C:\Program Files\Microsoft Threat Management Gateway\Templates\CookieAuthTemplates\PINsafeExchange\HTML\usr_pwd.htm". Locate the following lines:

<input class="btn" id="btnImage" type="button" value="@@L_StartSession_Text" onclick="ShowTuring();" />

<input class="btn" id="btnMessage" type="button" value="@@L_SendMessage_Text" onclick="ShowMessage();" />

and delete them.

Once you have made this change and saved the file, you have to restart the Microsoft Gateway service for the change to take effect. Also, be aware that you need to make the same change on all TMG servers in the farm.

These instructions assume you have the latest version of the TMG filter.

1.12.4 Disabling the Auto TURing feature

When a TURing image is generated it expects the user to authenticate with that image for the length of the Session Cleanup.

When using the XML authentication the automatic display of the TURing image can be prevented by editing the file: "C:\Program Files\Microsoft Threat Management Gateway\Templates\CookieAuthTemplates\PINsafeExchange\HTML\usr_pwd.htm". Delete the line *ShowTuring();* within the function *setUserExists(attribute)*.

1.13 Uninstalling

1.13.1 Modify the Listener

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

?PINsafeOWA? for Outlook Web Access

Modify the properties for the relevant policy rule.

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

Uninstall the Swivel software using the Remove Programs.

reboot the ISA server

1.14 Known Issues

1.15 Troubleshooting

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

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

1.15.1 Filter status Check

This should be made in a web browser against the TMG login.

https://<path_to_TMG server>/PINsafeTMGFilter.dll?usepinsafe

This should return a series of 0s and 1s, Example: 10100110, the order can show the status as below:

1 - Show one-time code field

2 ? Allow unknown users

3 ? Show TURing image

4 ? Show Message on demand

5 - Show Pinpad

6 ? Ignore domain prefix

7 ? Ignore domain suffix

If it cannot contact the Swivel server, or if the filter is disabled, the first digit will be 0. NOTE: for versions of the TMG earlier than 1.4, the PINpad flag is not present.

1.15.2 Enabling Swivel logging

The Swivel authentication filter can optionally log its activity to a file. By default, no logging takes place, but you can enable logging by editing the filter registry key directly, using Regedit. The key to edit is

\\HKEY_LOCAL_MACHINE\Software\Swivel Secure\PINsafeTMGFilter

Create a DWORD value named "LogOptions". Set it to 2 to enable logging to a file. Set it to 1 to enable logging to the Windows debug log (see below), or 3 to enable both. Setting it to 0, or omitting it entirely, results in no logging.

The default log file is

C:\Users\Public\Documents\PINsafeTMGFilter.log

If you want to log to a different file, create a String registry value in the filter key named "LogFile", and set the value to the full path of the log file.

Older versions of the filter always log activity to the standard Windows debug log. Newer versions can optionally do this as well. This can be accessed using a tool such Sysinternals DebugView available as freeware from:

Sysinternals DebugView

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

1.15.3 Single Channel image does not appear

- Check Swivel TMG filter settings
- Use a fully qualified hostname instead of IP address for the Swivel server
- Is an SSL connection being used
- Is a self signed cert being used, if so try without SSL using http or install a valid public certificate
- Is the certificate using the internal hostname or the external hostname? The hostname used by Swivel must match the certificate hostname.
- Check the Swivel TMG filter is correctly installed. On the TMG Server Management: under System, on the Web Filters tab, "Swivel Authentication Filter" should be enabled
- From the TMG server check a Single Channel image can be generated in a web browser connecting to the Swivel server using:

Swivel appliance

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

or

https://<PINsafe server IP>:8443/proxy/SCImage?username=test

For a software only install see Software Only Installation

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

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

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

1.15.4 Page fails to display after failed login

An **Access Forbidden message** is displayed. After a login failure, the user is redirected to https://hostname/, rather than https://hostname/owa. You can configure the TMG firewall rule to automatically redirect to /owa. This external link shows how to configure this redirect: Setting up an OWA redirect in Forefront TMG 2010 the easy way

1.15.5 Adding Swivel authentication stops other pages appearing

You can specify that PINsafe authentication only applies to certain host names, in which case the others are ignored. On the Swivel TMG filter disable Swivel authentication in the default configuration, then add an application with the host name that DOES require authentication, and set Swivel authentication ON for that one only, or if you want to be explicit, add all three host names, and disable Swivel authentication for the ones you don't want.

1.16 Additional Information

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

For assistance in Swivel installation and configuration please contact your reseller.

2 Microsoft TMG RADIUS Integration

3 Microsoft Threat Management Gateway Integration

This guide describes how to integrate Swivel with Microsoft Forefront Threat Management Gateway using RADIUS authentication. No additional software is required.

If you want more control over authentication, with support for restricting Swivel to certain hostnames and allowing non-Swivel users to authenticate, see the TMG filter documentation for more information.

3.1 Configuring Swivel

- Log on to the Swivel Admin Console
- Under RADIUS -> Server, make sure that the server is enabled. All the other settings can be left as default.
- Under RADIUS -> NAS, enter a name in the blank identifier box (e.g. ?TMG?). Enter the name or IP address of the TMG server, and a chosen secret. Remember what you enter in the Secret box, as you will need it later.
- Click Apply.

3.2 Configuring Firewall Rules

It is assumed that you already have a firewall rule set up to support the website you need to protect. If not, use the appropriate wizard under Firewall Policy Tasks to set up the rule.

3.2.1 Modifying the Website Access Rule

To support Swivel authentication, all you need to do is to right-click on the Listener for the rule and select Properties. On the Authentication tab, select HTML Form Authentication, if it is not already selected.

Under most circumstances, you will need to authenticate to Windows Active Directory as well as to Swivel. Configure both AD and Swivel as authentication servers. To use Windows and Swivel authentication, check the box marked ?Collect additional delegation credentials in the form?. Make sure ?RADIUS OTP? is selected in the lower box, then click on ?Configure Validation Servers?. On the RADIUS Servers tab, click Add. Enter the IP or name of the Swivel server and the shared secret that you entered earlier for the Swivel NAS.

If you only want to use Swivel to authenticate, and no other method, then leave the option for additional delegation credentials unchecked and select either RADIUS or RADIUS OTP. You can only select RADIUS OTP if the Authentication Delegation option on the main rule is No Delegation.

NOTE: As described below, you may choose to create a new set of custom login pages, rather than replacing the existing ones. If you do, you will need to check the option to use custom HTML forms (on the Forms tab), and enter the name of the custom forms set.

3.2.2 Proxying the TURing Image

In order to allow Swivel to deliver a TURing image to the end user without exposing the Swivel server to the internet, it is necessary to create a firewall rule to proxy it. If you are using dual channel only, except for dual channel on demand, you can skip this step.

- Click on Publish Web Sites.
- Call the rule Swivel Image, or as required.
- Accept the defaults for the first few steps.
- Under internal site name, enter the name of the Swivel server. Note that this name must match the name of the SSL certificate on the Swivel server, since SSL requests through this rule must not generate any errors. Alternatively, you can configure Swivel not to use HTTPS.
- For Path, enter /proxy/SCImage (assuming this is an appliance, or /pinsafe/SCImage if not). For dual channel on demand, change SCImage to DCMessage.
- Select Any domain name.
- Create a new Listener. Call it TURing, or whatever you like.
- Require SSL (if you don't have an SSL certificate installed, select non-SSL)
- Select External networks only
- Select an SSL certificate if required
- Select No Authentication
- The remaining Listener options do not require configuration
- Back on the publishing wizard, accept the defaults for the remaining options.
- Once the rule is complete, right-click and select Properties
- On the Bridging tab, choose to redirect to port 8443 for context /proxy, or 8080 for context /pinsafe.

3.3 Customising Login Pages

If you are using dual channel authentication in Swivel, and do not require an embedded TURing image in your login page, you do not need to customise the login pages. This does not apply to dual-channel on-demand, for which the customisation IS required.

You can choose either to customise the default login pages, or to create a custom set of pages. If you are not using Swivel for all authentication rules on this TMG, you must create a custom set.

To create a custom set of rules:

- In Explorer, go to the TMG root folder: under a default installation, this is C:\Program Files\Microsoft Forefront Threat Management Gateway.
- Select the Templates sub-folder
- Select the CookieAuthTemplates sub-folder.
- Make a copy of one of the folders you find underneath here: for an Exchange firewall rule, select Exchange, and for other rules select ISA.
- Give the folder an appropriate name. NOTE: remember to change the custom forms option on the listener to specify the name of this folder.

If you choose to replace the existing login pages, select the CookieAuthTemplates folder as described above, then select either the ISA sub-folder, or the Exchange sub-folder, depending on whether or not you are customising Exchange access. If you have created a custom set, select that. Select the HTML sub-folder.

NOTE: if you are replacing existing standard login pages, make sure you take backup copies of any files you replace.

There are 3 files you might need to replace, depending on which authentication option you selected:

- For RADIUS authentication only, replace usr_pwd.htm
- For RADIUS OTP authentication only, replace usr_pcode.htm
- For dual Windows and RADIUS OTP authentication, replace usr_pwd_pcode.htm

The custom pages can be found here.

You will need to edit the file(s), and change the value of imageUrl to the appropriate external URL for the TURing image, as determined by the firewall rule you created earlier.

3.3.1 Changing the OTC button text

To change the OTC label, edit the following file:

C:\Program Files\Microsoft Forefront Threat Management Gateway\Templates\CookieAuthTemplates\PINsafeExchange\HTML\usr_pwd.htm.

Search for OTC as a whole word. You should find the following line:

```
<td class="nowrap"><label for="otc">OTC</label></td>
```

Change the prompt as required, and restart the firewall service.

3.3.2 Automatic sending of SMS

The login page can be configured to automatically send the user an SMS message when they have entered the username and proceed to the next field. On a default installation, edit the file "C:\Program Files\Microsoft Threat Management Gateway\Templates\CookieAuthTemplates\PINsafeExchange\HTML\usr_pwd.htm".locate the following lines:

locate the following

function setUserExists(attribute)

Approximately 20 lines below this, you should find the following section:

```
if (btnMessage) {
if (showMessage) {
btnMessage.style.display = "";
} else {
btnMessage.style.display = "none";
}
}
```

Insert a new line, as follows:

```
if (btnMessage) {
if (showMessage) {
btnMessage.style.display = "";
ShowMessage();
} else {
btnMessage.style.display = "none";
}
}
```

Once you have made this change and saved the file, you have to restart the Microsoft Gateway service for the change to take effect. Also, be aware that you need to make the same change on all TMG servers in the farm.

These instructions assume you have the latest version of the TMG filter.

3.3.3 Removing the OTC button

If you don't want the button to appear at all, on a default installation, edit the file "C:\Program Files\Microsoft Threat Management Gateway\Templates\CookieAuthTemplates\PINsafeExchange\HTML\usr_pwd.htm".locate the following lines:

<input class="btn" id="btnImage" type="button" value="@@L_StartSession_Text" onclick="ShowTuring();" />

<input class="btn" id="btnMessage" type="button" value="@@L_SendMessage_Text" onclick="ShowMessage();" />

and delete them.

Once you have made this change and saved the file, you have to restart the Microsoft Gateway service for the change to take effect. Also, be aware that you need to make the same change on all TMG servers in the farm.

These instructions assume you have the latest version of the TMG filter.

3.4 Troubleshooting

The thing you are most likely to have problems with in this integration is SSL certificates. When linking to a server that requires SSL, the TMG will fail if there are any errors in SSL handshaking. The guidelines here should help.

NOTE: to import a certificate from a Swivel appliance into a TMG to use as a proxy for the Swivel server, you must generate the private key with the argument -keyalg RSA. This is NOT the default when using the CMI options, so the certificate must be generated from the command line.

If you create SSL certificates using an internal Windows certificate authority, and generate the certificate request from the web interface, be aware that certificates generated using the Web Server template are not exportable. You need to create a new template for exportable web server certificates, as detailed here. Also, TMG does not support CNG / Windows 2008 certificates, so when creating the new template, make sure you select Windows 2003 compatibility. For the same reason, if you generate a new certificate request using the certificates MMC plug-in (details not given here), make sure you select Legacy rather than CNG. Our recommendation, however, is to use Keystore Explorer (see SSL Solutions) and to generate the certificate request with that.

As a last resort, particularly if the Swivel Appliance is not to be visible on the internet, you can simply disable HTTPS on the Swivel server. See the appliance documentation for details on this. Note that if you do disable https, you must alter the TURing Listener to match the settings.

If users are allowed to authenticate without Swivel authentication ensure 'Require all users to authenticate' option is checked.