Table of Contents

1 Microsoft IIS version 6 Integration

1.1 Overview

This document outlines the steps required to integrate the Internet Information Server (IIS) with PINsafe using dual or single channel authentication. The PINsafe install requires configuring an agent on the PINsafe server and setting up a shared secret with the IIS server to allow communication for authentication. An ISAPI filter installed on the IIS server allows access to protected resources through the PINsafe authentication.

NOTE: This document refers to the version of the filter numbered 1.1.0.1, and the configuration application with the same version number.

32 bit and 64 bit versions of the filter are available.

If Windows 2008 Server server is being used, or only ASP.Net applications are being protected an alternative authentication is available, see Microsoft IIS version 7 ASP.NET Integration. However, this filter will still work in these situations if you prefer.

1.2 Prerequisites

Internet Information Server on Windows server 2000, 2003, 2008

PINsafe server

The appropriate PINsafe ISAPI filter software can be downloaded from here, depending on your operating system:

- 32-bit ISAPI Filter
- 64-bit ISAPI Filter

These links refer to the latest version of the filter: 1.3.8.

The previous version (1.2) is provided here:

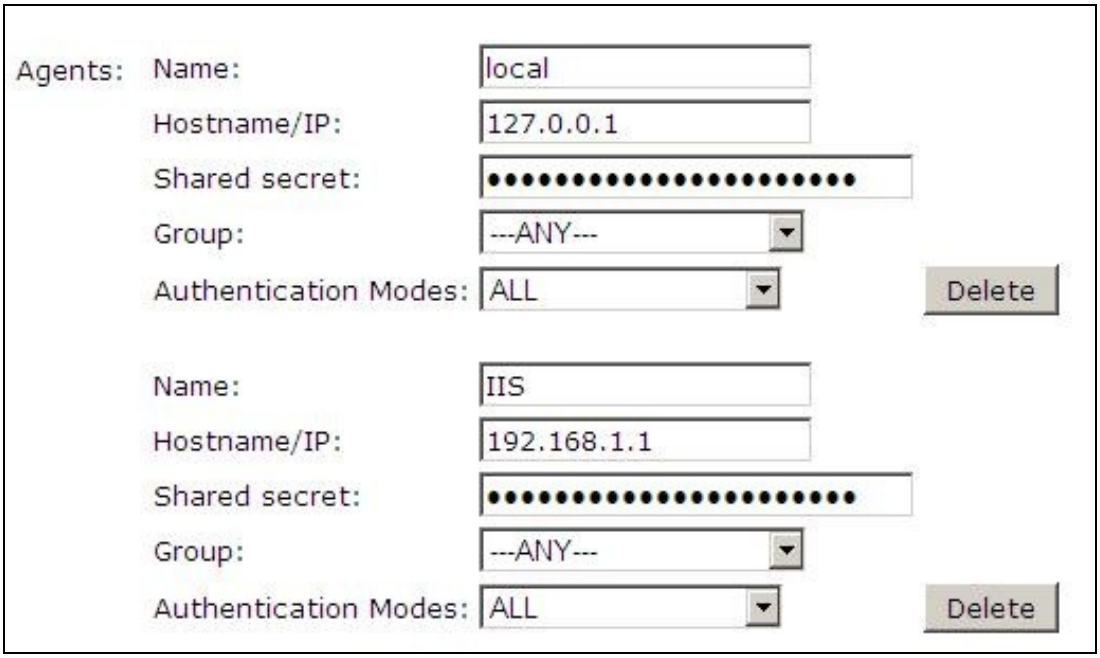
- 32-bit ISAPI Filter
- 64-bit ISAPI Filter

1.3 PINsafe Configuration

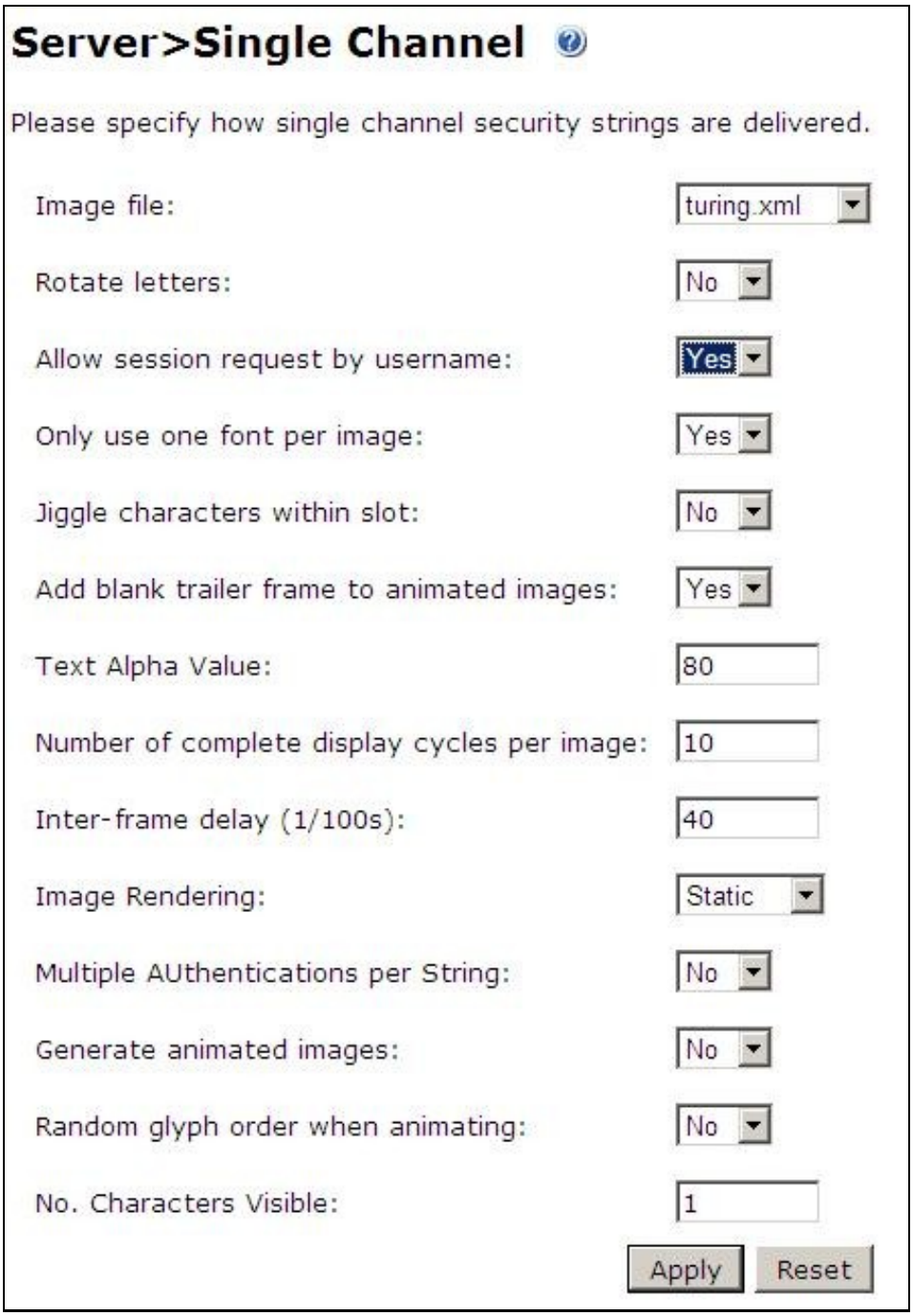
On the PINsafe server configure the agent that is permitted to request authentication. On the PINsafe Administration Console select from the server menu Agents and enter the details of the IIS server IP address and a shared key, then click on apply.

Example:

```
Name : IIS server 1,
Hostname/IP : 192.168.1.1,
shared secret : secret
```



If Single Channel communication is to be used, select from the PINsafe Administration Console Single Channel, and set the Allow image request by username to Yes then click on apply.



1.4 Configuring the IIS Server

1.4.1 Install the PINsafeIISFilter.exe

1. On the IIS server run the PINsafeIISFilter.exe. The IIS filter may need to be run as an Administrator user (The filter needs to be installed by IIS running as Administrator user but it can run as a normal user).

2. Choose the Path to Install to - the default is as C:\Program Files\Swivel Secure\Swivel IIS Filter

3. Select Start Menu Folder

4. When details are correct click on Install

5. If the error ?Incorrect Command Line Parameters? is seen click on OK

NOTE: you will see that there are two installation options: "Filter" and "Configuration". Typically, you would install both on the web server, but the configuration program requires Microsoft.Net Framework 4.0 or higher installed. If your web server doesn't have this, and you prefer not to install it, then you can install the configuration program on a separate machine. You would then need to create the configuration file locally, and copy it to the web server.

1.4.2 Configure the ISAPI filter

When the installation is completed, you will be presented with the configuration program. See below for details on using this.

1.4.3 Create a PINsafe virtual directory

1. On the Internet Information Services Manager right click on the website and select New, Virtual Directory

2. Create an Alias called PINsafe

3. Point the path to the PINsafe directory Web folder, by default C:\Program Files\Swivel Secure\Swivel IIS Filter\Web.

4. Set the permissions to Read and Run Scripts

5. Right-click on the newly-created virtual directory and choose Properties. On the Virtual Directory tab, click the Remove button next to Application name and then click OK.

1.4.4 Install The IIS ISAPI filter

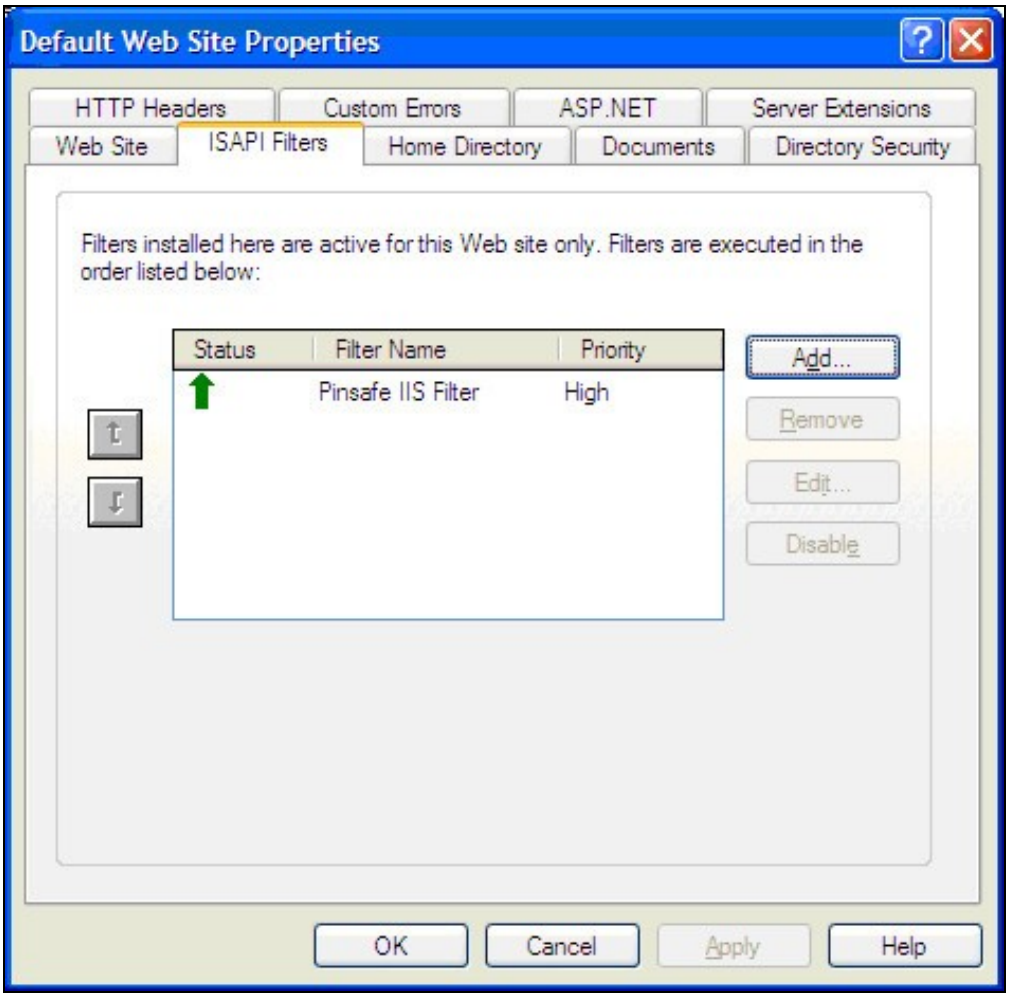
1. On the Internet Information Services Manager Select the Properties for the website

2. Select ISAPI filters

3. Select Add ISAPI filter

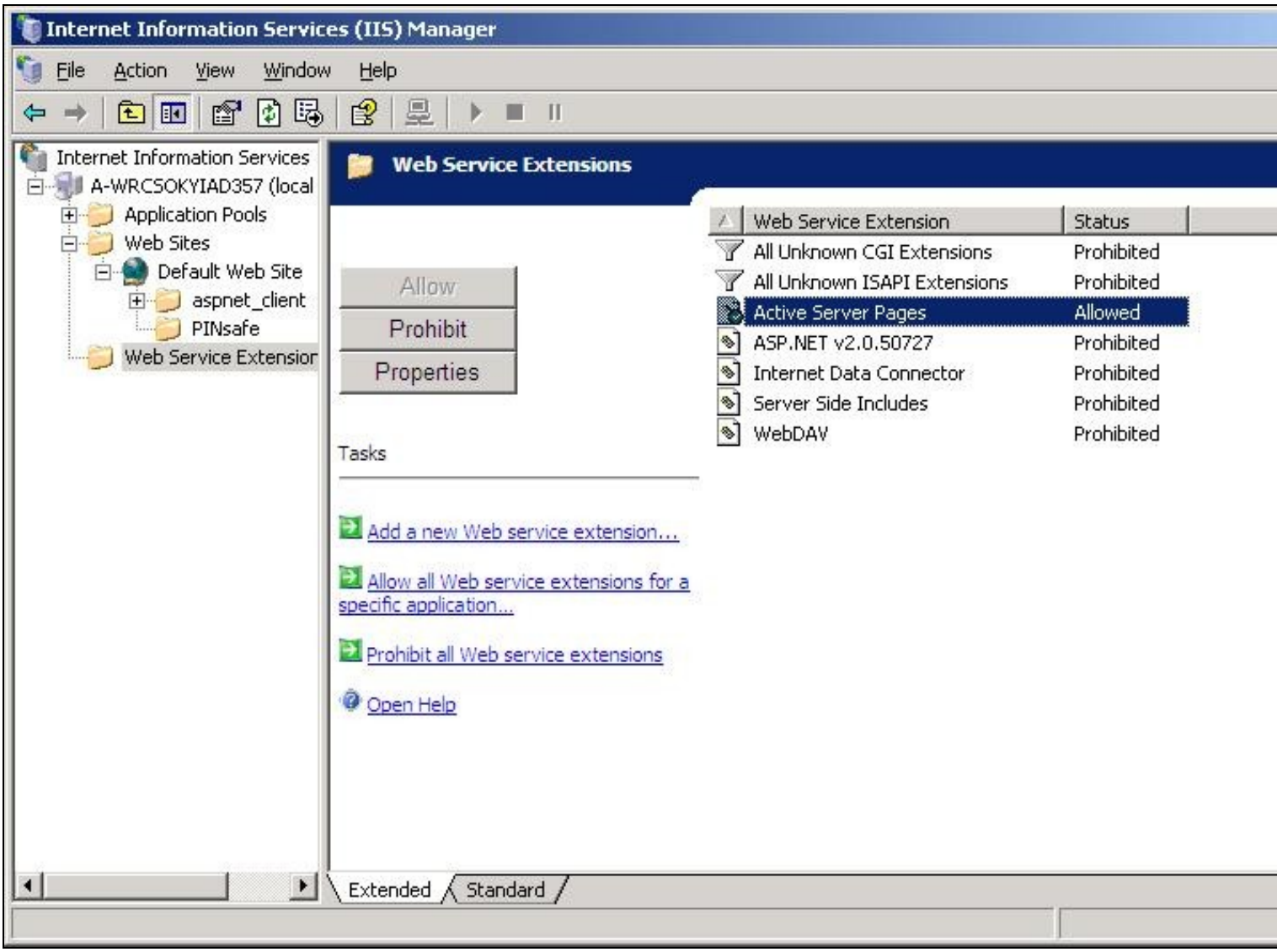
4. Select the Path to the PINsafe ISAPI filter. Note that the actual file you require will be PINsafeIISFilter.dll, located in the installation folder.

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



From the Services application, usually found from the Control Panel Administrative Tools, restart the World Wide Web Publishing Services.

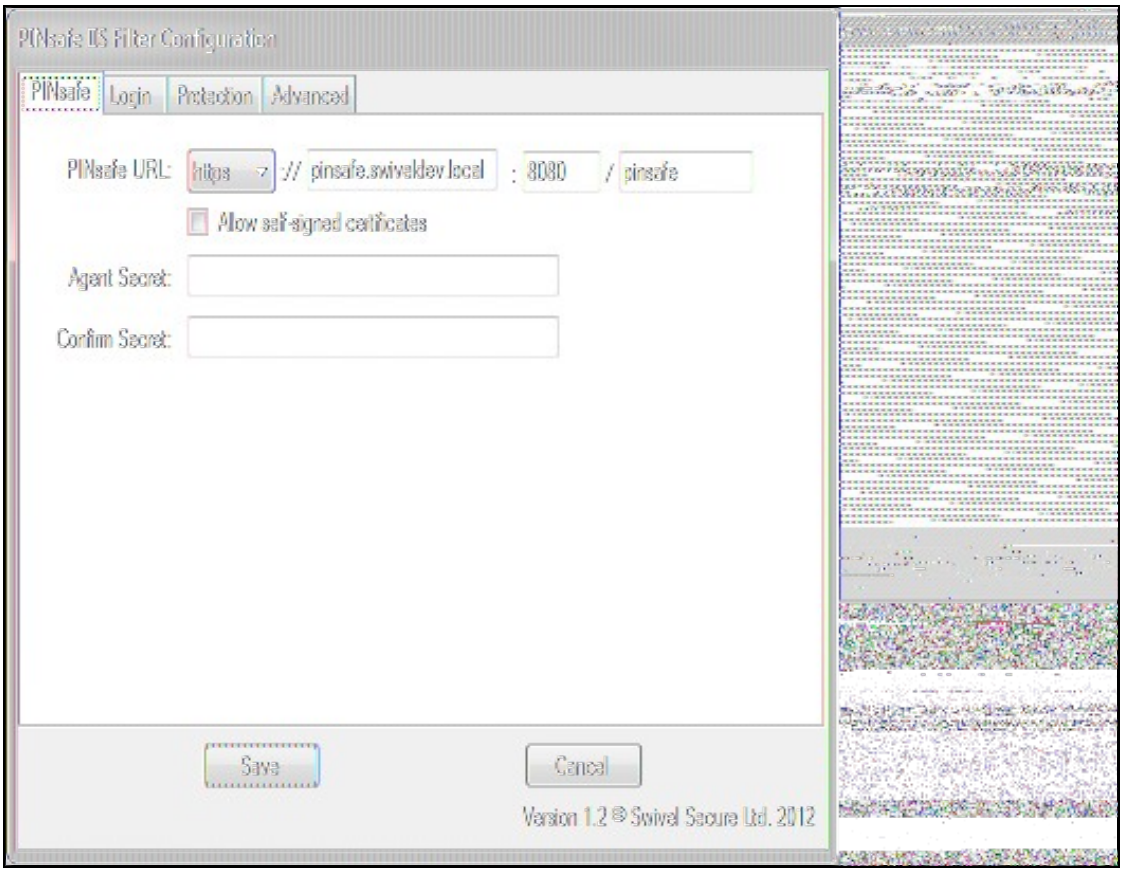
Allow Active Server Pages: to verify this, select the Internet Information Services Manager expand the required server then click on Web Service Extension.



1.5 Configure the ISAPI Filter

This documentation refers to version 1.2 of the configuration program. If you are still using an older version, see the next section for a description of the configuration program.

1.5.1 PINsafe Server Settings



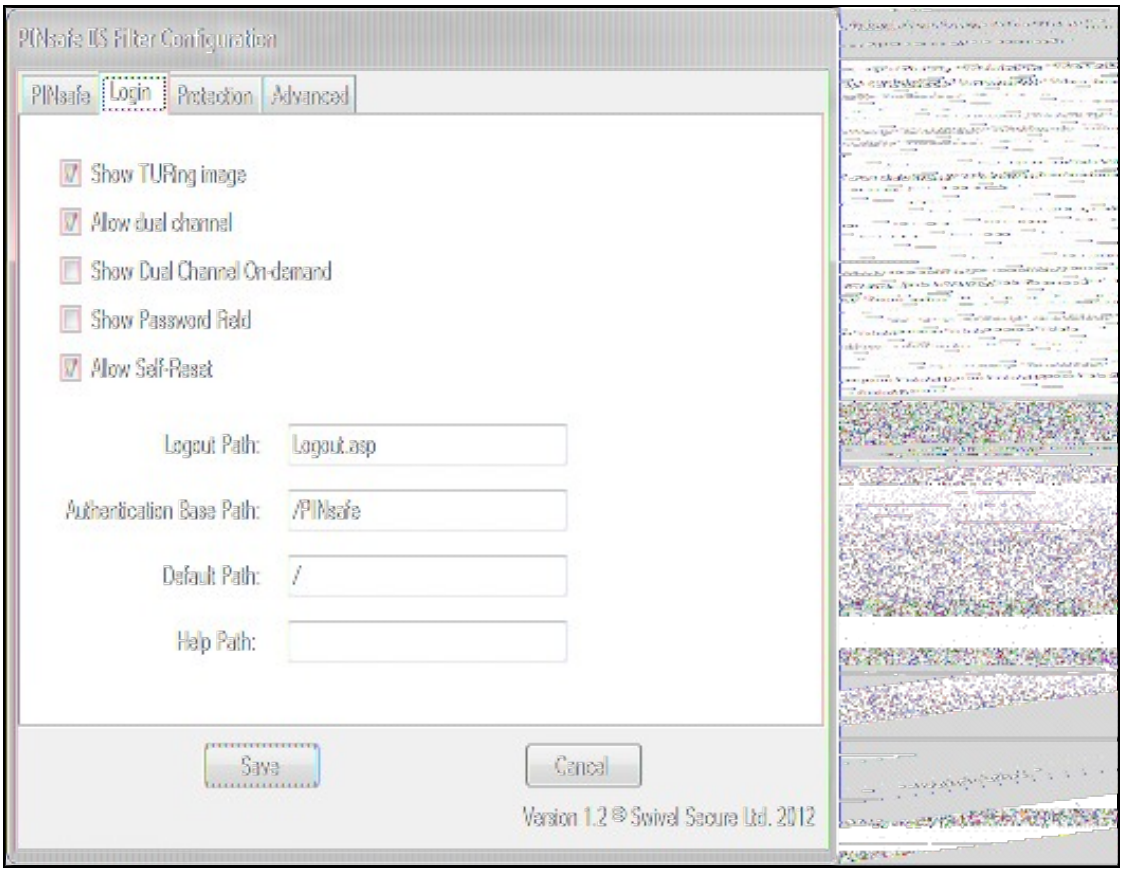
This page defines the connection to the PINsafe server.

In the first line, enter the URL for the PINsafe server. As you will see, it is entered in several parts: http/https, the server host name or IP address, port number and context.

The check box on the second line indicates whether self-signed SSL certificates are allowed for https. This actually ignores all SSL certificate errors, including incorrect host name and expired certificates. You should only use this option if the connection is internal only, and you are confident that the PINsafe server settings are correct.

The final option on this page is the shared Agent secret. This should be the same as the secret entered for the Agent entry on the PINsafe configuration. It is not normally displayed, and you should only enter a value if you wish to change it: a blank entry will result in no change. You need to enter the same value twice to ensure it is entered correctly.

1.5.2 Login Page Settings



This page defines how the login page is displayed, and what happens on login.

The first 5 checkboxes enable or disable features on the page:

Show TURing image: displays a button to show a TURing image.

Allow dual channel: has no obvious effect - dual channel authentication is always allowed if PINsafe policy permits it.

Show Dual Channel On-demand: displays a button to request an on-demand security string.

Show Password Field: requests a PINsafe password as well as the one-time code. This will also enable repository (e.g. AD) password if the Agent has "Check Repository Password" enabled.

Allow Self-Reset: shows a link on the page to the self-reset page, in case the user has forgotten their one-time code.

The four paths are:

Logout Path: if the filter detects this path, the PINsafe authentication cookie is removed, so the user must log in again.

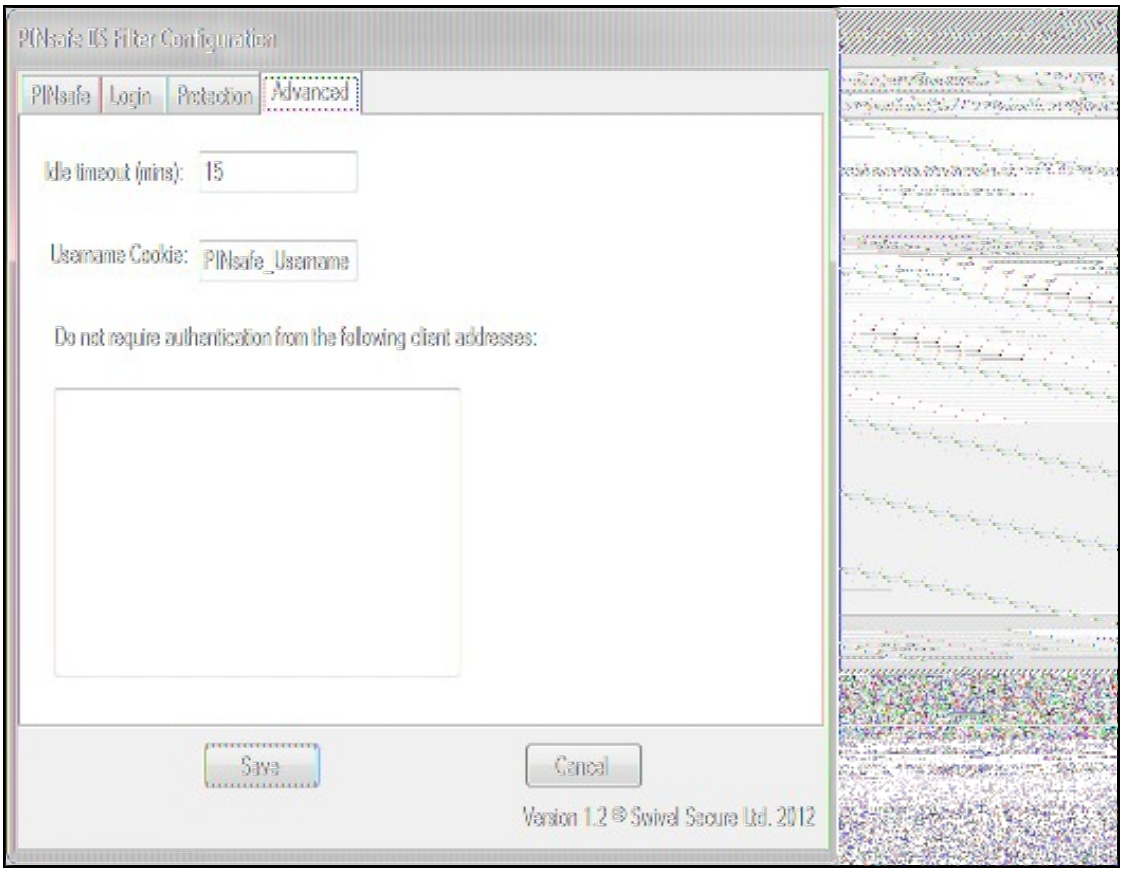
Authentication Base Path: the virtual path containing the PINsafe authentication pages.

Default Path: if a user navigates directly to the PINsafe login page, rather than being redirected by the filter, this is the path the user will be redirected to on successful authentication.

Help Path: if present, a link will be displayed to this path if the user requires help. This must be provided by the customer: Swivel does not provide any help pages.

1.5.3 Advanced Settings

Let us take the last tab out of order, as the Protection tab is the most complicated one:



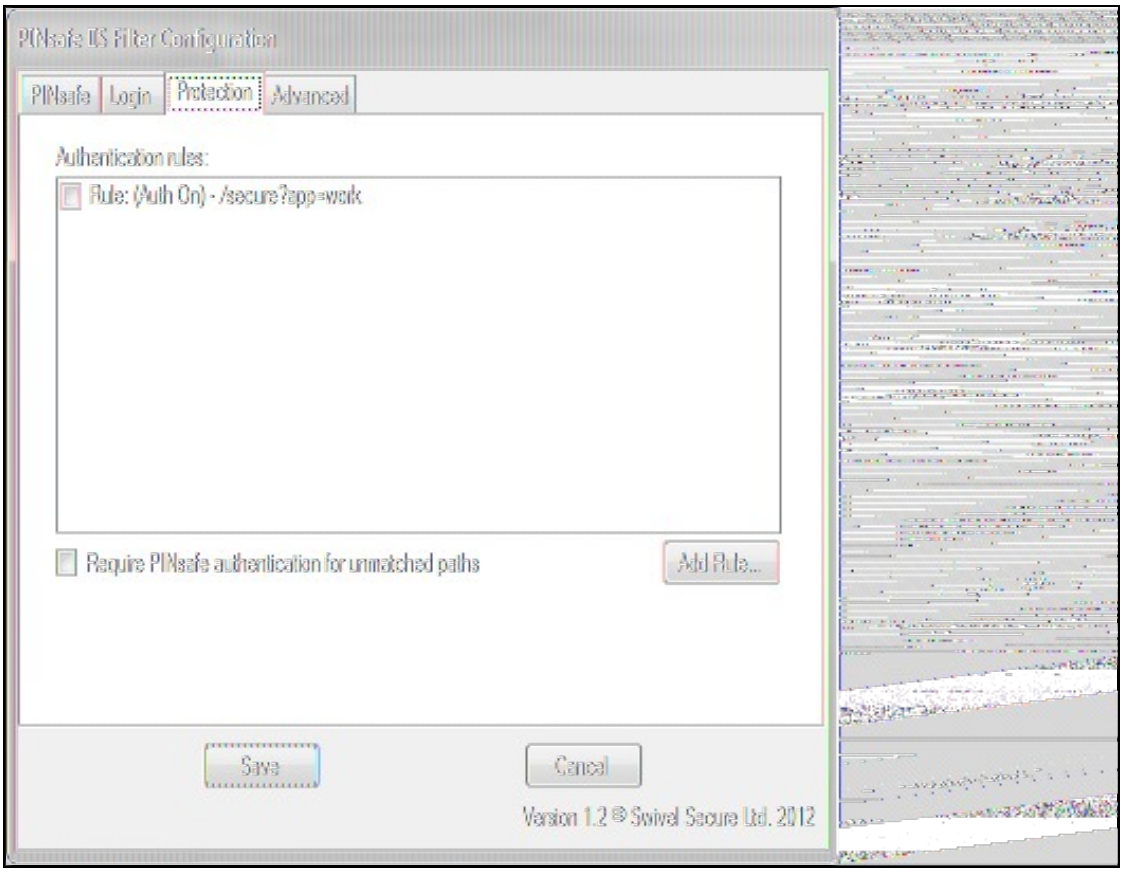
Idle timeout is the time (in minutes) that the user can leave a page open without refreshing it or navigating to another page: in other words, the lifetime of the authentication cookie. However, if the user requests a new page (or refreshes the current one) within that time, the cookie expiration time is updated.

Username cookie, if entered, specifies the name of a cookie that will contain the name of the authenticated user. Other applications can make use of this cookie if they are written to read it.

The final option on this page allows you to specify a list of source addresses that are not required to authenticate to PINsafe. Typically, these will be internal addresses.

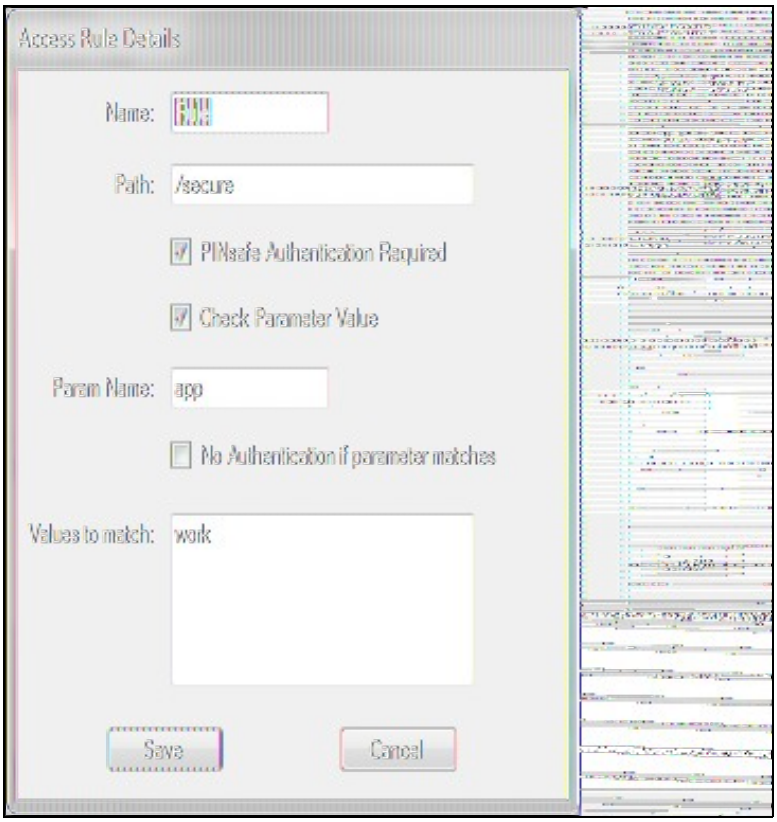
1.5.4 Protection Settings

This tab replaces the Included and Excluded paths of the older filter:



In order to define which paths PINsafe protects, you need to define rules. The main part of this tab summarises the current list of rules.

To add a new rule, click "Add Rule...", and you will see the following page.



The rule name is just a means of identifying the rule: it doesn't affect how the rule works.

The path is the URL that must match the URL entered for the rule to apply. The path must start at the slash immediately after the host name (and port if given). The match is case-insensitive, and the entire entered URL does not have to match the path: it just has to match as far as the path is specified. So, for example, if the path is "/secure", it will match "/secure/default.aspx", or even "/securepage", but not "/somewhere/secure".

The next checkbox indicates what happens if the path is matched. If it is checked, PINsafe authentication is required, and if no PINsafe cookie is found, the user is redirected to the login page. If this box is unchecked, the user is permitted to continue without authenticating, and no further rules are tested.

The remainder of the rule allows you to restrict PINsafe authentication according to the value of a particular parameter in the query string. Check the "Check Parameter Value" checkbox to enable this option.

Param Name is the name of the parameter that must be matched. Values to match allows you to specify a list of values that are accepted. The parameter must match one of these values.

The final checkbox defines how PINsafe authentication is affected depending on the value of this parameter. Normally, PINsafe authentication is applied if any of the values match. Checking this box reverses the logic, so PINsafe authentication is applied only if the parameter DOESN'T match any of these values.

Note that the parameter value only affects whether or not PINsafe authentication is applied, not whether or not the rule matches. Rule matching is done by path only.

Note also that parameter matching only applies to HTTP GET requests, i.e. when the query string is part of the URL. It cannot handle POST requests, when the parameters are in the body of the request.

So, using the example rule above: if the URL entered is "/secure/default.aspx?app=work", then PINsafe authentication is required. If the path is "/secure/default.aspx?app=play", or "/secure/default.aspx" (i.e. no parameter), then PINsafe authentication is NOT required.

NOTE: all comparisons, of path, parameter name and parameter value are case-insensitive.

The filter works by checking each rule in the order given. The first rule that matches determines whether or not PINsafe authentication is required for that URL.

You can change the order of the rules by right-clicking on the list. There are options to move sets of rules to the top or bottom, to move individual rules up or down the list, or to delete rules. You also use this menu to modify an existing rule. The dialog displayed is the same as above.

Finally, you can specify what happens if the entered URL doesn't match any rules: by default, no PINsafe authentication is required. If you check the final checkbox, PINsafe authentication will be required for all URLs that don't match any explicit rules.

1.5.5 Special Consideration for Windows Server 2003 / Windows XP

The settings are saved to the Windows common data folder. In Windows Server 2008 / Windows 7 and later, this is usually **C:\ProgramData**. In Windows Server 2003 and Windows XP or earlier, it is **C:\Documents and Settings\All Users\Application Data**.

The configuration program, and the filter itself, automatically select the correct folder. However, the web page **settings.asp** has the path hard-coded. If you are using Windows Server 2003 or earlier, or if you have changed the common data folder for some reason, you need to edit settings.asp to set the correct folder for config.xml. Edit the file **C:\Program Files\Swivel Secure\Swivel IIS Filter\Web\settings.asp** and look for the following line:

```
configDoc.load("C:\ProgramData\Swivel Secure\IIS Filter\config.xml")
```

Change the file path to the correct path for your environment.

1.5.6 Reading and Saving Configurations Elsewhere

The File menu on the configuration program allows you to save a copy of the configuration elsewhere, or to read a configuration file from elsewhere. This is useful if you are configuring the filter from a different machine, or if you have multiple configurations.

Additionally, you may find that you are unable to save the configuration to the default location (C:\ProgramData\Swivel Secure\IIS Filter\). You may find that the program appears to save it, but when you check, it has not been saved there. In this case, save a copy of the configuration file (config.xml) to a different location, and then copy it to the correct location.

You will also need to do this if you have installed the configuration program on a separate computer.

1.6 Configure the ISAPI filter (Version 1.0-1.1)

This documentation applies to the older version of the filter.

1. Select Start Programs/PINsafe IIS Filter/Filter Configuration. This will look for the location of config.xml, this will be created when first used and this must be located in web/bin.

2. You will be asked to select the location of the configuration file. It is important that you select the right location. It should be in the same folder as the ISAPI filter. Initially, this file will not exist, but will be created as a result of running this configuration application.

1.6.1 PINsafeIISFilter Options

PINsafeServer: The 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 (normally 8080).

Context: The context (i.e. web application name) of the PINsafe instance on that server

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 configured earlier.

SSL enabled: Tick this box to require SSL (HTTPS) communication with the PINsafe server.

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.

Authentication: The Authentication tab contains the following settings:

Idle time (s): The time (in seconds) for which the authentication cookie will be valid if the web page is not used.

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.

Exclusions and Inclusions: Use the inclusion and exclusion tabs to enter which paths should be protected by PINsafe:

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.

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.

Misc: On the Misc tab, edit any custom paths as follows:

Default path: This is the path to which authenticated requests are directed if the login page is targeted directly. 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. Note: The logout path must be an included file location.

Virtual web path: This is the path to the PINsafe authentication pages. See the next section for details on setting this up. You should normally set this to be ?/pinsafe?, unless you have a particular reason not to.

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.

1.7 Installing the Filter on Multiple Websites

Most of the instructions above assume that you are installing the IIS filter on the single default website of a web server. However, if you want to use the filter on multiple websites on the same server, you need to carry out a few extra steps. Firstly, if all the settings on all the websites are exactly the same, you can configure it once, and then carry out the same steps to activate the filter on each website. In this case, simply save the settings to all the relevant locations.

If, however, you need different settings for each website, you will need to do the following for all except the first website:

1. Make a copy of the entire Web folder, including the bin sub-folder. You can copy it as a sub-folder of PINsafe IIS filter, with a different name, or you can put it somewhere completely different. It is important, however, that you keep the structure the same ? all the .asp files must remain intact, and the filter DLL must be in a sub-folder called ?bin?. You do not, however, have to copy the FilterConfig.exe file (but it does no harm if you do).

2. When you come to configure each filter, navigate to the bin sub-folder of the copy you have just made. Otherwise, configuration is exactly as before.

3. When selecting the IIS filter to install, and also when defining the virtual directory for PINsafe web pages, you should use the copy you have just created, rather than the original. This is important, as both the filter and the web pages look for the configuration file relative to their own location.

1.8 Testing

Browse to a web page that has been configured for protection. This should display a PINsafe login dialog:

Enter the Username.

For dual channel, enter the One Time Code:

Or click start session to enter a single channel OTC. The PINsafe log will record that a single channel session has started.

If authentication is successful it should redirect to the login page. If failed an error message will appear. The PINsafe log will record any successful log attempt for the agent.

1.9 Troubleshooting

Verify the correct filter version has been installed for the operating system i.e. 32 bit or 64 bit.

Check for error messages in the PINsafe log

Check the IIS log messages

Filter Install issues: The IIS service needs to run as an administrator in order to install the filter. Once the filter is installed, it will run as the normal user. Open the Services applet and locate World Wide Web Publishing. Select properties, then go to the Log On tab. Assuming you are logged in as an administrator, select Local System account. Then restart the service. Hopefully, this will start the filter. You can then switch back to the default account and restart again.

If you are not redirected to the PINsafe login page when trying to access a protected page, open IIS manager and check that the ISAPI filter is installed and has loaded properly (there should be a green arrow next to it, and the priority should be ?High?). If this is not the case, restart IIS, if you have not already done so, and try again. The filter doesn't try to install until you try to access a web page from that website, so try that before assuming it hasn't worked.

If the filter is listed, but showing a red cross, then it failed to start. In this case, check the error messages in the event log showing.

If the filter shows as green, with priority unknown, it may not be installed. In this case, you need to check. You can do this with a debug viewer, such as the one supplied by SysInternals (http://technet.microsoft.com/en-us/sysinternals/bb896647.aspx). Download this and run it (there's no need to install it) on the server, then restart IIS. If you don't see any messages relating to the PINsafe IIS filter, then it's not installed properly.

If the page is still not redirected, try the following:

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. Try accessing a protected page again. Hopefully this time you will be redirected.

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.

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 an virtual or hardware appliance Install

https://<pinsafe_server_ip>:8443/proxy/SCImage?username=<username>

For a software only install see Software Only Installation

If the web page is redirected to the /PINsafe/login.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 Extension.

1.9.1 Error Messages

AgentXML request failed, error: The agent is not authorised to access the server

User fails to authenticate with the above error message in the PINsafe log. An Agent on PINsafe server has not been defined for the IIS server. Go to Server/Agents in the PINsafe admin console, and add a new entry, using the IP address of the IIS server. Make sure the agent secret is the same as on the IIS filter configuration.

This installation package is not supported on this processor type. Contact your product vendor

The 32 bit version is being attempted to be installed on a 64 bit OS or the 64 bit version is being attempted to be installed on a 32 bit OS. Verify the OS version and install the correct PINsafe software version.

2 Microsoft IIS version 7 ASP.NET Forms Integration

2.1 Introduction

Swivel allows ASP.NET application authentication using Agent-XML for IIS 7 and IIS 6 ASP.NET

NOTE: the method listed here uses standard ASP.Net forms-based authentication to authenticate to PINsafe. We now have an alternative solution that uses a HTTP module. This might be an easier solution than the manual method described below, as all installation and configuration is done using provided applications. Documentation for this solution can be found here.

2.2 Prerequisites

PINsafe

ASP.NET application

ASP.NET Server

2.3 Baseline

PINsafe 3.7

IIS6 and IIS7

2.4 Architecture

The ASP.NET application makes authentication requests against the PINsafe server by Agent-XML.

2.5 ASP.NET Sample Files

ASP.NET Sample File is available here: ASP.NET Sample File

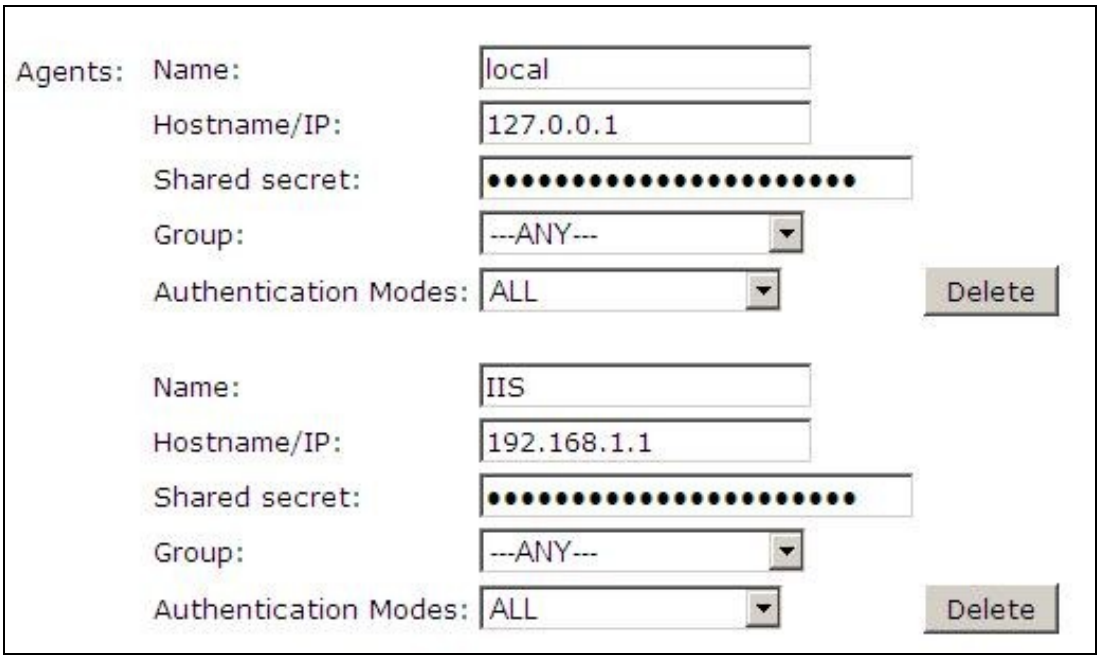
ASP.NET Sample file for 2008 server is available here: ASP.NET for 2008 Server

The pinsafe folder contains an example login page, plus aspx pages which render a TURing image or request a dual channel image.

2.6 PINsafe Configuration

2.6.1 Configure a PINsafe Agent

1. On the PINsafe Management Console select Server/Agent
2. Enter a descriptive name for the Agent
3. Enter the IP address or hostname of the server on which the ASP.NET will be running
4. Enter the shared secret used above on the ASP.NET
5. Click on Apply to save changes



Note: Session creation by username is not required for this integration as PINsafe can use session ID.

2.7 ASP.NET Configuration

2.7.1 Integrating the ASP.NET

First of all, extract the sample zip file to a temporary location. There should be 2 folders:

- App_Code
- pinsafe

and one file:

- web.config.

Copy the pinsafe folder and its contents into the ASP.NET application you want to protect or the root of the website to protect the entire website. It is important that the folder is contained within the application, and is not an application in its own right. You will need to set IIS (or other ASP.NET server) to allow anonymous access to the pinsafe folder, and you may need to modify permissions on the files to ensure that the default IIS (or other ASP.NET server) user has read access.

Copy the contents of the App_Code folder into the App_Code folder of the application or create one if it doesn't already have one.

Edit the web.config file for the application, and add the contents of the enclosed web.config in the appropriate locations. You will need to change the PINsafe server settings as appropriate.

2.7.2 Configure the web.config file

This file contains the information for communication with the PINsafe server. The options are displayed below:

PINsafeServer: The IP address or hostname of the PINsafe server or appliance

PINsafePort: The port used for communication, usually 8080

PINsafeContext: The install name of pinsafe, usually pinsafe

PINsafeSecret: The shared secret key, which must be the same as that entered on the PINsafe server

PINsafeSecure: This is if the connection to the PINsafe server is https for SSL or http. The default value is true, which is for https

PINsafePassword: This is to display the password field, the default value of false will not display a password field

PINsafeImage: This is to display a button to generate a Single Channel Image of the security string

PINsafeMessage: This is to display a button to generate a Dual Channel security string to be sent to the user

PINsafeAcceptSelfSigned: If self signed certificates are accepted, defualt is yes

NOTE: As the requests are made using Agent-XML, they must be made to the pinsafe appliance on port 8080 and the context of pinsafe and not the proxy port of 8443. Security is usually provided by the IIS server proxying the request to the PINsafe server.

Default Settings, suitable for a software install of PINsafe are:

```
<add key="PINsafeServer" value="pinsafe_server" />
<add key="PINsafePort" value="8080" />
<add key="PINsafeContext" value="pinsafe" />
<add key="PINsafeSecret" value="secret" />
<add key="PINsafeSecure" value="true" />
<add key="PINsafePassword" value="false" />
<add key="PINsafeImage" value="true" />
<add key="PINsafeMessage" value="false" />
<add key="PINsafeAcceptSelfSigned" value="true" />
```

Appliance settings are likely to be:

```
<add key="PINsafeServer" value="pinsafe_server" />
<add key="PINsafePort" value="8080" />
<add key="PINsafeContext" value="pinsafe" />
<add key="PINsafeSecret" value="secret" />
<add key="PINsafeSecure" value="true" />
<add key="PINsafePassword" value="false" />
<add key="PINsafeImage" value="true" />
<add key="PINsafeMessage" value="false" />
<add key="PINsafeAcceptSelfSigned" value="true" />
```

2.7.3 Additional web.config file IIS7 Options

The loginUrl setting assumes that you are protecting the entire website. If you are only protecting an application, add the path for that application to this URL. For example, to protect an application with URL "/secure", loginUrl="/secure/pinsafe/Login.aspx".

The <modules> section is not relevant if you are protecting an application that is ASP.NET only. These changes allow ASP.NET authentication to be used for static web pages as well as .aspx pages. This is a new feature of IIS7.

2.7.4 Enabling Authentication

For IIS, open the IIS manager, locate the website or application that you are protecting, and double-click the Authentication icon. Make sure that anonymous authentication is disabled, and that forms authentication is enabled, and the URL is as set earlier. Go to the pinsafe sub-folder, select Authentication under there, and make sure anonymous authentication is enabled (you need to be able to access the login pages anonymously).

2.8 Additional Configuration Options

2.9 Testing

Navigate to the login page. Attempting to login with a correct username and password but no one time code should result in failure. Only when a correct PINsafe one time code is entered should the user be logged in. If the Single Channel button is displayed then an image should appear.

2.10 Troubleshooting

To verify the Single Channel Image works, on the ASP.NET server enter the following into a web browser, which should display a Turing image if the sever is functioning correctly:

For a PINsafe appliance install:

https://<pinsafe_server_ip>:8080/pinsafe/SCImage?username=test

For a software only install see Software Only Installation

2.11 Known Issues and Limitations

Requesting a Security String Index would require modification of the login page for an existing button. See also Multiple Security Strings How To Guide

2.12 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

3 Microsoft IIS version 7 ASP.NET Integration

3.1 Introduction

This solution uses ASP.Net technology, specifically an HTTP Module, to protect specified web pages using Swivel authentication.

NOTE: the method listed elsewhere uses standard ASP.Net forms-based authentication to authenticate to PINsafe. The solution described on this page is simpler to install and maintain, but if you are familiar with forms-based authentication and want more control over the look and feel of the login page, you may prefer the alternative solution.

3.2 Prerequisites

PINsafe server version 3.6 or later

ASP.NET application running on Microsoft IIS version 7 (or later). The latest release is compatible with Server 2012 R2 IIS 8.5 and with Server 2016 IIS 10.0. Testing on Windows Server 2019 pending.

Versions: Latest Version 2.3.2.0 available from here. This version fixes several reported vulnerabilities relating to redirecting after login and same-site cookies. It requires Microsoft.Net framework 4.8 or later, and ASP.Net 4.0.

Version 2.2.1.1 available from here. This version is compatible with the Microsoft.Net framework version 4.5 or later, and ASP.Net 4.0.

Version, 2.1.1.1, available from here. This version is compatible with Microsoft.Net framework version 4.0 or later, but does not support TLS versions higher than 1.0, so should only be used in Windows Server 2008 R1, which doesn't have native TLS 1.1/1.2 support.

3.3 Architecture

A HTTP module is installed into a specific ASP.Net application, where it checks all incoming requests. Any request requiring PINsafe authentication will be redirected to the Swivel login page, unless the user has already been authenticated to PINsafe.

3.4 PINsafe Configuration

3.4.1 Configure a PINsafe Agent

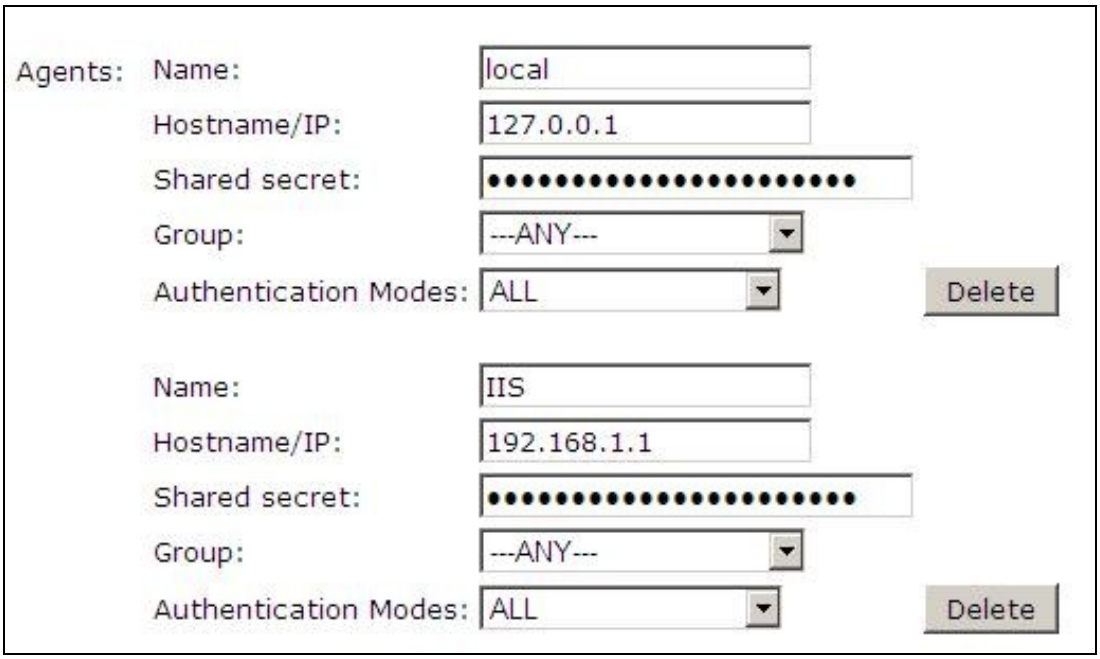
1. On the PINsafe Management Console select Server/Agent

2. Enter a descriptive name for the Agent

3. Enter the IP address or hostname of the server on which the ASP.NET will be running

4. Enter the shared secret used above on the ASP.NET

5. Click on Apply to save changes



Note: Session creation by username is not required for this integration as PINsafe can use session ID.

3.5 Filter Installation

To install the filter, simply run the executable program found in the downloadable zip file. You can generally accept the default recommendations, unless you have reason to change them.

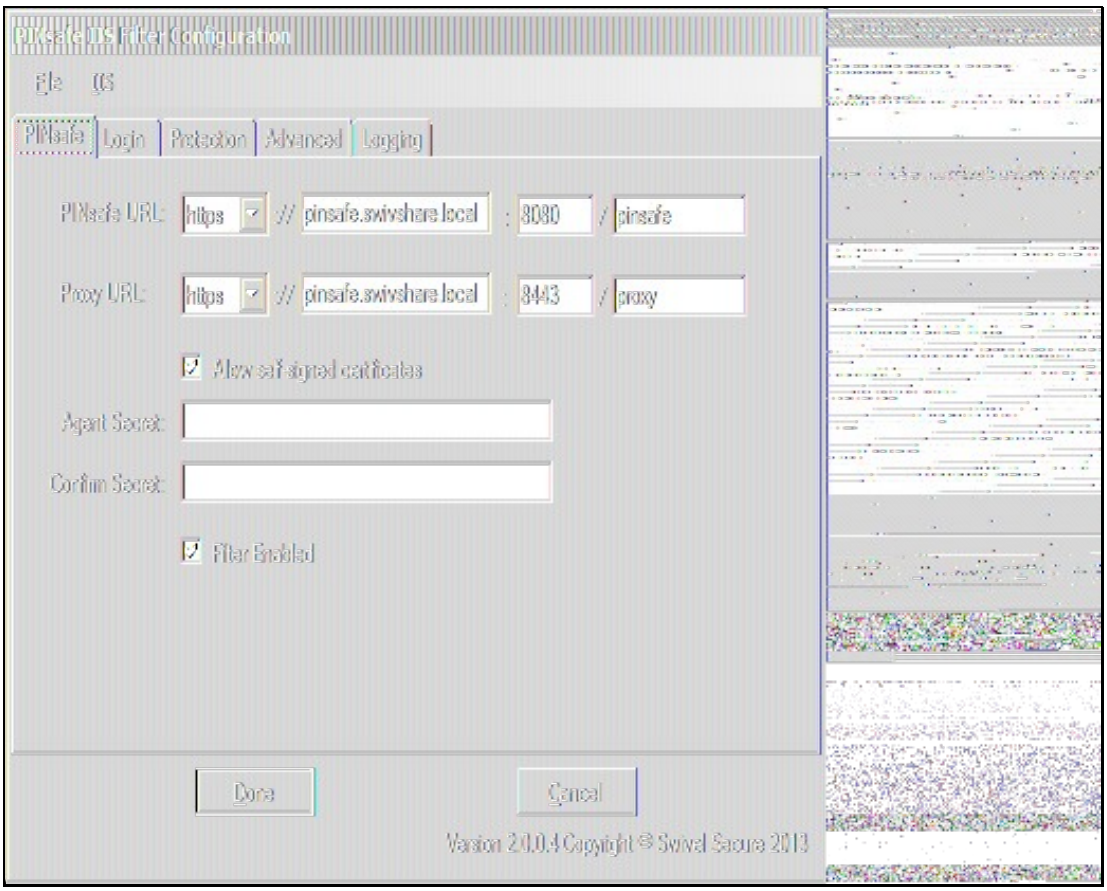
Once the filter is installed, you will be taken to the configuration program (unless you choose not to do so yet).

3.6 Filter Configuration

The filter configuration program enables you to set up which PINsafe server to use for authentication, and also the rules governing which URLs need PINsafe authentication.

The program displays a form with multiple tabs. The tabs are described in separate sections below.

3.6.1 PINsafe Tab



On this page, you define the PINsafe server settings used for authentication.

Firstly, you define the URL for the PINsafe server, as used to authenticate users.

Secondly, you define the URL for the proxy server, used to deliver single channel images (TURing or PINpad) or dual channel on-demand messages. This may be the same as the PINsafe URL - typically the host name or IP address will be the same. However, if you have an virtual or hardware appliance running PINsafe 3.8 or earlier, PINpad is not available directly from PINsafe. You need to install a recent version of the proxy application, in which case the port and context should be ":8443/proxy", rather than the usual ":8080/pinsafe". These settings will always work for any version of the virtual or hardware appliance. If you have a PINsafe version 3.9 or newer, or are not using PINpad, you can safely use ":8080/pinsafe" for both.

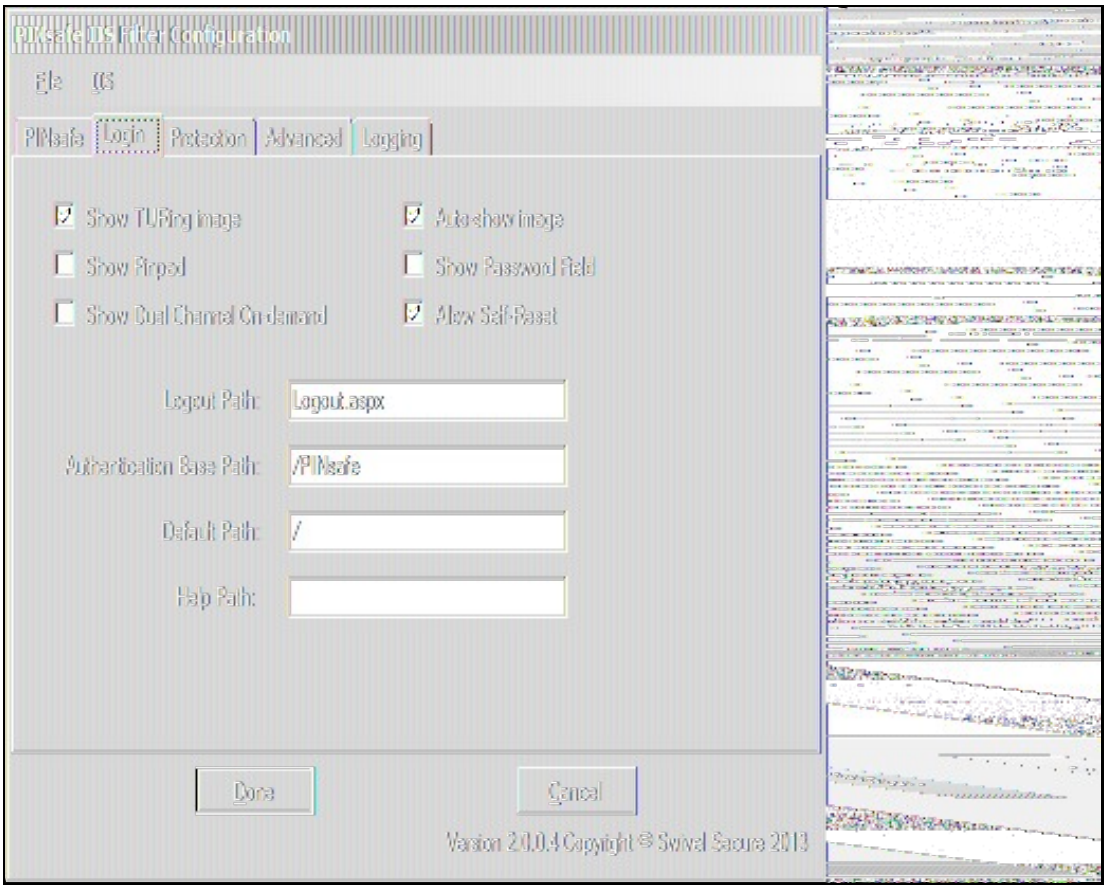
Note that the URLs only need to be resolvable and accessible from the web server. Direct access for the end user to the PINsafe server is not required - the filter proxies all requests.

The next option is "Allow self-signed certificates". If you are using https (recommended), and have specified an IP address for the PINsafe server (not recommended), or have a self-signed or untrusted SSL certificate (not recommended), you need to check this option. For production use, it is recommended that you install a certificate on the Swivel virtual or hardware appliance with the fully-qualified name that you are using to connect to it. If the Swivel virtual or hardware appliance is not visible externally, the certificate can be self-signed or signed by an internal certificate authority, and you can install the signing authority certificate as a trusted certificate on the web server. This is the recommended solution for production use.

Next, you need to enter the Agent secret, which you entered on the PINsafe Agent definition earlier. Enter it twice to confirm it.

The final option on this tab enables or disables the filter. Should you wish to disable the filter temporarily for any reason, you can do this for all websites on this server using this checkbox.

3.6.2 Login Tab



This tab allows you to control the login page used to authenticate to PINsafe.

The 3 checkboxes on the left-hand side allow you to display TURing image, PINpad or a dual-channel on-demand button. You can't have both TURing and PINpad at the same time, but either one can be combined with dual-channel on-demand.

Auto-show image, if checked, will display the TURing image or Pinpad as soon as the username has been entered and the focus moves away from it. This doesn't affect dual-channel on-demand - you always need to click the button for this.

Show Password Field, if checked, will display a password field as well as the OTC field. You only need this if PINsafe passwords are enabled, or the Agent is configured to check the repository password.

Allow self-reset, if checked, will display a link for the self-reset page on the login page. **NOT IMPLEMENTED IN THIS VERSION**.

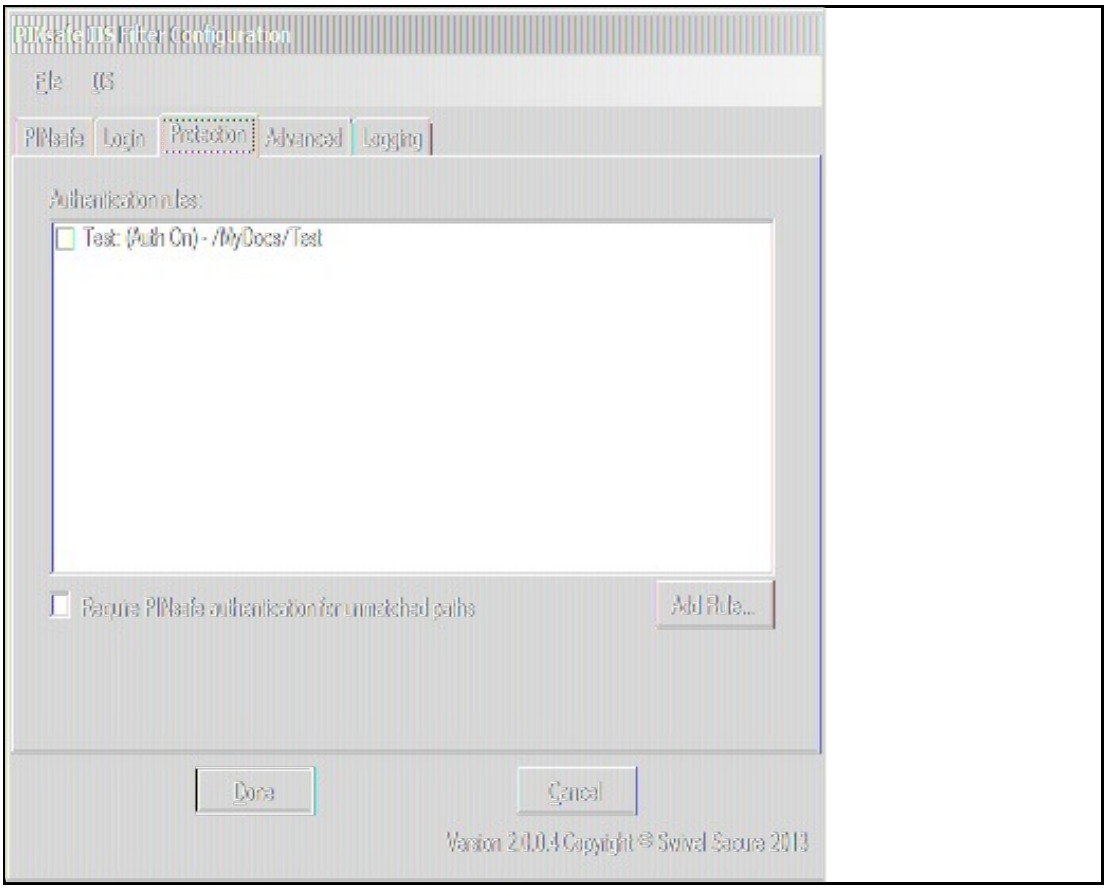
Logout path is the full path used to log out from PINsafe. Typically, this will be /PINsafe/Logout.aspx. If this is detected in the URL, the PINsafe authentication cookie will be removed, and users must re-authenticate to access protected URLs.

Authentication Base Path is the path containing the PINsafe login pages. It will be used when deploying to a web application as the virtual directory. The default is "/PINsafe", and typically you should not need to change this.

Default Path is the path to which the user is redirected after authentication if no source path is provided - for example, if the user navigates directly to the login page. Typically, the user attempts to access a page directly, and is redirected to the login page, with the intended page as the source path.

Help Path is a path to a help file describing how to authenticate to PINsafe. Swivel do not provide such a page, but if the customer wishes to do so, they can enter it here, and a link will be provided on the login page. **NOT IMPLEMENTED IN THIS VERSION**.

3.6.3 Protection Tab

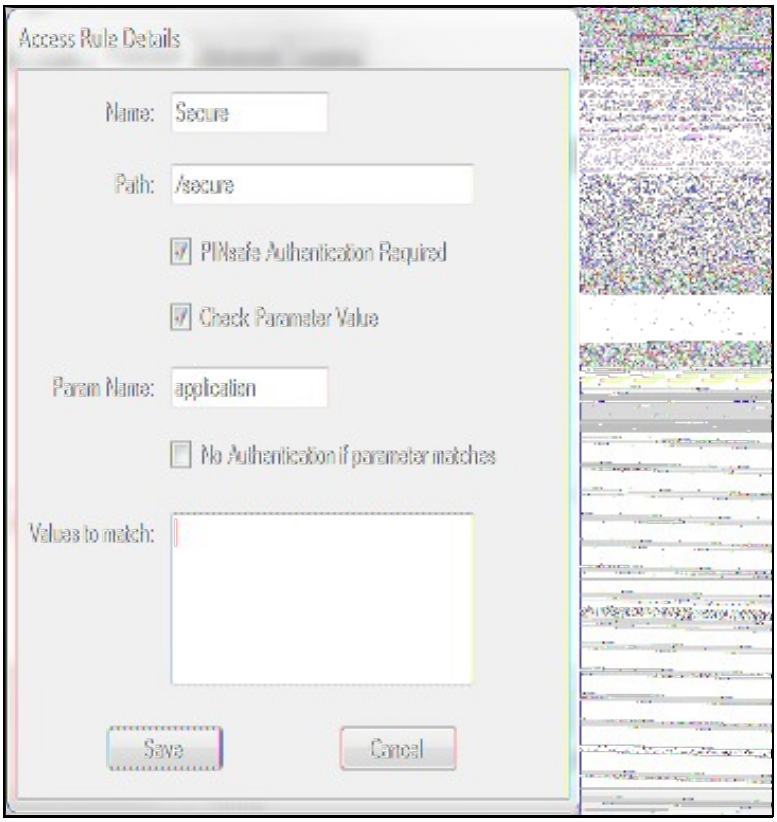


On this page, you specify which paths should require PINsafe authentication. You do this by defining a list of rules. Each rule is a path to be matched, with a flag indicating whether or not PINsafe authentication is required. The filter runs through the rules in order until it matches one, and determines whether or not to check for PINsafe authentication according to that rule.

If no rules match, the default rule can either specify that PINsafe authentication is required or is not required.

NOTE: if you specify the default rule to require PINsafe authentication, make sure that any paths used by the login page are excluded. In particular, you will need a rule for the authentication base path (e.g. "/PINsafe") that does NOT require PINsafe authentication. This is not necessary if the default rule does not require PINsafe authentication.

You can create new rules by clicking the "Add Rule" button. The following dialog appears:



The name is just a label for the rule - it has no intrinsic meaning.

Path is the path that must be matched. By default, the path specified must match the **START** of the request path, so must start with "/": for example, "/secure" will match "/secure/default.aspx" or "/secure/subite/default.aspx", but not "/home/secure/default.aspx". However, if you start the path with a "*", it will match the **END** of the request path: for example "*/default.aspx" will match any page called "default.aspx" anywhere in the website.

"PINsafe Authentication Required" indicates whether or not this rule requires PINsafe authentication.

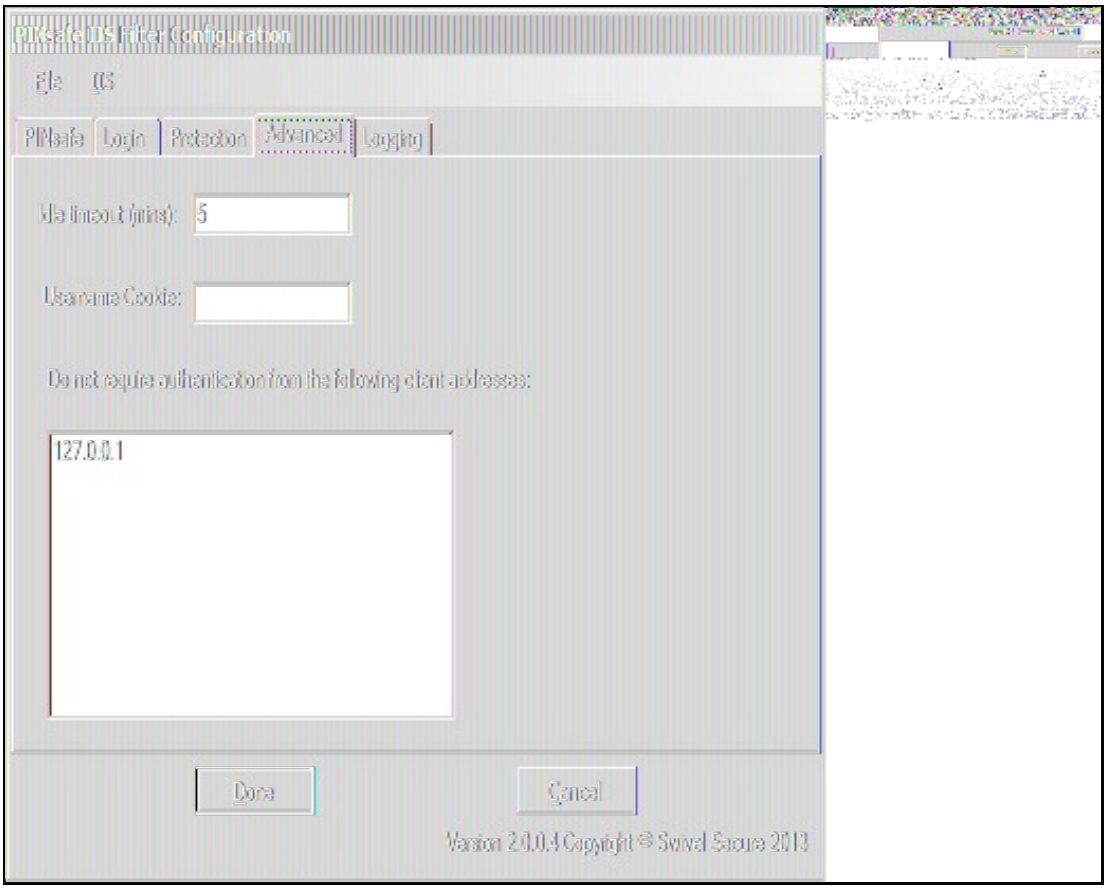
"Check Parameter Value" allows finer control over PINsafe authentication. When checked, you can specify the name of a single query parameter that is checked to determine whether or not PINsafe authentication is required. You can specify a list of possible values for the parameter, but if you specify no values, the presence or absence of the parameter determines whether or not to require authentication.

The final control on this page, "No Authentication if parameter matches", allows you to reverse the parameter check. So for example, if the rule requires authentication, but this option is enabled, PINsafe authentication is required UNLESS the parameter value matches one of the specified values.

A final note of clarification: the rule is matched purely on the path, not on the parameters. Specifying "Check Parameter Value" only allows you to change whether or not authentication is required.

Going back to the main form and the list of rules, to change a rule, change the order of rules, or delete rules, check the rules you want to move/change/delete and right-click to bring up a context menu.

3.6.4 Advanced Tab



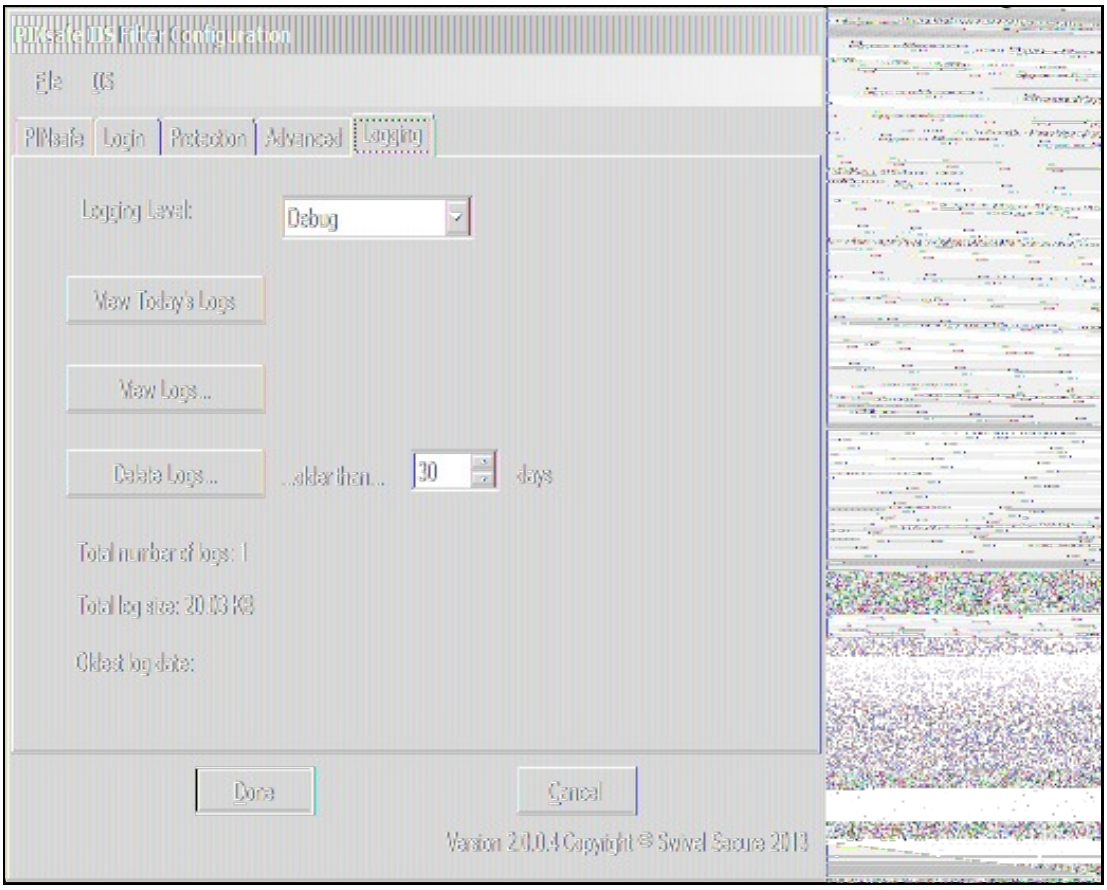
There are 3 settings on this tab:

Idle timeout: this specifies how long the PINsafe authentication cookie is valid if the web page is not refreshed. The default is 5 minutes. If the page is idle for more than 5 minutes, you will need to re-authenticate. You can make this longer if you wish. Note that this doesn't mean that you have to reauthenticate after every 5 minutes - only if you do not refresh the page (or view a different page). Every time a request is made to the website, the timeout resets.

Username cookie: this is provided for additional web development. If you specify a name here, the filter will provide a cookie with the name of the authenticated PINsafe user. **NOT IMPLEMENTED IN THIS VERSION**.

Excluded clients: the final option allows you to specify that PINsafe authentication is not required if the request comes from specified client IP addresses.

3.6.5 Logging Tab

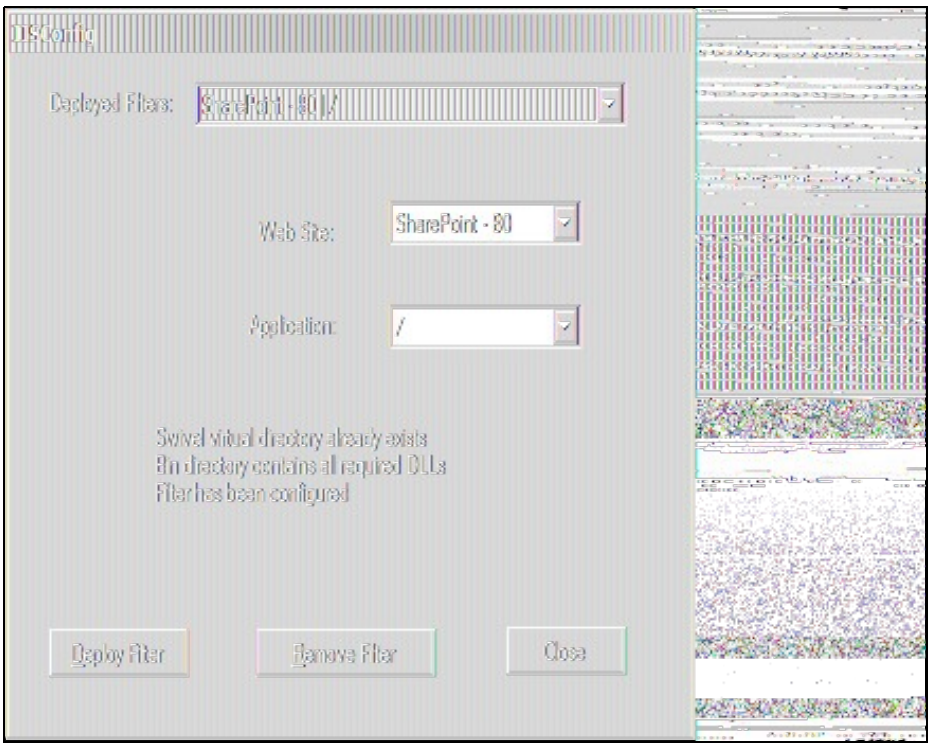


This page allows you to specify what logging the filter does, and to view or delete logs.

There are 4 logging levels: Debug, Info, Error and None. The most verbose, Debug, logs all activity, and all pages checked. Info logs only when a redirect to the login page occurs. Error only logs error events. None disables all logging.

3.6.6 IIS Configuration

None of the option specified above have any effect on any website until the filter is deployed to the website. To do this, Select the IIS menu option, then the Configure sub-menu. The following dialog is displayed:



The first drop-down lists all websites where the filter has been deployed. Initially, therefore, it is empty. If you have already deployed to a website, you can select it to check the status.

The second drop-down lists all websites on the current server. Select one to enable the application drop-down.

The third drop-down list all web applications on the selected website. Select one to check, deploy or remove the filter.

One you have selected a web application, you can choose to deploy or remove the Swivel filter.

3.7 Additional Configuration Options

3.8 Testing

Navigate to the login page. Attempting to login with a correct username and password but no one time code should result in failure. Only when a correct PINsafe one time code is entered should the user be logged in. If the Single Channel button is displayed then an image should appear.

3.9 Troubleshooting

To verify the Single Channel Image works, on the ASP.NET server enter the following into a web browser, which should display a Turing image if the sever is functioning correctly:

For a PINsafe virtual or hardware appliance installs:

https://<pinsafe_server_ip>:8080/pinsafe/SCImage?username=test

For a software only install see Software Only Installation

3.10 Known Issues and Limitations

Requesting a Security String Index would require modification of the login page for an existing button. See also Multiple Security Strings How To Guide

3.11 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

4 Microsoft IIS version 7 Integration

4.1 Overview

This document outlines the steps required to integrate the Internet Information Server (IIS) with Swivel using dual or single channel authentication. The Swivel install requires configuring an agent on the Swivel server and setting up a shared secret with the IIS server to allow communication for authentication. An ISAPI filter installed on the IIS server allows access to protected resources through the Swivel authentication.

NOTE: This document refers to the version of the filter numbered 1.2, and the configuration application with the same version number. 32-bit and 64-bit versions of the filter are available. Version 1.3.4, with PINpad support, is available for 64-bit only.

If Windows 2008 Server server is being used, or only ASP.Net applications are being protected an alternative authentication is available, see Microsoft IIS version 7 ASP.NET Integration

4.2 Prerequisites

Internet Information Server on Windows server 2008, 32-bit or 64-bit operating system.

Swivel server

The appropriate Swivel ISAPI filter software can be downloaded from here, depending on your operating system:

The latest release is version 1.3.9. Support for PINpad is included from 1.3.0 onwards. Version 1.3.4 adds PINpad support for change PIN as well:

- 64-bit ISAPI Filter
- 32-bit ISAPI Filter

These links refer to version 1.2 of the filter, provided for legacy purposes.

- 32-bit ISAPI Filter
- 64-bit ISAPI Filter

4.3 IIS Filter Version History

1.2 32 bit and 64 bit

1.3.3 (64-bit only): PINpad support added

1.3.4 (64-bit only): added PINpad support for ChangePIN

1.3.5 (64-bit only): enhancements to ChangePIN support

1.3.6 (64-bit only): added a default logout page

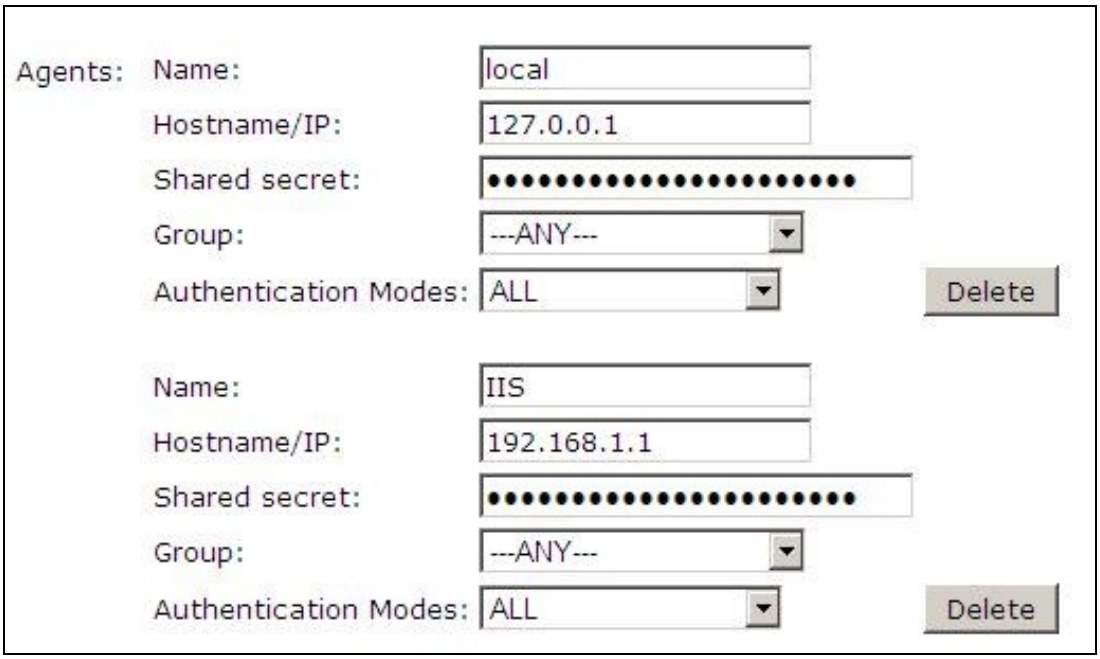
1.3.7-9: various bug fixes

4.4 Swivel Configuration

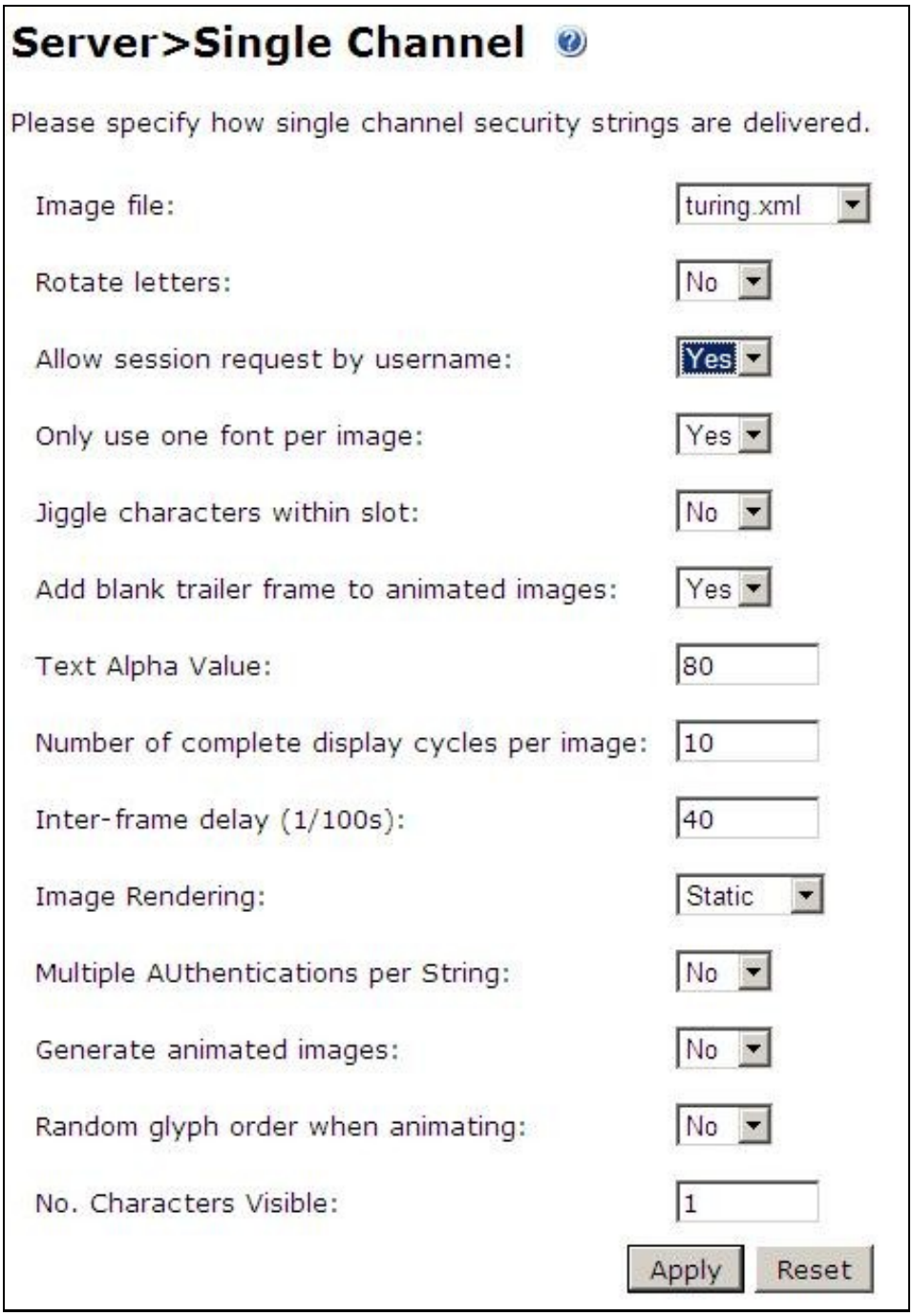
On the Swivel server configure the agent that is permitted to request authentication. On the Swivel Administration Console select from the server menu Agents and enter the details of the IIS server IP address and a shared key, then click on apply.

Example:

```
Name : IIS server 1,
Hostname/IP : 192.168.1.1,
shared secret : secret
```



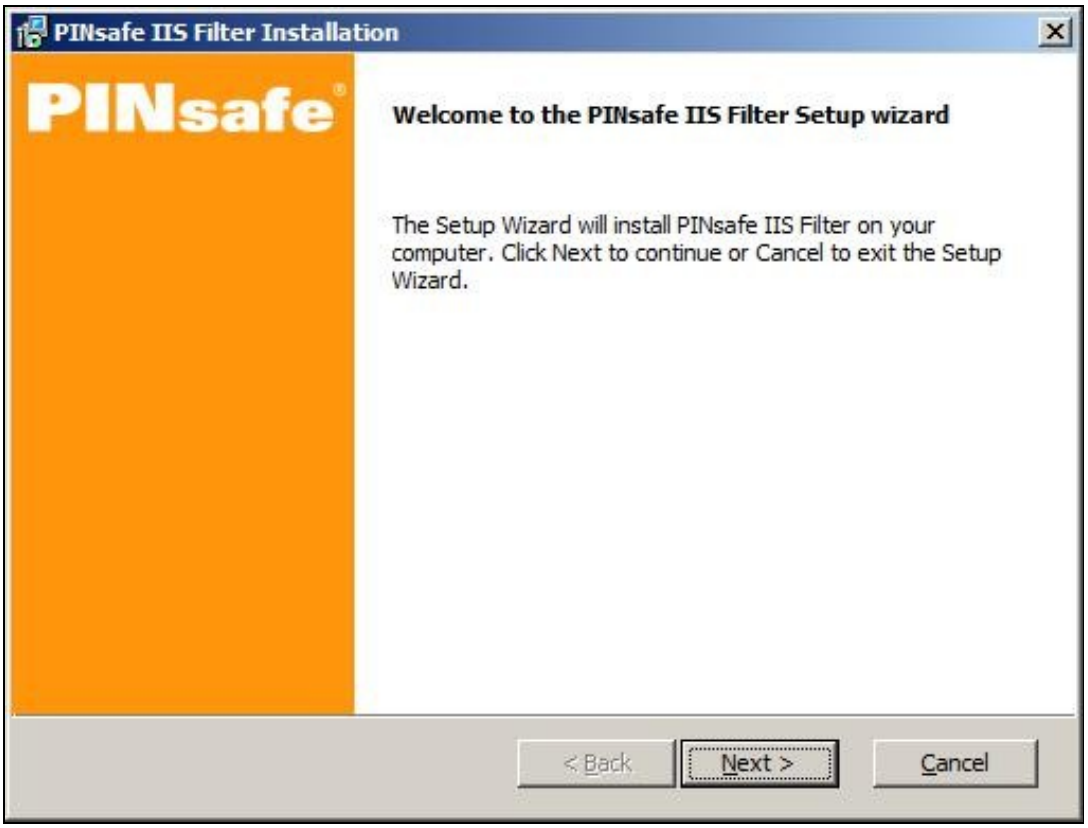
If Single Channel communication is to be used, select from the Swivel Administration Console Single Channel, and set the Allow image request by username to Yes then click on apply.



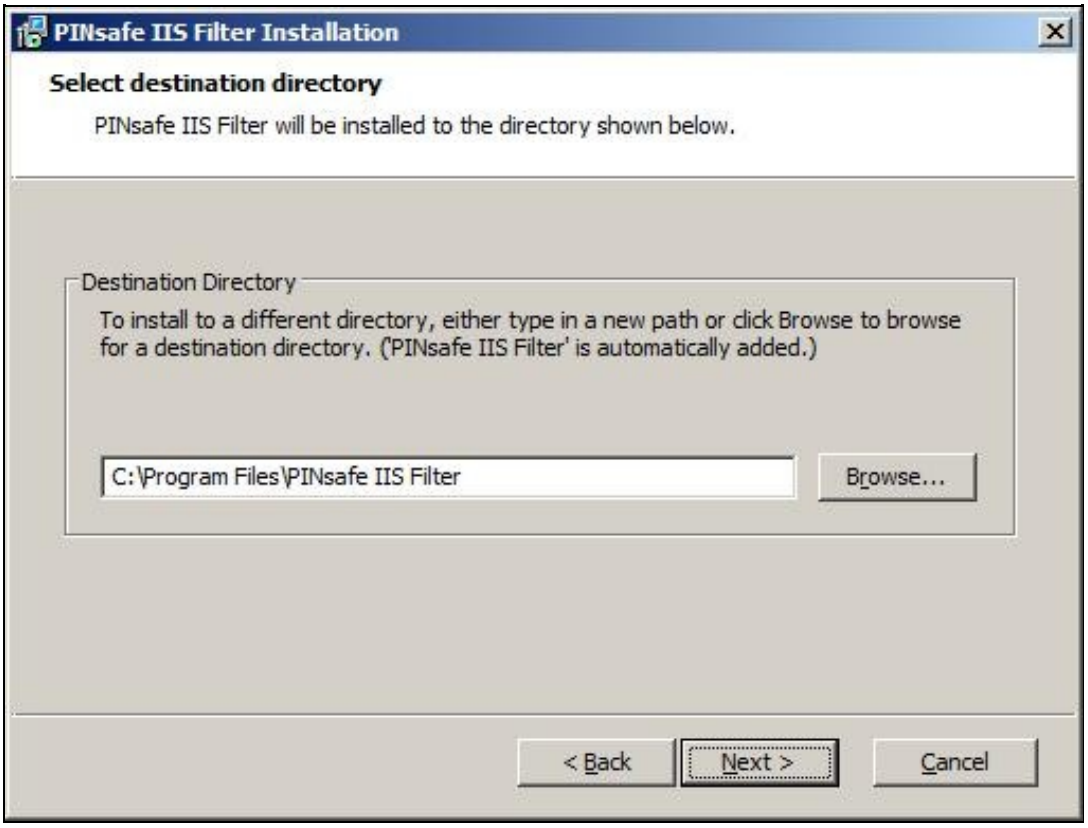
4.5 Configuring the IIS Server

4.5.1 Install the Swivel Filter

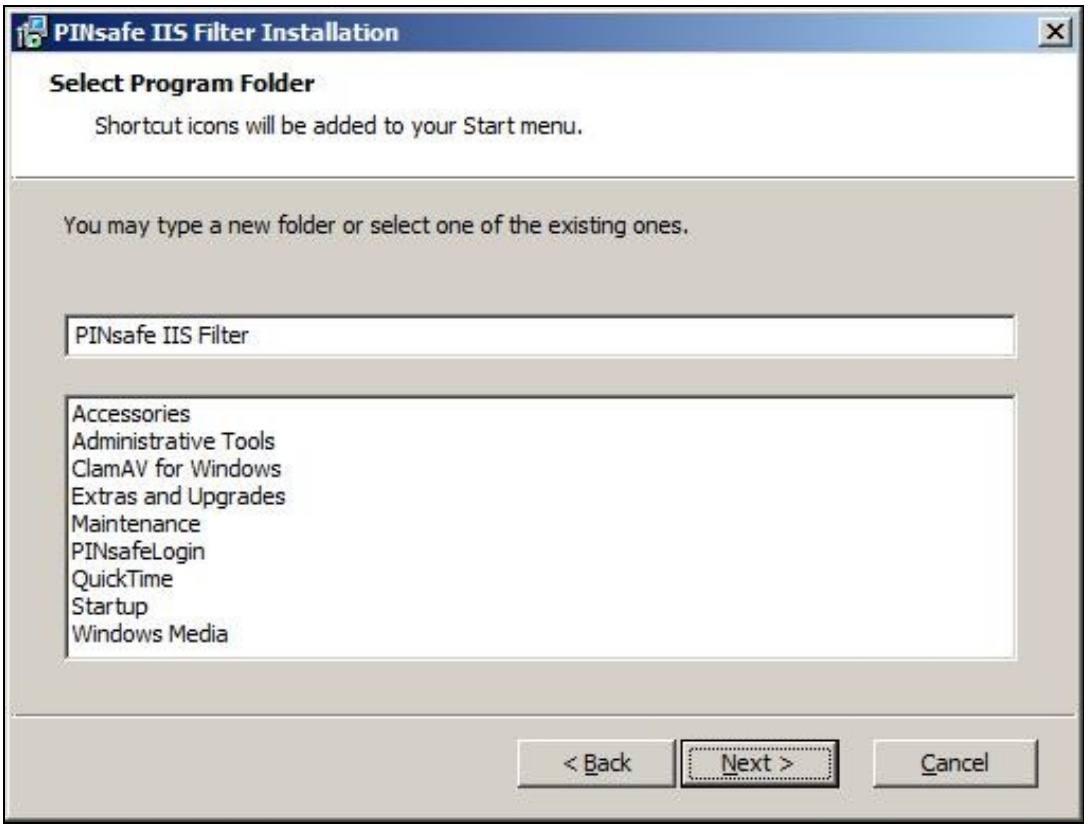
1. On the IIS server run the PINsafeISFilter.exe. The IIS filter may need to be run as an Administrator user (The filter needs to be installed by IIS running as Administrator user but it can run as a normal user).



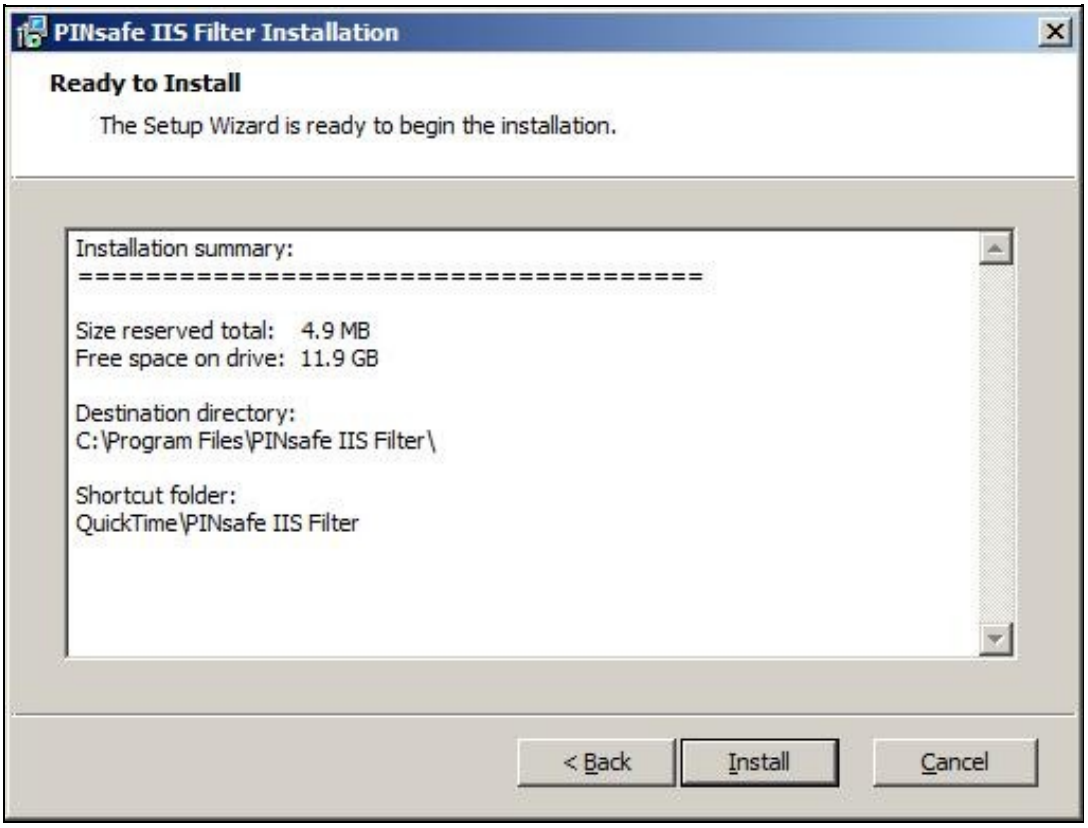
2. Choose the Path to Install to such as C:\Program Files\PINsafe IIS Filter



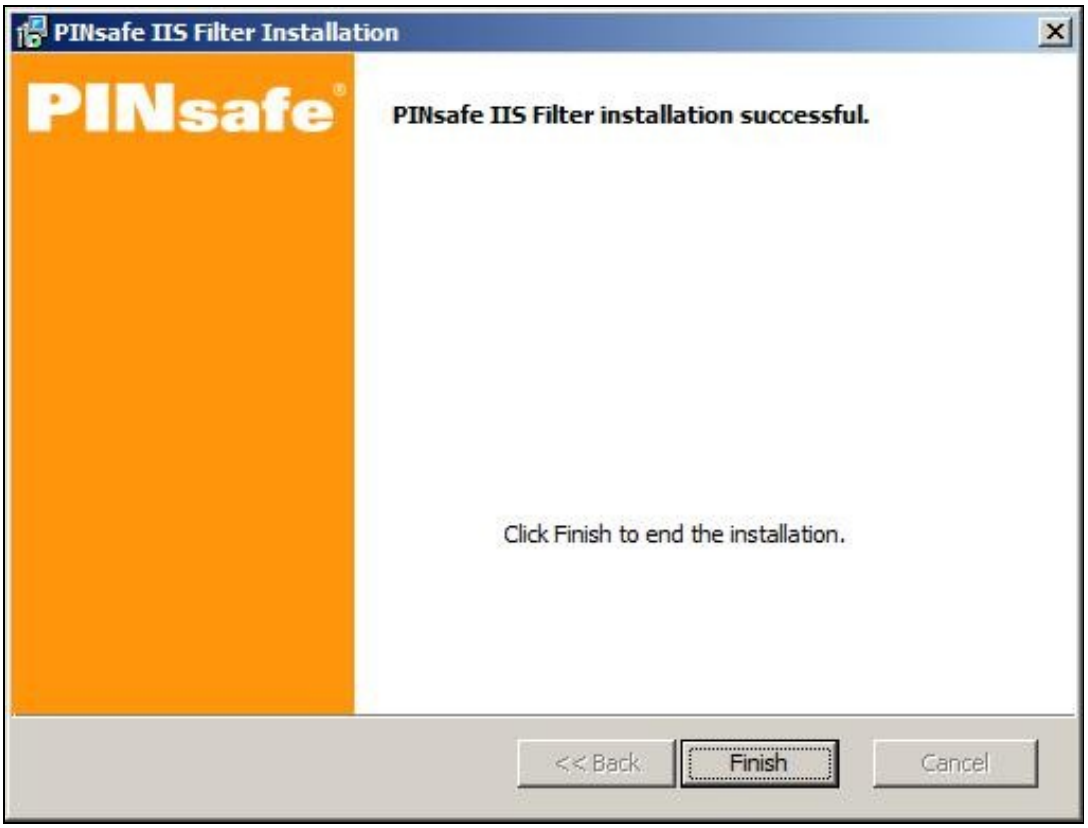
3. Select Start Menu Folder



4. When details are correct click on Install

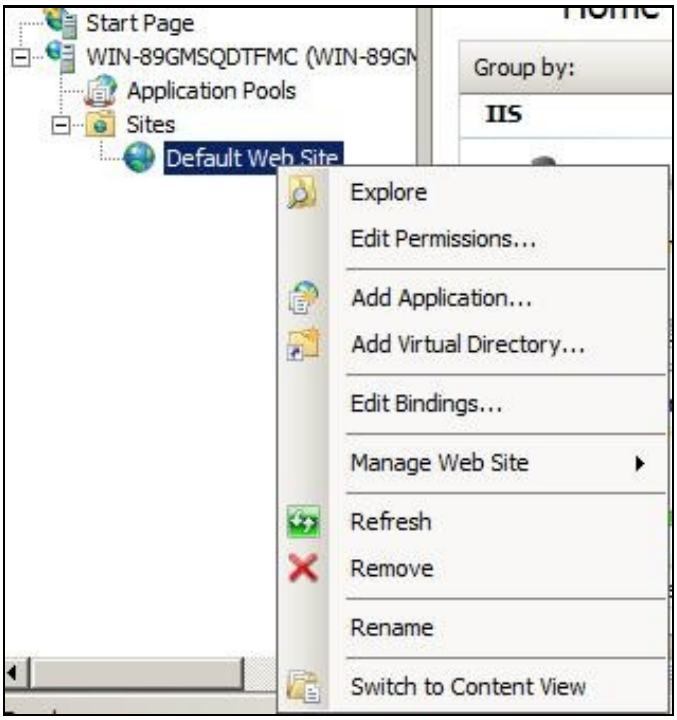


5. If the error ?Incorrect Command Line Parameters? is seen click on OK

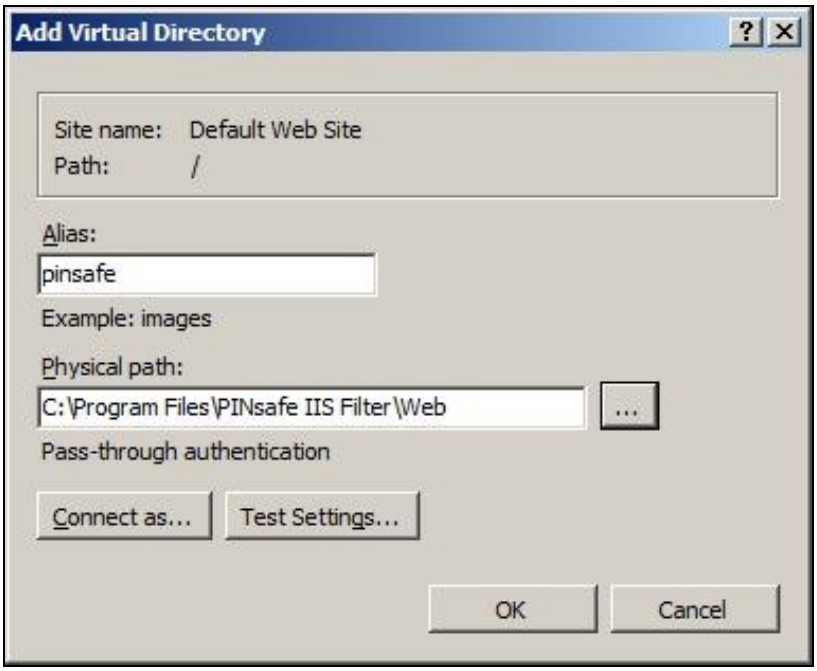


Create a PINsafe virtual directory

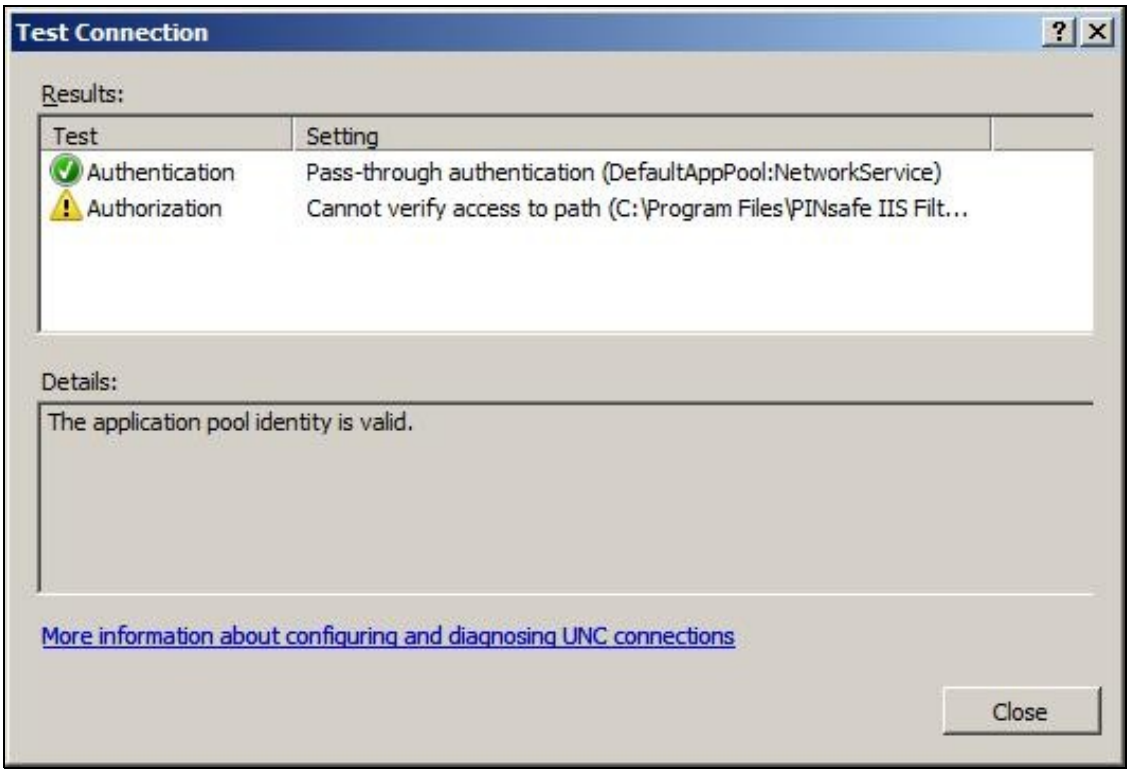
1. On the Internet Information Services Manager right click on the website and select Add Virtual Directory



2. Create an Alias called PINsafe



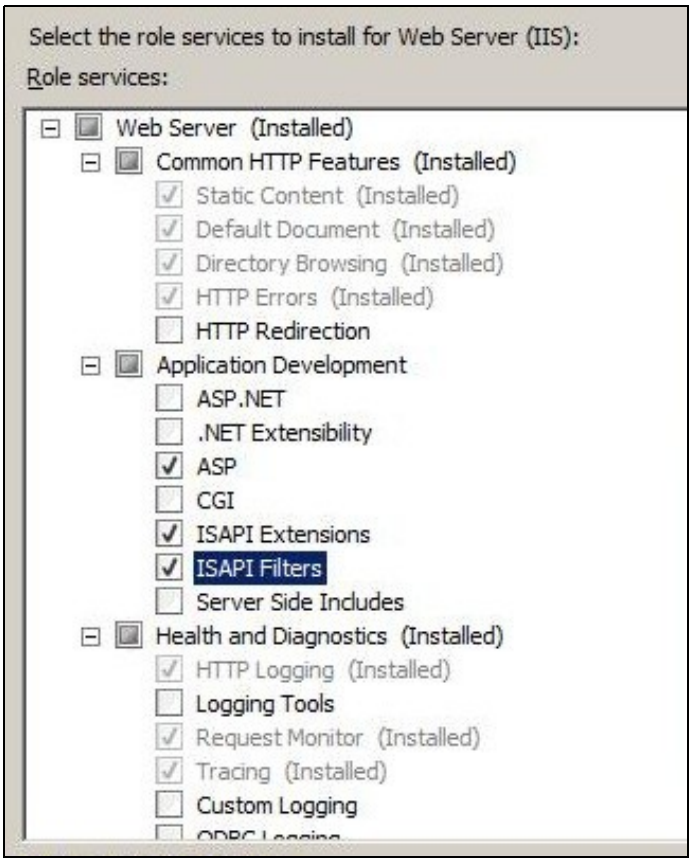
3. Point the path to the PINsafe directory Web folder, by default C:\Program Files\PINsafe IIS Filter\Web. Test Connection verifies the path, and Connect As allows Application User for pass through authentication.



4. Set the permissions to Read and Run Scripts

4.5.2 Installing the ISAPI Filters, extensions and ASP on IIS

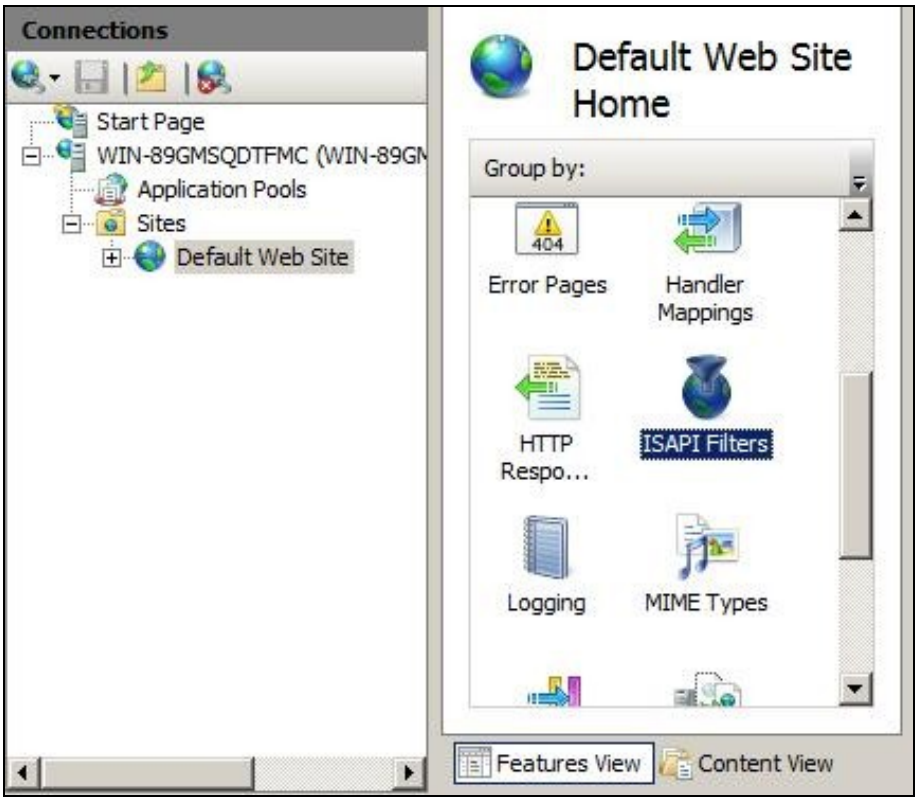
This requires the ISAPI filters, ISAPI extensions and ASP to be installed. To verify or install these, for Windows 2008, on the IIS server start the Server Manager by selecting Start/Administrative Tools/Server Manager then expand the tab for Roles, click on the Web Server (IIS), then look under Role Services to ensure that the *ISAPI Filters*, *ISAPI Extensions* and ASP are installed. If it is not click on Add Role Services and add them.



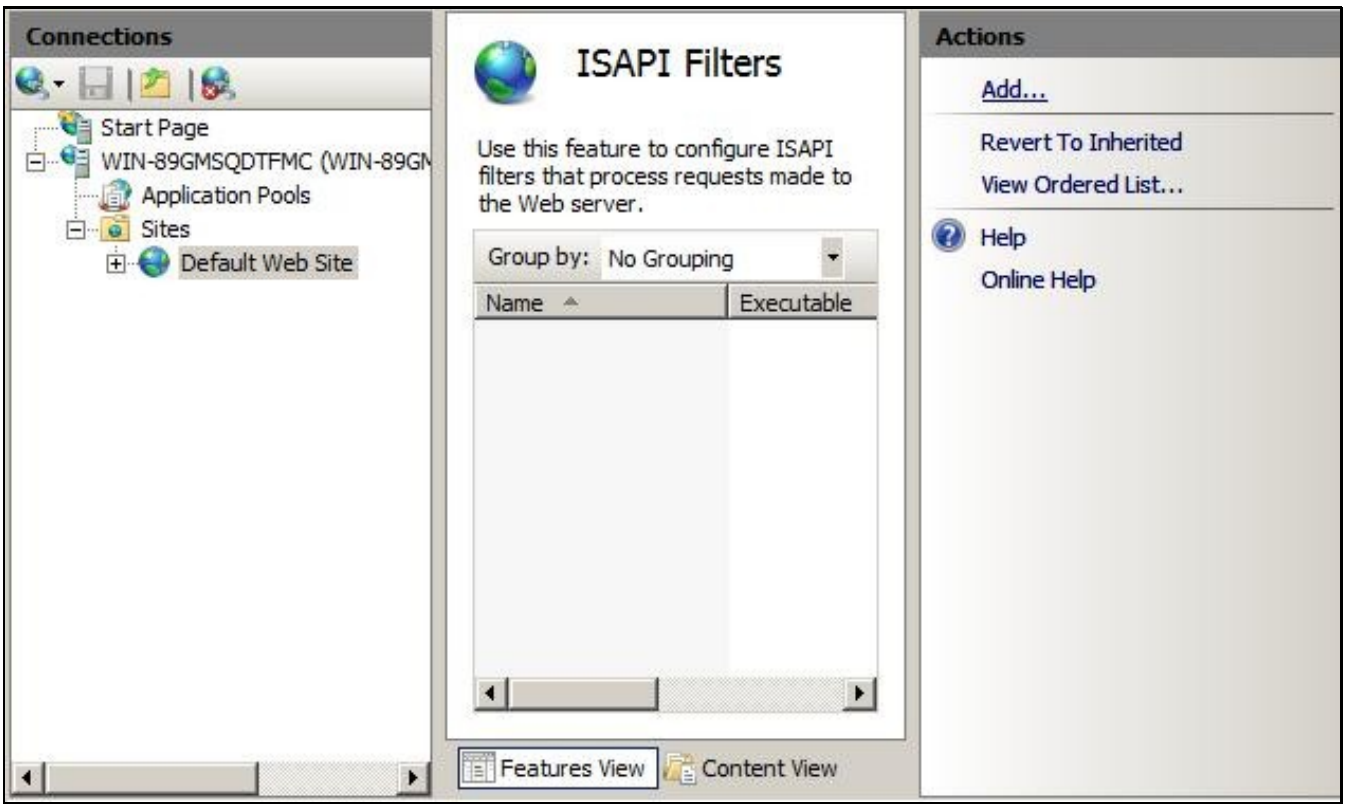
4.5.3 Install the Swivel ISAPI Filter

1. On the Internet Information Services Manager Select the website

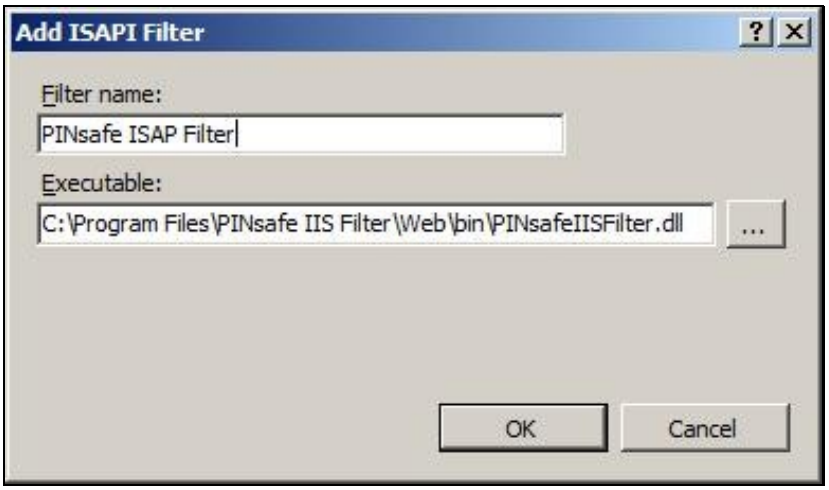
2. Select ISAPI filters by double clicking on the ISAPI filters icon



3. Under Actions select Add



4. Select the Path to the Swivel ISAPI filter. Note that the actual file you require will be PINsafeIISFilter.dll, located in the sub-folder Web\bin of the installation folder. Enter a name for the Filter such as *PINsafe ISAPI Filter*. When information is complete click on Ok.



5. Ensure the Swivel ISAPI filter is the top filter by selecting the 'View Ordered List...'

4.5.4 Configure the ISAPI filter

1. Select Start Programs/PINsafe IIS Filter/Filter Configuration. This will look for the location of config.xml, this will be created when first used and this must be located in web/bin.

Note: If the Swivel Filter Configuration does not exist in the Start Menu, it can be started by running it from its install location. The default install location is C:\Program Files\PINsafe IIS Filter\Web\bin\ConfigApp.exe

2. You will be asked to select the location of the configuration file. It is important that you select the right location. It should be in the same folder as the ISAPI filter. Initially, this file will not exist, but will be created as a result of running this configuration application.

PINsafeIISFilter Options

PINsafeServer: The PINsafe Server tab contains settings which define the Swivel server which will be used to authenticate users.

Hostname/IP: The name or IP address of the Swivel server.

Port: The port number used by the Swivel server (normally 8080, or 8443 for HTTPS).

Context: The context (i.e. web application name) of the Swivel instance on that server

Secret: The common secret used to communicate with the Swivel server. This value must be the same as the secret defined for the Swivel agent configured earlier.

SSL enabled: Tick this box to require SSL (HTTPS) communication with the Swivel server.

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.

Authentication: The Authentication tab contains the following settings:

Idle time (s): The time (in seconds) for which the authentication cookie will be valid if the web page is not used.

Username header: The name of a cookie which will pass the username of the authenticated Swivel 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 Swivel password as well as OTC.

Permit self-reset: Indicates that the user self-reset page should be enabled.

Exclusions and Inclusions: Use the inclusion and exclusion tabs to enter which paths should be protected by Swivel:

Included paths: This is a list of paths within the current website which require Swivel 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.

Excluded paths: This is a list of paths within the current website which should be exempt from Swivel 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 Swivel.

Excluded addresses: This is a list of IP addresses which are exempt from Swivel authentication. All requests from these addresses are passed through without authentication.

Misc: On the Misc tab, edit any custom paths as follows:

Default path: This is the path to which authenticated requests are directed if the login page is targeted directly. 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.

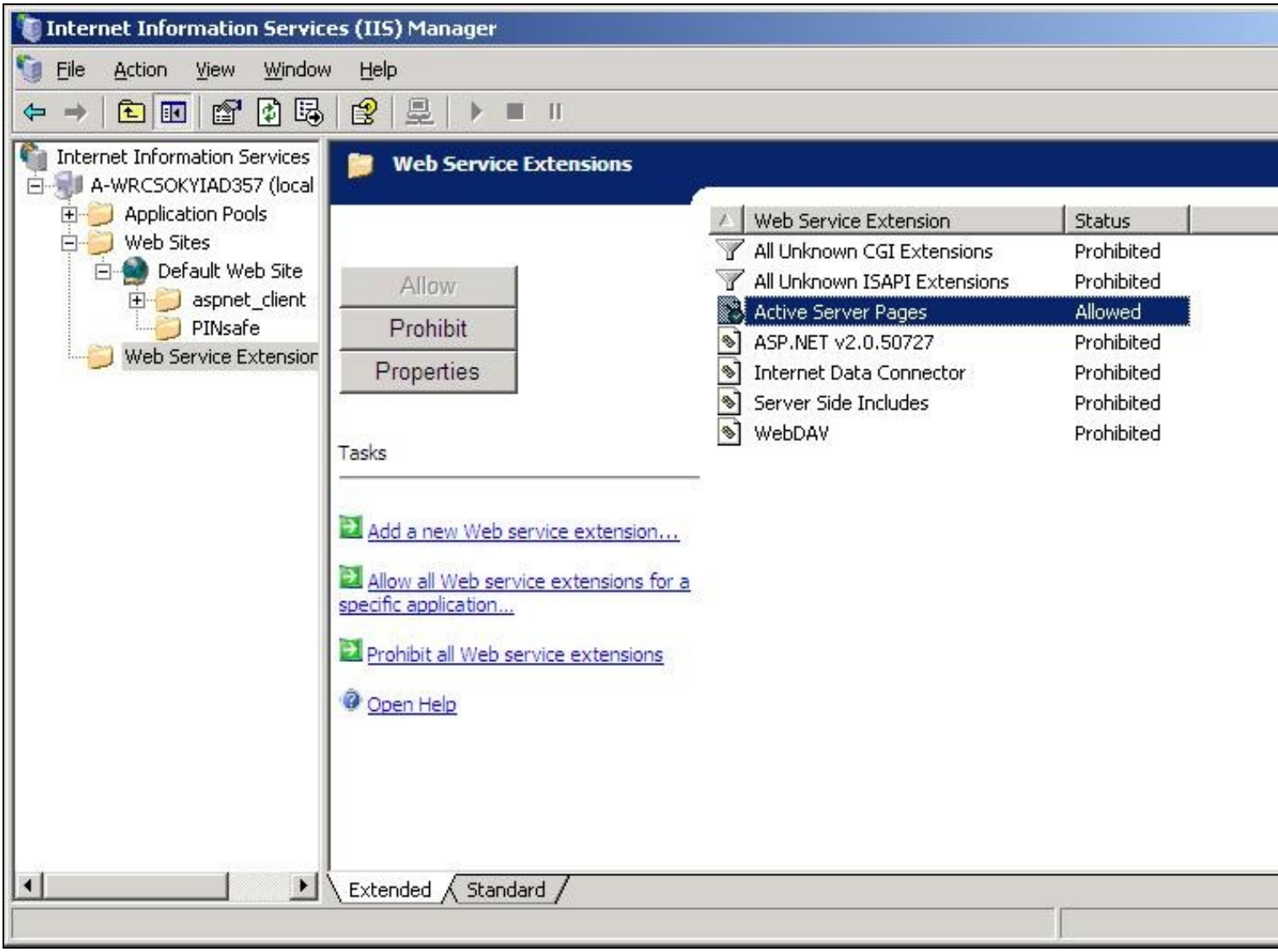
Logout path: Requesting this path will result in the user being logged out. Subsequent requests will require re-authentication, if relevant. If this path is empty, users can only be logged out by closing the browser, or if the authentication times out. Note: The logout path must be an included file location.

Virtual web path: This is the path to the Swivel authentication pages. See the next section for details on setting this up. You should normally set this to be ?/pinsafe?, unless you have a particular reason not to.

Help URL: The URL for Swivel 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.

After configuration is complete Apply the settings and restart the World Wide Web Publishing Services.

Allow Active Server Pages: to verify this, select the Internet Information Services Manager expand the required server then click on Web Service Extension.



4.6 Installing the Filter on Multiple Websites

Most of the instructions above assume that you are installing the IIS filter on the single default website of a web server. However, if you want to use the filter on multiple websites on the same server, you need to carry out a few extra steps.

Firstly, if all the settings on all the websites are exactly the same, you can configure it once, and then carry out the same steps to activate the filter on each website.

If, however, you need different settings for each website, you will need to do the following for all except the first website:

1. Make a copy of the entire Web folder, including the bin sub-folder. You can copy it as a sub-folder of Swivel IIS filter, with a different name, or you can put it somewhere completely different. It is important, however, that you keep the structure the same ? all the .asp files must remain intact, and the filter DLL must be in a sub-folder called ?bin?.

2. When you come to configure each filter, navigate to the bin sub-folder of the copy you have just made. Otherwise, configuration is exactly as before.

3. When selecting the IIS filter to install, and also when defining the virtual directory for Swivel web pages, you should use the copy you have just created, rather than the original. This is important, as both the filter and the web pages look for the configuration file relative to their own location.

4.7 Testing

Browse to a web page that has been configured for protection. This should display a Swivel login dialogue:

Enter the Username.

For dual channel, enter the One Time Code:

Or click start session to enter a single channel OTC. The Swivel log will record that a single channel session has started.

If authentication is successful it should redirect to the login page. If failed an error message will appear. The Swivel log will record any successful log attempt for the agent.

4.8 Uninstalling the filter

To remove the Filter, remove role services that are not required by other applications, to do this for Windows 2008, on the IIS server start the Server Manager by selecting Start/Administrative Tools/Server Manager then expand the tab for Roles, click on the Web Server (IIS), then look under Role Services to remove the *ISAPI Filters*, *ISAPI Extensions* and ASP are installed. The system will require a restart to complete.

From the IIS Manager right click on the Swivel Virtual Directory, then select Remove, Click on Yes to Confirm.

To uninstall the Swivel IIS Filter, choose Start/All Programs/PINsafe IIS Filter/PINsafe IIS Filter Uninstaller, then click Yes on the confirmation to uninstall.

The Swivel Filter config may be left after uninstalling, so to completely remove this, remove the folder Program Files\PINsafe IIS Filter.

4.9 Troubleshooting

Verify the correct filter version has been installed for the operating system i.e. 32 bit or 64 bit.

Check for error messages in the Swivel log

Check the IIS log messages

Filter Install issues: The IIS service needs to run as an administrator in order to install the filter. Once the filter is installed, it will run as the normal user. Open the Services applet and locate World Wide Web Publishing. Select properties, then go to the Log On tab. Assuming you are logged in as an administrator, select Local System account. Then restart the service. Hopefully, this will start the filter. You can then switch back to the default account and restart again.

If you are not redirected to the Swivel login page when trying to access a protected page, open IIS manager and check that the ISAPI filter is installed and has loaded properly (there should be a green arrow next to it, and the priority should be ?High?). If this is not the case, restart IIS, if you have not already done so, and try again. The filter doesn't try to install until you try to access a web page from that website, so try that before assuming it hasn't worked.

If the filter is listed, but showing a red cross, then it failed to start. In this case, check the error messages in the event log showing.

If the filter shows as green, with priority unknown, it may not be installed. In this case, you need to check. You can do this with a debug viewer, such as the one supplied by SysInternals (http://technet.microsoft.com/en-us/sysinternals/bb896647.aspx). Download this and run it (there's no need to install it) on the server, then restart IIS. If you don't see any messages relating to the Swivel IIS filter, then it's not installed properly.

If the page is still not redirected, try the following:

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. Try accessing a protected page again. Hopefully this time you will be redirected.

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.

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 Swivel server or the Allow Image request by username may be set to No.

For a virtual or hardware appliance Install

https://<pinsafe_server_ip>:8443/proxy/SCImage?username=<username>

For a software only install see Software Only Installation

If the web page is redirected to the /PINsafe/login.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 Extension.

No authentication on main page

Open IIS Manager and disable Anonymous authentication for the root folder. Refresh the browser to prevent caching and try again.

You may need to ensure that Anonymous authentication is enabled for the PINsafe folder, though, so you don't run into problems showing the TURing image.

Authentication working internally but not externally

If it is working internally, but not externally, ensure that there is no caching by openine a new browser. Also specify the default redirect URL as "/default.htm", rather than "./default.htm". The latter will redirect to default.htm within the pinsafe folder.

4.9.1 Error Messages

AgentXML request failed, error: The agent is not authorised to access the server

User fails to authenticate with the above error message in the Swivel log. An Agent on Swivel server has not been defined for the IIS server. Go to Server/Agents in the Swivel admin console, and add a new entry, using the IP address of the IIS server. Make sure the agent secret is the same as on the IIS filter configuration.

This installation package is not supported on this processor type. Contact your product vendor