Microsoft IIS version 6 Integration

Contents

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.

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:

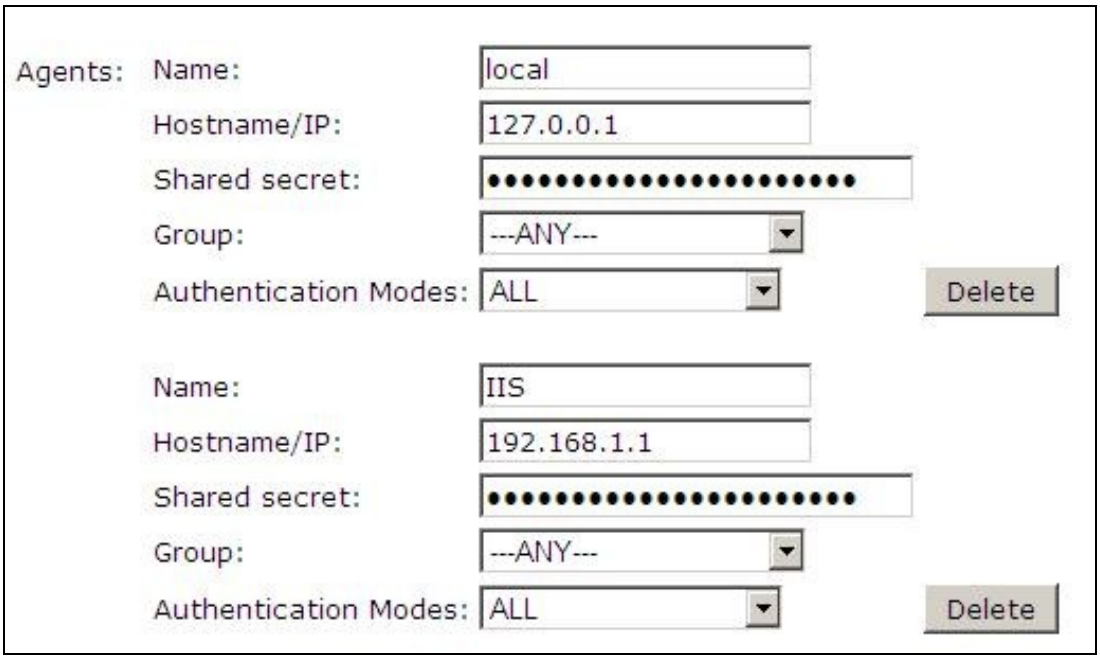
- 32-bit ISAPI Filter
- 64-bit ISAPI Filter

PINsafe Configuration

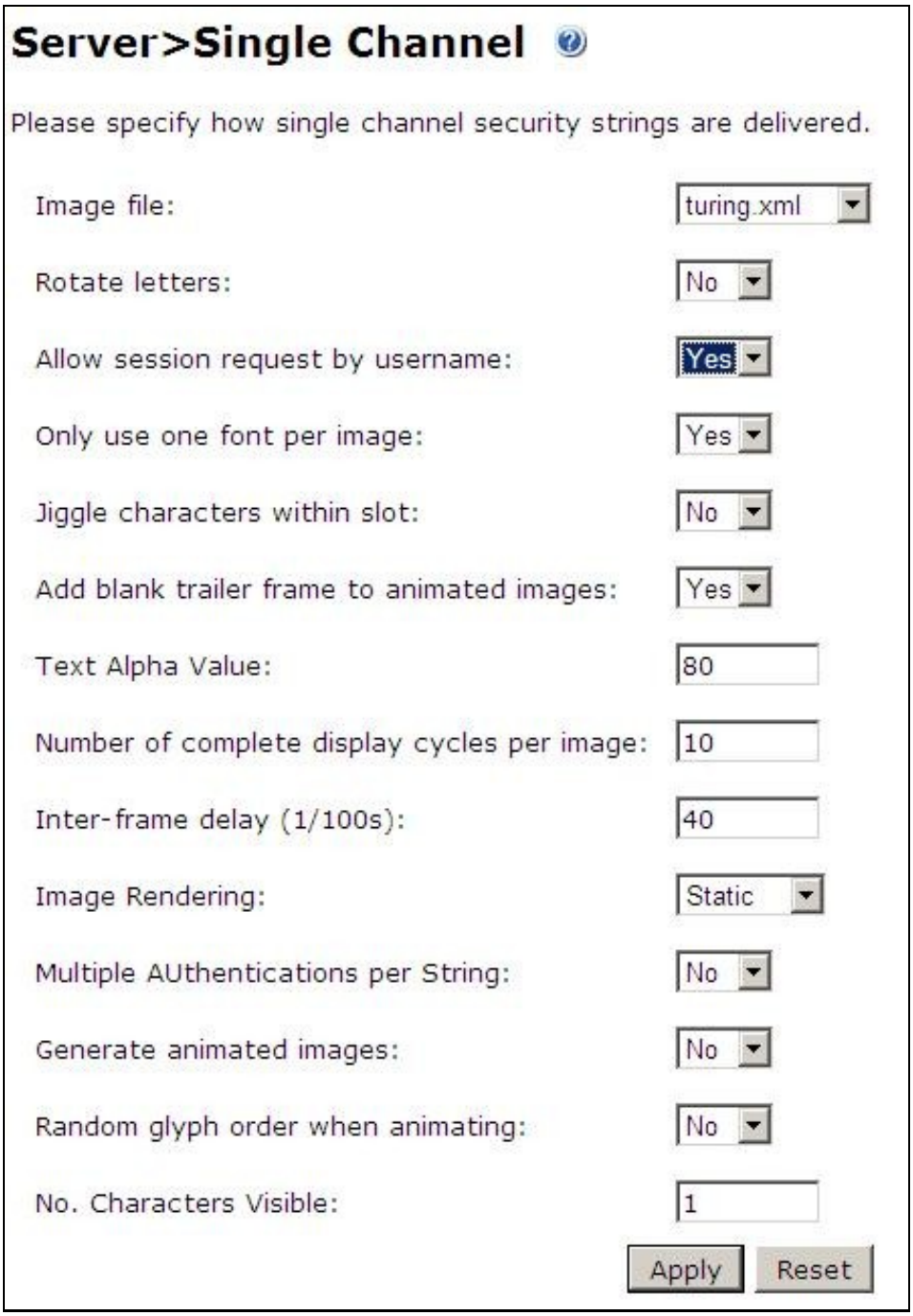
On the PINsafe server configure the agent that is permitted to request authentication. On the PINsafe Administration Console select from the server menu Agents and enter the details of the IIS server IP address and a shared key, then click on apply.

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.



Configuring the IIS Server

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.

Configure the ISAPI filter

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

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.

Install The IIS ISAPI filter

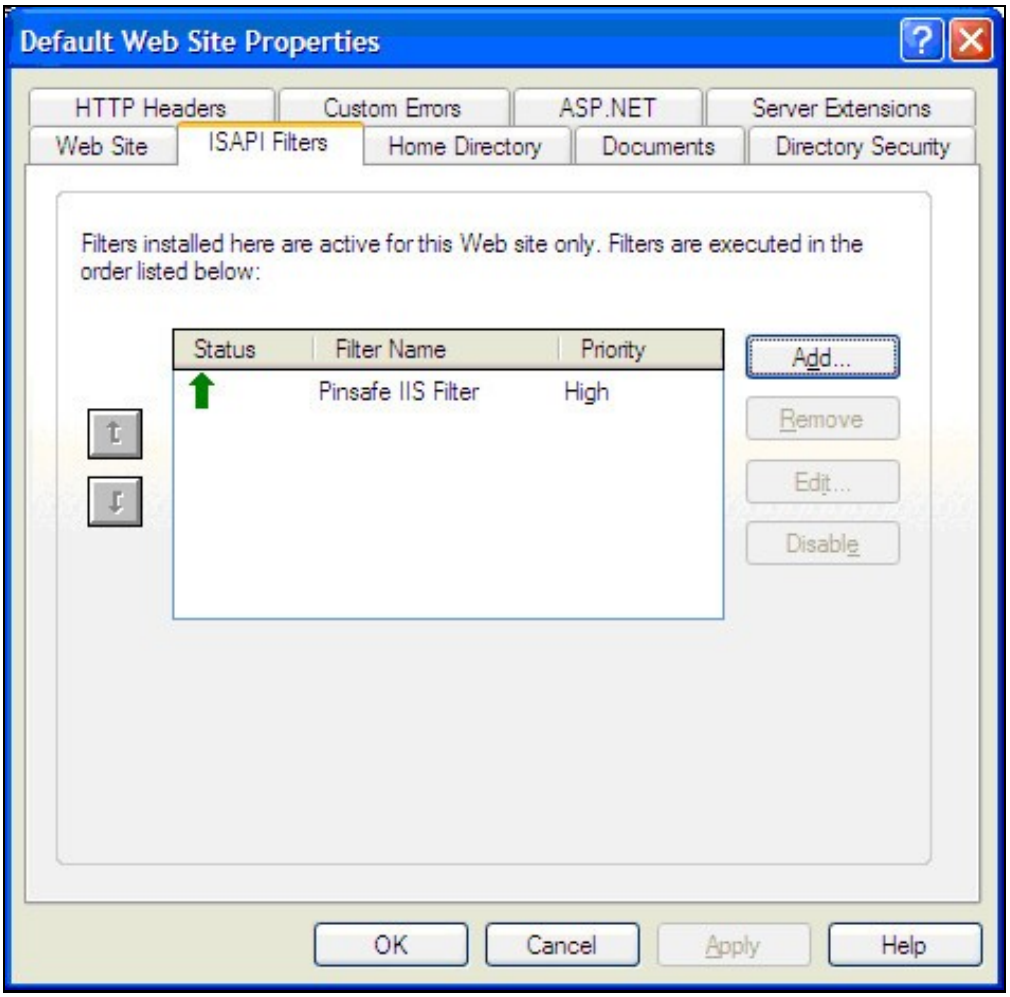
1. On the Internet Information Services Manager Select the Properties for the website

2. Select ISAPI filters

3. Select Add ISAPI filter

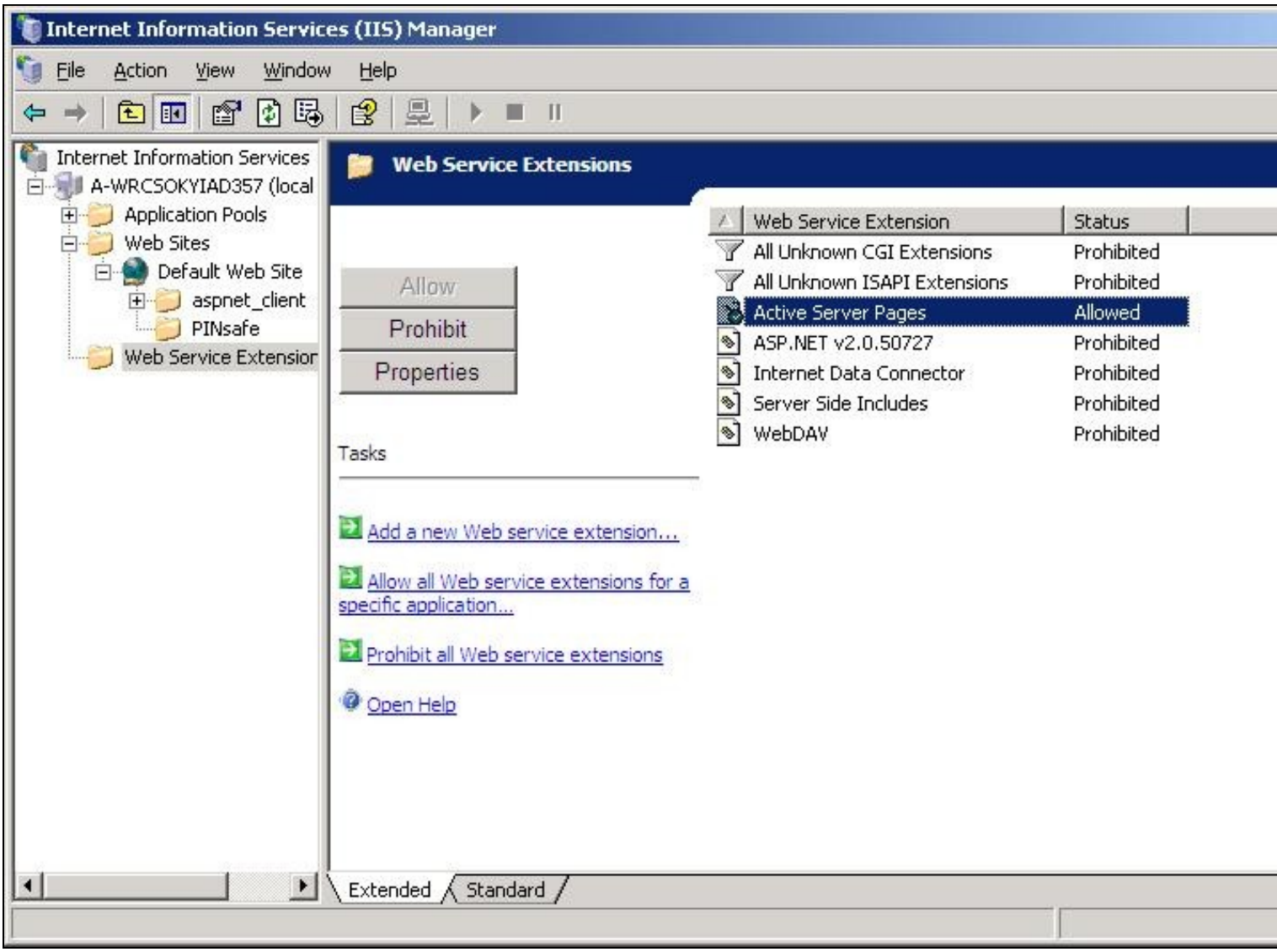
4. Select the Path to the PINsafe ISAPI filter. Note that the actual file you require will be PINsafeIISFilter.dll, located in the installation folder.

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.

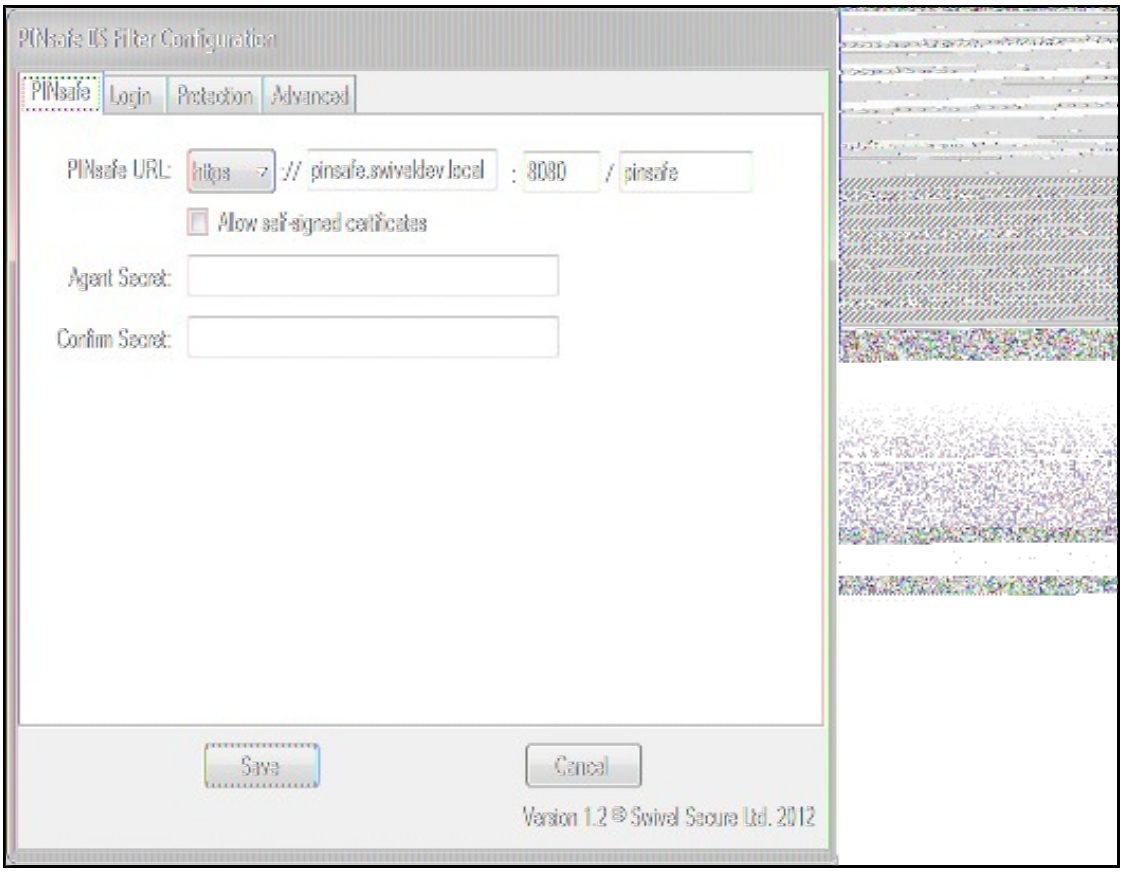
Allow Active Server Pages: to verify this, select the Internet Information Services Manager expand the required server then click on Web Service Extension.



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.

PINsafe Server Settings



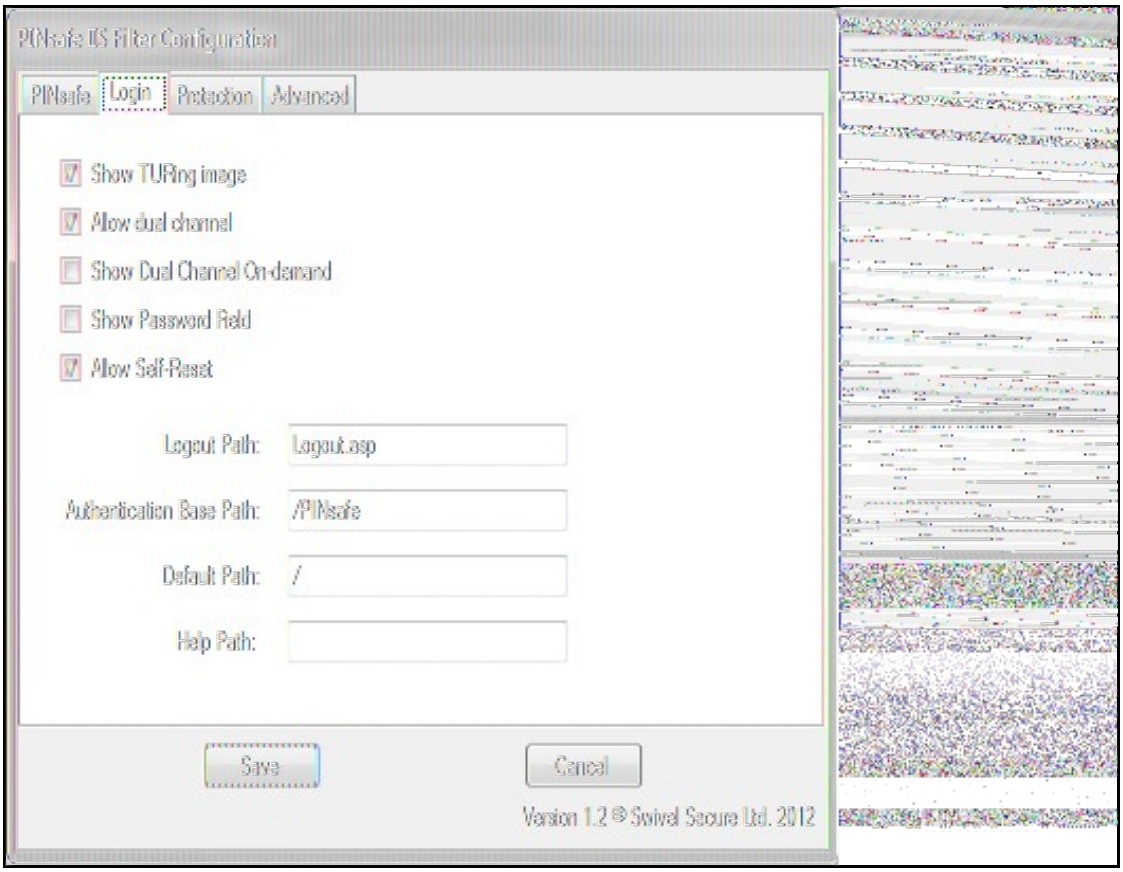
This page defines the connection to the PINsafe server.

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.

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.

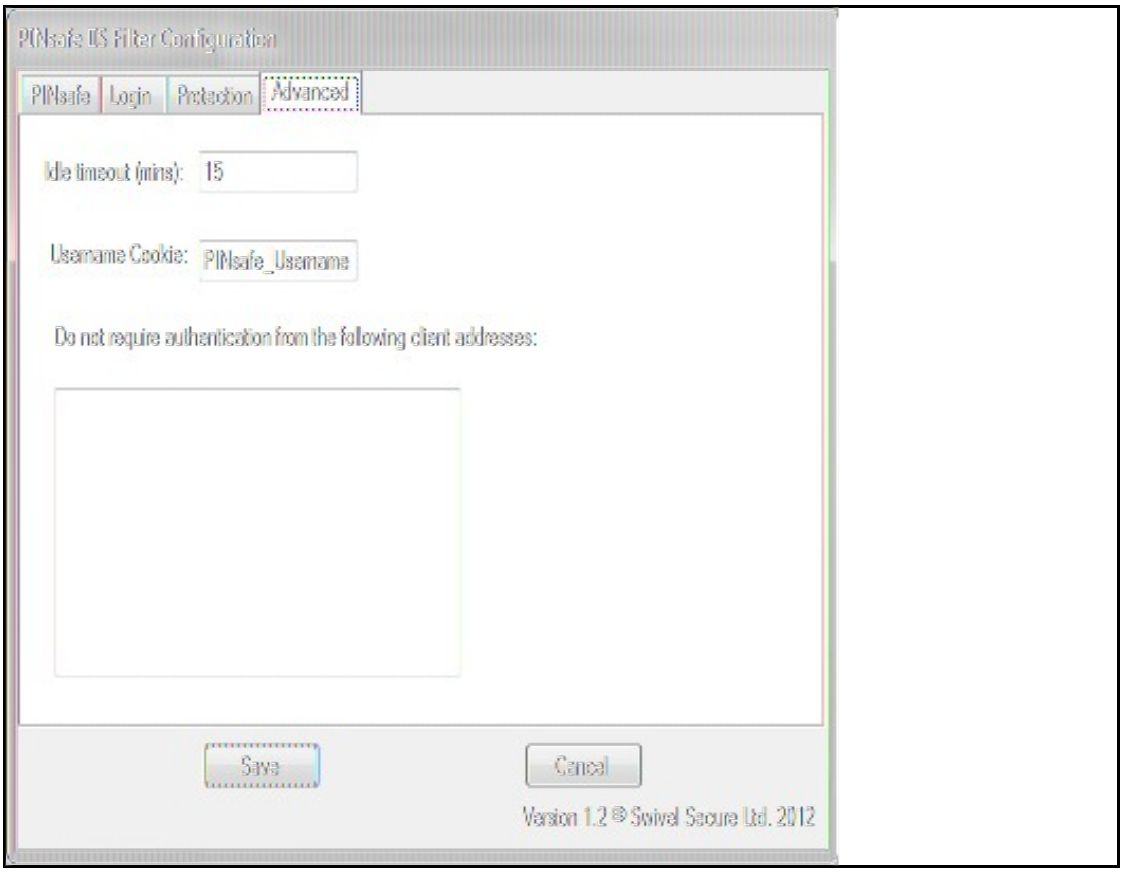
Authentication Base Path: the virtual path containing the PINsafe authentication pages.

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.

Advanced Settings

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



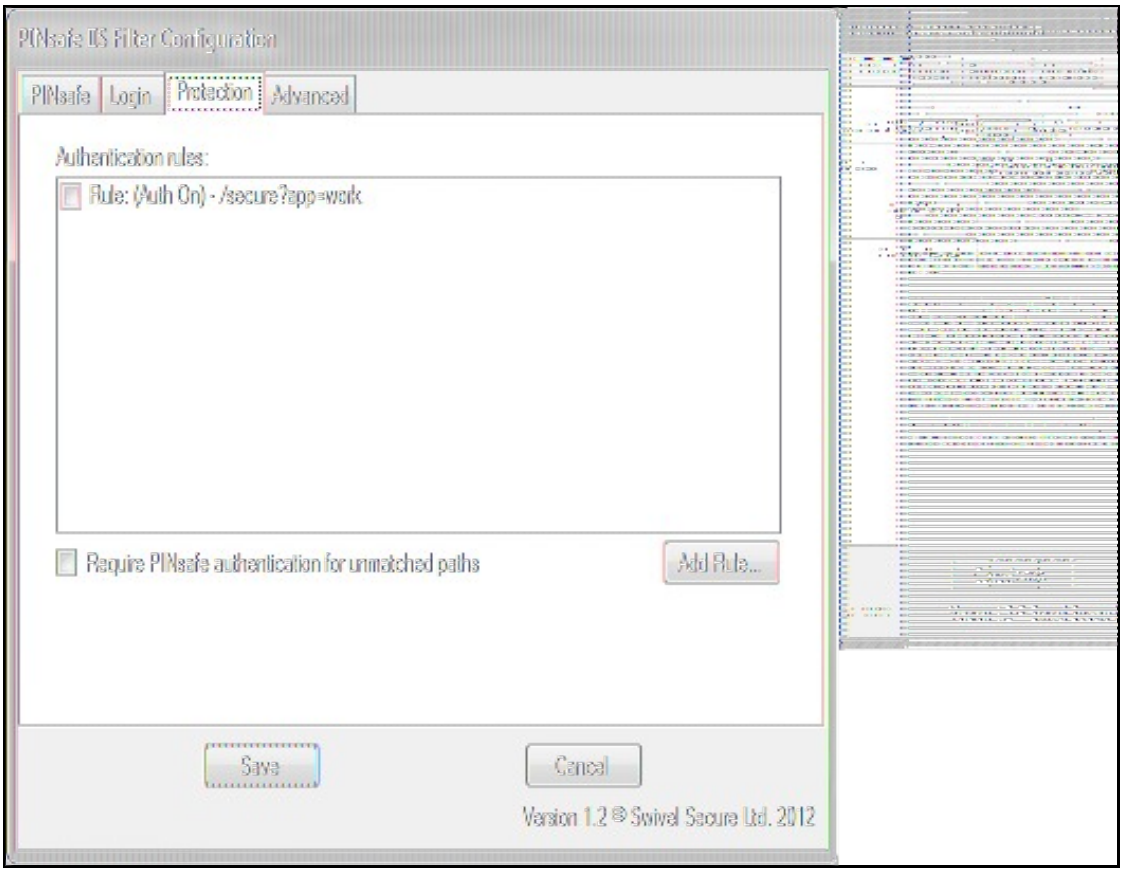
Idle timeout is the time (in minutes) that the user can leave a page open without refreshing it or navigating to another page: in other words, the lifetime of the authentication cookie. However, if the user requests a new page (or refreshes the current one) within that time, the cookie expiration time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

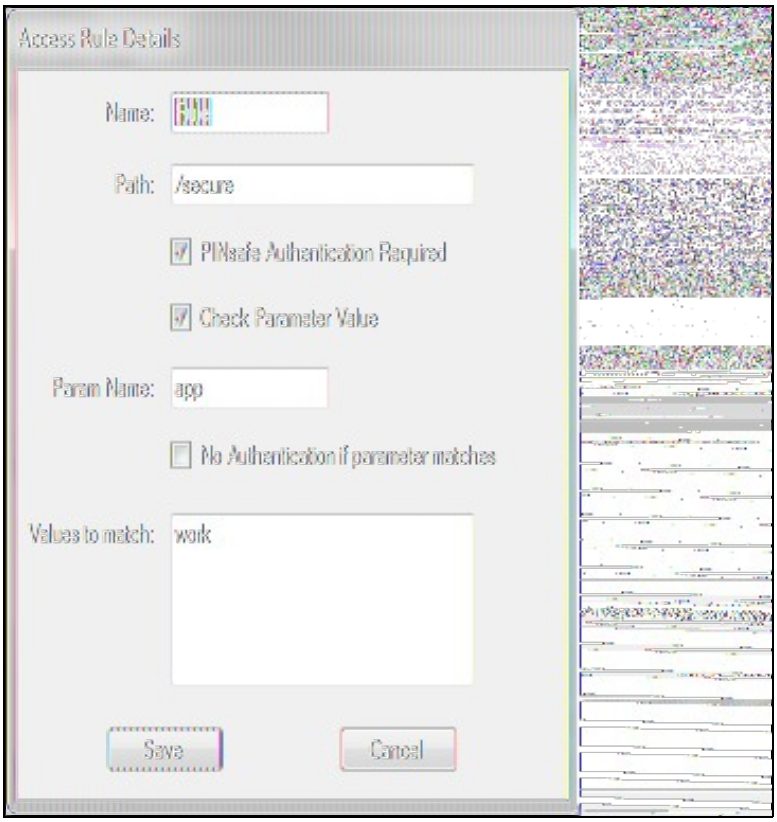
Protection Settings

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.

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.

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.

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.

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.

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.

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.

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.

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.