Microsoft IIS version 7 ASP.NET Integration

Contents

- 1 Introduction
- 2 Prerequisites
- 3 Architecture
- 4 PINsafe Configuration
    - 4.1 Configure a PINsafe Agent
- 5 Filter Installation
- 6 Filter Configuration
    - 6.1 PINsafe Tab
    - 6.2 Login Tab
    - 6.3 Protection Tab
    - 6.4 Advanced Tab
    - 6.5 Logging Tab
    - 6.6 IIS Configuration
- 7 Additional Configuration Options
- 8 Testing
- 9 Troubleshooting
- 10 Known Issues and Limitations
- 11 Additional Information

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.

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.

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.

PINsafe Configuration

Configure a PINsafe Agent

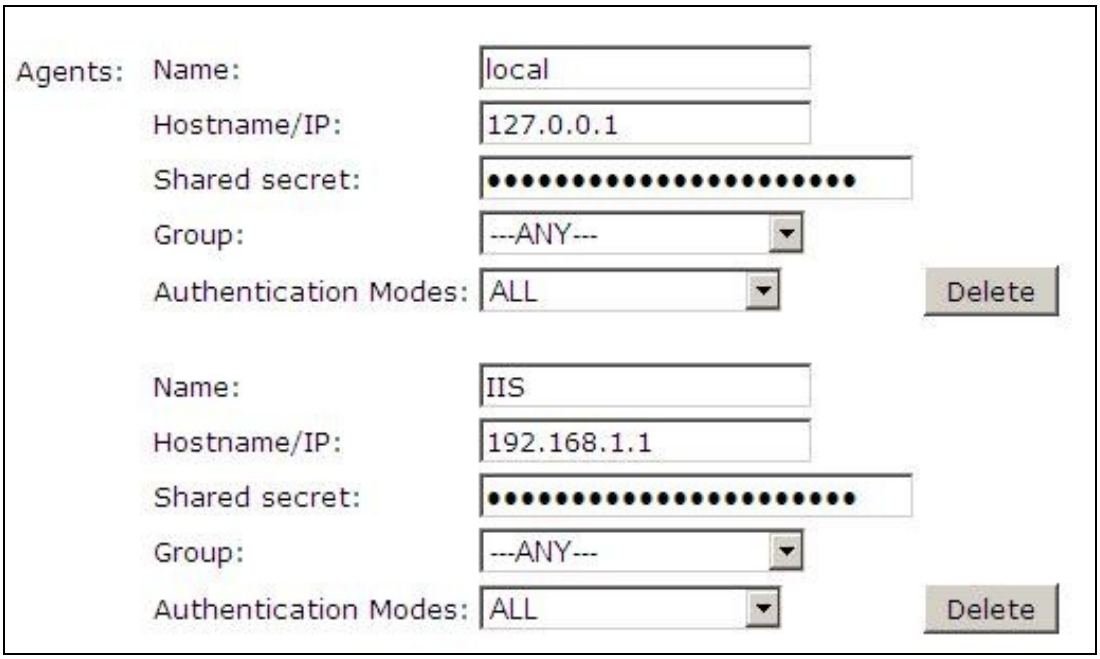
1. On the PINsafe Management Console select Server/Agent

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.

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.

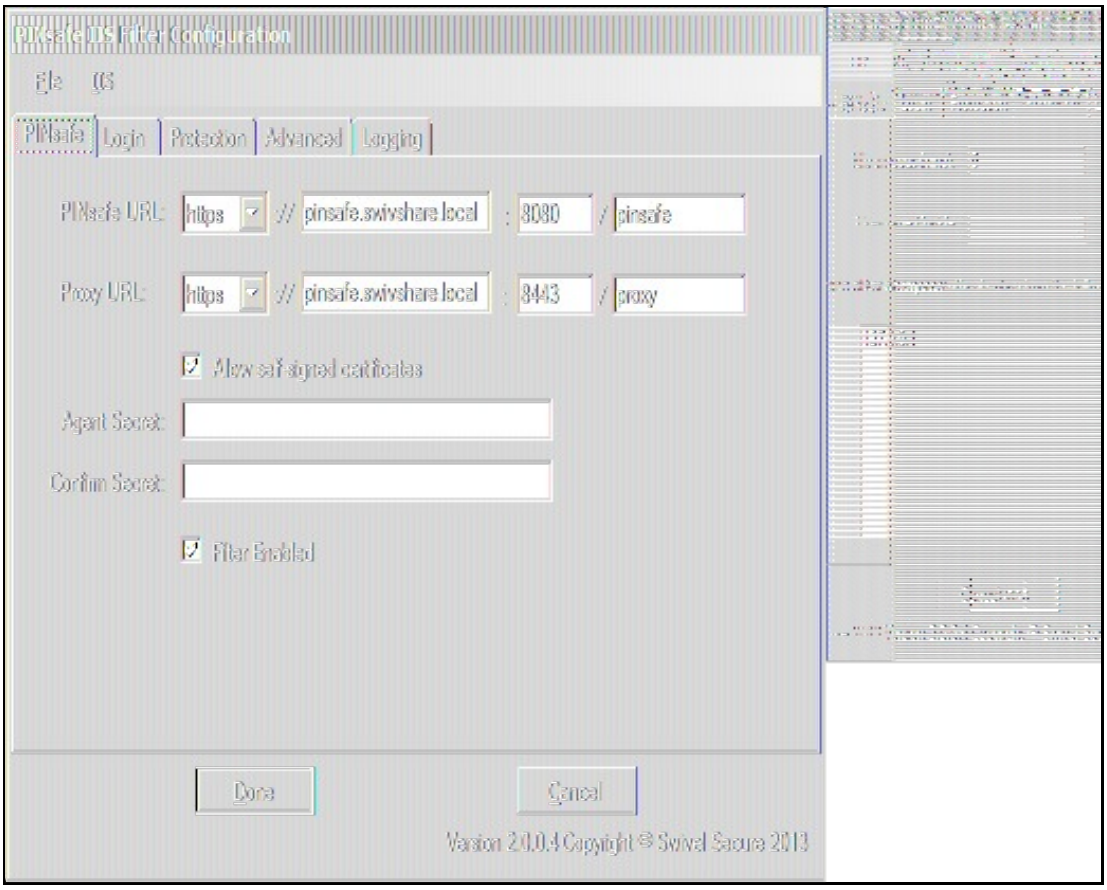
Once the filter is installed, you will be taken to the configuration program (unless you choose not to do so yet).

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.

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.

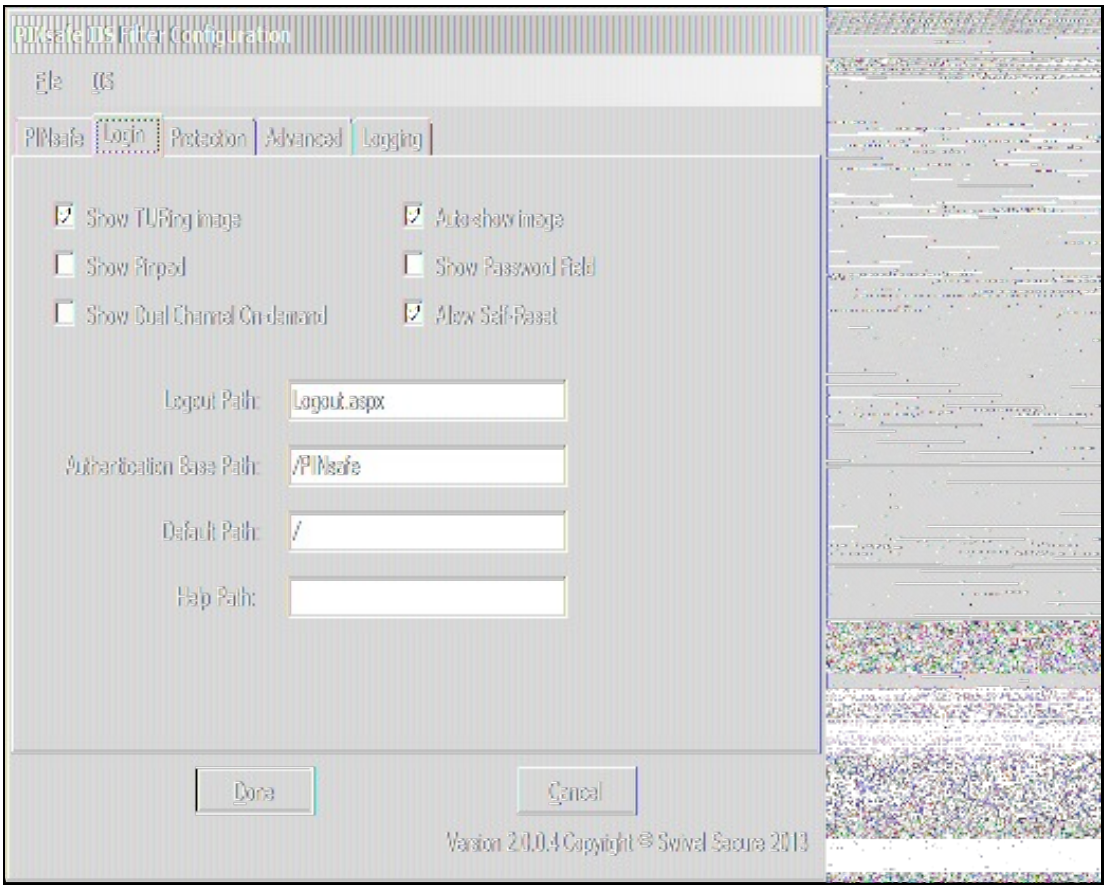
Note that the URLs only need to be resolvable and accessible from the web server. Direct access for the end user to the PINsafe server is not required - the filter proxies all requests.

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.

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**.

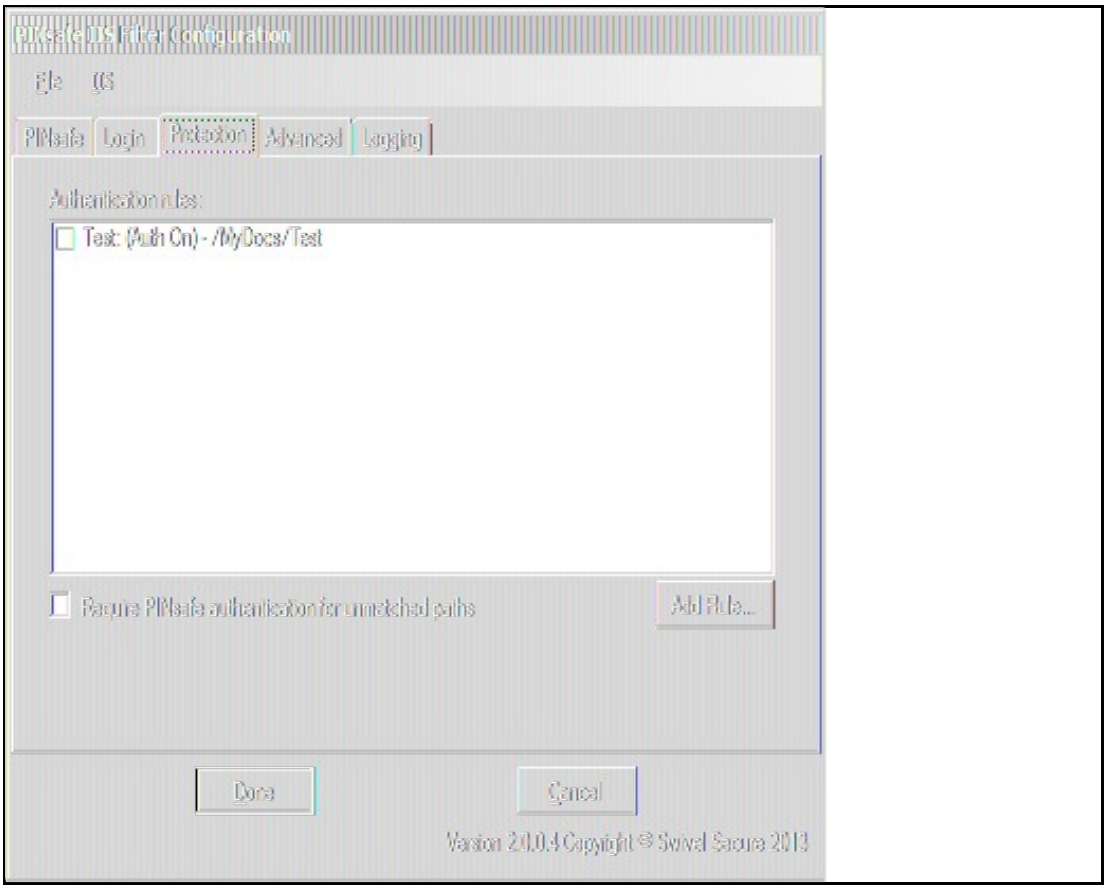
Logout path is the full path used to log out from PINsafe. Typically, this will be /PINsafe/Logout.aspx. If this is detected in the URL, the PINsafe authentication cookie will be removed, and users must re-authenticate to access protected URLs.

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**.

Protection Tab

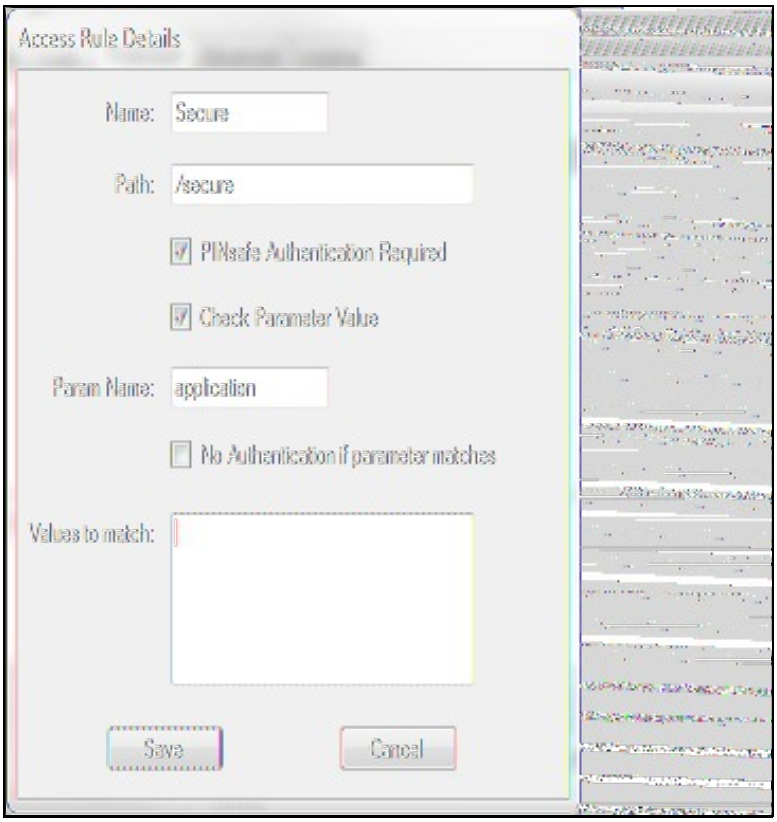


On this page, you specify which paths should require PINsafe authentication. You do this by defining a list of rules. Each rule is a path to be matched, with a flag indicating whether or not PINsafe authentication is required. The filter runs through the rules in order until it matches one, and determines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

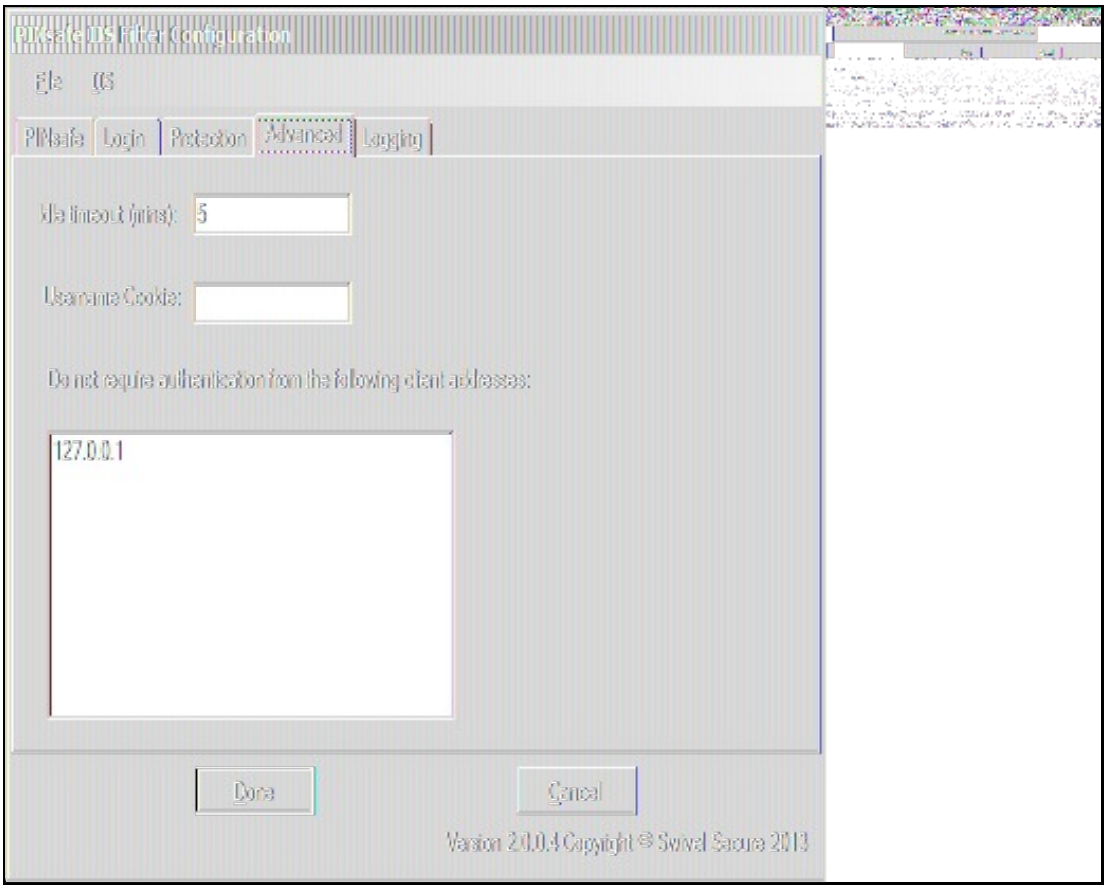
"Check Parameter Value" allows finer control over PINsafe authentication. When checked, you can specify the name of a single query parameter that is checked to determine whether or not PINsafe authentication is required. You can specify a list of possible values for the parameter, but if you specify 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.

Advanced Tab



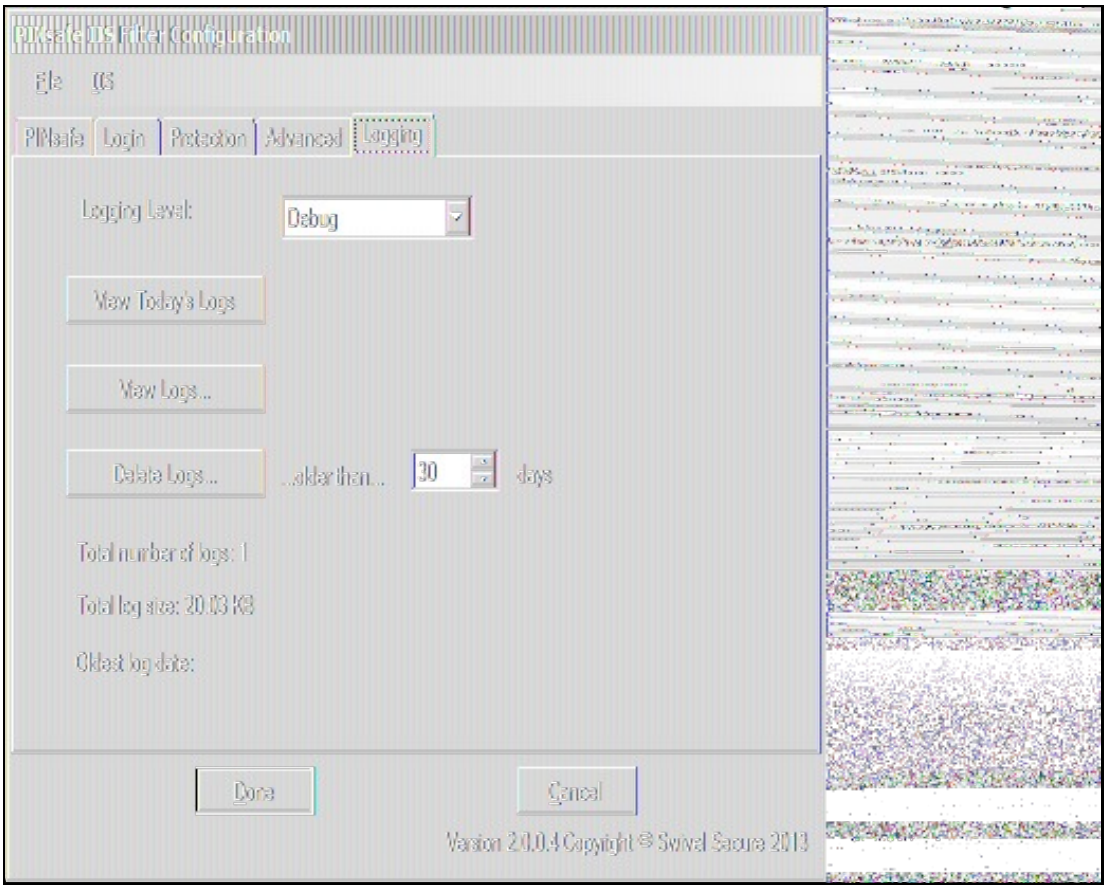
There are 3 settings on this tab:

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.

Logging Tab

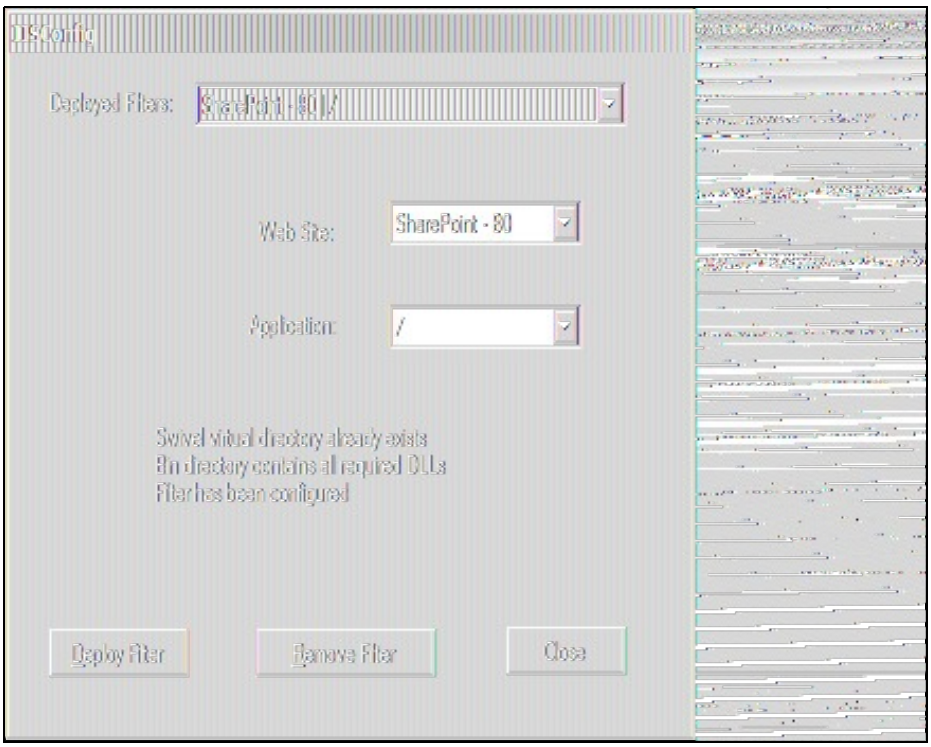


This page allows you to specify what logging the filter does, and to view or delete logs.

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.

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.

Additional Configuration Options

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.

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

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

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