Table of Contents

Table of Contents

Table of Contents

1 Arx Co-Sign Integration

Arx Co-Sign Integration Guide

2 Authentication Manager

3 SAML based Authentication

Swivel Secure is developing a new SAML integration provides a new range of capabilities that optimise the application of Swivel Authentication for accessing Cloud Applications.

This is now part of version 4 of the Swivel authentication platform, renamed as "Sentry". For more information, please see Sentry User Guide.

These capabilities include

1. Adaptive, Risk-based authentication: Enforcing the appropriate level of authentication depending on various risk factors

2. Single-Sign-On across multiple cloud applications

The mechanism behind these capabilities is a points system. Points are awarded to a user for successful authentication but also for other factors such as their IP address, the time of day etc etc.

The number of points awarded for different forms of authentication can be varies as can the number of points required to access each service or application.

This means a completely customised and optimised authentication system can be deployed.

4 Prerequisites

Swivel Version 3.10.3 or later

Swivel Authentication software (Product in development and not yet available)

5 Configuring the Swivel server

5.1 Configuring the Swivel Agent

On the Swivel Administration console configure the Swivel Agent, see Agents How to Guide. By default there is a local Agent, and if the Authentication manager and Swivel are on the server it can use this.

5.1.1 Enabling Session creation with username

To allow the TURing image, Pinpad and other single channel images, under Server/Single Channel set Allow session request by username to Yes.

5.2 Configuring the Admin login

An Administrator account is required to login who is a member of the PINsafeAdministrators group, or group as defined below.

6 Authentication Manager Installation on a Swivel Appliance

The software comes as a web-archive (.war) file called swivelauthenticationmanager.war. Using WinSCP or similar copy the swivelauthenticationmanager.war file to /usr/local/tomcat/webapps2 folder.

This should automatically create the following folders:

/usr/local/tomcat/swivelauthenticationmanager

/home/swivel/.swivel/db/SwivelAuthenticationManagerDB

6.1 Configuring the Swivel Authentication Settings

Edit the settings.properties file in

/usr/local/tomcat/swivelauthenticationmanager/classes/settings.properties

The following values should be set for a Swivel hardware or virtual appliance:

```
pinsafessl=false
pinsafeserver=localhost
pinsafecontext=pinsafe
pinsafesecret=secret
pinsafeport=8181
imagessl=true
imageserver=Swivel_DNS_Public_Name
imagecontext=proxy
imageport=8443
selfsigned=true
certificateIssuer=SAML_SP
encryptionType=DSA
publicKeyFilePath=/keys/pinsafe/ssl/dsapubkey.der
privateKeyFilePath=/keys/pinsafe/ssl/dsaprivkey.der
certificateFilePath=/keys/pinsafe/ssl/dsacert.pem
administrationGroup=PINsafeAdministrators
timeoutPolling=60000
```

Note: Sentry's administrationGroup by default is set to Swivel Admin, after a migration this group must match the admin group set in the core, which by default was PINsafeAdministrators.

After saving the settings restart Tomcat, such as through the CMI

If you have changed the shared-secret for the local agent on the Swivel core server you need to set the secret on the authentication manager to match.

pinsafessl=false True/False, Comunication with the Swivel core, using SSL or not

pinsafeserver=localhost Comunication with the Swivel core, localhost if installed on the same server

pinsafecontext=pinsafe Comunication with the Swivel core, the Swivel installation name

pinsafesecret=secret Comunication with the Swivel core, the shared secret defined on the core

pinsafeport=8181 Comunication with the Swivel core, port used for communication, 8181 for the proxy

imagessl=true True/False Comunication with the Swivel core, using SSL for images

imageserver=Swivel_DNS_Public_Name Comunication with the Swivel core, The IP addrss used for Swivel images and usually publicly available through the Swivel proxy

imagecontext=proxy Comunication with the Swivel core, for obtaining authentication images, use proxy for an appliance

imageport=8443 Comunication with the Swivel core, for obtaining authentication images, use 8443 for an appliance

selfsigned=true True/False Comunication with the Swivel core, for obtaining authentication images, True to allow self signed certificates

certificateIssuer=SAML_SP

encryptionType=DSA

publicKeyFilePath=/keys/pinsafe/ssl/dsapubkey.der

privateKeyFilePath=/keys/pinsafe/ssl/dsaprivkey.der

certificateFilePath=/keys/pinsafe/ssl/dsacert.pem

administrationGroup=PINsafeAdministrators

timeoutPolling=60000

6.1.1 Additional settings

federatedIDAttribute=email The Federated ID Attribute can be defined, if it is not specified, it defaults to email.

6.2 Key and Certificate generation

Key and Certificate Generation

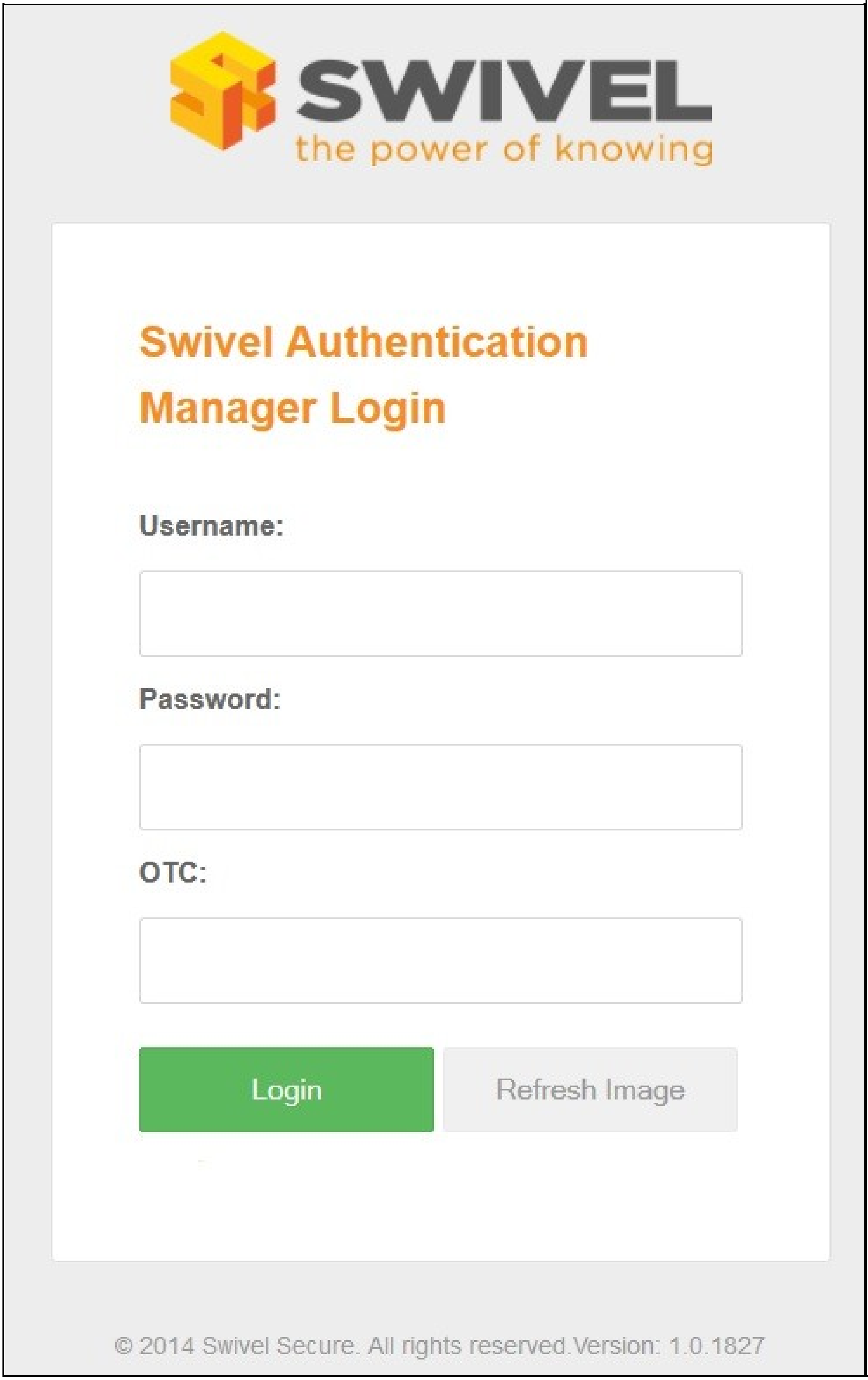
6.3 Swivel Authentication Manager Login

Using a web browser connect to the Swivel Authentication Manager:

https://IP_or_Hostname:8443/swivelauthenticationmanager

Login with a user who is a member of the administrationGroup on the Swivel server, the default value for this is administrationGroup=PINsafeAdministrators, which is the default Swivel Administrators group.

Adinistrative login can also be restricted by IP source, see Filter IP How to Guide.



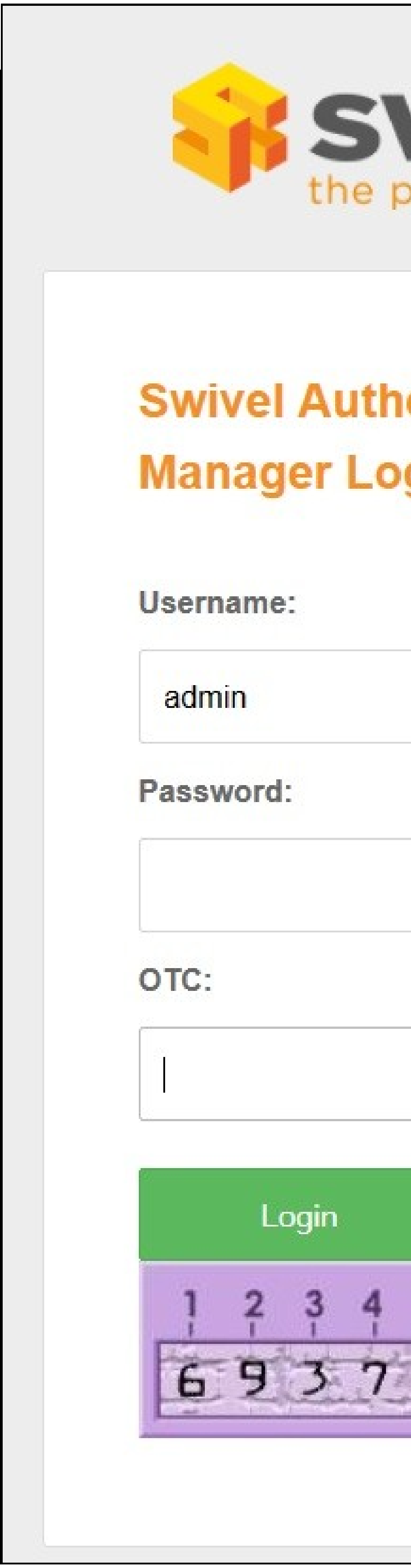
Swivel Authentication Manager Login

Username:

Password:

OTC:

© 2014 Swivel Secure. All rights reserved.Version: 1.0.1827



Swivel Auth

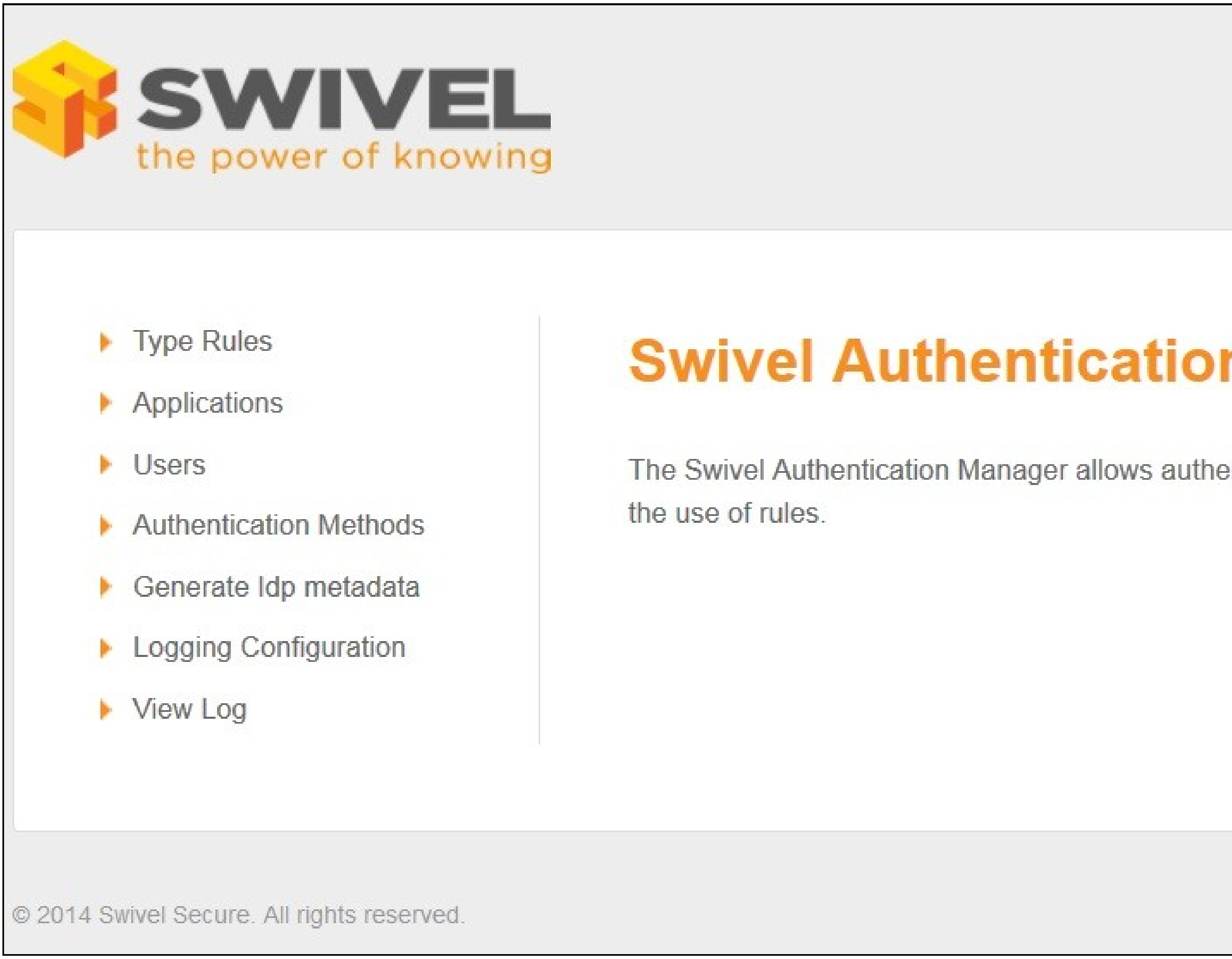
Manager Log

Username: admin

Password:

OTC:

A succesful login should load the Swivel Authentication manager default page:



Swivel Authenticatio

The Swivel Authentication Manager allows authe the use of rules.

© 2014 Swivel Secure. All rights reserved.

6.4 Integration

Integration of SAML-enabled services and applications will depend in detail on the applications themselves. However on the Authentication Manager side of the integration you need to

1) Give the service provider a name.

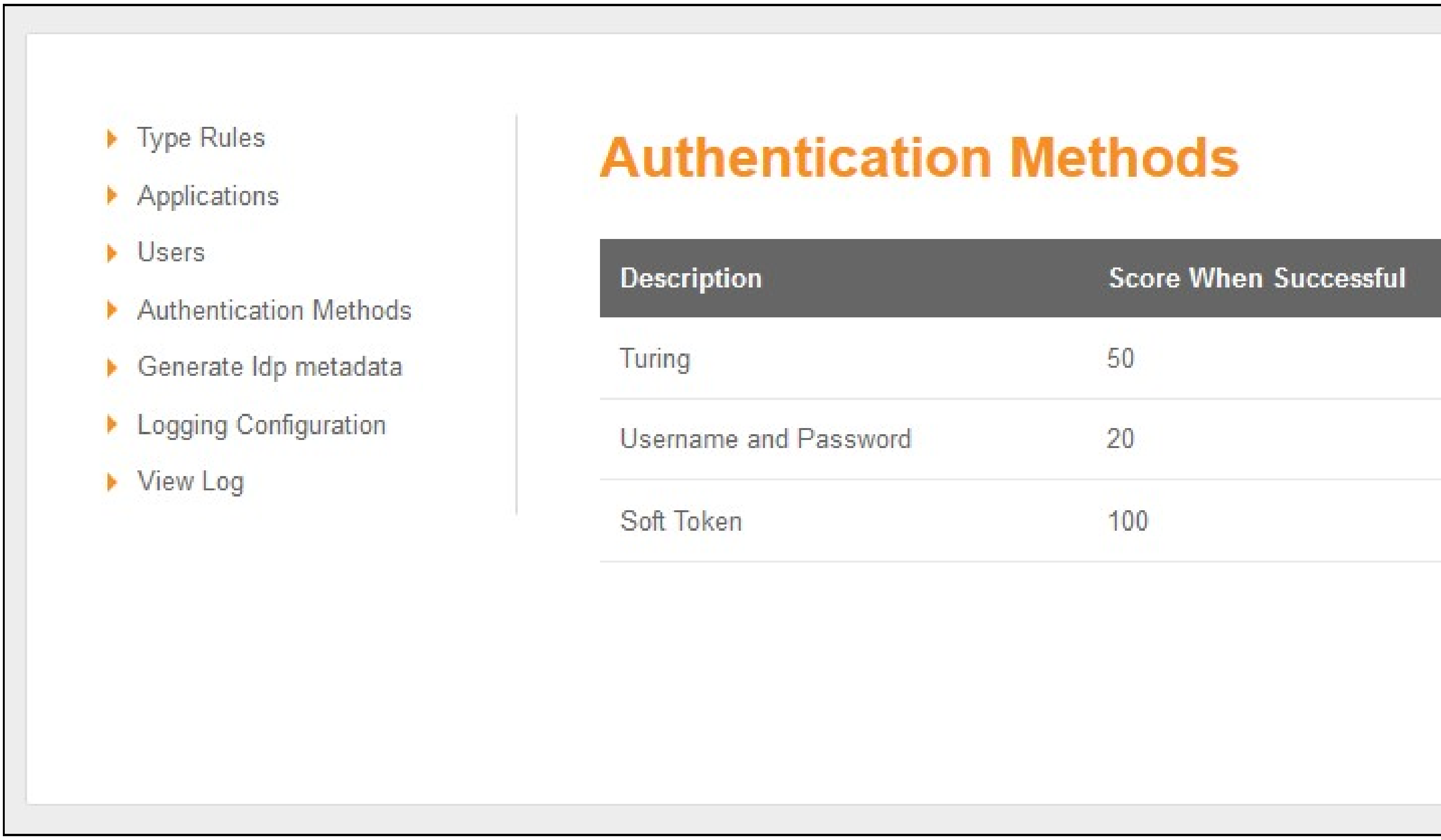
2) State the number of points required before the user can gain access.

3) The IP addess or host name of the cloud service, specically the SAML2.0 Endpoint for the service

4) The cloud servive URN, this will be part of the SAML Assertion that the cloud service will send

If required the Authentication Manager's metadata can be generated by using the Generate IdP metadata function.

6.5 Authentication Methods



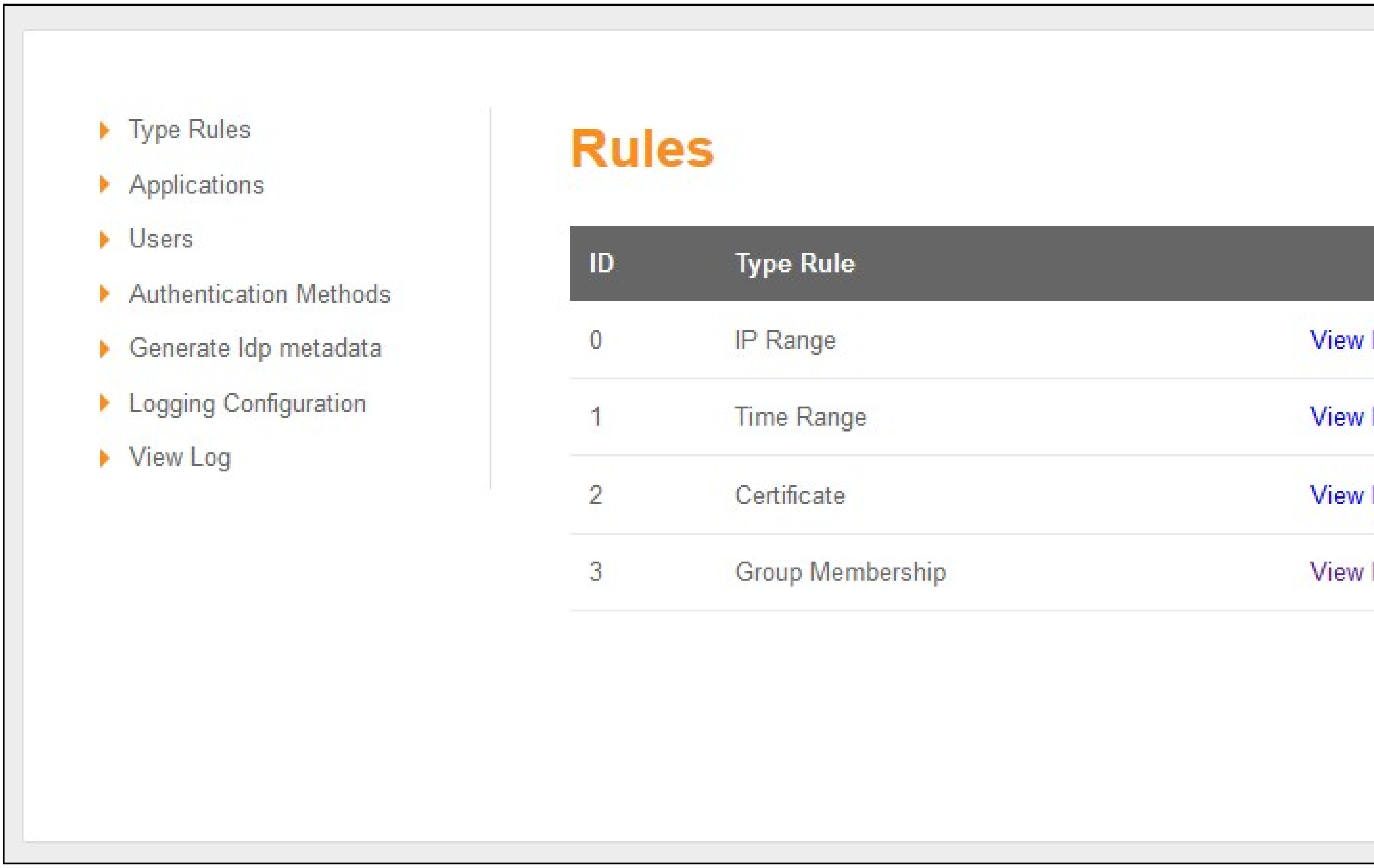
Authentication Methods

Description	Score When Successful
Turing	50
Username and Password	20
Soft Token	100

In order for a user to be allowed access to the cloud applications they must attain a significant number of points. Points can be attained by "rules" or by successfully authenticating to the Authentication Manager

The number of points awarded for each for of authentication is defined on the Authentication Methods Screen.

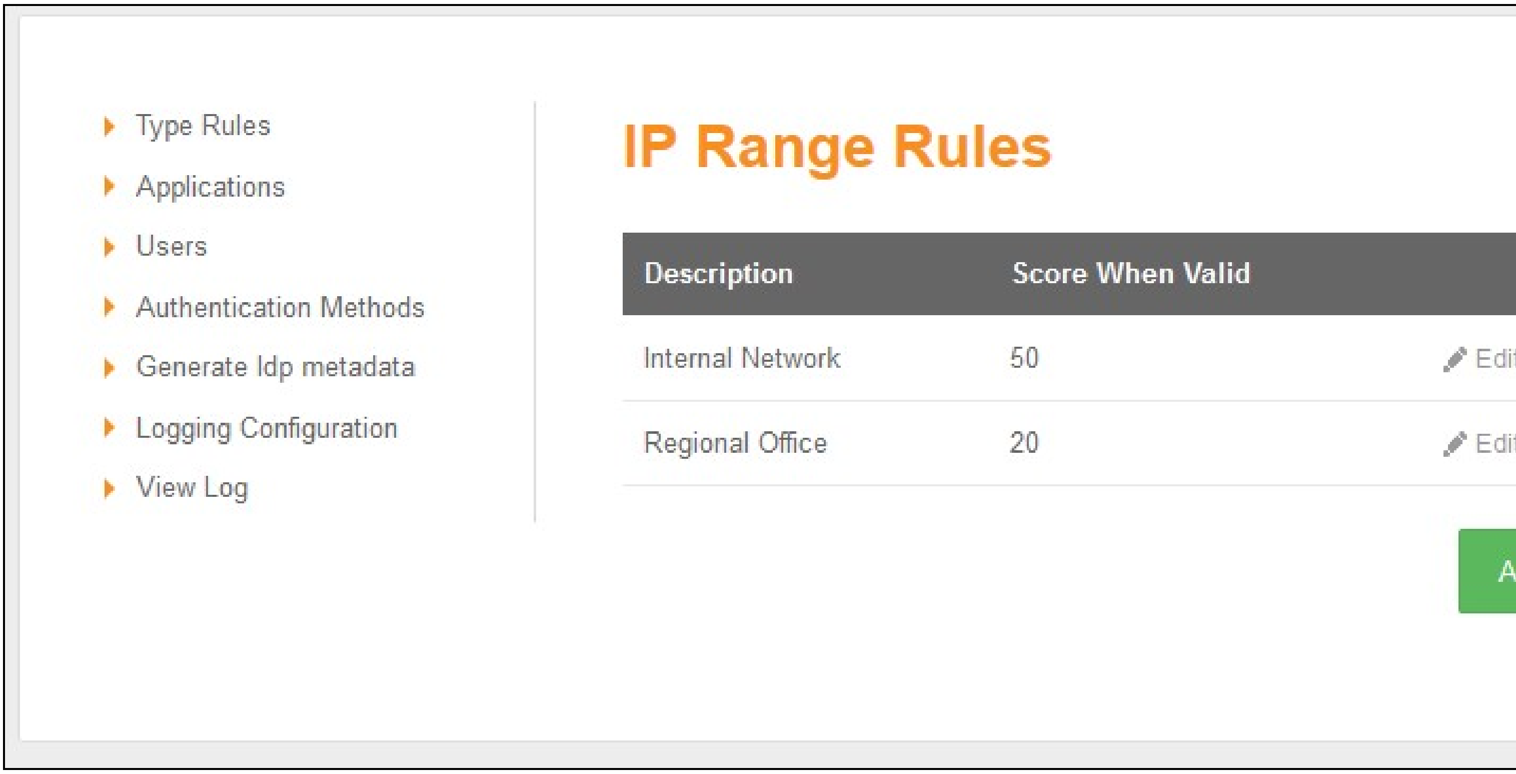
6.6 Rules



Rules

ID	Type Rule	
0	IP Range	View
1	Time Range	View
2	Certificate	View
3	Group Membership	View

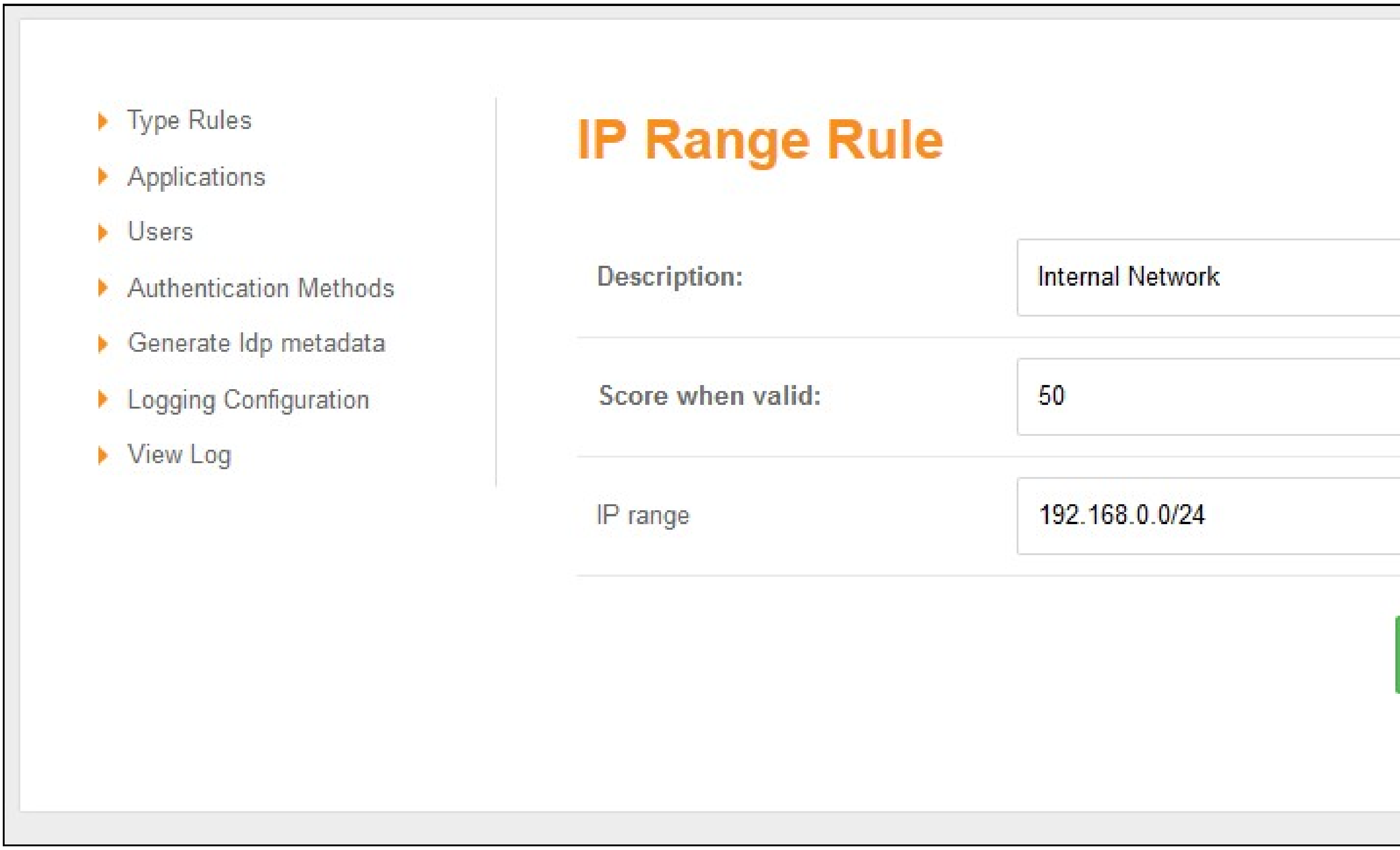
Rules are the means by which the system administrator can take into account a number of risk factors into account when deciding how a user should authenticate. The admin specifies the rule and then how many points the user is awarded (or penalised) should the rule be true for that user.



IP Range Rules

Description	Score When Valid	
Internal Network	50	Edi
Regional Office	20	Edi

For example a user accessing from the local office network may be deemed to be less risky than from other IP addresses and therefore a rule may be defined that awards 50 points to a user that is accessing from the office.



IP Range Rule

Description: Internal Network

Score when valid: 50

IP range 192.168.0.0/24

New Rules are being made avaialable all the time. The current list of rules includes

6.6.1 IP address

If the user's IP address falls within a given range or ranges (since June 2014)

6.6.2 Time of Day

Points awarded (or subtracted) if the authentication takes place within a given time period (since June 2014)

6.6.3 X509 Certificate

Points awarded if the user has a valid X509 client installed on their computer (since July 2014)

6.6.4 Group Membership

Points awarded (or subtracted) if the user is a member of a defined group (eg Active Directory group) of users (since Sept 2014)

6.6.5 Known IP Address

Points awarded to a user if they are authenticating from an IP address from which they have previously successfully authenticated from (Due Dec 2014)

6.6.6 Location (Geo-IP)

Points awarded (or subtracted) based on a user's location as derived from their IP address(Due Q1 2015)

6.7 Users

Shows users who have made a log in displaying the following information:

Username

Points

Federated ID

IP

Applications

6.8 Logging

6.8.1 Logging Configuration

Log Level: default TRACE, options TRACE, DEBUG, ERROR, WARN, FATAL, The level to log, logs everything below the selected list

6.8.2 View Log

This Displays the Swivel Authentication manager login

Events Per Page: default 10, The number of events to display per page

Page Number: default 1, The page number of logs to display

Log Level: default TRACE, options TRACE, DEBUG, ERROR, WARN, FATAL, The log level to show, displays everything below the selected list

Ascending Date Order: default not ticked, Show as Ascending or descending date

6.9 Logging Out

The Authentiation manager will remember a users session for a period of time, not requiring them to login, unless a logout option has been enabled. For testing purposes it is useful to logout when the option is not available, and this can be done by deleting cookies, or some browsers such as firefox allow individual cookies to be deleted or removing them form the file system. The cookie name is usually that of the Authentication Manager URL.

7 Testing

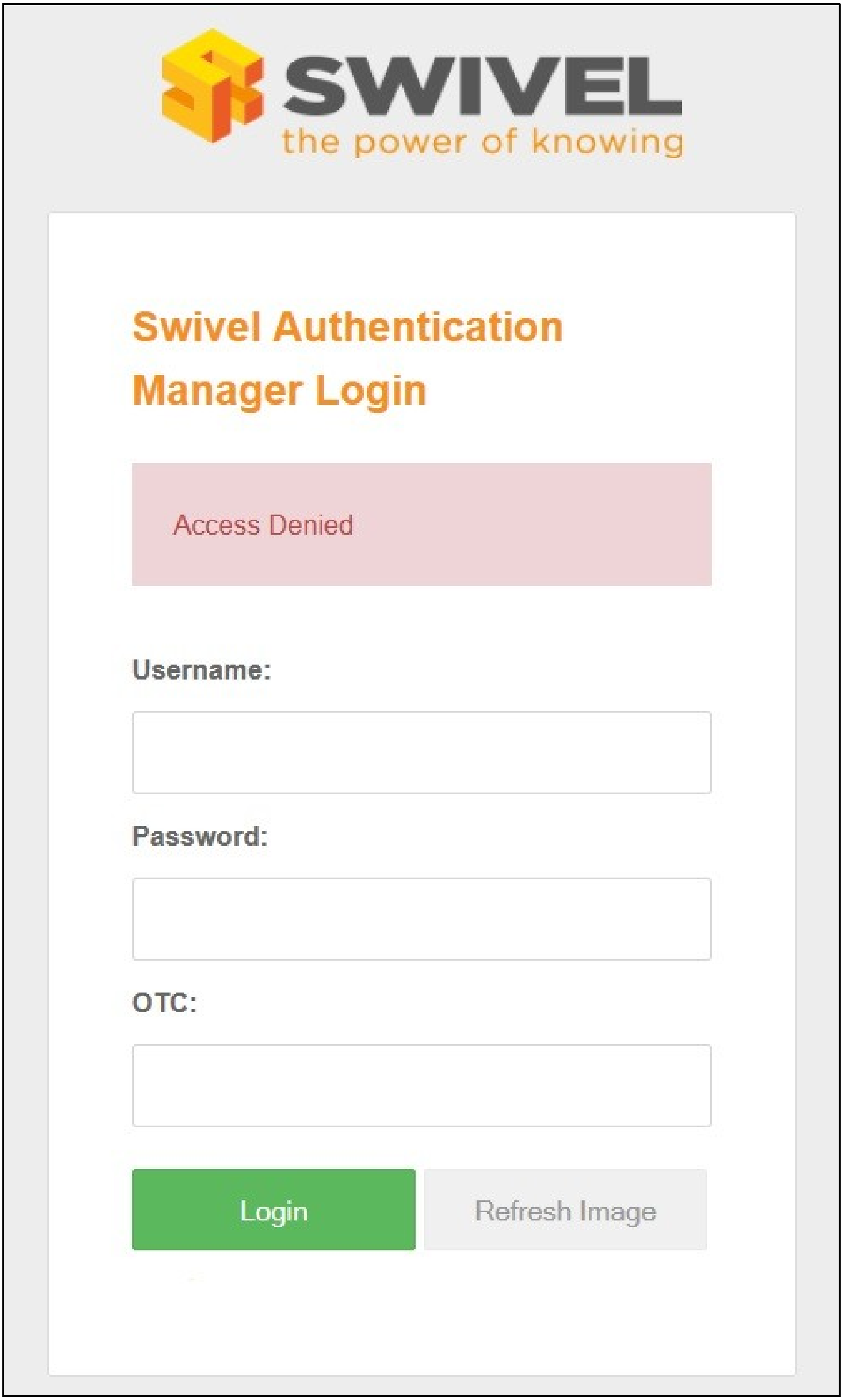
8 Known Issues

9 Troubleshooting

Check the Authentication Manager logs, the Swivel Administration Console logs and the Tomcat logs for any error messages

Swivel appliances /var/log/tomcat/catalina.out

No Username entered, or the application does not have permission. Check the logs.



Swivel Authentication Manager Login

Access Denied

Username:

Password:

OTC:

Administrative User cannot login

This is usualy the admin user and by default on the Swivel core, they must be a member of the Swivel Repository Group PINsafeAdministrators, unless a different setting is configured in the settings.properties file, the default is: administrationGroup=PINsafeAdministrators. If it is different the Swivel core will show a successful authentication, but the Authentication Manager fails due to the incorrect group.

Sample Swivel core login information

```
Primary:Read user: admin.

Searching encryption key for the IP: 192.168.12.110, agent name found: Primary

Primary:Login successful for user: admin.

Pimary:Processing user admin as channel SINGLE
```

9.1 Error Messages

Authentication failed for username:

The login attempt failed for the user

Cannot find application for URN:

The application is not configured for authentication, check the Application settings. The URN is supplied to the Authentication manager, and check against the configured applications to find a matching Entity ID. To have the rule match a particular application set the Entity ID to the URN.

No LoggedUser in session, directing to username page

The user has not logged in so is directed to the authentication page.

Error XBM0H: Directory /home/swivel/SwivelAuthenticationManagerDB cannot be created.

java.lang.OutOfMemoryError: PermGen space

"ActiveMQ ShutdownHook" java.lang.OutOfMemoryError: PermGen space

These errors have been seen when there has not been enough memory available to run the Swivel Authentication Manager. See Heap Space Memory Management How to guide.

10 Google Apps Integration

11 Using Swivel for Google Apps Authentication

GoogleApps is a Software-as-a-Service approach to email, calendars and online document sharing. Swivel can provide Two Factor authentication with SMS, Token, Mobile Phone Client and strong Single Channel Authentication TURing, Pinpad or in the Taskbar using RADIUS.

Organisations can configure their GoogleApps domain to use single-sign-on (SSO), all users in the domain are required to use the Swivel authentication, although with the Authentication Manager it is possible for Swivel to log users in to other applications. This means that rather than supply GoogleApps with a username/password, you configure GoogleApps to refer to an authentication portal to authenticate the user. The portal collects and checks the users credentials and passes back the result of the authentication to GoogleApps.

This document describes how Swivel can be configured to act as the authentication portal for GoogleApps.

12 Prerequisites

Swivel authentication platform 3.x

Google account

The authentication page must be placed in a location that can be accessed through the internet, usually by using a NAT to a Swivel virtual or hardware appliance.

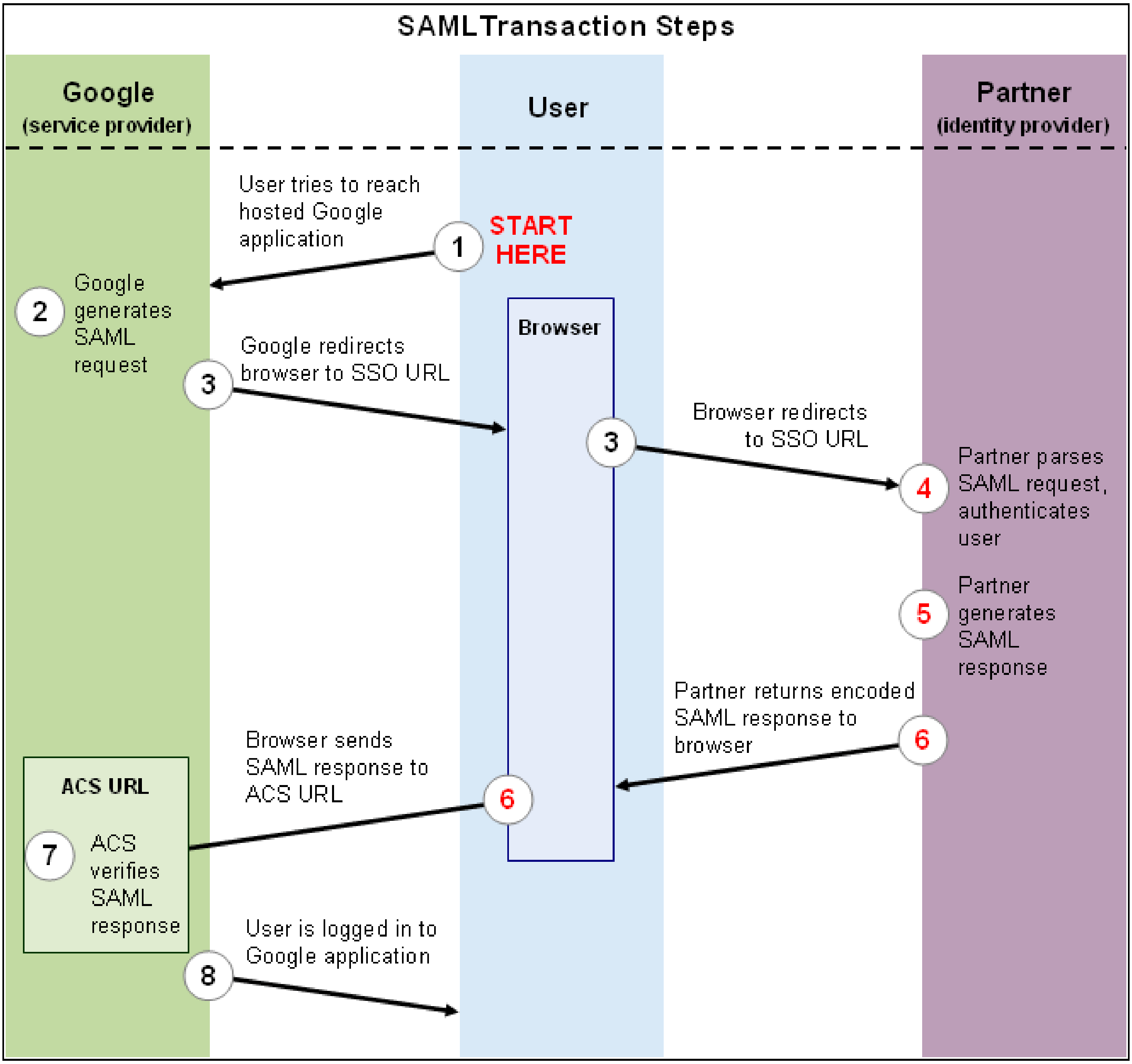
Swivel Google Authentication Portal.

13 Google SSO

The diagram below is taken from Google Apps reference site

When a user attempts to access a Google Apps application Google Apps will look for the presence of a cookie that indicates that the user is an authenticated user. If that cookie is not present the user is redirected to the Partner (Identity Provider) Site.

That redirect will include a SAML request. The request includes the url of the Google Apps ACS (Assertion Consumer Service). This is the Google Apps Service that controls access to Google Apps

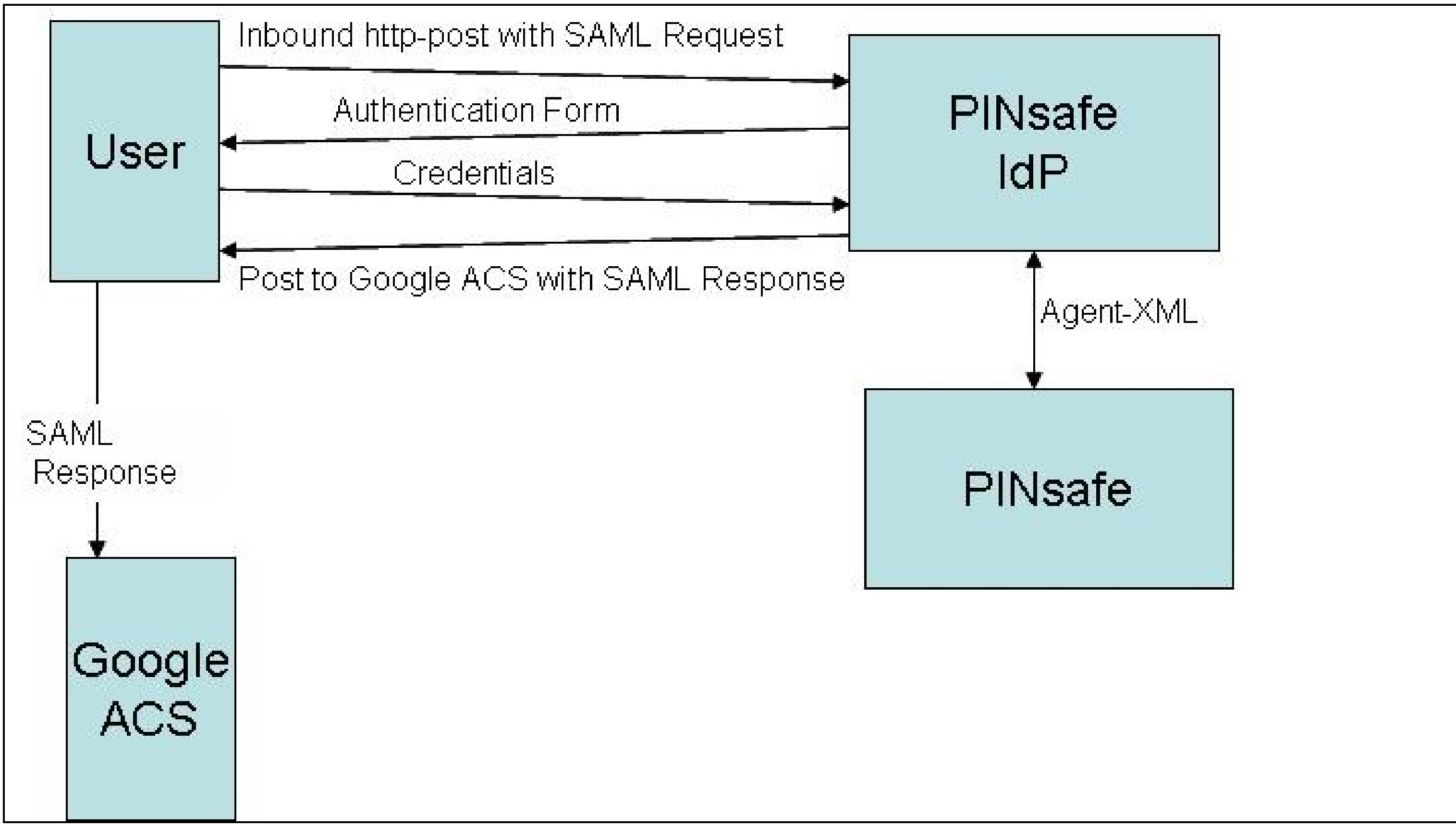


SAMLTransaction Steps
Google
(service provider)
User
Partner
(identity provider)
User tries to reach hosted Google application
1
START HERE
2
Google generates SAML request
Browser
3
Google redirects browser to SSO URL
3
Browser redirects to SSO URL
4
Partner parses SAML request, authenticates user
5
Partner generates SAML response
6
Partner returns encoded SAML response to browser
Browser sends SAML response to ACS URL
6
ACS URL
7
ACS verifies SAML response
8
User is logged in to Google application

The Identity Provider (IdP) authenticates the user. If the authentication is successful it creates a SAML response and posts that response to the url of the Google Apps ACS that it was passed in the SAML request. The ACS then allows the user access as appropriate.

14 Swivel and Google Apps

Swivel has its own XML-based API that it uses for authentication. There is now an external Swivel application that can interpret the inbound SAML request, carry out a standard Swivel authentication via Agent-XML and then post the associated SAML response.



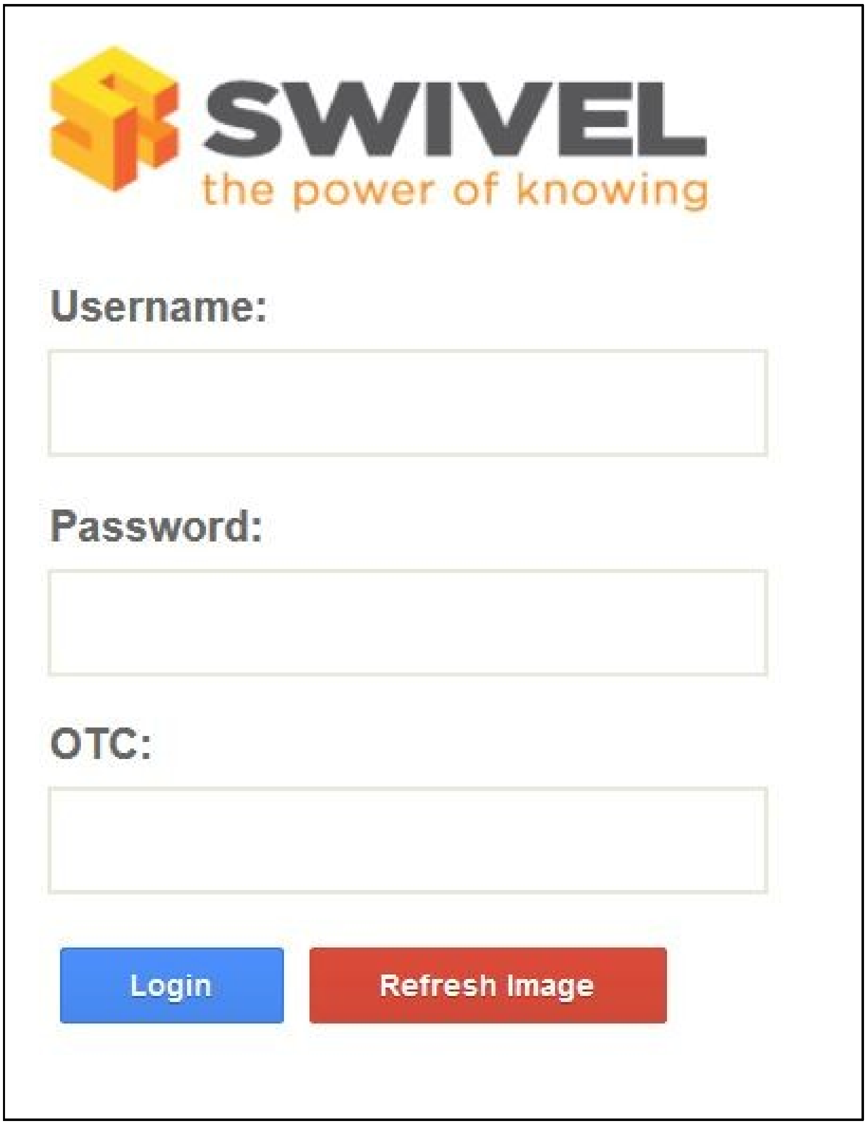
This application needs to be publicly accessible so that users can authenticate to it, it also needs to be configured as an agent on a Swivel server. More detailed configuration information appears later in this document.

15 User Experience

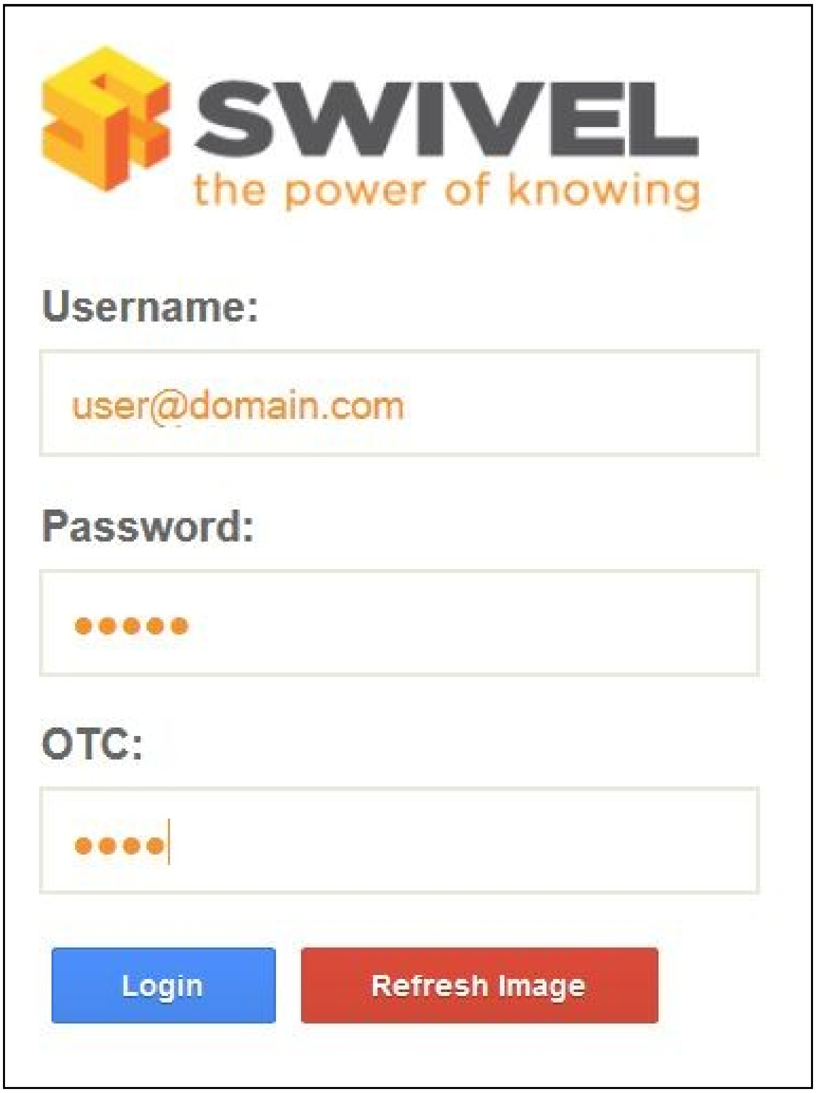
The user opens a browser and accesses googleApps e.g. http://mail.google.com/a/swivelsecure.net this is then redirected in a new URL includes the encrypted SAML request.

What the user sees is a login page familiar to Swivel users. This page can be modified depending on the form of Swivel authentication required. The user authenticates to this form in the same way as any other Swivel authentication form.

Swivel login page



Dual Channel Authentication



Username:

user@domain.com

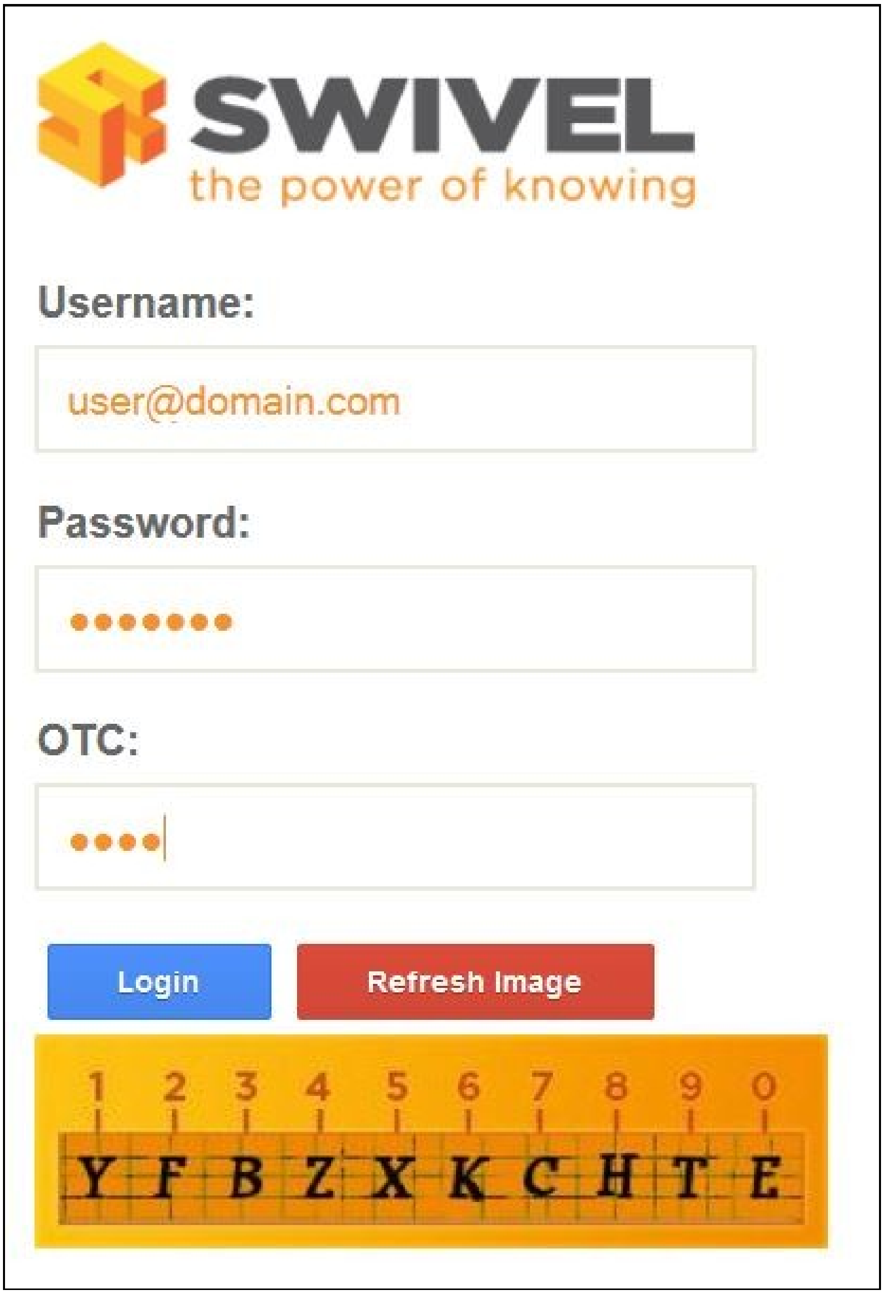
Password:

●●●●●

OTC:

●●●●

Single Channel Authentication



Username:

user@domain.com

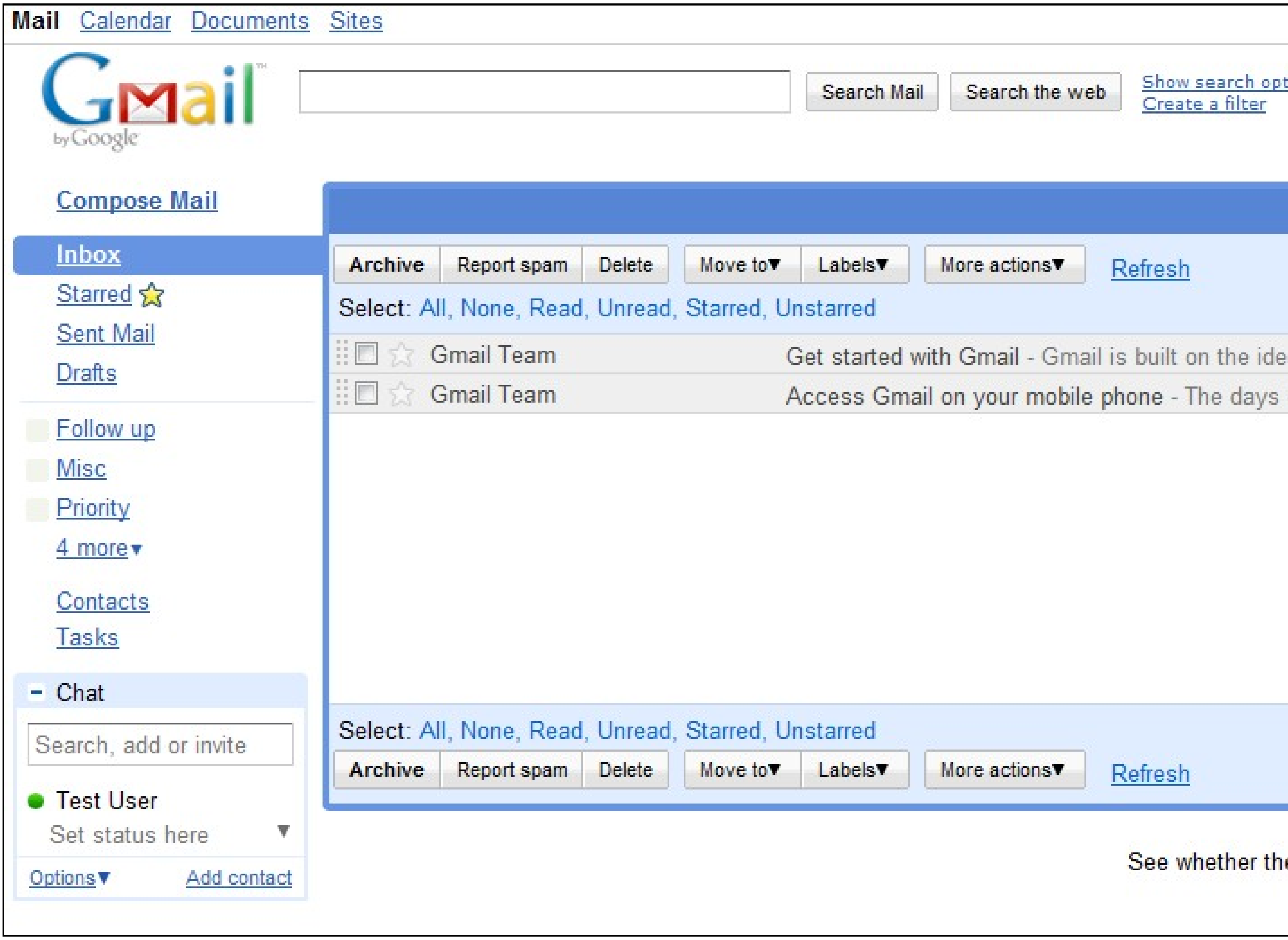
Password:

●●●●●●●

OTC:

●●●●

After the user has submitted the correct credentials, the browser is redirected to the GoogleApps ACS page and then again to the user's landing page. The user is now authenticated and can access any of their GoogleApps.



□ ☆ Gmail Team	Get started with Gmail - Gmail is built on the ide
□ ☆ Gmail Team	Access Gmail on your mobile phone - The days

See whether th

16 Install the Swivel Google software

This is usually deployed on the Swivel server, but may be deployed within a Java container such as Apache Tomcat on another server. In HA deployments with multiple Swivel instances, the Software can be deployed in each instance.

Swivel virtual or hardware appliances: Use WinSCP to copy the AuthenticationPortal-google.war file to /usr/local/tomcat/webapps2

Software installs and older virtual or hardware appliances: copy the AuthenticationPortal-google.war file to the webapps folder of the Apache Tomcat installation.

The google software should create a AuthenticationPortal-google folder.

17 Create private keys and certificates

Communication between Google and the Swivel instance is secure through the use of certificates.

17.1 Creating DSA Private Key

DSA key generation involves two steps, and can be done through the command line on a Swivel virtual or hardware appliance:

1.

```
openssl dsaparam -out dsaparam.pem 2048
```

2.

```
openssl gendsa -out dsaprivkey.pem dsaparam.pem
```

The first step creates a DSA parameter file, dsaparam.pem, which in this case instructs OpenSSL to create a 2048-bit key in Step 2. The dsaparam.pem file is not itself a key, and can be discarded after the public and private keys are created. The second step actually creates the private key in the file dsaprivkey.pem which should be kept secret.

Export the key into a DER (binary) format. You can do so with the following steps:

1.

```
openssl dsa -in dsaprivkey.pem -outform DER -pubout -out dsapubkey.der
```

2.

```
openssl pkcs8 -topk8 -inform PEM -outform DER -in dsaprivkey.pem -out dsaprivkey.der -nocrypt
```

Step 1 extracts the public key into a DER format. Step 2 converts the private key into the pkcs8 and DER format. Once you've done this, you can use this public (dsapubkey.der) and private (dsaprivkey.der) key pair.

17.2 Creating a Certificate

Once you have your key pair, it's easy to create an X.509 certificate. The certificate holds the corresponding public key, along with some metadata relating to the organization that created the certificate. Follow this step to create a self-signed certificate from either an RSA or DSA private key:

```
openssl req -new -x509 -key dsaprivkey.pem -out dsacert.pem
```

After you answer a number of questions, the certificate will be created and saved as dsacert.pem.

The created keys, dsapubkey.der and dsapubkey.der need to be copied to the keys folder or wherever specified within settings.xml

The **dsacert.pem** certificate needs to be uploaded to the GoogleApps server.

18 Configure the Google Swivel install

Edit the AuthenticationPortal-google\WEB-INF\settings.xml file.

pinsafessl default: false - To use SSL communications on the pinsafeport set this to TRUE, to use without SSL set this to False.

pinsafeserver default: adouglas.swivelsecure.net - The hostname or IP address of the Swivel server.

pinsafecontext default: pinsafe - The installation name of the Swivel application.

pinsafesecret default: secret - The shared secret configured on the Swivel server.

pinsafeport default: 8080 - The communication port for the Swivel server.

imagessl default: false - To use SSL communications on the imageserver port set this to TRUE, to use without SSL set this to False.

imageserver default: adouglas.swivelsecure.net - The hostname or IP address used for retrieving images from the Swivel server. This must be contactable from the internet.

imagecontext default: pinsafe - The Swivel installation name used for retrieving images from the Swivel server. For virtual or hardware appliances this is usually *proxy*. For Software installations this is usually *pinsafe*.

imageport default: 8080 - The port used for retrieving images from the Swivel server. For virtual or hardware appliances this is usually 8443. For a software only install see Software Only Installation.

selfsigned default: true - To use SSL communications on the imageserver port with a self signed or invalid certificate set this to TRUE, to use without only the correct SSL certificate set this to False.

certificateIssuer default: SwivelSecure

publicKeyFilePath default: /keys/pinsafe/robssl/dsapubkey.der

privateKeyFilePath default: /keys/pinsafe/robssl/dsaprivkey.der

certificateFilePath default: /keys/pinsafe/robssl/dsacert.pem

19 Writing the configuration data

From a web browser run the following:

For a virtual or hardware appliance

https://Swivel_google_server:8443/AuthenticationPortal-google/configuration.jsp

For a software only install see Software Only Installation

Click on the Generate *Idp Metadata* button.

The *Idp WS-Metadata* button is provided for future enhancements and is not currently used.

This will then generate Metadata files.

Example:

Swivel Virtual Appliance or hardware Appliance:

Metadata successfully written to /usr/local/tomcat/webapps2/AuthenticationPortal-google/generatedIdPMetadata.xml

Software installation:

Metadata successfully written to C:\Program Files (x86)\Apache Software Foundation\Tomcat 6.0\webapps\AuthenticationPortal-google\generatedIdPMetadata.xml

19.1 Configuring Swivel for Agent XML Authentication

The IdP is usually deployed on the Swivel hardware or virutal appliance, and a default localhost Agent is usually pre-configured. To make any changes to this see Agents How to Guide

19.2 Configuring Swivel for Single Channel Images

If Swivel Single Channel images are to be used for authentication, then the following guide can be used.

Single Channel How To Guide

19.3 Configuring Swivel for Dual Channel Authentication

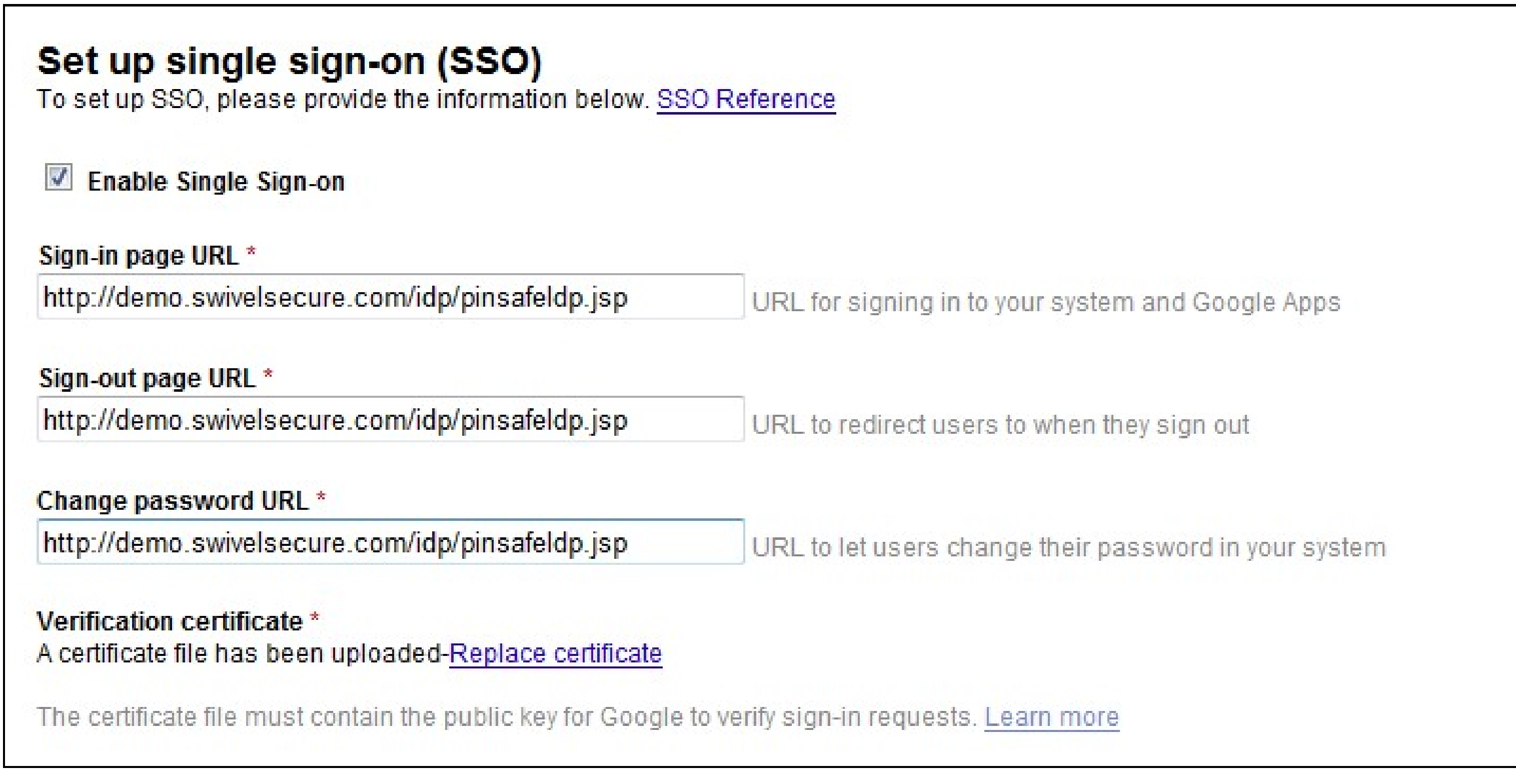
If Swivel Dual Channel authentication methods are to be used, refer to the following guide:

Transport Configuration

20 Configuring Google Apps to use the Swivel IdP

To set GoogleApps to use the Swivel IdP you need to configure the service from the Google Apps admin console.

The settings are under: Security, Advanced settings -> Set up single sign-on (SSO).



Set up single sign-on (SSO)

To set up SSO, please provide the information below. SSO Reference

☑ Enable Single Sign-on

Sign-in page URL *

http://demo.swivelsecure.com/idp/pinsafeldp.jsp

URL for signing in to your system and Google Apps

Sign-out page URL *

http://demo.swivelsecure.com/idp/pinsafeldp.jsp

URL to redirect users to when they sign out

Change password URL *

http://demo.swivelsecure.com/idp/pinsafeldp.jsp

URL to let users change their password in your system

Verification certificate *

A certificate file has been uploaded-Replace certificate

The certificate file must contain the public key for Google to verify sign-in requests. Learn more

You need to enter the public IP address of the Swivel IdP, including the port number and upload the certificate generated in the previous section.

You will need to include the port numbers of the Idp unless you have configured the virtual or hardware appliance firewall (see How to run PINsafe on non-default ports) to map port 80 to the port the Idp is listening on

The **dsacert.pem** certificate needs to be uploaded to the GoogleApps server. If the existing certificate is being replaced and clicking to **Replace certificate** is not working, try in Chrome or Safari web browsers.

21 Testing

Browse to the Swivel Google login page to check that it is working:

Swivel virtual or hardware appliance install: https://swivel_appliance:8443/AuthenticationPortal-google/identity_provider.jsp

For a software only install see Software Only Installation

If these work then browse to the google login page, the browser should be directed to a sign-in page. This page is the Swivel IdP. The url is something like:

http://<idp IP address>/pinsafeIdp.jsp?SAMLRequest=fVLJTsMwEL0j8Q%2BW79kqKiGrCSpFiEosEQ0cuDnOpHXxEjxOA3%2BPm
4KAA72%2BmXnLzMwu3rUiO3AorclpFqeUgBG2kWad06fqOjqnF8XpyQy5Vh2b935jHuGtB%2FQkTBpkYyGnvTPMcpTIDNeAzAu2mt
%2Fdskmcss5Zb4VVlCyvcmqbjkvV1FKDsOZVSWj0tjU1r7fbRnMtTVtvBKwpef62NdnbWiL2sDToufEBSrM0SqdRNqmyKUvP2dn0h
ZLyS%2BlSmkOCY7bqQxOym6oqo%2FJhVY0EO9mAuw%2FdOV1bu1YQC6v38iVHlLsAt1whUDJHBOeDwYU12GtwK3A7KeDp8TanG%2B
87ZEkyDEP8Q5PwBIfAEeZF7yA24BMukBbjftkY0f1a7PEA%2FNsALX4kZskvquLrbvs4y6vSKik%2ByFwpOywccB%2ByeNeHKNfWae
7%2FV8vibERkE7VjK%2BsNdiBkG65HSVIcVP8%2BSHibTw%3D%3D&RelayState=https%3A%2F%2Fwww.google.com%2Fa%2F
swivelsecure.net%2FServiceLogin%3Fservice%3Dmail%26passive%3Dtrue%26rm%3Dfalse%26continue%3Dhttp%253A
%252F%252Fmail.google.com%252Fa%252Fswivelsecure.net%252F%26bsv%3D1eic6yu9oa4y3%26ltmpl%3Ddefault%26ltmplcache%3D2

22 Troubleshooting

Check the Swivel logs.

The Tomcat catalina.out file will display error messages relating to creation of the Meta Data.

Virtual or hardware appliance : /var/logs/tomcat/catalina.out

22.1 Error Messages

This account cannot be accessed because the login credentials could not be verified.

We are unable to process your request at this time, please try again later.

The certificates, address or ports may be incorrect.

Login Failed: Invalid user.

Verify the username used is present on the Swivel instance. Check the Swivel logs for failed authentications.

23 Huddle

WORK IN PROGRESS PLEASE CONTACT SWIVEL IF YOU REQUIRE THIS INTEGRATION

24 Overview

Huddle is a content management and enterprise collaboration in the cloud. This document outlines how to add Swivel Two factor and strong authentication. When a user browses to their huddle account example: https://swivelsecure.huddle.net/ they are redirected to the Swivel login page for authentication.

25 Prerequisites

Swivel authentication platform 3.x

Huddle account

The authentication page must be placed in a location that can be accessed through the internet, usually by using a NAT to a Swivel appliance.

25.1 Downloads

AuthenticationPortal-huddle.war software

26 Baseline

(The version tested with)

Swivel authentication platform 3.9.5

27 Architecture

28 Installation

28.1 Configure The Swivel Server

Configure a Swivel Agent (For standard XML Authentication)

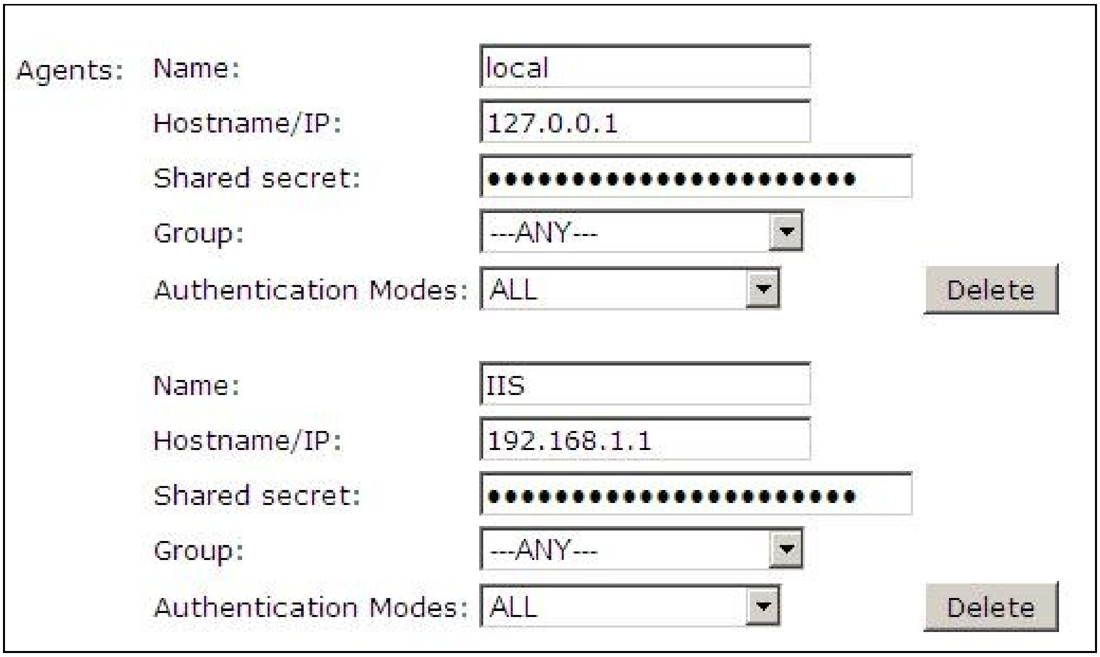
1. On the Swivel Management Console select Server/Agent

2. Enter a name for the Agent

3. Enter the Exchange IP address

4. Enter the shared secret used above on the Exchange Filter

5. Click on Apply to save changes



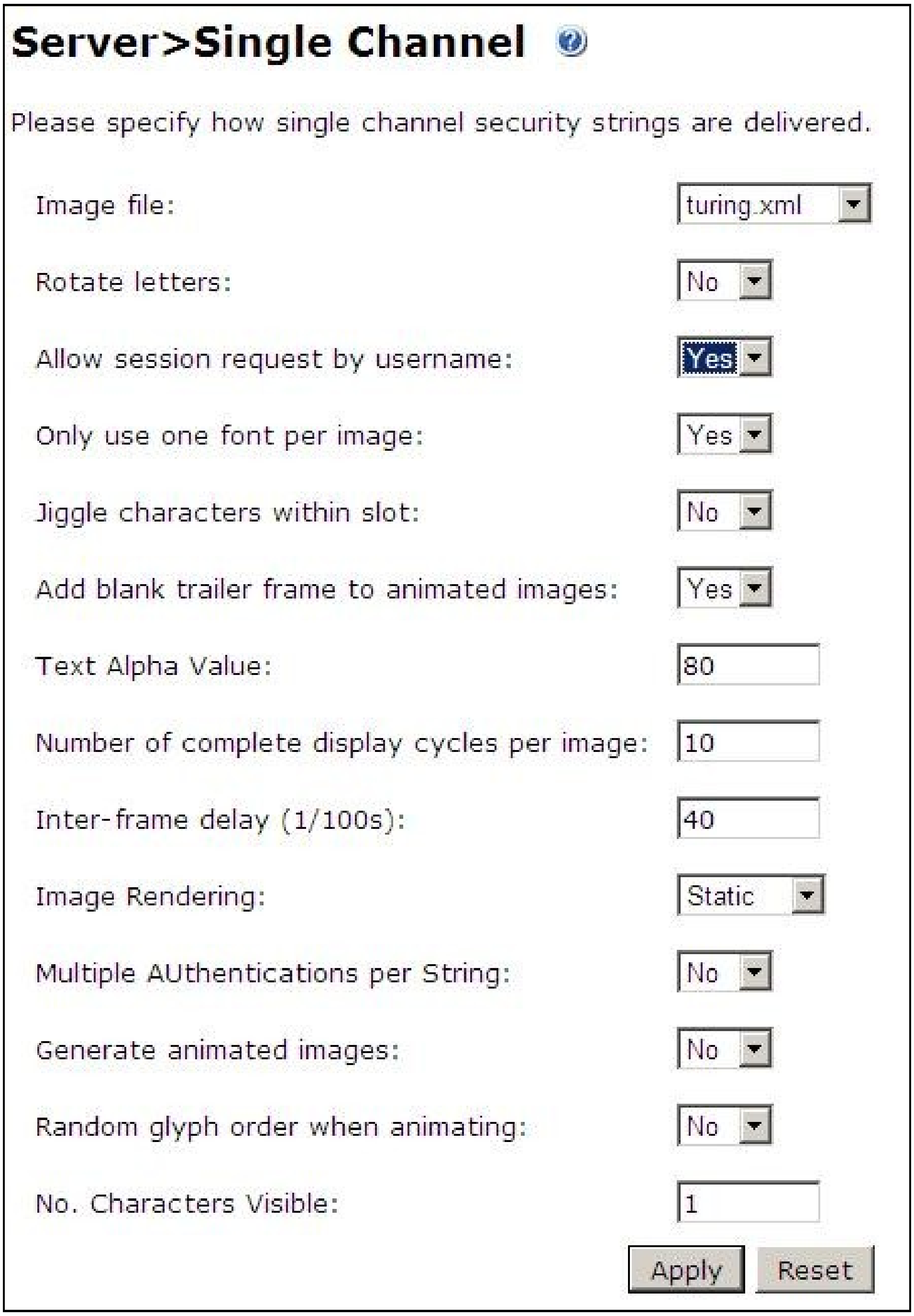
Agents: Name: local
Hostname/IP: 127.0.0.1
Shared secret: ●●●●●●●●●●●●●●●●●●●●●●●
Group: ---ANY---
Authentication Modes: ALL

Name: IIS
Hostname/IP: 192.168.1.1
Shared secret: ●●●●●●●●●●●●●●●●●●●●●●●
Group: ---ANY---
Authentication Modes: ALL

Configure Single Channel Access

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

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



Server>Single Channel

Please specify how single channel security strings are delivered.

Image file:	turing.xml
Rotate letters:	No
Allow session request by username:	Yes
Only use one font per image:	Yes
Jiggle characters within slot:	No
Add blank trailer frame to animated images:	Yes
Text Alpha Value:	80
Number of complete display cycles per image:	10
Inter-frame delay (1/100s):	40
Image Rendering:	Static
Multiple AUthentications per String:	No
Generate animated images:	No
Random glyph order when animating:	No
No. Characters Visible:	1

28.2 Using additional attributes for authentication

When using additional attributes for authentication see User Attributes How To

28.3 Install the Swivel Huddle software

This is usually deployed on the Swivel server, but may be deployed within a Java container such as Apache Tomcat on another server. In HA deployments with multiple Swivel instances, the Software can be deployed in each instance.

Swivel appliances: Use WinSCP to copy the AuthenticationPortal-huddle.war file to /usr/local/tomcat/webapps2

Software installs and older appliances: copy the AuthenticationPortal-huddle.war file to the webapps folder of the Apache Tomcat installation.

The huddle software should create a AuthenticationPortal-huddle folder.

28.4 Create private keys and certificates

Communication between Huddle and the Swivel instance is secure through the use of certificates.

28.4.1 Creating DSA Private Key

DSA key generation is given below, and can be done through the command line on a Swivel appliance:

1. Create a DSA parameter file, dsaparam.pem, which in this case instructs OpenSSL to create a 1024-bit key. The dsaparam.pem file is not itself a key, and can be discarded after the public and private keys are created.

```
openssl dsaparam -out dsaparam.pem 1024
```

2. create a private key in the file dsaprivkey.pem which should be kept secret.

```
openssl gendsa -out dsaprivkey.pem dsaparam.pem
```

3. Export the key into a DER (binary) format.

```
openssl dsa -in dsaprivkey.pem -outform DER -pubout -out dsapubkey.der
```

4. Convert the private key into the pkcs8 and DER format. Once you've done this, you can use this public (dsapubkey.der) and private (dsaprivkey.der) key pair.

```
openssl pkcs8 -topk8 -inform PEM -outform DER -in dsaprivkey.pem -out dsaprivkey.der -nocrypt
```

28.4.2 Creating a Certificate

Once you have your key pair, it's easy to create an X.509 certificate. The certificate holds the corresponding public key, along with some metadata relating to the organization that created the certificate. Follow this step to create a self-signed certificate from either an RSA or DSA private key:

```
openssl req -new -x509 -key dsaprivkey.pem -out dsacert.pem
```

After you answer a number of questions, the certificate will be created and saved as dsacert.pem. The created keys, dsapubkey.der and dsapubkey.der need to be copied to the keys folder or wherever specified within settings.xml

The dsacert.pem certificate needs to be sent to the Huddle team, see below.

28.5 Configure the Huddle Swivel install

Edit the AuthenticationPortal-huddle\WEB-INF\settings.xml file.

pinsafessl default: false, To use SSL communications on the pinsafeport set this to TRUE, to use without SSL set this to False.

pinsafeserver default: adouglas.swivelsecure.net, The hostname or IP address of the Swivel server.

pinsafecontext default: pinsafe, The installation name of the Swivel application.

pinsafesecret default: secret, The shared secret configured on the Swivel server.

pinsafeport default: 8080, The communication port for the Swivel server.

imagessl default: false, To use SSL communications on the imageserver port set this to TRUE, to use without SSL set this to False.

imageserver default: adouglas.swivelsecure.net, The hostname or IP address used for retrieving images from the Swivel server. This must be contactable from the internet.

imagecontext default: pinsafe, The Swivel installation name used for retrieving images from the Swivel server. For appliances this is usually *proxy*. For Software installations this is usually *pinsafe*.

imageport default: 8080, The port used for retrieving images from the Swivel server. For appliances this is usually 8443. For a software only install see Software Only Installation.

selfsigned default: true, To use SSL communications on the imageserver port with a self signed or invalid certificate set this to TRUE, to use without only the correct SSL certificate set this to False.

certificateIssuer default: SwivelSecure,

publicKeyFilePath default: /keys/pinsafe/robssl/dsapubkey.der,

privateKeyFilePath default: /keys/pinsafe/robssl/dsaprivkey.der,

certificateFilePath default: /keys/pinsafe/robssl/dsacert.pem,

28.6 Writing the configuration data

From a web browser run the following:

For an appliance

https://Swivel_huddle_server:8443/AuthenticationPortal-huddle/configuration.jsp

For a software only install see Software Only Installation

Click on the Generate *Idp Metadata* button.

The *Idp WS-Metadata* button is provided for future use.

This will then generate Metadata files.

Example:

Appliance:

Metadata successfully written to /usr/local/tomcat/webapps2/AuthenticationPortal-huddle/generatedIdPMetadata.xml

Software installation:

Metadata successfully written to C:\Program Files (x86)\Apache Software Foundation\Tomcat 6.0\webapps\AuthenticationPortal-huddle\generatedIdPMetadata.xml

28.7 Huddle Integration

Send the following files to the Huddle team sales@huddle.com together with the company name:

dsacert.pem

generatedIdPMetadata.xml

28.8 Additional Installation Options

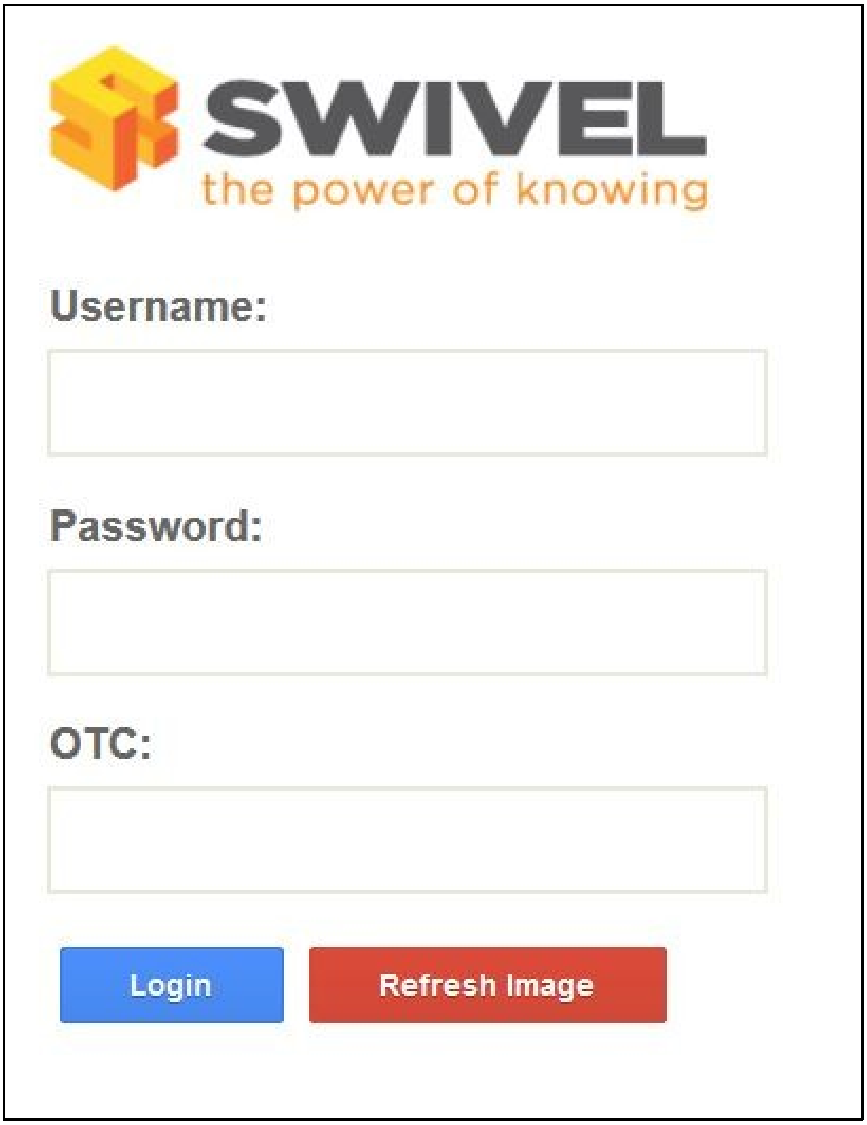
29 Testing the Installation

Browse to the Swivel huddle login page to check it is working:

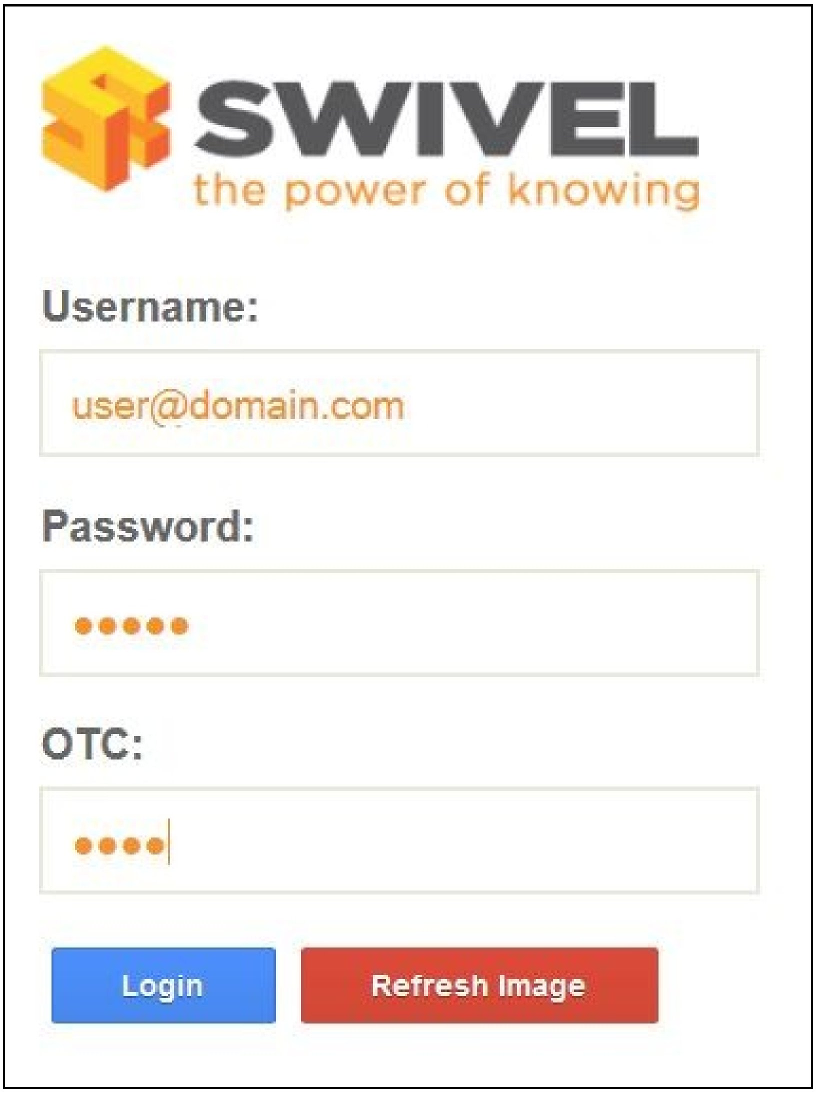
Swivel appliance install: https://swivel_appliance:8443/AuthenticationPortal-huddle/identity_provider.jsp

For a software only install see Software Only Installation

Swivel login page



Dual Channel Authentication



Username:

user@domain.com

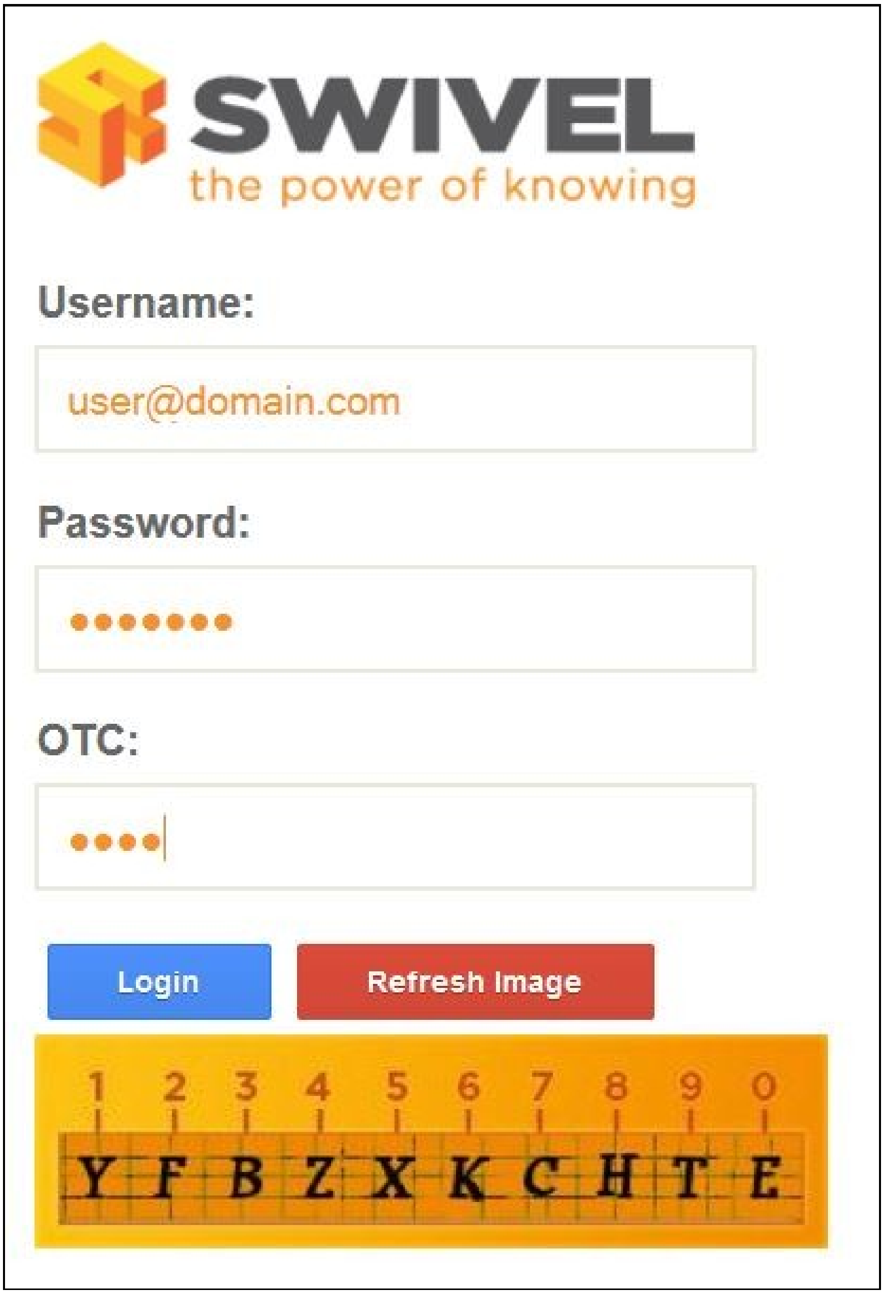
Password:

●●●●●

OTC:

●●●●

Single Channel Authentication



Username:

user@domain.com

Password:

●●●●●●●

OTC:

●●●●

If these work then browse to the huddle login page which should redirect to the Swivel authentication page to give a login. Example: https://swivelsecure.huddle.net/

30 Uninstalling the Swivel Integration

31 Troubleshooting

Check the Swivel logs.

The Tomcat catalina.out file will display error messages relating to creation of the Meta Data.

Appliance : /var/logs/ctomcat/catalina.out

32 Known Issues and Limitations

33 Additional Information

For assistance in the Swivel installation and configuration please firstly contact your reseller and then email Swivel Secure support at support@swivelsecure.com.

34 Microsoft IIS version 6 Integration

34.1 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.

34.2 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:

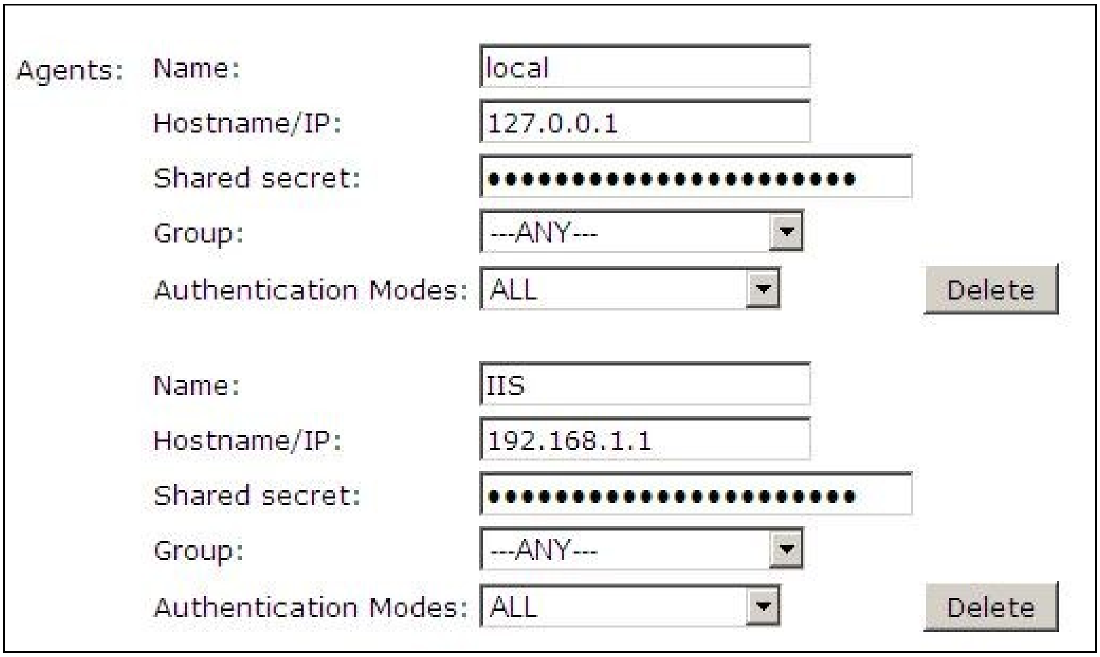
- 32-bit ISAPI Filter
- 64-bit ISAPI Filter

34.3 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:

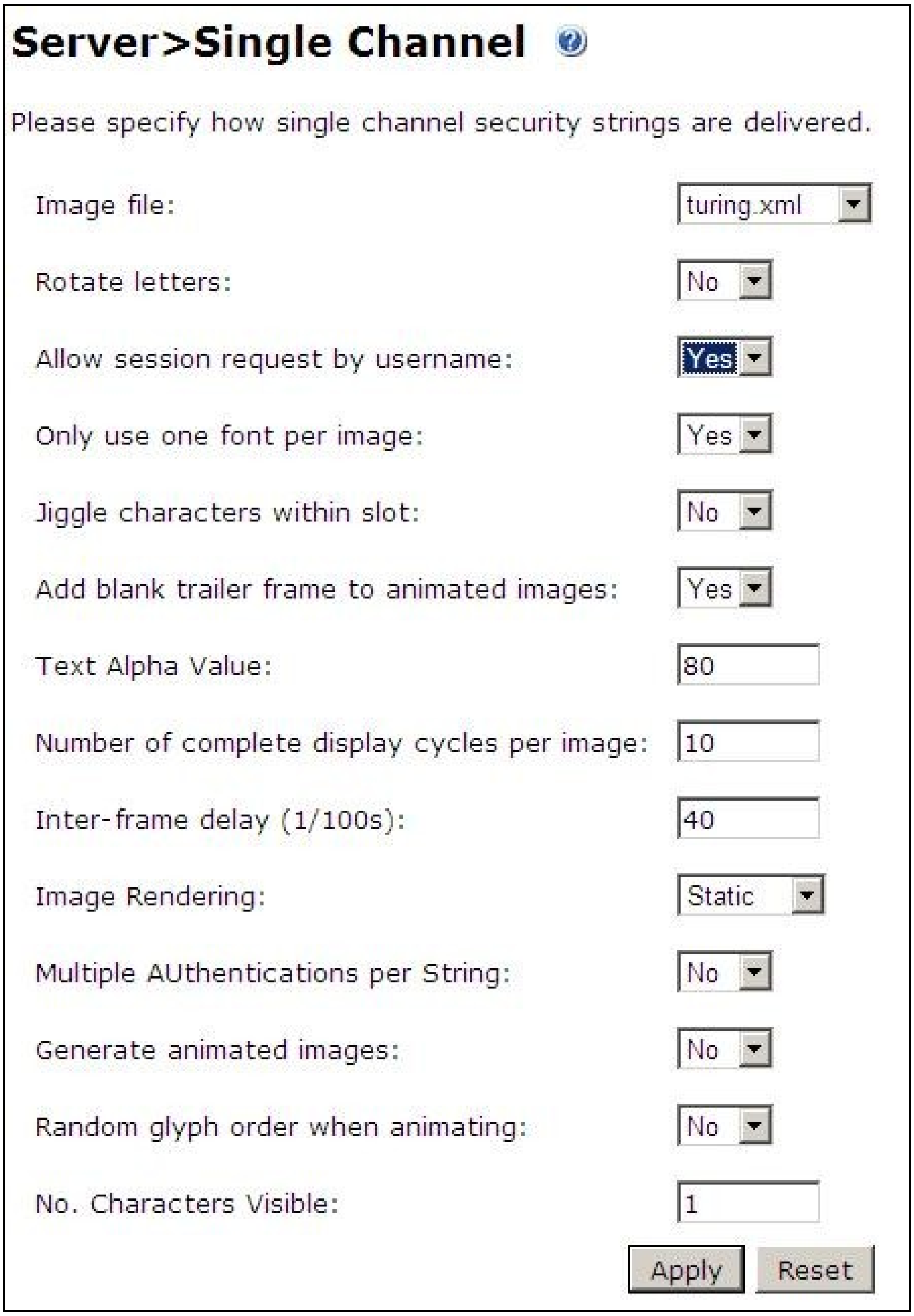
```
Name : IIS server 1,
Hostname/IP : 192.168.1.1,
shared secret : secret
```



Agents: Name: local
Hostname/IP: 127.0.0.1
Shared secret: ●●●●●●●●●●●●●●●●●●●●●●
Group: ---ANY---
Authentication Modes: ALL

Name: IIS
Hostname/IP: 192.168.1.1
Shared secret: ●●●●●●●●●●●●●●●●●●●●●●
Group: ---ANY---
Authentication Modes: ALL

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.



Server>Single Channel

Please specify how single channel security strings are delivered.

Image file:	turing.xml
Rotate letters:	No
Allow session request by username:	Yes
Only use one font per image:	Yes
Jiggle characters within slot:	No
Add blank trailer frame to animated images:	Yes
Text Alpha Value:	80
Number of complete display cycles per image:	10
Inter-frame delay (1/100s):	40
Image Rendering:	Static
Multiple AUthentications per String:	No
Generate animated images:	No
Random glyph order when animating:	No
No. Characters Visible:	1

34.4 Configuring the IIS Server

34.4.1 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.

34.4.2 Configure the ISAPI filter

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

34.4.3 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.

34.4.4 Install The IIS ISAPI filter

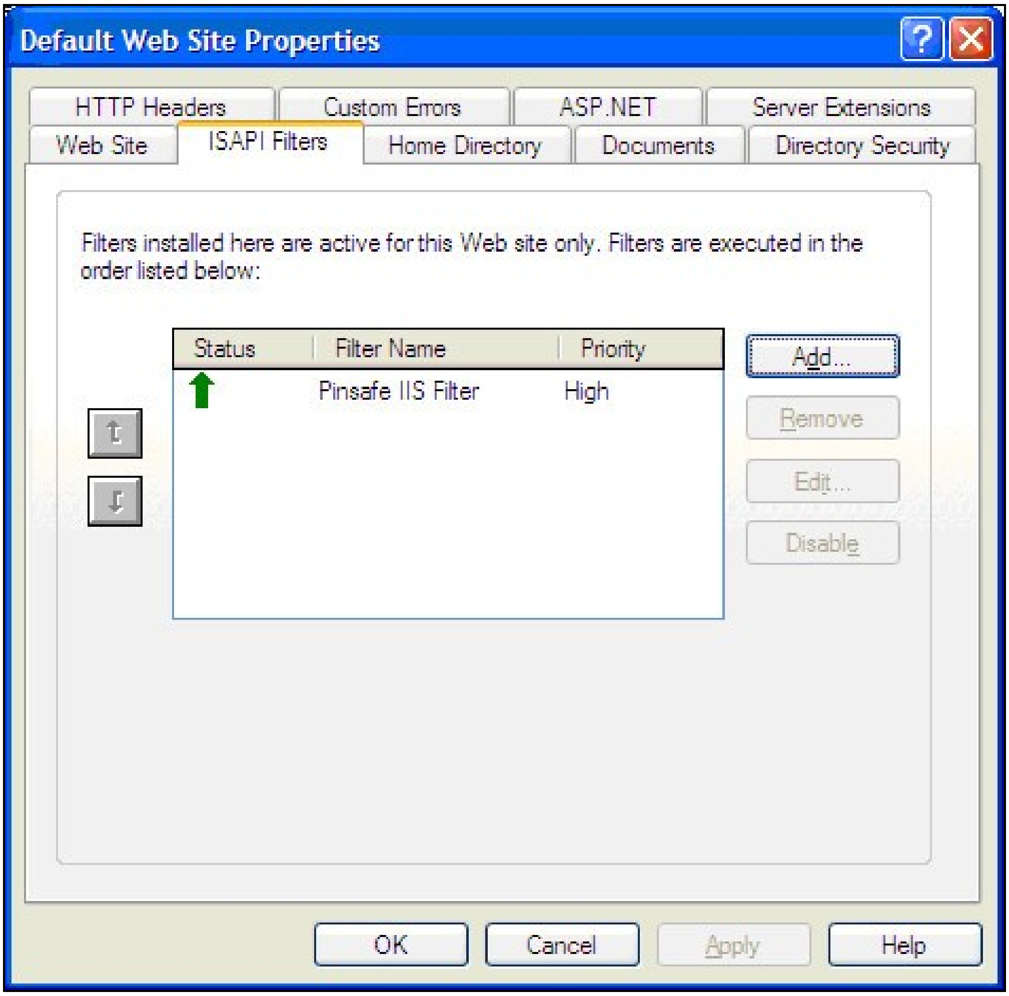
1. On the Internet Information Services Manager Select the Properties for the website

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

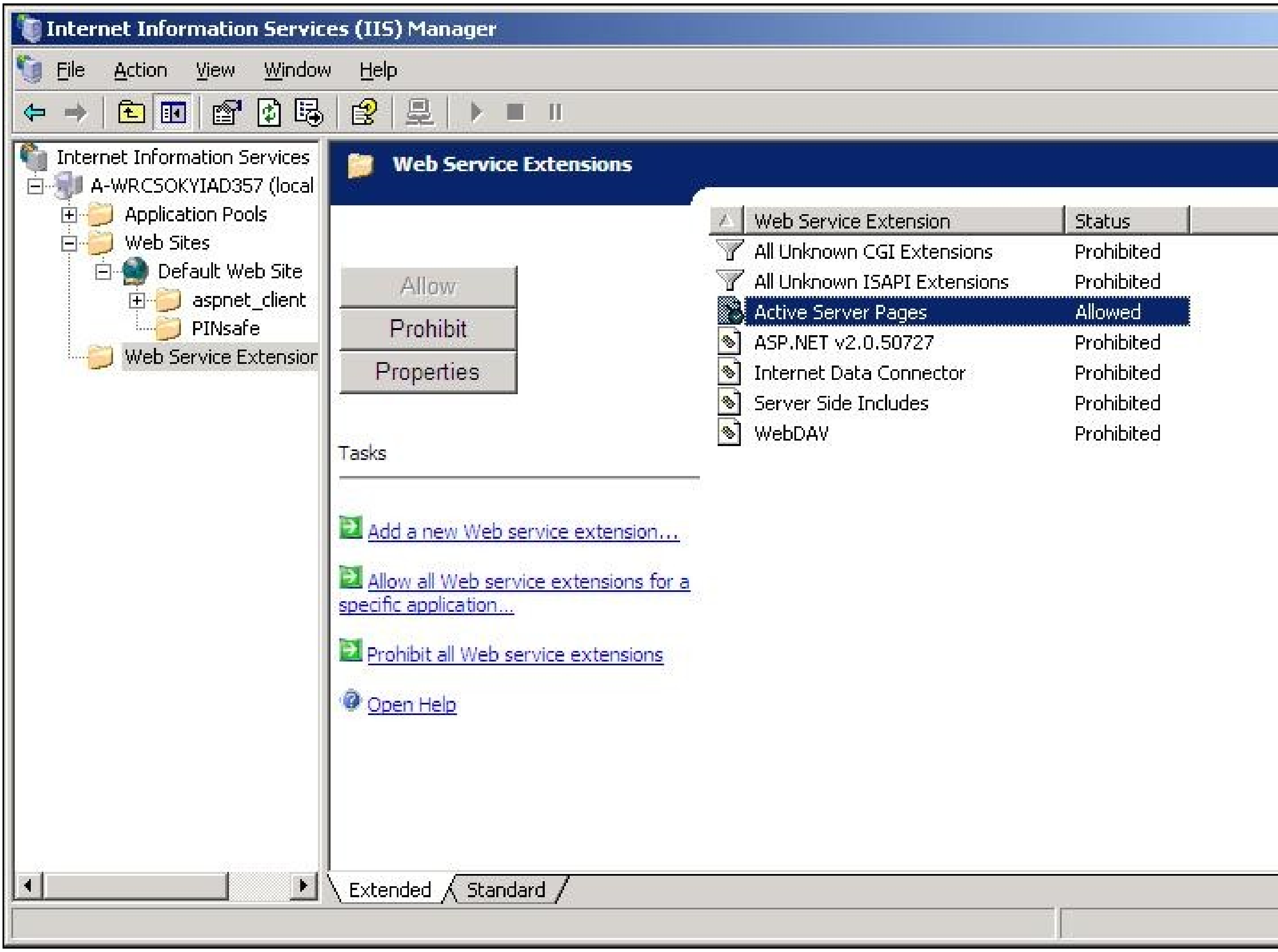


Filters installed here are active for this Web site only. Filters are executed in the order listed below:

Status	Filter Name	Priority
↑	Pinsafe IIS Filter	High

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.

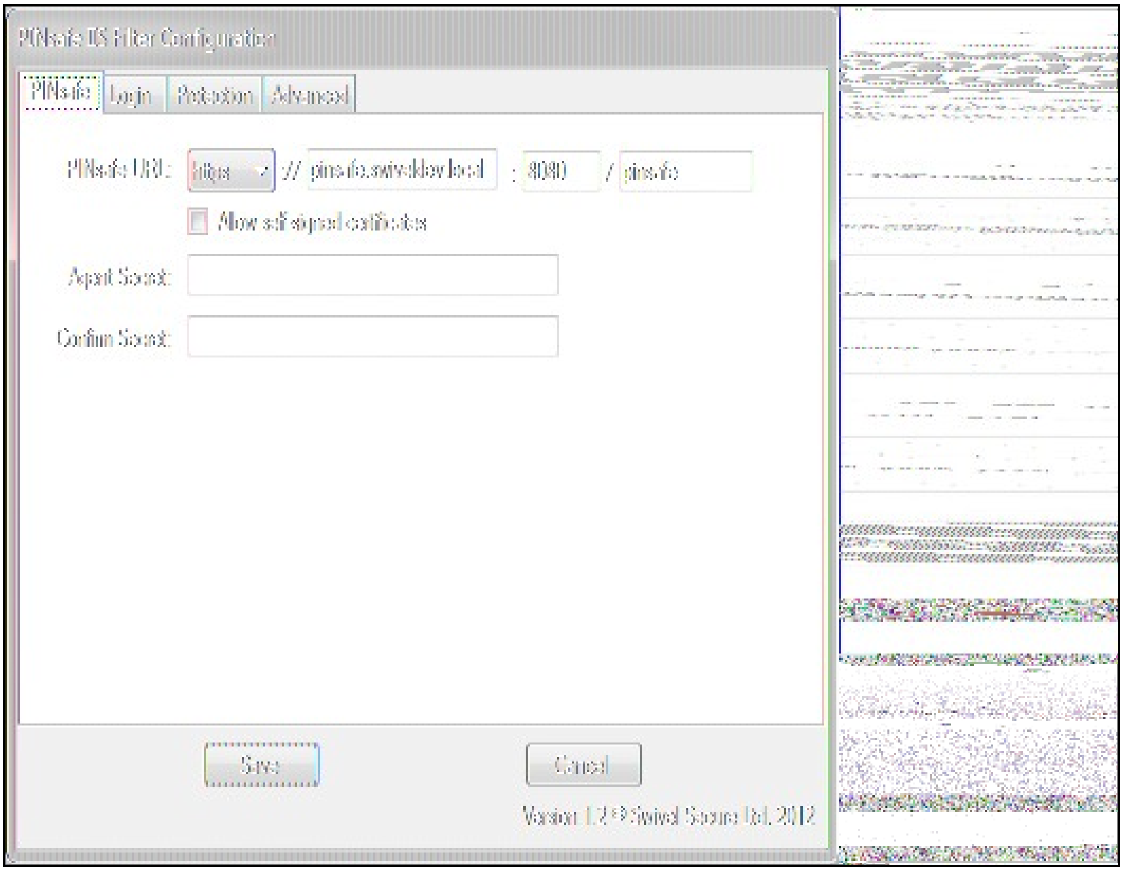


Web Service Extension	Status
All Unknown CGI Extensions	Prohibited
All Unknown ISAPI Extensions	Prohibited
Active Server Pages	Allowed
ASP.NET v2.0.50727	Prohibited
Internet Data Connector	Prohibited
Server Side Includes	Prohibited
WebDAV	Prohibited

34.5 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.

34.5.1 PINsafe Server Settings


PINsafe IIS Filter Configuration
PINsafe
Login
Protection
Advanced
Save
Cancel
Version 1.2 © Swivel Secure Ltd. 2012

PINsafe URL: https :// pinsafe.swiveldev.local : 8080 / pinsafe

□ Allow self signed certificates

Agent Secret:

Confirm Secret:

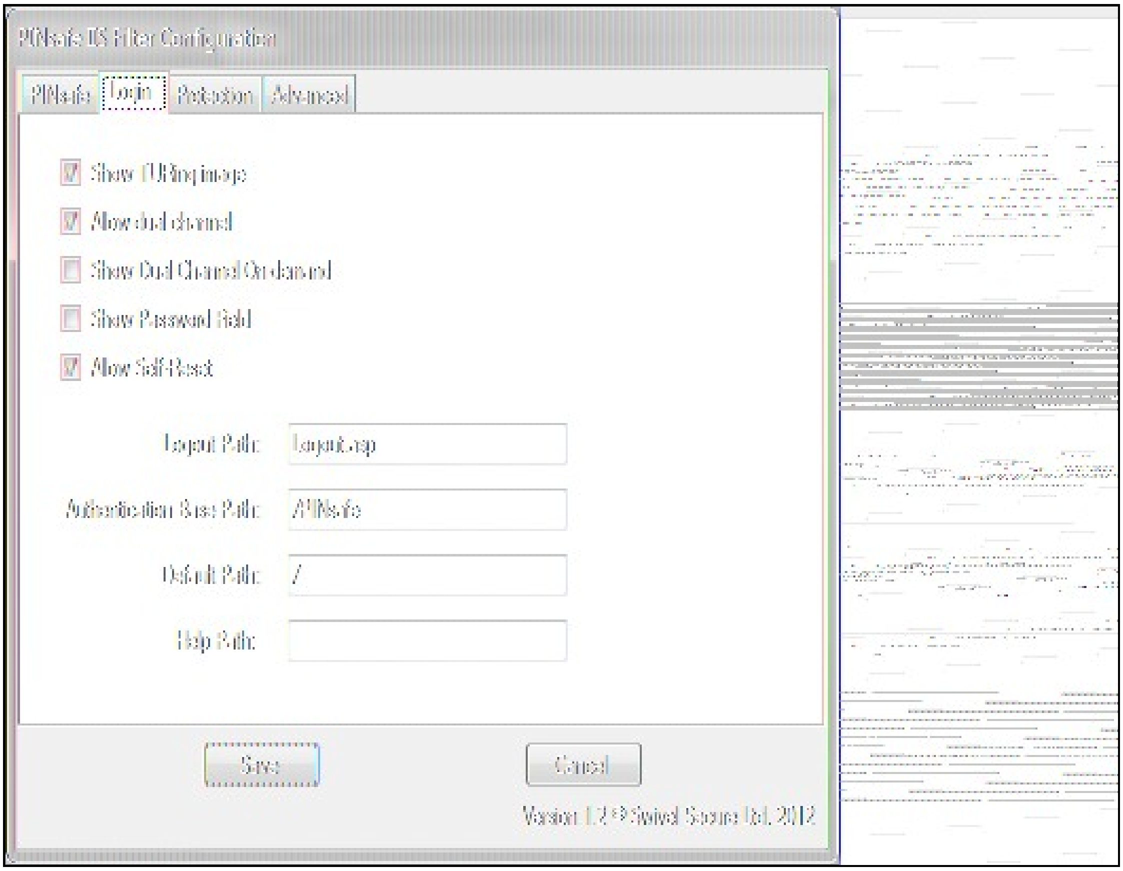
This page defines the connection to the PINsafe server.

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.

34.5.2 Login Page Settings


PINsafe IIS Filter Configuration
PINsafe
Login
Protection
Advanced
Save
Cancel
Version 1.2 © Swivel Secure Ltd. 2012

☑ Show TURing image

☑ Allow dual channel

□ Show Dual Channel On-demand

□ Show Password Field

☑ Allow Self-Reset

Logout Path: logout.asp

Authentication Base Path: /PINsafe

Default Path: /

Help Path:

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.

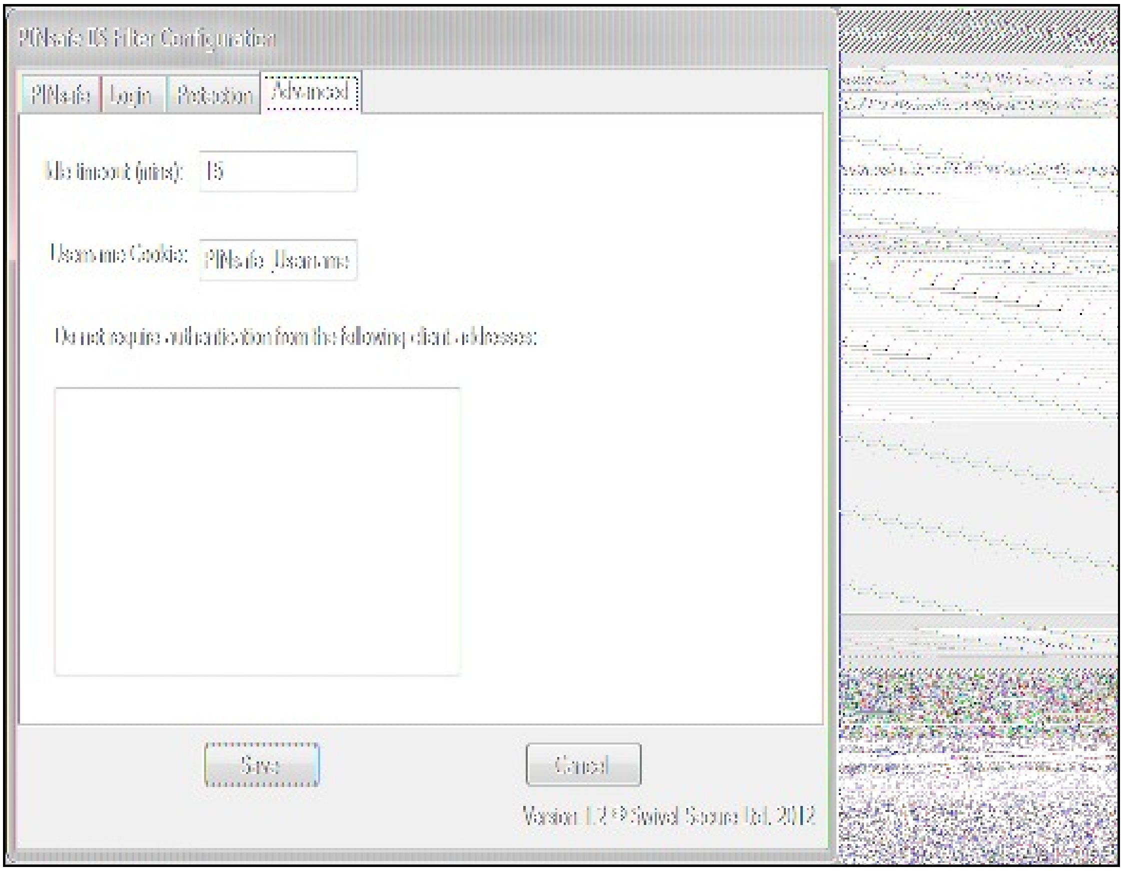
Authentication Base Path: the virtual path containing the PINsafe authentication pages.

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.

34.5.3 Advanced Settings

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


PINsafe IIS Filter Configuration
PINsafe
Login
Protection
Advanced
Save
Cancel
Version 1.2 © Swivel Secure Ltd. 2012

Idle timeout (mins): 15

Username Cookie: PINsafe_Username

Do not require authentication from the following client addresses:

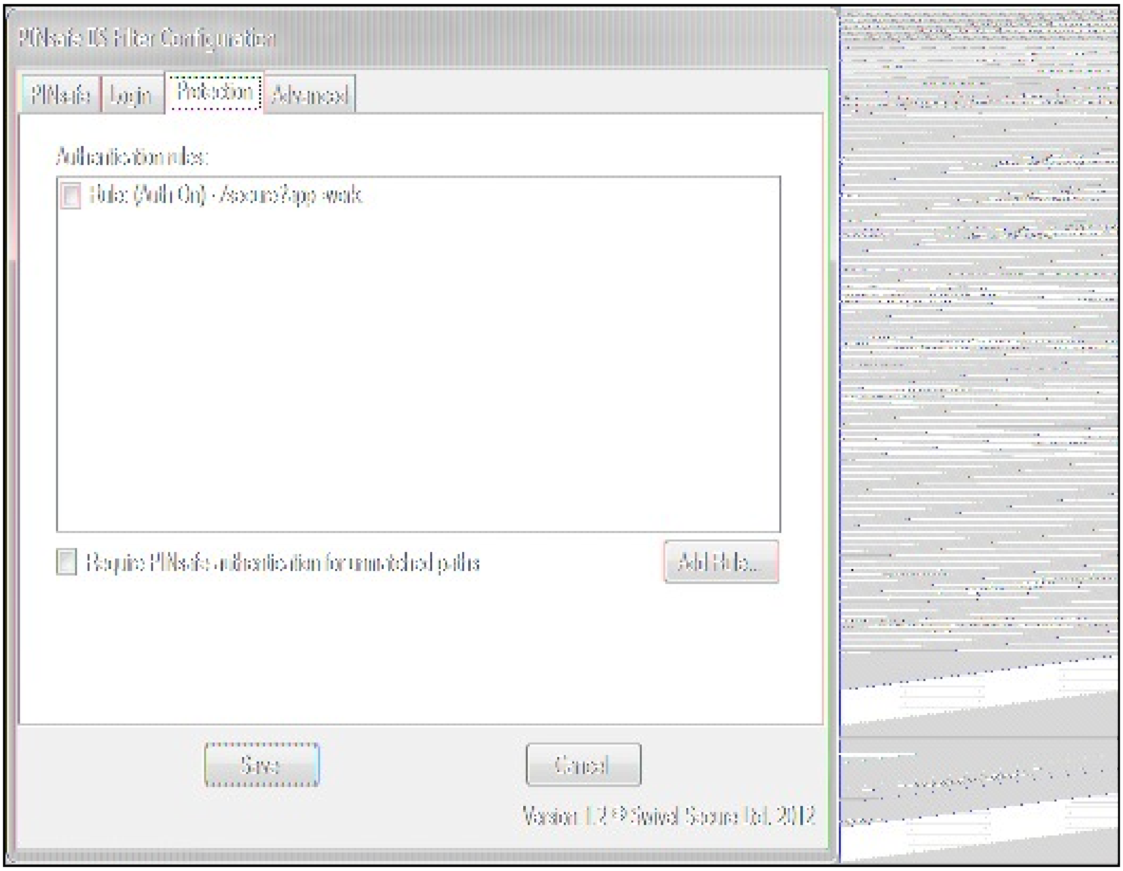
Idle timeout is the time (in minutes) that the user can leave a page open without refreshing it or navigating to another page: in other words, the lifetime of the authentication cookie. However, if the user requests a new page (or refreshes the current one) within that time, the cookie expiration time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

34.5.4 Protection Settings

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



PINsafe IIS Filter Configuration

PINsafe | Login | Protection | Advanced

Authentication rules:

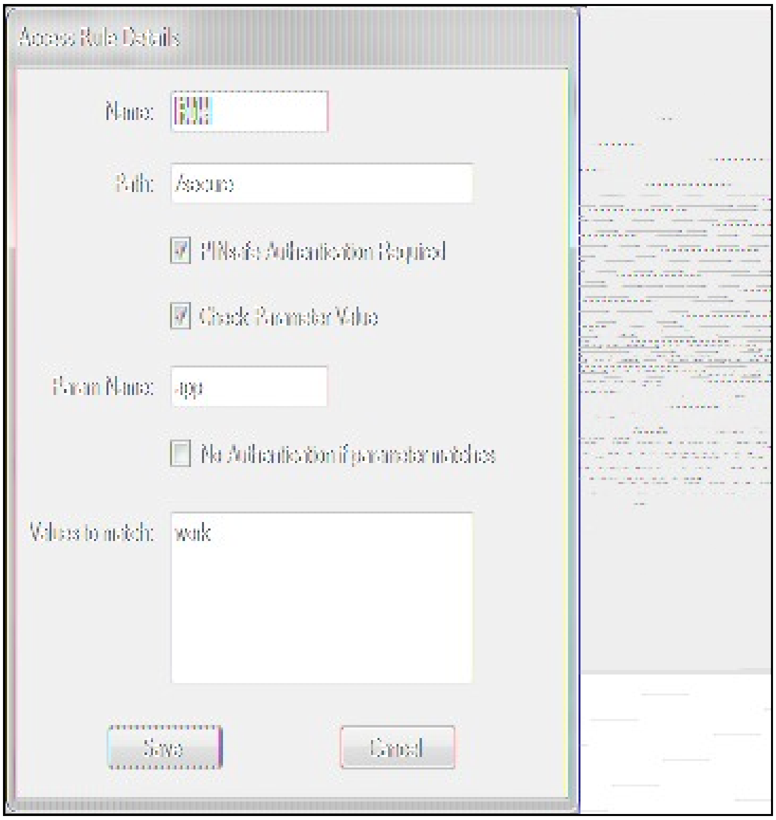
☐ Rule: (Auth On) - /secure?app=work

☐ Require PINsafe authentication for unmatched paths

Version 1.2 © Swivel Secure Ltd. 2012

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.



Access Rule Details

Name: Rule

Path: /secure

☑ PINsafe Authentication Required

☑ Check Parameter Value

Param Name: app

☐ No Authentication if parameter matches

Values to match: work

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.

34.5.5 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.

34.5.6 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.

34.6 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.

34.6.1 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.

34.7 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:

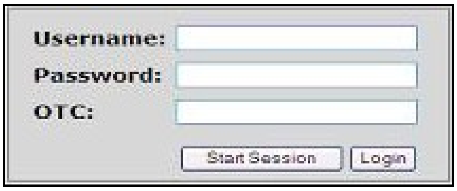
1. Make a copy of the entire Web folder, including the bin sub-folder. You can copy it as a sub-folder of PINsafe IIS filter, with a different name, or you can put it somewhere completely different. It is important, however, that you keep the structure the same ? all the .asp files must remain intact,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

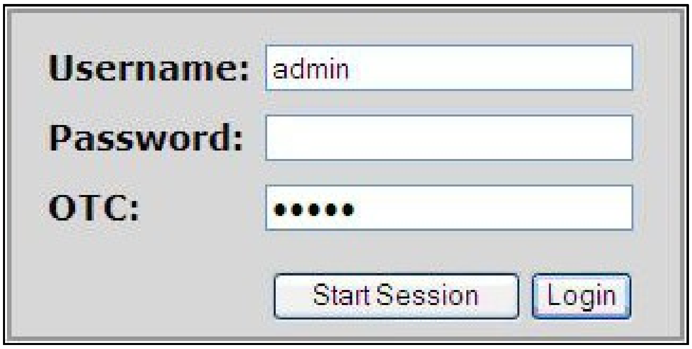
34.8 Testing

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:

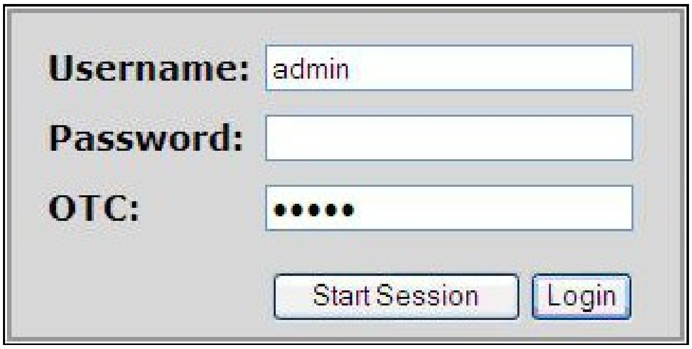


Username: admin

Password:

OTC: •••••

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

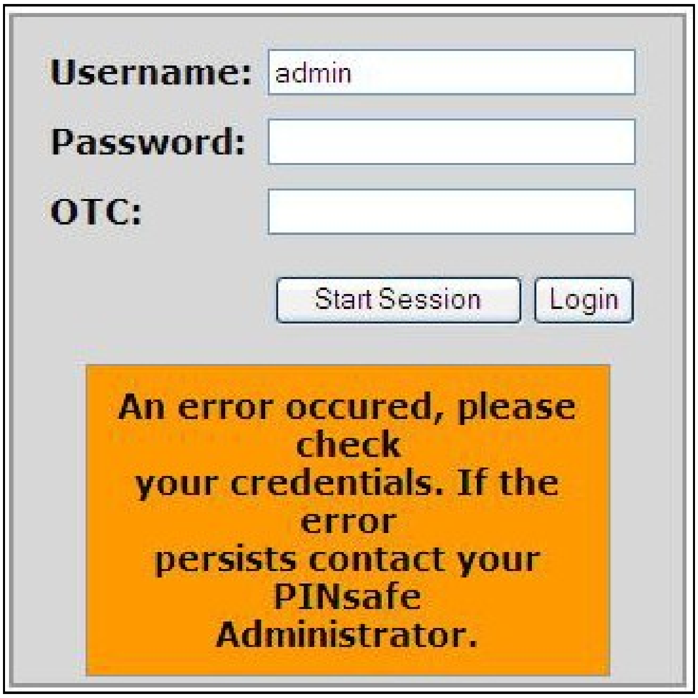


Username: admin

Password:

OTC: •••••

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.



Username: admin

Password:

OTC:

An error occured, please check
your credentials. If the error
persists contact your PINsafe Administrator.

34.9 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.

34.9.1 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.

35 Microsoft IIS version 7 ASP.NET Forms Integration

35.1 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.

35.2 Prerequisites

PINsafe

ASP.NET application

ASP.NET Server

35.3 Baseline

PINsafe 3.7

IIS6 and IIS7

35.4 Architecture

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

35.5 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.

35.6 PINsafe Configuration

35.6.1 Configure a PINsafe Agent

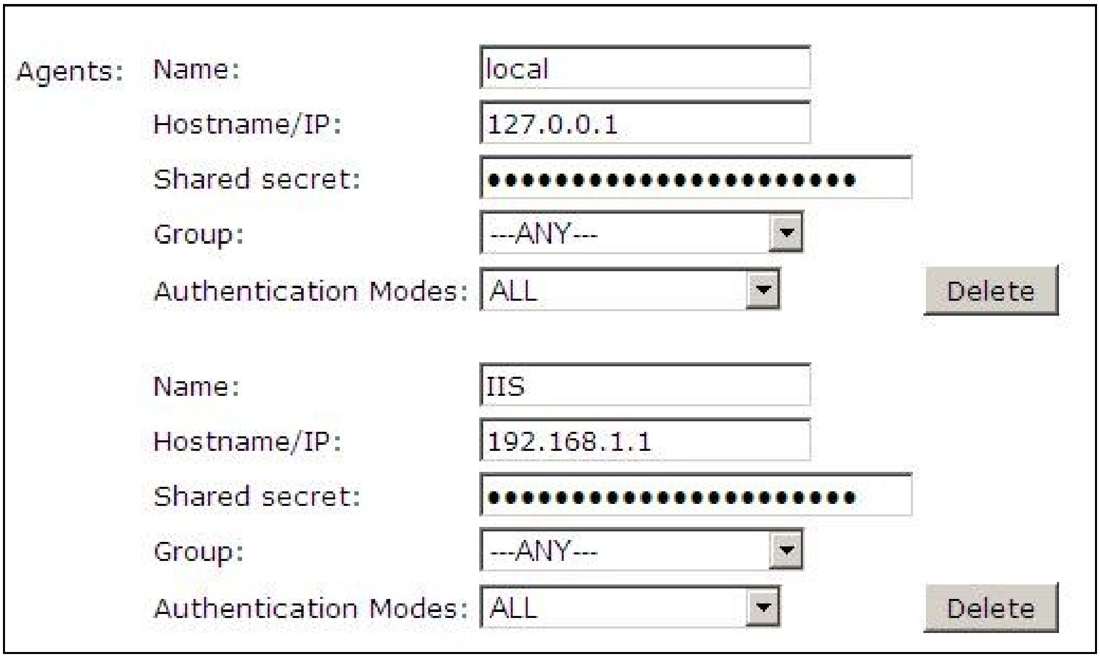
1. On the PINsafe Management Console select Server/Agent

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



Agents:

Name: local

Hostname/IP: 127.0.0.1

Shared secret: ••••••••••••••••••••••

Group: ---ANY---

Authentication Modes: ALL

Name: IIS

Hostname/IP: 192.168.1.1

Shared secret: ••••••••••••••••••••••

Group: ---ANY---

Authentication Modes: ALL

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

35.7 ASP.NET Configuration

35.7.1 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.

35.7.2 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" />
```

35.7.3 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.

35.7.4 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).

35.8 Additional Configuration Options

35.9 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.

35.10 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

35.11 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

35.12 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

36 Microsoft IIS version 7 ASP.NET Integration

36.1 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.

36.2 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.

36.3 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.

36.4 PINsafe Configuration

36.4.1 Configure a PINsafe Agent

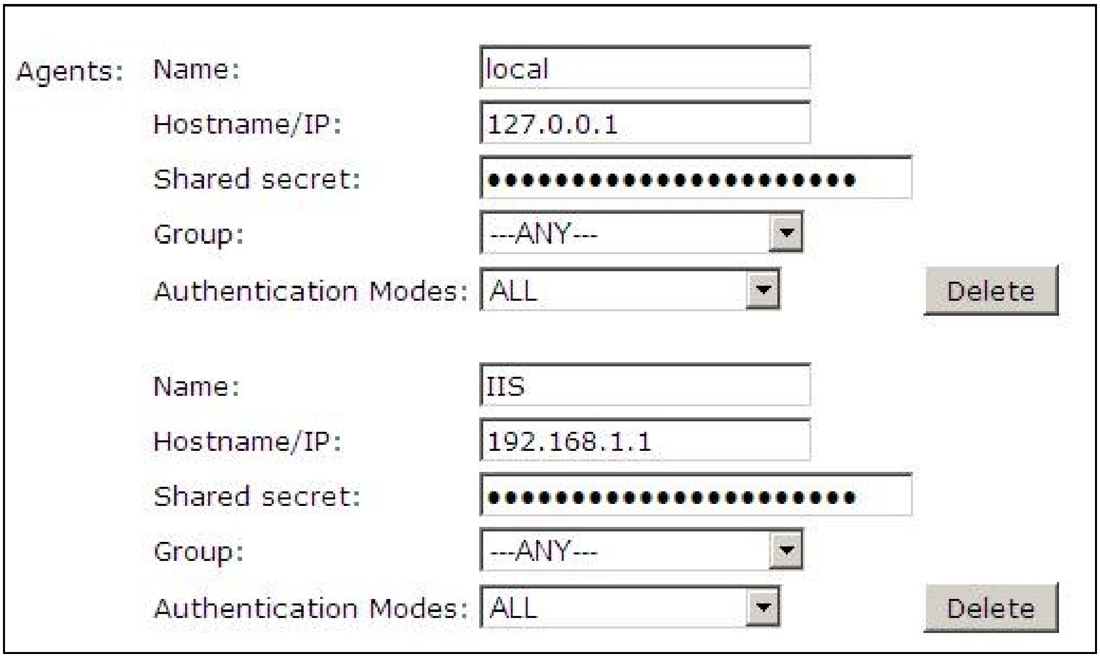
1. On the PINsafe Management Console select Server/Agent

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



Agents: Name: local
Hostname/IP: 127.0.0.1
Shared secret: •••••••••••••••••••••••
Group: ---ANY---
Authentication Modes: ALL

Name: IIS
Hostname/IP: 192.168.1.1
Shared secret: •••••••••••••••••••••••
Group: ---ANY---
Authentication Modes: ALL

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

36.5 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.

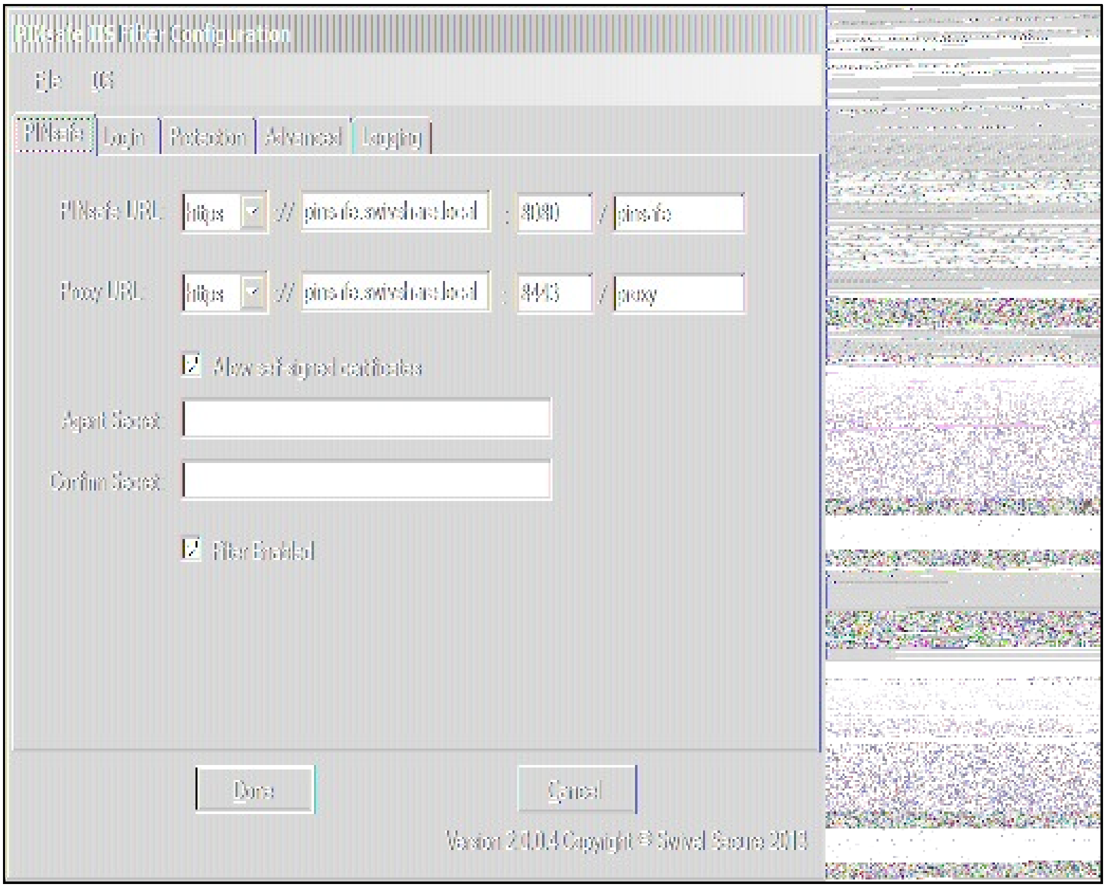
Once the filter is installed, you will be taken to the configuration program (unless you choose not to do so yet).

36.6 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.

36.6.1 PINsafe Tab


PINsafe IIS Filter Configuration
File
OK
PINsafe
Login
Protection
Advanced
Logging
Done
Cancel
Version 2.0.0.4 Copyright © Swivel Secure 2013

PINsafe URL: https :// pinsafe.swivelsecure.local : 8080 / pinsafe

Proxy URL: https :// pinsafe.swivelsecure.local : 8443 / proxy

☑ Allow self-signed certificates

Agent Secret:

Confirm Secret:

☑ Filter Enabled

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.

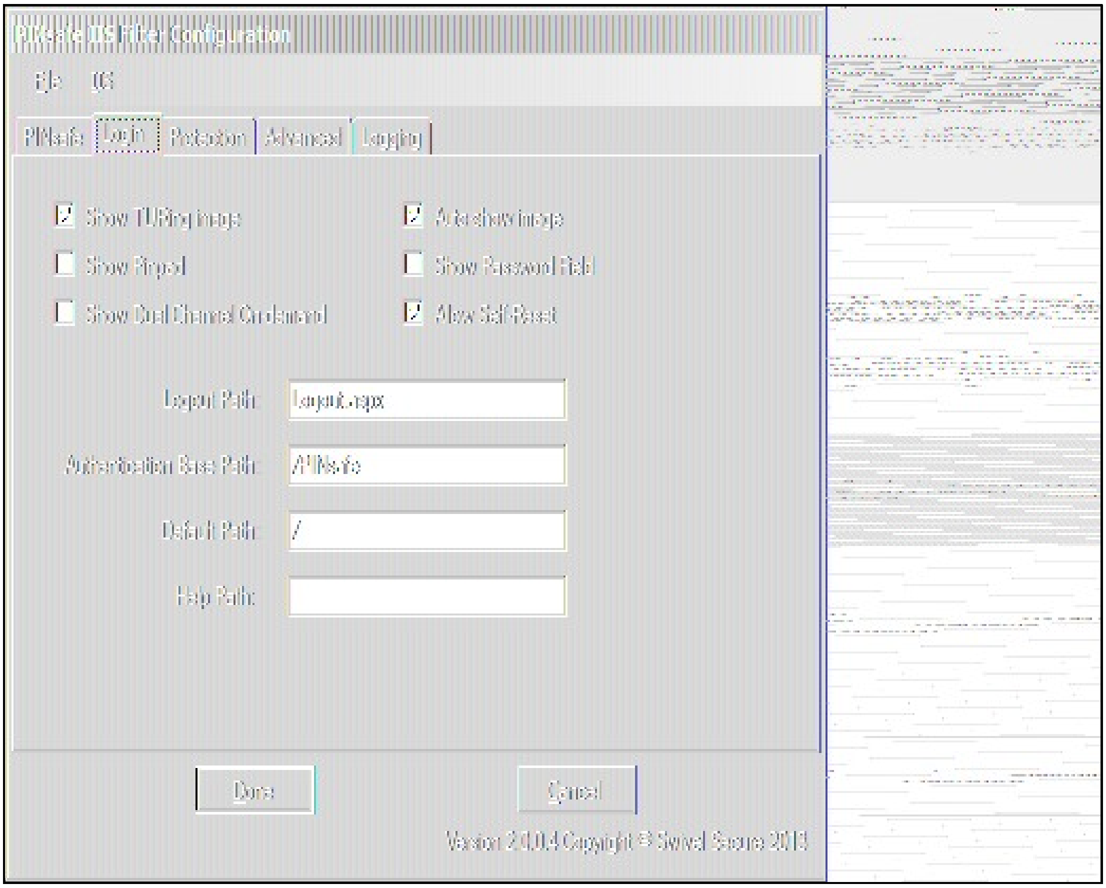
Note that the URLs only need to be resolvable and accessible from the web server. Direct access for the end user to the PINsafe server is not required - the filter proxies all requests.

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.

36.6.2 Login Tab



☑ Show TURing image
☑ Auto show image
□ Show Pinpad
□ Show Password Field
□ Show Dual Channel On demand
☑ Allow Self-Reset

Logout Path: Logout.aspx
Authentication Base Path: /PINsafe
Default Path: /
Help Path:

Version 2.0.0.4 Copyright © Swivel Secure 2013

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**.

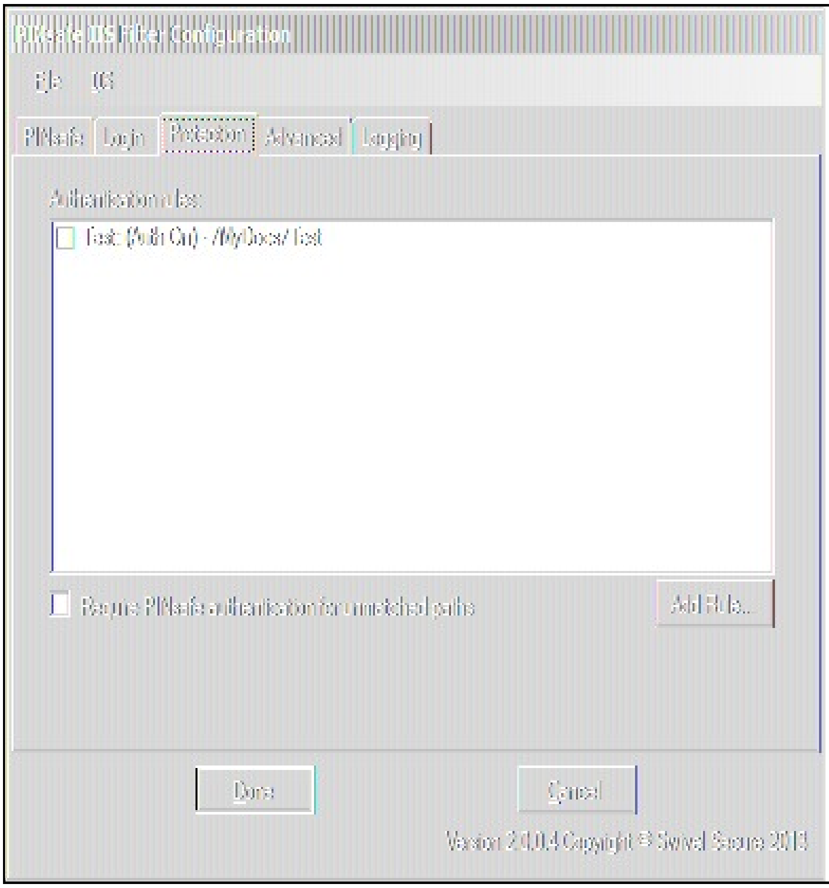
Logout path is the full path used to log out from PINsafe. Typically, this will be /PINsafe/Logout.aspx. If this is detected in the URL, the PINsafe authentication cookie will be removed, and users must re-authenticate to access protected URLs.

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**.

36.6.3 Protection Tab



Authentication rules:

□ Test: (Auth On) - /MyDocs/Test

□ Require PINsafe authentication for unmatched paths

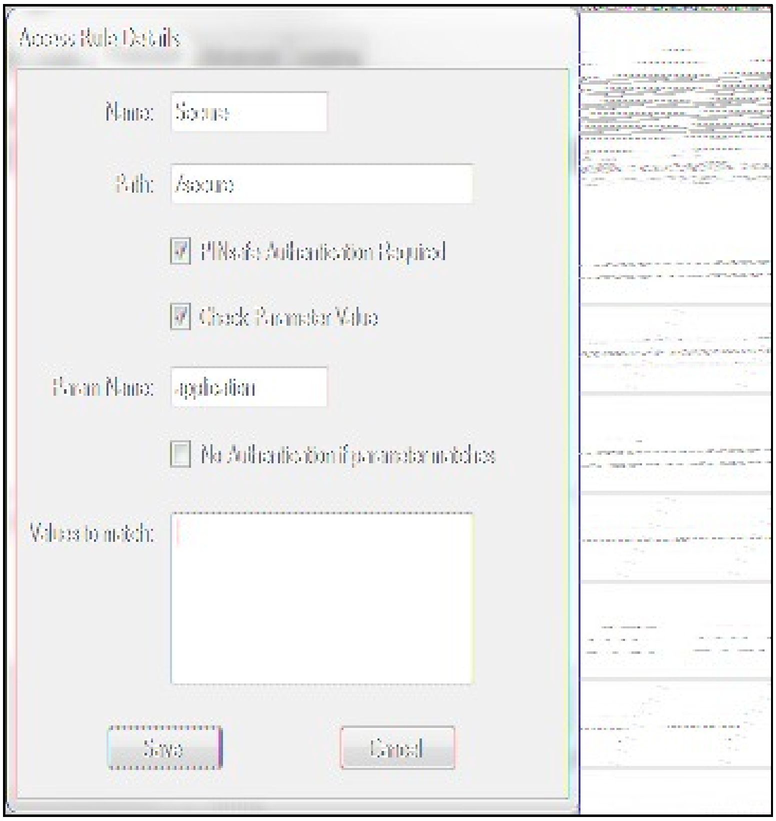
Version 2.0.0.4 Copyright © Swivel Secure 2013

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:



Access Rule Details

Name: Secure

Path: /secure

☑ PINsafe Authentication Required

☑ Check Parameter Value

Param Name: application

□ No Authentication if parameter matches

Values to match:

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.

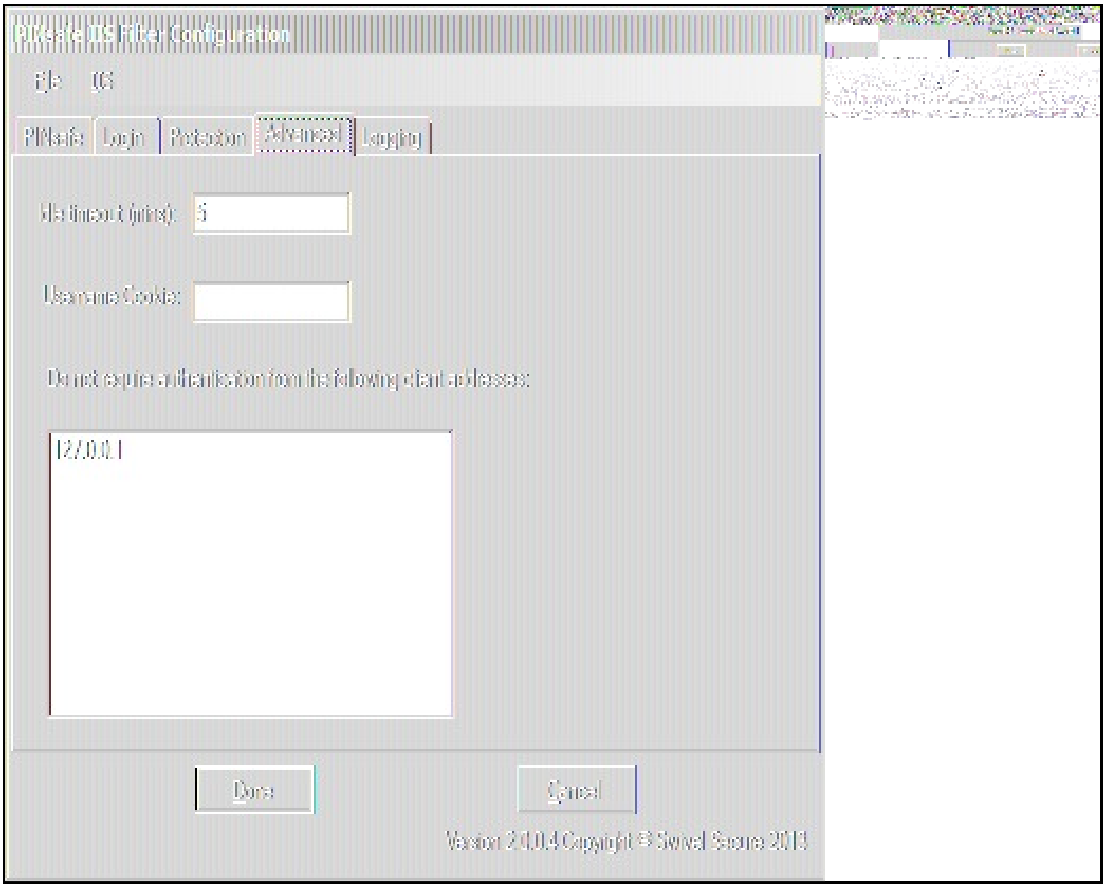
"Check Parameter Value" allows finer control over PINsafe authentication. When checked, you can specify the name of a single query parameter that is checked to determine whether or not PINsafe authentication is required. You can specify a list of possible values for the parameter, but if you specify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

36.6.4 Advanced Tab


PINsafe IIS Filter Configuration

Idle timeout (mins): 5

Username Cookie:

Do not expire authentication from the following client addresses:

127.0.0.1

Version 2.0.0.4 Copyright © Swivel Secure 2013

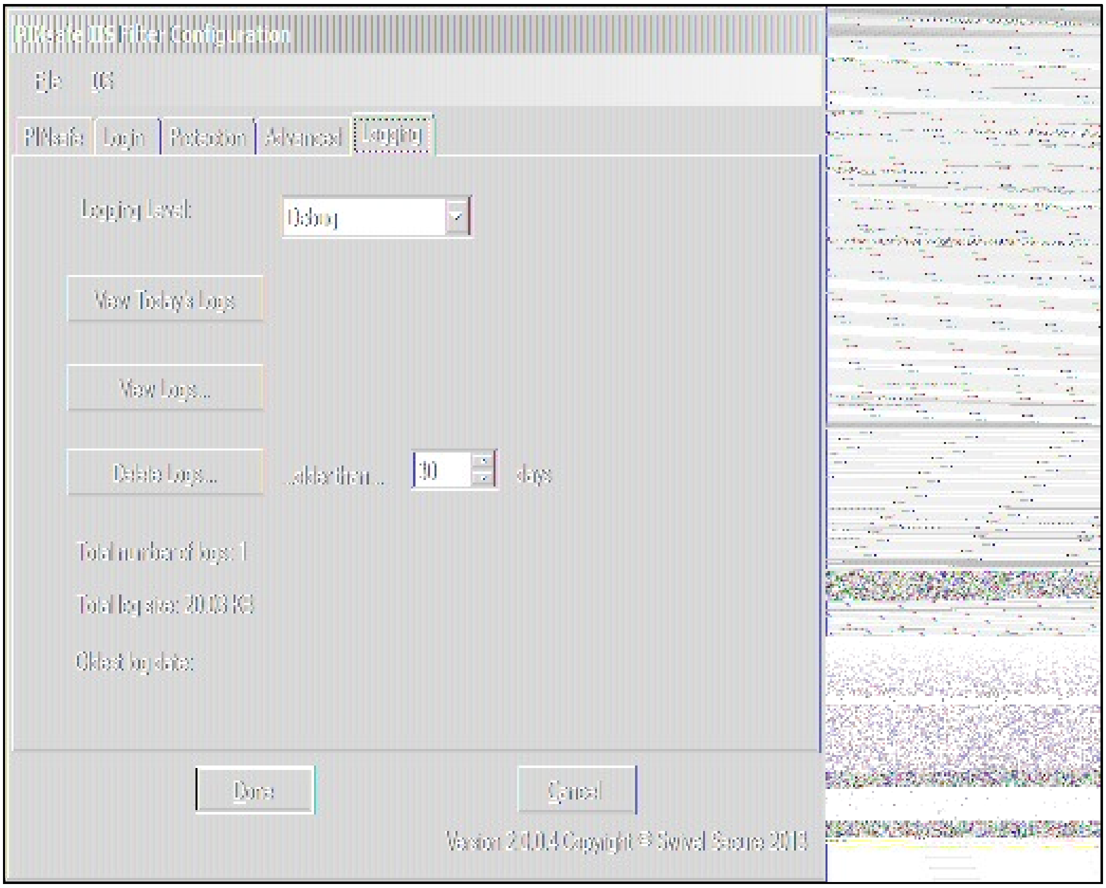
There are 3 settings on this tab:

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.

36.6.5 Logging Tab


PINsafe IIS Filter Configuration

File IIS

PINsafe | Login | Protection | Advanced | Logging

Logging Level: Debug

View Today's Logs

View Logs...

Delete Logs... ...older than ... 30 days

Total number of logs: 1

Total log size: 20.03 KB

Oldest log date:

Done | Cancel

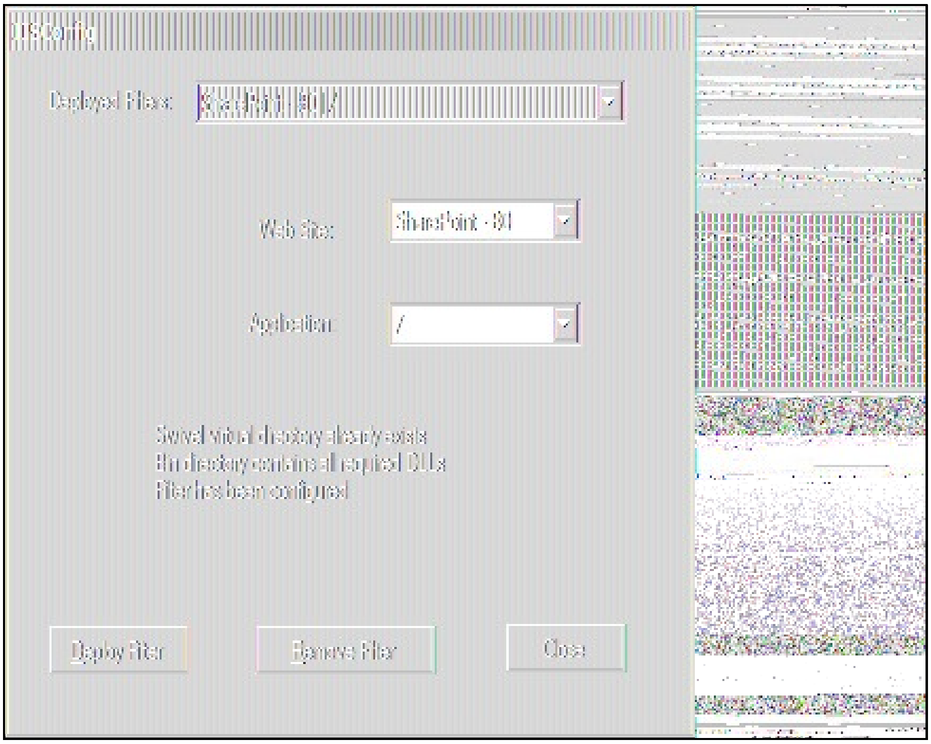
Version 2.0.0.4 Copyright © Swivel Secure 2013

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.

36.6.6 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:


IISConfig

Deployed Filters: SharePoint - 80 /

Web Site: SharePoint - 80

Application: /

Swivel virtual directory already exists
Bin directory contains all required DLLs
Filter has been configured

Deploy Filter | Remove Filter | Close

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.

36.7 Additional Configuration Options

36.8 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.

36.9 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

36.10 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

36.11 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

37 Microsoft IIS version 7 Integration

37.1 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

37.2 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

37.3 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

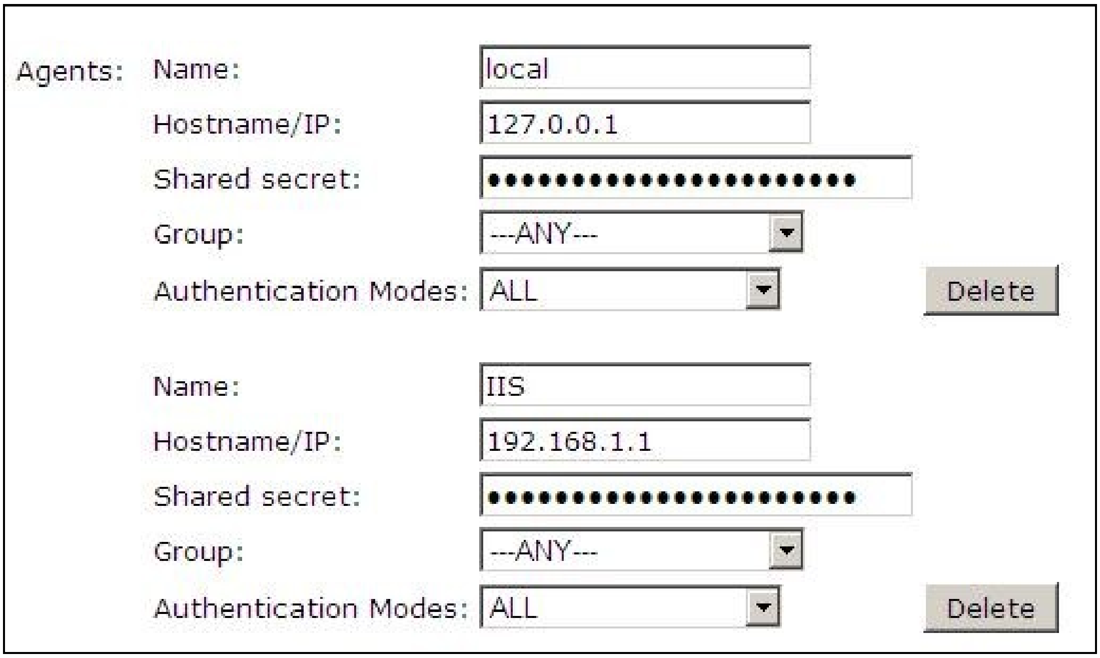
1.3.7-9: various bug fixes

37.4 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
```



Agents:

Name: local

Hostname/IP: 127.0.0.1

Shared secret: ●●●●●●●●●●●●●●●●●●●●●●●

Group: ---ANY---

Authentication Modes: ALL

Name: IIS

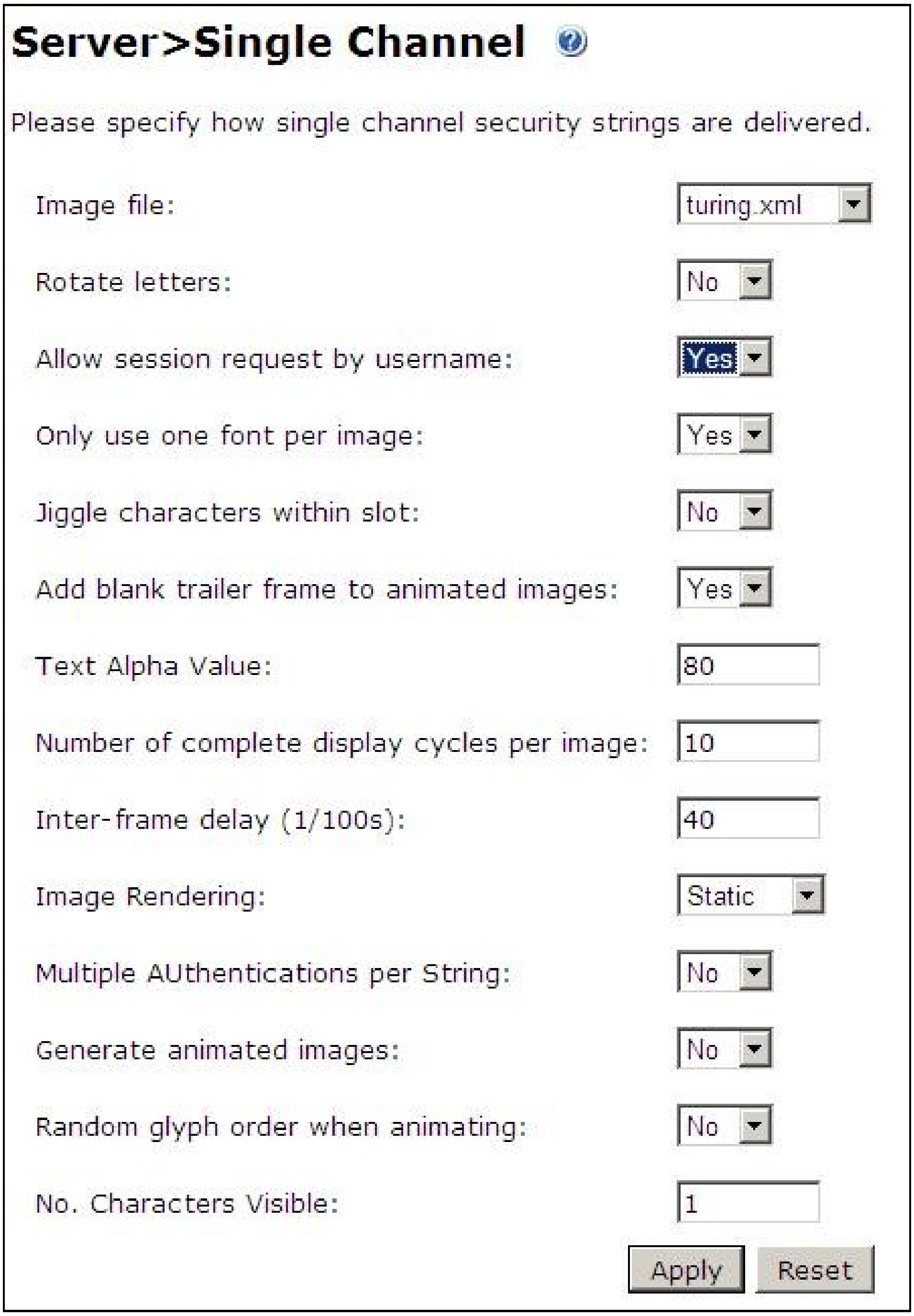
Hostname/IP: 192.168.1.1

Shared secret: ●●●●●●●●●●●●●●●●●●●●●●●

Group: ---ANY---

Authentication Modes: ALL

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.



Server>Single Channel

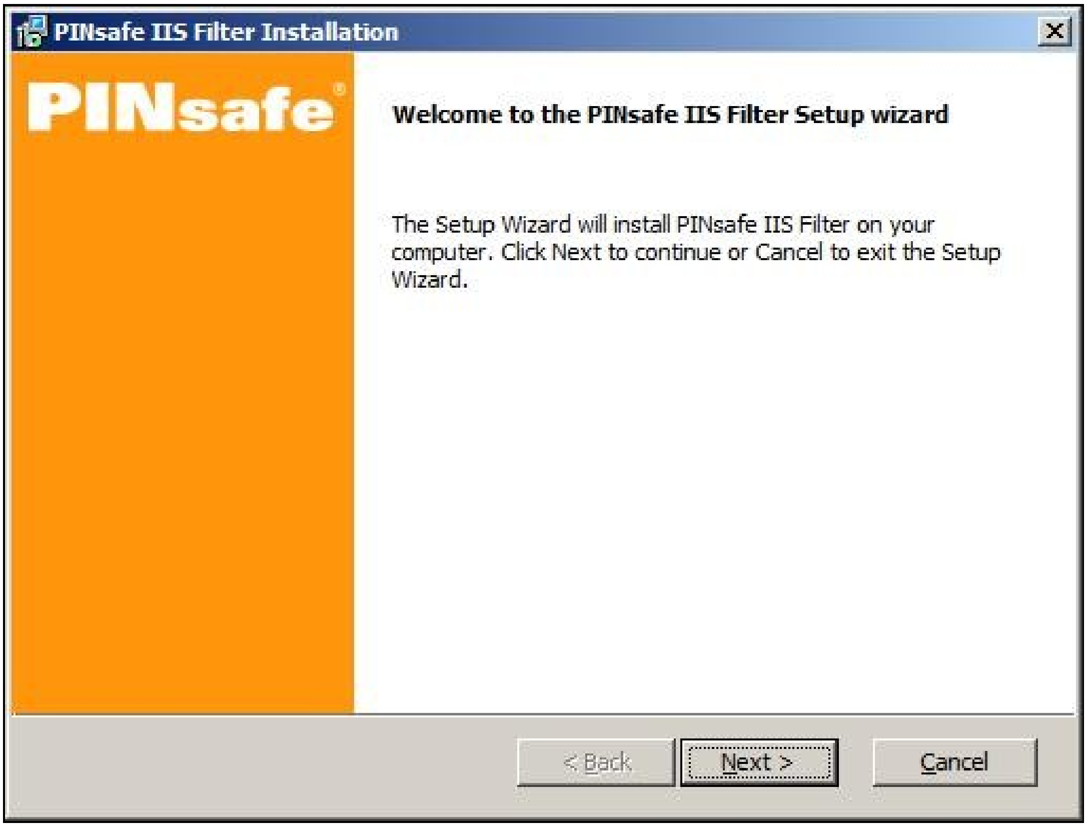
Please specify how single channel security strings are delivered.

Image file:	turing.xml
Rotate letters:	No
Allow session request by username:	Yes
Only use one font per image:	Yes
Jiggle characters within slot:	No
Add blank trailer frame to animated images:	Yes
Text Alpha Value:	80
Number of complete display cycles per image:	10
Inter-frame delay (1/100s):	40
Image Rendering:	Static
Multiple AUthentications per String:	No
Generate animated images:	No
Random glyph order when animating:	No
No. Characters Visible:	1

37.5 Configuring the IIS Server

37.5.1 Install the Swivel Filter

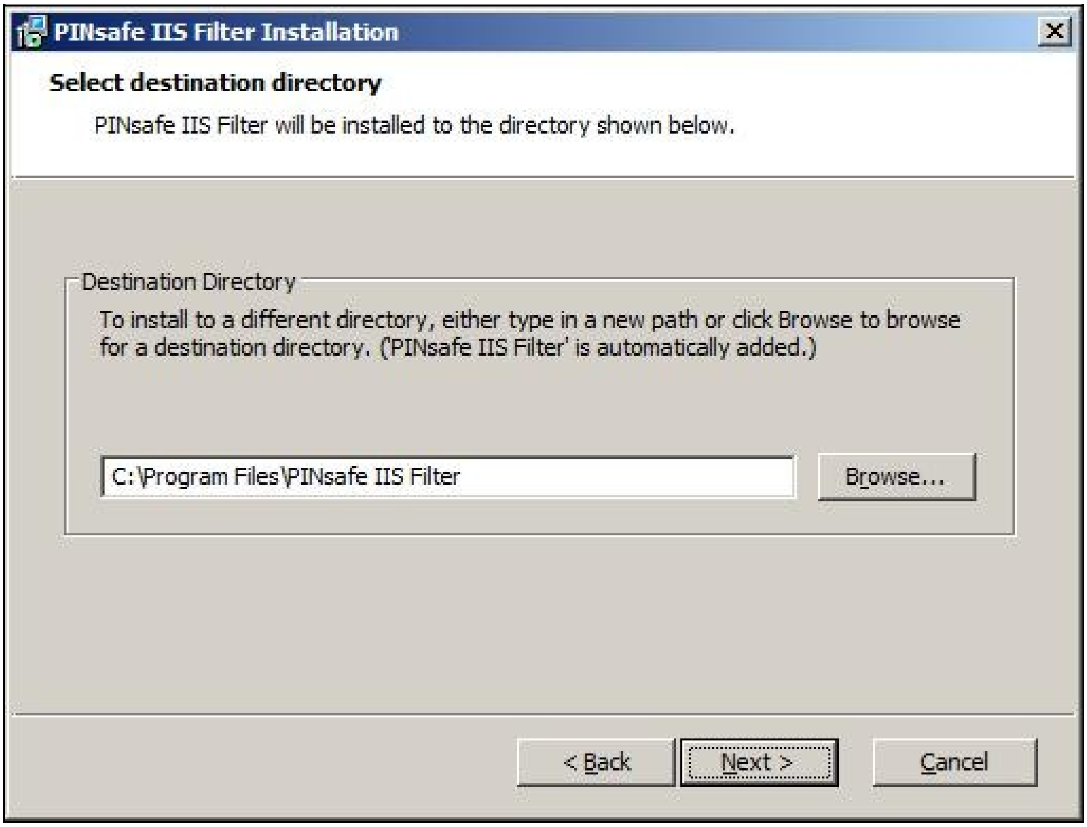
1. On the IIS server run the PINsafeIISFilter.exe. The IIS filter may need to be run as an Administrator user (The filter needs to be installed by IIS running as Administrator user but it can run as a normal user).


PINsafe IIS Filter Installation

Welcome to the PINsafe IIS Filter Setup wizard

The Setup Wizard will install PINsafe IIS Filter on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

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


PINsafe IIS Filter Installation

Select destination directory

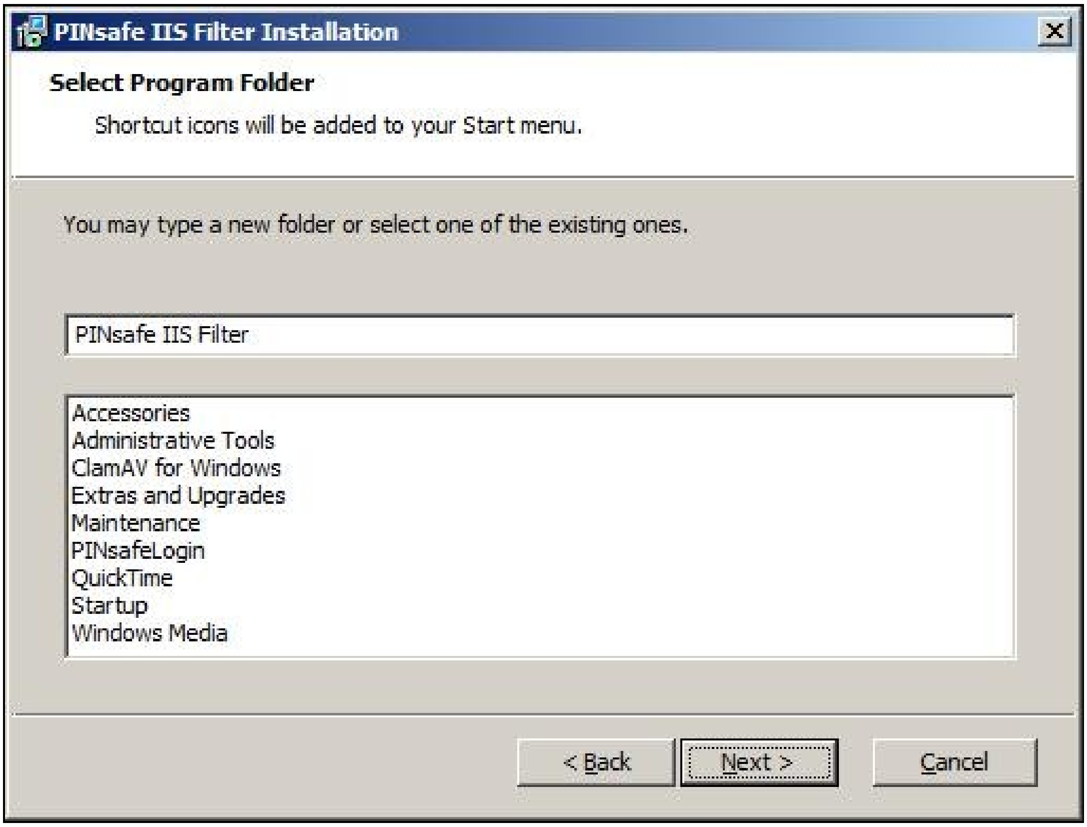
PINsafe IIS Filter will be installed to the directory shown below.

Destination Directory

To install to a different directory, either type in a new path or click Browse to browse for a destination directory. ('PINsafe IIS Filter' is automatically added.)

C:\Program Files\PINsafe IIS Filter

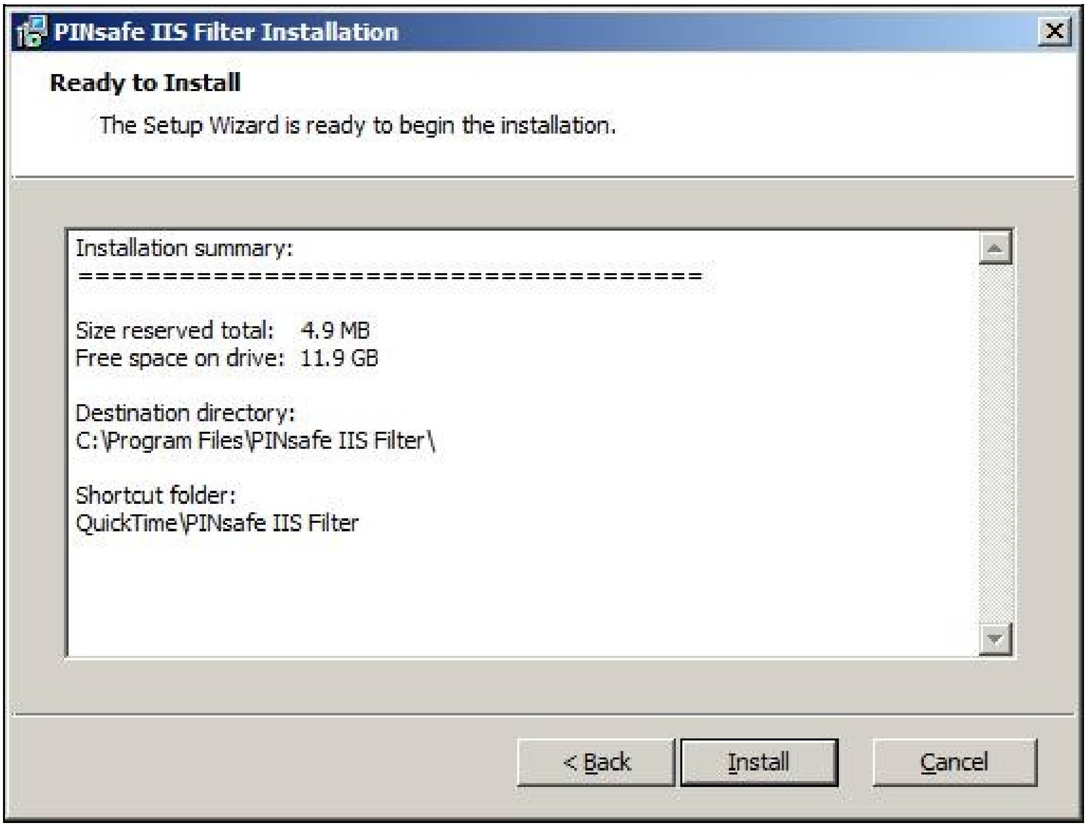
3. Select Start Menu Folder


PINsafe IIS Filter Installation
Select Program Folder
Shortcut icons will be added to your Start menu.
You may type a new folder or select one of the existing ones.
< Back
Next >
Cancel

PINsafe IIS Filter

Accessories
Administrative Tools
ClamAV for Windows
Extras and Upgrades
Maintenance
PINsafeLogin
QuickTime
Startup
Windows Media

4. When details are correct click on Install


PINsafe IIS Filter Installation
Ready to Install
The Setup Wizard is ready to begin the installation.
< Back
Install
Cancel

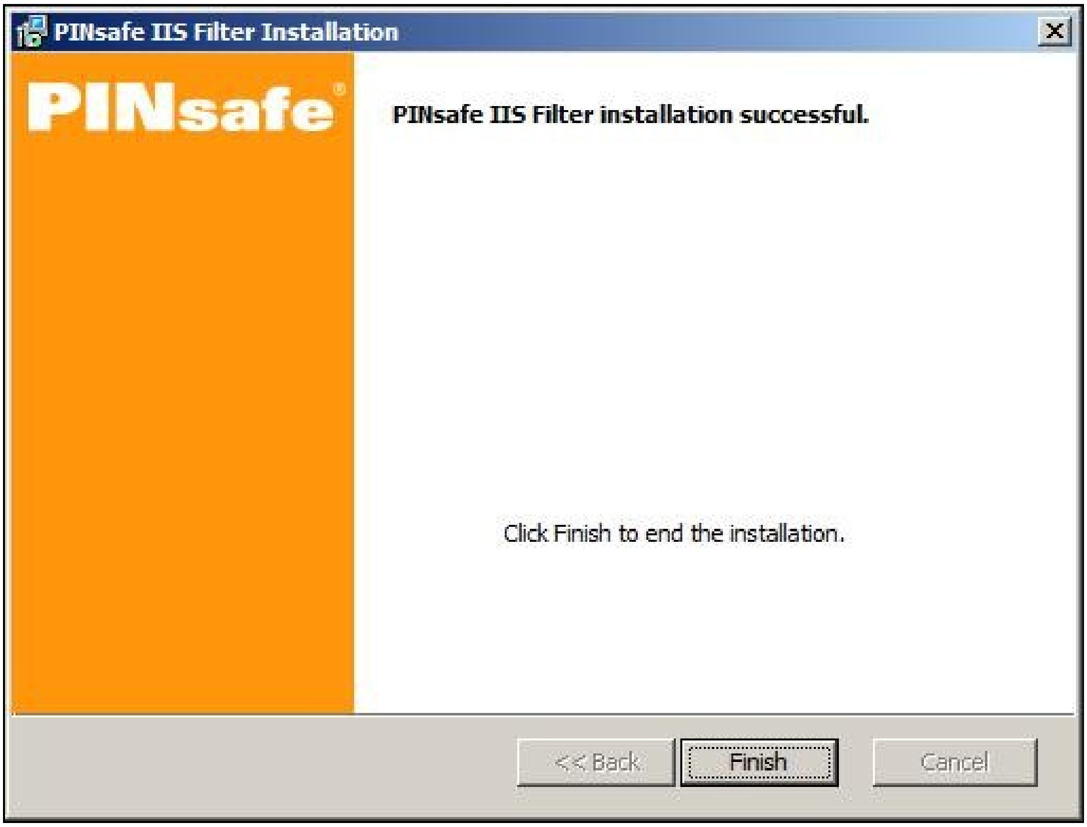
```
Installation summary:
====================================

Size reserved total:    4.9 MB
Free space on drive:  11.9 GB

Destination directory:
C:\Program Files\PINsafe IIS Filter\

Shortcut folder:
QuickTime\PINsafe IIS Filter
```

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

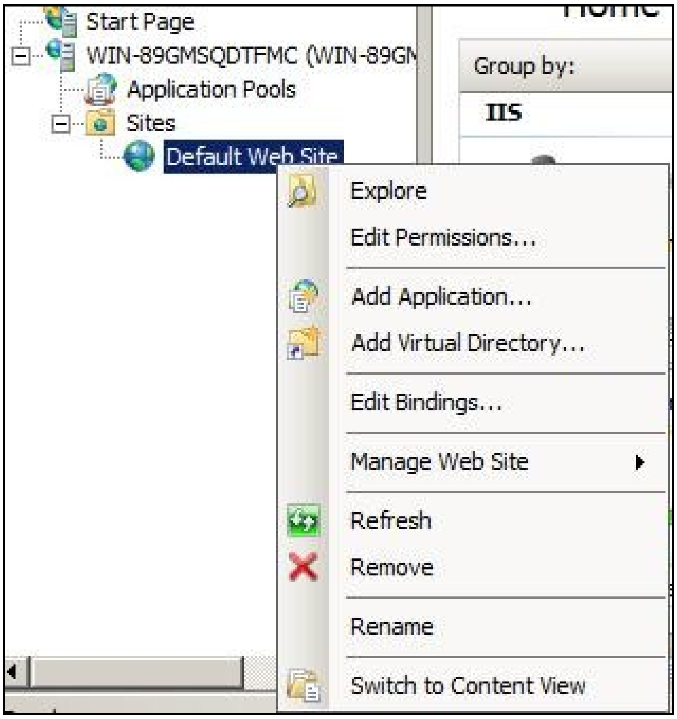

PINsafe IIS Filter Installation

PINsafe IIS Filter installation successful.

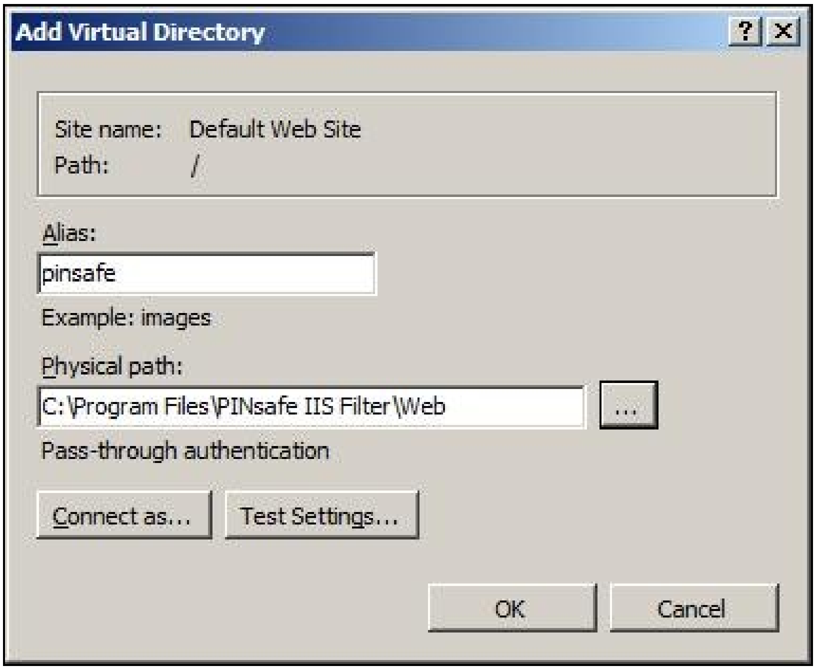
Click Finish to end the installation.

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



Site name: Default Web Site
Path: /

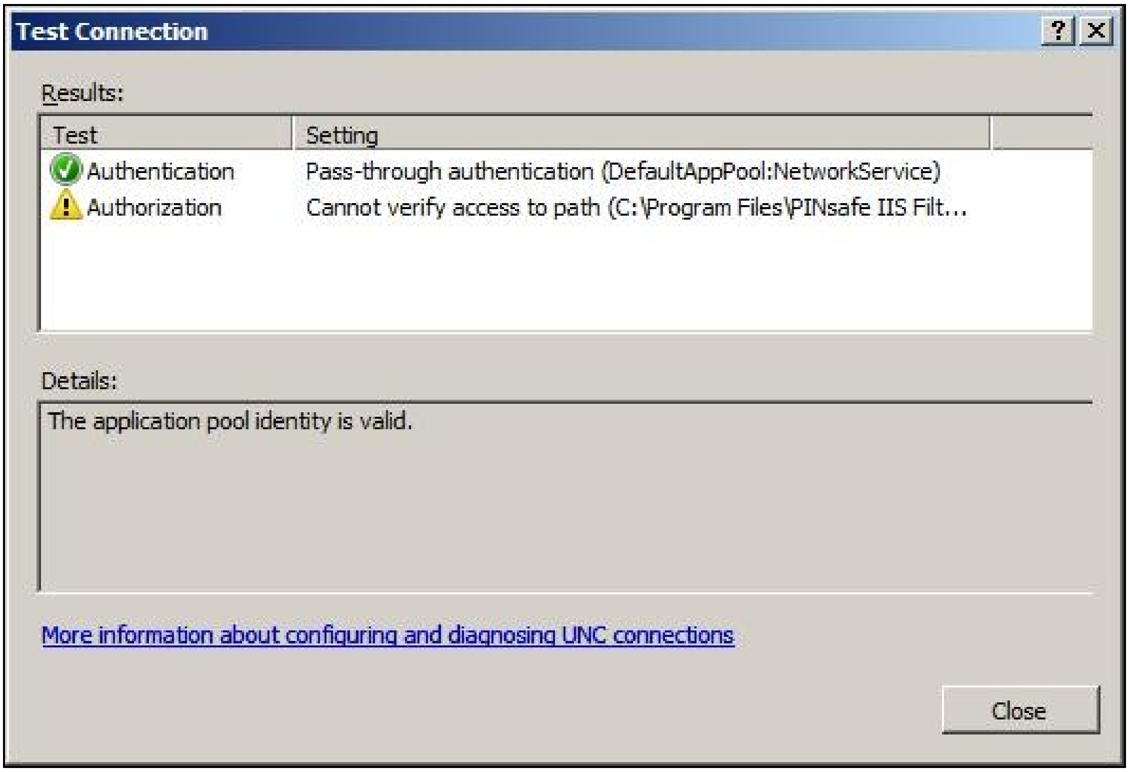
Alias: pinsafe

Example: images

Physical path: C:\Program Files\PINsafe IIS Filter\Web

Pass-through authentication

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.


Test Connection
?
More information about configuring and diagnosing UNC connections
Close

Results:

Test	Setting
✓ Authentication	Pass-through authentication (DefaultAppPool:NetworkService)
⚠ Authorization	Cannot verify access to path (C:\Program Files\PINsafe IIS Filt...

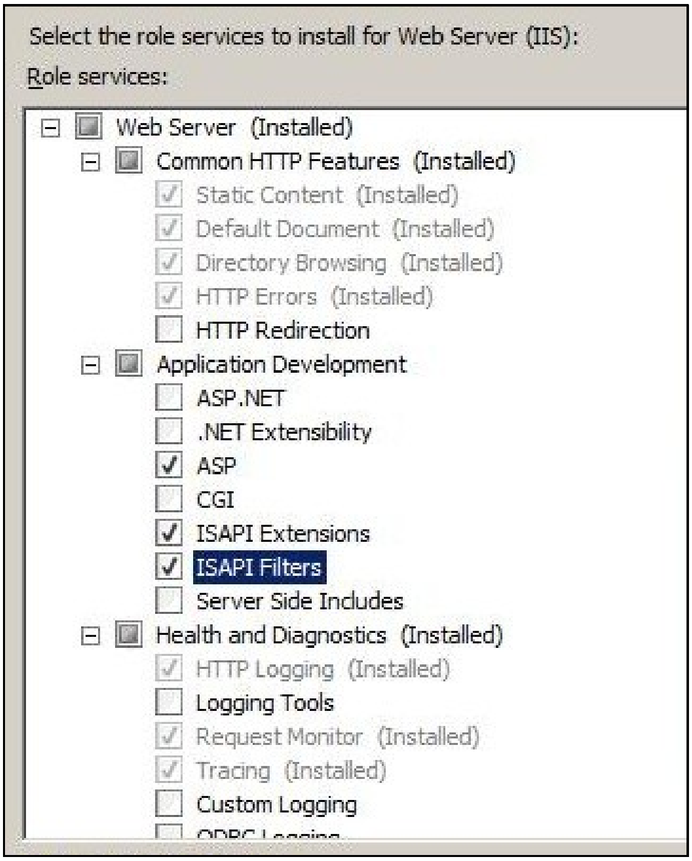
Details:

The application pool identity is valid.

4. Set the permissions to Read and Run Scripts

37.5.2 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.



Select the role services to install for Web Server (IIS):

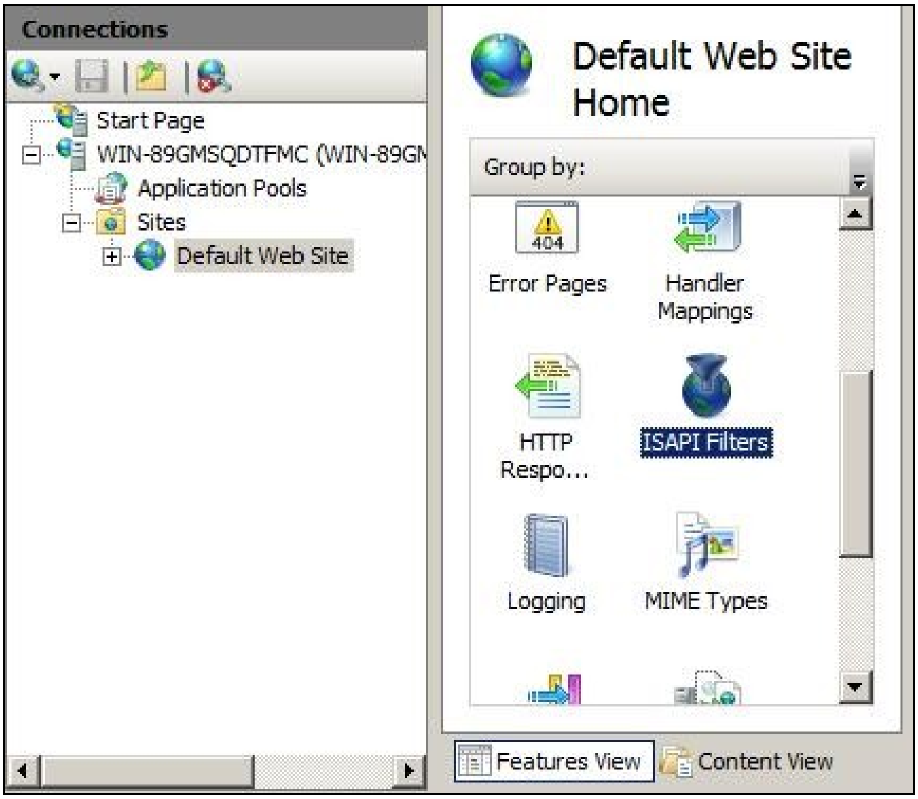
Role services:

- ⊟ ▣ Web Server (Installed)
  - ⊟ ▣ Common HTTP Features (Installed)
    - ☑ Static Content (Installed)
    - ☑ Default Document (Installed)
    - ☑ Directory Browsing (Installed)
    - ☑ HTTP Errors (Installed)
    - □ HTTP Redirection
  - ⊟ ▣ Application Development
    - □ ASP.NET
    - □ .NET Extensibility
    - ☑ ASP
    - □ CGI
    - ☑ ISAPI Extensions
    - ☑ ISAPI Filters
    - □ Server Side Includes
  - ⊟ ▣ Health and Diagnostics (Installed)
    - ☑ HTTP Logging (Installed)
    - □ Logging Tools
    - ☑ Request Monitor (Installed)
    - ☑ Tracing (Installed)
    - □ Custom Logging
    - □ ODBC Logging

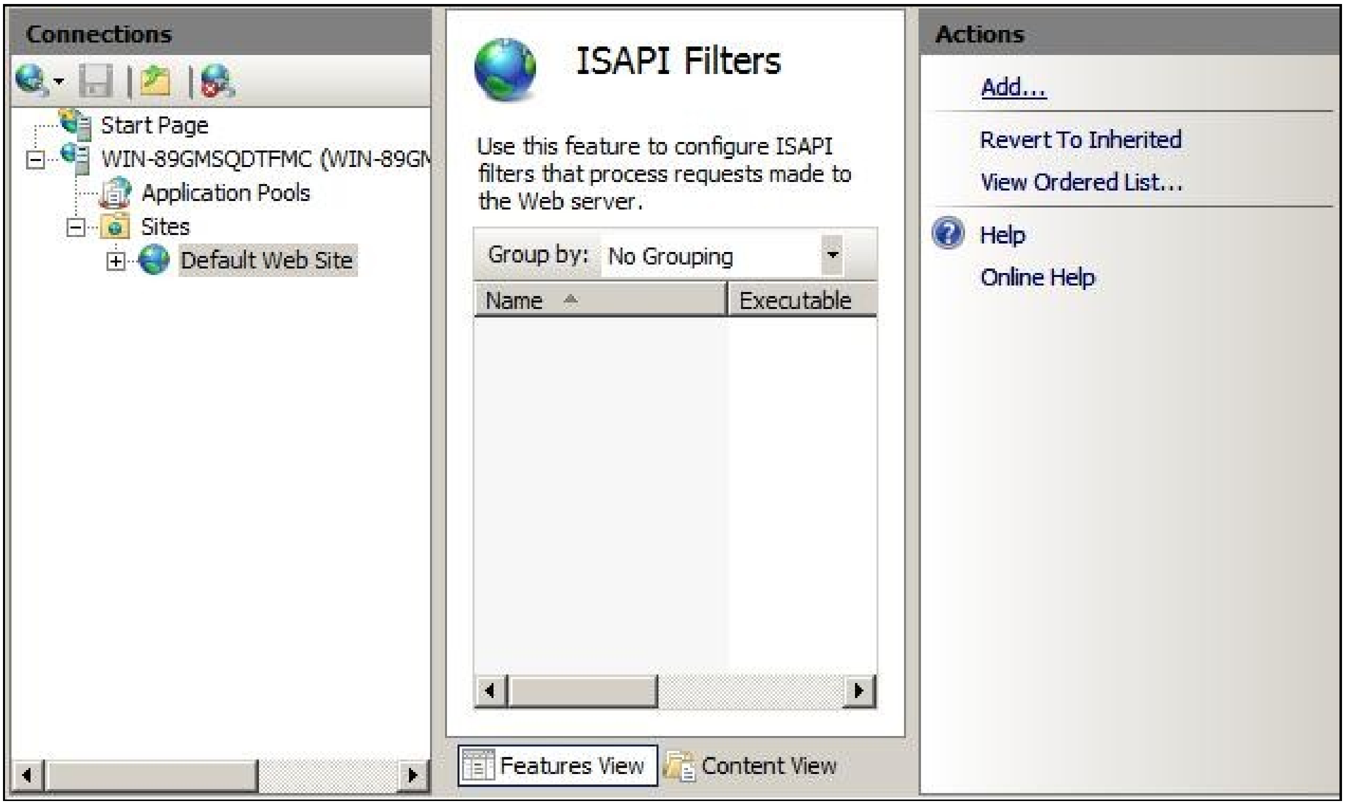
37.5.3 Install the Swivel ISAPI Filter

1. On the Internet Information Services Manager Select the website

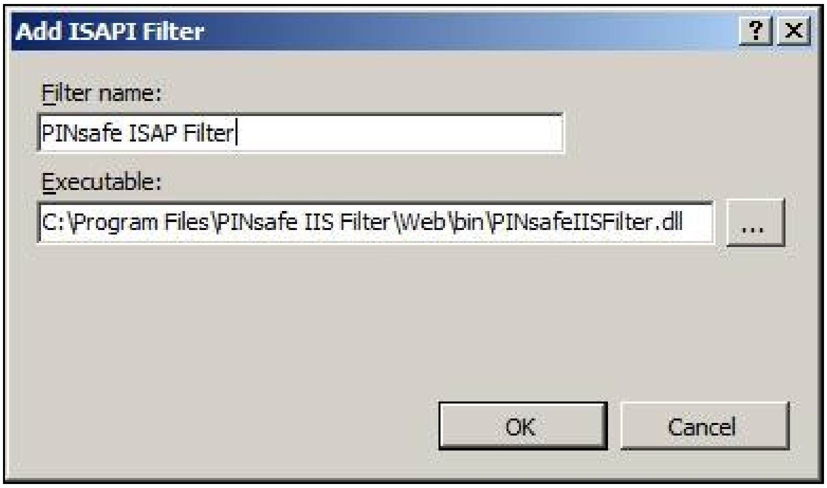
2. Select ISAPI filters by double clicking on the ISAPI filters icon



3. Under Actions select Add



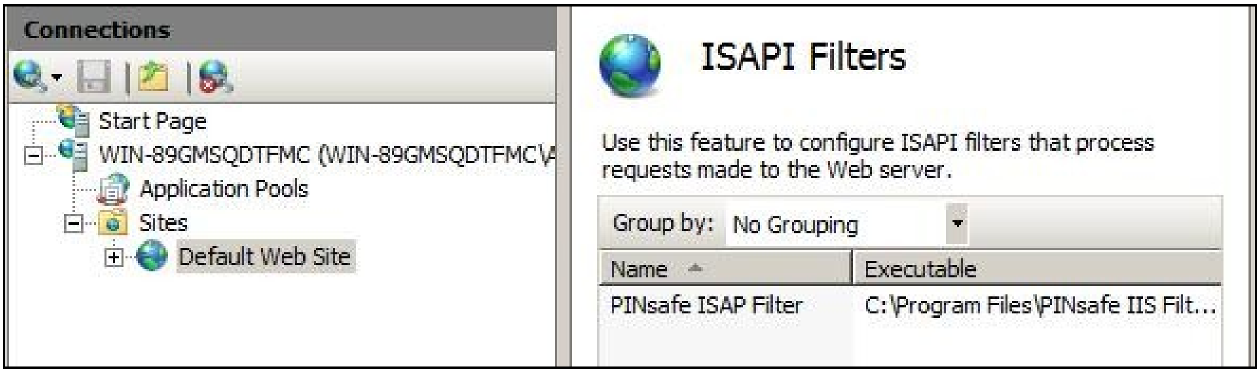
4. Select the Path to the Swivel ISAPI filter. Note that the actual file you require will be PINsafeIISFilter.dll, located in the sub-folder Web\bin of the installation folder. Enter a name for the Filter such as *PINsafe ISAPI Filter*. When information is complete click on Ok.



Filter name:
PINsafe ISAP Filter

Executable:
C:\Program Files\PINsafe IIS Filter\Web\bin\PINsafeIISFilter.dll

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



Use this feature to configure ISAPI filters that process requests made to the Web server.

Group by: No Grouping

Name	Executable
PINsafe ISAP Filter	C:\Program Files\PINsafe IIS Filt...

37.5.4 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.

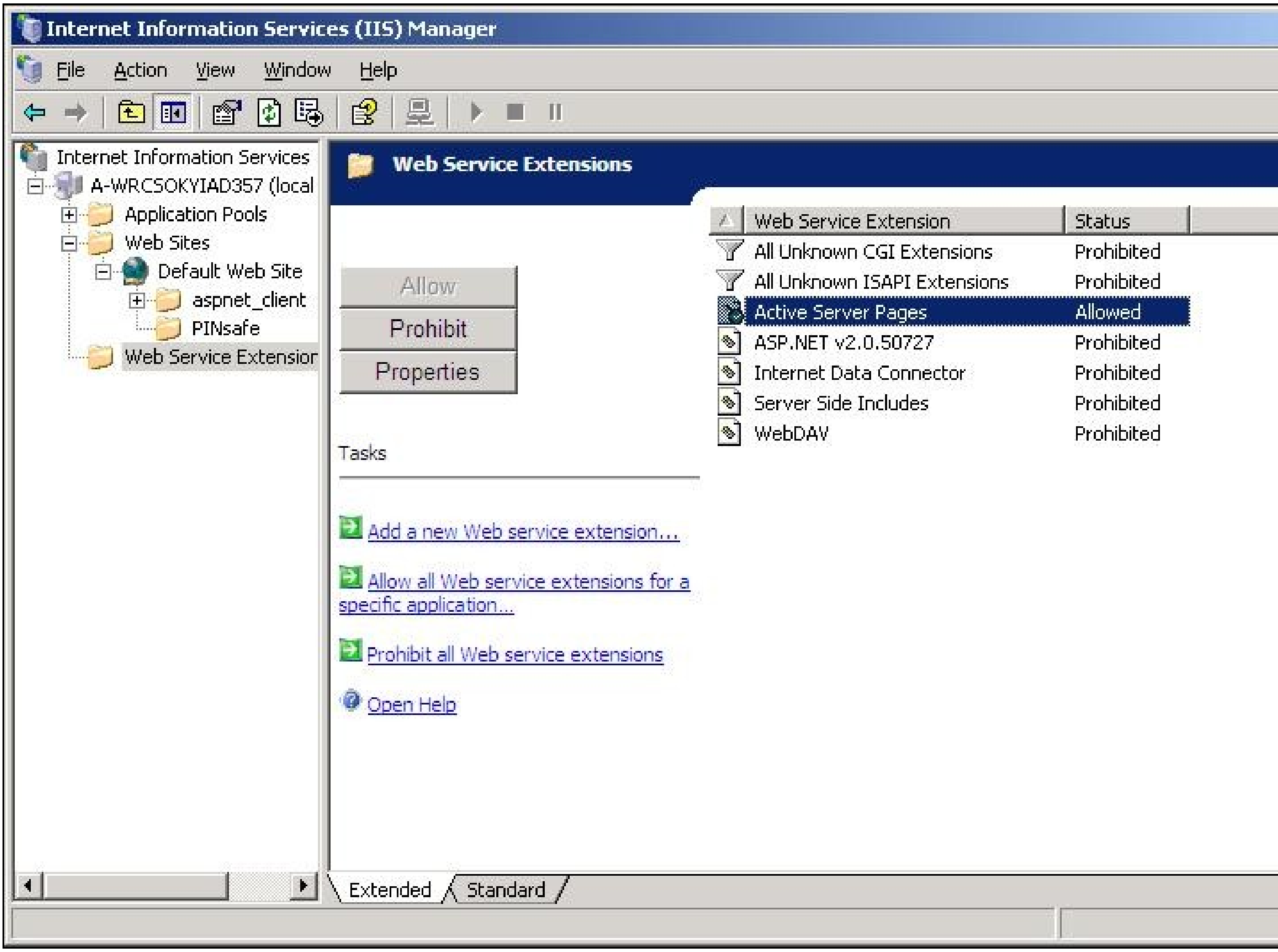
Logout path: Requesting this path will result in the user being logged out. Subsequent requests will require re-authentication, if relevant. If this path is empty, users can only be logged out by closing the browser, or if the authentication times out. Note: The logout path must be an included file location.

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.



Web Service Extension	Status
All Unknown CGI Extensions	Prohibited
All Unknown ISAPI Extensions	Prohibited
Active Server Pages	Allowed
ASP.NET v2.0.50727	Prohibited
Internet Data Connector	Prohibited
Server Side Includes	Prohibited
WebDAV	Prohibited

37.6 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:

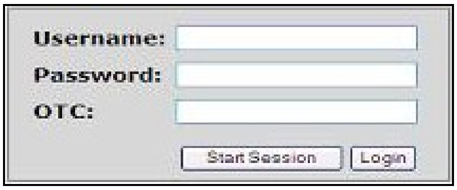
1. Make a copy of the entire Web folder, including the bin sub-folder. You can copy it as a sub-folder of Swivel IIS filter, with a different name, or you can put it somewhere completely different. It is important, however, that you keep the structure the same ? all the .asp files must remain intact,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

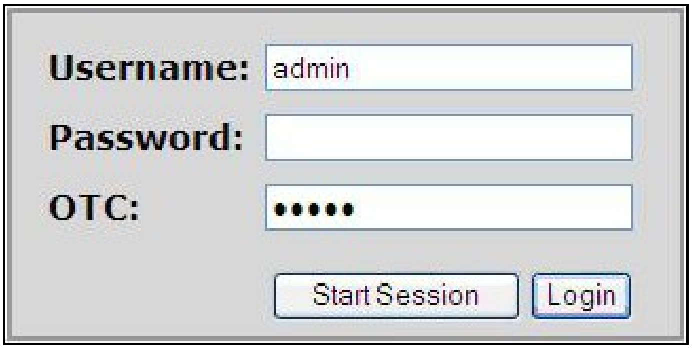
37.7 Testing

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



Enter the Username.

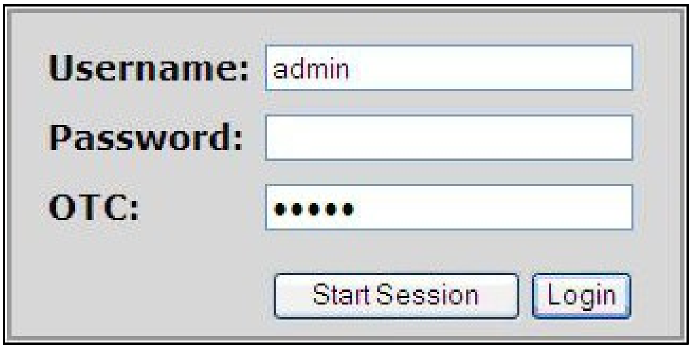
For dual channel, enter the One Time Code:


Username: admin

Password:

OTC: •••••

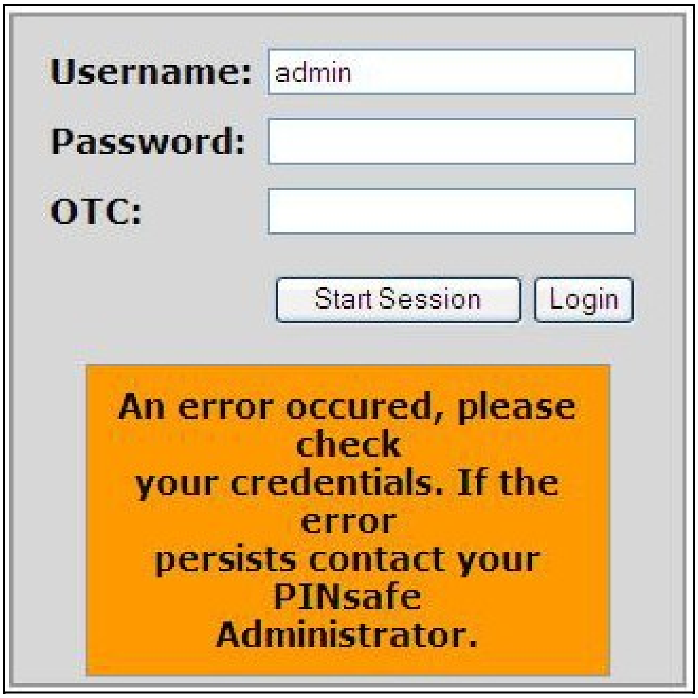
Or click start session to enter a single channel OTC. The Swivel log will record that a single channel session has started.


Username: admin

Password:

OTC: •••••

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.


Username: admin

Password:

OTC:

An error occured, please check
your credentials. If the error
persists contact your PINsafe Administrator.

37.8 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.

37.9 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.

37.9.1 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

38 Microsoft Office 365

39 Introduction

This article describes how to manually integrate Swivel with Microsoft Office 365 to provide strong and two factor authentication. A more recent integration with a swivel installer and configuration program is available in the Microsoft ADFS 2 Integration. For ADFS version 3 see Microsoft ADFS 3 Authentication.

39.1 Video showing login to Office 365 using ADFS with PINpad

Swivel Authenticating Office365 using ADFS with PINpad from Swivel Secure.

40 Prerequisites

Swivel authentication platform 3.x

ADFS Proxy 2.0, ADFS Proxy 2.1

Microsoft Office 365

40.1 Downloads

ADFS Integration files

41 Baseline

(The version tested with)

Swivel 3.9.5

ADFS Proxy 2.0, ADFS Proxy 2.1

Microsoft Office 365

42 Architecture

The process of the filter is quite simple and verifies the credentials against the Swivel server and, if correct, passes the user through to ADFS for issuing of the secure token. The filter plays no role in interpreting ADFS authentication requests or in generating responses.

43 Installation

43.1 Configure The Swivel Server

Configure a Swivel Agent (For standard XML Authentication)

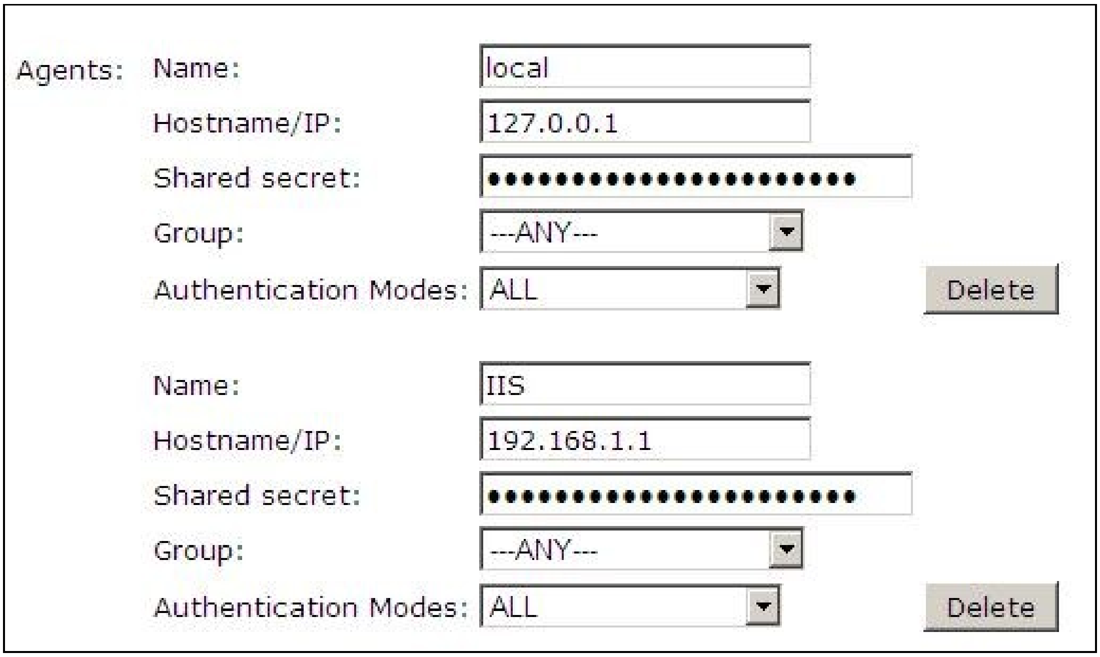
1. On the Swivel Management Console select Server/Agent

2. Enter a name for the Agent

3. Enter the Exchange IP address

4. Enter the shared secret used above on the Exchange Filter

5. Click on Apply to save changes



Agents: Name: local

Hostname/IP: 127.0.0.1

Shared secret: ●●●●●●●●●●●●●●●●●●●●●●●

Group: ---ANY---

Authentication Modes: ALL

Name: IIS

Hostname/IP: 192.168.1.1

Shared secret: ●●●●●●●●●●●●●●●●●●●●●●●

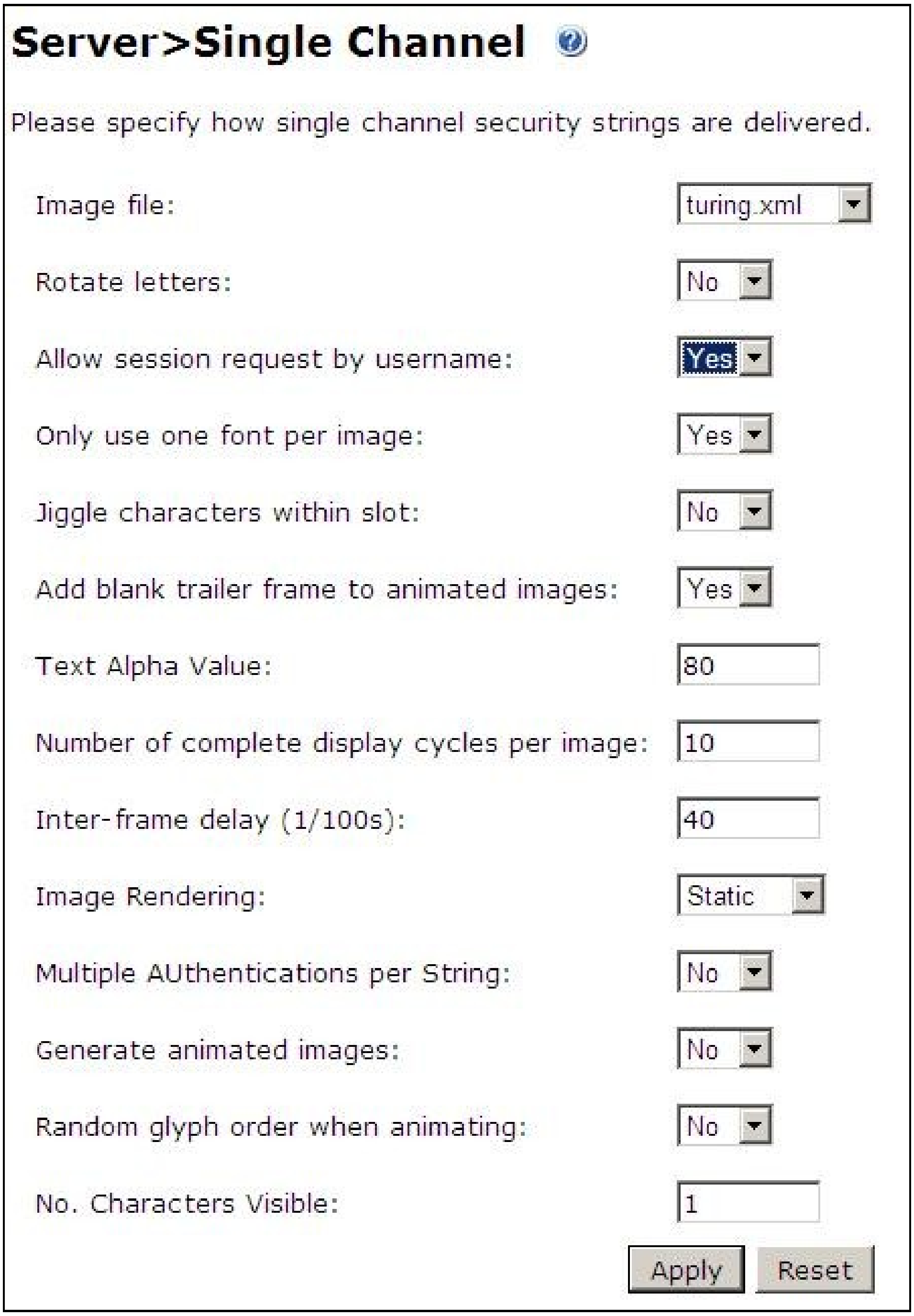
Group: ---ANY---

Authentication Modes: ALL

Configure Single Channel Access

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

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



Server>Single Channel

Please specify how single channel security strings are delivered.

Image file:	turing.xml
Rotate letters:	No
Allow session request by username:	Yes
Only use one font per image:	Yes
Jiggle characters within slot:	No
Add blank trailer frame to animated images:	Yes
Text Alpha Value:	80
Number of complete display cycles per image:	10
Inter-frame delay (1/100s):	40
Image Rendering:	Static
Multiple AUthentications per String:	No
Generate animated images:	No
Random glyph order when animating:	No
No. Characters Visible:	1

43.2 Using additional attributes for authentication

When using additional attributes for authentication see User Attributes How To

43.3 ADFS Integration

The Swivel integration needs to be made on the internet facing ADFS proxy server that customers use for their OWA login.

The following files are used for integration

- FormsSignIn.aspx ? example logon page
- Web.config ? example configuration file
- Pinsafe_image.aspx ? TURing image proxy web page
- Exists.aspx ? utility web page to check if a user exists
- Bin\PINsafeASPNetFilter.dll ? the PINsafe HTTP module that manages authentication
- Bin\PINsafeClient.dll ? manages PINsafe communication

43.3.1 Copy required files to the ADFS server

Copy *pinsafe_image.aspx* and *exists.aspx* to the *adfs\ls*

Copy the *PINsafeASPNetFilter.dll* and *PINsafeClient.dll* to adfs\ls\bin (you may need to create this folder).

43.3.2 Modify the ADFS login pages

The other two files, FormsSignIn.aspx and web.config, are example files only. You should examine these files, and copy the relevant parts to your existing versions of these files, modifying them as appropriate. Instructions are included in the files themselves. Each section that needs to be changed or inserted is prefixed by and ended by .

43.3.2.1 web.config options

PINsafeServer default: 192.168.78.103, The IP address or hostname of the Swivel server.

PINsafePort default: 8080, The port used to communicate with the Swivel server. This usually should be 8080 for appliance and software installations.

PINsafeContext default: pinsafe, The Swivel application installation name, usually *pinsafe*.

PINsafeSecure default: True, On the *PINsafePort* if the Swivel server is using SSL communication this should be set to Yes, if no SSL is used this should be set to False.

PINsafeSecret default: secret, This needs to be set to the same as that set on the Swivel server Agent.

PINsafeLogonPath default: /adfs/ls/, the logon path to be used.

PINsafeLogoffPath default: /adfs/ls/, the logoff path to be used.

PINsafeExcludedPaths default: /adfs/ls/MasterPages/;./pinsafe_image.aspx, Add any custom paths that need to be accessed during authentication here.

PINsafeIgnoreDomain default: true, If True it will strip off the domain name to get the PINsafe username, if False it will not alter the user login name.

PINsafeAcceptSelfSigned default:True, If set to True it will allow self signed and invalid certificates to be used on the Swivel server. If set to False, the certificate must be correct for that of the Swivel server.

PINsafePassword default: True"

PINsafeImage default: True, If True Display a single Channel authentication image, if False do not display an image.

PINsafeMessage default: False, If True send the user an dual channel message, if False do not send the user a message.

PINsafeCookieSecret default: will be generated randomly.

PINsafeIdleTimeSecs default: 300

AllowNonPINsafeUsers default: False, If True allow non Swivel users to authenticate without Swivel authentication, if False do not permit non Swivel users to authenticate. the option to allow unknown users to authenticate without Swivel authentication only applies to users not known to Swivel at all. You cannot specify that it only applies to a group of users, and not to other users who are known to Swivel, but not in a particular group.

PINsafeFilterEnabled default: True, If true the Swivel ADFS filter is working, if False the Swivel ADFS filter is present but Swivel authentication is disabled.

PINsafeAuthenticationDomain default:

PINsafeUsernameField default: ctl00$ContentPlaceHolder1$UsernameTextBox

PINsafeOTCField default: otc, The prompt displayed to users where the Swivel authentication details should be entered.

43.3.3 Restart IIS

Restart IIS on the ADFS server for the changes to take effect.

43.4 Additional Installation Options

43.4.1 Disabling or enabling the Automated TURing

If login methods other than the TURing are to be used such as SMS, Mobile Client or Token, then the automated TURing must be disabled. This is for Swivel ADFS filter version 1.2.

Backup then edit the file C:\inetpub\adfs\FormsSignIn.aspx

Find the line with only showTuring(); and comment out using as below. To re-enable remove the comments.

```
    rowTuring.style.display = "";
 showTuring();
     {
```

to

```
     rowTuring.style.display = "";


   {
```

Reload the browser and verify that the login page is now correct.

43.4.2 Changing the Show TURing Button

After applying the Swivel customisation, go to C:\inetpub\adfs\ls and edit as an Administrator the FormsSignIn.aspx. Look for "Show TURing" and alter it as appropriate.

44 Testing the Installation

The next time you try to access the ADFS login page, there will be no apparent difference to the login page. However, after you enter the username, for an existing user, you should see an additional field for one-time code, and a button to request a TURing image. You should not be able to authenticate to ADFS without entering both the AD password AND the PINsafe one-time code.

45 Uninstalling the Swivel Integration

46 Troubleshooting

Check the Swivel logs

Check the ADFS server logs

47 Known Issues and Limitations

The ADFS proxy currently does not support a redirect if the user is required to Change their PIN.

48 Additional Information

49 Additional documentation

49.1 Swivel

Swivel ADFS and Office 365

High Level Overview Document

50 Microsoft Sharepoint 2010 Integration

50.1 Overview

The solution described here is for SharePoint 2010 only, as it relies on claims-based authentication features introduced in that version. A similar solution is also available for SharePoint 2013.

For earlier versions of SharePoint, see this article.

50.2 Downloading the Filter

The latest solution for PINsafe SharePoint 2010 filter is version 1.5.3. It can be found here. Full instructions for installing the filter and configuring SharePoint to support it are included in the zip file.

50.3 Upgrading the Swivel SharePoint Filter

It is recommended to uninstall the old filter and then reinstall the new filter in order to remove the previous filter from the assembly cache. Choose the appropriate upgrade option when installing the new version.

50.4 Uninstalling the Swivel SharePoint filter

To uninstall the filter select the Add/Remove Programs on the SharePoint server then uninstall. The settings are not removed in the uninstall process.

50.5 SharePoint PINsafe FAQ

50.5.1 Can the Swivel SharePoint filter Manage the AD Credentials

Yes, version 1.4 or later of the SharePoint filter has the ability to set the AD password. See documentation included in the download for more information.

50.5.2 Can the filter detect an expired AD password

Yes, version 1.4 or later of the filter will detect if the AD password has expired, and will redirect to a page suitable for changing the AD password. See documentation included in the download for more information.

50.5.3 Can the filter allow users to reset a forgotten AD password

Yes, version 1.5 or later of the SharePoint filter has the ability to reset forgotten AD passwords as well as PINs. See included documentation for more information.

Note that the password reset feature requires version 3.9.6 or later of the Swivel Core server. However, if you do not wish to upgrade, a patch is available for version 3.8, from here, to add the required feature. If you want to use this feature, please contact support@swivelsecure.com to check if your version of PINsafe can be upgraded to support this feature. Please also contact support@swivelsecure.com for help in installing this patch.

50.5.4 Can the filter work with Membership Providers other than Active Directory

Yes, version 1.5.2 or later will work with other membership providers. However, the AD password management facilities must be disabled. These only work with the AD membership provider, and authentication with other membership providers will fail if this feature is enabled.

50.6 Troubleshooting

50.6.1 TURing image does not appear

A red cross may be present where the TURing image should appear. The usual causes are:

Incorrect path to PINsafe appliance

Self Signed Certificate is used, but the allow self signed certificate option has not been selected

Firewall blocking access to PINsafe server

Network issue

HTTP request against the PINsafe running HTTPS

50.6.2 Error Messages

502 - Bad Gateway

This has been seen where the SharePoint cannot connect to the PINsafe server. Check the above, particularly the settings for SSL or HTTP access.

Authentication provider not found

PINsafe cannot be accessed by the SharePoint server, verify connectivity settings.

51 Microsoft Sharepoint 2013 Integration

51.1 Overview

The solution described here is for SharePoint 2013 only. A similar solution is available for SharePoint 2010. Do not use version 1.6 of the filter for SharePoint 2010, and do not use earlier versions for SharePoint 2013.

For earlier versions of SharePoint, see this article.

51.2 Downloading the Filter

The latest solution for PINsafe SharePoint 2013 filter is version 1.6.1. It can be found here. The only change from 1.6.0 is that removing the domain prefix and/or suffix from usernames is now optional. In 1.6.0, they were always removed.

Full instructions for installing the filter and configuring SharePoint to support it are included in the zip file, or you can download it separately from here.

The previous version, 1.6.0, can be found here.

51.3 Upgrading the Swivel SharePoint Filter

It is recommended to uninstall the old filter and then reinstall the new filter in order to remove the previous filter from the assembly cache. You should then choose the appropriate upgrade option when prompted. Note that upgrading from a SharePoint 2010 filter has not been tested, but as the technology is very similar, no problems are anticipated. If you do have a problem when upgrading an existing SharePoint 2010 filter to SharePoint 2013, it is recommended that you uninstall and treat it as a new installation.

51.4 Uninstalling the Swivel SharePoint filter

To uninstall the filter select the Add/Remove Programs on the SharePoint server then uninstall. The settings are not removed in the uninstall process.

51.5 SharePoint PINsafe FAQ

51.5.1 Can the Swivel SharePoint filter Manage the AD Credentials

Yes, version 1.4 or later of the SharePoint filter has the ability to set the AD password. See documentation included in the download for more information.

51.5.2 Can the filter detect an expired AD password

Yes, version 1.4 or later of the filter will detect if the AD password has expired, and will redirect to a page suitable for changing the AD password. See documentation included in the download for more information.

51.5.3 Can the filter allow users to reset a forgotten AD password

Yes, version 1.5 or later of the SharePoint filter has the ability to reset forgotten AD passwords as well as PINs. See included documentation for more information.

However, the password reset feature requires version 3.9.6 or later of the Swivel Core server, which at the time of writing had not been released. However, a patch is available for version 3.8, from here, to add the required feature. If you want to use this feature, please contact support@swivelsecure.com to check if your version of PINsafe can be upgraded to support this feature. Please also contact support@swivelsecure.com for help in installing this patch.

51.5.4 Can the filter work with Membership Providers other than Active Directory

Yes, version 1.5.2 or later will work with other membership providers. However, the AD password management facilities must be disabled. These only work with the AD membership provider, and authentication with other membership providers will fail if this feature is enabled.

51.6 Troubleshooting

51.6.1 TURing image does not appear

A red cross may be present where the TURing image should appear. The usual causes are:

Incorrect path to PINsafe appliance

Self Signed Certificate is used, but the allow self signed certificate option has not been selected

Firewall blocking access to PINsafe server

Network issue

HTTP request against the PINsafe running HTTPS

51.6.2 Error Messages

502 - Bad Gateway

This has been seen where the SharePoint cannot connect to the PINsafe server. Check the above, particularly the settings for SSL or HTTP access.

Authentication provider not found

PINsafe cannot be accessed by the SharePoint server, verify connectivity settings.

52 Microsoft Sharepoint 2019 Integration

52.1 Overview

NOTE: this solution is based on the SharePoint 2013 solution. As such, it has had limited testing on SharePoint 2019, but it appears to be working successfully.

The solution described here is for SharePoint 2019 only. Similar solutions are available for SharePoint 2013 and SharePoint 2010. Do not use version 1.8 of the filter for previous versions of SharePoint, and do not use earlier versions for SharePoint 2019.

Please note that the illustrations in this article are from the SharePoint 2013 integration. The forms will looks slightly different in 2019, but functionality is essentially the same. There may also be some outdated references to SharePoint 2013. This article will be updated in due course.

52.2 Downloading the Filter

The latest solution for PINsafe SharePoint 2019 filter is version 1.8.0. It can be found here.

Full instructions for installing the filter and configuring SharePoint to support it can be downloaded from here. This article refers to version 1.6 for SharePoint 2013, but the instructions are unchanged.

52.3 Upgrading the Swivel SharePoint Filter

It is recommended to uninstall the old filter and then reinstall the new filter in order to remove the previous filter from the assembly cache. You should then choose the appropriate upgrade option when prompted. Note that upgrading from a SharePoint 2010 filter has not been tested, but as the technology is very similar, no problems are anticipated. If you do have a problem when upgrading an existing SharePoint 2010 filter to SharePoint 2013, it is recommended that you uninstall and treat it as a new installation.

52.4 Uninstalling the Swivel SharePoint filter

To uninstall the filter select the Add/Remove Programs on the SharePoint server then uninstall. The settings are not removed in the uninstall process.

52.5 SharePoint PINsafe FAQ

52.5.1 Can the Swivel SharePoint filter Manage the AD Credentials

Yes, version 1.4 or later of the SharePoint filter has the ability to set the AD password. See documentation included in the download for more information.

52.5.2 Can the filter detect an expired AD password

Yes, version 1.4 or later of the filter will detect if the AD password has expired, and will redirect to a page suitable for changing the AD password. See documentation included in the download for more information.

52.5.3 Can the filter allow users to reset a forgotten AD password

Yes, version 1.5 or later of the SharePoint filter has the ability to reset forgotten AD passwords as well as PINs. See included documentation for more information.

However, the password reset feature requires version 3.9.6 or later of the Swivel Core server, which at the time of writing had not been released. However, a patch is available for version 3.8, from here, to add the required feature. If you want to use this feature, please contact support@swivelsecure.com to check if your version of PINsafe can be upgraded to support this feature. Please also contact support@swivelsecure.com for help in installing this patch.

52.5.4 Can the filter work with Membership Providers other than Active Directory

Yes, version 1.5.2 or later will work with other membership providers. However, the AD password management facilities must be disabled. These only work with the AD membership provider, and authentication with other membership providers will fail if this feature is enabled.

52.6 Troubleshooting

52.6.1 TURing image does not appear

A red cross may be present where the TURing image should appear. The usual causes are:

Incorrect path to PINsafe appliance

Self Signed Certificate is used, but the allow self signed certificate option has not been selected

Firewall blocking access to PINsafe server

Network issue

HTTP request against the PINsafe running HTTPS

52.6.2 Error Messages

502 - Bad Gateway

This has been seen where the SharePoint cannot connect to the PINsafe server. Check the above, particularly the settings for SSL or HTTP access.

Authentication provider not found

PINsafe cannot be accessed by the SharePoint server, verify connectivity settings.

53 Microsoft Sharepoint Integration Methods

53.1 Overview

This document describes methods of integrating Swivel authentication with earlier versions of SharePoint that do not support claims-based authentication. Although these methods will work with later versions of SharePoint, it is recommended that you use the appropriate dedicated filters for SharePoint 2010 and 2013, in the following links:

SharePoint 2010

SharePoint 2013

53.2 Integration Using TMG or ISA

Our recommended solution for earlier versions of SharePoint is to use Microsoft TMG integration with RADIUS authentication (see here or here), or Microsoft ISA Server with RADIUS authentication (see Microsoft ISA 2006 Integration). However, the following article shows how to integrate with SharePoint as a 2-stage authentication process.

53.3 Authenticating to Earlier Versions of SharePoint as a 2-Stage Process

The solution is to use the PINsafe IIS7 filter. Install as per the included instructions.

The result should be that you will need to authenticate first to the Active Directory domain, if you are not already logged in. Subsequently, you will be redirected to the PINsafe login page to complete the second part of the authentication process, before being finally redirected to the SharePoint home page.

One issue which is not addressed by the IIS filter documentation, which might cause problems, particularly in Windows 2008 Server, is that the Windows account running the SharePoint application (normally Network Service) needs to have read and execute permission on the pinsafe virtual directory.

54 Oracle Access Manager Integration

54.1 Overview

This article provides a basis for integration with Oracle Access Manager 10g.

Client code is included which you can deploy in conjunction with your Oracle Access Manager and PINsafe environment.

54.2 Prerequisites

- Oracle Access Manager 10g
- PINsafe 3.8

Download GenericIntegration.zip to obtain the client code for this integration. The code contains Eclipse project settings and a pre-built version of the WAR file for deployment.

54.3 Deployment

Deploy the war file into the Apache Tomcat webapps folder of your existing PINsafe 3.8 installation.

If using a PINsafe appliance, you can use WinSCP. See the WinSCP How To Guide for further information on transferring files to a PINsafe appliance.

54.4 Integration

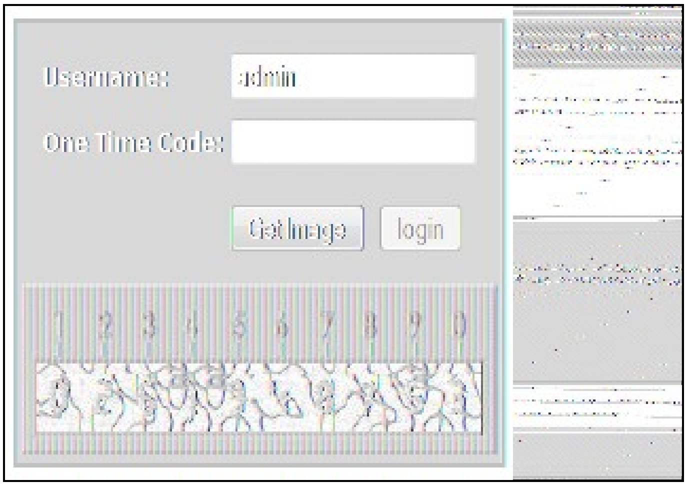


Image showing the Generic Integration login page
The integration requires a JSP containing username, password, OTC and the TURing image. Upon ?Logon? this is posted to a servlet which extracts the username, password and OTC from the request and calls the login (username, password, otc) of the PINsafeClient class (supplied in the jar). This method sends an HTTP request to PINsafe to allow a user to login or change their PIN.

Some pointers regarding the sample code provided:

- Marked in the code is the point in login.jsp where the creating of the OAM cookie described below should occur.
- WEB-INF/settings.xml contains the configuration to point to the PINsafe server, where to redirect upon success and whether or not to use a password.
- WEB-INF/settings2.xml contains a configuration for secondary server, for high availability purposes.

54.5 Authentication Process

During authentication, if the user is authenticated by PINsafe then depending on elements specific to your integration, you would either:

- Create an OAM cookie, which would require knowledge and availability of the OAM API;
- Redirect to the location for normal processing of the login (typically /oblix/login.cgi as detailed on the Oracle website). This would require a filter to stop anyone calling /oblix/login.cgi directly.