Huddle

WORK IN PROGRESS PLEASE CONTACT SWIVEL IF YOU REQUIRE THIS INTEGRATION

Contents

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.

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.

Downloads

AuthenticationPortal-huddle.war software

Baseline

(The version tested with)

Swivel authentication platform 3.9.5

Architecture

Installation

Configure The Swivel Server

Configure a Swivel Agent (For standard XML Authentication)

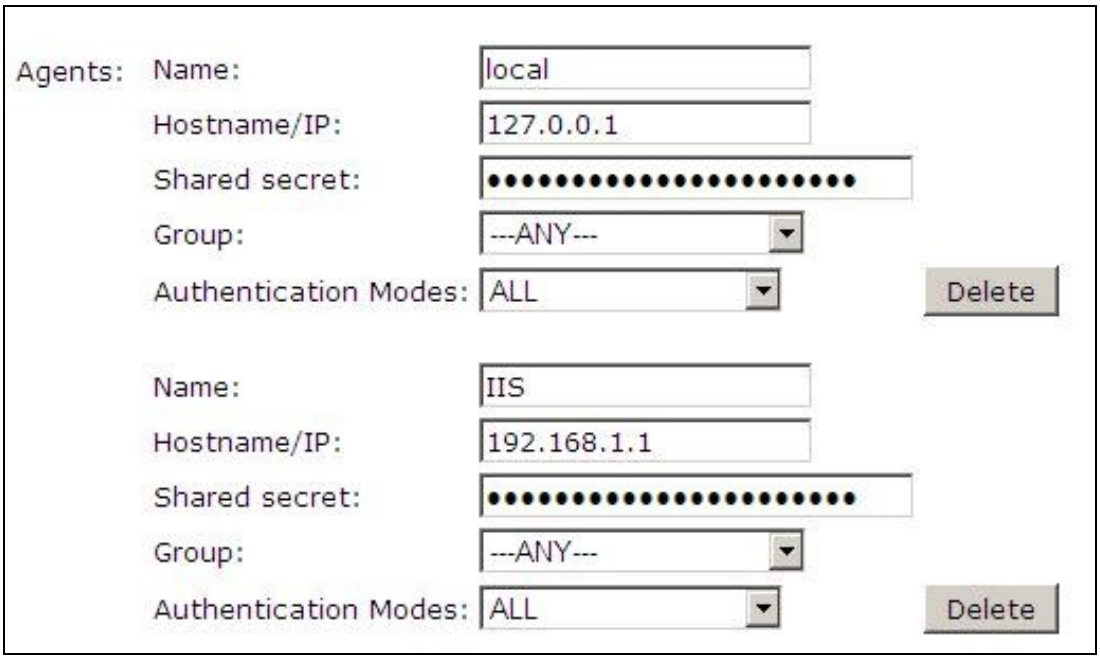
1. On the Swivel Management Console select Server/Agent

2. Enter a name for the Agent

3. Enter the Exchange IP address

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

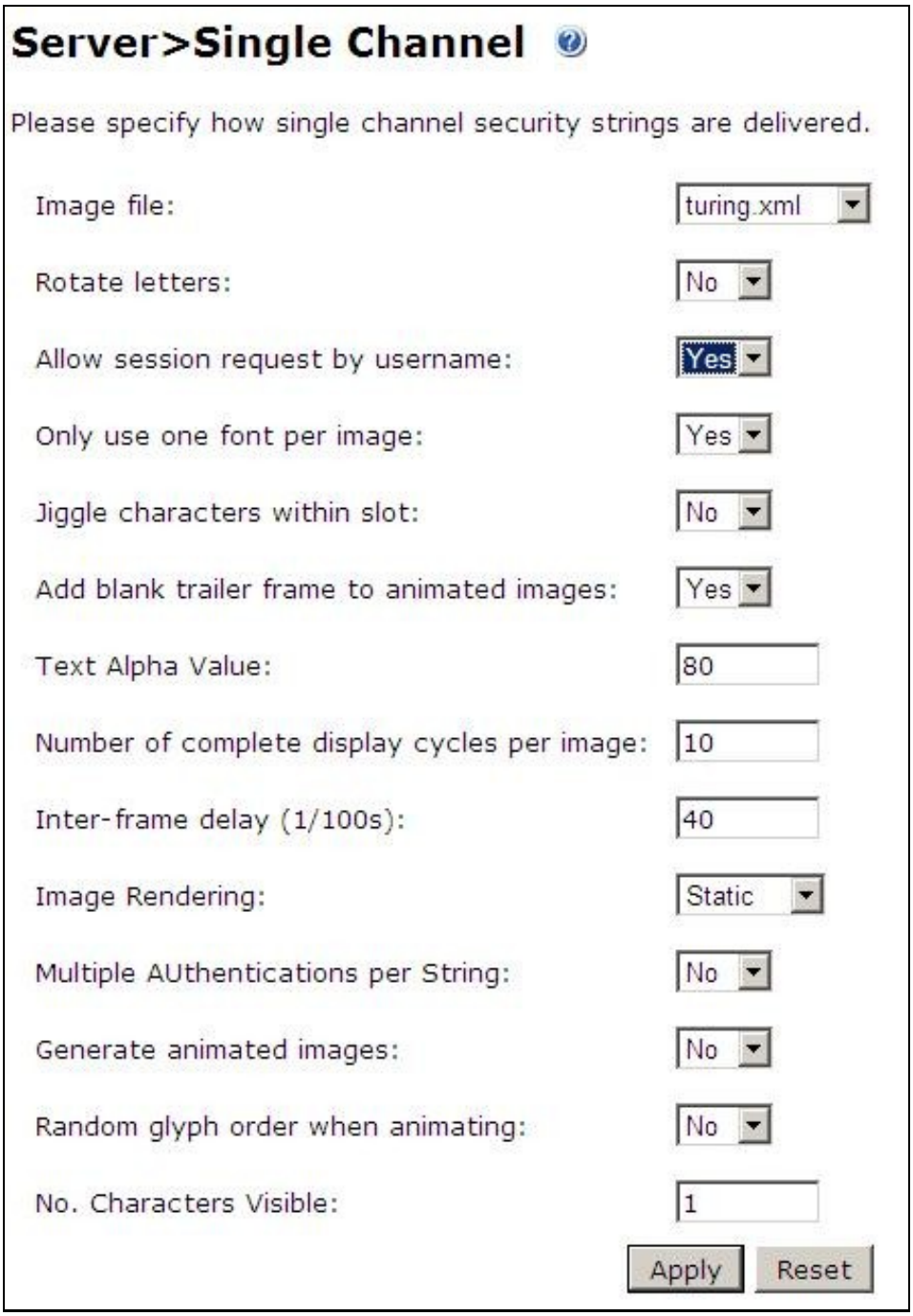
5. Click on Apply to save changes



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



Using additional attributes for authentication

When using additional attributes for authentication see User Attributes How To

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.

Create private keys and certificates

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

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
```

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.

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,

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

Huddle Integration

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

dsacert.pem

generatedIdPMetadata.xml

Additional Installation Options

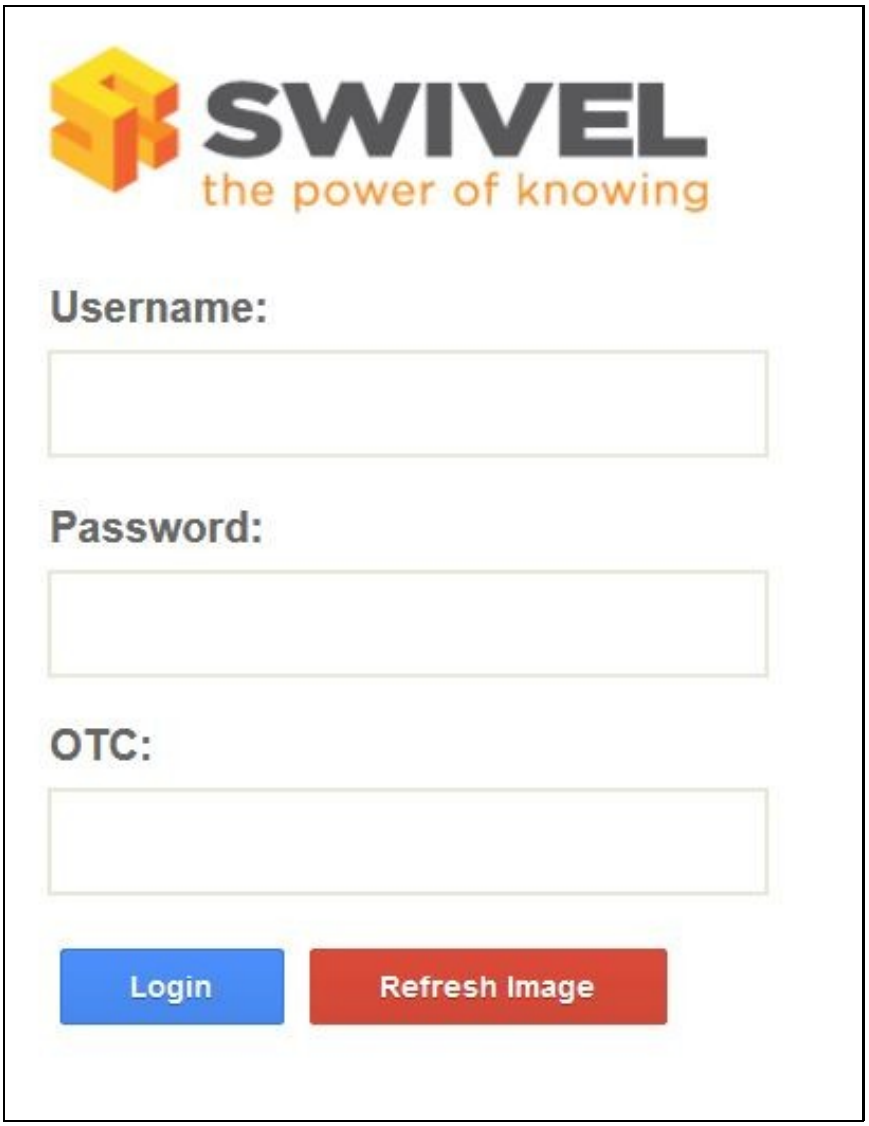
Testing the Installation

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

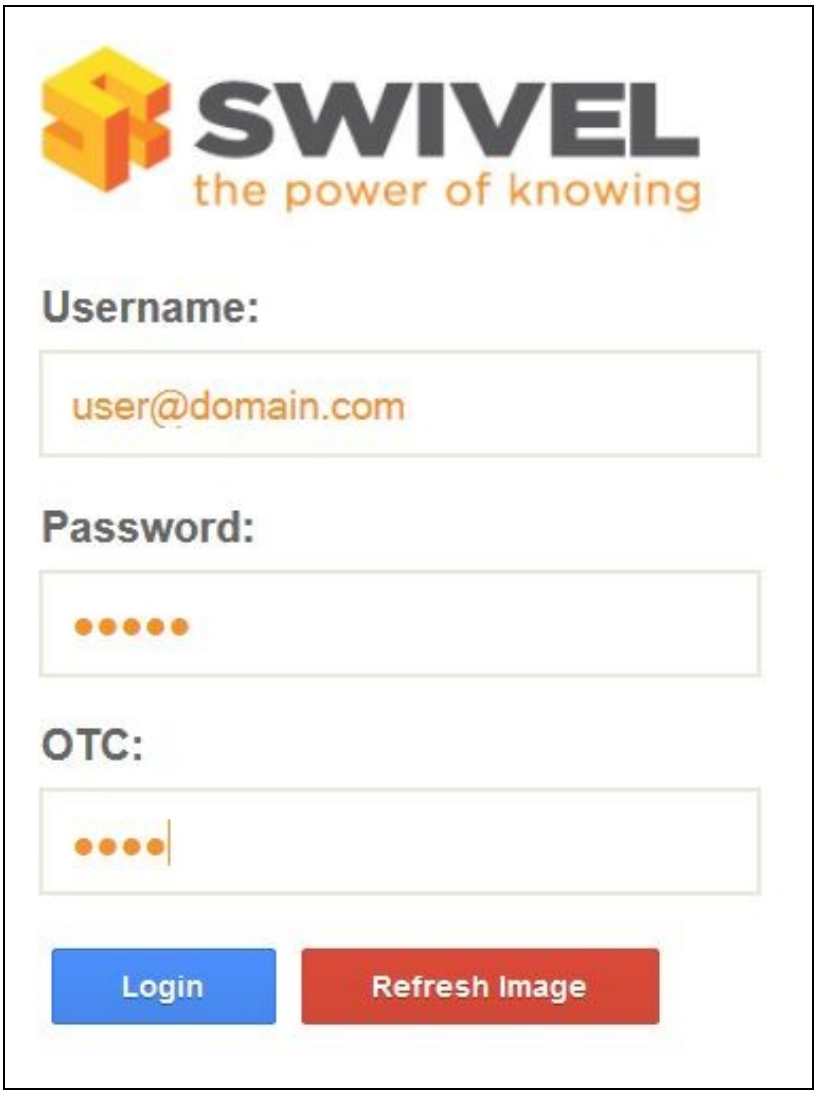
Swivel appliance install: https://swivel_appliance:8443/AuthenticationPortal-huddle/identity_provider.jsp

For a software only install see Software Only Installation

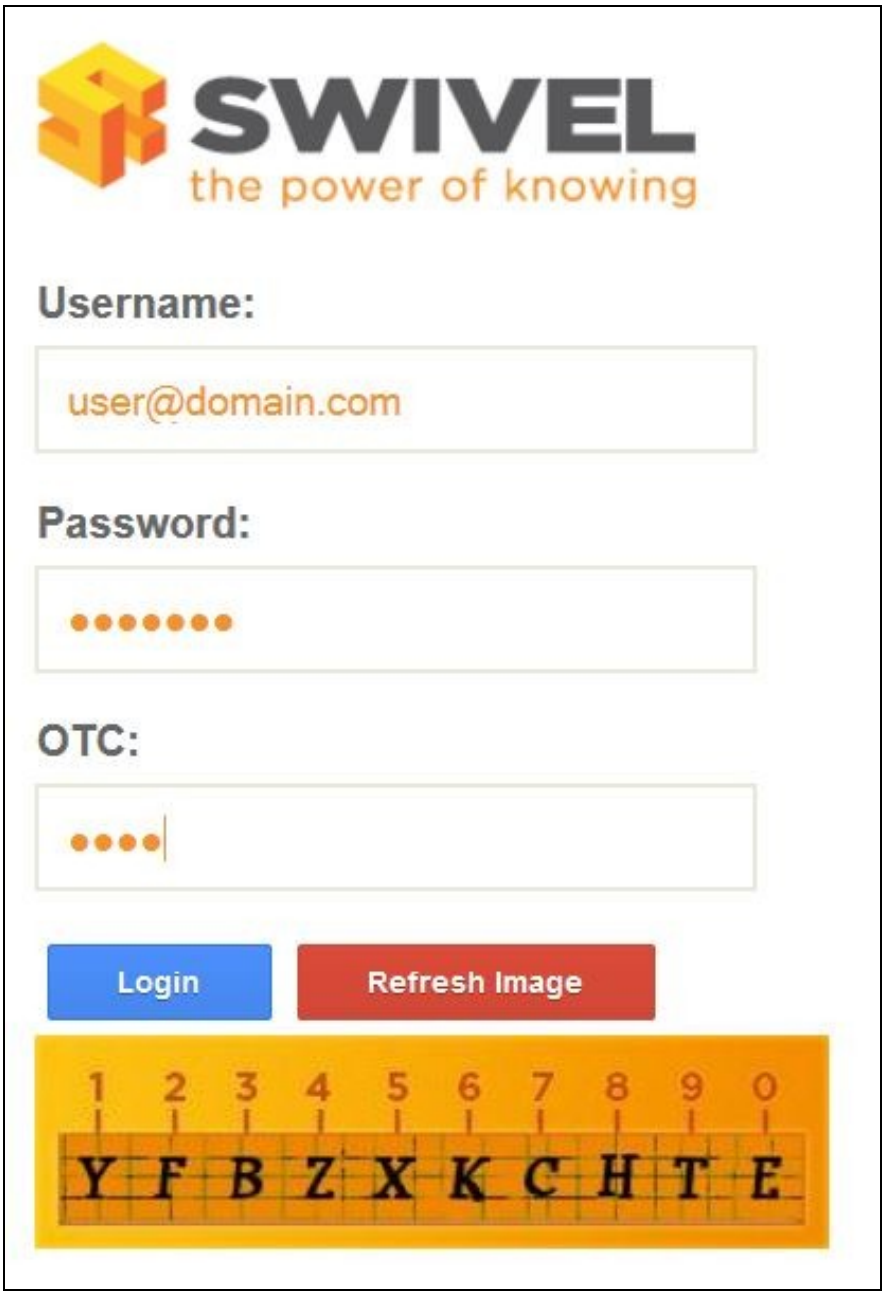
Swivel login page



Dual Channel Authentication



Single Channel Authentication



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/

Uninstalling the Swivel Integration

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

Known Issues and Limitations

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.