Table of Contents

Table of Contents

1 Authentication Manager

2 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.

3 Prerequisites

Swivel Version 3.10.3 or later

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

4 Configuring the Swivel server

4.1 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.

4.1.1 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.

4.2 Configuring the Admin login

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

5 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

5.1 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

5.1.1 Additional settings

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

5.2 Key and Certificate generation

Key and Certificate Generation

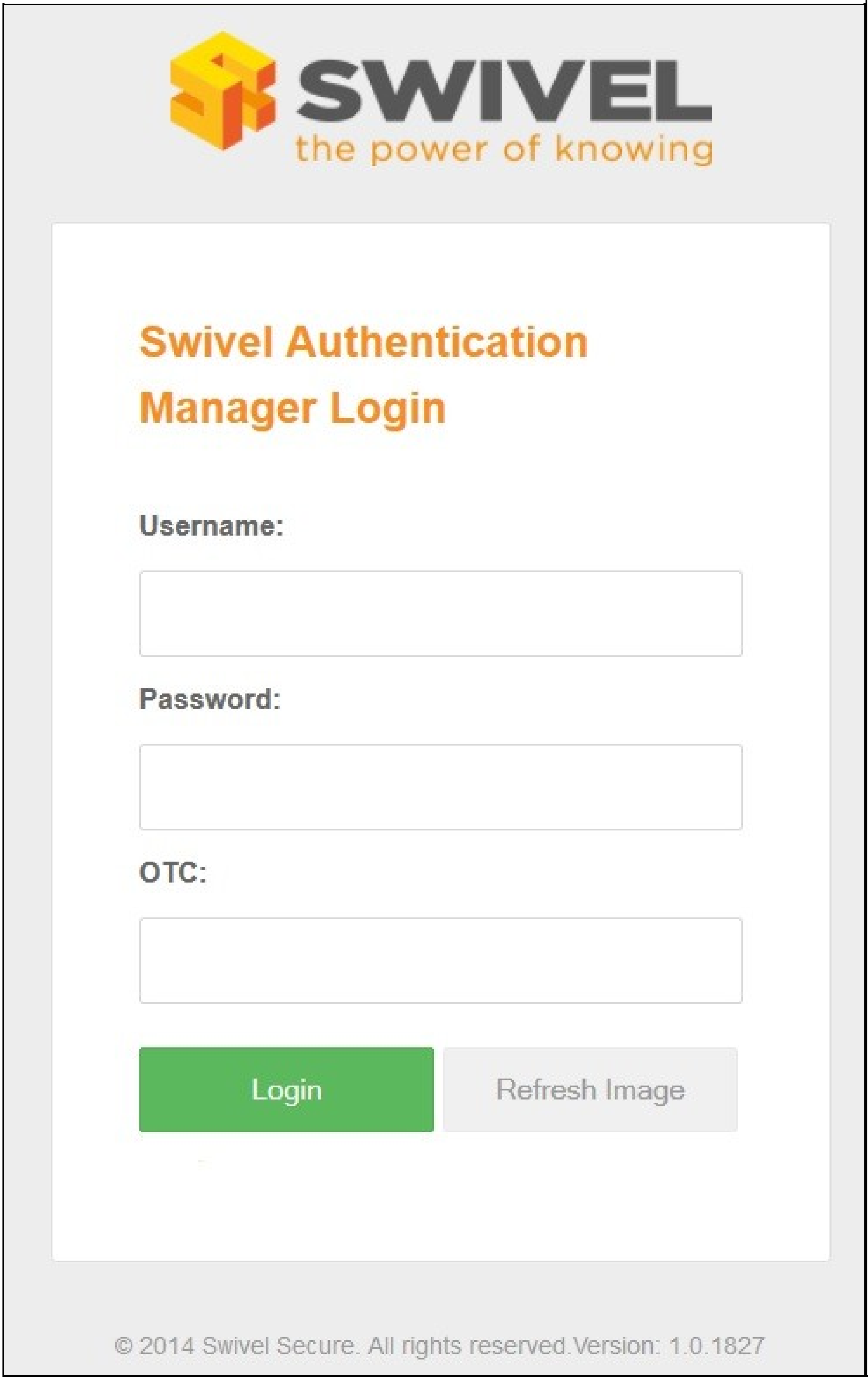
5.3 Swivel Authentication Manager Login

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.



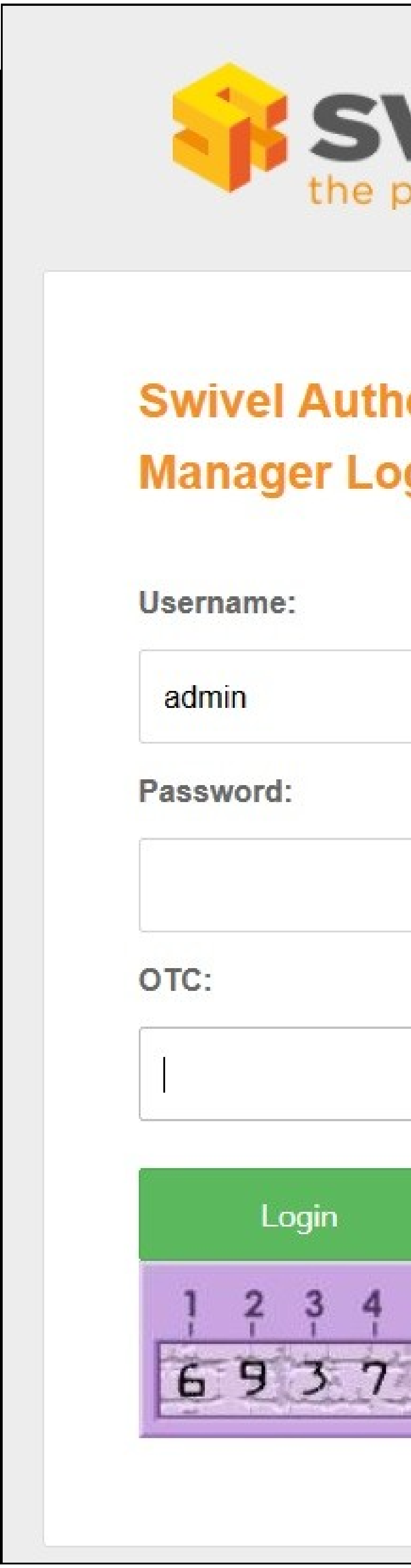
Swivel Authentication Manager Login

Username:

Password:

OTC:

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



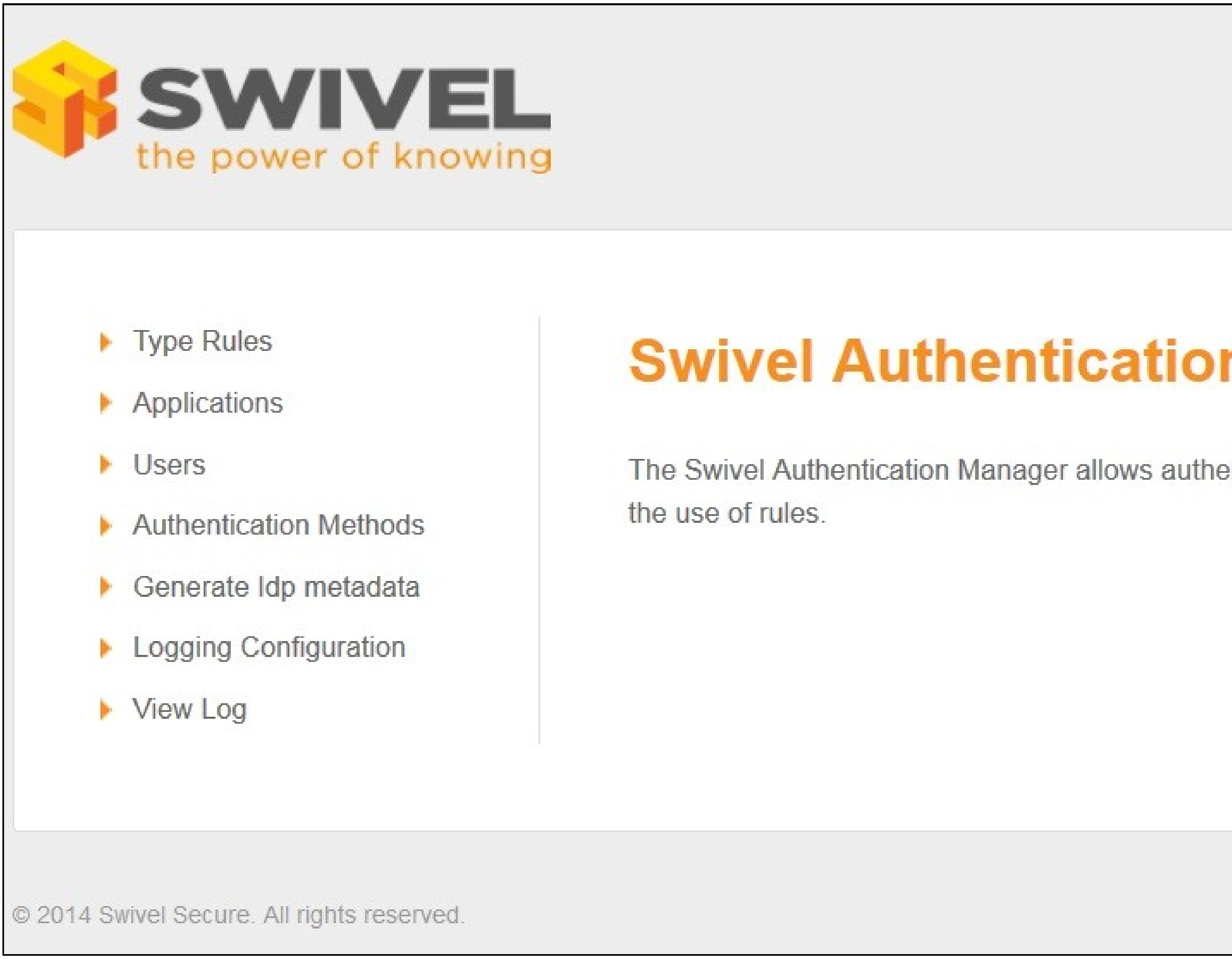
Swivel Authe
Manager Lo

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.

5.4 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.

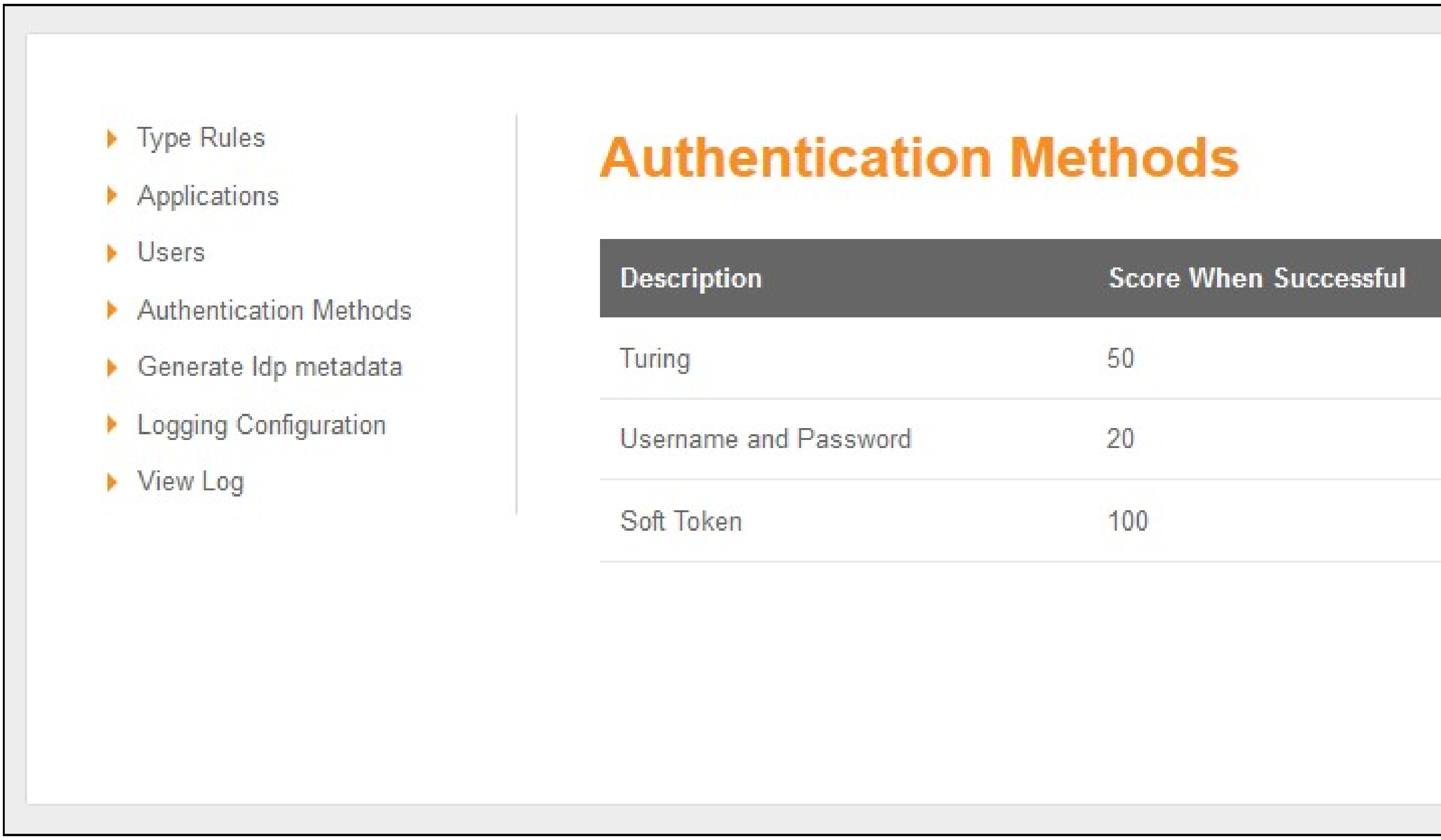
2) State the number of points required before the user can gain access.

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.

5.5 Authentication Methods



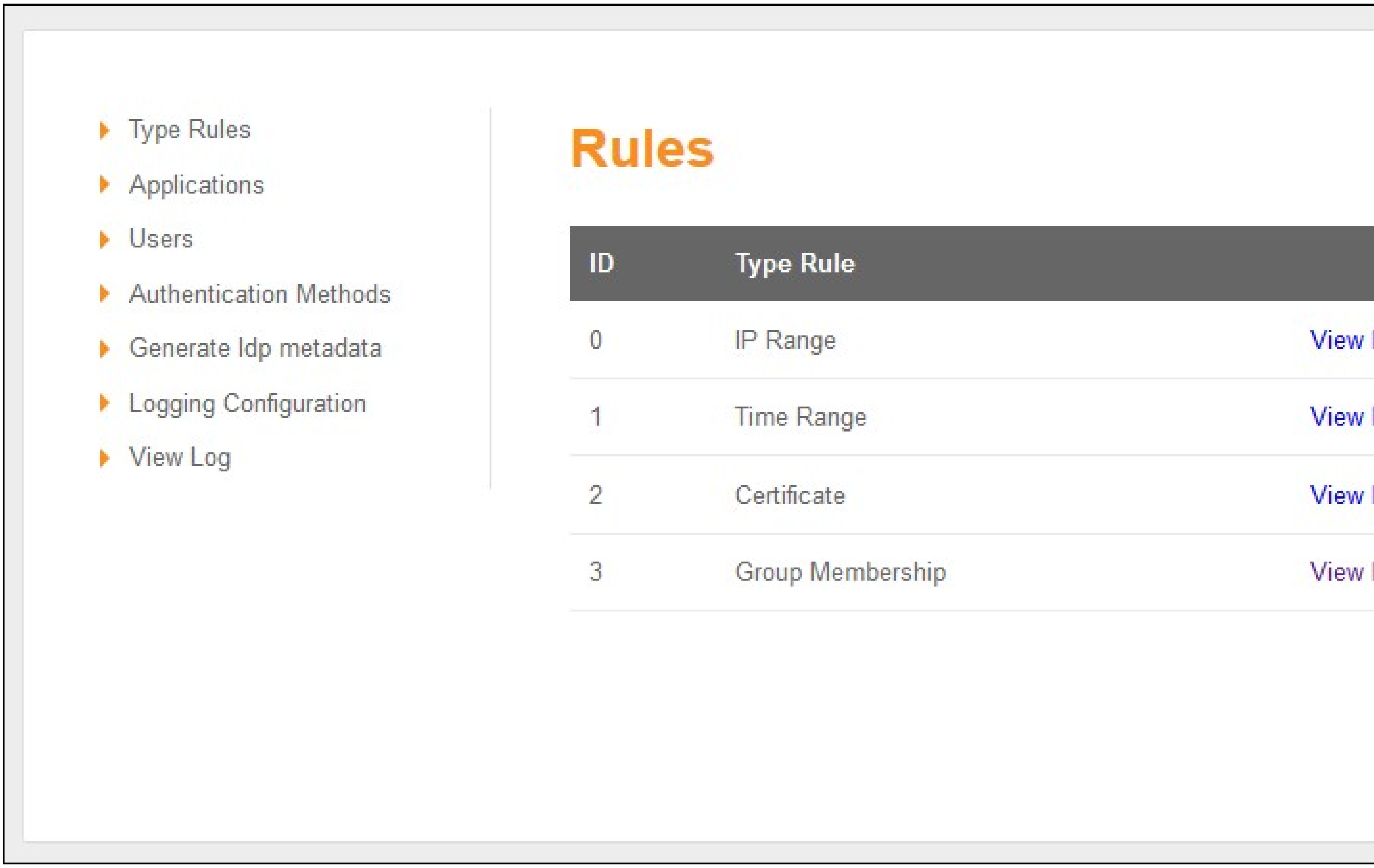
Authentication Methods

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.

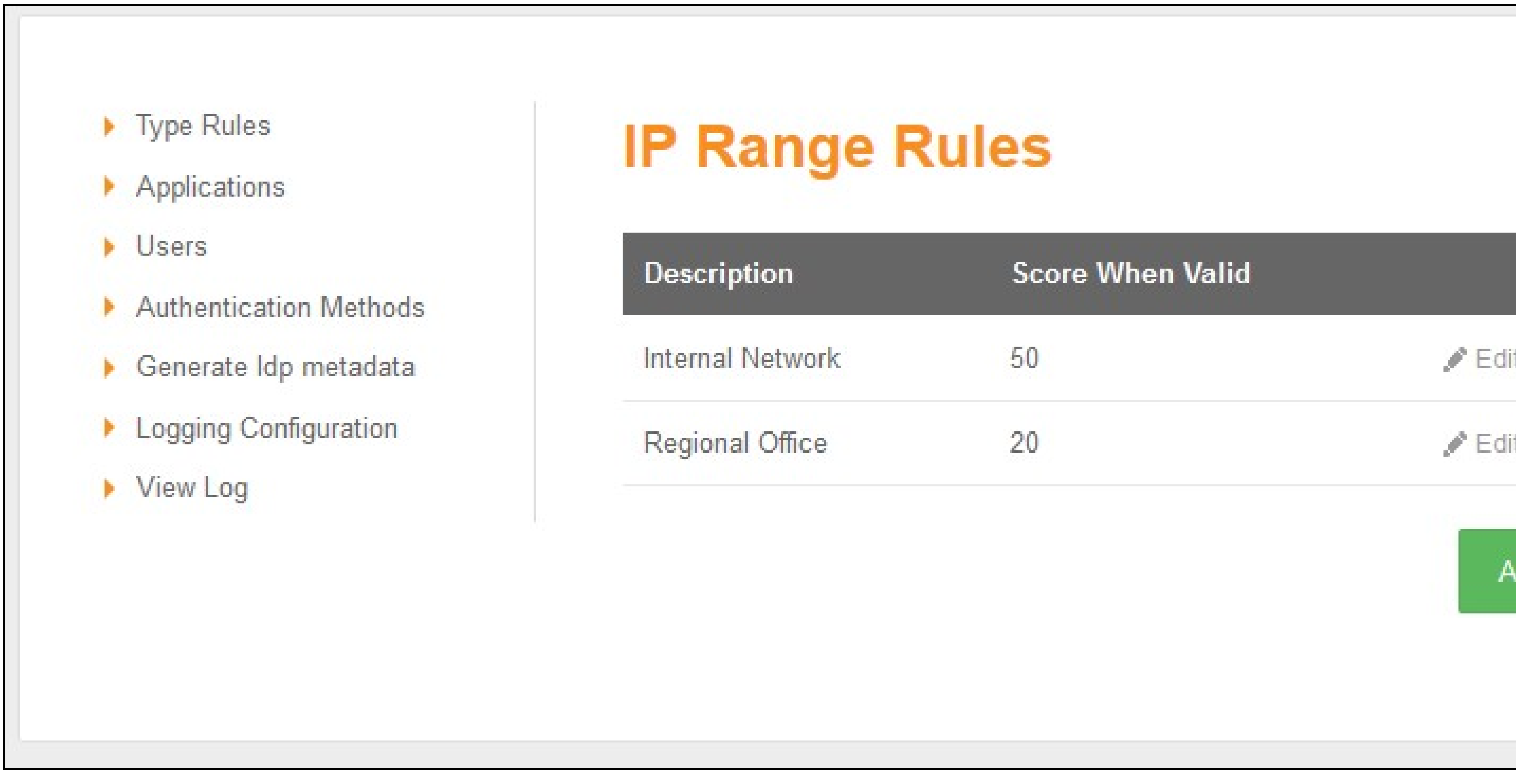
5.6 Rules



Rules

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

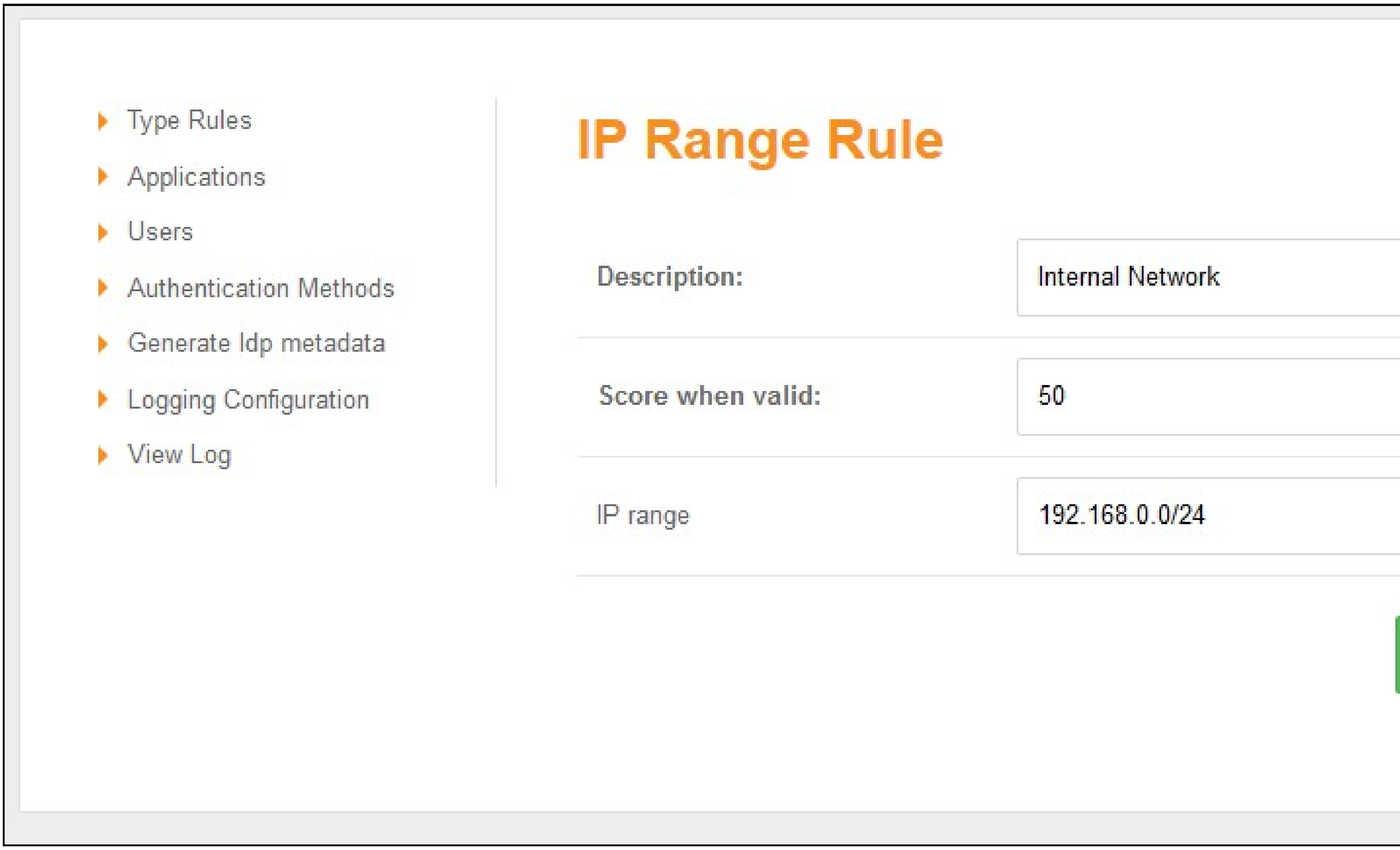
Rules are the means by which the system administrator can take into account a number of risk factors into account when deciding how a user should authenticate. The admin specifies the rule and then how many points the user is awarded (or penalised) should the rule be true for that user.



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

5.6.1 IP address

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

5.6.2 Time of Day

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

5.6.3 X509 Certificate

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

5.6.4 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)

5.6.5 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)

5.6.6 Location (Geo-IP)

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

5.7 Users

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

Username

Points

Federated ID

IP

Applications

5.8 Logging

5.8.1 Logging Configuration

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

5.8.2 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

5.9 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.

6 Testing

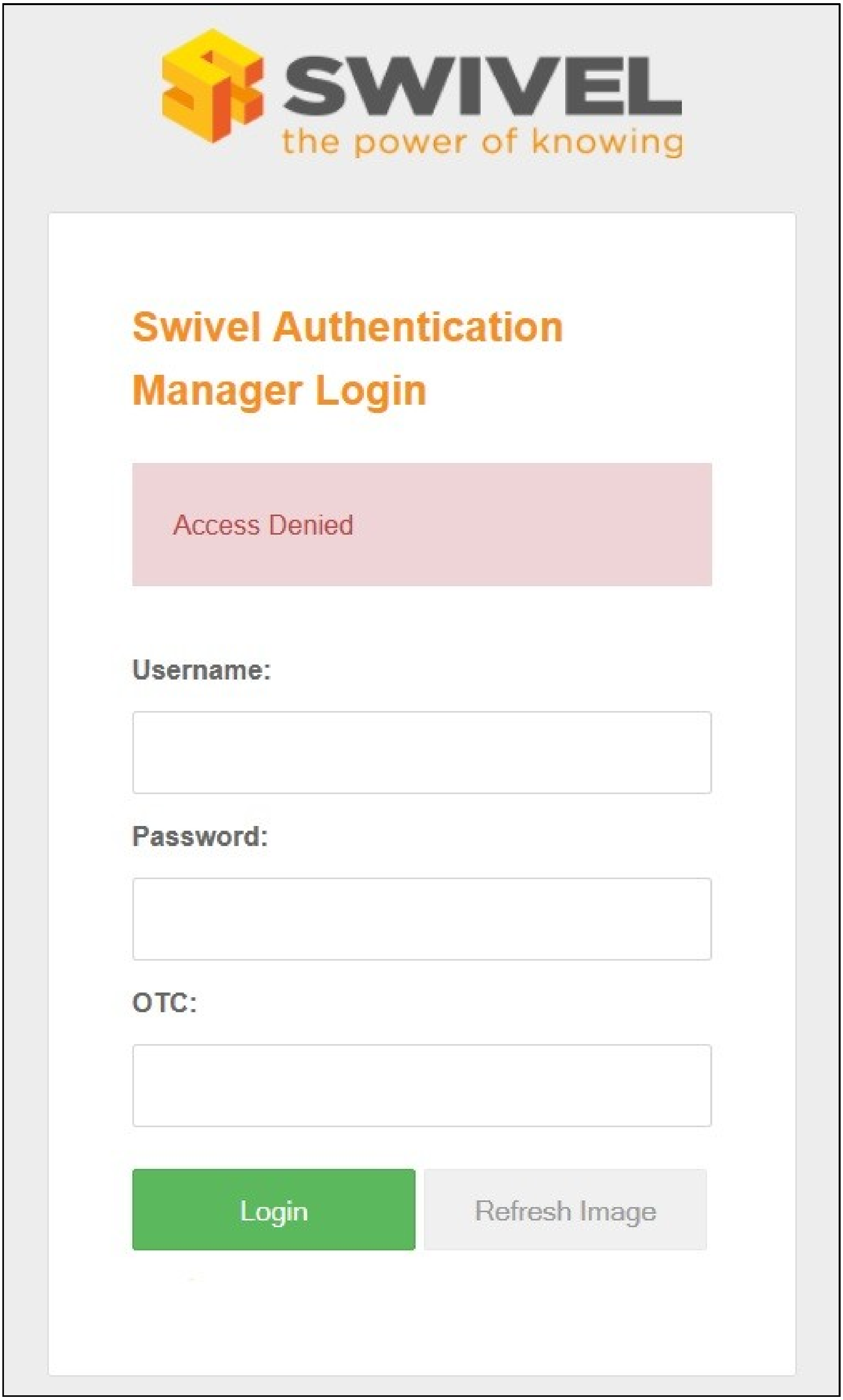
7 Known Issues

8 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
```

8.1 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.

9 Google Apps Integration

10 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.

11 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.

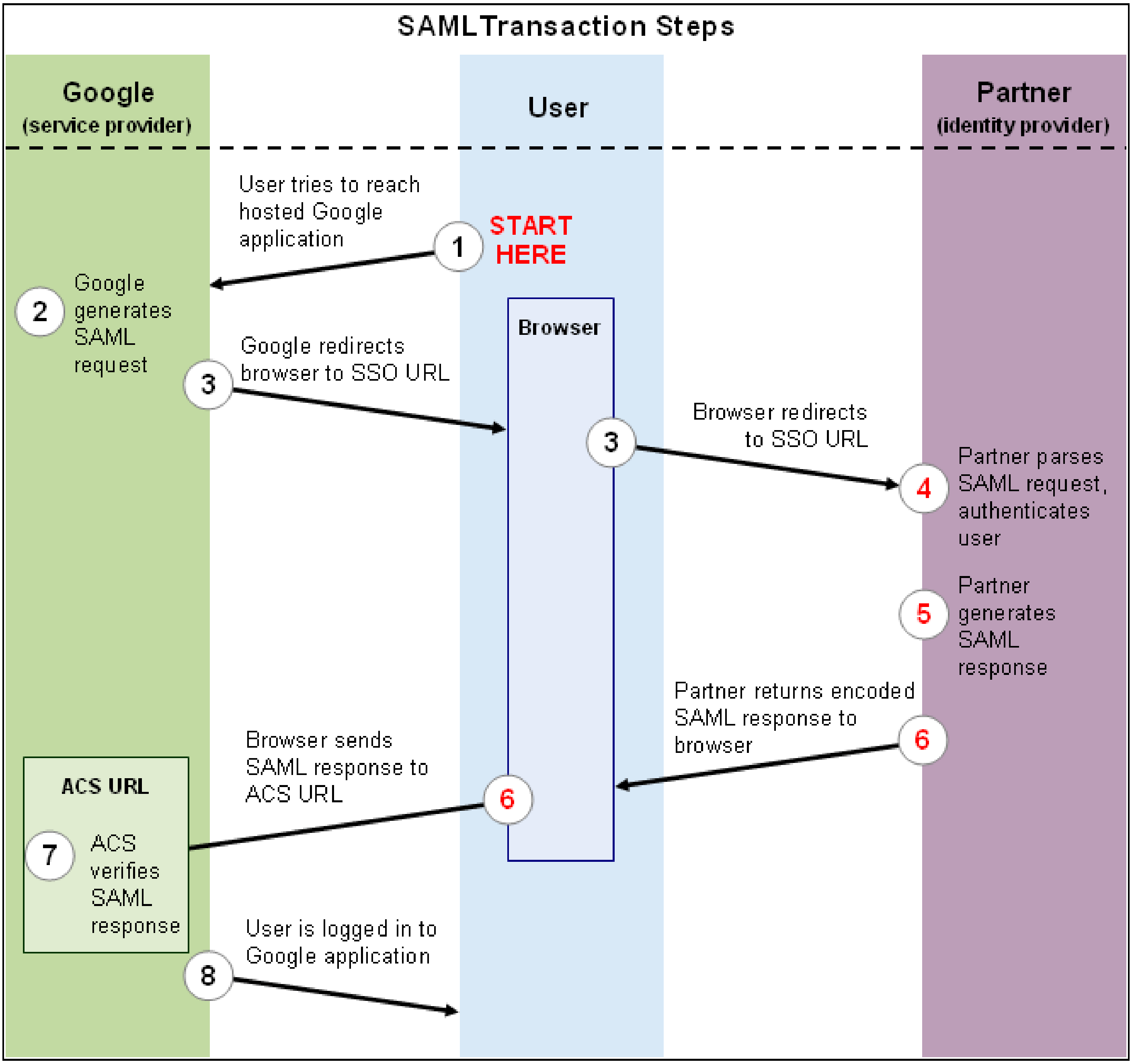
Swivel Google Authentication Portal.

12 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.

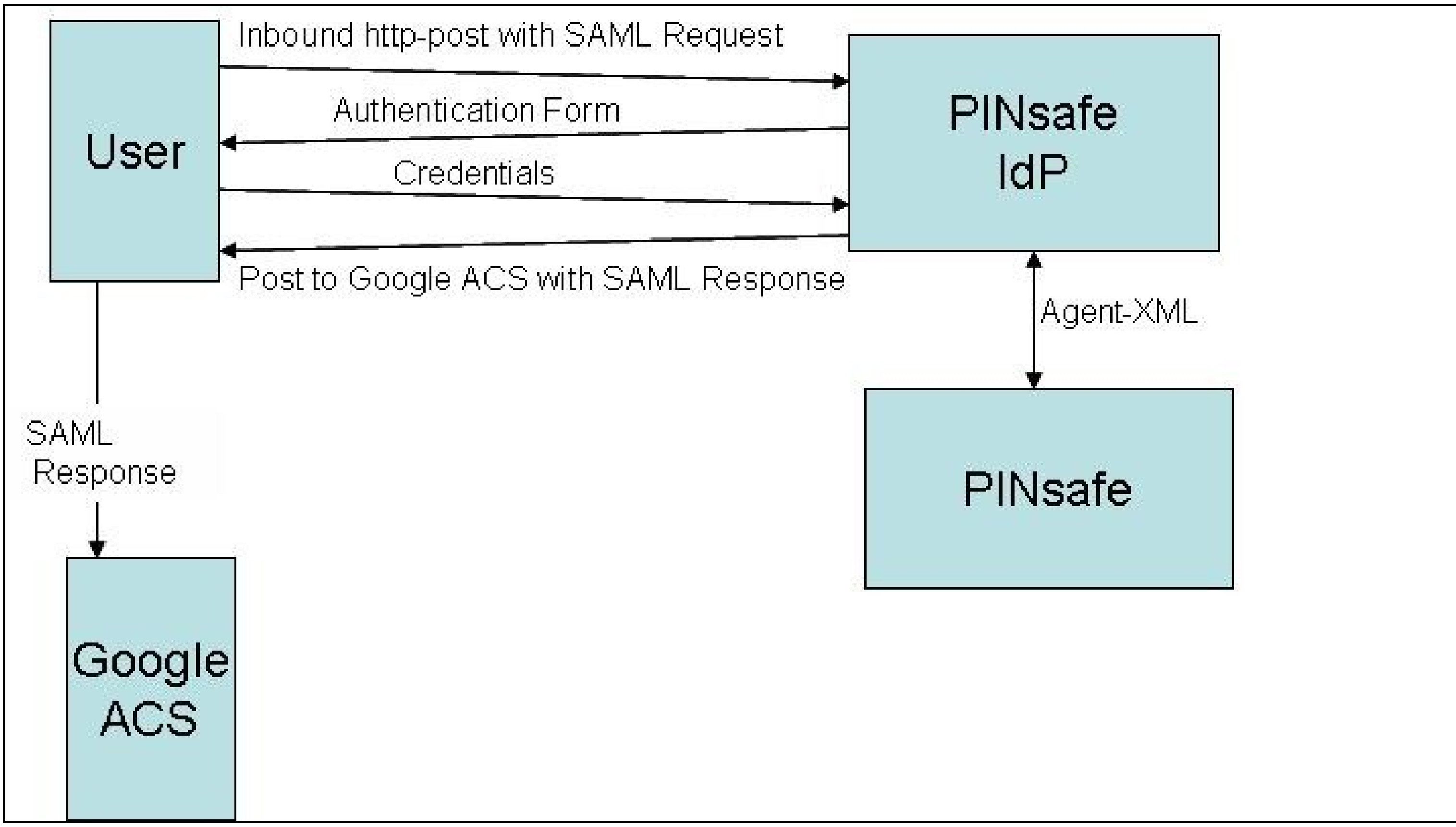
That redirect will include a SAML request. The request includes the url of the Google Apps ACS (Assertion Consumer Service). This is the Google Apps Service that controls access to Google Apps


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
Google redirects browser to SSO URL
3
Browser redirects to SSO URL
3
4
Partner parses SAML request, authenticates user
5
Partner generates SAML response
Partner returns encoded SAML response to browser
6
Browser sends SAML response to ACS URL
6
ACS URL
7
ACS verifies SAML response
User is logged in to Google application
8

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.

13 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.



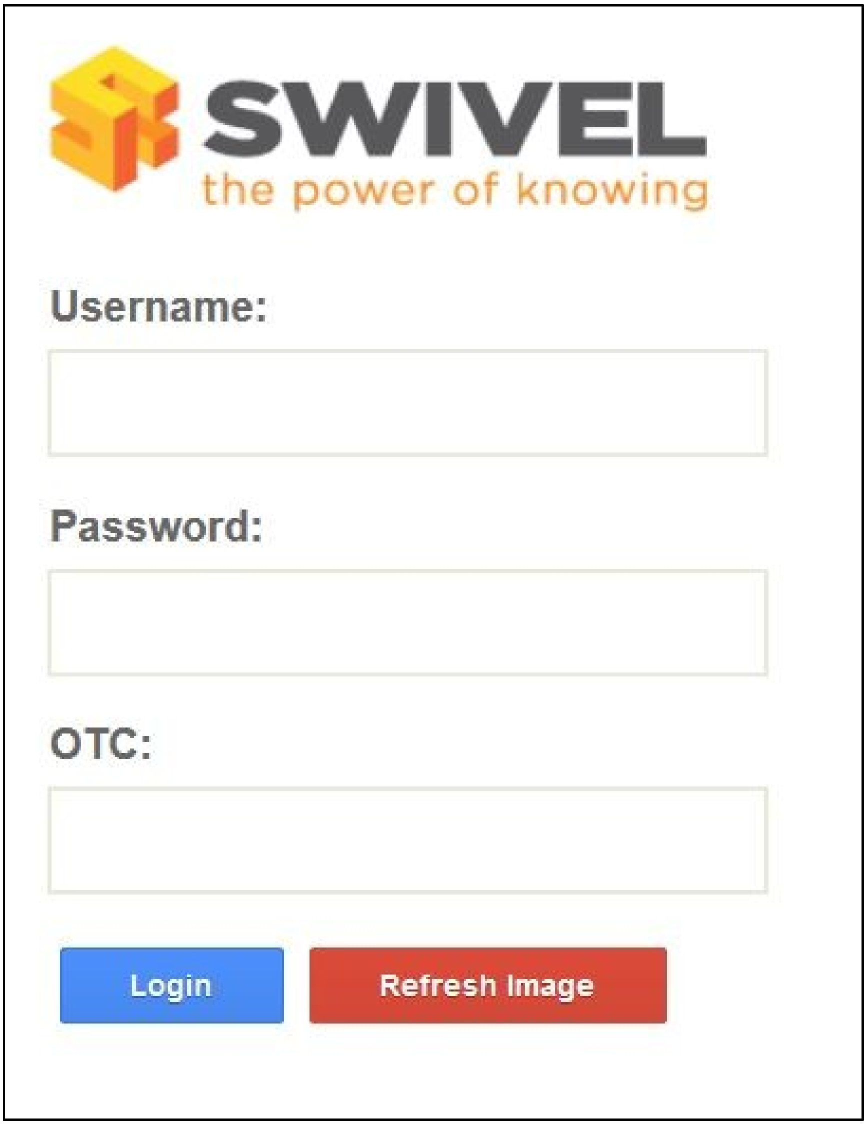
This application needs to be publicly accessible so that users can authenticate to it, it also needs to be configured as an agent on a Swivel server. More detailed configuration information appears later in this document.

14 User Experience

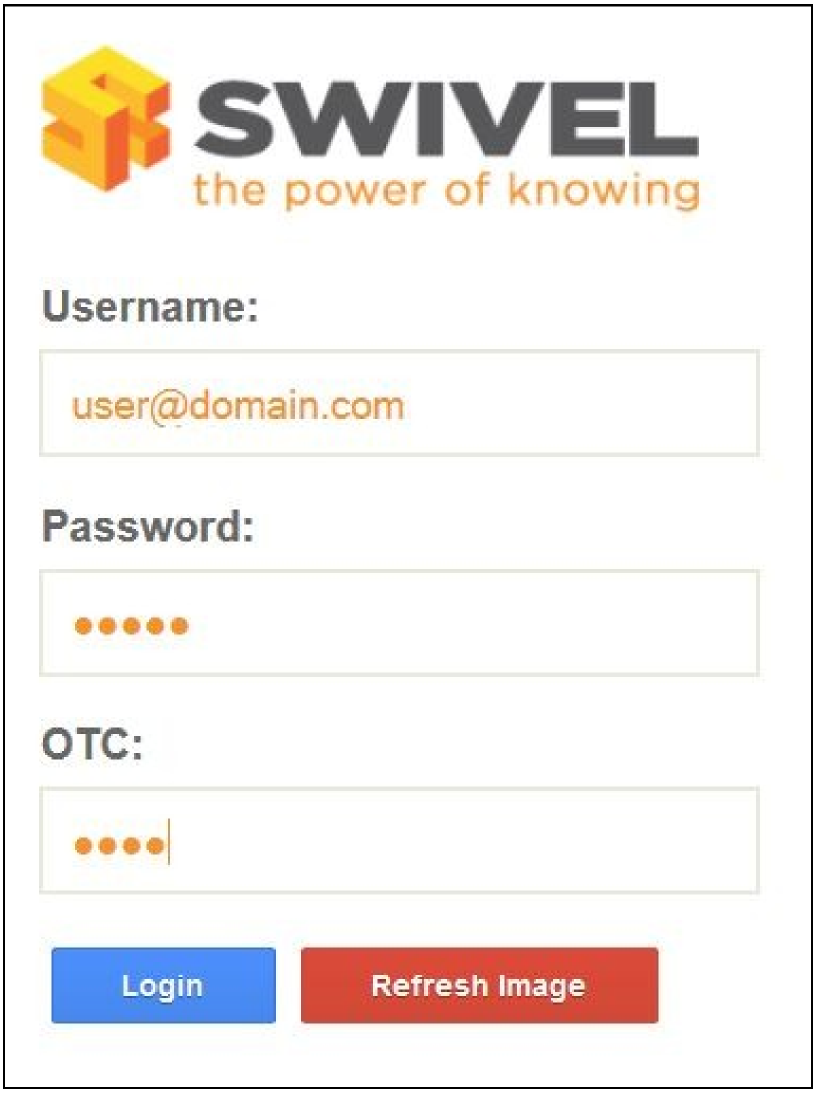
The user opens a browser and accesses googleApps e.g. http://mail.google.com/a/swivelsecure.net this is then redirected in a new URL includes the encrypted SAML request.

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

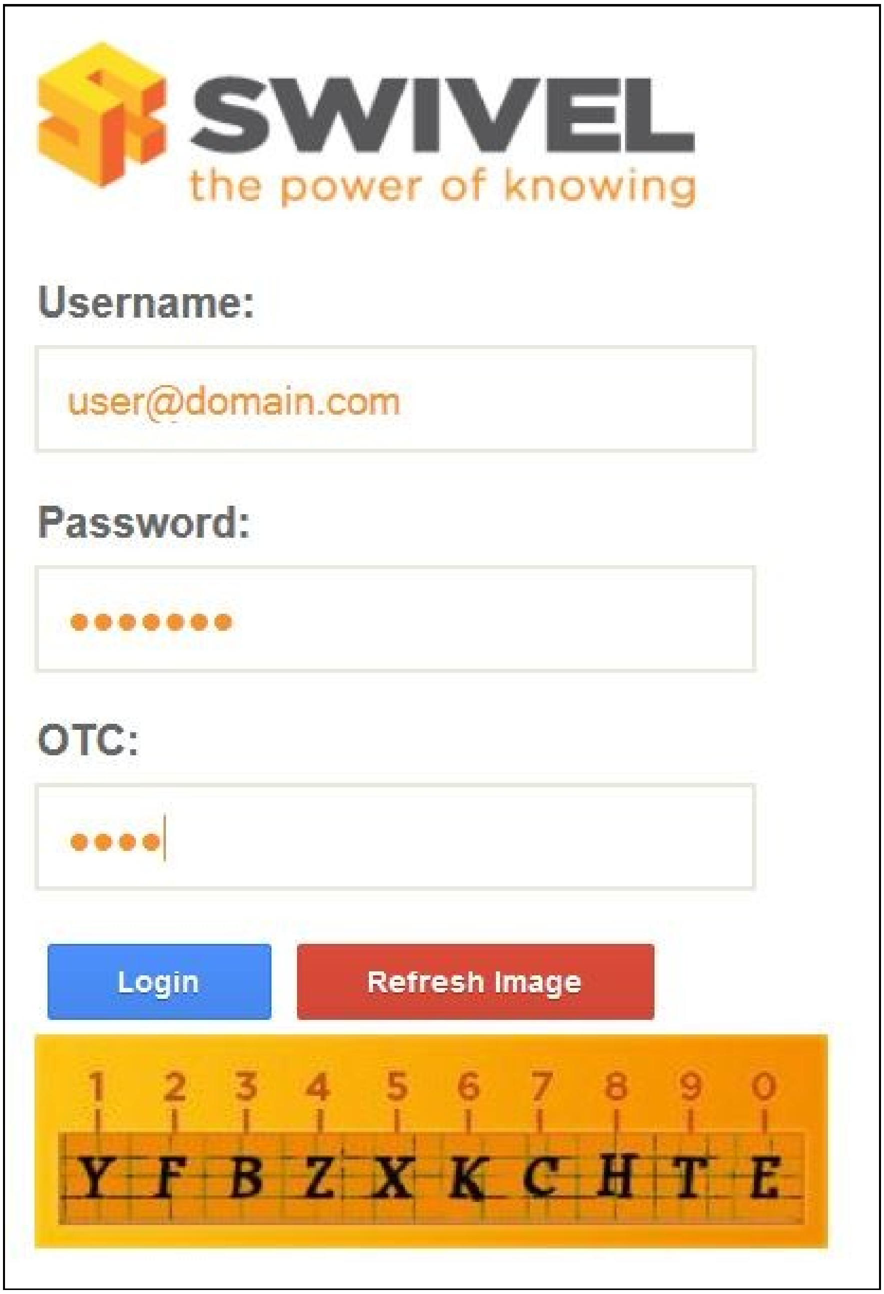


Username: user@domain.com

Password: ●●●●●

OTC: ●●●●

Single Channel Authentication



Username:

user@domain.com

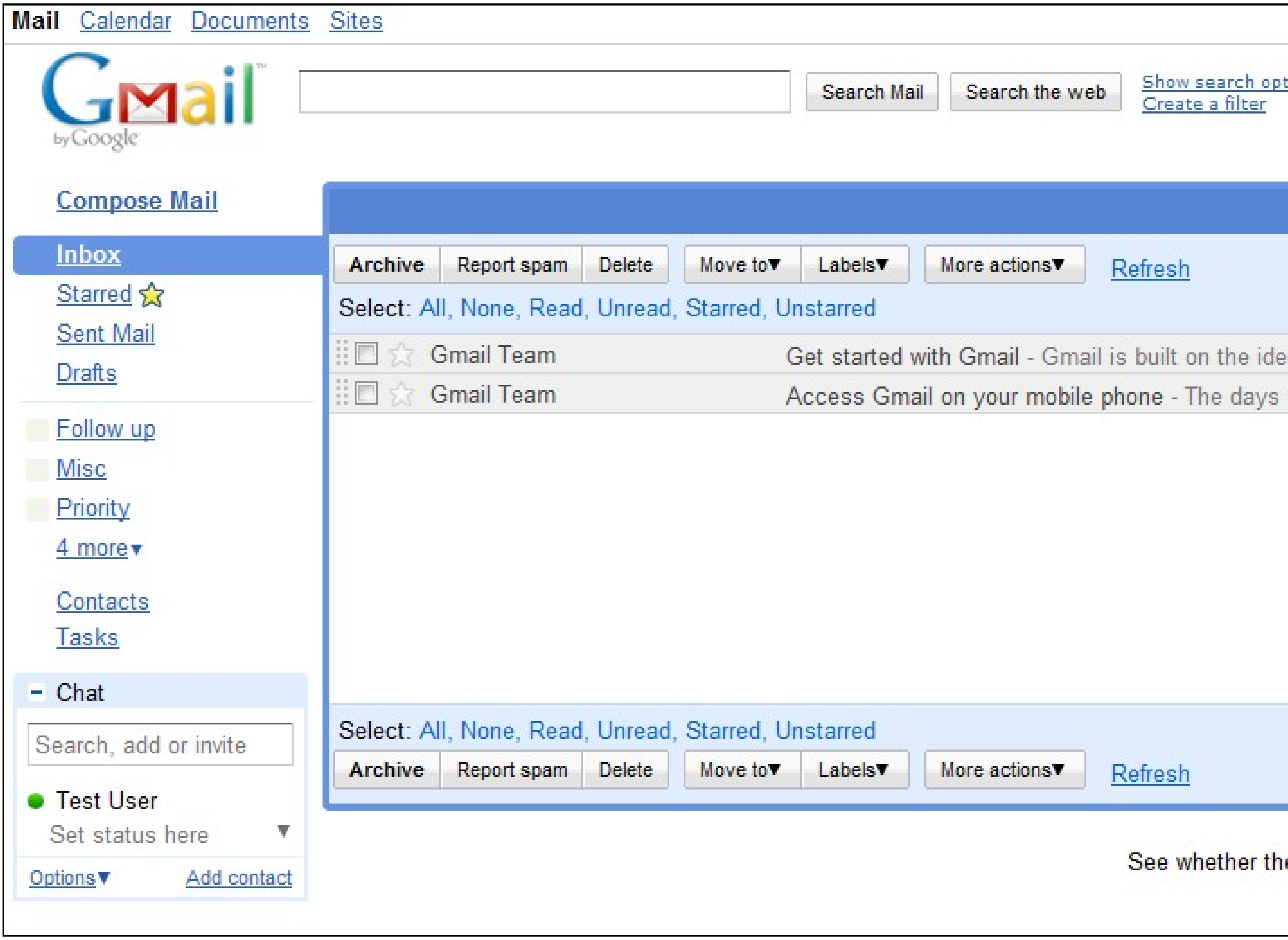
Password:

●●●●●●●

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

15 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.

16 Create private keys and certificates

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

16.1 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.

16.2 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.

17 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

18 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

18.1 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

18.2 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

18.3 Configuring Swivel for Dual Channel Authentication

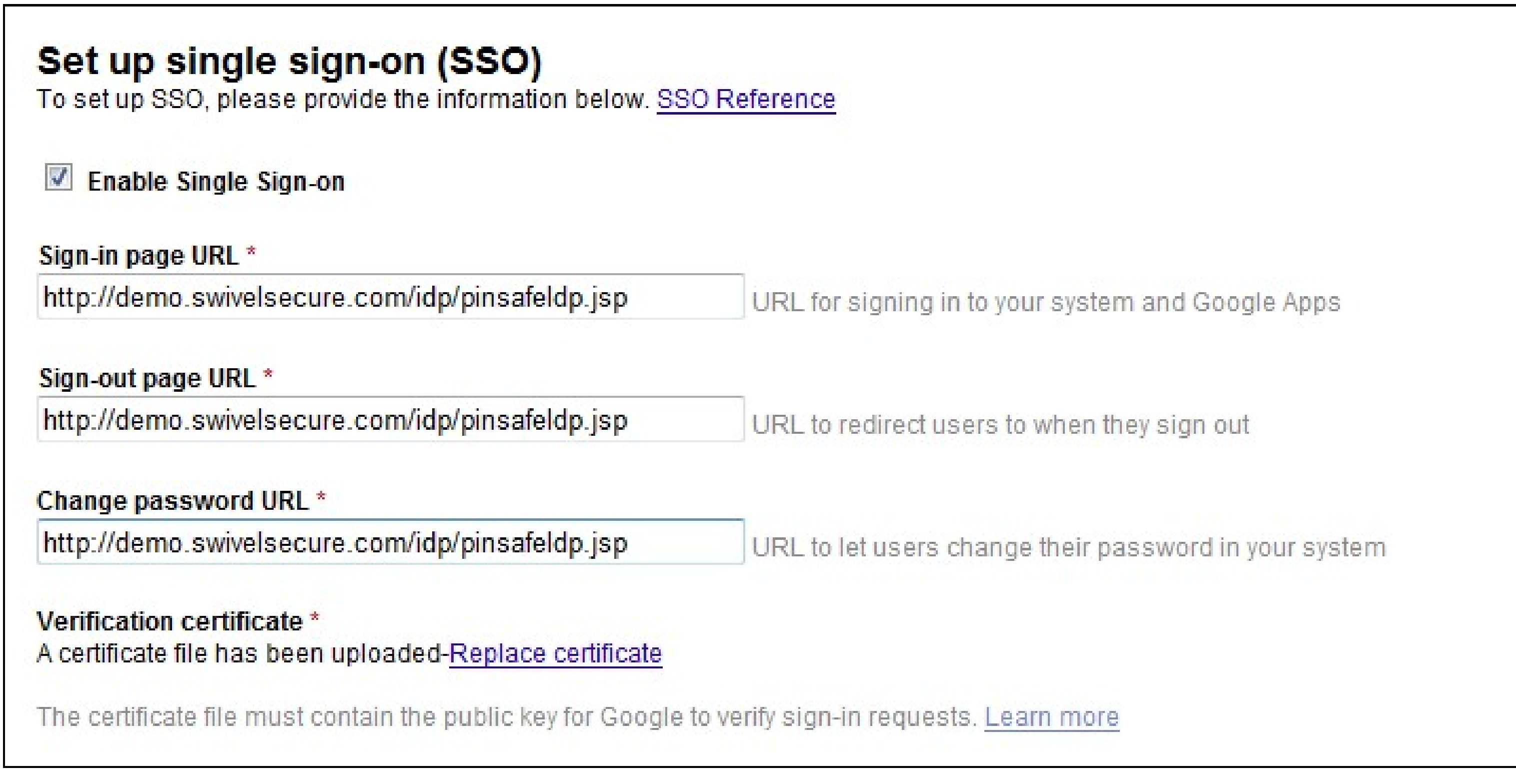
If Swivel Dual Channel authentication methods are to be used, refer to the following guide:

Transport Configuration

19 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.

20 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
```

21 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

21.1 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.

22 Google Docs Integration

See Google Apps Integration

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)

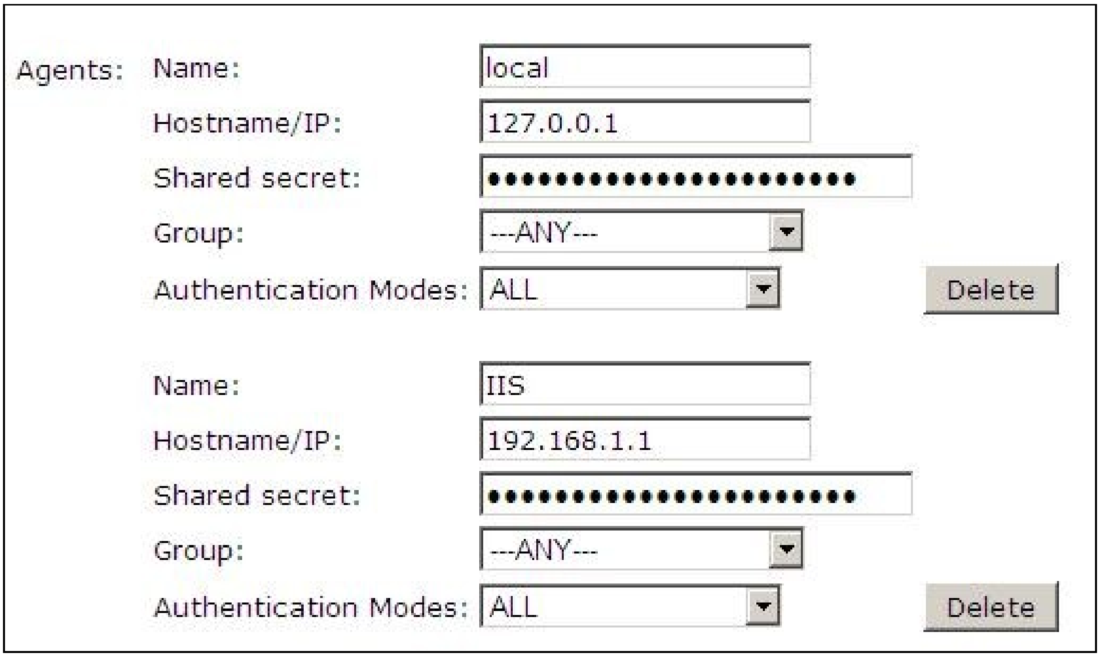
1. On the Swivel Management Console select Server/Agent

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

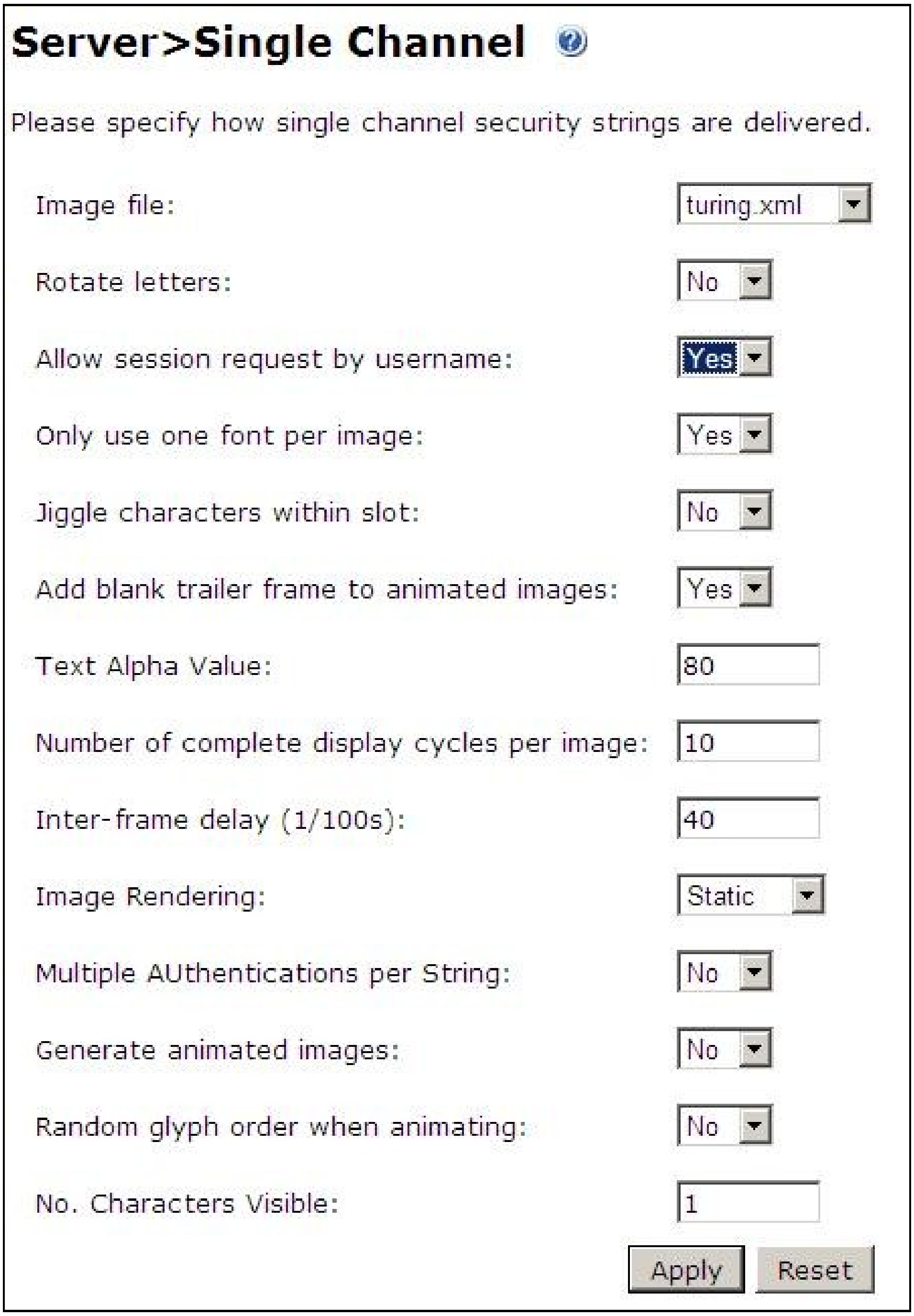


Agents:	Name:	local	
	Hostname/IP:	127.0.0.1	
	Shared secret:	••••••••••••••••••••••	
	Group:	---ANY---	
	Authentication Modes:	ALL	Delete
	Name:	IIS	
	Hostname/IP:	192.168.1.1	
	Shared secret:	••••••••••••••••••••••	
	Group:	---ANY---	
	Authentication Modes:	ALL	Delete

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

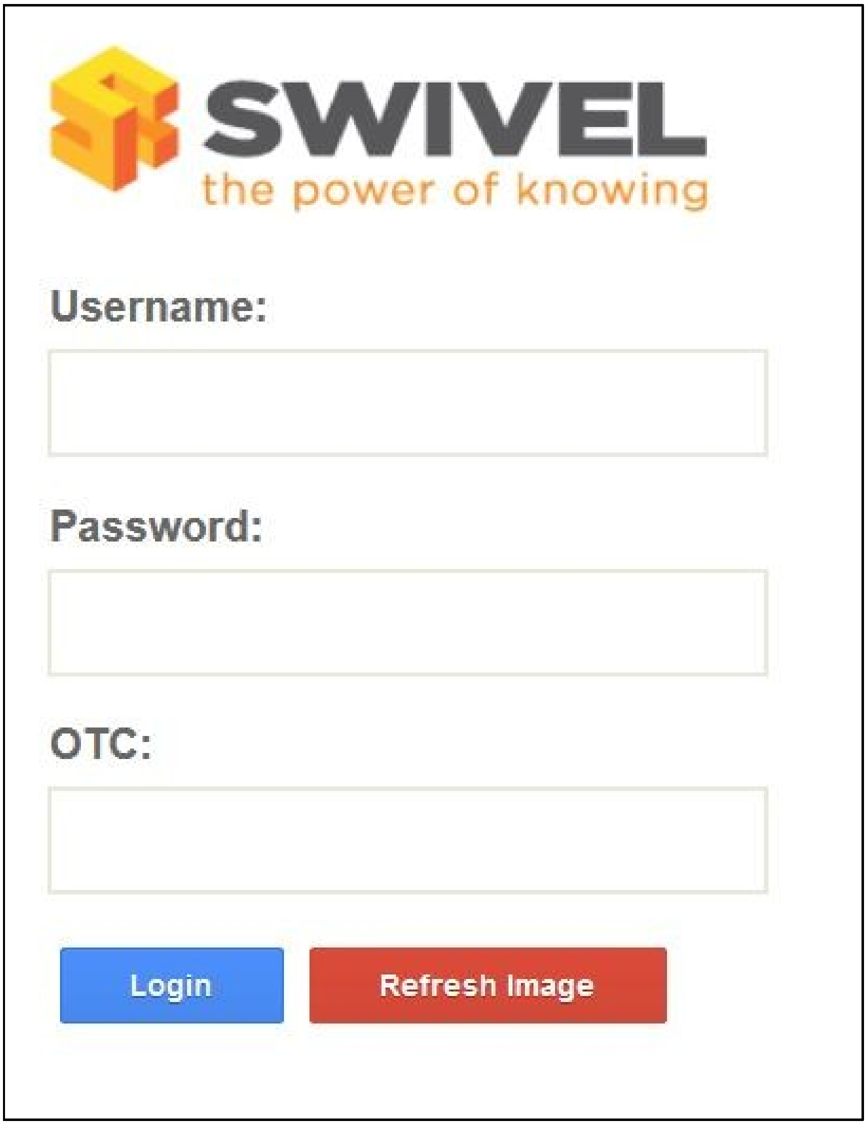
29 Testing the Installation

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

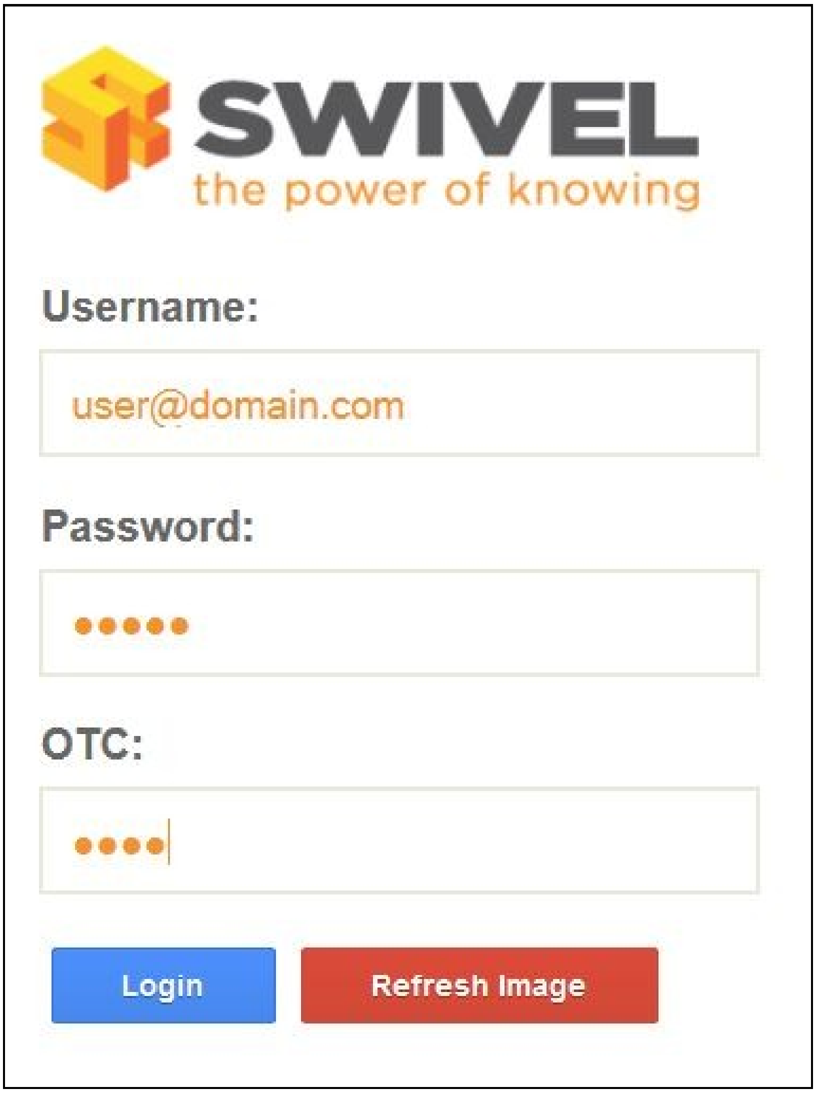
Swivel appliance install: https://swivel_appliance:8443/AuthenticationPortal-huddle/identity_provider.jsp

For a software only install see Software Only Installation

Swivel login page



Dual Channel Authentication

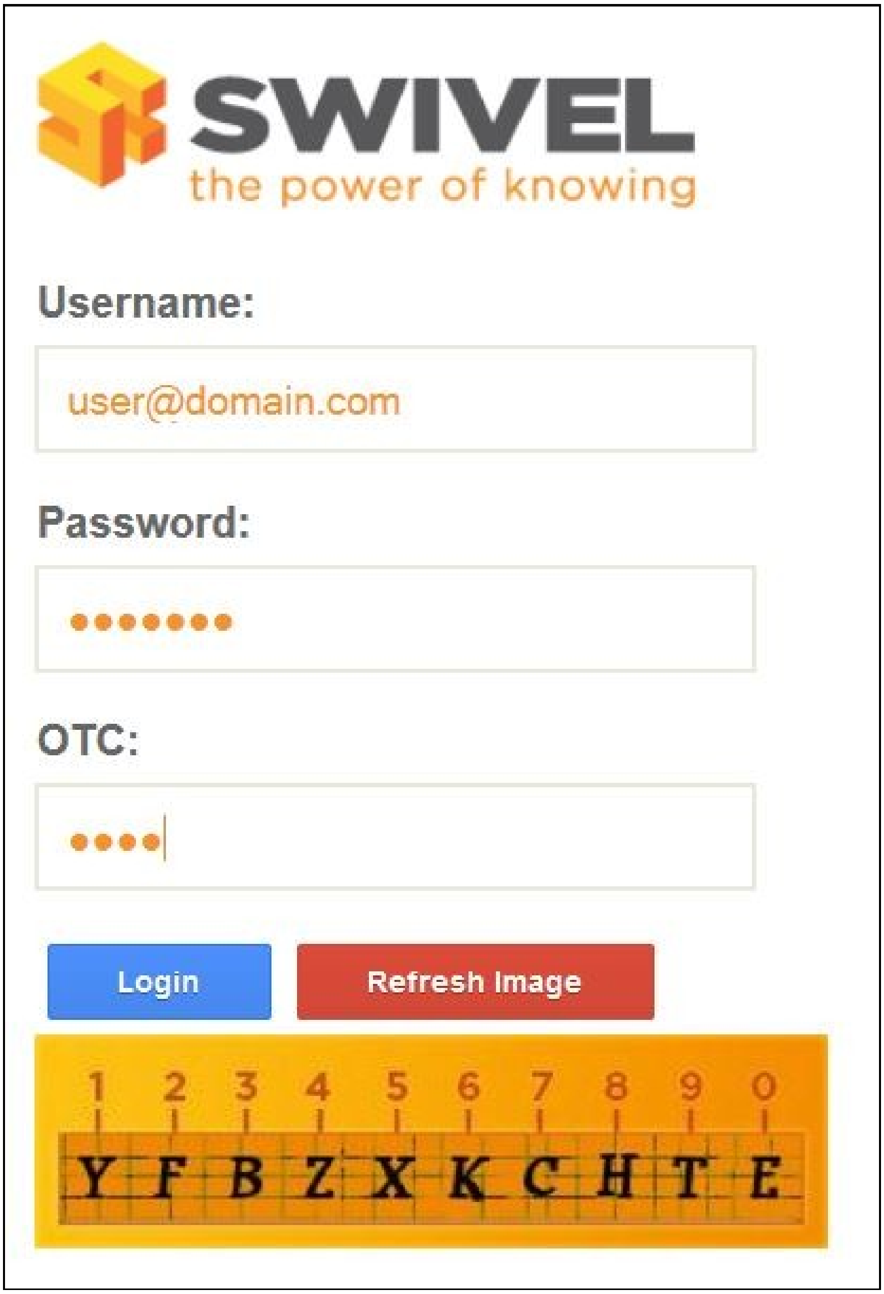


Username:
user@domain.com

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 Oracle WebLogic

35 Overview

This document outlines the integration of Oracle WebLogic with Swivel using SAML with Swivel as an Identity Provider (IdP). It assumes that the Identity Provider and SAMLSwivelDemo app are installed on the same Swivel appliance.

Swivel can provide Two Factor authentication with SMS, Token, Mobile Phone Client and strong Single Channel Authentication TURing, Pinpad or in the Taskbar.

To use the Single Channel Image such as the TURing Image, the Swivel server must be made accessible. **The client requests the images from the Swivel server, and is usually configured using a NAT** (Network Address Translation), often with a proxy server. The Swivel virtual appliance or hardware appliance is configured with a proxy port to allow an additional layer of protection.

36 Prerequisites

Oracle WebLogic

Swivel 3.9 onwards

Swivel AuthenticationPortal.zip. The file containing the IdP and login page to authenticate using Swivel.

Swivel SAMLSwivelDemo.zip. A simple app which sits on the service provider server to demonstrate how a user needs to be authenticated.

37 Baseline

Swivel 3.9, 3.10

Oracle WebLogic 12.1.1

38 Architecture

Swivel is configured as an Identity Provider, see the following Oracle Documentation.

39 Installation

To implement the solution there are several steps:

- Setup up the Identity Provider (IdP) (Authentication Portal)
- Generate the IdP metadata (which is used to create the relationship between the IdP and Service Provider).
- Setup the service provider (the federation service and its association with the Idp)
- Create a user within PINsafe and Weblogic
- Install the demonstration application
- Test the solution

39.1 Swivel Integration Configuration

39.1.1 Configuring Swivel for Agent XML Authentication

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

39.1.2 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

39.1.3 Configuring Swivel for Dual Channel Authentication

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

Transport Configuration

39.2 Configuring the Swivel Authentication Portal

Download and extract the AuthenticationPortal.war file from the AuthenticationPortal.zip and copy this file using WinSCP to /usr/local/tomcat/webapps2 where a a folder called AuthenticationPortal should appear.

Within the AuthenticationPortal folder, there will be folder called WEB-INF, with the settings.xml file (/usr/local/tomcat/webapps2/WEB-INF/settings.xml). Right click settings.xml and either Edit the file or Open in another editor such as Notepad++.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE properties SYSTEM "http://java.sun.com/dtd/properties.dtd">
<properties>
<entry key="pinsafessl">false</entry>
<entry key="pinsafeserver">localhost</entry>
<entry key="pinsafecontext">pinsafe</entry>
<entry key="pinsafesecret">secret</entry>
<entry key="pinsafeport">8080</entry>
<entry key="imagessl">false</entry>
<entry key="imageserver">localhost</entry>
<entry key="imagecontext">pinsafe</entry>
<entry key="imageport">8080</entry>
<entry key="selfsigned">true</entry>
<entry key="serviceProviderEndpointURL">https://login.salesforce.com/?saml=02HKiPoin4nQspKPHoScmudQmsKtM.qRKnViSBCmhO5IC52m5VptCNwO.p</entry
<entry key="audience">https://saml.salesforce.com</entry>
<entry key="certificateIssuer">SAML_SP</entry>
<entry key="publicKeyFilePath">/keys/pinsafe/ssl/dsapubkey.der</entry>
<entry key="privateKeyFilePath">/keys/pinsafe/ssl/dsaprivkey.der</entry>
<entry key="certificateFilePath">/keys/pinsafe/ssl/dsacert.pem</entry>
</properties>
```

pinsafessl Communication between the IdP and Swivel. If SSL is used on the Swivel server set this to true, otherwise false. For a Swivel Hardware or Virtual appliance this should be changed to false when using port 8181 if Swivel is deployed in webapps2.

pinsafeserver Communication between the IdP and Swivel. Where the IdP is installed on the same server as Swivel this should be set to localhost.

pinsafecontext Communication between the IdP and Swivel. This is the install context and is usually pinsafe.

pinsafesecret Communication between the IdP and Swivel. By default a Swivel hardware or virtual appliance uses this value as the shared secret.

pinsafeport Communication port between the IdP and Swivel. For a Swivel Hardware or Virtual appliance this should be changed to 8181 if Swivel is deployed in webapps2 and uses a non SSL connection.

imagessl Communication between the IdP and User. If SSL is used on the Swivel server set this to true, otherwise false.

imageserver Communication between the IdP and User. If SSL is used on the Swivel server set this to true, otherwise false. By default a Swivel hardware or virtual appliance uses SSL.

imagecontext Communication between the IdP and User. This is the install context and is usually pinsafe.

imageport Communication between the IdP and User. For a Swivel Hardware or Virtual appliance this should be changed to 8443 although 443 or other port can also be used.

selfsigned Communication between the IdP and User. If SSL is used on the Swivel server with a self signed certificate then set this to true, otherwise false. By default a Swivel hardware or virtual appliance uses SSL with a self signed certificate.

serviceProviderEndpointURL the Published Site URL, defined in Setting up the Service Provider. Example:https://192.168.10.10/saml2

audience

certificateIssuer SAML_SP

publicKeyFilePath path to the public key usually /keys/pinsafe/ssl/dsapubkey.der

privateKeyFilePath path to the private key usually /keys/pinsafe/ssl/dsaprivkey.der

certificateFilePath path to the certificate usually /keys/pinsafe/ssl/dsacert.pem

39.3 Create private keys and certificates

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

39.3.1 Creating DSA Private Key

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

39.3.2 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

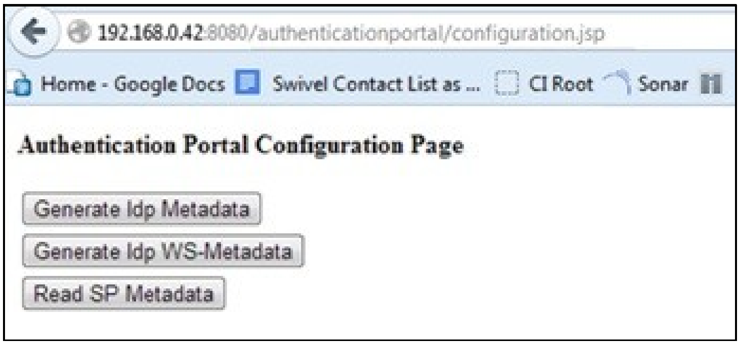
The **dsacert.pem** certificate needs to be uploaded to the GoogleApps server.

39.4 Generating IdP metadata

SAML metadata is generated by the IdP to simplify the mapping process between itself and the Service Provider.

The AuthenticationPortal folder should be located under /usr/local/tomcat/webapps2. In order to gain access to the Authentication Portal webpage, you must navigate to https://<IPAddress>:8443/AuthenticationPortal/configuration.jsp. (case sensitive).

This will display the configuration page as shown below. From here you should press ?Generate Idp Metadata?.


192.168.0.42:8080/authenticationportal/configuration.jsp
Home - Google Docs
Swivel Contact List as ...
CI Root
Sonar

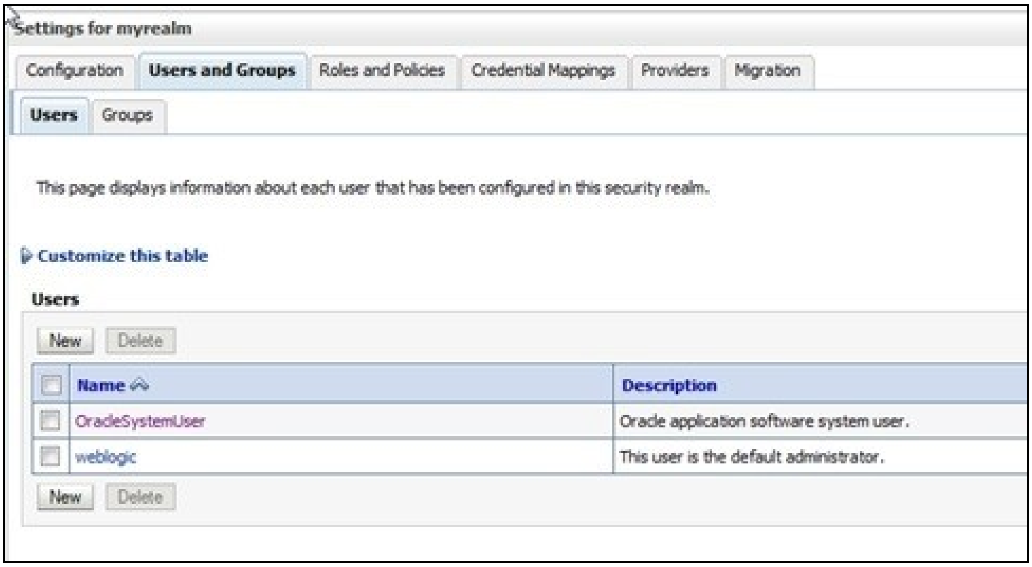
Authentication Portal Configuration Page

If successful, he metadata will be written to the root of the web application with the message "Metadata successfully written to" and the full path and filename displayed. Make a note of the destination which will be used later when configuring the Service Provider.

39.5 WebLogic Integration Configuration

39.5.1 Configure a WebLogic User

On the WebLogic Administration console main menu select Security Realms, select myrealm then select Users and Groups and then the Users tab to show following main screen:

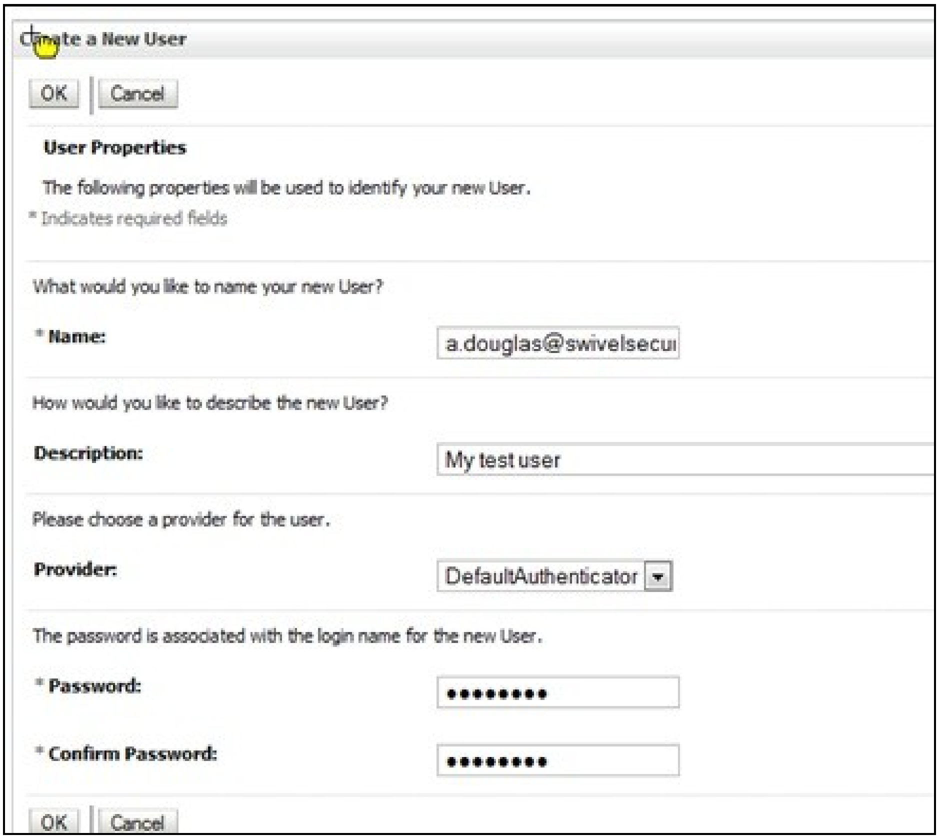

Settings for myrealm

This page displays information about each user that has been configured in this security realm.

Users

☐	Name	Description
☐	OracleSystemUser	Oracle application software system user.
☐	weblogic	This user is the default administrator.

Select New then input a username, this should match to the e-mail address of a Swivel user test user. Enter a dummy password as this will not be used by this integration, then press OK to save.



Create a New User

User Properties

The following properties will be used to identify your new User.

* Indicates required fields

What would you like to name your new User?

* Name: a.douglas@swivelsecui

How would you like to describe the new User?

Description: My test user

Please choose a provider for the user.

Provider: DefaultAuthenticator

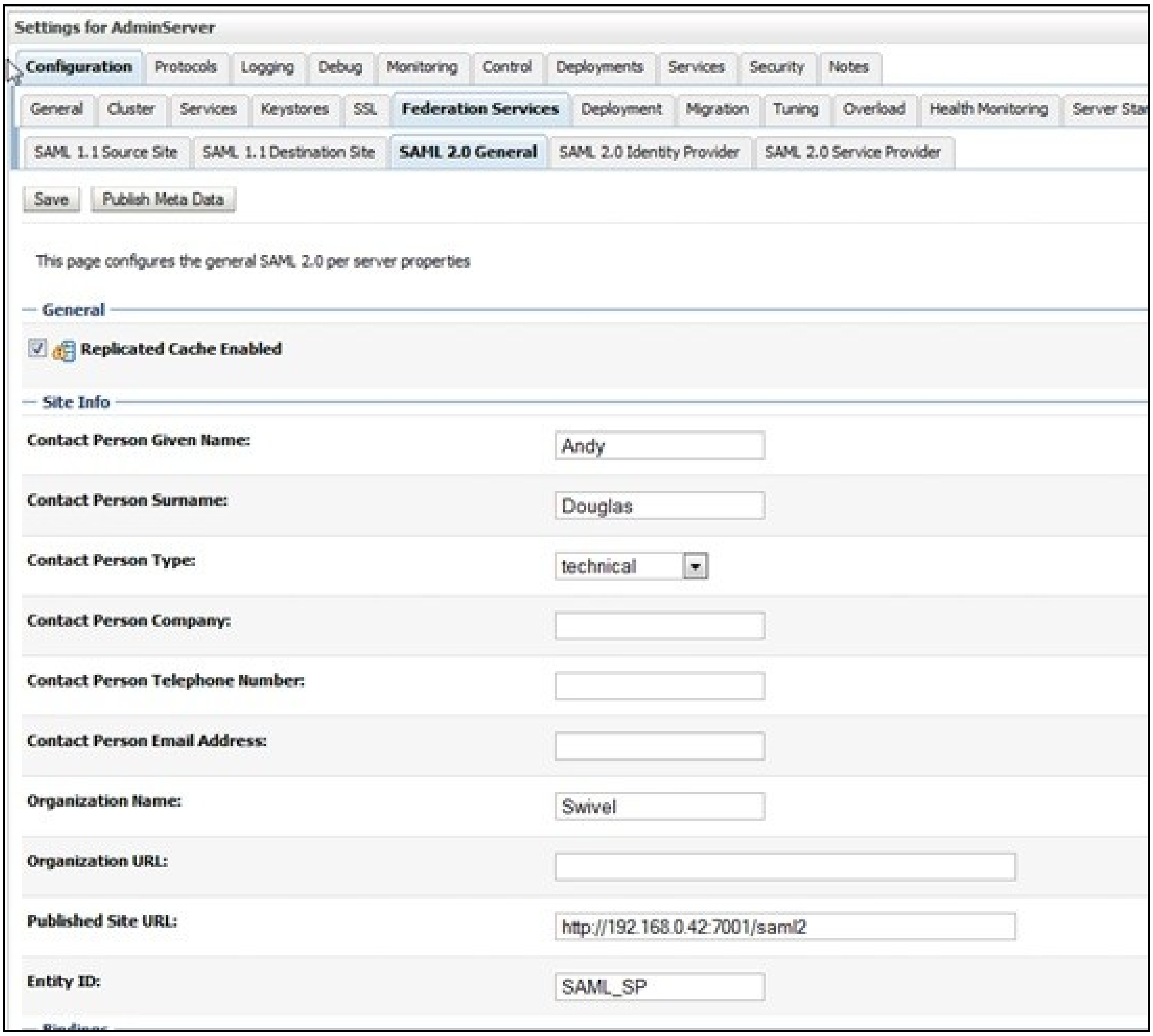
The password is associated with the login name for the new User.

* Password: ••••••••

* Confirm Password: ••••••••

39.5.2 Setting up the Service Provider

On the WebLogic Administration console main menu select Environment, Servers then select AdminServer(admin). Then select Configuration, Federation Services and SAML 2.0 General to get the following screen:



This page configures the general SAML 2.0 per server properties

General

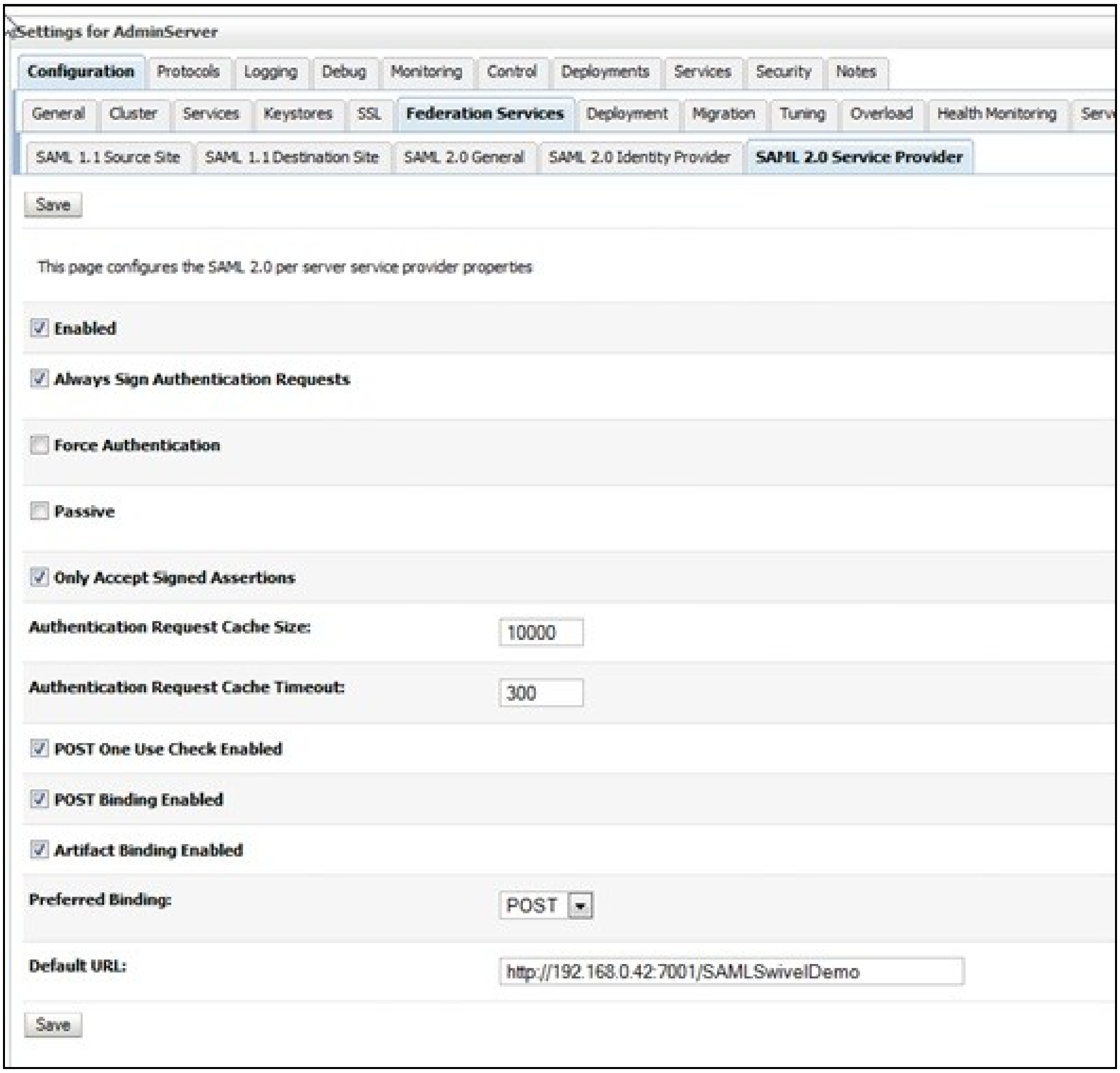
☑ Replicated Cache Enabled

Site Info

Contact Person Given Name:	Andy
Contact Person Surname:	Douglas
Contact Person Type:	technical
Contact Person Company:	
Contact Person Telephone Number:	
Contact Person Email Address:	
Organization Name:	Swivel
Organization URL:	
Published Site URL:	http://192.168.0.42:7001/saml2
Entity ID:	SAML_SP

Published Site URL should be your WebLogic URL + /saml2 and the Entity ID should be SAML_SP to match up other aspects of the configuration. Ensure that under the Bindings option, Recipient Check Enabled is not checked and is therefore disabled. Enter other details as appropriate then press Save.

Then, from the same screen, select SAML 2.0 Service Provider to get the following screen:



Settings for AdminServer

This page configures the SAML 2.0 per server service provider properties

☑ Enabled

☑ Always Sign Authentication Requests

☐ Force Authentication

☐ Passive

☑ Only Accept Signed Assertions

Authentication Request Cache Size: 10000

Authentication Request Cache Timeout: 300

☑ POST One Use Check Enabled

☑ POST Binding Enabled

☑ Artifact Binding Enabled

Preferred Binding: POST

Default URL: http://192.168.0.42:7001/SAMLSwivelDemo

Ensure the checkboxes are set as above and for the Default URL enter the path to the SAMLSwivelDemo. Press Save. Making sure that the Published Site URL is your WebLogic URL and by adding /saml2. E.g. http://192.168.10.10/saml2 - This is your serviceProviderEndpointURL.

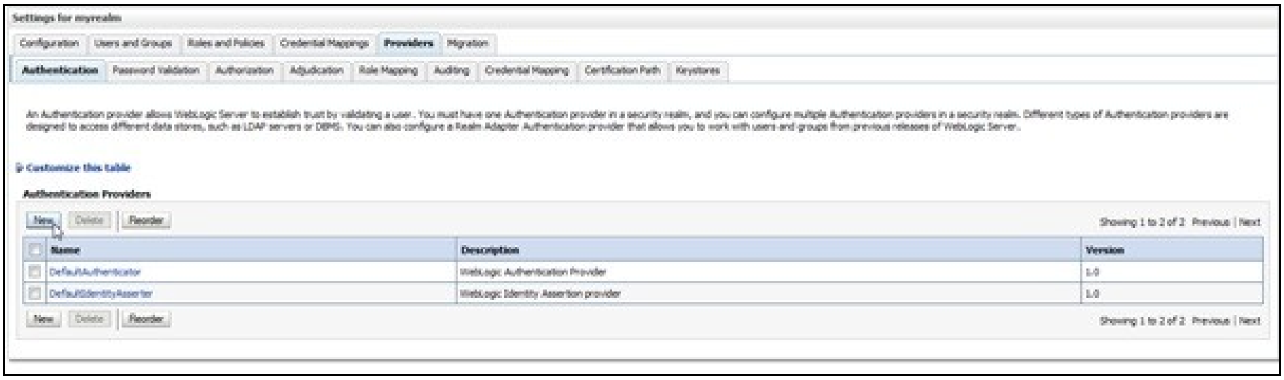
Going back to the section Setting up the IdP, you can go back to the settings.xml and add for example:

```
<entry key="serviceProviderEndpointURL">https://192.168.10.10/saml2</entry>
```

?

39.5.3 Specifying the IdP

On the WebLogic Administration console main menu select Security Realms, select myrealm then select Providers and Authentication to show following main screen:



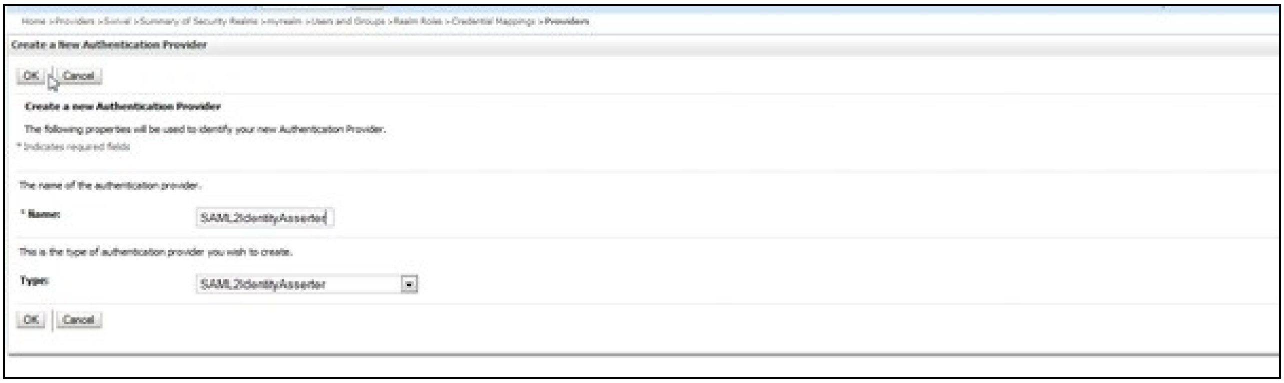
Settings for myrealm

An Authentication provider allows WebLogic Server to establish trust by validating a user. You must have one Authentication provider in a security realm, and you can configure multiple Authentication providers in a security realm. Different types of Authentication providers are designed to access different data stores, such as LDAP servers or DBMS. You can also configure a Realm Adapter Authentication provider that allows you to work with users and groups from previous releases of WebLogic Server.

Authentication Providers

☐	Name	Description	Version
☐	DefaultAuthenticator	WebLogic Authentication Provider	1.0
☐	DefaultIdentityAsserter	WebLogic Identity Assertion provider	1.0

Select New to create a SAML2IdentityAsserter and name it SAML2IdentityAsserter as shown here:



Home >Providers >Sunval >Summary of Security Realms >myrealm >Users and Groups >Realm Roles >Credential Mappings >**Providers**

Create a New Authentication Provider

Create a new Authentication Provider

The following properties will be used to identify your new Authentication Provider.
* Indicates required fields

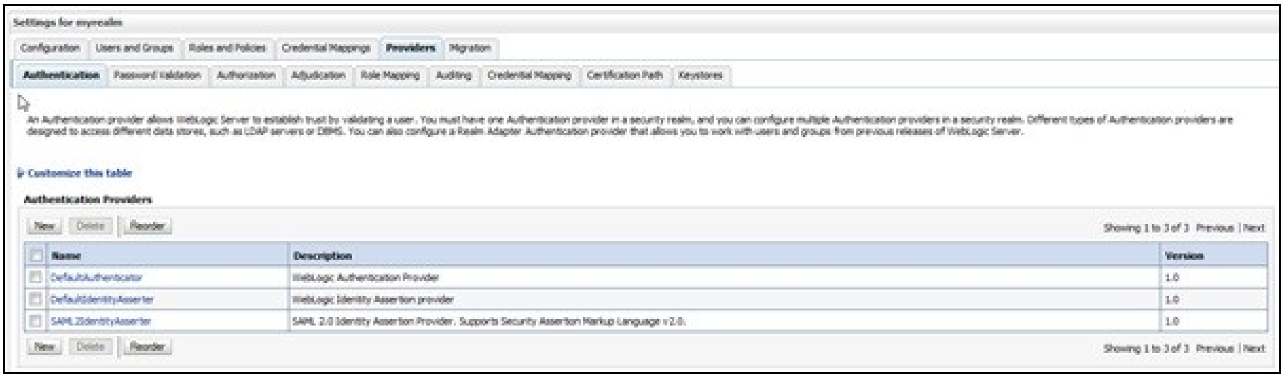
The name of the authentication provider.

*** Name:** SAML2IdentityAsserter

This is the type of authentication provider you wish to create.

Type: SAML2IdentityAsserter

Pressing OK will take you to the following screen.



Settings for myrealm

An Authentication provider allows WebLogic Server to establish trust by validating a user. You must have one Authentication provider in a security realm, and you can configure multiple Authentication providers in a security realm. Different types of Authentication providers are designed to access different data stores, such as LDAP servers or DBMS. You can also configure a Realm Adapter Authentication provider that allows you to work with users and groups from previous releases of WebLogic Server.

Authentication Providers

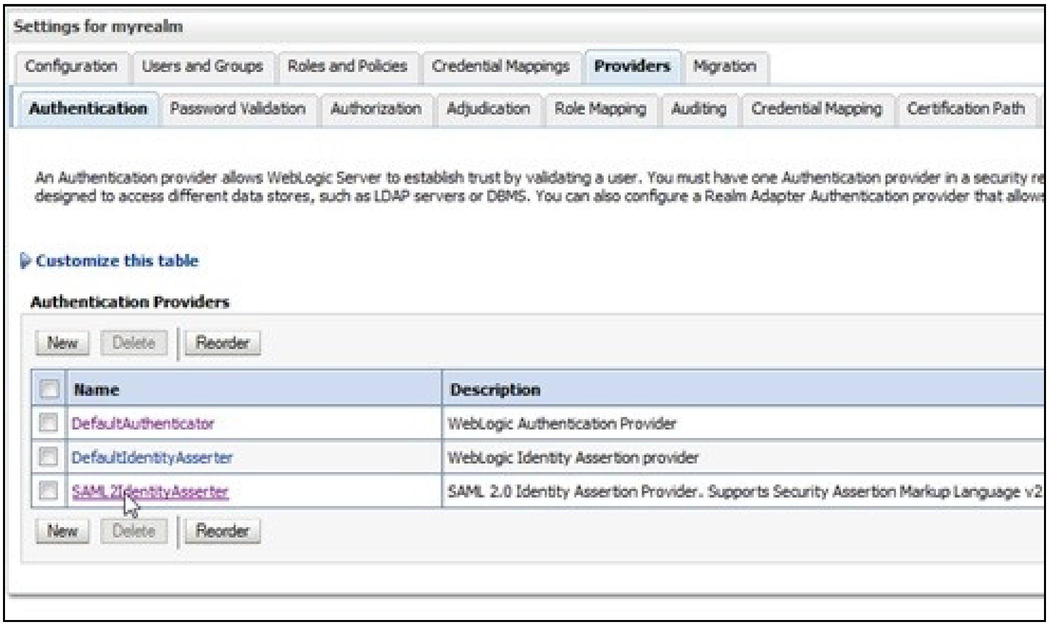
Showing 1 to 3 of 3 Previous | Next

□	Name	Description	Version
□	DefaultAuthenticator	WebLogic Authentication Provider	1.0
□	DefaultIdentityAsserter	WebLogic Identity Assertion provider	1.0
□	SAML2IdentityAsserter	SAML 2.0 Identity Assertion Provider. Supports Security Assertion Markup Language v2.0.	1.0

Showing 1 to 3 of 3 Previous | Next

At this point you need to activate the changes. One way you can do this is from the main menu select Environment, select Servers then select AdminServer(admin). Then select Control. Select the checkbox next to AdminServer(admin) and Shutdown. Then restart the server and logon to the admin console.

Return to the same screen and select the SAML2IdentityAsserter.



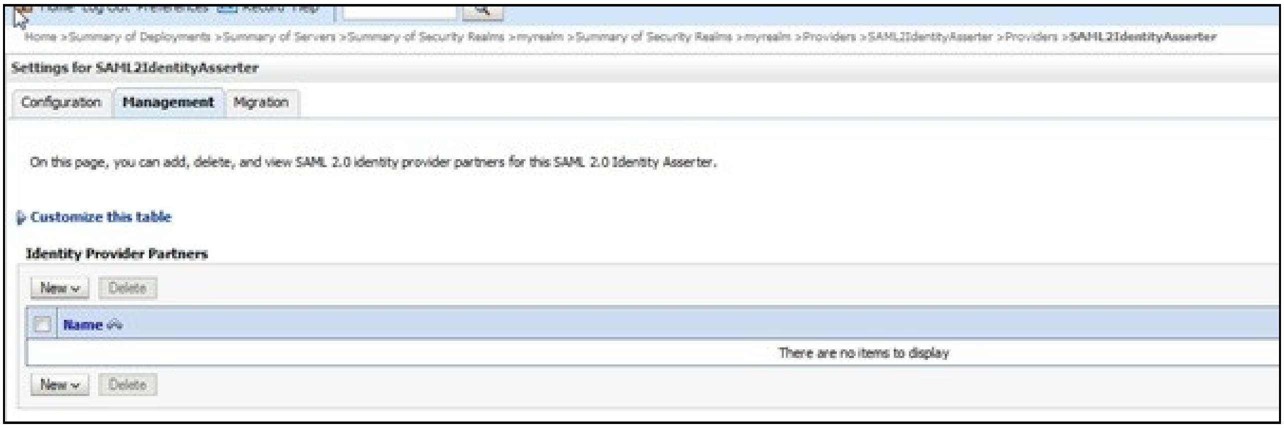
Settings for myrealm

An Authentication provider allows WebLogic Server to establish trust by validating a user. You must have one Authentication provider in a security re
designed to access different data stores, such as LDAP servers or DBMS. You can also configure a Realm Adapter Authentication provider that allows

Authentication Providers

□	Name	Description
□	DefaultAuthenticator	WebLogic Authentication Provider
□	DefaultIdentityAsserter	WebLogic Identity Assertion provider
□	SAML2IdentityAsserter	SAML 2.0 Identity Assertion Provider. Supports Security Assertion Markup Language v2

Then select Management to get the screen below:


Home Log Out Preferences Record Help
Home >Summary of Deployments >Summary of Servers >Summary of Security Realms >myrealm >Summary of Security Realms >myrealm >Providers >SAML2IdentityAsserter >Providers >SAML2IdentityAsserter
Configuration
Management
Migration
Customize this table
New
Delete
Name

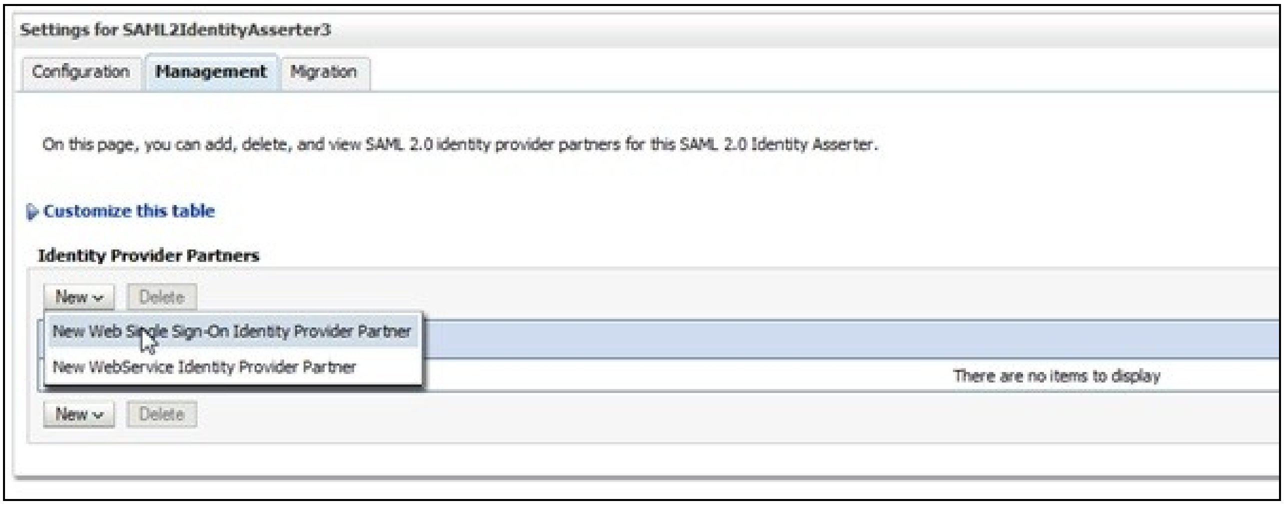
Settings for SAML2IdentityAsserter

On this page, you can add, delete, and view SAML 2.0 identity provider partners for this SAML 2.0 Identity Asserter.

Identity Provider Partners

There are no items to display

Select New and New Web Single Sign-On Identity Provider Partner as shown below:


Configuration
Management
Migration
Customize this table
New
Delete
New Web Single Sign-On Identity Provider Partner
New WebService Identity Provider Partner

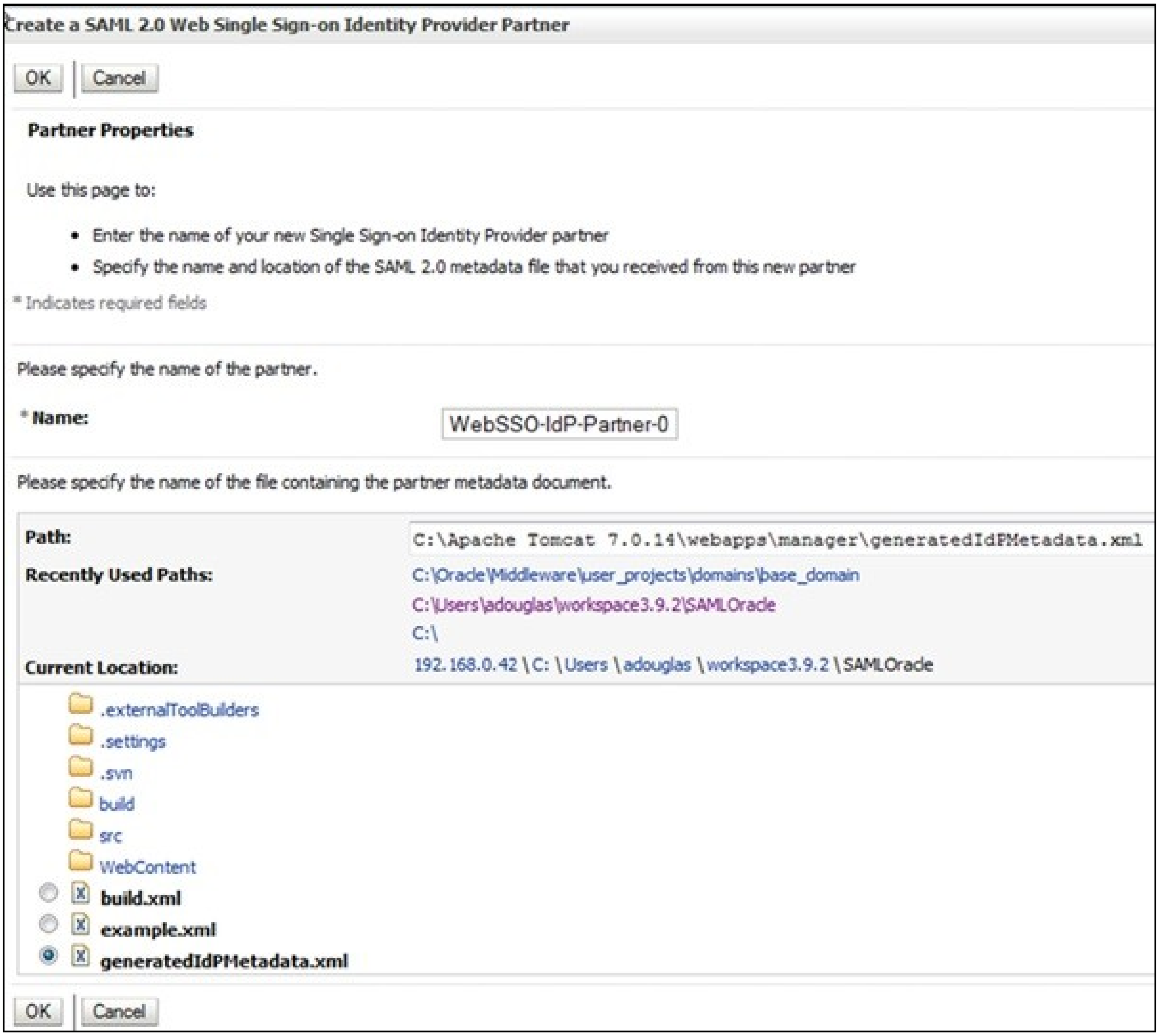
Settings for SAML2IdentityAsserter3

On this page, you can add, delete, and view SAML 2.0 identity provider partners for this SAML 2.0 Identity Asserter.

Identity Provider Partners

There are no items to display

Select New then locate and select the IdP metadata as shown below. Press OK to save



Create a SAML 2.0 Web Single Sign-on Identity Provider Partner

Partner Properties

Use this page to:

- Enter the name of your new Single Sign-on Identity Provider partner
- Specify the name and location of the SAML 2.0 metadata file that you received from this new partner

* Indicates required fields

Please specify the name of the partner.

* Name: WebSSO-IdP-Partner-0

Please specify the name of the file containing the partner metadata document.

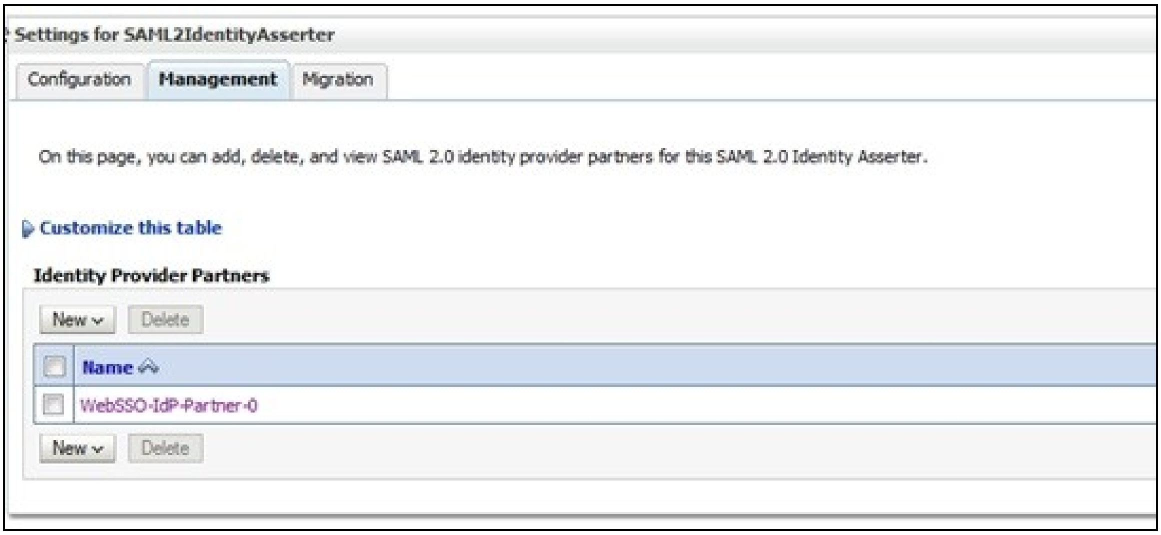
Path: C:\Apache Tomcat 7.0.14\webapps\manager\generatedIdPMetadata.xml

Recently Used Paths: C:\Oracle\Middleware\user_projects\domains\base_domain
C:\Users\adouglas\workspace3.9.2\SAMLOracle
C:\

Current Location: 192.168.0.42 \ C: \ Users \ adouglas \ workspace3.9.2 \ SAMLOracle

.externalToolBuilders
.settings
.svn
build
src
WebContent
○ build.xml
○ example.xml
● generatedIdPMetadata.xml

Thus will take you to the following screen:



Settings for SAML2IdentityAsserter

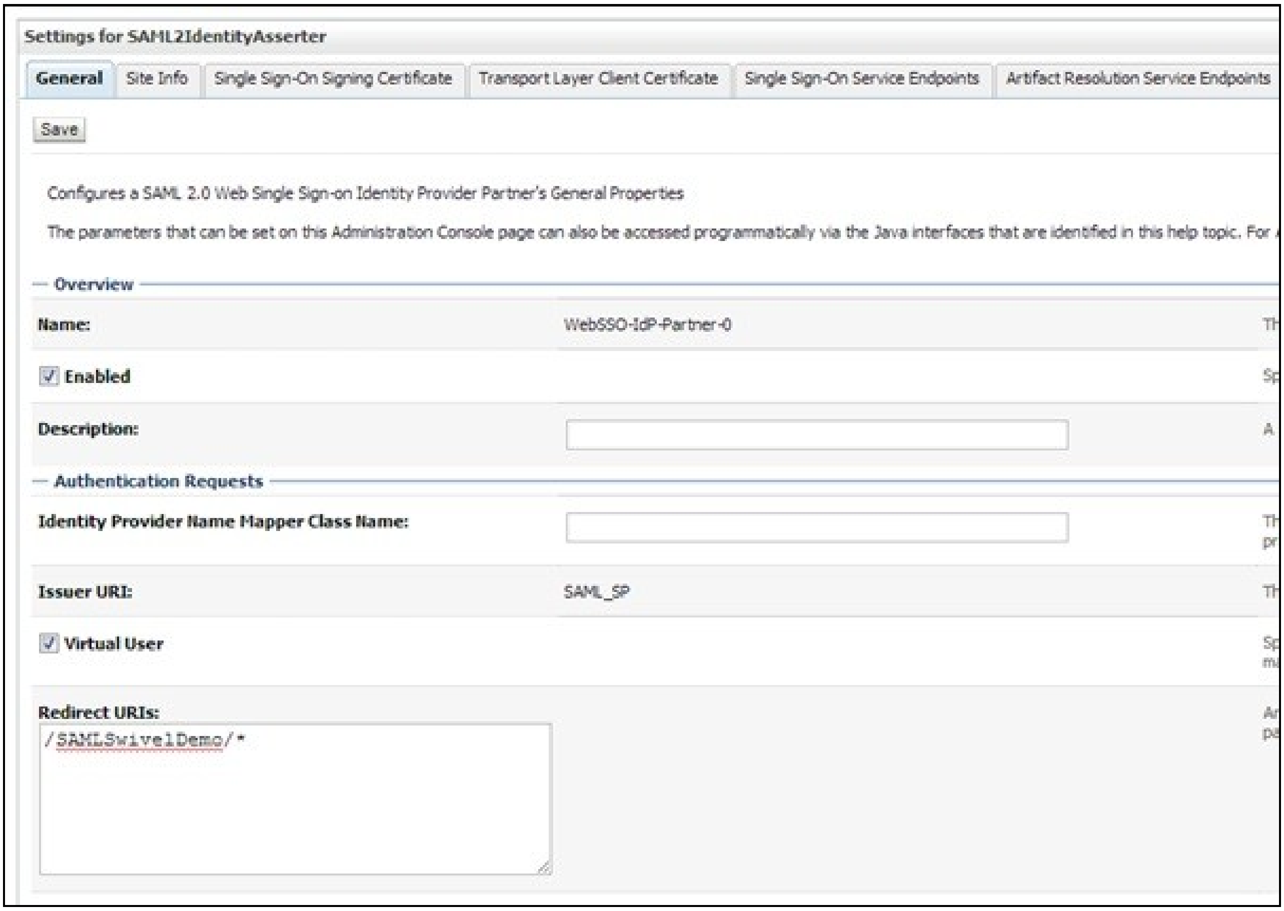
On this page, you can add, delete, and view SAML 2.0 identity provider partners for this SAML 2.0 Identity Asserter.

Customize this table

Identity Provider Partners

☐	Name
☐	WebSSO-IdP-Partner-0

? Select WebSSO-IdP-Partner-0 which will take you to the following screen:


Settings for SAML2IdentityAsserter
General
Site Info
Single Sign-On Signing Certificate
Transport Layer Client Certificate
Single Sign-On Service Endpoints
Artifact Resolution Service Endpoints
Save
Overview
Authentication Requests

Configures a SAML 2.0 Web Single Sign-on Identity Provider Partner's General Properties

The parameters that can be set on this Administration Console page can also be accessed programmatically via the Java interfaces that are identified in this help topic. For

Name: WebSSO-IdP-Partner-0

☑ Enabled

Description:

Identity Provider Name Mapper Class Name:

Issuer URI: SAML_SP

☑ Virtual User

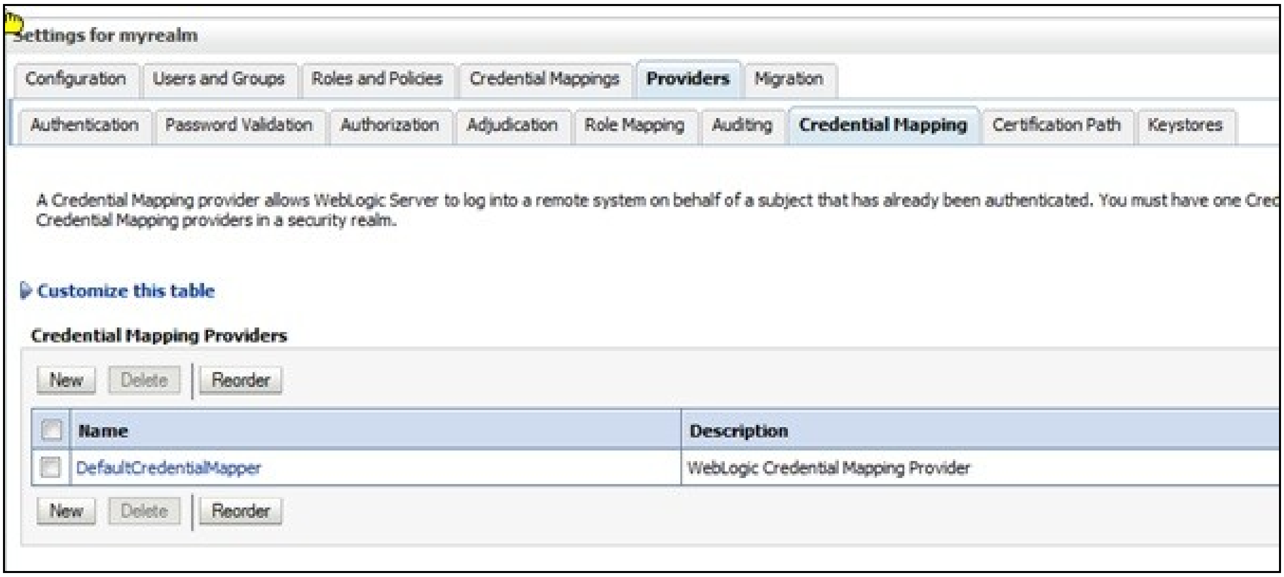
Redirect URIs:

```
/SAMLSwivelDemo/*
```

Ensure Enabled and Virtual User are checked and that Redirect URIs is set to /SAMLSwivelDemo/*. Press Save to save your settings.

39.5.4 Credential Mapping Provider

On the WebLogic Administration console main menu select Security Realms, myrealm then select Providers and Authentication to show following main screen:

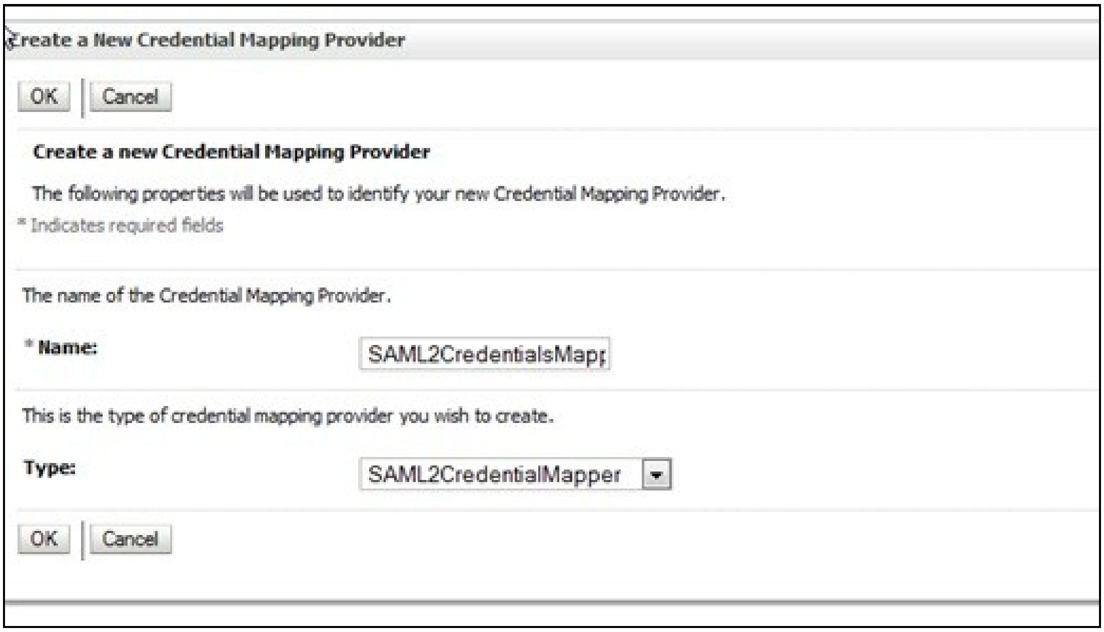


A Credential Mapping provider allows WebLogic Server to log into a remote system on behalf of a subject that has already been authenticated. You must have one Cred Credential Mapping providers in a security realm.

Credential Mapping Providers

□	Name	Description
□	DefaultCredentialMapper	WebLogic Credential Mapping Provider

Select New and then enter a name of SAML2CredentialsMapper and select type of SAML2CredentialsMapper as below (then Press OK to save):



Create a New Credential Mapping Provider

Create a new Credential Mapping Provider

The following properties will be used to identify your new Credential Mapping Provider.

* Indicates required fields

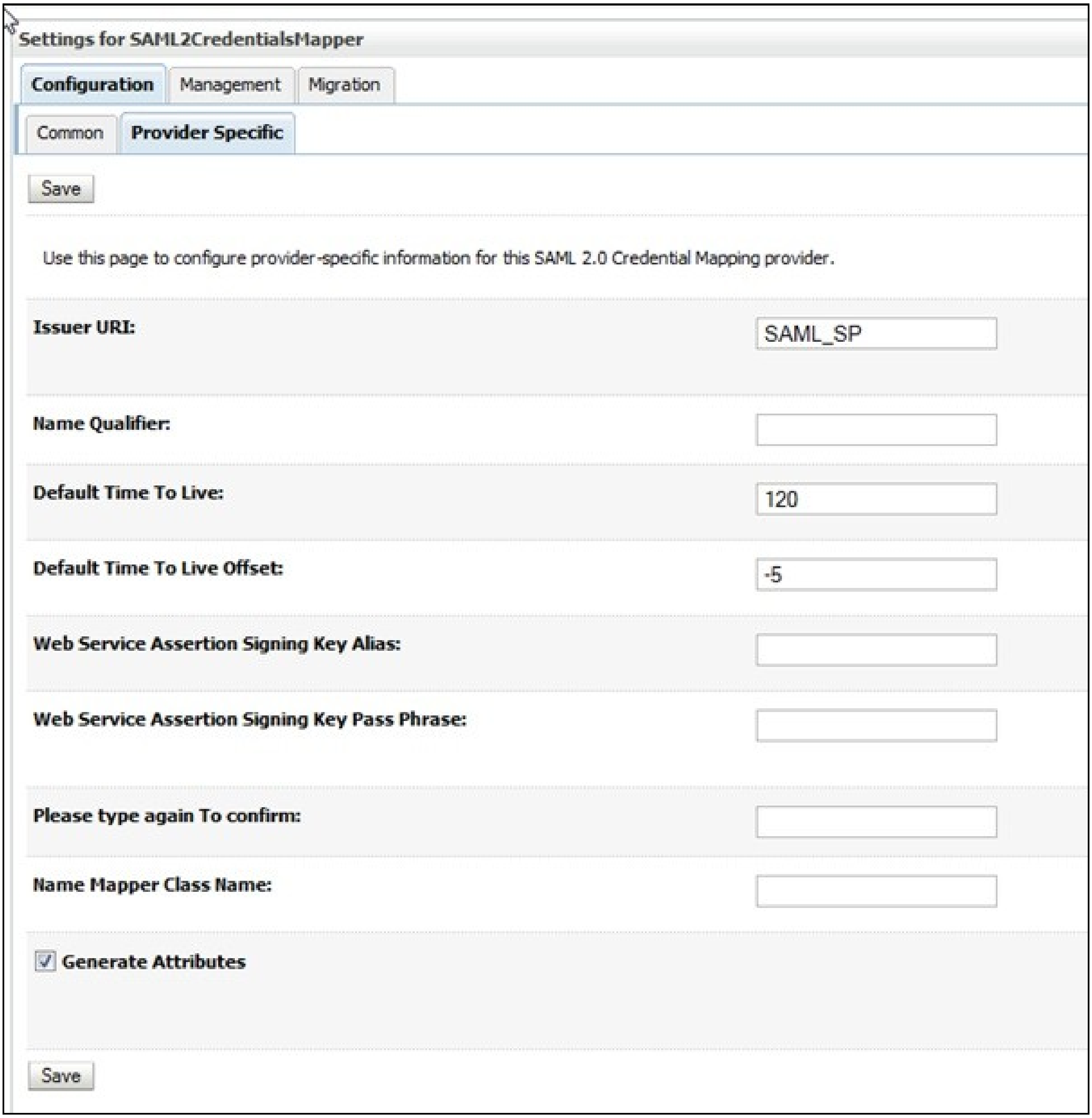
The name of the Credential Mapping Provider.

* Name: SAML2CredentialsMapp

This is the type of credential mapping provider you wish to create.

Type: SAML2CredentialMapper

Select SAML2CredentialsMapper then configuration and Provider Specific. For the Issuer URI enter SAML_SP as shown below (then press Save):


Settings for SAML2CredentialsMapper

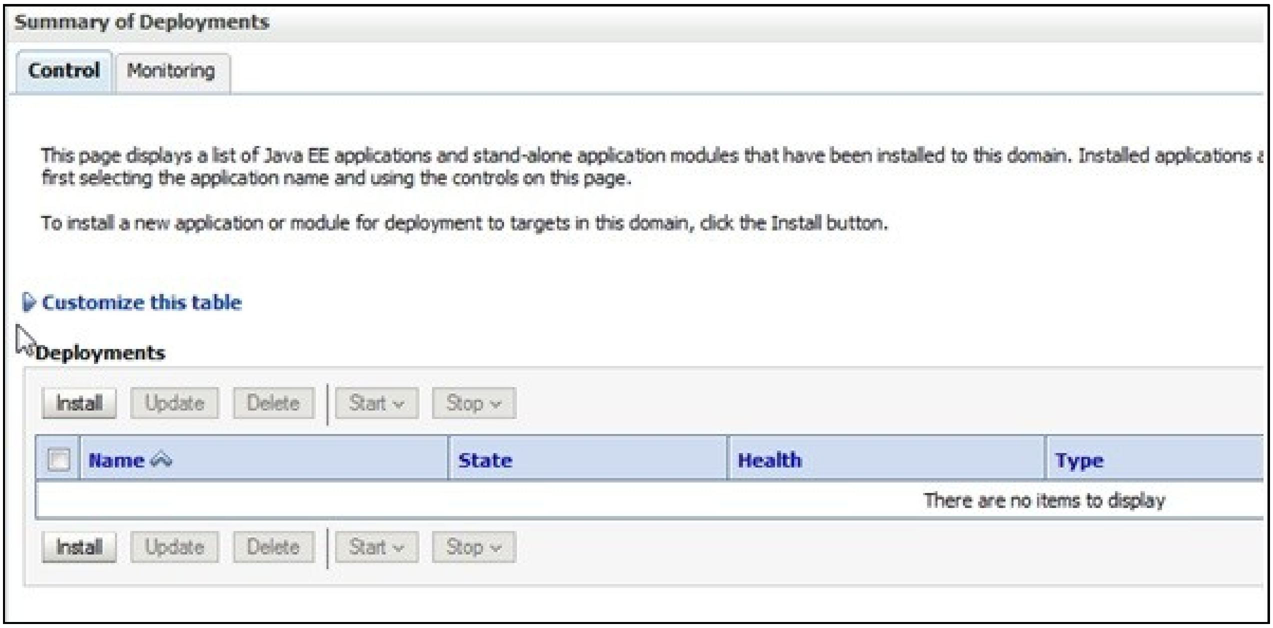
Use this page to configure provider-specific information for this SAML 2.0 Credential Mapping provider.

Issuer URI:	SAML_SP
Name Qualifier:	
Default Time To Live:	120
Default Time To Live Offset:	-5
Web Service Assertion Signing Key Alias:	
Web Service Assertion Signing Key Pass Phrase:	
Please type again To confirm:	
Name Mapper Class Name:	

☑ Generate Attributes

39.5.5 Setting up the demo application

On the WebLogic Administration console main menu select Deployments to get the main screen looking as such:



Summary of Deployments

This page displays a list of Java EE applications and stand-alone application modules that have been installed to this domain. Installed applications a
first selecting the application name and using the controls on this page.

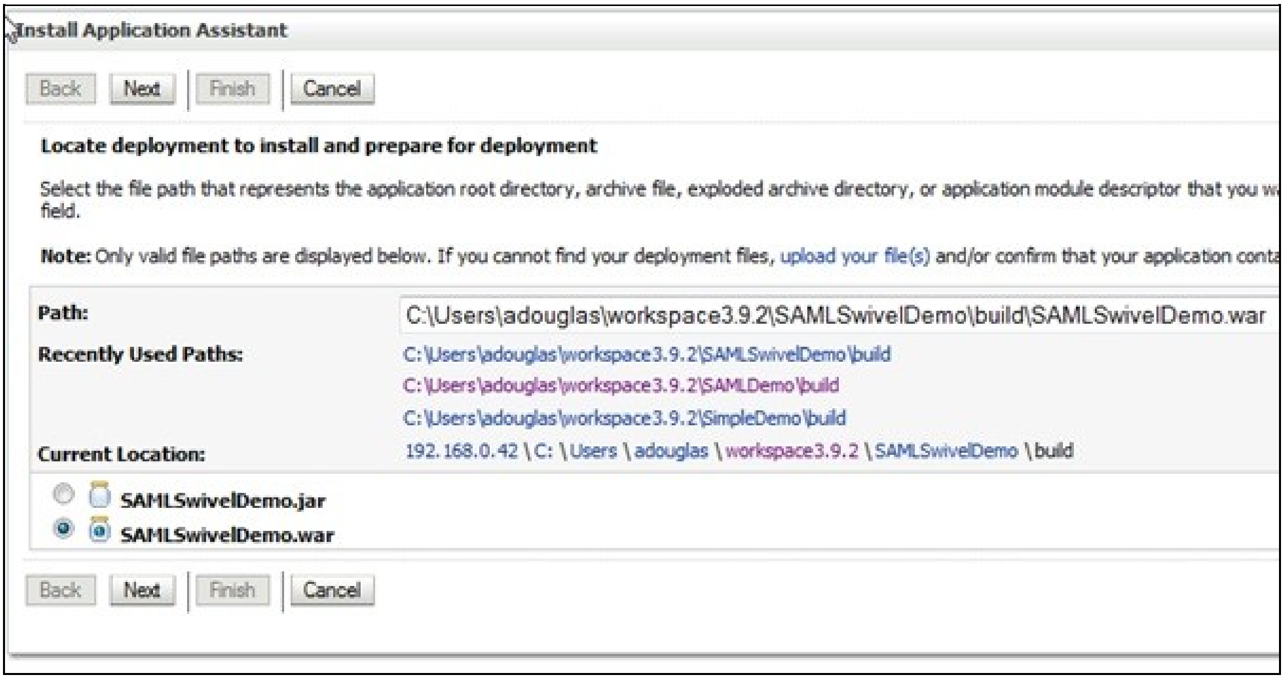
To install a new application or module for deployment to targets in this domain, click the Install button.

Customize this table

Deployments

□	Name	State	Health	Type
			There are no items to display	

Select Install then locate the WAR file for the SAMLSwivelDemo as such:



Install Application Assistant

Locate deployment to install and prepare for deployment

Select the file path that represents the application root directory, archive file, exploded archive directory, or application module descriptor that you w
field.

Note: Only valid file paths are displayed below. If you cannot find your deployment files, upload your file(s) and/or confirm that your application conta

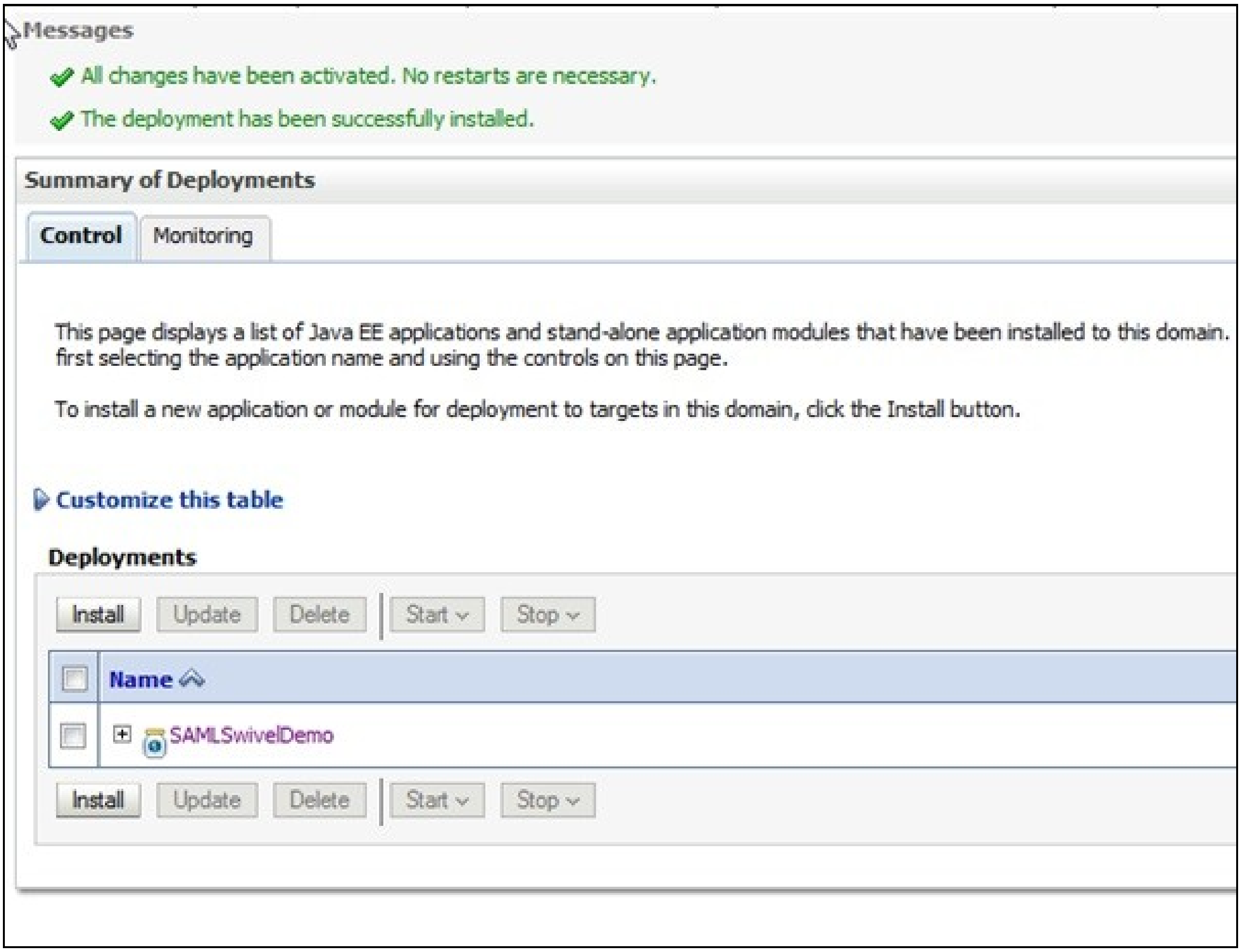
Path: C:\Users\adouglas\workspace3.9.2\SAMLSwivelDemo\build\SAMLSwivelDemo.war

Recently Used Paths: C:\Users\adouglas\workspace3.9.2\SAMLSwivelDemo\build
C:\Users\adouglas\workspace3.9.2\SAMLDemo\build
C:\Users\adouglas\workspace3.9.2\SimpleDemo\build

Current Location: 192.168.0.42 \ C: \ Users \ adouglas \ workspace3.9.2 \ SAMLSwivelDemo \ build

○ SAMLSwivelDemo.jar
● SAMLSwivelDemo.war

? Click Next, Next then Finish (using all the default options) to result in the following Screen:



Messages

✓ All changes have been activated. No restarts are necessary.

✓ The deployment has been successfully installed.

Summary of Deployments

This page displays a list of Java EE applications and stand-alone application modules that have been installed to this domain. first selecting the application name and using the controls on this page.

To install a new application or module for deployment to targets in this domain, click the Install button.

Deployments

□	Name
□	⊞ SAMLSwivelDemo

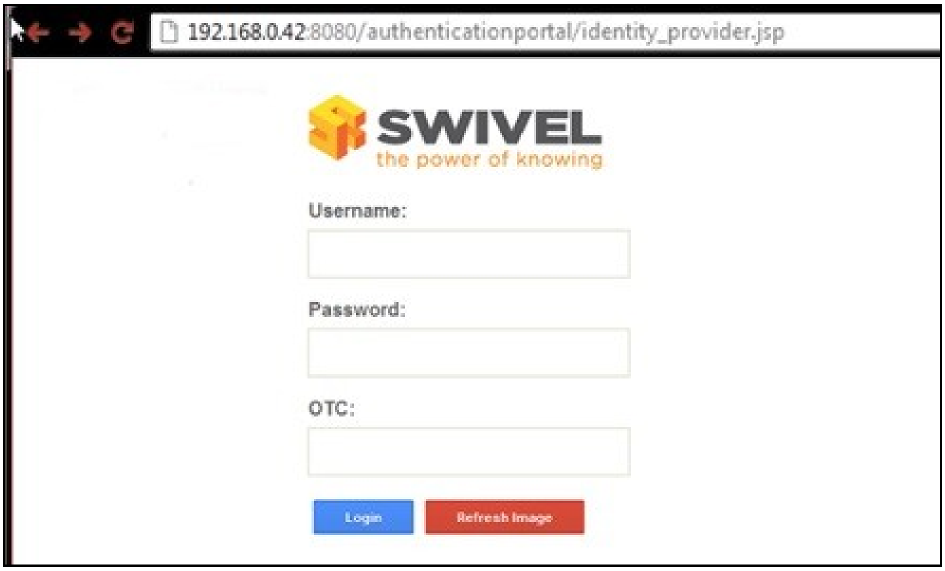
The Demo should now be accessible.

39.6 Additional Installation Options

40 Verifying the Installation

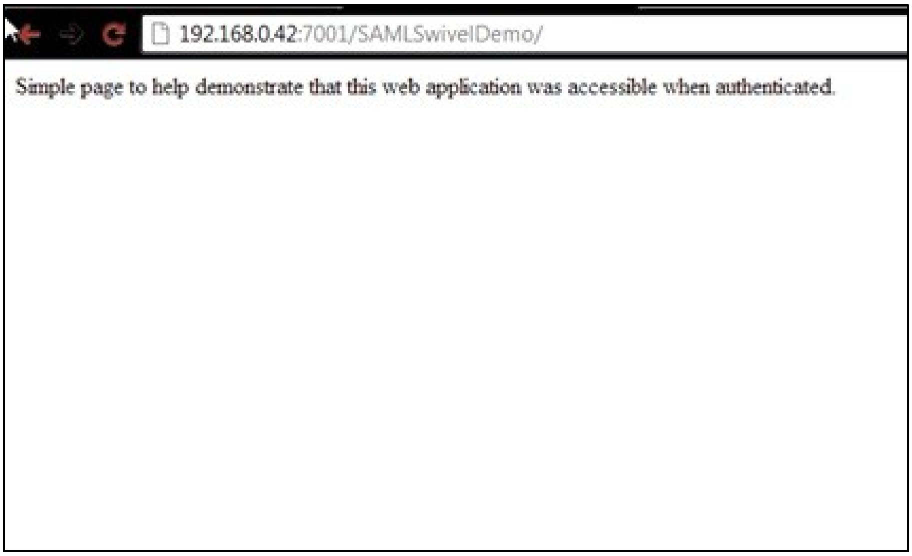
Open a web browser and enter the URL for the root of the demo. In this case: http://weblogicserverURL:7001/SAMLSwivelDemo

This will direct the user to the identity provider?s login page as such:



As per standard logon, enter the username and password (if required), start the session, enter the OTC and press ?Login?

If successful you will be authenticated and redirected to the SAMLDemo page as such:



Simple page to help demonstrate that this web application was accessible when authenticated.

41 Uninstalling the Swivel Integration

42 Troubleshooting

Check the Swivel logs

42.1 Enabling WebLogic debugging

To enable SAML logging On the WebLogic Administration console main menu select AdminServer->Configuration->Debug->Weblogic->Security->SAML2 and enable.

Now you can go to Diagnostics ->Log files ->ServerLog to view what is happening.

42.2 Error Messages

javax.security.auth.login.LoginException: [Security:090377]Identity Assertion Failed, weblogic.security.spi.IdentityAssertionException: [Security:090377]Identity Assertion Failed, weblogic.security.spi.IdentityAssertionException: [Security:096537]Assertion is not yet valid (NotBefore condition). at com.bea.common.security.internal.service.IdentityAssertionServiceImpl.assertIdentity(IdentityAssertionServiceImpl.java:89)

This has been seen where the time on the Swivel server is ahead of the WebLogics server. Ensure they both have the same time.

<BEA-000000> <[Security:096552]Illegal destination: https://<server_name>:<port>/saml2/sp/acs/post of assertion response.>

This is due to the Recipient destination value not matching the local (SP) assertion consumer URL. On the Weblogic Console => Environment => Servers => AdminServer => Configuration => Federation Services => SAM 2.0 General => disable ?Recipient Check Enabled? checkbox.

43 Known Issues and Limitations

44 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.

45 Salesforce.com

46 Introduction

This document covers the integration of Swivel with Salesforce.com.

47 Prerequisites

Salesforce.com Adminisrative Account

Swivel virtual or hardware appliance or server

PINsafe salesforce software Download and unzip the salesforce.war file

The Swivel server needs to be accessible accross the internet for the Salesforce.com server to connect, and the IDP is usually deployed so that it can also be access from the Internet. For security using a Swivel hardware or virtual appliance, the IDP is usually deployed in /webapps2 and accessible on port 8443 (or using a PAT on the appliance using 443)

48 Baseline

Salesforce 11, 12

Swivel 3.8, 3.9

49 Architecture

Salesforce.com users authenticate using SAM-L authentication against Swivel

50 Installation

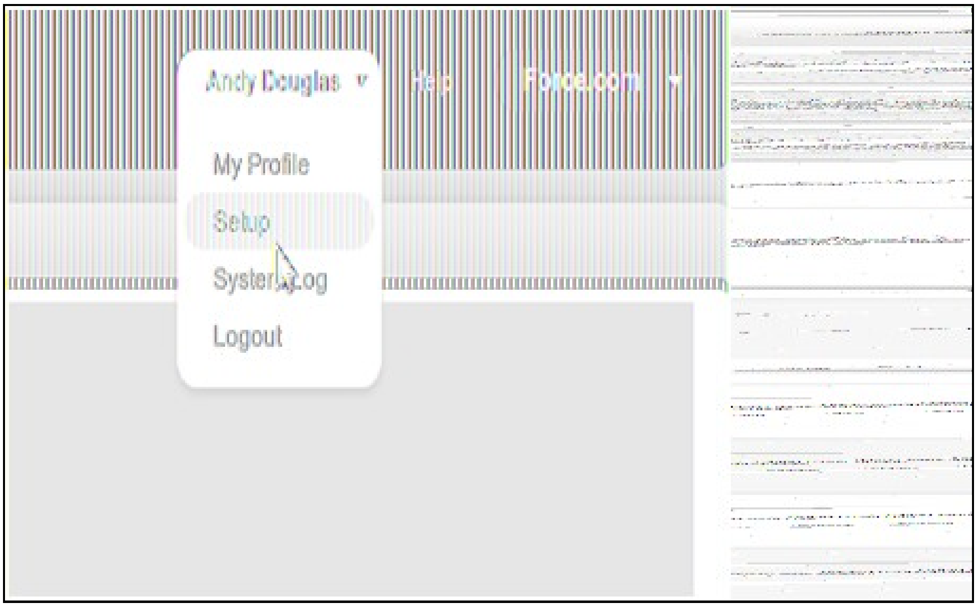
50.1 Salesforce.com Configuration

50.1.1 Allow Authentication

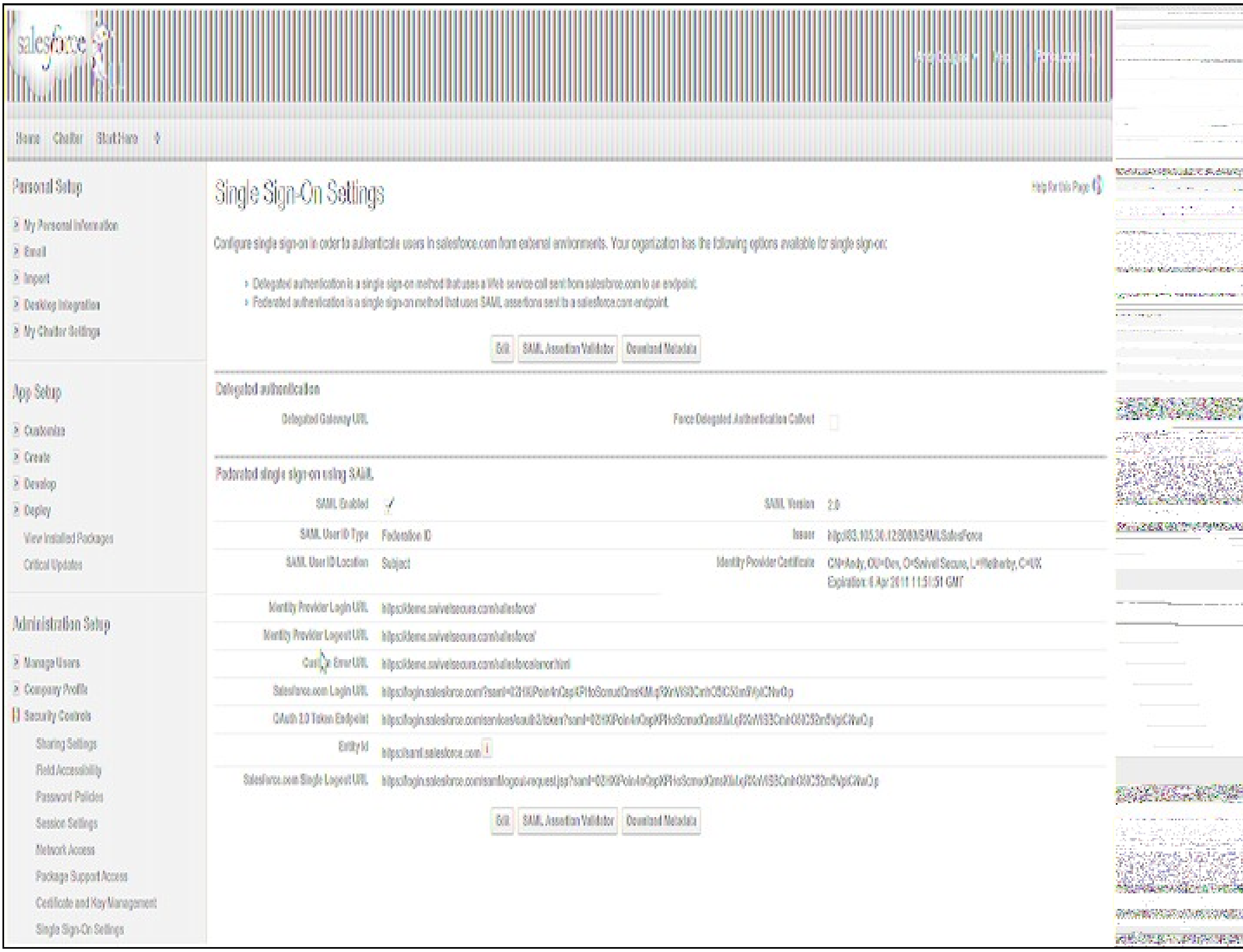
Contact Salesforce.com to enable Federated SSO

50.1.2 Configure Single Sign On

Using an administrative user logon to Salesforce.com and select 'Setup' from the top right button with the the user name on.



Each version of Salesforce is slightly different but each should have a screen similar to the below reached from Setup->Administrative Setup->Security Controls->Single Sign-On Settings



Single Sign-On Settings

Configure single sign-on in order to authenticate users in salesforce.com from external environments. Your organization has the following options available for single sign-on:

- Delegated authentication is a single sign-on method that uses a Web service call sent from salesforce.com to an endpoint.
- Federated authentication is a single sign-on method that uses SAML assertions sent to a salesforce.com endpoint.

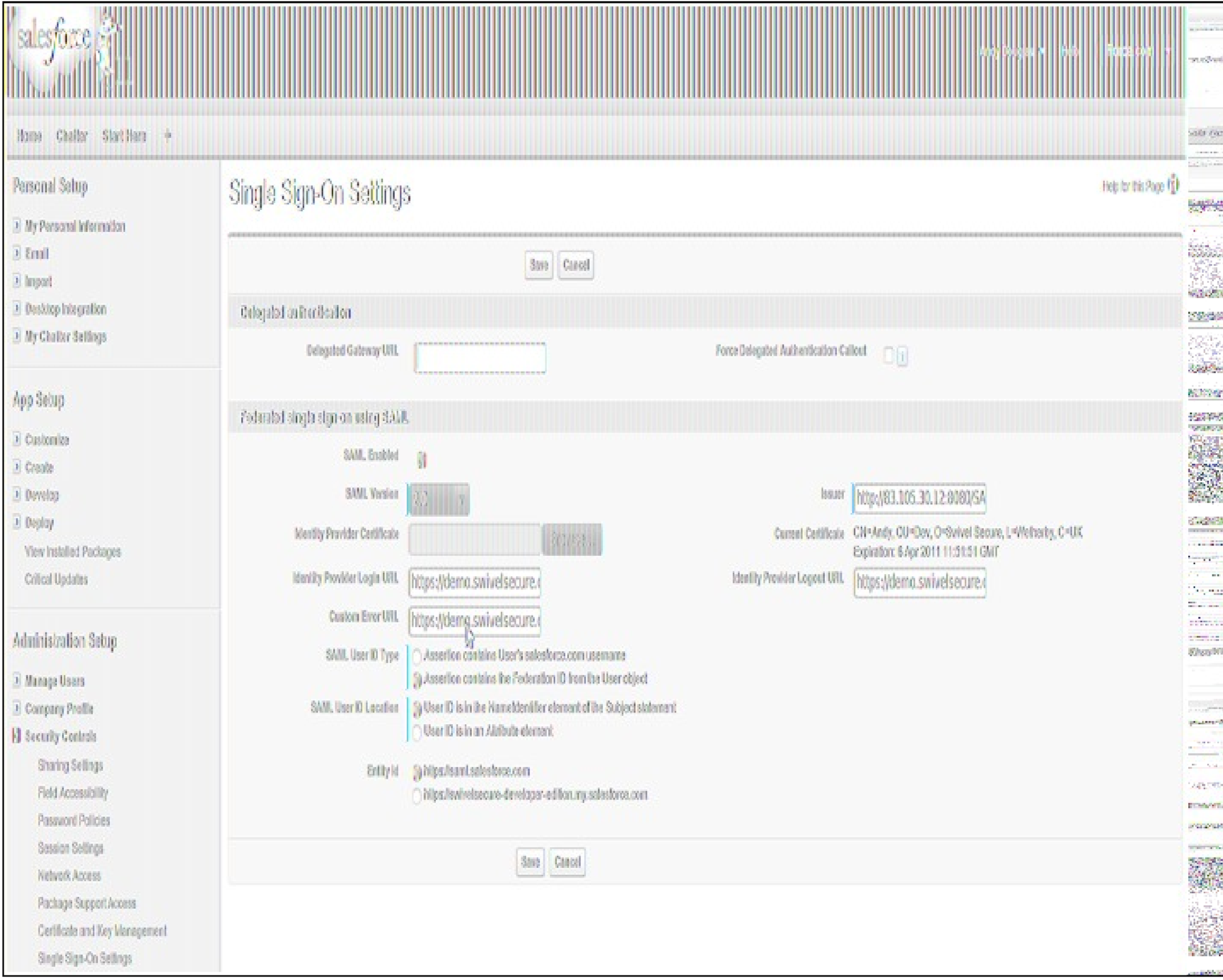
Delegated authentication

Delegated Gateway URL		Force Delegated Authentication Callout	□

Federated single sign-on using SAML

SAML Enabled	✓	SAML Version	2.0
SAML User ID Type	Federation ID	Issuer	http://83.105.36.12:8080/SAMLSalesForce
SAML User ID Location	Subject	Identity Provider Certificate	CN=Andy, OU=Dev, O=Swivel Secure, L=Wetherby, C=UK Expiration: 6 Apr 2011 11:51:51 GMT
Identity Provider Login URL	https://demo.swivelsecure.com/salesforce/		
Identity Provider Logout URL	https://demo.swivelsecure.com/salesforce/		
Custom Error URL	https://demo.swivelsecure.com/salesforce/error.html		
Salesforce.com Login URL	https://login.salesforce.com/?saml=02HKiPoin4nQspKPHoSomudQmsKMuq59rNS3CmhO5C53m5VpiCNwO.p		
OAuth 2.0 Token Endpoint	https://login.salesforce.com/services/oauth2/token?saml=02HKiPoin4nQspKPHoSomudQmsX8uLqf5bVtS3CmhO5C53m5VpiCNwO.p		
Entity Id	https://saml.salesforce.com		
Salesforce.com Single Logout URL	https://login.salesforce.com/saml/logout-request.jsp?saml=02HKiPoin4nQspKPHoSomudQmsX8uLqf5bVtS3CmhO5C53m5VpiCNwO.p		

Click on Edit. At this point you should get something similar to the screen below:



Single Sign-On Settings

Delegated authentication

Delegated Gateway URL:

Force Delegated Authentication Callout: □

Federated single sign-on using SAML

SAML Enabled: ☑

SAML Version: 2.0

Issuer: http://83.105.30.12:8080/SA

Identity Provider Certificate:

Current Certificate: CN=Andy, OU=Dev, O=Swivel Secure, L=Wetherby, C=UK
Expiration: 6 Apr 2011 11:51:51 GMT

Identity Provider Login URL: https://demo.swivelsecure.c

Identity Provider Logout URL: https://demo.swivelsecure.c

Custom Error URL: https://demo.swivelsecure.c

SAML User ID Type:
○ Assertion contains User's salesforce.com username
● Assertion contains the Federation ID from the User object

SAML User ID Location:
● User ID is in the NameIdentifier element of the Subject statement
○ User ID is in an Attribute element

Entity Id:
● https://saml.salesforce.com
○ https://swivelsecure-developer-edition.my.salesforce.com

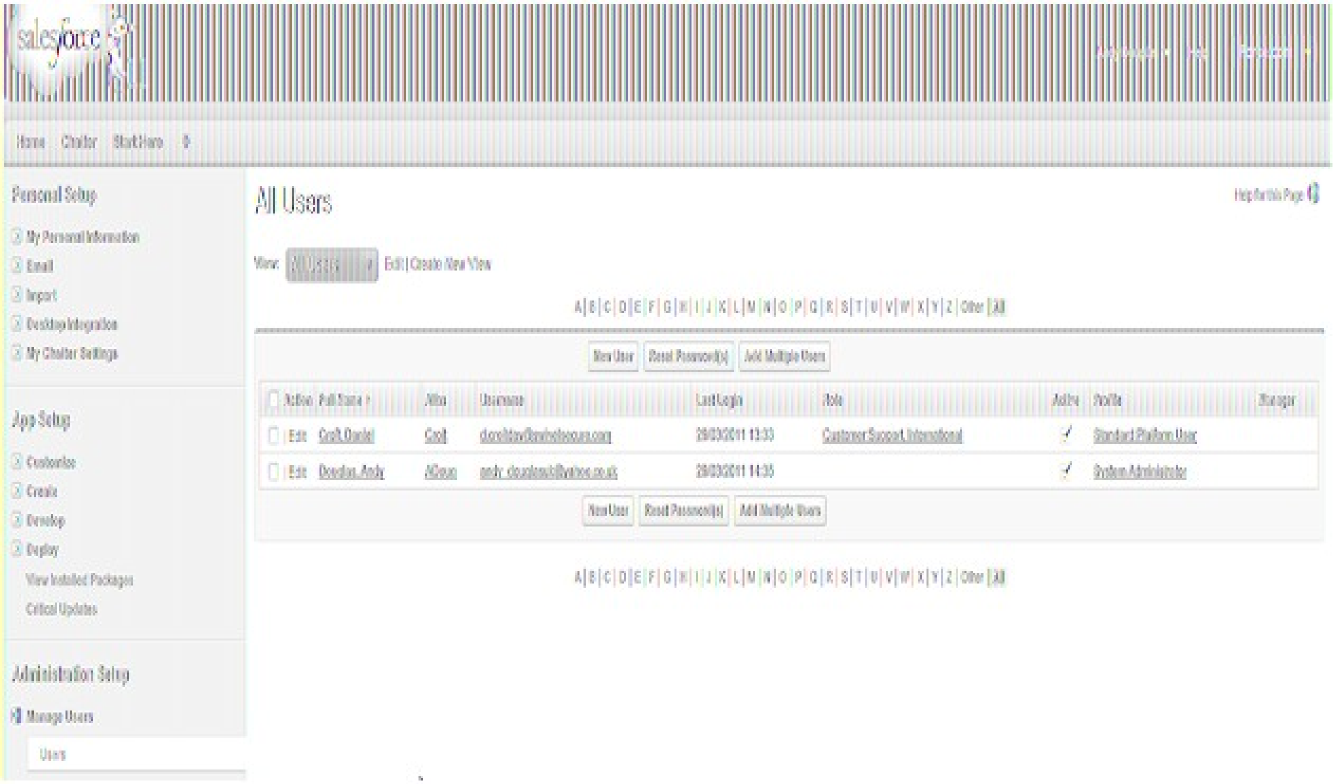
a) upload the certificate and set the issuer

b) set the login URL and logout URL to point to the instance of salesforce-pinsafe you will have running (pointing to the instance is fine as it will re-direct to the logon page automatically)

c) set the remaining settings as above

Entity ID The issuer in SAML requests generated by Salesforce, and is also the expected audience of any inbound SAML Responses. If you don?t have domains deployed, this value is always Entity ID https://saml.salesforce.com. If you have domains deployed, Salesforce recommends that you use your custom domain name.

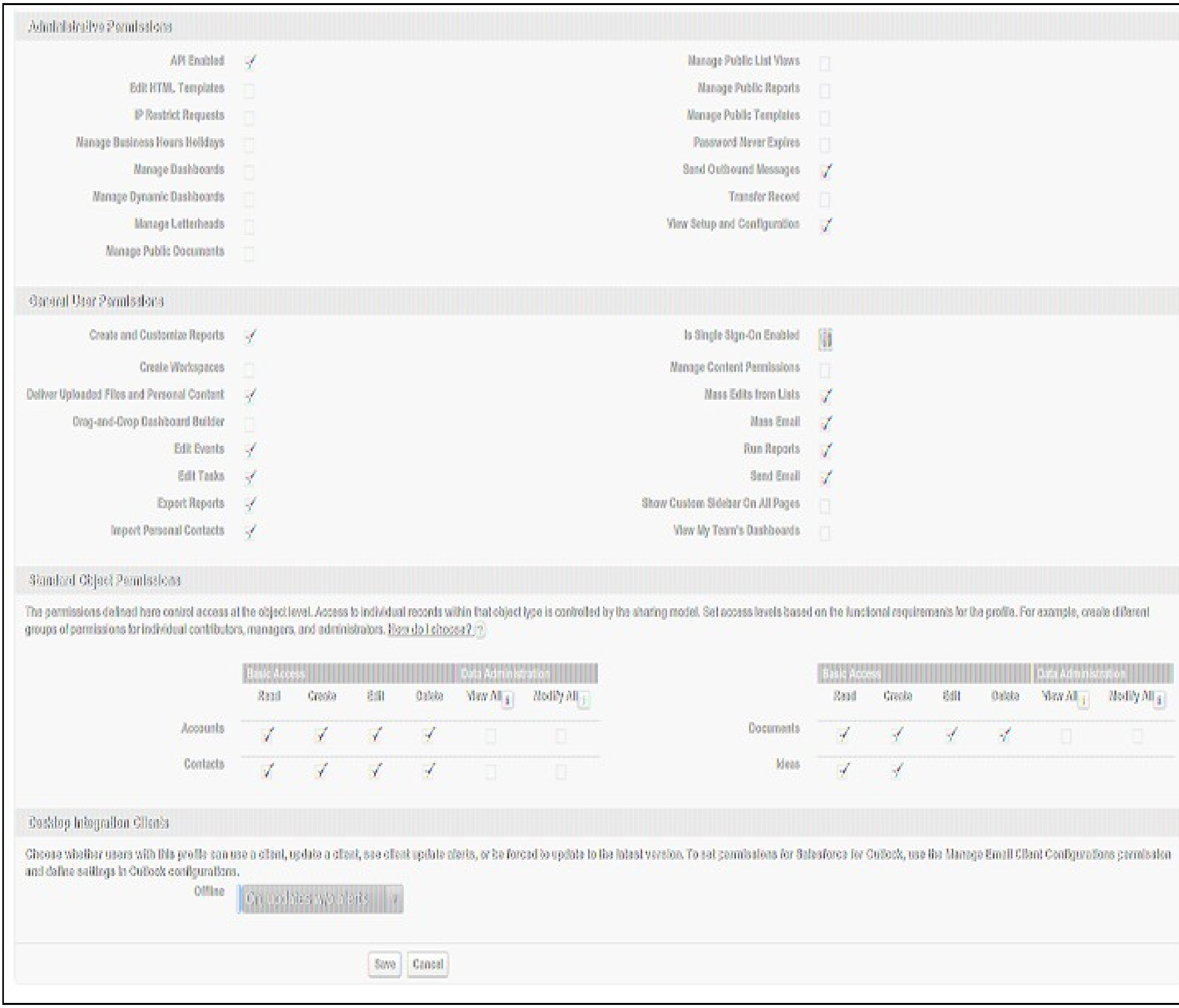
Ensure the users that you wish to use SSO are using a profile that has SSO enabled. Click Manage Users->Users. The profile assigned to each user is on the right hand side.



All Users

□ Action	Full Name ↑	Alias	Username	Last Login	Role	Active	Profile	Manager
□ | Edit	Croft, Daniel	Croft	[illegible]	28/03/2011 13:33	Customer Support, International	✓	Standard Platform User	
□ | Edit	Douglas, Andy	ADoug	andy_douglas@yahoo.co.uk	28/03/2011 14:35		✓	System Administrator	

Click on the profile and find the SSO option as shown below, ensure it is enabled. If it isn't then click edit and enable it.



Administrative Permissions

API Enabled	✓	Manage Public List Views	□
Edit HTML Templates	□	Manage Public Reports	□
IP Restrict Requests	□	Manage Public Templates	□
Manage Business Hours Holidays	□	Password Never Expires	□
Manage Dashboards	□	Send Outbound Messages	✓
Manage Dynamic Dashboards	□	Transfer Record	□
Manage Letterheads	□	View Setup and Configuration	✓
Manage Public Documents	□		

General User Permissions

Create and Customize Reports	✓	Is Single Sign-On Enabled	☑
Create Workspaces	□	Manage Content Permissions	□
Deliver Uploaded Files and Personal Content	✓	Mass Edits from Lists	✓
Drag-and-Drop Dashboard Builder	□	Mass Email	✓
Edit Events	✓	Run Reports	✓
Edit Tasks	✓	Send Email	✓
Export Reports	✓	Show Custom Sidebar On All Pages	□
Import Personal Contacts	✓	View My Team's Dashboards	□

Standard Object Permissions

The permissions defined here control access at the object level. Access to individual records within that object type is controlled by the sharing model. Set access levels based on the functional requirements for the profile. For example, create different groups of permissions for individual contributors, managers, and administrators. How do I choose? ?

	Basic Access				Data Administration	
	Read	Create	Edit	Delete	View All	Modify All
Accounts	✓	✓	✓	✓	□	□
Contacts	✓	✓	✓	✓	□	□

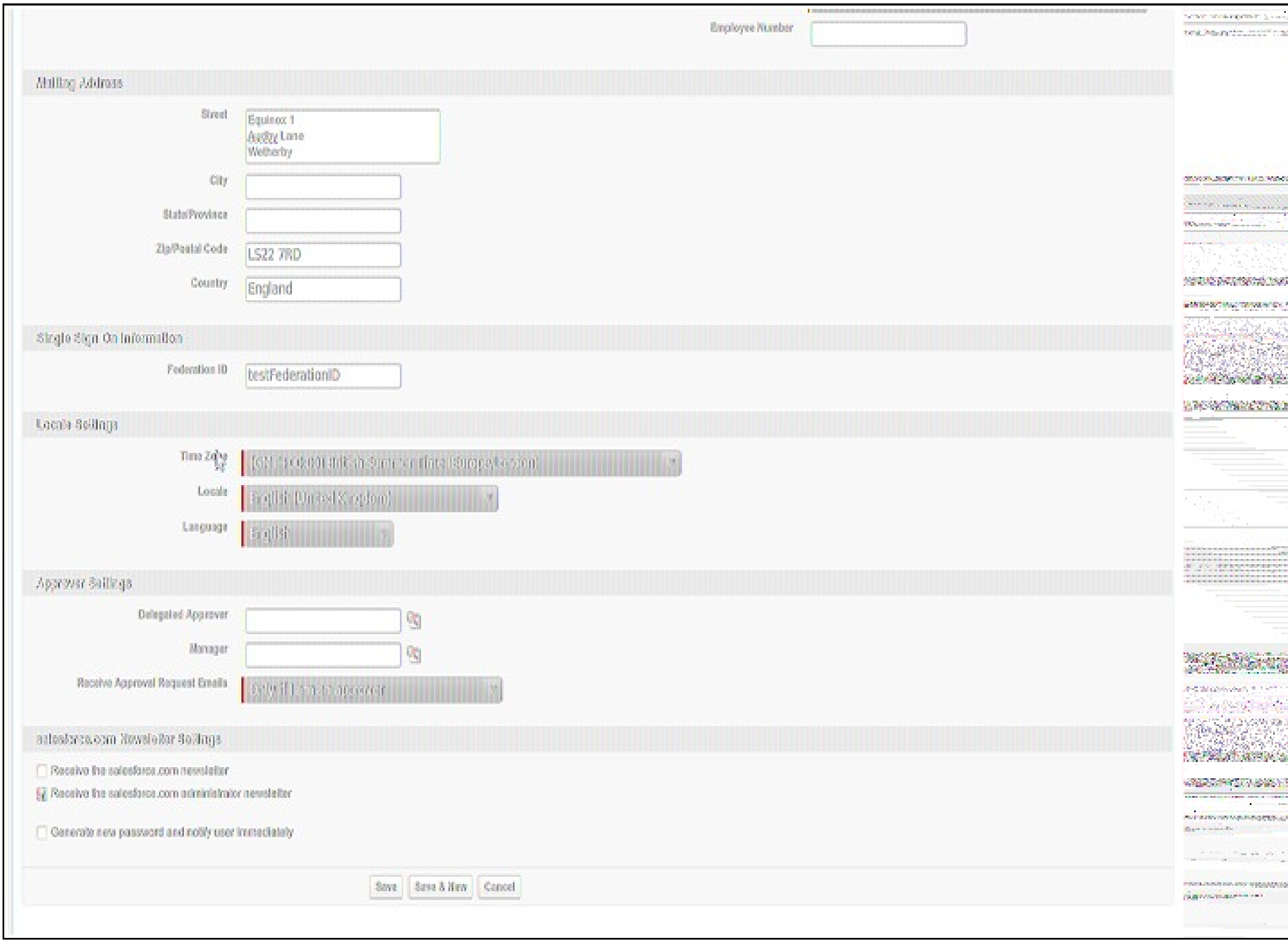
	Basic Access				Data Administration	
	Read	Create	Edit	Delete	View All	Modify All
Documents	✓	✓	✓	✓	□	□
Ideas	✓	✓				

Desktop Integration Clients

Choose whether users with this profile can use a client, update a client, see client update alerts, or be forced to update to the latest version. To set permissions for Salesforce for Outlook, use the Manage Email Client Configurations permission and define settings in Outlook configurations.

Offline: On, updates w/o alerts

Ensure the users have a Federation ID which will map to their Swivel username. Click Manage Users->Users, select a user then enter the Federation ID



Employee Number

Mailing Address

Street: Equinox 1
Audby Lane
Wetherby

City:

State/Province:

Zip/Postal Code: LS22 7RD

Country: England

Single Sign On Information

Federation ID: testFederationID

Locale Settings

Time Zone: (GMT+01:00) British Summer Time (Europe/London)

Locale: English (United Kingdom)

Language: English

Approver Settings

Delegated Approver:

Manager:

Receive Approval Request Emails: Only if I am an approver

salesforce.com Newsletter Settings

□ Receive the salesforce.com newsletter

☑ Receive the salesforce.com administrator newsletter

□ Generate new password and notify user immediately

50.2 Configure The Swivel Server

Configure a Swivel Agent (For standard XML Authentication)

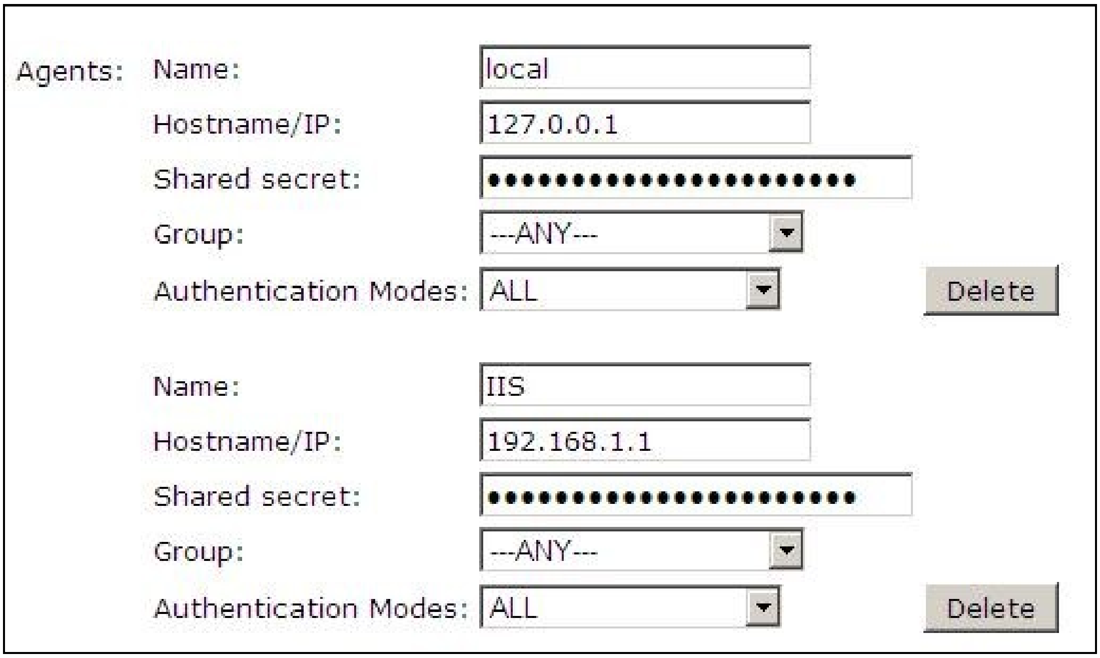
1. On the Swivel Management Console select Server/Agent

2. Enter a name for the Agent

3. Enter the IP address or hostname for the server where the salesforce.war is installed, if installed on the same server as the Swivel server use 127.0.0.1 or localhost, a default entry may already exist for this

4. Enter the shared secret to be used above on the below server configuration.

5. Click on Apply to save changes

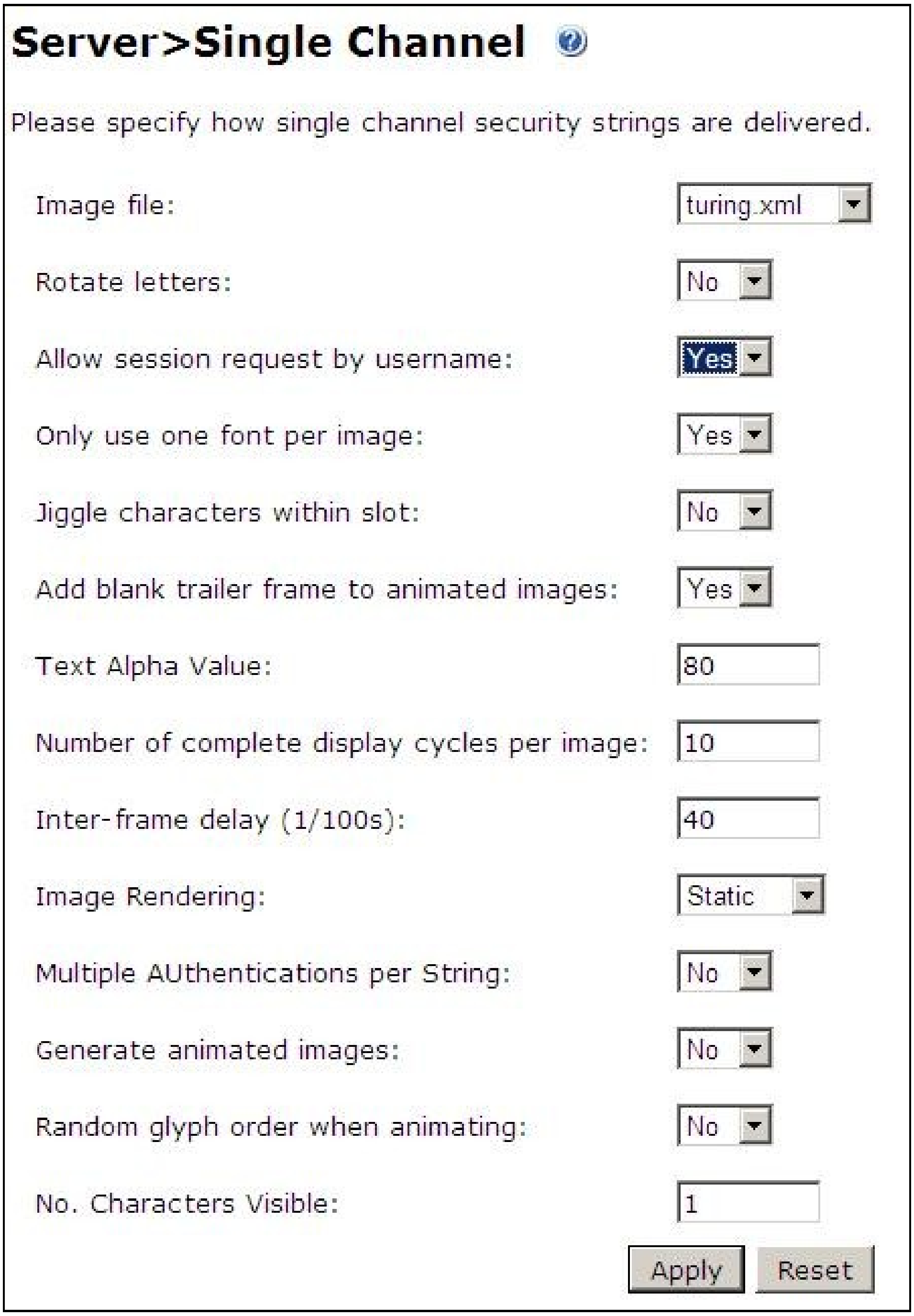


Agents:	Name:	local
	Hostname/IP:	127.0.0.1
	Shared secret:	•••••••••••••••••••••••
	Group:	---ANY---
	Authentication Modes:	ALL
	Name:	IIS
	Hostname/IP:	192.168.1.1
	Shared secret:	•••••••••••••••••••••••
	Group:	---ANY---
	Authentication Modes:	ALL

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

50.3 Access Device or Application Integration

Client Side Installation

1.The SAML-salesforce war (salesforce.war) should be placed near a Swivel installation on a webserver. This could be a Swivel virtual or hardware appliance. On a Swivel virtual or hardware appliance this would need to be copied to the /usr/local/tomcat/webapps2 folder.

2.Inside the saleforce war exists a properties file (WEB-INF->settings.xml). Initially this will look something like:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE properties SYSTEM "http://java.sun.com/dtd/properties.dtd">

<properties>
<entry key="ssl">false</entry>
<entry key="server">localhost</entry>
<entry key="port">8080</entry>
<entry key="context">pinsafe</entry>
<entry key="imagessl">true</entry>
<entry key="imageserver">demo.swivelsecure.com</entry>
<entry key="imagecontext">proxy</entry>
<entry key="imageport">8443</entry>
<entry key="secret">secret</entry>
<entry key="selfsigned">true</entry>
<entry key="salesforceURL">https://login.salesforce.com/?saml=02HKiPoin4nQspKPHoScmudQmsKtM.qRKnViSBCmhO5IC52m5VptCNwO.p</entry>
<entry key="audience">https://saml.salesforce.com</entry>
```

```
<entry key="certificateIssuer">http://83.105.30.12:8080/SAMLSalesForce</entry>
<entry key="publicKeyFilePath">./keys/pinsafe/ssl/dsapubkey.der</entry>
<entry key="privateKeyFilePath">./keys/pinsafe/ssl/dsaprivkey.der</entry>
<entry key="certificate">./keys/pinsafe/ssl/dsacert.pem</entry>
</properties>
```

These settings should be changed to match, additional field values may need to be created as above:

- The settings for the local Swivel server

For a Swivel virtual or hardware appliance the settings may be:

```
<entry key="ssl">false</entry>
<entry key="server">localhost</entry>
<entry key="context">pinsafe</entry>
<entry key="port">8181</entry>
<entry key="imagessl">true</entry>
<entry key="imageserver">demo.swivelsecure.com</entry>
<entry key="imagecontext">proxy</entry>
<entry key="imageport">8443</entry>
<entry key="secret">secret</entry>
<entry key="selfsigned">true</entry>
```

For a Swivel software install the settings may be:

```
<entry key="ssl">false</entry>
<entry key="server">localhost</entry>
<entry key="context">pinsafe</entry>
<entry key="port">8080</entry>
<entry key="imagessl">false</entry>
<entry key="imageserver">demo.swivelsecure.com</entry>
<entry key="imagecontext">pinsafe</entry>
<entry key="imageport">8080</entry>
<entry key="secret">secret</entry>
<entry key="selfsigned">true</entry>
```

- The settings as per the salesforce setup (Setup->Administrative Setup->Security Controls->Single Sign-On Settings)
- The location of the keys (which must match the certificate installed in salesforce)

```
<entry key="publicKeyFilePath">./keys/pinsafe/ssl/dsapubkey.der</entry>
<entry key="privateKeyFilePath">./keys/pinsafe/ssl/dsaprivkey.der</entry>
```

50.4 Key and Certificate Generation

see Key and Certificate Generation

50.5 Additional Installation Options

51 Verifying the Installation

In a browser, go to the root URL for the saml-salesforce client. This will redirect to the logon page. Logging in as a user will send a saml assertion for the username you logged in as. If this username matches to a FederationID for a user in Saleforce (see above) then you will be logged in as that user

52 Uninstalling the Swivel Integration

53 Troubleshooting

54 Known Issues and Limitations

55 Additional Information