

Contents

- 1 Introduction
- 2 Prerequisites
- 3 Baseline
- 4 Architecture
- 5 Installation
 - ◆ 5.1 Salesforce.com Configuration
 - ◇ 5.1.1 Allow Authentication
 - ◇ 5.1.2 Configure Single Sign On
 - ◆ 5.2 Configure The Swivel Server
 - ◆ 5.3 Access Device or Application Integration
 - ◆ 5.4 Key and Certificate Generation
 - ◆ 5.5 Additional Installation Options
- 6 Verifying the Installation
- 7 Uninstalling the Swivel Integration
- 8 Troubleshooting
- 9 Known Issues and Limitations
- 10 Additional Information

Introduction

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

Prerequisites

Salesforce.com Administrative 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 across 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)

Baseline

Salesforce 11, 12

Swivel 3.8, 3.9

Architecture

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

Installation

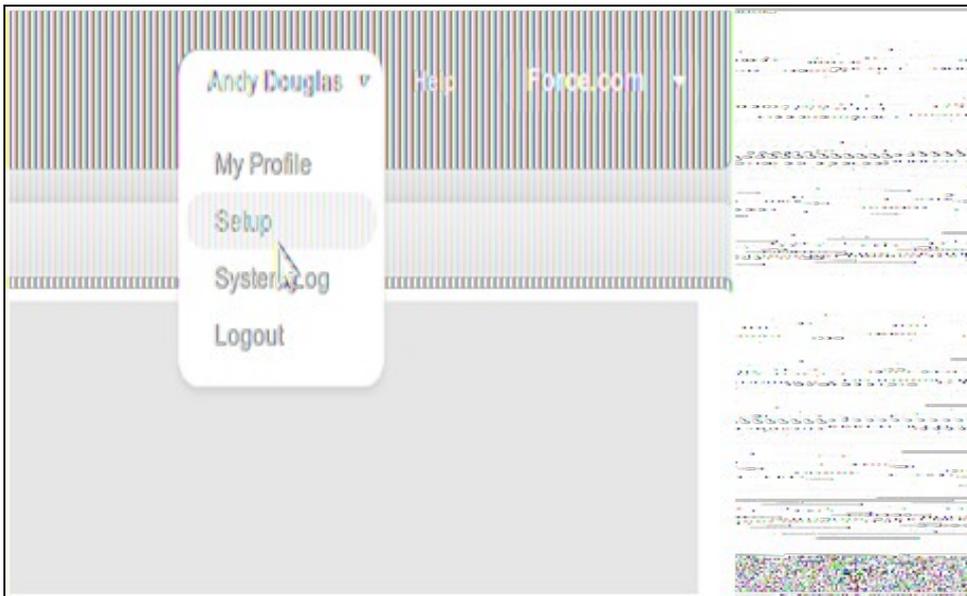
Salesforce.com Configuration

Allow Authentication

Contact Salesforce.com to enable Federated SSO

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

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.

[Edit](#) [SAML Assertion Validator](#) [Download Metadata](#)

Delegated authentication

Delegated Gateway URL: _____ Force Delegated Authentication Collect:

Federated single sign-on using SAML

SAML Enabled	SAML Version
<input checked="" type="checkbox"/>	2.0
SAML User ID Type	Federation ID
SAML User ID Location	Subject
Identity Provider Login URL	https://idm.snlivesecure.com/salesforce/
Identity Provider Logout URL	https://idm.snlivesecure.com/salesforce/
SAML Error URL	https://idm.snlivesecure.com/salesforce/error.html
Salesforce.com Login URL	https://login.salesforce.com/?saml=2&HXPointInCap?PHoScmodQmsKMLqjSWVNSBcmhOC32mDyICWdOp
OAuth 2.0 Token Endpoint	https://login.salesforce.com/services/oauth2/token?saml=2&HXPointInCap?PHoScmodQmsKMLqjSWVNSBcmhOC32mDyICWdOp
Entity ID	https://saml.salesforce.com/
Salesforce.com Single Logout URL	https://login.salesforce.com/saml/logout/request.jspx?saml=2&HXPointInCap?PHoScmodQmsKMLqjSWVNSBcmhOC32mDyICWdOp

[Edit](#) [SAML Assertion Validator](#) [Download Metadata](#)

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

- 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.

The screenshot displays the Salesforce 'All Users' interface. On the left, there are navigation menus for 'Personal Setup', 'App Setup', and 'Administration Setup'. The 'Administration Setup' menu is expanded to show 'Manage Users' and 'Users'. The main content area is titled 'All Users' and includes a search bar, a view selector (set to 'List View'), and a list of users. The user list has the following data:

<input type="checkbox"/>	Active	Full Name	Alias	Username	Last Login	Role	Active	Profile	Storage
<input type="checkbox"/>	Esti	Carl Daniel	Carl	dcarl@virentos.com	28/03/2011 13:30	Customer Support International	✓	Standard Platform User	
<input type="checkbox"/>	Esti	Douglas Andy	ADougl	andy.douglas@virentos.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	<input checked="" type="checkbox"/>	Manage Public List Views	<input type="checkbox"/>
Edit HTML Templates	<input type="checkbox"/>	Manage Public Reports	<input type="checkbox"/>
IP Restrict Requests	<input type="checkbox"/>	Manage Public Templates	<input type="checkbox"/>
Manage Business Hours Holidays	<input type="checkbox"/>	Password Never Expires	<input type="checkbox"/>
Manage Dashboards	<input type="checkbox"/>	Send Outbound Messages	<input checked="" type="checkbox"/>
Manage Dynamic Dashboards	<input type="checkbox"/>	Transfer Record	<input type="checkbox"/>
Manage Letterheads	<input type="checkbox"/>	View Setup and Configuration	<input checked="" type="checkbox"/>
Manage Public Documents	<input type="checkbox"/>		

General User Permissions

Create and Customize Reports	<input checked="" type="checkbox"/>	Is Single Sign-On Enabled	<input checked="" type="checkbox"/>
Create Workspaces	<input type="checkbox"/>	Manage Content Permissions	<input type="checkbox"/>
Deliver Uploaded Files and Personal Content	<input checked="" type="checkbox"/>	Mass Edits from Lists	<input checked="" type="checkbox"/>
Drag-and-Drop Dashboard Builder	<input type="checkbox"/>	Mass Email	<input checked="" type="checkbox"/>
Edit Events	<input checked="" type="checkbox"/>	Run Reports	<input checked="" type="checkbox"/>
Edit Tasks	<input checked="" type="checkbox"/>	Send Email	<input checked="" type="checkbox"/>
Export Reports	<input checked="" type="checkbox"/>	Show Custom Sidebar On All Pages	<input type="checkbox"/>
Import Personal Contacts	<input checked="" type="checkbox"/>	View My Team's Dashboards	<input type="checkbox"/>

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	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Contacts	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

	Basic Access				Data Administration	
	Read	Create	Edit	Delete	View All	Modify All
Documents	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Mass	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				

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 with 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

City

State/Province

Zip/Postal Code

Country

Single Sign On Information

Federation ID

Locale Settings

Time Zone ▼

Locale ▼

Language ▼

Approver Settings

Delegated Approver 

Manager 

Receive Approval Request Emails ▼

salesforce.com Newsletter Settings

Receive the salesforce.com newsletter

Receive the salesforce.com administrator newsletter

Generate new password and notify user immediately

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:	<input type="text" value="local"/>	
	Hostname/IP:	<input type="text" value="127.0.0.1"/>	
	Shared secret:	<input type="password" value="....."/>	
	Group:	<input type="text" value="---ANY---"/>	
	Authentication Modes:	<input type="text" value="ALL"/>	<input type="button" value="Delete"/>
	Name:	<input type="text" value="IIS"/>	
	Hostname/IP:	<input type="text" value="192.168.1.1"/>	
	Shared secret:	<input type="password" value="....."/>	
	Group:	<input type="text" value="---ANY---"/>	
	Authentication Modes:	<input type="text" value="ALL"/>	<input type="button" value="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:	<input type="text" value="turing.xml"/>
Rotate letters:	<input type="text" value="No"/>
Allow session request by username:	<input checked="" type="text" value="Yes"/>
Only use one font per image:	<input type="text" value="Yes"/>
Jiggle characters within slot:	<input type="text" value="No"/>
Add blank trailer frame to animated images:	<input type="text" value="Yes"/>
Text Alpha Value:	<input type="text" value="80"/>
Number of complete display cycles per image:	<input type="text" value="10"/>
Inter-frame delay (1/100s):	<input type="text" value="40"/>
Image Rendering:	<input type="text" value="Static"/>
Multiple AUTHentications per String:	<input type="text" value="No"/>
Generate animated images:	<input type="text" value="No"/>
Random glyph order when animating:	<input type="text" value="No"/>
No. Characters Visible:	<input type="text" value="1"/>

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 salesforce 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="imagesssl">>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.qRKnViSBCmh05IC52m5VptCNw0.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="imagesssl">>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="imagesssl">>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>
```

Key and Certificate Generation

see [Key and Certificate Generation](#)

Additional Installation Options

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 Salesforce (see above) then you will be logged in as that user

Uninstalling the Swivel Integration

Troubleshooting

Known Issues and Limitations

Additional Information