

Sentry SSO with Salesforce

Contents

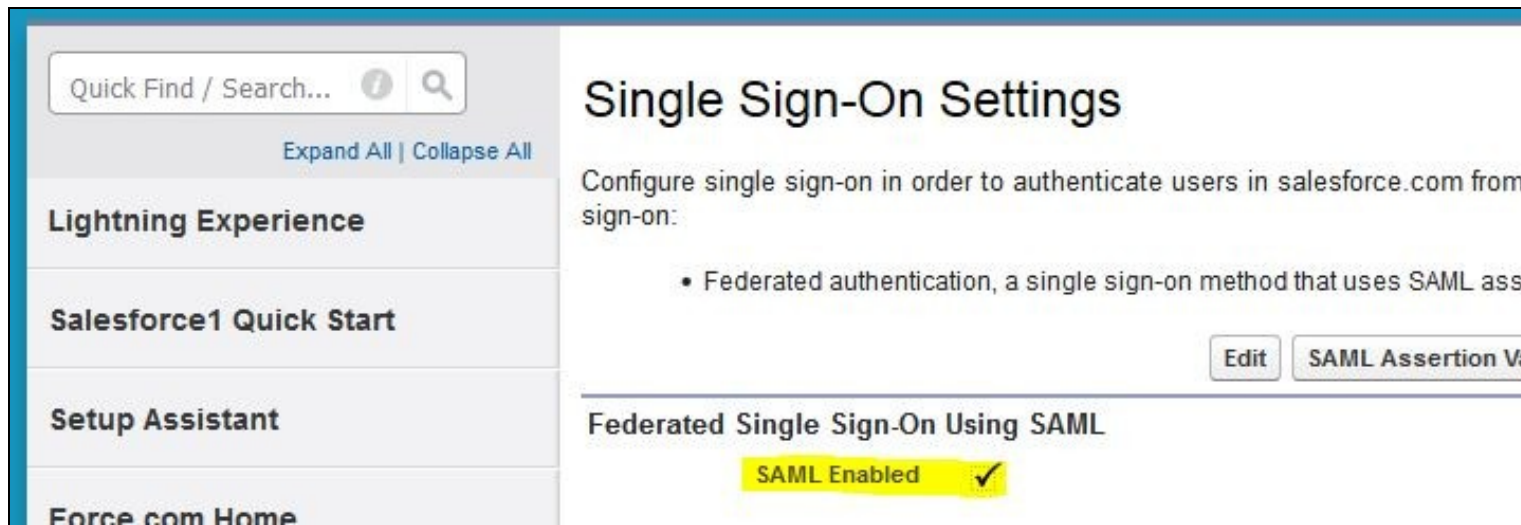
- 1 Setup Sentry Keys
- 2 Enable SAML on Salesforce.com
- 3 Create a new Single Sign-On Settings entry on Salesforce.com
- 4 Determine and configure your SSO username attribute
- 5 Configuring the federated ID in Salesforce.com
- 6 Configuring alternative username attributes in the Swivel Core
- 7 Configure Check Password with Repository on the Swivel Core
- 8 Setup Sentry Application definition
- 9 Setup Sentry Authentication definition
- 10 Assign the Salesforce domain to the SSO definition
- 11 Testing authentication to Salesforce via Swivel Sentry
- 12 Troubleshooting

Setup Sentry Keys

Before you are able to create a Single Sign On configuration on Salesforce.com, you will need to setup some Keys. Please see a separate article: [HowToCreateKeysOnCmi](#). You will need the certificate you generate in a later section of this article. This can be retrieved from the View Keys menu option of Swivel Sentry.

Enable SAML on Salesforce.com

Enable SAML. A checkbox option entitled ?SAML Enabled? should be available in Salesforce under the menu Setup -> Security Controls -> Single Sign-On Settings.



If this option is not available, then you will need to request this feature from Salesforce support or your Salesforce reseller partner.

Create a new Single Sign-On Settings entry on Salesforce.com

Under the menu Setup -> Security Controls -> Single Sign-On Settings, create a new SAML Single Sign-On Settings entry by clicking the New button.

Quick Find / Search...

[Expand All](#) | [Collapse All](#)

Lightning Experience

Salesforce1 Quick Start

Setup Assistant

Force.com Home

Administer

Single Sign-On Settings

Configure single sign-on in order to authenticate users in salesforce.com from sign-on:

- Federated authentication, a single sign-on method that uses SAML as

Edit

SAML Assertion V

Federated Single Sign-On Using SAML

SAML Enabled ☒

SAML Single Sign-On Settings

New

New from Metadat

Populate all required fields and **upload the certificate you generated earlier** (this can be retrieved from the View Keys menu option of Swivel Sentry):

SAML Single Sign-On Settings

SaveSave & NewCancel

Name

Swivel Sentry

SAML Version

2.0

Issuer

SAML_SP

Identity Provider Certificate

Browse...

No file selected.

Request Signing Certificate

Default Certificate

Request Signature Method

RSA-SHA1

Assertion Decryption Certificate

Assertion not encrypted

SAML Identity Type

☐ Assertion contains User's salesforce.com username

☒ Assertion contains the Federation ID from the User object

☐ Assertion contains the User ID from the User object

SAML Identity Location

☒ Identity is in the NameIdentifier element of the Subject statement

☐ Identity is in an Attribute element

Service Provider Initiated Request Binding

☒ HTTP POST

☐ HTTP Redirect

Identity Provider Login URL

https://dc.dev.swivelsecure.net:8443/sentry/saml20endpoint

Identity Provider Logout URL

https://dc.dev.swivelsecure.net:8443/sentry/singlelogout

Custom Error URL

https://dc.dev.swivelsecure.net:8443/sentry/error

Just-in-time User Provisioning

User Provisioning Enabled

☐ i

SaveSave & NewCancel

Name = Swivel Sentry (arbitrary value)

Issuer = Sentry endpoint URL (<https://yourdomain/sentry/saml20endpoint>)

Identity Provider Certificate = Browse to the RSA PEM file created earlier to upload the certificate. When you click save, if successfully imported, the details of the certificate will appear on the right hand side under the ?Current Certificate? field.

Request Signing Certificate = Default Certificate

Request Signature Method = RSA-SHA1

Assertion Decryption Certificate = Assertion not encrypted

SAML Identity Type = Assertion contains the Federation ID from the User object

SAML Identity Location = Identity is in the NameIdentifier element of the Subject statement

Service Provider Initiated = HTTP POST

Set the Login, Logout and Error URLs below, where <FQDN_OF_SENTRY_SERVER> is the public DNS entry of your Swivel Sentry server, e.g. swivel.mycompany.com or if you do not have a redirect from port 443 to 8443 in place, you may need to include a port number e.g. swivel.mycompany.com:8443

Identity Provider Login URL = `https://<FQDN_OF_SENTRY_SERVER>/sentry/saml20endpoint`

Identity Provider Logout URL = `https://<FQDN_OF_SENTRY_SERVER>/sentry/singlelogout`

Custom Error URL = `https://<FQDN_OF_SENTRY_SERVER>/sentry/error` (ensure that the firewall 443 to 8443 port redirect and open port is in place for these URLs)

API Name = `Swivel_Sentry`

Entity ID = `https://saml.salesforce.com`

Determine and configure your SSO username attribute

Prior to configuration, you will need to determine which username attribute will be used for authentication and single sign on. For example you may wish to use the email attribute, or the sAMAccountName (default Active Directory username) or something else like an employee or security ID.

Username attribute examples:

Email attribute: email e.g. j.smith@mycompany.net

AD username: sAMAccountName e.g. jsmith

When a user attempts to authenticate to the Salesforce Application or any other configured application, they will need to enter this username in the Login page presented by the Swivel Sentry.

Configuring the federated ID in Salesforce.com

Against the User's profile there is an area when you can configure the user's federated ID. This could be their email address or Active Directory username for example.

Mailing Address

Street

City

State/Province

Zip/Postal Code

Country

Single Sign On Information

Federation ID

dcroft

Additional Information

Can Delete Opportunities

☐

Locale Settings

Time Zone

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

Locale

English (United Kingdom)

Language

English

Currency


GBP - British Pound

Configuring alternative username attributes in the Swivel Core

If you have already imported the users into the Swivel Core with a particular username attribute, but wish to use another attribute for SSO and authentication, then you will need to configure an alternative attribute or delete and import the users into the Swivel Core again with the correct attribute.

The Swivel Core allows the use of any attribute for the username provided that it is imported into the Swivel Core database during User Sync. The use of alternative attributes can be configured upon the Server -> Agent definition in the Swivel Core.

Below you can see an example of email attribute.



SWIVEL

Adaptable. Active. Authentication

• [Status](#)

• [Log Viewer](#)

⊞ Server

⊞ Policy

⊞ Logging

⊞ Transport

⊞ Database

⊞ Mode

⊞ Repository

- [Servers](#)
- [Types](#)
- [Groups](#)
- [Attributes](#)
- [SimpleLDAP](#)
- [default](#)
- [swivelsecure-local](#)

Repository>Attributes

Please enter the repository attributes for the transport types

Name:

email

Phone Number?

No

Sync Rule

Synchronised

Add repository qualifier?

None

Attribute:

SimpleLDAP:

mail

default:

mail

swivelsecure-local:

mail

Delete

As another example, here is another attribute you might consider, on the Repository -> Attributes screen (altusername) which maps to the userPrincipalName on the Active Directory repository:

- [Administration Guide](#)
- [Logout](#)

Name:

Phone Number?

Sync Rule

Add repository qualifier?

Attribute:

Delete

SimpleLDAP:

default:

swivelsecure-local:

Name:

Phone Number?

Sync Rule

Add repository qualifier?

Attribute:

Delete

SimpleLDAP:

default:

swivelsecure-local:

Again you need to be careful to enter the ?Name? such as username or altusername (highlighted) and not one of the repository mappings such as sAMAccountName or userPrincipalName.

Configure Check Password with Repository on the Swivel Core

In order to check the user's Active Directory password, ensure that the local Agent is configured as explained [here](#)

Setup Sentry Application definition

Please note: you must have setup a Salesforce domain prior to defining this Application entry within Swivel Sentry. This is so that you are able to populate the Endpoint URL field. Login to the Swivel Sentry Administration Console. Click Applications in the left hand menu. To add a new Application definition for Salesforce, click the Add Provider button.

Rules

Applications

Authentication Methods

View IdP Metadata

Keys

Users Active Sessions

User History

Log Viewer

General Configuration

Application Images

SAML Application



Note: The Endpoint URL is used only if the ACP is SAML (Security Assertion Markup Language)

Name

Salesforce

Image

Salesforce.png

Points

0

Portal URL

https://yourdomain.salesforce.com

Endpoint URL

Entity ID

https://saml.salesforce.com

Federated Id

email

- **Name:** Salesforce (Type an Arbitrary name for this Application)
- **Image:** Salesforce.png (selected by default)
- **Points:** 100 (the number of points the user needs to score from their Authentication Method in order to successfully authenticate to this Application)
- **Portal URL:** (this Endpoint URL can be found on the Setup -> Security Controls -> Single Sign-On Settings page in Salesforce.com, listed as ?Salesforce Login URL? under the Endpoints section. It is unique to your Salesforce.com instance and domain. Example: <https://companyname.my.salesforce.com?so=00E32000000cx7O>. This requires that you have previously setup a Salesforce domain under Setup -> Domain Management -> Domains and that it is at least listed as ?Domain Ready for Testing? status on Salesforce.com)
- **EndPoint URL:** N/A
- **Entity ID:** <https://saml.salesforce.com> (at the time of writing this documentation, this settings is always the same when using Salesforce, but may be subject to change by Salesforce.com, so please review the online Salesforce documentation if you find that this Entity ID no longer works)
- **Federated id:** email (That needs to match with the attributed defined on Salesforce.com and Swivel Core)

Setup Sentry Authentication definition

As an example here we will be using Turing authentication as the Primary method required for Salesforce authentication.

Login to the Swivel Sentry Administration Console. Click Authentication Methods in the left hand menu. Click the Edit button against the Turing option in the list of Authentication Methods. Give this Authentication Method 100 points. This will mean that when a login attempt is made to the Salesforce Application, this Authentication Method will be offered during login.

Assign the Salesforce domain to the SSO definition

On Salesforce, select Domain Management -> My Domains. Under the **Authentication Configuration** section, click Edit.

Deselect the **Login Page** checkbox and enable the checkbox of the authentication service that you created on the SAML SSO Settings screen. Click the Save button.

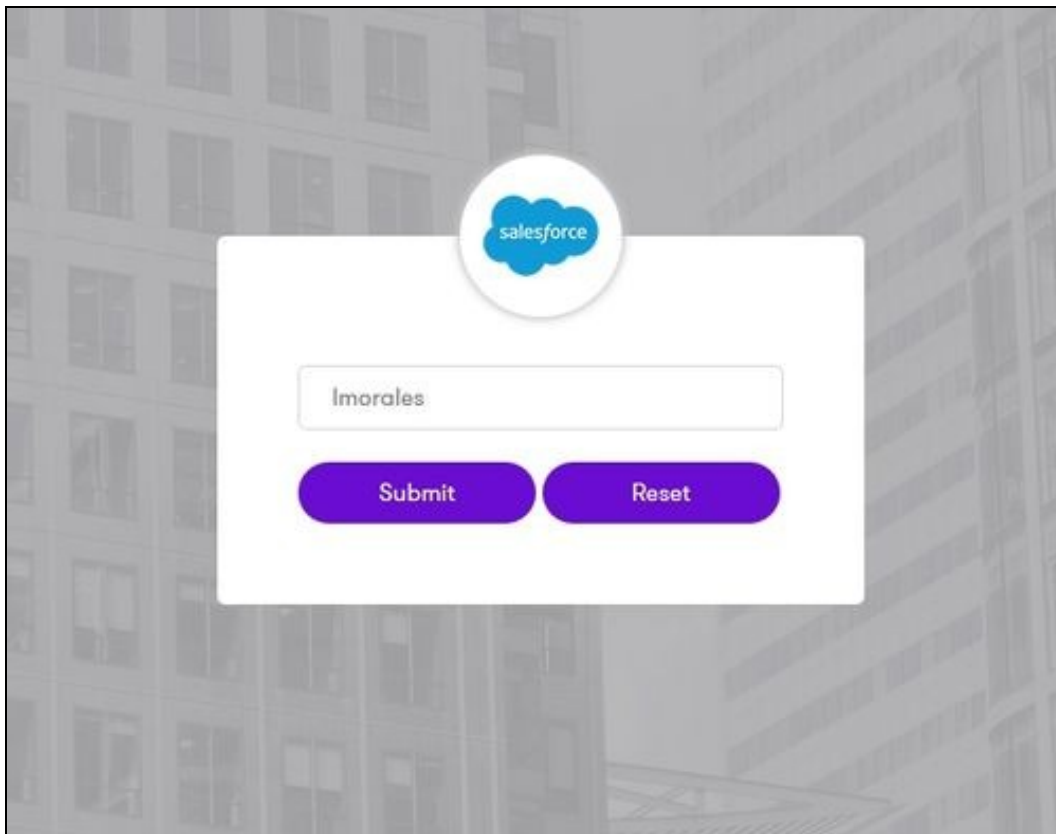
Testing authentication to Salesforce via Swivel Sentry

This should be the final step after all previous elements have been configured.

In a web browser, visit the Domain URL that you setup in Salesforce.com which also constitutes the FQDN part of your Endpoint URL e.g. <https://companyname.my.salesforce.com>

When you visit this URL you will notice that the domain should redirect to the identity provider login URL that you setup, once you have submitted your username. You should be presented with the page of the Authentication Method which can score enough points to match the points required by the Salesforce Application definition.

In this login example we are using the username attribute as the federated ID.



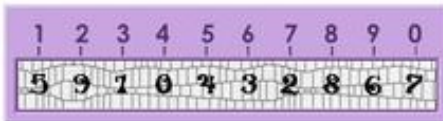


Imorales

Password

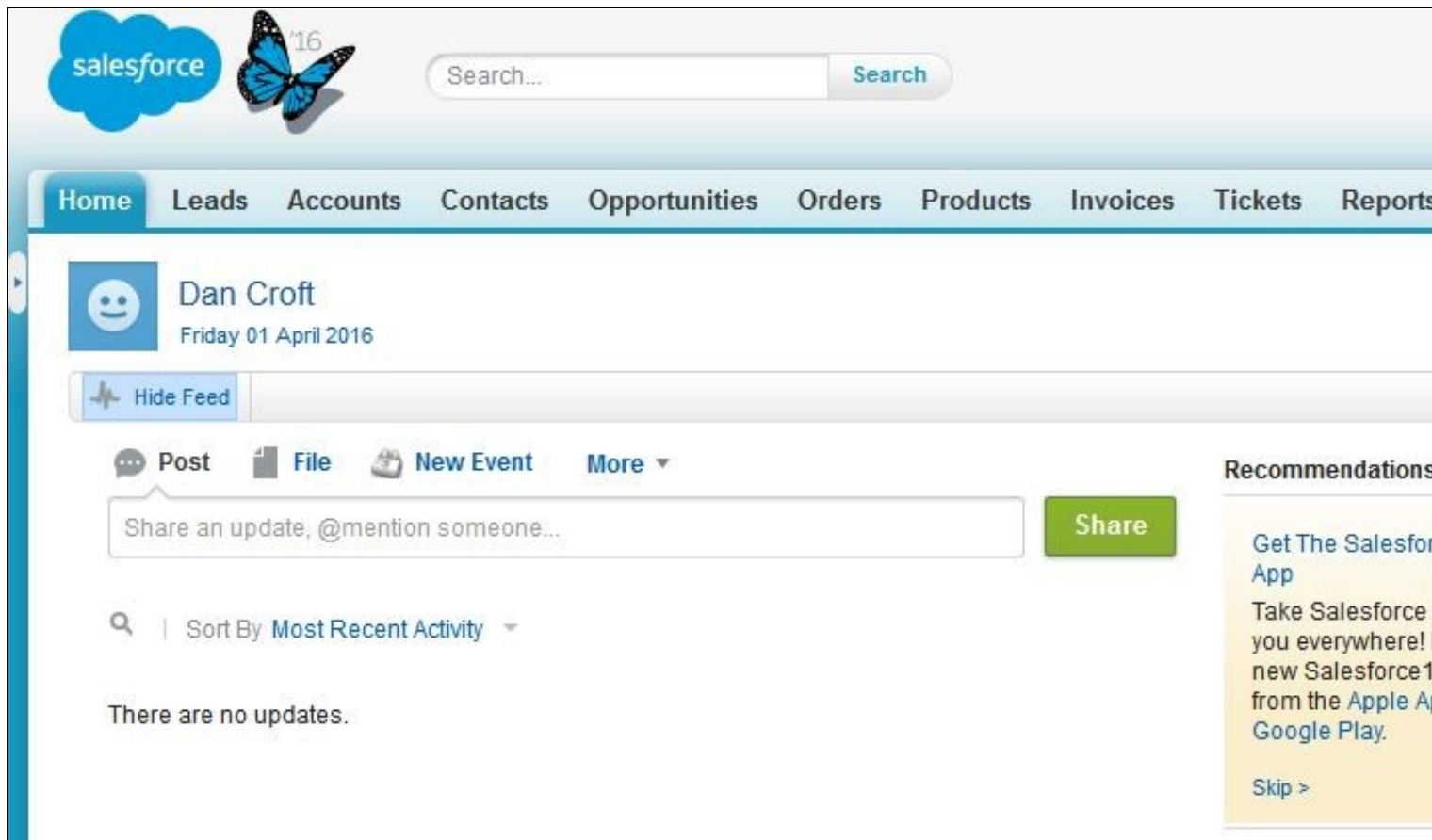
OTC

TURing



Login

Refresh Image



Troubleshooting

There are various logging components available for this particular integration which can aid in diagnosis at different points during authentication.

- The Swivel Core has a Log Viewer menu item which can reveal information concerning user status e.g. is the user locked, has a session been started for the image request;
- The Swivel Sentry has a View Log menu item which provides details about the SAML assertion and response received from Salesforce and can be useful for comparison with the Salesforce SAML Assertion Validator output;
- Salesforce has a SAML Assertion Validator which can provide diagnostics about the latest SAML authentication attempt. This can be particularly useful for verifying the federated ID and various elements within the SAML assertion that takes place between the Swivel Sentry and Salesforce.com. To get to the SAML Assertion Validator in Salesforce.com select Setup -> Security Controls -> Single Sign-On Settings. At the top of the page you will see the SAML Assertion Validator button:

Quick Find / Search...

[Expand All](#) | [Collapse All](#)

Lightning Experience

Salesforce1 Quick Start

Setup Assistant

Force.com Home

Administer

▸ Manage Users

▸ Manage Apps

▸ Company Profile

▣ Security Controls

Health Check **New!**

Sharing Settings

Field Accessibility

Password Policies

Session Settings

Login Flows

Network Access

Activations

Session Management

Login Access Policies

Certificate and Key Management

Single Sign-On Settings

Single Sign-On Settings

Configure single sign-on in order to authenticate users in salesforce.com from

- Federated authentication, a single sign-on method that uses SAML as

EditSAML Asses

Federated Single Sign-On Using SAML

SAML Enabled ☒

SAML Single Sign-On Settings

NewNew from M

Action	Name	SAML Version
Edit Del	Swivel Sentry	2.0

Click the button and you will be taken to a screen when you select the name of your Single Sign-On Setting and click Validate:

SAML Validator

Enter your SAML response in base64-encoded, deflated and base64-encoded, or plain xml format into the field below, and click V

You can select a config to use to validate the response, or you can automatically detect the config from the response. If the page i manually selecting the appropriate config.

The validator will try to continue validation even if it finds an error. However, the validator cannot recover from some errors. More e errors not related to the assertion itself will not be detected by this validator. Please refer to the login history for more information

Your organization is configured to use SAML Version 2.0

SAML Response

Validate

Swivel Sentry



Once you have clicked the validate button, the Results screen will appear and show some diagnostics.

Results

Unexpected Exceptions

Unable to parse the response
Premature end of file.

1. Validating the Status

Unknown

2. Looking for an Authentication Statement

Unknown

3. Looking for a Conditions statement

Unknown

4. Checking that the timestamps in the assertion are valid

Unknown

5. Checking that the Attribute namespace matches, if provided

Unknown

6. Miscellaneous format confirmations

Unknown

7. Confirming Issuer matches

Unknown

8. Confirming a Subject Confirmation was provided and contains valid timestamps

Unknown

9. Checking that the Audience matches

Unknown

10. Checking the Recipient

Unknown

11. Validating the Signature

Unknown

12. Checking that the Site URL Attribute contains a valid site url, if provided

Unknown

13. Looking for portal and organization id, if provided

Unknown

14. Checking if session security level is valid, if provided

Unknown

Subject:

Unable to map the subject to a Salesforce.com user

AssertionId:

It is crucial when troubleshooting, to pinpoint where the authentication is failing. For example, you may find that the Swivel Core logs show a successful authentication (which would indicate that the user has entered their Password and OTC correctly), but the Sentry logging or Salesforce.com validator shows that there is a problem with the SAML assertion.

Two common issues which can be diagnosed with the validator are:

- Certificate or decryption issues;
 - ◆ Can Sentry find the Certificate locally, is it the correct one?
 - ◆ Has the correct Certificate been uploaded to Salesforce.com?
- Federated ID mismatch.
 - ◆ Has the Federated ID value been added to the user's Salesforce.com profile?
 - ◆ Has Tomcat been restarted after populating the Sentry settings.properties file with the federated ID username attribute?
 - ◆ Does the Repository -> Attribute name being used actually map to a Repository attribute? Has a User Sync occurred in the Swivel Core since modifying this?