EFT SAML SSO with Salesforce as IDP

THE INFORMATION IN THIS ARTICLE APPLIES TO:

- EFT v7.3.3 and later

NOTE: This article provides guidelines for using a third-party tool with EFT. This article is not meant as formal support for that tool, but only as an example of setup options. Contact the third-party seller's support for detailed information about their product. Globalscape is not responsible for any configuration errors involving the third-party tool.

DISCUSSION

Overview

- This document describes how to setup and test the EFT SSO feature with Salesforce as the IDP.

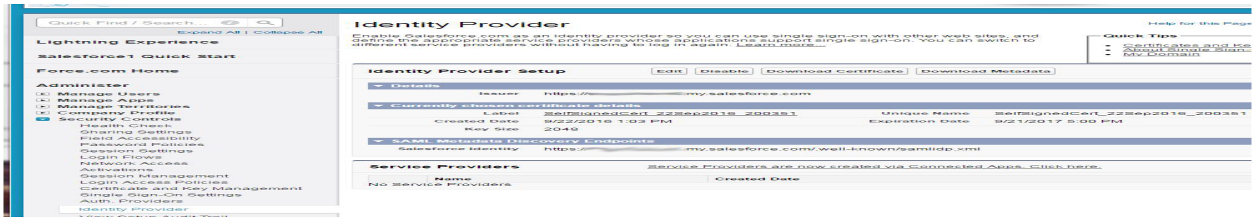
Get a salesforce developer account

- Signup for a salesforce developer account at: https://developer.salesforce.com/en/

Get a salesforce Domain and enable for IDP

- Salesforce does a good job documenting the process for becoming a IDP. Just follow their instructions:
  - o https://help.salesforce.com/HTViewHelpDoc?id=identity_provider_enable.htm&language=en_US
- When you get to the step where you create your domain be sure to bookmark it. For example Safeforce will create a domain for access to your IDP app such as:

  https://mypc-dev-ed.my.salesforce.com/setup/forcecomHomepage.apexp?setupid=ForceCom
- Once you've completed the setup your IDP and SSO Settings should look similar to the following:



Identity Provider

Enable Salesforce.com as an identity provider so you can use single sign-on with other web sites, and define the appropriate service providers whose applications support single sign-on. You can switch to different service providers without having to log in again. Learn more...

Identity Provider Setup

▼ Details

Issuer https://[redacted]my.salesforce.com

▼ Currently chosen certificate details

Label	SelfSignedCert_22Sep2016_200351	Unique Name	SelfSignedCert_22Sep2016_200351
Created Date	9/22/2016 1:03 PM	Expiration Date	9/21/2017 5:00 PM
Key Size	2048		

▼ SAML Metadata Discovery Endpoints

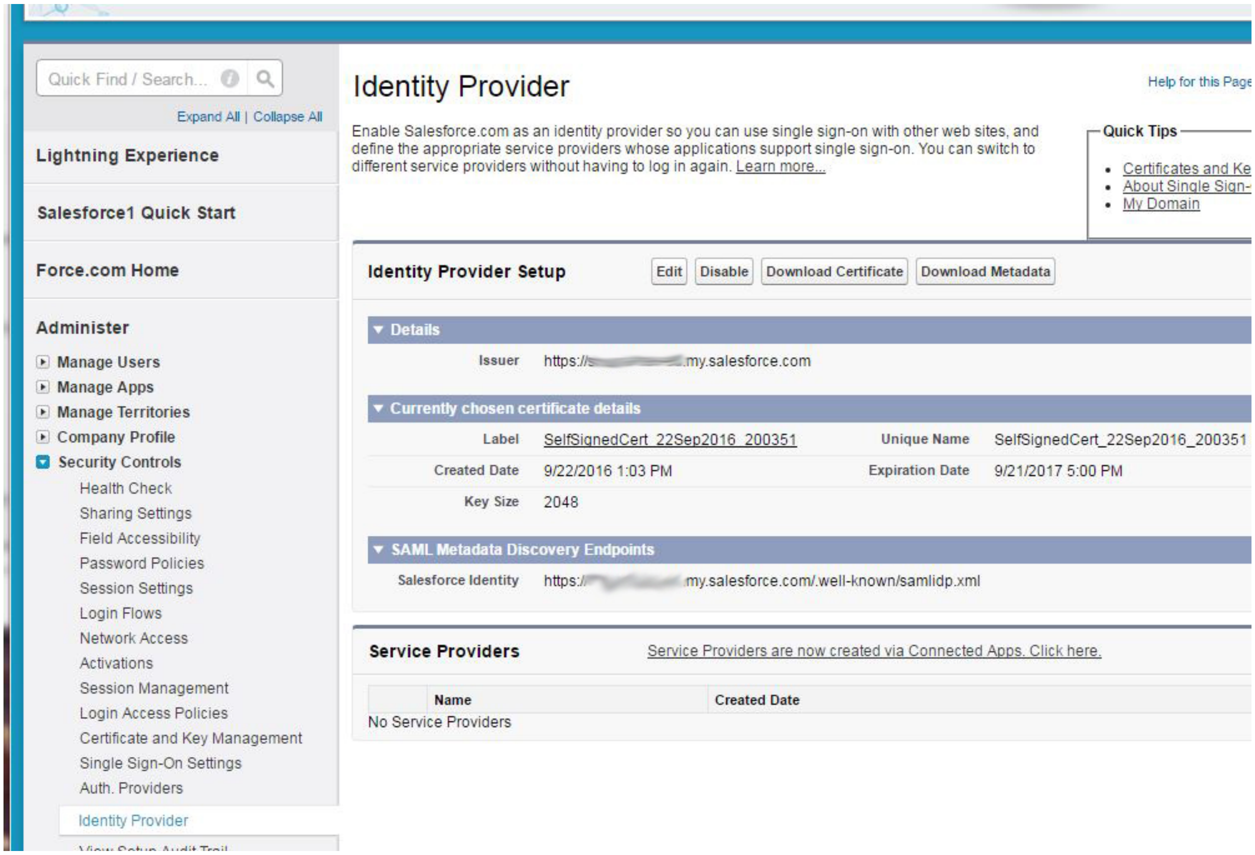
Salesforce Identity https://[redacted]my.salesforce.com/.well-known/samlidp.xml

Service Providers — Service Providers are now created via Connected Apps. Click here.

Name	Created Date
No Service Providers	

Configure EFT as a SP to the Salesforce IDP

- Once you've enabled and configured Salesforce as an IDP you'll need to define EFT As a Service Provider to the IDP. Follow Salesforce's instructions on adding an SP:
- https://help.salesforce.com/HTViewHelpDoc?id=service_provider_define.htm&language=en_US
- Once you've completed setup your SP settings should look similar to the following:



Identity Provider

Enable Salesforce.com as an identity provider so you can use single sign-on with other web sites, and define the appropriate service providers whose applications support single sign-on. You can switch to different service providers without having to log in again. Learn more...

Identity Provider Setup

Details

Issuer https://[redacted]my.salesforce.com

Currently chosen certificate details

Label	SelfSignedCert_22Sep2016_200351	Unique Name	SelfSignedCert_22Sep2016_200351
Created Date	9/22/2016 1:03 PM	Expiration Date	9/21/2017 5:00 PM
Key Size	2048		

SAML Metadata Discovery Endpoints

Salesforce Identity https://[redacted]my.salesforce.com/.well-known/samlidp.xml

Service Providers — Service Providers are now created via Connected Apps. Click here.

Name	Created Date
No Service Providers	

Create Users

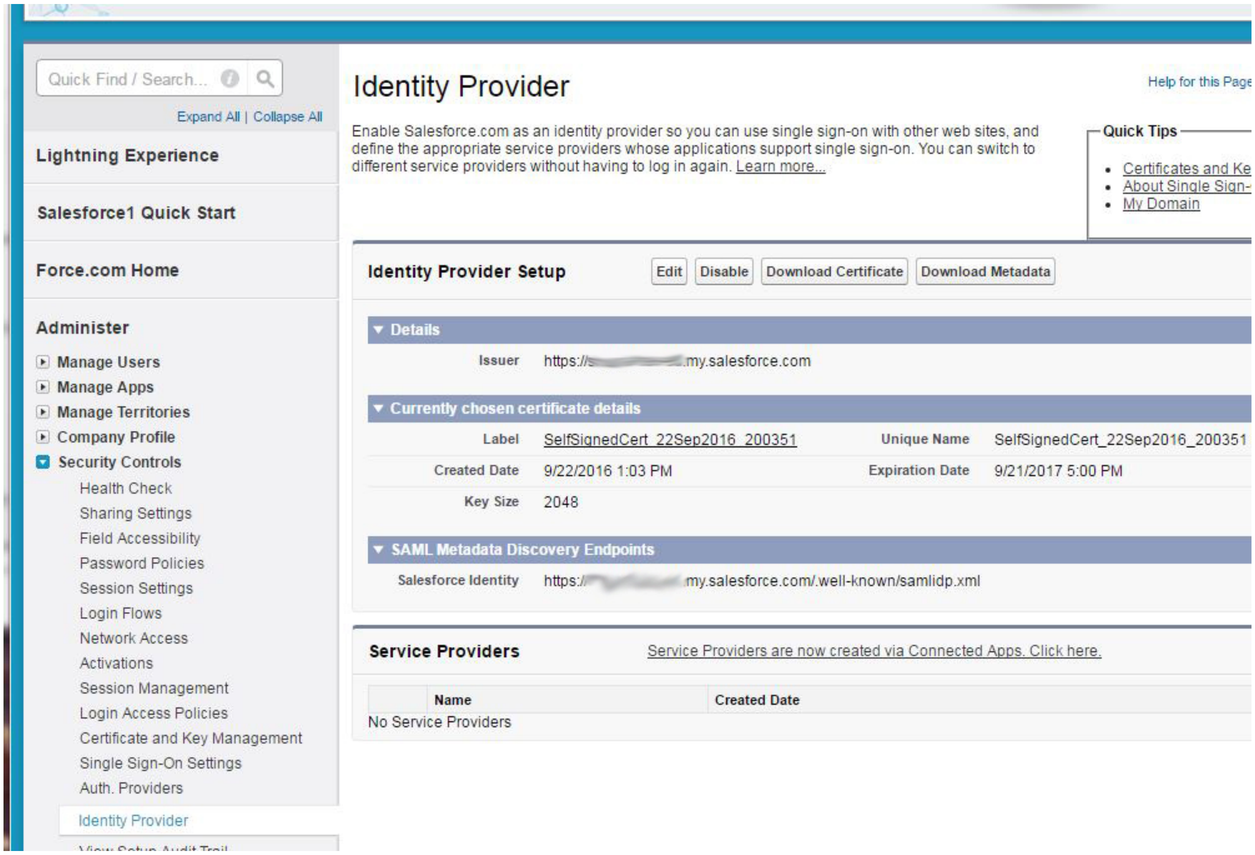
- Create some users in your Salesforce app, similarly create these same users in EFT.
- When creating your users be sure to set the User License to **Salesforce**. If you don't then you won't be able to add the user to the SSO permissions group.

All Users

On this page you can create, view, and manage users.

Create and add users to the SSO Permissions group

- In Salesforce go to Manage Users > Permission Sets
- Create your permission set then click on Manage Assignments and add your users for SSO.



Identity Provider

Enable Salesforce.com as an identity provider so you can use single sign-on with other web sites, and define the appropriate service providers whose applications support single sign-on. You can switch to different service providers without having to log in again. Learn more...

Quick Tips

- Certificates and Ke
- About Single Sign-
- My Domain

Identity Provider Setup

Details

Issuer: https://s[redacted].my.salesforce.com

Currently chosen certificate details

Label	SelfSignedCert_22Sep2016_200351	Unique Name	SelfSignedCert_22Sep2016_200351
Created Date	9/22/2016 1:03 PM	Expiration Date	9/21/2017 5:00 PM
Key Size	2048		

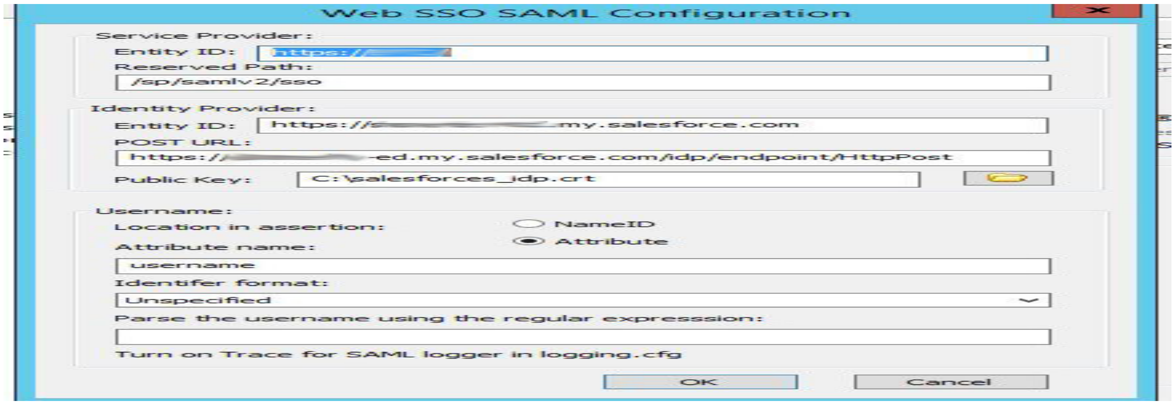
SAML Metadata Discovery Endpoints

Salesforce Identity: https://[redacted]my.salesforce.com/.well-known/samlidp.xml

Service Providers Service Providers are now created via Connected Apps. Click here.

Name	Created Date
No Service Providers	

Configure EFT with Salesforce as the IDP Server



Service Provider:

Entity ID: https://[redacted]

Reserved Path: /sp/samlv2/sso

Identity Provider:

Entity ID: https://s[redacted]my.salesforce.com

POST URL: https://[redacted]-ed.my.salesforce.com/idp/endpoint/HttpPost

Public Key: C:\salesforces_idp.crt

Username:

Location in assertion: ○ NameID ● Attribute

Attribute name: username

Identifer format: Unspecified

Parse the username using the regular expresssion:

Turn on Trace for SAML logger in logging.cfg

Some tips

- We do not support user provisioning so do not enable this feature when configuring your Salesforce IDP
- We only support HTTP POST so when configuring your SP and IDP be sure to specify and use the POST endpoint.
- Make sure your IDP matching attribute matches the attribute search you specify in EFT.

GlobalSCAPE Knowledge Base
https://kb.globalscape.com/Knowledgebase/11321/EFT-SAML-SSO-with-Salesforce...