

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

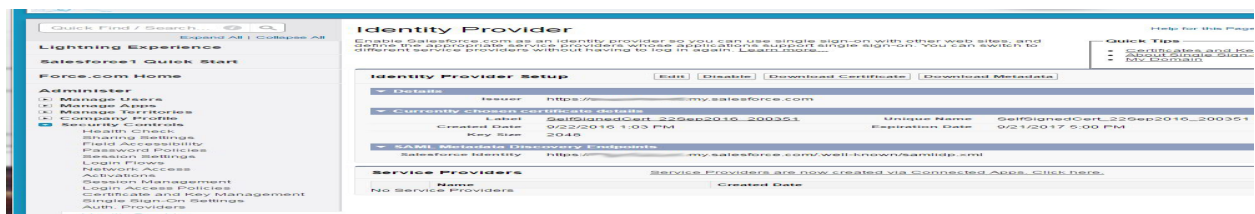
- This document describes how to setup and test the EFT SSO feature with Salesforce as the IDP.

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:
 - 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 Safeorce 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:



EFT SAML SSO with Salesforce as IDP



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:

A screenshot of the Salesforce Identity Provider Setup page. The left sidebar contains navigation links: Lightning Experience, Salesforce1 Quick Start, Force.com Home, and Administer (with sub-links for Manage Users, Manage Apps, Manage Territories, Company Profile, Security Controls, Health Check, 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, Auth. Providers, Identity Provider, and View Setup Audit Trail). The main content area is titled 'Identity Provider' and includes a description: '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...'. Below this is the 'Identity Provider Setup' section with buttons for Edit, Disable, Download Certificate, and Download Metadata. It contains three expandable sections: 'Details' (Issuer: https://...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), and 'SAML Metadata Discovery Endpoints' (Salesforce Identity: https://...my.salesforce.com/weil-known/samlidp.xml). At the bottom is the 'Service Providers' section with a note: 'Service Providers are now created via Connected Apps. Click here.' and a table with columns 'Name' and 'Created Date' showing '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.



EFT SAML SSO with Salesforce as IDP

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.

The screenshot shows the Salesforce Identity Provider Setup page. On the left is a navigation sidebar with sections: Lightning Experience, Salesforce1 Quick Start, Force.com Home, and Administer. Under Administer, Security Controls is expanded, showing options like Health Check, 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, and Auth. Providers. The Identity Provider link is highlighted. The main content area is titled 'Identity Provider' and includes a description: '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...](#)'. Below this are buttons for 'Identity Provider Setup', 'Edit', 'Disable', 'Download Certificate', and 'Download Metadata'. The 'Details' section shows the Issuer as 'https://s[redacted].my.salesforce.com'. The 'Currently chosen certificate details' section shows a table with columns: Label, Unique Name, Created Date, Expiration Date, and Key Size. The values are: 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', and Key Size '2048'. The 'SAML Metadata Discovery Endpoints' section shows a table with columns: Name and Created Date. The value is: Name 'Salesforce Identity', Created Date 'https://s[redacted].my.salesforce.com/well-known/samlidp.xml'. The 'Service Providers' section has a link: 'Service Providers are now created via Connected Apps. [Click here.](#)'. Below this is a table with columns: Name and Created Date. The value is: Name 'No Service Providers', Created Date ''.

Configure EFT with Salesforce as the IDP Server

The screenshot shows the 'Web SSO SAML Configuration' dialog box. It has two main sections: 'Service Provider' and 'Identity Provider'. The 'Service Provider' section has fields for 'Entity ID' (https://[redacted]) and 'Reserved Path' (/sp/samlv2/ssso). The 'Identity Provider' section has fields for 'Entity ID' (https://s[redacted].my.salesforce.com), 'POST URL' (https://[redacted]-ed.my.salesforce.com/idp/endpoint/HttpPost), and 'Public Key' (C:\salesforces_idp.crt). Below these are fields for 'Username' configuration: 'Location in assertion' (radio buttons for NameID and Attribute, with Attribute selected), 'Attribute name' (username), 'Identifier format' (Unspecified), and 'Parse the username using the regular expression' (checkbox checked). There is also a checkbox for 'Turn on Trace for SAML logger in logging.cfg'. At the bottom are 'OK' and 'Cancel' buttons.

EFT SAML SSO with Salesforce as IDP

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...>