



ComponentSpace SAML for ASP.NET Salesforce Service Provider Integration Guide

Contents

Introduction..... 1

Single Sign-On Settings 1

Identity Provider Configuration 5

SP-Initiated SSO 6

IdP-Initiated SSO 7

SAML Logout..... 9

Introduction

This document describes integration with Salesforce as the service provider.

For information on configuring Salesforce for SAML SSO, refer to the following articles.

https://developer.salesforce.com/docs/atlas.en-us.sso.meta/sso/sso_about.htm

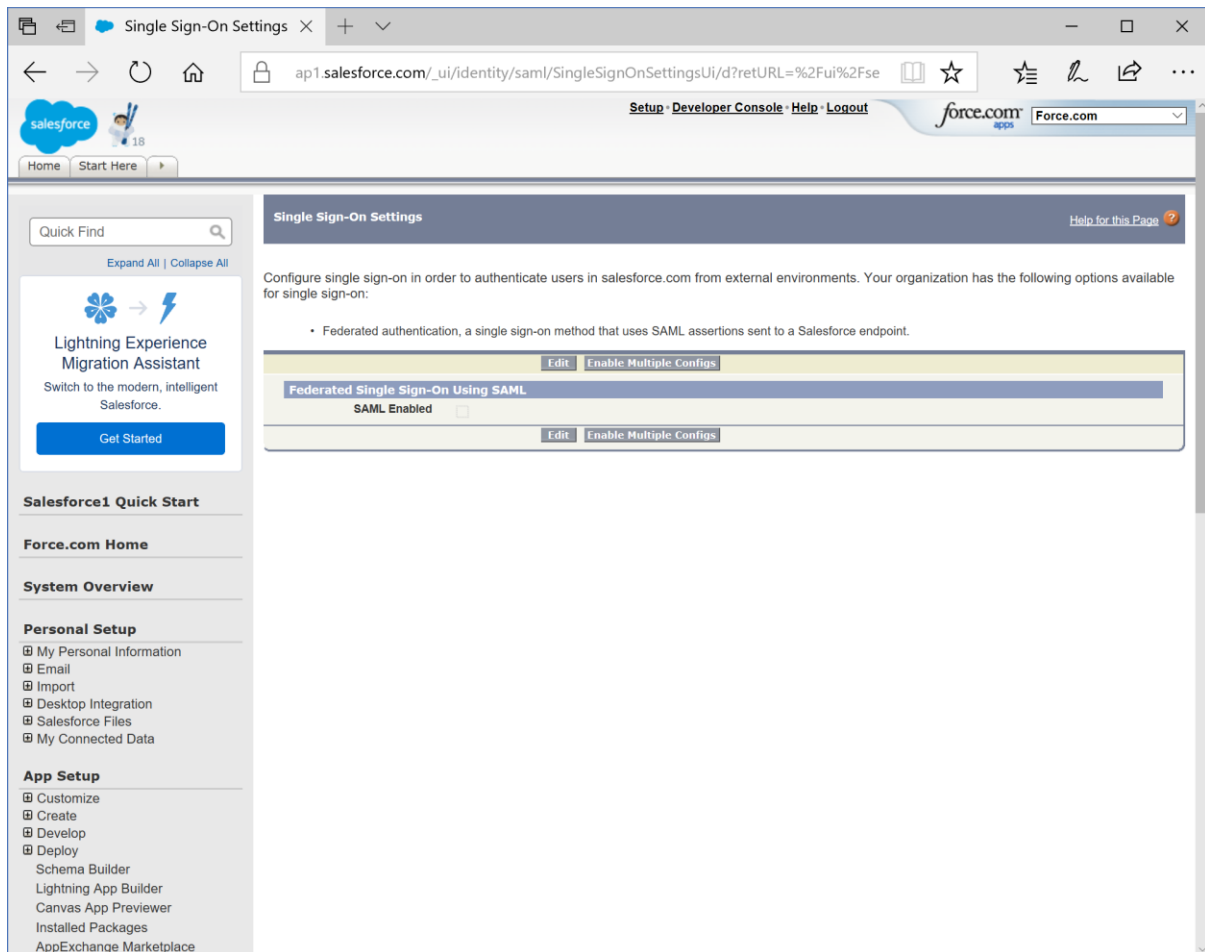
https://resources.docs.salesforce.com/208/latest/en-us/sfdc/pdf/salesforce_single_sign_on.pdf

Single Sign-On Settings

Log into Salesforce as an administrator.

<https://login.salesforce.com>

Select Setup > Administration Setup > Security Controls > Single Sign-On Settings.



Enable SAML and specify the identity provider's configuration.

The issuer is the name of the identity provider.

For example:

<https://ExampleIdentityProvider>

The identity provider Login URL is the SSO service that receives the SAML authn request as part of SP-initiated SSO.

For example:

<https://localhost:44313/SAML/SingleSignOnService>

The certificate is the identity provider certificate used to verify signatures.

For example:

idp.cer

The screenshot shows the Salesforce 'Single Sign-On Settings' page for 'Federated Single Sign-On Using SAML'. The page is titled 'Single Sign-On Settings' and includes a 'Help for this Page' link. The main configuration area is titled 'Federated Single Sign-On Using SAML' and contains the following settings:

- SAML Enabled:** ☒
- SAML Version:** 2.0
- Issuer:** https://ExampleIdentityPr
- Identity Provider Certificate:** Browse...
- Identity Provider Login URL:** https://localhost:44313/S/ (Note: If you remove the Login URL, you must enable Multiple SAML Configs to add one again.)
- Custom Error URL:**
- SAML Identity Type:** ☒ Assertion contains the User's Salesforce username; ☐ Assertion contains the Federation ID from the User object
- SAML Identity Location:** ☒ Identity is in the NameIdentifier element of the Subject statement; ☐ Identity is in an Attribute element
- Entity ID:** ☒ https://saml.salesforce.com; ☐ https://component-space-dev-ed.my.salesforce.com
- Service Provider Initiated Request Binding:** ☒ HTTP POST; ☐ HTTP Redirect
- User Provisioning Enabled:** ☐
- Current Certificate:** CN=www.idp.com, Expiration: 31 Dec 2049 14:00:00 GMT
- Custom Logout URL:**

The page also features a left sidebar with navigation links: 'Quick Find', 'Expand All | Collapse All', 'Lightning Experience Migration Assistant', 'Salesforce1 Quick Start', 'Force.com Home', 'System Overview', 'Personal Setup' (with links to My Personal Information, Email, Import, Desktop Integration, Salesforce Files, and My Connected Data), and 'App Setup' (with links to Customize, Create, Develop, Deploy, Schema Builder, Lightning App Builder, Canvas App Previewer, Installed Packages, and AppExchange Marketplace).

Save the changes.

ComponentSpace SAML for ASP.NET Salesforce Service Provider Integration Guide

The screenshot displays the 'Single Sign-On Settings' page in the Salesforce Developer Console. The page is titled 'Single Sign-On Settings' and includes a 'Help for this Page' link. It provides instructions on configuring single sign-on for external environments. A list of available options is shown, including 'Federated authentication, a single sign-on method that uses SAML assertions sent to a Salesforce endpoint.'

The 'Federated Single Sign-On Using SAML' section is expanded, showing a table of configuration details:

Federated Single Sign-On Using SAML	
SAML Enabled	☒
SAML Identity Type	Username
SAML Identity Location	Subject
Identity Provider Certificate	CN=www.idp.com Expiration: 31 Dec 2049 14:00:00 GMT
Identity Provider Login URL	https://localhost:44313/SAML/SingleSignOnService
Custom Logout URL	
Custom Error URL	
Salesforce Login URL	https://login.salesforce.com
OAuth 2.0 Token Endpoint	https://login.salesforce.com/services/oauth2/token
Entity ID	https://saml.salesforce.com
Service Provider Initiated Request Binding	HTTP POST

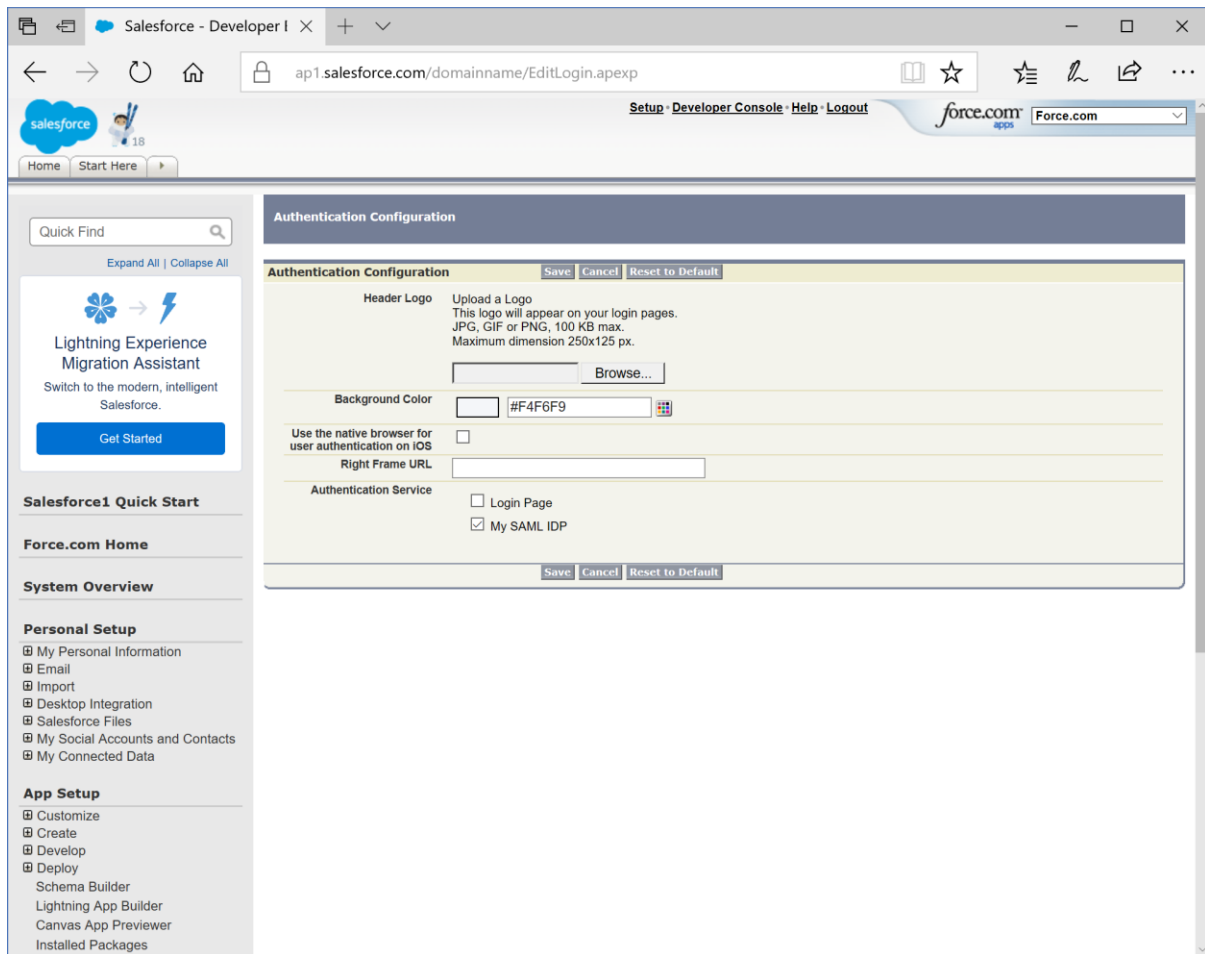
Buttons at the top of the table include 'Edit', 'Enable Multiple Configs', 'SAML Assertion Validator', and 'Download Metadata'. The 'Download Metadata' button is highlighted.

Download the metadata as this is used to configure the identity provider.

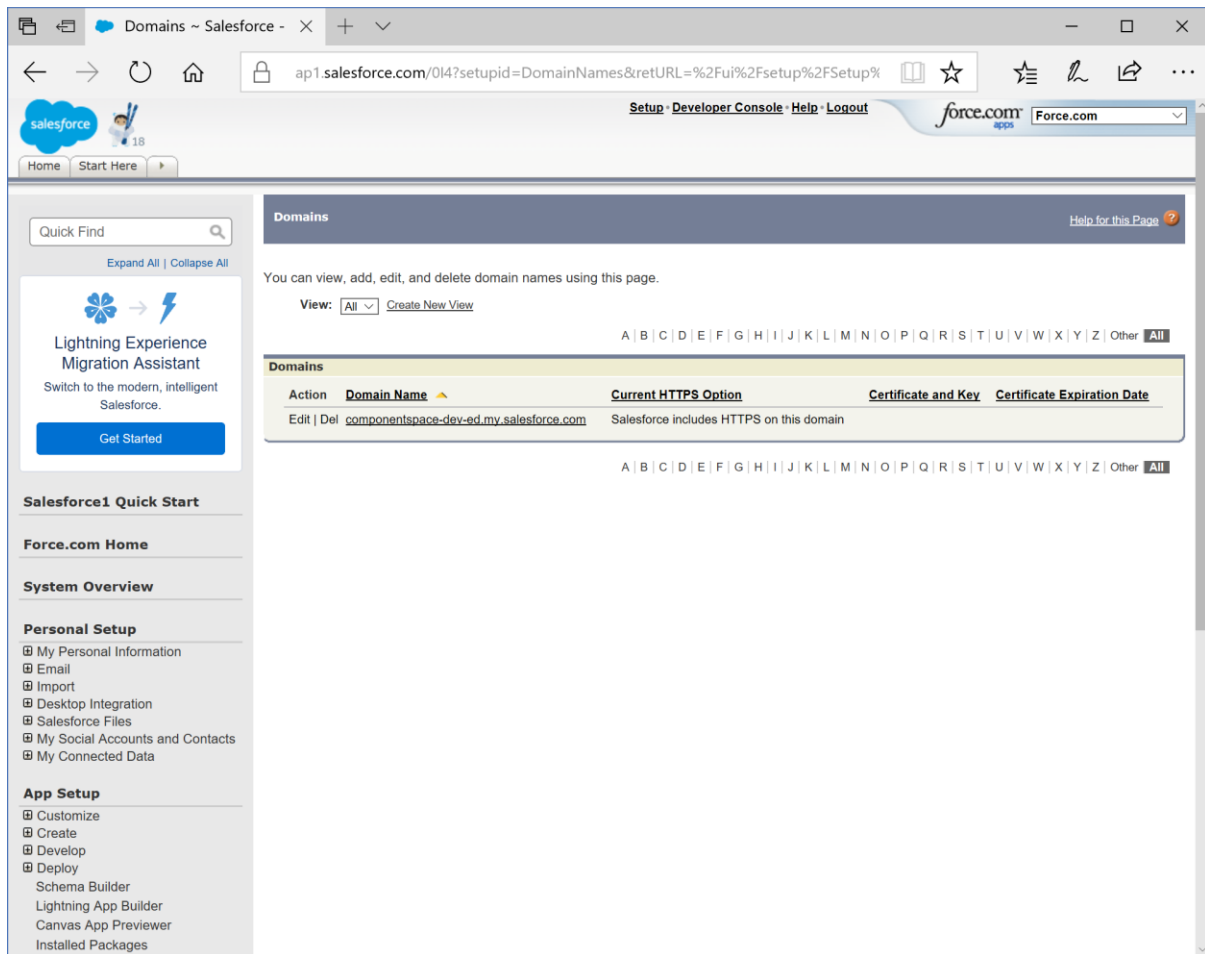
For SP-initiated SSO, select Setup > Domain Management > My Domain.

Ensure the Authentication Service is set to My SAML IDP.

ComponentSpace SAML for ASP.NET Salesforce Service Provider Integration Guide



Take note of the domain name.



Identity Provider Configuration

The following partner service provider configuration is included in the example identity provider's SAML configuration.

```
<PartnerServiceProvider
  Name="https://saml.salesforce.com"
  Description="Salesforce"
  WantAuthnRequestSigned="true"
  SignAssertion="true"
  AssertionConsumerServiceUrl="https://login.salesforce.com">
  <PartnerCertificates>
    <Certificate FileName="Certificates\salesforce.cer"/>
  </PartnerCertificates>
</PartnerServiceProvider>
```

Some of this information was extracted from the Salesforce SAML metadata.

The partner certificate file corresponds to the signing certificate included in the metadata.

Ensure the PartnerName specifies the correct partner service provider.

```
<add key="PartnerName" value="https://saml.salesforce.com"/>
```

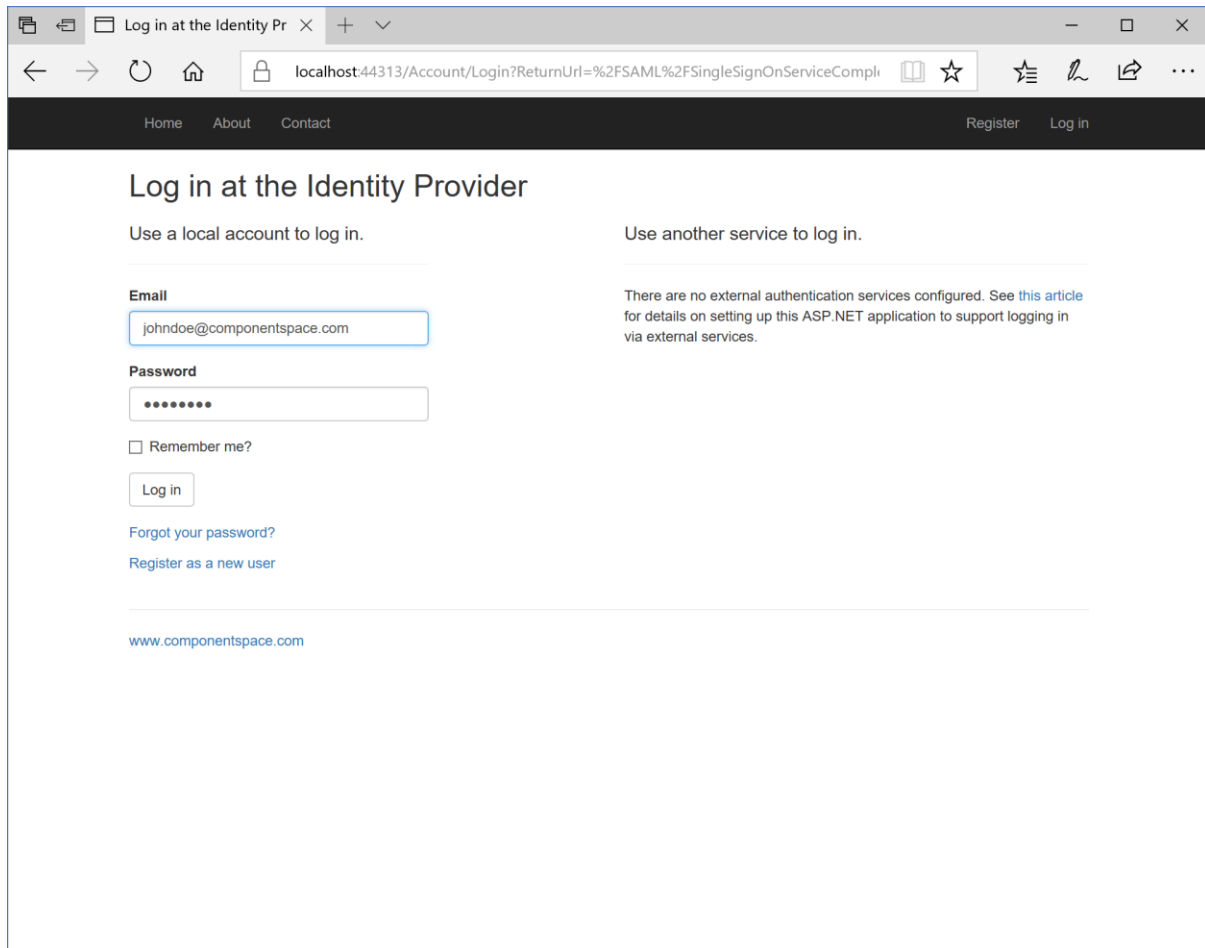
SP-Initiated SSO

Browse to domain URL.

For example:

<http://componentspace-dev-ed.my.salesforce.com/>

Log in at the example identity provider.



The screenshot shows a web browser window with the address bar displaying `localhost:44313/Account/Login?ReturnUrl=%2FSAML%2FSingleSignOnServiceCompl`. The page title is "Log in at the Identity Provider". The page is divided into two main sections: "Use a local account to log in." and "Use another service to log in.".

Under "Use a local account to log in.", there are two input fields: "Email" with the value `john.doe@componentspace.com` and "Password" with masked characters. Below these fields is a checkbox labeled "Remember me?" and a "Log in" button. There are also links for "Forgot your password?" and "Register as a new user".

Under "Use another service to log in.", there is a message: "There are no external authentication services configured. See [this article](#) for details on setting up this ASP.NET application to support logging in via external services."

At the bottom of the page, there is a link to www.componentspace.com.

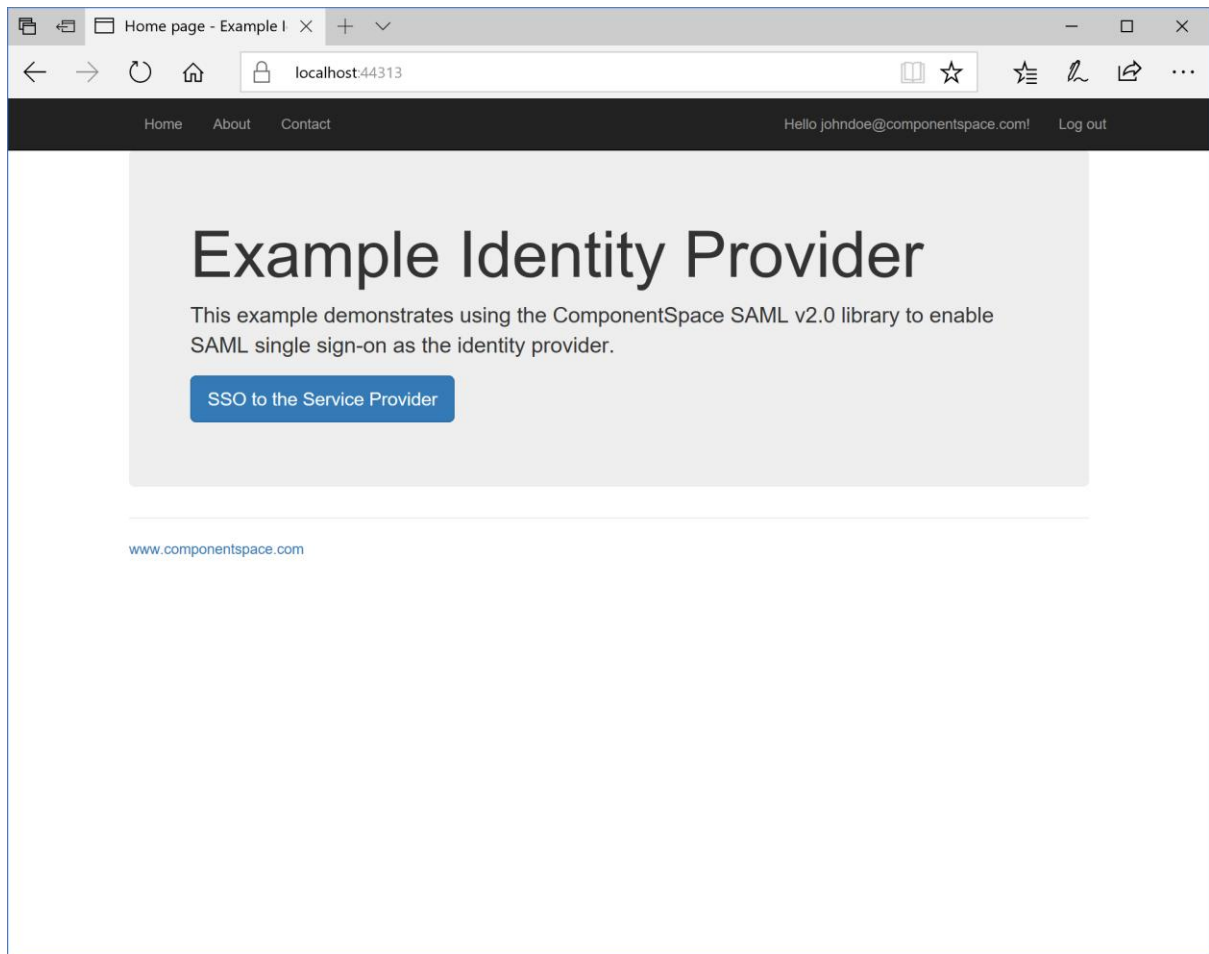
The user is automatically logged in at the service provider.

The screenshot shows the Salesforce 'Personal Information' settings page. The browser address bar displays 'ap1.lightning.force.com/one/one.app#/settings/personal/PersonalInformation/home'. The page features a left-hand navigation menu with options like 'My Personal Information', 'Advanced User Details', 'Approvers Settings', 'Change My Password', 'Connections', 'Grant Account Login Access', 'Language & Time Zone', 'Login History', 'Personal Information' (selected), 'Reset My Security Token', 'Security Central', 'Display & Layout', 'Email', 'Salesforce Files', 'Desktop Add-Ons', and 'Import'. The main content area is titled 'Personal Information' and includes a 'Help for this Page' link. It contains three sections: 'Details' (with fields for First Name, Last Name, Alias, Email, Username, Nickname, Phone, Extension, Fax, and Mobile), 'Address' (with fields for Street, City, State/Province, Zip/Postal Code, and Country), and 'My Work Information' (with fields for Company Name, Title, Department, Division, Employee Number, Start of Day, and End of Day). A red bar at the top of the 'Details' section indicates 'Required Information'.

IdP-Initiated SSO

Browse to the example identity provider and login.

Click the SSO to the Service Provider button.



The user is automatically logged in at the service provider.

The screenshot shows the Salesforce 'Personal Information' settings page. The browser address bar displays 'ap1.lightning.force.com/one/one.app#/settings/personal/PersonalInformation/home'. The left sidebar contains a 'Quick Find' search bar and a list of settings categories: 'My Personal Information' (expanded), 'Advanced User Details', 'Approver Settings', 'Change My Password', 'Connections', 'Grant Account Login Access', 'Language & Time Zone', 'Login History', 'Personal Information' (selected), 'Reset My Security Token', 'Security Central', 'Display & Layout', 'Email', 'Salesforce Files', 'Desktop Add-Ons', and 'Import'. The main content area is titled 'Personal Information' and includes a 'Help for this Page' link. It contains three sections: 'Details', 'Address', and 'My Work Information'. The 'Details' section has fields for First Name (John), Last Name (Doe), Alias (jdoe), Email (johndoe@componentspa), Username (johndoe@componentspace.com), Nickname (johndoe), Phone, Extension, Fax, and Mobile. The 'Address' section has fields for Street, City, State/Province, Zip/Postal Code, and Country. The 'My Work Information' section has fields for Company Name, Title, Department, Division, Employee Number, Start of Day (6:00 AM), and End of Day (11:00 PM). A red bar at the top of the 'Details' section indicates 'Required Information'.

Field	Value
First Name	John
Last Name	Doe
Alias	jdoe
Email	johndoe@componentspa
Username	johndoe@componentspace.com
Nickname	johndoe
Phone	
Extension	
Fax	
Mobile	

Field	Value
Street	
City	
State/Province	
Zip/Postal Code	
Country	

Field	Value
Company Name	
Title	
Department	
Division	
Employee Number	
Start of Day	6:00 AM
End of Day	11:00 PM

SAML Logout

Salesforce doesn't support SAML logout.