

Configuring Salesforce

Complete the following steps to configure Salesforce:

- **Step 1A:** Download the SP metadata only (If IDP configuration already exists) OR
- **Step 1B:** Create IDP configuration and Download the metadata
- **Step 2:** Update the IDP configuration

Step 1A: Download metadata for existing IdP configuration

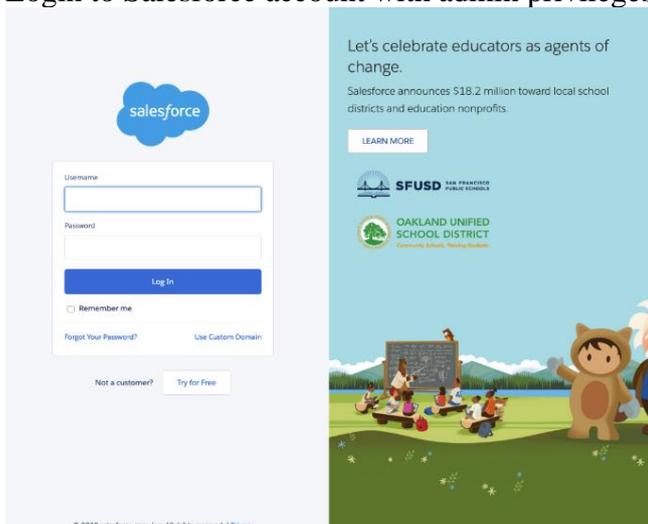
If you already have an IdP configuration set up, then use the below procedure to download the metadata for IdP:

Prerequisites

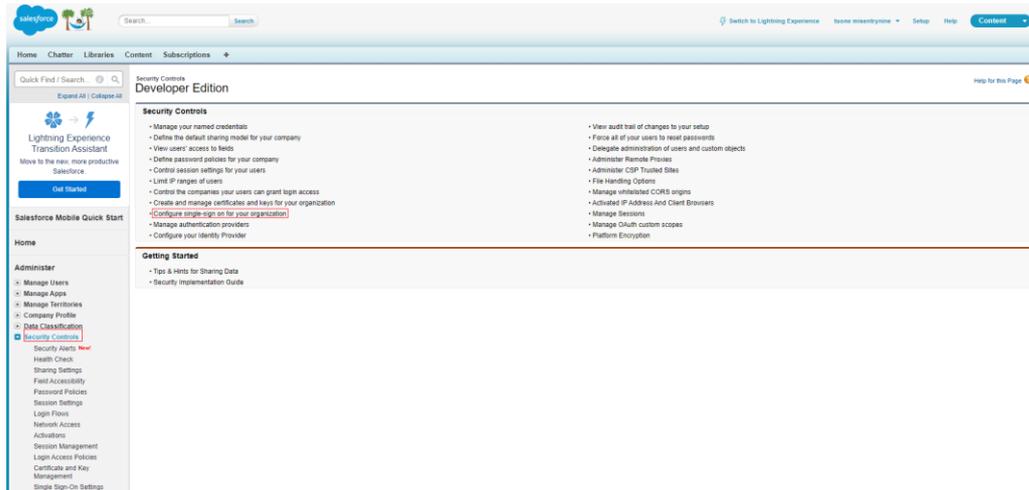
- Ensure that the IdP configuration is existing; else follow **Step 1B**.
- Ensure that you are in the classic view for Salesforce.

Procedure

1. Login to Salesforce account with admin privileges.



2. Under **Administer**, click **Security Controls** > **Configure single-sign on for your organization**.



3. On the **Single Sign-On Settings** page, click on the IdP name to view the configuration.

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:

- Federated authentication, a single sign-on method that uses SAML assertions sent to a Salesforce endpoint.

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

Federated Single Sign-On Using SAML

SAML Enabled

SAML Single Sign-On Settings

[New](#) [New from Metadata File](#) [New from Metadata URL](#)

Action	Name	SAML Version	Issuer	Entity ID
Edit Del	[Redacted]	2.0	[Redacted]	[Redacted]
Edit Del	[Redacted]	2.0	[Redacted]	[Redacted]
Edit Del	[Redacted]	2.0	[Redacted]	[Redacted]
Edit Del	[Redacted]	2.0	[Redacted]	[Redacted]
Edit Del	adfs	2.0	http://adfs.[Redacted]/adfs/services/trust	[Redacted]
Edit Del	[Redacted]	2.0	[Redacted]	[Redacted]

4. Click **Download Metadata** and save the file as "sp-metadata.xml".

SAML Single Sign-On Settings

[Back to Single Sign-On Settings](#)

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

Name	adfs	API Name	adfs
SAML Version	2.0	Entity ID	https://[Redacted].my.salesforce.com
Issuer	http://adfs.[Redacted].com/adfs/services/trust		
Identity Provider Certificate	CN=ADFS Signing - adfs.[Redacted].com Expiration: 4 Oct 2020 04:50:37 GMT		
Request Signing Certificate	SelfSignedCert_24Sep2019_230626		
Request Signature Method	RSA-SHA256		
Assertion Decryption Certificate	Assertion not encrypted		
SAML Identity Type	Username		
SAML Identity Location	Subject		
Service Provider Initiated Request Binding	HTTP POST		
Identity Provider Login URL	https://adfs.[Redacted].com/adfs/ls/		
Custom Logout URL			
Custom Error URL			
Single Logout Enabled	<input checked="" type="checkbox"/>		
Identity Provider Single Logout URL	https://adfs.[Redacted].com/adfs/ls/		
Single Logout Request Binding	HTTP Redirect		

Just-in-time User Provisioning

User Provisioning Enabled

Endpoints

View SAML endpoints for your organization, communities, or custom domains.

Your Organization

Login URL	https://[Redacted].salesforce.com/?so=00D0b000000vMGs
Logout URL	https://[Redacted].my.salesforce.com/services/auth/psam2/logout
OAuth 2.0 Token Endpoint	https://[Redacted].my.salesforce.com/services/oauth2/token?so=00D0b000000vMGs

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

Step 1B: Creating IDP configuration and download the metadata

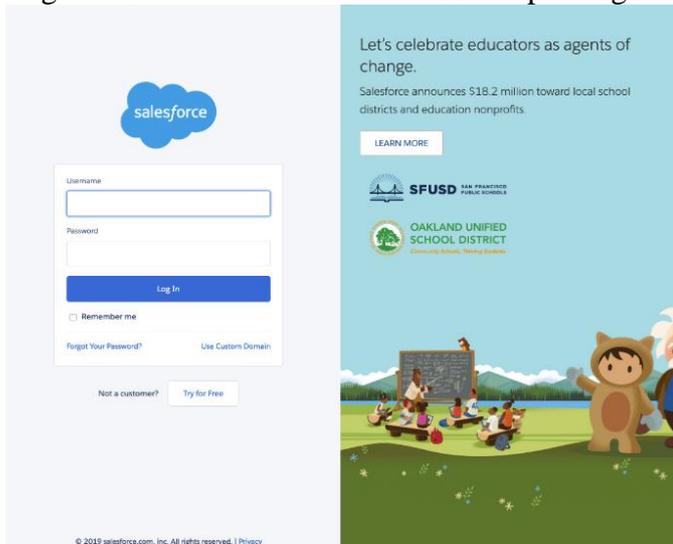
If you do not have the IdP configuration created, then follow the below procedure to add an IdP configuration and then download the metadata file:

Prerequisites

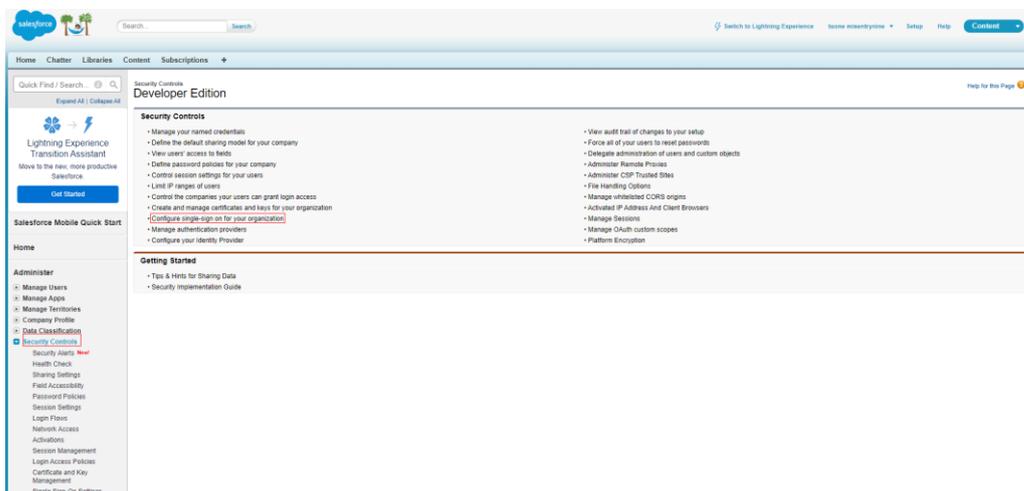
- You must have a Salesforce account with admin privileges.

Procedure

1. Login to Salesforce account with admin privileges.



2. Under **Administer**, click **Security Controls** > **Configure single-sign on for your organization**.



3. On the Single-sign on settings page, click **New from Metadata File**.

Single Sign-On Settings

Help for this Page

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:

- Federated authentication, a single sign-on method that uses SAML assertions sent to a Salesforce endpoint.

Edit SAML Assertion Validator

Federated Single Sign-On Using SAML

SAML Enabled

Action	Name	SAML Version	Issuer	Entity ID
Edit Del		2.0		
Edit Del		2.0		
Edit Del		2.0		
Edit Del		2.0		

- On the **SAML single sign-on settings** page, click **Choose File** and upload the "**idp-metadata.xml**" downloaded when creating an application in IdP. Click **Create**. The settings for single-sign on displays.

SAML Single Sign-On Settings

Create configuration using an XML file (1 MB or smaller) containing SAML 2.0 settings from your identity provider. (Salesforce doesn't store this file.)

Create Cancel

Metadata File **Choose File** No file chosen

Create Cancel

- On the **SAML single-sign on settings** page, provide the configuration in the following fields:

- Name
- API Name
- Select **HTTP POST** in "**Service Provider Initiated Request Binding**".
- Click **Save**.

SAML Single Sign-On Settings

Help for this Page

Save Save & New Cancel

Name

SAML Version 2.0

Issuer

Identity Provider Certificate **Choose File** No file chosen

Request Signing Certificate

Request Signature Method

Assertion Decryption Certificate

SAML Identity Type Assertion contains the User's Salesforce 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

Warning: The metadata file specifies multiple bindings for the login URL.

Identity Provider Login URL

Custom Logout URL

Custom Error URL

Single Logout Enabled

Identity Provider Single Logout URL

Single Logout Request Binding HTTP POST
 HTTP Redirect

Warning: The metadata file specifies multiple bindings for the single logout URL.

Just-in-time User Provisioning

User Provisioning Enabled

Save Save & New Cancel

- The configuration is complete. Click **Download Metadata** and save the file as "**sp-metadata.xml**".

SAML Single Sign-On Settings

[Back to Single Sign-On Settings](#)

		Edit	Delete	Clone	Download Metadata	SAML Assertion Validator	
Name	adfs					API Name	adfs
SAML Version	2.0					Entity ID	https://[redacted].my.salesforce.com
Issuer	http://adfs.[redacted].com/adfs/services/trust						
Identity Provider Certificate	CN=ADFS Signing - adfs.[redacted].com Expiration: 4 Oct 2020 04:50:37 GMT						
Request Signing Certificate	SelfSignedCert_24Sep2019_230626						
Request Signature Method	RSA-SHA256						
Assertion Decryption Certificate	Assertion not encrypted						
SAML Identity Type	Username						
SAML Identity Location	Subject						
Service Provider Initiated Request Binding	HTTP POST						
Identity Provider Login URL	https://adfs.[redacted].com/adfs/ls/						
Custom Logout URL							
Custom Error URL							
Single Logout Enabled	<input checked="" type="checkbox"/>						
Identity Provider Single Logout URL	https://adfs.[redacted].com/adfs/ls/						
Single Logout Request Binding	HTTP Redirect						

Just-in-time User Provisioning

User Provisioning Enabled

Endpoints

View SAML endpoints for your organization, communities, or custom domains.

Your Organization

Login URL	https://[redacted].salesforce.com?so=00D0b000000vMGs
Logout URL	https://[redacted].my.salesforce.com/services/auth/sp/saml2/logout
OAuth 2.0 Token Endpoint	https://[redacted].my.salesforce.com/services/oauth2/token?so=00D0b000000vMGs

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

Next Steps: [Create a Federated Pair in Access](#). For more information, see [Overview](#).

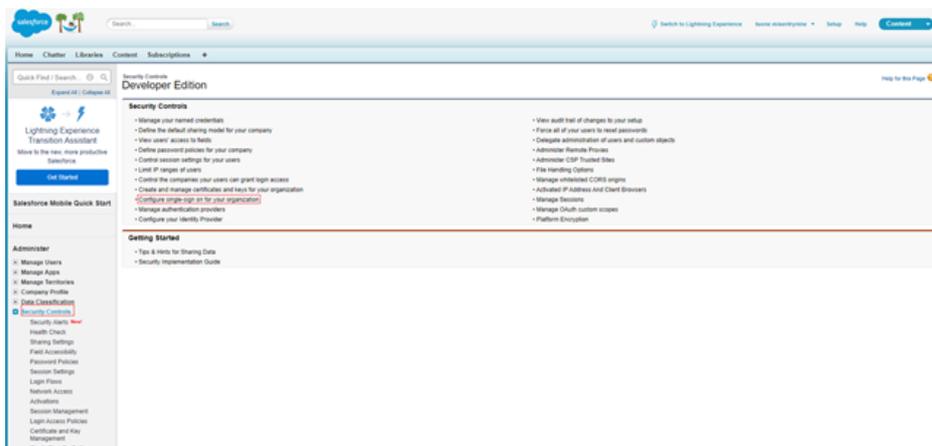
Step 2: Updating IdP configuration

Prerequisites

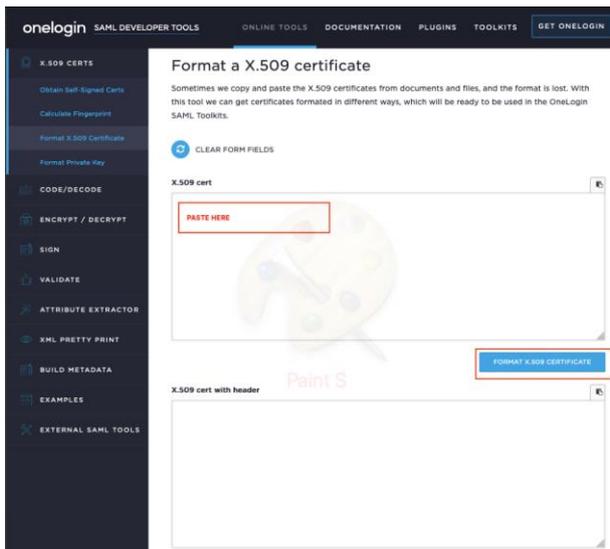
- The IdP configuration is updated after creating a federated pair in MobileIron Access. You must download the proxy metadata files from Access.

Procedure

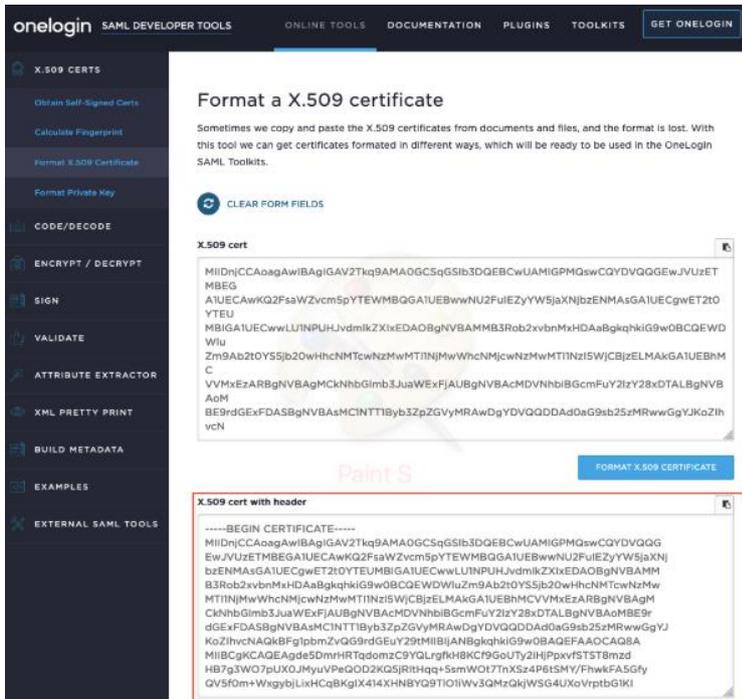
- Login to Salesforce account with admin privileges.
- Under **Administer**, click **Security Controls** > **Configure single-sign on for your organization**.



- On the **Single Sign-On Settings** page, click on the IdP name to view the configuration.



- e. Copy the value in "X.509 cert with header" text area after formatting.
- f. Open a text editor and paste the value in a new text file.
- g. Save the file as "**access-idp-certificate.crt**".



5. In **Salesforce**, on **Edit SAML Sign on Settings page**, do the following:

- a. Copy "**entityId**" attribute value from "EntityDescriptor" Element from "**access-idp-metadata.xml**" and paste in the "issuer" text box.
- b. Copy "**Location**" attribute value from "**SingleSignOnService**" Element from "access-idp-metadata.xml" and paste in the "Identity Provider Login URL" text box.
- c. Copy "**Location**" attribute value from "**SingleLogoutService**" Element from "**access-idp-metadata.xml**" and paste in "Identity Provider Single Logout URL" text box.
- d. Click on "**Browse**" in the "Identity Provider Certificate" to open a file upload

dialog. Upload "access-idp-certificate.crt" formatted in above step.
e. Click **Save**.

The screenshot displays the 'SAML Single Sign-On Settings' configuration page in Salesforce. The page is divided into several sections: 'General Information', 'Certificates', 'SAML Configuration', 'Service Provider Initiated', and 'Just-in-time User Provisioning'. The 'General Information' section includes fields for Name (IDP), API Name (IDP), SAML Version (2.0), and Entity ID (https://app.onelogin.com/s). The 'Certificates' section shows the Identity Provider Certificate (https://app.onelogin.com/s) and the Request Signing Certificate (SetSignedCert_24Sep2019_230E28). The 'SAML Configuration' section includes SAML Identity Type (Assertion contains the User's Salesforce username), SAML Identity Location (Identity is in the NameIdentifier element of the Subject statement), and Service Provider Initiated (HTTP POST). The 'Service Provider Initiated' section includes Identity Provider Login URL (https://m01/saml2/http-post/iss/993972) and Single Logout Enabled (checked). The 'Just-in-time User Provisioning' section includes a checkbox for User Provisioning Enabled. The page also features a 'Paint S' watermark over the Identity Provider Login URL field.

Updating IDP Configuration in Salesforce can be error prone if copy/paste is required.

Alternative is to create another entry in Salesforce 'Single-Sign-on Settings' by uploading the proxy-metadata file from Access and using the new entry in Domain Management in My Domain.

Procedure

1. Click Administer > Domain Management > My domain.
2. Edit Authentication configuration.
3. Enable the authentication service.
4. Click save.

This enables the service with Salesforce domain.