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

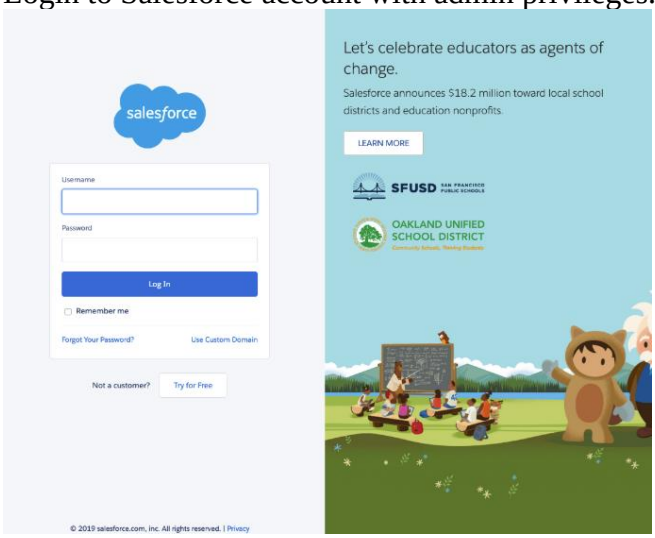
If you already have an IdP configuration set up, then use the below procedure to download the metadata for IdP:

Prerequisites

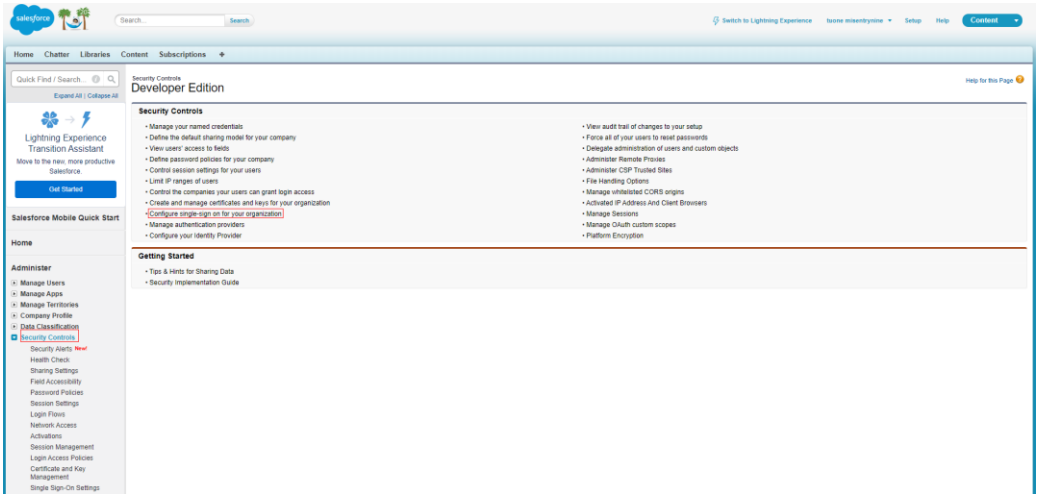
- Ensure that the IdP configuration is existing; else follow **Step 1B**.
- Ensure that you are in the classic view for Salesforce.

Procedure

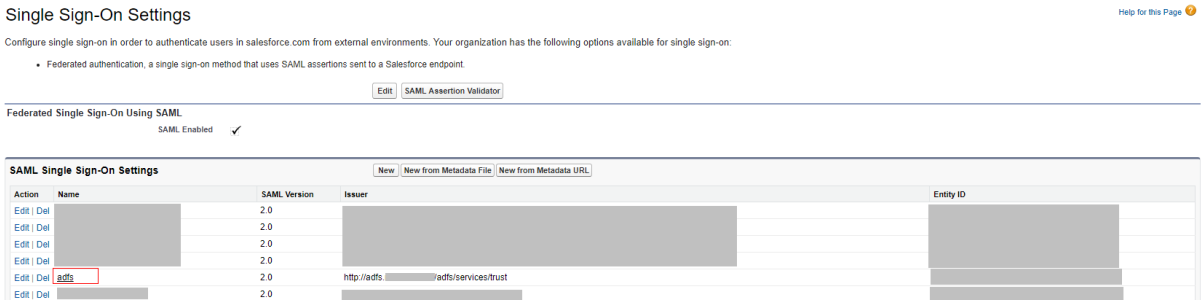
1. Login to Salesforce account with admin privileges.



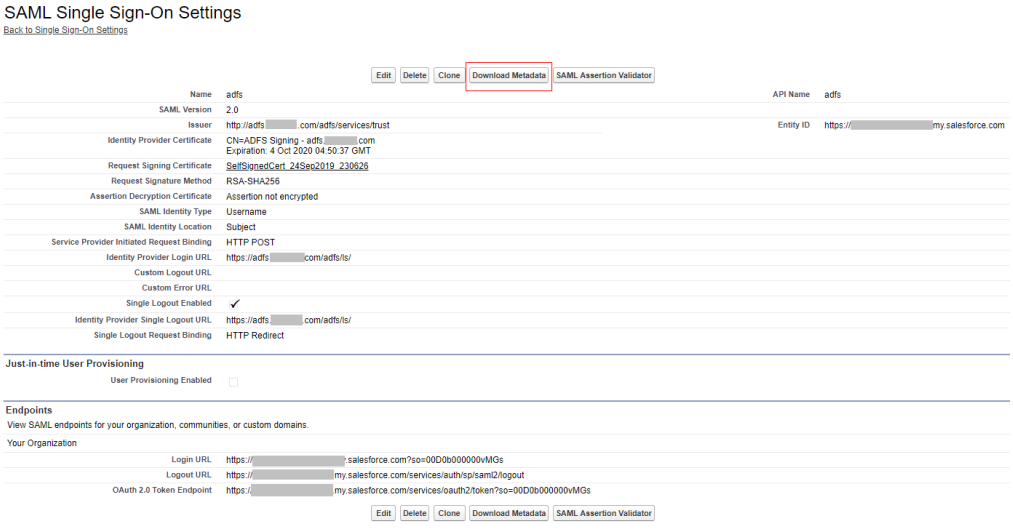
2. Under **Administer**, click **Security Controls** > **Configure single-sign on for your organization**.



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



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



Step 1B: Creating IDP configuration and download the metadata

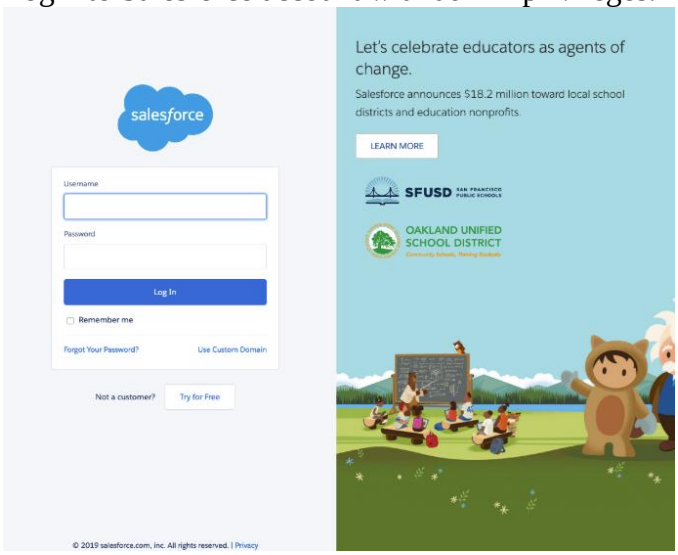
If you do not have the IdP configuration created, then follow the below procedure to add an IdP configuration and then download the metadata file:

Prerequisites

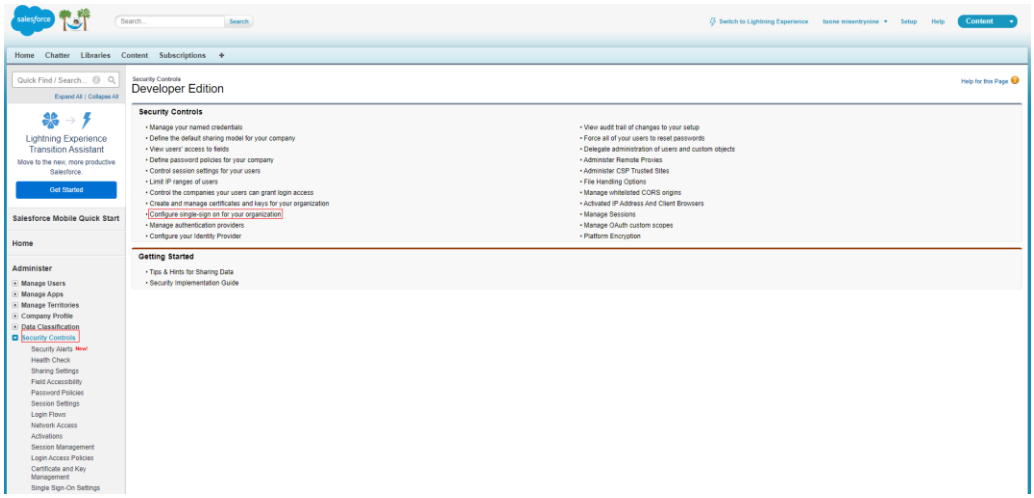
- You must have a Salesforce account with admin privileges.

Procedure

1. Login to Salesforce account with admin privileges.

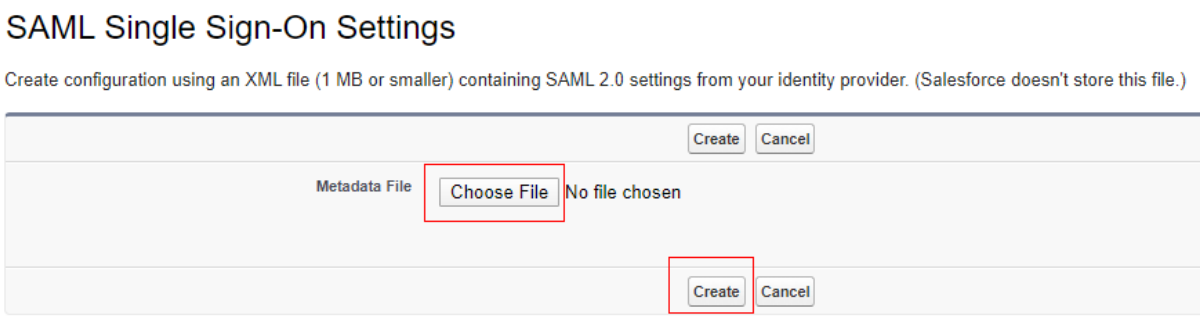


2. Under **Administer**, click **Security Controls** > **Configure single-sign on for your organization**.



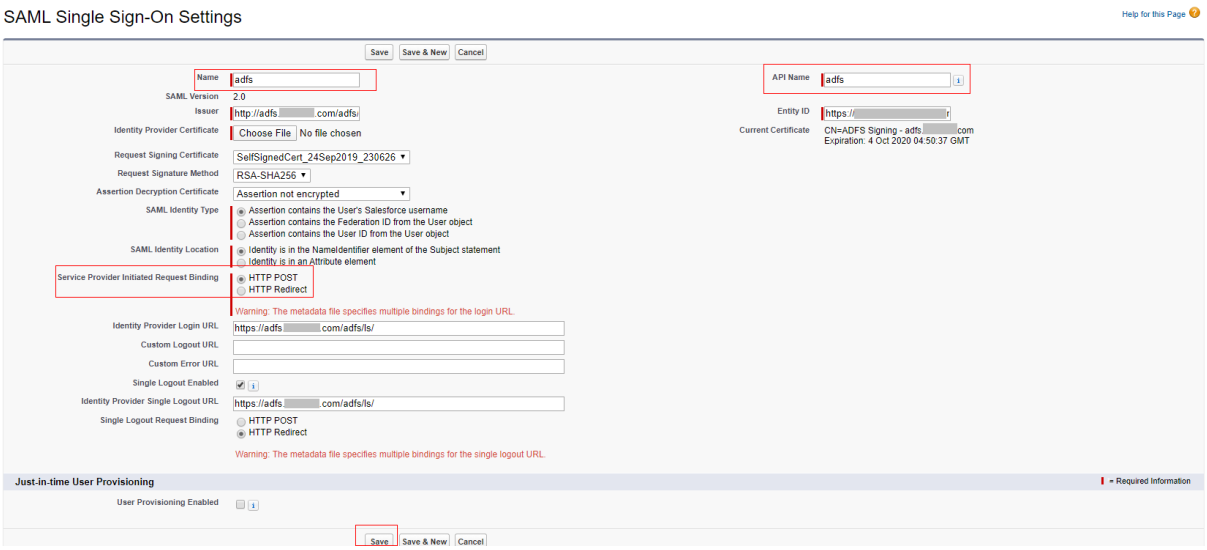
3. On the Single-sign on settings page, click **New from Metadata File**.

4. 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.

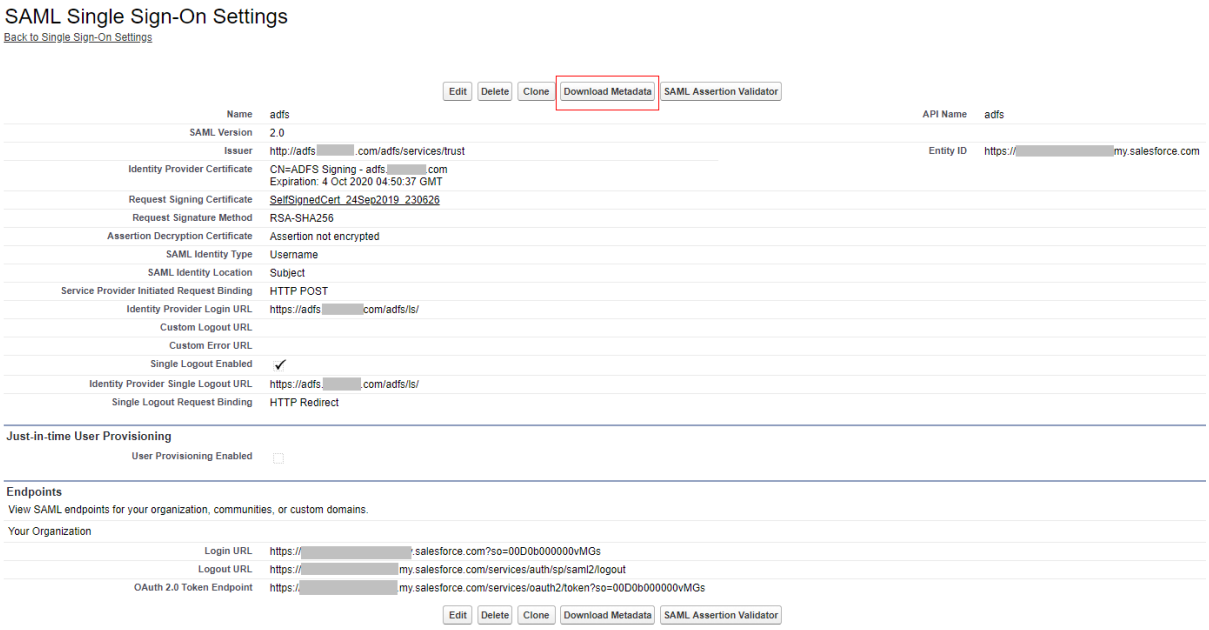


5. On the **SAML single-sign on settings** page, provide the configuration in the following fields:

a. Name
b. API Name
c. Select **HTTP POST** in "**Service Provider Initiated Request Binding**".
d. Click **Save**.



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



Next Steps: Create a Federated Pair in Access. For more information, see Overview.

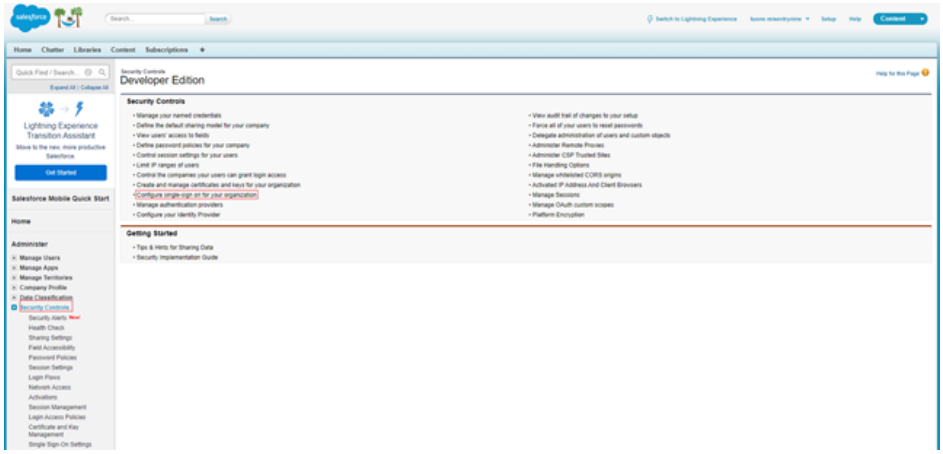
Step 2: Updating IdP configuration

Prerequisites

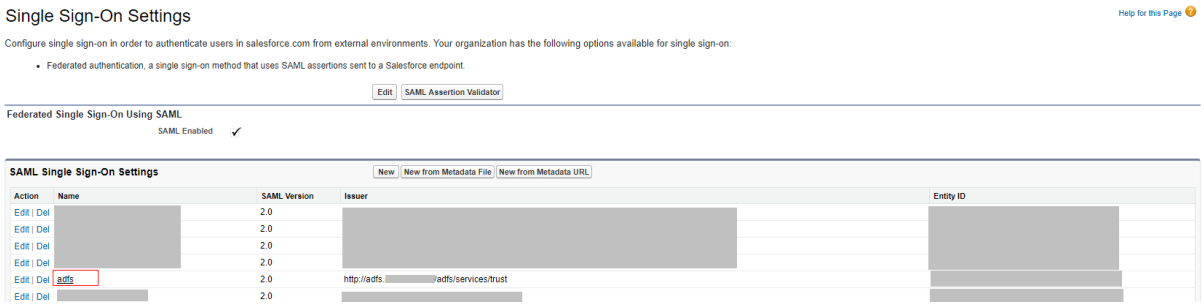
- The IdP configuration is updated after creating a federated pair in MobileIron Access. You must download the proxy metadata files from Access.

Procedure

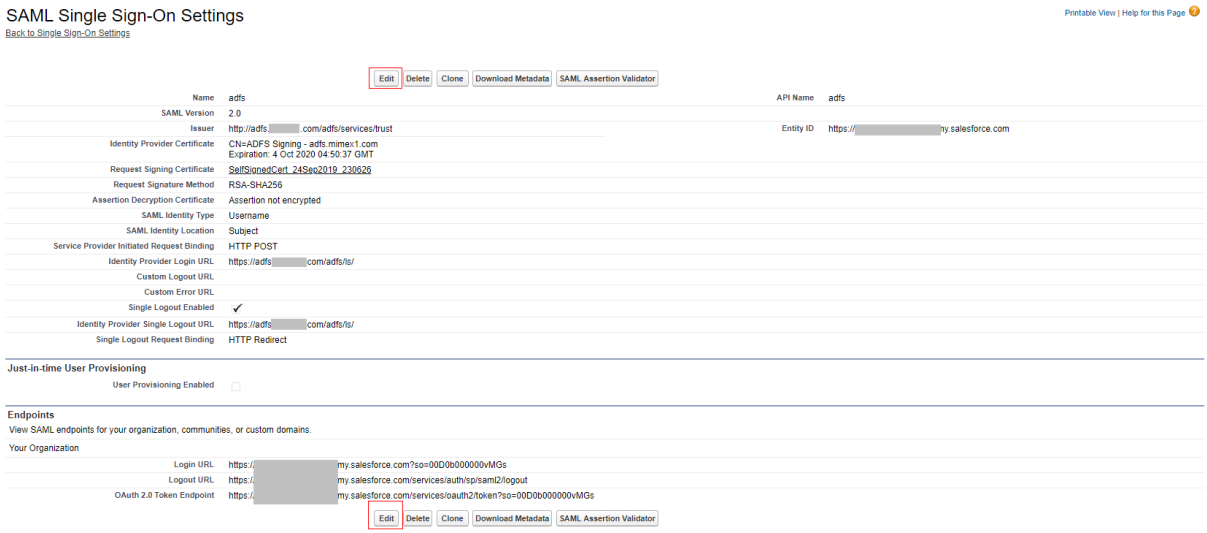
1. Login to Salesforce account with admin privileges.
2. Under **Administer**, click **Security Controls** > **Configure single-sign on for your organization**.



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

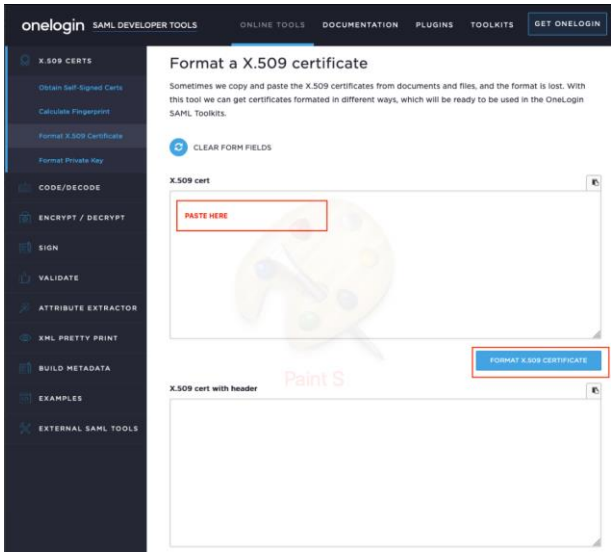


4. Click **Edit** in the configuration page.

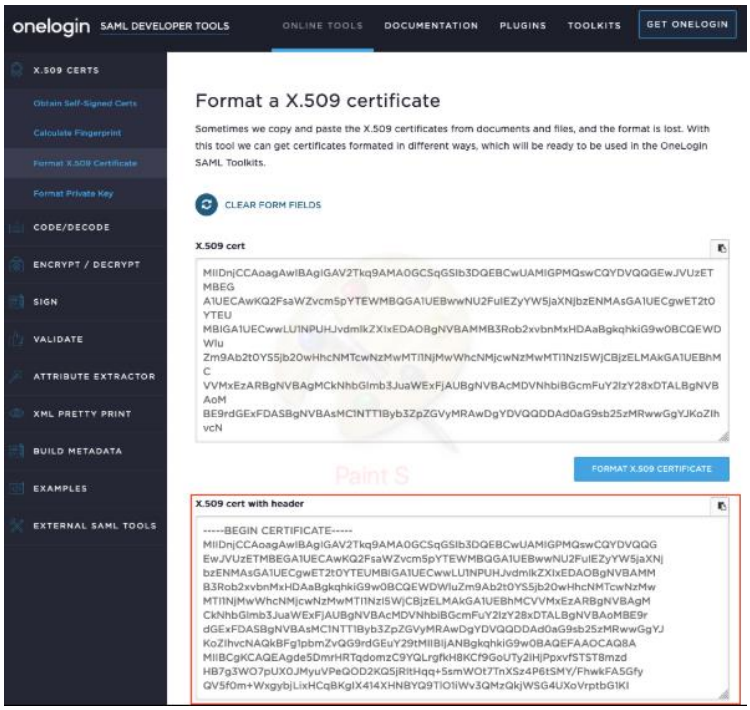


a. Open the "**Access IDP Metadata**" in a viewer that is available in MobileIron Access after creating a federated pair.

b. Copy "X.509Certificate" value.
c. Open the certificate format site and paste the "X.509 cert" in the text area: https://www.samltool.com/format_x509cert.php
d. Click "Format X.509 Certificate".



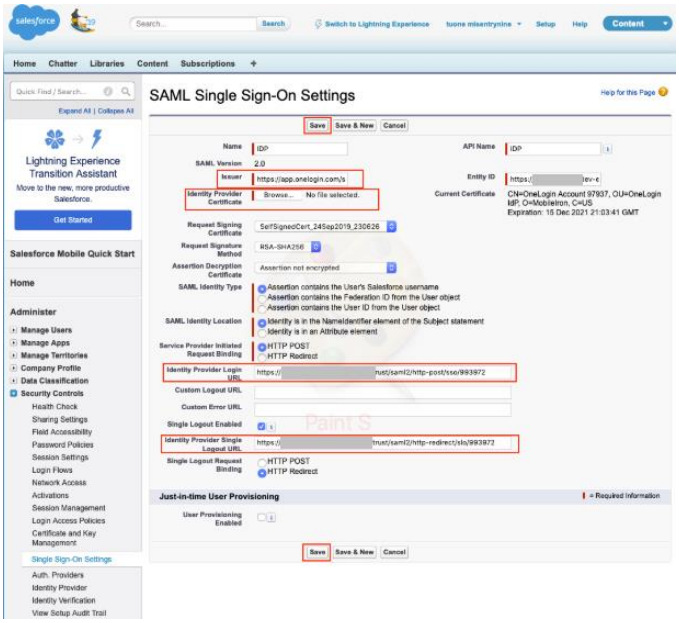
e. Copy the value in "X.509 cert with header" text area after formatting.
f. Open a text editor and paste the value in a new text file.
g. Save the file as "**access-idp-certificate.crt**".



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**.



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.