SETUP GUIDE FOR SAML IDP PLUGIN

STEP 1: Get the following information from the Service Provider (SP):

1. *SP Entity ID / Issuer*
2. *ACS URL (Assertion Consumer Service URL)*
3. *NameID Format*
4. *Single Logout URL*
5. *Single Logout Binding Type : HTTP-POST or HTTP-REDIRECT*
6. *Attributes which the Service Provider needs in the SAML response*
7. *Does the Service Provider send signed AuthnRequest? If yes, then get the X.509 Certificate for validating the signed Request.*
8. *Does the Service Provider need the Response Signed?*
9. *Does the Service Provider need the Assertion Signed?*
10. *Does the Service Provider need the Encrypted Assertion? If yes, then get the X.509 certificate for encryption.*

STEP 2: After you have all the information from STEP 1 go to ***Identity Provider*** tab in the plugin and enter the following values:

- **Service Provider Name** : Of your choosing.
- **SP Entity ID or Issuer** : SP Entity ID from STEP 1.
- **ACS URL** : ACS URL from STEP 1.
- **Single Logout URL** : Enter the Single Logout URL of the SP.
- **X.509 Certificate (optional) [For Signed Request]** : Paste X.509 Certificate from STEP 1 for Signed Request.
- **NameID Format** : Select NameID format as mentioned by your SP in STEP 1.
- **Response Signed** : Check if the SP needs a signed Response.
- **Assertion Signed** : Check if the SP needs a signed Assertion.
- **Encrypted Assertion** : Check if the SP needs an encrypted Assertion.

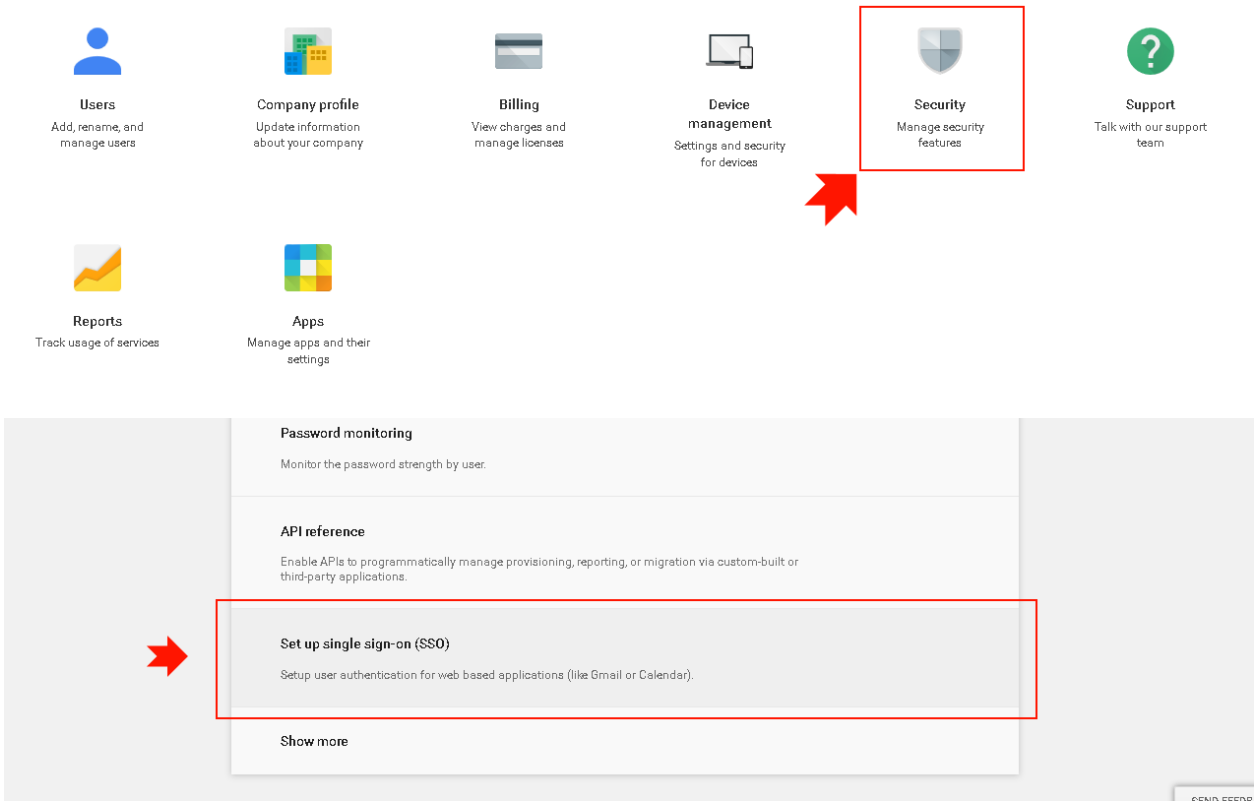
Click on ***Save*** to save your settings.

STEP 3: There are two ways to setup the SP. You can either import the metadata file of the IdP or provide individual values required by the SP from your Identity Provider (plugin). You can find both under the ***Service Provider Tab*** in the plugin.

For example:

Here is an example of setting up Google Apps as a Service Provider:

1. Log in to your Google App's Admin Console.
2. Go to ***Security Settings***.
3. Under Security Settings go to ***Setup up single sign-on (SSO)*** settings.

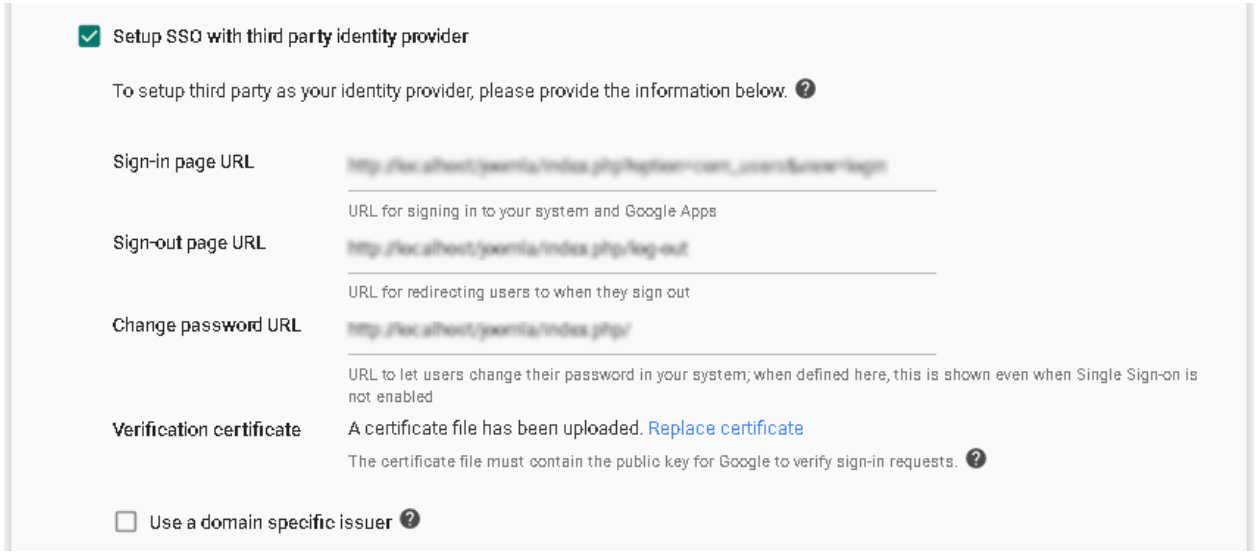


4. You will need to provide the following information in google apps from the plugin's ***Service Provider Tab*** under the *Setup SSO with Third party identity Provider* Section:

   a. **Sign-in page URL** : **SAML Login URL** from the Service Provider Tab.

   b. **Sign-out page URL** : **SAML Logout URL** from the Service Provider Tab.

   c. **Verification Certificate** : Upload the **certificate** from the Service Provider Tab



5. Configure the following settings in the plugin's ***Identity Provider Tab*** :

   a. **Service Provider Name** : GoogleApps

   b. **SP Entity ID or Issuer** : google.com

   c. **ACS URL** : https://www.google.com/a/<domain-name>/acs

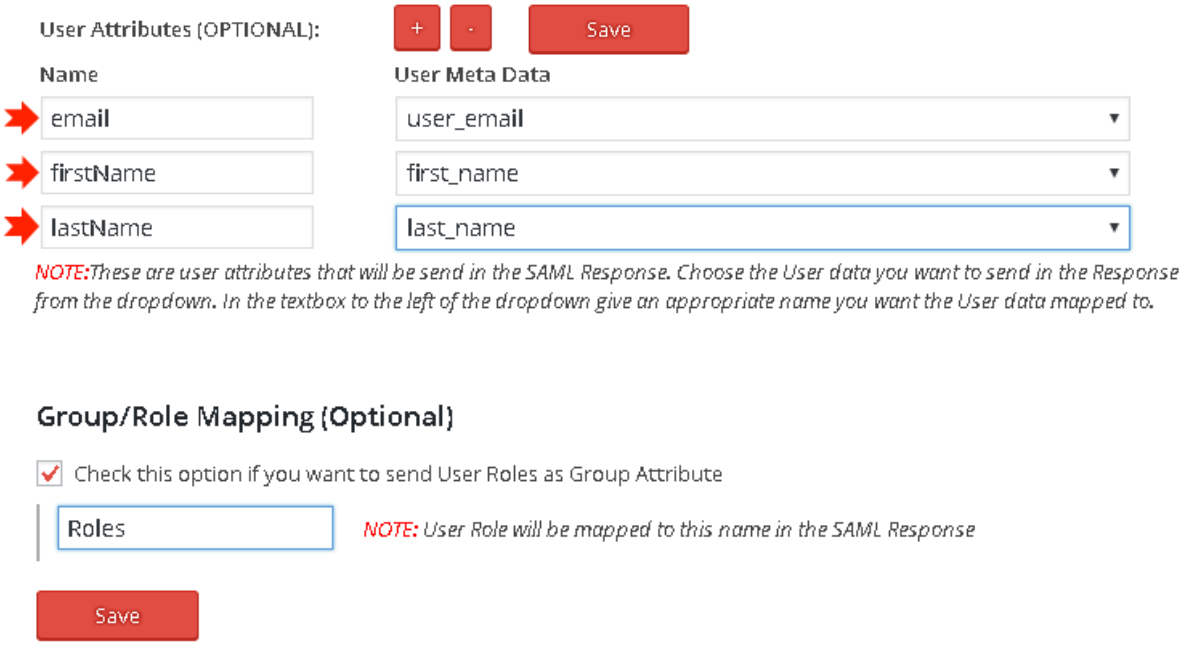
   d. **Response Signed** : Checked

e. **NameID Format** : urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress

f. **Default Relay State** : Google App URL

Example: https://mail.google.com/mail/u/ for Gmail

STEP 4: If your Service Provider needs extra user attributes or custom attributes to be sent in the SAML response then you can configure this under the ***Attribute/Role Mapping Tab.***



STEP 5: Once you have completed STEPs 1-4 then you can test your settings by using the Test Button/Link under the ***Identity Provider Tab***.