2. SimpleSAMLphp and G Suite for Education

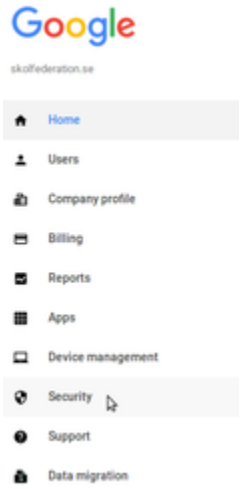
2. SimpleSAMLphp and G Suite for Education

Introduction

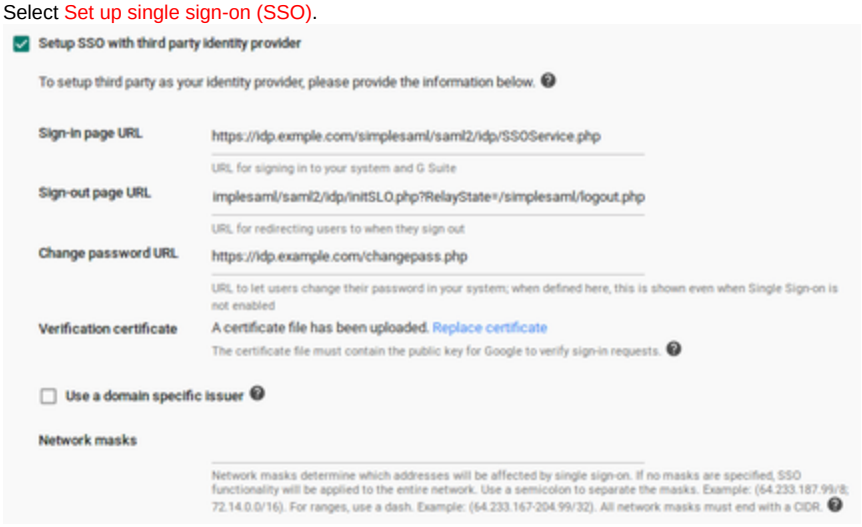
This guide describes how to enable Single Sign-On for G Suite for Education (G Suite) using simpleSAMLphp as the identity provider (IdP). G Suite is not part of the federation. The G Suite's metadata must be known to the IdP and vice versa, the G Suite SP must now the IdP metadata.

Configure G Suite for Education

Log in to the Admin console and then select Security.



Select Set up single sign-on (SSO).



Sign-in page URL

Change the hostname idp.example.com to the hostname of your IdP. https://idp.exmple.com/simplesaml/saml2/idp/SSOService.php

Sign-out page URL

Change the hostname idp.example.com to the hostname of your IdP. The RelayState parameter is the address that the browser will be redirected to after logout. https://idp.example.com/simplesaml/saml2/idp/initSLO.php?RelayState=/simplesaml/logout.php

Verification certificate

Upload the certificate that are used by the IdP (/var/simplesamlphp/cert/server.crt).

Add G Suite's SP metadata to SimpleSAMLphp

In the file metadata/saml20-sp-remote.php there should be an example configuration for G Suite.
$metadata['google.com'] = array(
'AssertionConsumerService' =>'https://www.google.com/a/g.feide.no /acs',
'NameIDFormat' => 'rn:oasis:names:tc:SAML:2.0:nameid-format:emailAddress',
'simplesaml.nameidattribute' => 'uid',
'simplesaml.attributes' => FALSE,
);

AssertionConsumerService

Change the domainname g.feide.se to the domain used in G Suite.

simplesaml.nameidattribute

The Google Accounts username is sent in the SAML response in the XML element NameID. G Suite parses the NameID, and expects that this element either contains a G Suite username or a full G Suite email address. In the example NameID is set to the attribute uid