

2. SimpleSAMLphp and G Suite for Education

2. SimpleSAMLphp and G Suite for Education

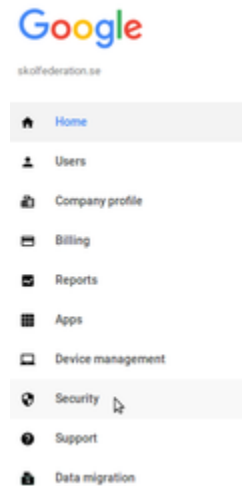
- [Configure G Suite for Education](#)
 - [Sign-in page URL](#)
 - [Sign-out page URL](#)
 - [Verification certificate](#)
- [Add G Suite's SP metadata to SimpleSAMLphp](#)
 - [AssertionConsumerService](#)
 - [simplesaml.nameidattribute](#)

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)**.

☒ **Setup SSO with third party identity provider**

To setup third party as your identity provider, please provide the information below. ⓘ

Sign-in page URL	<input type="text" value="https://idp.example.com/simplesaml/saml2/idp/SSOService.php"/> <small>URL for signing in to your system and G Suite</small>
Sign-out page URL	<input type="text" value="simplesaml/saml2/idp/initSLO.php?RelayState*/simplesaml/logout.php"/> <small>URL for redirecting users to when they sign out</small>
Change password URL	<input type="text" value="https://idp.example.com/changepass.php"/> <small>URL to let users change their password in your system; when defined here, this is shown even when Single Sign-on is not enabled</small>
Verification certificate	A certificate file has been uploaded. Replace certificate <small>The certificate file must contain the public key for Google to verify sign-in requests. ⓘ</small>

☐ **Use a domain specific issuer** ⓘ

Network masks

Network masks determine which addresses will be affected by single sign-on. If no masks are specified, SSO functionality will be applied to the entire network. Use a semicolon to separate the masks. Example: (64.233.187.99/8; 72.14.0.0/16). For ranges, use a dash. Example: (64.233.167-204.99/32). All network masks must end with a CIDR ⓘ

Sign-in page URL

Change the hostname **idp.example.com** to the hostname of your IdP: <https://idp.example.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' => 'urn: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`