

Introduction

This is an overview guide on how to implement SSO (Single-Sign-On) with Claromentis and Google Workspace

Prerequisite

- Claromentis 9+ with Login Handler Module version 4+
- Google Workspace account
- Google Workspace administrator right

Google Workspace

☐ Google Documentation: SAML SSO configuration using Google Workspace

Step 1: Configure Google Workspace for single sign-on (SSO)

- 1. Navigate to the Google Admin Portal
- 2. In Google Workspace Admin Console, go to Apps > Web and mobile apps.
- 3. Select Add Custom SAML app.
- 4. In the App name field, add a name that will help you identify this SAML app for example:

Claromentis Intranet SSO

- 5. Click Continue.
- 6. Download IdP metadata which is to be uploaded to Claromentis



ACS URL: get this from Single SignOn URL field in Claromentis example:

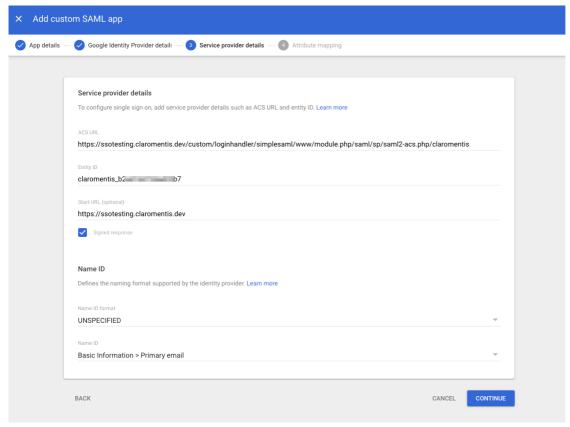
https://{your-system-url}/custom/loginhandler/simplesaml/www/module.php/saml/sp/saml2-acs.php/claromentis

Entity ID: get Entity ID under IDP Configuration in Claromentis

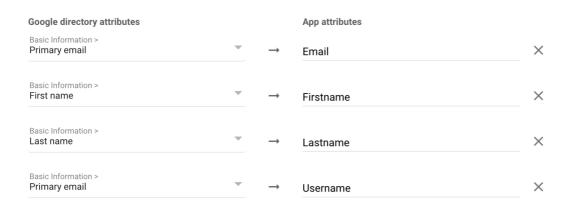
Start URL (optional): this is typically is your system URL

Name ID format: UNSPECIFIED

NAME ID: Basic Information > Primary email



8. Attributes Mapping



Google doesn't have a Username and uses Primary email which needs to be mapped as Username in Claromentis

Claromentis

Step 2: Configure SSO in Claromentis

Navigate to Admin \rightarrow Custom Login handler \rightarrow SSO Configuration

- 1. Select Identity Provider "Google"
- 2. Upload Federation Metadata XML (you will need XML from Google Workspace containing IdP metadata)
- 3. Populate Security Configuration
- 4. IDP Identifier: this should be populated from the XML

- 5. Entity ID you will need to copy this to Google Workspace SSO Configuration
- 7. Name ID Policy: Unspecified
- 6. Save Options

Testing & Troubleshooting

Navigate back to Google Workspace and click on Test SAML login

Created on 30 January 2025 by Michael Christian. Last modified on 4 February 2025