



## Implementing SSO with Login Handler and Google Workspace

### 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

×

Add custom SAML app

✓

App details

2

Google Identity Provider detail:

3

Service provider details

4

Attribute mapping

To configure single sign-on (SSO) for SAML apps, follow your service provider's instructions. [Learn more](#)

Option 1: Download IdP metadata

DOWNLOAD METADATA

OR

7. Service Provider Details

**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

×

Add custom SAML app

✓ App details

✓ Google Identity Provider detail:

3 Service provider details

4 Attribute mapping

Service provider details

To configure single sign on, add service provider details such as ACS URL and entity ID. [Learn more](#)

ACS URL

https://ssotesting.claromentis.dev/custom/loginhandler/simplesaml/www/module.php/saml/sp/saml2-acs.php/claromentis

Entity ID

claromentis\_b2b7

Start URL (optional)

https://ssotesting.claromentis.dev

☒ Signed response

Name ID

Defines the naming format supported by the identity provider. [Learn more](#)

Name ID format

UNSPECIFIED

Name ID

Basic Information > Primary email

BACK

CANCEL

CONTINUE

## 8. Attributes Mapping

| Google directory attributes       |   | App attributes |   |
|-----------------------------------|---|----------------|---|
| Basic Information > Primary email | → | Email          | × |
| Basic Information > First name    | → | Firstname      | × |
| Basic Information > Last name     | → | Lastname       | × |
| Basic Information > Primary email | → | Username       | × |

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** → **Custom Login handler** → **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