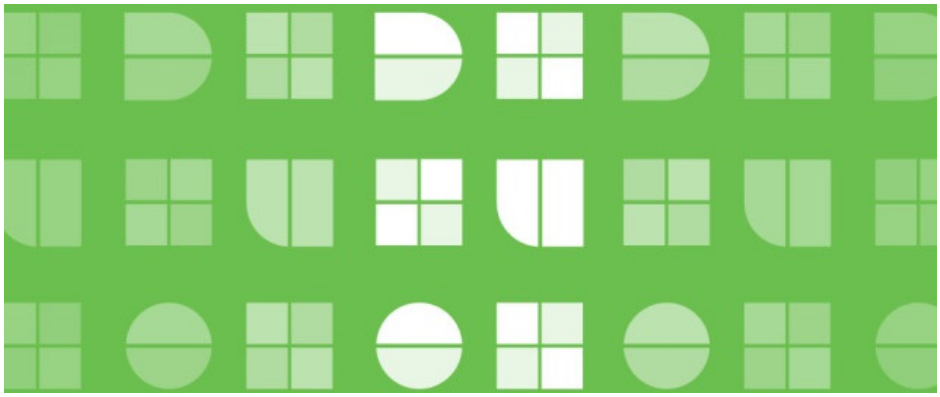
Link to article: https://discover.claromentis.com/knowledgebase/articles/999/implementing-sso-with-login-handler-and-duo



Implementing SSO with Login Handler and DUO

Introduction

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

Prerequisite

- Claromentis 9+ with Login Handler Module version 4+
- Duo Essentials package with Single Sign-On
- Duo Admin account with the Owner role.
- Active Directory or a SAML identity provider that can be used as your primary authentication source for Duo Single Sign-On.

Important: Duo isn't an Identity Provider and it requires Active Directory or a SAML identity Provider

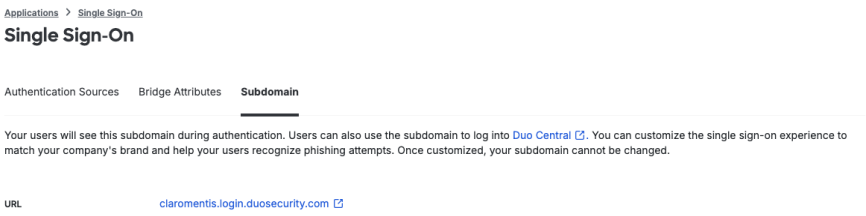
Duo

Duo Documentation: Duo Single Sign-on for Generic SAML Service Providers

Step 1: Enable Duo Single Sign On

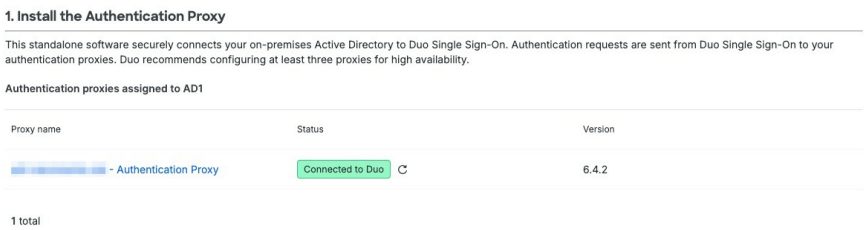
1.Log in to the Duo Admin Panel and navigate to **Applications → SSO Settings.**

2. On the **Customize SSO Subdomain** page you can specify a subdomain you'd like your users to see when they are logging in with Duo Single Sign-On. For example, you can enter companyname and users would see companyname.login.duosecurity.com in the

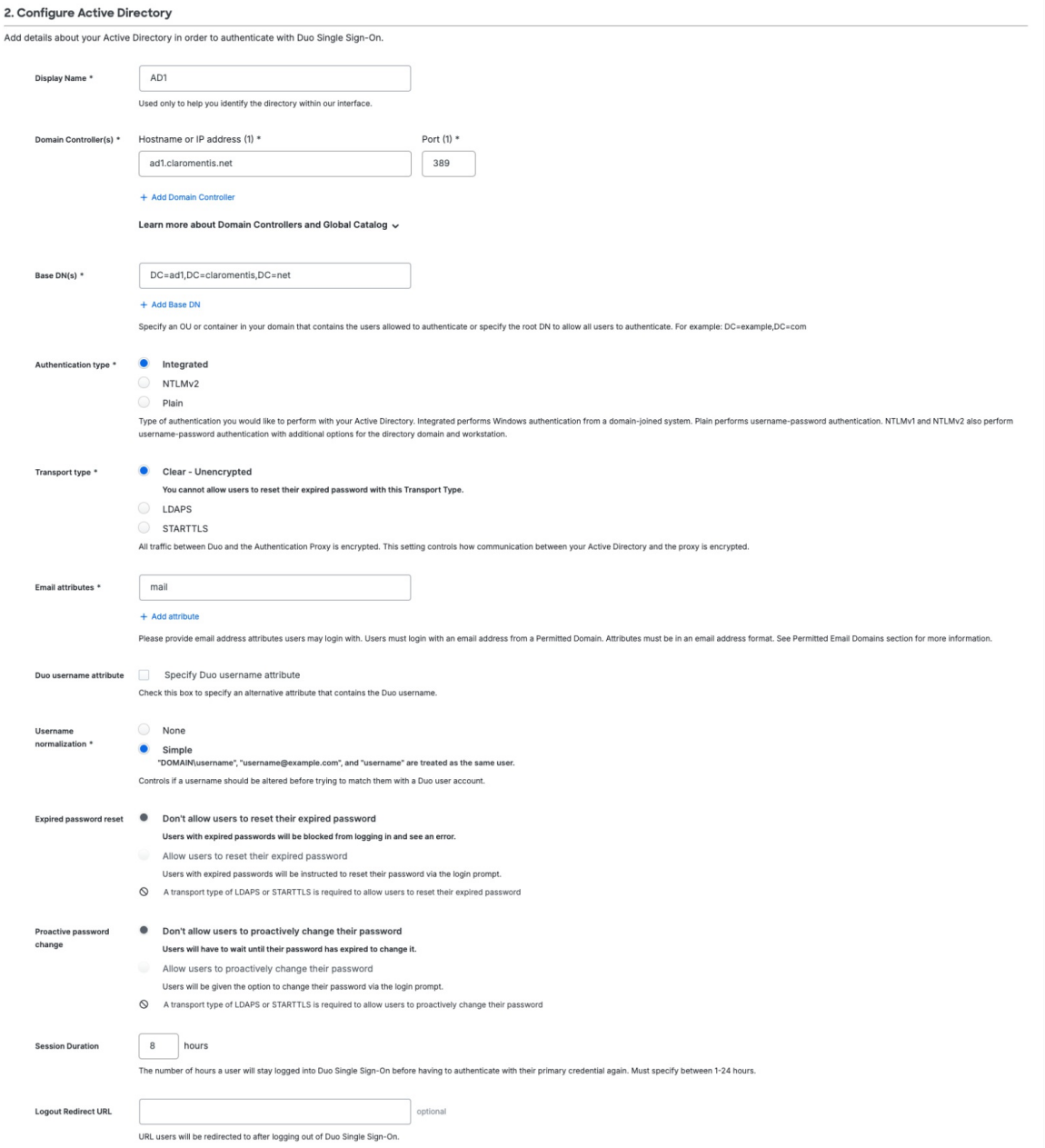


3. On the Add **Authentication Source** page choose between using **Active Directory** or a SAML Identity Provider as your authentication source.

4. If you are using Active Directory, follow the guide to install **Authentication Proxy**

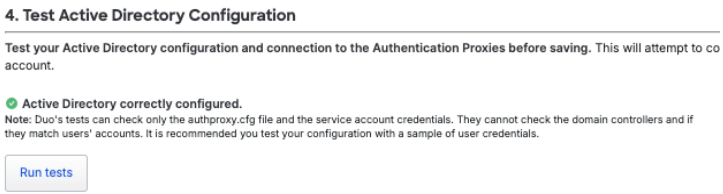


5. Configure Active Directory



6. Set Permitted Email Domains

7. Test Active Directory Configuration



Claromentis

Step 2: Configure SSO in Claromentis

Navigate to **Admin → Custom Login handler → SSO Configuration**

1. Select Identity Provider "**Duo**"

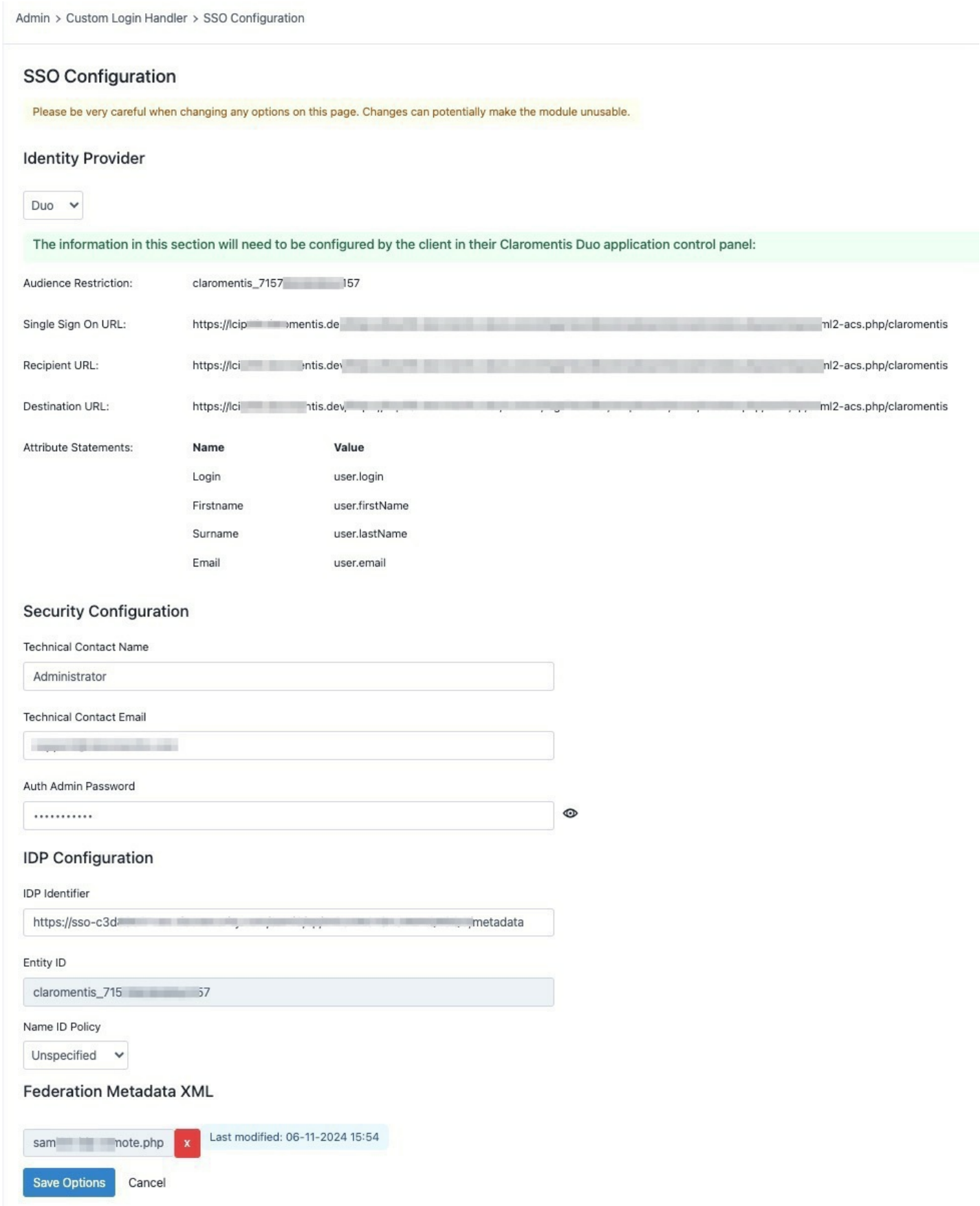
2. Notice the following information which needs to be configured in the Duo Application

3. Populate **Security Configuration**

4. **IDP Identifier** (you will need this information from Duo Application)

5. **Federation Metadata XML** (you will need XML from Duo Application)

6. **Save** Options



Step 3: Getting Service Provider Metadata XML

On the browser navigate to:

`https://{yoursystemurl}/custom/loginhandler/simplesaml/www/module.php/saml/sp/metadata.php/claromentis`

Replace **{yoursystemurl}** with your system address for example **companyname.myintranet.com**

Username: admin

Enter the password by revealing password in **Auth Admin Password**

Rename the file downloaded called **claromentis** by adding .XML extension for example **claromentis.xml**

You will need this file to be uploaded to Duo in Step 4

Duo

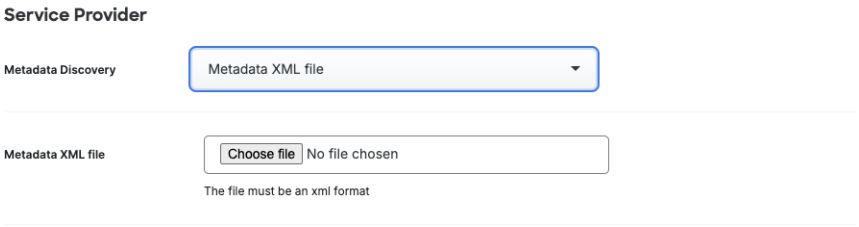
Step 4: Protect an Application

Duo Documentation: Create Your Cloud Application in Duo

1. Log on to the Duo Admin Panel and navigate to **Applications → Protect an Application**.

2. Locate the entry for **Generic SAML Service Provider**

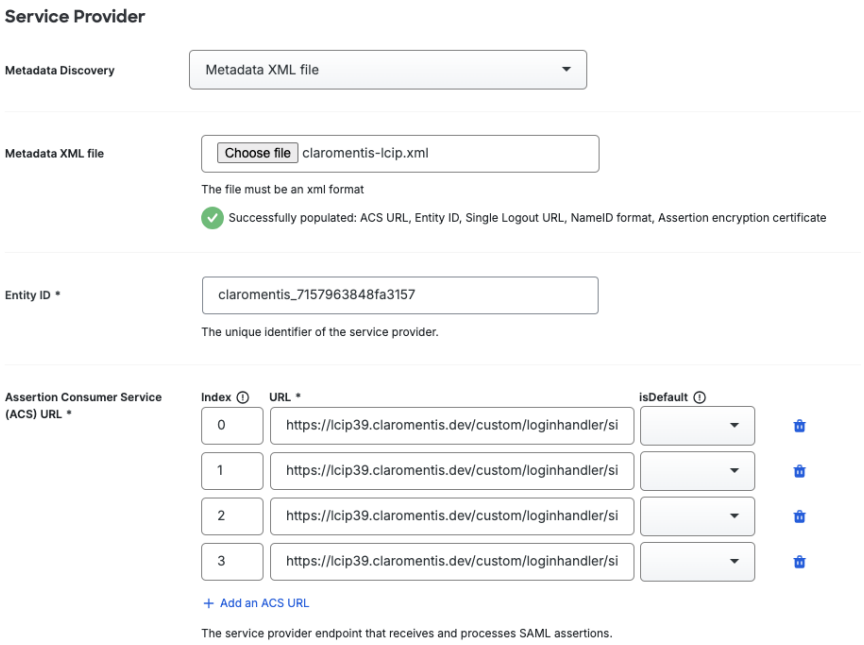
3. Service Provider



Metadata Discover: **Metadata XML file**

Metadata XML File: upload file **claromentis.xml**

This XML file is going to populate: ACS URL, Entity ID, Single Logout URL, NameID format, Assertion encryption certificate



4. SAML Response

NameIDformat: **urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified**

NameID attribute: **<Username>**

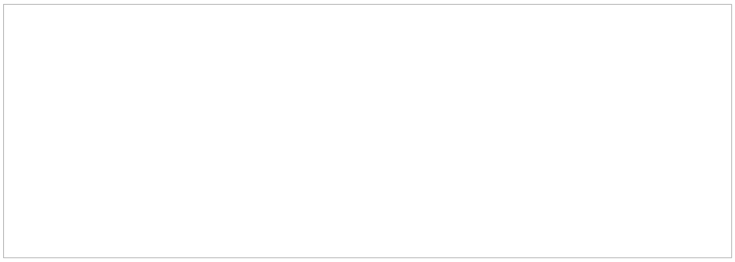
Signature algorithm: **SHA256**

Signing options: Checked both **Sign response Sign assertion**

Assertion encryption **Encrypt the SAML assertion**

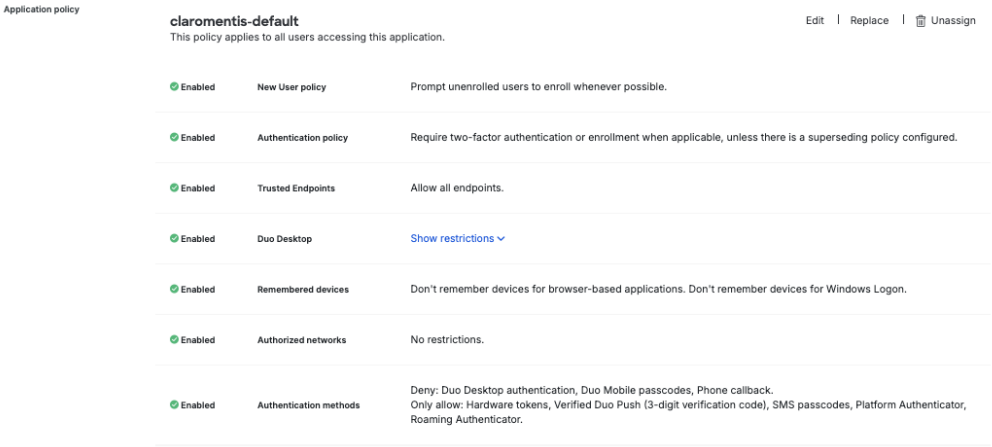
Certificate: Upload Assertion encryption

Map attributes:



5. Policy

Setup Application Policy, here is an example:



6. Save configuration.

Last modified on 18 March 2025 by Mike Leggatt

Created on 21 November 2024 by Michael Christian