

# 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.

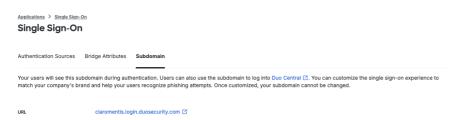
Important: Duo isn't an Identity Provider and it requires Active Directory or a SAML identity Provider

# 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

| Configure Active Dir        | rectory   |  |  |  |  |
|-----------------------------|---|--|--|--|--|
| details about your Active   | Directory in order to authenticate with Duo Single Sign-On.   |  |  |  |  |
| Display Name *              | AD1   |  |  |  |  |
|                             | Used only to help you identify the directory within our interface.  |  |  |  |  |
| Domain Controller(s) *      | Hostname or IP address (1) * Port (1) *   |  |  |  |  |
|                             | ad1.claromentis.net 389   |  |  |  |  |
|                             | + Add Domain Controller   |  |  |  |  |
|                             | Learn more about Domain Controllers and Global Catalog 🗸  |  |  |  |  |
| Base DN(s) *                | DC=ad1,DC=claromentis,DC=net  |  |  |  |  |
|                             | + Add Base DN   |  |  |  |  |
|                             | Specify an OU or container in your domain that contains the users allowed to authenticate or specify the root DN to allow all users to authenticate. For example; DC=example, DC=com  |  |  |  |  |
| Authentication type *       | Integrated  |  |  |  |  |
|                             | NTLMV2  |  |  |  |  |
|                             | Plain  Type of authentication you would like to perform with your Active Directory, Integrated performs Windows authentication from a domain-joined system. Plain performs username-password authentication. NTLMv1 and NTLMv2 also perform |  |  |  |  |
|                             | username-password authentication with additional options for the directory domain and workstation.  |  |  |  |  |
| Transport type *            | Clear - Unencrypted     You cannot allow users to reset their expired password with this Transport Type.  |  |  |  |  |
|                             | LDAPS   |  |  |  |  |
|                             | STARTILS  |  |  |  |  |
|                             | All traffic between Duo and the Authentication Proxy is encrypted. This setting controls how communication between your Active Directory and the proxy is encrypted.  |  |  |  |  |
| Email attributes *          | mail  |  |  |  |  |
|                             | + Add attribute   |  |  |  |  |
|                             | Please provide email address attributes users may login with. Users must login with an email address from a Permitted Domain. Attributes must be in an email address format. See Permitted Email Domains section for more information.      |  |  |  |  |
| Duo username attribute      | Specify Duo username attribute  Check this box to specify an alternative attribute that contains the Duo username.  |  |  |  |  |
|                             |   |  |  |  |  |
| Username<br>normalization * | None  |  |  |  |  |
|                             | Simple "DOMAIN\username", "username@example.com", and "username" are treated as the same user.  |  |  |  |  |
|                             | Controls if a username should be altered before trying to match them with a Duo user account.   |  |  |  |  |
| Expired password reset      | Don't allow users to reset their expired password   |  |  |  |  |
|                             | Users with expired passwords will be blocked from logging in and see an error.  |  |  |  |  |
|                             | Allow users to reset their expired password  Users with expired passwords will be instructed to reset their password via the login prompt.  |  |  |  |  |
|                             | A transport type of LDAPS or STARTTLS is required to allow users to reset their expired password  |  |  |  |  |
| Proactive password          | Don't allow users to proactively change their password  |  |  |  |  |
| change                      | Users will have to wait until their password has expired to change it.  |  |  |  |  |
|                             | Allow users to proactively change their password  |  |  |  |  |
|                             | Users will be given the option to change their password via the login prompt.  A transport type of LDAPS or STARTTLS is required to allow users to proactively change their password  |  |  |  |  |
| Session Duration            | 8 hours   |  |  |  |  |
|                             | The number of hours a user will stay logged into Duo Single Sign-On before having to authenticate with their primary credential again. Must specify between 1-24 hours.   |  |  |  |  |
| Logout Redirect URL         | octional  |  |  |  |  |
| Follows Kedirect OKF        | Optional  URL users will be redirected to after logging out of Duo Single Sign-On.  |  |  |  |  |
|                             |   |  |  |  |  |

# 6. Set Permitted Email Domains

7. Test Active Directory Configuration

| 4. Test Active Directory Configuration   |      |  |  |  |  |  |
|--|------|--|--|--|--|--|
| Test your Active Directory configuration and connection to the Authentication Proxies before saving. This will attempt to account.   | ) CO |  |  |  |  |  |
| • Active Directory correctly configured. Note: Duo's tests can check only the authoroxy.cfg file and the service account credentials. They cannot check the domain controllers and if they match users' accounts. It is recommended you test your configuration with a sample of user credentials. |      |  |  |  |  |  |
| Run tests  |      |  |  |  |  |  |

# **Claromentis**

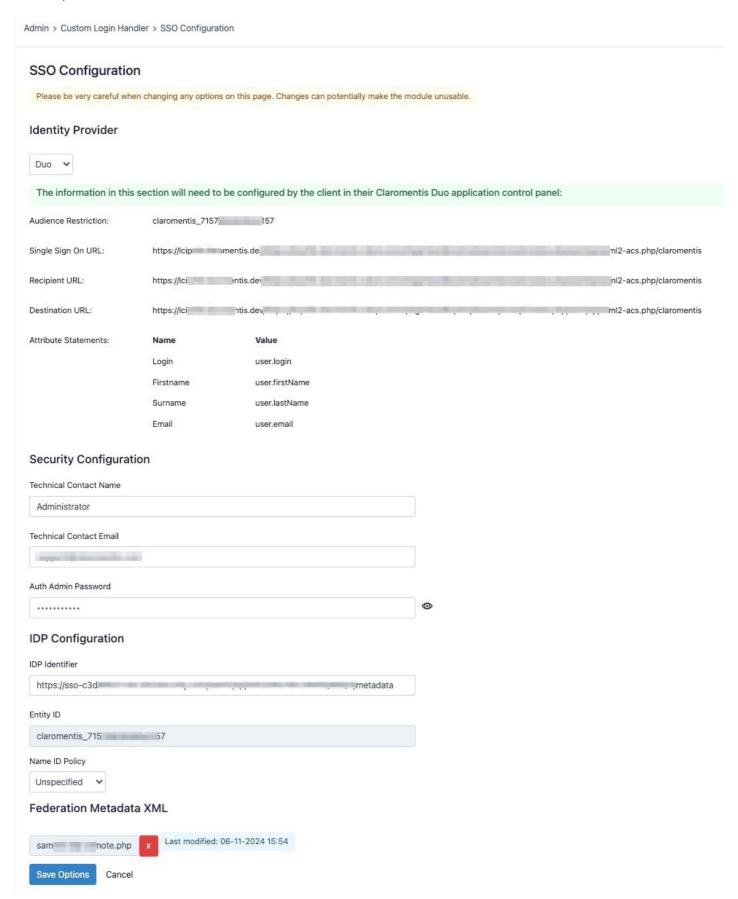
Step 2: Configure SSO in Claromentis

Navigate to Admin o Custom Login handler o 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

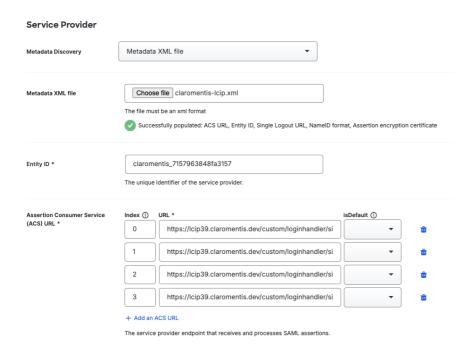
- 1. Log on to the Duo Admin Panel and navigate to Applications → Protect an Application.
- 2. Locate the entry for Generic SAML Service Provider
- 3. Service Provider

| Service Provider   |                                |  |  |  |  |
|--------------------|--------------------------------|--|--|--|--|
| Metadata Discovery | Metadata XML file  ▼           |  |  |  |  |
| Metadata XML file  | Choose file No file chosen     |  |  |  |  |
|                    | The file must be an xml format |  |  |  |  |

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

 $\label{lem:name} Name ID format: {\color{blue} urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified} \\$ 

NameID attribute: <Username>

Signature algorithm: SHA256

| Certificate: Uploa | d Asserti  | ion encryption               |  |  |
|--------------------|--|------------------------------|--|--|
| Map attributes:    |  |                              |  |  |
|                    |  |                              |  |  |
|                    |  |                              |  |  |
|                    |  |                              |  |  |
|                    |  |                              |  |  |
|                    |  |                              |  |  |
| 5. Policy          |  |                              |  |  |
| Setup Application  | Policy, I  | here is an exam <sub>l</sub> | ole:   |  |
| Application policy | claromentis-default This policy applies to all users accessing this application. |                              |  | Edit l Replace l 値 Unassign  |
|                    | Enabled  | New User policy              | Prompt unenrolled users to enroll whenever possible.   |  |
|                    | Enabled  | Authentication policy        | Require two-factor authentication or enrollment when applicable  | e, unless there is a superseding policy configured.                |
|                    | Enabled  | Trusted Endpoints            | Allow all endpoints.   |  |
|                    | Enabled  | Duo Desktop                  | Show restrictions ✓  |  |
|                    | Enabled  | Remembered devices           | Don't remember devices for browser-based applications. Don't   | remember devices for Windows Logon.                                |
|                    | Enabled  | Authorized networks          | No restrictions.   |  |
|                    | Enabled  | Authentication methods       | Deny: Duo Desktop authentication, Duo Mobile passcodes, Phot<br>Only allow: Hardware tokens, Verified Duo Push (3-digit verifica<br>Roaming Authenticator. | ne callback.<br>tion code), SMS passcodes, Platform Authenticator, |
|                    |  |                              |  |  |
| 6. Save configura  | ition.   |                              |  |  |
|                    |  |                              |  |  |
|                    |  |                              |  |  |

Signing options: Checked both Sign response Sign assertion

Assertion encryption Encrypt the SAML assertion

Last modified on 18 March 2025 by Mike Leggatt

Created on 21 November 2024 by Michael Christian