



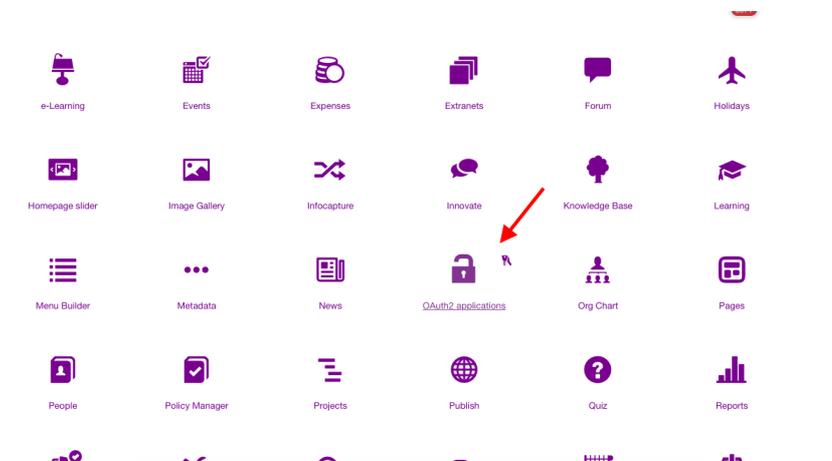
OAuth2 Applications module walkthrough

Overview

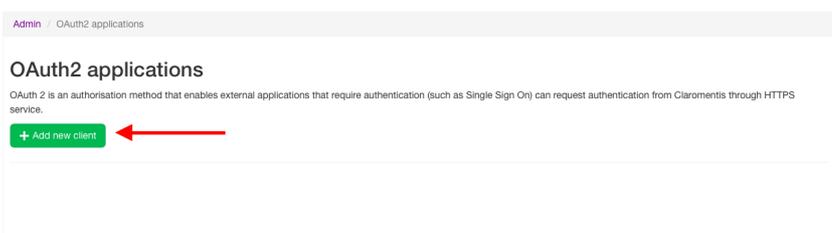
OAuth2 Applications module is developed to enable access to third-party applications through Claromentis intranet.

In this walk-through, we are using 'RocketChat' which is located on a fictitious <https://test.application.com> server as an example of a third-party application. In this example, Intranet is located on <https://workplace.myintranet.com>

Step 1. Go to Admin > OAuth2 Applications



Step 2. Create a new application within the module



Step 3. Populate the panel with relevant information

Create new OAuth2 client ✕

Client Name e.g. Rocket Chat

Human-readable client/app name, this is shown to the User on the permissions confirmation screen. **Choose wisely, you will not be able to change it**

Authorised Redirect URIs

https://test.application.com

One URI per line. Needs to have a protocol, no URL fragments, and no relative paths.

Cancel
Save

Step 4. Once saved, please review the config on Claromentis

OAuth2 applications

OAuth 2 is an authorisation method that enables external applications that require authentication (such as Single Sign On) can request authentication from Claromentis through HTTPS service.

[+ Add new client](#)

Client Name	Rocket Chat
Client ID	MhXWGU8l1Tn9eKwctrFUVsmzyvGXbN1M9C3NHngkL4m8wiHNmJ3dEuJUCE3J
Client Secret	f2BmIk2XvYbt6jwkl32RFAMqimq
Redirect URIs	https://test.application.com

Step 5. Configure the external application to work with Intranet (example)

Please note that each third-party application will have their own configuration interface.

Here are the specifics for each field. Items in quotes must be entered exactly as they appear

- URL - please place the url of your intranet
- Token Path - "/oauth2/access_token"
- Token Sent Via - "Header"
- Identity Token Sent Via - "Header"
- Identity Path - "/oauth2/user"
- Authorize Path - "/oauth2/auth"
- Scope - please leave empty
- ID and Secret are copied from step 4
- Username field - "name_slug"
- Login Style - "Popup"

The following three fields are optional configuration, which would vary from application to application

- Button Text/Text Color/Color - please adjust as required for visual representation in step 6

Custom OAuth: Claro COLLAPSE

When setting up your OAuth Provider, you'll have to inform a Callback URL: **e.g. https://test.application.com/_oauth/claro**

Enable True False 🔍

URL **e.g. https://workplace.myintranet.com** 🔍

Token Path /oauth2/access_token 🔍

Token Sent Via Header 🔍

Identity Token Sent Via **Header** 🔍

Identity Path /oauth2/user 🔍

Authorize Path /oauth2/auth 🔍

Scope 🔍

Id MRKWGJ8in1TNeKwctPFUvzmyVGZbV1M6C3NhnqL4mbwRhmJ3eUJCESJ 🔍

Secret 1ZBMKXxvYt8tYenL32RFAMqmq 🔍

Login Style Poppup 🔍

Button Text Login with ClaroMentis 🔍

Button Text Color #FFFFFF 🔍

Button Color #13679A 🔍

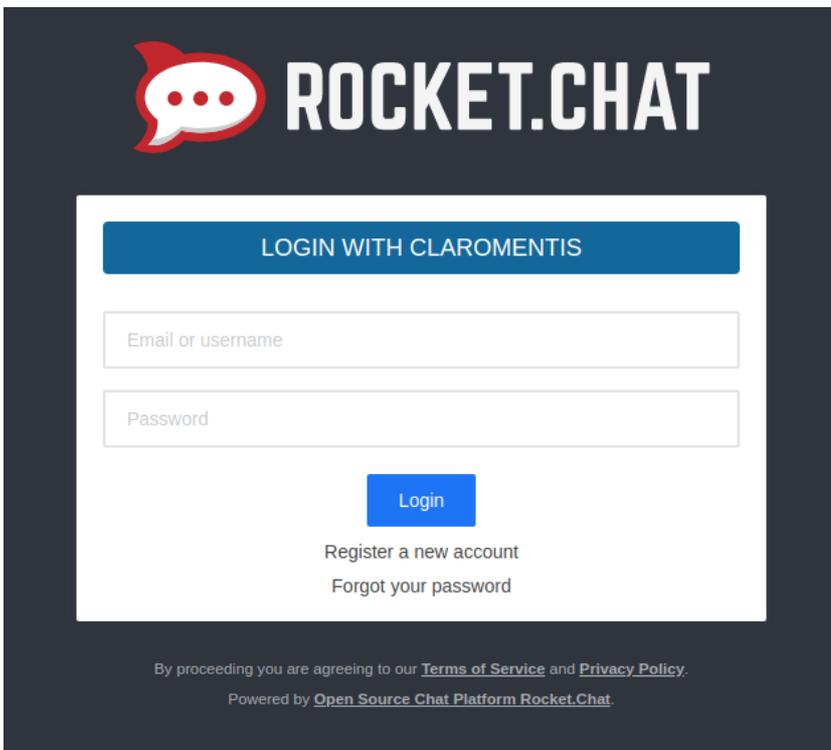
Username field name_slug 🔍

Merge users True False 🔍

Reset Section Settings **RESET**

Step 6. Review the third-party application access

You can now either create a fast access button or menu link to the application and run it.



For any additional information and configuration help, please contact your onboarding specialist, project manager or support team.

Last modified on 30 November 2023 by Hannah Door

Created on 5 July 2018 by Stas Dreiling

Tags: How to configure OAuth2 Applications