



CAcert OpenID Connect Registration Examples



Drupal

I am using Drupal CMS (a version of Drupal 11) for my example. However, other versions of Drupal 10 or 11 will be very similar.

First, ensure that you have installed and enabled the PHP GMP module for your version of PHP.

There are several different modules available for Drupal to provide various OpenID services to Drupal.

In our case, we are using the miniOrange OpenID module.

As the documentation instructs, use Composer to install the OAuth Login – OAuth OIDC SSO module, also known as the miniOrange OpenID module:

```
composer require 'drupal/oauth_login_oauth2:^3.0'
```

Go in to your Drupal installation, and go to the Administration Extend page. Search for (use Filter) OAuth, look for “miniOrange,” and check and Install that.

Go to the Configuration main menu item and choose miniOrange OAuth Client Configuration. Enter that configuration page.

Note: the following screen shots are from the general Configuration menu item for the page, which Gmay be slightly different from the initial configuration.

Back to site Manage Shortcuts admin This site is intended for demonstration purposes. Announcements Edit

Content Structure Appearance Extend Configuration People Reports Help

Home Administration Configuration People

OAuth/OIDC Client Configuration

Request 7-days trial

Configure OAuth Attribute & Role Mapping Sign In Settings Login Reports Upgrade Plans

CONFIGURE APPLICATION

Select Application* - Select - Select an OAuth Server

Callback/Redirect URL ① https://bb.buadh-brath.com/web/mo_login Copy

Custom App Name*

Login Link Text* Log in using ##app_name## Note: The login link will appear on the user login page in this manner

Grant Types 🏆
 ☒ Authorization Code Grant ?
 ☐ Authorization Code with PKCE ?
 ☐ Password Grant ?
 ☐ Implicit Grant ?

Client ID*

Choose “Custom OAuth 2.0 App” from the dropdown and click the Next button.

Back to site Manage Shortcuts admin This site is intended for demonstration purposes. Announcements Edit

Content Structure Appearance Extend Configuration People Reports Help

Home Administration Configuration People

OAuth/OIDC Client Configuration

Request 7-days trial

Configure OAuth Attribute & Role Mapping Sign In Settings Login Reports Upgrade Plans

CONFIGURE APPLICATION

Custom setup guide

Select Application* Custom OAuth 2.0 Provider Select an OAuth Server

Callback/Redirect URL ① https://bb.buadh-brath.com/web/mo_login Copy



Custom App Name*

Login Link Text* Log in using ##app_name## Note: The login link will appear on the user login page in this manner

Grant Types 🏆
 ☒ Authorization Code Grant ?
 ☐ Authorization Code with PKCE ?
 ☐ Password Grant ?
 ☐ Implicit Grant ?

Client ID*

Copy the “Callback / Redirect URL” and go to the CAcert OpenID Registration Site and start the “Register A New Site” process.



How to Register a New Site

To make use of this system and register a site, you need the following things:

1. A unique name to identify your site registration
2. The "Redirect URL" that the OpenID plugin for the site that you are registering requires.
3. Does your plugin use Post or Basic authentication? The default is POST. If you have requirements other than those two, please contact the CAcert OpenID development team at bmccullough@cacert.org
4. Optional notes for yourself.



You may download the various URLs provided by the OpenID component [here](#)

Site Name	<input type="text"/>
Redirect URL	<input type="text"/>
Auth Method	<input checked="" type="radio"/> Post <input type="radio"/> Basic
Notes	<input type="text"/>

Copyright © CAcert, Inc 2025

Create a name to identify your new connection.

Use the Redirect URL given above from the Drupal machine for the Redirect URL.



How to Register a New Site

To make use of this system and register a site, you need the following things:

1. A unique name to identify your site registration
2. The "Redirect URL" that the OpenID plugin for the site that you are registering requires.
3. Does your plugin use Post or Basic authentication? The default is POST. If you have requirements other than those two, please contact the CAcert OpenID development team at bmccullough@cacert.org
4. Optional notes for yourself.

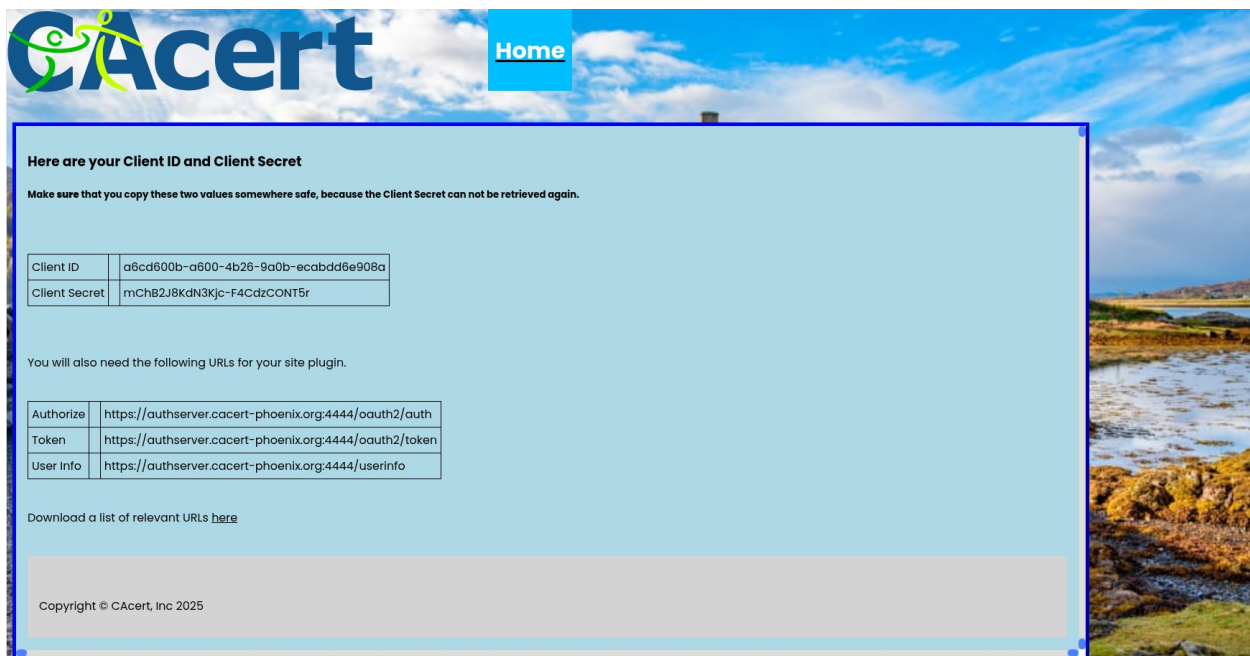
You may download the various URLs provided by the OpenID component [here](#)

Site Name	My Drupal Site
Redirect URL	https://bb.buadh-brath.com/web/mo_login
Auth Method	<input checked="" type="radio"/> Post <input type="radio"/> Basic
Notes	<input type="text"/>

Copyright © CAcert, Inc 2025

In the CAcert Site, click Register Site.

Save the Client ID and Client Secret in a safe place. The Registration Site WILL NOT allow you to retrieve those values again.



CAcert Home

Here are your Client ID and Client Secret

Make sure that you copy these two values somewhere safe, because the Client Secret can not be retrieved again.

Client ID	a6cd600b-a600-4b26-9a0b-ecabdd6e908a
Client Secret	mChB2J8KdN3Kjc-F4CdZcONT5r

You will also need the following URLs for your site plugin.

Authorize	https://authserver.cacert-phoenix.org:4444/oauth2/auth
Token	https://authserver.cacert-phoenix.org:4444/oauth2/token
User Info	https://authserver.cacert-phoenix.org:4444/userinfo

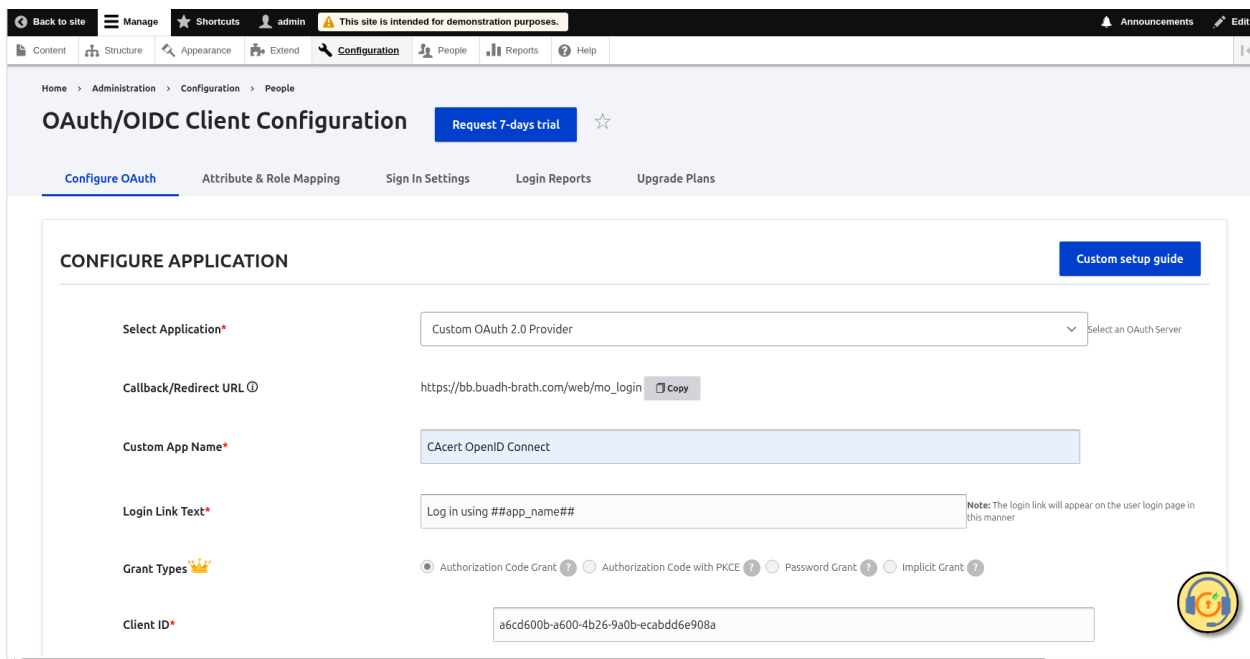
Download a list of relevant URLs [here](#)

Copyright © CAcert, Inc 2025

In your Drupal machine, continue the configuration of the miniOrange module.

Edit the first field, “Text of the SSO login link on the login page” as you wish.

Insert the Client ID and Client Secret from the CAcert Registration page in to the two fields on your Drupal site.



Back to site Manage Shortcuts admin This site is intended for demonstration purposes. Announcements Edit

Content Structure Appearance Extend Configuration People Reports Help

Home > Administration > Configuration > People

OAuth/OIDC Client Configuration

Request 7-days trial ☆

Configure OAuth Attribute & Role Mapping Sign In Settings Login Reports Upgrade Plans

CONFIGURE APPLICATION

Custom setup guide

Select Application* Custom OAuth 2.0 Provider Select an OAuth Server

Callback/Redirect URL ④ https://bb.buadh-brath.com/web/mo_login Copy

Custom App Name* CAcert OpenID Connect

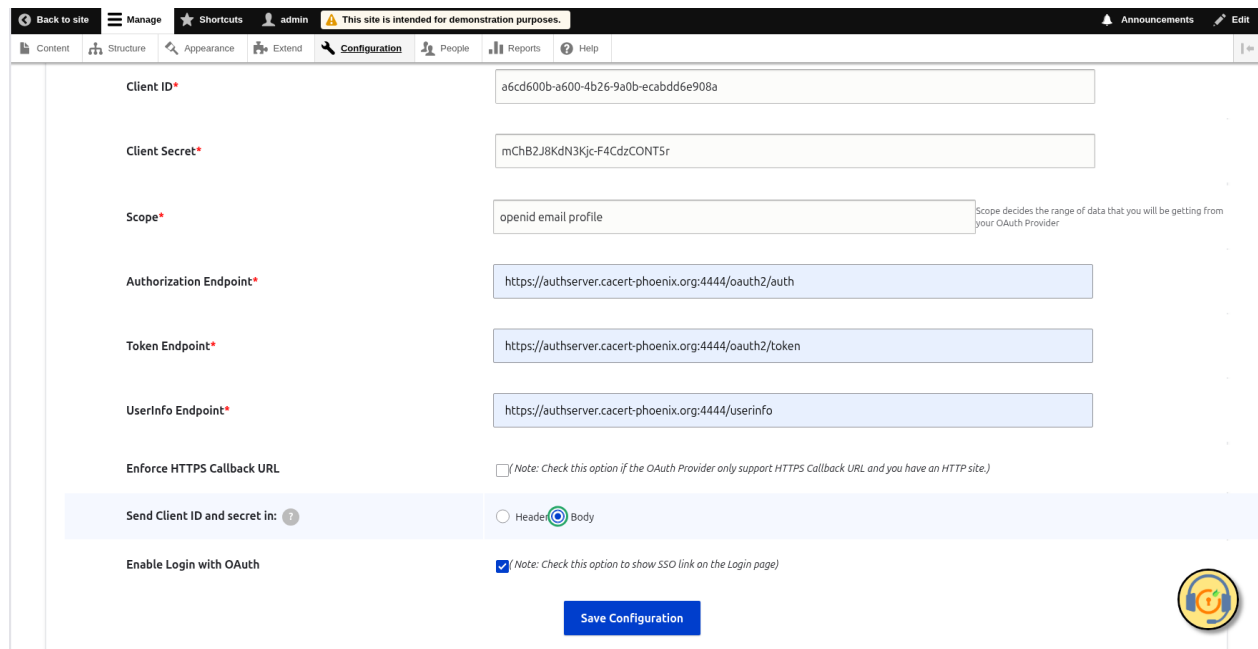
Login Link Text* Log in using ##app_name## Note: The login link will appear on the user login page in this manner

Grant Types 🏆 ☒ Authorization Code Grant ☐ Authorization Code with PKCE ☐ Password Grant ☐ Implicit Grant

Client ID* a6cd600b-a600-4b26-9a0b-ecabdd6e908a

Enter the three URLs from the CAcert Registration page into the appropriate places on the page. You do not need to change the Scope.

Also ensure that you click the radio button for “Body,” not “Header.”



The screenshot shows the Drupal Configuration page for an OAuth2 client. The top navigation bar includes links for Back to site, Manage, Shortcuts, admin, and a warning that the site is intended for demonstration purposes. The Configuration menu is active, showing sub-menus for Content, Structure, Appearance, Extend, Configuration, People, Reports, and Help. The main content area contains the following fields and options:

- Client ID***: a6cd600b-a600-4b26-9a0b-ecabdd6e908a
- Client Secret***: mChB2J8KdN3Kjc-F4CdzcCONT5r
- Scope***: openid email profile (A tooltip indicates: Scope decides the range of data that you will be getting from your OAuth Provider)
- Authorization Endpoint***: https://authserver.cacert-phoenix.org:4444/oauth2/auth
- Token Endpoint***: https://authserver.cacert-phoenix.org:4444/oauth2/token
- Userinfo Endpoint***: https://authserver.cacert-phoenix.org:4444/userinfo
- Enforce HTTPS Callback URL**: ☐ (Note: Check this option if the OAuth Provider only support HTTPS Callback URL and you have an HTTP site.)
- Send Client ID and secret in:** ☐ Header ☒ Body
- Enable Login with OAuth**: ☒ (Note: Check this option to show SSO link on the Login page)

A blue **Save Configuration** button is located at the bottom right of the form area. A circular logo with a stylized 'G' is visible in the bottom right corner of the page.

Click the “All Done!” Or “Save Configuration” button.

You will be taken to the next page, showing the “Test Configuration” button.

You should not need to change anything on this page. Just click “Test Configuration”.



Authenticate with a client certificate

The application **My Drupal Site** requests a login.

You have presented a valid client certificate for multiple email addresses. Please choose which one you want to present to the application:

- ☐ bdmc@buadh-brath.com
- ☒ bdmc@bdmcc-us.com
- ☐ bdmc@bdmcc.com
- ☐ bmccullough@cacert.org

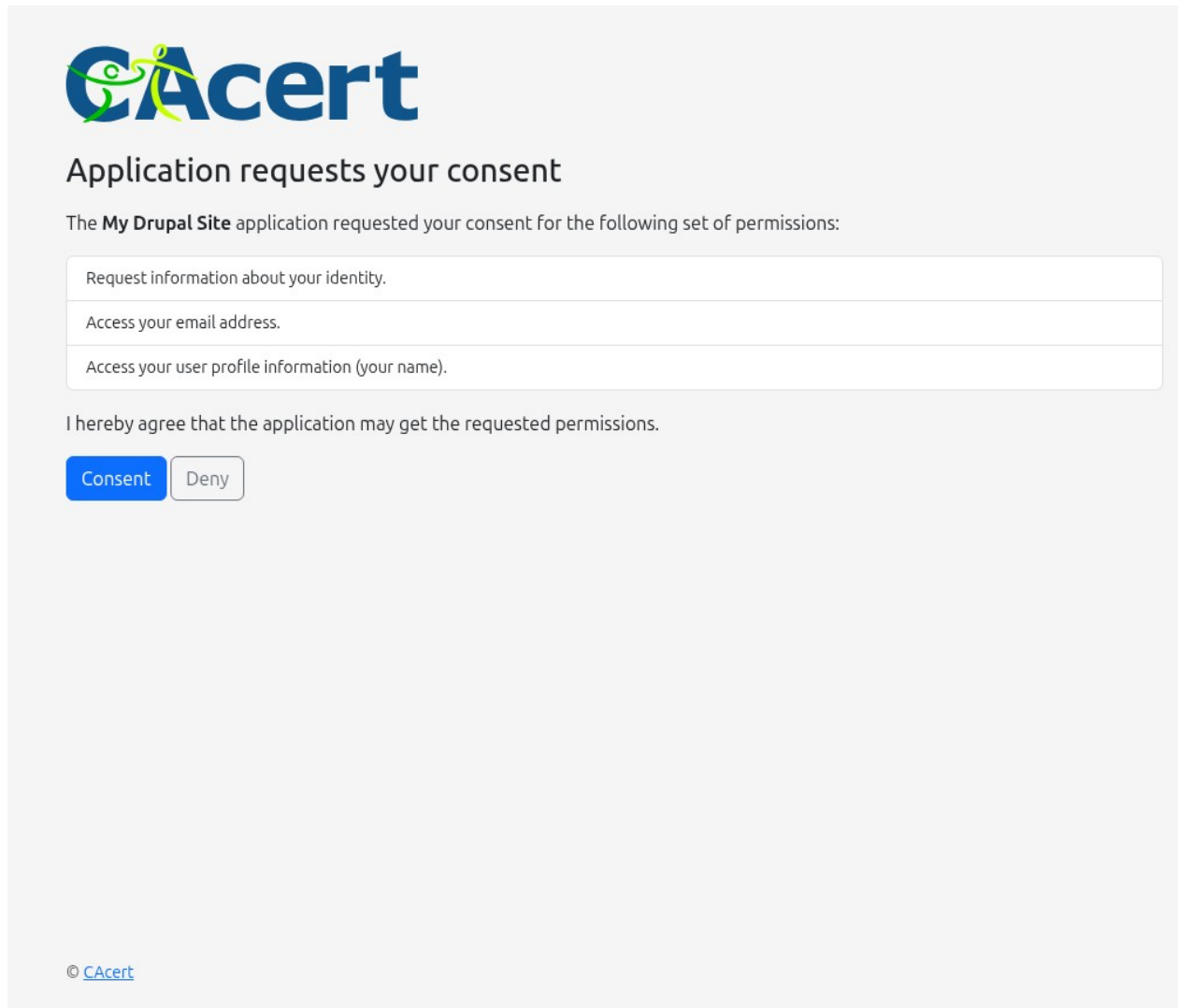
Do you want to use the chosen identity from the certificate for authentication?

Yes, please use this identity

No, please send me back

Select the e-mail address associated with your Drupal site. And click “Yes, please use this identity.”

The next CAcert page asks you to confirm that you want your Drupal site to have access to certain information associated with your certificate.

The image shows a web interface for CAcert. At the top left is the CAcert logo, which consists of a stylized green figure with arms raised next to the word "CAcert" in blue. Below the logo is the heading "Application requests your consent". Underneath this is a line of text: "The **My Drupal Site** application requested your consent for the following set of permissions:". Below this text is a list of three permissions, each in a separate white box with a thin border: "Request information about your identity.", "Access your email address.", and "Access your user profile information (your name).". Below the list is a line of text: "I hereby agree that the application may get the requested permissions.". At the bottom of this section are two buttons: a blue button labeled "Consent" and a white button labeled "Deny". At the very bottom left of the page is a small copyright notice: "© CAcert".

CAcert

Application requests your consent

The **My Drupal Site** application requested your consent for the following set of permissions:

- Request information about your identity.
- Access your email address.
- Access your user profile information (your name).

I hereby agree that the application may get the requested permissions.

© CAcert

If you are comfortable with this request, click “Consent.”

If you have done everything correctly, you should be successful and you should see a green check mark.



Hello, bdmcc@bdmcc-us.com

Your Test Connection is successful. Now, follow the below steps to complete the last step of your configuration:

Please select the **Attribute Name** in which you are getting **Email ID**.

Email Attribute

You can also map the Username attribute from the Attribute and Role Mapping tab in the module.

Click on the **Done** button to save your changes.

Done

ATTRIBUTES RECEIVED:

ATTRIBUTE NAME	ATTRIBUTE VALUE
acr	urn:cacert:1fa:cert
aud > 0	a6cd600b-a600-4b26-9a0b-ecabdd6e908a
auth_time	1751974465
email	bdmcc@bdmcc-us.com

Below the green check mark, you will see a list of the various attributes that CAcert has sent to Drupal. Among those, you will see the E-Mail address and probably Name.

Click Done, and you will be taken to the “Attribute Mapping” page. On the right-hand side, you will see a column named “Drupal Attributes” and to the right of that, OAuth Server Attributes.

Under those, you will see “Email:” and “Username:” in the Drupal column. In the OAuth column, “email” should be pre-selected, but you will have to set the appropriate item for the Username attribute. In the right-hand column, you will see a list of all of the attributes returned from the CAcert Server. In the Username dropdown, select the appropriate item. Both of these are required to complete your configuration.

The screenshot shows the CAcert OpenID Connect configuration interface. At the top is a navigation bar with tabs: Content, Structure, Appearance, Extend, Configuration (selected), People, Reports, and Help. Below this is a sub-navigation bar with links: Configure OAuth, Attribute & Role Mapping (selected), Sign In Settings, Login Reports, and Upgrade Plans. A green status message at the top left indicates that configurations were saved successfully. The main content area is divided into two panels. The left panel, titled 'Attribute Mapping', contains a section for 'Basic Attribute Mapping' with two columns: 'Drupal Attributes' and 'OAuth Server Attributes'. Under 'Drupal Attributes', there are labels for 'Email:' and 'Username:'. Under 'Email:', the 'email' attribute is selected in a dropdown. Under 'Username:', '- Select Username Attribute -' is selected in a dropdown. A 'Save Configuration' button is at the bottom of this panel. The right panel, titled 'Attributes received from the OAuth Server:', contains a table with two columns: 'ATTRIBUTE NAME' and 'ATTRIBUTE VALUE'. The table lists four attributes: 'acr' with value 'urn:ca-cert:1fa:cert', 'aud > 0' with a long alphanumeric string, 'auth_time' with value '1751974465', and 'email' with value 'bdmc@bdmcc-us.com'. A 'Clear Attribute List' button is at the bottom of this panel. A note at the bottom right says 'NOTE: Please clear this list after configuring the module to'. A small circular icon with a magnifying glass is also visible in the bottom right corner.

ATTRIBUTE NAME	ATTRIBUTE VALUE
acr	urn:ca-cert:1fa:cert
aud > 0	a6cd600b-a600-4b26-9a0b-ecabdd6e908a
auth_time	1751974465
email	bdmc@bdmcc-us.com

Below the Attribute Mapping section, there are many other items which may be configured, but are not necessary.

Click “Save Configuration.”

If you wish, you may click “Sign in Settings” in the top menu and you will see the following screen.

Content
Structure
Appearance
Extend
Configuration
People
Reports
Help

Home
Administration
Configuration
People

OAuth/OIDC Client Configuration

Request 7-days trial

Configure OAuth
Attribute & Role Mapping
Sign In Settings
Login Reports
Upgrade Plans

Debugging & Troubleshoot

☐ Enable Logging
Enabling this checkbox will add loggers under the [Reports](#) section

Save Configuration


Download Module Logs

Auto Create Users

☐ Check this option if you want to enable **auto creation** of users if user does not exist.
This feature provides you with an option to automatically create a user if the user is not already present in Drupal.

Page Restriction

☐ Protect website against anonymous access
Note: Users will be redirected to your OAuth server for login in case user is not logged in and tries to access website.

[\[What is Page restriction and How to Set up\]](#)


If you wish to log all use of the OAuth Login option, you may check the first check box and Save.

Click on the “Back to site” button at the top left corner of your screen.

Back to site
Manage
Shortcuts
admin
This site is intended for demonstration purposes.
Announcements
Edit

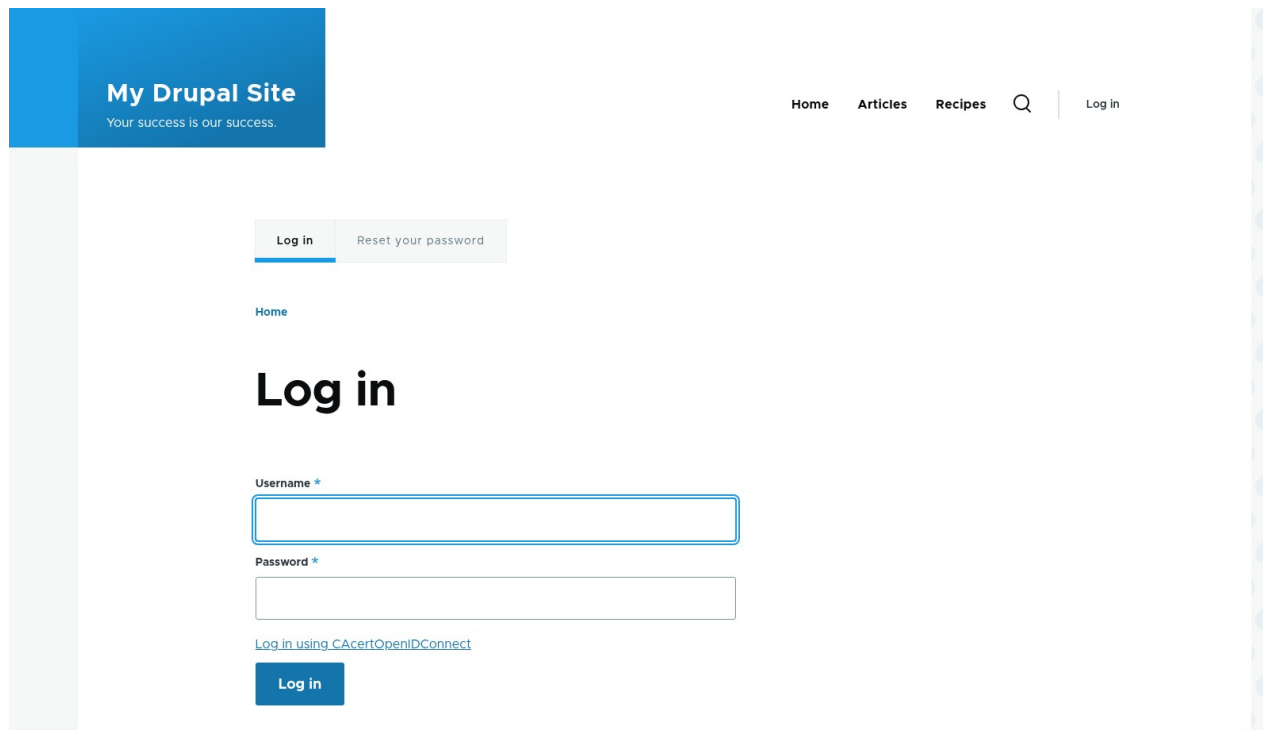
Content
Structure
Appearance
Extend
Configuration
People
Reports
Help

Home
Administration

Configuration

[Hide descriptions](#)

Log out, and you will see a new link under the traditional Login form.



The screenshot shows the Drupal login interface. At the top left, a blue header contains the text "My Drupal Site" and "Your success is our success." To the right, a navigation bar includes links for "Home", "Articles", "Recipes", a search icon, and a "Log in" link. Below the header, there are two buttons: "Log in" (highlighted with a blue underline) and "Reset your password". A link labeled "Home" is positioned above the main heading "Log in". The login form consists of two input fields: "Username *" and "Password *". Below these fields is a link that reads "Log in using CAcertOpenIDConnect". At the bottom of the form is a blue "Log in" button.

Here is a closer look:

Log in

Username *

Password *

[Log in using CAcertOpenIDConnect](#)

Log in

Click that new link, answer the questions about your CAcert Certificate and you should be logged in!

Notes regarding the miniOrange Contributed Module.

This module is free for anyone, but has a couple of notable restrictions.

Those restrictions are lifted with the subscription (paid) version of this module.

1. First, only one OAuth service can be configured at a time.
2. Secondly, only existing users of the site may use OAuth Login. Another use case that people may desire is for new, authenticated users be automatically added to the Drupal site. This is not allowed with the free version.