

# GOCDDB's Integration with IRIS IAM Service

---

# Basic integration with IAM using OIDC

## Welcome to GOCDB

Use of GOCDB is governed by the [EGI Acceptable Use Policy](#) which places restrictions on your use of the service.

The [GOCDB Privacy Notice](#) describes what personal data is collected and why, and your rights regarding this data.

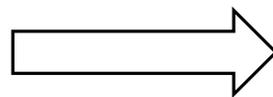
Please read these documents before accessing GOCDB.

[Access GOCDB](#)

Browse the [GOCDB documentation index](#) on the EGI wiki.



The GOCDB service is provided by STFC for EGI, co-funded by EGI.eu and EOSC-hub. Licensed under the Apache 2 License.



## Welcome to GOCDB

Use of GOCDB is governed by the [EGI Acceptable Use Policy](#) which places restrictions on your use of the service.

The [GOCDB Privacy Notice](#) describes what personal data is collected and why, and your rights regarding this data.

Please read these documents before accessing GOCDB.

[Access GOCDB using your IGTF X.509 Certificate](#)

or

Access GOCDB using one of the following:

[EGI Check-In](#)

[IRIS IAM](#)

Browse the [GOCDB documentation index](#) on the EGI wiki.



The GOCDB service is provided by STFC, part of UK Research and Innovation, for EGI, co-funded by EGI.eu and EOSC-hub. Licensed under the Apache 2 License.

# Configuration

```
<directory /usr/share/GOCDB5/htdocs/web_portal>
  options +Indexes -FollowSymLinks

  authname "openid-connect"
  require valid-user
  authtype openid-connect

  require ssl-verify-client

</directory>
```

Here shows the configuration used for the web portal (above) and the API (right). Listed below are the configuration values required by mod-auth-openidc

```
oidcclientid
oidcclientsecret
oidcredirecturi
oidccryptopassphrase
oidcdiscoverurl
oidcmetadatadir
```

```
oidcoauthclientid
oidcoauthclientsecret
oidcoauthintrospectionendpoint
```

```
<directory /usr/share/GOCDB5/htdocs/PI/public>
  options +Indexes -FollowSymLinks
  sslverifyclient optional

  require all granted

</directory>

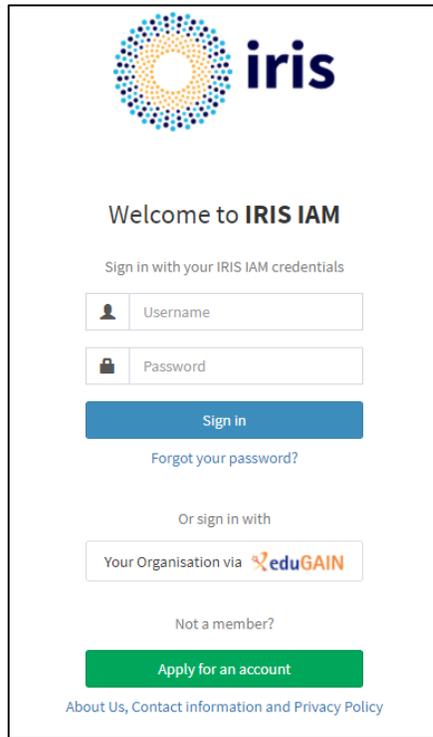
<directory /usr/share/GOCDB5/htdocs/PI/private>
  options +Indexes -FollowSymLinks

  authname "oauth20"
  require valid-user
  authtype oauth20

  require ssl-verify-client

</directory>
```

# Registering as a client – web portal



Welcome to IRIS IAM

Sign in with your IRIS IAM credentials

Username

Password

Sign in

Forgot your password?

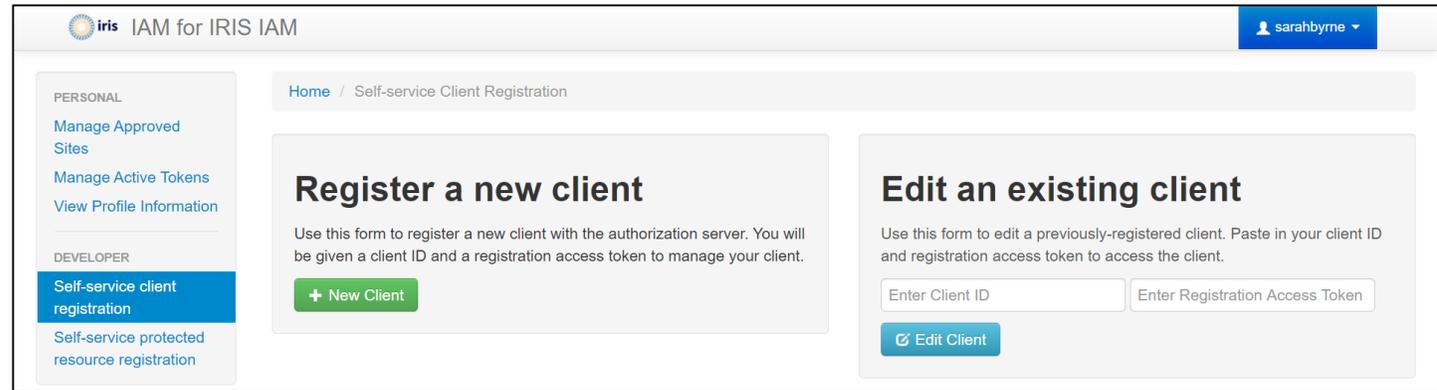
Or sign in with

Your Organisation via eduGAIN

Not a member?

Apply for an account

[About Us, Contact information and Privacy Policy](#)



iris IAM for IRIS IAM sarahbyrne

Home / Self-service Client Registration

**Register a new client**

Use this form to register a new client with the authorization server. You will be given a client ID and a registration access token to manage your client.

+ New Client

**Edit an existing client**

Use this form to edit a previously-registered client. Paste in your client ID and registration access token to access the client.

Enter Client ID

Enter Registration Access Token

Edit Client



Simple and easy client registration process

- Redirect URI entered
- Client ID and secret given

All information was then added to the config as per mod\_auth\_openidc requirements

openid	<input checked="" type="checkbox"/>
profile	<input checked="" type="checkbox"/>
email	<input checked="" type="checkbox"/>
address	<input type="checkbox"/>
phone	<input type="checkbox"/>
offline_access	<input type="checkbox"/>
preferred_username	<input type="checkbox"/>
eduperson_scoped_affiliation	<input type="checkbox"/>
eduperson_entitlement	<input type="checkbox"/>

# Using group information to authenticate

---

Created a new group on IRIS IAM called gocdb to help handle access .

Moved our group checks into code base not the configuration – allowed custom messages (right).

The meant the groups array ended up as a string after being handled by apache (we think).

*“You do not belong to the correct group to gain access to this site. Please visit [iris-iam.stfc.ac.uk](http://iris-iam.stfc.ac.uk) and submit a request to join the GOCDB group. This shall be reviewed by a GOCDB admin.”*

- For anyone not belonging to the gocdb group

*“You must login via your organisation on IAM to gain access to this site.”*

- For locally created accounts on IRIS IAM

# Registering as a new GOCDDB user

---

Please provide the following data for your account.  
[AuthenticationRealm] [IRIS IAM - OIDC,]

Title

Forename \* (unaccentuated letters, spaces, dashes and quotes)

Surname \* (unaccentuated letters, spaces, dashes and quotes)

E-Mail \* (valid e-mail format)

Telephone Number (numbers, optional +, dots spaces or dashes)

Information taken from the token can be used when first logging in and registering your account on GOCDDB.

# Registering as a protected resource - API

iris IAM for IRIS IAM sarahbyrne

Home / Self-service Protected Resource Registration

**PERSONAL**  
Manage Approved Sites  
Manage Active Tokens  
View Profile Information

**DEVELOPER**  
Self-service client registration  
Self-service protected resource registration

**Register a new protected resource**  
Use this form to register a new resource with the authorization server. You will be given a client ID and a registration access token to manage your resource.  
+ New Resource

**Edit an existing protected resource**  
Use this form to edit a previously-registered resource. Paste in your client ID and registration access token to access the client.  
Enter Client ID Enter Registration Access Token  
Edit Resource

Almost same process as registering client:

- No redirect URIs
- Same scope

API was originally accessible via the web portal, but after integration is only available machine to machine due to differing auth type used

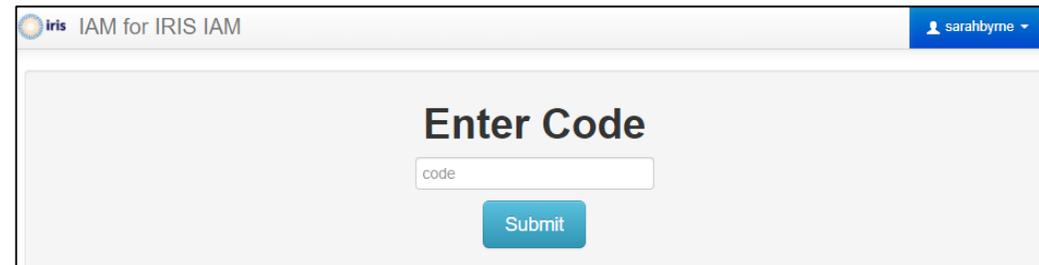
# Accessing the API with oidc-agent

oidc-agent is a set of tools you can use to manage oidc tokens, making them easily usable from the command line

```
Issuer [https://iris-iam.stfc.ac.uk/]: https://iris-iam.stfc.ac.uk
The following scopes are supported: openid profile email address phone offline_access pr
Scopes or 'max' (space separated) [openid profile offline_access]: openid profile email
Registering Client ...
Generating account configuration ...
accepted

Using a browser on another device, visit:
https://iris-iam.stfc.ac.uk/device

And enter the code: V3SOC6
```



The screenshot shows a web browser window with the title 'Iris IAM for IRIS IAM'. In the top right corner, there is a user profile icon and the name 'sarahbyrne'. The main content area is titled 'Enter Code' and contains a text input field with the placeholder text 'code' and a blue 'Submit' button below it.

Simple to generate the token and store it

```
export TOKEN=`oidc-tken --time=3600 iris-iam`
```

Ready to be used to access the API

```
curl -k -H "Authorization: Bearer $TOKEN" https://host/gocdbpi/private/?method=get_site
```

# Adding write API credentials

GOCDDB's write API requires each site to have a list of authorised credentials

- Added option for OIDC subject
- Uses regex to ensure correct format

**Add new API credential to SWITCH**

Caution: it is possible to delete information using the write functionality of the API.

Identifier (e.g. Certificate DN or OIDC Subject)\*

Credential type\*

X509

Add X509

OIDC Subject

Credentials authorised to use the GOCDDB write API (Only shown if you have the relevant permissions)

Type	Identifier	Edit	Delete
OIDC Subject	4786aefa-60eb-4fcc-996a-1ca51f9ae386		
X509	/C=UK/O=eScience/OU=CLRC/L=RAL/CN=greg.corbett		

Add new API credential

# Difference between portal and API

---

Other than the difference between client and protected resource, we also noticed a difference in the identity string seen between two access methods.

```
130.246.161.32:58916 - 4786aefa-60eb-4fcc-996a-1ca51f9ae386@iris-iam.stfc.ac.uk/  
[21/Jan/2021:12:19:55 +0000] "GET /portal/img/new_window.png HTTP/1.1" 200 454 2203 -
```

```
172.16.112.152:44818 - 4786aefa-60eb-4fcc-996a-1ca51f9ae386 [21/Jan/2021:12:29:47 +0000] "GET  
/gocdbpi/private/?method=get_site HTTP/1.1" 200 8655 3012962 -
```

Thank you

---

# Links

---

mod\_auth\_openidc: [https://github.com/zmartzone/mod\\_auth\\_openidc](https://github.com/zmartzone/mod_auth_openidc)

oidc-agent: <https://github.com/indigo-dc/oidc-agent>

IRIS IAM: <https://iris-iam.stfc.ac.uk>