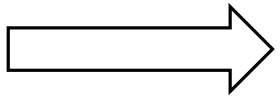
GOCDB’s Integration with IRIS IAM Service

Basic integration with IAM using OIDC



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>
```

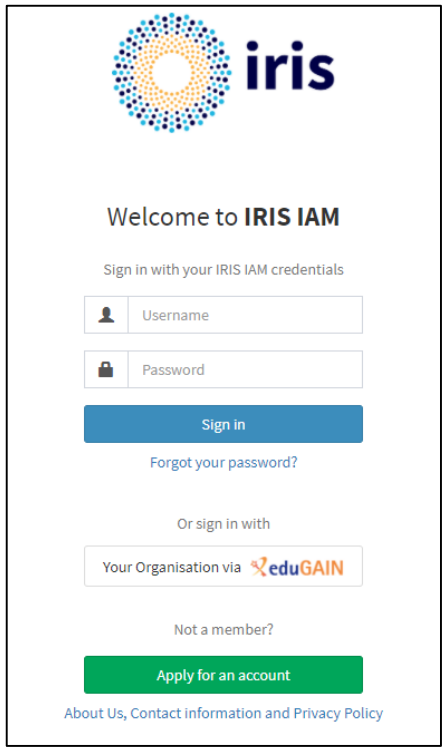
Here shows the configuration used for the web portal (above) and the API (right). Listed below are the configuration values required by mod-auth-openidc

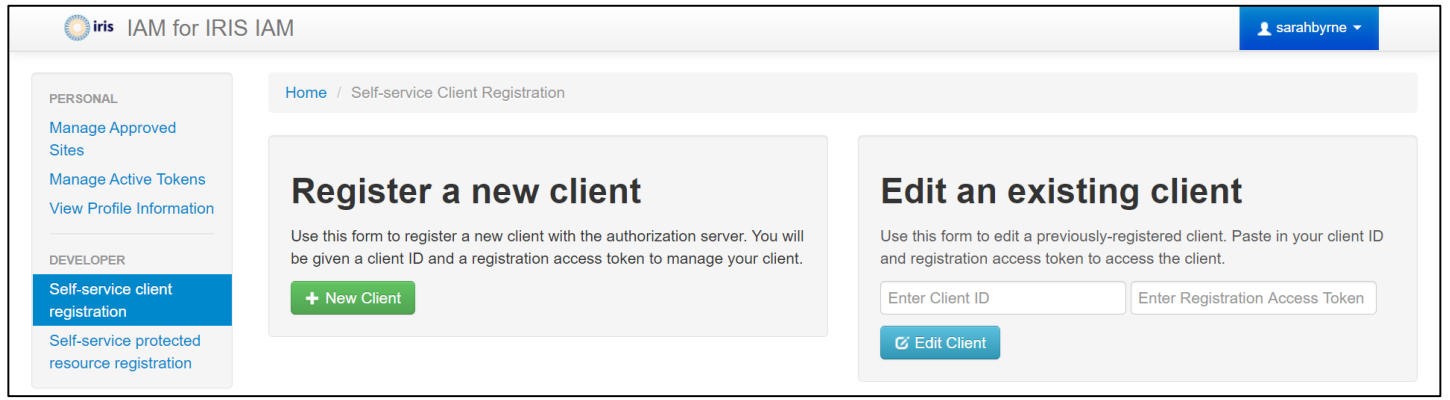
```
oidcclientid
oidcclientsecret
oidcredirecturi
oidccryptopassphrase
oidcdiscoverurl
oidcmetadatadir
```

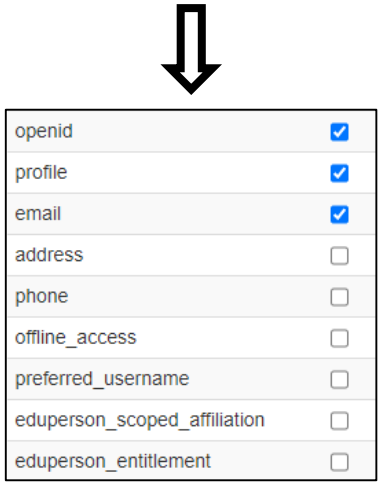
```
oidcoauthclientid
oidcoauthclientsecret
oidcoauthintrospectionendpoint
```

```
<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







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

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).

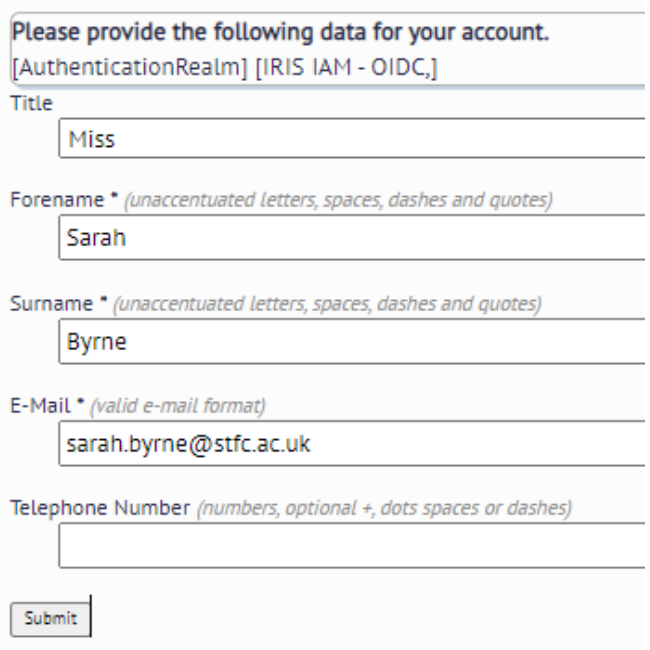
"You do not belong to the correct group to gain access to this site. Please visit iris-iam.stfc.ac.uk and submit a request to join the GOCDB group. This shall be reviewed by a GOCDB admin."

- For anyone not belonging to the gocdb group

"You must login via your organisation on IAM to gain access to this site."

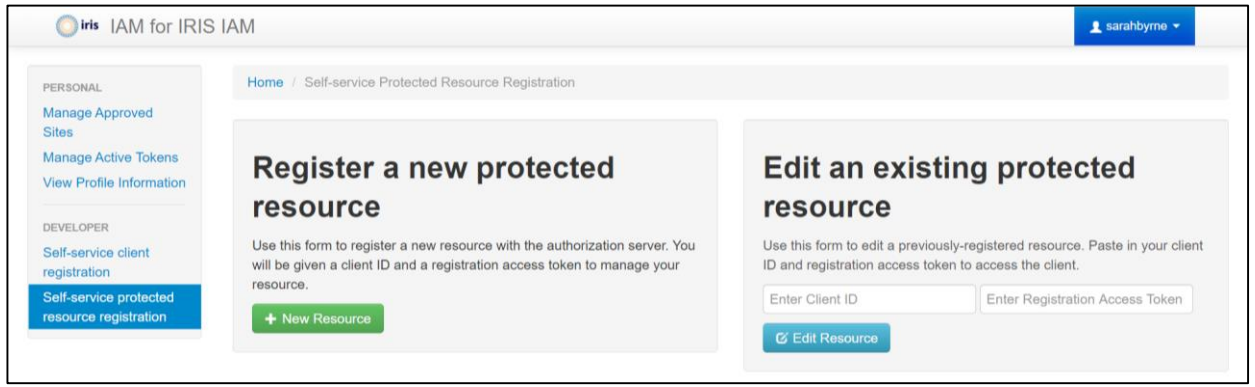
- For locally created accounts on IRIS IAM

Registering as a new GOCDB user



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

Registering as a protected resource - API



Almost same process as registering client:

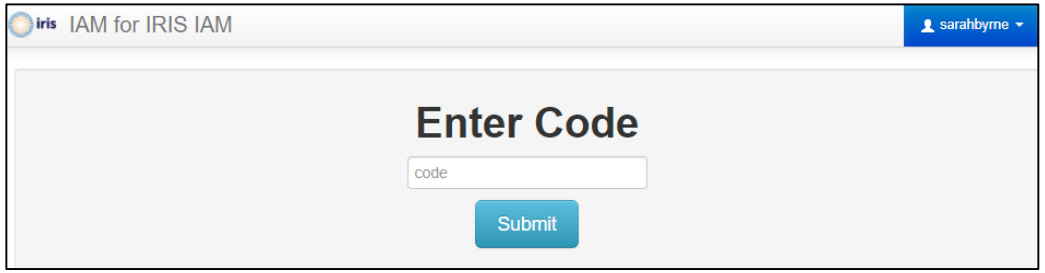
- No redirect URIs
- Same scope

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
```



Simple to generate the token and store it

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

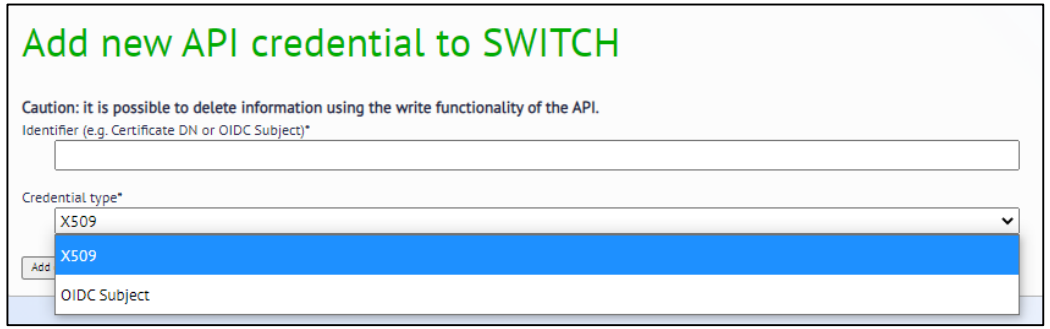
Ready to be used to access the API

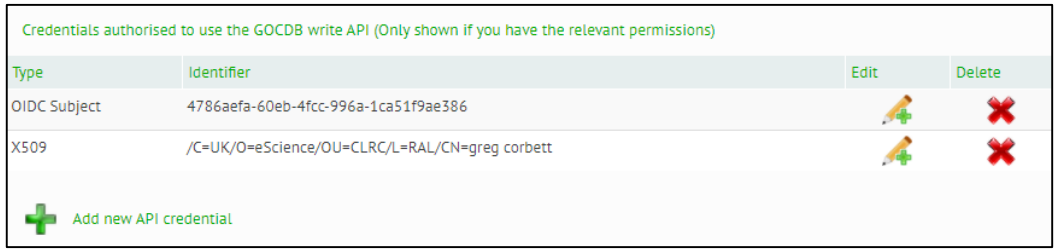
```
curl -k -H "Authorization: Bearer $TOKEN" https://host/gocdbpi/private/?method=get_site
```

Adding write API credentials

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

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





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

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

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