**OAuth2-Proxy (AZURE)**

URL: https://oauth2-proxy.github.io/oauth2-proxy/  
  
STEP 1: SETUP ON AZURE

* Login into Azure: portal.azure.com

Create App Registration

* Go to app registrations page and create new registration
* Give it a name
* In the Redirect URI section create a new Web platform entry for each app that you want to protect by the oauth2 proxy(e.g. <https://internal.yourcompany.com/oauth2/callback>)
* Click on register to create the app registration

Assign Permissions

* Next we need to add group read permissions for the app registration, on the API Permissions page of the app, click on Add a permission, select Microsoft Graph, then select Application permissions, then click on Group and select Group.Read.All. Hit Add permissions and then on Grant admin consent (you might need an admin to do this).

Create Secret

* On the Certificates & secrets page of the app, add a new client secret and note down the value after hitting Add.

STEP 2: SETUP FILES ON VIRTUAL MACHINE / LOCAL MACHINE

* Install docker and docker compose plugin  
  curl -fsSL https://get.docker.com -o get-docker.sh

sudo sh get-docker.sh

sudo apt-get install docker-compose-plugin

* Install nginx (for reverse proxy), start nginx service  
  sudo apt install nginx -y && sudo systemctl start nginx
* Install certbot (for issuing ssl certificates)  
  sudo snap install --classic certbot

sudo ln -s /snap/bin/certbot /usr/bin/certbot

* If on linux machine then, generate a random cookie secret with this command

dd if=/dev/urandom bs=32 count=1 2>/dev/null | base64 | tr -d -- '\n' | tr -- '+/' '-\_' ; echo

* If on windows machine then use this powershell command to generate a random cookie secret

# Add System.Web assembly to session, just in case

Add-Type -AssemblyName System.Web

[Convert]::ToBase64String([System.Text.Encoding]::UTF8.GetBytes([System.Web.Security.Membership]::GeneratePassword(32,4))).Replace("+","-").Replace("/","\_")

* Create a docker compose file (replace: app\_url, client\_id, client\_secret, tenant\_id, cookie\_secret)  
  nano docker-compose.yml  
  paste the below content and save the file

version: '3.8'

services:

  oauth2-proxy:

    image: quay.io/oauth2-proxy/oauth2-proxy:latest

    container\_name: oauth2\_proxy

    ports:

      - "4180:4180"

    environment:

      - OAUTH2\_PROXY\_PROVIDER=azure

      - OAUTH2\_PROXY\_CLIENT\_ID=<client\_id>

      - OAUTH2\_PROXY\_CLIENT\_SECRET=<client\_secret>

      - OAUTH2\_PROXY\_AZURE\_TENANT=<tenant\_id>

      - OAUTH2\_PROXY\_OIDC\_ISSUER\_URL=https://login.microsoftonline.com/<tenant\_id>/v2.0

      - OAUTH2\_PROXY\_EMAIL\_DOMAINS=\*

      - OAUTH2\_PROXY\_UPSTREAMS=http://nginx:80

      - OAUTH2\_PROXY\_REDIRECT\_URL=https://<app\_url>/oauth2/callback

      - OAUTH2\_PROXY\_HTTP\_ADDRESS=0.0.0.0:4180

      - OAUTH2\_PROXY\_COOKIE\_SECRET=<cookie\_secret>

      - OAUTH2\_PROXY\_SKIP\_PROVIDER\_BUTTON=true

      - OAUTH2\_PROXY\_LOGGING\_DEBUG=true

    restart: always

  nginx:

    image: nginx:latest

    container\_name: nginx

    ports:

      - "8080:80"

    depends\_on:

      - oauth2-proxy

    restart: unless-stopped

* Go to /etc/nginx/sites-available & create a new file ex: ‘oauth’  
  cd /etc/nginx/sites-available && sudo nano oauth  
  paste the below content and the save the file

upstream auth\_container {

server localhost:4180;

}

server {

server\_name <app\_url>;

location / {

proxy\_pass http://auth\_container;

proxy\_set\_header Host $host;

proxy\_set\_header X-Real-IP $remote\_addr;

proxy\_set\_header X-Forwarded-For $proxy\_add\_x\_forwarded\_for;

proxy\_set\_header X-Forwarded-Proto $scheme;

client\_max\_body\_size 200M;

}

}

* Soft link sites-available with sites-enabled  
  sudo ln -s /etc/nginx/sites-available/\* /etc/nginx/sites-enabled/
* Generate ssl certificate using certbot (make sure ‘A’ type record is created on dns management portal)  
  sudo certbot --nginx --domain <app\_url> --agree-tos --no-eff-email --non-interactive --redirect --email <your\_email>@gmail.com
* # Important information

When using the Azure Auth provider with nginx and the cookie session store you may find the cookie is too large and doesn't get passed through correctly.

Increasing the proxy\_buffer\_size in nginx should resolve this.

Just add these lines inside http block in the end.

File location is /etc/nginx/nginx.conf (Base nginx which is installed on vm)

proxy\_buffer\_size 128k;

proxy\_buffers 4 256k;

proxy\_busy\_buffers\_size 256k;

* Reload nginx service: sudo systemctl reload nginx
* Go to the directory where docker compose file is present  
  sudo docker compose up -d
* Wait for containers to start properly and then go to the <app\_url> to test the oauth login (azure)