Auth @ CERN

CSC on IT Services 2024

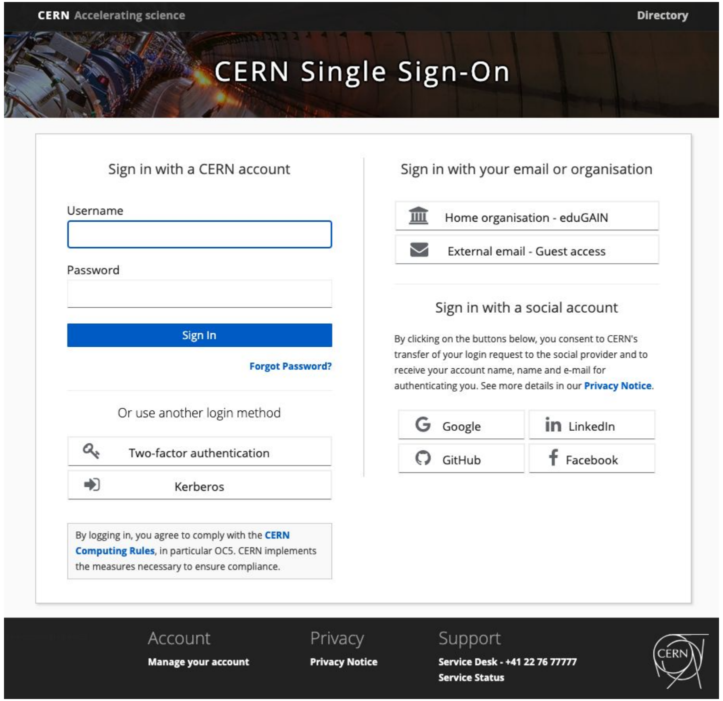
Slides and exercises by: Hannah Short , Paul Van Uytvinck and Sebastian Lopienski

Service Provided by IT-PW-IAM

What we’ll look at

- Authentication
- Exercise 0
- Exercise 1
- Authorisation
- Exercise 2
- Advanced use - calling an API
- Exercise 3

Authentication at CERN



CERN Accelerating science
Directory

CERN Single Sign-On

Sign in with a CERN account

Username

Password

Or use another login method

Two-factor authentication
Kerberos

By logging in, you agree to comply with the CERN Computing Rules, in particular OC5. CERN implements the measures necessary to ensure compliance.

Sign in with your email or organisation

Home organisation - eduGAIN
External email - Guest access

Sign in with a social account

By clicking on the buttons below, you consent to CERN's transfer of your login request to the social provider and to receive your account name, name and e-mail for authenticating you. See more details in our Privacy Notice.

Support

Service Desk - +41 22 76 77777

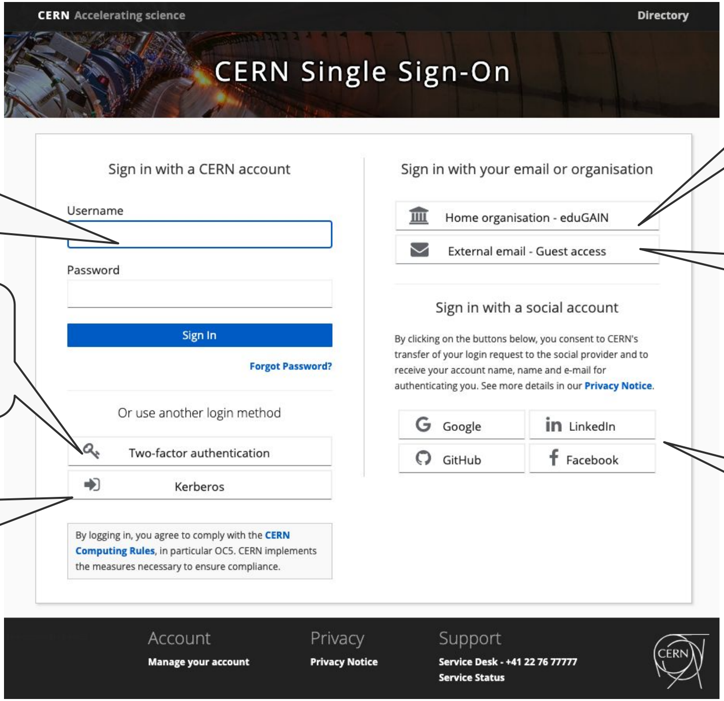
Service Status

Authentication at CERN

CERN **username & password** for an account in **Active Directory**

Just ignore this… it will disappear once everyone has 2FA for their accounts…

Kerberos with a CERN account in Active Directory



CERN Accelerating science

Directory

CERN Single Sign-On

Sign in with a CERN account

Username

Password

Sign In

Forgot Password?

Or use another login method

Two-factor authentication

Kerberos

By logging in, you agree to comply with the CERN Computing Rules, in particular OC5. CERN implements the measures necessary to ensure compliance.

Sign in with your email or organisation

Home organisation - eduGAIN

External email - Guest access

Sign in with a social account

By clicking on the buttons below, you consent to CERN's transfer of your login request to the social provider and to receive your account name, name and e-mail for authenticating you. See more details in our Privacy Notice.

Google

LinkedIn

GitHub

Facebook

Account

Manage your account

Privacy

Privacy Notice

Support

Service Desk - +41 22 76 77777

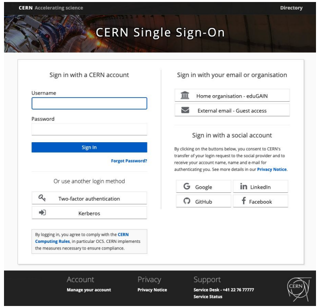
Service Status

SAML connections to eduGAIN

Inbuilt **Keycloak** users

OAuth connections to social providers

Authentication at CERN



CERN Accelerating science

Directory

CERN Single Sign-On

Sign in with a CERN account

Username

Password

Sign In

Forgot Password?

Or use another login method

Two-factor authentication

Kerberos

By logging in, you agree to comply with the CERN Computing Rules, in particular OC5. CERN implements the measures necessary to ensure compliance.

Sign in with your email or organisation

Home organisation - eduGAIN

External email - Guest access

Sign in with a social account

By clicking on the buttons below, you consent to CERN's transfer of your login request to the social provider and to receive your account name, name and e-mail for authenticating you. See more details in our Privacy Notice.

Google

LinkedIn

GitHub

Facebook

Account

Manage your account

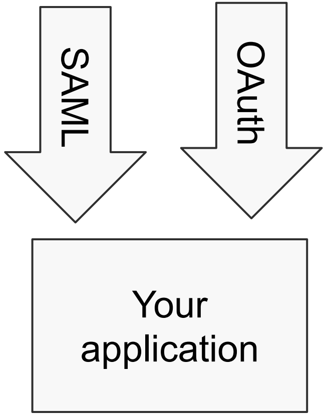
Privacy

Privacy Notice

Support

Service Desk - +41 22 76 77777

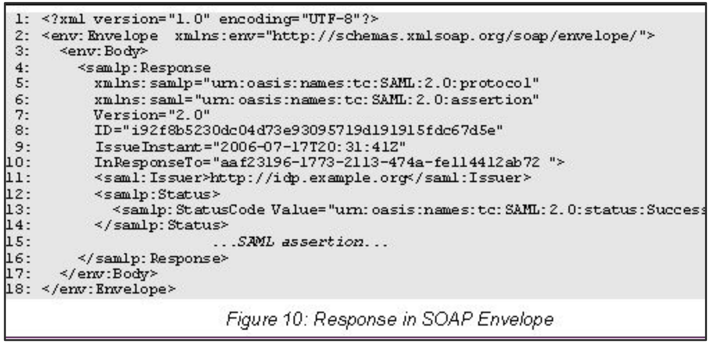
Service Status



SAML

- **Often used for Single-Sign-On implementations & older off the shelf software**
- **Limited to web services**
- **Each SAML provider provides public XML metadata that contains**
  - Signing and encryption certificates, endpoints, and various other bits
- **Authentication assertions sent as XML packets**
  - Can be encrypted or not
  - Contain user attributes, can contain authorisation
- **CERN Docs: https://auth.docs.cern.ch/user-documentation/saml/saml/**

Q: Which certificates would go into the public metadata?



```
<?xml version="1.0" encoding="UTF-8"?>
<env:Envelope  xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
  <env:Body>
    <samlp:Response
      xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
      xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
      Version="2.0"
      ID="i92f8b5230dc04d73e93095719d191915fdc67d5e"
      IssueInstant="2006-07-17T20:31:41Z"
      InResponseTo="aaf23196-1773-2113-474a-fe114412ab72 ">
      <saml:Issuer>http://idp.example.org</saml:Issuer>
      <samlp:Status>
        <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success
      </samlp:Status>
                 ...SAML assertion...
    </samlp:Response>
  </env:Body>
</env:Envelope>
```

Figure 10: Response in SOAP Envelope

http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html

OAuth & OIDC

- Uses bearer tokens, i.e. strings signed by an OAuth2 Provider
- Bearer tokens are often JSON Web Tokens (JWTs) that contain user information
- Non-web and API friendly
- OIDC (OpenID Connect) is a set profile for OAuth, that specifies a fixed set of attributes
- Client IDs and secrets
- https://auth.docs.cern.ch/user-documentation/oidc/oidc/

```
eyJhbGciOiJSUzI1NiIsInR5cCIgOiAiSldUIiwia2lkIiA6ICJWYUQzRDBQUm5QVzB5MXpBLTBieVIx
ZkhsSFVqalNFZzAxNngyY3JjaHljIn0.eyJleHAiOjE2NTQ2MDI1OTgsImlhdCI6MTY1NDYwMTM5OCwi
YXV0aF90aW1lIjoxNjU0NjAwOTc4LCJqdGkiOiI4MTUwMmM2ZS0xNGU5LTRlYjgtYTA4NC0zZThjZTMz
NDY3MjgiLCJpc3MiOiJodHRwczovL2F…qEGafQajAxfifRBniadLMEgDRHE5p1cRy2joPLU1F4MdyVLE
ypYndDdFSMl_mSkGopvWdbZpST0TMGTIXKubuy9Ia8PK-XidFWyHLVH3S00Gv1AG_TmPKskBdfGk14Qc
nYxuqecGtWnR-NzuQHNoNKaiqgPHYqh6MqbDWh_EH816J8jL2_lDTIXszx5FqYQOfGCQPbG5-C1GW-UU
Maht5smCYjWq7RmN8erD0T3ZrnIuKvOKJ7DWirTUUh_noiQlIYOqf_TK65aNTc7TiROVYYcoYDn6U36O
e_HnXxtiIgtGcM0ZdkDuVLXz7Wg
```

⇨

```
{
  "exp": 1654602388,
  "iat": 1654601188,
  "iss": "https://auth.cern.ch/auth/realms/cern",
  "aud": "oidc-attribute-viewer",
  "sub": "hshort",
  "typ": "Bearer",
  "azp": "oidc-attribute-viewer",
  "scope": "openid profile groups email",
  "name": "Hannah Short",
  "cern_mail_upn": "hshort@cern.ch",
  "preferred_username": "hshort",
  "given_name": "Hannah",
  "cern_roles": [
    "role2",
    "mfarole"
  ],
  "cern_preferred_language": "EN",
  "family_name": "Short",
  "email": "hannah.short@cern.ch",
  "eduperson_orcid": "0000-0003-2187-0980",
  "cern_upn": "hshort"
}
```

OAuth & OIDC

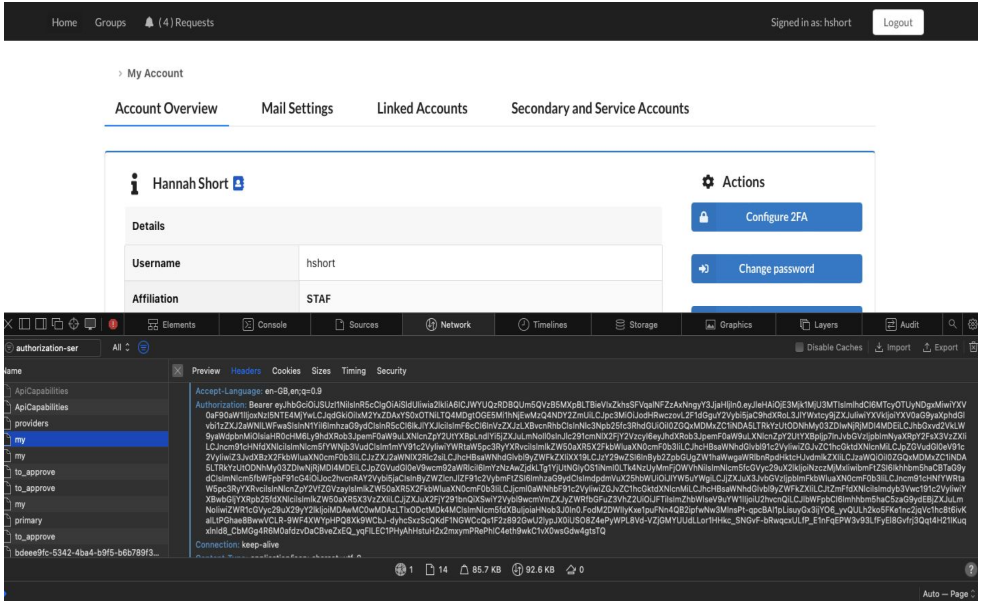
Q: Why would client secret be optional?

You can use your client ID and (optional) client secret to request tokens from CERN SSO.

Token	**Lifetime at CERN**	**Use**
Access / Bearer	20 minutes	Authorisation to clients
ID	20 minutes (but not applicable)	Snapshot of information about a user/subject
Refresh	12 hours or indefinite if offline_access scope requested	To get more access tokens

Exercise 0 - Tokens at CERN

- The Users Portal sends your token to a backend API called the Authorization Service API. Let's see how it works!
- Go to https://users-portal.web.cern.ch
- Open the web inspector, then the network tab, refresh the page and search for *authorization-service-api*
- In the web request headers you will see "Bearer A_LONG_STRING", this is your OAuth jwt token
- Go to https://jwt.io, paste your token and have a look at what's inside

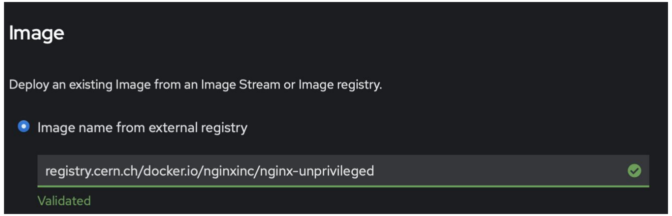


Details	
Username	hshort
Affiliation	STAF

```
Accept-Language: en-GB,en;q=0.9
Authorization: Bearer eyJhbGciOiJSUzI1NiIsInR5cCIgOiAiSldUIiwia2lkIiA6ICJWYUQzRDBQUm5QVzB5MXpBLTBieVlxZkhsSFVqalNFZzAxNngyY3JjaHljIn0.eyJleHAiOjE3Mjk1MjU3MTIsImlhdCI6MTcyOTUyNDgxMiwiYXV
    0aF90aW1lIjoxNzI5NTE4MjYwLCJqdGkiOiIxM2YxZDAxYS0xOTNiLTQ4MDgtOGE5Mi1hNjEwMzQ4NDY2ZmUiLCJpc3MiOiJodHRwczovL2F1dGguY2Vybi5jaC9hdXRoL3JlYWxtcy9jZXJuIiwiYXVkIjoiYXV0aG9yaXphdGl
    vbi1zZXJ2aWNlLWFwaSIsInN1YiI6ImhzaG9ydCIsInR5cCI6IkJlYXJlciIsImF6cCI6InVzZXJzLXBvcnRhbCIsInNlc3Npb25fc3RhdGUiOiI0ZGQxMDMxZC1iNDA5LTRkYzUtODNhMy03ZDIwNjRjMDI4MDEiLCJhbGxvd2VkLW
    9yaWdpbnMiOlsiaHR0cHM6Ly9hdXRob3JpemF0aW9uLXNlcnZpY2UtYXBpLndlYi5jZXJuLmNoIl0sInJlc291cmNlX2FjY2VzcyI6eyJhdXRob3JpemF0aW9uLXNlcnZpY2UtYXBpIjp7InJvbGVzIjpbImNyaXRpY2FsX3VzZXIi
    LCJncm91cHNfdXNlciIsImNlcm5fYWNjb3VudCIsIm1mYV91c2VyIiwiYWRtaW5pc3RyYXRvciIsImlkZW50aXR5X2FkbWluaXN0cmF0b3IiLCJhcHBsaWNhdGlvbl91c2VyIiwiZGJvZC1hcGktdXNlcnMiLCJpZGVudGl0eV91c
    2VyIiwiZ3JvdXBzX2FkbWluaXN0cmF0b3IiLCJzZXJ2aWNlX2Rlc2siLCJhcHBsaWNhdGlvbl9yZWFkZXIiXX19LCJzY29wZSI6InByb2ZpbGUgZW1haWwgaWRlbnRpdHktcHJvdmlkZXIiLCJzaWQiOiI0ZGQxMDMxZC1iNDA
    5LTRkYzUtODNhMy03ZDIwNjRjMDI4MDEiLCJpZGVudGl0eV9wcm92aWRlciI6ImYzNzAwZjdkLTg1YjUtNGIyOS1iNmI0LTk4NzUyMmFjOWVhNiIsImNlcm5fcGVyc29uX2lkIjoiNzczMjMxIiwibmFtZSI6Ikhhbm5haCBTaG9y
    dCIsImNlcm5fbWFpbF91cG4iOiJoc2hvcnRAY2Vybi5jaCIsInByZWZlcnJlZF91c2VybmFtZSI6ImhzaG9ydCIsImdpdmVuX25hbWUiOiJIYW5uYWgiLCJjZXJuX3JvbGVzIjpbImFkbWluaXN0cmF0b3IiLCJncm91cHNfYWRta
    W5pc3RyYXRvciIsInNlcnZpY2VfZGVzayIsImlkZW50aXR5X2FkbWluaXN0cmF0b3IiLCJjcml0aWNhbF91c2VyIiwiZGJvZC1hcGktdXNlcnMiLCJhcHBsaWNhdGlvbl9yZWFkZXIiLCJtZmFfdXNlciIsImdyb3Vwc191c2VyIiwiY
    XBwbGljYXRpb25fdXNlciIsImlkZW50aXR5X3VzZXIiLCJjZXJuX2FjY291bnQiXSwiY2Vybl9wcmVmZXJyZWRfbGFuZ3VhZ2UiOiJFTiIsImZhbWlseV9uYW1lIjoiU2hvcnQiLCJlbWFpbCI6Imhhbm5haC5zaG9ydEBjZXJuLm
    NoIiwiZWR1cGVyc29uX29yY2lkIjoiMDAwMC0wMDAzLTIxODctMDk4MCIsImNlcm5fdXBuIjoiaHNob3J0In0.FodM2DWIlyKxe1puFNn4QB2ipfwNw3MInsPt-qpcBAI1pLisuyGx3ijYO6_yvQULh2ko5FKe1nc2jqVc1hc8t6ivK
    alLtPGhae8BwwVCLR-9WF4XWYpHPQ8Xk9WCbJ-dyhcSxzScQKdF1NGWCcQs1F2z892GwU2lypJX0iUSO8Z4ePyWPL8Vd-VZjGMYUUdLLor1HHkc_SNGvF-bRwqcxULfP_E1nFqEPW3v93LfFyEl8Gvfrj3Qqt4H21IKuq
    xlnld8_CbMGg4R6M0afdzvDaCBveZxEQ_yqFILEC1PHyAhHstuH2x2mxymPRePhIC4eth9wkC1vX0wsGdw4gtsTQ
Connection: keep-alive
```

Exercise 1 - Authentication on Openshift

- **Open an existing Openshift (test) application**
- **If you don’t have one**
  - Create a test site at https://webservices-portal.web.cern.ch/paas and find it in https://paas.cern.ch
  - Make sure you are on “Developer” view rather than “Administrator”
  - +Add -> “Container images” -> **`registry.cern.ch/docker.io/nginxinc/nginx-unprivileged`**
  - It should create a service called “nginx-unprivileged” on port 8080



Image

Deploy an existing Image from an Image Stream or Image registry.

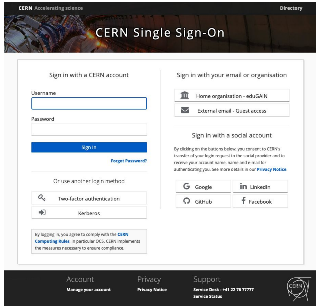
● Image name from external registry

registry.cern.ch/docker.io/nginxinc/nginx-unprivileged ✓

Validated

- **Add the SSO Proxy helm chart https://paas.docs.cern.ch/4._CERN_Authentication/2-deploy-sso-proxy/#deployment-from-openshift-console-web-ui**
  - Be careful to specify the correct service and ports for it to connect to, and the route e.g. your-paas-project.web.cern.ch

Authorisation at CERN


CERN Accelerating science
Directory

CERN Single Sign-On

Sign in with a CERN account

Username

Password

Or use another login method

Two-factor authentication
Kerberos

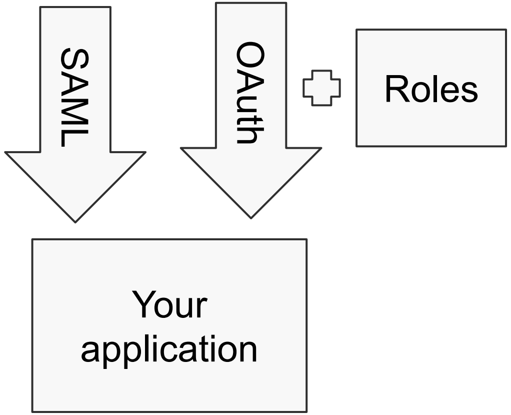
By logging in, you agree to comply with the CERN Computing Rules, in particular OC5. CERN implements the measures necessary to ensure compliance.

Sign in with your email or organisation

Home organisation - eduGAIN
External email - Guest access

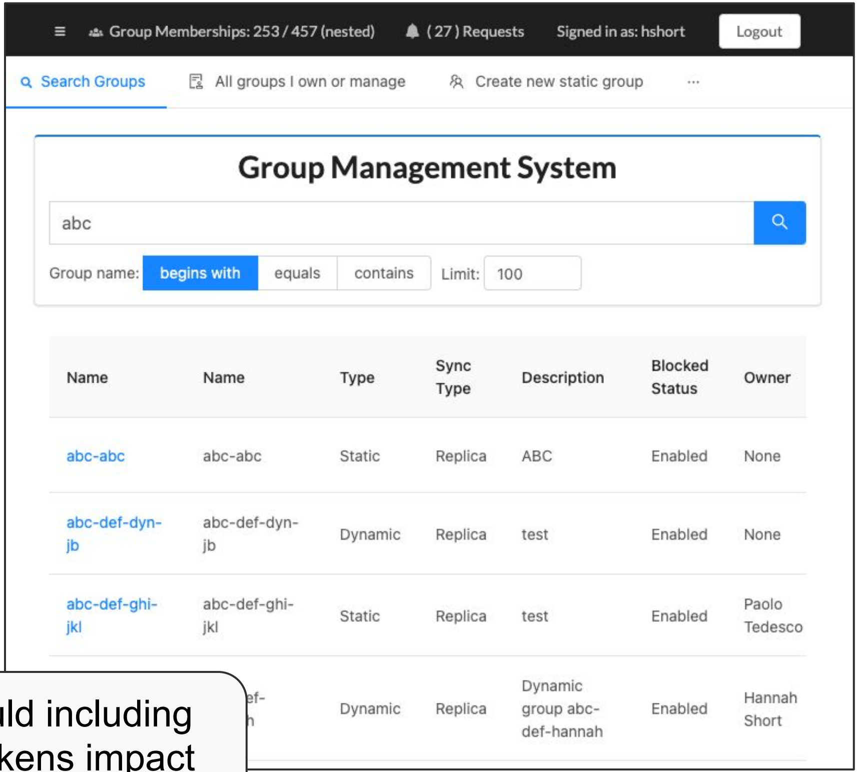
Sign in with a social account

By clicking on the buttons below, you consent to CERN's transfer of your login request to the social provider and to receive your account name, name and e-mail for authenticating you. See more details in our Privacy Notice.



Authorisation at CERN

- Unlike at many organisations, here we can define our own groups!
- Currently egroups, but the future = GMS
- To improve user privacy (and SSO usability) we do not send all groups through SSO tokens. Instead we create roles per application, that can be linked to groups as needed.



Group Management System

abc

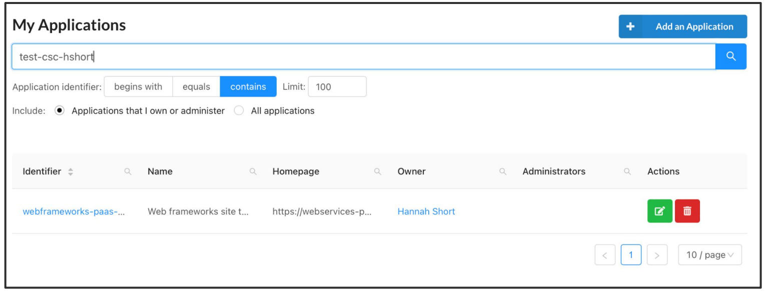
Group name: begins with | equals | contains Limit: 100

Name	Name	Type	Sync Type	Description	Blocked Status	Owner
abc-abc	abc-abc	Static	Replica	ABC	Enabled	None
abc-def-dyn-jb	abc-def-dyn-jb	Dynamic	Replica	test	Enabled	None
abc-def-ghi-jkl	abc-def-ghi-jkl	Static	Replica	test	Enabled	Paolo Tedesco
	ef- h	Dynamic	Replica	Dynamic group abc-def-hannah	Enabled	Hannah Short

Q: Why would including groups in tokens impact usability?

Exercise 2 - Authorisation on Openshift

- Find your Openshift application in https://application-portal.web.cern.ch (search for “contains” with your Openshift project name)
- Create a static group in https://groups-portal.web.cern.ch and add yourself and some colleagues from the school
- In the application portal, “Roles” tab, add a required role that is assigned to your new group (see https://auth.docs.cern.ch/applications/role-based-permissions/)
- Share your application with your colleagues and see whether they can access
- Have a look in the pod logs for the proxy in Openshift to see what’s going on



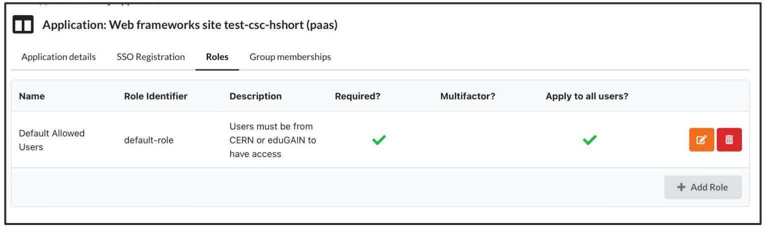
My Applications

test-csc-hshort

Application identifier: begins with | equals | contains (selected) Limit: 100

Include: ● Applications that I own or administer ○ All applications

Identifier	Name	Homepage	Owner	Administrators	Actions
webframeworks-paas-...	Web frameworks site t...	https://webservices-p...	Hannah Short		



Application: Web frameworks site test-csc-hshort (paas)

Name	Role Identifier	Description	Required?	Multifactor?	Apply to all users?
Default Allowed Users	default-role	Users must be from CERN or eduGAIN to have access	✓		✓

Don’t make Security chase you: make good choices ;)

Rule	**Why?**	**What to do?**
No local accounts	Increases security risk. Removes login traceability at CERN wide level	Disable local account options. **Use SSO**!
Do not extend user sessions	A compromised user would still be able to access your service	Use OAuth refresh tokens. Expire sessions after 12 hours.
Groups are sensitive - treat them as such	Group names can expose confidential information	Use SSO roles to receive authZ data relevant to your service
Keep secrets private	Avoid others impersonating users or services	Use Gitlab/Openshift variables/secrets, or centrally provided solutions teigi/vault
Use a well supported library	These protocols are complex and you may well miss important security steps if you implement them yourself.	https://auth.docs.cern.ch/user-documentation/oidc/libraries/

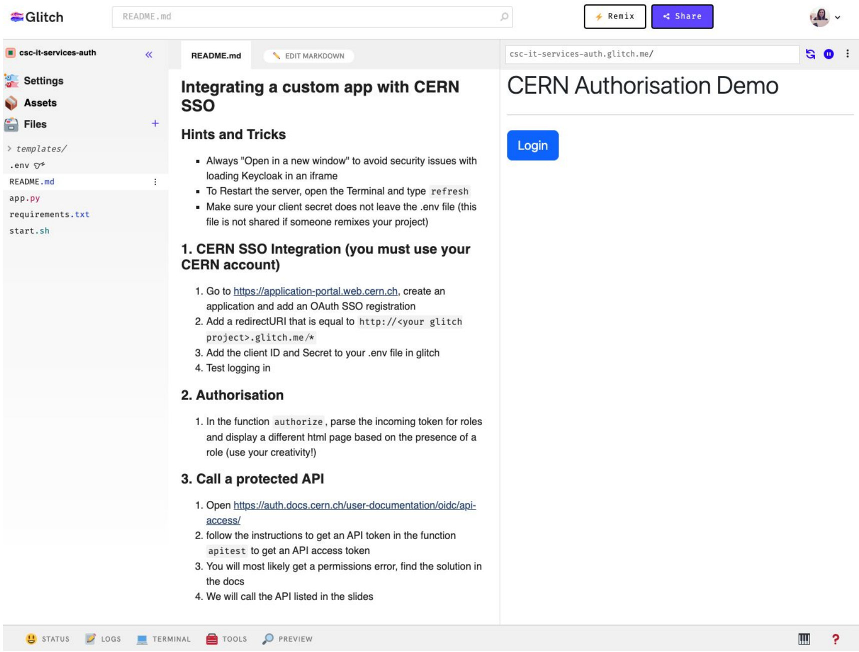
Advanced use - calling a protected API

- **API Access token endpoint**
  https://auth.docs.cern.ch/user-documentation/oidc/api-access/
  - For calling an API with your client ID and secret, much **like a service account**
  - Not OAuth standard token request, this has been developed at CERN
  - In real life the downstream API may need to add you to some roles

- **Token exchange**
  https://auth.docs.cern.ch/user-documentation/oidc/exchange-for-api/
  - For calling a downstream API **as the logged in user**
  - The downstream API will need to grant you Token Exchange permissions

Exercise 3 - Your own custom application

- Go to https://glitch.com/edit/#!/csc-it-services-auth and “remix”
- Follow the instructions in the readme (read the hints and tricks section!)
- We will call the API https://auth-test-api.web.cern.ch which accepts the token audience “auth-test-api”



Integrating a custom app with CERN SSO

Hints and Tricks

- Always "Open in a new window" to avoid security issues with loading Keycloak in an iframe
- To Restart the server, open the Terminal and type `refresh`
- Make sure your client secret does not leave the .env file (this file is not shared if someone remixes your project)

1. CERN SSO Integration (you must use your CERN account)

1. Go to https://application-portal.web.cern.ch, create an application and add an OAuth SSO registration
2. Add a redirectURI that is equal to `http://<your glitch project>.glitch.me/*`
3. Add the client ID and Secret to your .env file in glitch
4. Test logging in

2. Authorisation

1. In the function `authorize`, parse the incoming token for roles and display a different html page based on the presence of a role (use your creativity!)

3. Call a protected API

1. Open https://auth.docs.cern.ch/user-documentation/oidc/api-access/
2. follow the instructions to get an API token in the function `apitest` to get an API access token
3. You will most likely get a permissions error, find the solution in the docs
4. We will call the API listed in the slides

CERN Authorisation Demo

Login

Enjoy the school!

Thanks for participating and come back to us if you need help with authentication or authorisation