Keycloak & umbrellaID integration

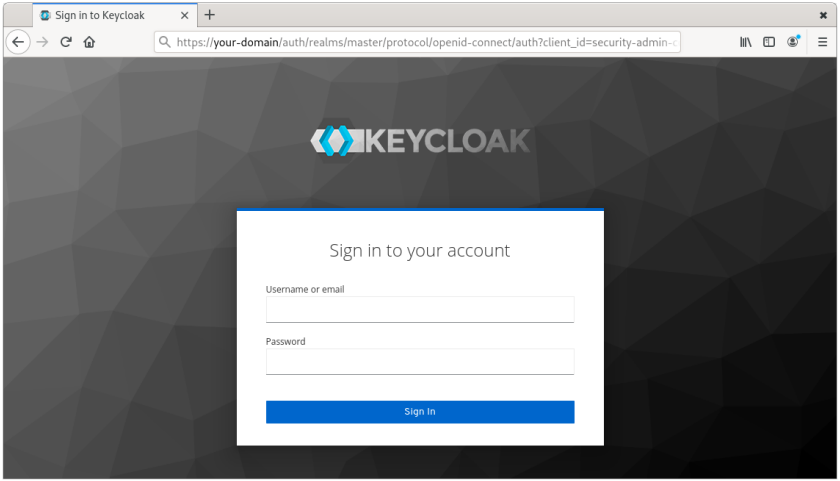
European Synchrotron Radiation Facility

May 3rd 2022

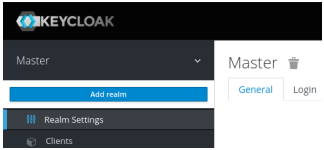
- You will need
  - A public domain name
  - Your machine exposed (or behind a reverse-proxy)
  - A valid SSL certificate for your domain

- You will need
  - A public domain name
  - Your machine exposed (or behind a reverse-proxy)
  - A valid SSL certificate for your domain
- optionnaly
  - A LDAP directory
  - An AD one
- if any, you can create local users

Login page

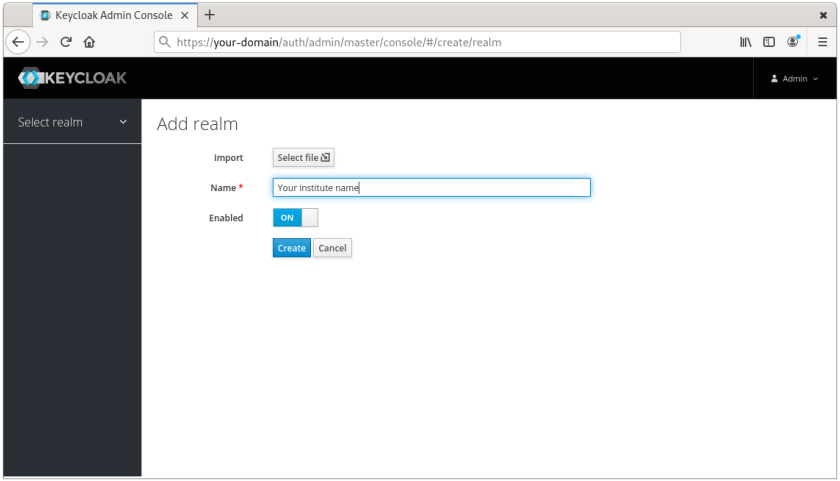

Sign in to Keycloak
https://your-domain/auth/realms/master/protocol/openid-connect/auth?client_id=security-admin-c
KEYCLOAK
Sign in to your account
Username or email
Password
Sign In

Keycloak configuration

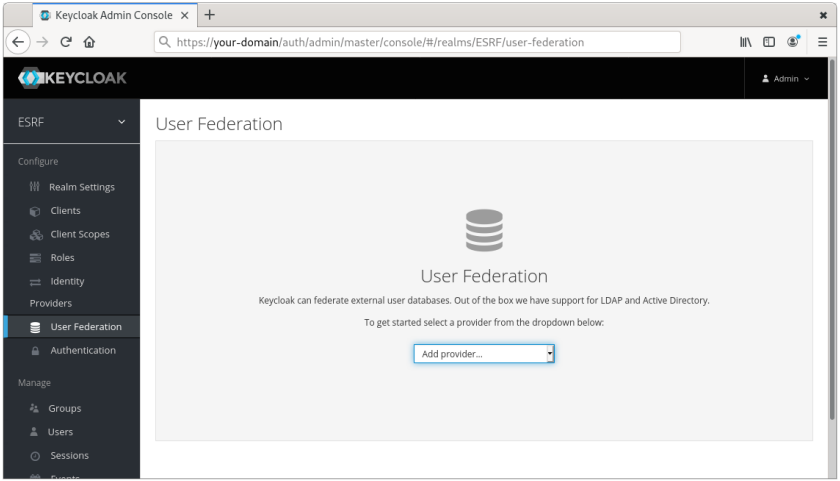


- Create a dedicated realm
  - The master realm is here for Keycloak's internals, do not use it !
  - Name it with the name of your institute

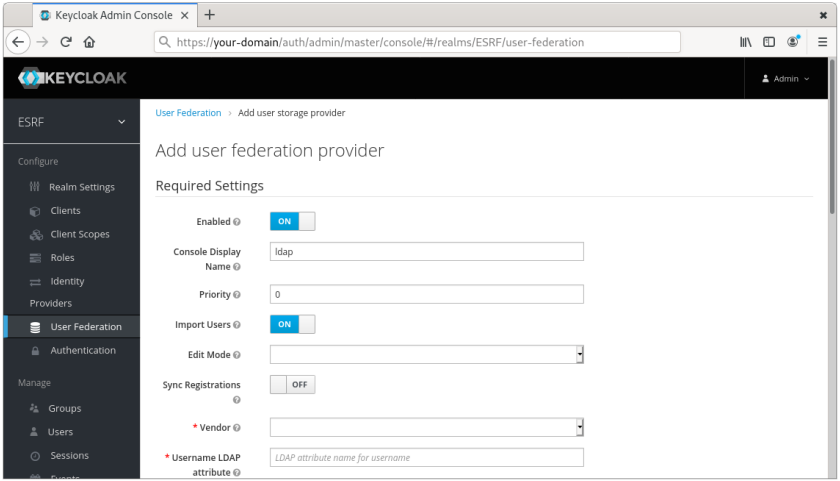
Realm creation



Add a user database (not mandatory)



Fill the form to fit your local infra

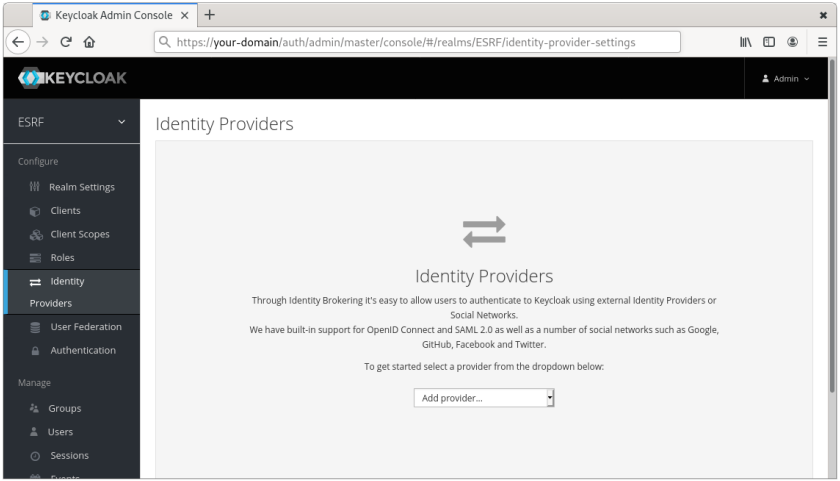


Keycloack

umbrellaID integration

Useful tools to debug SAML

Add an Identity Provider



umbrellaID configuration (SAML)

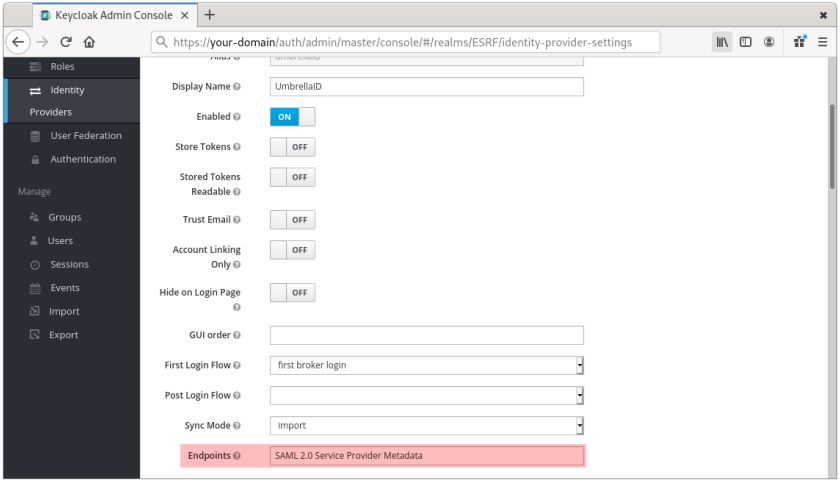
- SSO Service URL
  - `https://proxy.umbrellaid.org/saml2sp/sso/post`
  - `https://proxy.acc.umbrellaid.org/saml2sp/sso/post`
- HTTP-POST Binding Response : `True`
- HTTP-POST Binding for AuthnRequest : `True`
- Want AuthnRequests Signed : `True`
- Validate Signature : `True`

umbrellaID certificate


```
-----BEGIN CERTIFICATE-----
MIIC5DCCAcwCCQCDHiNiZPpPhTANBgkqhkiG9w0BAQsFADAOMTIwMAYDVQQDDCl1
bWJyZWxsYWlkIHByb2QgcHJveHkgc2FtbF9wcm94eV9mcm9udGVuZDAeFw0xOTA5
MTcxNjQONDVaFw0yOTA5MTQxNjQONDVaMDQxMjAwBgNVBAMMKXVtYnJlbGxhaWQg
cHJvZCBwcm94eSBzYW1sX3Byb3h5X2Zyb250OZW5kMIIBIjANBgkqhkiG9w0BAQEF
AAOCAQ8AMIIBCgKCAQEAxCF5q0f4HB4oaE/naU3LPfyy9bXwYkONoBvA/AUMqNJt
XDs0gmkqSweIEhdVKTK1fHRK3mSq5ydFywwmF1GpKS1pAxwcvLdCVqHtX7kLoLZm
KzCbuEXaOgDU5asK+JY1KNIM/nDz3MxGqSSYnZgNv/NijT2HFr+f35awkbLxyGyk
2UVWIzH8p77/TrreVg9hjlfzllJOfiznBurTXtA0EjNsfPOJktiEX+doftXID2lv
zA+ebQj2kBc/jzTOl4bHBiofhIn+J5kQh9vtqLEWqYuZi8oeRbxc3cgwfeDmYfOT
n3zsr4LE5rY1eC3hewH8bQ3Qzu4q7A1hNxBWxAAHZQIDAQABMA0GCSqGSIb3DQEB
CwUAA4IBAQA7c+FG1oz/XCtxMxUbbx2juwfR8ryQrXMDEqRcCUVKfHHFiY6YyiW/
PNeKWyGnqFlDCyle9xwK/vCkNrKmkzmmMGYehu+fTNSywqgdG3LAnkHOyGoGGIdu
pXLXNgARNqsY6p7NcpZf+Jq8SyDpmghtyQfa+Z21OaTw3bZpagNCmsS21RprC7OD
pm1Tx85+4mV0yB6EfRBbftXreDA3BQfYcpS2uvAPi9wrqnNmlrUT3JgzNSKpAVle
SqZoKykKJSILi3D/MsMiKhBNTsxVJrEL7PZ2lAq8u7lc1x4PlVZRLNkB/34dVcFt
HTw0kqEgIxumBecJbZNwpz3kwgo/PRF/
-----END CERTIFICATE-----
```


Complete metadata at https://proxy.umbrellaid.org/metadata/frontend.xml and https://proxy.acc.umbrellaid.org/metadata/frontend.xml

Give to umbrellaID your SP-metadata



Login flow

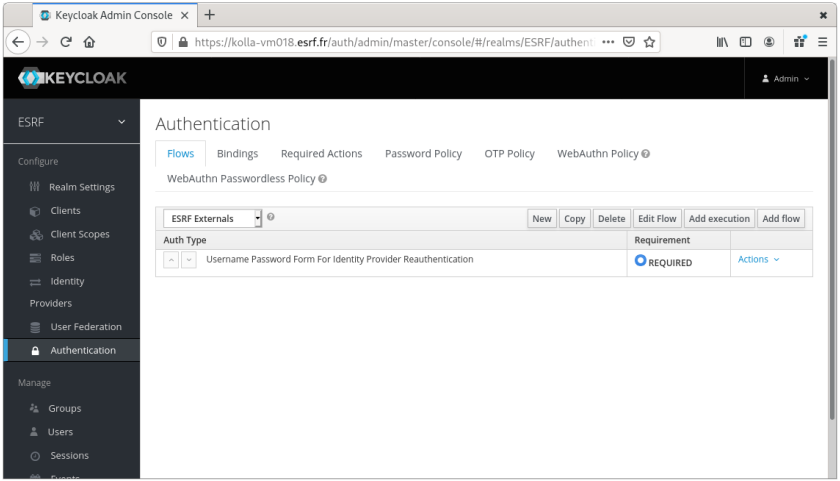
- Default Keycloak authentication flow
  - Create a new local user for each umbrellaID one
- New authentication flow needed
  - Just allowing user to link to an existing account

Login flow

- Default Keycloak authentication flow
  - Create a new local user for each umbrellaID one
- New authentication flow needed
  - Just allowing user to link to an existing account

- Authentication → Flow
- New, then Add an execution
- "Username Password Form For Identity Provider Reauthentication"

Custom authentication flow

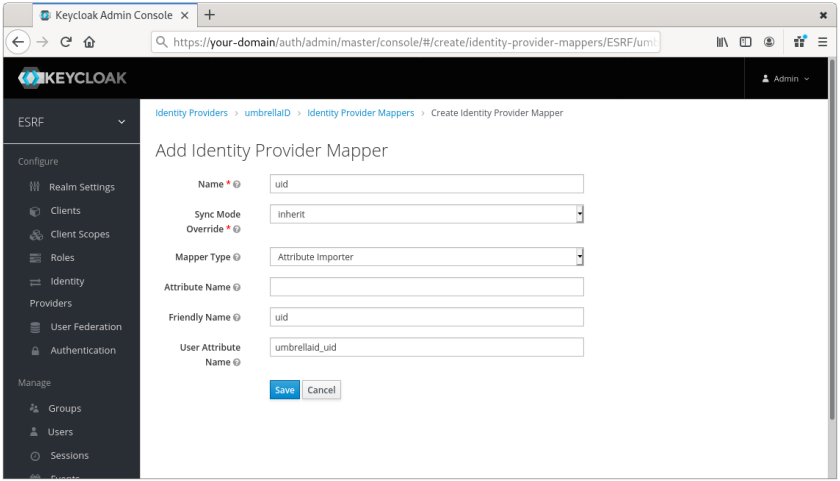


Sample SAML response from umbrellaID

```
<ns1:AttributeStatement>
    <ns1:Attribute FriendlyName="uid" Name="urn:oid:0.9.2342.19200300.100.1.1"
        NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
        <ns1:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
            xsi:type="xs:string">anroux</ns1:AttributeValue>
    </ns1:Attribute>
    <ns1:Attribute FriendlyName="eduPersonPrincipalName" Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6"
        NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
        <ns1:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
            xsi:type="xs:string">xxxxxxxx-d4d9-4b0f-b207-xxxxxxxxxxxx@umbrellaid.org</ns1:AttributeValue>
    </ns1:Attribute>
    [...]
</ns1:AttributeStatement>
```

EAAHash, EAAKey, uid, displayName, mail, cn, eduPersonTargetedID, eduPersonUniqueId, eduPersonScopedAffiliation, eduPersonAffiliation, eduPersonPrincipalName and schacHomeOrganization are returned

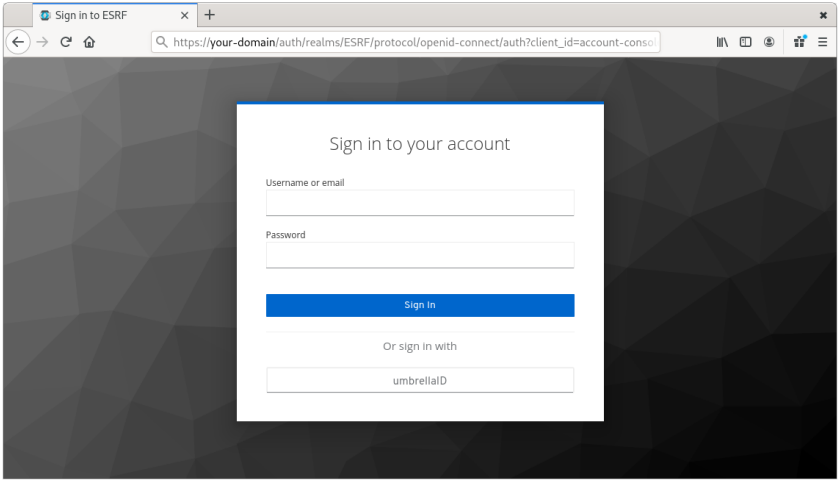
Attribute mapping



Try it at

`https://your-domain/auth/realms/YOUR-REALM/account`

The login screen with umbrellaID



- https://chrome.google.com/webstore/detail/saml-chrome-panel/paijfdbeoenhembfhkhllainmocckace