

Keycloak & umbrellaID integration

European Synchrotron Radiation Facility

May 3rd 2022



Keycloak

umbrellaID integration

Useful tools to debug SAML



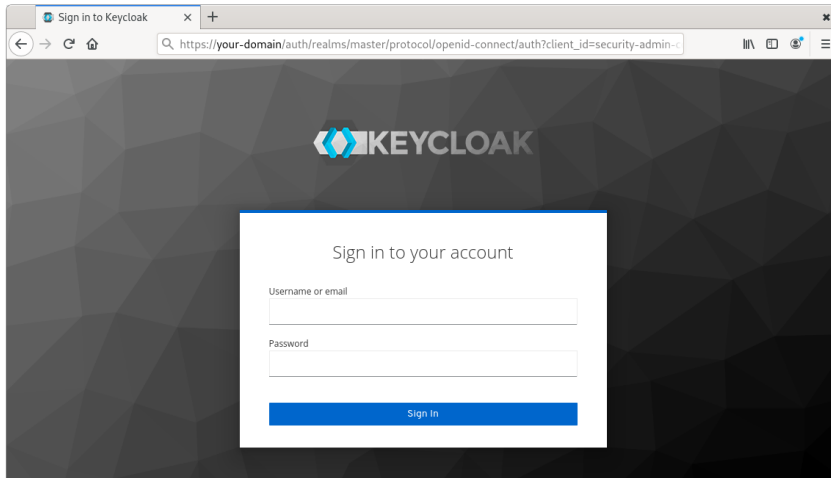


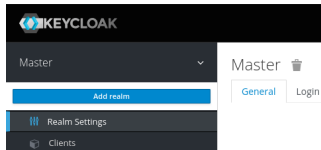
- ▶ You will need
 - ▶ A public domain name
 - ▶ Your machine exposed (or behind a reverse-proxy)
 - ▶ A valid SSL certificate for your domain



- ▶ 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

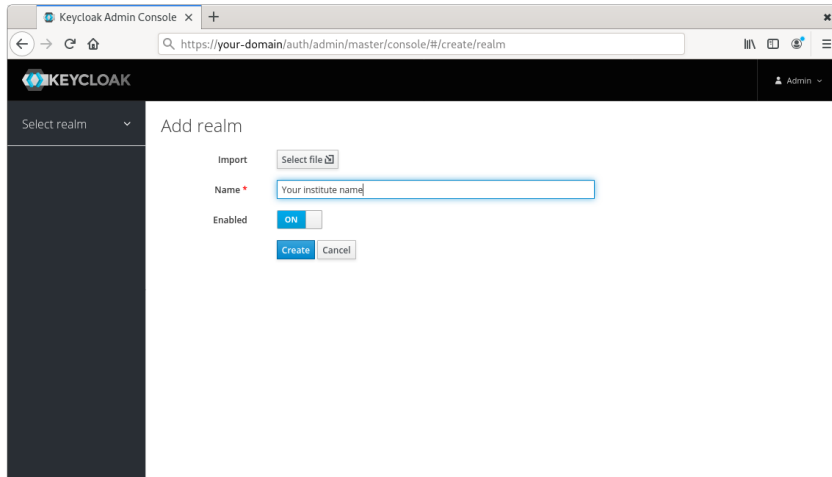
Login page



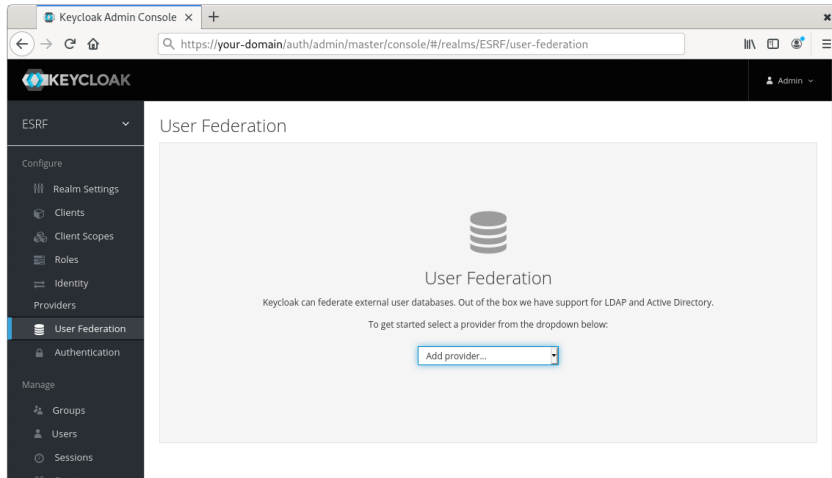


- ▶ Create a dedicated realm
 - ▶ The master realm is here for Keycloak's internals, do not use it!
 - ▶ Name it with the name of your institute

Realm creation



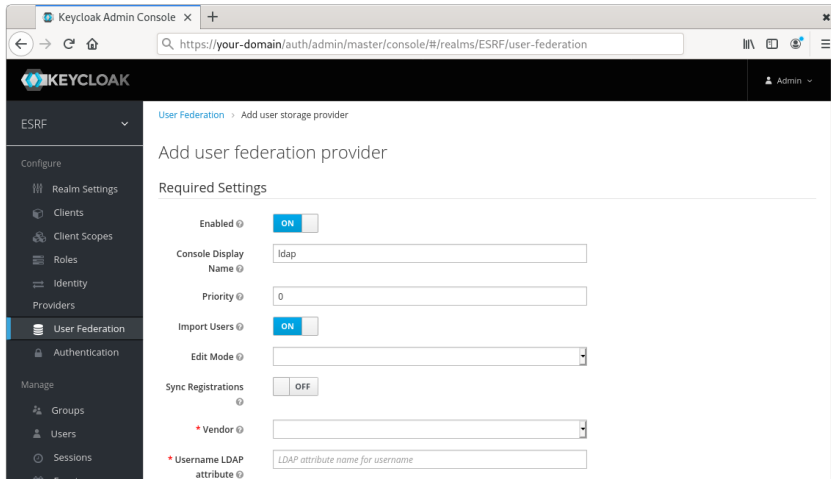
Add a user database (not mandatory)



The screenshot shows the Keycloak Admin Console interface. The browser address bar displays the URL: `https://your-domain/auth/admin/master/console/#/realms/ESRF/user-federation`. The page title is "User Federation". The left sidebar menu is expanded to show "User Federation" under the "ESRF" realm. The main content area features a database icon and the text: "User Federation. Keycloak can federate external user databases. Out of the box we have support for LDAP and Active Directory. To get started select a provider from the dropdown below." Below this text is a dropdown menu with the text "Add provider..." and a downward arrow.



Fill the form to fit your local infra



The screenshot shows the Keycloak Admin Console interface. The browser address bar displays the URL: `https://your-domain/auth/admin/master/console/#/realms/ESRF/user-federation`. The page title is "Add user federation provider". The left sidebar shows the navigation menu with "User Federation" selected. The main content area displays the "Required Settings" for adding a user federation provider:

- Enabled: ON
- Console Display Name:
- Priority:
- Import Users: ON
- Edit Mode:
- Sync Registrations: OFF
- * Vendor:
- * Username LDAP attribute:

Keycloak

umbrellaID integration

Useful tools to debug SAML



Add an Identity Provider

The screenshot shows the Keycloak Admin Console interface. The browser address bar displays the URL: `https://your-domain/auth/admin/master/console/#/realms/ESRF/identity-provider-settings`. The page title is "Identity Providers". The left sidebar contains a navigation menu with the following items: "Configure" (with sub-items: "Realm Settings", "Clients", "Client Scopes", "Roles"), "Identity" (with sub-item: "Providers"), "User Federation", "Authentication", "Manage" (with sub-items: "Groups", "Users", "Sessions", "Events"). The main content area features a large double-headed arrow icon, the heading "Identity Providers", and the following text: "Through Identity Brokering it's easy to allow users to authenticate to Keycloak using external Identity Providers or Social Networks. We have built-in support for OpenID Connect and SAML 2.0 as well as a number of social networks such as Google, GitHub, Facebook and Twitter. To get started select a provider from the dropdown below:". Below the text is a dropdown menu with the placeholder text "Add 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-----
MIIC5DCCAacwCCQCDHiNiZPpPhTANBgkqhkiG9w0BAQsFADAOMTIwMAYDVQQDDC11
bWJyZWxsYWlkIHByb2QgcHJveHkgc2FtbF9wcm94eV9mcm9udGVuZDAeFw0xOTA5
MTcxNjQONDVaFw0yOTA5MTQxNjQONDVaMDQxMjAwBgNVBAMMKXVtYnJlbGxhaWQg
cHJvZCBwcm94eSBzYW1sX3Byb3h5X2Zyb250ZW5kMIIBIjANBgkqhkiG9w0BAQEF
AAOCAQ8AMIIBCgKCAQEACF5qOf4HB4oaE/naU3LPfyy9bXwYk0NoBvA/AUMqNjT
XDsOgmKqSweIEhdVVKt1fHRK3mSq5ydFywwmF1GpKS1pAxwcvLdCVqHtX7kLoLZm
KzCbuEXaOgDU5asK+JY1KNIM/nDz3MxGqSSYnZgNv/NijT2HFr+f35awkbLxyGyk
2UUVWIZH8p77/TrreVg9hJfz11J0fiznBurTXtA0EjNsfP0JktiEX+dofTXID21v
zA+ebQj2kBc/jzT014bHBiofhIn+J5kQh9vtqLEWqYuZi8oeRbxc3cgwfeDmYfOT
n3zsr4LE5rY1eC3hewH8bQ3Qzu4q7A1hnxBWxAAHZQIDAQABMAOGCSqGSIb3DQEB
CwUAA4IBAQA7c+FG1oz/XCtXmXUbbx2juwFR8ryQrXMDEqRcCUVKfHHFiY6YyiW/
PNeKWyGnqF1DCyle9xwK/vCkNrKmkzmmMGYehufTNSywgqgdG3LAnkH0yGoGGIdu
pXLXNgARnqsY6p7NcpZf+Jq8SyDpmghtyQfa+Z210aTw3bZpagNCmsS21RprC70D
pm1Tx85+4mV0yB6EfrBbftXreDA3BQfYcpS2uvAPi9wrqnNmlrUT3JgzNSKpAVLe
SqZoKyKJSILi3D/MsMiKhBNTsxVJrEL7PZ21Aq8u71c1x4P1VZRLNkE/34dVcFt
HTwOkqEgIxumBecJbZnWpz3kwgo/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

The screenshot shows the Keycloak Admin Console interface. The left sidebar contains navigation options: Roles, Identity, Providers, User Federation, Authentication, Manage, Groups, Users, Sessions, Events, Import, and Export. The main content area displays the configuration for an identity provider named 'UmbrellaID'. The configuration includes several toggle switches and dropdown menus:

- Display Name: UmbrellaID
- Enabled: ON
- Store Tokens: OFF
- Stored Tokens Readable: OFF
- Trust Email: OFF
- Account Linking Only: OFF
- Hide on Login Page: OFF
- GUI order: (empty text input)
- First Login Flow: first broker login
- Post Login Flow: (empty dropdown)
- Sync Mode: import
- Endpoints: SAML 2.0 Service Provider Metadata (highlighted in red)



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

The screenshot shows the Keycloak Admin Console interface. The browser address bar indicates the URL: `https://kolla-vm018.esrf.fr/auth/admin/master/console/#/realms/ESRF/authentication`. The page title is "Authentication" and the user is logged in as "Admin".

The left sidebar shows the navigation menu with the following items:

- ESRF (selected)
- Configure
 - Realm Settings
 - Clients
 - Client Scopes
 - Roles
 - Identity
 - Providers
 - User Federation
 - Authentication (selected)
- Manage
 - Groups
 - Users
 - Sessions
 - Events

The main content area shows the "Authentication" configuration for the "ESRF" realm. The "Flows" tab is active, and the "WebAuthn Passwordless Policy" is visible. Below this, there is a table of authentication flows:

Auth Type	Requirement	Actions
ESRF Externals		
Username Password Form For Identity Provider Reauthentication	REQUIRED	Actions



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 schachHomeOrganization are returned



Attribute mapping

Keycloak Admin Console x +

https://your-domain/auth/admin/master/console/#/create/identity-provider-mappers/ESRF/uml

KEYCLOAK Admin

ESRF

Identity Providers > umbrellaID > Identity Provider Mappers > Create Identity Provider Mapper

Add Identity Provider Mapper

Name *

Sync Mode

Override *

Mapper Type

Attribute Name

Friendly Name

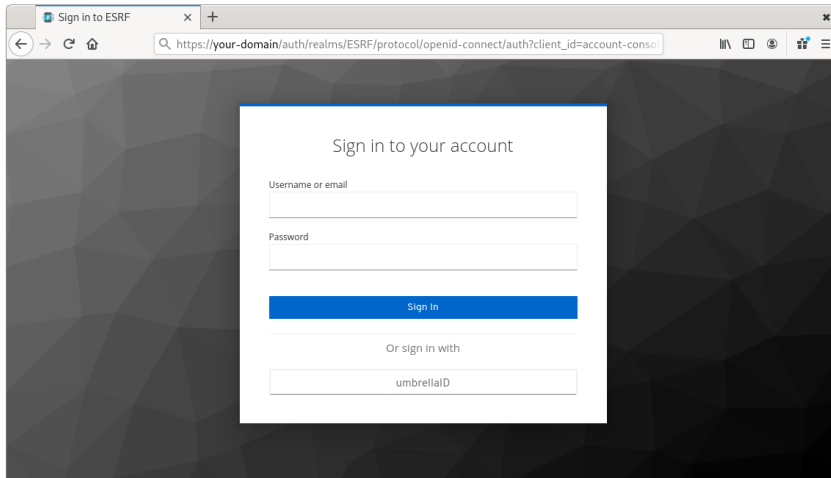
User Attribute Name

Try it at

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



The login screen with umbrellaID



Keycloak

umbrellaID integration

Useful tools to debug SAML





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