

France Connect

OIDC France connect

La création d'un compte d'administration sur France connect sera nécessaire afin d'enregistrer l'adresse du serveur de demande, utilisé notamment lors de la redirection effectuée apres l'authentification sur France Connect.

\$home/cas/build.gradle

```
dependencies {  
    compile "org.apereo.cas:cas-server-support-pac4j-webflow:${project.'cas.version'}"  
}
```

\$home/etc/cas/config/cas.properties

```
#Rajoute un prefix sur l'ID  
cas.authn.pac4j.typedIdUsed=true  
#information à recuperer a partir du compte franceConnect  
cas.authn.pac4j.oidc[0].clientName=FranceConnect  
cas.authn.pac4j.oidc[0].id=Find_your_id_on_france_connect  
cas.authn.pac4j.oidc[0].secret=Find_your_key_on_france_connect  
# ce fichier devrait etre fourni par france connect mais dans notre cas ne l'est pas  
cas.authn.pac4j.oidc[0].discoveryUri=http://localhost/cas/france_connect/fc.json  
cas.authn.pac4j.oidc[0].useNonce=true  
cas.authn.pac4j.oidc[0].preferredJwsAlgorithm=HS256  
# Une erreur apparait sur la version 5.0 si cette option n'est pas activé  
cas.authn.pac4j.oidc[0].maxClockSkew=1
```

Contenu du fichier http://localhost/cas/france_connect/fc.json

fc.json

```
{
  "issuer": "https://fcp.integ01.dev-franceconnect.fr",
  "authorization_endpoint": "https://fcp.integ01.dev-franceconnect.fr/api/v1/authorize",
  "token_endpoint": "https://fcp.integ01.dev-franceconnect.fr/api/v1/token",
  "userinfo_endpoint": "https://fcp.integ01.dev-franceconnect.fr/api/v1/userinfo",
  "end_session_endpoint": "https://fcp.integ01.dev-franceconnect.fr/api/v1/logout",
  "jwks_uri": "http://non_necessaire_pour_fc_mais_obligatoire_dapres_la_spec_oidc",
  "response_types_supported": [
    "code",
    "token",
    "id_token",
    "none"
  ],
  "subject_types_supported": [
    "public"
  ],
  "id_token_signing_alg_values_supported": [
    "HS256"
  ],
  "scopes_supported": [
    "openid",
    "email",
    "birth",
    "profile"
  ],
  "token_endpoint_auth_methods_supported": [
    "client_secret_post"
  ],
  "claims_supported": [
    "aud",
    "email",
    "email_verified",
    "exp",
    "family_name",
    "given_name",
    "iat",
    "iss",
    "locale",
    "name",
    "phone",
    "address",
    "birthcountry",
    "birthplace",
    "gender",
    "preferred_username",
    "sub"
  ],
  "code_challenge_methods_supported": [
    "plain",
    "S256"
  ]
}
```

Ajouter le lien entre OIDC ID et UID

Un [article](#) a été créé sur le blog de Apereo, expliquant la mise en place du code.

Cette article repose sur deux projets Github:

1. [Le code afin de modifier CAS pour communiquer les informations OIDC](#)
2. [Le serveur reliant les IDS](#)

Pour résumer, 3 étapes seront nécessaire :

1. Ajouter le nouveau code dans cas/src
2. Ajouter / Modifiez les fichiers de service nécessaire
3. Mettre en place le serveur claExternalID

Ajouter le nouveau code dans cas/src

Un bug est présent dans le package `OIDC Pac4j`, l'url de redirection `"unauthorizedRedirectUrl"` de `"accessStrategy"` provenant du service ne fonctionne pas en CAS v5.2.2. Vous devrez ajouter manuellement un patch. Copier le contenu du repository dans le dossier `cas/src`. Repackager ensuite.

Allez dans le repository <https://github.com/EsupPortail/cas-server-support-claExternalID/tree/5.2.x>, prenez le contenu de `src` et copiez le dans `"$home/cas/src"`

Ajouter / Modifiez les fichiers de service nécessaire

Suivez la description du `README.md` du [projet claExternalID](#) dans la section `#integration-dans-cas`

Ajoutez ainsi le fichier `claExternalID-Associate-55.json` et modifiez le fichier `all-01.json` avec le code donné.

Mettre en place le serveur claExternalID

Faites un git clone et suivez le `README`