Holder group login

- Holder group login
- Steps to configure
- Use cases

Holder group login

Introduction

In some organizations is necessary to assign roles that affect only a part of the structure, for instance, a department, a division or a country. A **Holder Group** can be defined as a collection of entities (referred to as "holders") that share similar characteristics, roles, permissions, or access requirements. The concept of a Holder Group simplifies the management of identities by enabling administrators to apply policies, assign roles, and manage permissions at the group level rather than individually.

The Soffid federation allows a new way to login, the **Holder group login**. This new way, allows the user to login to applications, Service Provider, indicating with which group the user wants to log in. Soffid will share with the application the roles and permissions according to the selected group.

If you want an application to allow Holder group login, the option Ask for group membership after authentication of the Service Provider must be activated (Yes option selected).

Once the user has logged in using the federation, Soffid will share with the Service Provider application the following information:

- **Holder group**: Group selected by the user when logging in.
- **Roles list**:
  - Roles directly assigned to the user.
  - Roles assigned to the user in compliance with a Role Assignment Rule.
  - Roles assigned in the group selected by the user when logging in.
- **Scope**: the scope will be shared when you try to log in using OpenID-Connect.

How Holder group login works?

1. The user is not logged in to the Identity Provider.

1.1. The user type the user and password into the Identity Provider.

1.2. The Identity Provider validates the user credentials, and requires a 2FA if it is necessary.

1.2.1. If the credentials are not correct, an error message is displayed.

1.2.2. If the credentials are correct, the Identity Provider get a list of all groups to which the user can log in. This list is obtained by selecting all groups, primary and/or

secondary, that have as type one with Rol holder Yes. The groups are not repeated in this list.

1.2.2.1. If there is no group with these characteristics, the Identity Provider automatically logs the user, and shares the data with the Service Provider.

1.2.2.2. If there is only one group with these characteristics, the Identity Provider automatically logs the user into this group, and shares the data with the Service Provider.

1.2.2.3. If there is more than one group, the Identity Provider displays a list of the groups for the user to select which one to log in to. Here the user selects the group and logs in, then Identity Provider shares the updated data with the Service Provider.

2. The user is already logged in to the Identity Provider.

2.1. The user login to a new application, Service Provider.

2.2. The Identity Provider checks if there are any additional adaptive rules required to perform the login.

2.2.1. If the credentials are not correct, an error message is displayed.

2.2.2. If the credentials are correct, the user logs in to the application with the group to which the user was previously logged in. The Identity Provider shares the updated data with the Service Provider, so if there have been any changes in the user's roles, these updates are reflected in the shared data.

Service providers that allow Holder group login

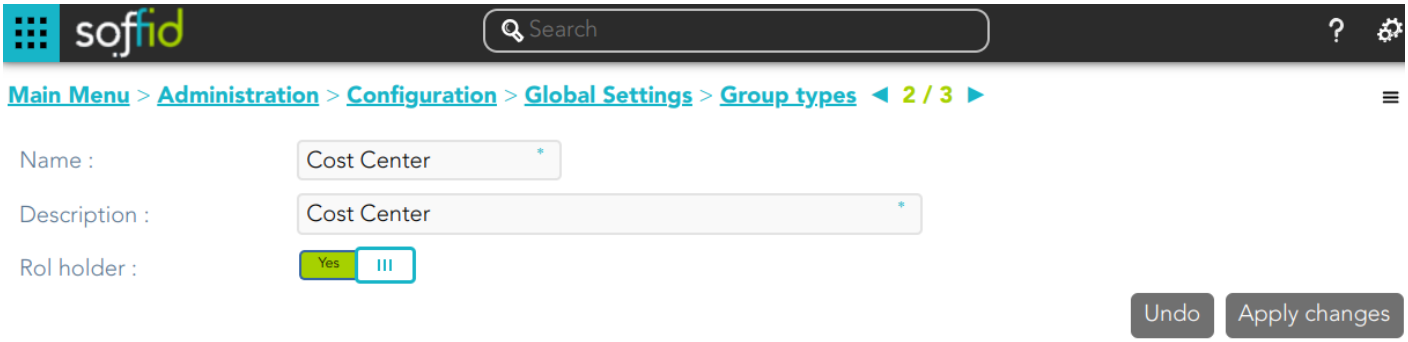
The following Service Providers allow you to configure the login with Holder group

- SAML
- SAML API client
- OpenID-Connect
- CAS client

Steps to configure

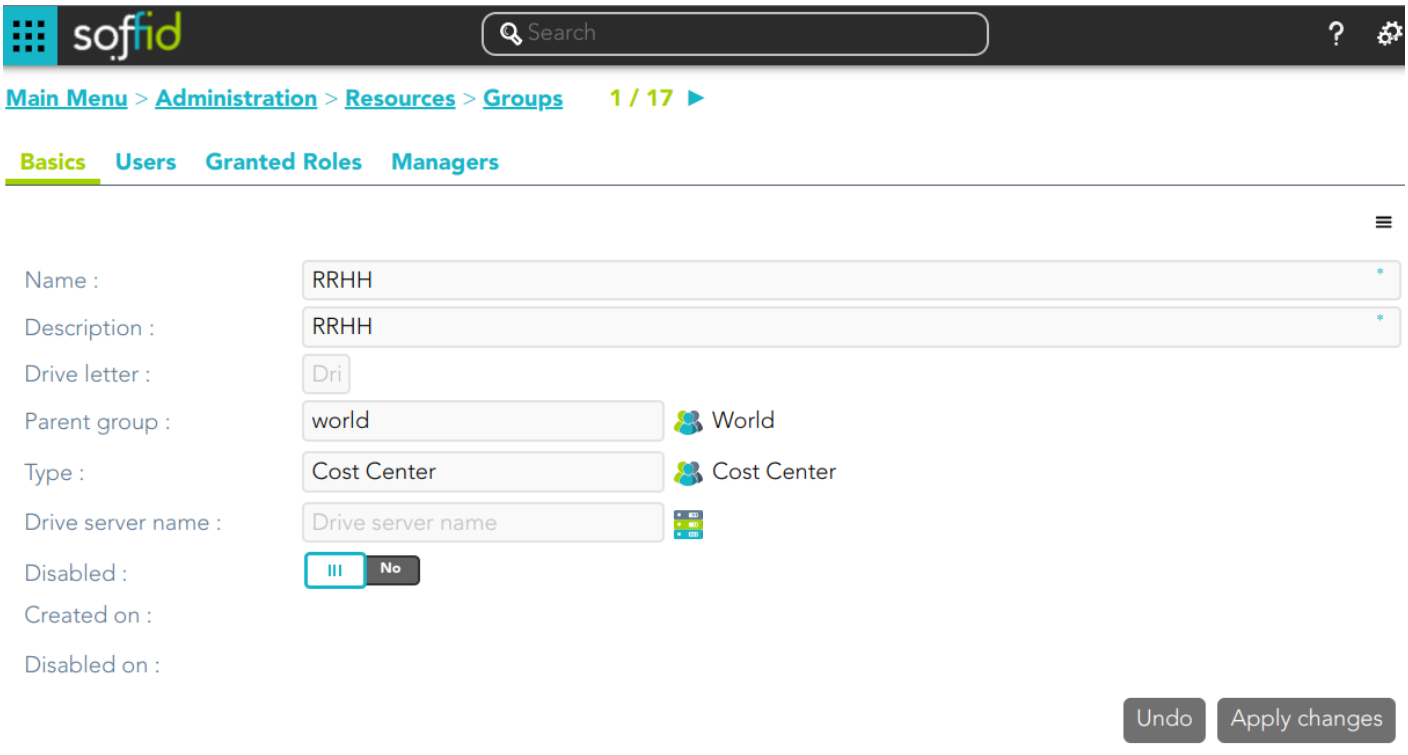
Steps to configure

1. **Group type:** Create at least one organizational unit with the role holder attribute active (yes).



https://bookstack.soffid.com/books/soffid-3-reference-guide/page/group-type

2. Groups: Assign Groups to the organizational unit. Define groups with the appropriate group type.

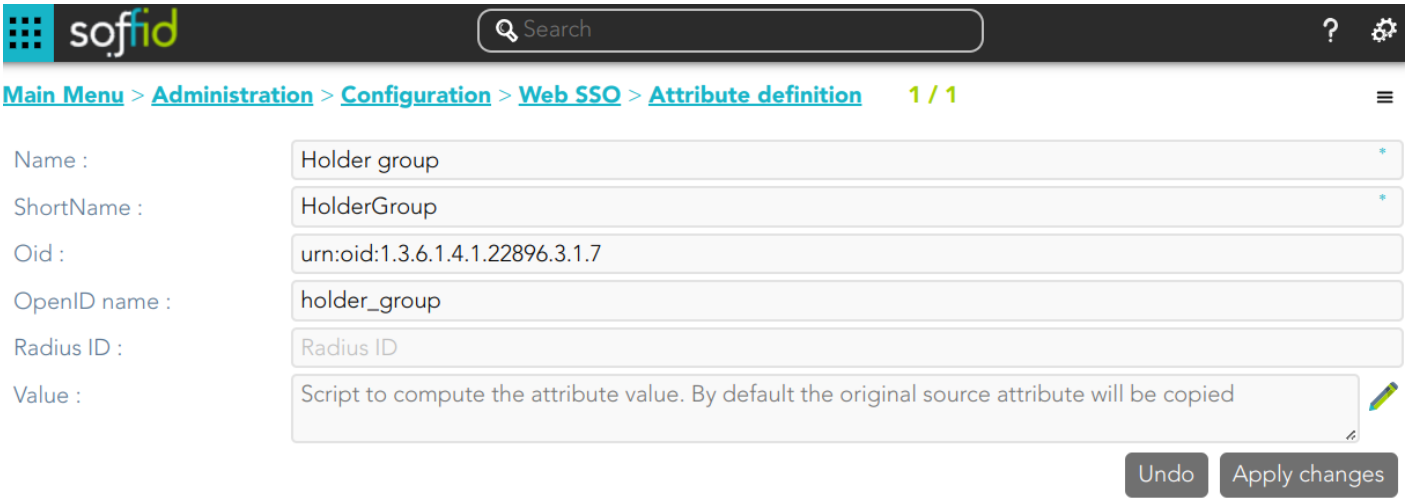


https://bookstack.soffid.com/books/soffid-3-reference-guide/page/groups

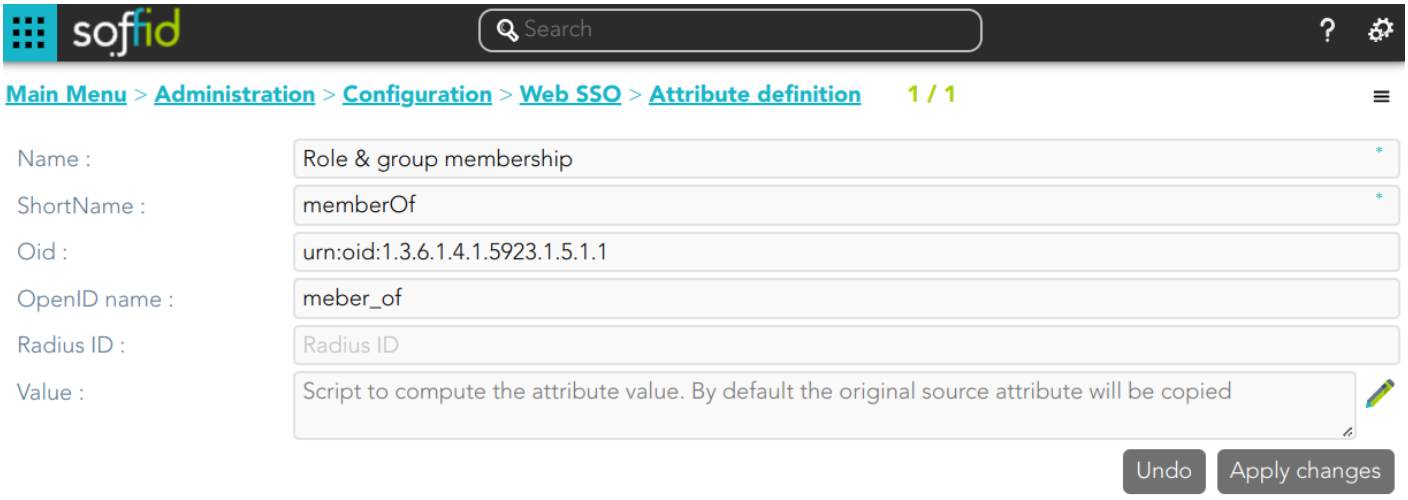
3. Custom attributes: (Optional) You can include new custom attributes to this membership relationship, go to Metadata page and select the GroupUser to add these attributes.

4. Attribute definition: Define the **Attributes to deliver** from the identity providers to the service providers

4.1. Holder group

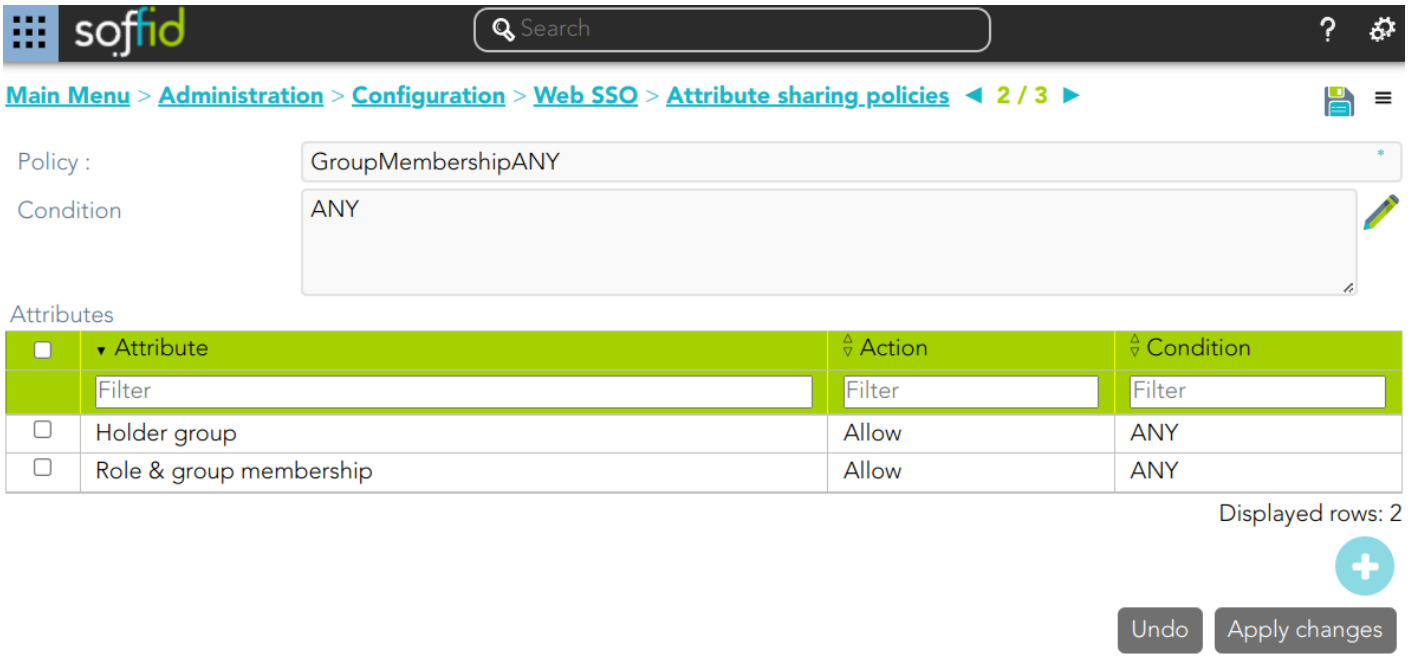


4.2. Role & group membership

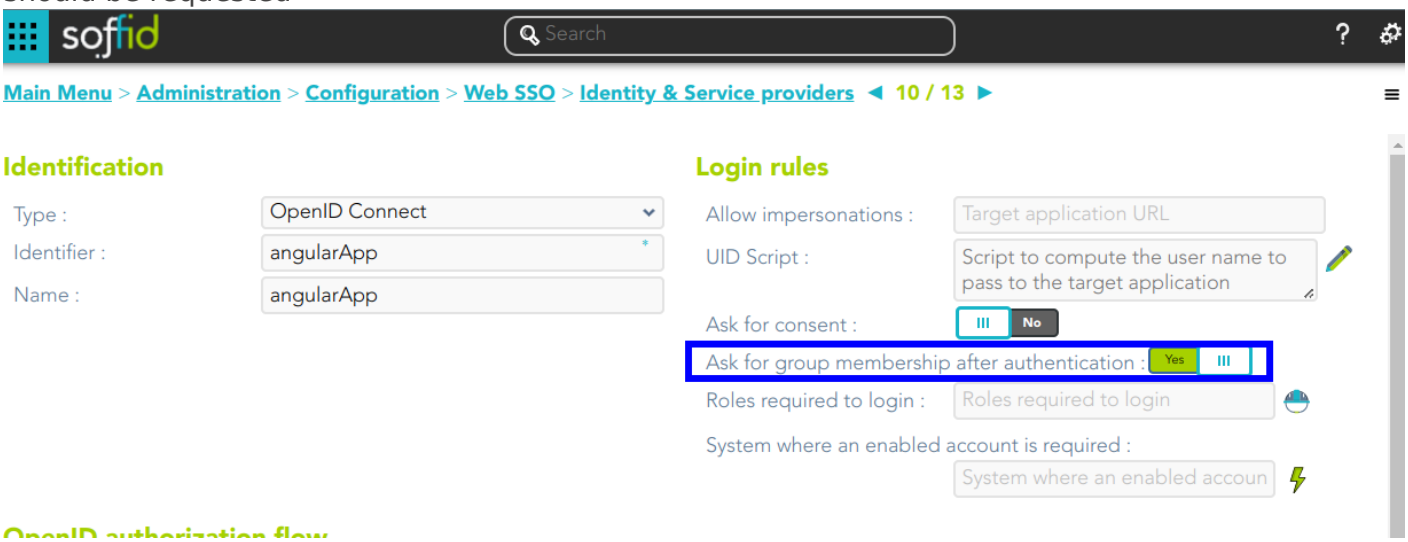


5. Attribute sharing policies: Define the policies to share the attributes with each service provider.

In this case, the Holder group, and Role & group membership attributes will be always shared.



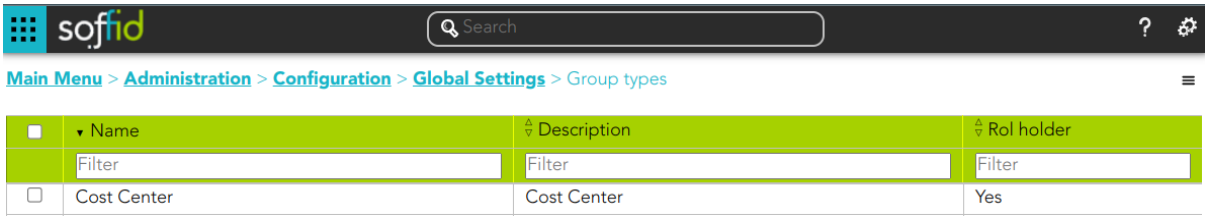
6. Service Provider: Configure the service providers, indicating in which ones the headline group should be requested



Use cases

Premises

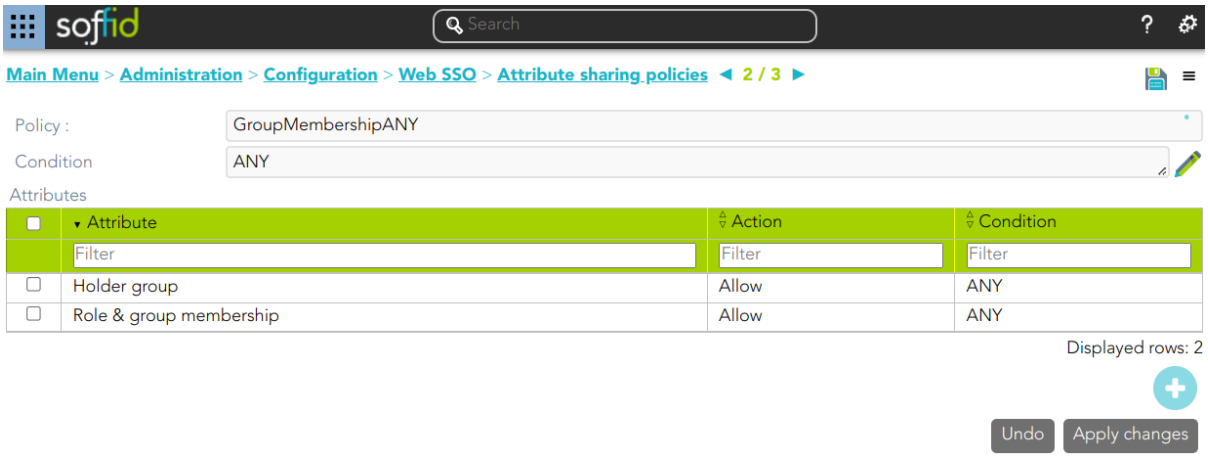
1. An Organizational Unit has been defined as Role holder Yes.



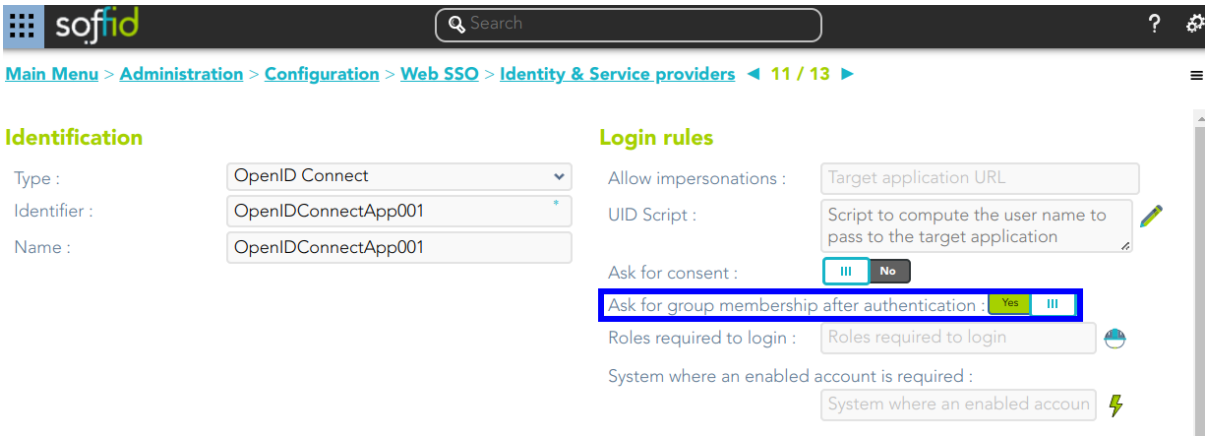
2. Several groups have been defined with type organizational unit with role holder Yes.



3. An attribute sharing policy has been defined.



4. Indicates which Service Providers will be required group membership after authentication.



Use cases

Use case 1 - Log in to an application

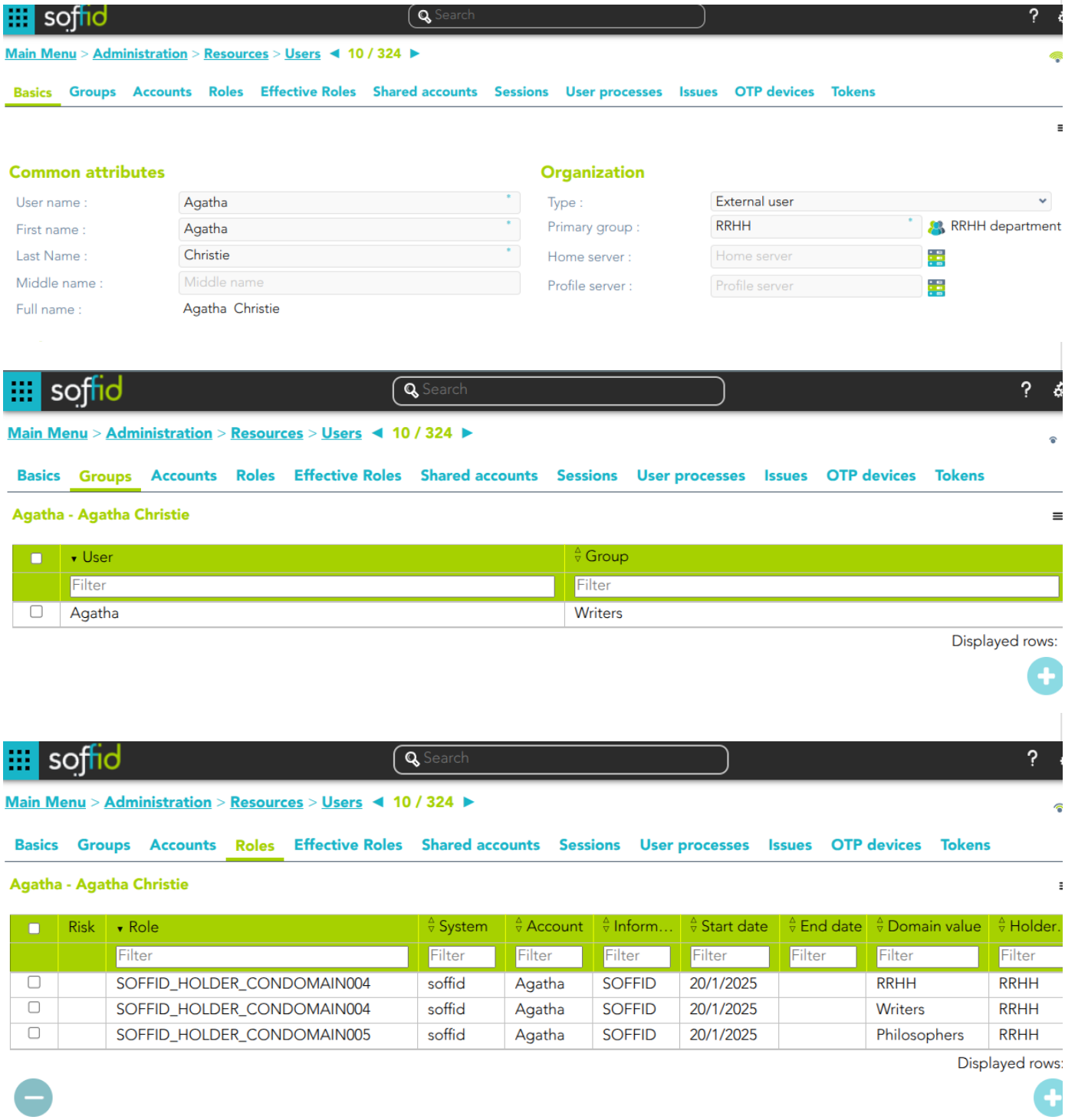
User with no groups, Primary or Secundary, with type holder group Yes. When this user log into an application --> The user login normally to the application

Use case 2 - Log in to an application

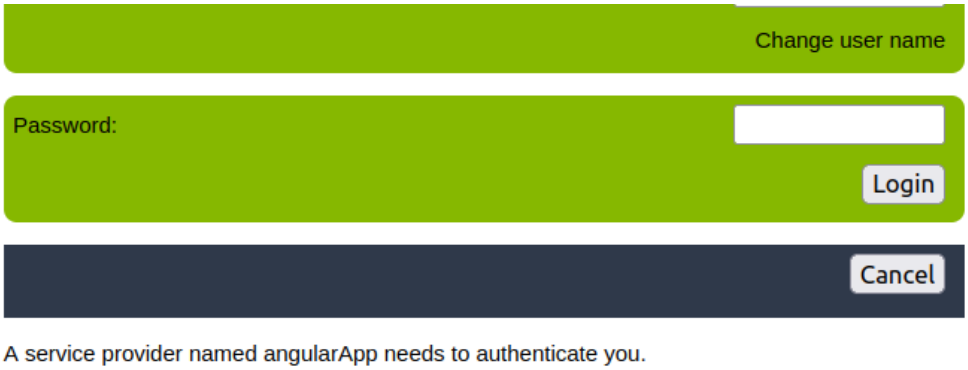
User with only one group, Primary or Secondary, with type holder group Yes. This users can have more groups with holder group No. When this user logs in to an application --> The user will be loged-in the application with the group with type holder group yes.

OpenID-Connect

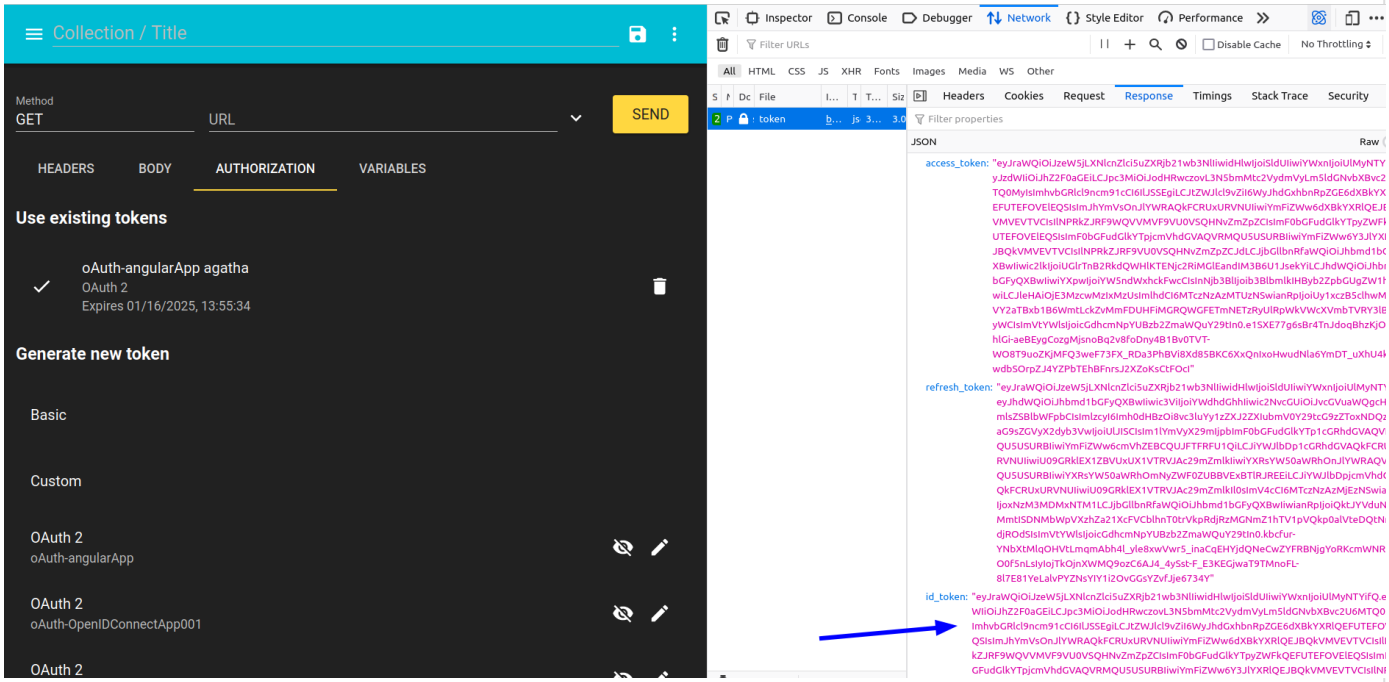
a. User Agatha with Primary group RRHH (Role holder Yes)



b. Login: the user type the user and password to login



c. Get the JSON id_token



d. Decode the JSON Web Token using https://jwt.io

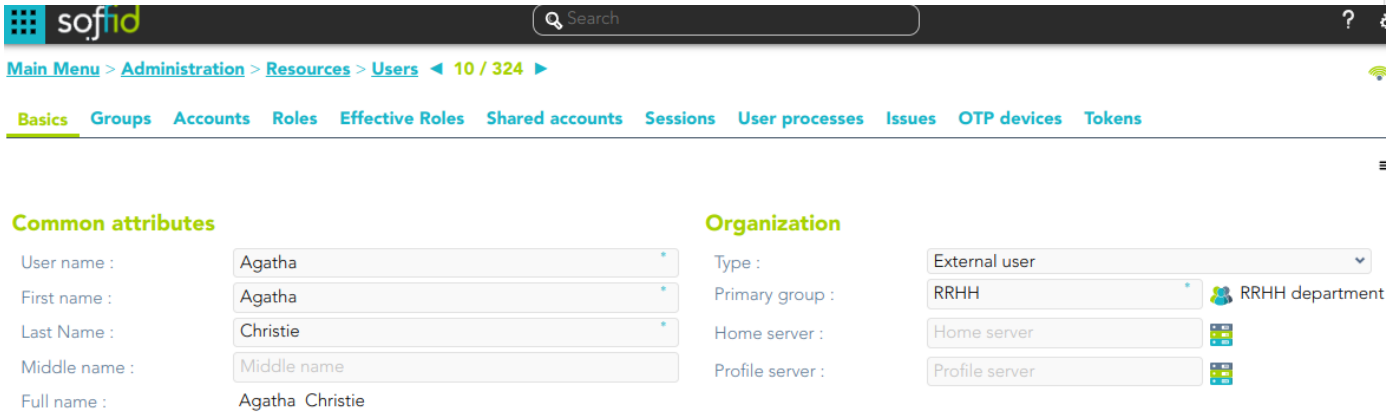
Here you are the scope, the holder_group and the member_of data

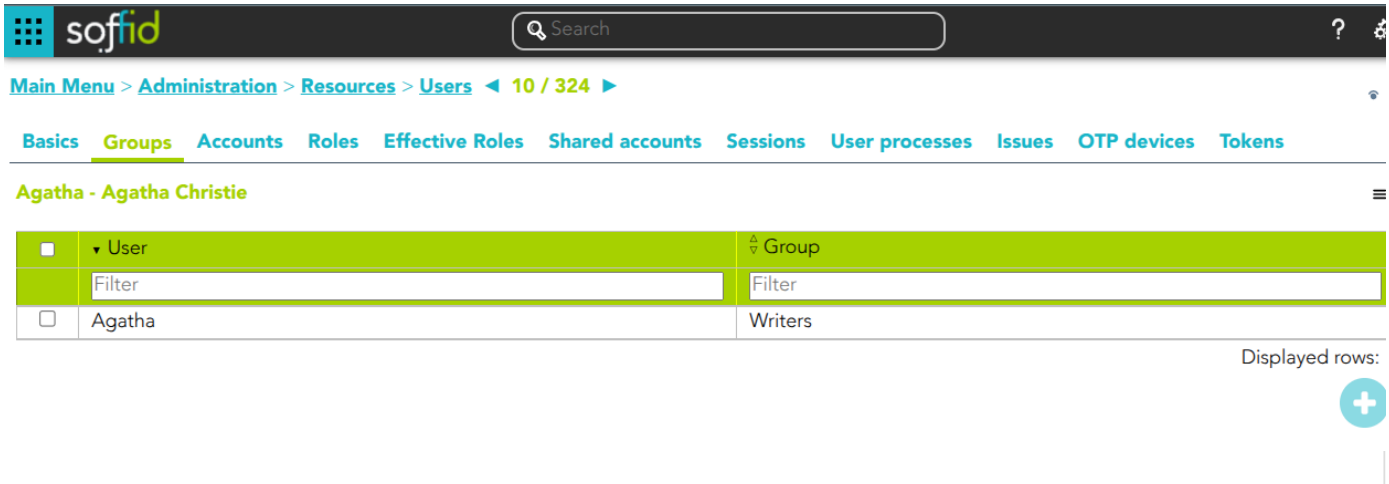

```
{
  "sub": "agatha",
  "iss": "https://sync-server.netcompose:1443",
  "holder_group": "RRHH",
  "meber_of": [
    "SOFFID_HOLDER_CONDOMAIN004/RRHH@soffid",
```

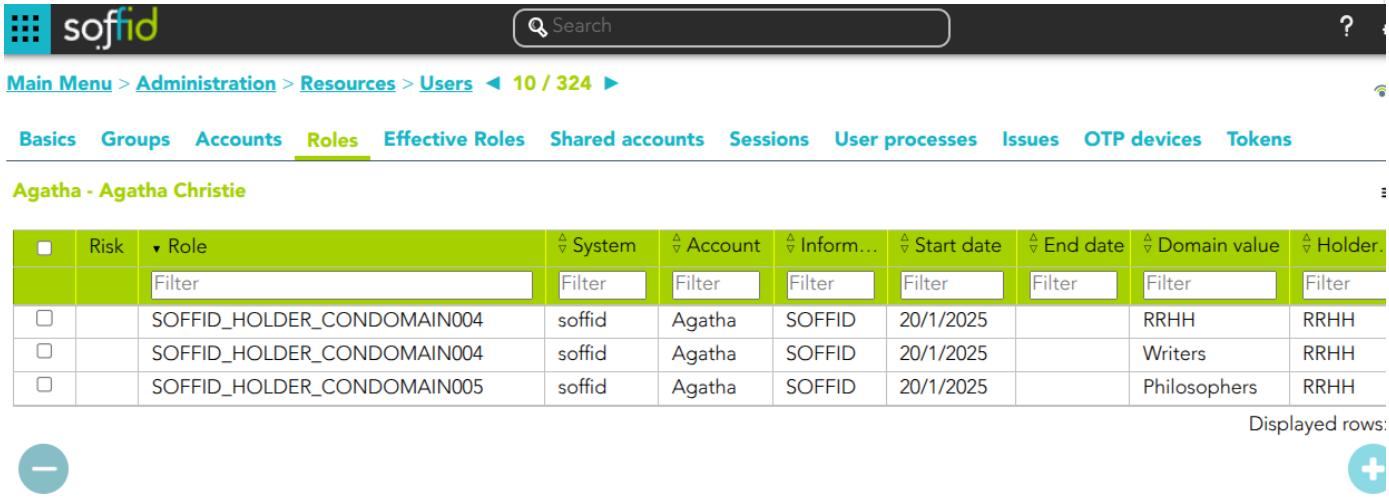
```
    "SOFFID_HOLDER_CONDOMAIN005/Philosophers@soffid",
    "SOFFID_VAULT_USER@soffid",
    "SOFFID_HOLDER_CONDOMAIN004/Writers@soffid",
    "SOFFID_USER@soffid"
  ],
  "nonce": null,
  "sid": "oeB51Jr/+rb5yE+lbG9iYsAHy1TxOFYm",
  "aud": "angularApp",
  "azp": "angularApp",
  "auth_time": 1737365621,
  "scope": "openid profile email",
  "exp": 1737366221,
  "iat": 1737365622,
  "jti": "WW1wwRD-HaE9DCXfQv4wLRuFgGRbI1lB_9wDFBd6X4lLJBv4vS6mL1yG3S0Ee_Nv",
  "email": "agatha@soffid.com"
}
```


SAML

a. User Agatha with Primary group RRHH (Role holder Yes)







b. Login: the user type the user and password to login





c. Get the SAML response


```
<?xml version="1.0" encoding="UTF-8"?>
<saml2p:Response xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
Destination="https://pat.soffid.lab:8443/soffid/saml/log/post" ID="_6699870c490dcef896cb33d70187de62"
InResponseTo="_edec4bcc9b7bf081e970867995369df9" IssueInstant="2025-01-20T09:35:53.249Z"
Version="2.0">
 <saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">https://sync-
server.netcompose</saml2:Issuer>
 <saml2p:Status>
  <saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"></saml2p:StatusCode>
 </saml2p:Status>
 <saml2:Assertion xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:xs="http://www.w3.org/2001/XMLSchema" ID="_8d730eeaaa1bcfbf419568e5edc77d27"
```

IssueInstant="2025-01-20T09:35:53.249Z" Version="2.0">
<saml2:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">https://sync-server.netcompose</saml2:Issuer>
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:SignedInfo>
<ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"></ds:CanonicalizationMethod>
<ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"></ds:SignatureMethod>
<ds:Reference URI="#_8d730eeaaa1bcfbf419568e5edc77d27">
<ds:Transforms>
<ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"></ds:Transform>
<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
<ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="xs"></ec:InclusiveNamespaces>
</ds:Transform>
</ds:Transforms>
<ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"></ds:DigestMethod>
<ds:DigestValue>qEEAkYqFFZxatl6DaVme4IfrojC3zafaKFH+TpIDurY=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>

<ds:SignatureValue>TeVSWaALsRLMwYxi71/b1k8jKYOrFb7qS9qva2T5T3yKpNLwZxnmRqWznbBM7wpr9U3V0scfh5M1ex/NGflbADbxih7uwUVK8YSAZPwIx/4LXEx0uOxpQi7ZiDOvhb2jkKLdvztvUkBGeJhJGCJy/2WrOHIEdzsn4T4c7TBdWZc=</ds:SignatureValue>
<ds:KeyInfo>
<ds:X509Data>

<ds:X509Certificate>MIICKTCCAZKgAwIBAgIGAY3q71O5MA0GCSqGSIb3DQEBCwUAMFgxJzAlBgNVBAMMHmh0dHBzOi8v
c3luYy1zZXJ2ZXIubmV0Y29tcG9zZTEcMBoGA1UECwwTRmVkZXJhdGlvbiBzZXJ2aWNlczEPMA0G
A1UECgwGU09GRklEMB4XDTI0MDIyNzE0MjkyOVoXDTM0MDIyNzE0MjkyOVowWDEnMCUGA1UEAwwe
aHR0cHM6Ly9zeW5jLXNlcnZlci5uZXRjb21wb3NlMRwwGgYDVQQLDBNGZWRlcmF0aW9uIHNlcnZp
Y2VzMQ8wDQYDVQQKDAZTT0ZGSUQwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAJZ5G9BnTSLh
X8VOVbdyY01EUkgHexi97+e1iGA0r1WM6cTu4Ku3k7/efIB5ZZfteRKbPwa719y8Ytb5W4RFcZ6O
XzHz9o+FhG64tZHEo4xwVdukv6rOatSSlhomEhruhxX+x7OpFnnlXNSCypi1xjEQyIm8GJKxpxjk
RJvkgfXLAgMBAAEwDQYJKoZIhvcNAQELBQADgYEATbs8iLBYEcPdPBjtmNHYrQpXb3nc83Acmxyy

/pEe4hXaMoB1rBuxNf47IiqJaJld9H6k5oXWcGgG8FyrdOxpY3eE8cw1s+6tM/MACMRuhuV4bQhR
FD1aizcW6fQUfvmkRLUgS1o8BMZZjCWW22FPeSklFXATE/FvmncRGpT9JWs=</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
</ds:Signature>
<saml2:Subject>
<saml2:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent"
NameQualifier="https://sync-server.netcompose">Agatha</saml2:NameID>
<saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
<saml2:SubjectConfirmationData Address="172.18.0.1"
InResponseTo="_edec4bcc9b7bf081e970867995369df9" NotOnOrAfter="2025-01-20T09:40:53.249Z"
Recipient="https://pat.soffid.lab:8443/soffid/saml/log/post"></saml2:SubjectConfirmationData>
</saml2:SubjectConfirmation>
</saml2:Subject>
<saml2:Conditions NotBefore="2025-01-20T09:35:53.249Z" NotOnOrAfter="2025-01-20T09:40:53.249Z">
<saml2:AudienceRestriction>
<saml2:Audience>https://pat.soffid.lab:8443/soffid-iam-console</saml2:Audience>
</saml2:AudienceRestriction>
</saml2:Conditions>
<saml2:AuthnStatement AuthnInstant="2025-01-20T09:35:53.197Z"
SessionIndex="_cd9afa8aac3a7a35abc90b488b01d458">
<saml2:SubjectLocality Address="172.18.0.1"></saml2:SubjectLocality>
<saml2:AuthnContext>

<saml2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</saml
2:AuthnContextClassRef>
</saml2:AuthnContext>
</saml2:AuthnStatement>
<saml2:AttributeStatement>
<saml2:Attribute FriendlyName="mail" Name="urn:oid:0.9.2342.19200300.100.1.3"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
<saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">agatha@soffid.com</saml2:AttributeValue>
</saml2:Attribute>
<saml2:Attribute FriendlyName="uid" Name="urn:oid:0.9.2342.19200300.100.1.1"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
<saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">Agatha</saml2:AttributeValue>

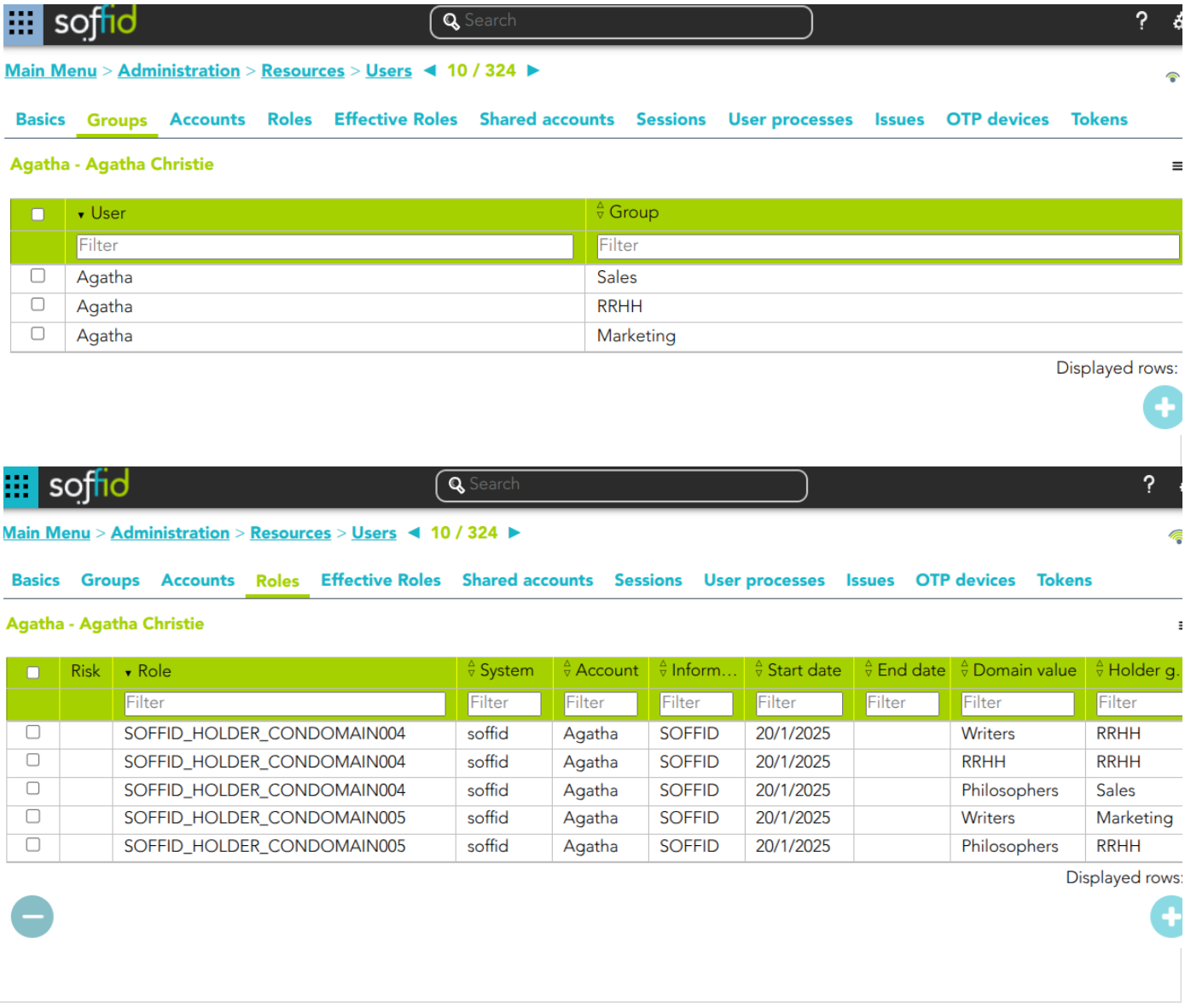
```
   </saml2:Attribute>
   <saml2:Attribute FriendlyName="memberOf" Name="urn:oid:1.3.6.1.4.1.5923.1.5.1.1"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
    <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">SOFFID_HOLDER_CONDOMAIN004/RRHH@soffid</saml2:AttributeValue>
    <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">SOFFID_HOLDER_CONDOMAIN005/Philosophers@soffid</saml2:AttributeValue>
    <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">SOFFID_VAULT_USER@soffid</saml2:AttributeValue>
    <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">SOFFID_HOLDER_CONDOMAIN004/Writers@soffid</saml2:AttributeValue>
    <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">SOFFID_USER@soffid</saml2:AttributeValue>
   </saml2:Attribute>
   <saml2:Attribute FriendlyName="HolderGroup" Name="urn:oid:1.3.6.1.4.1.22896.3.1.7"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
    <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">RRHH</saml2:AttributeValue>
   </saml2:Attribute>
  </saml2:AttributeStatement>
 </saml2:Assertion>
</saml2p:Response>
```

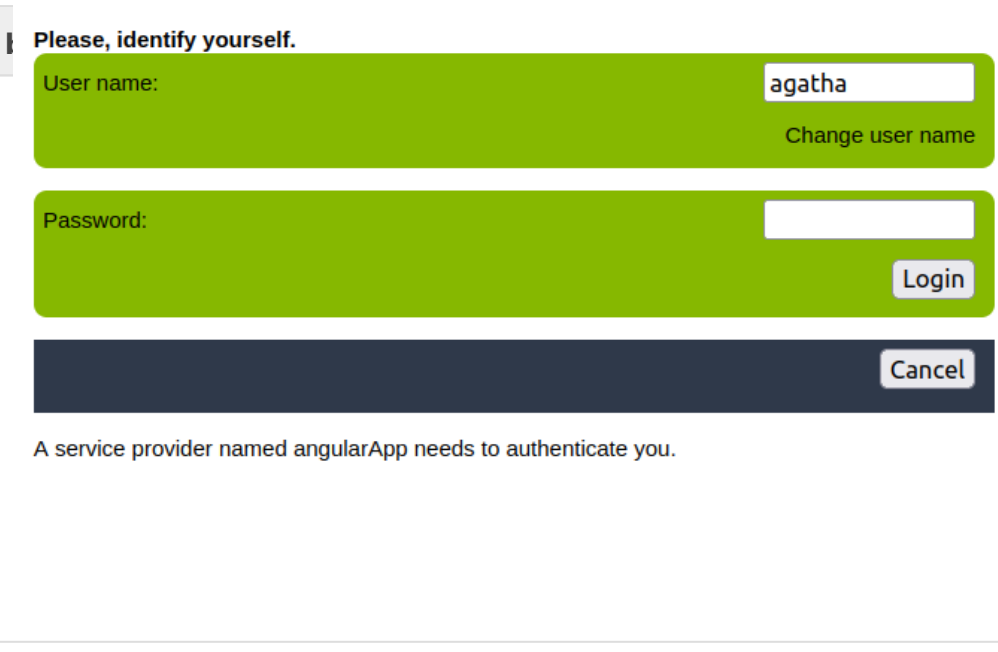

Use case 3 - Log in to an application

User with more than one group, Primary or Secondary, with type holder group Yes. When this user log into an application --> The user will have to choose the holder group to login the application. The user will be loged-in the application with the holder group selected.

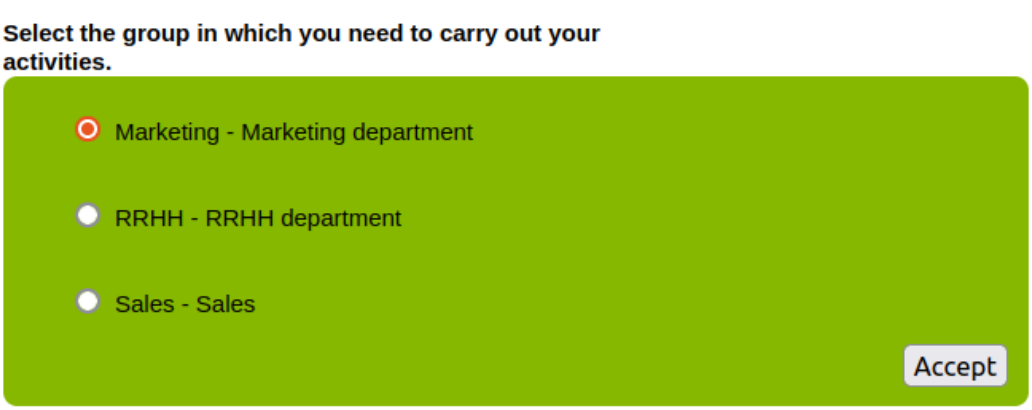
OpenID-Connect

a. User Agatha with three groups with Role holder Yes

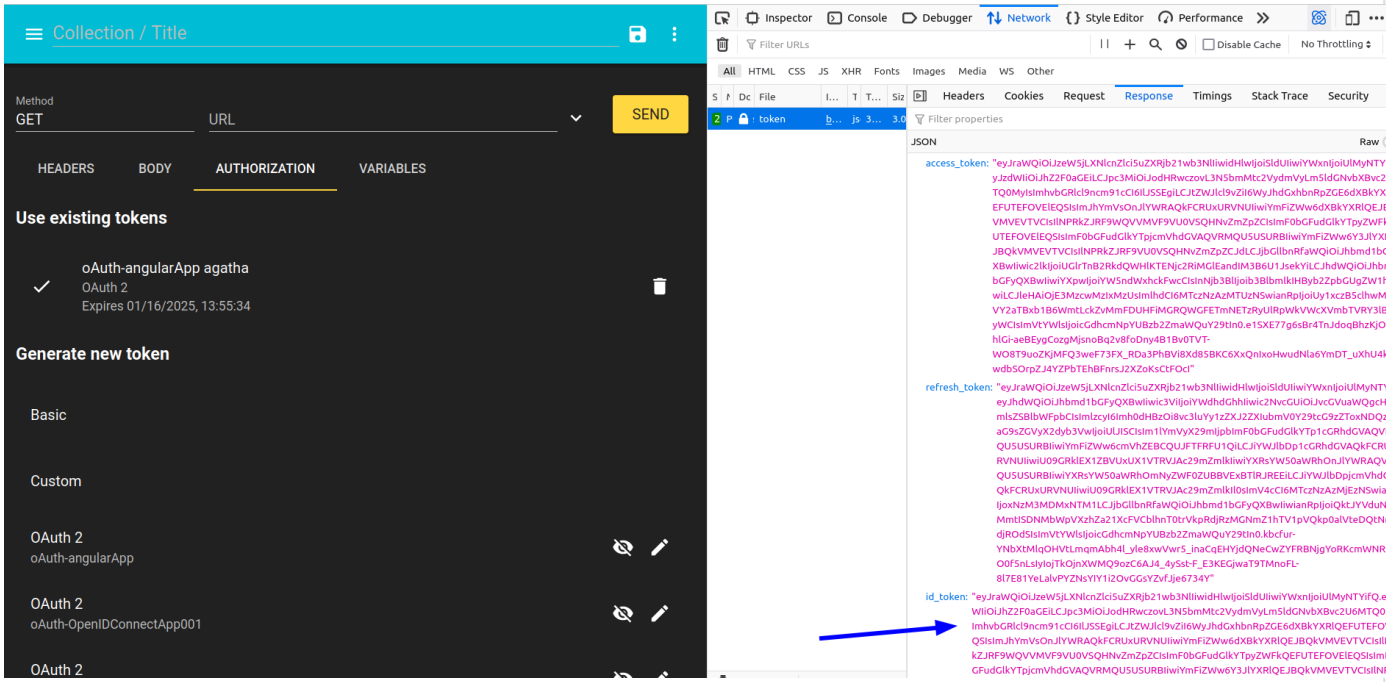




c. The user has to select the holder group to login



d. Get the JSON id_token



e. Decode the JSON Web Token using https://jwt.io

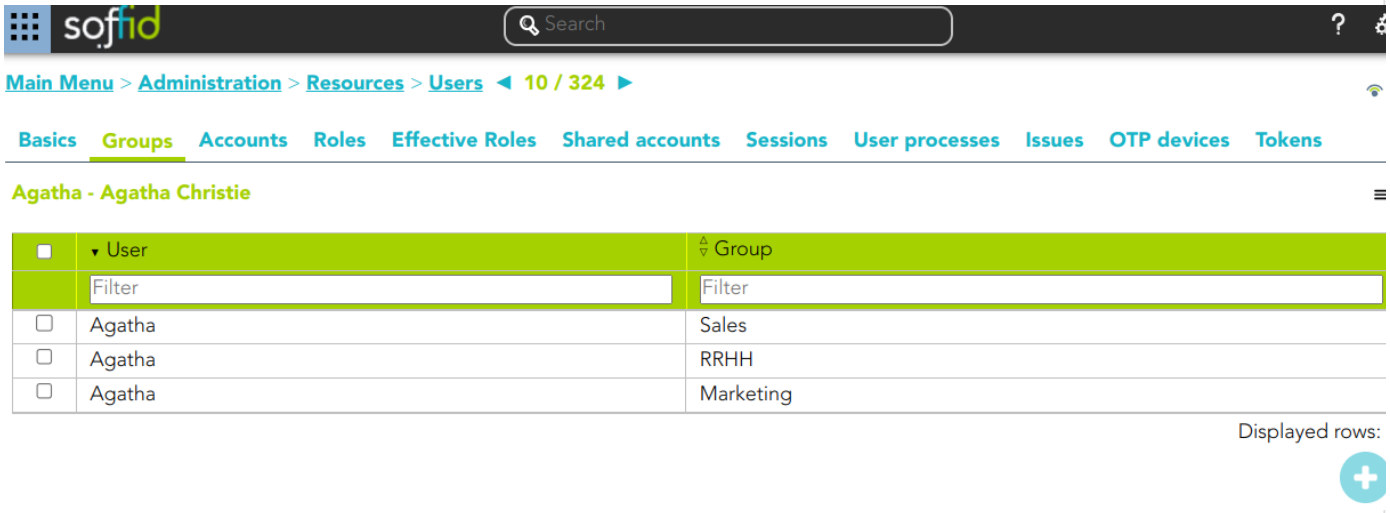
Here you are the scope, the holder_group and the member_of data


```
{
  "sub": "agatha",
  "iss": "https://sync-server.netcompose:1443",
  "holder_group": "Marketing",
```

```
  "meber_of": [
    "SOFFID_VAULT_USER@soffid",
    "SOFFID_HOLDER_CONDOMAIN005/Writers@soffid",
    "SOFFID_USER@soffid"
  ],
  "nonce": null,
  "sid": "+cr0VQjlUcwmuJg0jraIO4DwtPfFOH9b",
  "aud": "angularApp",
  "azp": "angularApp",
  "auth_time": 1737366858,
  "scope": "openid profile email",
  "exp": 1737367458,
  "iat": 1737366858,
  "jti": "X1kvNUqr_-LJgz_EHneva0-mtHTLSkhN00d3UX-dtA7LVcjpkyM0yvl5UPst9vV2",
  "email": "agatha@soffid.com"
}
```


SAML

a. User Agatha with three groups with Role holder Yes



soffid

Search

Main Menu > Administration > Resources > Users ◄ 10 / 324 ►

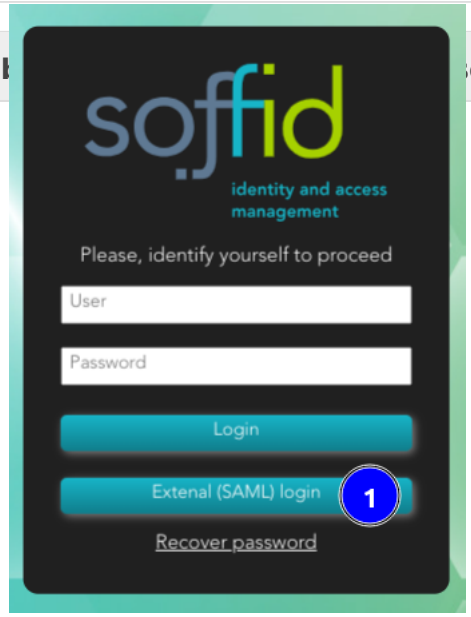
Basics | Groups | Accounts | Roles | Effective Roles | Shared accounts | Sessions | User processes | Issues | OTP devices | Tokens

Agatha - Agatha Christie

Risk	Role	System	Account	Inform...	Start date	End date	Domain value	Holder g.
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
	SOFFID_HOLDER_CONDOMAIN004	soffid	Agatha	SOFFID	20/1/2025		Writers	RRHH
	SOFFID_HOLDER_CONDOMAIN004	soffid	Agatha	SOFFID	20/1/2025		RRHH	RRHH
	SOFFID_HOLDER_CONDOMAIN004	soffid	Agatha	SOFFID	20/1/2025		Philosophers	Sales
	SOFFID_HOLDER_CONDOMAIN005	soffid	Agatha	SOFFID	20/1/2025		Writers	Marketing
	SOFFID_HOLDER_CONDOMAIN005	soffid	Agatha	SOFFID	20/1/2025		Philosophers	RRHH

Displayed rows:

er and password to login



Please, identify yourself.

User name: agatha

Change user name

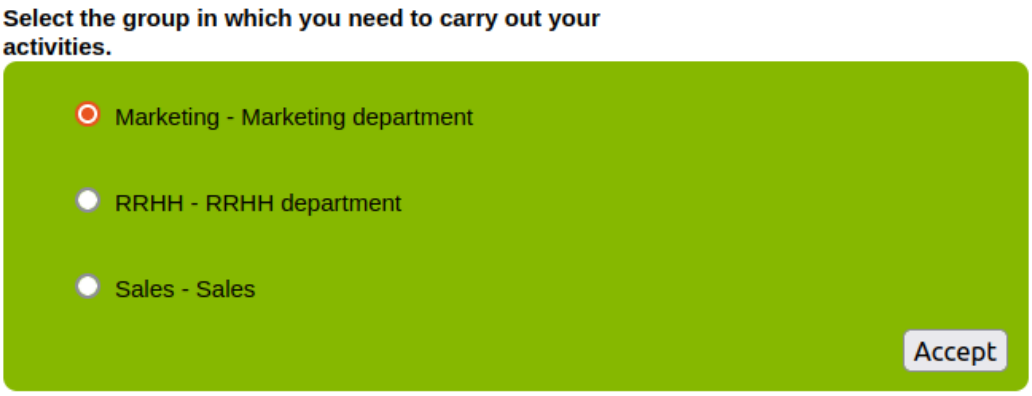
Password: ••••••

Login

Forgot your password?

A service provider named https://pat.soffid.lab:8443/soffid-iam-console needs to authenticate you.

c. The user has to select the holder group to login



d. Get the SAML response


```
<?xml version="1.0" encoding="UTF-8"?>
<saml2p:Response xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
Destination="https://pat.soffid.lab:8443/soffid/saml/log/post" ID="_82e187f91ad03509cbb5adc502dc75ec"
InResponseTo="_5ffefaae23a7626917de0e0d8c4866e5" IssueInstant="2025-01-20T09:56:45.504Z"
Version="2.0">
 <saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">https://sync-
server.netcompose</saml2:Issuer>
 <saml2p:Status>
  <saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"></saml2p:StatusCode>
 </saml2p:Status>
 <saml2:Assertion xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:xs="http://www.w3.org/2001/XMLSchema" ID="_f351bb2c2cb39df3eeb29f31f4e6ea02"
IssueInstant="2025-01-20T09:56:45.504Z" Version="2.0">
  <saml2:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">https://sync-
server.netcompose</saml2:Issuer>
  <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
   <ds:SignedInfo>
    <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"></ds:CanonicalizationMethod>
    <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-
sha256"></ds:SignatureMethod>
    <ds:Reference URI="#_f351bb2c2cb39df3eeb29f31f4e6ea02">
```

<ds:Transforms>
<ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"></ds:Transform>
<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
<ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="xs"></ec:InclusiveNamespaces>
</ds:Transform>
</ds:Transforms>
<ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"></ds:DigestMethod>
<ds:DigestValue>FIIpGC4P+i4OYv+1MxIw2tdgPgheB6zsE2QhbHTUP3U=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>

<ds:SignatureValue>VI2a9cx7vPKH+fppjyRQ4g+/NPknfxVzgbekaWomAxHvgNegRonlalUiRiiVLC5DdcT1dkO85c9FJgf5x8CgEfKFRKVNcaNWRVMZIZYUR/DKjyVH0F8a8lZMdHyxB9z3xj0QVqs7536dalA38hD5p4TG4PoNttYLhE1tFGd8QsI=</ds:SignatureValue>
<ds:KeyInfo>
<ds:X509Data>

<ds:X509Certificate>MIICKTCCAZKgAwIBAgIGAY3q71O5MA0GCSqGSIb3DQEBCwUAMFgxJzAlBgNVBAMMHmh0dHBzOi8v
c3luYy1zZXJ2ZXIubmV0Y29tcG9zZTEcMBoGA1UECwwTRmVkZXJhdGlvbiBzZXJ2aWNlczEPMA0G
A1UECgwGU09GRklEMB4XDTI0MDIyNzE0MjkyOVoXDTM0MDIyNzE0MjkyOVowWDEnMCUGA1UEAwwe
aHR0cHM6Ly9zeW5jLXNlcnZlci5uZXRjb21wb3NlMRwwGgYDVQQLDBNGZWRlcmF0aW9uIHNlcnZp
Y2VzMQ8wDQYDVQQKDAZTT0ZGSUQwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAJZ5G9BnTSLh
X8VOVbdyY01EUkgHexi97+e1iGA0r1WM6cTu4Ku3k7/efIB5ZZfteRKbPwa719y8Ytb5W4RFcZ6O
XzHz9o+FhG64tZHEo4xwVdukv6rOatSSlhomEhruhxX+x7OpFnnlXNSCypi1xjEQyIm8GJKxpxjk
RJvkgfXLAgMBAAEwDQYJKoZIhvcNAQELBQADgYEATbs8iLBYEcPdPBjtmNHYrQpXb3nc83Acmxyy
/pEe4hXaMoB1rBuxNf47liqJaJld9H6k5oXWcGgG8FyrdOxpY3eE8cw1s+6tM/MACMRuhuV4bQhR
FD1aizcW6fQUfvmkRLUgS1o8BMZZjCWW22FPeSklFXATE/FvmncRGpT9JWs=</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
</ds:Signature>
<saml2:Subject>
<saml2:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent" NameQualifier="https://sync-server.netcompose">Agatha</saml2:NameID>
<saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
<saml2:SubjectConfirmationData Address="172.18.0.1"

InResponseTo="_5ffefaae23a7626917de0e0d8c4866e5" NotOnOrAfter="2025-01-20T10:01:45.504Z"
Recipient="https://pat.soffid.lab:8443/soffid/saml/log/post"></saml2:SubjectConfirmationData>
</saml2:SubjectConfirmation>
</saml2:Subject>
<saml2:Conditions NotBefore="2025-01-20T09:56:45.504Z" NotOnOrAfter="2025-01-20T10:01:45.504Z">
<saml2:AudienceRestriction>
<saml2:Audience>https://pat.soffid.lab:8443/soffid-iam-console</saml2:Audience>
</saml2:AudienceRestriction>
</saml2:Conditions>
<saml2:AuthnStatement AuthnInstant="2025-01-20T09:56:45.461Z"
SessionIndex="_31bb4c1105aa3c363a69b299e577d9cd">
<saml2:SubjectLocality Address="172.18.0.1"></saml2:SubjectLocality>
<saml2:AuthnContext>

<saml2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</saml
2:AuthnContextClassRef>
</saml2:AuthnContext>
</saml2:AuthnStatement>
<saml2:AttributeStatement>
<saml2:Attribute FriendlyName="mail" Name="urn:oid:0.9.2342.19200300.100.1.3"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
<saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">agatha@soffid.com</saml2:AttributeValue>
</saml2:Attribute>
<saml2:Attribute FriendlyName="uid" Name="urn:oid:0.9.2342.19200300.100.1.1"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
<saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">Agatha</saml2:AttributeValue>
</saml2:Attribute>
<saml2:Attribute FriendlyName="memberOf" Name="urn:oid:1.3.6.1.4.1.5923.1.5.1.1"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
<saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">SOFFID_VAULT_USER@soffid</saml2:AttributeValue>
<saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">SOFFID_HOLDER_CONDOMAIN005/Writers@soffid</saml2:AttributeValue>
<saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">SOFFID_USER@soffid</saml2:AttributeValue>
</saml2:Attribute>

```
   <saml2:Attribute FriendlyName="HolderGroup" Name="urn:oid:1.3.6.1.4.1.22896.3.1.7"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
    <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">Marketing</saml2:AttributeValue>
   </saml2:Attribute>
  </saml2:AttributeStatement>
 </saml2:Assertion>
</saml2p:Response>
```

Use case 4 - Log in to a second application

a. Agatha user was previously loged-in to an application

Agatha user is loged-in the angularApp Service Provider

```
{
  "sub": "agatha",
  "iss": "https://sync-server.netcompose:1443",
  "holder_group": "Marketing",
  "meber_of": [
    "SOFFID_VAULT_USER@soffid",
    "SOFFID_HOLDER_CONDOMAIN005/Writers@soffid",
    "SOFFID_USER@soffid"
  ],
  "nonce": null,
  "sid": "+cr0VQjIUcwmuJg0jraIO4DwtPfFOH9b",
  "aud": "angularApp",
  "azp": "angularApp",
  "auth_time": 1737366858,
  "scope": "openid profile email",
  "exp": 1737367458,
  "iat": 1737366858,
  "jti": "X1kvNUqr_-LJgz_EHneva0-mtHTLSkhN00d3UX-dtA7LVcjpkyM0yvl5UPst9vV2",
  "email": "agatha@soffid.com"
}
```

b. Agata user is loged-in to a second application

Agatha user is loged-in the OpenIDConnectApp001 Service Provider, with the same holder group


```
{
  "sub": "agatha",
  "iss": "https://sync-server.netcompose:1443",
  "holder_group": "Marketing",
  "meber_of": [
    "SOFFID_VAULT_USER@soffid",
    "SOFFID_HOLDER_CONDOMAIN005/Writers@soffid",
    "SOFFID_USER@soffid"
  ],
  "nonce": null,
  "sid": "WDSQEzO6LIgxvQkq/zyIzL/LddKKy/j0",
  "aud": "OpenIDConnectApp001",
  "azp": "OpenIDConnectApp001",
  "auth_time": 1737367082,
  "scope": "openid",
  "exp": 1737367683,
  "iat": 1737367083,
  "jti": "C5xSE7UK0lgwgff5Cl7SPnpZvcRSm8WI0GZMXXObKdCMOuP50qbZjCcuGW7KpJqN",
  "email": "agatha@soffid.com"
}
```