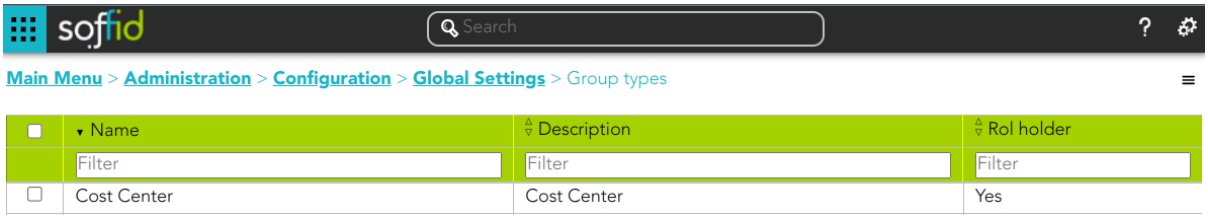
Use cases

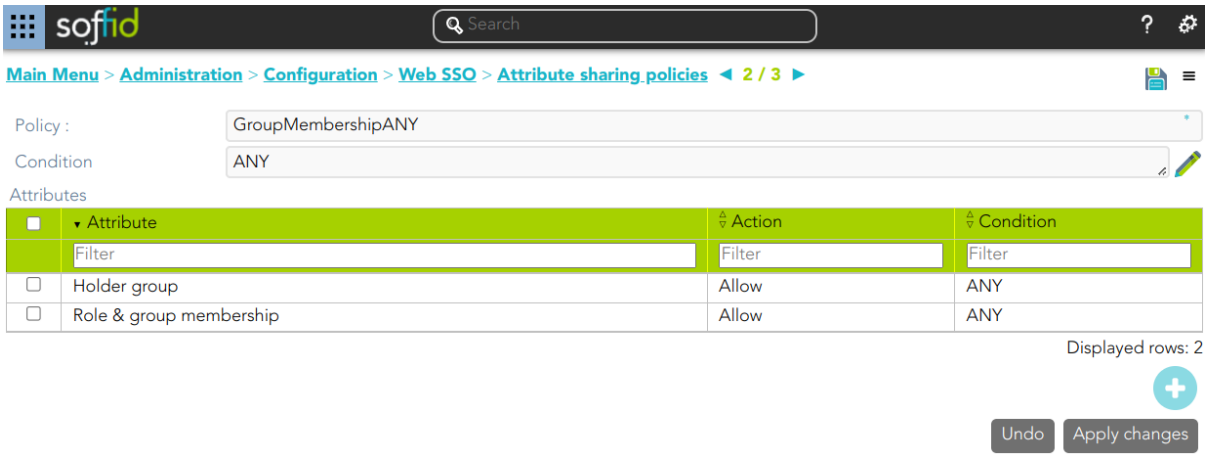
Premises

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

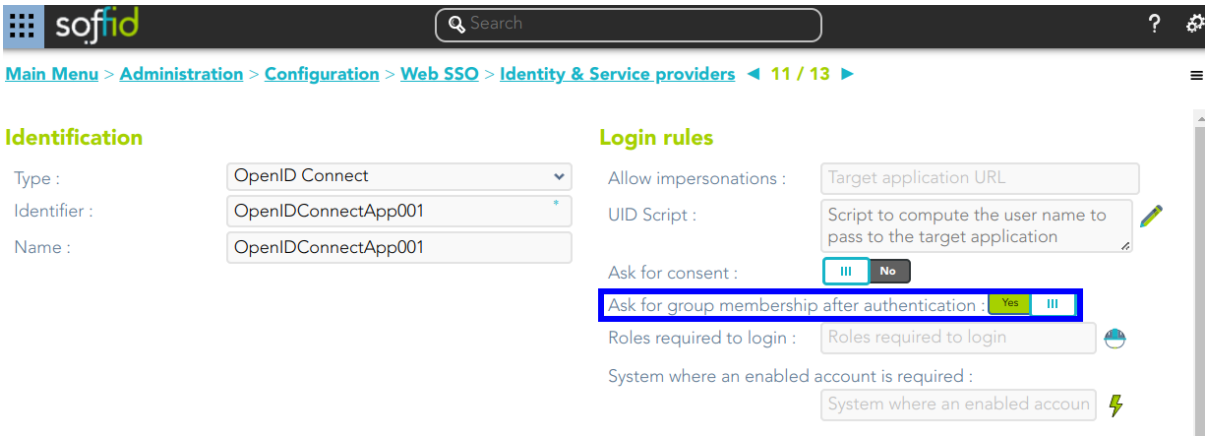


2. Several groups have been defined with type organizational unit with role holder Yes.

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

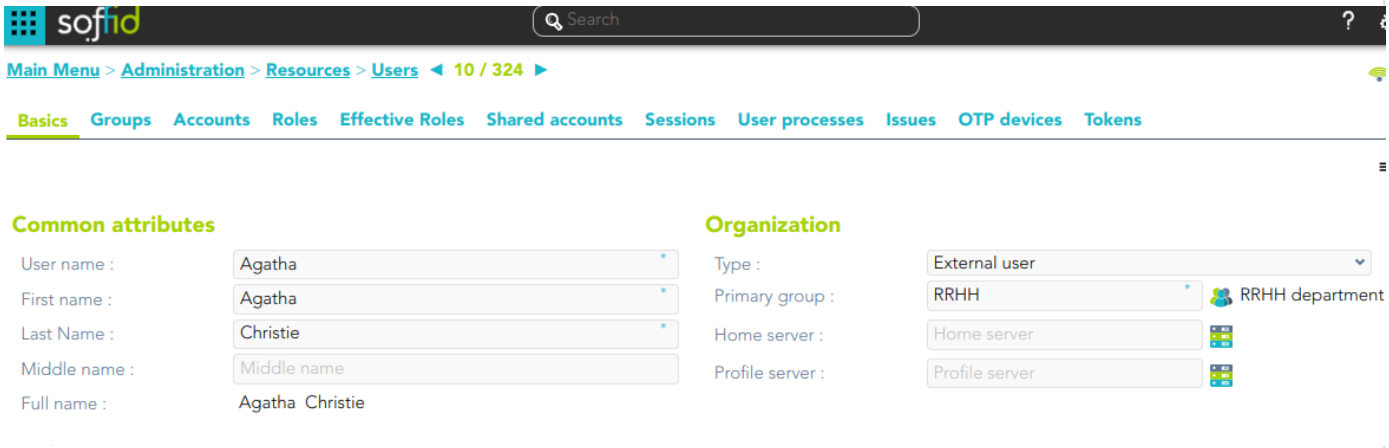
User with no groups, Primary or Secundary, with type holder group Yes. When this user log into an application --> The user login normally to the application

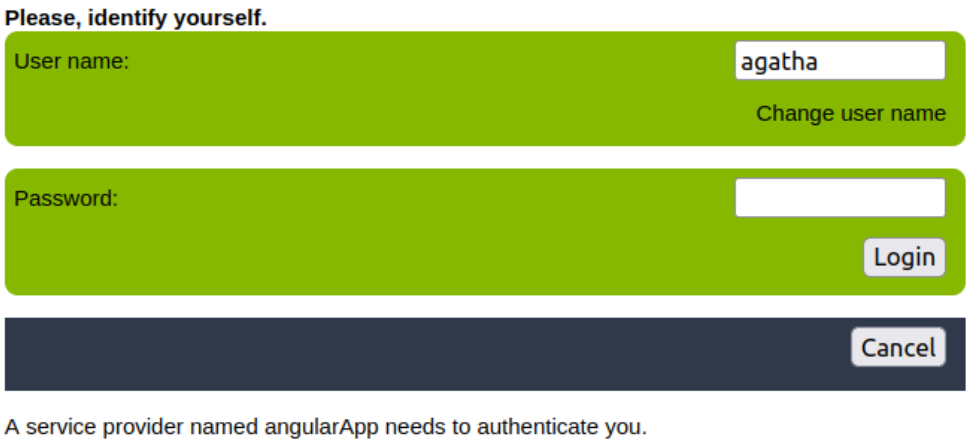
Use case 2 - Log in to an application

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.

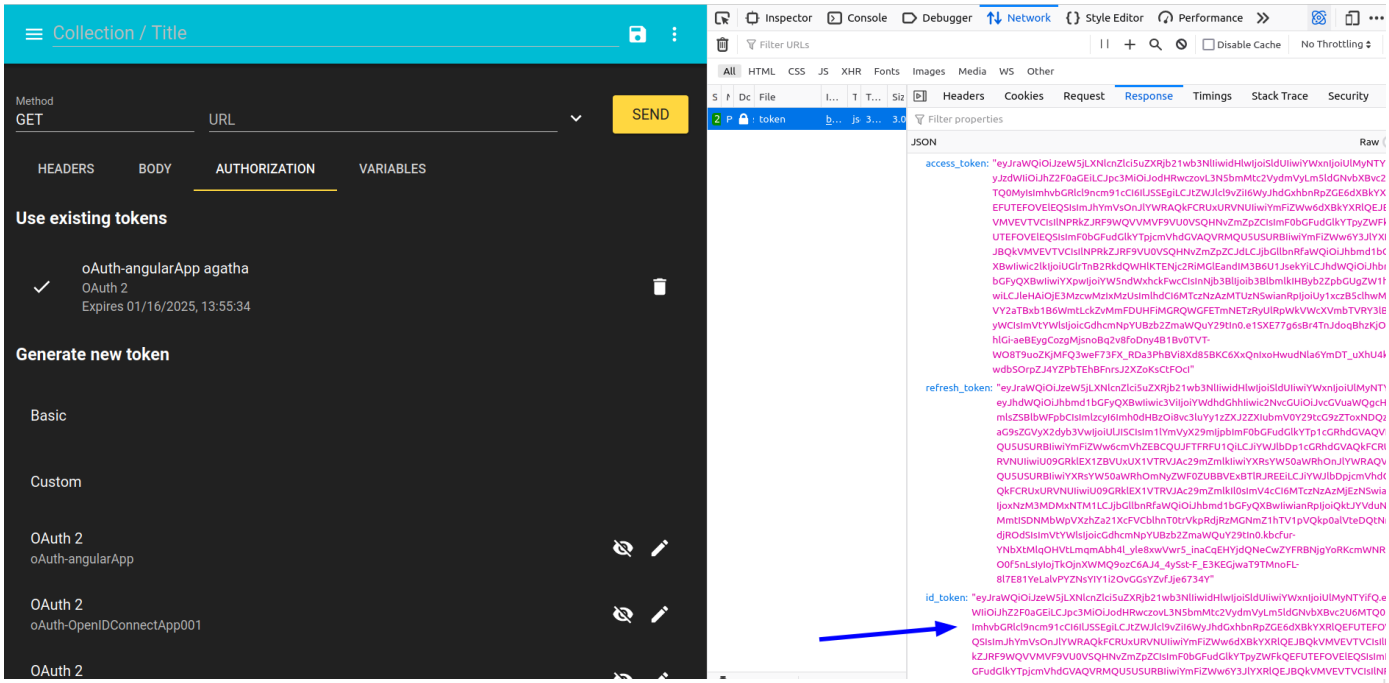
OpenID-Connect

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





c. Get the JSON id_token



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

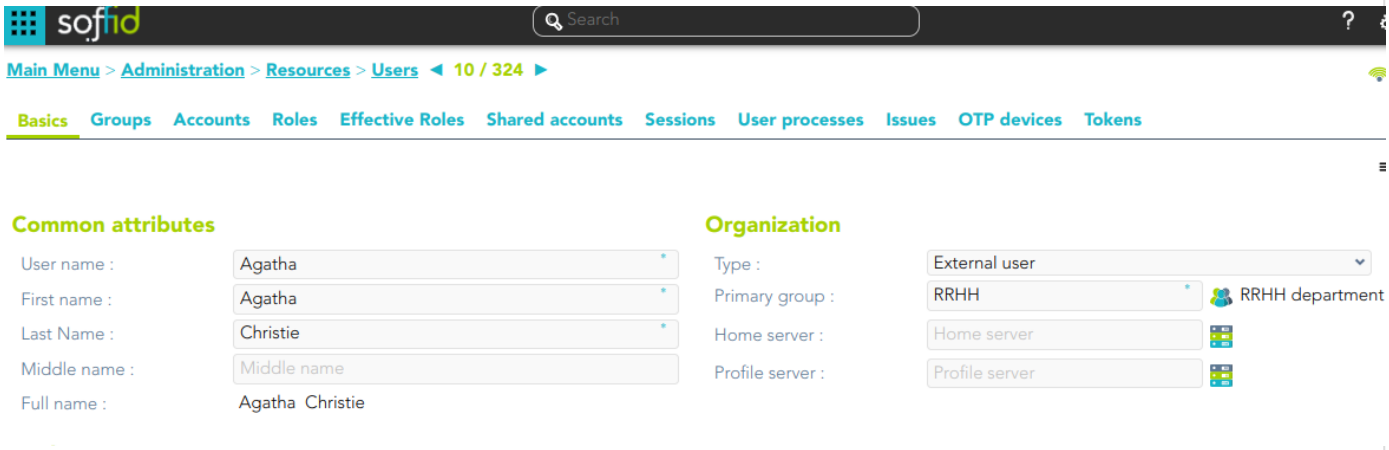
Here you are the scope, the holder_group and the member_of data


```
{
 "sub": "agatha",
 "iss": "https://sync-server.netcompose:1443",
 "holder_group": "RRHH",
 "meber_of": [
  "SOFFID_HOLDER_CONDOMAIN004/RRHH@soffid",
  "SOFFID_VAULT_USER@soffid",
  "SOFFID_USER@soffid"
 ],
 "nonce": null,
 "sid": "mx3LQHuUdN0xpMthHAWYapFjba00r9H5",
 "aud": "angularApp",
 "azp": "angularApp",
 "auth_time": 1737014499,
 "scope": "openid profile email",
 "exp": 1737015099,
 "iat": 1737014499,
 "jti": "NYnenM6r7YDUQHfTfJEdw78gYtYEr2H7aaLkxp52LpWK-QpJY4TXBvaRxaH-VuKB",
 "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="_6743cb92d3e0ebe0572843361b8afb8f"
InResponseTo="_5888a034d161c2f45e7c3d62c1ffd939" IssueInstant="2025-01-16T08:11:30.043Z"
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="_8ae443bf62a5b0fabceef1ba20e8330f"
```

IssueInstant="2025-01-16T08:11:30.043Z" 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="#_8ae443bf62a5b0fabceef1ba20e8330f">
<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>XvRUs/lrZYcgR9xjTjGQJ5VLRBtHHDbprEoa9ROxqzw=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>

<ds:SignatureValue>F2+sP+Aq8SHll56/9mYi2B+f6oFerlaMUn81Y5lK5wD+oYNGNsOjMHbwkK5gaHWk2Isr+TEhK0YMQTFfJUK0NLVuXHVQtyAfN3p6kxjXTXOq6TaLAfbivuUdzh1dEX61I63id//rGi92NbLU+p2TV/dmTS4fCOhpxm5Sry5i49o=</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="_5888a034d161c2f45e7c3d62c1ffd939" NotOnOrAfter="2025-01-16T08:16:30.043Z"
Recipient="https://pat.soffid.lab:8443/soffid/saml/log/post"></saml2:SubjectConfirmationData>
</saml2:SubjectConfirmation>
</saml2:Subject>
<saml2:Conditions NotBefore="2025-01-16T08:11:30.043Z" NotOnOrAfter="2025-01-16T08:16:30.043Z">
<saml2:AudienceRestriction>
<saml2:Audience>https://pat.soffid.lab:8443/soffid-iam-console</saml2:Audience>
</saml2:AudienceRestriction>
</saml2:Conditions>
<saml2:AuthnStatement AuthnInstant="2025-01-16T08:11:30.008Z"
SessionIndex="_d6a8c2cecd0e8bd085da5c4c82794444">
<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>

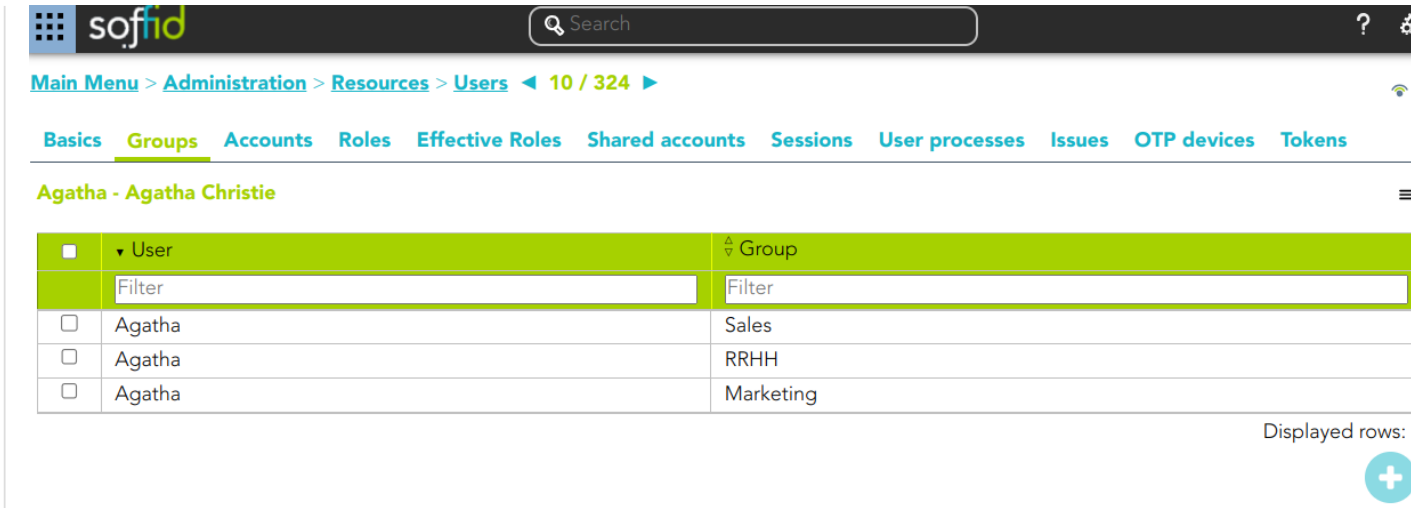
```
   </saml2:Attribute>
   <saml2:Attribute FriendlyName="memberOf" Name="urn:oid:1.3.6.1.4.1.5923.1.5.1.1"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
    <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">SOFFID_HOLDER_CONDOMAIN004/RRHH@soffid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

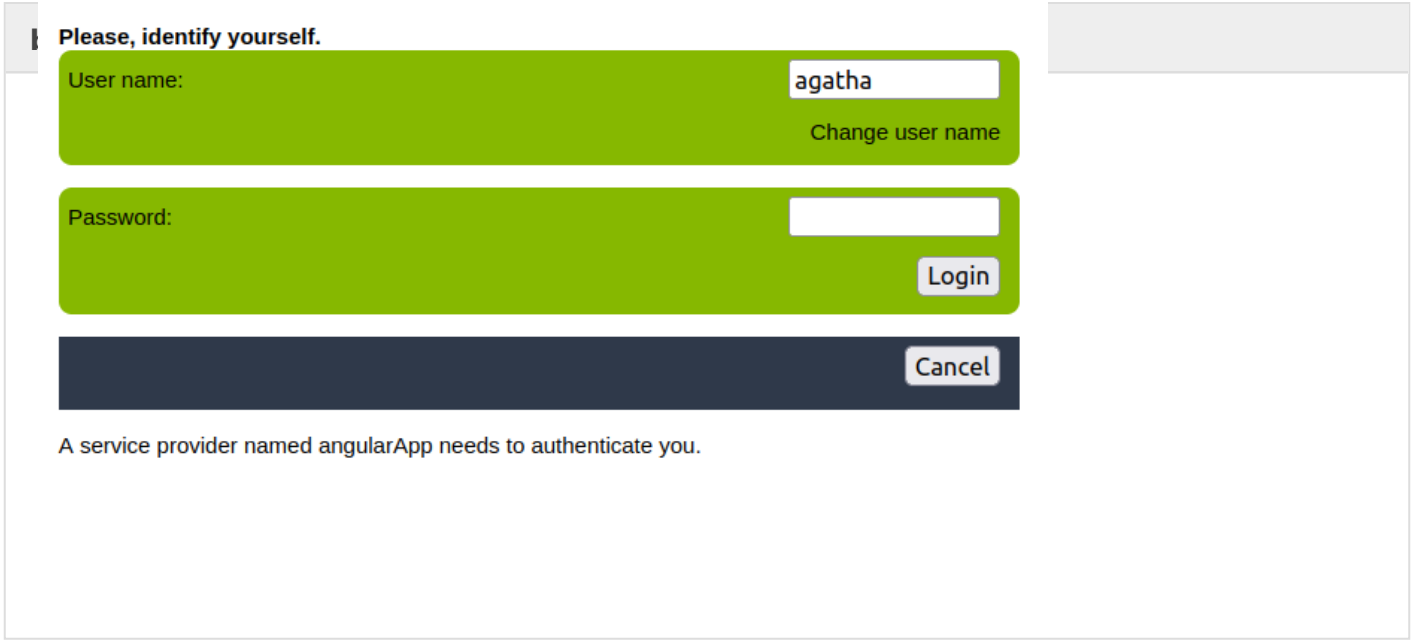

Use case 3 - Log in to an application

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.

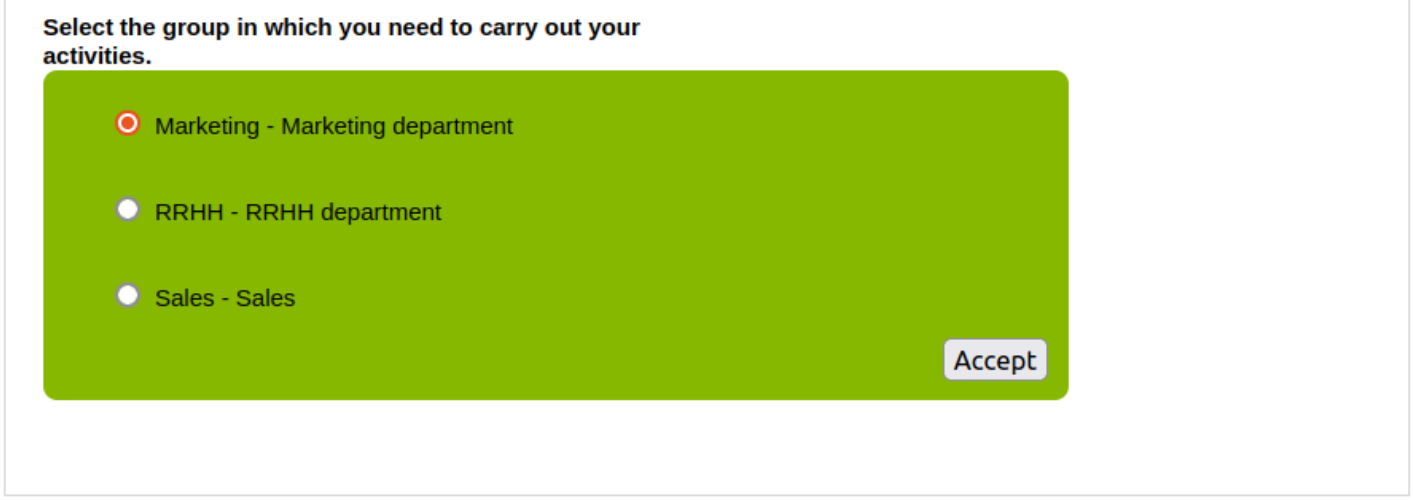
OpenID-Connect

a. User Agatha with three groups with Role holder Yes

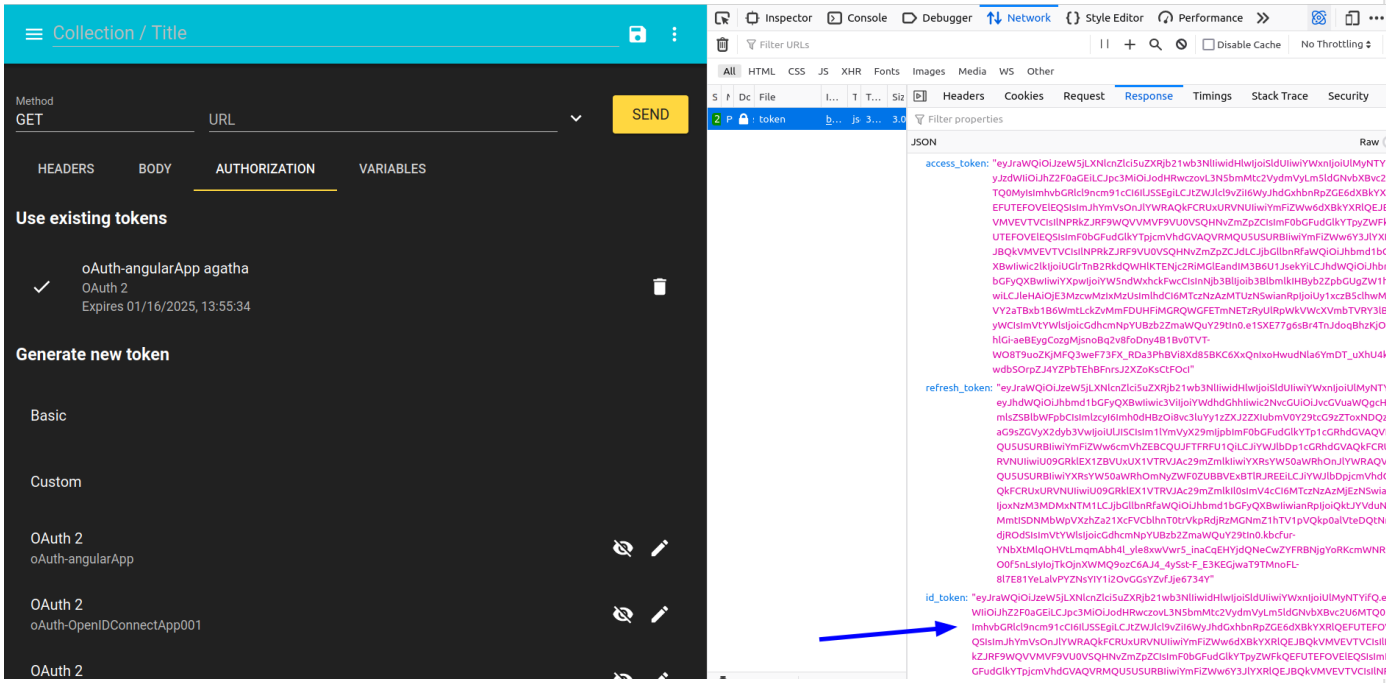




c. The user has to select the holder group to login



d. Get the JSON id_token



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

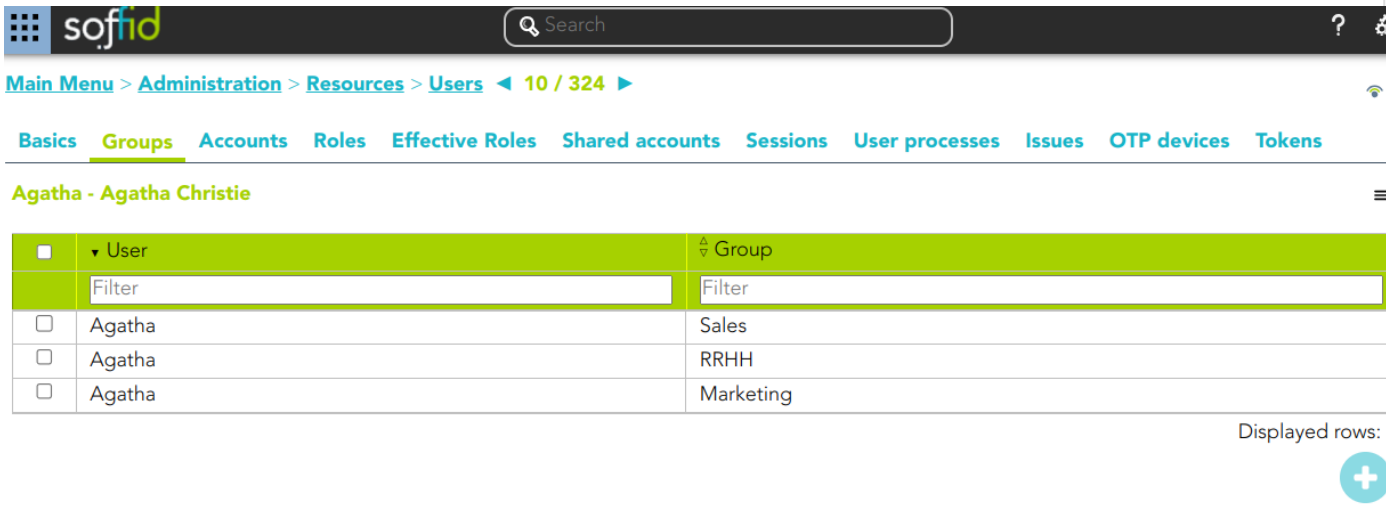
Here you are the scope, the holder_group and the member_of data


```
{
  "sub": "agatha",
  "iss": "https://sync-server.netcompose:1443",
  "holder_group": "Marketing",
  "meber_of": [
    "SOFFID_VAULT_USER@soffid",
    "SOFFID_USER@soffid"
  ],
  "nonce": null,
  "sid": "EiY52JY80Em1pzSFCypkStff2ckQzrX/",
  "aud": "angularApp",
  "azp": "angularApp",
  "auth_time": 1737038230,
  "scope": "openid profile email",
  "exp": 1737038830,
```

```
  "iat": 1737038230,
  "jti": "Bit8hOnhBsUnLQ5HbQ6XRnbs2n0S_TSdZpf4DdByg3Fc1_6yPZ3QotJa7gU_C7u4",
  "email": "agatha@soffid.com"
}
```

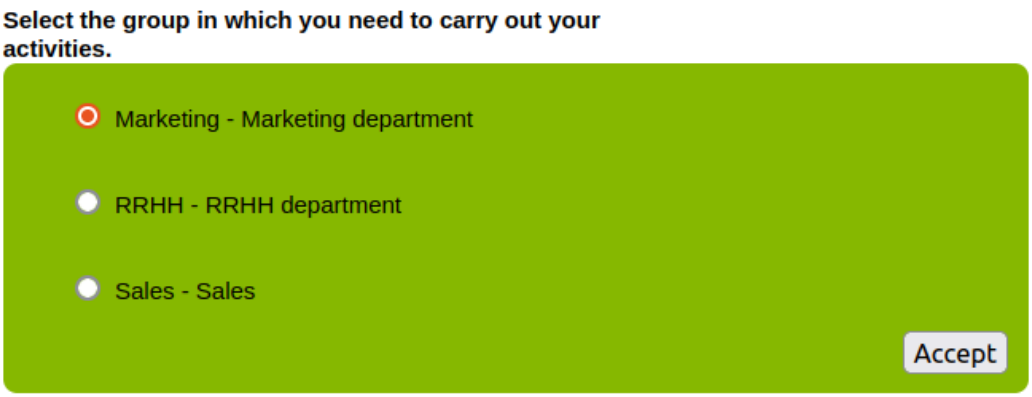

SAML

a. User Agatha with three groups with Role holder Yes



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

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="_1930e94d002cf87fcaa1387dbd69b930"
InResponseTo="_6d9a8a243f6009879f8493febb683619" IssueInstant="2025-01-16T14:42:08.273Z"
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="_febb3fe55db97a047426313f51c9e04e"
IssueInstant="2025-01-16T14:42:08.273Z" 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="#_febb3fe55db97a047426313f51c9e04e">
     <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>iAUWStZjBdxEjBwMfF3ivxJlIXxHPpK9mVf2GZeziu8=</ds:DigestValue>
    </ds:Reference>
   </ds:SignedInfo>

<ds:SignatureValue>N6ZRA6LXJiuve7qIkVlsdmmBp/YKrnGb4bfeV32xdPgLLvWRVQhNWSfWtidoxJUxTESnJOy
wpiwth/NHIHzSJi4X/4ChV3XeP3xUZ1QV29iNm2w16KGuAUIwME/mIGMDuUdSAehaOa/2j17jVTrFL9f2QUFKcbPJ

obswDR9vOqs=</ds:SignatureValue>
<ds:KeyInfo>
<ds:X509Data>

<ds:X509Certificate>MIICKTCCAZKgAwIBAgIGAY3q71O5MA0GCSqGSIb3DQEBCwUAMFgxJzAlBgNVBAMMHmh0dHBzOi8v
c3luYy1zZXJ2ZXIubmV0Y29tcG9zZTEcMBoGA1UECwwTRmVkZXJhdGlvbiBzZXJ2aWNlczEPMA0GA1UECgwGU09GRklEMB4XDTI0MDIyNzE0MjkyOVoXDTM0MDIyNzE0MjkyOVowWDEnMCUGA1UEAwweaHR0cHM6Ly9zeW5jLXNlcnZlci5uZXRjb21wb3NlMRwwGgYDVQQLDBNGZWRlcmF0aW9uIHNlcnZpY2VzMQ8wDQYDVQQKDAZTT0ZGSUQwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAJZ5G9BnTSLhX8VOVbdyY01EUkgHexi97+e1iGA0r1WM6cTu4Ku3k7/efIB5ZZfteRKbPwa719y8Ytb5W4RFcZ6OXzHz9o+FhG64tZHEo4xwVdukv6rOatSSlhomEhruhxX+x7OpFnnlXNSCypi1xjEQyIm8GJKxpxjkRJvkgfXLAgMBAAEwDQYJKoZIhvcNAQELBQADgYEATbs8iLBYEcPdPBjtmNHYrQpXb3nc83Acmxyy/pEe4hXaMoB1rBuxNf47IiqJaJld9H6k5oXWcGgG8FyrdOxpY3eE8cw1s+6tM/MACMRuhuV4bQhRFD1aizcW6fQUfvmkRLUgS1o8BMZZjCWW22FPeSklFXATE/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="_6d9a8a243f6009879f8493febb683619" NotOnOrAfter="2025-01-16T14:47:08.273Z" Recipient="https://pat.soffid.lab:8443/soffid/saml/log/post"></saml2:SubjectConfirmationData>
</saml2:SubjectConfirmation>
</saml2:Subject>
<saml2:Conditions NotBefore="2025-01-16T14:42:08.273Z" NotOnOrAfter="2025-01-16T14:47:08.273Z">
<saml2:AudienceRestriction>
<saml2:Audience>https://pat.soffid.lab:8443/soffid-iam-console</saml2:Audience>
</saml2:AudienceRestriction>
</saml2:Conditions>
<saml2:AuthnStatement AuthnInstant="2025-01-16T14:42:08.193Z" SessionIndex="_8a28efb06654a2bafe0eceb3eb6ea35b">
<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_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_USER@soffid"
  ],
  "nonce": null,
  "sid": "/sYgJRDQqH2GFHsJq7SAS+JHx9ujvray",
  "aud": "angularApp",
  "azp": "angularApp",
  "auth_time": 1737042386,
  "scope": "openid profile email",
  "exp": 1737042986,
  "iat": 1737042386,
  "jti": "IQ8Ga-VB3wehrRiIj6wrE9lUtnpVlo0rEwcHTbhndDuV4_kPpA7PDwCTNXhMbGIy",
  "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_USER@soffid"
  ],
  "nonce": null,
  "sid": "WP5bktBjtQG4bWJ6gR73EgB0pBvHNcgU",
  "aud": "OpenIDConnectApp001",
  "azp": "OpenIDConnectApp001",
  "auth_time": 1737042392,
```

```
  "scope": "openid",
  "exp": 1737042992,
  "iat": 1737042392,
  "jti": "L6e3Ln6-NrELNAsY8s33gz8il7sE63PH6CSIvJhlKm6LmZsxW2F-2X81h1nyAEBc",
  "email": "agatha@soffid.com"
}
```


Revision #17
Created 16 January 2025 08:21:09 by pgarcia@soffid.com
Updated 16 January 2025 15:52:31 by pgarcia@soffid.com