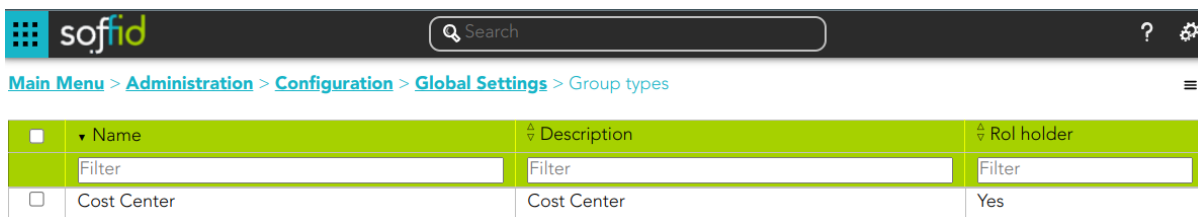


Use cases

Premises

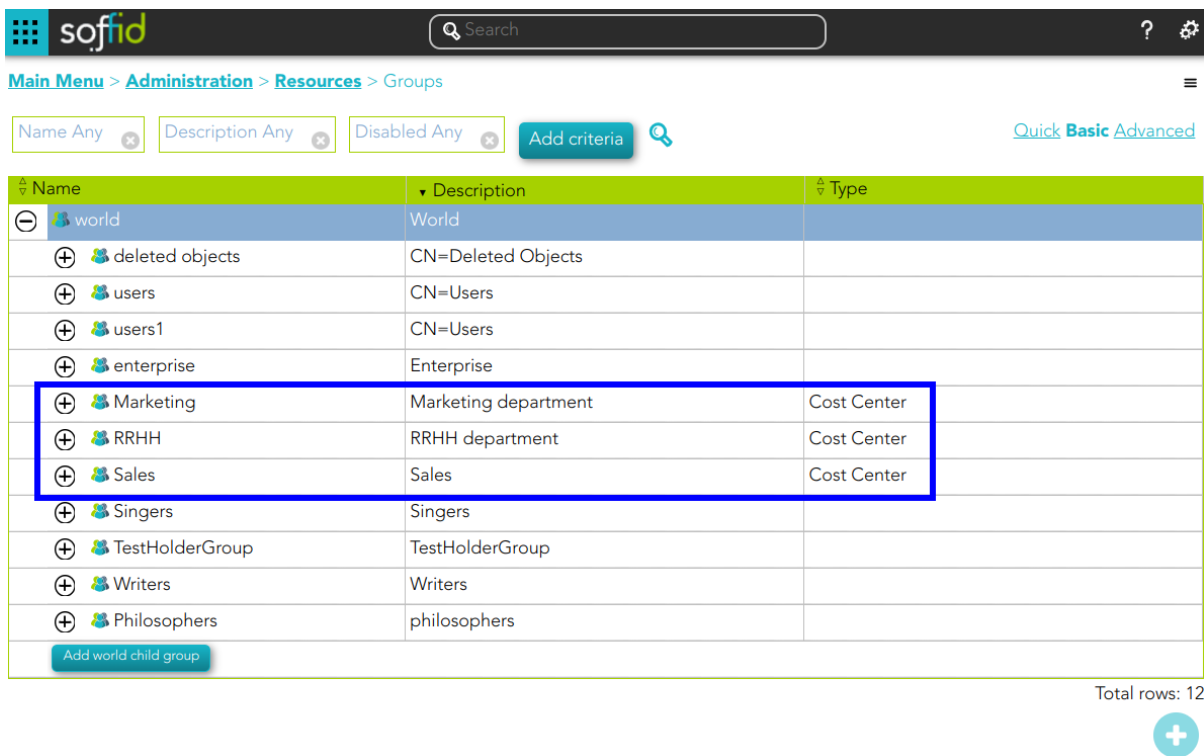
1. An Organizational Unit has been defined as Role holder Yes.



The screenshot shows the 'soffid' application interface. The breadcrumb trail is 'Main Menu > Administration > Configuration > Global Settings > Group types'. Below the header is a table with three columns: 'Name', 'Description', and 'Rol holder'. The first row is a filter row with 'Filter' in each column. The second row shows a checkbox, 'Cost Center' in the Name column, 'Cost Center' in the Description column, and 'Yes' in the Rol holder column.

	Name	Description	Rol holder
	Filter	Filter	Filter
<input type="checkbox"/>	Cost Center	Cost Center	Yes

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



The screenshot shows the 'soffid' application interface. The breadcrumb trail is 'Main Menu > Administration > Resources > Groups'. Below the header are filter boxes for 'Name Any', 'Description Any', and 'Disabled Any', along with an 'Add criteria' button. To the right are links for 'Quick', 'Basic', and 'Advanced'. Below is a table with three columns: 'Name', 'Description', and 'Type'. The table lists various groups, with 'Marketing', 'RRHH', and 'Sales' highlighted by a blue box. These three groups are all of type 'Cost Center'. At the bottom right, it says 'Total rows: 12' and there is a '+' button.

Name	Description	Type
world	World	
+ deleted objects	CN=Deleted Objects	
+ users	CN=Users	
+ users1	CN=Users	
+ enterprise	Enterprise	
+ Marketing	Marketing department	Cost Center
+ RRHH	RRHH department	Cost Center
+ Sales	Sales	Cost Center
+ Singers	Singers	
+ TestHolderGroup	TestHolderGroup	
+ Writers	Writers	
+ Philosophers	philosophers	

3. An attribute sharing policy has been defined.

sofid

Search

Main Menu > Administration > Configuration > Web SSO > Attribute sharing policies 2 / 3

Policy : GroupMembershipANY

Condition : ANY

Attributes

Attribute	Action	Condition
Filter	Filter	Filter
<input type="checkbox"/> Holder group	Allow	ANY
<input type="checkbox"/> Role & group membership	Allow	ANY

Displayed rows: 2

Undo Apply changes

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

sofid

Search

Main Menu > Administration > Configuration > Web SSO > Identity & Service providers 11 / 13

Identification

Type : OpenID Connect

Identifier : OpenIDConnectApp001

Name : OpenIDConnectApp001

Login rules

Allow impersonations : Target application URL

UID Script : Script to compute the user name to pass to the target application

Ask for consent : No

Ask for group membership after authentication : Yes

Roles required to login : Roles required to login

System where an enabled account is required : System where an enabled account

Use cases

Use case 1 - Log in to an application

User with no groups, Primary or Secondary, 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 logged-in the application with the group with type holder group yes.

OpenID-Connect

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

sofid

Search

?

Main Menu > Administration > Resources > Users

◀ 10 / 324 ▶

Basics

Groups

Accounts

Roles

Effective Roles

Shared accounts

Sessions

User processes

Issues

OTP devices

Tokens

Common attributes

User name :
Agatha

First name :
Agatha

Last Name :
Christie

Middle name :
Middle name

Full name :
Agatha Christie

Organization

Type :
External user

Primary group :
RRHH

Home server :
Home server

Profile server :
Profile server

RRHH department

Please, identify yourself.

User name:

agatha

Change user name

Password:

Login

Cancel


A service provider named angularApp needs to authenticate you.


c. Get the JSON id_token


}

SAML

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





[Main Menu](#) > [Administration](#) > [Resources](#) > [Users](#) ◀ 10 / 324 ▶ 

[Basics](#) [Groups](#) [Accounts](#) [Roles](#) [Effective Roles](#) [Shared accounts](#) [Sessions](#) [User processes](#) [Issues](#) [OTP devices](#) [Tokens](#)

Common attributes

User name :

First name :


Last Name :


Middle name :


Full name :

Organization

Type :

Primary group :  RRHH department

Home server : 

Profile server : 

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



Please, identify yourself.

User name:
[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. 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>XvRU5/lrZYcgR9xjTjGQJ5VLRBtHHDbprEoa9ROxqzw=</ds:DigestValue>
        </ds:Reference>
      </ds:SignedInfo>

      <ds:SignatureValue>F2+sP+Aq8SHII56/9mYi2B+f6oFerlaMU81Y5IK5wD+oYNGNsOjMHbwkK5gaHWk2Isr+
TEhK0YMQTFfjUK0NLVuXHvQTyAfN3p6kxjXTXOq6TaLAfbivuUdzh1dEX61I63id//rGi92NbLU+p2TV/dmTS4fCOh
pxm5Sry5i49o=</ds:SignatureValue>
      <ds:KeyInfo>
        <ds:X509Data>

        <ds:X509Certificate>MIICKTCCAZKgAwIBAgIGAY3q71O5MA0GCSqGSIb3DQEBCwUAMFgxJzAIBgNVBAMMHm
h0dHBzOi8v
c3luYy1zZXJ2ZXlubmV0Y29tcG9zZTEcMBoGA1UECwwTRmVkZXJhdGlvbiBzZXJ2aWNlc3RMA0G
A1UECgwGU09GRkiEMB4XDTI0MDIyNzE0MjkyOVVoXDTM0MDIyNzE0MjkyOVowWDEnMCUGA1UEAwwe
aHR0cHM6Ly9zeW5jLXNlcnZlci5uZXRjb21wb3NIMRwwGgYDVQQQLDBNGZWRLcmF0aW9uIHNIcnZp
Y2VzMq8wDQYDVQQKDAZTT0ZGSUQwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAJZ5G9BnTSLh
X8VOVbdyY01EUkgHexi97+e1iGA0r1WM6cTu4Ku3k7/eflB5ZZfteRKbPwa719y8Ytb5W4RFcZ6O
XzHz9o+FhG64tZHEo4xwVdukv6rOatSSlhomEhruhX+x7OpFnnlXNSCypi1xjEQylm8GJKxpxjk
RjvkgfXLAgMBAAEwDQYJKoZIhvcNAQELBQADgYEATbs8iLBYEcPdPBjtmNHYrQpXb3nc83Acmxxy
```

```
/pEe4hXaMoB1rBuxNf47liqJd9H6k5oXWcGgG8FyrdOxpY3eE8cw1s+6tM/MACMRuhuV4bQhR
FD1aizcW6fQUfvmkRLUgS1o8BMZZjCWW22FPeSkIFXATE/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="_d6a8c2cecd0e8bd085da5c4c8279444">
  <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 logged-in the application with the holder group selected.

OpenID-Connect

a. User Agatha with three groups with Role holder Yes

Agatha - Agatha Christie



<input type="checkbox"/>	▼ User	▲ ▼ Group
	<input type="text" value="Filter"/>	<input type="text" value="Filter"/>
<input type="checkbox"/>	Agatha	Sales
<input type="checkbox"/>	Agatha	RRHH
<input type="checkbox"/>	Agatha	Marketing

Displayed rows:



Please, identify yourself.

User name:

[Change user name](#)

Password:

[Login](#)[Cancel](#)

A service provider named angularApp needs to authenticate you.

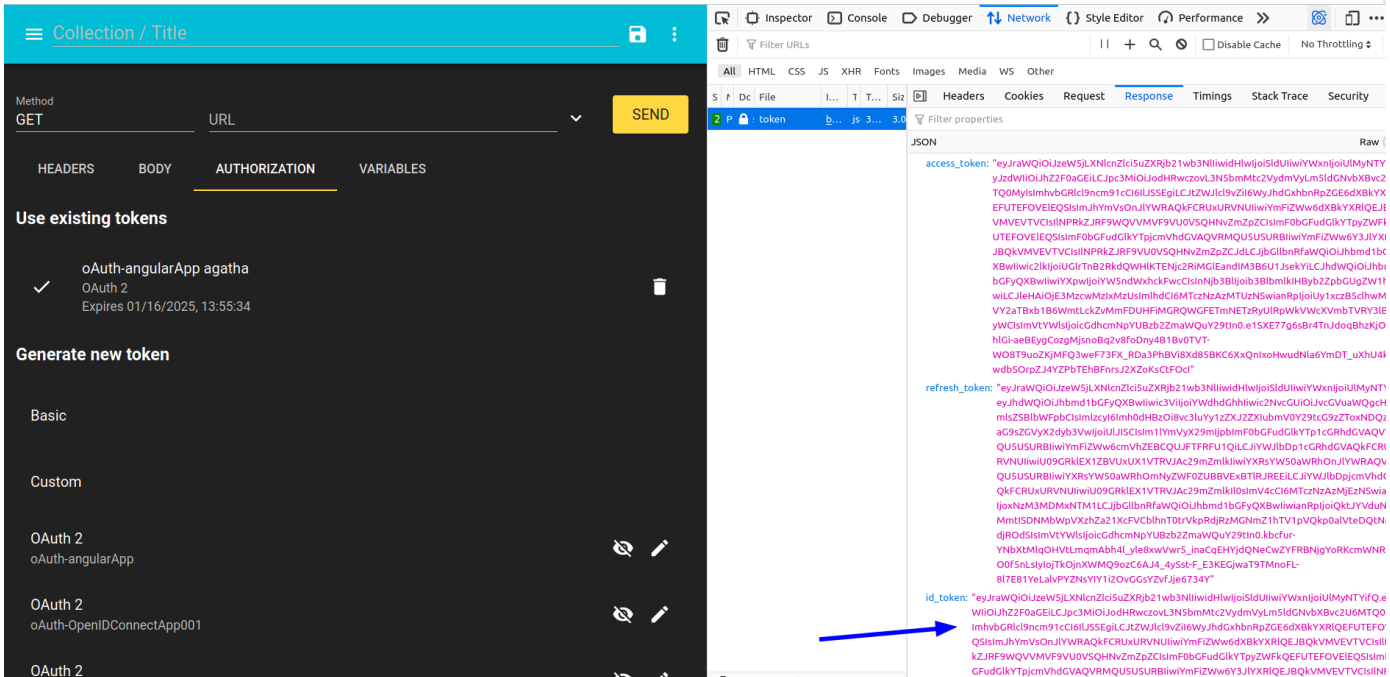
c. The user has to select the holder group to login

Select the group in which you need to carry out your activities.

- ☒ Marketing - Marketing department
- ☐ RRHH - RRHH department
- ☐ Sales - Sales

[Accept](#)

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




[Main Menu](#) > [Administration](#) > [Resources](#) > [Users](#) ◀ 10 / 324 ▶

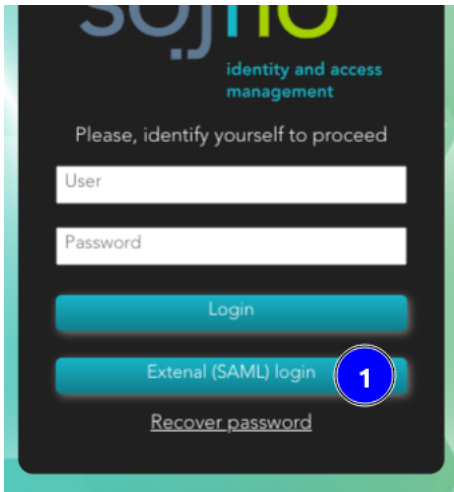
[Basics](#) [Groups](#) [Accounts](#) [Roles](#) [Effective Roles](#) [Shared accounts](#) [Sessions](#) [User processes](#) [Issues](#) [OTP devices](#) [Tokens](#)

Agatha - Agatha Christie

<input type="checkbox"/>	▼ User	⬆ Group
	<input type="text" value="Filter"/>	<input type="text" value="Filter"/>
<input type="checkbox"/>	Agatha	Sales
<input type="checkbox"/>	Agatha	RRHH
<input type="checkbox"/>	Agatha	Marketing

Displayed rows: 

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



Please, identify yourself.

User name: [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

Select the group in which you need to carry out your activities.

- ☒ Marketing - Marketing department
- ☐ RRHH - RRHH department
- ☐ Sales - Sales

[Accept](#)

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/xmllenc#sha256"></ds:DigestMethod>
          <ds:DigestValue>iAUWStZjBdxEjBwMff3ivxJlIXxHPpK9mVf2GZeziu8=</ds:DigestValue>
        </ds:Reference>
      </ds:SignedInfo>

    <ds:SignatureValue>N6ZRA6LXJiuve7qIkVlsdmmBp/YKrnGb4bfeV32xdPgLLvWRVQhNWSfWtidoxJUxTESnJOy
wpiwth/NHIHzSji4X/4ChV3XeP3xUZ1QV29iNm2w16KGuAUlwME/mIGMDuUdSAehaOa/2j17jVTrFL9f2QUFKcbPJ
```

```
obsWDR9vOqs=</ds:SignatureValue>
  <ds:KeyInfo>
    <ds:X509Data>

      <ds:X509Certificate>MIICKTCCA ZKgAwIBAgIGAY3q71O5MA0GCSqGSIb3DQEBCwUAMFgxJzAIBgNVBAMMHm
      h0dHBzOi8v
      c3luYy1zZXJ2ZXlubmV0Y29tcG9zZTEcMBoGA1UECwwTRmVkZXJhdGlvbiBzZXJ2aWNlczEPMA0G
      A1UECgwGU09GRKIEMB4XDTI0MDIyNzE0MjkyOVVoXDTM0MDIyNzE0MjkyOVowWDEnMCUGA1UEAwwe
      aHR0cHM6Ly9zeW5jLXNlcnZlci5uZXRjb21wb3NIMRwwGgYDVQLDBNGZWRIcmF0aW9uIHNIcnZp
      Y2VzMqQ8wDQYDVQQKDAZTT0ZGSUQwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAJZ5G9BnTSLh
      X8VOVbdyY01EUkgHexi97+e1iGA0r1WM6cTu4Ku3k7/efIB5ZZfteRKbPwa719y8Ytb5W4RfcZ6O
      XzHz9o+FhG64tZHEo4xwVdukv6rOatSSlhomEhruhX+x7OpFnnlXNSCyp11xjEQylm8GJKxpjk
      RjvkgfXLA gMBAAEWdQYJKoZIhvcNAQELBQADgYEATbs8iLBYEcPdPBjtmNHyrQpXb3nc83Acmxyy
      /pEe4hXaMoB1rBuxNf47liqJlD9H6k5oXWcGgG8FyrdOxpY3eE8cw1s+6tM/MACMRuhuV4bQhR
      FD1aizcW6fQUfvmkRLUgS1o8BMZZjCWW22FPeSkIFXATE/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="_8a28efb06654a2baf0e0ceb3eb6ea35b">
  <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 logged-in to an application

Agatha user is logged-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-VB3wehrRilj6wrE9lUtnpVlo0rEwcHTbhndDuV4_kPpA7PDwCTNXhMbGly",
  "email": "agatha@soffid.com"
}
```

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

Agatha user is logged-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-NrELNAsY8s33gz8il7sE63PH6CSlvJhIKm6LmZsxW2F-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