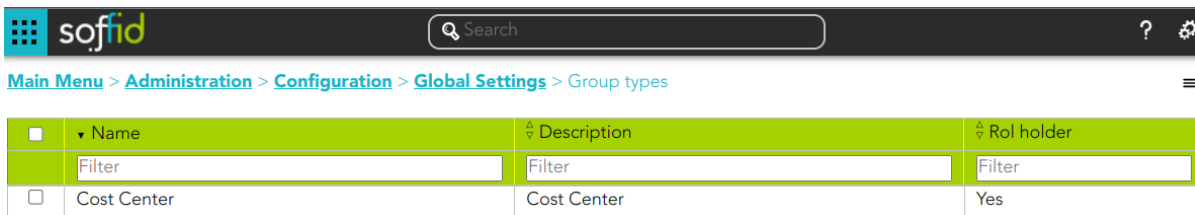


Use cases

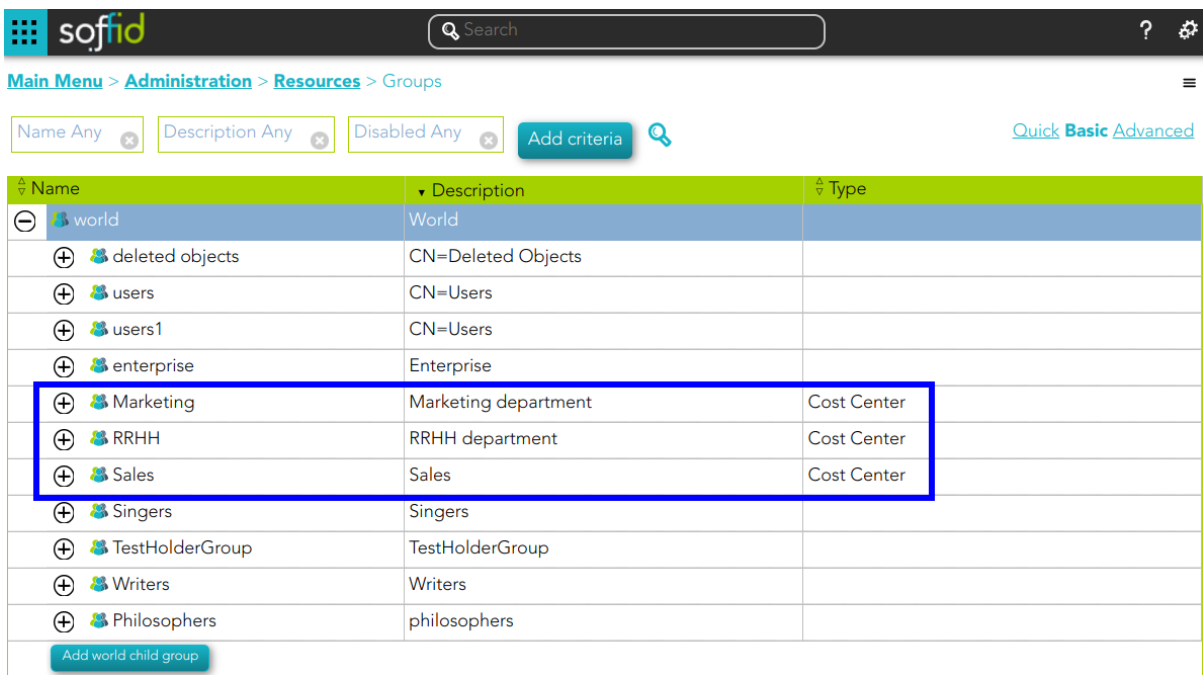
Premises

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



Name	Description	Rol holder
Filter	Filter	Filter
Cost Center	Cost Center	Yes

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



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	

Total rows: 12



3. An attribute sharing policy has been defined.

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.

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)

The screenshot shows the user profile for Agatha Christie in the sofid system. The navigation path is Main Menu > Administration > Resources > Users < 10 / 324 >. The 'Basics' tab is active, showing user details and organization information.

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 (RRHH department)
- Home server : Home server
- Profile server : Profile server

The screenshot shows the user profile for Agatha Christie in the sofid system, with the 'Groups' tab selected. The navigation path is Main Menu > Administration > Resources > Users < 10 / 324 >. The 'Agatha - Agatha Christie' page title is visible.

Agatha - Agatha Christie

<input type="checkbox"/>	▼ User	⬇ Group
	Filter	Filter
<input type="checkbox"/>	Agatha	Writers

Displayed rows: +

The screenshot shows the user profile for Agatha Christie in the sofid system, with the 'Roles' tab selected. The navigation path is Main Menu > Administration > Resources > Users < 10 / 324 >. The 'Agatha - Agatha Christie' page title is visible.

Agatha - Agatha Christie

<input type="checkbox"/>	Risk	▼ Role	⬇ System	⬇ Account	⬇ Inform...	⬇ Start date	⬇ End date	⬇ Domain value	⬇ Holder.
		Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
<input type="checkbox"/>		SOFFID HOLDER_CONDOMAIN004	soffid	Agatha	SOFFID	20/1/2025		RRHH	RRHH
<input type="checkbox"/>		SOFFID HOLDER_CONDOMAIN004	soffid	Agatha	SOFFID	20/1/2025		Writers	RRHH
<input type="checkbox"/>		SOFFID HOLDER_CONDOMAIN005	soffid	Agatha	SOFFID	20/1/2025		Philosophers	RRHH

Displayed rows: +

-

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

Change user name

Password:

Login

Cancel

A service provider named angularApp needs to authenticate you.

c. Get the JSON id_token

The screenshot shows the Chrome DevTools Network tab. A request to 'token' is selected, and the 'Response' tab is active, displaying a JSON object. The 'id_token' field is highlighted with a blue arrow. The 'id_token' value is a long Base64-encoded string. On the left, the 'Authorization' tab shows an existing token for 'oAuth 2' with an expiration time of 01/16/2025, 13:55:34.

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",
  "member_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-HaE9DCXfQv4wLRuFgGRbI1B_9wDFBd6X4ILJBv4vS6mL1yG3S0Ee_Nv",
"email": "agatha@soffid.com"
}
```

SAML

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

The screenshot displays the user management interface for 'soffid'. The breadcrumb trail is 'Main Menu > Administration > Resources > Users < 10 / 324 >'. The navigation menu includes 'Basics', 'Groups', 'Accounts', 'Roles', 'Effective Roles', 'Shared accounts', 'Sessions', 'User processes', 'Issues', 'OTP devices', and 'Tokens'. The 'Basics' tab is active. The user details are organized into two columns: 'Common attributes' and 'Organization'.

Common attributes		Organization	
User name :	Agatha	Type :	External user
First name :	Agatha	Primary group :	RRHH RRHH department
Last Name :	Christie	Home server :	Home server
Middle name :	Middle name	Profile server :	Profile server
Full name :	Agatha Christie		

Agatha - Agatha Christie

<input type="checkbox"/>	▼ User	▲ Group
	Filter	Filter
<input type="checkbox"/>	Agatha	Writers

Displayed rows:



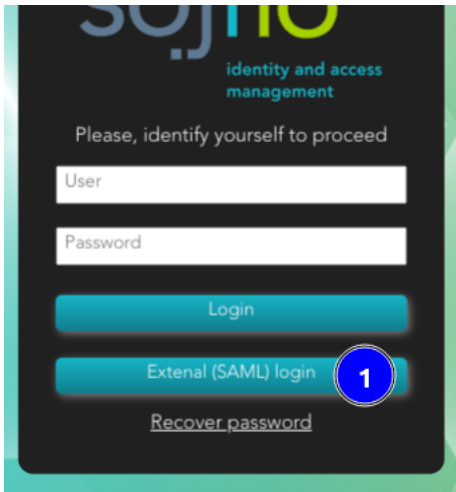
Agatha - Agatha Christie

<input type="checkbox"/>	Risk	▼ Role	▲ System	▲ Account	▲ Inform...	▲ Start date	▲ End date	▲ Domain value	▲ Holder
		Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
<input type="checkbox"/>		SOFFID_HOLDER_CONDOMAIN004	soffid	Agatha	SOFFID	20/1/2025		RRHH	RRHH
<input type="checkbox"/>		SOFFID_HOLDER_CONDOMAIN004	soffid	Agatha	SOFFID	20/1/2025		Writers	RRHH
<input type="checkbox"/>		SOFFID_HOLDER_CONDOMAIN005	soffid	Agatha	SOFFID	20/1/2025		Philosophers	RRHH

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. 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>qEEAkYqFFZxatl6DaVme4lfrojC3zafaKFH+TpiDurY=</ds:DigestValue>
        </ds:Reference>
      </ds:SignedInfo>

      <ds:SignatureValue>TeVSWaALsRLMwYxi71/b1k8jKYOrFb7qS9qva2T5T3yKpNLwZxnmRqWznbBM7wpr9U3V
0scfh5M1ex/NGflbADbxih7uwUVK8YSAZPwlx/4LXEx0uOxpQi7ZiDOvhb2jkKLdvztvUkBGGeJhJGCJy/2WrOHIEdzs
n4T4c7TBdWZc=</ds:SignatureValue>
      <ds:KeyInfo>
        <ds:X509Data>

        <ds:X509Certificate>MIICKTCCAZKgAwIBAgIGAY3q71O5MA0GCSqGSIb3DQEBCwUAMFgxJzAlBgNVBAMMHm
h0dHBzOi8v
c3luYy1zZXJ2ZXlubmV0Y29tcG9zZTEcMBoGA1UECwwTRmVkZXJhdGlvbiBzZXJ2aWNlczEPMA0G
A1UECgwGU09GRkiEMB4XDTI0MDIyNzE0MjkyOVowXDTM0MDIyNzE0MjkyOVowWDEnMCUGA1UEAwwe
aHR0cHM6Ly9zeW5jLXNlcnZlci5uZXRjb21wb3NIMRwwGgYDVQQQLDBNGZWRIcmF0aW9uIHNIcnZp
Y2VzMQ8wDQYDVQQKDAZTT0ZGSUQwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAJZ5G9BnTSLh
X8VOVbdyY01EUkgHexi97+e1iGA0r1WM6cTu4Ku3k7/efIB5ZZfteRkbpwa719y8Ytb5W4RfcZ6O
XzHz9o+FhG64tZHEo4xwVdukv6rOatSSlhomEhruhX+x7OpFnnIXNSCypi1xjEQyIm8GJKxpxjk
RjvkgfXLAgMBAAEwDQYJKoZIhvcNAQELBQADgYEATbs8iLBYEcPdPBjtmNHYrQpXb3nc83Acmyyy
```

```
/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="_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 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:



Agatha - Agatha Christie

<input type="checkbox"/>	Risk	▼ Role	▲ System	▲ Account	▲ Inform...	▲ Start date	▲ End date	▲ Domain value	▲ Holder g.
		<input type="text" value="Filter"/>	<input type="text" value="Filter"/>	<input type="text" value="Filter"/>	<input type="text" value="Filter"/>	<input type="text" value="Filter"/>	<input type="text" value="Filter"/>	<input type="text" value="Filter"/>	<input type="text" value="Filter"/>
<input type="checkbox"/>		SOFFID HOLDER_CONDOMAIN004	soffid	Agatha	SOFFID	20/1/2025		Writers	RRHH
<input type="checkbox"/>		SOFFID HOLDER_CONDOMAIN004	soffid	Agatha	SOFFID	20/1/2025		RRHH	RRHH
<input type="checkbox"/>		SOFFID HOLDER_CONDOMAIN004	soffid	Agatha	SOFFID	20/1/2025		Philosophers	Sales
<input type="checkbox"/>		SOFFID HOLDER_CONDOMAIN005	soffid	Agatha	SOFFID	20/1/2025		Writers	Marketing
<input type="checkbox"/>		SOFFID HOLDER_CONDOMAIN005	soffid	Agatha	SOFFID	20/1/2025		Philosophers	RRHH

Displayed rows:



Please, identify yourself.

User name:

[Change user name](#)

Password:

A service provider named angularApp needs to authenticate you.

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


```

"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-dtA7LVcjpyM0yvI5UPst9vV2",
"email": "agatha@soffid.com"
}

```

SAML

a. User Agatha with three groups with Role holder Yes

The screenshot shows the Soffid user management interface. At the top, there is a search bar and a navigation menu with options like Basics, Groups, Accounts, Roles, Effective Roles, Shared accounts, Sessions, User processes, Issues, OTP devices, and Tokens. The current view is for a user named Agatha - Agatha Christie. Below the user name, there is a table with two columns: User and Group. The table contains three rows, each representing a group assigned to the user Agatha.

<input type="checkbox"/>	User	Group
<input type="checkbox"/>	Agatha	Sales
<input type="checkbox"/>	Agatha	RRHH
<input type="checkbox"/>	Agatha	Marketing

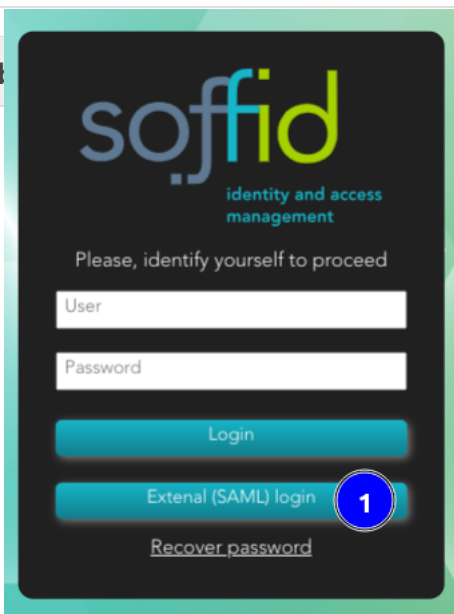
Displayed rows:



Agatha - Agatha Christie

<input type="checkbox"/>	Risk	Role	System	Account	Inform...	Start date	End date	Domain value	Holder g.
		<input type="text" value="Filter"/>	<input type="text" value="Filter"/>	<input type="text" value="Filter"/>	<input type="text" value="Filter"/>	<input type="text" value="Filter"/>	<input type="text" value="Filter"/>	<input type="text" value="Filter"/>	<input type="text" value="Filter"/>
<input type="checkbox"/>		SOFFID_HOLDER_CONDOMAIN004	soffid	Agatha	SOFFID	20/1/2025		Writers	RRHH
<input type="checkbox"/>		SOFFID_HOLDER_CONDOMAIN004	soffid	Agatha	SOFFID	20/1/2025		RRHH	RRHH
<input type="checkbox"/>		SOFFID_HOLDER_CONDOMAIN004	soffid	Agatha	SOFFID	20/1/2025		Philosophers	Sales
<input type="checkbox"/>		SOFFID_HOLDER_CONDOMAIN005	soffid	Agatha	SOFFID	20/1/2025		Writers	Marketing
<input type="checkbox"/>		SOFFID_HOLDER_CONDOMAIN005	soffid	Agatha	SOFFID	20/1/2025		Philosophers	RRHH

Displayed rows:



Enter user and password to login

Please, identify yourself.

User name: [Change user name](#)

Password: [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="_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/xmlsig#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>FllpGC4P+i4OYv+1MxIw2tdgPgheB6zsE2QhbHTUP3U=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>

<ds:SignatureValue>VI2a9cx7vPKH+fppjyRQ4g+/NPknfxVzgbekaWomAxHvgNegRonlalUiRiiVLC5DdcT1dkO
85c9FJgf5x8CgEfKFRKVNcaNWRVMZIZYUR/DKjyVH0F8a8IZMdHyxB9z3xj0QVqs7536dalA38hD5p4TG4PoNttY
LhE1tFGd8Qsl=</ds:SignatureValue>
  <ds:KeyInfo>
  <ds:X509Data>

<ds:X509Certificate>MIICKTCCA ZKgAwlBAglGAY3q71O5MA0GCSqGSIb3DQEBCwUAMFgxjzAIBgNVBAMMHm
h0dHBzOi8v
c3luYy1zZXJ2ZXlubmV0Y29tcG9zZTEcMBoGA1UECwwTRmVkZXJhdGlvbiBzZXJ2aWNlczEPMA0G
A1UECgwGU09GRKIEMB4XDTI0MDIyNzE0MjkyOVVoXDTM0MDIyNzE0MjkyOVowWDEnMCUGA1UEAwwe
aHR0cHM6Ly9zeW5jLXNlcnZlci5uZXRjb21wb3NIMRwwGgYDVQLDBNGZWRlcmF0aW9uIHNIcnZp
Y2VzMQ8wDQYDVQQKDAZTT0ZGSUQwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAJZ5G9BnTSLh
X8VOVbdyY01EUkgHexi97+e1iGA0r1WM6cTu4Ku3k7/efIB5ZZfteRKbPwa719y8Ytb5W4RFcZ6O
XzHz9o+FhG64tZHEo4xwVdukv6rOatSSlhomEhruhX+x7OpFnnlXNSCypi1xjEQyIm8GJKxpxjk
RjvkgfXLAGMBAAEwDQYJKoZIhvcNAQELBQADgYEATbs8iLBYEcPdPBjtmNHyrQpXb3nc83Acmxyy
/pEe4hXaMoB1rBuxNf47liqJajld9H6k5oXWcGgG8FyrdOxpY3eE8cw1s+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="_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 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_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-dtA7LVcjpyM0yvi5UPst9vV2",
  "email": "agatha@soffid.com"
}
```

b. Agatha 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",
  "member_of": [
    "SOFFID_VAULT_USER@soffid",
    "SOFFID HOLDER_CONDOMAIN005/Writers@soffid",
    "SOFFID_USER@soffid"
  ],
  "nonce": null,
  "sid": "WDSQEzO6LIgxvQkq/zylzL/LddKKy/j0",
  "aud": "OpenIDConnectApp001",
  "azp": "OpenIDConnectApp001",
  "auth_time": 1737367082,
  "scope": "openid",
  "exp": 1737367683,
  "iat": 1737367083,
  "jti": "C5xSE7UK0lgwgff5CI7SPnpZvcRSm8WI0GZMXXObKdCMOuP50qbZjCcuGW7KpJqN",
  "email": "agatha@soffid.com"
}
```

Revision #22

Created 16 January 2025 08:21:09

Updated 20 January 2025 12:06:47