New features

- 2026-06-12 New feature: inheriting authorisations in new applications
- 2026-06-12 New feature: use holder group in UID script
- 2026-09-30 New feature: hide root page

2026-06-12 New feature: inheriting authorisations in new applications

The new feature

> Now, on the Application access tree page, when creating an entry point, a **folder** or an **application**, the **authorizations** from the **parent** folder are now **inherited**.

Bear in mind

Please note the following points:

- If there are multiple levels of folders, **only** the **authorizations** from the **parent folder** are **inherited**.

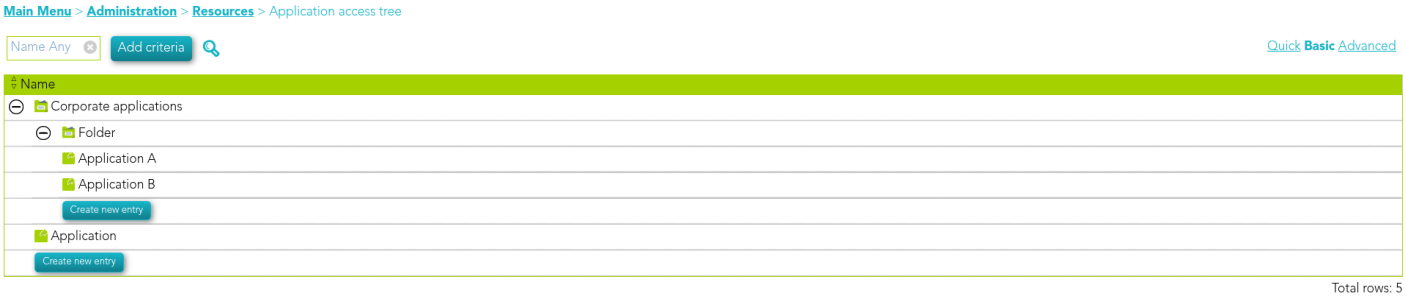
How to configure it?

The following **components** must be installed:

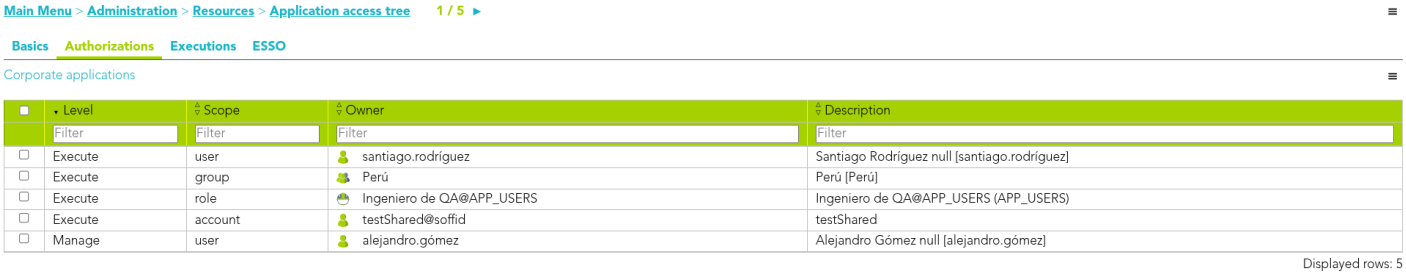
- Console 3.6.75 (or higher)

Let's look at an example

On our "'**Application access tree**" page, there are **two** levels of **folders**.



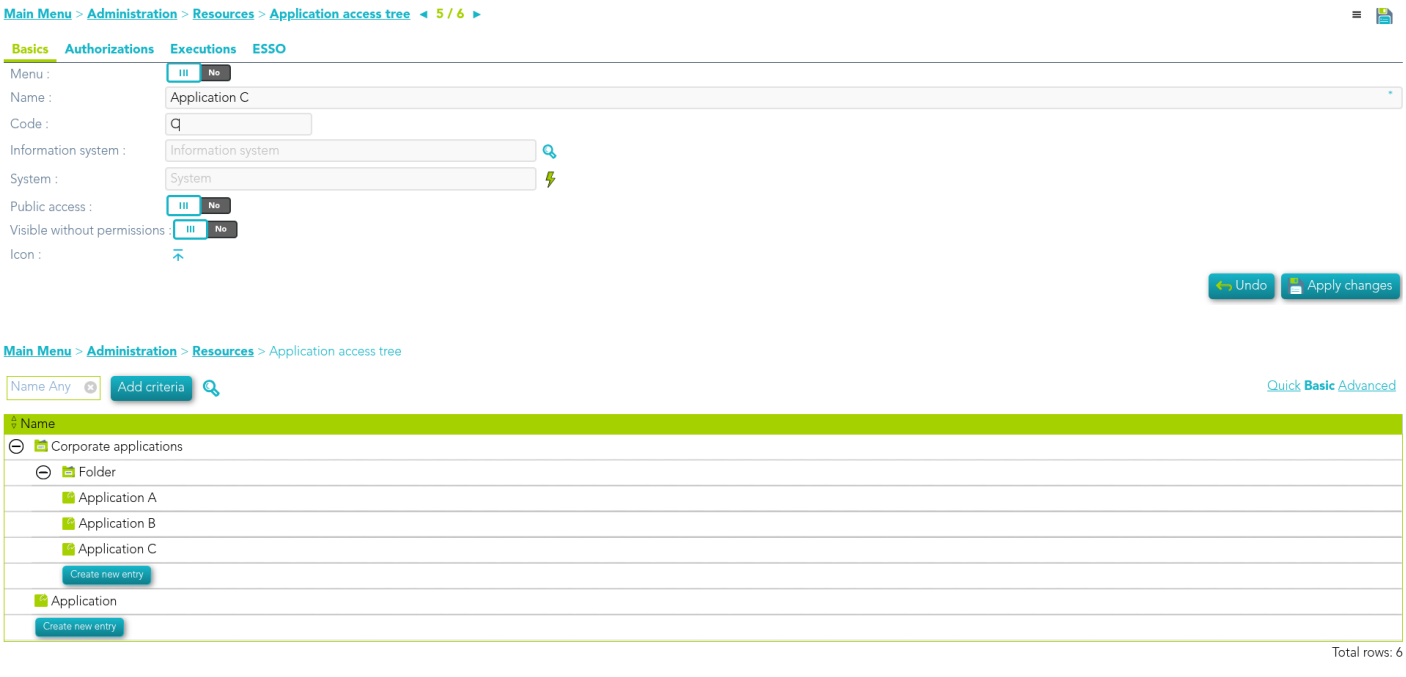
The **first folder** contains the following authorisations.



The **second folder** contains the following authorisations, the "Manager" user is different.



Now, let's **create a new application** in the **second folder**.



If we access it, we can see that it has the **authorizations** of its **parent Folder**.

Basics | Authorizations | Executions | ESSO

Application C

Level	Scope	Owner	Description
Filter	Filter	Filter	Filter
Execute	user	santiago.rodríguez	Santiago Rodríguez null [santiago.rodríguez]
Execute	group	Perú	Perú [Perú]
Execute	role	Ingeniero de QA@APP_USERS	Ingeniero de QA@APP_USERS (APP_USERS)
Execute	account	testShared@soffid	testShared
Manage	user	benjamín.flores	Benjamín Flores null [benjamín.flores]

Displayed rows: 5

2026-06-12 New feature: use holder group in UID script

The new feature

> Now, on the Service provider configuration page, the **holder group** can now be used in the **UID** selection **script**.

Bear in mind

Please note the following points:

- If there are multiple levels of folders, **only** the **authorizations** from the **parent folder** are **inherited**.

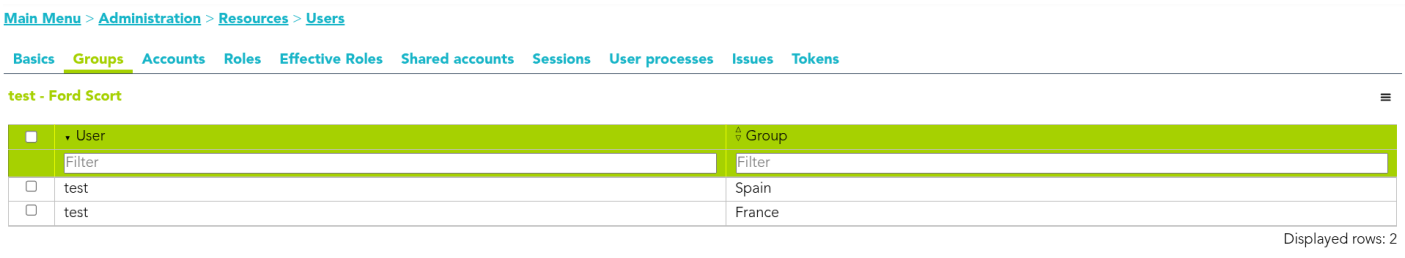
How to configure it?

The following **components** must be installed:

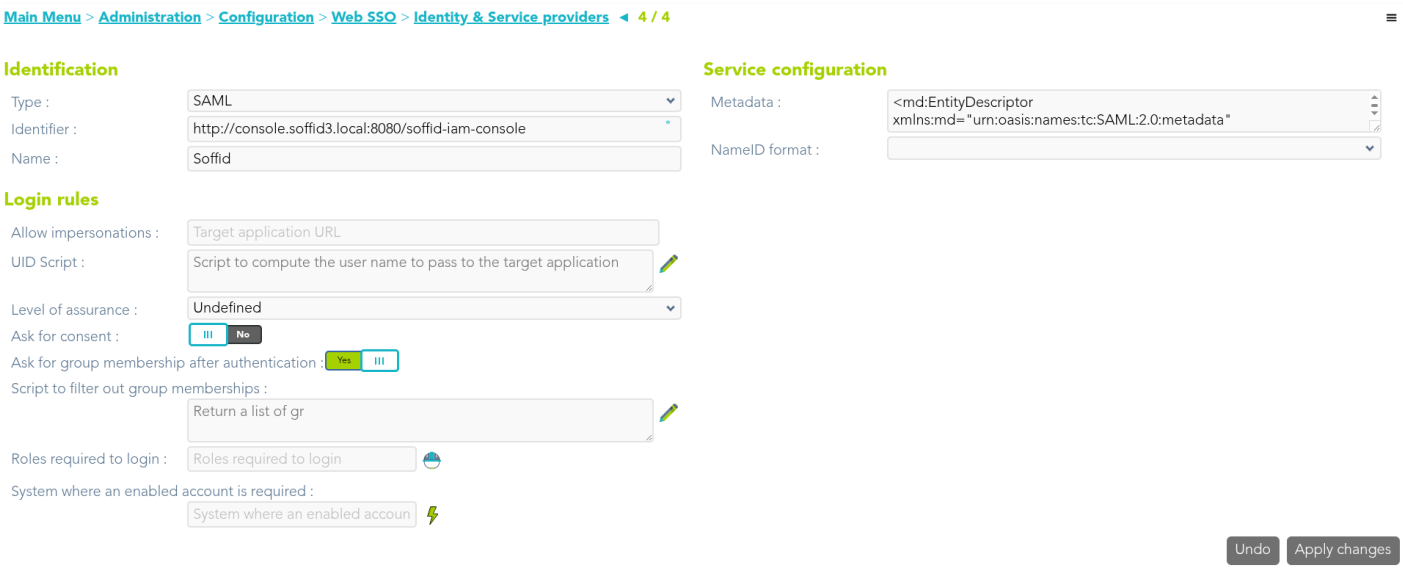
- Federation addon 3.6.92 (or higher)

Let's look at an example

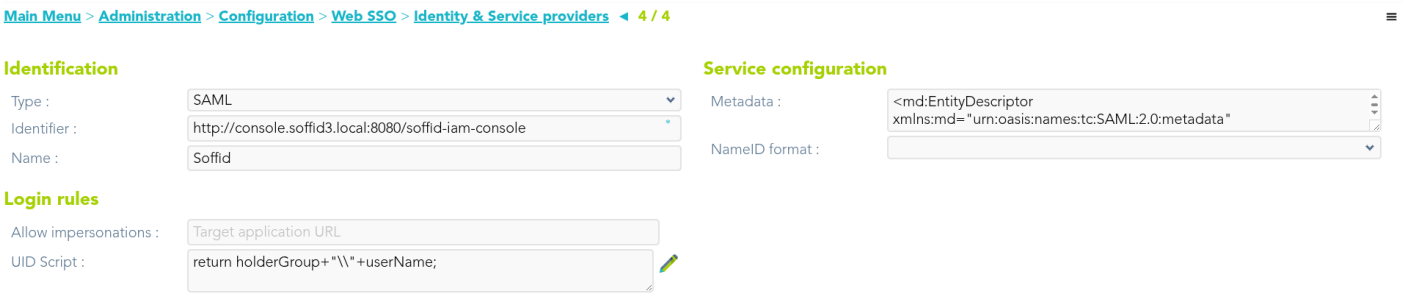
First of all, we check that we have a **user** with **holder groups**.



We can now confirm that the **service provider** has the option "" enabled.



We use the **holderGroup** attribute in the **UID script**.



Finally, we're going to authenticate with the service provider and **check the value of the UID attribute**.

English Español Català



Please, identify yourself.

User name: test

Change user name

Password: ••••••••••

Login

A service provider named http://console.soffid3.local:8080/soffid-iam-console needs to authenticate you.

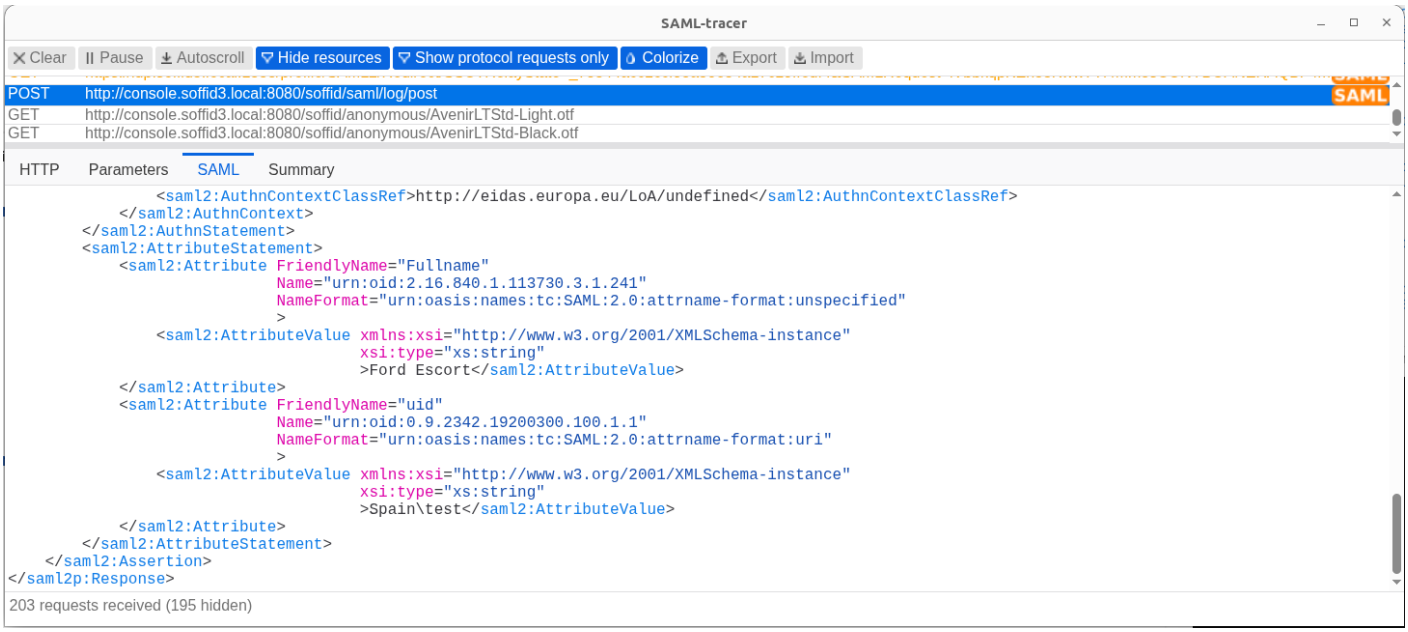
English Español Català



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

- ○ France - France
- ◉ Spain - Spain

Accept


SAML-tracer
Clear
Pause
Autoscroll
Hide resources
Show protocol requests only
Colorize
Export
Import
POST http://console.soffid3.local:8080/soffid/saml/log/post
SAML
GET http://console.soffid3.local:8080/soffid/anonymous/AvenirLTStd-Light.otf
GET http://console.soffid3.local:8080/soffid/anonymous/AvenirLTStd-Black.otf
HTTP
Parameters
SAML
Summary
<saml2:AuthnContextClassRef>http://eidas.europa.eu/LoA/undefined</saml2:AuthnContextClassRef>
</saml2:AuthnContext>
</saml2:AuthnStatement>
<saml2:AttributeStatement>
<saml2:Attribute FriendlyName="Fullname"
Name="urn:oid:2.16.840.1.113730.3.1.241"
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"
>Ford Escort</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"
>Spain\test</saml2:AttributeValue>
</saml2:Attribute>
</saml2:AttributeStatement>
</saml2:Assertion>
</saml2p:Response>
203 requests received (195 hidden)

2026-09-30 New feature: hide root page

The new feature

> On the **Identity providers** configuration page, the option "**Hide root page**" has been added so that nothing is displayed at the IdP’s root URL.

Bear in mind

Please note the following points:

- This change only affects the IdP’s base URL: https://hostname:port

How to configure it?

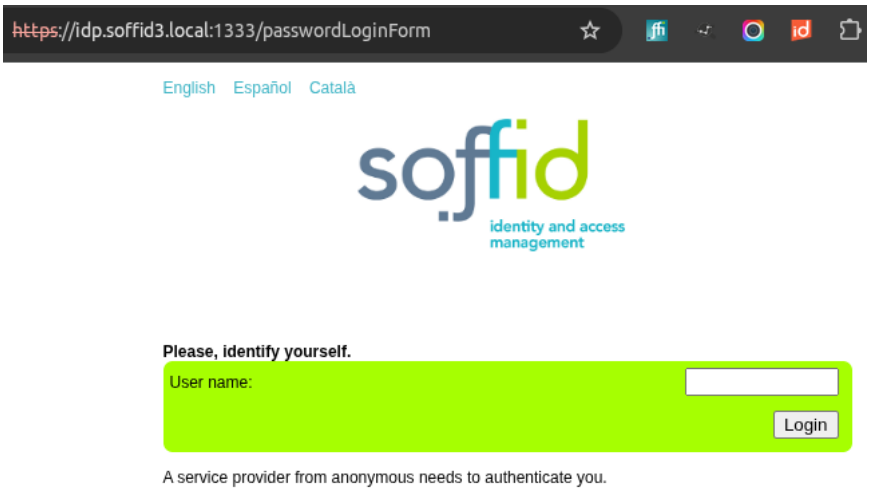
The following **components** must be installed:

- Federation addon 3.6.96 (or higher)

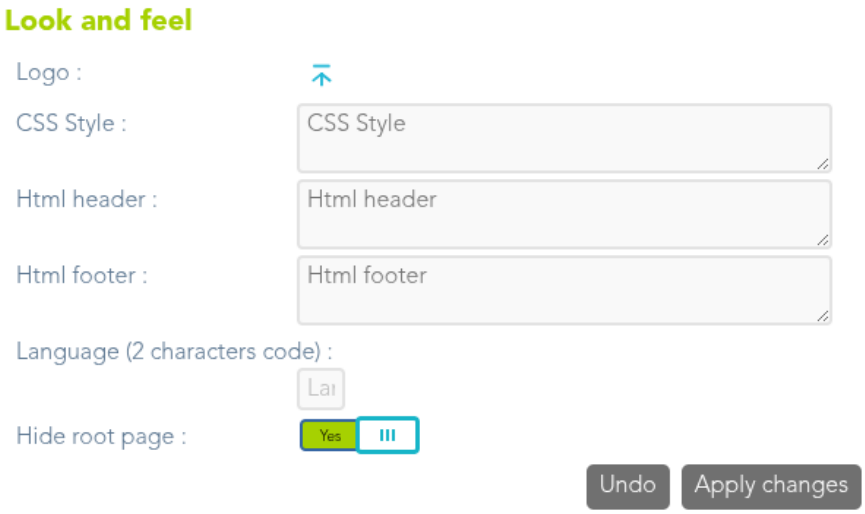
Let's look at an example

If we go directly to the IdP’s URL, the IdP’s login page appears.

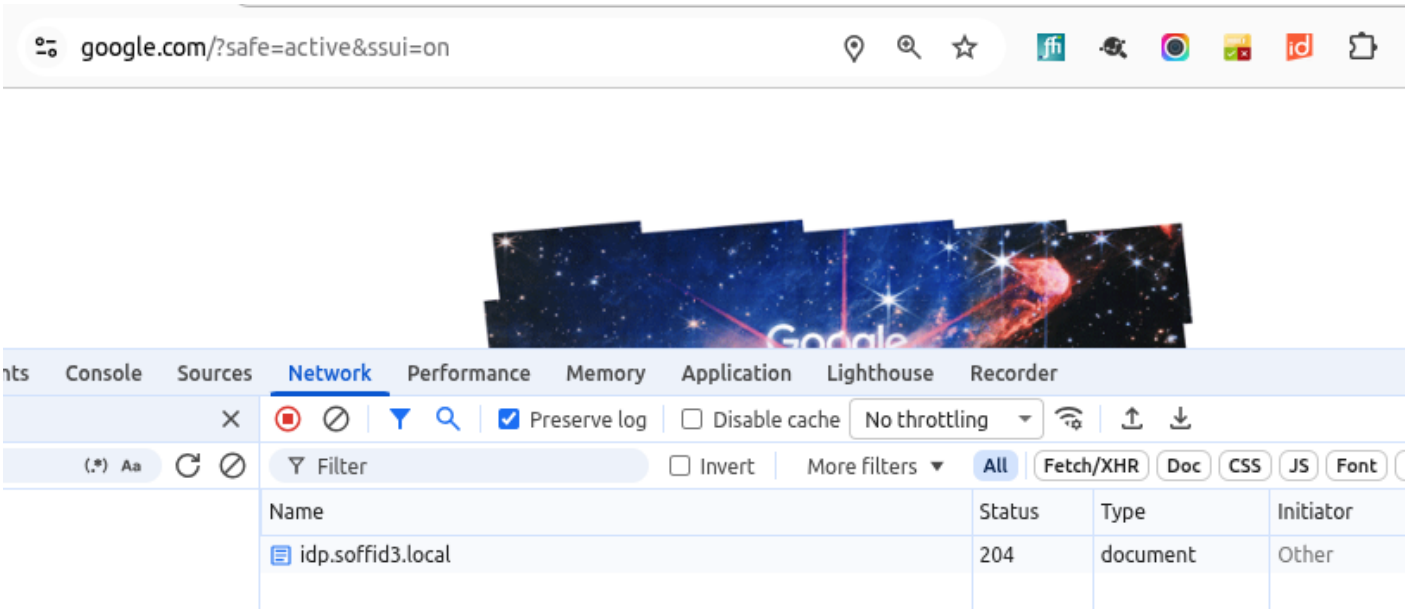
https://idp.soffid3.local:1333



If we want to disable this behaviour so that the IdP does nothing, we need to go to the **Soffid IdP** and **enable** the "**Hide root page**" attribute.



Now, when accessing to the IdP's **root URL**, the browser will **reject** the request and display the **same page as before**.


google.com/?safe=active&ssui=on
Console
Sources
Network
Performance
Memory
Application
Lighthouse
Recorder
Preserve log
Disable cache
No throttling
Filter
Invert
More filters
All
Fetch/XHR
Doc
CSS
JS
Font
Name
Status
Type
Initiator
idp.soffid3.local
204
document
Other