Steps to configure
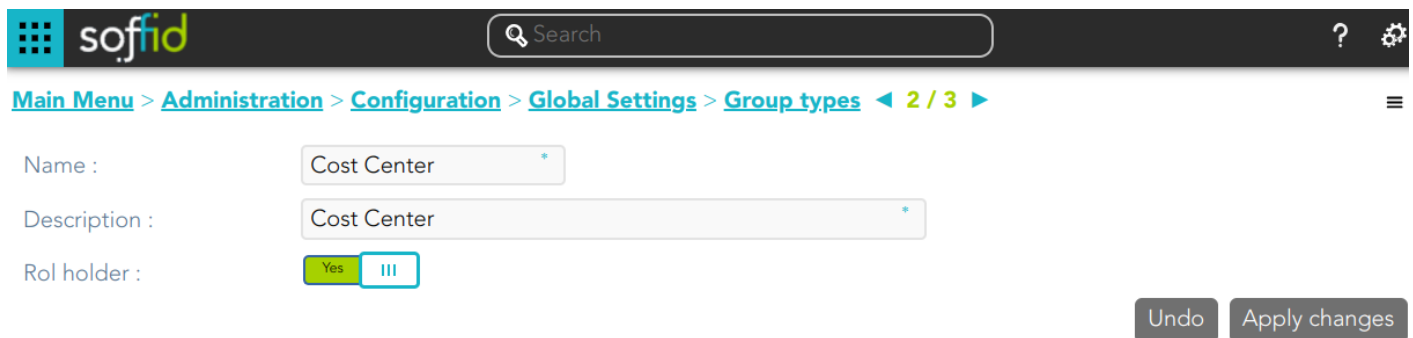
Steps to configure

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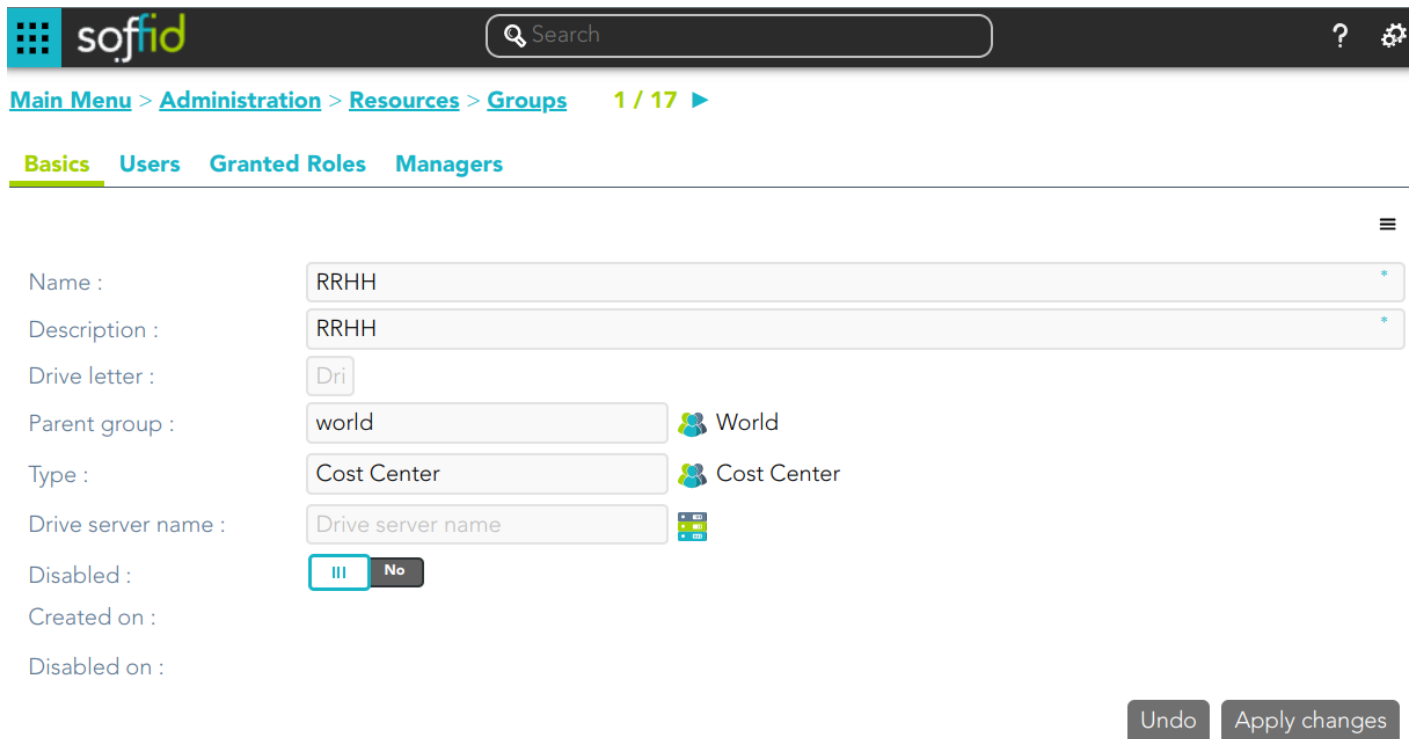
2. Groups: Assign Groups to the organizational unit. Define groups with the appropriate group type.

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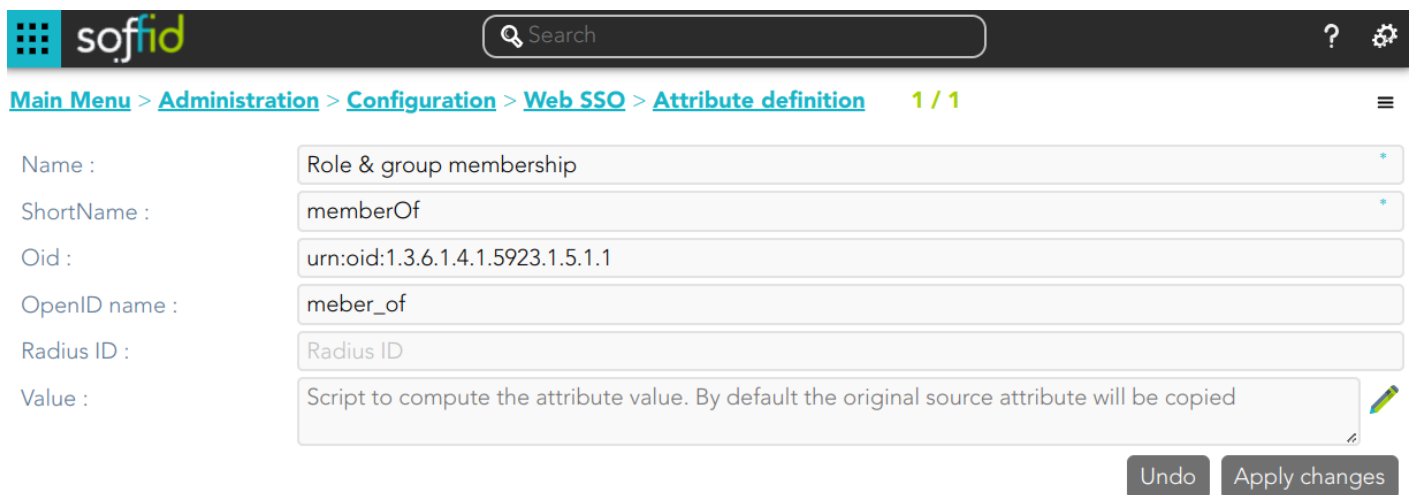
4. Attribute definition: Define the **Attributes to deliver** from the identity providers to the service providers

4.1. Holder group

soffid	Q Search	? ⚙

Main Menu > Administration > Configuration > Web SSO > Attribute definition   1 / 1   ≡

Name :	Holder group	*
ShortName :	HolderGroup	*
Oid :	urn:oid:1.3.6.1.4.1.22896.3.1.7	
OpenID name :	holder_group	
Radius ID :	Radius ID	
Value :	Script to compute the attribute value. By default the original source attribute will be copied	✏

Undo   Apply changes

4.2. Role & group membership

soffid	Q Search	? ⚙

Main Menu > Administration > Configuration > Web SSO > Attribute definition   1 / 1   ≡

Name :	Role & group membership	*
ShortName :	memberOf	*
Oid :	urn:oid:1.3.6.1.4.1.5923.1.5.1.1	
OpenID name :	meber_of	
Radius ID :	Radius ID	
Value :	Script to compute the attribute value. By default the original source attribute will be copied	✏

Undo   Apply changes

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.

Policy : GroupMembershipANY *

Condition : ANY

Attributes

▼ Attribute	Action	Condition
Filter	Filter	Filter
Holder group	Allow	ANY
Role & group membership	Allow	ANY

Displayed rows: 2

Undo   Apply changes

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

Identification

Type :	OpenID Connect
Identifier :	angularApp *
Name :	angularApp

Login rules

Allow impersonations :	Target application URL
UID Script :	Script to compute the user name to pass to the target application
Ask for consent :	III No
Ask for group membership after authentication :	Yes III
Roles required to login :	Roles required to login
System where an enabled account is required :	System where an enabled accoun

OpenID authorization flow

Revision #6
Created 16 January 2025 08:20:49 by pgarcia@soffid.com
Updated 17 January 2025 10:08:14 by pgarcia@soffid.com