Example Role centric PEP

Role centric Enforcement Point

Use case example

We want to define a policy to restrict access to the Soffid console role's page (MainMenu > Administration > Resources > Roles).

The users who belong to the "enterprise" group as primary group (from this point forward: *end-users*) will have limitations to perform some actions on the Soffid console roles page.

1. The *end-users* could query all the roles information.
2. The *end-users* could update any role in the information systems "ERP RRHH"
3. The *end-users* could not create any role.
4. The *end-users* could not delete any role.

XACML Editor

Policy set

First of all, we define a policy set. We need to define the subject, in that case users who belong to "enterprise" as primary group.

Policy set

Identifier: : TestRoleCentricPEP

Version: : 1

Description: : TestRoleCentricPEP

Policy Combining Algorithm: :

Permit overrides

Target

Subjects	Operator	Value
urn:com:soffid:xacml:subject:primaryGroup	=	enterprise

Displayed rows: 1

Resources	Operator	Value

Displayed rows: 0

Actions	Operator	Value

Displayed rows: 0

Environments	Operator	Value

Displayed rows: 0

Obligations

Obligation	Full fill on	Attribute	Value

Displayed rows: 0

Then, we can define a policy to manage the different actions that the *end-users* could perform.

TestRoleCentricPEP (1)	TestRoleCentricPEP
RoleCentricPolicy (1)	RoleCentricPolicy

Policy

The policy will apply to an only one user. That policy will be to protect the role resource.

Policy

Identifier: : RoleCentricPolicy

Version: : 1

Description: : RoleCentricPolicy

Rule Combining Algorithm: :

Permit overrides

Target

Subjects	Operator	Value

Displayed rows: 0

Resources	Operator	Value
com:soffid:iam:xacml:1.0:resource:soffid-object	=	role

Displayed rows: 1

Actions	Operator	Value

Displayed rows: 0

Environments	Operator	Value

Displayed rows: 0

Variables

Variable	Expression
iSystem	"ERP RRHH"

Displayed rows: 1

Rules

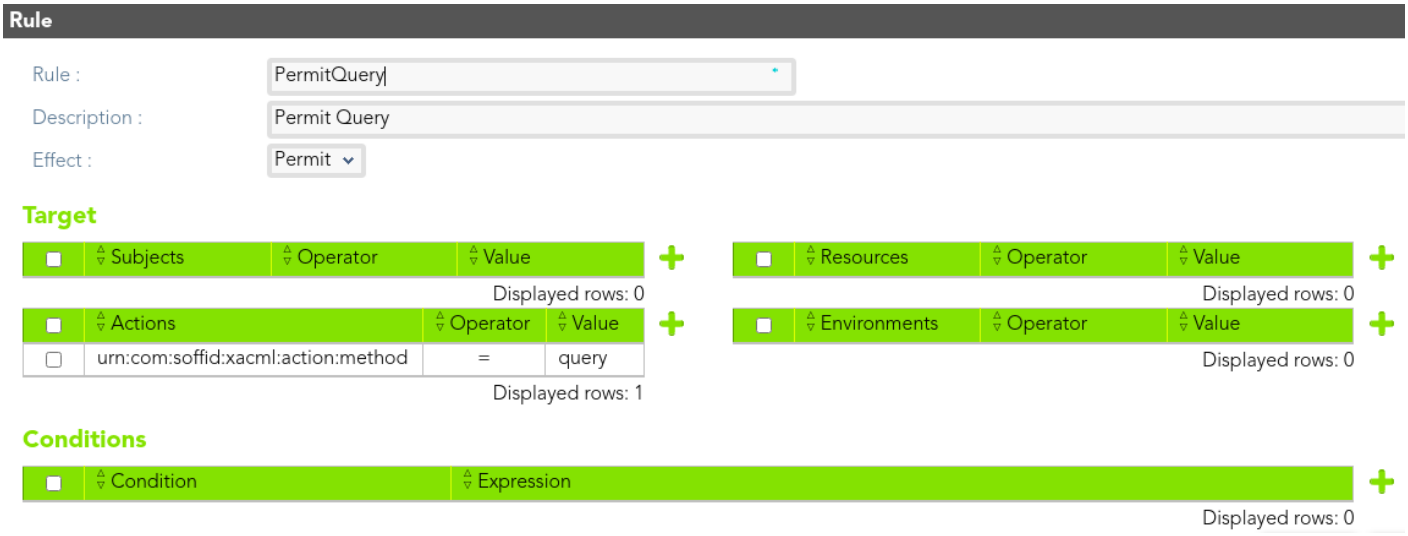
Rule	Description	Effect
DenyUpdate	Deny Update	Deny
PermitQuery	Permit Query	Permit
DenyDelete	Deny Delete	Deny
DenyCreate	Deny Create	Deny

Displayed rows: 4

Rule 1

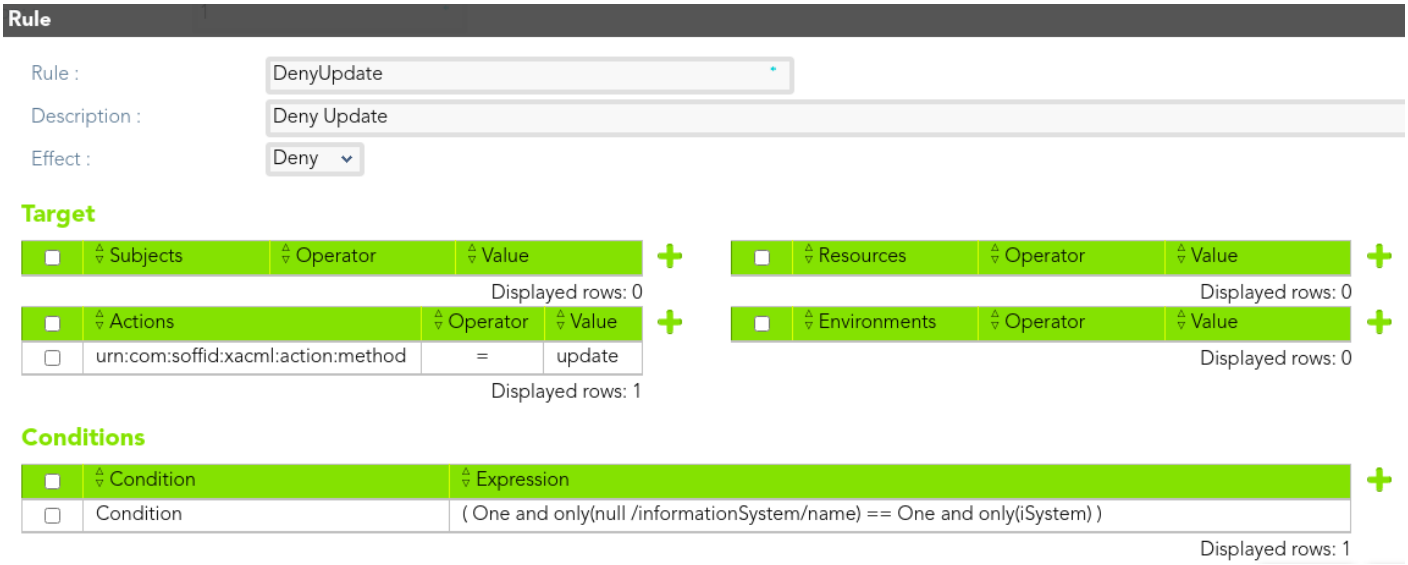
> The *end-users* could query all the roles information.

We define the rule that allow to the end-users to query all the roles information.



Rule 2

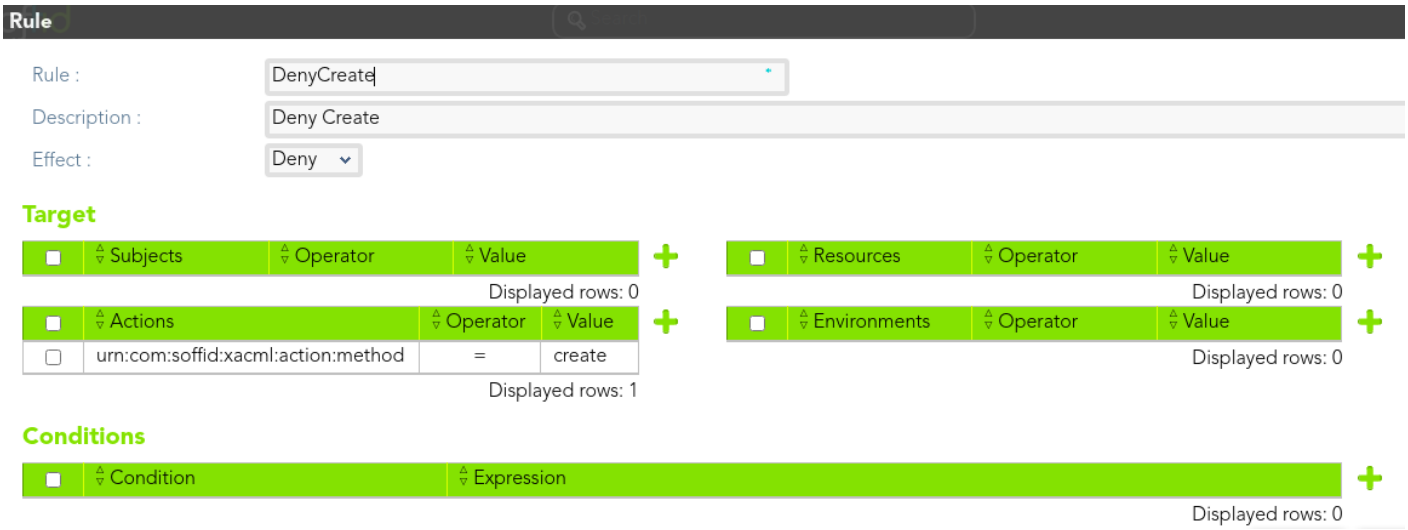
> The *end-users* could update any role in the information systems "ERP RRHH"



Rule 3

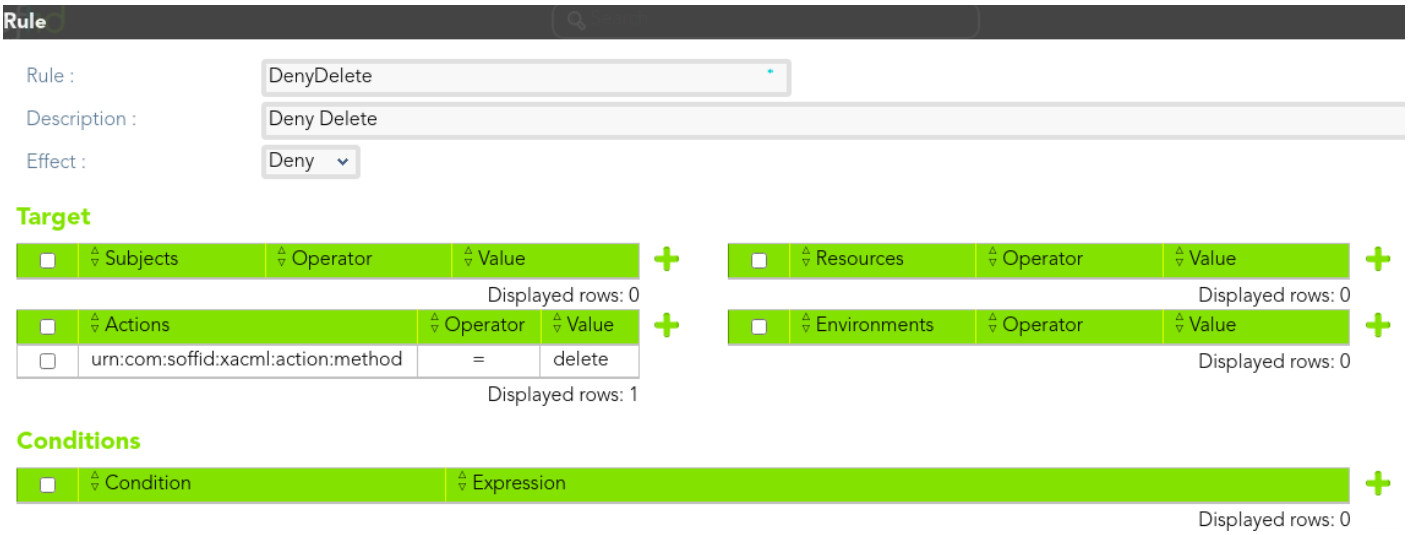
>

> The *end-users* could not create any role.



Rule 4

> The *end-users* could not delete any role.

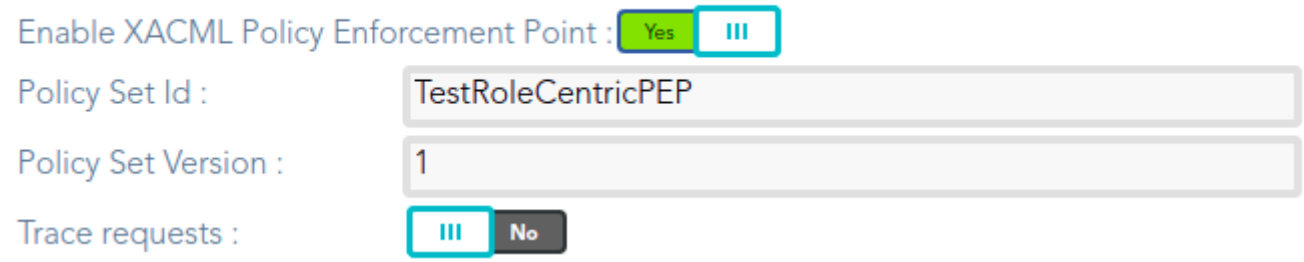


Download XML

> You can download a XML file with the example: policy-TestRoleCentricPEP.xml

Configure PEP

Role centric Policy Enforcement Point



Revision #12
Created 3 August 2021 10:50:26
Updated 6 August 2021 08:45:45