
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

<input type="checkbox"/>	Subjects	Operator	Value	+	<input type="checkbox"/>	Resources	Operator	Value	+
<input checked="" type="checkbox"/>	urn:com:soffid:xacml:subject:primaryGroup	=	enterprise						
Displayed rows: 1					Displayed rows: 0				
<input type="checkbox"/>	Actions	Operator	Value	+	<input type="checkbox"/>	Environments	Operator	Value	+
Displayed rows: 0					Displayed rows: 0				

Obligations

<input type="checkbox"/>	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

<input type="checkbox"/>	Subjects	Operator	Value	+	<input type="checkbox"/>	Resources	Operator	Value	+
					<input type="checkbox"/>	com:soffid:iam:xacml:1.0:resource:soffid-object	=	role	
Displayed rows: 0					Displayed rows: 1				
<input type="checkbox"/>	Actions	Operator	Value	+	<input type="checkbox"/>	Environments	Operator	Value	+
Displayed rows: 0					Displayed rows: 0				

Variables

<input type="checkbox"/>	Variable	Expression	+
<input type="checkbox"/>	iSystem	"ERP RRHH"	
Displayed rows: 1			

Rules

<input type="checkbox"/>	Rule	Description	Effect	+
<input type="checkbox"/>	DenyUpdate	Deny Update	Deny	
<input type="checkbox"/>	PermitQuery	Permit Query	Permit	
<input type="checkbox"/>	DenyDelete	Deny Delete	Deny	
<input type="checkbox"/>	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

Rule : PermitQuery

Description : Permit Query

Effect : Permit

Target

<input type="checkbox"/>	Subjects	Operator	Value	+	<input type="checkbox"/>	Resources	Operator	Value	+
				Displayed rows: 0					Displayed rows: 0
<input type="checkbox"/>	Actions	Operator	Value	+	<input type="checkbox"/>	Environments	Operator	Value	+
<input type="checkbox"/>	urn:com:soffid:xacml:action:method	=	query	Displayed rows: 1					Displayed rows: 0

Conditions

<input type="checkbox"/>	Condition	Expression	+
			Displayed rows: 0

Rule 2

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

Rule

Rule : DenyUpdate

Description : Deny Update

Effect : Deny

Target

<input type="checkbox"/>	Subjects	Operator	Value	+	<input type="checkbox"/>	Resources	Operator	Value	+
				Displayed rows: 0					Displayed rows: 0
<input type="checkbox"/>	Actions	Operator	Value	+	<input type="checkbox"/>	Environments	Operator	Value	+
<input type="checkbox"/>	urn:com:soffid:xacml:action:method	=	update	Displayed rows: 1					Displayed rows: 0

Conditions

<input type="checkbox"/>	Condition	Expression	+
<input type="checkbox"/>	Condition	(One and only(null /informationSystem/name) == One and only(iSystem))	Displayed rows: 1

Rule 3

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

Rule

Rule :

DenyCreate

Description :

Deny Create

Effect :

Deny

Target

Subjects

Operator

Value

Displayed rows: 0

Actions

Operator

Value

urn:com:soffid:xacml:action:method

=

create

Displayed rows: 1

Resources

Operator

Value

Displayed rows: 0

Environments

Operator

Value

Displayed rows: 0

Conditions

Condition

Expression

Displayed rows: 0

Rule 4

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

Rule

Rule :

DenyDelete

Description :

Deny Delete

Effect :

Deny

Target

Subjects

Operator

Value

Displayed rows: 0

Actions

Operator

Value

urn:com:soffid:xacml:action:method

=

delete

Displayed rows: 1

Resources

Operator

Value

Displayed rows: 0

Environments

Operator

Value

Displayed rows: 0

Conditions

Condition

Expression

Displayed rows: 0

Download XML

You can download a XML file with the example: [policy-TestRoleCentricPEP.xml](#)

Configure PEP

Role centric Policy Enforcement Point

Enable XACML Policy Enforcement Point : ☒ Yes ☐ No

Policy Set Id :

Policy Set Version :

Trace requests : ☐ Yes ☒ No

Revision #12

Created 3 August 2021 10:50:26 by pgarcia@soffid.com

Updated 6 August 2021 08:45:45 by pgarcia@soffid.com