

Example Web PEP

Web Policy Enforcement Point

Use case example

We want to define a policy to restrict access to some pages of the Soffid console.

The users who are assigned to the SOFFID_RRHH role (from this point forward: end-users) will have limitations to access to some Soffid console pages:

1. The end-users who belong to the "enterprise" group as primary group, could not access to the groups page.
2. The end-users could not access to role page.
3. En other cases permit access.

XACML Editor

Policy set

First of all, we define a policy set.

Policy set

Identifier:

Version:

Description:

Policy Combining Algorithm:

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	+
Displayed rows: 0					Displayed rows: 0				

Obligations

<input type="checkbox"/>	Obligation	Full fill on	Attribute	Value	+
Displayed rows: 0					

Policy

Then, we can define a policy to manage the access. We need to define the subject, in that case users with SOFFID_RRHH role assigned.

Also, we can define a variable that contains the group name to establish the restrictions.

Policy

Identifier:

Version:

Description:

Rule Combining Algorithm:

Target

<input type="checkbox"/>	Subjects	Operator	Value	+	<input type="checkbox"/>	Resources	Operator	Value	+
<input type="checkbox"/>	urn:oasis:names:tc:xacml:2.0:subject:role	=	SOFFID_RRHH@soffid						
				Displayed rows: 1					Displayed rows: 0
<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"/>	pGroup	"enterprise"	
			Displayed rows: 1

Rules

<input type="checkbox"/>	Rule	Description	Effect	+
<input type="checkbox"/>	Other	Other	Permit	
<input type="checkbox"/>	DenyRoles	Deny access to role page	Deny	
<input type="checkbox"/>	DenyGroups	Deny access to groups page	Deny	
				Displayed rows: 3

Rule 1

“ The end-users who belong to the "enterprise" group as primary group, could not access to the groups page.

Rule

Rule : DenyGroups

Description : Deny access to groups page

Effect : Deny

Target

Subjects	Operator	Value	Resources	Operator	Value
Displayed rows: 0			urn:oasis:names:tc:xacml:1.0:resource:resource-location	=	/resource/group/group.zul
Displayed rows: 0			Displayed rows: 1		
Displayed rows: 0			Displayed rows: 0		

Conditions

Condition	Expression
Condition	(One and only(null /primaryGroup/name) == One and only(pGroup))
Displayed rows: 1	

Rule 2

“ The end-users could not access to role page.

Rule

Rule : DenyRoles

Description : Deny access to role page

Effect : Deny

Target

Subjects	Operator	Value	Resources	Operator	Value
Displayed rows: 0			urn:oasis:names:tc:xacml:1.0:resource:resource-location	=	/resource/application/role.zul
Displayed rows: 0			Displayed rows: 1		
Displayed rows: 0			Displayed rows: 0		

Conditions

Condition	Expression
Displayed rows: 0	

Rule 3

“ En other cases permit access.

Rule 🔍

Rule :

Description :

Effect :

Target

<input type="checkbox"/> <input type="text" value="Subjects"/> <input type="text" value="Operator"/> <input type="text" value="Value"/> <input type="button" value="+"/>	<input type="checkbox"/> <input type="text" value="Resources"/> <input type="text" value="Operator"/> <input type="text" value="Value"/> <input type="button" value="+"/>
Displayed rows: 0	Displayed rows: 0
<input type="checkbox"/> <input type="text" value="Actions"/> <input type="text" value="Operator"/> <input type="text" value="Value"/> <input type="button" value="+"/>	<input type="checkbox"/> <input type="text" value="Environments"/> <input type="text" value="Operator"/> <input type="text" value="Value"/> <input type="button" value="+"/>
Displayed rows: 0	Displayed rows: 0

Conditions

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

Download XML

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

Configure PEP

Web Policy Enforcement Point

Enable XACML Policy Enforcement Point :

Policy Set Id :

Policy Set Version :

Trace requests :

Revision #14

Created 3 August 2021 10:14:37 by pgarcia@soffid.com

Updated 6 August 2021 09:25:00 by pgarcia@soffid.com