

# Example Password Vault PEP

## Password Vault Policy Enforcement Point

### Use case example 1

We want to define a policy to restrict access to the Soffid Password Vault.

The users who are assigned to the SOFFID\_ADMIN role (from this point forward: end-users) will have limitations to perform some actions on the folder "demoFolder" of the Soffid Password Vault

1. The end-users only be able to access the accounts of that folder on labor time. The permissions will be denied in another case.

### Policy set

First of all, we define a policy set that could contain other policy sets and policies.

#### Policy set

Identifier: : VaultDemoPolicies

Version: : 1

Description: : Vault polices

Policy Combining Algorithm: :

Deny overrides

#### 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 set 2

Then, we can create another policy set as a child of the former to manage the folder and to define the subject, in that case, users with SOFFID\_ADMIN role assigned.

Policy set

Identifier: :

demoFolder

Version: :

1

Description: :

Policies for demoFolder

Policy Combining Algorithm: :

Deny overrides

Target

Subjects

Operator

Value

urn:oasis:names:tc:xacml:2.0:subject:role

=

SOFFID\_ADMIN@soffid

Displayed rows: 1

Resources

Operator

Value

urn:com:soffid:xacml:resource:vault

=

/vault/demoFolder

Displayed rows: 1

Actions

Operator

Value

Displayed rows: 0

Environments

Operator

Value

Displayed rows: 0

Obligations

Obligation

Full fill on

Attribute

Value

Displayed rows: 0

That policy set will contain the policies.

⊖ VaultDemoPolicies (1)	Vault polices
⊖ demoFolder (1)	Policies for demoFolder
⊕ TimeToAccess (1)	Time to access to the resources
⊕ UsersRestrictions (1)	Users Restrictions

## Policies

### Policy 1

“ The end-users only be able to access the accounts of that folder on labour time.  
The permissions will be denied in other case.

## Policy

Identifier: : TimeToAccess

Version: : 1

Description: : Time to access to the resources

Rule Combining Algorithm: : Permit overrides

## 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				

## Variables

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

## Rules

<input type="checkbox"/>	⚙️ Rule	⚙️ Description	⚙️ Effect	+
<input type="checkbox"/>	LabourTime	Labour Time	Permit	
<input type="checkbox"/>	Other	Other Deny	Deny	
Displayed rows: 2				

# Rule

We define the rule that permit access to the *end-user*

**Rule**

Rule : LabourTime

Description : Labour Time

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	+
Displayed rows: 0					Displayed rows: 0				

### Conditions

<input type="checkbox"/>	Condition	Expression	+
<input type="checkbox"/>	Between 6:00 and 20:00	(( One and only(Current time) > "6:00:00" ) && ( One and only(Current time) < "20:00:00" ) )	
Displayed rows: 1			

And we define other to deny access.

Rule

Rule :

Other

Description :

Other Deny

Effect :

Deny

Target

Subjects

Operator

Value

+

Displayed rows: 0

Resources

Operator

Value

+

Displayed rows: 0

Actions

Operator

Value

+

Displayed rows: 0

Environments

Operator

Value

+

Displayed rows: 0

Conditions

Condition

Expression

+

Displayed rows: 0

## Use case example 2

We want to define a policy to restrict access to the Soffid Password Vault.

The users who are assigned to the SOFFID\_ADMIN role (from this point forward: end-users) will have limitations to perform some actions on the folder "demoFolder" of the Soffid Password Vault

1. The end-users only be able to access the accounts of that folder on labor time. The permissions will be denied in another case. (Use case example 1)
2. To connect there are some obligations to fulfill

Policy set

Identifier :

demoFolder

Version :

1

Description :

Policies for demoFolder

Policy Combining Algorithm :

Deny overrides

Target

Subjects

Operator

Value

+

urn:oasis:names:tc:xacml:2.0:subject:role

=

SOFFID\_ADMIN@soffid

Displayed rows: 1

Resources

Operator

Value

+

urn:com:soffid:xacml:resource:vault

=

/vault/demoFolder

Displayed rows: 1

Actions

Operator

Value

+

Displayed rows: 0

Environments

Operator

Value

+

Displayed rows: 0

Obligations

Obligation

Full fill on

Attribute

Value

+

urn:soffid:obligation:otp

Permit

timeout

30

urn:soffid:obligation:bpm

Permit

process

Grant account

urn:soffid:obligation:message

Permit

text

This is a protected system. Do not enter without authorization, please.

Displayed rows: 3

Test policy set

Undo

Apply changes

## Use case example 3

We want to define a policy to restrict access to the Soffid Password Vault.

The access will be denied on Sunday.

The screenshot shows the 'soffid' XACML configuration tool. A modal window titled 'Rule' is open, displaying the configuration for a rule named 'DayOfWeek'. The rule's description is 'DayOfWeek' and its effect is 'Deny'. The 'Target' section contains four rows, each with a checkbox, a field for the target type, an operator, a value field, and a 'Displayed rows' count. The 'Conditions' section contains one row with a checkbox, a condition name, and an expression. The 'Undo' and 'Close' buttons are visible at the bottom right of the modal.

Target	Operator	Value	Displayed rows
Subjects			0
Resources			0
Actions			0
Environments			0

Condition	Expression	Displayed rows
Sunday	( Day of week(Current time) == "1" )	1

## Download XML

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

## Configure PEP

**Password vault Policy Enforcement Point ( <https://iam-sync-lab.soffidnetlab:1760//XACML/vault> )**

Enable XACML Policy Enforcement Point : ☒ Yes ☐ No

Policy Set Id :

Policy Set Version :

Trace requests : ☒ Yes ☐ No

---

Revision #16

Created 3 August 2021 10:26:41 by pgarcia@soffid.com

Updated 25 September 2023 13:28:07 by pgarcia@soffid.com