

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"/>	Δ Variable	Δ 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

<input type="checkbox"/>	Subjects	Operator	Value	+
Displayed rows: 0				
<input type="checkbox"/>	Actions	Operator	Value	+
Displayed rows: 0				

<input type="checkbox"/>	Resources	Operator	Value	+
Displayed rows: 0				
<input type="checkbox"/>	Environments	Operator	Value	+
Displayed rows: 0				

Conditions

<input type="checkbox"/>	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

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

<input type="checkbox"/>	Resources	Operator	Value	+
<input type="checkbox"/>	urn:com:soffid:xacml:resource:vault	=	/vault/demoFolder	
Displayed rows: 1				

<input type="checkbox"/>	Actions	Operator	Value	+
Displayed rows: 0				

<input type="checkbox"/>	Environments	Operator	Value	+
Displayed rows: 0				

Obligations

<input type="checkbox"/>	Obligation	Full fill on	Attribute	Value	+
<input type="checkbox"/>	urn:soffid:obligation:otp	Permit	timeout	30	
<input type="checkbox"/>	urn:soffid:obligation:bpm	Permit	process	Grant account	
<input type="checkbox"/>	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.

Rule

Rule : DayOfWeek
Description : DayOfWeek
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: 1
Sunday	(Day of week(Current time) == "1")	

Undo Close

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 III

Policy Set Id : VaultDemoPolicies

Policy Set Version : 1

Trace requests : Yes III

Revision #16

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

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