XACML PEP configuration

Description

The **PEP, Policy enforcement point**, is a component of policy-based management, **where enforce the policies**. It is the component that serves as the gatekeeper to access a digital resource. The PEP gives the PDP, Policy Decision Point, the job of deciding whether or not to authorize the user based on the description of the user's attributes.

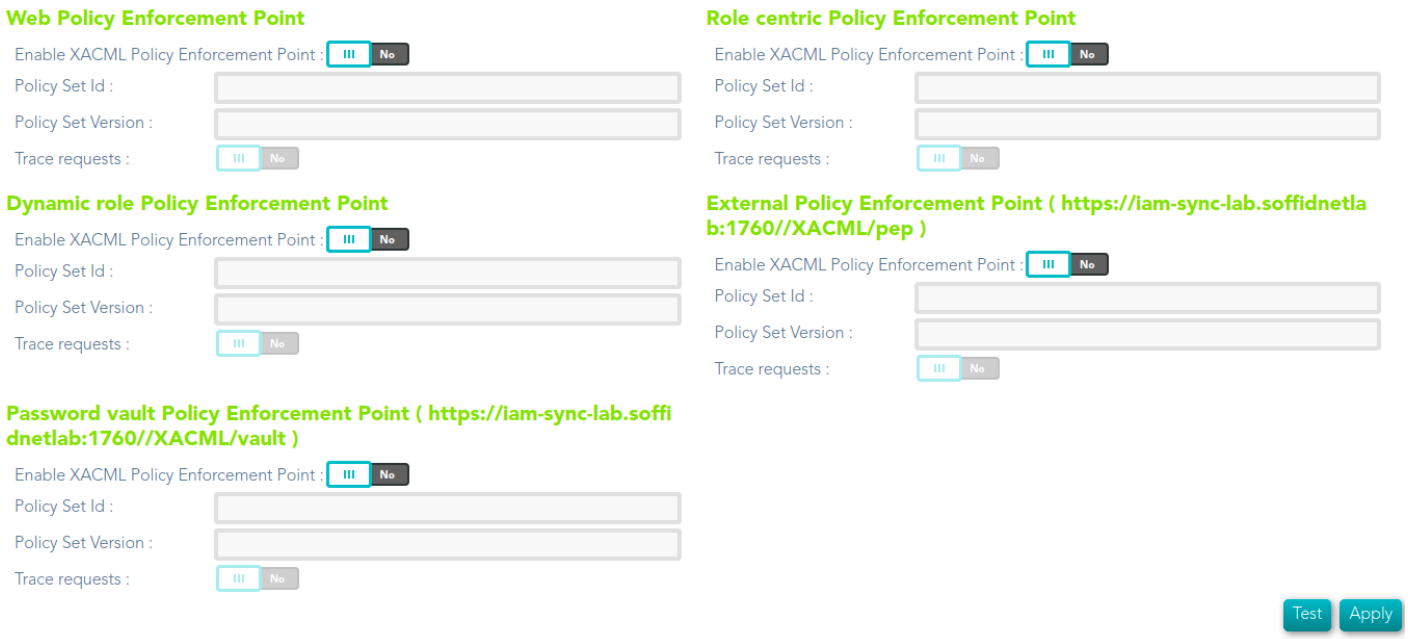
XACML PEP configuration

Soffid allows you to configure different policies enforcement points, each of then can use a different policy set.

Main Menu > Administration > Configuration > Security settings > XACML PEP configuration

- Web Policy Enforcement Point
- Role centric Policy Enforcement Point
- Dynamic role Policy Enforcement Point
- External Policy Enforcement Point
- Password vault Policy Enforcement Point

Screen



Common attributes

Common attributes for each PEP:

- **Enable XACML Policy Enforcement Point**: select the Yes option to enable the PEP.
- **Policy Set Id**: policy set identifier.
- **Policy Set Version**: version of the policy set to enforce.
- **Trace requests**: select the Yes option to enable the trace.

Policies enforcement points

Web Policy Enforcement Point

The policy will be enforced when the user open a new Soffid page. Using this PEP you can define the rules to access to Soffid pages.

SUBJECTS	RESOURCES	ACTIONS	ENVIRONMENTS

User User attributes Account System Role Group Primary Gorup IP Address	Server URL	Get Put Post	Current Time Current Date Current DateTime

Role centric Policy Enforcement Point

The policy will be enforced when the user login into Soffid. It will calculate the user authorizations as of the permissions that the user has assigned.

SUBJECTS	RESOURCES	ACTIONS	ENVIRONMENTS
User User attributes Account System Role Group Primary Gorup IP Address	Soffid object Attributes	create update delete query	Current Time Current Date Current DateTime

Dynamic role Policy Enforcement Point

The policy will be enforced when the user performs an action to evaluate if the user has or not authorization. The user must have the proper role and comply with the XACML rule.

You can use that PEP to split the permissions, for instance, a support group can update the permission of a specific group of user, and another support group can update the permissions of another group of users.

SUBJECTS	RESOURCES	ACTIONS	ENVIRONMENTS
User User attributes Account System Role Group Primary Gorup IP Address	Soffid object Attributes (*)	create update delete query	Current Time Current Date Current DateTime

(*) It is allowed to use "Attribute Selector" to configure Dynamic role policy.

External Policy Enforcement Point (https://iam-sync-lab.soffidnetlab:1760//XACML/pep)

PEP of general purpose. Calling the web service, the clients can made validations and figure out if the users have access.

SUBJECTS	RESOURCES	ACTIONS	ENVIRONMENTS
User User attributes Account System Role Group Primary Gorup IP Address	Token Method Soffid object	Get Put	Current Time Current Date Current DateTime

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

The policy will be enforced when the password vault is used.

SUBJECTS	RESOURCES	ACTIONS	ENVIRONMENTS
User User attributes Account System Role Group Primary Gorup IP Address	Access level Account System Login Vault Folder Server URL	setPassword queryPassword queryPasswordBypassPolicy launch	Current Time Current Date Current DateTime

Revision #4
Created 17 June 2022 07:23:03
Updated 30 November 2022 10:20:26