Implementation

This document summarizes how Soffid has been implemented for this project.

Agents

These agents have been defined in `Main Menu > Administration > Configuration > Integration engine > Agents`:

1. IdP Agent

This agent has been created for the identity provider, for managing and authenticating the identities of users. It would be linked to the identity provider through its Public ID.

2. Source AD Agent

This agent has been created to connect the Soffid console with the Active Directory, so we can carry out the authoritative load, to retrieve identities, and the reconciliation process, to request the accounts and ensure that all users are aligned with their respective roles and responsibilities.

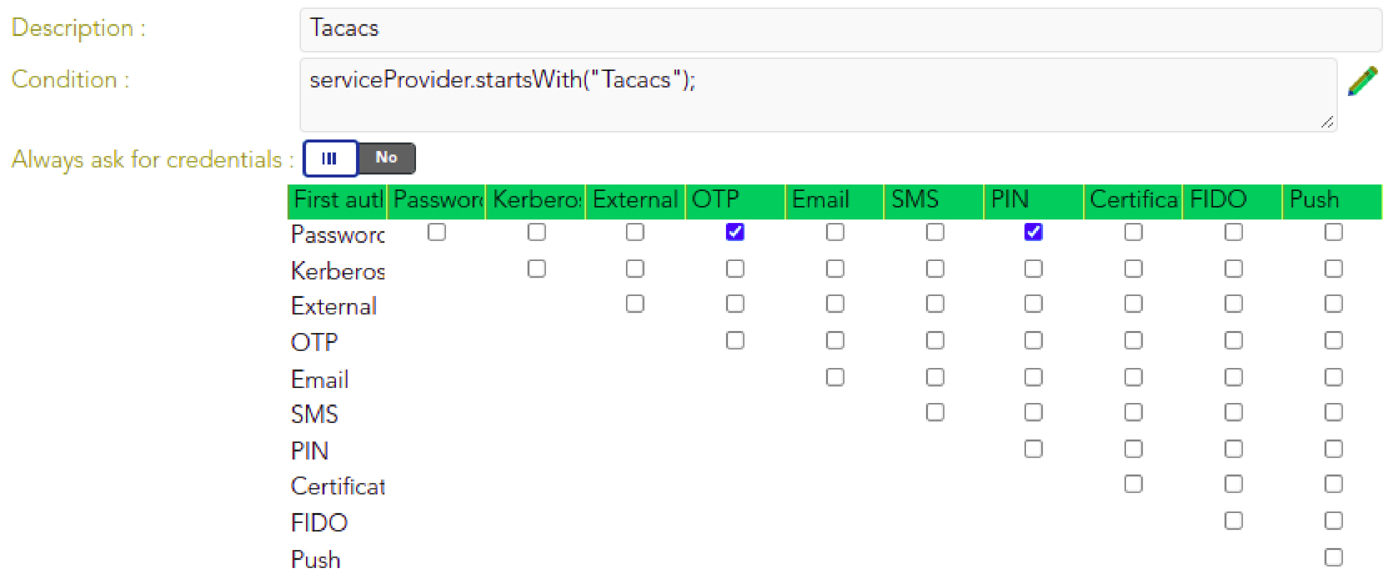
For more information, please refer to Agents.

Identity & Service providers

Only one Entity Group has been created (*Postbank*) in `Main Menu > Administration > Configuration > Web SSO > Identity & Service providers`. The providers defined within this group are:

1. Identity Providers

The identity provider uses Soffid IdP for identity authentication. Adaptive authentication is configured, so if the name of the service provider requesting authentication begins with "Tacacs," two-factor authentication (2FA) will be required, as shown below.



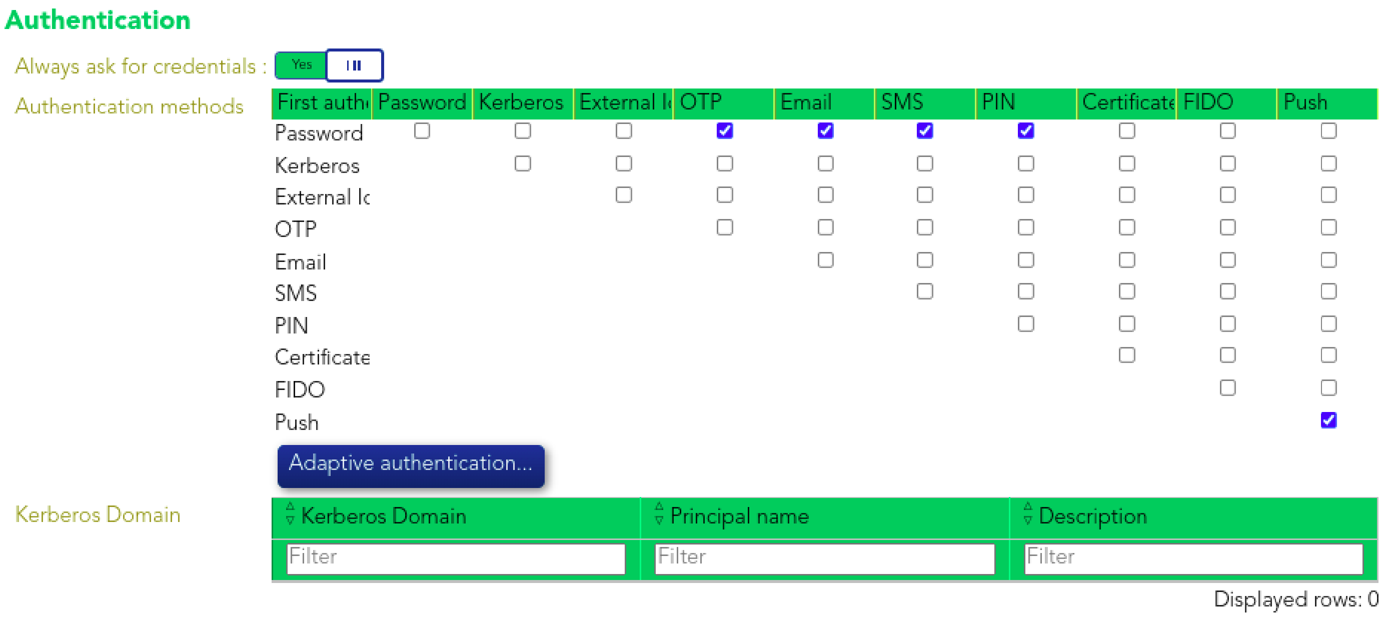
Description : Tacacs

Condition : serviceProvider.startsWith("Tacacs");

Always ask for credentials : No

First autl	Passworc	Kerbero:	External	OTP	Email	SMS	PIN	Certifica	FIDO	Push
Passworc	□	□	□	☑	□	□	☑	□	□	□
Kerberos		□	□	□	□	□	□	□	□	□
External			□	□	□	□	□	□	□	□
OTP				□	□	□	□	□	□	□
Email					□	□	□	□	□	□
SMS						□	□	□	□	□
PIN							□	□	□	□
Certificat								□	□	□
FIDO									□	□
Push										□

Otherwise multi-factor authentication (MFA) will be required.



Authentication

Always ask for credentials : Yes

Authentication methods

First auth	Password	Kerberos	External I	OTP	Email	SMS	PIN	Certificate	FIDO	Push
Password	□	□	□	☑	☑	☑	☑	□	□	□
Kerberos		□	□	□	□	□	□	□	□	□
External Ic			□	□	□	□	□	□	□	□
OTP				□	□	□	□	□	□	□
Email					□	□	□	□	□	□
SMS						□	□	□	□	□
PIN							□	□	□	□
Certificate								□	□	□
FIDO									□	□
Push										☑

Kerberos Domain

Kerberos Domain	Principal name	Description
Filter	Filter	Filter

Displayed rows: 0

Additionally, TLS and SAML can be configured using certificates and private keys, uploading the PKCS12 files.

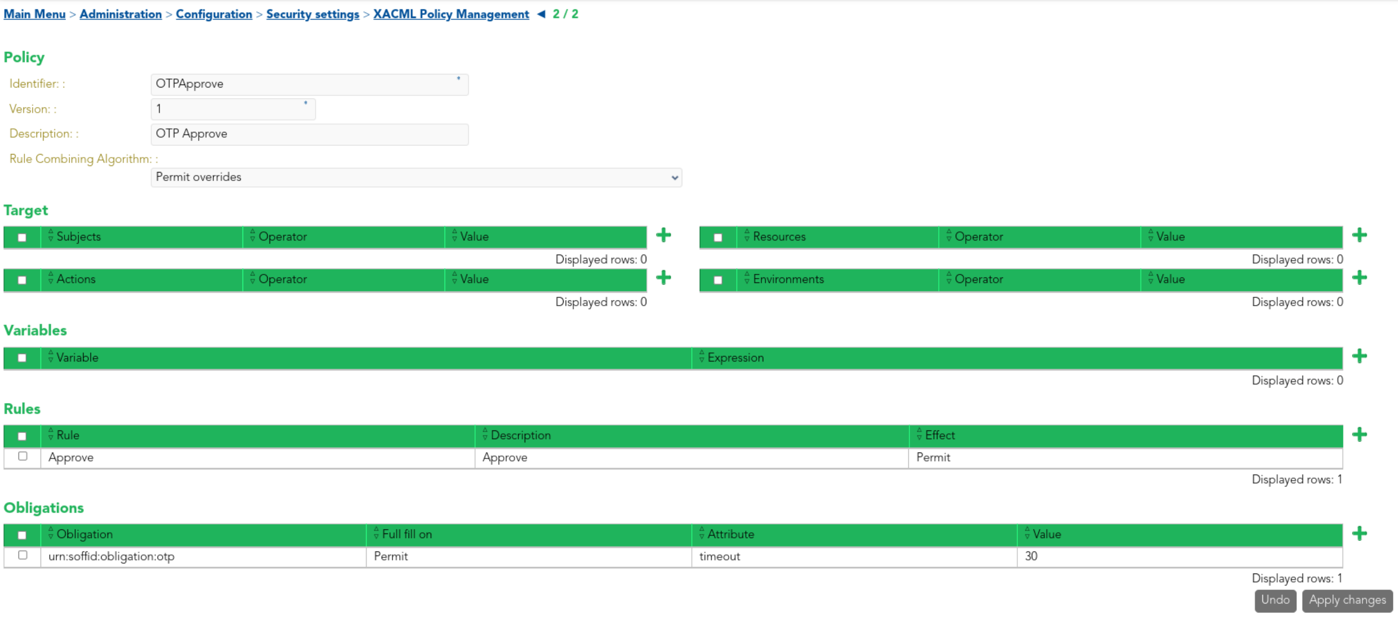
2. Service Providers

Some service providers which grant access to firewalls, routers and other systems, are prefixed with "Tacacs", thus 2FA will be required. For the remaining service providers, which allow access to proxies and other systems, MFA will be enforced, as stated previously. These providers allow users to connect to various systems directly, without initiating the connection through Soffid, while still ensuring identity authentication through the identity provider.

For more information, please refer to Identity & Service Providers.

XACML Policy Management

In `Main Menu > Administration > Configuration > Security Settings > XACML Policy Management` the policy set *PAMMFA* has been created, within which the policy OTPApprove has been defined. It has the obligation to request an OTP with a timeout when launching a connection through PAM.



Main Menu > Administration > Configuration > Security settings > XACML Policy Management ◀ 2 / 2

Policy

Identifier: : OTPApprove

Version: : 1

Description: : OTP Approve

Rule Combining Algorithm: : Permit overrides

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

Variables

□	Variable	Expression

Displayed rows: 0

Rules

□	Rule	Description	Effect
□	Approve	Approve	Permit

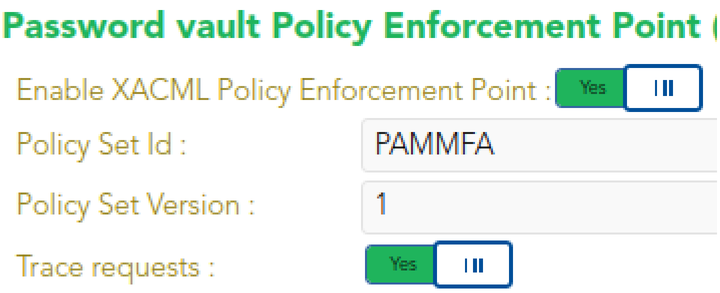
Displayed rows: 1

Obligations

□	Obligation	Full fill on	Attribute	Value
□	urn:soffid:obligation:otp	Permit	timeout	30

Displayed rows: 1

This policy is enabled through the Password vault Policy Enforcement Point in Main Menu > Administration > Configuration > Security Settings > XACML PEP configuration, where the Policy Set Id and the Policy Set Version must be specified.



Password vault Policy Enforcement Point (

Enable XACML Policy Enforcement Point : Yes

Policy Set Id : PAMMFA

Policy Set Version : 1

Trace requests : Yes

For more information, please refer to XACML Policy Management and XACML PEP configuration.

Password Vault

As an example, in `Main Menu > Administration > Resources > Password vault` the *PAM Tests* folder has been created, within which two accounts have been created aswell.

1. PAM TEST RDP

This account allows us to launch a connection to a machine through the PAM Launcher of Soffid. For this purpose, in "Basics", it is mandatory to indicate the login URL, where the network protocol must be specified (RDP in this case), together with the IP of the machine that we want to connect to. We also need to specify the Launch type, indicating it is a PAM Jump Server, and the Jump server group corresponding to the PAM Jump Server. Additionally, owners can be selected to handle privileged access.

Consequently, in "Actions", a password must be set in the "Set now" option, so we can launch the connection and unlock the use of the account. Have in mind that we can change the password policies in Main Menu > Administration > Configuration > Security Settings > Password Policies. However, when launching the connection an OTP will be requested, due to the Password vault policy previously explained.

2. PAM TEST SSH

Another account has been defined for launching a connection through SSH. The concepts explained in the previous account extend to this one.

For more information, please refer to Password vault.

Revision #25
Created 8 October 2024 12:45:29 by araja@soffid.com
Updated 15 October 2024 07:38:58 by araja@soffid.com