Password vault

Description

> Soffid provides a protected storage, to save and manage accounts for multiple applications, that is the Password vault. Here you can save the accounts and passwords to access to critical systems and to your applications as well. Password vault allows you to handle the access control list to these accounts. Sometimes these accounts can be used by a specific user or a set of users.

The accounts are organized in folders depending on the permissión, and the criticality level, ... These accounts can be system accounts or user accounts.

The Password vault exposes a subset of accounts to some users. These accounts are available through the Self-services portal. You can visit My applications page for more information.

When a privileged account is being config, it will be able to assign a workflow or approval process to request in order to use that account. For more information visit the link How to apply policies.

Users can be authorized to manage their own personal accounts, **sso:manageAccounts.** For more info visit the Authorizations page.

Folders

In the password vault, two kinds of folders are used: **personal folders** and **shared folders**, which depend on the Owners configuration you define.

On one hand, each user has their own personal folder. Inside this folder, the user can create accounts. That account will not be shared with any other user.

On the other hand, the shared folders could be used or managed by the owner/manager/SSO users.

Accounts

Soffid allows you to create new accounts on a specific folder on the password vault page, to add a new account will be mandatory to fill in some attributes, like System, name, and login name. You can consult the existing accounts related to a folder. For each account, you can update or delete the account, view and set a password.

Also, you can create accounts on the Account page and assign the appropriate vault folder.

Soffid allows administrator users to configure a workflow to request permissions when a user try to change the password of a privileged account in the password vault. That process can be defined with the BPM Editor as an Account reservation type. For more information you can visit the BPM Editor book.

Overview

https://www.youtube.com/embed/QOyvGTXo9dQ?rel=0

Related objects

1. **Accounts**

Standard attributes

Folder attributes

- **Folder detail**
  - **Name**: folder name which will be displayed in My Applications.
  - **Description**: folder description.
  - **PAM policy**: when using PAM system, you could choose the policy that will comply with for each folder. When you define a policy for a folder, that policy will apply to all accounts hanging from this folder. For more information you can visit the Configure PAM page.
- **Owners**: allows you to handle the full privileged access control list.
  - **Owner users**: list of users who will be the folder owners.

    - **Owner groups**: list of groups, whose users will be the owners of the folder.
    - **Owner roles**: list of roles. Users who have been granted these permissions will be the owners of the folder.
- **Managers**
    - **Manager users**: list of users who can manage the folder. Those users can view the password depending on the password policy.
    - **Manager groups**: list of groups, whose users can manage the folder. Those users can view the password depending on the password policy.
    - **Manager roles**: list of roles. Users who have been granted these permissions can manage the folder. Those users can view the password depending on the password policy.
- **SSO users**
    - **Granted users**: list of users who can use the account of that folder.
    - **Granted groups**: list of groups, whose users can manage the account of that folder
    - **Granted roles**: list of roles. Users who have been granted these permissions can manage the account of that folder.
- **Browse folder**
    - **Users**: list of users who can browse the folder, but can not perform any action.
    - **Groups**: list of groups, whose users can browse the folder, but can not perform any action.
    - **Roles**: list of roles. Users who have been granted these permissions can browse the folder, but can not perform any action.

Accounts attributes

Actions Tab

This tab shows the read-only attributes of the user account:

- **Name**: user account name.
- **Description**: a brief description.
- **System**: target system to which the account will be connected.
- **Login name**: login name to connect to the target system.
- **Login URL**: URL to connect.
- **In use by**: user name who is using that account.

Also, this tab allows you to launch the connection to the target system, view the password, set the password to launch the connection, and unlock the use of that account. All those options depend on the account definition and user privileges.

Basics Tab

This tab displais all the account attributes and allows you to update the account configuration.

Visit theAccount page to view more information about the standard attributes of an account.

Actions

Folders query actions

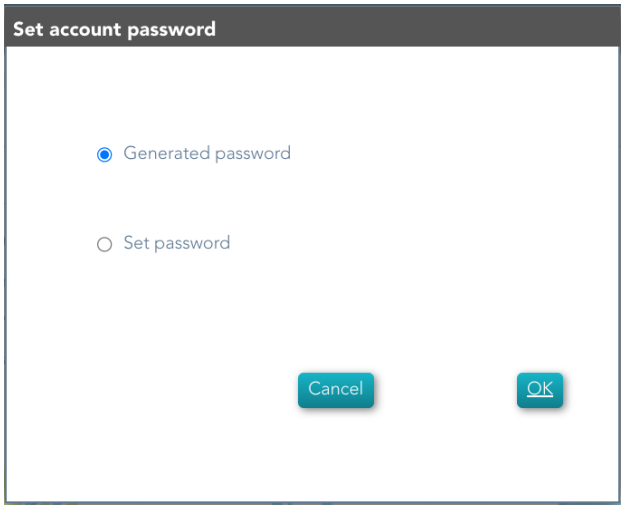
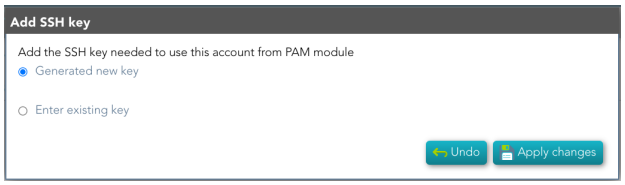
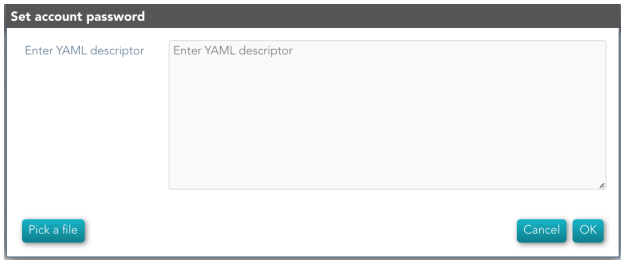
Query	Allows you to query folders through, only Quick search is available.
Add new	Allows you to create a new folder. You can choose that option on the hamburger menu or by clicking the add button (+). To add a new folder it will be mandatory to fill in the required fields. A folder needs to have, at less, an owner to manage it.

Folder actions

Apply changes	Allows you to save a new folder or update an existing folder. To save the data it will be mandatory to fill in the required fields. Be in mind that is important to indicate who are the owners of the folder.
Undo	Allows you to quit without saving any change made.
Delete	Allows you to delete a folder if you have the right permissions. To delete a folder you can click on the hamburger icon and then click the delete button (trash icon). Soffid will ask you for confirmation to perform that action, you could confirm or cancel the operation.

Account actions

Apply changes	Allows you to save a new account. To save the data it will be mandatory to fill in the required fields. Be in mind that is important to indicate who are the owners of the folder. If the account exists on the system, you can assign the vault folder to the account window.
Undo	Allows you to quit without saving any change made.
Delete	Allows you to delete an account from a folder if you have the right permissions. To delete a host you can click on the hamburger icon and then click the delete button (trash icon). Soffid will ask you for confirmation to perform that action, you could confirm or cancel the operation.

Set password	This option depends on the credential type selected. **Password**: • Allows you to set a new password to the account or a SSH key. • The password can be generated automatically, or you can set the password. • It will be mandatory the password complies with the Password policies defined for the domain. • If an account is unmanaged, the password will not be sent to the target system. **Image**  **SSH key**: • Allows you to generate a new key or enter an existing key. **Image**  **Kubernetes key**: • Allows you to add a YAML descriptor **Image** 

How to apply policies

Soffid allows you to define policies and rules to apply to a specific folder or a set of folders. To do that is needed to install the XACML addon and configure the proper policies and rules.

Also, you can config a workflow or approval process to request in order to use accounts saved on a folder.

It is mandatory to enable the Password Vault PEP and populate the information about the XACML policy set and the version which applies.

Example

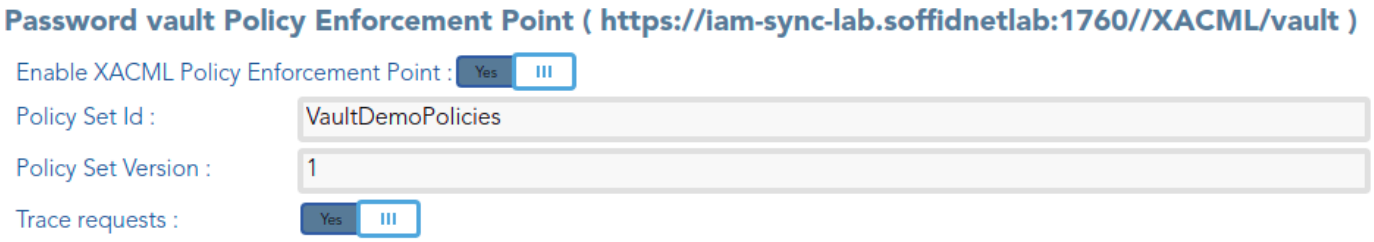
XACML PEP config

It is mandatory to enable the Password Vault PEP and populate the information about the XACML policy set and the version which applies.

Password Vault:



XACML PEP config:



XACML Policy Management

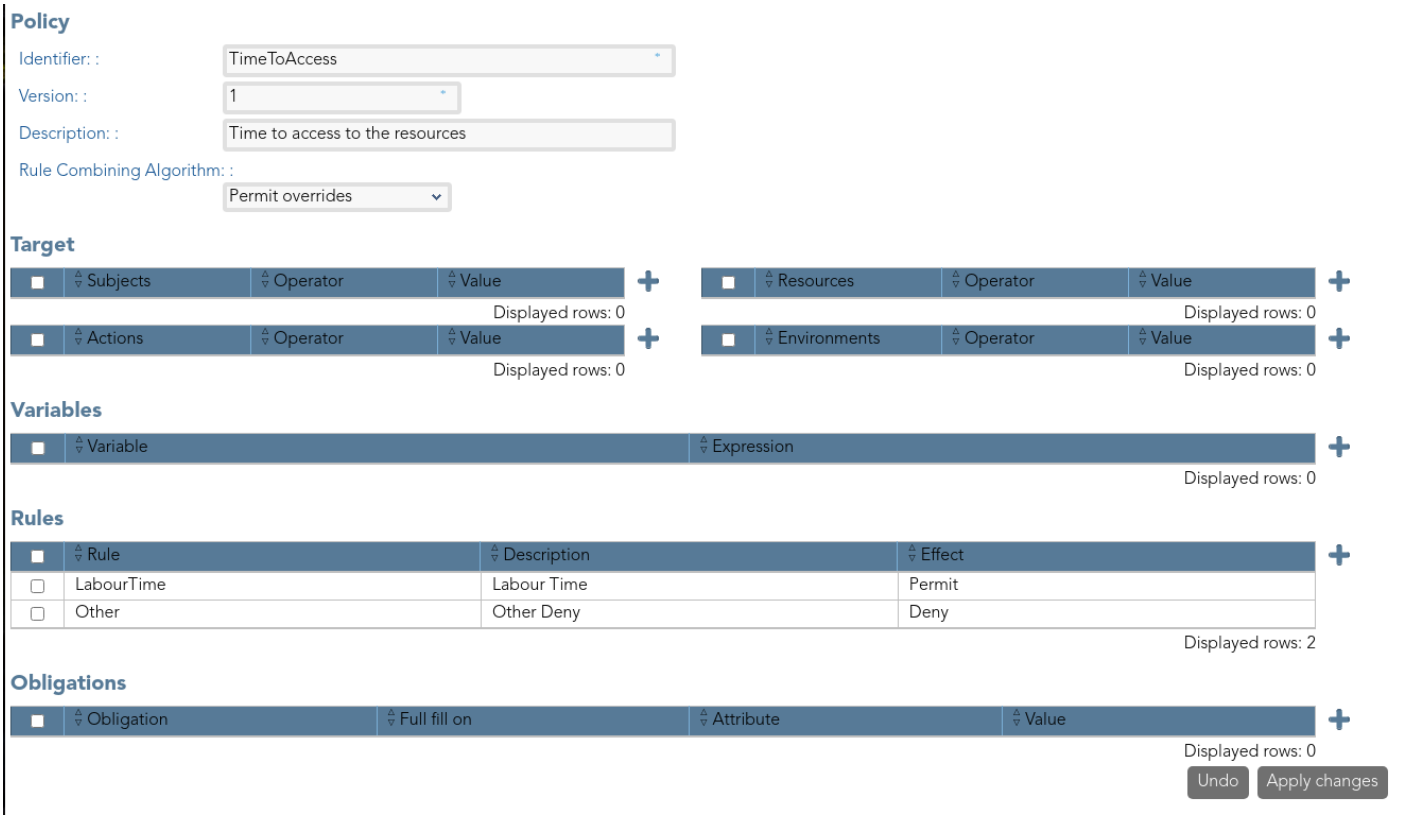
You need to configure the access to the folder "VaultFolder", that folder can contain other folders and accounts. It will be mandatory to config the access list, who are the owners, managers, and so on. You need to know if you need to config the control access list by accounts, by folders, or both.

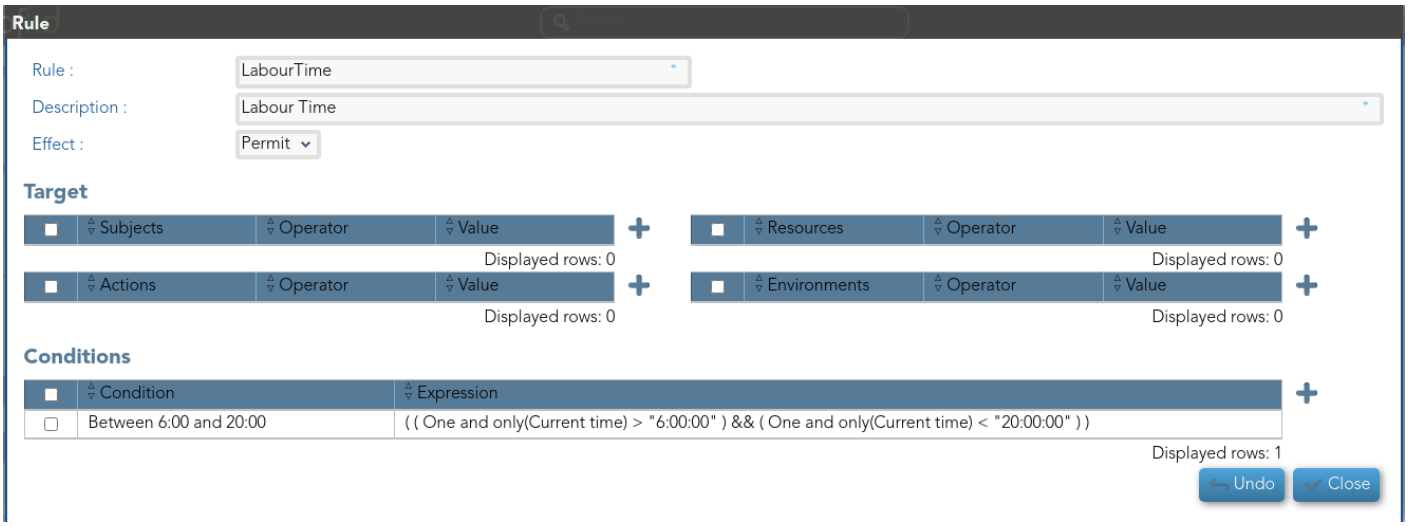
demoFolder	demoFolder
soffid	administrator
patricia	patricia
subFolderDemo	subFolderDemo

Create new folder | Create new account

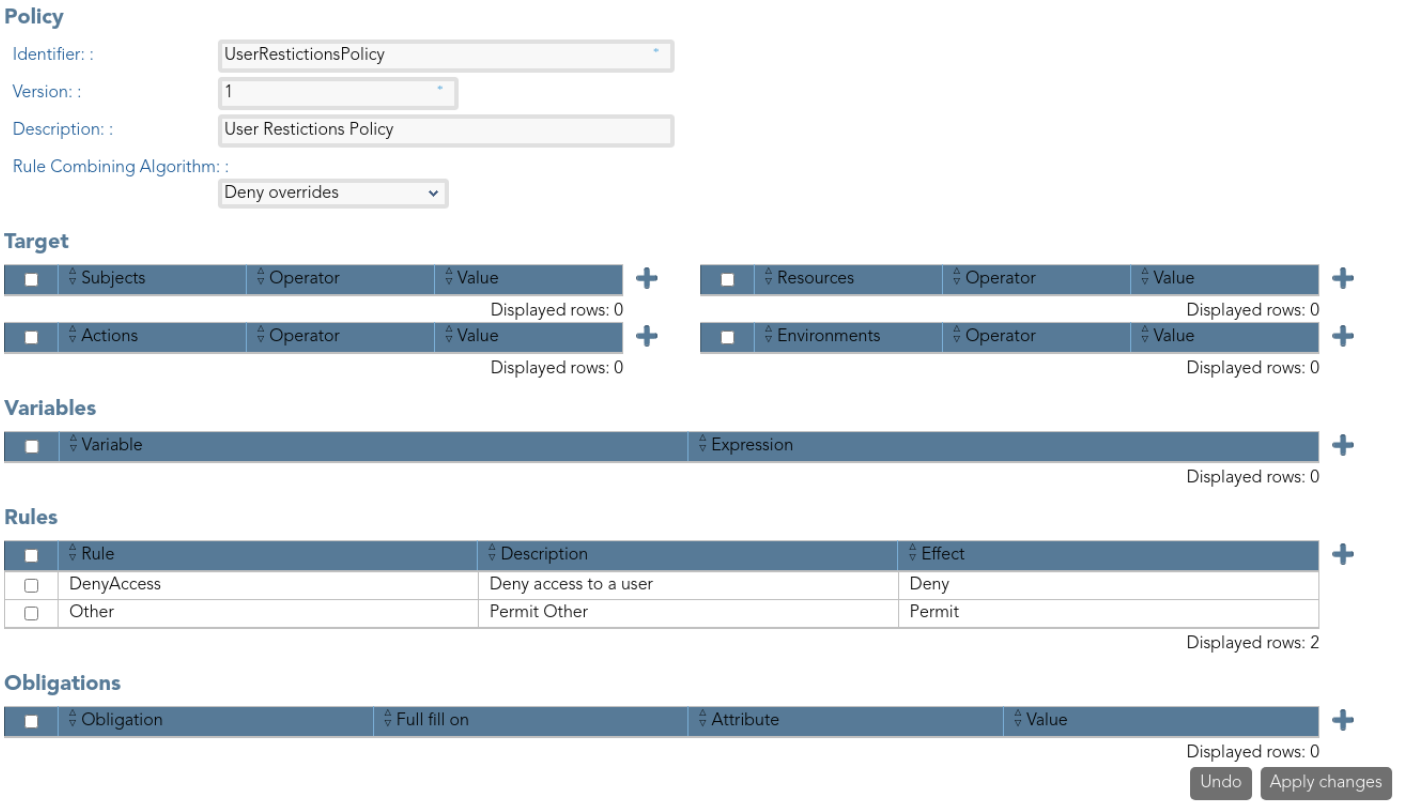
For instance, the policies you need to implement are the following:

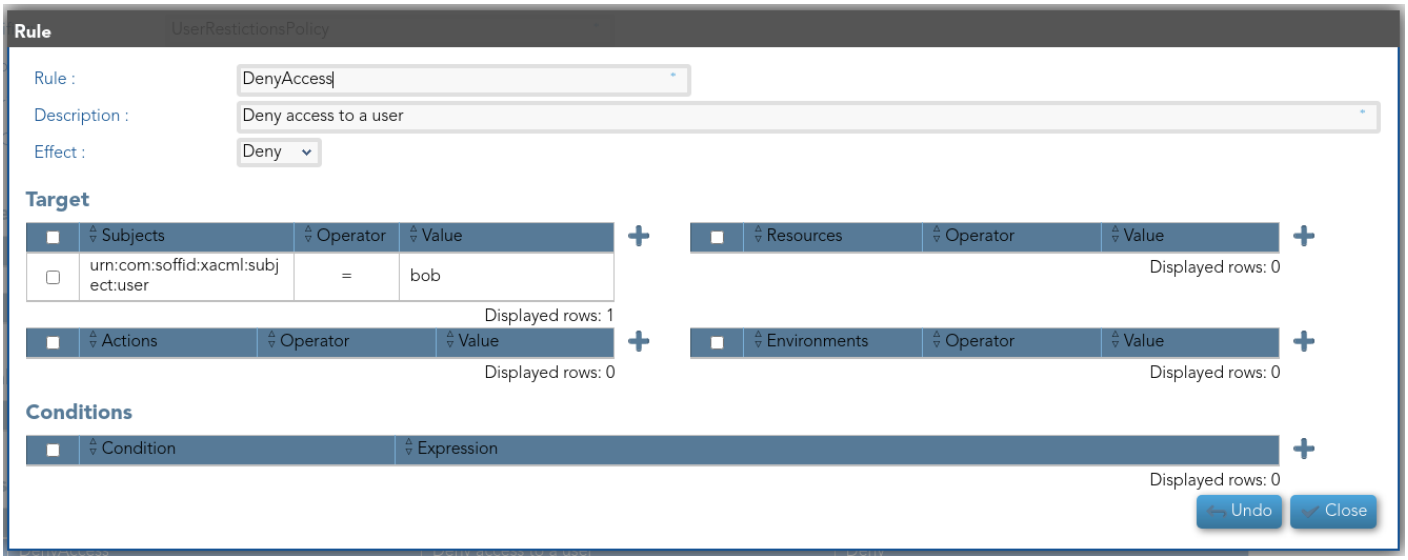
1. Only users between 6:00 and 18:00 could use the accounts inside the "demoFolder".





2.- User "bob" never could use the accounts of demoFolder.





3. Users with result permits, need the authorization to use the accounts.

You need to config the workflow that will be called, to config you need to include the bpm obligation on the policy. Also, you can include a message to the user, or other obligations.

Policy

Identifier: : PAM

Version: : 1

Description: : PAM service

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
Other	Other	Deny
Labourtime	Labour time	Permit

Displayed rows: 2

Obligations

Obligation	Full fill on	Attribute	Value
urn:soffid:obligation:message	Permit	text	This is a protected system. Do not enter without authorization, please.
urn:soffid:obligation:bpm	Permit	process	Grant account

> Visit the XACML Book for more information.

> Visit the BPM Editor Book for more information.

Revision #34
Created 8 April 2021 10:57:40
Updated 21 June 2024 08:29:21