PAM

Privileged Access Management

- Discover your assets
- Publish accounts in the password vault
- Create monitoring and recording policies
- Create MFA policies

Discover your assets

Description

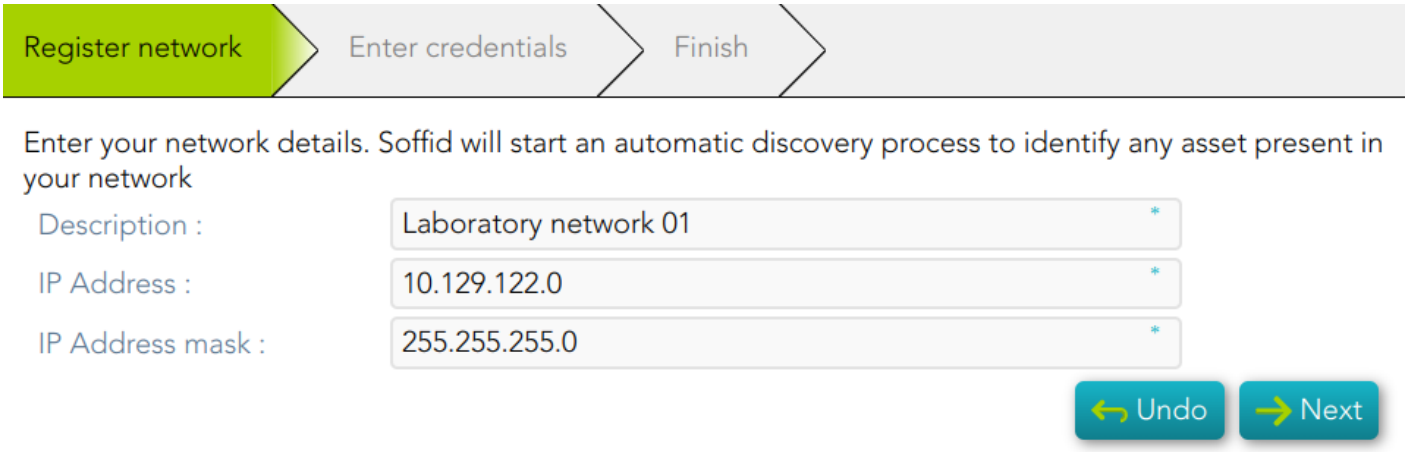
Soffid allows you to configure the network discovery tool in a way to run the process to identify any asset present in your network.

> For more information, you can visit the Network discovery page.

Step-by-step

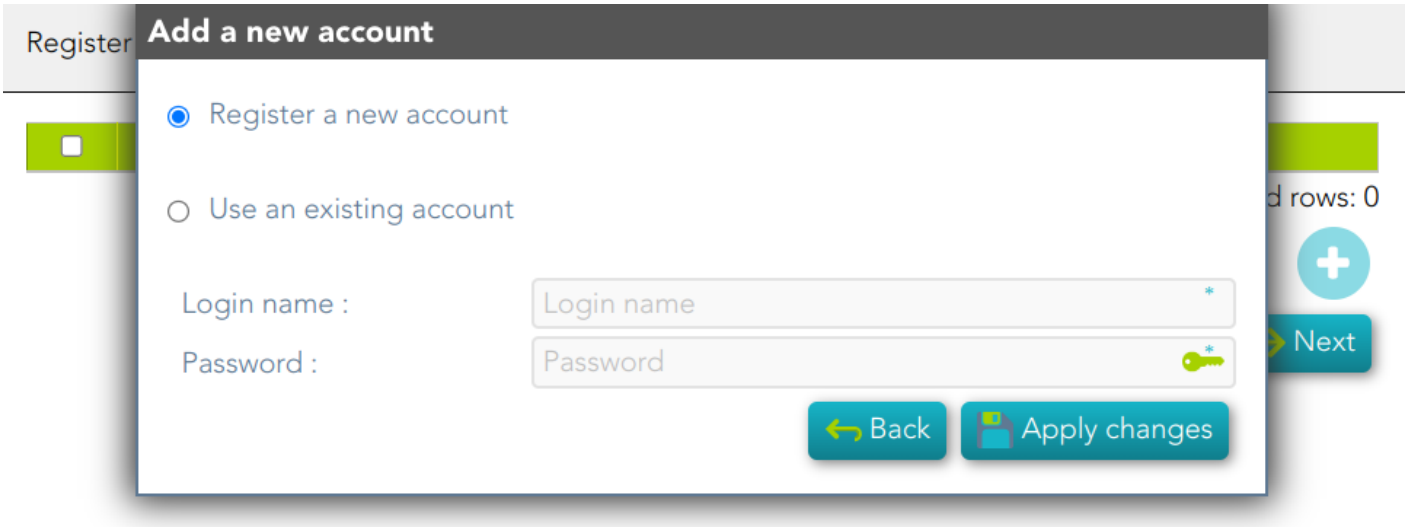
1. Once you select the Discover you assets option, Soffid will display the form to fill in.

2. You need to register your network data and click the Next button.

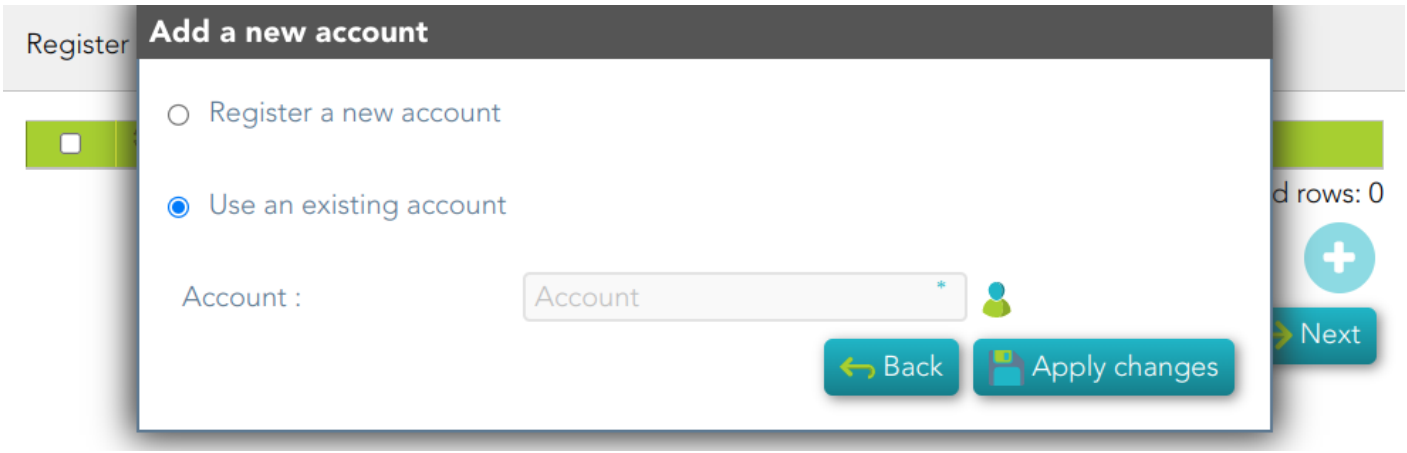


3. You need to register an account. You can choose to register a new one or to use an existing account.

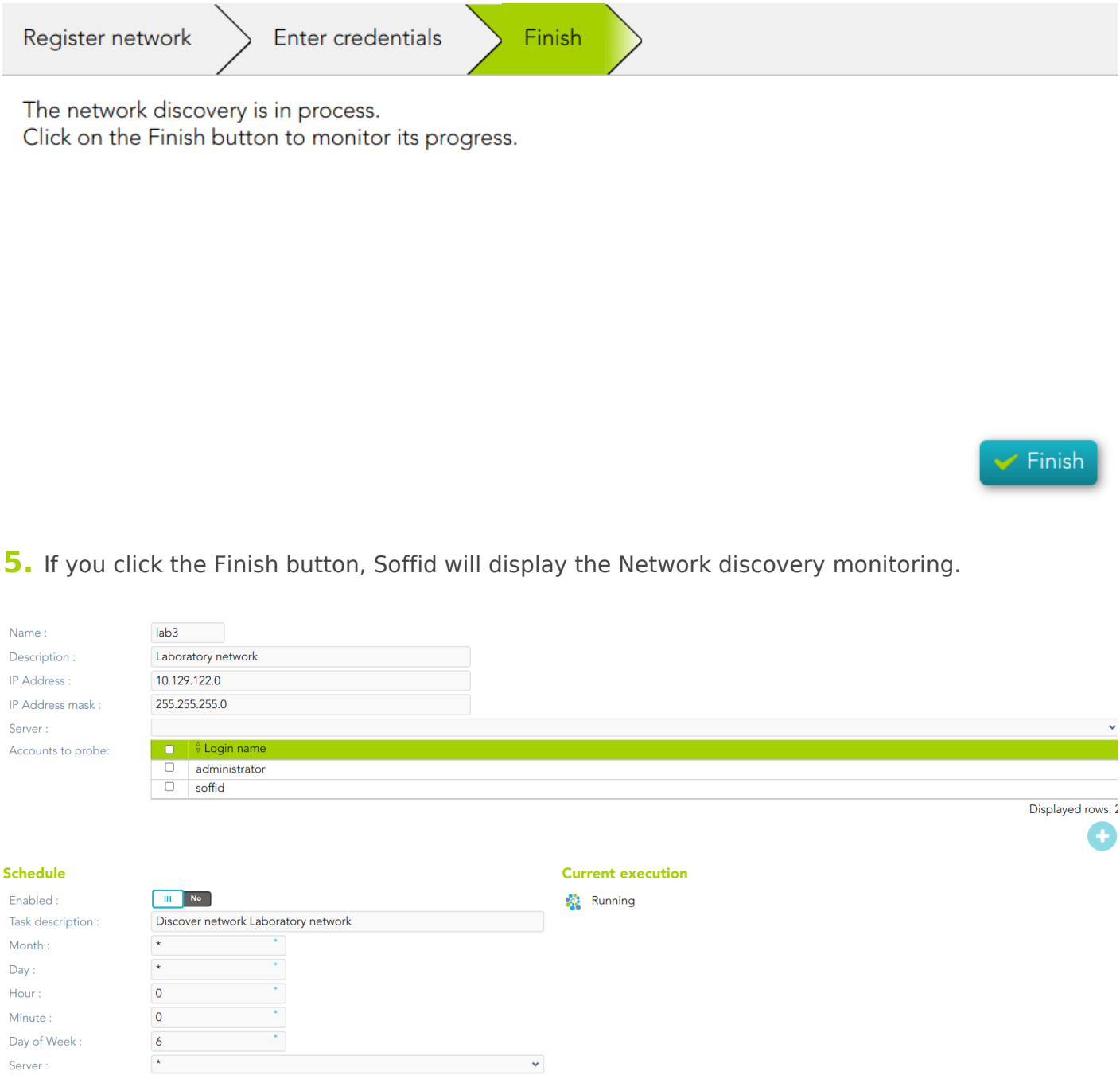
3.1. If you select the *Register a new account* option, you must fill in the Login name and the password and click the Apply changes button



3.2. If you select *Use an existing account*, you must select an existing account in the system and click the Apply changes button.



4. Soffid display this message to indicate the network discovery is in process



5. If you click the Finish button, Soffid will display the Network discovery monitoring.

Publish accounts in the password vault

Description

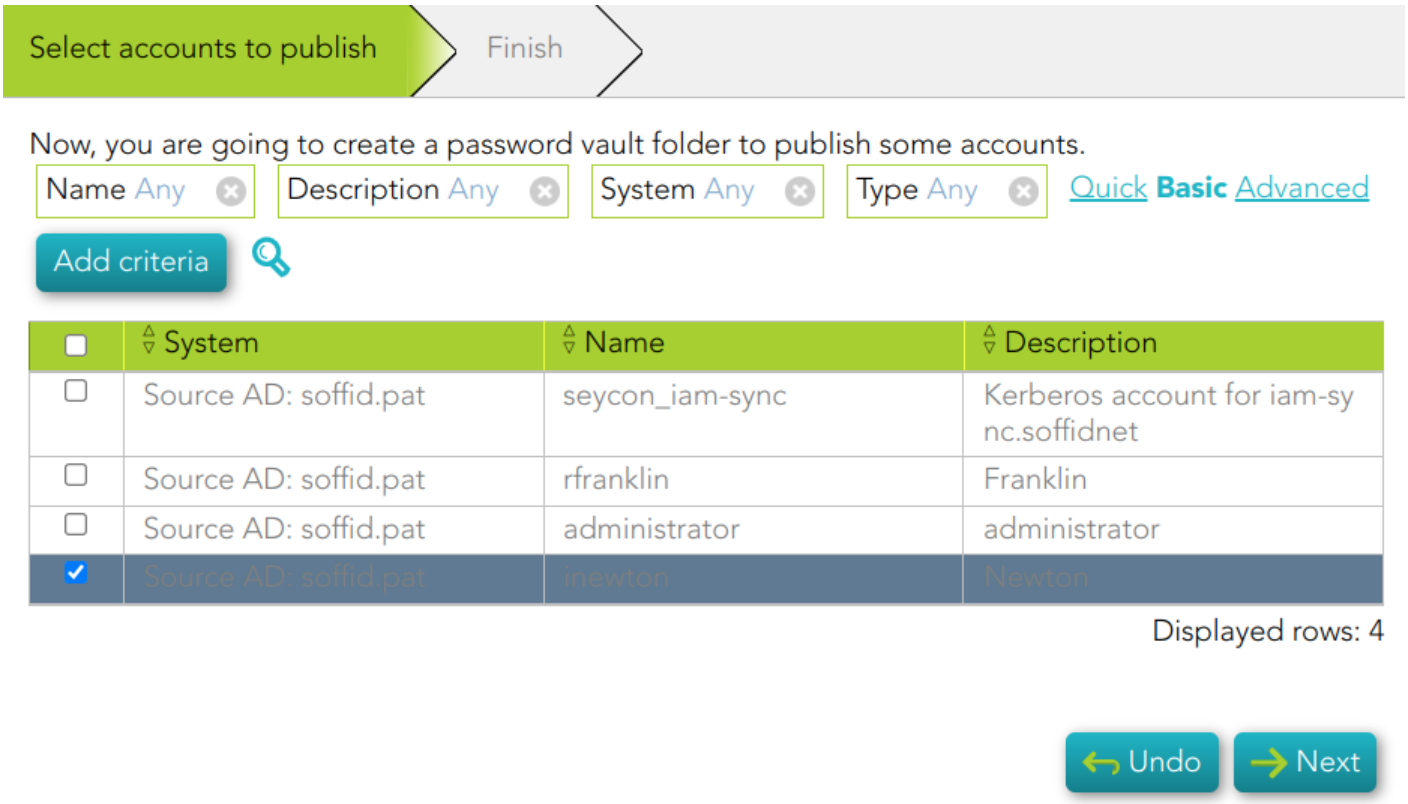
This wizard allows you to publish some accounts in the password vault in order to save and manage these accounts and their password.

> For more information, you can visit the Password vault page.

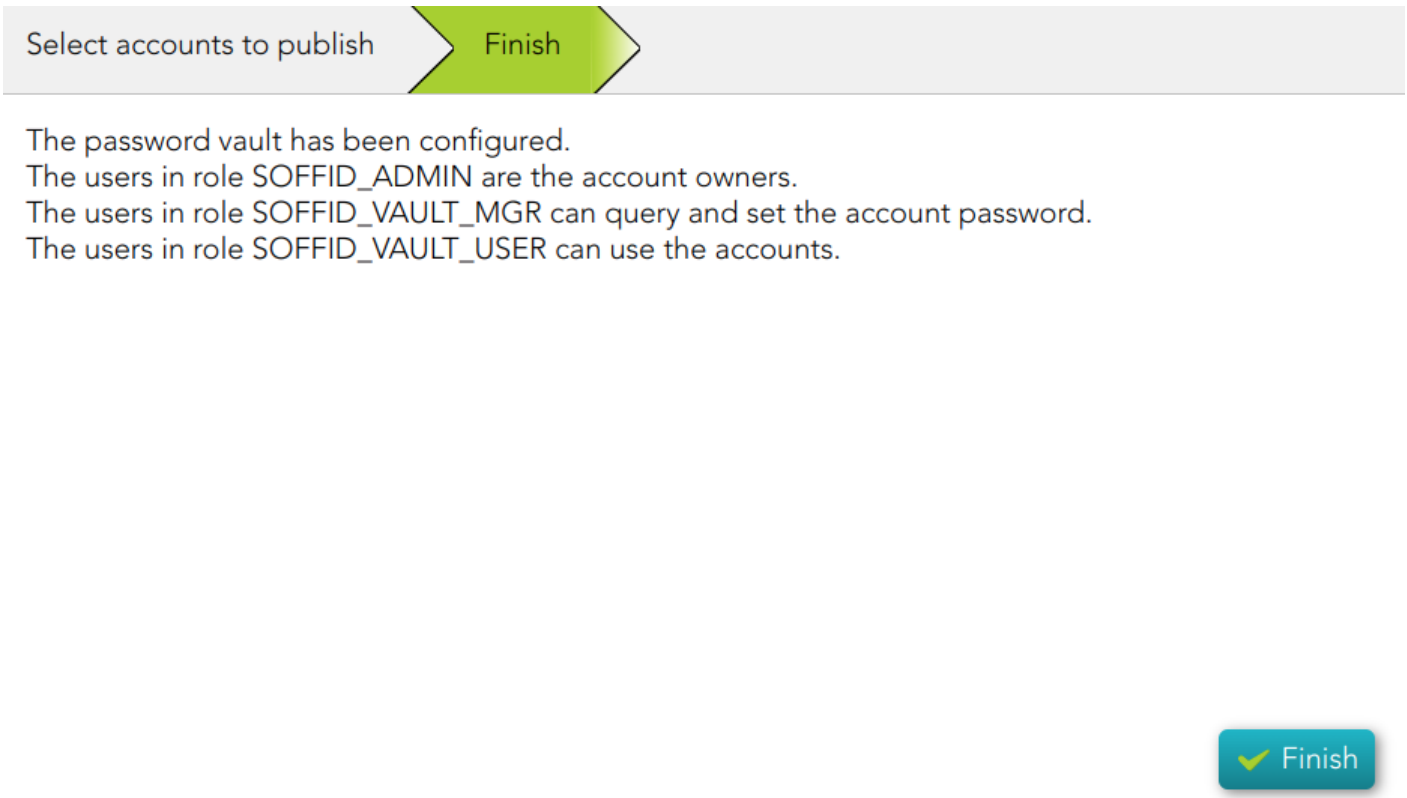
Step-by-step

1. Once you select the *Public accounts in the password vault* option, Soffid will display the following wizard

2. You must select the accounts you want to publish and click the Next button.



3. Then, Soffid will configure the password vault.



4. When you click the Finish button, Soffid will browse to the Password vault page. On this page, you could check and update the permissions.

Main Menu > Administration > Resources > Password vault

Name	Description
Personal accounts	Accounts that won't be shared
Shared accounts	Shared accounts

Total rows: 2

Main Menu > Administration > Resources > Password vault ◄ 3 / 4 ►

Actions Basics

Common attributes

System : soffid - Soffid system
Name : inewton
Description : Newton
Type : Unmanaged
Status : Enabled
Password policy : SSO account

Owners

Owner groups :
Owner users :
Owner roles : SOFFID_ADMIN@soffid SOFFID Administrator

Managers

Manager groups :
Manager users :
Manager roles : SOFFID_VAULT_MGR@soffid Password vault manager

SSO Users

Granted groups :
Granted users :
Granted roles : SOFFID_VAULT_USER@soffid Password vault user

Password vault

Vault folder : Shared accounts
Inherit new permissions : Yes

Launch properties

Login url :
Login name : inewton
Launch type :

Create monitoring and recording policies

Description

PAM policy is a subset of cybersecurity policies that deal with privileged access. This determines which users can have privileged access to specific systems, when, and for how long.

You can check the policies in the following menu option: `Main Menu > Administration > Configuration > Security settings > PAM policies`

> For more information, you can visit the PAM policies page.

Step-by-step

1. Once you click the *Create monitoring and recording policies* option, Soffid will create a default policy.



2. When you click the Ok button, Soffid will browse to the created policy and allows you to update the default configuration.

Name : default *

Description : Default Policy

Modified by : pgarcia Patricia García

Modified on : 3/6/2023 12:04

Rule	Close se…	Lock acc…	Open is…	Notify
cd .. (tenant)	☐	☐	☐	☑
Drop table	☐	☐	☐	☑
ipconfig	☐	☐	☐	☑
Massive delete	☐	☐	☐	☑
passwd	☐	☐	☐	☑
pwd (tenant)	☐	☐	☐	☑
rm *-r (tenant)	☐	☐	☐	☑
sudo	☑	☐	☐	☑
sudo (tenant)	☐	☐	☐	☑
write (tenant)	☐	☐	☐	☑

Displayed rows: 10

Undo Apply changes

Create MFA policies

Description

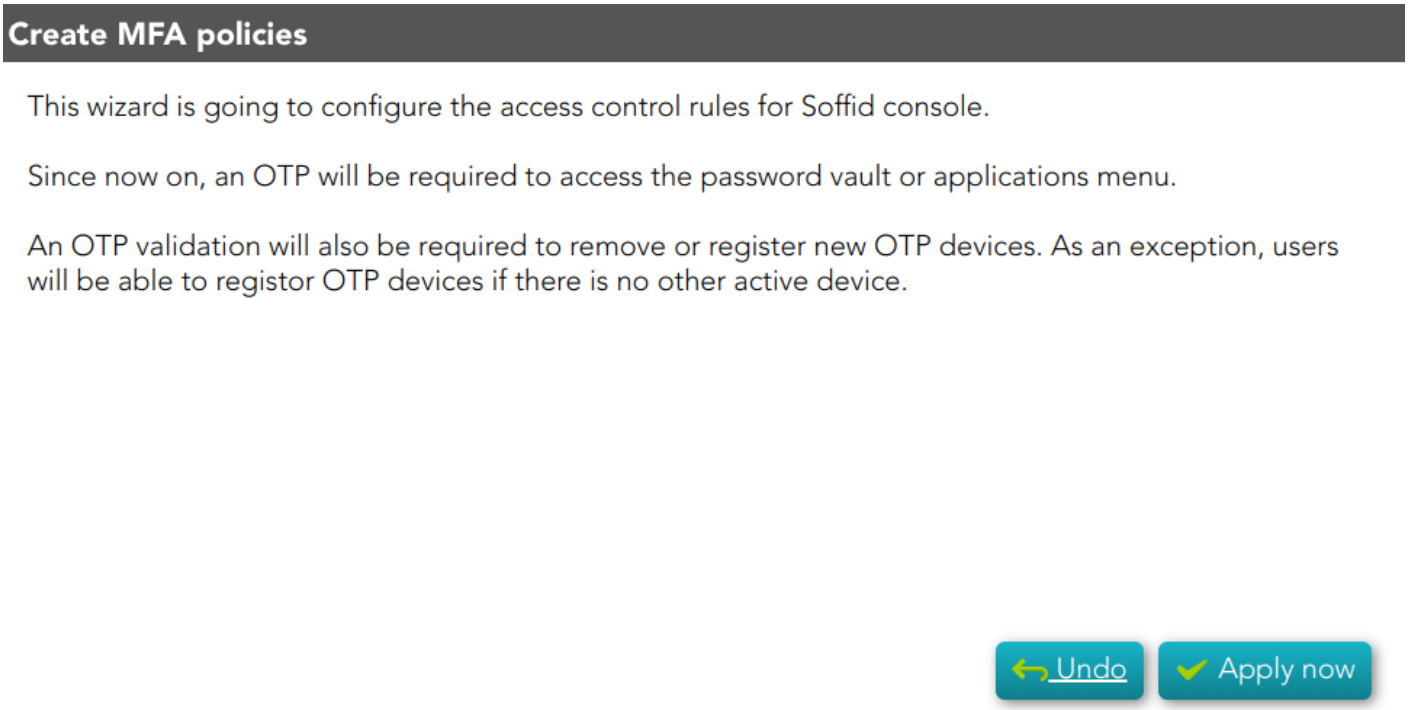
This wizard allows you to configure the access control rules for Soffid Console. By default, an OTP will be required to access to the Password vault or application menu.

You can check the configuration in the following menu option: `Main Menu > Administration > Configuration > Security settings > Authentication`

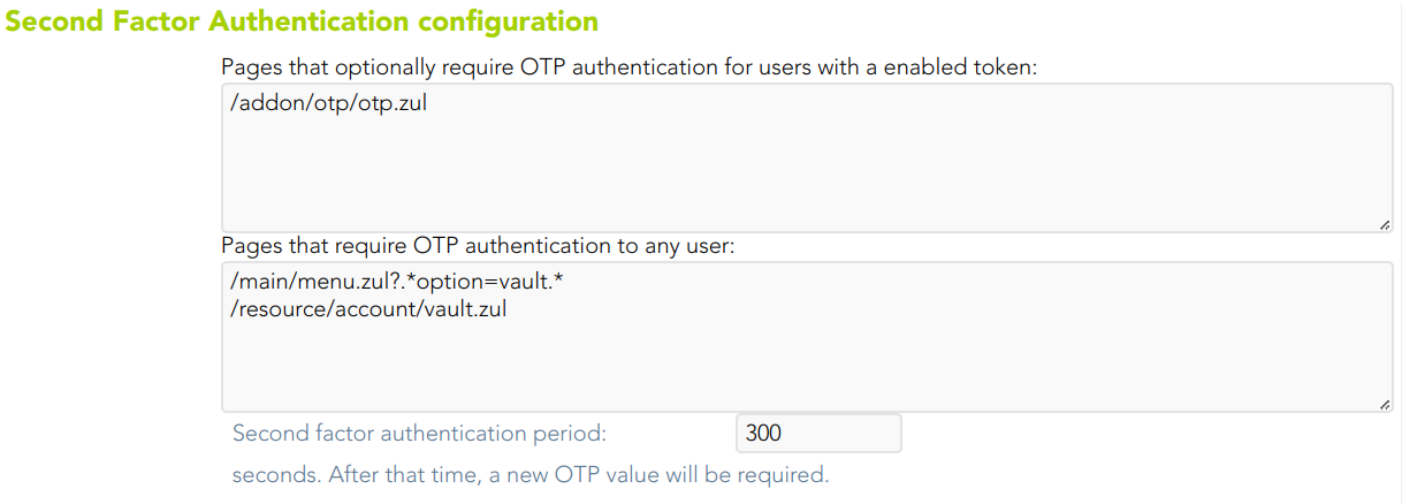
> For more information, you can visit the Two-factor authentication (2FA) book and the Second Factor Authentication configuration

Step-by-step

1. Once you select the *Create monitoring and reporting policies* option, Soffid will launch the following wizard



2. If you click the Apply now button, Soffid will browse to the Authentication page, allowing you to configure the Second Factor Authentication.



3. To confirm the changes, you must click the Confirm changes button.