

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.

Register network > Enter credentials > Finish >

Enter your network details. Soffid will start an automatic discovery process to identify any asset present in your network

Description :	Laboratory network 01
IP Address :	10.129.122.0
IP Address mask :	255.255.255.0

Undo Next

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

Register **Add a new account**

☒ Register a new account

☐ Use an existing account

Login name :

Password :

[← Back](#) [Apply changes](#)

Rows: 0

[+](#)

[Next](#)

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

Register **Add a new account**

☐ Register a new account

☒ Use an existing account

Account :

[← Back](#) [Apply changes](#)

Rows: 0

[+](#)

[Next](#)

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

The network discovery is in process.
Click on the Finish button to monitor its progress.

✓ Finish

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

Name :

lab3

Description :

Laboratory network

IP Address :

10.129.122.0

IP Address mask :

255.255.255.0

Server :

Accounts to probe:

☐

⚙ Login name

☐

administrator

☐

soffid

Displayed rows: 2

Schedule

Enabled :

III

No

Task description :

Discover network Laboratory network

Month :

*

⌵

Day :

*

⌵

Hour :

0

⌵

Minute :

0

⌵

Day of Week :

6

⌵

Server :

*

⌵

Current execution

⚙

Running

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.

Now, you are going to create a password vault folder to publish some accounts.

Name Any

Description Any

System Any

Type Any

Quick Basic Advanced

Add criteria

<input type="checkbox"/>	System	Name	Description
<input type="checkbox"/>	Source AD: soffid.pat	seycon_iam-sync	Kerberos account for iam-sy nc soffidnet
<input type="checkbox"/>	Source AD: soffid.pat	rfranklin	Franklin
<input type="checkbox"/>	Source AD: soffid.pat	administrator	administrator
<input checked="" type="checkbox"/>	Source AD: soffid.pat	inewton	Newton

Displayed rows: 4

3. Then, Soffid will configure the password vault.

The password vault has been configured.
The users in role SOFFID_ADMIN are the account owners.
The users in role SOFFID_VAULT_MGR can query and set the account password.
The users in role SOFFID_VAULT_USER can use the accounts.

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.

🔍

⬆️ Name	▼ Description
⊕ 📁 Personal accounts	Accounts that won't be shared
⊕ 📁 Shared accounts	Shared accounts

Total rows: 2



Actions

Basics

Common attributes

System :soffid - Soffid system

Name :

inewton

Description :

Newton

Type :

Unmanaged

Status :

Enabled

Password policy :

SSO account

Managers

Manager groups :

Manager groups

Manager users :

Manager users

Manager roles :

SOFFID_VAULT_MGR@soffid

Password vault manager

Manager roles :

Password vault

Vault folder :

Shared accounts

Inherit new permissions :

Yes

III

Owners

Owner groups :

Owner groups

Owner users :

Owner users

Owner roles :

SOFFID_ADMIN@soffid

SOFFID Administrator

Owner roles :

SSO Users

Granted groups :

Granted groups

Granted users :

Granted users

Granted roles :

SOFFID_VAULT_USER@soffid

Password vault user

Granted roles :

Launch properties

Login url :

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)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Drop table	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
ipconfig	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Massive delete	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
passwd	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
pwd (tenant)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
rm *-r (tenant)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
sudo	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
sudo (tenant)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
write (tenant)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

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

Create MFA policies

This wizard is going to configure the access control rules for Soffid console.

Since now on, an OTP will be required to access the password vault or applications menu.

An OTP validation will also be required to remove or register new OTP devices. As an exception, users will be able to register OTP devices if there is no other active device.

 [Undo](#)

 [Apply now](#)

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

Second Factor Authentication configuration

Pages that optionally require OTP authentication for users with a enabled token:

/addon/otp/otp.zul

Pages that require OTP authentication to any user:

/main/menu.zul?*option=vault.*
/resource/account/vault.zul

Second factor authentication period:

300

seconds. After that time, a new OTP value will be required.

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