

Configuration wizard

Configuration wizard

- Getting started
- IGA
 - Connect Soffid IdaaS to your on-premise network
 - Create identities (manually, CSV file or authoritative source)
 - Add applications
 - Design user life cycle workflows
- IRC
 - Create SoD matrix
 - Schedule weekly risk report
 - Design a recertification campaign
 - Create advanced authorization rules
- PAM
 - Discover your assets
 - Publish accounts in the password vault
 - Create monitoring and recording policies
 - Create MFA policies
- AM
 - Create identities (manually, CSV file, or authoritative source)
 - Add applications
 - Create MFA policies
 - Create adaptive authentication rules

Getting started

Introduction

Soffid provides you a 360° perspective of the identities of your organization employees, providers and customers:

- Identity governance to manage the identities life-cycle
- Access management identifies your users accessing applications, including multi-factor authentication
- Privileged access management tracks usage and access of service and system management accounts
- Identity risk and compliance

Screen overview

<https://www.youtube.com/embed/jTmFj1Ab8Pc?rel=0>

IGA

Identity Governance Administration

Connect Soffid IdaaS to your on-premise network

Description

In order to manage your information system, a component named Sync Server must be installed along with Soffid Console. You must choose one platform as your Sync Server Soffid host and follow the instructions.

Once you have run the corresponding scripts, Soffid will detect the new Sync server. You could check the new Sync server on the [Synchronization servers page](#).

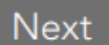
Step-by-step

1. First, you must select the platform and click the Next button

In order to manage your information system, a component named sync server must be installed along with Soffid Console.

Please, select the platform you want to use to host your Soffid Sync Server:

- ☐ Debian, Ubuntu or any other Debian derivatives
- ☐ Redhat, Centos or Suse
- ☐ Windows
- ☐ Docker

 Undo Next

2. You must follow the instructions depending on the previous selection.

2.1. Debian, Ubuntu, or any other Debian derivatives

Description

Description

Finish

The installation script has been downloaded. Please, execute it issuing the following command from a bash shell:

```
wget -O /tmp/syncserver.deb
```

```
'https://download.soffid.com/maven/com/soffid/iam/sync/syncserver/3.4.0-SNAPSHOT/syncserver-3.4.0-SNAPSHOT.deb'
```

```
sudo DEBIAN_FRONTEND=noninteractive apt install /tmp/syncserver.deb
```

```
sudo /opt/soffid/iam-sync/bin/configure -configurl
```

```
'https://gbr.demo.soffid.net/soffid/anonymous/syncserver/script/50XB2u-oYuYpglsNnPYJZaUn5auS0c70iJywQ7nXUW6no_wg2yrfbKQl97G5EJrxeF3rYNCpu0UXTaz'
```

← Undo

2.2. Redhat, Centos, or Suse

Description

Description

Finish

The installation script has been downloaded. Please, execute it issuing the following command from a bash shell:

```
wget -O /tmp/syncserver.rpm  
'https://download.soffid.com/maven/com/soffid/iam/sync/syncserver/3.4.0-  
SNAPSHOT/syncserver-3.4.0-SNAPSHOT.rpm'
```

```
sudo yum install java-11-openjdk
```

```
sudo rpm -i /tmp/syncserver.rpm
```

```
sudo /opt/soffid/iam-sync/bin/configure -configurl  
'https://gbr.demo.soffid.net/soffid/anonymous/syncserver/script/l-ZB-  
QsbCMR3jCj0dbGskZbXDFMjXxXeFR7VQwf6LLV0Dg7yrsN6uF0EpL20LMv-  
U3rBshtr9AnyMCLUK0Ei'
```

← Undo



2.3. Windows

Description

Description

Finish

The installation script has been downloaded. Please, execute it issuing the following command from powershell:

```
Invoke-WebRequest -Uri syncserver.msi -OutFile  
'https://download.soffid.com/maven/com/soffid/iam/sync/syncserver/3.4.0-  
SNAPSHOT/syncserver-3.4.0-SNAPSHOT.msi'
```

```
msiexec /i syncserver.msi
```

```
c:\program files\soffid\iam-sync\bin\configure -configurl  
'https://gbr.demo.soffid.net/soffid/anonymous/syncserver/script/i24pmTcue  
rC0SJWlVrHkdGExrdn9QYdVmuli899cw1QEr0PNcjLaL'
```

← Undo



2.4. Docker

Description

Description

Finish

The installation script has been downloaded. Please, execute it issuing the following command from a bash shell:

```
docker run -d --name syncserver -e  
SOFFID_CONFIG='https://gbr.demo soffid.net/soffid/anonymous/syncserver/s  
yY8At010wJ90c9JQ0-  
SXn3utxJIPvF2_igitRMuCOymdSY2FA01qppZh_8zYikVS230y1BsXaeVU' --restart  
always soffid/iam-sync:3.4.0-SNAPSHOT
```

← Undo



3. Finally, Soffid will detect that the Sync Server has been successfully installed and you can click the Finish button.

Description

Description

Finish

Congratulations. Your sync server is now properly configured.

Now, you can deploy agents on it.

↩ Undo

→ Finish

Create identities (manually, CSV file or authoritative source)

Description

You need to register the identities to manage and protect them. This wizard allows you to choose the easiest way to do it.

Step-by-step

1. First, you must select one option to register the identities. Soffid allows you three options.

Load identities

You need to register the identities to manage and protect. Here you have some ways to do it:

- ☐ Load from a CSV file
- ☐ Configure an authoritative data source to always have up-to-date information
- ☐ Register them manually

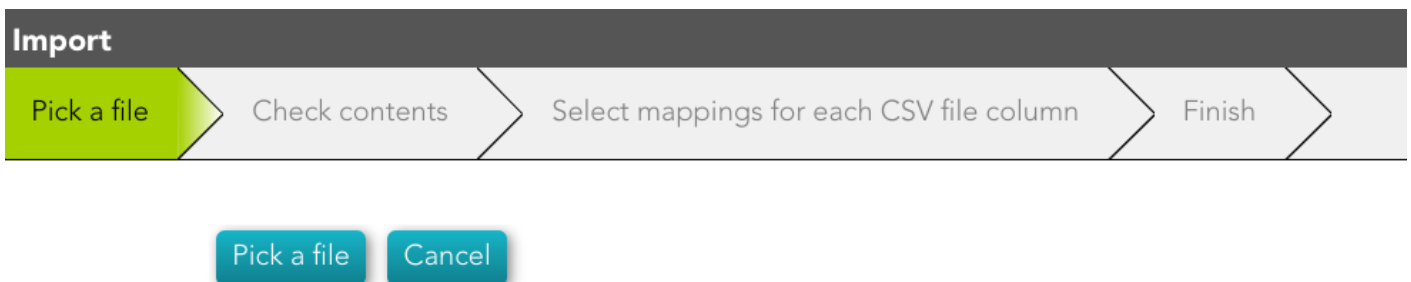
← Undo

Next

2. You must follow the steps, depending on the selected option:

2.1. Load from a CSV file: this option allows you to load identities from a CSV file.

2.1.1. First of all, you need to pick up the CSV file.



2.1.2. Second, Soffid will display the file data to check contents

Import

Pick a file

Check contents

Select mappings for each CSV file column

Finish

Character set :

UTF-8

Separator :

,

Quote character :

"

Escape character :

\

Contains header row :

Yes



Reload

Picture	User...	Full ...	Prim...	Ena...	Birth...	First ...	Last ...	Mid...	Type
	rfranklin	Rosalind Franklin	scientist	Si		Rosalind	Franklin		I
	aeinstein	Albert Einstein	scientist	Si		Albert	Einstein		I

← Back

→ Next

2.1.3. Then you must select the proper mapping for each CSV file column. And finally, click the Import Button and Soffid will add the identities to the platform.

Import

Pick a file

Check contents

Select mappings for each CSV file column

Finish


Select mappings for each CSV file column

CSV column	Target object attribute
Picture	Don't load
User name	User name
Full name	Full name
Primary group	Primary group
Enabled	Enabled
Birth Date	Don't load
First name	First name
Last Name	Last Name
Middle name	Middle name
Type	Type

Back

Import

2.1.4. Soffid will display the result of the process.

 soffid

Search

?

⚙

[Main Menu](#) > [Administration](#) > [Resources](#) > Users

User name Any

First name Any

Last Name Any

Primary group Any

Add criteria

[Quick](#) [Basic](#) [Advanced](#)

☐


▼ User name


⬆ Full name

⬆ Primary group

⬆ Enabled

Displayed rows: 0



 Added 0 new rows, 2 rows updated, 0 rows removed and 0 rows without any change

OK

2.2. Configure an authoritative data source to always have up-to-date information: this option allows you to configure an Active Directory agent, or a Relational database agent to load the identities.

Once the process will finish, you could check the new agent on the agent's page [Main Menu > Administration > Configuration > Integration engine > Agents](#)

For more information about the agents, you can visit [the Agents page](#).

Load identities

Please, select a the type of data source to fetch identities from

- ☐ Active Directory
- ☐ Relational database (SQL)

 Undo

Next

2.2.1. Active Directory

- To configure the AD connection you must fill in the required fields and click the Next button.
- Then Soffid will run the Authoritative load and the Reconcile process
- Finally, you could check the result on the [Scheduled tasks](#) page.

Configure connection

Load users information

Load users permissions

Active directory name :

dc=soffid,dc=pat

*

User name :

SOFFID\Administrator

*

Password :

●●●●●●●●●●



← Undo

→ Next

2.2.2. Relational database (SQL)

Configure SQL connection

Load users information

Load users permissions

Database type :

Mysql or Mariadb

Database url :

jdbc:mariadb://172.20.0.6/BABELTEST

User name :

babeluser

Password :

••••••••


SQL Sentence :


select * from USERS

← Undo

→ Next

2.3. Register them manually: this option browses to the **User page** to register the identities manually





[Main Menu](#) > [Administration](#) > [Resources](#) > [Users](#)

[Basics](#) [Groups](#) [Accounts](#) [Roles](#) [Effective Roles](#) [Shared accounts](#) [Sessions](#) [User processes](#) [OTP devices](#) [Tokens](#) [Backups](#)

Common attributes

User name :

First name :

Last Name :

Middle name :

Full name :

Mail service

eMail :

Mail alias :

Mail server :

Audit information

Controlled by :

Organization

Type :

Primary group :

Home server :

Profile server :

User status

Enabled : ☐ No

Multi session : ☐ No

Comments :

Add applications

Description

The wizard allows you to add Applications or **Information Systems** to Soffid as well. The wizard allows you to choose from an application list. Once you choose one of them, you must fill in the required fields to connect to this application. Then the Reconcile process will be launched.

Step-by-step

1. First, you need to select the proper application to add. Soffid provides you a huge application list to configure.

Load identities

Add new application



Active
Directory



SAP R/3



Network
discovery



Service now



AWS



Google
workplace



Microsoft 365



Atlassian



MariaDB



Oracle DB



2. Once you select the application, you must configure the connection parameters.

Configure connection

Load accounts

Set account owners

Finish

Host :

172.20.0.6

*

Port :

3306


User name :

root

*

Password :

••••••••



↩ Undo

➡ Next

3. Then, Soffid allows you to choose the strategy to load accounts.

Configure connection

Load accounts

Set account owners

Finish

Soffid manages two different concepts: users and accounts.
After loading the existing accounts into Soffid database, you need to bind each account to the owner user.
Some accounts can temporary be left without a single owner, as they are service or shared accounts.
By the time being, we should find the right owner for each account.
Select the right strategy:

☐ Automatically, based on a user attribute

User name

▼

☐ Automatically, based on a script for each account


☐ Manually, with automatic suggestions

☐ Do not bind accounts to users

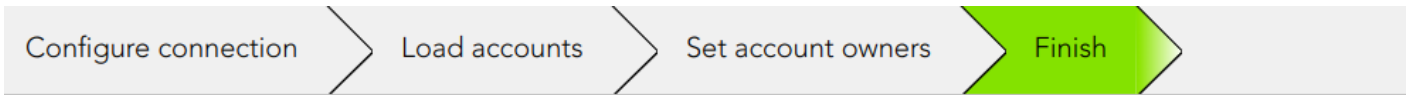
➡ Next

4. Then Soffid will run the reconcile process



Reconcile all accounts from Mariadb 172.20.0.6 

5. Finally, the process ends.



The system has been connected, now you can tailor its agent

 Close

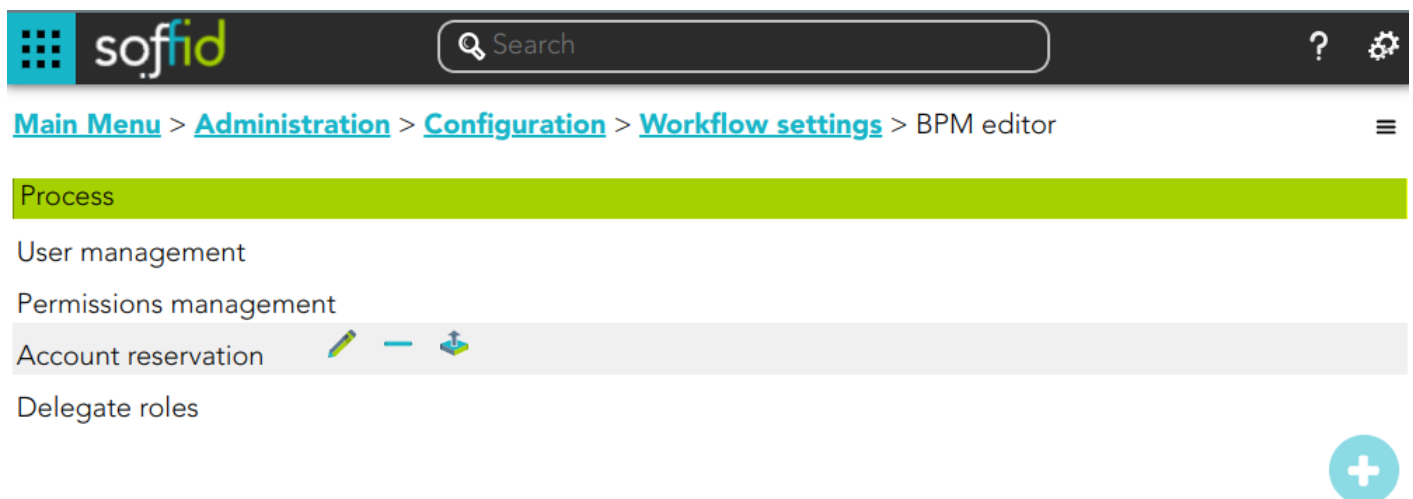
Design user life cycle workflows

Description

When you select the option "Design user life cycle workflows", Soffid will browse to the BPM Editor page, where you could define new workflows or import existing workflows from a file.

For more information, you can visit [the BPM Editor book](#).

Screen overview



IRC

Identity Risk & Compliance

Create SoD matrix

Description

The segregation of duties (SoD) is a fundamental element of internal controls, defined to prevent error and fraud. Segregation of duties ensures that at least two individuals are responsible for the separate parts of any task.

You can find additional information by visiting [the Segregation of Duties page](#).

Step-by-step

1. First, you must select the Create SoD matrix and click the OK button.



In the Segregation of Duties rule editor, you can create rules to detect risky role assignments.

⚠ These rules can include one or several roles from one or more systems.

Click OK to jump to the SoD rule editor.

OK

2. Once you click the OK button, Soffid will browse to the Segregation of Duties page in order to add a new SoD

soffid

Search

?

⚙

[Main Menu](#) > [Administration](#) > [Resources](#) > [Segregation of Duties](#)

Name :

Information system :

🔍

Type :

- Select value -

Risk :

- Select value -

Roles list

	⚙ Name	⚙ Description	⚙ System
	<input type="text" value="Filter"/>	<input type="text" value="Filter"/>	<input type="text" value="Filter"/>

Displayed rows: 0


+

↶ Undo


📄 Apply changes

3. Finally you must save or Apply changes to save the SoD.

[Main Menu](#) > [Administration](#) > [Resources](#) > Segregation of Duties ≡

name Any × application Any × [Add criteria](#)  [Basic](#) [Advanced](#)

<input type="checkbox"/>	▼ Qualified name	▲ ▼ Name
<input type="checkbox"/>	SOFFID	Rule01

Displayed rows: 1 

Standard attributes

- **Name:** name of the segregation separation of duties
- **Information System:** asset or application, from a functional point of view, on which the permissions are granted or revoked.
- **Type:** type of segregation
 - **Trigger on all permissions:** no user can be assigned the roles added to the role list.
 - **Trigger on some permissions:** if you select that option, you have to fill in the number of roles that can not match. Soffid will not allow you to assign to a user more than the number indicated of the roles added to the role list.
 - **Query permissions matrix:** Soffid displays a matrix that allows you to select the risk between pairs of roles, those roles are the roles added to the role list.
- **Risk:** level of risk:
 - **Low.**
 - **High.**
 - **Forbidden:** it is not allowed that one user to have assigned the roles defined on the role list.
 - **None:** there is no risk.
- **Role List:** list of roles to keep in mind on the segregation of duties.

Schedule weekly risk report

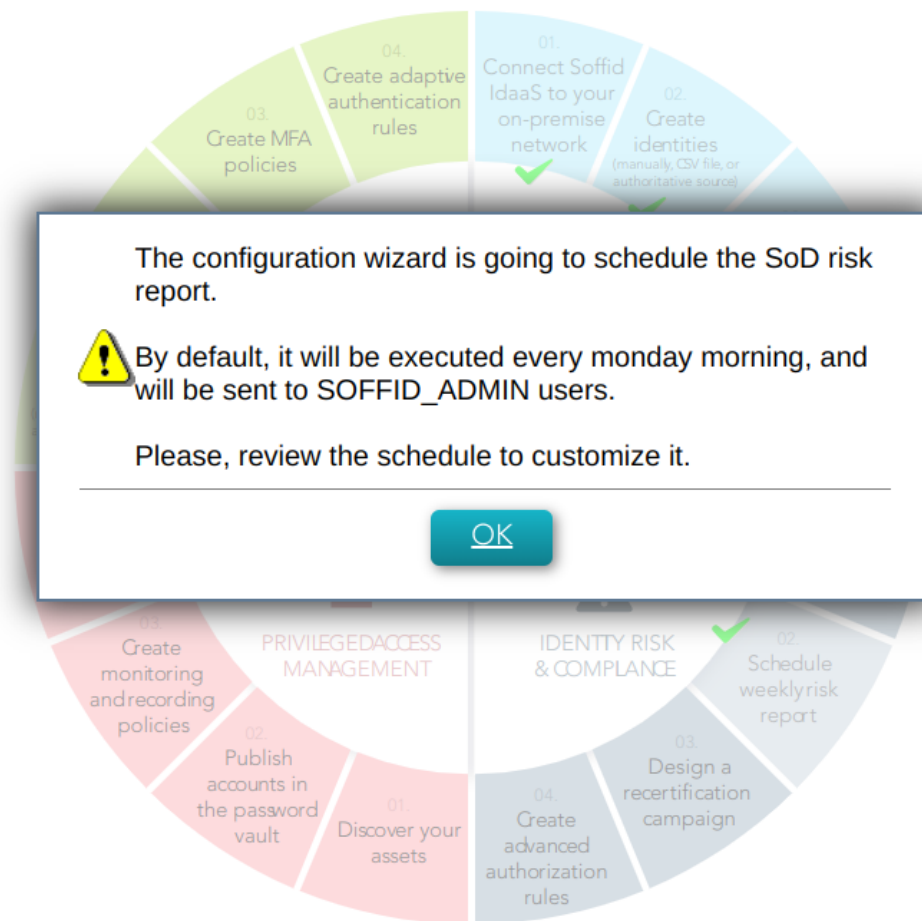
Description

The wizard allows you to schedule a new Weekly risk report. It is a document that provides an overview of the potential risks. The information in this document is related to the rules defined in the SoD.

For more information, you can visit [the Scheduled reports page](#).

Step-by-step

1. First, you must select the Schedule weekly risk report and click the OK button.



2. Then, Soffid will browse to the configure report page and allows you to configure the Weekly risk report.

Report : Weekly risk report

Schedule name:

Schedule name: : Weekly risk report

Month : *

Day : *

Hour : 6

Minute : 0

Day of week : 1

Parameters

highRisk	true
all	true
lowRisk	true
forbiddenRisk	true
app	

Access Control List

<input type="checkbox"/>	Object type	Name
	Filter	Filter
<input type="checkbox"/>	role	SOFFID_ADMIN @ soffid

Displayed rows: 1

+

Accept Cancel

3. Finally you must accept the changes, and the report will be displayed on the Scheduled reports page

[Main Menu](#) > [Administration](#) > [Monitoring and reporting](#) > Reports

[Executed reports](#) [Scheduled reports](#) [Report definitions](#)

<input type="checkbox"/>	Report
	Filter
<input type="checkbox"/>	Weekly risk report

Displayed rows: 1

+

Standard attributes

- **Report:** name of the report.
- **Schedule name:** identified name.
- **Month:** number of the month (1-12) when the task will be performed.
- **Day:** number of the day (1-31) when the task will be performed.

- **Hour:** hour (0-23) when the task will be performed.
- **Minute:** minute (0-59) when the task will be performed.
- **Day of week:** number of the day (0-7 where 0 means Sunday) of the week when the task will be performed.
- **Access Control List:** to prevent unauthorized usage. Will be granted to users, groups or roles.

For each value of month, day, hour, minute, or day of the week:

- * means any month, day, hour, minute, or day of the week. e.g. */5 to schedule every five minutes.
- A single number specifies that unit value: 3
- Some comma separated numbers: 1,3,5,7
- A range of values: 1-5

Design a recertification campaign

Description

The wizard allows you to create a new recertification campaign. To be able to do this, Soffid has created two recertification policies, *All permissions* and *Critical permissions*.


For more information, you can visit [**the Recertification book**](#).

Step-by-step

1. First, you must select the Design a recertification campaign and click the OK button.

Soffid will automatically create two recertification policies:

- All permissions: Review any permission granted to the users
- Critical permissions: Review permissions with any kind of risk. The risk level is governed by the Segregation of Duties rules.

 Click OK to create a new recertification campaign. To successfully start a new recertification campaign, you must:

1. Select the proper policy
2. Select the organization scope, i.e. the groups whose members will be recertified.
3. Select the informatin scope, i.e. the applications whose grants will be recertified.

OK

Cancel

2. Then Soffid will browse the New recertification campaign

soffid

New recertification campaign

?

⚙

[Main Menu](#) >
 [Admin](#)

Name Any

Pr

☐

⚙

Name

Select template

Select groups

Select information systems

Finish

Name :

Name

Select template :

- Select value -

↶ Undo

Next ➡

Basic

Advanced

Displayed rows: 0

+

3. In this step you must write a campaign name and select a template.

3.1. Complete access review

3.1.1. Write a name, select the Complete access review, and click the Next button

New recertification campaign

Progress: Select template > Select groups > Select information systems > Finish

Name : Any

Select template : Complete access review

Buttons: Undo, Next

3.1.2. Select the group or groups to apply the campaign and click the Next button

New recertification campaign

Progress: Select template > Select groups > Select information systems > Finish

Select groups : world

World

Select groups

Buttons: Back, Next

3.1.3. Select the Information systems to apply the campaign and click the Finish button

New recertification campaign

Progress: Select template > Select groups > Select information systems > Finish

Select information systems : Source AD: soffid.pat

Authoritative data source dc=soffid,dc=pat

Select information systems

Buttons: Back, Finish

Standard attributes

- **Name:** name to identify the campaign.
- **Template:** select the policy that will be applied. That has to be defined previously on the [Recertification policies page](#).
- **Groups:** list of user groups where the campaign will be applied. You can choose one or more.
- **Information Systems:** list of information systems where the campaign will be applied. You can choose one or more.

Create advanced authorization rules

Description

This wizard allows you to browse the XACML Policy Management page to create new policies to add more complex and restricted rules to the authorizations.

For more information, you can visit [the XACML page](#).

Screen overview

The XACML rule editor allows you to create five different type of authorization rules:

- Roles: Are evaluated at login time and filters out which Soffid authorizations will be enabled for the user.
- Dynamic roles: Are evaluated at each service invocation. Mind that performance issues can arise using this module.
- PAM rules: Are evaluated when trying to use an account protected by the password vault
- Web rules: Are evaluated whenever a new web page is open. It's evaluated once per page.
- External rules: Are used by third party applications.

Now, you will be redirected to the XACML rule editor. Once the rule is designed, you can enable it using the XACML PEP option.

Screen overview

<https://www.youtube.com/embed/C3LMc4rrEQI?ref=0>

Related objects

- Policy set
- Policy
- Policy set reference

- Policy reference

PAM

Privileged Access Management

Discover your assets

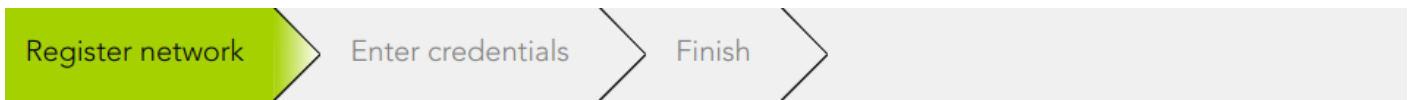
Description

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.



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

Description :	<input type="text" value="Laboratory network 01"/>
IP Address :	<input type="text" value="10.129.122.0"/>
IP Address mask :	<input type="text" value="255.255.255.0"/>

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.



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.

AM

Access Management & SSO

Create identities (manually, CSV file, or authoritative source)

Description

You need to register the identities to manage and protect them. This wizard allows you to choose the easiest way to do it.

Step-by-step

1. First, you must select one option to register the identities. Soffid allows you three options.

Load identities

You need to register the identities to manage and protect. Here you have some ways to do it:

- ☐ Load from a CSV file
- ☐ Configure an authoritative data source to always have up-to-date information
- ☐ Register them manually

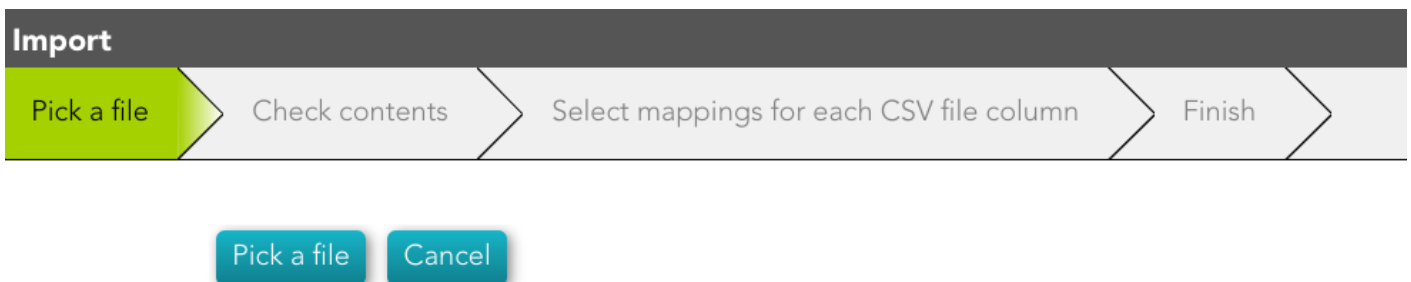
← Undo

Next

2. You must follow the steps, depending on the selected option:

2.1. Load from a CSV file: this option allows you to load identities from a CSV file.

2.1.1. First of all, you need to pick up the CSV file.



2.1.2. Second, Soffid will display the file data to check contents

Import

Pick a file

Check contents

Select mappings for each CSV file column

Finish

Character set :

UTF-8

Separator :

,

Quote character :

"

Escape character :

\

Contains header row :

Yes



Reload

Picture	User...	Full ...	Prim...	Ena...	Birth...	First ...	Last ...	Mid...	Type
	rfranklin	Rosalind Franklin	scientist	Si		Rosalind	Franklin		I
	aeinstein	Albert Einstein	scientist	Si		Albert	Einstein		I

← Back

→ Next

2.1.3. Then you must select the proper mapping for each CSV file column. And finally, click the Import Button and Soffid will add the identities to the platform.

Import

Pick a file

Check contents

Select mappings for each CSV file column

Finish


Select mappings for each CSV file column

CSV column	Target object attribute
Picture	Don't load
User name	User name
Full name	Full name
Primary group	Primary group
Enabled	Enabled
Birth Date	Don't load
First name	First name
Last Name	Last Name
Middle name	Middle name
Type	Type

Back

Import

2.1.4. Soffid will display the result of the process.

 soffid

Search

?

⚙

[Main Menu](#) > [Administration](#) > [Resources](#) > Users

User name Any

First name Any

Last Name Any

Primary group Any

Add criteria

Quick

Basic

Advanced

☐


▼ User name


▲ Full name

▲ Primary group

▲ Enabled

Displayed rows: 0



 Added 0 new rows, 2 rows updated, 0 rows removed and 0 rows without any change

OK

2.2. Configure an authoritative data source to always have up-to-date information: this option allows you to configure an Active Directory agent, or a Relational database agent to load the identities.

Once the process will finish, you could check the new agent on the agent's page [Main Menu > Administration > Configuration > Integration engine > Agents](#)

For more information about the agents, you can visit [the Agents page](#).

Load identities

Please, select a the type of data source to fetch identities from

- ☐ Active Directory
- ☐ Relational database (SQL)

[← Undo](#) [Next](#)

2.2.1. Active Directory

- To configure the AD connection you must fill in the required fields and click the Next button.
- Then Soffid will run the Authoritative load and the Reconcile process
- Finally, you could check the result on the [Scheduled tasks](#) page.

Configure connection

Load users information

Load users permissions

Active directory name :

dc=soffid,dc=pat

*

User name :

SOFFID\Administrator

*

Password :

●●●●●●●●●●



← Undo

→ Next

2.2.2. Relational database (SQL)

Configure SQL connection

Load users information

Load users permissions

Database type :

Mysql or Mariadb

Database url :

jdbc:mariadb://172.20.0.6/BABELTEST

User name :

babeluser

Password :

••••••••


SQL Sentence :


select * from USERS

← Undo

→ Next

2.3. Register them manually: this option browses to the **User page** to register the identities manually





[Main Menu](#) > [Administration](#) > [Resources](#) > [Users](#)

[Basics](#) [Groups](#) [Accounts](#) [Roles](#) [Effective Roles](#) [Shared accounts](#) [Sessions](#) [User processes](#) [OTP devices](#) [Tokens](#) [Backups](#)

Common attributes

User name :

First name :

Last Name :

Middle name :

Full name :

Organization

Type :

Primary group :

Home server :

Profile server :

Mail service

eMail :

Mail alias :

Mail server :

User status

Enabled : ☐ No

Multi session : ☐ No

Comments :

Audit information

Created by :

Add applications

Description

This wizard allows you to add a new Service Provider, that is, to configure an application that relies on an Identity Provider (IdP) to authenticate users and provide access to its services.

Step-by-step

1. Once you select the *Add application* option, Soffid will display the wizard to register the Identity Provider, if it does not exist previously.

Add applications

Register identity provider

Select application

Configure application

Configure Soffid

Finish

First, you need to configure the Soffid identity provider. It must have a public DNS Name, and should be reachable from the Internet.

Host name :

HTTPS port :

[← Undo](#) [→ Next](#)

2. You must select the application you want to add.

Add applications

Register identity provider

Select application

Configure application

Configure Soffid

Finish

Add new application



This console



AWS



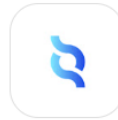
Google
workplace



Microsoft 365



Openid



SAML 2.0

← Undo

2.1. Soffid app:

2.1.1. The Finish step will be displayed.

Add applications

Register identity provider

Select application

Configure application

Configure Soffid

Finish

The application wizard has finished. Click Finish to review its settings.

✓ Finish

2.1.1. If you click the Finish button, Soffid will display the Service Provider page.

Identification

Type :	SAML
Identifier :	https://gbr.demo.soffid.net/soffid-iam-console
Name :	Soffid

Service configuration

Metadata :	<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" entityID="https://gbr.demo.soffid.net/soffid-iam-console">
------------	---

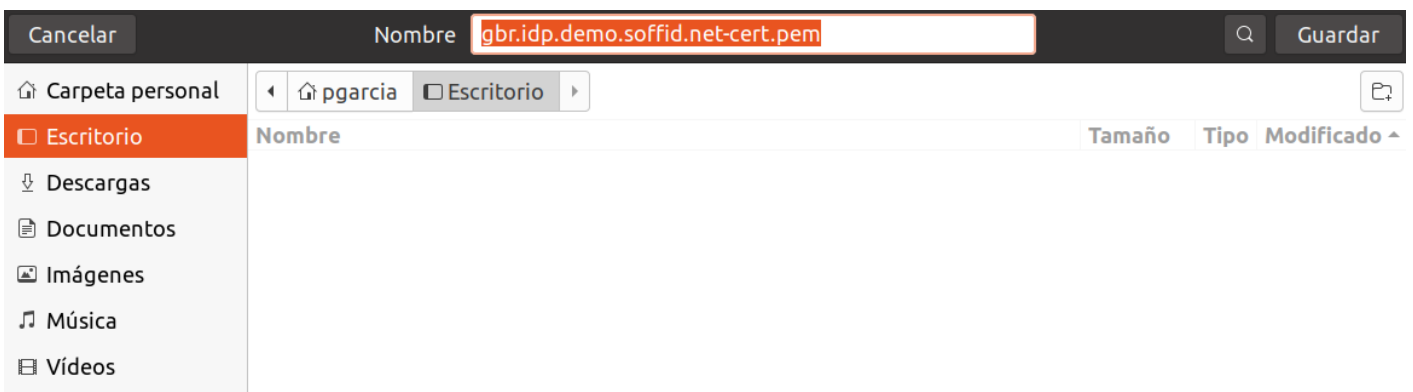
Login rules

Allow impersonations :	Target application URL
UID Script :	Script to compute the user name to pass to the target application
Ask for consent :	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
Roles required to login :	Roles required to login
System where an enabled account is required :	

Undo Apply changes

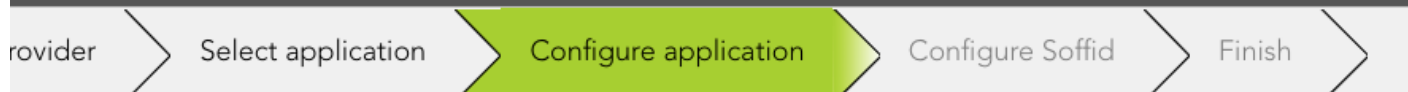
2.2. AWS app:

2.2.1 Soffid will download the proper certificate.





2.2.2 Once, you download the certificate, Soffid will display the Configure application step. You must follow the indicated steps at this point and click the Next button.

Add applications



Please, follow the next steps:

- 1: Save the certificate that is being downloaded from Soffid wizard
- 2: Enter int to your [AWS IAM platform](#)
- 3: Enable **IAM Identity center**, if it is not enabled yet
- 4: Click on **Choose your identity source**
- 5: Click on **Change identity source** and select **External identity provider**
- 6: Enter the following IdP sign-in URL: <https://gbr.idp.demo.soffid.net:443/profile/SAML2/Redirect/SSO> 
- 7: Enter the following IdP issuer URL: <http://idp.demo.soffid.net/gbr> 
- 8: Click on the **Choose file** button to upload the **IdP certificate**, and upload the certificate previously loaded from Soffid wizard
- 9: Click on **Download metadata file** button in the Service provider metadata box, save it for the next step
- 10: Click on the **Next** button, in the right bottom corner of the AWS page.
- 11: Type in **ACCEPT** and click on **Change identity source**
- 12: Optionally, click on the button to **Enable** Automatic provisioning

When finished, click on the Next button below and upload the metadata file you have just downloaded.



2.2.2 Then, you must upload the metadata of your service provider and click the Finish button.

Add applications

Provider

Select application

Configure application

Configure Soffid

Finish

Please, upload the metadata file generated by the service provider

Pick a file

← Undo

2.3. Google workplace app:

2.3.1 Soffid will download the proper certificate.

Cancelar

Nombre gbr.idp.demo.soffid.net-cert.pem

Guardar

Carpeta personal

Escritorio

Descargas

Documentos

Imágenes

Música

Videos

pgarcia

Escritorio

Nombre	Tamaño	Tipo	Modificado
--------	--------	------	------------

2.3.2 Once, you download the certificate, Soffid will display the Configure application step. You must follow the indicated steps at this point, fill in the Domain, and click the Next button.

Add applications

Provider

Select application

Configure application

Configure Soffid

Finish

Please, follow the next steps:

- 1: Save the certificate that is being downloaded from Soffid wizard
- 2: Enter int to your [Google apps administration console](#)
- 3: Enable **Third party SSO Profile**, if it is not enabled yet
- 4: Enter the following IdP sign-in URL: <https://gbr.idp.demo.soffid.net:443/profile/SAML2/Redirect/SSO>
- 5: Enter the following IdP logout URL: <https://gbr.idp.demo.soffid.net:443/logout.jsp>
- 6: Click on the **IdP certificate** button, and upload the certificate previously loaded from Soffid wizard
- 7: Check the **domain specific issuer entity** box
- 8: Enter the following URL to change passwords:
<https://gbr.idp.demo.soffid.net:443/protected/passwordChange>
- 9: Click on the **Save changes** button, in the right bottom corner of the Google page.

When finished, click on the Next button below

Domain :

← Undo

→ Next

2.3.3 Then, you must click the Finish button.

Add applications

Provider

Select application

Configure application

Configure Soffid

Finish

The application wizard has finished. Click Finish to review its settings.

✓ Finish

2.3.4 Finally, Soffid will browse to the Service Provider page where you can finish the Service provider configuration.

[Main Menu](#) > [Administration](#) > [Configuration](#) > [Web SSO](#) > [Identity & Service providers](#) ◀ 5 / 10 ▶

Identification

Type : SAML
Identifier : google.cam/a/soffid.pat.lab
Name : Google google.cam/a/soffid.pat.lab

Service configuration

Metadata :

```
<EntityDescriptor entityID="google.cam/a/soffid.pat.lab"
xmlns="urn:oasis:names:tc:SAML:2.0:metadata">
  <SPSSODescriptor
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol"
>
    <NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-
format:email</NameIDFormat>
```

Login rules

Allow impersonations : Target application URL
UID Script : Script to compute the user name to pass to the target application
Ask for consent : ☒ Yes ☐ No
Roles required to login : Roles required to login
System where an enabled account is required :

Undo Apply changes

2.4. Microsoft 365 app:

2.4.1. When you select this option, Soffid will display the Configure application step. You must follow the indicated steps at this point, and click the Next button.

Add applications

Provider

Select application

Configure application

Configure Soffid

Finish

Please, follow the next steps:

1: Open **powershell**

2: Enter the following command: Install-Module MSOnline

3: Enter the following command: Connect-MsolService

4: Execute the following commands:

```
Set-MsolDomainAuthentication `
-FederationBrandName "Soffid IdP" `
-Authentication Federated `
-PassiveLogOnUri
"https://gbr.idp.demo.soffid.net:443/profile/SAML2/Redirect/SSO" `
-SigningCertificate $MySigningCert
"MIICKTCCAZKgAwIBAgIGAYYdp3W2MA0GCSqGSIb3DQEBCwUAMFgxJzAlBgNVBAMMHmh0dHA6L
```

When finished, click on the Next button below and upload the metadata file you have just downloaded.

← Undo

→ Next

2.4.2 Then, you must click the Finish button.

Add applications

Provider

Select application

Configure application

Configure Soffid

Finish

The application wizard has finished. Click Finish to review its settings.

✓ Finish

2.4.3 Finally, Soffid will browse to the Service Provider page where you can finish the Service provider configuration.

[Main Menu](#) > [Administration](#) > [Configuration](#) > [Web SSO](#) > [Identity & Service providers](#) 4 / 4

Identification

Type : SAML
Identifier : urn:federation:MicrosoftOnline
Name : Azure

Service configuration

Metadata : <EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:alg="urn:oasis:names:tc:SAML:metadata:algsupport">

Login rules

Allow impersonations : Target application URL
UID Script : Script to compute the user name to pass to the target application
Ask for consent : ☒ Yes ☐ No
Roles required to login : Roles required to login
System where an enabled account is required :

Undo Apply changes

2.5. OpenID app:

2.5.1. When you select this option, Soffid will display the Configure application step. You must configure your Service Provider, and click the Next button.

Add applications

Provider

Select application

Configure application

Configure Soffid

Finish

Name :

OpenIDTest

OpenID authorization flow

Implicit :

☒ No

Authorization code :

Yes ☒

User's password :

☒ No

User's password + Client credentials :

☒ No

Response URL :

https://gbr.demo.soffid.net:4204

Response URL

← Undo

→ Next

2.5.2. Then Soffid will return you the Client id and Client secret

Add applications

provider

Select application

Configure application

Configure Soffid

Finish

Please, configure your application with the following client id and client secret

Client id :

SLdmOb6XdNkvcqrkT8ziG6Sdo8Qw6UPel0Tbbj9/xaEbSAQI

Client secret :

eoibGguBFaYaGckIDbTjfRtNvHaNm0MZxRf0G6vSfhDFWZH8

← Undo

→ Next

2.5.3 Then, you must click the Finish button.

Add applications

Provider

Select application

Configure application

Configure Soffid

Finish

The application wizard has finished. Click Finish to review its settings.

✓ Finish

2.5.4 Finally, Soffid will browse to the Service Provider page where you can finish the Service provider configuration.

[Main Menu](#) > [Administration](#) > [Configuration](#) > [Web SSO](#) > [Identity & Service providers](#) ◀ 4 / 4

Identification

Type :

Identifier :

Name :

Login rules

Allow impersonations :

UID Script :

Ask for consent :

Roles required to login :

System where an enabled account is required :

OpenID authorization flow

Implicit :

Authorization code :

User's password :

User's password + Client credentials :

Client id :

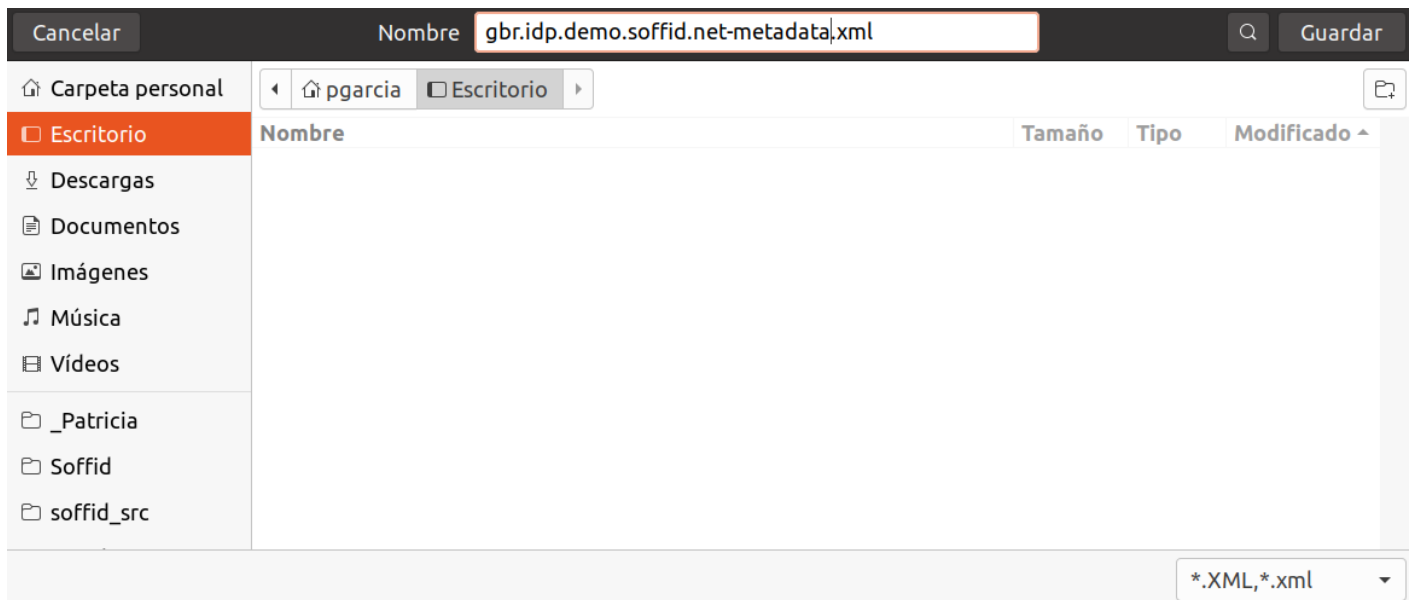
Client secret :

Sector identifier URI :

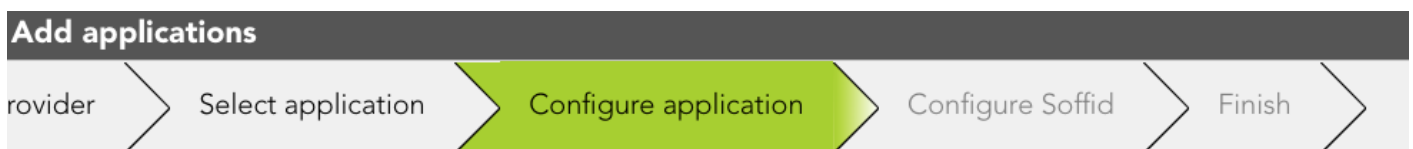
Response URL :

2.6. SAML 2.0 app:

2.6.1 Soffid will download the metadata XML file.



2.5.2 Once, you download the metadata file, Soffid will display the steps to follow.



Please, save the metadata file that is being downloaded from Soffid wizard and upload it to your SAML application.

Alternatively, tell your SAML application to download it from <https://gbr.idp.demo soffid.net:443/SAML/metadata.xml>

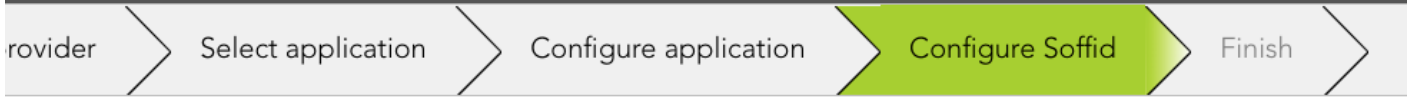
Next, download you application metadata from your application configuration web page.

When finished, click on the Next button below and upload the metadata file you have just downloaded.



2.5.3 Then, you have to upload the metadata file generated by the Service Provider

Add applications



Please, upload the metadata file generated by the service provider

Pick a file

← Undo

Create MFA policies

Description

This wizard will help you to configure multi-factor authentication in order to expand security. This process requires users to provide two or more forms of identification before being granted access to a system or application.

For more information, you can visit [the Two-factor authentication \(2FA\) book](#).

Step-by-step

1. First, you must select the authentication factor to use

Enable multi-factor authentication

Select OTP type

Delivery method

Activation

Finish

Select the strong authentication factor type to use

- ☐ Email
- ☐ SMS
- ☐ Time-based HMAC OTP
- ☐ Event-based HMAC OTP
- ☐ Security PIN
- ☐ Certificate
- ☐ FIDO Token

← Undo

→ Next

2. Second, you must select the delivery method to use. If you select the second option, you have to select the users to whom the instructions will be sent.

Enable multi-factor authentication

Select OTP type

Delivery method

Activation

Finish

Select the desired method to provision the strong authentication factor.

- ☐ Send instructions by email to everyone
- ☐ Send instructions by email to some selected users
- ☐ Do not send it yet

Email message :

Dear \${fullName},

Please, follow this [link](#) to register your authentication email address.
It will be used by Soffid to verify your identity.

Sincerely yours, Gabriel Buades

← Undo

→ Next

3. Next, you must select which users will have the second authentication factor activated.

Enable multi-factor authentication

Select OTP type

Delivery method

Activation

Finish

Select which users will be required to use its second authentication factor

- ☐ Everyone
- ☐ Only users that have completed the enrollment process.
- ☐ No one yet

← Undo

→ Next

3. Finally, the changes will be applied and the process will be finished.

Enable multi-factor authentication

Select OTP type

Delivery method

Activation

Finish

Applying changes

✓ Finish

Create adaptive authentication rules

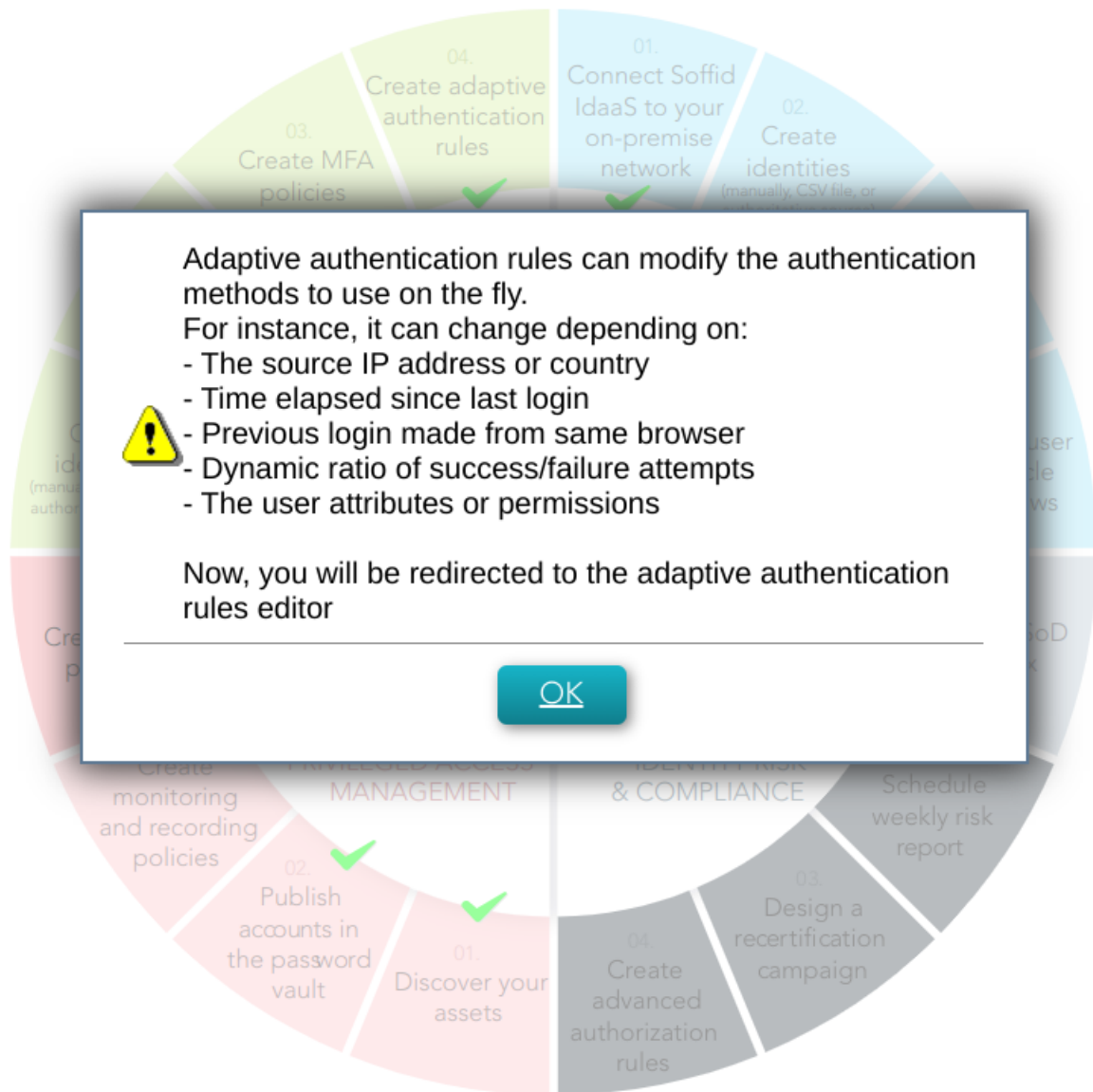
Description

Adaptive authentication rules are a set of security policies and mechanisms that adjust authentication requirements. These rules determine the strength of authentication required for each user, based on factors such as their location, device, past login behavior, and other risk indicators.

For more information, you can visit the [Condition for Adaptive authentication page](#).

Step-by-step

1. First, you must select the *Create adaptive authentication rules* and then click the Ok button.



2. Then, Soffid will browse to the Adaptive authentication window, where you could configure it

Adaptive authentication

Description : Brute force Attack

Condition : failuresRatio > 0.8

Always ask for credentials : ☒ No

	First a	Passw	Kerbe	Extern	OTP	Email	SMS	PIN	Certifi	FIDO
Passw		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Kerber			<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Extern				<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
OTP					<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Email						<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
SMS							<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
PIN								<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Certific									<input type="checkbox"/>	<input type="checkbox"/>
FIDO										<input type="checkbox"/>

Description : Foreign country

Condition : ! sourceCountry.equals("ES") && false

Always ask for credentials : Yes ☒

First a	Passw	Kerbe	Extern	OTP	Email	SMS	PIN	Certifi	FIDO
---------	-------	-------	--------	-----	-------	-----	-----	---------	------



← Close