

# AM

## Access Management & SSO

- Create identities (manually, CSV file, or authoritative source)
- Add applications
- Create MFA policies
- Create adaptive authentication rules

# 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

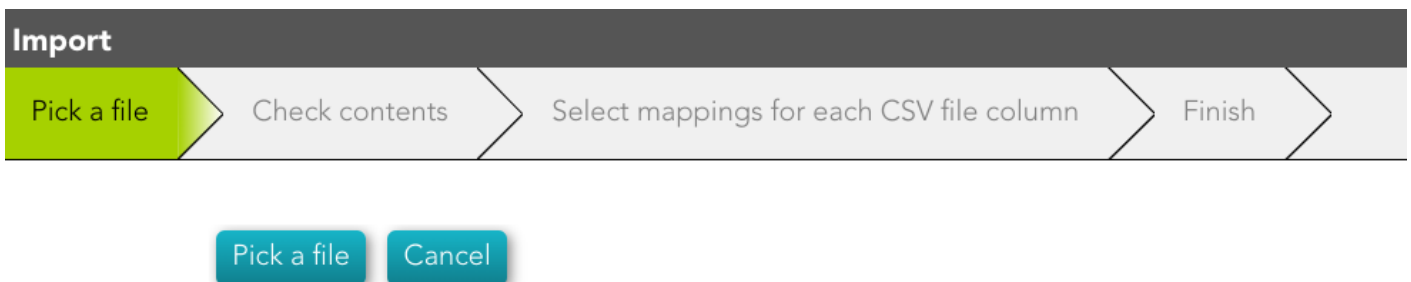
← Undo

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)



❄

✱



→ Next

?



\*



- 100%
- 100%
- 100%

- **WED**
- **WED**
- **WED**

- **WCD**
- **WCD**
- **WCD**

No

Comments

Figure 1





# 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 :

iam-sync-35.soffidnet

HTTPS port :

443

← 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



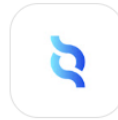
Google  
workplace



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">
------------	---

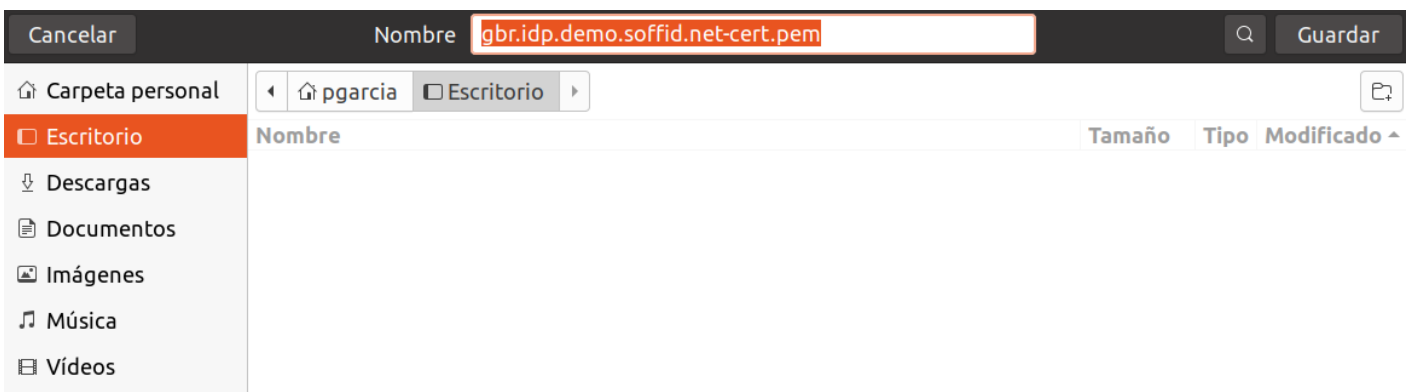
## Login rules

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

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 [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.

← Undo

→ Next

**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 : OpenID Connect  
Identifier : OpenIDTest  
Name : OpenIDTest

### Login rules

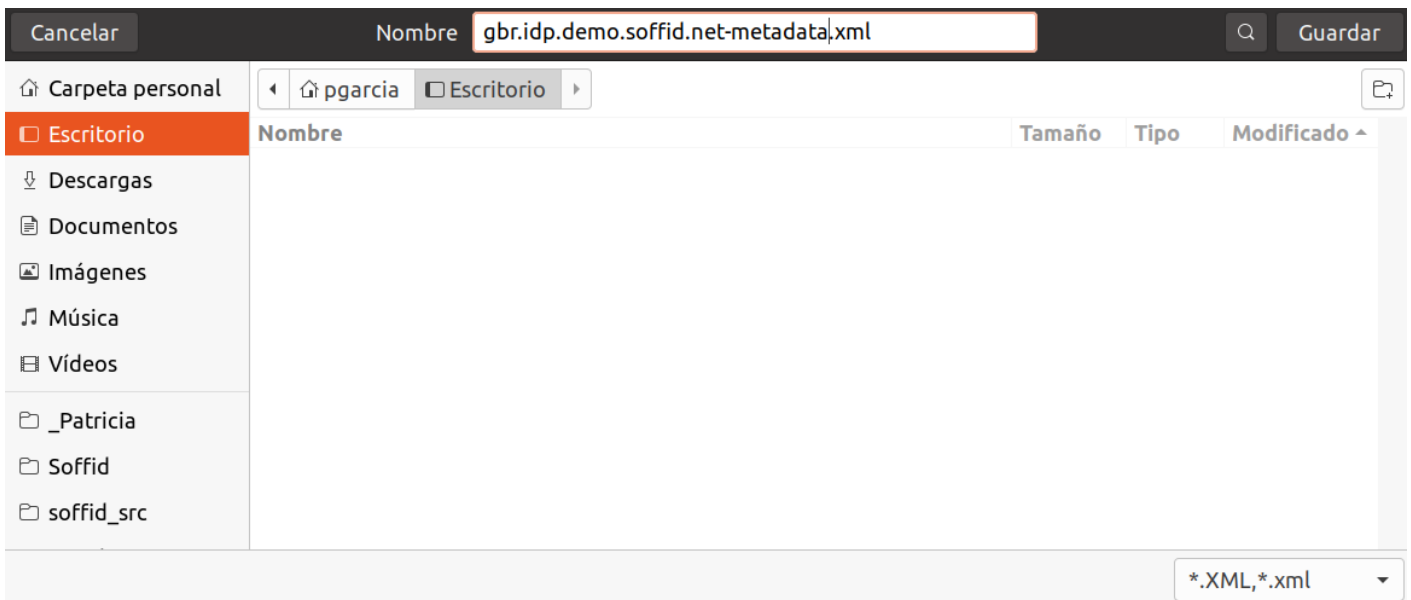
Allow impersonations : Target application URL  
UID Script : Script to compute the user name to pass to the target application  
Ask for consent : ☒ Yes ☐ No  
Roles required to login : Roles required to login  
System where an enabled account is required :

### OpenID authorization flow

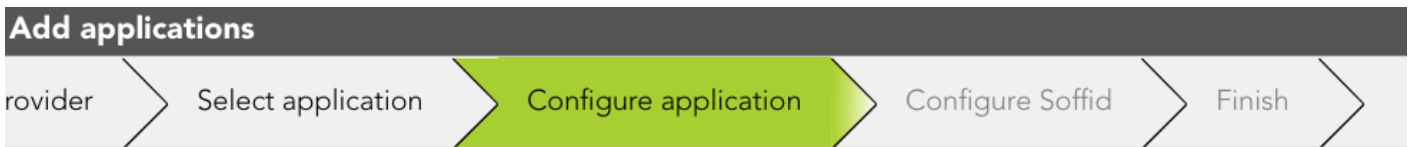
Implicit : ☒ Yes ☐ No  
Authorization code : ☒ Yes ☐ No  
User's password : ☒ Yes ☐ No  
User's password + Client credentials : ☒ Yes ☐ No  
Client id : SLdmOb6XdNkvcqrkT8ziG6Sdo8Qw6UPel0Tbbj9/xaEbSAQI  
Client secret : \*\*\*\*\*  
Sector identifier URI : Sector identifier URI  
Response URL : https://gbr.demo.soffid.net:4204

## 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>

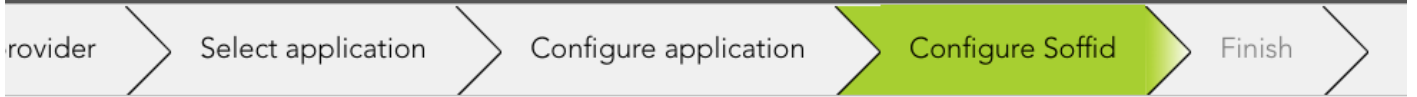
Next, download you application metadata from your application configuration web page.

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