

Add applications

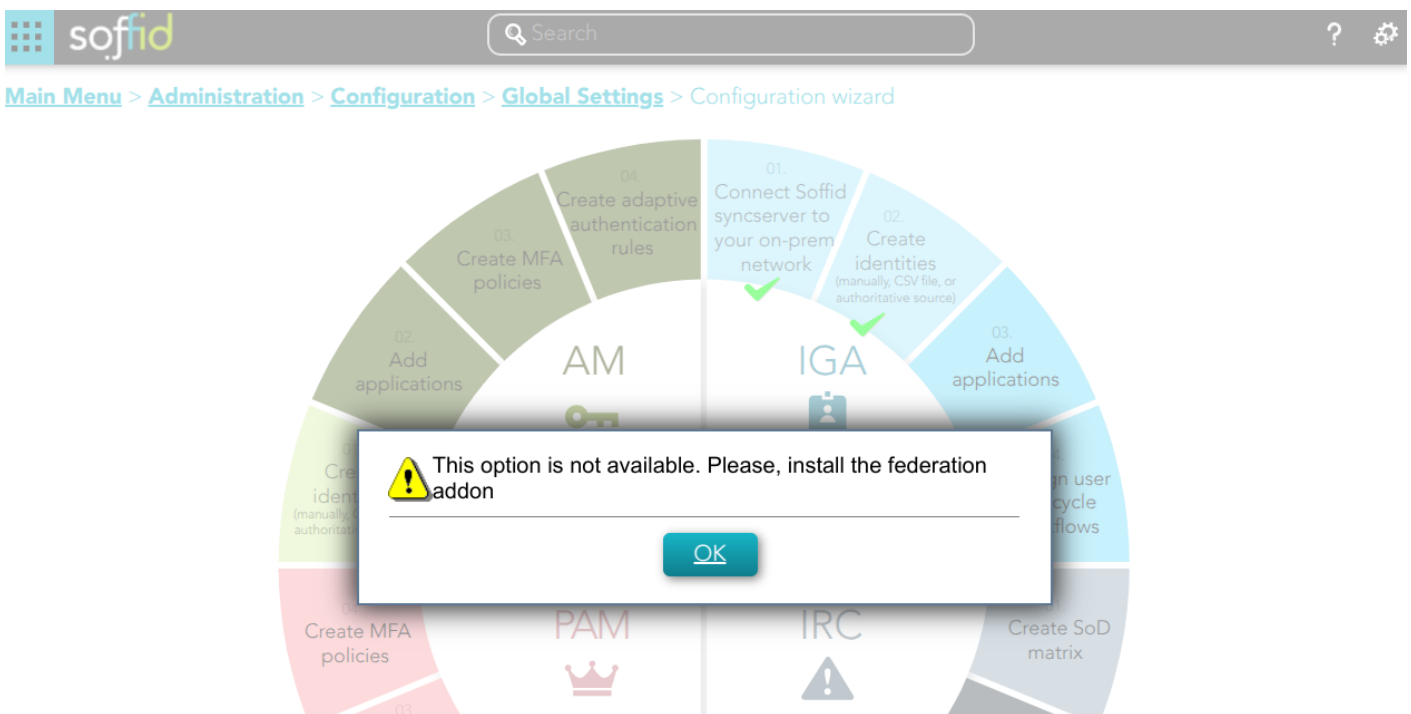
Description

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.

To be able to add new applications (SP), you must install the Federation Addon.

Step-by-step

1. If you have not previously installed the Federation Addon, the first time you select the *Add application* option, Soffid will require to **install the Federation Addon**.



When you click the OK button, Soffid will browse to the Soffid Download Area where you can find the Federation Addon. To install Federation Addon you can follow the steps [How to install Federation in Soffid?](#)

2. 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 :






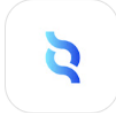
[← Undo](#) [→ Next](#)

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

Add applications

Register identity provider > **Select application** > Configure application > Configure Soffid > Finish

Add new application

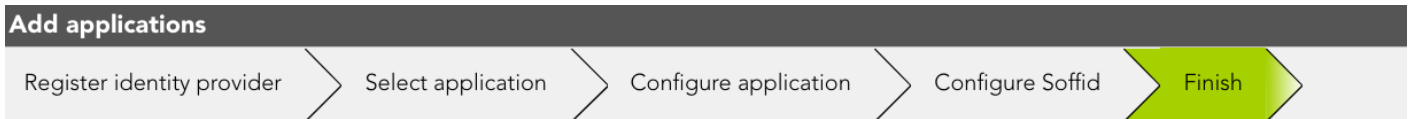
     

This console AWS Google workplace Microsoft 365 Openid SAML 2.0

[← Undo](#)

3.1. Soffid app:

3.1.1. The Finish step will be displayed.



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



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

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

Identification

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

Login rules

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

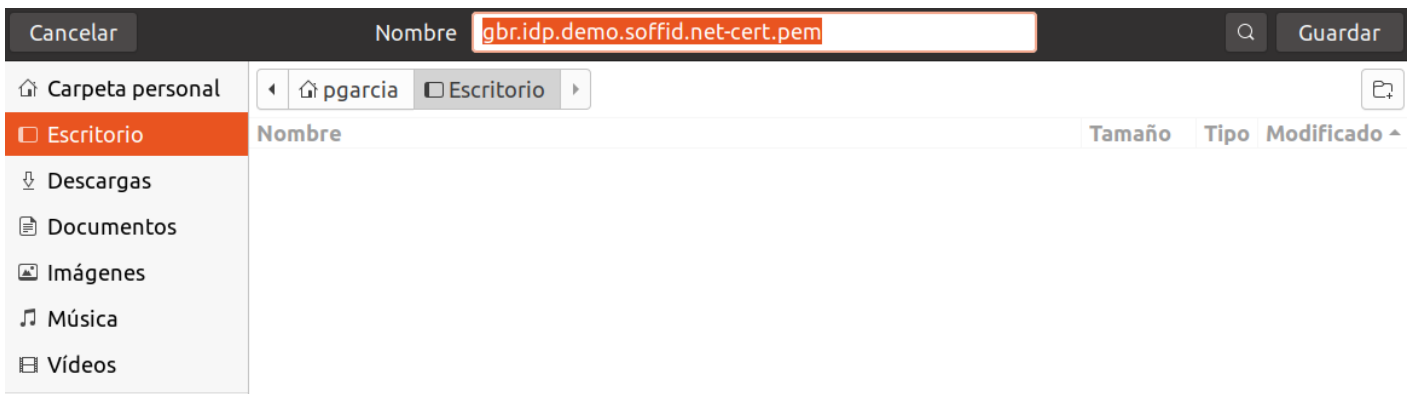
Service configuration

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

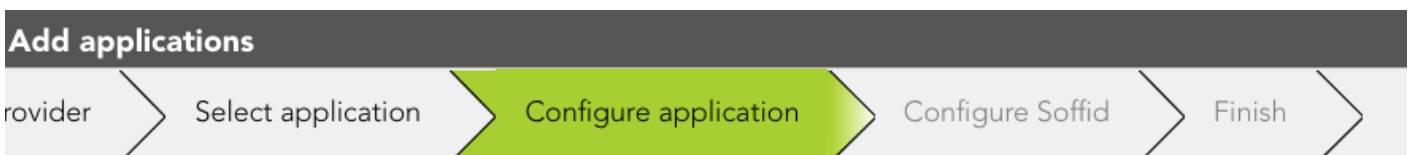
Undo Apply changes

3.2. AWS app:

3.2.1 Soffid will download the proper certificate.



3.2.2 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.



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.



3.2.2 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

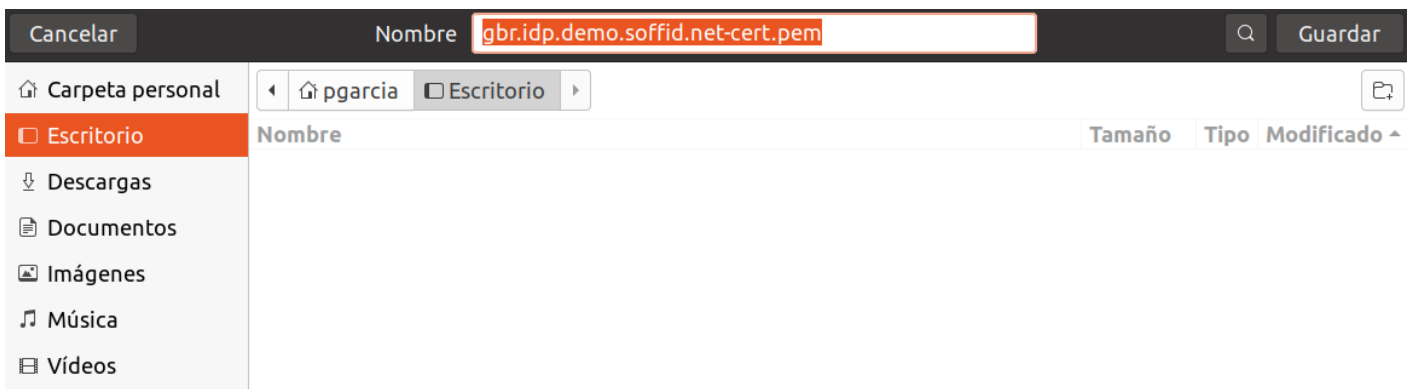
Please, upload the metadata file generated by the service provider

Pick a file

← Undo

3.3. Google workplace app:

3.3.1 Soffid will download the proper certificate.



3.3.2 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.

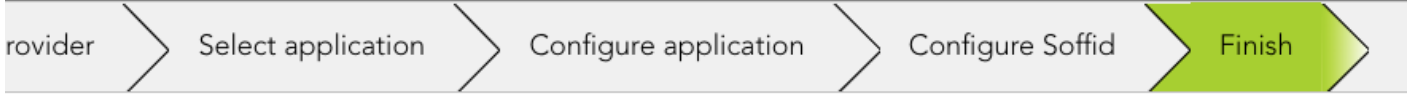
When finished, click on the Next button below

Domain :

 Undo  Next

3.3.3 Then, you must click the Finish button.

Add applications



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



3.3.4 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 :

Identifier :

Name :

Login rules

Allow impersonations :

UID Script :

Ask for consent :

Roles required to login :

System where an enabled account is required :

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:persistent/(NameIDFormat)</NameIDFormat>
  </SPSSODescriptor>
</EntityDescriptor>
```

3.4. Microsoft 365 app:

3.4.1. 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
```



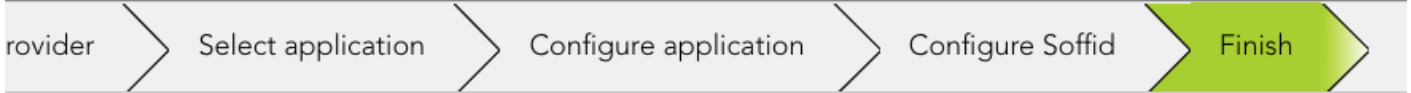
When finished, click on the Next button below and upload the metadata file you have just downloaded.

 Undo

 Next

3.4.2 Then, you must click the Finish button.

Add applications



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



3.4.3 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 :

Identifier :

Name :

Service configuration

Metadata :

Login rules

Allow impersonations :

UID Script :

Ask for consent : Yes No

Roles required to login :

System where an enabled account is required :

3.5. OpenID app:

3.5.1. 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

3.5.2. 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 :

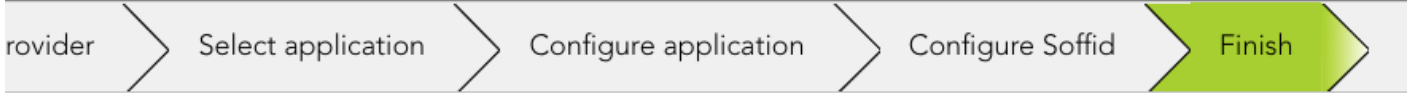
eoibGguBFaYaGckIDbTjfRtNvHaNm0MZxRf0G6vSfhDFWZH8

← Undo

→ Next

3.5.3 Then, you must click the Finish button.

Add applications



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



3.5.4 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

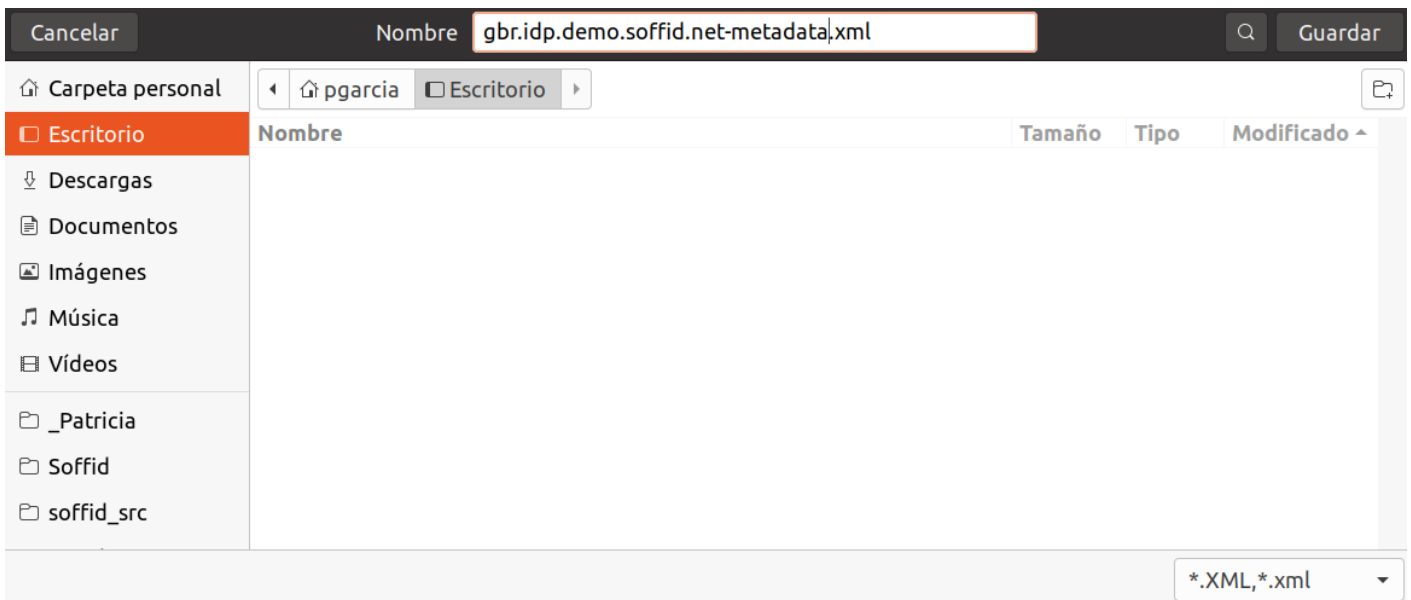
Allow impersonations :	Target application URL
UID Script :	Script to compute the user name to pass to the target application
Ask for consent :	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
Roles required to login :	Roles required to login
System where an enabled account is required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

OpenID authorization flow

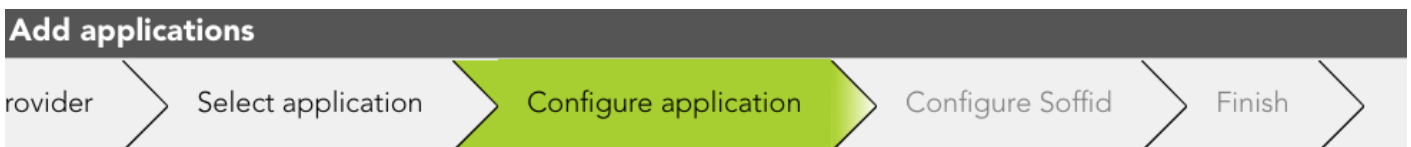
Implicit :	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
Authorization code :	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
User's password :	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
User's password + Client credentials :	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
Client id :	SLdmOb6XdNkvcqrkT8ziG6Sdo8Qw6UPel0Tbbj9/xaEbSAQI
Client secret :	****
Sector identifier URI :	Sector identifier URI
Response URL :	https://gbr.demo.soffid.net:4204

3.6. SAML 2.0 app:

3.6.1 Soffid will download the metadata XML file.



3.5.2 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>

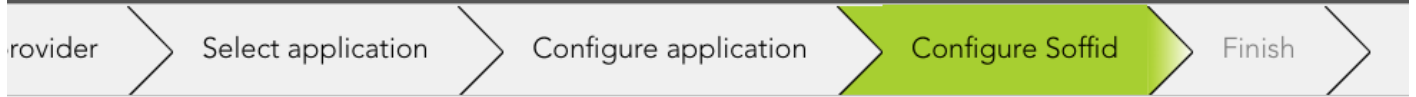
Next, download you application metadata from your application configuration web page.

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



3.5.3 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

Revision #16

Created 22 February 2023 13:59:20

Updated 12 February 2025 12:04:42