

How to deploy the identity & service provider

- [How to deploy the identity & service provider](#)
- [Change Password URL](#)
- [How to perform unsolicited login](#)

How to deploy the identity & service provider

Step-by-step

1. To deploy the identity provider is advisable to install a dedicated sync server. It can be configured as a proxy sync server as it does not need direct access to Soffid database. Instead, it will connect to main sync servers to get users and federation information. Also, you can deploy the identity provider in your existing sync.

To install a proxy sync server follow the instructions at the [Install sync server page](#).

2. If the installation is in a **dedicated Sync server**:

2.1. You need open the Sofid Console and approve the Task to accept the new Sync server.

Process	4149943	Soffid agent enrollment (Version 1.0.4)
Task	4149946	New sync server request
Task	Actions log	Attachments Comments
User	admin	
Name	Soffid	
Surname	Administrator	
Server name	iam-sync-IdP-2.soffidnet	
Server address	172.20.0.6	
Approve	<div>Select an action to do</div>	
Add comment	<div>Add comment</div>	

2.1. You need tune the **Sync server memory usage**.

Main Menu > Administration > Configure Soffid > Integration engine > Synchronization servers

Name :	iam-sync-IdP.soffidnet
URL :	https://iam-sync-IdP.soffidnet:1760/
Type :	Synchronization agent proxy ▼
Java options :	-Xmx512m

3. Once the Sync server is registered, if you want to create a **Soffid IdP** you must create a new **Identity Provider Agent**.

Main Menu > Administration > Configure Soffid > Integration engine > Agents

- **Type:** Soffid Identity Provider.
- **Server:** select the sync server that will host the identity provider.
- **Trust password:** must be unchecked.
- **Read only:** must be unchecked.
- **Manual account creation:** usually is unchecked, but could be useful to check it during initial tests.
- **Role based:** usually is unchecked, despite it could be used to limit the users that can use it.
- **Groups:** select the groups that can use it. Leave it blank to allow any user.
- **User domain:** use default users domain. Nevertheless, depending on your needs, creating another user domain could be a good option.
- **Password domain:** use default password domain.
- **User types:** check the user types that can use the identity provider.
- **Public ID:** enter the public ID assigned in the federation management page.

Your identity provider agent should look like this one:

Task engine mode: Automatic (each change is automatically sent to target systems)

Name: newIdP *

Alert: The accounts for this system should be re-evaluated. [Preview changes](#)

Description: New IdP

Type: Soffid Identity Provider Class:es.caib.seycon.idp.agent.IDPAgent

Server: iam-sync-IdP.soffidnet ▼

Shared Thread: III No Dedicated threads: 1

Task timeout (ms): Long task timeout (ms):

Trust passwords: III No

Read only: III No

Manual account creation: III No

Role-based: III No

Groups: +

User domain: Default user domain ▼ *

Passwords domain: Default password domain ▼ *

User Type

<input type="checkbox"/> User Type
<input checked="" type="checkbox"/> External user
<input checked="" type="checkbox"/> Internal user
<input type="checkbox"/> SSO account (USE IT)

Connector parameters:

Public ID: new-idp-public-IdP (Must match the public ID defined in Federation)

4. Upload the **Federation addon** to the Soffid Console:

To upload the addon follow the instructions at the [How to install Federation in Soffid page](#).

5. Once you are connected to the Soffid console, you can start creating an **Entity Group**.

5.1. First of all, open the **Identity & Service providers** page

Main Menu > Administration > Configure Soffid > Web SSO > Identity & Service providers

5.2. Then, click the "Add group" button and Soffid will display a new window to fill in the **Entity group** attributes.

5.3. Once you fill in the fields, you need to save (disk button) or apply changes (Apply changes button) to save the data.

When the Entity Group is created, inside there will be two options, one to create the Identity Providers and other to create the Service Providers.

Entity Group :

Url Metatada :

<input type="checkbox"/>	Providers
	Filter
<input type="checkbox"/>	Identity Providers
<input type="checkbox"/>	Service Providers

Displayed rows: 2

5.3.1. Clicking on the Identity Providers record a identity providers list will be displayed and it will be able to create new identity providers. To create a new Identity Provider continue on step 5rd.

5.3.2. Clicking on the Service Providers record a service provider list will be displayed and it will be able to create new service providers. To create a new Service Provider continue on step 6th.

6. New Identity Provider:

6.1. To create a new Identity Provider you can click on the "Add identity provider" button on the tree view, or click the add button (+) on the Identity Provider list. Then Soffid will display a new window.

6.2. At the new window you must select the IdP type you want to create and fill in the required fields. The fields to full fill depend on the IdP type selected.

- You can visit the [Identity Provider page](#) for more detail.

6.2.1. When creating a Soffid identity provider, it will be mandatory to create an agent. The agent will have to be a Soffid Identity Provider agent. On the connector parameters you must define a unique *Public ID* which will be used on the Identity Provider configuration.

Connector parameters:

Public ID

(Must match the public ID defined in Federation)

6.3. Once you fill in all the data, you need to enable the proper profiles by clicking on the profile list and configuring them.

- You can fin more information visiting the [Profile page](#) where the available protocols are defined.

6.4. Finally, you need to save (disk button) or apply changes (Apply changes button) to save the data.

Note that in some cases it will be necessary to **restart the synchronization server**, so Soffid will generate the additional metadata or certificate data needed.

Note that you may have to **open the standard port**.

Soffid Identity Provider Screenshot

Identification

IdP type :	Soffid IdP
Identifier :	idp003
Name :	Soffid IdP
Organization :	Soffid
Contact :	pgarcia@soffid.com

Network

Host Name :	iam-sync-35.soffidnet
Standard port :	1443
TLS PublicKey	Missing key Generates public / private key Upload PKCS12 file
Client certificate header :	Client certificate header
TLS Certificate chain :	TLS Certificate chain

Session management

Session timeout (secs) :	Session timeout (secs)
oAuth Session timeout (secs) :	oAuth Session timeout (secs)
Maximum session duration (secs) :	Maximum session duration (secs)
SSO Cookie name :	soffid_sso_session
SSO Cookie domain :	SSO Cookie domain

Advanced authentication

Allow user to recover passwords :	Yes No
Allow users to self-register :	Yes No
Registration process :	
Register identities identified by external IDPs :	Yes No
Store last user name in browser :	Yes No
Enable reCaptcha v3 service :	Yes No

Look and feel

CSS Style :	CSS Style
Html header :	Html header
Html footer :	Html footer

Service configuration

Metadata :	<pre><EntityDescriptor entityID="idp003" xmlns="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"> <IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:1.1:protocol urn:oasis:names:tc:SAML:2.0:protocol"></pre>
------------	---

SAML Security

PublicKey	Change public / private key Delete public / private key Generate PKCS10
Certificate chain :	-----BEGIN CERTIFICATE----- MIIB+TCCAwwKAwIBAgIGAYnj+SrAMAA0GCSqGSIb3DQEBCwUAMEAxZzANBgNVBAMM

Authentication

Always ask for credentials :	Yes No																																																																																																																									
Authentication methods	<table><tr><th>First auth</th><th>Password</th><th>Kerberos</th><th>External</th><th>OTP</th><th>Email</th><th>SMS</th><th>PIN</th><th>Certifica</th><th>FIDO</th><th>Push</th></tr><tr><td>Password</td><td><input checked="" type="checkbox"/></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>Kerberos</td><td></td><td><input type="checkbox"/></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>External</td><td></td><td></td><td><input type="checkbox"/></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>OTP</td><td></td><td></td><td></td><td><input type="checkbox"/></td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>Email</td><td></td><td></td><td></td><td></td><td><input type="checkbox"/></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>SMS</td><td></td><td></td><td></td><td></td><td></td><td><input type="checkbox"/></td><td></td><td></td><td></td><td></td></tr><tr><td>PIN</td><td></td><td></td><td></td><td></td><td></td><td></td><td><input type="checkbox"/></td><td></td><td></td><td></td></tr><tr><td>Certificat</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td><input type="checkbox"/></td><td></td><td></td></tr><tr><td>FIDO</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td><input type="checkbox"/></td><td></td></tr><tr><td>Push</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td><input type="checkbox"/></td></tr></table>	First auth	Password	Kerberos	External	OTP	Email	SMS	PIN	Certifica	FIDO	Push	Password	<input checked="" type="checkbox"/>										Kerberos		<input type="checkbox"/>									External			<input type="checkbox"/>								OTP				<input type="checkbox"/>							Email					<input type="checkbox"/>						SMS						<input type="checkbox"/>					PIN							<input type="checkbox"/>				Certificat								<input type="checkbox"/>			FIDO									<input type="checkbox"/>		Push										<input type="checkbox"/>
First auth	Password	Kerberos	External	OTP	Email	SMS	PIN	Certifica	FIDO	Push																																																																																																																
Password	<input checked="" type="checkbox"/>																																																																																																																									
Kerberos		<input type="checkbox"/>																																																																																																																								
External			<input type="checkbox"/>																																																																																																																							
OTP				<input type="checkbox"/>																																																																																																																						
Email					<input type="checkbox"/>																																																																																																																					
SMS						<input type="checkbox"/>																																																																																																																				
PIN							<input type="checkbox"/>																																																																																																																			
Certificat								<input type="checkbox"/>																																																																																																																		
FIDO									<input type="checkbox"/>																																																																																																																	
Push										<input type="checkbox"/>																																																																																																																

Kerberos Domain	Adaptive authentication...	
Kerberos Domain	Principal name	Description
Filter	Filter	Filter

Displayed rows: 0

Profiles

Name
Filter
GasProfile
OpenidProfile
RadiusProfile
SAML1ArtifactResolutionProfile
SAML1AttributeQueryProfile
SAML2ArtifactResolutionProfile
SAML2AttributeQueryProfile
SAML2ECPPProfile
SAML2SSOProfile
Tacacs+Profile

Displayed rows: 10

[Undo](#) [Apply changes](#)

You could check your Identity Provider

```
https://<YOUR_SYNCSEVER_HOSTNAME>:1443/protected
```

For instance: `https://iam-sync-idp.soffidnet:1443/protected`

You could view your IdP metadata

```
https://<YOUR_SYNCSEVER_HOSTNAME>:1443/SAML/metadata.xml
```

For instance: `https://iam-sync-idp.soffidnet:1443/SAML/metadata.xml`

In addition, the complete metadata of soffid

```
https://<YOUR_SYNCSEVER_PRINCIPAL>:1760/SAML/metadata.xml
```

For instance: `https://iam-sync.soffidnet:1760/SAML/metadata.xml`

7. New **Service Provider**:

7.1. To create a new Service Provider you can click on the "Add service provider" button on the tree view, or click the add button (+) on the Service Provider list. Then Soffid will display a new window.

7.2. At the new window you must select the Service provider type you want to create and fill in the required fields. The fields to full fill depend on the IdP type.

- You can visit the [Service Provider page](#) for more detail.

7.3. One you fill in all the data, you need to save (disk button) or apply changes (Apply changes button) to save the data.

SAML Service Provider Screenshot

Identification

Type :

publicID :

Name :

Service configuration

Metadata :

```
<!-- This is the metadata for the SAMLtest SP, named by entityID -->

<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" ID="SAMLtestSP" valid
Until="2100-01-01T00:00:42Z" entityID="https://samitest.id/saml/sp">

<!-- This list enumerates the cryptographic algorithms acceptable to this SP -->
<md:Extensions xmlns:alg="urn:oasis:names:tc:SAML:metadata:alg:support">
<alg:DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#sha512"/>
<alg:DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#sha384"/>
<alg:DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#sha256"/>
<alg:DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#sha224"/>
<alg:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<alg:SigningMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha512"/>
```

Login rules

Allow impersonations :

UID Script :

Ask for consent :

Roles required to login :

System where an enabled account is required :

OpenID Connect Service Provider Screenshot

Identification

Type :

publicID :

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 :

Response URL :

oAuth Session timeout (secs) :

Allowed scopes

Scope name	Required roles
Filter	Filter
<input type="checkbox"/> api.person.read	
<input type="checkbox"/> api.person.write	
<input type="checkbox"/> openid	

Displayed rows: 3

8. Enable, when it will be necessary, the External SAML identity provider. To do that you need to access to the Authentication page:

Main Menu > Administration > Configure Soffid > Security settings > Authentication

External SAML identity provider

Enabled

Soffid server host name:

SAML federation metadata URL:

Cache limit (seconds):

Identity provider:


You can visit the [Authentication page](#) for more information.

Change Password URL


There is a service point to allow users change their passwords. Simply redirect the user to:

`https://<YOUR_SYNC_SERVER_HOSTNAME>:1443/protected/passwordChange`

For instance: <https://iam-sync-idp.soffidnet:1443/protected/passwordChange>

 **Image**

English Español Català



Password change

Please, enter a new password to proceed. Mind the listed complexity requirements to be met.

User name: pgarcia

Current password:

New password:

New password (again):

Login

The password will be valid for 365 days past change

The user will be required to enter identify itself and enter a new password. Optionally, you can enter a web page to return after password change is complete:

[https://**servername:port**/protected/changePassword?return=**URL**](https://servername:port/protected/changePassword?return=URL)

How to perform unsolicited login

Soffid Identity Provider supports unsolicited login (Idp initiated login) profile. In order to enable it, you must be sure that federation metadata for the target service provider allows it. It is configured using the AuthnRequestsSigned attribute of the SPSSODescriptor tag:

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" ID="...." entityID="...Service Provider Public ID...">  
  <md:SPSSODescriptor AuthnRequestsSigned="0"  
    protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
```

Once it is enabled, you can access to:

<https://IdentityProvider:port/profile/SAML2/Unsolicited/SSO?providerId=<ServiceProviderPublicID>>

Now, you will be requested to show your credentials. If they are valid, you will be redirected to the service provider initial page.

Another way to achieve the same functionality when the service provider is Shibboleth, is to send the request directly to the service provider. This approach has an additional advantage, as you can specify which URL must be served by the service provider.

<https://ServiceProvider:port/Shibboleth.sso/Login?target=TargetURL>