

# Authentication

## Definition

Soffid could use different kinds of external authentication sources. These mechanisms could be selectively enabled or disabled.

## Screen overview



[Main Menu](#) > [Administration](#) > [Configuration](#) > [Security settings](#) > Authentication

### Global status

No Maintenance mode (only administrators can log in)  
Message to display before logging in:   
Session timeout in minutes:

### Username and password

Yes Enabled  
  No Forward authentication requests to trusted target systems

### External SAML identity provider

No Enabled  
Soffid server host name:   
SAML federation metadata URL:   
Cache limit (seconds):   
Identity provider:    
SAML attribute containing user name:   
  No Enable SAML debug log

## Webservice authentication

Yes  No User name and password

Yes  No JWT token

JWT configuration URL:

https://sync-server.netcompose:1443/.well-known/jwks.json

JWT Issuer:

https://sync-server.netcompose:1443

JWT Audience:

angularApp

## Enable LinOTP integration

Yes  No Enabled

LinOTP server URL:

LinOTP admin user:

LinOTP admin password:

LinOTP users domain:

- select -

## 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.

Download metadata

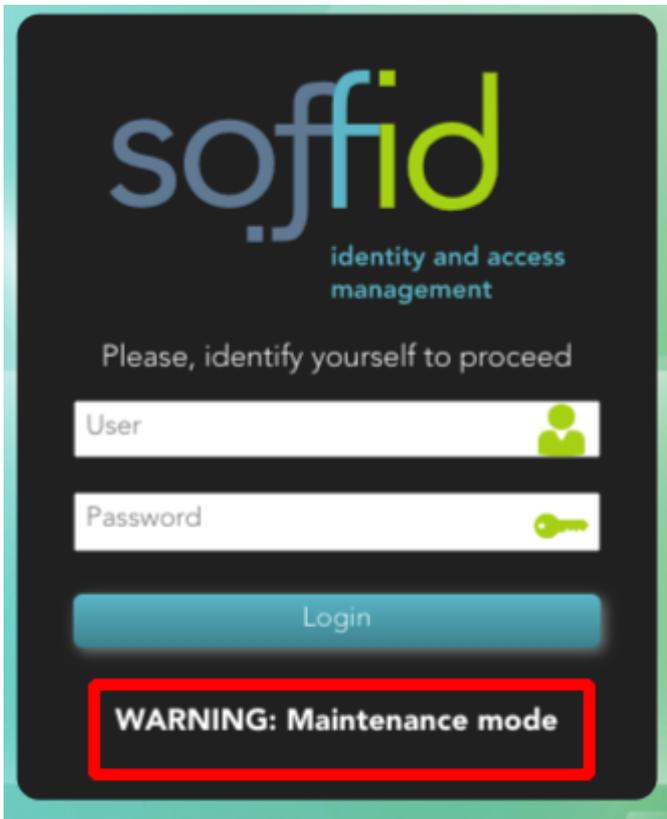
Confirm changes

# Standard attributes

## Global status

- **Maintenance mode (only administrators can log in):** if this option is checked (value is Yes), only the administrators could connect to Soffid Console.

 Image

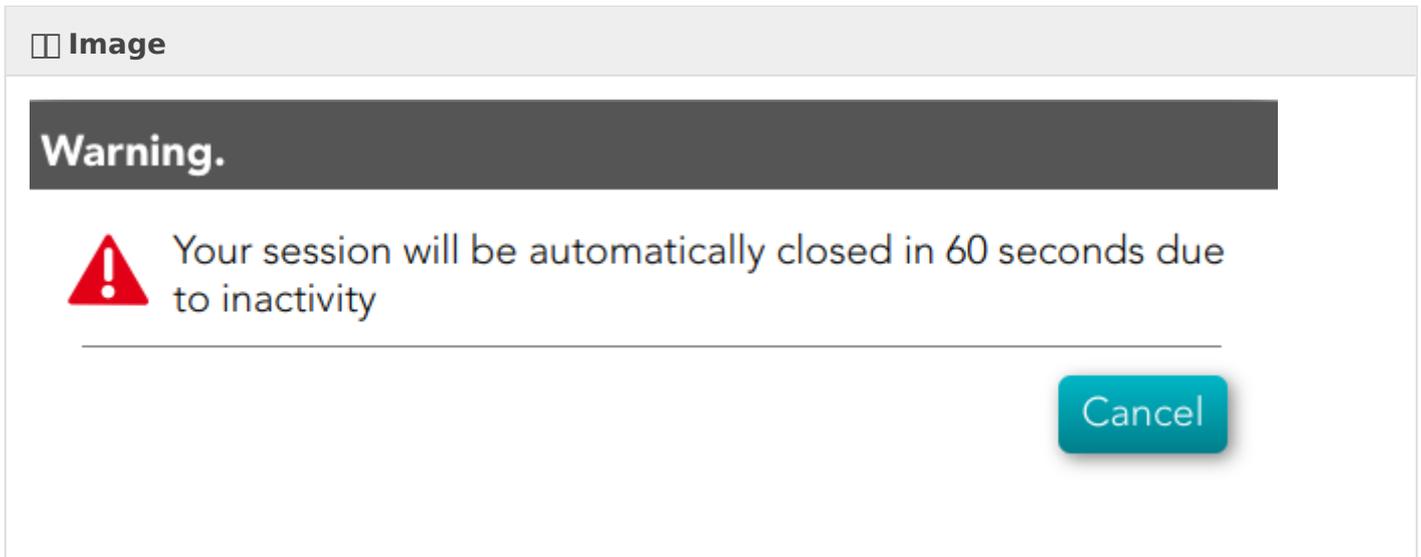


- **Message to display before logging in:** administrators can configure a banner that will be displayed before the user logging in. This banner will display security advice.

#### ☐ Image



- **Session timeout in minutes:** time in seconds it takes for the console to display the message indicating that the session is being closed. If nothing is indicated, the session does not expire. (Available since console version 3.5.26)



# Username and password

## Internal

- **Enabled:** the only one enabled by default in the installation of Soffid. It is the internal username and password authentication mechanism. Therefore, the authentication is made with the username and password of the soffid account.

## External

- **Forward authentication requests to trusted target systems:** to use external username and password sources. Therefore, the authentication is made with the username and password of an account of an external system.

Not all the external systems are included, only the ones that have marked the check "Trust password" on the agent. For more information about agents please visit the [Agents](#) page.

Once an agent is configured, Soffid will still use its internal tables to authenticate usernames and passwords.

If the password entered by the user does not match, the Soffid core will issue a "ValidatePassword" task for each trusted target system. If any of the trusted target systems accepts the password, it will be hashed and stored in Soffid tables and login will be accepted.

# External SAML identity provider

It should be noted this feature does not depend on the federation addon. That is a feature included by default in the Soffid smart engine to allow you to include in the authentication flow a

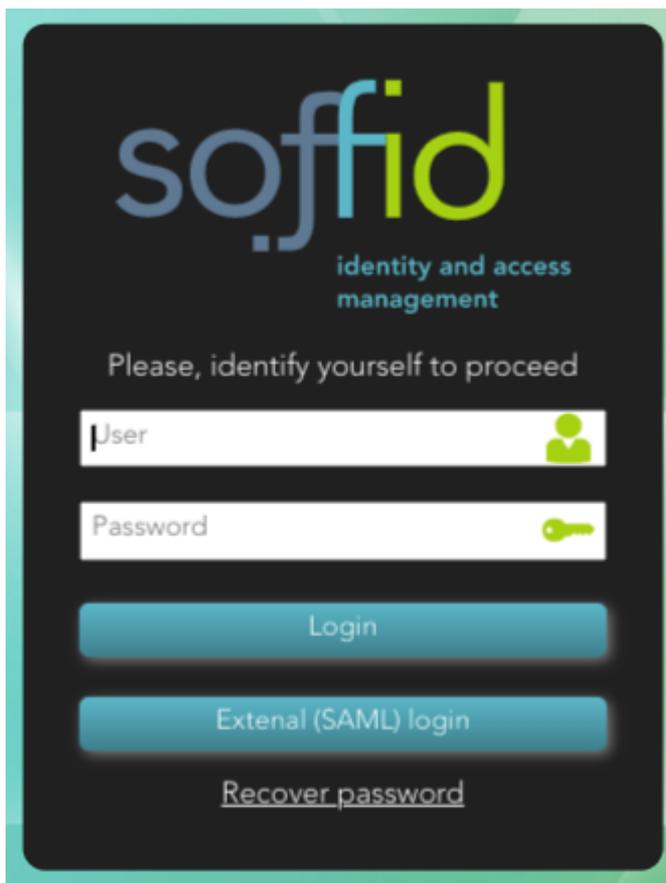
mechanism to use a third-party SAML system.

- **Enable:** check it (select value Yes) to use an external SAML Identity Provider.
- **Soffid Server host name:** the URL that will be used by external IdP. This URL will be resolved by end user's browser in order to send the SAML assertion.
- **SAML federation metadata:** the URL where federation information can be found. If the Soffid console can fetch federation metadata, the Identity provider drop-down will be filled in with any identity provider found in the federation metadata URL.
- **Cache limit (seconds):** how often the federation information will be refreshed. By default, 10 minutes will be taken.
- **Identity provider:** Identity Provider to use for authentication.

Finally, download the Soffid Console and load it into your SAML Identity Provider federation.

If SAML Identity Provider is enabled, as well as username and password, the user will have the chance to select the preferred authentication method. Otherwise, if only SAML is enabled, the user will be automatically redirected to SAML Identity Provider.

#### Image

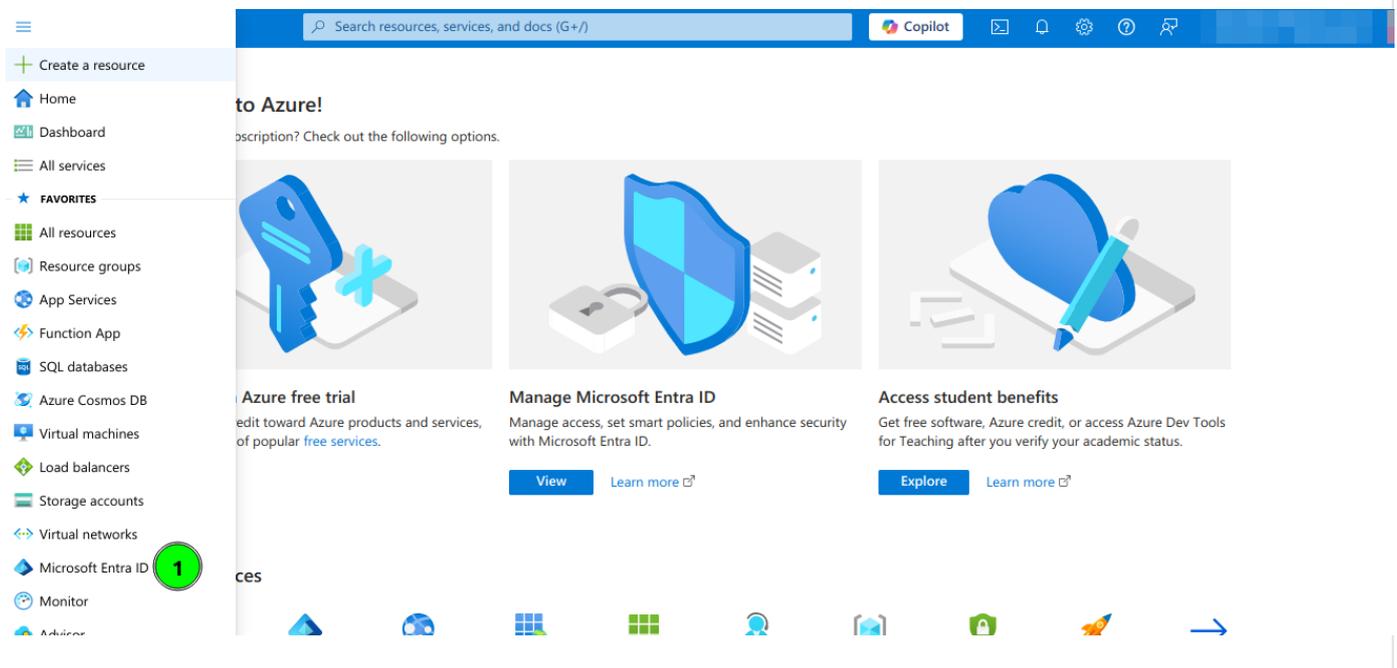


# Introduction

Steps to configure Office 365 as External SAML identity provider.

## Step-by-Step

1. Open a <https://portal.azure.com>
2. Open **Microsoft Entra ID** and then select **Enterprise applications** option



Microsoft Azure Search resources, services, and docs (G+)

Home > Soffid IAM, S.L. | Overview

Overview | Monitoring | Properties | Recommendations | Setup guides

Search your tenant

**Basic information**

Name	Soffid IAM, S.L.	Users	10
Tenant ID	25bc9848-d3c2-423f-93f1-cf465332a68d	Groups	5
Primary domain	soffidcom.onmicrosoft.com	Applications	10
License	Microsoft Entra ID Free	Devices	1

**Alerts**

**Migrate to the converged Authentication methods policy**  
Please migrate your authentication methods off the legacy MFA and SSPR policies by September 2025 to avoid any service impact

Enterprise applications 1

### 3. Select **All applications** and click **New Application**

Microsoft Azure Search resources, services, and docs (G+)

Home > Enterprise applications

Enterprise applications | All applications

New application Refresh Download (Export) Preview info Columns Preview features Got feedback?

View, filter, and search applications in your organization that are set up to use your Microsoft Entra tenant as their Identity Provider.

The list of applications that are maintained by your organization are in [application registrations](#).

Search by application name or object ID Application type == Enterprise Applications Application ID starts with Add filters

11 applications found

Name	Object ID	Application ID	Homepage URL	Created on	Certificate Expir...	Active Certificat.
GE				/12/2020	-	-
S				0/23/2024	Current	10/23/2027
SC				/20/2020	-	-
O				/25/2022	-	-
				0/23/2024	-	-
PA				/29/2020	-	-
TS				1/28/2023	-	-
A				/10/2020	-	-

All applications 1

### 4. Select Create your own application

## Browse Microsoft Entra Gallery

**1** [+ Create your own application](#) | [Got feedback?](#)

The Microsoft Entra App Gallery is a catalog of thousands of apps that make it easy to deploy and configure single sign-on (SSO) and automated user provisioning. When deploying an app from the App Gallery, you leverage prebuilt templates to connect your users more securely to their apps. Browse or create your own application here. If you are wanting to publish an application you have developed into the Microsoft Entra Gallery for other organizations to discover and use, you can file a request using the process described in [this article](#).

Single Sign-on : All User Account Management : All Categories : All

### Cloud platforms

<p>Amazon Web Services (AWS)</p> 	<p>Google Cloud Platform</p> 	<p>Oracle</p> 
<p>SAP</p>		

**5.** Type the name of your app and select the "Integrate any other application you don't find in the gallery (Non-gallery)" option

# Create your own application



 Got feedback?

If you are developing your own application, using Application Proxy, or want to integrate an application that is not in the gallery, you can create your own application here.

What's the name of your app?

pat.soffid.lab



What are you looking to do with your application?

- Configure Application Proxy for secure remote access to an on-premises application
- Register an application to integrate with Microsoft Entra ID (App you're developing)
- Integrate any other application you don't find in the gallery (Non-gallery)

Create

6. Click on **Set up single sign on**

Microsoft Azure Search resources, services, and docs (G+)

Home > Enterprise applications | All applications > Browse Microsoft Entra Gallery >

# pat.soffid.lab | Overview

Enterprise Application

- Overview
- Deployment Plan
- Diagnose and solve problems
- Manage
  - Properties
  - Owners
  - Roles and administrators
  - Users and groups
  - Single sign-on
  - Provisioning
  - Application proxy
  - Self-service
  - Custom security attributes
- Security
- Activity

## Properties

Name: pat.soffid.lab

Application ID: 6bb554ed-b96d-4631-9204-...

Object ID: 76afac14-c10f-4dde-94f7-8d...

## Getting Started

- 1. Assign users and groups**  
Provide specific users and groups access to the applications  
[Assign users and groups](#)
- 2. Set up single sign on**  
Enable users to sign into their application using their Microsoft Entra credentials  
[Get started](#)
- 3. Provision User Accounts**
- 4. Conditional Access**

## 7. Click the **SAML** option

Microsoft Azure Search resources, services, and docs (G+)

Home > Enterprise applications | All applications > Browse Microsoft Entra Gallery > pat.soffid.lab

# pat.soffid.lab | Single sign-on

Enterprise Application

- Overview
- Deployment Plan
- Diagnose and solve problems
- Manage
  - Properties
  - Owners
  - Roles and administrators
  - Users and groups
  - Single sign-on**
  - Provisioning
  - Application proxy
  - Self-service
  - Custom security attributes
- Security
- Activity

Single sign-on (SSO) adds security and convenience when users sign on to applications in Microsoft Entra ID by enabling a user in your organization to sign in to every application they use with only one account. Once the user logs into an application, that credential is used for all the other applications they need access to. [Learn more.](#)

## Select a single sign-on method [Help me decide](#)

- Disabled**  
Single sign-on is not enabled. The user won't be able to launch the app from My Apps.
- SAML**  
Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.
- Password-based**  
Password storage and replay using a web browser extension or mobile app.
- Linked**  
Link to an application in My Apps and/or Office 365 application launcher.

## 8. Enter the **Basic SAML Configuration** and Save:

- **Identifier:** https://<YOUR-SERVER>/soffid-iam-console
- **Reply URL:** https://<YOUR-SERVER>/soffid/saml/log/post
- **Sign on URL:** https://<YOUR-SERVER>/soffid/
- **Logout URL:** https://<YOUR-SERVER>/soffid/saml/slo/post

Microsoft Azure Search resources, services, and docs (G+)

Home > Enterprise applications | All applications > soffid.pat.lab

## soffid.pat.lab | SAML-based Sign-on

Enterprise Application

Upload metadata file | Change single sign-on mode | Test this application | Got feedback?

- Overview
- Deployment Plan
- Diagnose and solve problems
- Manage
  - Properties
  - Owners
  - Roles and administrators
  - Users and groups
  - Single sign-on**
  - Provisioning
  - Application proxy
  - Self-service
  - Custom security attributes

### Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. [Learn more.](#)

Read the [configuration guide](#) for help integrating soffid.pat.lab.

**1** Basic SAML Configuration Edit

Identifier (Entity ID)	https://pat.soffid.lab:8443/soffid-iam-console
Reply URL (Assertion Consumer Service URL)	https://pat.soffid.lab:8443/soffid/saml/log/post
Sign on URL	https://pat.soffid.lab:8443/soffid/
Relay State (Optional)	Optional
Logout Url (Optional)	https://pat.soffid.lab:8443/soffid/saml/slo/post

**2** Attributes & Claims Edit

givenname	user.givenname
-----------	----------------

# Basic SAML Configuration



Save

Got feedback?

## Identifier (Entity ID) \* ⓘ

The unique ID that identifies your application to Microsoft Entra ID. This value must be unique across all applications in your Microsoft Entra tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.

	Default
<input type="text" value="https://pat.soffid.lab:8443/soffid-iam-console"/>	<input checked="" type="checkbox"/> ⓘ

[Add identifier](#)

## Reply URL (Assertion Consumer Service URL) \* ⓘ

The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.

	Index	Default
<input type="text" value="https://pat.soffid.lab:8443/soffid/saml/log/post"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/> ⓘ

[Add reply URL](#)

## Sign on URL (Optional)

Sign on URL is used if you would like to perform service provider-initiated single sign-on. This value is the sign-in page URL for your application. This field is unnecessary if you want to perform identity provider-initiated single sign-on.

## Relay State (Optional) ⓘ

The Relay State instructs the application where to redirect users after authentication is completed, and the value is typically a URI or URI path that takes users to a specific location within the application.

**9.** Configure **Attributes & Claims** and change the attributes and claims to send the mailnickname as the user identifier (nameid)

# soffid.pat.lab | SAML-based Sign-on

Enterprise Application

Upload metadata file Change single sign-on mode Test this application Got feedback?

- Overview
- Deployment Plan
- Diagnose and solve problems
- Manage
  - Properties
  - Owners
  - Roles and administrators
  - Users and groups
  - Single sign-on**
  - Provisioning
  - Application proxy
  - Self-service
  - Custom security attributes
- Security
- Activity
- Troubleshooting + Support

## Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. [Learn more.](#)

Read the [configuration guide](#) for help integrating soffid.pat.lab.

- ### Basic SAML Configuration

Identifier (Entity ID)	https://pat.soffid.lab:8443/soffid-iam-console
Reply URL (Assertion Consumer Service URL)	https://pat.soffid.lab:8443/soffid/saml/log/post
Sign on URL	https://pat.soffid.lab:8443/soffid/
Relay State (Optional)	Optional
Logout Url (Optional)	https://pat.soffid.lab:8443/soffid/saml/slo/post
- ### Attributes & Claims

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.mailnickname
- ### SAML Certificates

## Attributes & Claims

Add new claim Add a group claim Columns Got feedback?

### Required claim

Claim name	Type	Value
Unique User Identifier (Name ID)	SAML	user.mailnickname [nam... <span>⋮</span>

### Additional claims

Claim name	Type	Value
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailadd...	SAML	user.mail <span>⋮</span>
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	SAML	user.givenname <span>⋮</span>
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SAML	user.userprincipalname <span>⋮</span>
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	SAML	user.surname <span>⋮</span>

Advanced settings

## 10. Copy the App Federation Metadata Url

Microsoft Azure | Search resources, services, and docs (G+)

Home > soffid.pat.lab

### soffid.pat.lab | SAML-based Sign-on

Enterprise Application

Upload metadata file | Change single sign-on mode | Test this application | Got feedback?

- Overview
- Deployment Plan
- Diagnose and solve problems
- Manage
  - Properties
  - Owners
  - Roles and administrators
  - Users and groups
  - Single sign-on**
  - Provisioning
  - Application proxy
  - Self-service
  - Custom security attributes
- Security
- Activity
- Troubleshooting + Support

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.mailnickname

#### SAML Certificates

**Token signing certificate** Edit

Status	Active
Thumbprint	560B064826325CB89F0CE229BDBDEE3A20E64587
Expiration	10/23/2027, 4:14:18 PM
Notification Email	admin@soffidcom.onmicrosoft.com
App Federation Metadata Url	<a href="https://login.microsoftonline.com/25bc9848-d3c2-423f-93f1-cf465332a68d/">https://login.microsoftonline.com/25bc9848-d3c2-423f-93f1-cf465332a68d/</a> <span>1</span>
Certificate (Base64)	<a href="#">Download</a>
Certificate (Raw)	<a href="#">Download</a>
Federation Metadata XML	<a href="#">Download</a>

**Verification certificates (optional)** Edit

Required	No
Active	0
Expired	0

## 11. Configure the External SAML identity Provider in the Soffid Console Authentication page

soffid | Search

Main Menu > Administration > Configuration > Security settings > Authentication 1

### Global status

No Maintenance mode (only administrators can log in)

Message to display before logging in:

Session timeout in minutes:

### Username and password

Yes  Enabled

No Forward authentication requests to trusted target systems

### External SAML identity provider

Yes  Enabled 2

Soffid server host name:

SAML federation metadata URL:  3

Cache limit (seconds):

Identity provider:  4

SAML attribute containing user name:

No Enable SAML debug log

## 12. Optional, enable any user to login

# Webservice authentication

Soffid allows you to configure the way to verify the identity of a user or system accessing to the Soffid Web Service, to ensure that only authorized entities can interact with the service.

- **User name and password:** allows you to use user and password to access to the Soffid Web Service.
- **JWT token:** allows you to use JWT token to access to the Soffid Web Service.
  - **JWT configuration URL:** URL where the jwks.json are available to download.
  - **JWT Issuer:** identifies the principal that issued the JWT.
  - **JWT Audience:** identifies the recipients that the JWT is intended for.

Bear in mind that the Identity Provider needs to have enabled the OpenID profile.

Also, the Identity Provider cert must be in the Console cacerts.

### Webservice authentication

Yes  No User name and password

Yes  No JWT token

JWT configuration URL:

https://sync-server.netcompose:1443/.well-known/jwks.json

JWT Issuer:

https://sync-server.netcompose:1443

JWT Audience:

angularApp

## Enable LinOTP integration

Soffid allows you to use an external OTP, LinOTP in this case. If you decide to use LinOTP, Soffid could be configured to request the user to authenticate using a second factor authentication to perform certain actions. In another case, you can use the Soffid OTP.

- **Enabled:** check it (select value Yes) to use an external SAML Identity Provider.
- **LinOTP server URL:** URL of your LINOTP service.
- **LinOTP admin username:** username of the admin account used by Soffid.
- **LinOTP admin password:** password of the admin account used by Soffid.
- **LinOTP users domain:** the user's domain for LinOTP authentication. The selected user domain will guess the LinOTP username for any Soffid identity. It is extremely important when LinOTP users do not match Soffid usernames. Please visit the [Account naming rules](#) page for more information

If you want to configure the **Soffid OTP** you could visit [Two factor authentication \(2FA\)](#) chapter.

## Second Factor Authentication configuration

- **Pages that optionally require OTP authentication for users with an enabled token:** (Optional) If a URL optionally requires OTP authentication, and the user does not have any OTP token, access will be granted. Otherwise, if the user has an OTP token, the OTP value will be required, and no access will be allowed until the user provides the right token value.
  - You can include the list of pages to include the two factors only for the users with the token.

### ☐ Example

Request only the OTP for these pages:

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

```
/resource/user/user.zul  
/resource/account/account.zul
```

- ○ You can add a regular expression to determine the list of pages to always include the second factor to the users with the token

### ☐ Example

Request OTP for all pages except those containing menu.zul or otp.zul:

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

```
(?!((.*menu.zul.*)|(.*otp.zul.*))).*
```

- **Pages that require OTP authentication to any user:** (Mandatory) You should include the list of pages to always include the second factor to the users with the token. Therefore, if a URL strictly requires OTP authentication, users with no token won't be allowed to use them.

### ☐ Example

## 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.

- **Second factor authentication period:** number of seconds after that, a new OTP value will be required.

In both configurations, if OTP is required by the user, a popup requesting the token value is raised to write the OTP value.

# Actions

<b>Download metada</b>	Allows you to download an XML file with metadata to load it into your SAML Identity Provider federation when you use an External SAML identity provider
<b>Confirm changes</b>	Allows you to save the changes made in the Authentication setup.

Revision #33

Created 18 May 2021 14:12:45 by pgarcia@soffid.com

Updated 23 October 2024 15:50:40 by pgarcia@soffid.com