

## Configure Single Sign-On with Salesforce

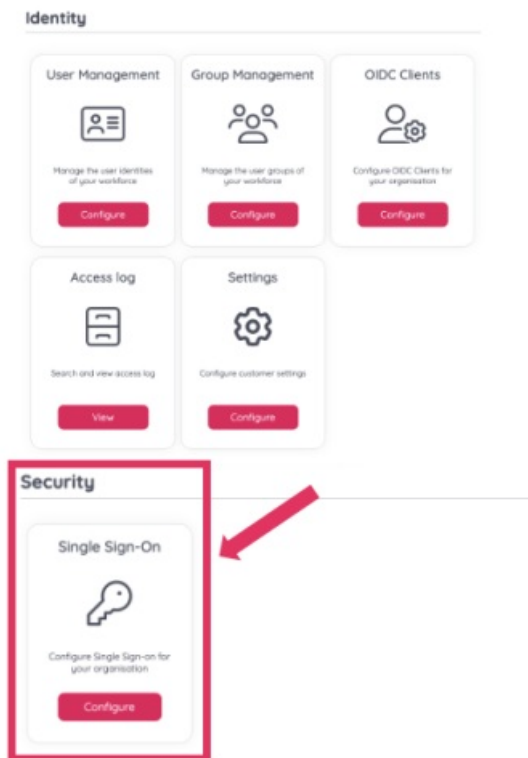
This article describes how to configure single sign-on (SSO) to Puzzel using Salesforce as an external provider.

This method utilizes Open IDConnect, see also: [Integrate Service Providers as Connected Apps with OpenID Connect](#) for more information.

### Step 1 : Create a new SSO Connection in Organisation settings portal

Start by creating a new Single Sign-on connection in the Organisation Settings portal to get the redirect URIs you need in the Connected App in Salesforce.

From the Organisation Settings home page, click on the “Single Sign-On” icon as shown below:



Depending on whether you have added SSO configurations previously or not you should either see a list of current configurations or just an empty list, either way you should also have the “Add” button displayed on the top right.

Click on the “Add” button and choose “OIDC” as illustrated below:


# Organisation Settings puzzel.

Home ↺

### Single Sign-on

+ Add

Enabled	Display name	Type	Tenant	
<input type="checkbox"/>	Puzzel IO (OIDC)	OIDC		<span>↗</span> <span>🗑️</span>
<input type="checkbox"/>	Salesforce Puzzel DEV	OIDC	puzzel.com	<span>↗</span> <span>🗑️</span>
<input type="checkbox"/>	Multi-tenant login with puzzel.io tena...	OIDC		<span>↗</span>



On the next screen you will be presented with two fields which you need to add to your Salesforce configuration, "Redirect URI" and "Front-channel logout URL". See screenshot below:

### Organisation Settings puzzel.

Home ↺

Display name  Type

Scheme

**Redirect URI**

Front-channel logout URL

Tenant

Authority


Client id  Client secret

External id claim  Response type

Scopes  Authorized Azure Tenant Ids

Get claims from UserInfo endpoint  Use PKCE

Disabled  Enabled  Cancel Save



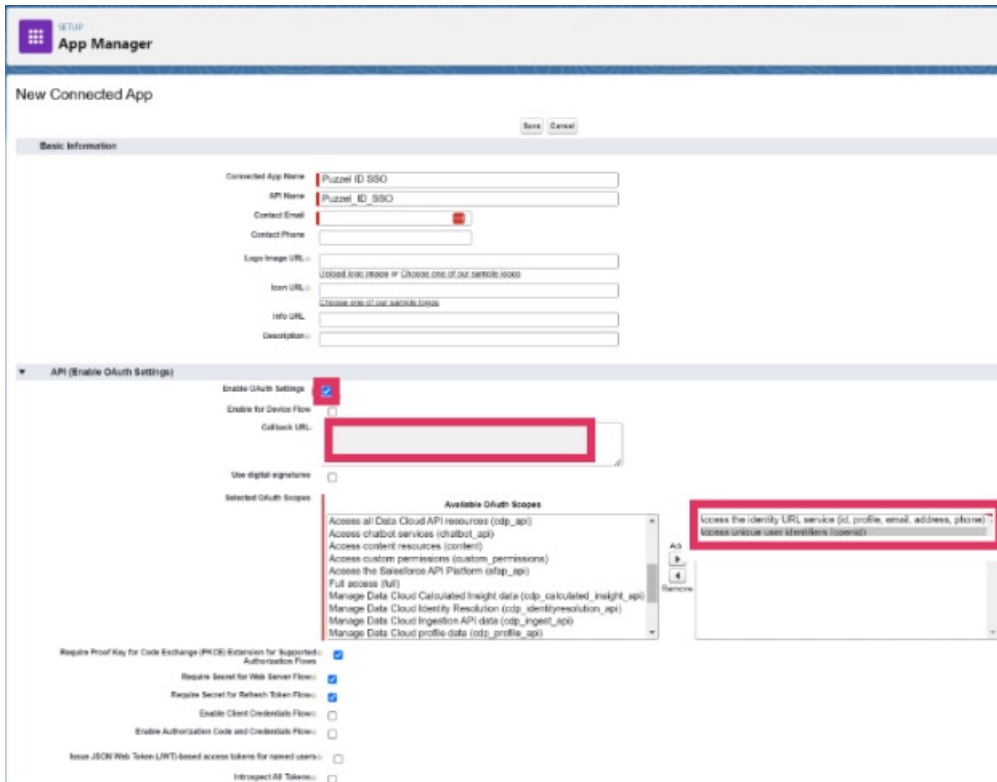
## Step 2: Create a new Salesforce Connected App and add initial config

From Setup, enter Apps in the Quick Find box, and select App Manager.

Click “New Connected App”.

Enter the connected app’s name, which displays in the App Manager and on its App Launcher tile. The connected app name must be unique within your organisation.

Enter the API name used when referring to your app from a program. It defaults to a version of the name without spaces. Only letters, numbers, and underscores are allowed, so if the original app name contains any other characters, edit the default name.



Check “Enable OAuth Settings”

Add Redirect URI from Puzzel ID Organisation Settings (see step 1) to “Callback URL”

Add the two scopes shown in the screenshot above in “Selected OAuth Scopes”.

The scope “Access the identity URL service (id, profile, email, address, phone)” is for sending the e-mail to match the user in Puzzel ID. You could use other claims to match the user as well, like the “sub” claim, and then this scope would not be needed.

Click the “Save” button on top of the screen.

### Step 3: Configure details in Puzzel ID

Once Saved, you need to fetch the consumer details to configure in Puzzel ID.

**SETUP** Manage Connected Apps

Connected App Name  
**Puzzel ID SSO**

[« Back to List: Custom Apps](#)

[Edit](#) [Delete](#) [Manage](#)

Changes can take up to 10 minutes to take effect. Deleting a parent org also deletes all connected apps with OAuth settings enabled.

Version	1.0
API Name	
Created Date	
Contact Email	
Contact Phone	
Last Modified Date	
Description	
Info URL	

▼ API (Enable OAuth Settings)

Consumer Key and Secret	<a href="#">Manage Consumer Details</a>
Selected OAuth Scopes	Access the identity URL service (id, profile, email, address, phone) Access unique user identifiers (openid)
Callback URL	https://app.puzzel.com/identity/oauth2/callback/?response_type=code&state=...

Connected App Name  
**Puzzel ID SSO**

[« Back to Manage Connected Apps](#)

**Consumer Details**

Consumer Key	[REDACTED]	<a href="#">Copy</a>
Consumer Secret	[REDACTED]	<a href="#">Copy</a>

**Staged Consumer Details**

Generate staged values for the consumer key and secret. When you apply the staged values, they replace the original consumer details.

Staged Consumer Key	Not generated
Staged Consumer Secret	Not generated

[Generate](#) [Apply](#) [Cancel](#)

Configure the Single Sign-on client in Puzzel ID Organisation Settings with values from Salesforce:

Organisation Settings **puzzel.**

Home

Display name  Type

Scheme

Redirect URI

Front-channel logout URL

Tenant

Authority

Client id  Client secret

External id claim  Response type

Scopes

Get claims from UserInfo endpoint  Use PKCE

Disabled

- In the field “Authority” enter the URL to your Salesforce tenant
- Copy the “Consumer Key” in Salesforce to “Client id”
- Copy the “Consumer Secret” in Salesforce to “Client secret”

Continuing in same form as in the previous step, the field “External id claim” requires special attention. Here you need to provide a valid Salesforce claim that will be used to map the user to Puzzel ID.

The easiest path is to set the External id claim to **email** (can also be i.e. **sub**).

### Note

When using the “email” claim here all users that are to use this SSO configuration needs to set email in their externalid field as shown below:

Organisation Settings **puzzel.**

Home Current customer: 1000 - Agent Team: 0100

### Basic information

First Name

Middle Name

Last Name

Mobile

Email \*

Puzzel ID \*

Time zone

Preferred language \*

External id

Role(s)

Cancel Save

For more information about external id see: [Validate users using external id](#).

## Step 5 - Save and enable the configuration

Still in the same form as in the previous step, make sure to toggle the configuration to “Enabled” if you wish to start using the configuration right away.

Click “Save” to store your configuration.

## Step 6 - Optional - Change scheme name

This is an optional step to improve readability when referring to a SSO configuration. It can be skipped if you just want to use the default GUID based scheme value or don't want to use the “idp=” query parameter at all.

You can use the “Scheme” value for a SSO configuration as the “idp” parameter for the agent. This is described in the section **“Accessing external providers directly”** in [this](#) article.

If you do not change the Scheme name it will use the default GUID for the scheme, as an example: `https://devapp.puzzel.com/agent/?idp=42bd9bd8-1486-4f05-ba7a-xxxxxxxxxxxxxxxx`.

To change the “Scheme” from the generated id to a readable name, you can edit the “Scheme” field as shown below and click save:

**Organisation Settings** **puzzel.**

Home | Current customer: [View](#) | [Logout](#) | [Team view](#)

---

Display name

Type

Scheme

Redirect URI

Front-channel logout URL

Tenant

Authority

Client id

Client secret

External id claim

Response type

Scopes

Authorized Azure Tenant Id's

Get claims from UserInfo endpoint  Use PKCE

Disabled  Enabled

**Note**

After you have saved the new scheme name, reopen the SSO configuration and note that the “Redirect URI” has now changed, and must be updated in the Connected App in Salesforce:

**App Manager**

**New Connected App**

Save | Cancel

**Basic Information**

Connected App Name

API Name

Contact Email

Contact Phone

Logo Image URL

Icon URL

Info URL

Description

**API (Enable OAuth Settings)**

Enable OAuth Settings

Enable for Device Flow

Callback URL

Use digital signatures

**Selected OAuth Scopes**

**Available OAuth Scopes**

- Access all Data Cloud API resources (cdp\_all)
- Access chatbot services (chatbot\_api)
- Access content resources (content)
- Access custom permissions (custom\_permissions)
- Access the Salesforce API Platform (sfapi\_api)
- Full access (full)
- Manage Data Cloud Calculated Insight data (cdp\_calculated\_insight\_api)
- Manage Data Cloud Identity Resolution (cdp\_identityresolution\_api)
- Manage Data Cloud Ingestion API data (cdp\_ingest\_api)
- Manage Data Cloud profile data (cdp\_profile\_api)

Access the identity URL service (id\_profile\_email\_address\_phone)  Access unique user identifiers (oidc)

Require Proof Key for Code Exchange (PKCE) Extension for supported Authorization Flows

Require Secret for Web Server Flows

Require Secret for Refresh Token Flows

Enable Client Credentials Flow

Enable Authorization Code and Credentials Flow

Issue JSON Web Tokens (JWT)-based access tokens for named users

Introspect All Tokens

The new “idp” parameter for the agent is now: <https://devapp.puzzel.com/agent/?idp=salesforce-devpuzzel>

### Step 7: Changing agentUrl setting

Finally you will have to change the “agentUrl” setting under “Additional Information” in SETUP.

The “agentUrl” value needs to be changed referring to a SSO connection within Puzzel ID using the “idp” parameter as explained in the previous step.

