Configuring Single Sign-On

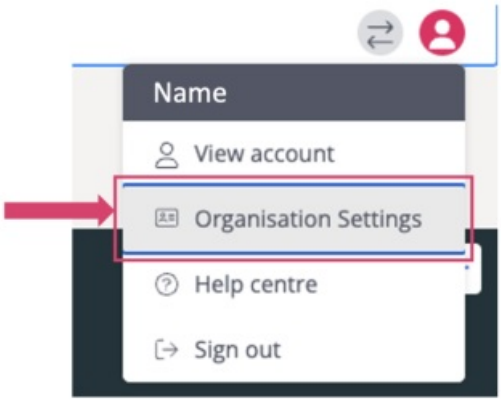
This article details how to configure single sign-on (SSO) to Puzzel using an external identity provider such as Entra ID (Azure AD), ADFS or Google Workspace.

Before you begin

There are a few things that need to be verified before starting the process of single sign-on configuration.

Access to Organisation Settings portal

To configure SSO, you must specify information about your Identity Provider using the “Single Sign-On” section in the Organisation Settings portal. All users with the role of “admin” or “sysadmin” should be able to see the “Organisation Settings” menu option from the Puzzel top bar:



If you don’t see this menu option, and you are a customer administrator, please contact your company’s Puzzel solution owner which should be able to give your user the needed access role. Alternatively reach out to Puzzel support if you are unable to resolve the access issues locally.

Access to your Identity Provider

You must have an existing OIDC or SAML identity provider (IdP) such as Azure AD or Google Workspace. Work with your IdP administrator to gather the necessary information depending on your Identity Provider.

As mentioned above, you also need a user with access to the Organsation Settings portal.

Using Single Sign-On in Puzzel ID

After Single Sign-On (SSO) has been configured and enabled with Puzzel ID there are two options of accessing the Puzzel applications via the SSO configuration:

1. Typing your username in the Puzzel login screen and clicking “Next” will automatically detect the SSO configuration and redirect to the external provider sign-in process.

2. Referring to the SSO provider as a query parameter (idp=) will take you directly to the external provider sign-in. Currently this only works for the Puzzel PCC Agent application (https://app.puzzel.com/agent).

See the chapter on “Accessing external providers directly” for more information.

Configuring SSO Provider

To set up SSO with Puzzel ID please follow one the below guides, then come back to this article to learn more about external id and how to access the configured external provider directly.

- Configure SSO with Entra ID (previously Azure AD)
- Configure SSO with Salesforce

Validate users using external id

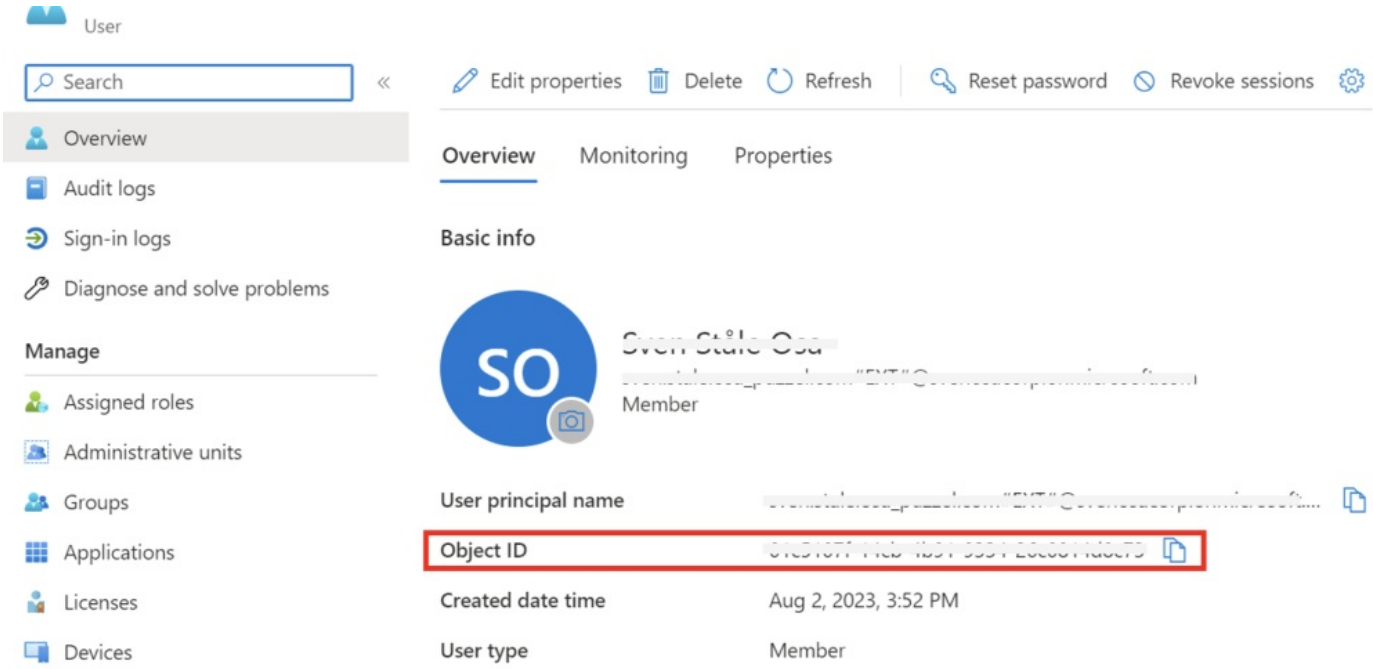
The Puzzel ID system will need to validate the presence of the specified claim and its value using the “External id claim” field in SSO configuration (which claim to use) and the “External id“ field (claim value) for a given user.

This chapter gives an example of how to do this using Azure AD “Object ID” (oid) as external id claim. An easier, but in some cases, less secure way is to use email as claim. In this case it is just a matter of using our feature of copying email to externalid to accomplish this.

> Note
>
> Note that even though we show below how to manually link between Azure AD and Puzzel external ID, populating the external ID field in Puzzel ID should preferably be done using bulk import or through Azure AD synchronisation. If you have a smaller organisation without too many users this can of course also be done manually, but the intention of the next steps is to explain the relation between what you add as “External ID claim” in the SSO configuration, Azure AD and the external ID field for a Puzzel ID user.

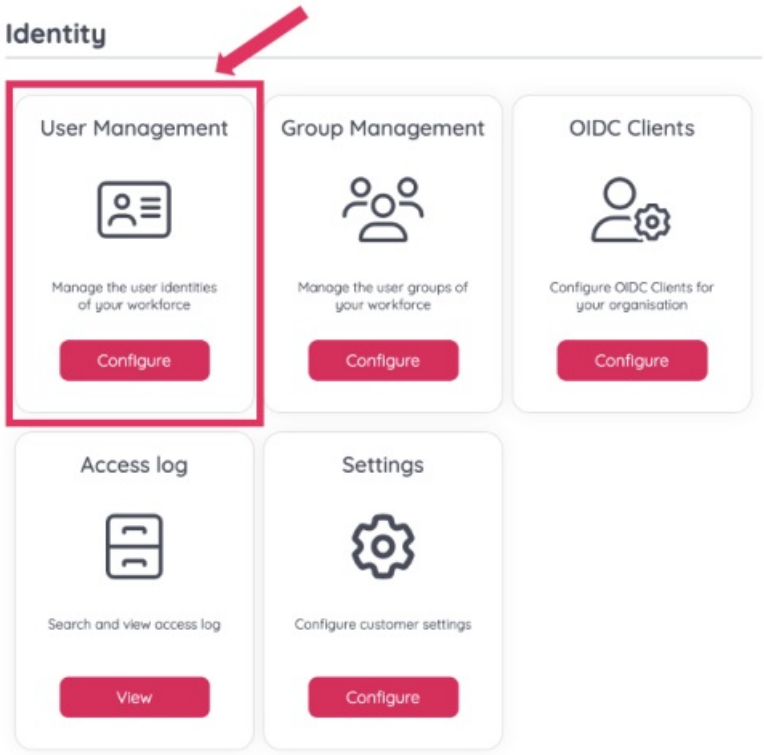
Example: Using oid as external id claim

Navigate to the “Users” section of Azure AD, choose a user to be used with Puzzel and click “Overview”. The oid can be found here as “Object ID” as shown below:

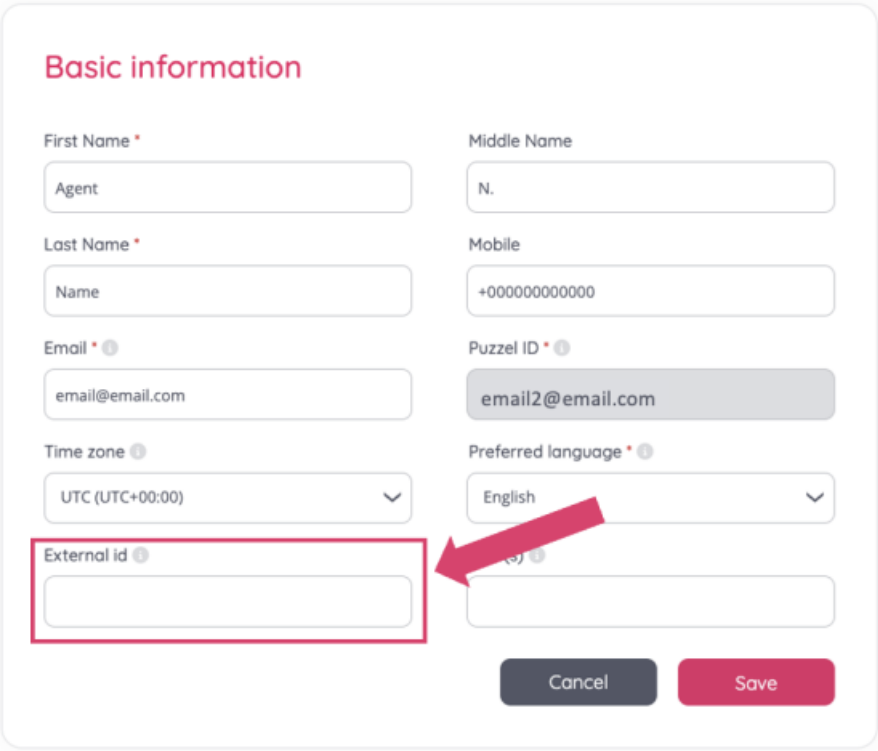


Copy the value of “Object ID” and switch back to the Organisation Settings webpage.

Navigate to the Identity - User Management section as shown below:



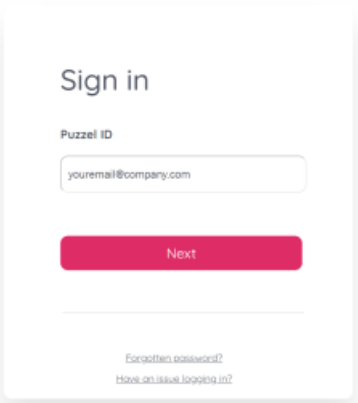
From the list of users, either click edit on an existing one, or add a new user corresponding to the Azure AD user that is to sign-in with SSO. For our configuration we have specified that the oid claim is the external id claim, so we need to make sure that the external ID field of the user has the oid (object ID) value from Azure AD. Verify that this value matches or paste the value from Object ID in Azure AD as shown above.

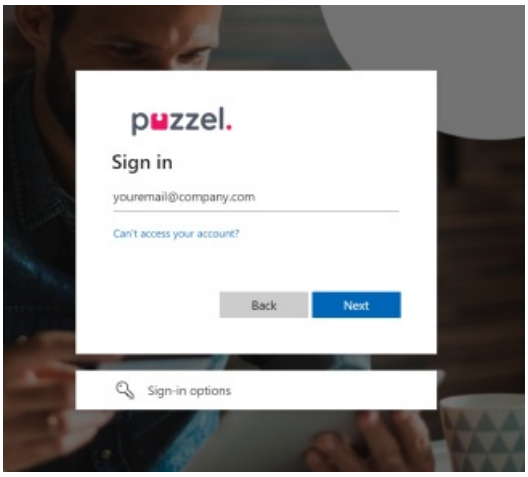


Click “Save” to store the updated information if any changes was made.

Accessing external providers directly

By default, the external provider will be detected after the users enter their Puzzel ID (email address) when signing in. An internal lookup will find that SSO is configured for the user and try to redirect them to the external provider as shown in the example below where Azure AD / Microsoft is the configured provider:

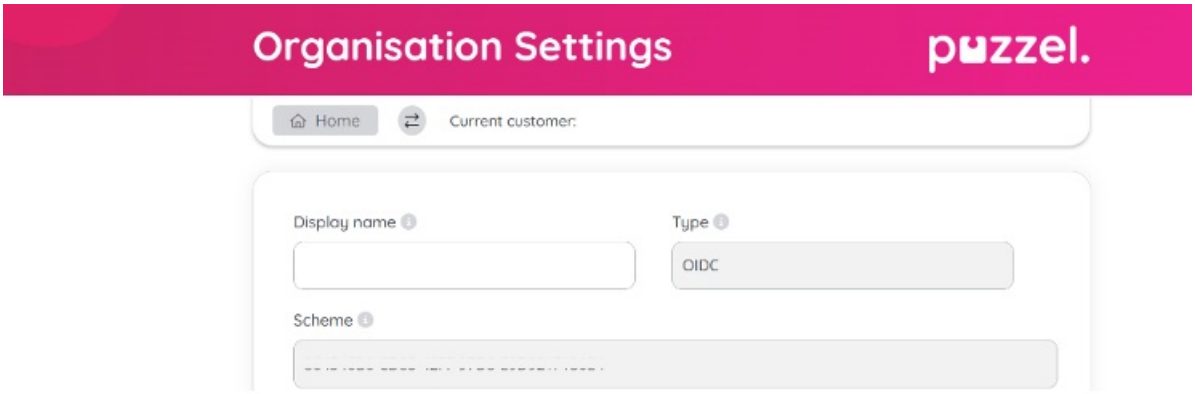




If users want to skip the part of entering their email address, there is an option to go directly to the external provider login screen. This is done by appending the query parameter idp to the Puzzel ID URL, with the “scheme” value from the relevant single sign-on configuration as parameter value.

If you chose to set up SSO using the Entra ID / Azure AD gallery application the value to use **ms-entra-id**. Example: https://app.puzzel.com/agent?idp=ms-entra-id

For manual SSO configuration, as an example, this a snippet from the single sign-on configuration used in examples above:



For manual configurations (not using the AD Gallery application), the “Scheme” value is to be used when identifying the external provider to use for direct SSO sign-in.

To use this directly with the agent application, the URL would be:
https://app.puzzel.com/agent?idp=864546B6-CD85-42FF-97D8-E9D921F130E4

> **Note**
>
> Note that the “Scheme” value can be modified to something more readable, but the redirect URLs will need to be modified accordingly in your external provider.

