

Using the Puzzel Entra ID (Azure AD) Gallery application

This article describes how to configure single sign-on (SSO) to Puzzel by installing the Puzzel app from the Entra Gallery. If you prefer a manual setup of SSO, please refer to **this guide**.

Step 1 - Find and add Puzzel application from Entra Gallery

Note

For this step you need access to your company's Microsoft Entra ID (Azure Active Directory) in the Azure portal including access to give administrative consent for the Azure tenant. If you are not an IT administrator for your company you would typically need help from one in order to complete this step.
See [What is application management? - Microsoft Entra ID](#) for more details on managing Entra ID apps.

To configure the integration of Puzzel into Entra ID for Single Sign-On, you need to add Puzzel from the gallery to your list of managed SaaS apps.

Log on to Entra ID portal and in the left side menu, select "Enterprise applications".

The screenshot shows the Microsoft Azure portal interface for the 'Development Puzzel' application in the Microsoft Entra ID section. The left sidebar contains a navigation menu with 'Enterprise applications' highlighted. The main content area displays the following information:

- Basic information:**

Name	Development Puzzel	Users	250
Tenant ID	xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx	Groups	17
Primary domain	devpuzzel.com	Applications	60
License	Microsoft Entra ID Free	Devices	3
- Alerts:**
 - Microsoft Entra Connect v1 Retirement:** All version 1.x builds of Microsoft Entra Connect (formerly AAD Connect) will soon stop working between October 2023 – March 2024. You must move to Cloud Sync or Microsoft Entra Connect v2.x.
 - Azure AD is now Microsoft Entra ID:** Microsoft Entra ID is the new name for Azure Active Directory. No action is required from you.
- My feed:**
 - Try Microsoft Entra admin center:** Secure your identity environment with Microsoft Entra ID, permissions management and more.
 - Global Administrator:** c2bb72d3-307c-4d4c-a652-2331df3aa6ed

On the next screen, click "New application":

Microsoft Azure

Home > Development Puzzel | Enterprise applications > Enterprise applications

Enterprise applications | All applications

Development Puzzel - Microsoft Entra ID

[+ New application](#)
[Refresh](#)
[Download \(Export\)](#)
[Preview info](#)
[Columns](#)
[Preview features](#)
[Got](#)

Overview

[Overview](#)
[Diagnose and solve problems](#)

Manage

- All applications
- Application proxy
- User settings
- App launchers
- Custom authentication extensions (Preview)

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](#).

Application type == Enterprise Applications
Application ID starts with

64 applications found

Name	Object ID	Application ID
FO FoMe	00011677-6634-4281-8269-31973d36925f	41666701-3051-4169-4291-9f297166995b
PO Puzzel Office 365 Connector	00000000-0000-0000-0000-000000000000	70000000-0000-0000-0000-000000000000
AA Azure AD B2C App	10000001-65f0-47e0-b200-000000000000	00017470-700b-4a00-b000-2d01072017e5
MT Microsoft Teams	10000000-0000-0000-0000-000000000000	00000000-0000-0000-0000-000000000000

In the search bar, search for "Puzzel" and you should find this app from Puzzel AS:

Microsoft Azure

Home > Development Puzzel | Enterprise applications > Enterprise applications | All applications >

Browse Microsoft Entra Gallery

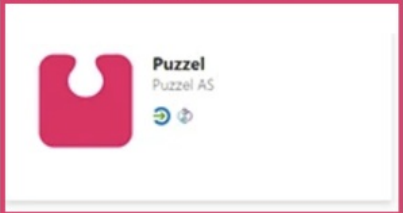
[+ Create your own application](#)
[Got feedback?](#)

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 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

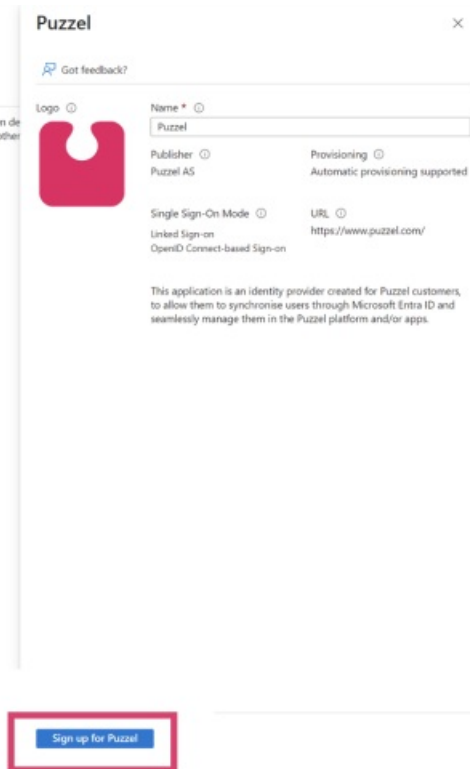
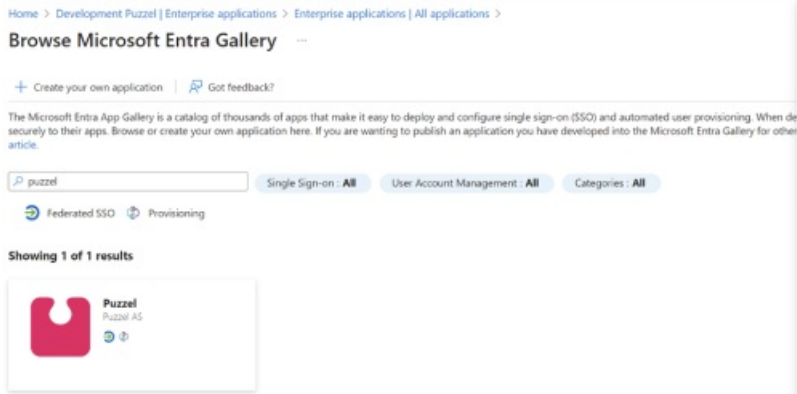
[Federated SSO](#)
[Provisioning](#)

Showing 1 of 1 results



The image shows a search result card for the 'Puzzel' application. It features a red puzzle piece icon on the left and the text 'Puzzel' and 'Puzzel AS' on the right. Below the text are two small circular icons representing authentication or provisioning options.

Click on the search result and you should see a screen on the right where you can choose to "Sign up for Puzzel":



Step 2 - Onboarding SSO identity

Note

For the next step you need a Puzzel ID user with admin role to be able to complete the onboarding process.

When clicking "Sign up for Puzzel", you are taken to the screen shown below. Click "Start Onboarding" to start the process.

Onboard Single Sign-On (SSO) identity

Onboarding instructions

Onboarding Single Sign-On (SSO) identity provider is the process of an administrator granting consent to the Azure AD application in its tenant.

First, you need to sign-in to Puzzel Id with an administrator account. That will redirect you to the next phase of the process where you confirm the customer to be onboarded. The final step is to sign-in and grant consent with an [Azure AD administrator account](#) from the Azure tenant you want to onboard. Once the tenant administrator signs in and consents to the app's requested permissions, this application's service principle is provisioned into the tenant.

Click the button below to initiate the process.

Start Onboarding

Next, verify that the customer name is correct (this is shown) right above the "Onboard SSO" button, click this button to continue the process.

Onboard Single Sign-On (SSO) identity

Onboarding

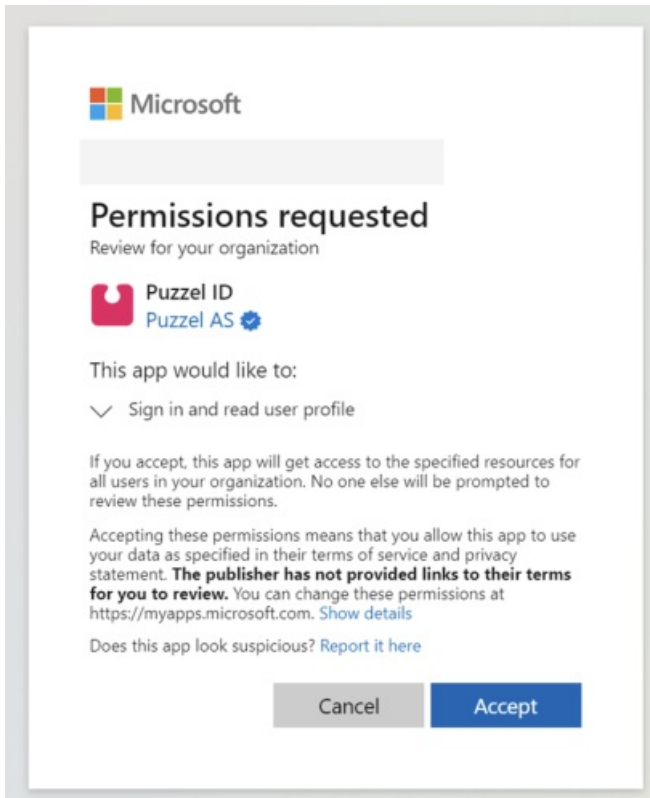
In this step confirm the customer to be onboarded. Afterwards, you will be asked to sign-in and grant consent with an [Azure AD administrator account](#) from the Azure tenant you want to onboard. Once the tenant administrator signs in and consents to the app's requested permissions, this application's service principle is provisioned into the tenant.

Click the button below to continue the process.

Puzzel AS

Onboard SSO

Next you will be asked to sign-in and grant consent with an Entra ID (Azure AD) administrator account from the Azure tenant you want to onboard.



Once accepted, the applications' service principle is now provisioned into the tenant and you should see the "onboarding completed" page:

Onboard Single Sign-On (SSO) identity

Onboarding Completed

The Single Sign-On (SSO) identity provider has been successfully onboarded with Puzzel Id.

You can close this window now.

Step 3 - Managing an onboarded identity provider

After initial configuration, a connection can be disabled / enabled in the Organisation Settings portal. Choose the "Configure" option in the Single Sign-On option.

Search and view access log

[View](#)


Configure customer settings

[Configure](#)

Manage rules for auto provisioning users

[Configure](#)

Event Log



Search and view event log

[View](#)

Security

Single Sign-On



Configure Single Sign-on for your organisation

[Configure](#)

Visitor SSO




Configure Single Sign-on for consumer

[Configure](#)

Next you should find the configured connection looking similar to the below screenshot, from this view, choose the “edit” icon.


Organisation Settings



[Home](#) [↔](#) Current customer: Puzzel AS

Single Sign-on

[+ Add](#)

Enabled	Display name	Type	Tenant
<input type="radio"/> No	Microsoft Entra ID	OIDC	

From the next screen it is possible to disable / enable the SSO connection. It is also possible to change which external id claim to use (e.g., change to use "udp").

The screenshot shows a configuration panel for an external ID claim. It includes the following elements:

- External id claim:** An empty text input field.
- Response type:** A dropdown menu currently set to "code".
- Scopes:** A container with three buttons labeled "email x", "profile x", and "openid x".
- Authorized Azure Tenant Id's:** An empty text input field.
- Checkboxes:** Two checked checkboxes: "Get claims from Userinfo endpoint" and "Use PKCE".
- Toggle:** A toggle switch currently set to "Disabled".
- Buttons:** "Cancel" and "Save" buttons.

Step 4 - Configure externalid for your users that are to use the SSO configuration

By default, the provider configuration behind the Puzzel Entra ID application uses the `oid` claim as external id claim to map the user to Puzzel ID.

This means that each user that is to use the configured SSO connection will need their respective Entra ID `objectid` added to their externalid field. Or if you changed External id claim to e.g. `upn` then you need to add `UserPrincipalName` from Azure (typically email address).

See the chapter ["Validate users using external id"](#) for more information.