

SSO Entra ID - How to configure?

Gathid user authentication has been designed to work with your existing identity provider. This guide will assist you with enabling your Gathid instance to use your existing MS Entra ID to for Single Sign-On.

This guide outlines the standard process of configuring Entra ID to act as an Identity Provider for Single Sign-On for your Gathid instance.

Summary

1. [Register an Entra ID Application for Gathid Single Sign-On](#)
2. [Create Entra ID Group\(s\) to be used for Gathid Roles](#)
3. [Provide the required information to your Gathid representative](#)

1. Register an Entra ID Application for Gathid Single Sign-On

- Browse to [Azure Portal](#) and log in to your organization.
- Navigate to: **App registrations** and select **New registration**.
- Provide a **Name** for the application: e.g. “*Gathid OIDC*”.
- Under **Supported account types** select: **Accounts in this organizational directory only**.
- In the **Redirect URI (optional)** section use the dropdown next to *Select a platform* to choose: **Web**.
- Enter your redirect URL in the form of: **https://<CUSTOMER_URL>/realms/access-analytics/broker/aad-oidc/endpoint**.

Obtain your <CUSTOMER_URL> from your Gathid representative.

Register an application

* Name

The user-facing display name for this application (this can be changed later).

Gathid OIDC ✓

Supported account types

Who can use this application or access this API?

- ☒ Accounts in this organizational directory only (Requires **My organization only** - Single tenant)
- ☐ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)
- ☐ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- ☐ Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web https://CUSTOMER_URL/realm/access-analytics/broker/aad-oidc/e... ✓

- Click to **Register** the application. You will be redirected to the **Overview** page of the new application registration just created.
- Copy the **Application (client) ID** GUID and store it for future use.
- Select **Endpoints** from the options at the top of the screen.

Gathid OIDC

Search Delete Endpoints Preview features

Overview

Quickstart

Integration assistant

Diagnose and solve problems

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Essentials

Display name : Gathid OIDC
Application (client) ID : a614fe9b-25c04502960a
Object ID : 3770a228-417714c5c58a
Directory (tenant) ID : ad4883e1-e73c73fedd91
Supported account types : [My organization only](#)

[Get Started](#) [Documentation](#)

- From the modal that pops up, copy the **OpenID Connect metadata document** URL and store it for future use.
- Close the **Endpoints** modal.

Endpoints

Authority URL (Accounts in this organizational directory only)	https://login.microsoftonline.com/ad4883e1-1712-408a-8f12-171217121712
Authority URL (Accounts in any organizational directory)	https://login.microsoftonline.com/organizations
Authority URL (Accounts in any organizational directory and personal Microsoft accounts)	https://login.microsoftonline.com/common
Authority URL (Personal Microsoft accounts only)	https://login.microsoftonline.com/consumers
OAuth 2.0 authorization endpoint (v2)	https://login.microsoftonline.com/ad4883e1-1712-408a-8f12-171217121712/oauth2/v2.0/authorize
OAuth 2.0 token endpoint (v2)	https://login.microsoftonline.com/ad4883e1-1712-408a-8f12-171217121712/oauth2/v2.0/token
OAuth 2.0 authorization endpoint (v1)	https://login.microsoftonline.com/ad4883e1-1712-408a-8f12-171217121712/oauth2/authorize
OAuth 2.0 token endpoint (v1)	https://login.microsoftonline.com/ad4883e1-1712-408a-8f12-171217121712/oauth2/token
SAML-P sign-on endpoint	https://login.microsoftonline.com/ad4883e1-1712-408a-8f12-171217121712/saml2
SAML-P sign-out endpoint	https://login.microsoftonline.com/ad4883e1-1712-408a-8f12-171217121712/saml2
WS-Federation sign-on endpoint	https://login.microsoftonline.com/ad4883e1-1712-408a-8f12-171217121712/wsfed
Federation metadata document	https://login.microsoftonline.com/ad4883e1-1712-408a-8f12-171217121712/federationmetadata/2007-06/federationmetadata.xml
OpenID Connect metadata document	https://login.microsoftonline.com/ad4883e1-1712-408a-8f12-171217121712/v2.0/well-known/openid-configuration
Microsoft Graph API endpoint	https://graph.microsoft.com

- Select the **Certificates & secrets** item from the blades on the left-hand-side (under the Manage heading).
- Ensure the **Client secrets** tab is selected and click on **New client secret**.
- Provide an optional *Description*. e.g.: Gathid Identities and set the *Expires* period to the maximum (730 days).
- Click **Add**.
- Copy the **Value** (*not* the Secret ID) and keep it for future use.

Diagnose and solve problems

Manage

- Branding & properties
- Authentication
- Certificates & secrets**
- Token configuration
- API permissions
- Expose an API
- App roles
- Owners

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) **Client secrets (1)** Federated credentials (0)

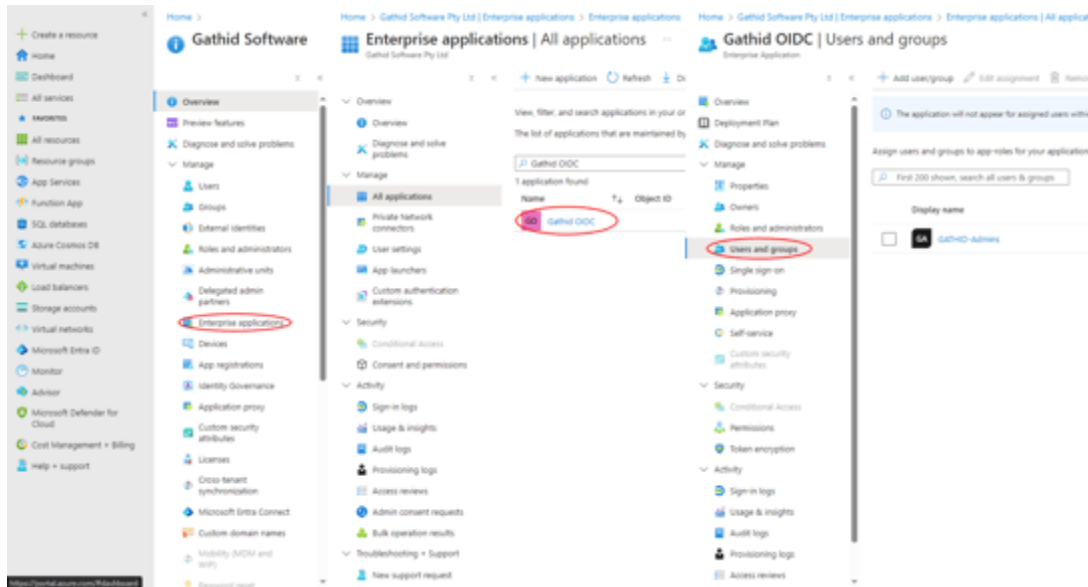
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	Secret ID
Gathid Cloud	8/28/2025	.Mg*****	ee426759-a2ac-4d0d-83ed-85d5e04a62df

- Select the **Token configuration** item from the blades on the left-hand side (under the Manage heading)
- Select **Add groups claim**.
 - For companies with under 50 security groups for Gathid users, select **Security groups**.
 - Otherwise, tick **Groups assigned to the application** in the modal that appears.

- This option requires that the groups that are used to access Gathid are assigned to the Enterprise Application.
- From the Entra ID Home page, navigate to **Enterprise Applications**, locate your Gathid Application, then select **Users and Groups** under the Manage blade on the left-hand-side.
- Select **Add user/group** from the menu at the top and locate the group to add.



- Click **Add**.

2. Create Entra ID Group(s) to be used for Gathid Roles

After the user has been authenticated in the Gathid application, authorisation to certain functionality or information is enforced by Role Base Access Control (RBAC).

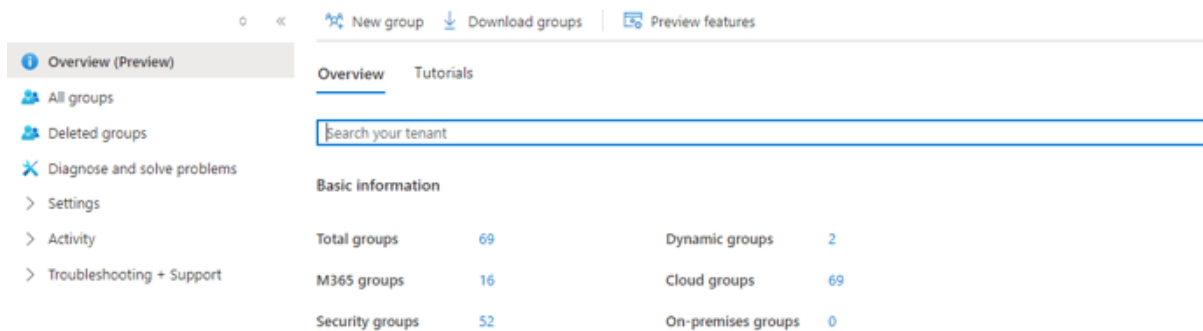
By default, Gathid has three roles defined: ADMINISTRATOR, USER and RESPONDER.

We recommend defining at least one ADMINISTRATOR and then create other roles that are suitable for your organization.

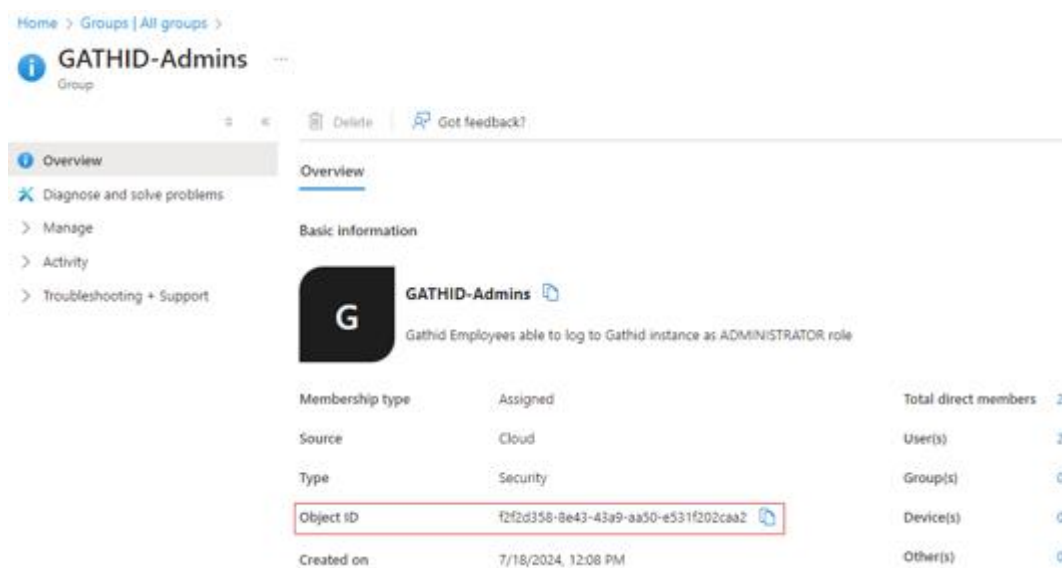
Gathid Roles are mapped to people in your organization's Entra ID using Groups. You can use the existing Entra ID groups or create specific ones for Gathid Roles.

Once you determine the group, you need to provide your Gathid representative information about the group in the form of the group's Object Id.

- In Entra ID, select: **Groups**



- Select the relevant groups to show details.



- Copy the **Object Id** and keep it for future use.

3. Provide the information to your Gathid representative

Make sure you have a copy of the following and provide to Gathid representative:

- Application (client) ID GUID
- OpenID Connect metadata document URL
- Client value
- Group Object Id for ADMINISTRATOR Role
- (Optional) Groups' Object Ids for other Roles