

Microsoft Entra ID App Registration

Step-by-step guide to registering Arealytics Single Sign-On in your Microsoft Entra ID (Azure AD) tenant: the app registration, client secret and token claims that Arealytics needs to trust your users.

WHAT THIS ACHIEVES

You create an app registration in your organisation's Microsoft Entra tenant. Arealytics uses it to sign your users into Arealytics Pro with their existing Microsoft work accounts, so they don't need a separate Arealytics password.

1

Get Redirect URI

Supplied by
Arealytics

2

Register app

Single tenant · Web
redirect

3

Client secret

Copy the Value once

4

Token claims

email · upn ·
xms_edov

5

Hand back

Client ID · Tenant ID ·
Secret

Before you begin

You need	Details
Azure access	Global Administrator, Application Administrator or Cloud Application Administrator on your organisation's Microsoft Entra tenant.
Redirect URI	The exact Redirect URI Arealytics generated for your company, in the form <a href="https://auth.arealytics.com.au/realms/arealytics/broker/<auto-generated>/endpoint">https://auth.arealytics.com.au/realms/arealytics/broker/<auto-generated>/endpoint .
Verified email domain	Your email address domain is added and verified under Entra ID → Custom domain names . Arealytics only trusts email addresses from a verified domain.
User email addresses	Each user's Email (mail) attribute in Entra is set and matches the email address they use with Arealytics.

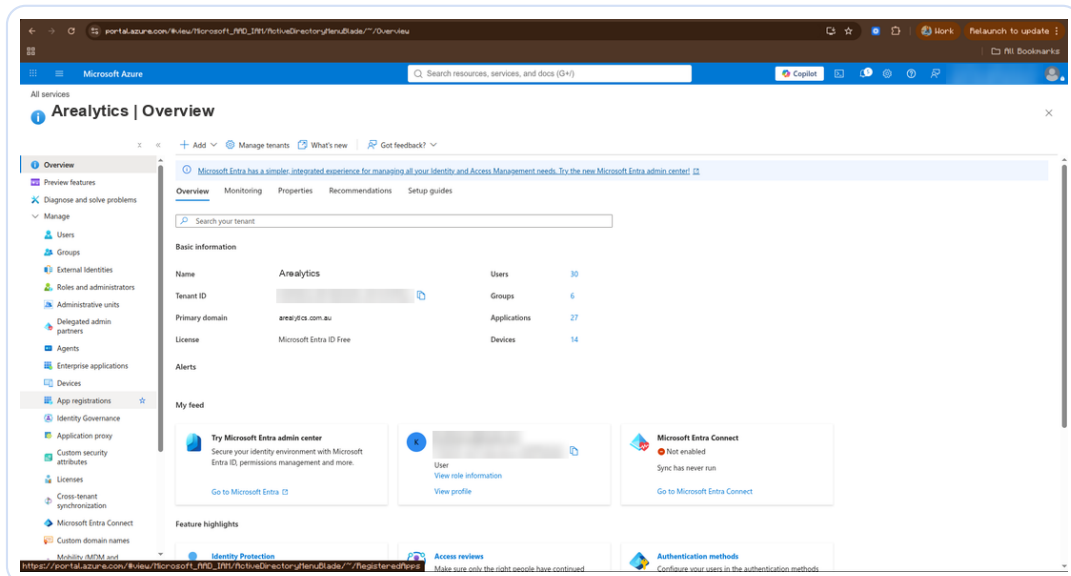
TASK 1 Register the application

Microsoft Entra ID — creates the app that Arealytics trusts.

- 1 **Open Microsoft Entra ID.** In the Azure portal, choose **More services**, scroll to the **Identity** section and select **Microsoft Entra ID**.

portal.azure.com > [All services](#) > [Identity](#) > [Microsoft Entra ID](#)

- 2 **Go to App registrations → New registration.** In the Entra sidebar, select **App registrations**, then click **+ New registration** at the top-left.



Azure — Microsoft Entra ID overview: **App registrations** is in the left menu. The tenant name is replaced with a sample, and the Tenant ID and user details are masked.

- 3 **Name the application.** Give it any recognisable name, for example **Arealytics SS0**.
- 4 **Choose Single tenant.** Under **Supported account types**, select **Accounts in this organizational directory only (Single tenant)**. This limits sign-in to your organisation's own directory.

- 5 **Set the Redirect URI and Register.** Under **Redirect URI**, choose the platform **Web** and paste the Redirect URI supplied by Arealytics exactly as given. Then click **Register**.

Microsoft Azure

Search resources, services, and docs (G+)

Register an application

Name

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

arealitics-ldap

Supported account types

Choose the account types that can use this application or access this API.

Single tenant only - Arealitics

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://aut.at.aarealitics.com.au/realms/arealitics/protocol/...

By proceeding, you agree to the Microsoft Platform Policies

Register

Azure — Register an application: enter a name, choose **Single tenant**, select the **Web** platform and paste the Redirect URI.

TASK 2 Create the client secret

Microsoft Entra ID — the credential Arealytics uses to call your tenant.

- 6 **Certificates & secrets → New client secret.** In the app's sidebar, open **Certificates & secrets** and click **+ New client secret**.

Microsoft Azure

Search resources, services, and docs (G+)

arealitics-ldap | Certificates & secrets

Overview

Quickstart

Integration assistant

Diagnose and solve problems

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators

Manifest

Support + Troubleshooting

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

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

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

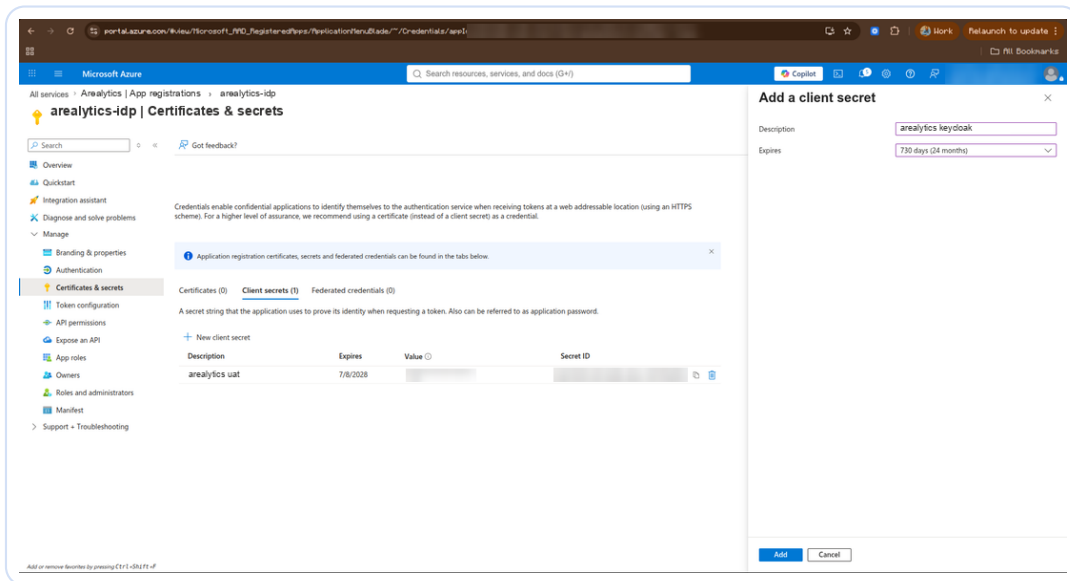
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	Secret ID
arealitics uat	7/6/2028	[Masked]	[Masked]

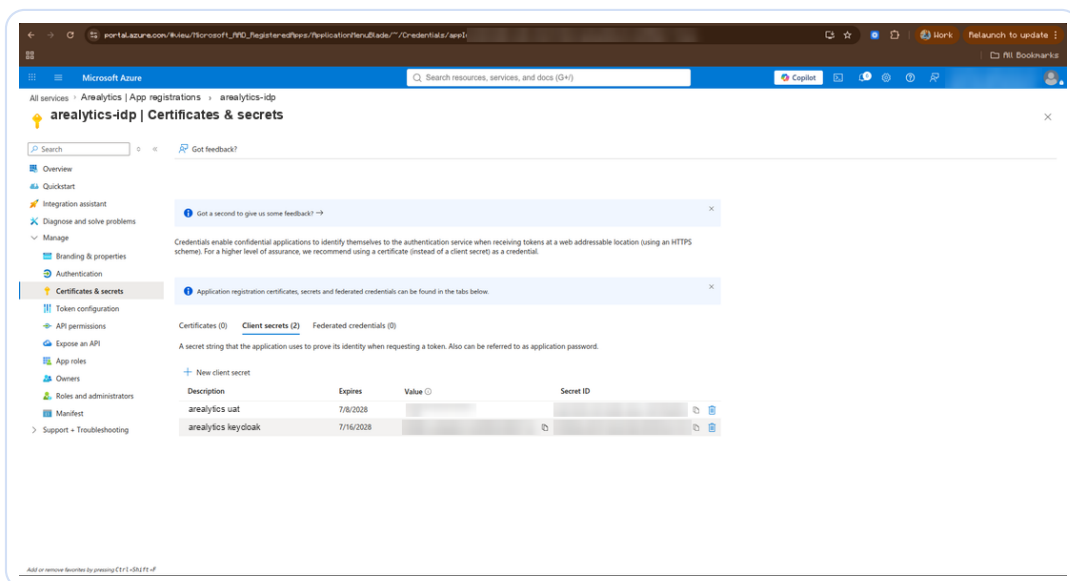
Azure — **Certificates & secrets** → **Client secrets** → **New client secret**. Secret values and IDs are masked.

- 7 **Add a description and expiry.** Enter a description (for example `arealitics-idp`) and an expiry (for example 24 months), then click **Add**. **Record the expiry date:** Arealytics needs it to plan secret rotation.



Azure — Add a client secret: set a description and an expiry, then click **Add**.

- 8 **Copy the secret Value immediately.** Copy the client secret's **Value** (not the Secret ID) and store it somewhere safe until you send it to Arealytics.



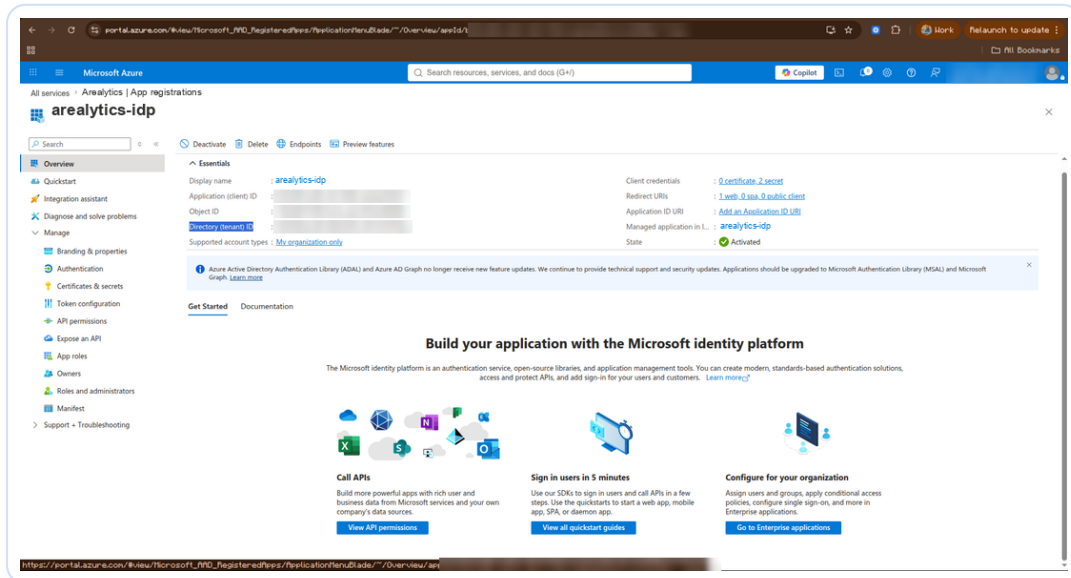
Azure — Copy the secret **Value** now; Azure masks it permanently once you leave the page. Secret values and IDs are masked.

THE SECRET VALUE IS SHOWN ONLY ONCE

Azure reveals the client secret Value exactly once, right after you create it. If you leave the page before copying it, delete that secret and create a new one. The **Secret ID** is not the Value, so don't confuse them.

TASK 3 Copy the application ID

- 9 Open the app's Overview page. Open the app's **Overview** and copy the **Application (client) ID** and the **Directory (tenant) ID**.



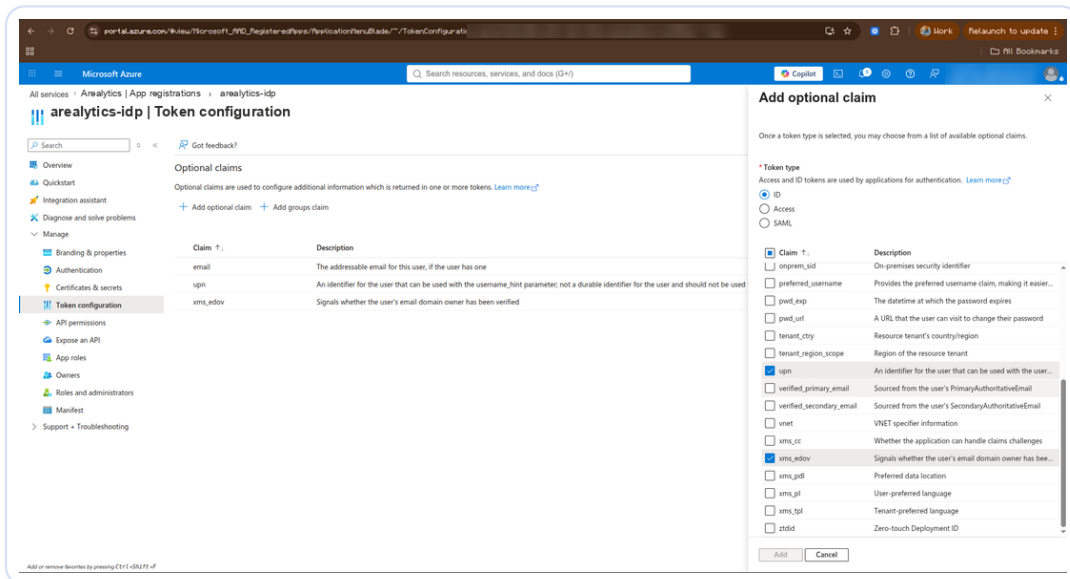
Azure — App overview: copy the **Application (client) ID** and the **Directory (tenant) ID**.

TASK 4 Token configuration (required)

Microsoft Entra ID — sends the claims Arealytics needs to verify the user's email.

- 10 Open **Token configuration**. In the app's sidebar, select **Token configuration**, then click **+ Add optional claim**.
- 11 Choose **token type ID** and add the claims. Set **Token type** to **ID**, then tick these three claims:

Claim	Why it's needed
email	The user's email address, used to match their Arealytics account.
upn	User principal name, used as a fallback identifier.
xms_edov	Email Domain Owner Verified. Proves the email belongs to a domain your tenant owns.



Azure — Token configuration → Add optional claim: token type ID with email, upn and xms_edov.

- 12 Save the claims.** If Azure asks you to turn on the Microsoft Graph **email / profile** permission, tick it and click **Add** to save. The Optional claims list should now show **email**, **upn** and **xms_edov** for token type ID.

DON'T SKIP XMS_EDOV

Without the **xms_edov** claim, Arealytics can't confirm that the email is verified and domain-owned, so it denies sign-in by design. A missing **xms_edov** is the most common cause of "Email could not be verified" at login.

Send the values to Arealytics

Hand-off — Arealytics completes the setup in ERC (Guide 1).

Send your Arealytics contact the following. Send the client secret through the agreed secure channel, separately from the IDs.

Value	Where to find it in Azure	Arealytics uses it as
Application (client) ID	App → Overview	Client ID
Directory (tenant) ID	App → Overview	Organization ID (Tenant ID)
Client secret Value (once only)	Copied in Step 8	Client Secret
Client secret expiry date	Certificates & secrets → Expires	Rotation reminder

Final checklist

- ✓ App registered with **Single tenant** supported account types.
- ✓ **Web** platform Redirect URI matches the Arealytics-supplied URI exactly.
- ✓ Client secret created, **Value** copied and expiry date recorded.
- ✓ Optional claims [email](#), [upn](#) and [xms_edov](#) added for token type **ID**.
- ✓ Users' email domain is a verified custom domain in your tenant, and users have an Email attribute set.
- ✓ Client ID, Tenant ID, secret Value and expiry date sent to Arealytics, with the secret sent through a secure channel.

BEFORE THE SECRET EXPIRES

When the expiry date approaches, create a **new** client secret in the same app (Task 2) and send the new Value to Arealytics. After Arealytics confirms that sign-in works with the new secret, delete the old one. If the secret is allowed to expire, sign-in stops for all of your users.

Troubleshooting

Symptom	Likely cause & fix
AADSTS50011 — redirect URI mismatch	The Web Redirect URI in Azure doesn't exactly match the one Arealytics supplied. Open the app's Authentication page and re-paste it exactly as supplied, matching case, with no extra spaces or trailing slash.
"Email could not be verified"	The xms_edov optional claim is missing. Add it in Token configuration (Task 4). Also check that the user's email domain is a verified custom domain in your tenant.
"Could not determine your email"	The email / upn optional claims are missing. Add them in Token configuration (Task 4). Also check that the user has an Email attribute set in Entra.