hStream™

Microsoft Entra ID (OIDC) Configuration

Auth0 Self Service — Connecting Microsoft Entra ID as an OpenID Connect identity provider for Single Sign-On into HealthStream.

Note: Only to be used if the HLC username is the email address

September 2026

Before You Begin

! Do not delete or remove your existing SSO connection in Entra ID while completing this guide. Keeping it active lets us fall back to it if anything below needs troubleshooting, and your users see no disruption in the meantime.

! This upgrade runs entirely behind the scenes. Anyone currently signing in through your existing SSO connection will not notice any difference until HealthStream switches your account over to the new connection after a successful test.

! Open your existing Entra ID SSO connection in a separate browser tab before you start. Several steps below ask you to copy values — attribute mapping and the access group — directly from it.

WHAT WE'LL COVER

Five Steps to a Working SSO Connection

1

Create Application

Register an OIDC application in Microsoft Entra ID and record its credentials.

2

Configure Connection

Bring the application's Client ID, Client Secret, and endpoints into Auth0 Self Service.

3

Claims Mapping

Translate Entra ID user attributes into the fields HealthStream expects.

4

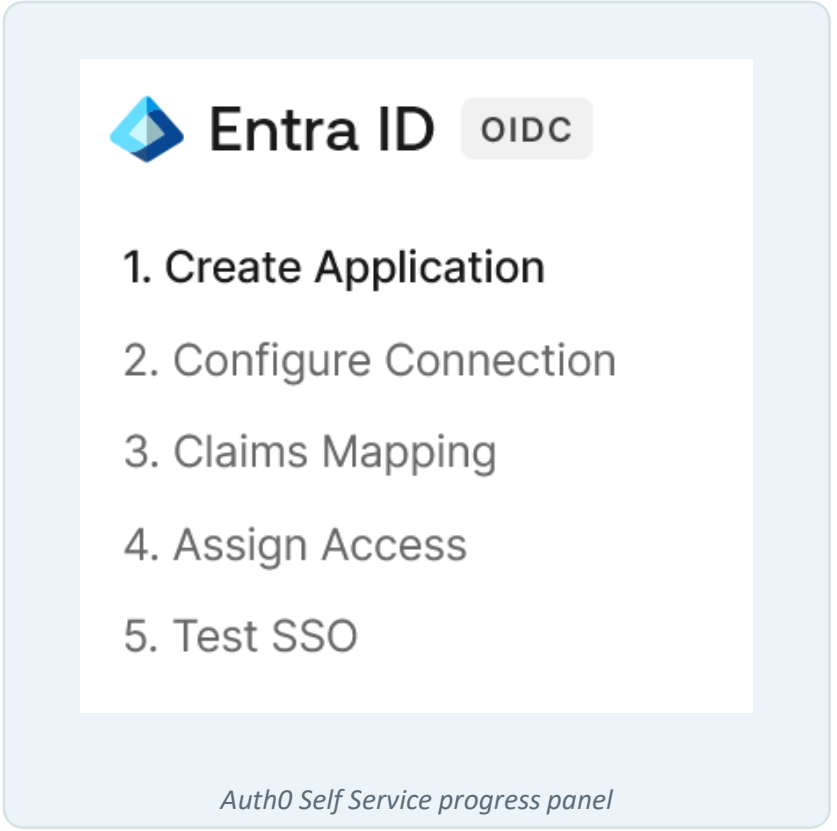
Assign Access

Choose which Entra ID users or groups can use this connection.

5

Test SSO

Sign in through Entra ID and confirm the test is successful

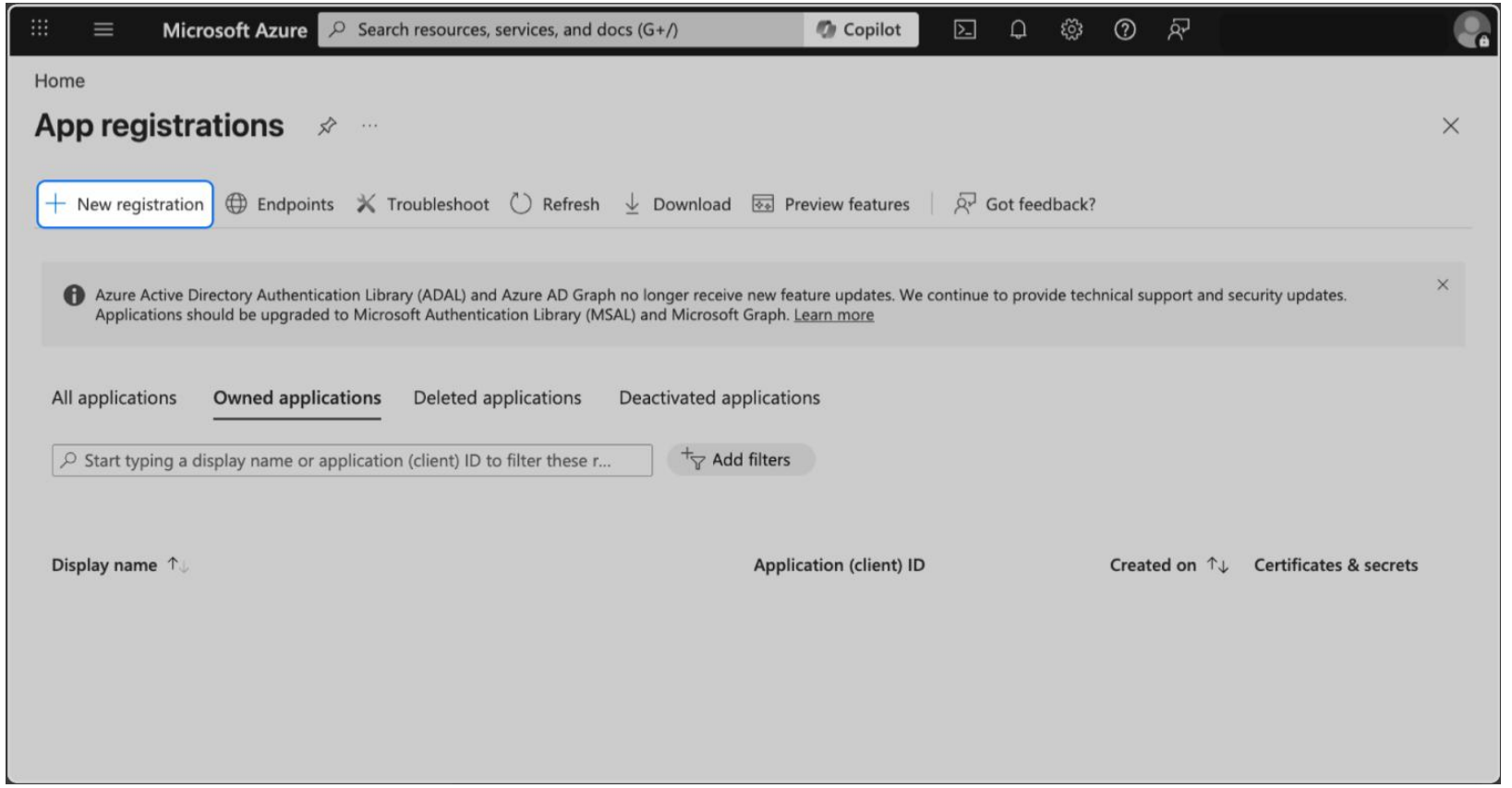


Auth0 Self Service progress panel

Navigate to App Registrations

1

- To connect your Entra ID tenant as an identity provider, you must create an OIDC application.
- In the Azure Portal, navigate to Microsoft Entra ID and select App Registrations.
- Select New Registration.



Azure Portal — App registrations

Register the Application

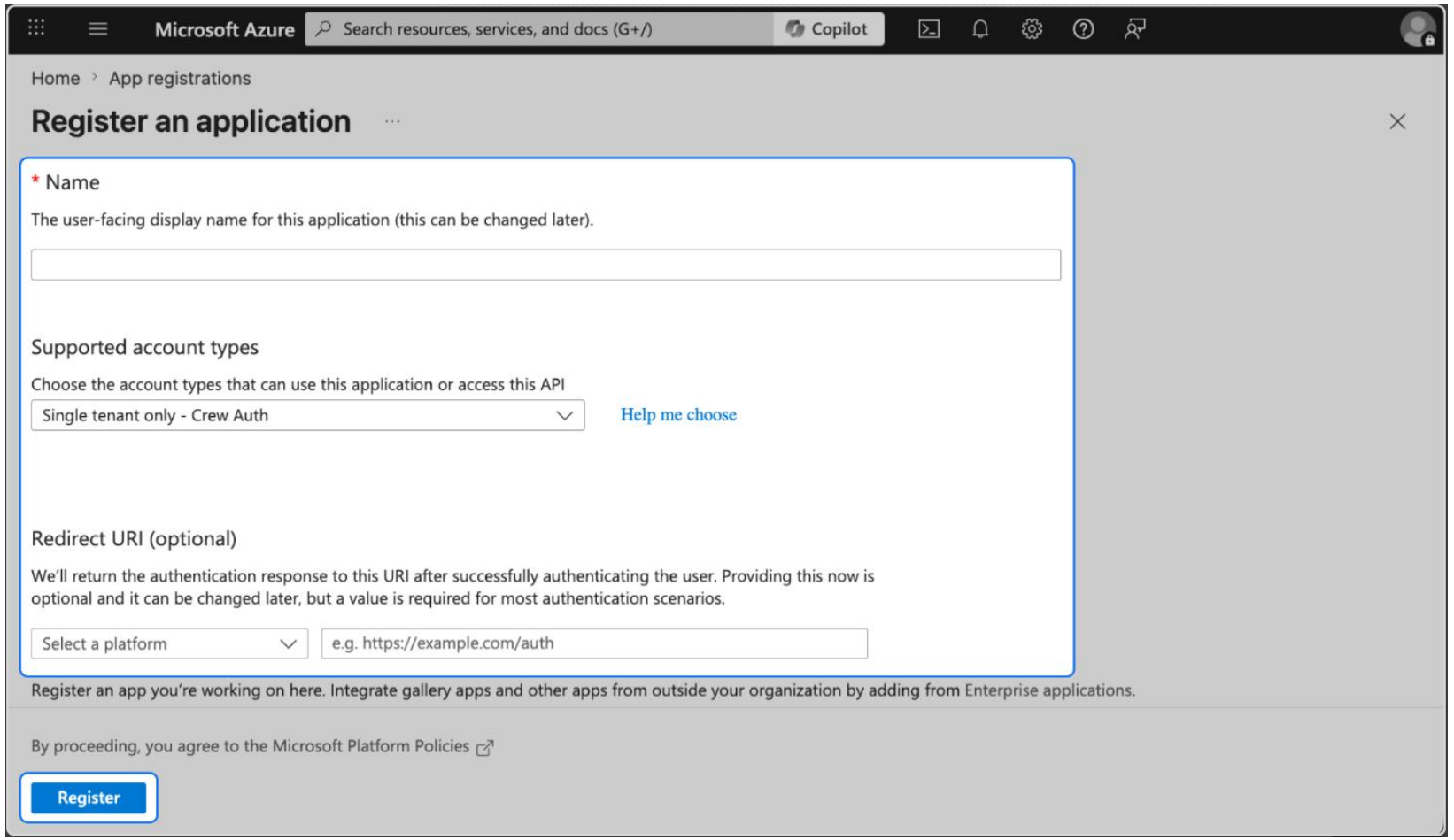
1

- Enter a name for the application, such as “hStream Auth0 SSO”.
- Under Supported account types, choose Single tenant only option.
- Under Redirect URIs, select Web and add the Callback URL provided by Auth0 Self Service:

https://connect.hstream.com/login/callback

https://connect.hstream.com/login/callback

Select Register.

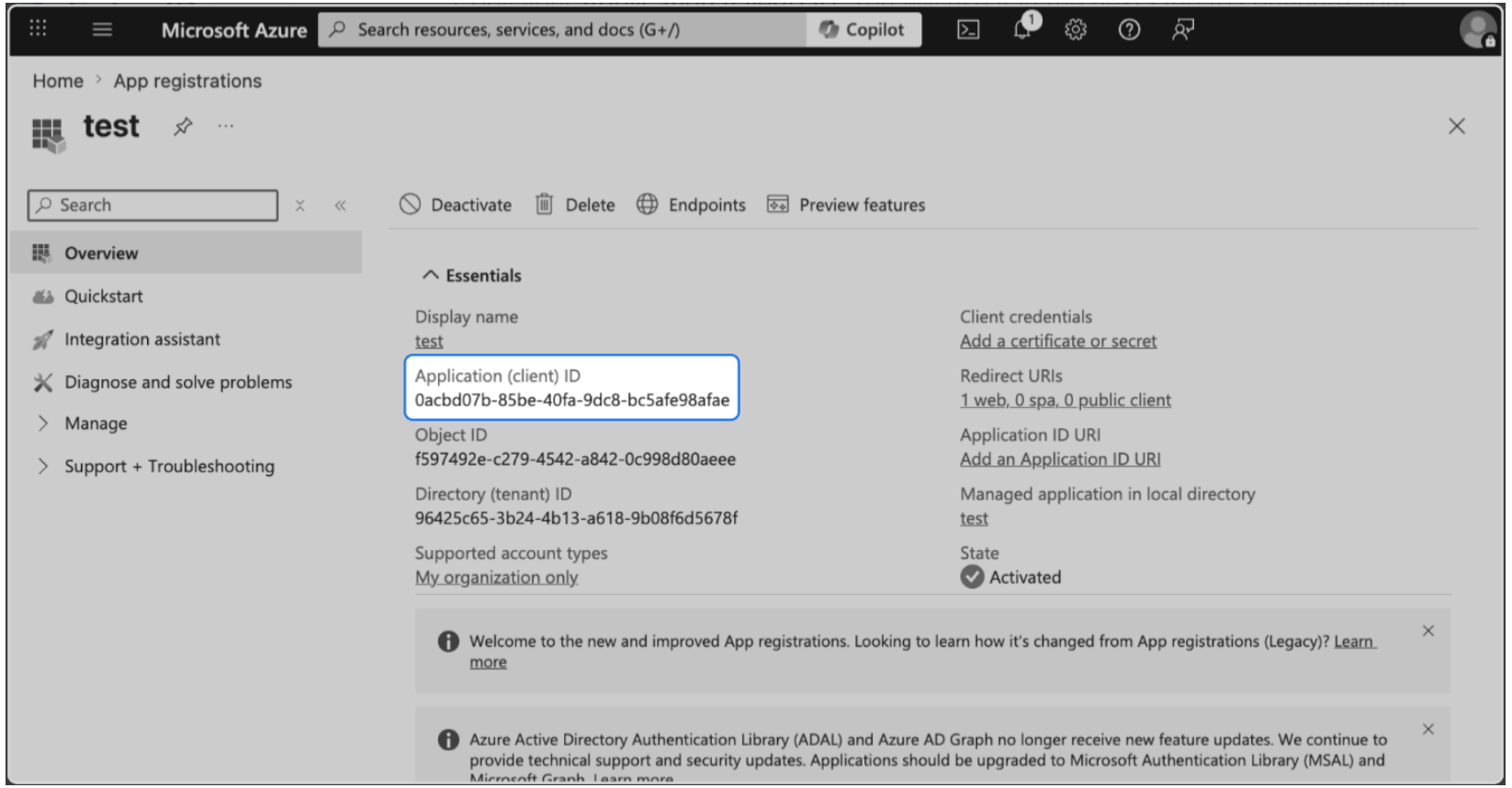


Register an application

Copy the Application (Client) ID

1

- After registering, the application's Overview page displays its identifiers.
- Copy the Application (client) ID.
- You will use it in the next step to configure your connection in Auth0 Self Service.

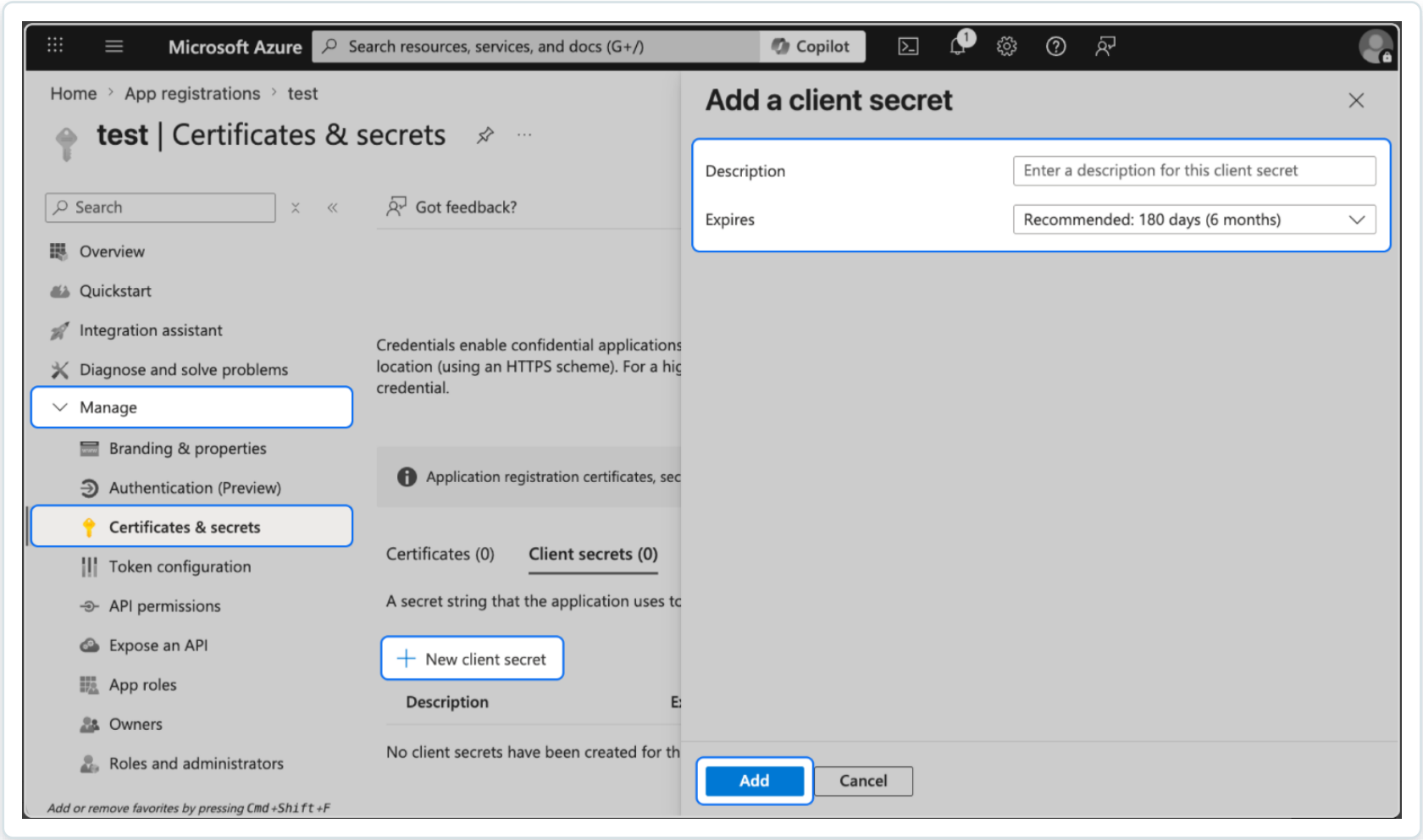


Application Overview — Application (client) ID

Create a Client Secret

1

- Under Manage in the left-hand navigation, select Certificates & secrets.
- Select New client secret.
- Enter a Description and set the expiration.
- Click Add.

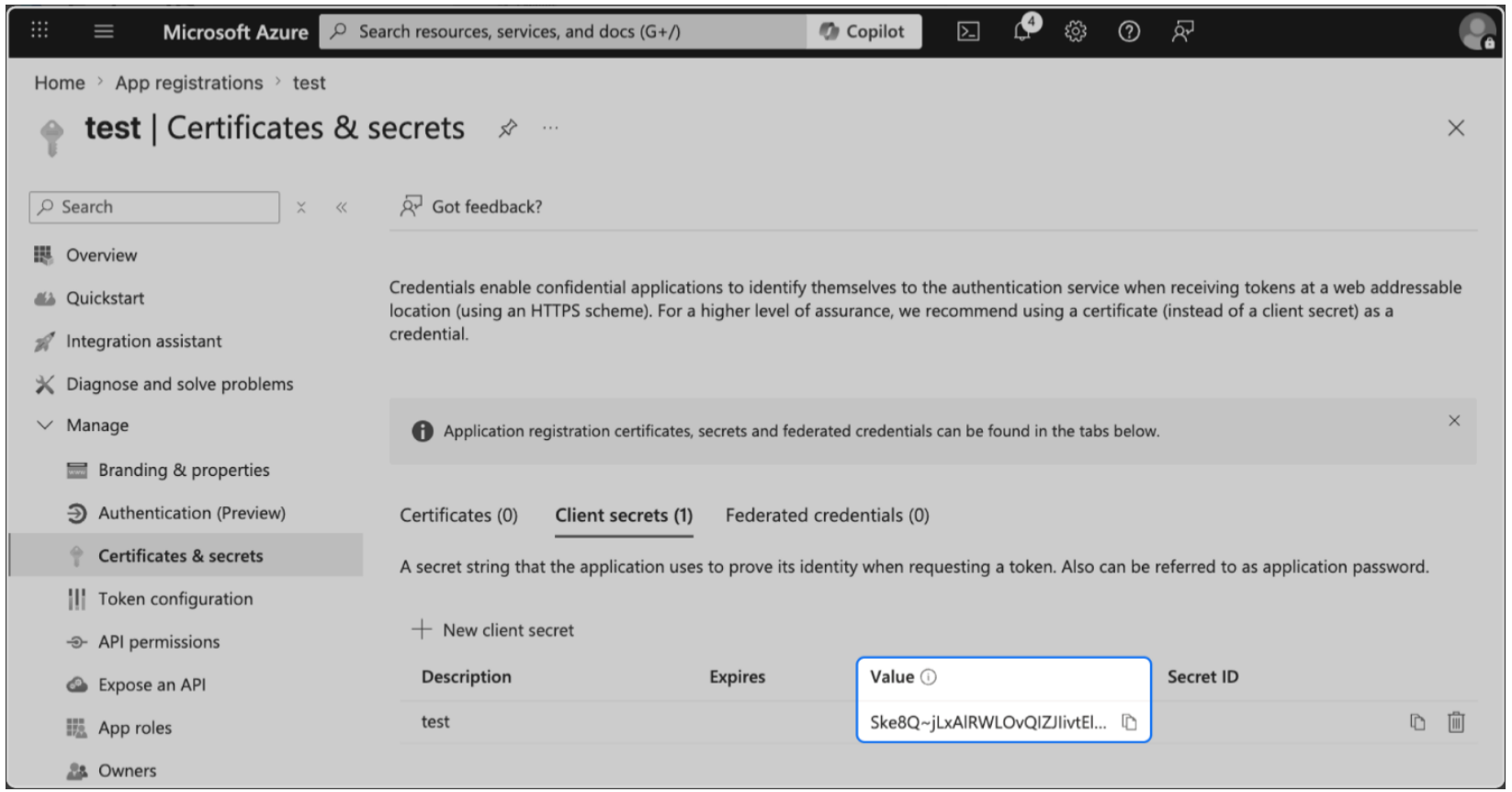


Certificates & secrets — Add a client secret

Copy the Client Secret Value

1

- Once the secret is created, copy the Value shown in the Client secrets list.
- This is the only time the full value is displayed — store it securely.



Client secrets — copy the Value

2

Bring the Application Details into Auth0

Return to the Auth0 Self Service portal and enter the required application information from Microsoft Entra ID.

1. **Client ID**
2. **Client Secret**
3. **Microsoft Entra ID Domain**

STEP 3 · CLAIMS MAPPING

Map Entra ID Attributes to HealthStream Fields

3

Claims mapping determines how user information from Microsoft Entra ID is translated into hStream user attributes. Review and map the required claims.

Microsoft Entra ID Claim - Required	HealthStream User Attribute
Email	Email Address
Given Name	First Name
Family Name	Last Name
Username	First Name + Last Name

Why this matters

- Ensure all required attributes are mapped correctly — these values are used for user identification and provisioning.
- After reviewing the mappings, select Next.

Enable Claims Mapping in the App Manifest

3

The following is required any time custom claims mapping is used. For example, when the HLC username is not the email address as mentioned previously.

- In your app registration, go to Manifest.
- Find **"acceptMappedClaims"** and set it to **true** (it defaults to null).
- Find **"groupMembershipClaims"** and set it to **"SecurityGroup"** (or "All," depending on which groups you want to pass) so group claims are included in the token.
- Save the manifest.

Why this matters

Without this change you will not be able to authenticate with HealthStream.

4

Add Required API (Graph) Permissions

Please confirm each permission below — a missing permission here is the single most common reason the test connection fails.

- In your app registration, go to API permissions > Add a permission > Microsoft Graph > Delegated permissions.
- Add the four permissions listed below.
- If your tenant requires it, click Grant admin consent for [your organization] after adding them.

Permission	Type	Notes
openid	Delegated	Required for OIDC sign-in.
profile	Delegated	Required for basic profile claims.
User.Read	Delegated	Required to read the signed-in user's profile.
Group.Read.All	Delegated	Read only — do not select the Read. Write variant.

Choose Who Can Use This Connection

4

1

Assign by group or tenant-wide

You can assign access to specific Microsoft Entra ID groups or allow access for all users within your tenant.

2

Start with a test group

It is recommended to begin with a test group during validation, before rolling out more broadly.

3

Save and proceed

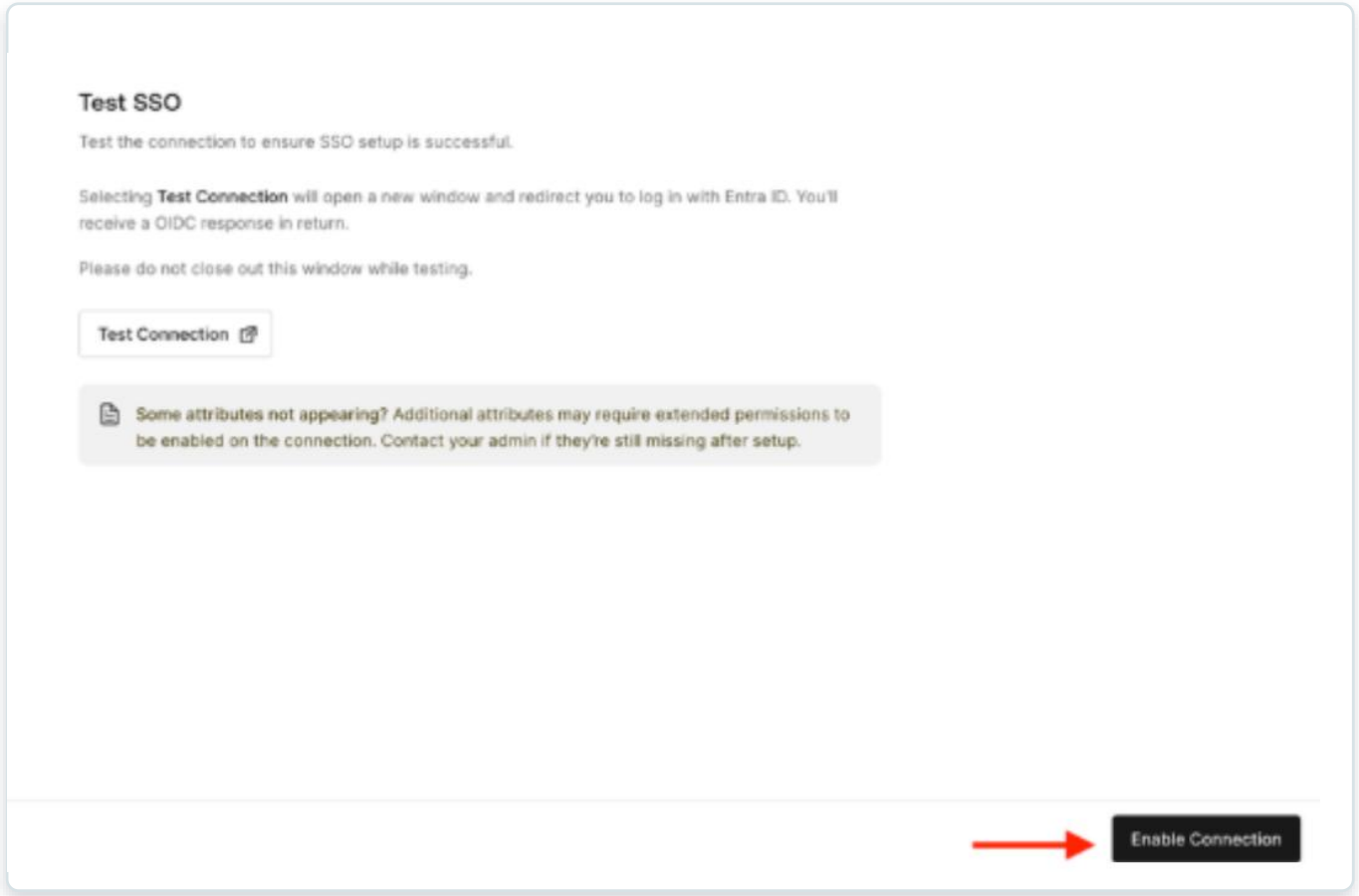
Once access has been assigned, save your configuration and proceed to testing.

Enable & Test Connection

5

- **Step 1 : Click on the Test Connection button**

- **Step 2 : Enable the Connection**



Auth0 Self Service — Enable Connection

BEFORE YOU GO LIVE

Validation Checklist

- ✓ Client ID and Client Secret match the Entra ID app registration
- ✓ Redirect URI (Callback URL) matches exactly
- ✓ Required claims are mapped correctly
- ✓ Test user is assigned access to the application
- ✓ Client secret has not expired

Thank You

Now your Entra ID connection has been successfully configured using Auth0 Self Service, HealthStream will make a final configuration change in the near future so that users can use your new connection to securely access HealthStream through Single Sign-On using their organization’s Entra ID credentials.

For additional assistance, contact the HealthStream Platform team or refer to the Auth0 Self Service User Guide.