hStream™

Okta (OIDC) Configuration

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

September 2026

Before You Begin

! Do not delete or remove your existing SSO connection in Okta 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 Okta 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 web application in Okta and record its credentials.

2

Configure Connection

Bring the Okta Domain URL, Client ID, and Client Secret into Auth0 Self Service.

3

Claims Mapping

Translate Okta user attributes into the fields HealthStream expects.

4

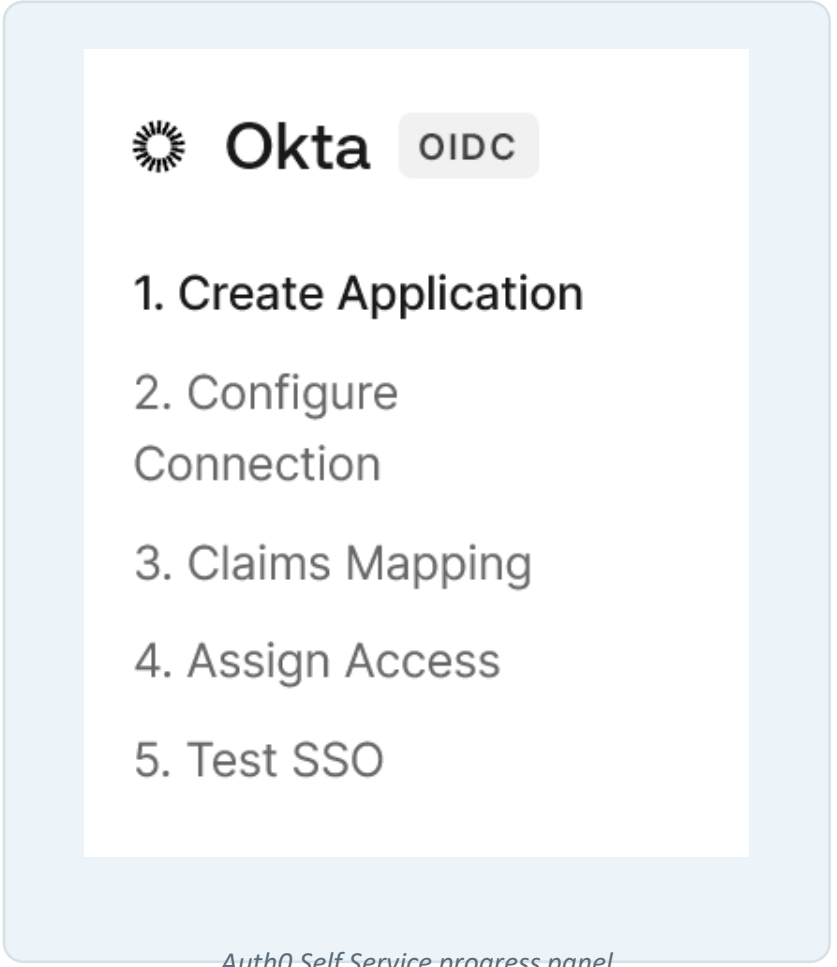
Assign Access

Choose which Okta users or groups can use this connection.

5

Test SSO

Sign in through Okta with a test account and confirm the user lands in hStream.

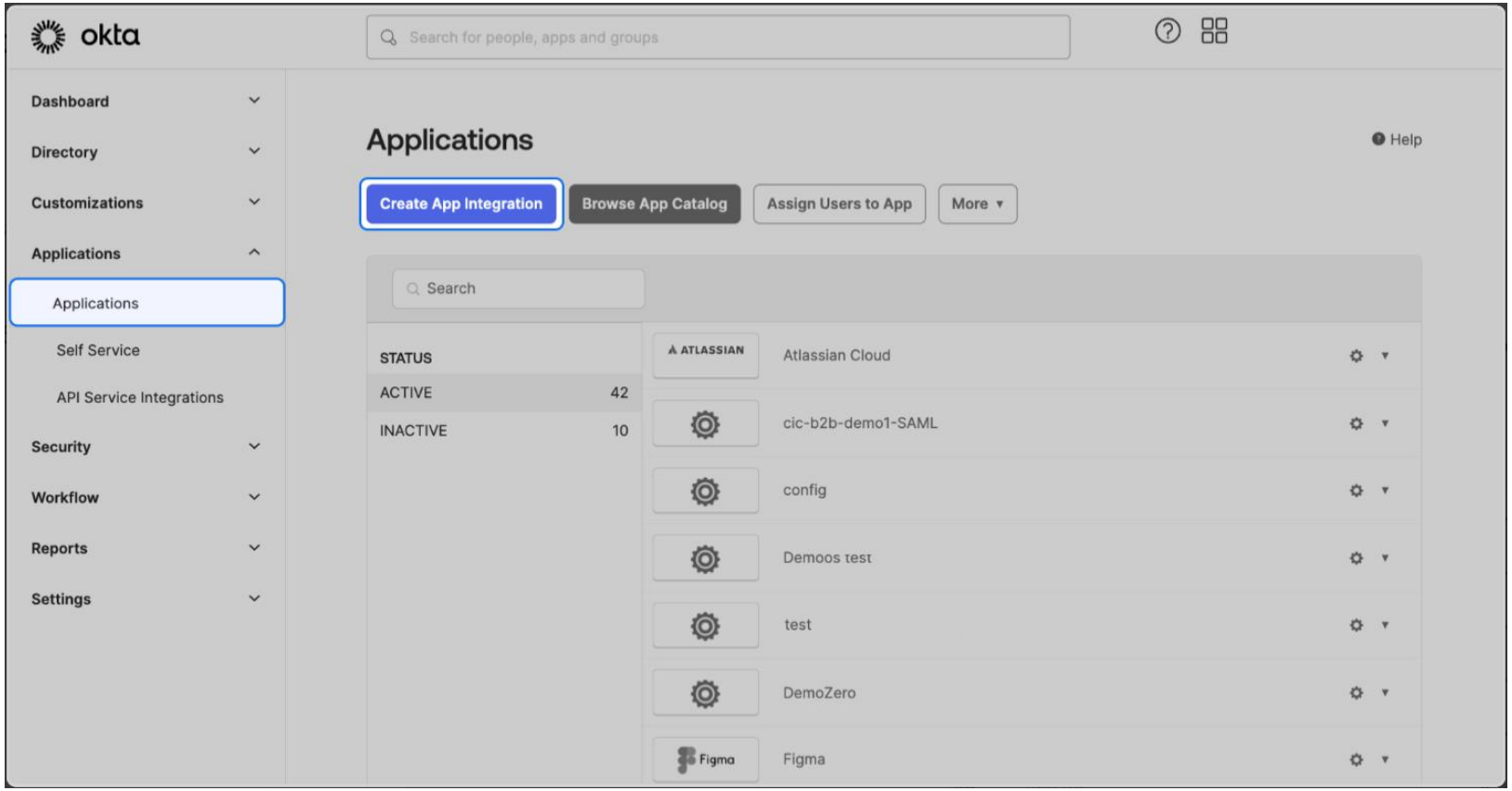


Auth0 Self Service progress panel

Create a New App Integration

1

- To connect your Okta tenant as an identity provider, you must create an OIDC application.
- Log in to the Okta Admin Console.
- Navigate to Applications › Applications.
- Select Create App Integration.

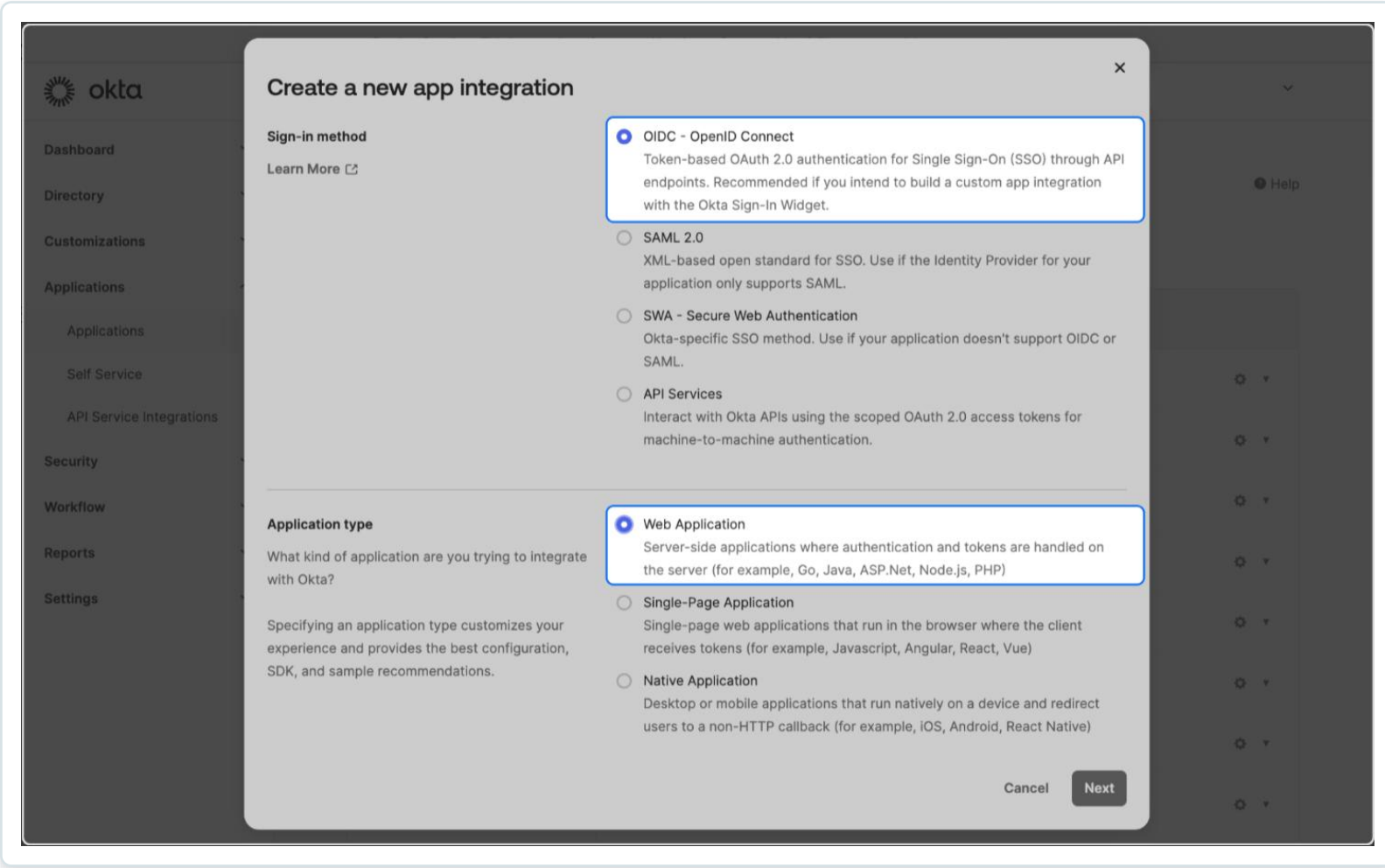


Okta Admin Console — Applications

Choose OIDC and Web Application

1

- For Sign-in method, choose OIDC – OpenID Connect.
- For Application type, choose Web Application.
- Select Next.



Create a new app integration

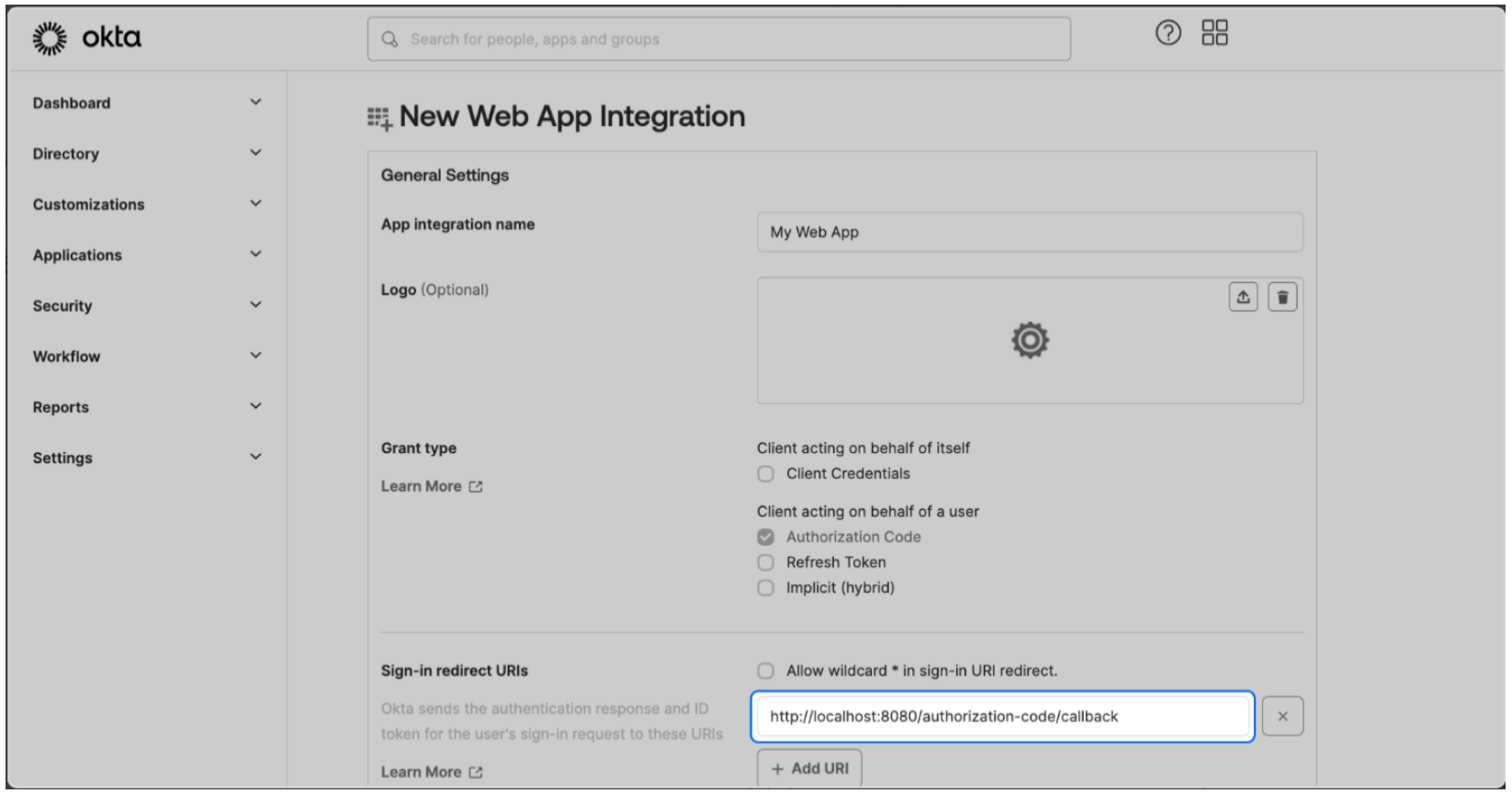
Name the App and Add the Redirect URI

1

- Enter your App integration name, such as “hStream Auth0 SSO”.
- Copy the Redirect URI provided by the Auth0 Self Service portal and add it to the Sign-in redirect URIs field:

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

Select Save.



New Web App Integration — Sign-in redirect URIs

Record the Application Credentials

After the application has been created, record the following values — you'll need them in the next step.

1. **Client ID**
2. **Client Secret**
3. **Okta Domain URL**

Copy the Client ID and Client Secret — you will use them next to configure your Okta connection.

STEP 2 · CONFIGURE CONNECTION

Bring the Okta Details into Auth0

2

Within the Auth0 Self Service portal, enter the values recorded from Okta.

1 **Okta Domain**

2 **Client ID**

3 **Client Secret**

Auth0 will use these values to establish a secure OIDC trust relationship with your Okta environment. Once all required fields have been completed and validated successfully, select Next.

STEP 3 · CLAIMS MAPPING

Map Okta Claims to HealthStream Attributes

3

Claims mapping allows Auth0 to understand which user attributes should be passed from Okta to hStream. Review and map the required user attributes.

Okta Claim - Required	hStream Attribute
email	Email Address
given_name	First Name
family_name	Last Name
sub or employee ID	External User Identifier
Username * Add this required attribute only if the HLC username is not the email address.	preferred_username

Why this matters

- Verify that all required fields are mapped correctly. Proper attribute mapping helps ensure users are identified and matched successfully during login.
- After confirming the mappings, continue to the next step.

4

Assign Access to Your Okta Users

1 Open Assignments

Within Okta, open the application you created and select Assignments.

2 Choose how to assign

Assign individual users, assign groups, or enable access for larger populations after testing.

3 Start with a test group

For initial validation, it is recommended to assign a small test group.

4 Return to Auth0

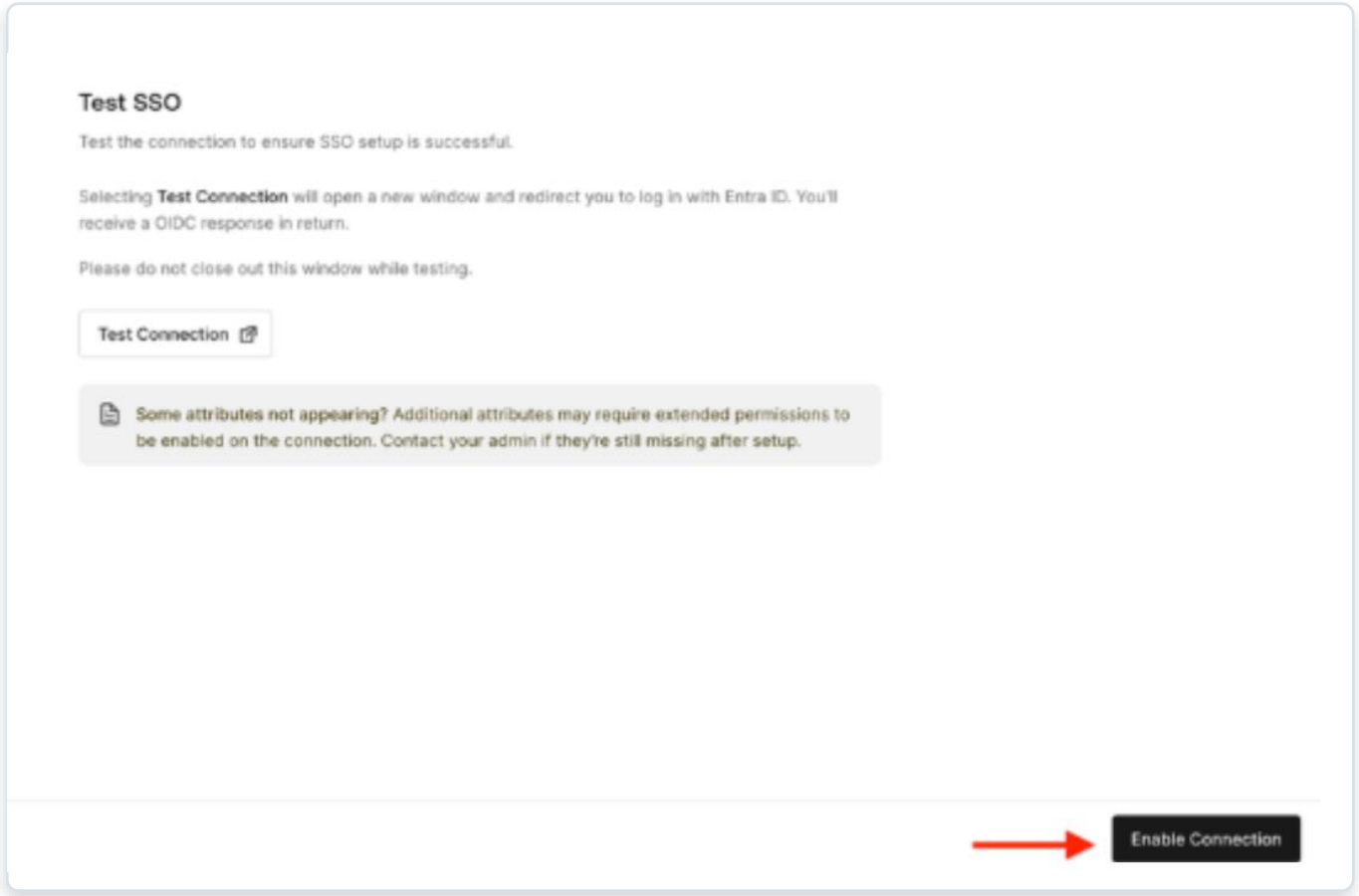
Once assignments have been completed, return to Auth0 Self Service and proceed.

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

Common Validation Checklist

Confirm the following before moving your users to production.

- ✓ Okta application created
- ✓ Client ID and Client Secret entered into Auth0
- ✓ Test users assigned
- ✓ Redirect URI copied correctly
- ✓ Required claims mapped

Thank You

Your Okta OpenID Connect connection is now configured using Auth0 Self Service. Users assigned to this application can now access HealthStream using their organization's Okta credentials through a secure Single Sign-On experience.

For additional assistance, refer to your organization's implementation guide or contact the HealthStream Platform team.