hStream™

ADFS (SAML) Configuration

Auth0 Self Service — Connecting Active Directory Federation Services as a SAML identity provider for Single Sign-On into HealthStream.

September 2026

Before You Begin

! Do not delete or remove your existing SSO connection in ADFS 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 ADFS 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.

Select Identity Provider

- From the self-service portal landing screen, select ADFS as your identity provider type.

This selects the ADFS-specific instructions for the remaining screens in this guide. If your organization uses a different IdP, choose that provider instead — the screens from here on will differ.

WHAT WE'LL COVER

Three Steps to a Working SSO Connection

1 Add a Relying Party Trust

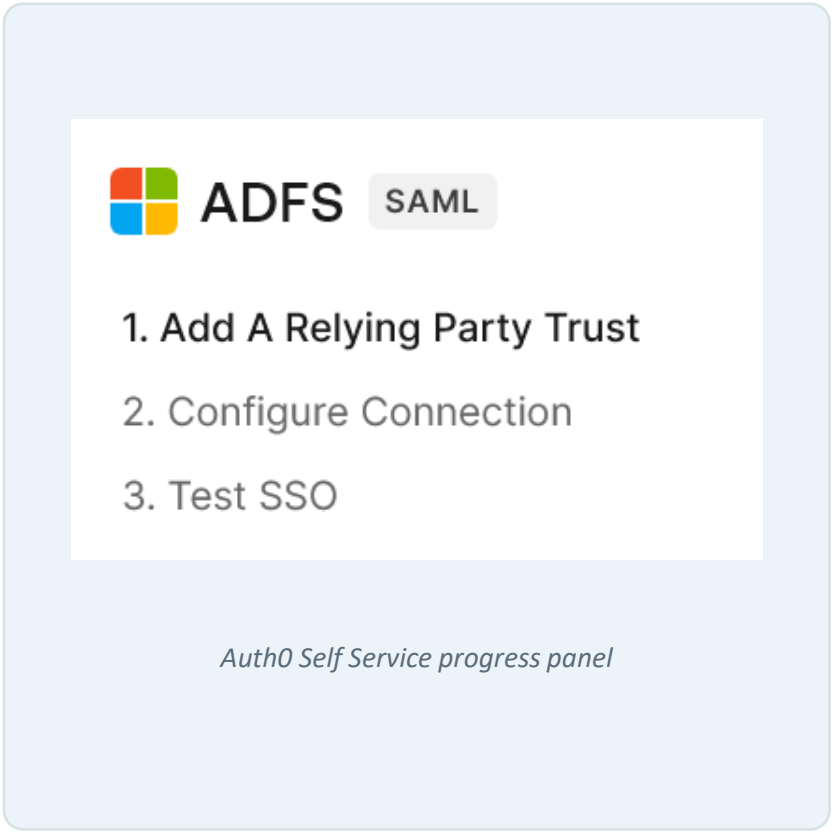
Create the trust in ADFS and issue the claims Auth0 needs (email, name, and a unique identifier).

2 Configure Connection

Bring the ADFS metadata into the Auth0 Self Service portal so it can validate SAML assertions.

3 Test SSO

Sign in through ADFS and confirm the test is successful.

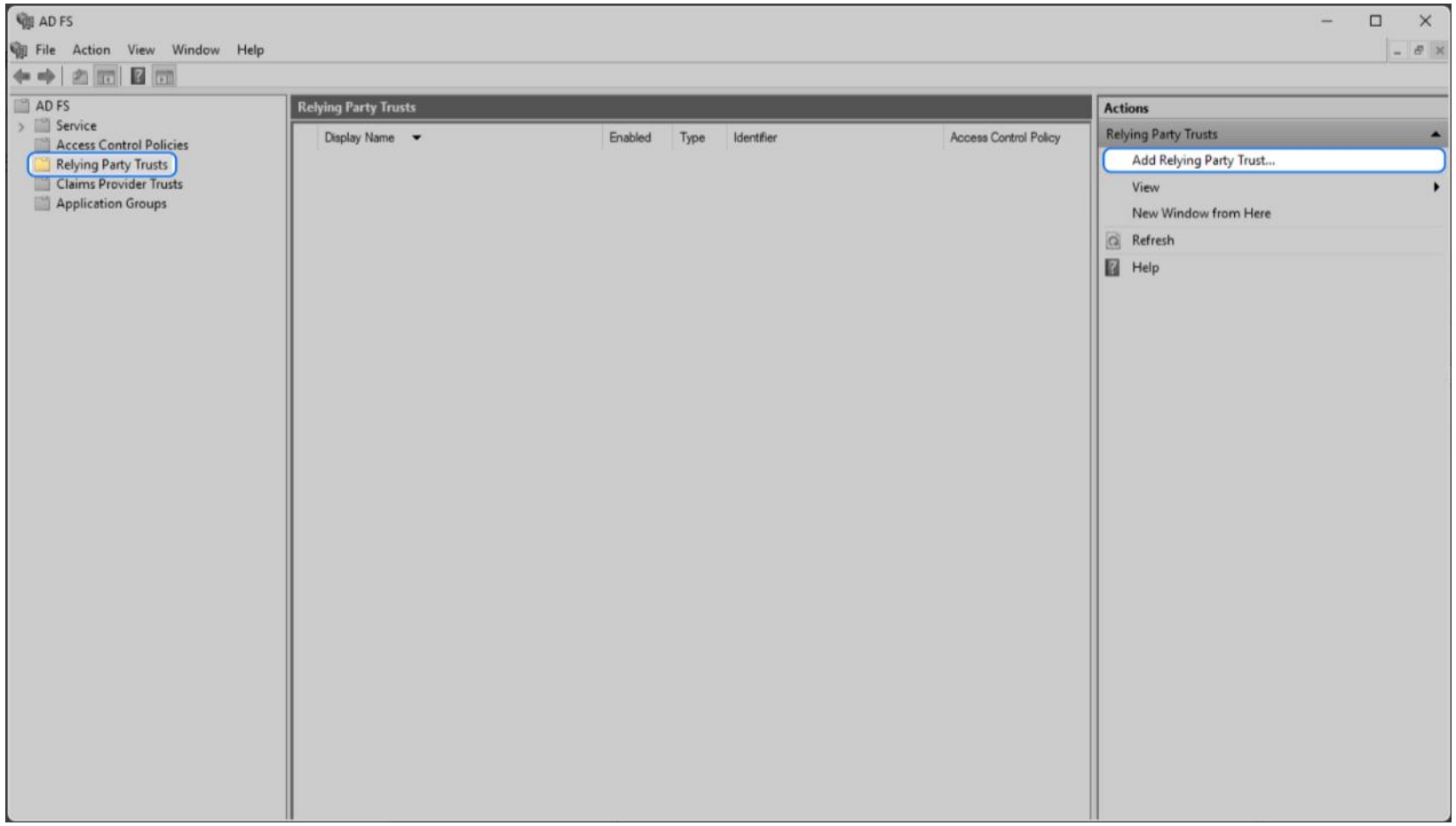


Auth0 Self Service progress panel

Launch the Add Relying Party Trust Wizard

1

- Open the ADFS Management Console.
- Expand Trust Relationships in the left panel.
- Select Relying Party Trusts.
- Under Actions, click Add Relying Party Trust…

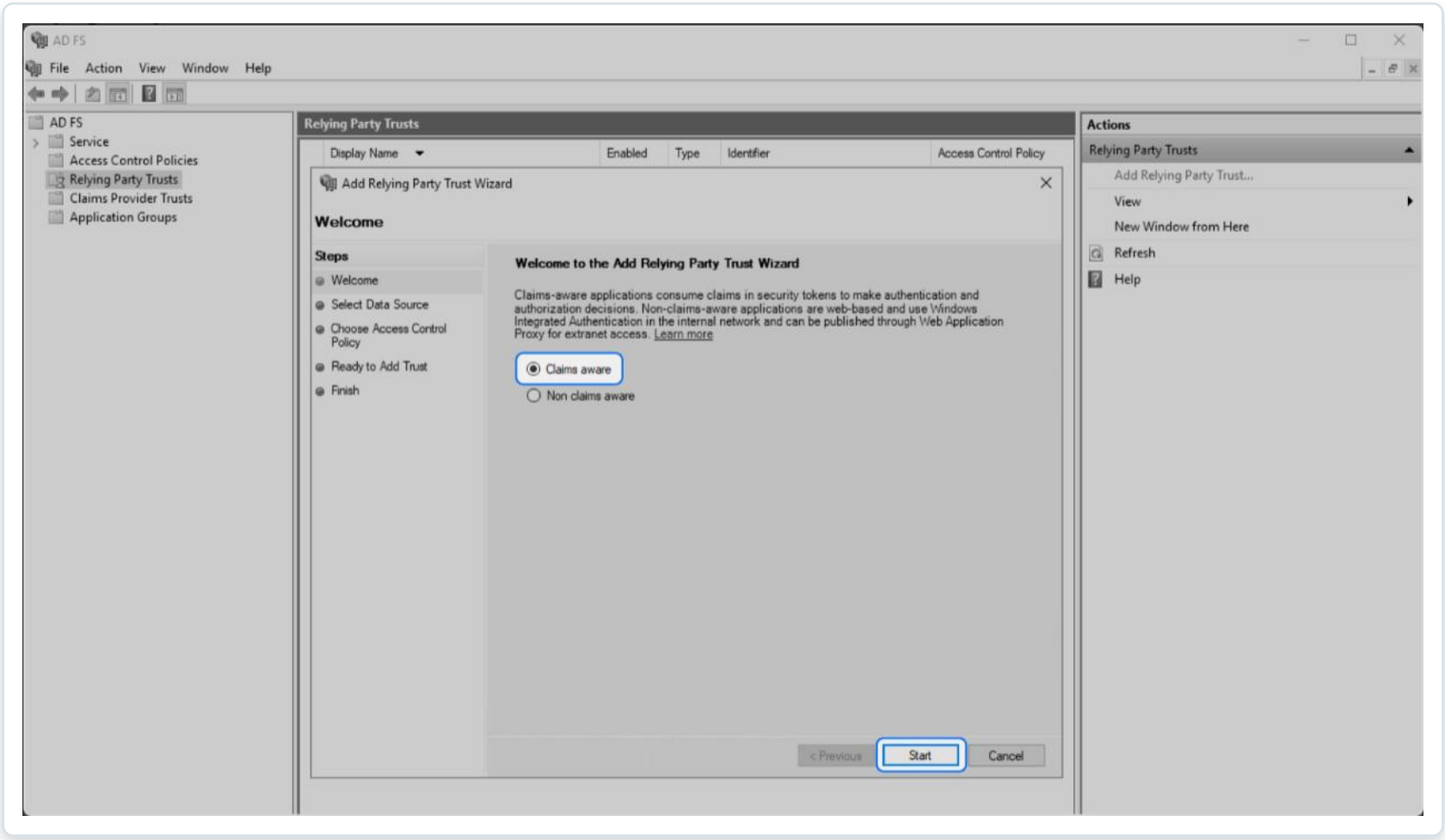


ADFS Management Console — Relying Party Trusts

Choose “Claims Aware”

1

- Select Claims aware, then click Start.

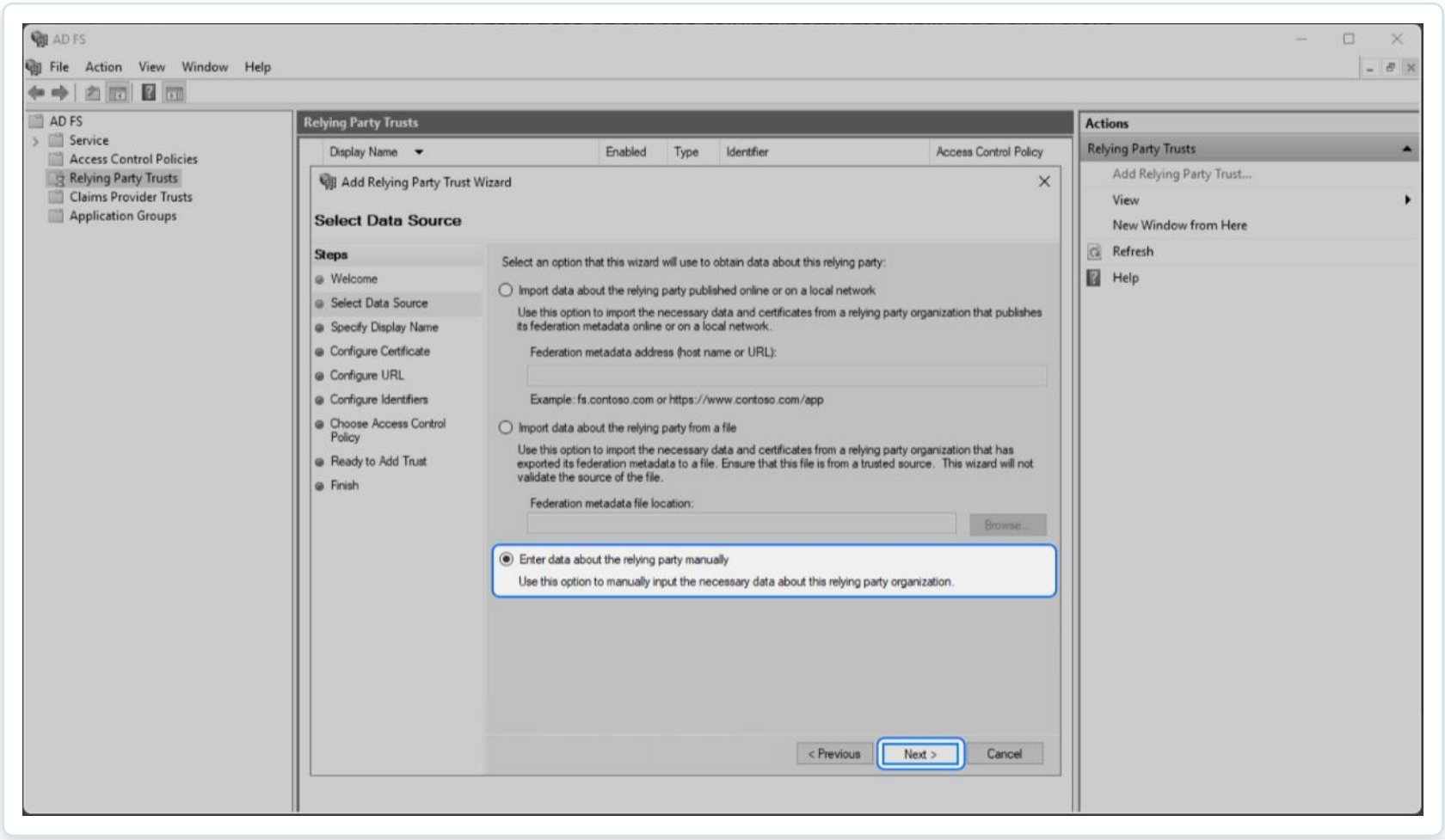


Welcome step — select Claims aware

Choose How to Supply Relying Party Data

1

- Select “Enter data about the relying party manually” and click Next.



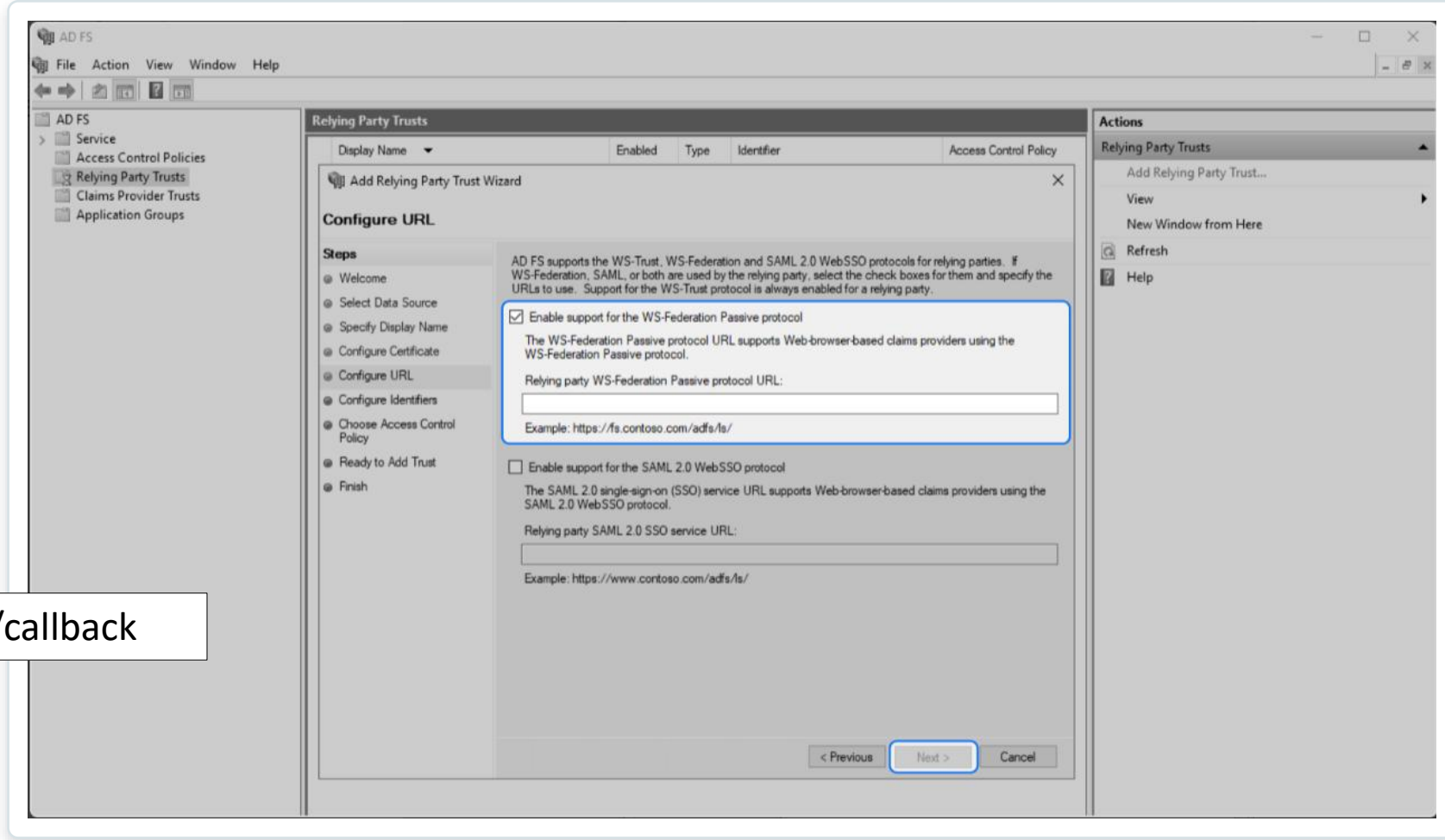
Select Data Source — manual entry

Configure the WS-Federation URL

1

- Enter a Display name and click Next.
- Skip the Configure Certificate step.
- On Configure URL, enable support for the WS-Federation Passive protocol.
- Paste the Reply URL provided by Auth0 Self Service:

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



Configure URL — WS-Federation Passive protocol URL

Configure the Relying Party Identifier

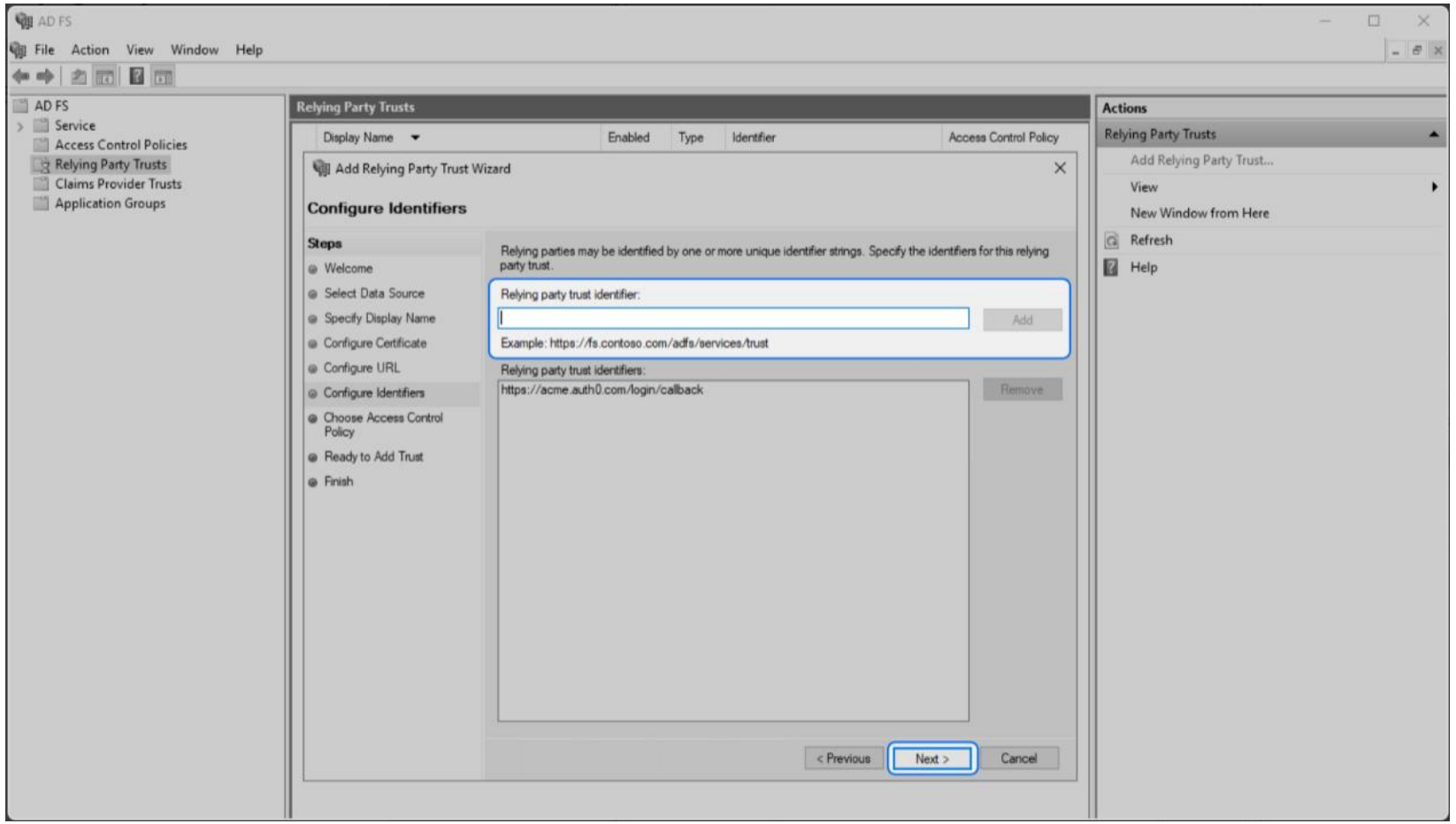
1

- On Configure Identifiers, add the Relying party trust identifier.
- This is the ADFS ID (Identifier) provided by Auth0 Self Service, for example:

urn:auth0:prod

urn:auth0:prod

Click Add, then Next.

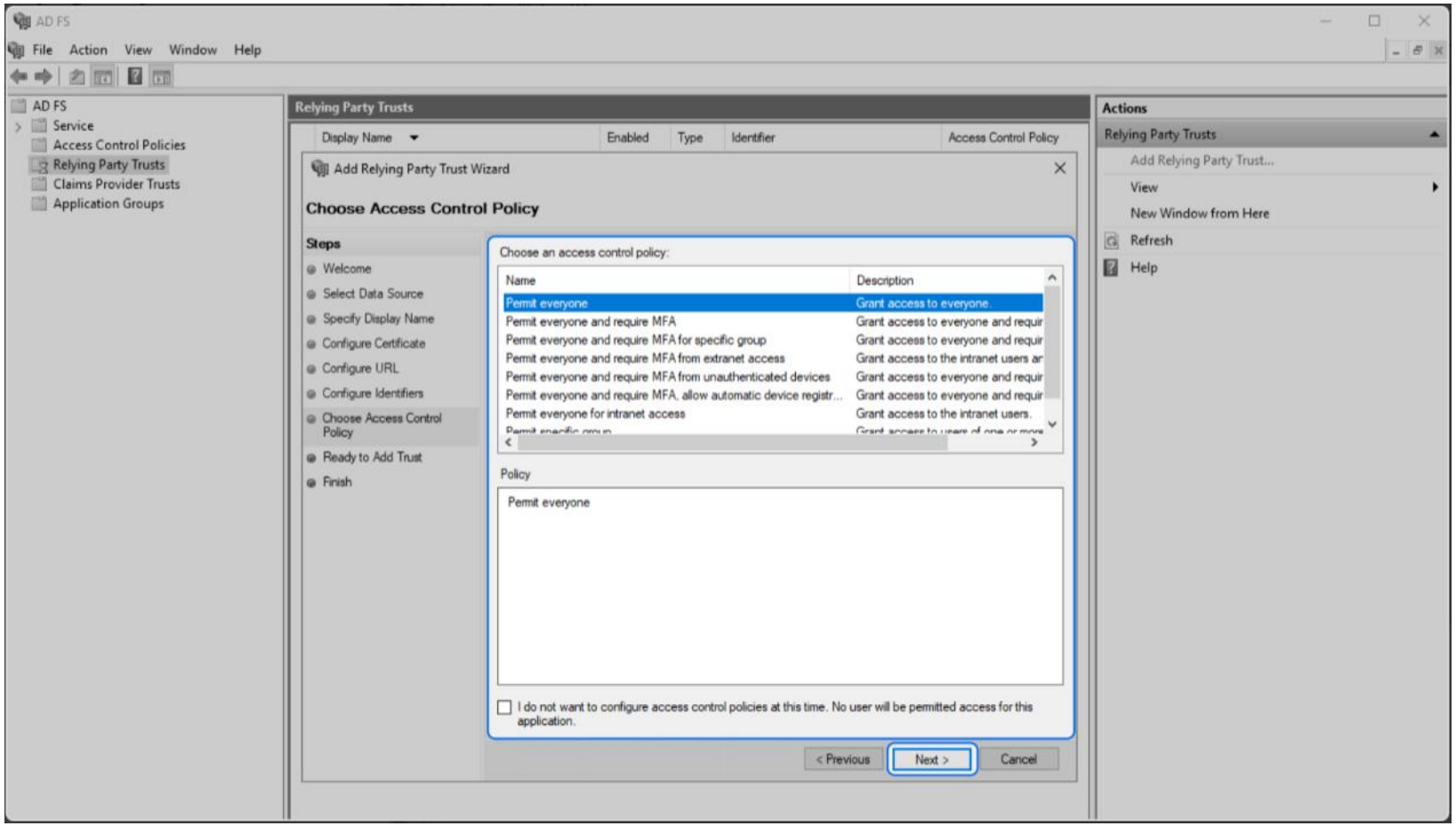


Configure Identifiers — relying party trust identifier

Choose an Access Control Policy

1

- On Choose Access Control Policy, grant users or groups access by selecting the permissions that fits your organization.
- Common choices include Permit everyone.
- Click Next, then Next again on Ready to Add Trust.

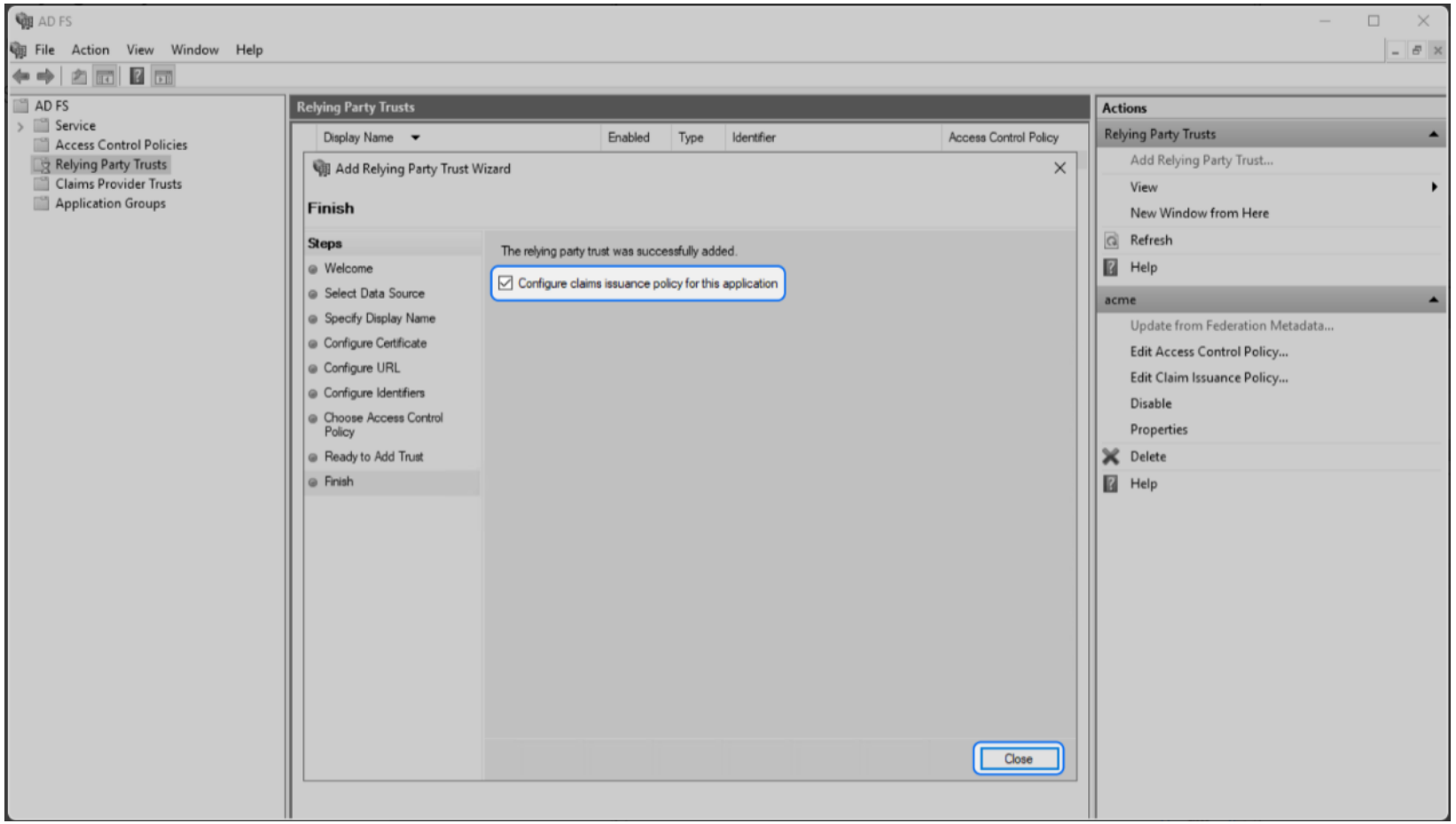


Choose Access Control Policy

Finish — Open the Claims Issuance Policy

1

- The relying party trust was successfully added.
- On the Finish step, keep “Configure claims issuance policy for this application” checked.
- Click Close to continue directly into claim rule setup.



Finish — trust added successfully

Configure Claim Rules

1

After creating the trust, edit it and open the Claims Issuance Policy. Create rules to send the required attributes to Auth0.

Active Directory Attribute Required	SAML Claim
E-Mail Address	email
Given Name	given_name
Surname	family_name
UPN or Employee ID	nameidentifier
Username * Add this required attribute only if the HLC username is not the email address.	preferred_username

Why this matters

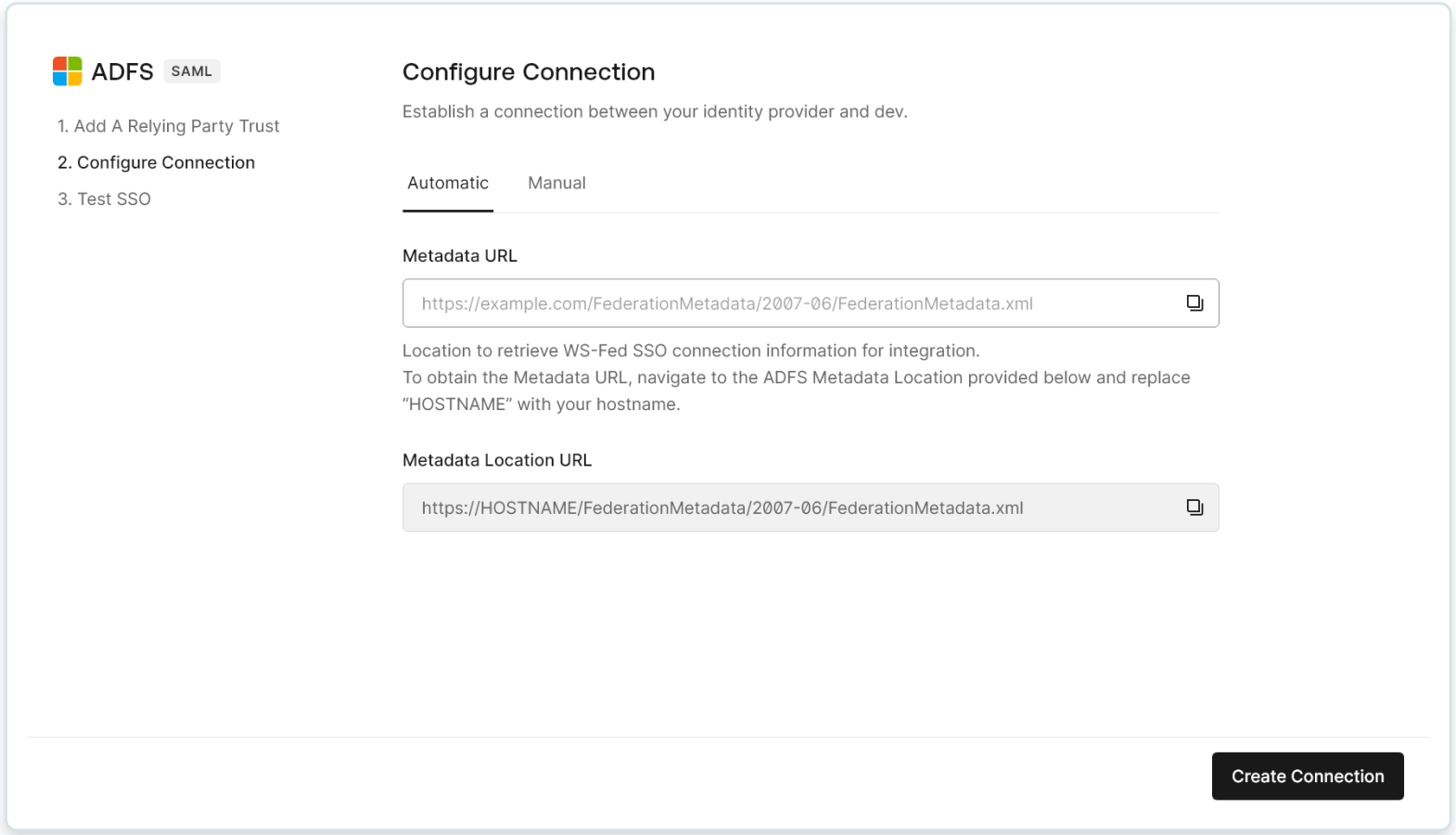
- Ensure the email claim is populated correctly — it's commonly used for user identification in hStream.
- Save the claim rules once configuration is complete.

STEP 2 · CONFIGURE CONNECTION

Bring ADFS Metadata into Auth0 Self Service

2

- Return to the Auth0 Self Service portal and enter the configuration information from ADFS.
- Typical values required:
- – Federation Metadata URL
- – Identity Provider Entity ID
- – SAML Sign-In URL
- – X.509 Signing Certificate
- These are often available directly from the ADFS Federation Metadata document.



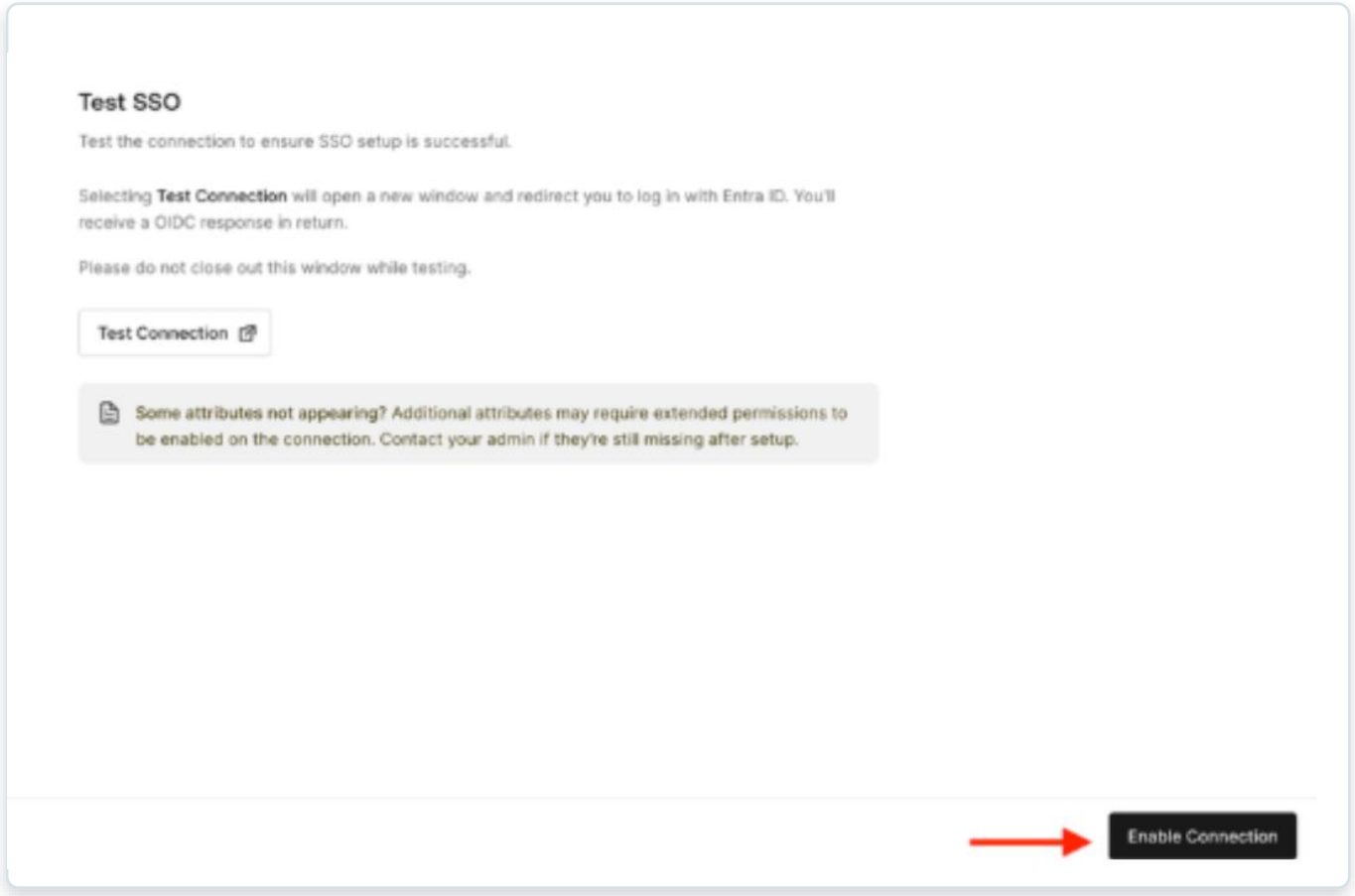
Auth0 Self Service — Configure Connection

Enable & Test Connection

2

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

- **Step 2 : Enable the Connection**



Auth0 Self Service — Enable Connection

BEFORE YOU GO LIVE

Validation Checklist

Confirm the following before enabling SSO for your organization.

- ✓ Relying Party Trust created in ADFS
- ✓ Trust Identifier configured
- ✓ Metadata information entered into Auth0
- ✓ Permissions granted for all user groups
- ✓ Test account authenticated successfully

Thank You

Now your ADFS SAML 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 ADFS credentials.

For additional assistance, contact your HealthStream Success Manager or your ADFS administrator.