Configure Custom SAML Single Sign-On

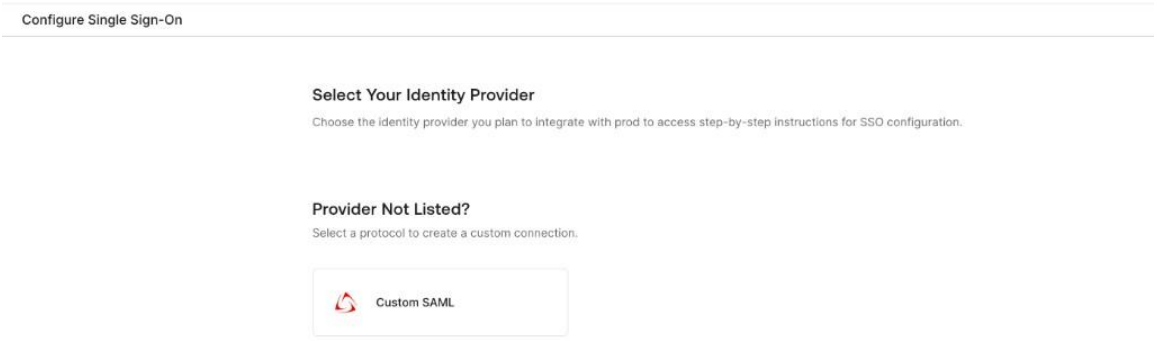
This guide walks you through setting up a **Custom SAML** connection so your users can sign in to HealthStream with your identity provider (IdP).

Your HealthStream Success Manager will send you a **self-service URL**. Open that link and follow the steps below.

It helps to have your IdP's **metadata URL** ready (or, for a manual connection: sign-in URL, entity ID, and signing certificate).

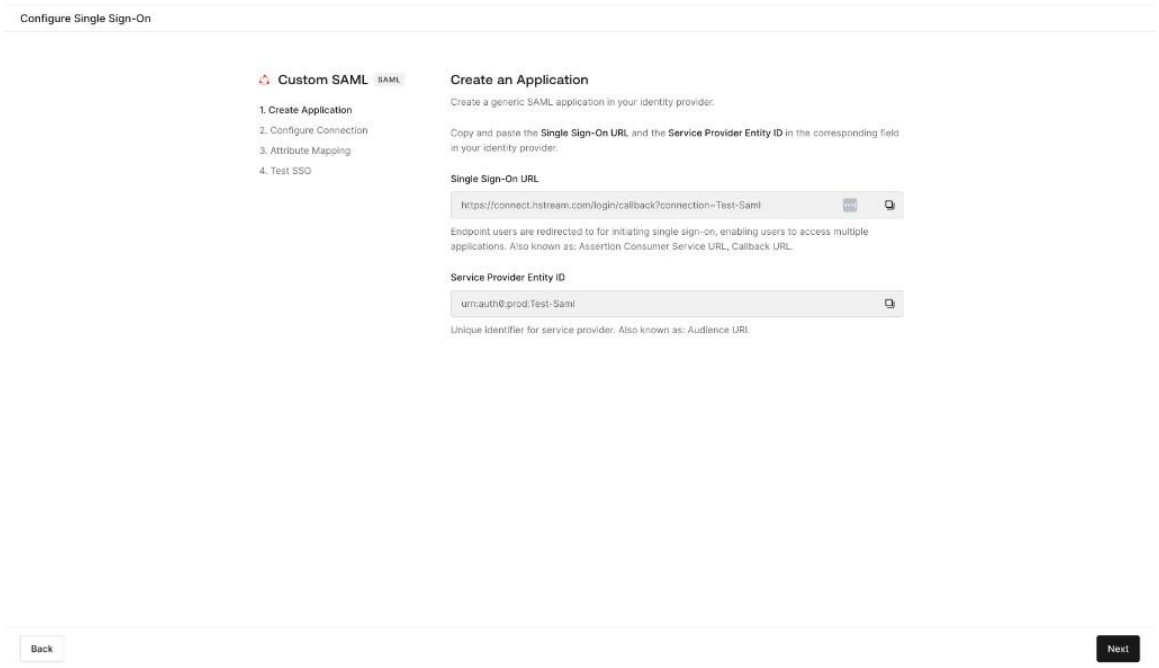
1. Select Custom SAML

1. Open the **self-service URL** from your HealthStream Success Manager. This opens **Configure Single Sign-On**.
2. Under **Select Your Identity Provider**, review the listed providers.
3. If your provider is not listed, under **Provider Not Listed?**, select **Custom SAML**.



2. Create an application in your identity provider

Create a generic SAML application in your IdP, then paste the Service Provider values shown in the wizard.



4. In your identity provider, create a **generic / custom SAML 2.0 application**.
5. In the wizard, use the **copy** buttons to copy **Single Sign-On URL** and **Service Provider Entity ID**, then paste them into the matching fields in your IdP.

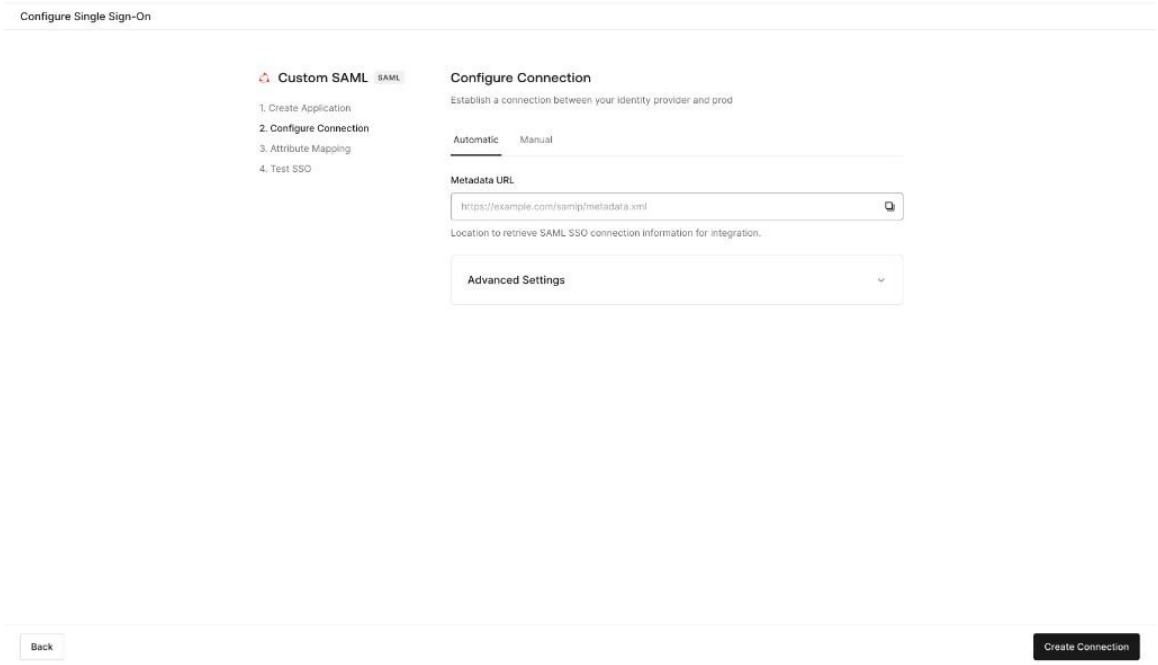
Wizard field	**Also known as in your IdP**
Single Sign-On URL	ACS URL, Callback URL, Reply URL
Service Provider Entity ID	Audience URI, Entity ID, SP Entity ID

Always copy these values from the wizard. Do not use sample values from this document.

6. Save the application in your IdP.
7. In the wizard, select **Next**.

3. Configure the connection

Provide your IdP metadata to connect your identity provider with HealthStream.



Automatic (recommended)

8. Select the **Automatic** tab.
9. In your IdP, locate the **SAML metadata URL** (sometimes called Federation Metadata URL).
10. Paste it into **Metadata URL** in the wizard.
11. Optionally expand **Advanced Settings** if your IdP needs non-default options.
12. Select **Create Connection**.

Manual

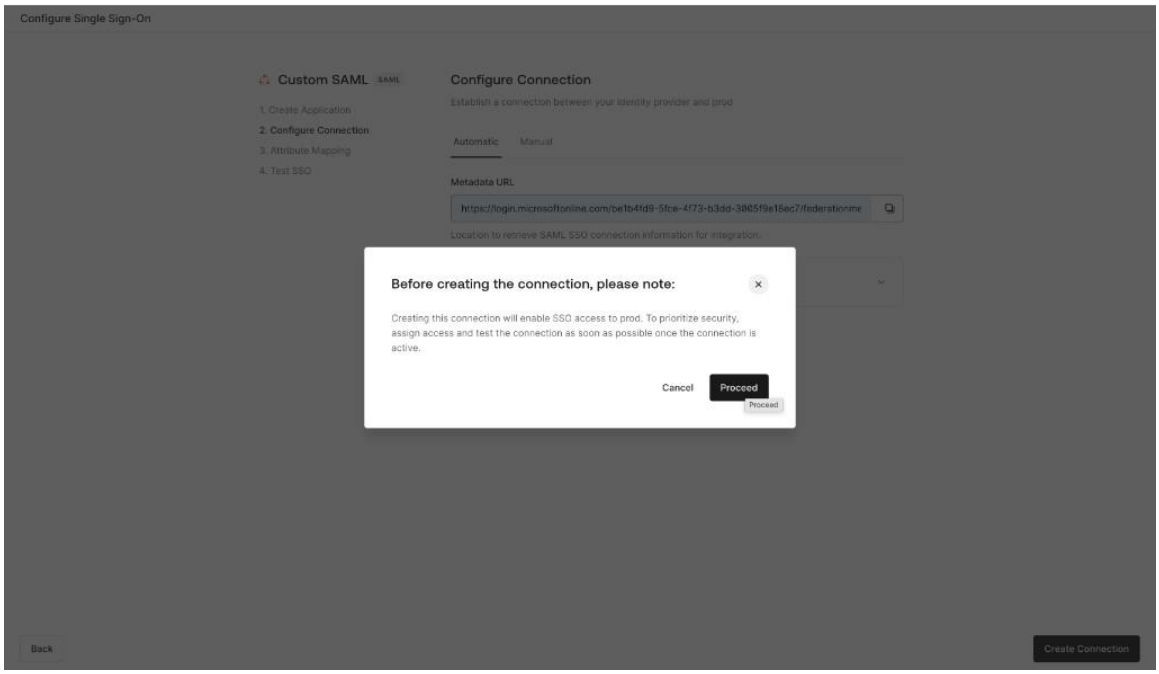
13. Select the **Manual** tab.
14. Enter the values from your IdP:

- Sign-in URL
- Entity ID / Issuer
- X.509 signing certificate

15. Select **Create Connection**.

Confirm creation

After you select **Create Connection**, a confirmation dialog appears:

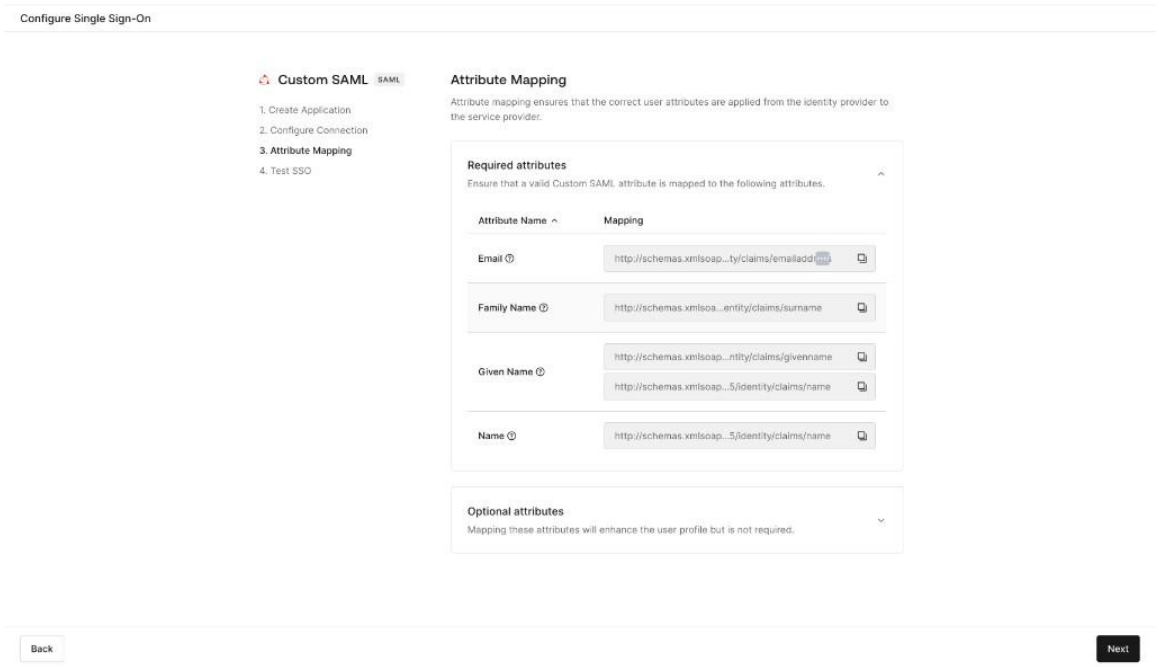


Important: Creating this connection enables SSO access to HealthStream. Assign access in your IdP and test the connection as soon as it is active.

Select **Proceed** to create the connection, or **Cancel** to go back.

4. Attribute mapping

Attribute mapping ensures the correct user attributes from your IdP are applied in HealthStream.



Required attributes

16. Open **Required attributes** in the wizard.

17. Use the **copy** buttons next to each mapping value.
18. Paste those values into the matching attribute / claim settings in your IdP.

Always copy mapping values from the wizard.

NameIdentifier (HLC User ID)

In addition to the attributes in the wizard, your IdP **must** send the user's **HLC User ID** as the SAML **NameIdentifier** (`NameID`).

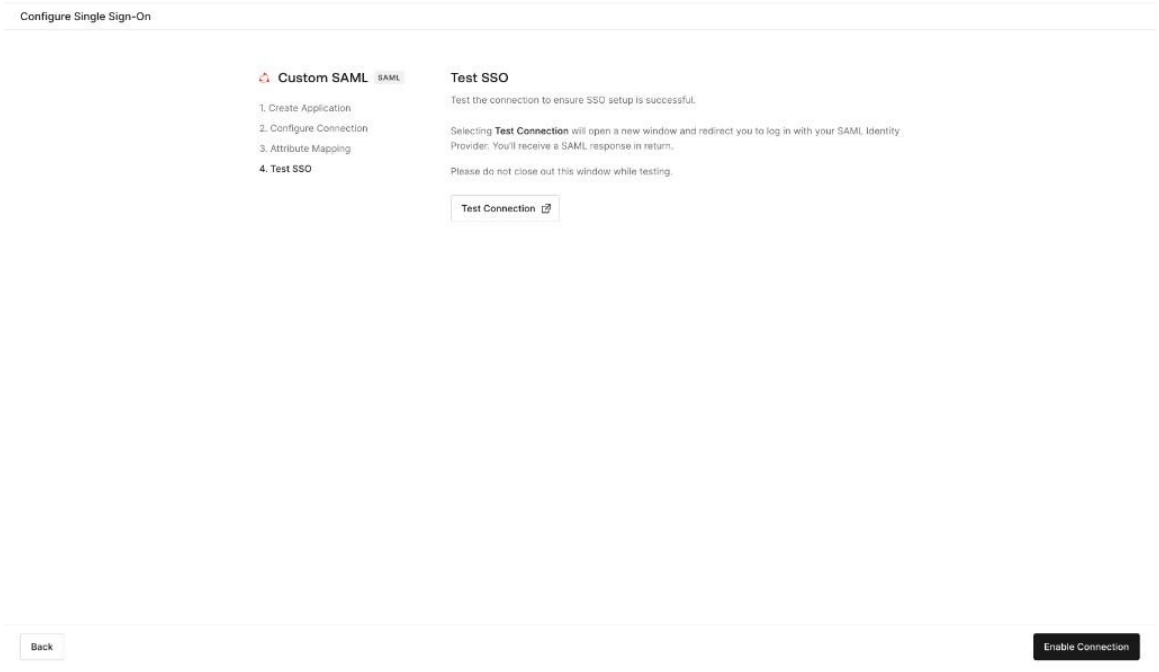
Configure this in your IdP (Subject NameID or equivalent). SSO will not work correctly if NameID is missing or is not the HLC User ID.

Optional attributes

Expand **Optional attributes** in the wizard if you want to enrich the user profile. These are not required for SSO.

When finished, select **Next**.

5. Test SSO and enable the connection



Test the connection

19. Select **Test Connection**. A new window opens and redirects you to your SAML identity provider.
20. Sign in with a test user that has access to the SAML application in your IdP.
21. After a successful login, you receive a SAML response confirming the connection works.
22. Do not close the original wizard window while testing.

Enable the connection

23. After a successful test, return to the wizard.

24. Select **Enable Connection** to turn on SSO for HealthStream.

Checklist

- Custom SAML application created in the IdP
- Single Sign-On URL and Entity ID copied from the wizard into the IdP
- Metadata URL (or manual IdP values) entered in the wizard
- Connection created
- Required attributes copied from the wizard into the IdP
- HLC User ID sent as SAML NameIdentifier (NameID)
- Test Connection successful
- Access assigned to the correct users/groups in the IdP
- Connection enabled

Troubleshooting

Issue	What to check
Users cannot sign in	Confirm the Single Sign-On URL and Entity ID in the IdP match the wizard exactly.
Metadata URL fails	Confirm the URL is reachable and returns valid SAML metadata. Use Manual if your IdP does not publish a metadata URL.
Login succeeds but profile is incomplete	Recopy required attribute mappings from the wizard; ensure Email is in the SAML assertion.
User cannot be matched in HLC	Confirm NameIdentifier (NameID) is the user's HLC User ID.
Test window does nothing / closes early	Keep the wizard open, allow pop-ups, and retry Test Connection.
Wrong users can access HealthStream	Restrict assignment in your IdP to the intended users or groups.

Need help?

Contact your HealthStream Success Manager or support with:

- Connection name
- IdP type
- The step where the issue occurred
- Any error message from **Test Connection**