

## SSO Configuration Process

Your organization and ProviderTrust will need to exchange SSO connection metadata so that both systems can know how to communicate with each other. Your system will act as the identity provider (IdP) and ProviderTrust software will be the service provider (SP).

The general process for exchanging metadata and configuring the connection is as follows:

1. Add ProviderTrust to your IdP and generate your metadata. Use the information in this document to configure your IdP. The process will differ depending on whether you are connecting with SAML or WS-Fed.
2. Return the completed SSO Questionnaire, along with your IdP metadata.
3. ProviderTrust's technical team will configure our side of the SSO connection. Once complete, we will notify your team as well as provide a copy of our SP metadata.

## Configuring a SAML connection

You can use the following values to configure a SAML connection with ProviderTrust.

- SP Entity Id = urn:auth0:providertrust:<CLIENTNAME>
- SP Assertion Consumer Service (ACS) URL = <https://login.providertrust.com/login/callback?connection=<CLIENTNAME>>
- SP Single Logout URL = <https://login.providertrust.com/logout>

## Configuring a WS-Fed connection

You can use the following values to configure a WS-Fed connection between your ADFS server and ProviderTrust.

- Realm Identifier = urn:auth0:providertrust
- WS-Fed Endpoint = <https://login.providertrust.com/login/callback>

It is expected that the Realm Identifier listed above is the only Identifier configured for your Relying Party Trust.

## SSO Attribute Mapping

Certain user attributes should be sent by your IdP during SSO login. You will need to configure your IdP to map these user attributes into the SSO response. This process will vary depending on your IdP.

The following table lists all required and recommended attributes used by Provider software, along with the expected name of each attribute in the SSO response.

User Attribute	Expected SSO Attribute Name
Name ID (required):	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier
Email (required):	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
First Name (optional):	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname
Last Name (optional):	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname
Display Name (optional):	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name

The Name ID attribute is required, but it can be sent in any format. This includes UPN, Email, and so on. Also note that the Email attribute must be sent as its own attribute in all scenarios, even if you send an email address as the Name ID attribute.

The provided SSO attribute names should be the default in most cases. If your SSO setup is unable to support this attribute naming convention for some reason, please note that in your SSO Questionnaire response. We may be able to provide a custom attribute mapping for your connection.

## Additional Configuration Info

ProviderTrust software only supports SP-initiated SSO. Login cannot be initiated directly from your IdP. The SSO login process is initiated by visiting one of the URLs provided in your SSO Questionnaire.