·✳· Structured

17.5 Salesforce as IdP QuickStart

Salesforce can act as an IdP via **SAML** or as an **OIDC Authorization Server**.

17.5.1 Salesforce as SAML IdP (most common)

1. **Enable Salesforce as Identity Provider** in your Salesforce org.
2. **Create a Connected App** for Structured AI:
   - Set SAML settings:
     - ACS URL:
       `https://AUTH_DOMAIN/auth-management/sso/saml/acs`.
     - Entity ID: provided by Structured AI.
     - NameID format: email address or persistent ID (aligned with our configuration).
   - Map SAML attributes:
     - `Email` → `email`.
     - `FirstName` → `firstName`.
     - `LastName` → `lastName`.
     - Custom attribute (e.g., `Account_Id__c`) → `account_id`.
3. **Download IdP metadata** from Salesforce.
4. **Provide metadata** to Structured AI.
5. **Structured AI configures SsoConfig** with Salesforce SAML IdP.
6. **Test SAML login** with pilot users.

17.5.2 Salesforce as OIDC Provider (Authorization Server)

1. Enable **Salesforce as OAuth 2.0 / OpenID Connect provider** (depending on your edition).
2. Create a **Connected App** that supports OIDC:
   - Configure callback URL:
     `https://AUTH_DOMAIN/auth-management/sso/callback`.
   - Enable `openid` scope.
3. Configure ID token claims to include `email`, `given_name`, `family_name`, and `account_id` (via custom attributes if necessary).
4. Provide discovery URL, clientId, clientSecret to Structured AI.
5. Test login and claim mapping.