Single Sign-On (SSO) Configuration Guide

This guide explains how to integrate your existing Identity Provider (IdP) with our platform through Single Sign-On (SSO). Following these steps will streamline user access, improve security, and enhance the overall user experience.

Overview

Supported Protocols and Providers:

We support a wide range of industry-standard SSO protocols and identity providers, including:

- **SAML 2.0**
- **OpenID Connect (OIDC)**
- **Azure Active Directory (Azure AD)**
- **Okta**
- **Google Workspace**

If you have a different IdP, please contact our support team to determine compatibility.

Prerequisites

Before you begin, ensure you have:

1. **An Enterprise Account:**

SSO integration typically requires an enterprise-tier subscription. Confirm your account status or contact sales if you need to upgrade.

2. **Administrative Access to Your IdP:**

The person performing these steps must have admin rights to configure SSO settings in the IdP's console.

3. **Required SSO Configuration Data:**

Gather the following information from your IdP:

- **Metadata URL or XML File:** This includes IdP configuration details (SAML only).
- **SSO URL (Login URL):** The endpoint where authentication requests are sent.
- **x509 Certificate:** The public signing certificate used by the IdP to validate SAML assertions (SAML only).
- **Entity ID (Issuer):** A unique identifier for your IdP.

For OIDC-based IdPs, you may need:

- **Well-Known Configuration URL (Discovery Document)**
- **Client ID and Secret (if applicable)**

Check your IdP's documentation for specifics.

Configuration Steps

Step 1: Initiate the Setup

1. **Contact Our Support Team:**

Send an email to support@syntheticusers.com or use your customer portal to request SSO setup assistance. Include your company name, account details, and the intended IdP.

2. **Provide IdP Details:**

Our team will request the SSO configuration data mentioned above. Ensure you have the correct metadata or relevant URLs ready.

Step 2: Configure in Our Platform

1. **Internal Configuration (Handled by Our Team):**

Once we receive your information, our engineers will set up the SSO integration within our Google Firebase-based identity infrastructure. This includes:

• Adding your IdP's metadata and SSO endpoints.

• Mapping required attributes/claims (e.g., email, name, groups).

• Configuring access policies and session durations as per your requirements.

2. **We Provide You With the Following (SAML scenario):**

• **Service Provider (SP) Entity ID:** Our platform's unique identifier for your IdP.

• **Assertion Consumer Service (ACS) URL:** The endpoint in our service where the IdP should send authentication responses.

• **Login URL (Optional):** A direct link for testing SSO logins.

For OIDC or other identity providers, we will provide the equivalent client and redirect URLs.

Step 3: Configure in Your IdP

With the details provided by our team, log into your IdP's admin console and:

1. **Create a New Application/Integration:**

Depending on your IdP, this could be creating a new enterprise application (Azure AD), a custom SAML app (Okta), or configuring a new OIDC client.

2. **Enter Our Platform's Details:**

- **Entity ID (Issuer)**
- **ACS (Redirect) URL**
- **Login URL** (if applicable)

Ensure these values match exactly what we've provided. Incorrect values may cause authentication failures.

3. **Map User Attributes/Claims:**

At a minimum, your IdP should pass through a unique user identifier (like email). Additional attributes can help personalize the user's experience (e.g., given_name, family_name, roles).

4. **Upload or Reference Our SP Certificate (If Required):**

Some IdPs require you to register the SP's public certificate for encrypting assertions. If this is needed, our team will provide it.

Step 4: Testing

1. **Initial Validation with Our Team:**

Once both sides are configured, our support team will guide you through a preliminary test.

2. **Perform Test Logins:**

From your IdP portal, attempt to sign into our platform. Confirm that:

- The login redirects to your IdP as expected.
- After successful authentication, the user is correctly logged into our platform without a separate password.

3. **Troubleshooting (If Needed):**

If any issues arise, our support team will review IdP logs, ACS responses, and potential attribute mismatches to resolve the problem.

Step 5: Production Rollout

After successful testing:

1. **Enable SSO for Production Users:**

Decide whether all users should sign in exclusively via SSO or if a fallback method (e.g., password-based login) will remain available.

2. **Communication & Onboarding:**

Inform your end-users of the new SSO process. Provide them with the updated login URL or instructions to access our platform through their IdP's app launcher.

3. **Ongoing Maintenance:**

Review and renew certificates before expiration, keep IdP configuration details current, and notify our support team if you anticipate user schema or claim changes.

Security and Compliance Considerations

- **Encryption and Signing:**

Ensure all authentication requests and responses are signed and encrypted via SSL/TLS.

- **Certificate Validity:**

Regularly update and maintain your x509 signing certificates. Expired or invalid certificates will cause login failures.

- **Attribute Minimization:**

Only send the attributes your organization needs. This reduces data exposure and maintains compliance with privacy regulations.

Additional Support

If you need assistance at any step, contact support@syntheticusers.com Enterprise customers receive priority support, including the option to schedule guided setup calls.