WebApp Authentication with Social IDPs (Google, Facebook & Apple ID)

Field	Details
Document Type	Runbook / How-To Guide
Applies To	Microsoft Entra ID External Identities (CIAM), Social Identity Providers (Google, Facebook, Apple), Third-party Web Applications
Audience	Systems Administrators / Identity Engineers / 2nd Line Support
Author	AK. Udofeh
Last Updated	March 2026

Overview

This guide documents how to integrate Social Identity Providers (Google, Facebook, and Apple) with a SAML-based web application for authentication using Microsoft Entra ID External Identities and Customer Identity & Access Management (CIAM). The configuration allows users to authenticate using social accounts while Microsoft Entra acts as the identity broker and issues a SAML assertion to the third-party or line-of-business (LOB) web application.

The process involves creating an external tenant, registering social identity providers, creating a user flow, configuring a SAML enterprise application, and updating the application configuration.

The Issue

Organisations often require users to authenticate using Social Identities (e.g. Google or Facebook) while maintaining a centralised identity broker for security and policy enforcement.

Without a configured identity broker:

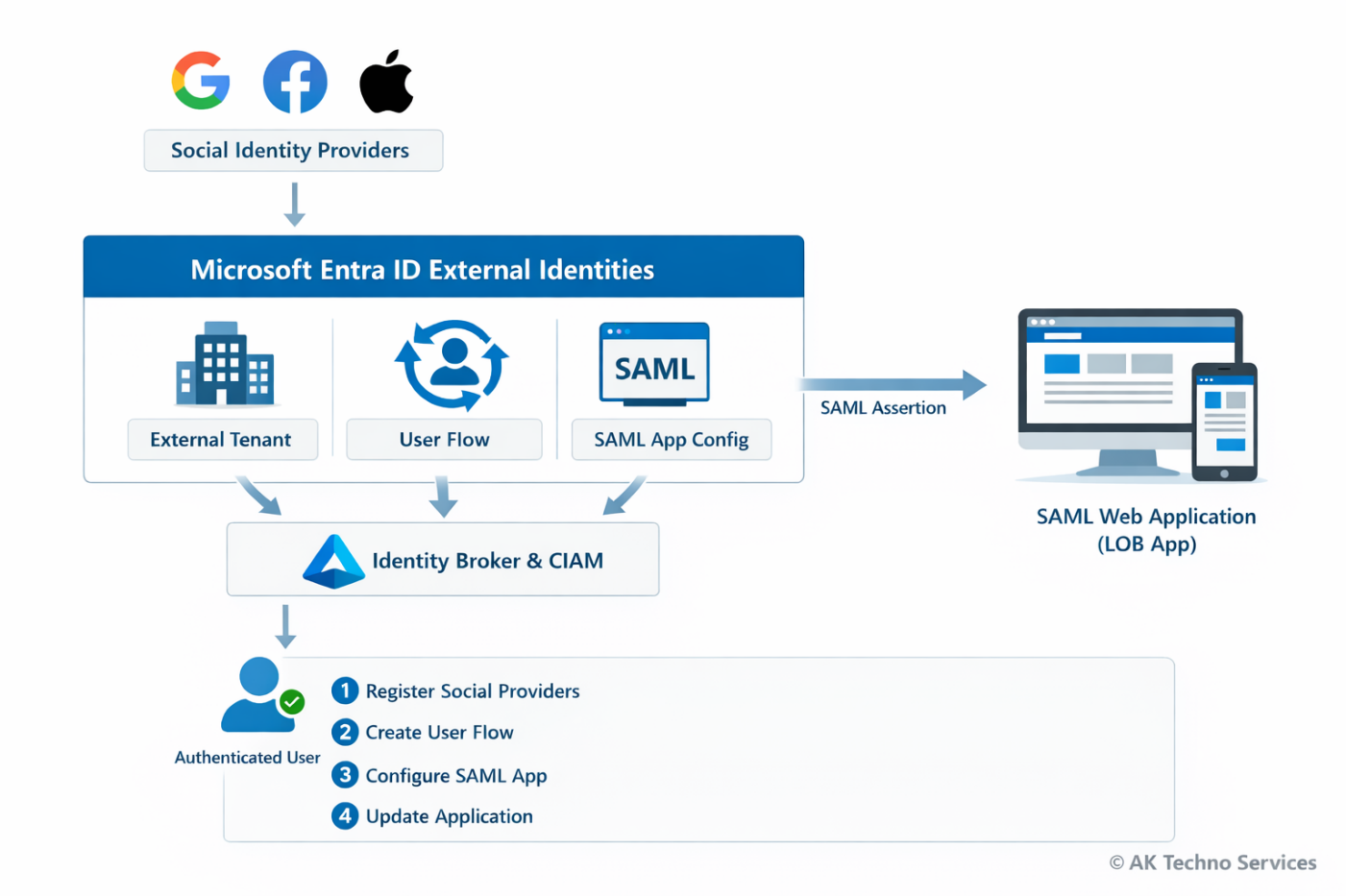
- Applications must integrate individually with each social provider.
- Identity attributes are inconsistent between providers.
- Access control and auditing become difficult to manage.

Basic authentication methods such as:

- Local application accounts
- Direct OAuth integration within the application

do not provide centralised identity management or federation capabilities.

Using Microsoft Entra External Identities resolves this by brokering authentication from social providers and issuing a standard SAML assertion to the application.



Context

Modern applications often require authentication from multiple identity providers while maintaining centralised access control.

Without a broker, the authentication flow typically looks like this:

```
User
  ↓
Application
  ↓
Direct OAuth with Google/Facebook
```

This causes several issues:

- Applications must implement provider-specific authentication logic
- Identity attributes differ between providers
- Access control cannot be centrally enforced

Using Microsoft Entra External Identities introduces an identity broker layer:

```
User
  ↓
Google / Facebook / Apple
  ↓  (OAuth / OIDC)
Microsoft Entra External Tenant (CIAM)
  ↓  (User Flow)
Enterprise Application (SAML)
  ↓
Flask Web Application
```

In this architecture:

- Social providers authenticate the user.
- Entra External Identities brokers the authentication.
- A SAML assertion is issued to the web application.

Before You Start

Check	Where
External tenant created	Microsoft Entra admin centre
Azure subscription linked	Tenant creation wizard
Google Developer Console account	console.cloud.google.com
Meta Developer account	developers.facebook.com
Apple Developer account (optional)	developer.apple.com
SAML web application deployed	Flask service
Service Provider metadata configured	`settings.json`

Implementation Steps (Per Environment)

Phase 1 - Create External Tenant

Step 1: Sign in to the Microsoft Entra admin centre:

https://entra.microsoft.com

Navigate to:

```
Microsoft Entra ID> Overview> Manage Tenants
```

Click:

```
Create> External
```

Enter the tenant details:

- Tenant Name: <Your tenant name>
- Domain Name: <Your domain name>

- Location: Europe or Africa
- Subscription: Azure subscription

Click:

```
Review + Create> Create
```

> Provisioning may take up to **30 minutes**.

Switch to the new tenant:

```
Settings> Directories + Subscriptions> Switch
```

Phase 2 - Add Social Identity Providers

Navigate to:

```
External Identities
> All Identity Providers
```

Integrate with Google Identity Provider

Step 1: Configure Google OAuth

Visit: https://console.cloud.google.com/

In Google Cloud Console:

```
APIs & Services
> Credentials
> OAuth2 Client ID
```

Fill in the Name of the Webapp

Add the Authorized redirect URI:

```
https://<tenant-subdomain>.ciamlogin.com/<tenant-subdomain>.onmicrosoft.com/federation/oauth2
```

Copy the following values and keep is save

```
> Client ID
> Client Secret
```

Step 2: Register Google as Idp in Entra ID

In Entra ID (Ext tenant directory) navigate to:

```
External Identities
> All Identity Providers
```

Enter:

```
Client ID
Client Secret
```

Click:

```
Save
```

Integrate with Facebook Identity Provider

Step 1: Create Meta Developer App

Visit to:

https://developers.facebook.com

Select:

```
My Apps > Create App
```

Choose:

```
Authenticate and request data from users with Facebook Login
```

Select platform:

```
Web
```

Add redirect URI:

```
https://<tenant-subdomain>.ciamlogin.com/<tenant-subdomain>.onmicrosoft.com/federation/oauth2
```

In **App Settings > Basic**, copy:

```
App ID
App Secret
```

Add application domain:

```
<your domain here> (e.g: example.com)
```

> Without adding the domain, Facebook login will fail with: "Can't load URL — domain isn't included in the app's domains"

Switch the application to:

```
Live Mode
```

Step 2: Register Facebook Idp in Entra ID

In Entra ID (Ext tenant directory) navigate to:

```
External Identities
> All Identity Providers
> + Facebook
```

Enter:

```
App ID
App Secret
```

Click:

```
Save
```

Integrate with Apple Identity Provider

> Prerequisite: ● An active Apple Developer Account (Paid membership).

Step 1: Configure Apple Developer Portal

Navigate to:

https://developer.apple.com

Create an **App ID** with:

```
Sign in with Apple enabled
```

Create a **Services ID**

Example:

```
com.example.samllab
```

Configure redirect URI:

```
https://<tenant-subdomain>.ciamlogin.com/<tenant-subdomain>.onmicrosoft.com/federation/oauth2
```

Create **Sign In with Apple Key**

Download:

```
.p8 private key
```

Record:

```
Key ID
Team ID
```

Step 2: **Register Apple Idp in Entra ID**

In Entra ID (Ext tenant directory) navigate to:

```
External Identities
> All Identity Providers
> + Apple
```

Configure:

```
Client ID: Your Apple services ID
Apple developer team ID: Your Apple Team ID here
Key ID: Your Apple Key ID here
Client Secret: Upload the .p8 key file here
```

Phase 3: Create a User Flow

In Entra ID (Ext tenant directory) navigate to:

```
External Identities
> User Flows
```

```
> + New User Flow
```

Configure:

Name: (e.g) PilotApp-Auth-via-Socials

Enable identity providers:

```
Email with Password
Google
Facebook
```

Select attributes:

```
Display Name
Email Address
Given Name
Surname
```

Click:

```
Create
```

Phase 4: Register the SAML Application in Entra ID Ext Tenant directory

Navigate to:

```
Enterprise Applications
> New Application
> Create Your Own Application
```

Name:

```
My PilotApp with Socials Idp
```

Select:

Integrate any other application you don't find in the gallery

Configure SAML

Navigate to:

```
Single Sign-On
> SAML
```

Configure:

Identifier (Entity ID)

```
https://mypilot-app.example.com
```

Reply URL (ACS)

```
https://mypilot-app.example.com/acs
```

Configure Attributes & Claims

Map attributes:

Claim	Value
givenname	user.givenname
surname	user.surname
emailaddress	user.mail

Obtain Federation Metadata

Download:

```
Federation Metadata XML
```

Extract:

```
IdP Entity ID
SSO URL
Signing Certificate
```

In Entra ID Ext Tenant Directory Link the Application to the User Flow

Navigate to:

```
External Identities
> User Flows
```

```
> saml_lab_signin
> Applications
```

Click: Add Application

Select: <The Enterprise App you want to integrate>

Phase 5: Update Third-party or LOB App that you want to integrate with Socials IDP

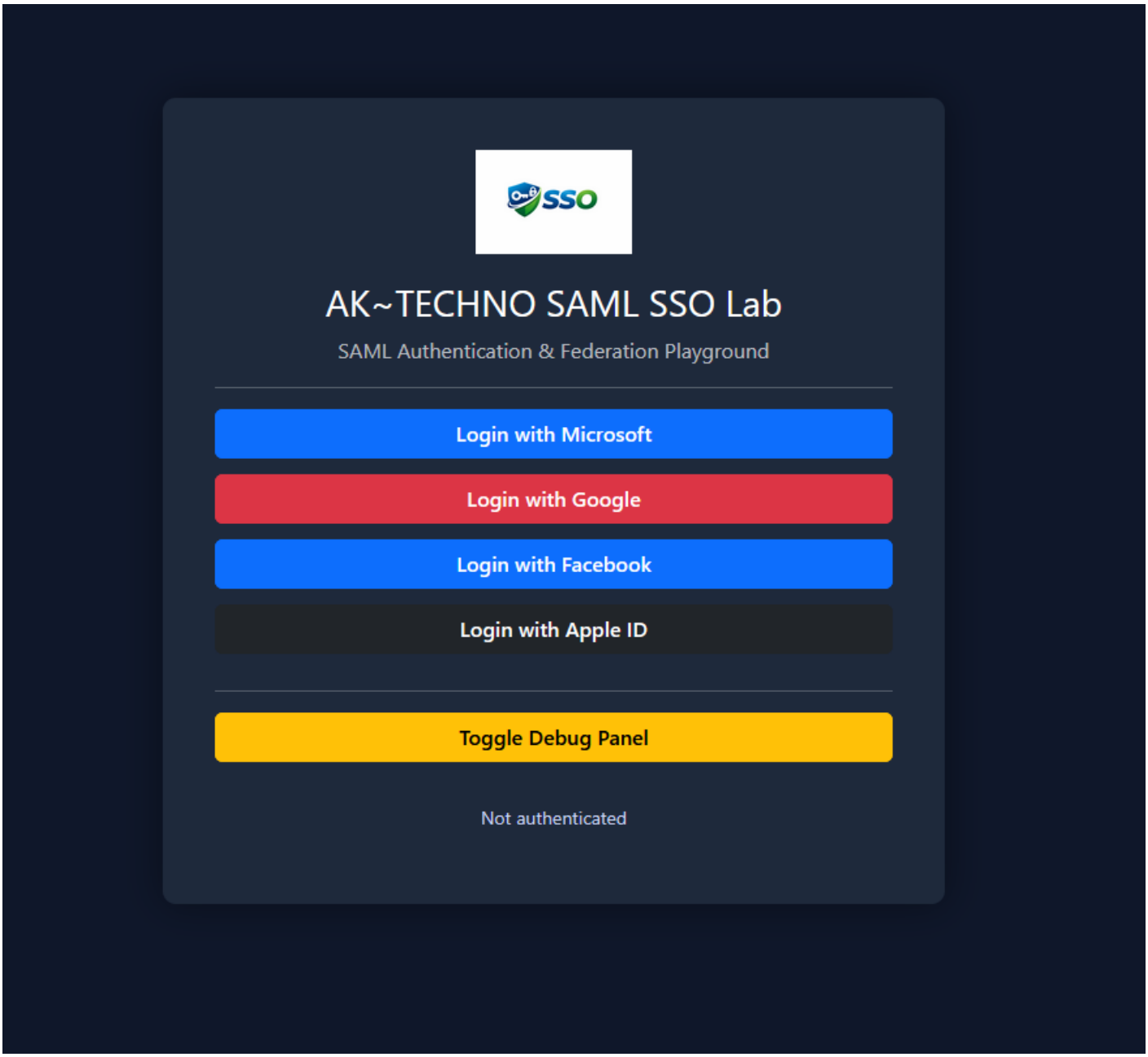
Replace workforce tenant values with the external tenant values.

```
# External Tenant Configuration


SAML_IDP_ENTITY_ID=https://<external-tenant-id>.ciamlogin.com/<external-tenant-id>/
SAML_IDP_SSO_URL=https://<tenant-name>.ciamlogin.com/<tenant-name>.onmicrosoft.com/saml2
SAML_IDP_X509CERT=<base64-certificate>
```

Save the configuration.

> **The application will now authenticate users through the External Tenant user flow.**



---------- Troubleshooting ----------

Facebook - Domain Not Included in App Domains

Error:

```
Can't load URL
The domain of this URL isn't included in the app's domains
```

Resolution:

Add the application domain in:

Meta Developer Console
> App Settings
> Basic
> App Domains

Facebook - Invalid Scopes Email

Error:

`Invalid Scopes: email`

Resolution:

Add the permission:

Permissions and Features
> email

Google - Redirect URI Mismatch

Error:

`redirect_uri_mismatch`

Resolution:

Ensure the redirect URI in Google Console matches:

https://.ciamlogin.com/.onmicrosoft.com/oauth2/authresp

SAML Login Failure

Error:

AADSTS75011 Authentication method mismatch

Resolution:

Disable strict authentication context in the Service Provider configuration.

Metric	Result
Resolution Time	~45–90 minutes
User Impact	Users can authenticate using social providers

Metric	Result
Authentication Method	Google, Facebook, Apple, or local account
Recurrence Risk	Low once identity providers are configured

Revision #11
Created 2026-03-10 12:40:00 UTC by AK. Udofeh
Updated 2026-03-19 10:45:36 UTC by AK. Udofeh