

Event Sponsors



Azure AD B2C in your next consumer app

Simon Waight, Microsoft MVP - Azure



Let's make things better!

A bit about me...

- ▶ Simon Waight | @simonwaight | <https://blog.siliconvalve.com/>
- ▶ Run the Azure Sydney User Group | Meetup site: <http://bit.ly/ZdRKke>
- ▶ Work for Kloud Solutions | <https://blog.kloud.com.au/>
- ▶ Microsoft MVP for Azure



Session overview

- ▶ Quick Azure AD (AAD) Business to Consumer (B2C) overview.
- ▶ Demo: our consumer application scenario.
- ▶ Wrap up.

Less death by PowerPoint. More...



Azure AD B2C overview

What is Azure AD B2C?

- ▶ Scalable and secure consumer identity management platform.
- ▶ Supports built-in or brokered identity providers.
- ▶ Configuration-over-code solution.
- ▶ Extensible profile system based on schema similar to Azure AD.
- ▶ A single AAD B2C instance can provide SSO for multiple apps.



“Azure Active Directory B2C helps us bring the stadium closer to our 450 million fans around the globe with simplified registration and login through social accounts, like Facebook, or traditional username/passwords.”

RAFAEL DE LOS SANTOS
HEAD OF DIGITAL
REAL MADRID

- Provided a seamless experience across mobile applications on any platform
- Built a fully customized login page without custom code
- Alleviated concerns about security, data breaches, and scalability
- <http://www.realmadrid.com/en/login>

Azure AD B2C overview

Identity Providers (IdPs)

- ▶ Built-in (email or username) or Social

The screenshot displays the Windows Identity Provider configuration interface, divided into three panes:

- Identity provider:** Shows a dropdown menu for 'Local accounts' with 'Email' selected. Below it, the 'Social identity providers' section is visible, showing 'Login with LinkedIn' and 'LinkedIn'.
- Add social identity pro...:** Contains three required fields:
 - Name:** A text input field with the placeholder text 'Enter an identity provider name'.
 - Identity provider type:** A dropdown menu currently showing 'None selected'.
 - Set up this identity provider:** A dropdown menu currently showing 'Required'.
- Select social identity pr...:** Lists several social identity providers: Microsoft Account, Google, Facebook, and Amazon.

User attributes

- ▶ Defines superset of attributes a user profile can have.

The screenshot displays the 'User attributes' management interface. The left pane shows a table of existing attributes, and the right pane shows the 'Add an attribute' form.

NAME	DATA TYPE	DESCRIPTION	ATTRIBUTE TYPE
City	String	The city in which the user is located.	Built-in
Country/Region	String	The country/region in which the user is located.	Built-in
Display Name	String	Display Name of the User	Built-in
Email Addresses	StringCollection	Email addresses of the user.	Built-in
Given Name	String	The user's given name (also known as first name).	Built-in
Identity Provider	String	The social identity provider used by the user to access to your ap...	Built-in
Job Title	String	The user's job title.	Built-in
Postal Code	String	The postal code of the user's address.	Built-in

Add an attribute

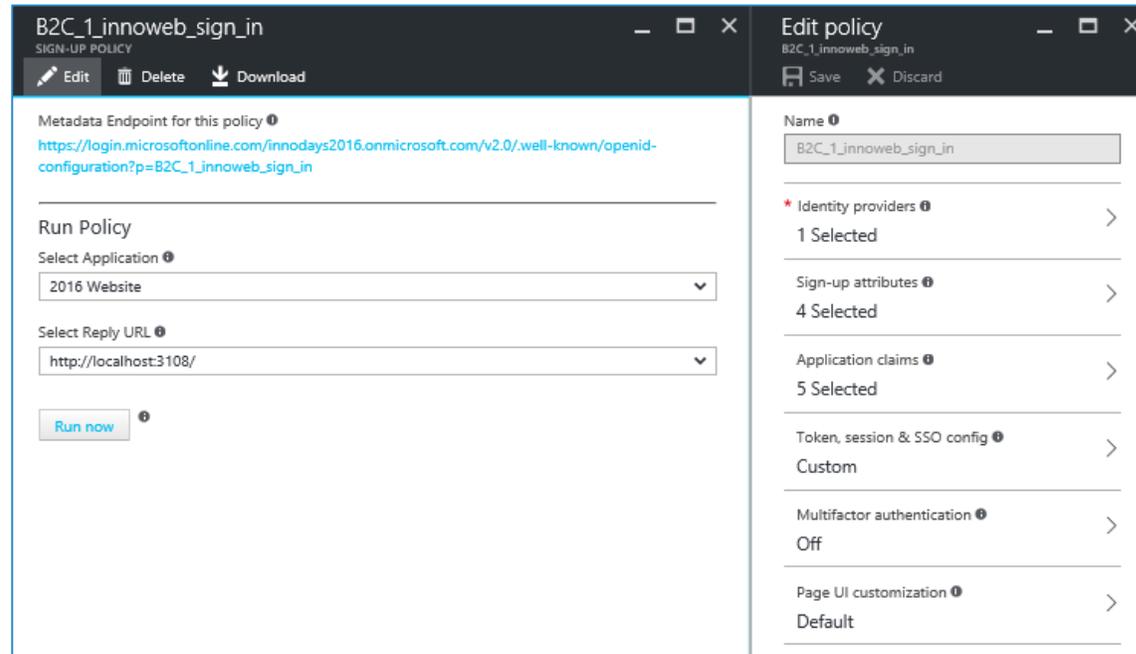
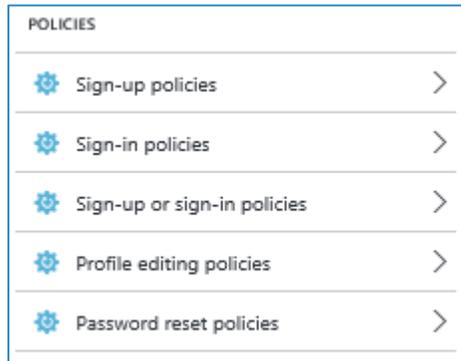
Name ⓘ
LikesOS ✓

Data Type ⓘ
String ▼

Description ⓘ
Which OS this user likes.

Policies

- ▶ Customise IdPs, profile attributes, claims, security and UX.
- ▶ Create multiple and invoke by appending to metadata endpoint.



https://login.microsoftonline.com/innodays2016.onmicrosoft.com/v2.0/.well-known/openid-configuration?p=B2C_1_innoweb_sign_in



Policy

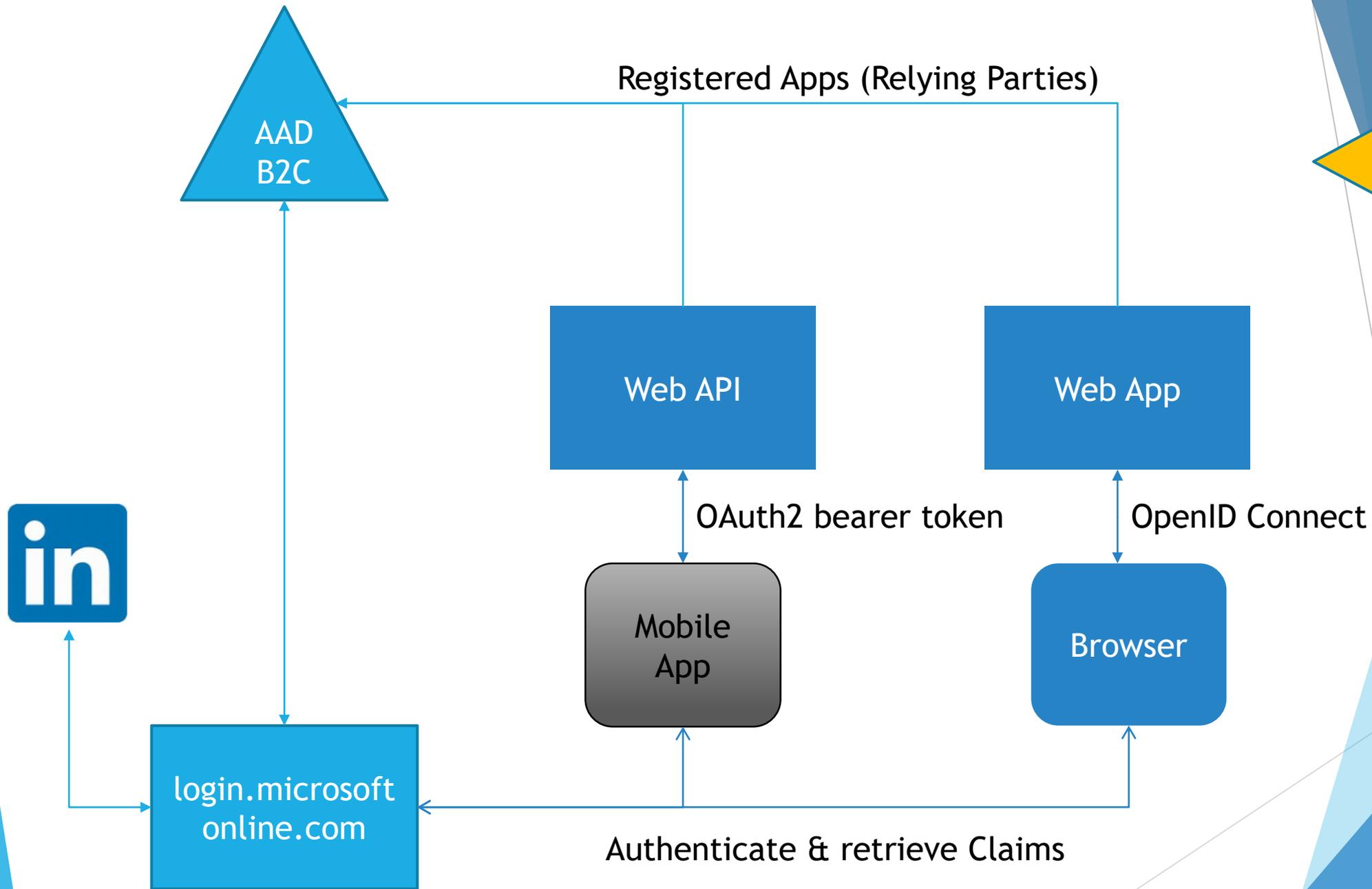
Applications

- ▶ Secured by identities and can access claims as determined by Policy invoked at authentication time.

The screenshot displays the Azure AD portal interface for configuring an application. On the left, a list of applications is shown, with '2016 Web API' selected. The main panel shows the configuration details for this application:

- Name:** 2016 Web API
- Application ID:** 3c1285f5-3d44-4338-b885-800000000000
- Web App / Web API:**
 - Include web app / web API: Yes
 - Allow implicit flow: Yes
- Redirect URIs:** A warning message states "Redirect URIs must all belong to the same domain".
- Reply URL:** A text input field containing a partially obscured URL.
- App key:** A button labeled "Generate key".
- Native client:**
 - Include native client: Yes
- Redirect URI:** urn:ietf:wg:oauth:2.0:oob

Our scenario



Not drawn to scale (or accuracy)





Innovation Days Login Demo

Update successful!

- Authentication
- Settings
- Roles
- Mobile
- JavaScript
- OS
- Usage & Limits
- My Applications

Authentication Keys

Client ID: 75lu0wcc270pg3

Client Secret: [REDACTED]

Default Application Permissions

r_basicprofile

r_emailaddress

rw_company_admin

w_share

OAuth 2.0

Authorized Redirect URLs:

Add

<https://login.microsoftonline.com/te/innodays2016.onmicrosoft.co>



Wrapping up

<https://github.com/sjwaight/innovationdays2016/>

In summary

- ▶ If you have identity or profile management needs AAD B2C has to be on your radar (seriously... stop writing and hosting your own).
- ▶ A single AAD B2C tenant can host a multitude of consuming apps that can share profile information as required. Perfect for large consumer-focused organisations.
- ▶ A few “gotchas”:
 - ▶ Only Generally Available (GA) in North America (September 2016)
 - ▶ OAuth 2.0 and OpenID Connect implementations not feature complete.
 - ▶ ADAL to MSAL migration ongoing.
 - ▶ User management experience in state of flux*.

Thanks for your time!

Tweet us @_innovationdays or tag #innovationdays

Top twitter of the day will win a gift

Event Sponsors

