

ADC 2016

# AAD B2C

Identity-as-a-Service for Web



Rainer Stropek

software architects gmbh

Web <http://www.timecockpit.com>  
Mail [rainer@timecockpit.com](mailto:rainer@timecockpit.com)  
Twitter @rstropek



**time cockpit**  
Saves the day.

# Yet Another Active Directory?

## Active Directory

Internal network

Needs VPN or ADFS for distributed networks and Internet

## Azure Active Directory

Mirror your AD into Azure

Let Microsoft worry about operations and latest standards (e.g. OpenID Connect)

Offers RESTful Web API for directory services

Optimized for commercial organizations

## Azure Active Directory B2C

AAD for SaaS providers whose customers don't have their own AAD (= "consumers")

Microsoft Azure | Check out the new portal | CREDIT STATUS | Subscriptions

### active directory

DIRECTORY | ACCESS CONTROL NAMESPACES | MULTI-FACTOR AUTH PROVIDERS | RIGHTS MANAGEMENT

NAME	STATUS	ROLE	SUBSCRIPTION	DATACENTER REGI...	C...
[REDACTED]	Active	Global Administrator	Shared by all devop...	Europe	Germany
[REDACTED]	Active	Global Administrator	Shared by all cubid...	Europe	Austria
Demo AAD B2C	Active	Global Administrator	Shared by all Demo ...	Europe	Austria
[REDACTED]	Active	Global Administrator	Shared by all Cloud...	Europe	Austria
[REDACTED]	Active	Global Administrator	Shared by all softwa...	Europe	Austria

ACTIVE DIRECTORY 5

This operation may take up to two minutes.

### Add directory

DIRECTORY ?  
Create new directory

NAME ?  
Demo AAD B2C

DOMAIN NAME ?  
rainerdemob2c .onmicrosoft.com

COUNTRY OR REGION ?  
Austria

This is a B2C directory. ?

# Demo

Creating AAD B2C

Create in „old“ portal

Manage in current portal

# Administration in Azure Portal

Microsoft Azure

Check out the new portal

CREDIT STATUS

Subs...

demo aad b2c

USERS GROUPS APPLICATIONS DOMAINS DIRECTORY INTEGRATION CONFIGURE

**Demo AAD B2C**

- devopscon15
- cubidoinformiert
- Cloudconf Berlin 2...
- software architects...

Your directory is ready to use.  
Here are a few options to get started.

LEARN

Read: Azure Active Directory B2C

ADMINISTER

**Manage B2C settings**

Microsoft Azure

AZURE AD B2C SETTINGS > Settings

AZURE AD B2C SETTINGS

rainerdemob2c.onmicrosoft.com

Settings

Essentials ^

Domain name	Tenant type
rainerdemob2c.onmicrosoft.com	Production-scale tenant

All settings →

Welcome to Azure AD B2C. Click Settings to get started.

Quick Start

Submit support request

# AAD Applications

## Application ID

Identifies your app

## Redirect URI

URI of your app that receives response from AAD B2C

## Implicit flow?

Possibility to enable/disable implicit flow

Microsoft Azure AZURE AD B2C SETTINGS > Settings > Applications > ADC Web Demo Search resources

Settings rainerdemob2c.onmicrosoft.com Applications + Add ADC Web Demo Save Discard Delete

Filter settings

MANAGE

- Applications >
- Identity providers >
- User attributes >
- Users and groups >

POLICIES

- Sign-up policies >
- Sign-in policies >
- Sign-up or sign-in policies >
- Profile editing policies >
- Password reset policies >
- All policies >

NAME

ADC Web Demo

\* Name ADC Web Demo

Application ID c1ab45be-b27f-4487-9537-2fdf3599367f

Web App / Web API

Include web app / web API  Yes  No

Allow implicit flow  Yes  No

Redirect URIs must all belong to the same domain

Reply URL https://localhost:44316

# Demo

Managing AAD B2C Apps

### Neues Projekt

Projektname

Die Projekt-ID lautet adc-2016 [Bearbeiten](#)

Erweiterte Optionen ausblenden...

App Engine-Region

[ABBRECHEN](#) [ERSTELLEN](#)

Anmeldedaten - ADC 2016

<https://console.developers.google.com/apis/credentials?project=adc-2016>

Google APIs ADC 2016

### Zugangsdaten

[Anmeldedaten erstellen](#) [Löschen](#)

API Manager

Dashboard

Bibliothek

Zugangsdaten

### Zugangsdaten

[JSON herunterladen](#) [Schlüssel zurücksetzen](#) [Löschen](#)

Client-ID für Webanwendung

Client-ID	457972 [redacted]@apps.googleusercontent.com
Clientschlüssel	[redacted]
Erstellungsdatum	23.10.2016, 09:27:58

Name

### Identity provider

[Add](#) [Save](#) [Discard](#)

Local accounts

Social identity providers

**ADC AAD B2C Google Demo**  
Google

### ADC AAD B2C Google ...

Google

[Save](#) [Discard](#) [Delete](#)

Identity provider type

\* Name

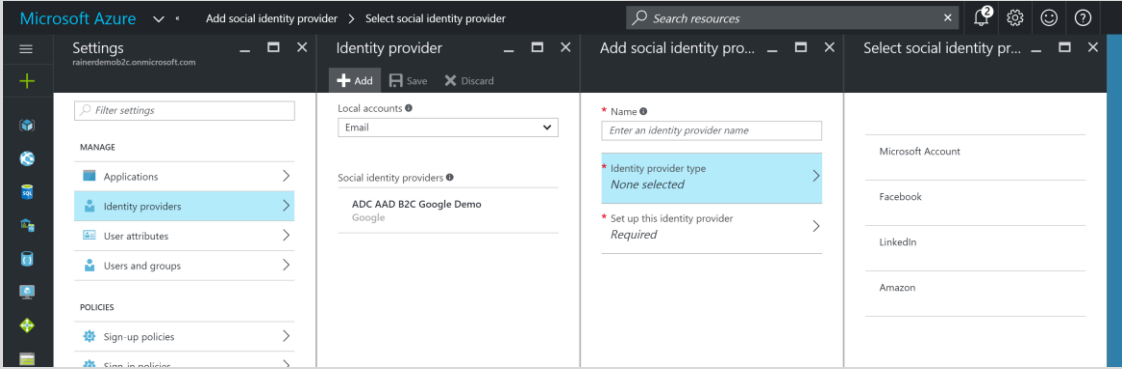
\* Client ID

\* Client secret

# Demo

Managing ID Providers

[Google Dev Console](#)





# Demo

User Attributes

## Extensible Data Model

The screenshot shows the Microsoft Azure portal interface for managing user attributes. The breadcrumb navigation indicates the path: Microsoft Azure > AZURE AD B2C SETTINGS > Settings > User attributes. The left-hand navigation pane is divided into 'MANAGE' and 'POLICIES' sections. Under 'MANAGE', 'User attributes' is selected. Under 'POLICIES', various sign-up and sign-in policies are listed. The main content area displays a table of user attributes.

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
Nickname	String	The user's nickname.	Custom
Postal Code	String	The postal code of the user's address.	Built-in
State/Province	String	The state or province in user's address.	Built-in
Street Address	String	The street address where the user is located	Built-in
Surname	String	The user's surname (also known as family name or last name).	Built-in
User is new	Boolean	True, if the user has just signed-up for your application	Built-in
User's Object ID	String	Object identifier (ID) of the user object in Azure AD.	Built-in

# Policies

## Named set of configurations

Account types

Attributes to be collected from the user

Multi-Factor Authentication

Look-and-feel of pages

Information that the application receives (tokens)

```
https://login.microsoftonline.com/rainerdemob2c.onmicrosoft.com/oauth2/v2.0/authorize?  
response_type=id_token&  
client_id=c1ab45be-0000-0000-0000-000000000000&  
redirect_uri=https%3A%2F%2Flocalhost:12345&  
response_mode=query&  
scope=openid%20profile&  
state=any_state&nonce=any_nonce&  
p=B2C_1_Signin
```

Microsoft Azure | AZURE AD B2C SETTINGS > Settings > Sign-up policies > B2C\_1\_Signup

Settings | Sign-up policies

MANAGE

- Applications >
- Identity providers >
- User attributes >
- Users and groups >

POLICIES

- Sign-up policies >
- Sign-in policies >
- Sign-up or sign-in policies >
- Profile editing policies >
- Password reset policies >
- All policies >

Search

B2C\_1\_Signup  
Default template

# Demo

Policies

Signup  
[Link](#)

Sign in  
[With/without MFA](#)

Profile Edit

```
<?xml version="1.0" encoding="utf-8"?>
<packages>
  <package id="Microsoft.Owin.Security.OpenIdConnect"
    version="3.0.1" targetFramework="net45" />
  ...
</packages>

// Note: Microsoft.AspNetCore.Authentication.OpenIdConnect
//       for .NET Core

public void ConfigureAuth(IApplicationBuilder app) {
  app.SetDefaultSignInAsAuthenticationType(
    CookieAuthenticationDefaults.AuthenticationType);
  app.UseCookieAuthentication(
    new CookieAuthenticationOptions());
  app.UseOpenIdConnectAuthentication(
    CreateOptionsFromPolicy(SignUpPolicyId));
  ...
}

[Authorize]
public ActionResult Claims() {
  // Read ClaimsPrincipal.Current.Identities.First()
  ...
}
```

# Demo

AAD B2C and ASP.NET MVC

<https://azure.microsoft.com/en-us/documentation/articles/active-directory-b2c-devquickstarts-web-dotnet/>

```
<?xml version="1.0" encoding="utf-8"?>
<packages>
  <package id="Microsoft.Owin.Security.OAuth" version="3.0.1"
    targetFramework="net45" />
  ...
</packages>
```

```
public void ConfigureAuth(IAppBuilder app) {
  app.UseOAuthBearerAuthentication(
    CreateBearerOptionsFromPolicy(signUpPolicy));
  ...
}
```

```
[Authorize]
public class TasksController : ApiController {
  public IEnumerable<Models.Task> Get() {
    // Read ClaimsPrincipal.Current
    ...
  }
}
```

```
var bootstrapContext =
  ClaimsPrincipal.Current.Identities.First().BootstrapContext
  as System.IdentityModel.Tokens.BootstrapContext;
```

# Demo

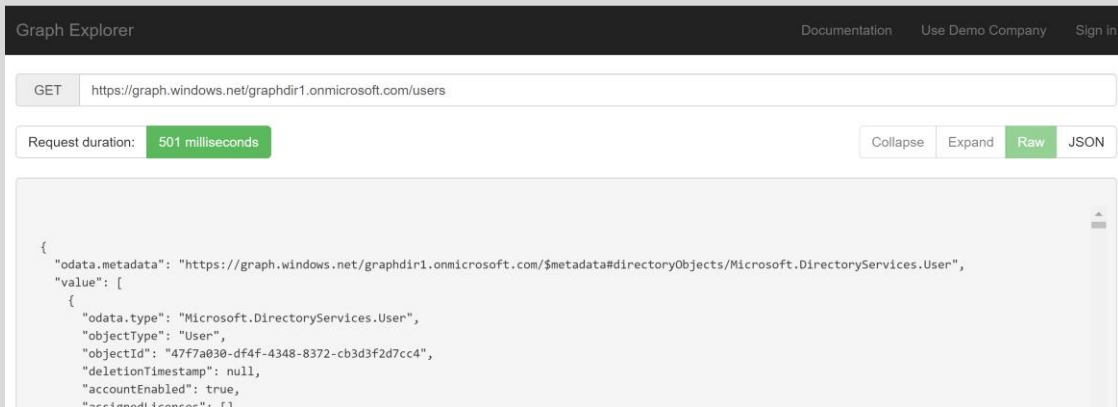
AAD B2C and Web API

<https://azure.microsoft.com/en-us/documentation/articles/active-directory-b2c-devquickstarts-api-dotnet/>

# Demo

Graph API

## Automate AAD B2C Management



Graph Explorer

Documentation Use Demo Company Sign in

GET

Request duration: 501 milliseconds

Collapse Expand Raw JSON

```
{
  "odata.metadata": "https://graph.windows.net/graphdir1.onmicrosoft.com/$metadata#directoryObjects/Microsoft.DirectoryServices.User",
  "value": [
    {
      "odata.type": "Microsoft.DirectoryServices.User",
      "objectType": "User",
      "objectId": "47f7a030-df4f-4348-8372-cb3d3f2d7cc4",
      "deletionTimestamp": null,
      "accountEnabled": true,
      "assignedLicenses": []
    }
  ]
}
```

<https://azure.microsoft.com/en-us/documentation/articles/active-directory-b2c-devquickstarts-graph-dotnet/>

# Limitations

## No production-scale B2C tenants outside of NorthAm

Limitation at the time of writing

Preview production-scale B2C available in Europe, too

[Details](#)

## Old and current portal necessary

Old portal for creation and management of users, groups, pwd reset, branding

New portal for configuring B2C settings

## Limited customization functionality

AAD company branding only for some areas (e.g. local account sign in, emails, etc.)

[Details](#)

# Limitations

## Default: 50k users limit

Contact support if you need more

## OAuth limitations

No SPAs

No Client Credentials flow

No standalone Web APIs (web frontend and web API have to have the same app ID)

## Further limitations

See [Azure Docs](#)



# Summary

## Identity as a Service

No need to run your own e.g. Identity Server

## Cost-efficient solution for lots of consumers

Pricing see <https://azure.microsoft.com/en-us/pricing/details/active-directory-b2c/>

## Great programmability

Platform and programming language independent

## However: Consider limitations

ADC 2016

Q&A

Thank your for coming!



Rainer Stropek

software architects gmbh

Mail  
Web  
Twitter

rainer@timecockpit.com  
<http://www.timecockpit.com>  
@rstropek



**time cockpit**  
Saves the day.