

# Office 365 Development

Mostafa Elzoghbi  
US DX – Microsoft  
<http://mostafa.rocks>  
@MostafaElzoghbi



<http://dev.office.com/>

# Deep dive into Azure AD with the Microsoft Graph

Mostafa Elzoghbi  
US DX – Microsoft  
<http://mostafa.rocks>  
@MostafaElzoghbi

# Agenda

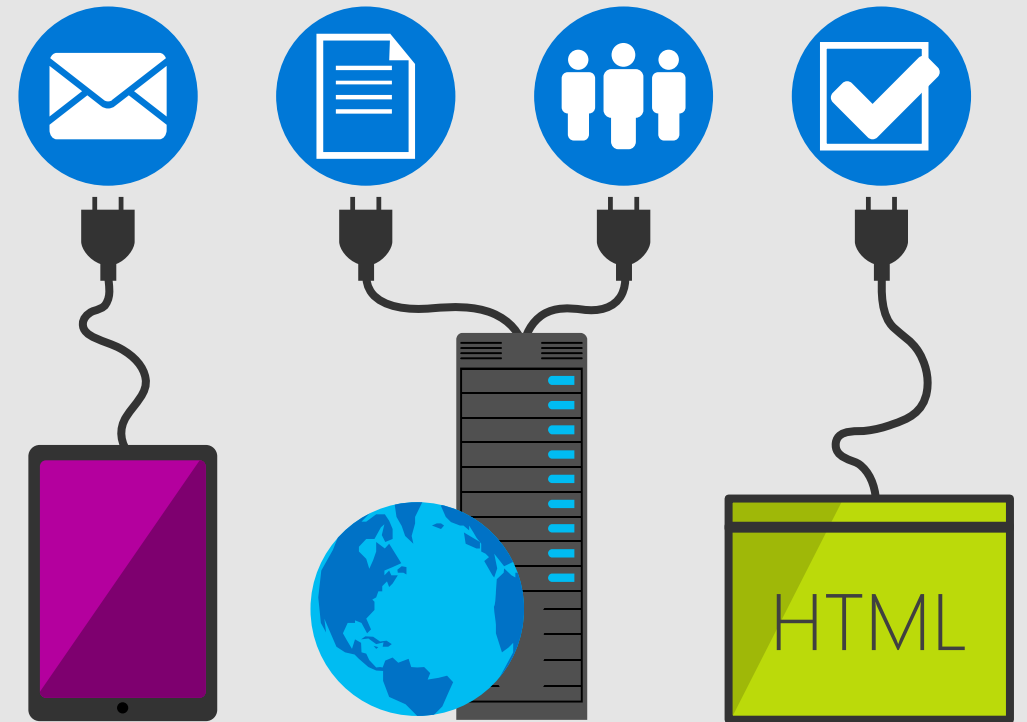
- ➡ Introduction
- ➡ OAuth basics and authentication flow
- ➡ App registration tool
- ➡ Azure Management Portal access
- ➡ Troubleshooting

# Developer vision

## USERS



## DATA

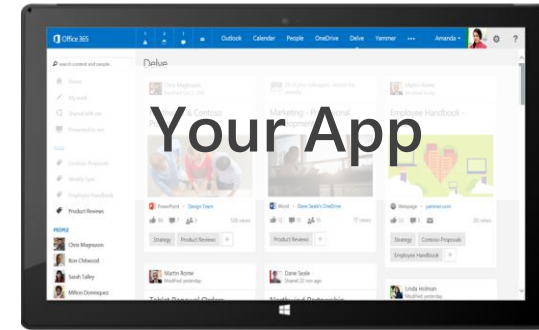
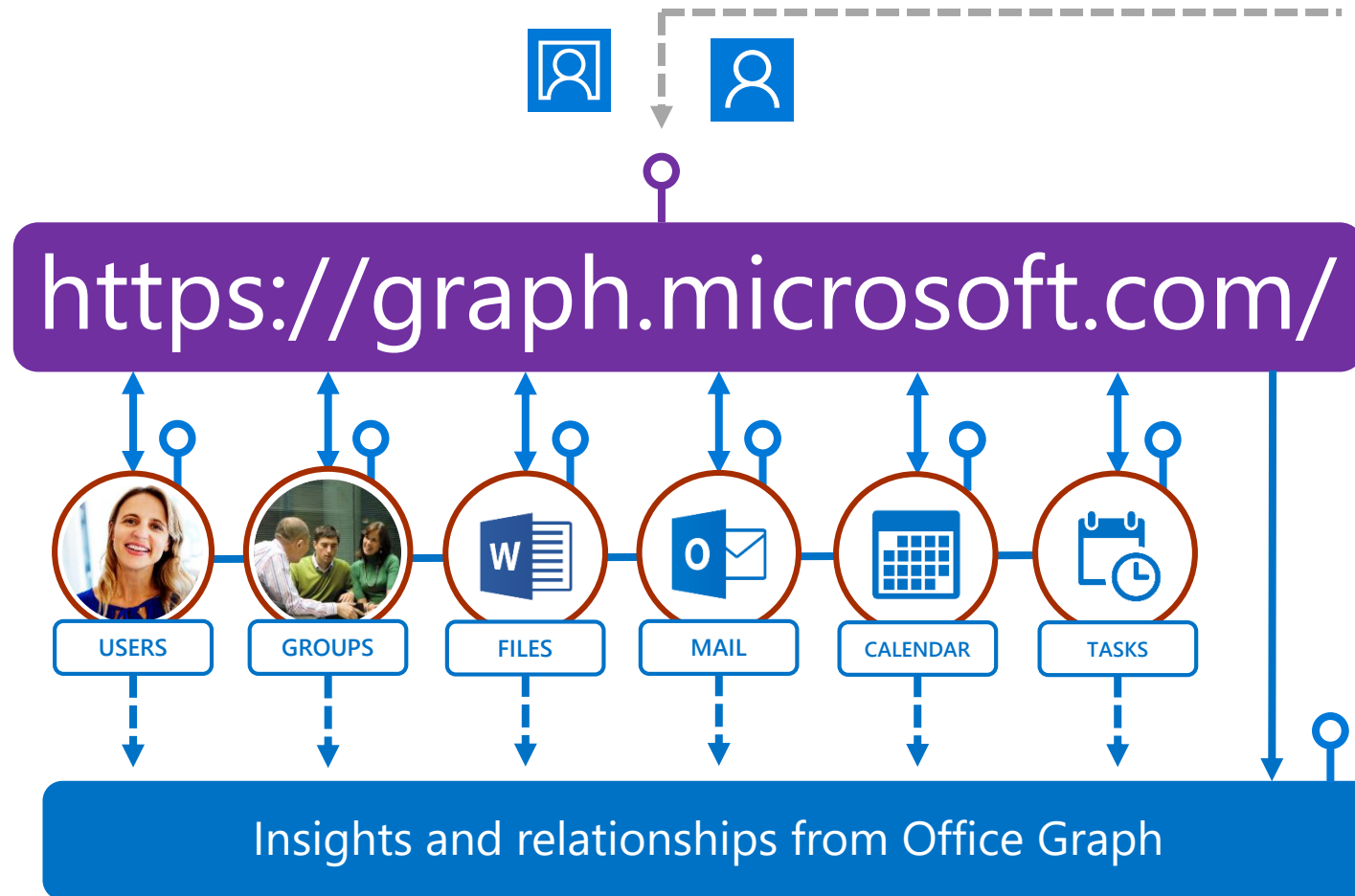


# 1

## Introduction



# Microsoft Graph API



# Azure AD OAuth in Office 365

## Single auth flow for Office 365

Azure AD Graph, Exchange, SharePoint

Device apps and web sites

Admin and end-user consent

## Secure protocol

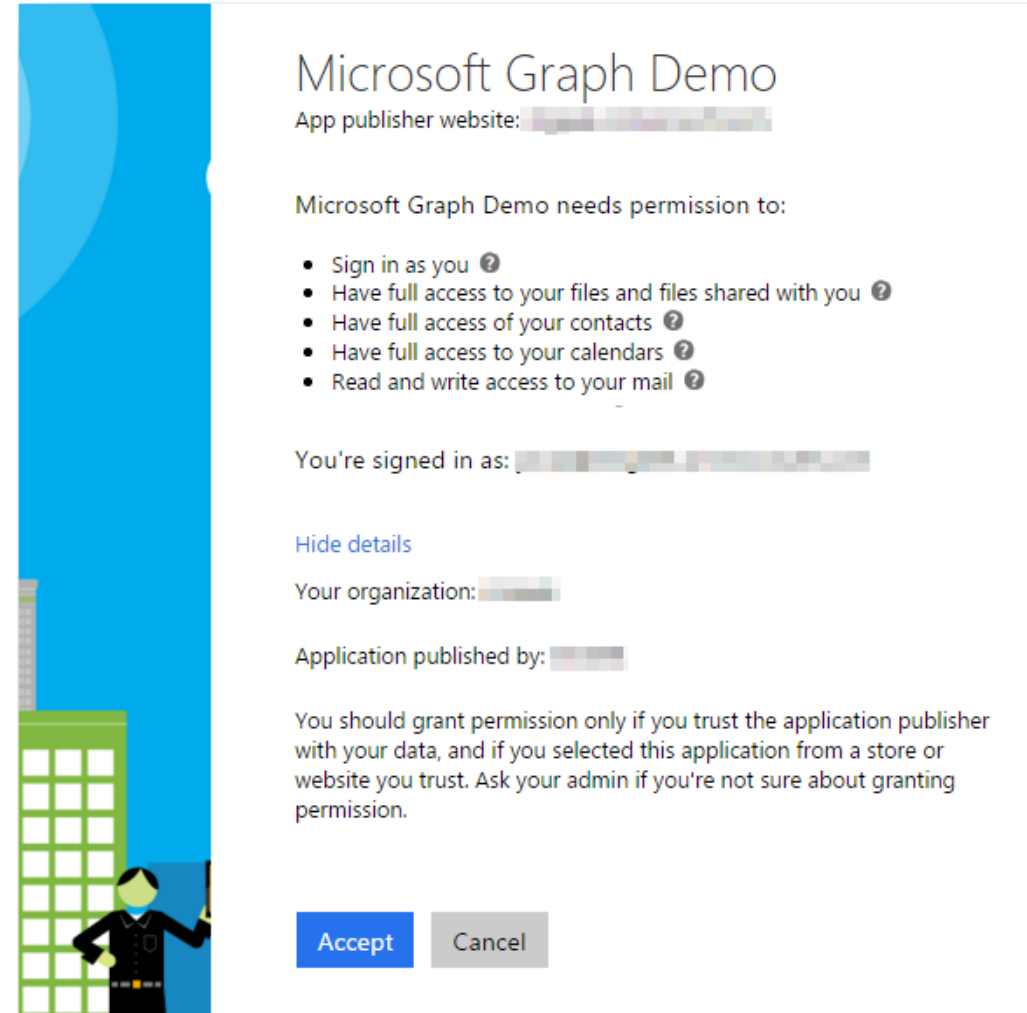
OAuth 2.0

No capturing user credentials

Fine-grained access scopes

Supports MFA and federated user sign-in

Long-term access through refresh tokens



# 2

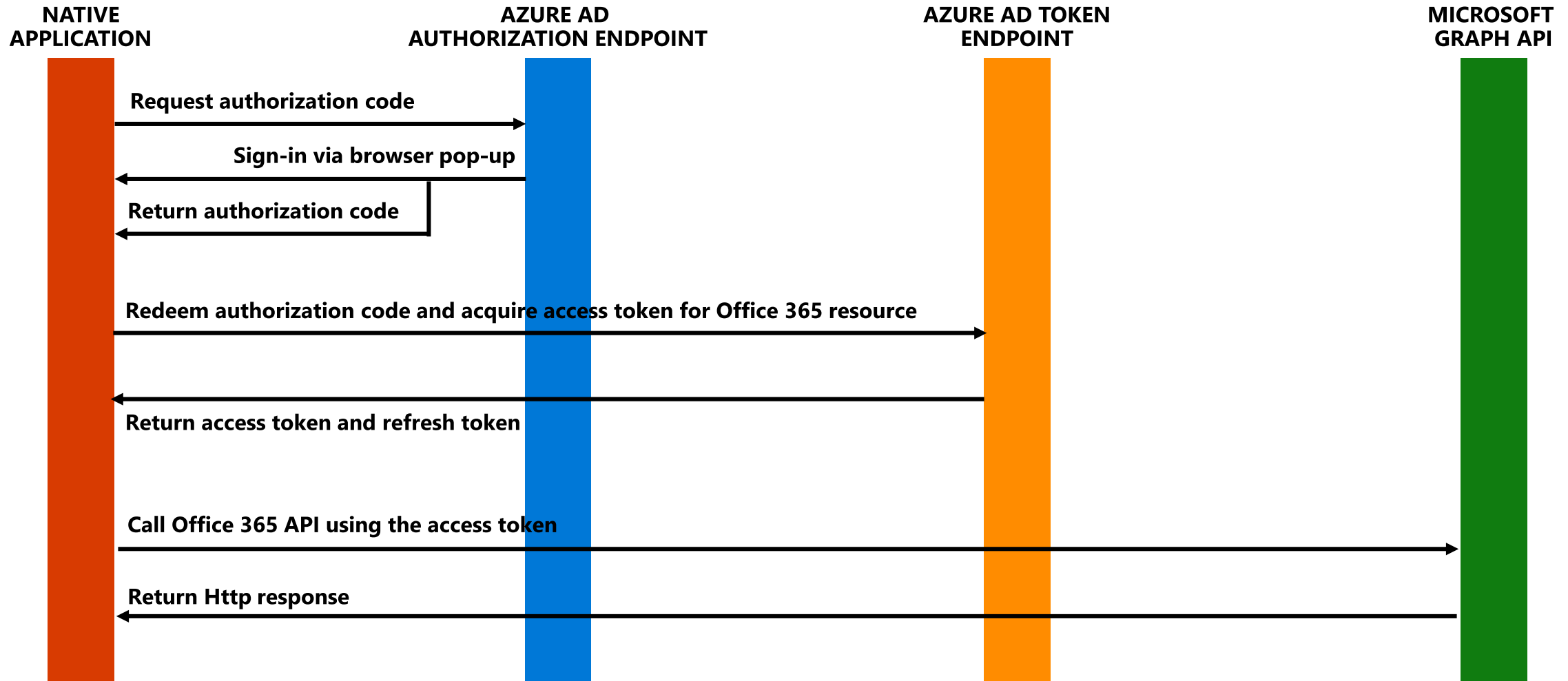
## OAuth basics and authentication flow





# Authentication to Microsoft Graph using resource ID

2 OAuth basics and authentication flow



# Authentication Options

## Azure AD only

Separate auth flow supports Azure AD accounts only

## Azure AD and Microsoft Accounts

Converged auth flow supports Azure AD accounts and Microsoft accounts (LiveID - hotmail.com, etc.)

# Microsoft Account + Azure AD

Many apps want to sign users in from both Microsoft account and Azure AD

Single endpoint, OpenID Connect and OAuth 2.0

Single SDK

Single end user sign in experience

Single app registration experience

## Works with Microsoft Graph

Single API endpoint, business and consumer data

# Libraries: <http://github.com/AzureAD>

- Client: Active Directory Authentication Library (ADAL)
  - .Net, Windows Store, Windows Phone
  - JavaScript
  - iOS
  - Android
  - Xamarin
  - Cordova
  - Node.js
  - Java
- Server
  - .Net: ASP.Net OWIN middleware for OpenID Connect and OAuth 2.0
  - Node.js
- More to come

# 3

## App registration tool



# App registration options

## App registration is stored in Azure AD

Simplified registration experience

- <http://graph.microsoft.io/app-registration>

## Two models for registration

App model v1

App model v2 (**NEW**)



# App registration options

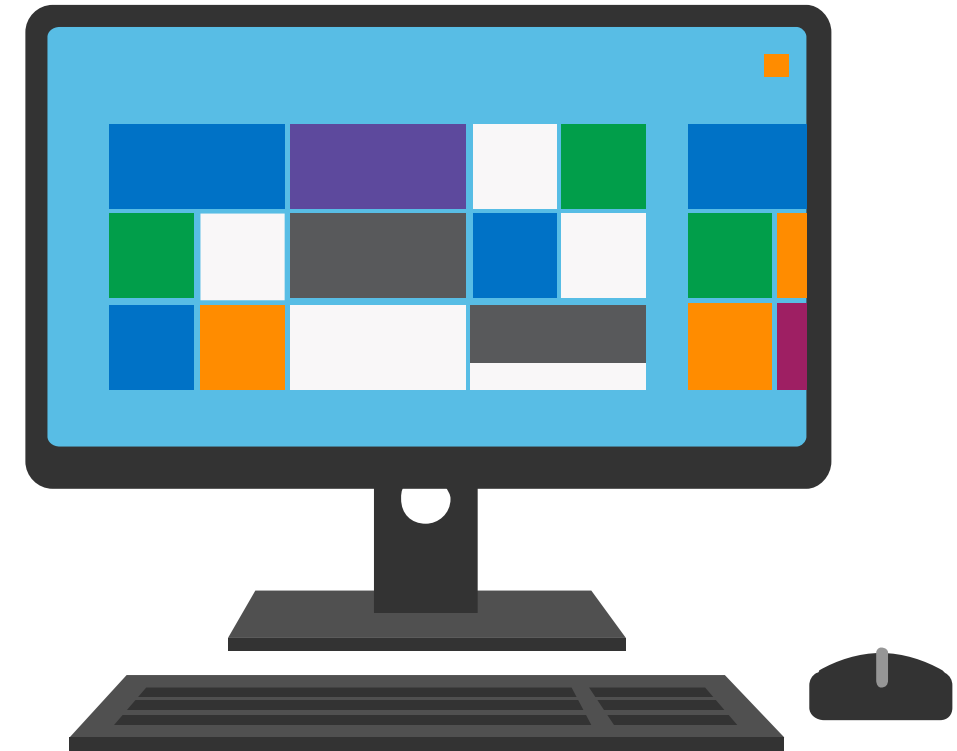
## Azure AD "app model v1"

Separate authentication flow

Supports **Azure AD accounts only**

Office 365 app registration tool

- <http://dev.office.com/app-registration>



# App registration options

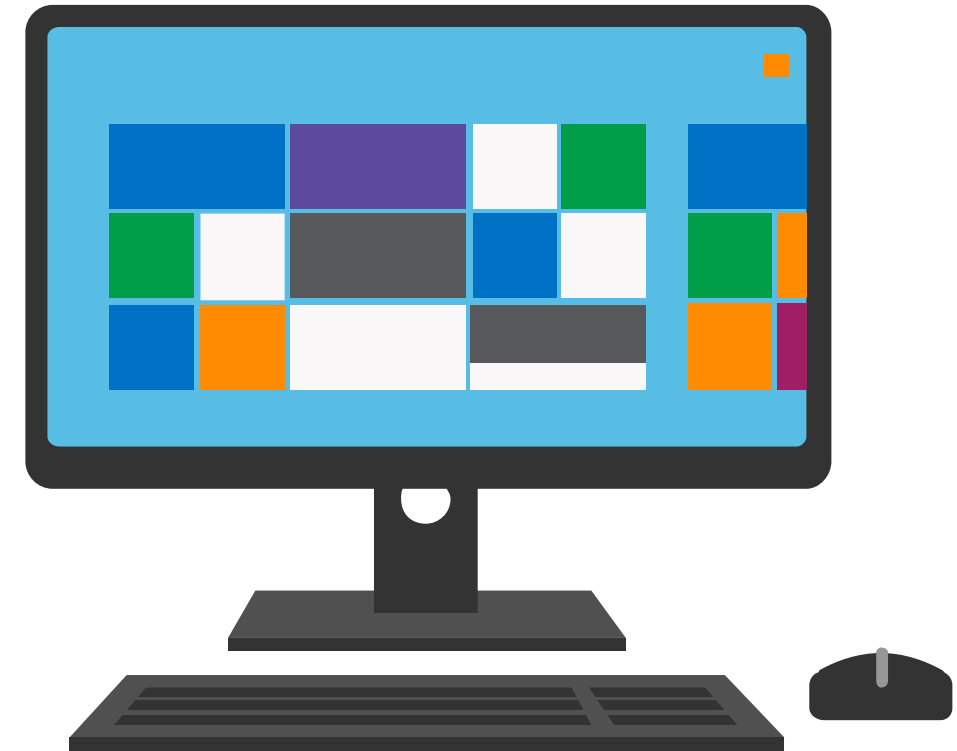
## Azure AD "app model v2"

Converged authentication flow

Supports **Azure AD accounts and Microsoft accounts** (LiveID—hotmail.com, etc.)

New app registration portal

- <http://apps.dev.microsoft.com/>





<http://graph.microsoft.io/app-registration>

Demo



# 4

## Azure Management Portal access



# Azure Active Directory (Azure AD)

Included in Office 365 subscription

Users and groups managed in Office 365 portal

Changes persisted in Azure AD

The image shows two overlapping web interfaces. The background interface is the Office 365 admin center, displaying the 'ACTIVE USERS' section. It includes a search bar, a sidebar with navigation options (DASHBOARD, SETUP, USERS, GROUPS, DOMAINS, BILLING), and a main content area with links for single sign-on, Active Directory synchronization, and password policy management. A table lists active users with columns for 'DISPLAY NAME' and 'USER NAME'.

The foreground interface is the Microsoft Azure portal, showing the 'wingtip office developer training' page. It features a navigation bar with 'CREDIT STATUS' and a user profile. The main content area displays a table of users synchronized from Windows Azure Active Directory.

DISPLAY NAME	USER NAME	SOURCED FROM
Joe	joe@wingtip.office.onmicrosoft.com	Windows Azure Active Directory
Paul	paul@wingtip.office.onmicrosoft.com	Windows Azure Active Directory

# Application registration

## Application types

Custom developed

Third party, published in the gallery

- Office 365 SharePoint, Exchange
- Dynamics CRM
- Thousands of others

## Custom applications

Web application and/or WebAPI

Native client

APPLICATION GALLERY

Add an application for my organization to use

FEATURED APPLICATIONS (13)

ALL (2390)

BUSINESS MANAGEMENT (86)

COLLABORATION (271)

CONSTRUCTION (3)

CONTENT MANAGEMENT (82)

Jive

Office 365 Exchange Online

Microsoft Dynamics

NAME Dynamics CRM

PUBLISHER Microsoft Corporation

APPLICATION URL <http://www.microsoft.com/en-us/dynamics/crm.aspx>

By default, Dynamics CRM works with Windows Azure AD. To get started, sign up for Dynamics CRM using an account in your instance of Windows Azure AD.

Requires an existing Dynamics CRM subscription.

→ Sign up for Dynamics CRM

ADD APPLICATION

Tell us about your application

NAME

Type

☒ WEB APPLICATION AND/OR WEB API ?
 ☐ NATIVE CLIENT APPLICATION ?

→ 2

# Custom application registration

## Key information

Client ID

Keys (aka **client secret**)

Redirect/Sign-on URI

The screenshot displays the 'Auth Flow Demo' application registration page in the Azure Management Portal. The left sidebar lists the application name and its supported platforms. The main content area is divided into sections for 'CLIENT ID', 'keys', 'single sign-on', and 'REPLY URL'.

**Auth Flow Demo**

- DiscoveryApp
- DiscoveryWin8
- Office 365 Exchang...
- Office 365 SharePo...

**CLIENT ID**

[Redacted Client ID]

**keys**

1 year	9/8/2014	9/8/2015	*****
Select du... ▼	VALID FROM	EXPIRES ON	THE KEY VALUE WILL BE DISPLAYED AFTER YOU SAVE IT.

**single sign-on**

**APP ID URI**

http://[Redacted].onmicrosoft.com/AuthFlowDemo ✓

**REPLY URL**

http://authflowdemo.com

(ENTER A REPLY URL)

# Application authentication

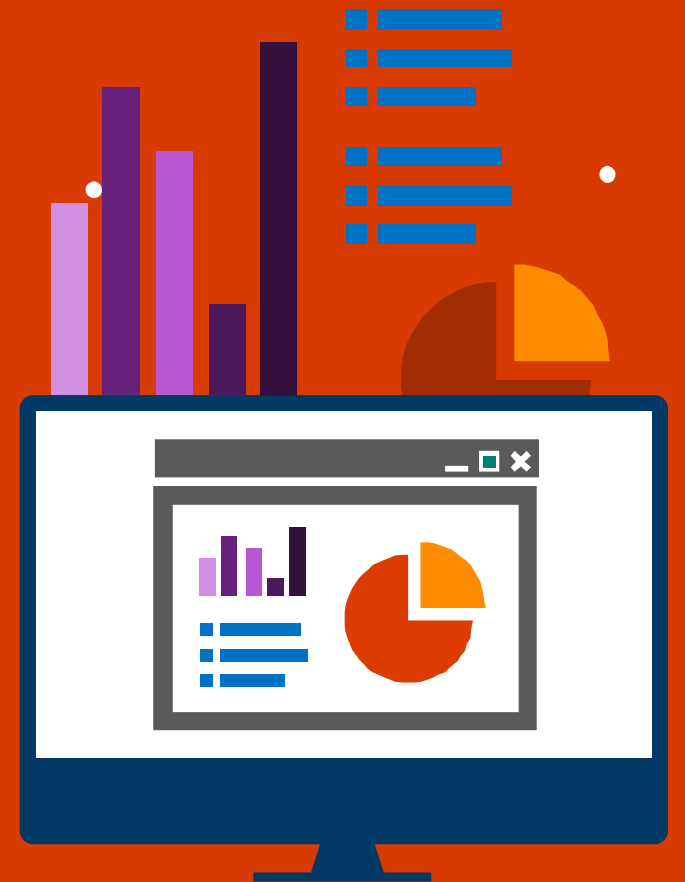
## App authentication uses client ID/secret

Protect this information just as you would a user name/password

```
var clientCredential = new ClientCredential(SettingsHelper.ClientId,  
                                           SettingsHelper.ClientSecret);  
var userIdentifier = new UserIdentifier(userObjectId,  
                                       UserIdentifierType.UniqueId);  
  
var result = await authContext.AcquireTokenSilentAsync(  
    SettingsHelper.AzureAdGraphResourceURL,  
    clientCredential,  
    userIdentifier);
```

# 5

## Troubleshooting



# Troubleshooting errors in Auth flow

## Login errors

Shown on web page

Additional technical information:

Correlation ID: 23ef28d3-bffa-4171-97db-a2a6f3f7f4c0

Timestamp: 2014-09-11 03:00:21Z

AADSTS70001: Application with identifier de43f8aa-6412-4abd-8abd-c423fe73c30a was not found in the directory

onmicrosoft.com

## Fiddler

Shows response/request from apps running on local computer

## Review response as JSON

Authentication errors (invalid values)

```
{"error": "invalid_grant", "error_description": "AADSTS70002: Error validating credentials. AADSTS50011: The reply address 'http://localhost:40298/Home/Discovery' is not valid."}
```



# Troubleshooting tokens

## Fiddler

Extension to view SharePoint 2013 App tokens

- <http://blogs.msdn.com/b/kaevans/archive/2013/08/25/creating-a-fiddler-extension-for-sharepoint-2013-app-tokens.aspx>

## Online

Paste token in web page

- <http://jwt.io/>

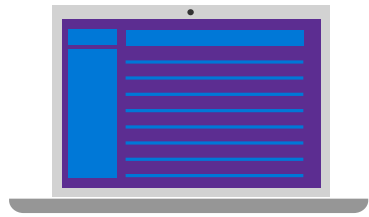
The screenshot shows the Fiddler Web Debugger interface. The left pane displays a list of intercepted requests. The right pane shows the details of a selected request, specifically the 'Headers' tab. The 'Headers' tab displays the raw response from the server, which is a JSON object representing an OAuth2 token. Below the raw response, a table lists the key-value pairs of the token.

Key	Value
aud	https://w.sharepoint.com
iss	https://sts.windows.net/...
iat	1410404456
nbf	9/11/2014 3:00:56 AM
exp	9/11/2014 4:05:56 AM
ver	1.0
tid	3742fa77-3e99-4ca0-b48e-4efd683935b0
amr	System.Object[]
oid	c0897439-6d22-4e69-ba54-61e70b5d4a2

# Summary

- ➡ Introduction
- ➡ OAuth basics and authentication flow
- ➡ App registration tool
- ➡ Azure Management Portal access
- ➡ Troubleshooting

# Developer Program launch



Email  
Newsletters



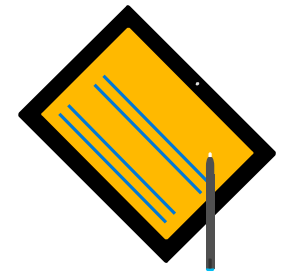
Free  
Developer  
Subscription



Free  
Training



Free  
Tools



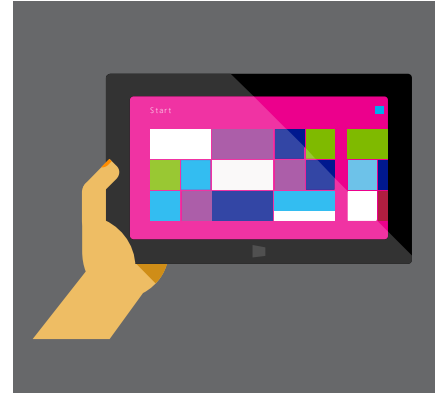
Webinars

<http://dev.office.com/devprogram>

# Engage

Office 365 Network

<https://www.yammer.com/itpronetwork>



Twitter  
[@OfficeDev](https://twitter.com/OfficeDev)



Stack overflow

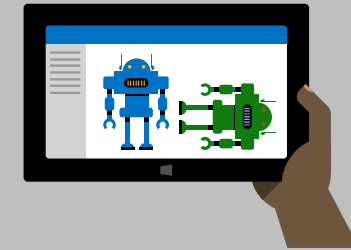


[ms-office]



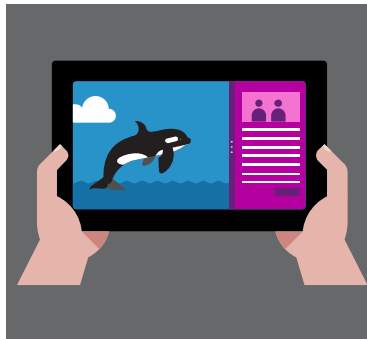
Channel 9  
Dev Show

<http://aka.ms/O365DevShow>



Podcasts

<http://dev.office.com/podcasts>



Snack Demos

YouTube

<http://aka.ms/o365DevSnackDemos>

UserVoice



<http://officespdev.uservoice.com/>

