

# Azure Active Directory

Reto Rechsteiner

Senior Software Engineer

bbv Software Services

Microsoft Azure

# Agenda

- Azure Active Directory (AAD) Introduction
- Getting Started with AAD
- SaaS Application Access
- Graph API
- Multi-Factor Authentication (MFA)
- AAD Premium Features

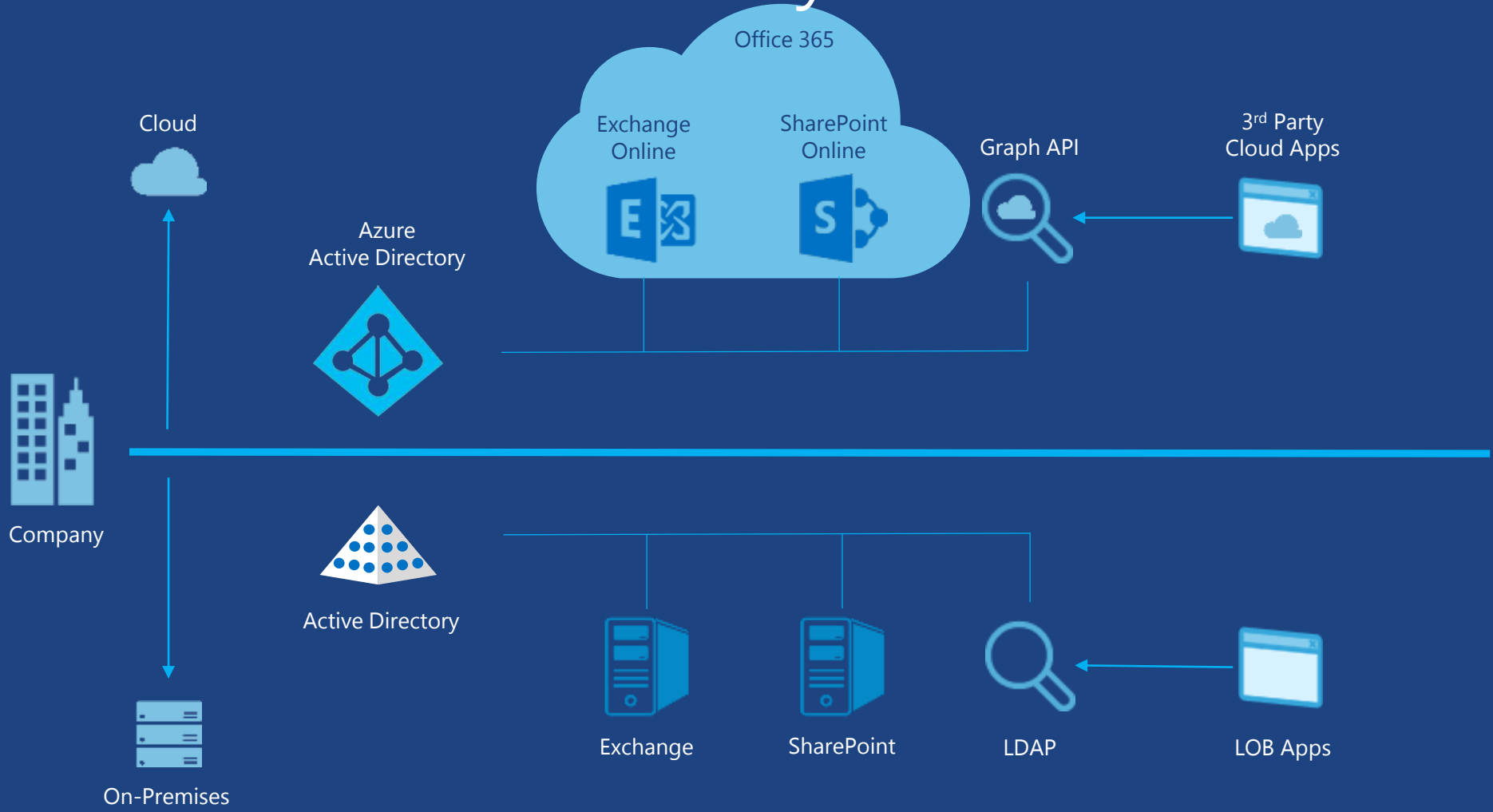
# What is it?

A multi-tenant service that provides enterprise-level identity and access management for the cloud.  
Built to global scale, reliability and availability.

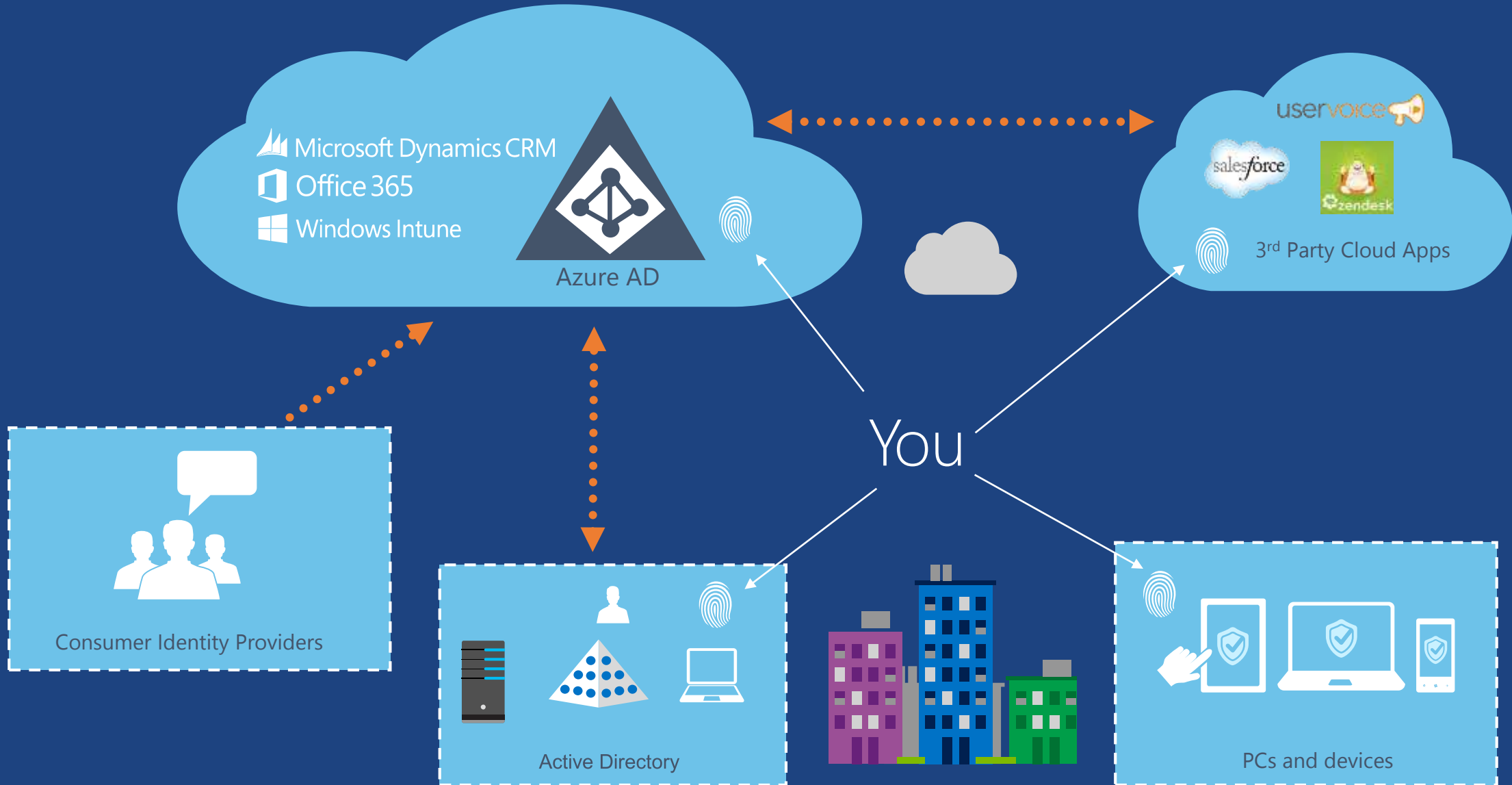
# What can I do with it?

- Manage users and access to cloud resources.
- Extend your on premise Active Directory to the cloud.
- Provide single-sign-on (SSO) across your cloud applications.
- Reduce risks by enabling multi-factor authentication.

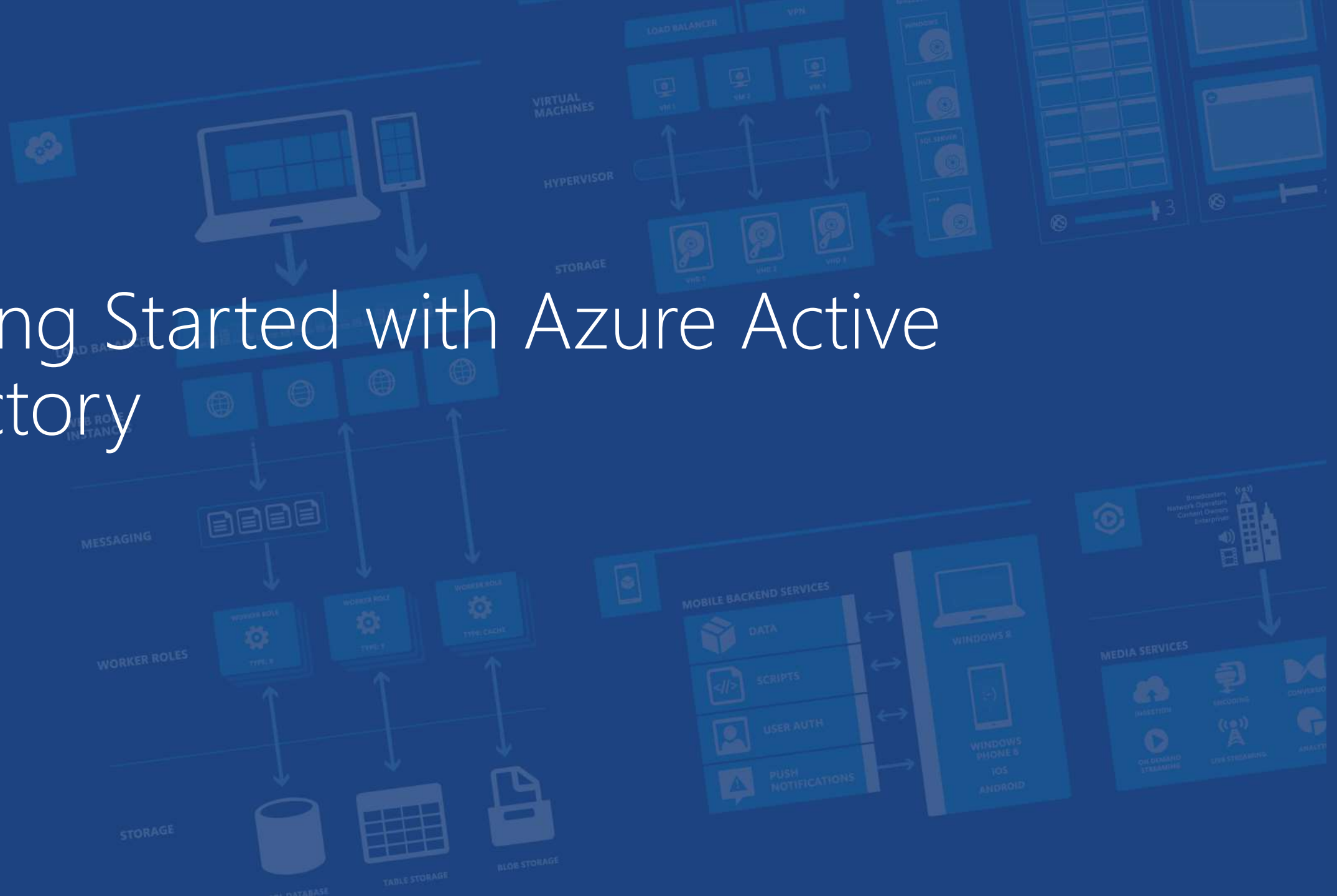
# Similarities between Active Directory & Azure Active Directory



# Your identity goes with you



# Getting Started with Azure Active Directory



# Create your own Subscription

Azure Subscription  
(Microsoft Account)



Office 365  
Subscription



Szenario 1		
Szenario 2		X
Szenario 3	X	
Szenario 4	X	X

<https://account.windowsazure.com/organization>

<http://azure.microsoft.com/de-de/pricing/free-trial/>

# SaaS Application Access





# Application Access Overview

## Software-as-a-Service (SaaS) Applications

Azure AD enables easy integration to many of today's popular SaaS applications, such as Salesforce, Google Apps, DocuSign, DropBox, Zendesk, Uservoice, etc.

## Integrating SaaS Apps with AAD

Single Sign-On (SSO) enables users to access their applications using their organizational ID.

Account synchronization enables user provisioning/de-provisioning into application based on changes in Windows Server AD and/or Azure AD.

Centralized application access management.

# Application Access Panel

<https://myapps.microsoft.com>

This is where users can discover the applications they have access to.

## Feature of the Access Panel

Users can change the password associated with their organizational account.

# AAD Demo



# Graph API



# Graph API



- RESTful interface to Azure Active Directory
  - Tenant Specific – queries are scoped to individual tenant context
  - Programmatic access to directory objects such as Users, Groups, Contacts, Tenant Information, Roles, Applications and Permissions
  - Access relationships: members, memberOf, manager, directReports
- Requests use standard HTTP methods
  - GET, POST, PATCH, DELETE to create, read, update, and delete
  - Response support JSON, XML, standard HTTP status codes
  - Compatible with OData V3
- OAuth 2.0 Support
  - Both Client Credentials and Authorization Code flow

# Graph API

Graph  
URL  
(static)

Tenant of interest –  
can be tenant's  
verified domain or  
objectId.

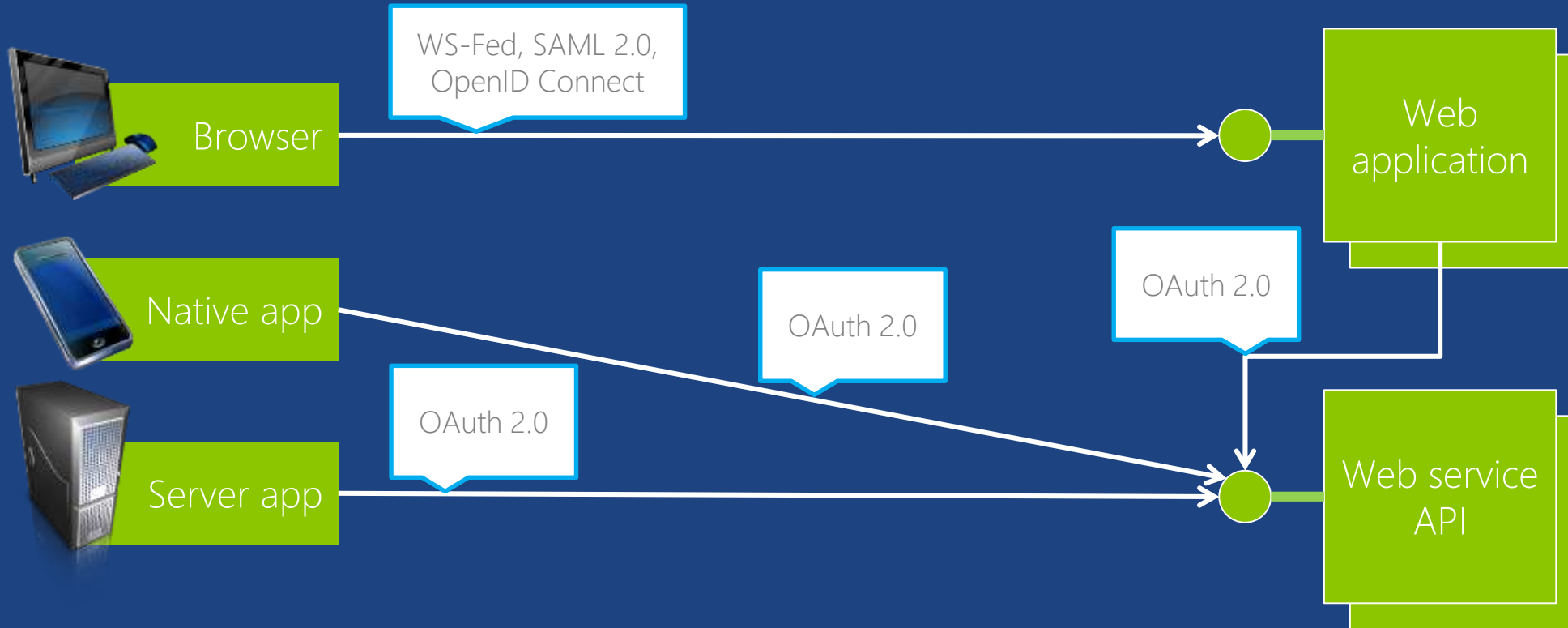
Specific entity type, such as users,  
groups, contacts, tenantDetails, roles,  
applications, etc.

[https://graph.windows.net/contoso.com/users?api-version=2013-04-05&\\$filter=state eq 'WA'](https://graph.windows.net/contoso.com/users?api-version=2013-04-05&$filter=state eq 'WA')

API version – "2013-04-05" is the 1.0 version

Optional Odata query arguments: \$filter, \$top

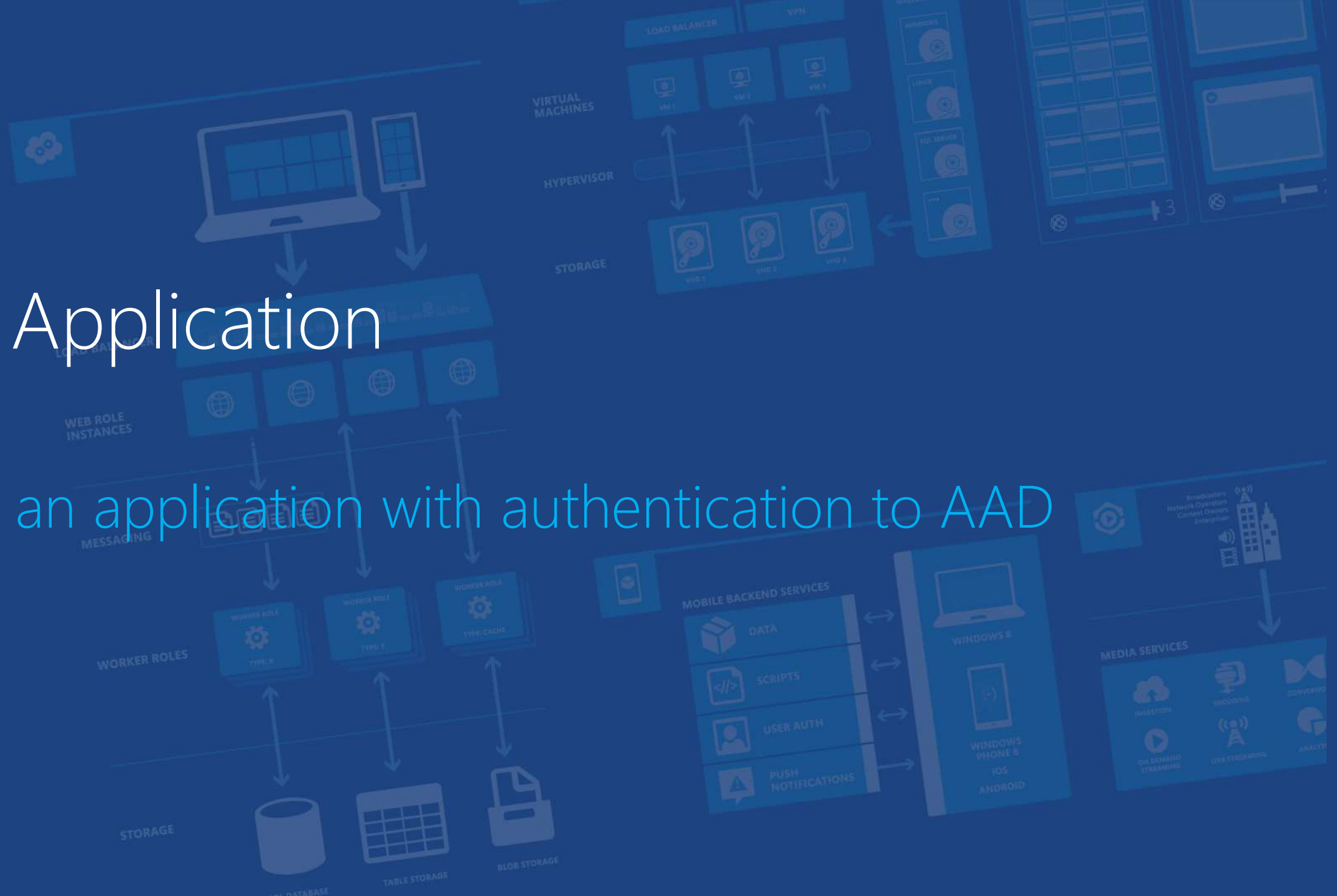
# Modern Authentication Protocols



*Standard, http-based protocols for maximum platform reach*

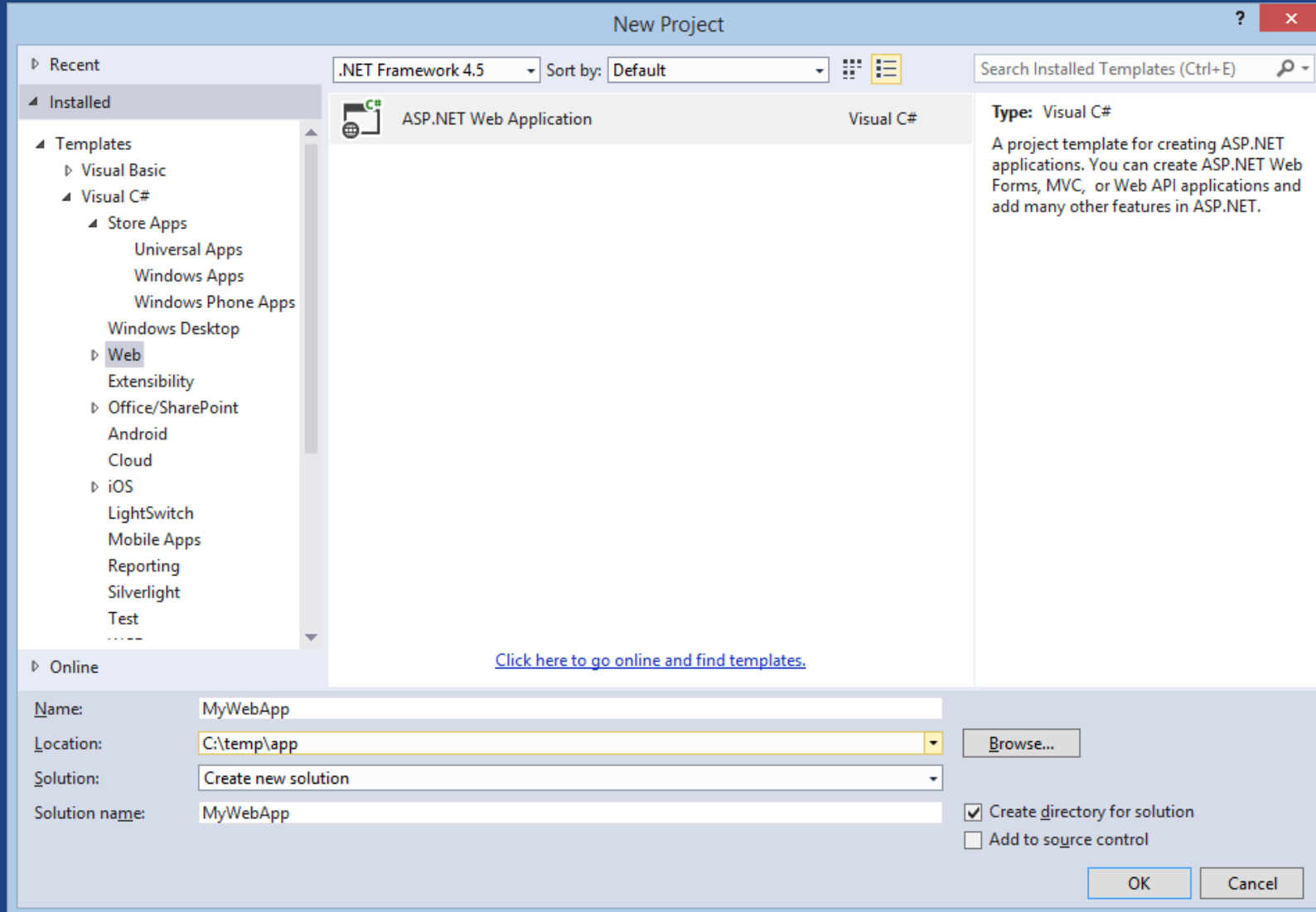
# Web Application

Create an application with authentication to AAD

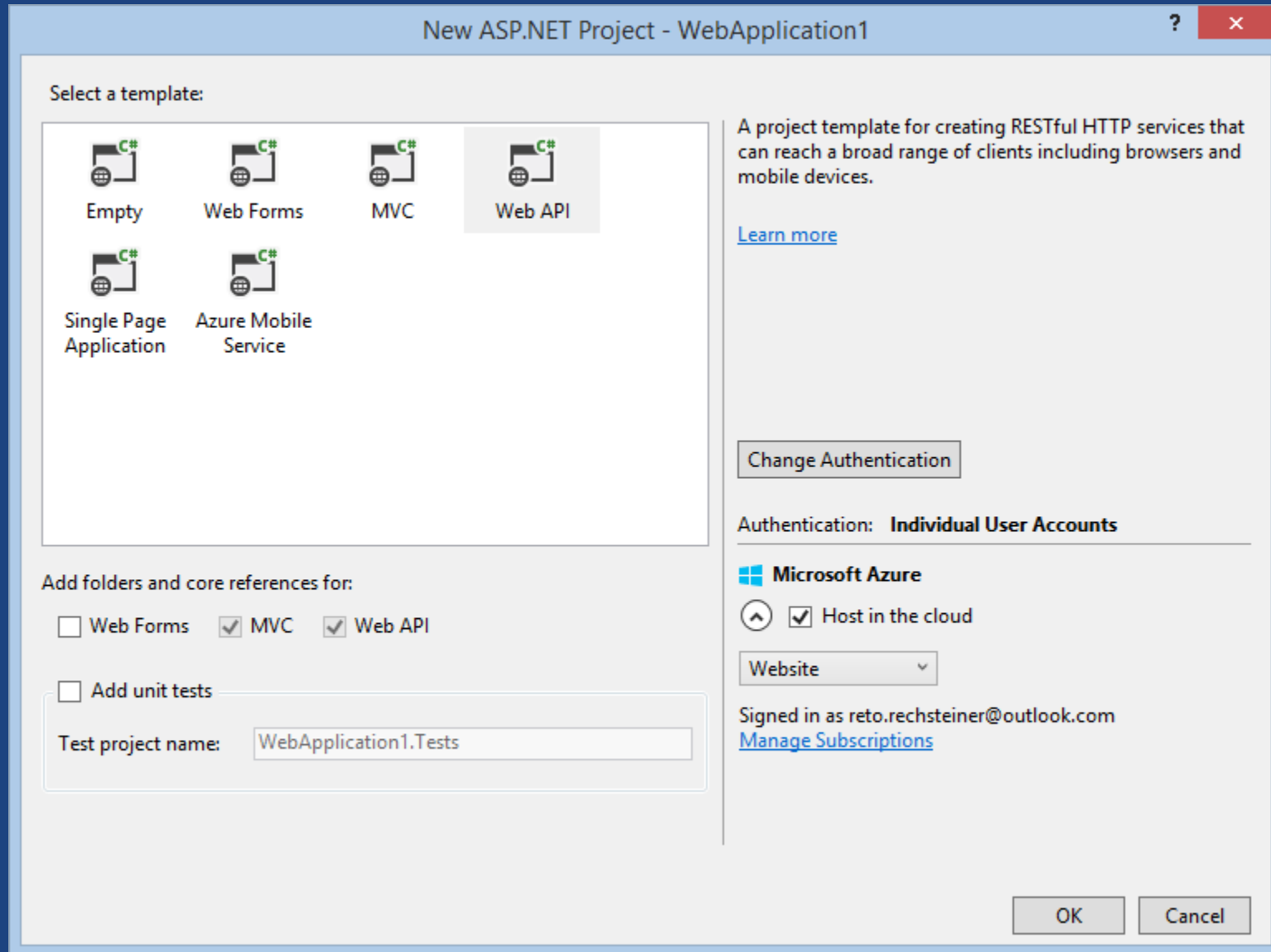




# Step 1: Visual Studio, file new project



# Step 2: Click "Change Authentication"



# Step 3: Configure organizational account

Change Authentication ✕

For applications that authenticate users with Active Directory, Microsoft Azure Active Directory, or Office 365.

[Learn more](#)

No Authentication

Individual User Accounts

Organizational Accounts

Windows Authentication

Cloud - Single Organization ⓘ

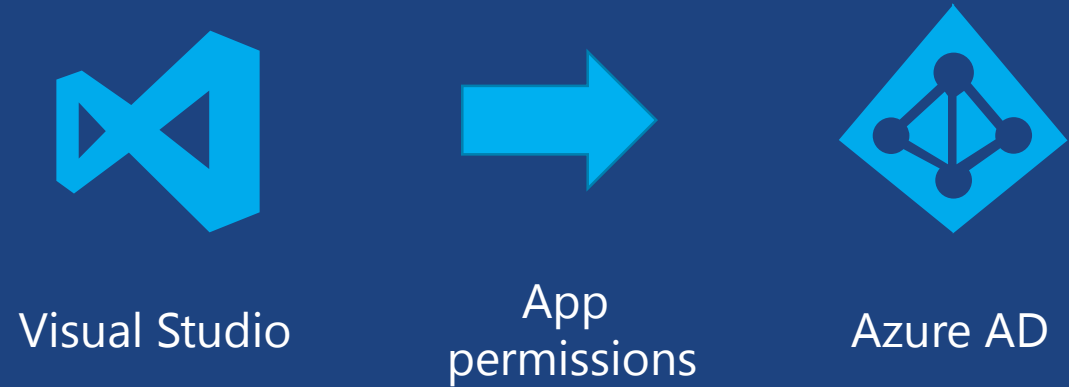
Domain:  
rechsteinerTest.onmicrosoft.com ⓘ

Access Level:  
Single Sign On ⓘ

⌵ More Options

OK Cancel

# What happens then:



Visual Studio configures the application permission settings for you on Azure Active Directory!

# Graph API Demo



# Multi-Factor Authentication



# Azure MFA

## What is it?

An application service requiring users to verify themselves using a **mobile app**, **automated phone call** or **text message** in addition to providing a password.

## Purchasing Windows Azure MFA

Free for Global Administrators of a Azure Active Directory Tenant

Options for purchasing

- Per User – Generally for a fixed number of users who **authenticate regularly**.
- Per Authentication – Generally for a large group of external users who **authenticate infrequently**.

# Azure MFA

How it works...



Login using username and password



Windows Azure MFA Challenge



Response to challenge from device





# Azure MFA Demo



# Azure Active Directory Premium Features



# WAAD Versions

Azure Active Directory is offered in three tiers: Free, Basic, and Premium.

Azure Active Directory Basic and Premium are licensed separately from Azure Services and are available for purchase through [Microsoft's Enterprise Agreement volume licensing program](#).

	FREE	BASIC	PREMIUM
Price (per user)	Free	Contact your <a href="#">Enterprise Agreement</a> representative	Contact your <a href="#">Enterprise Agreement</a> representative
Directory as a Service	✓	✓	✓
User and Group Management	✓	✓	✓
Directory Objects <sup>1</sup>	500K	Unlimited	Unlimited
End User Access Panel	✓	✓	✓
SSO for SaaS Apps	10 Apps / User <sup>2</sup>	10 Apps / User <sup>2</sup>	Unlimited
Directory Synchronization	✓	✓	✓
User-based Access Management and Provisioning	✓	✓	✓
Basic Security Reports	✓	✓	✓
Logon/Access Panel Branding Customization		✓	✓
Group-based Access Management and Provisioning		✓	✓

	FREE	BASIC	PREMIUM
Self-Service Password Reset for Cloud Users		✓	✓
Self-Service Password Reset for Users w/ writeback to on-premises directories			✓
Self-service group management for cloud users			✓
Multi-Factor Authentication (for cloud and on-premises applications)			✓
Advanced Usage and Security Reports			✓
Microsoft Identity Manager Server and User CAL			✓
Service Level Agreement		99.9%	99.9%

# Graph Resources

- Graph Explorer
  - <https://graphexplorer.cloudapp.net/>
- Graph API Documentation
  - <http://msdn.microsoft.com/en-us/library/hh974476.aspx>
- Graph API Sample Code
  - <http://msdn.microsoft.com/en-us/library/hh974459.aspx>
  - <https://github.com/AzureADSamples>

# Resources

- Windows Azure Active Directory
  - <http://msdn.microsoft.com/en-us/library/jj673460.aspx>
- Windows Azure Friday
  - <http://www.windowsazure.com/en-us/documentation/videos/windows-azure-friday>
- Microsoft Virtual Academy
  - <http://www.microsoftvirtualacademy.com/>
- Channel 9 Windows Azure
  - <http://channel9.msdn.com/WindowsAzure>
- Pricing
  - <http://azure.microsoft.com/en-us/pricing/calculator>

# Questions?

