Known and Unknown Facts of Azure AD

An Insight

ENTERPRISE PRODUCTIVITY

Contents

1. Introduction

Azure Active Directory (Azure AD) is a modern cloud service managed identity that provides identity management and authentication services to your application.

Windows Azure Active Directory - Capability

-Active Directory as a Service

-Single Sign on and single sign out for Windows Azure applications

-Manage Users and Groups

-Integrate with On-Premises Active Directory Servers

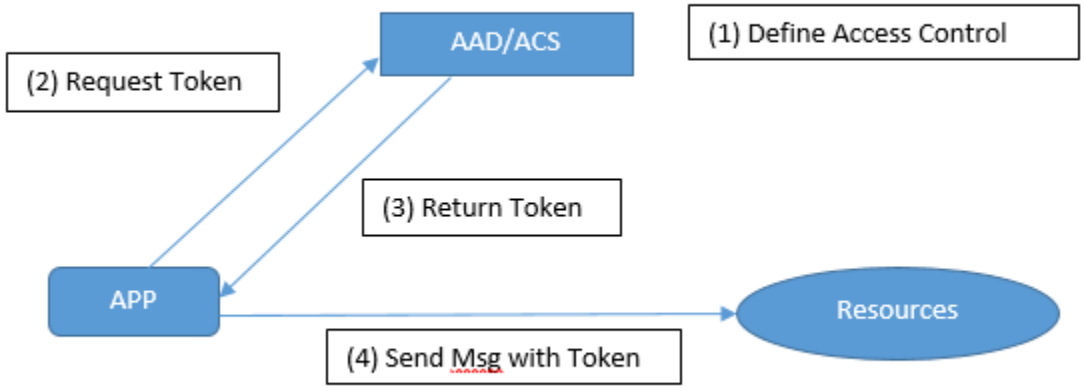
- Multi-Factor Authentication Support

Azure AD offered in three tiers: Free, Basic and Premium. Free Tier covers basic cloud application. Basic and Premium are designed for enterprise usage at scale and currently covered under MS Volume Licensing program

Authentication Protocols for Federated Identity Supported by Azure AD

- WS Federation-It is a passive Authentication protocol also has a modular architecture, Used in ADFS (ASP.Net WS Federation OWIN Middleware). The use of WS-Federation is appropriate when you want to maintain a single app codebase that can be deployed either against Azure AD or an on-premises provider such as an Active Directory Federation Services (ADFS) instance.
- SAML (Security Assertion Markup Language): It is an open standard for exchanging authentication and authorization data between parties, between an identity provider and a service provider, Used for Ping Identity. SAML 2.0 identity provider must implement to federate with Azure AD to enable sign-on to one or more Microsoft cloud services
- OpenID Connect: It is light weighted protocol and authentication Layer on top of Oath 2.0 (an authorization Layer). OpenID Connect allows a range of clients, including Web-based, mobile, and JavaScript clients, to request and receive information about authenticated sessions and end-users.

How Azure AD Authentication works?



2. Adding Users and Groups to Azure AD

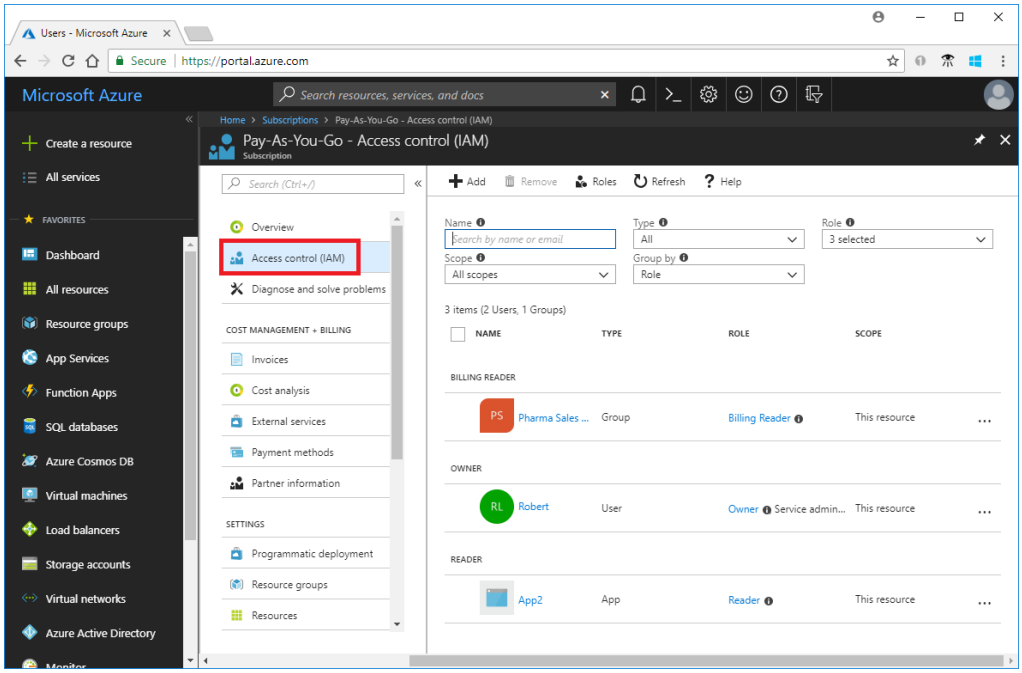
Role-based access control (RBAC) is the way that you manage access to resources in Azure. This article describes how you manage access for users, groups, and applications using RBAC and the Azure portal

2.1 Groups

- ✓ By synchronizing from an on-premises Windows Server Active Directory using AAD Connect. This is how most enterprise customers will get their users added to the directory and requires some additional server configuration on-premises to setup.
- ✓ Manually using the Azure Management Portal. The portal experience is very easy and intuitive.
- ✓ Scripted using PowerShell and the Azure Active Directory cmdlets. PowerShell makes automating this task very useful, particularly for large user bases.
- ✓ Programmatically using the Azure AD Graph API. This extremely powerful option essentially gives you full control of how users are added to the directory.

2.2 App Roles

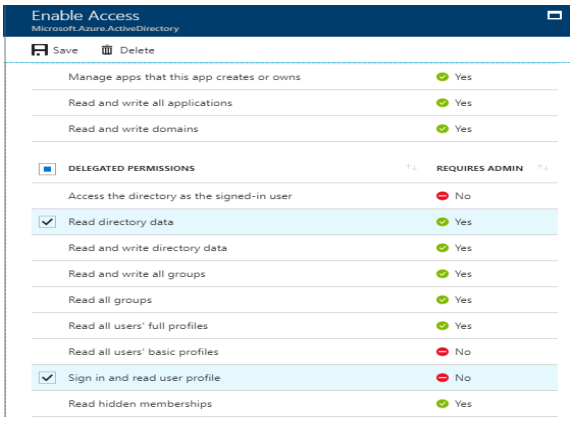
- ✓ Role based access to Azure client Application,
- ✓ Application roles are used to assign permissions to users.

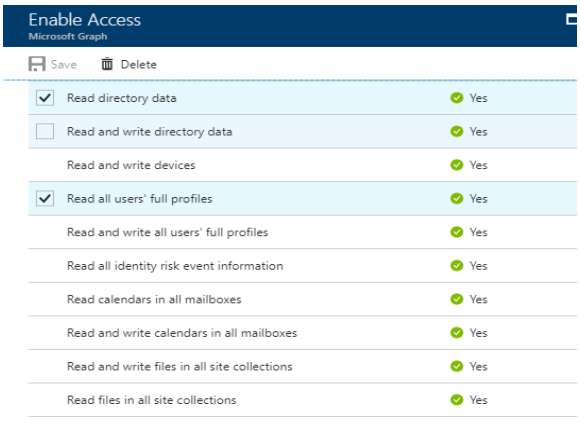


3. Azure Active Directory Graph API

The Azure Active Directory Graph API provides programmatic access to Azure AD through REST API endpoints. Applications can use Azure AD Graph API to perform create, read, update, and delete (CRUD) operations on directory data and objects.

Graph API, provides a REST API endpoint for you to interact with directory data and objects. You can perform creating users, updating user properties, checking user group membership and deleting user. The API supports both content type Json and XML. That you can use directly integrate with Azure AD objects for scenarios such as user managements and Role based access control (RBAC) programmatically





4. Application Tenancy Type

There are two categories of applications that can be developed and integrated with Azure AD

- Single tenant application: A single tenant application is intended for use in one organization. These are typically line-of-business (LoB) applications. A single tenant application only needs to be accessed by users in one directory, and as a result, it only needs to be provisioned in one directory. (abc.onmicrosoft.com)
- Multi-tenant application: A multi-tenant application is intended for use in many organizations, not just one organization. These are typically software-as-a-service (SaaS) applications. Multi-tenant applications need to be provisioned in each directory where they will be used, which requires user or administrator consent to register them. This consent process starts when an application has been registered in the directory and is given access to the Graph API or perhaps another web API. When a user or administrator from a different organization signs up to use the application, they are presented with a dialog that displays the permissions the application requires. (Other domain – xyz.onmicrosoft.com)

Configure Multitenant Service

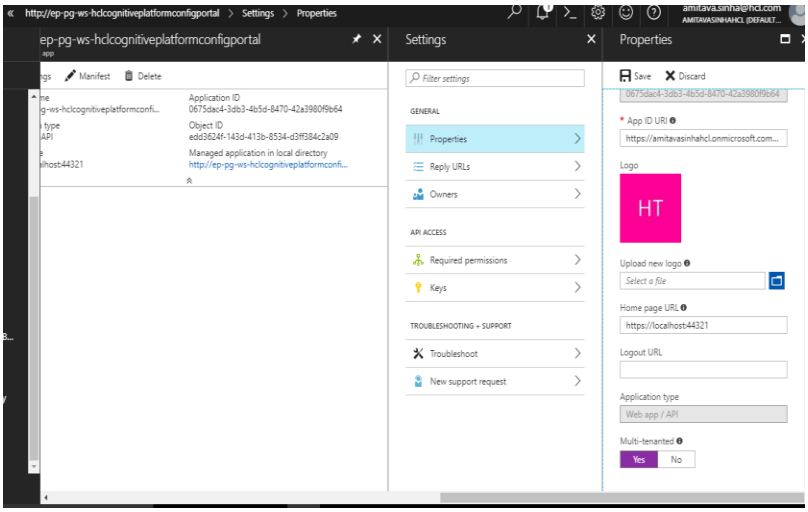
1. Sign In to the Azure Portal

2. In the left-hand navigation pane, click the Azure Active Directory service, click

App registrations, then find/click the application you want to configure. You are taken to the

Application's main registration page, which opens up the Settings page for the application.

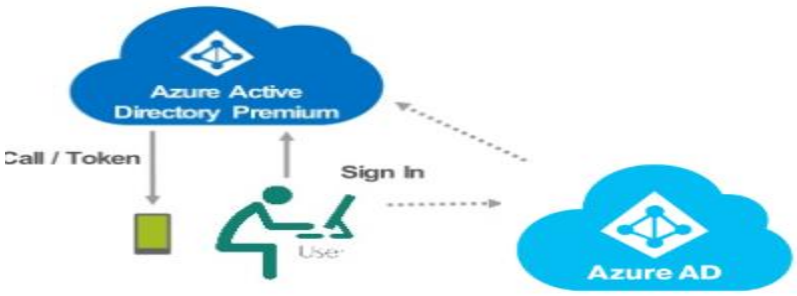
3. From the Settings Page, Click Properties and change the "Multi-Tenanted" to Yes.



5. Multi Factor Authentication

Azure Multi-Factor Authentication (MFA) helps safeguard access to data and applications while maintaining simplicity for users. It provides additional security by requiring a second form of authentication and delivers strong authentication via range of authentication method (password, Biometrics, OTP)

Two-step verification is a method of authentication that requires more than one verification method and adds a critical second layer of security to user sign-ins and transactions. It delivers strong authentication via a range of easy verification options—phone call, text message or mobile app notification and OTP



Azure MFA helps safeguard access to data and applications while meeting user demand for a simple sign-in process.

It is available through various Licensing programme (Open Volume License Programme) like Per – User Consumption and Per –Authentication Consumption

MFA Enabling Mechanism

- We can enable in two ways by MFA in the Cloud and MFA Server (That need to be installed and Configured)

What are we trying to secure	MFA in the cloud	MFA Server
SaaS apps in the app gallery	Yes	
Web applications published through Azure AD App	yes	
IIS applications not published through Azure AD App		yes

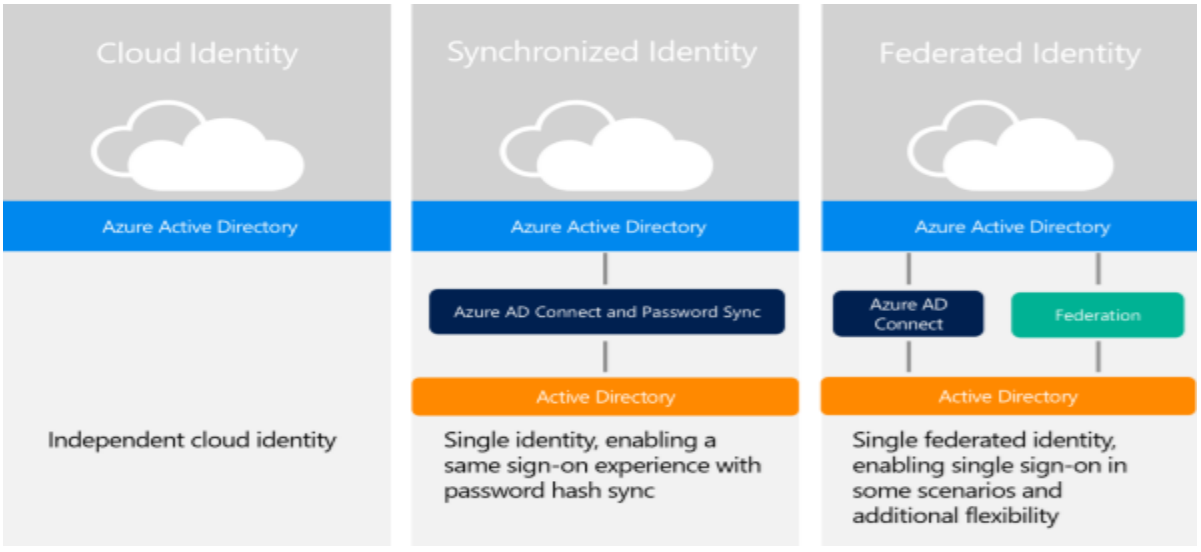
- Also the Configuration depends on User Location

User Location	MFA in the cloud	MFA Server
Azure Active Directory	yes	
Azure AD and on-premises AD using federation with AD FS	yes	yes
Azure AD and on-premises AD using Azure AD Connect - no password hash sync or pass-through authentication	yes	yes

- **Multi-Factor Authentication with a conditional access policy**

6. Azure AD Synchronization

Azure AD Connect will integrate your on-premises directories with Azure Active Directory. This allows you to provide a common identity for your users for Office 365, Azure, and SaaS applications integrated with Azure AD. It takes care of all the operations that are related to synchronize identity data between your on-premises environment and Azure AD.



Azure Active Directory Connect is made up of three primary components: the synchronization services, the optional Active Directory Federation Services component, and the monitoring component named Azure AD Connect Health

7. References

Please refer to the following URLs for further information

https://docs.microsoft.com/en-us/azure/active-directory/

https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-manage-groups

https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-federation-saml-idp