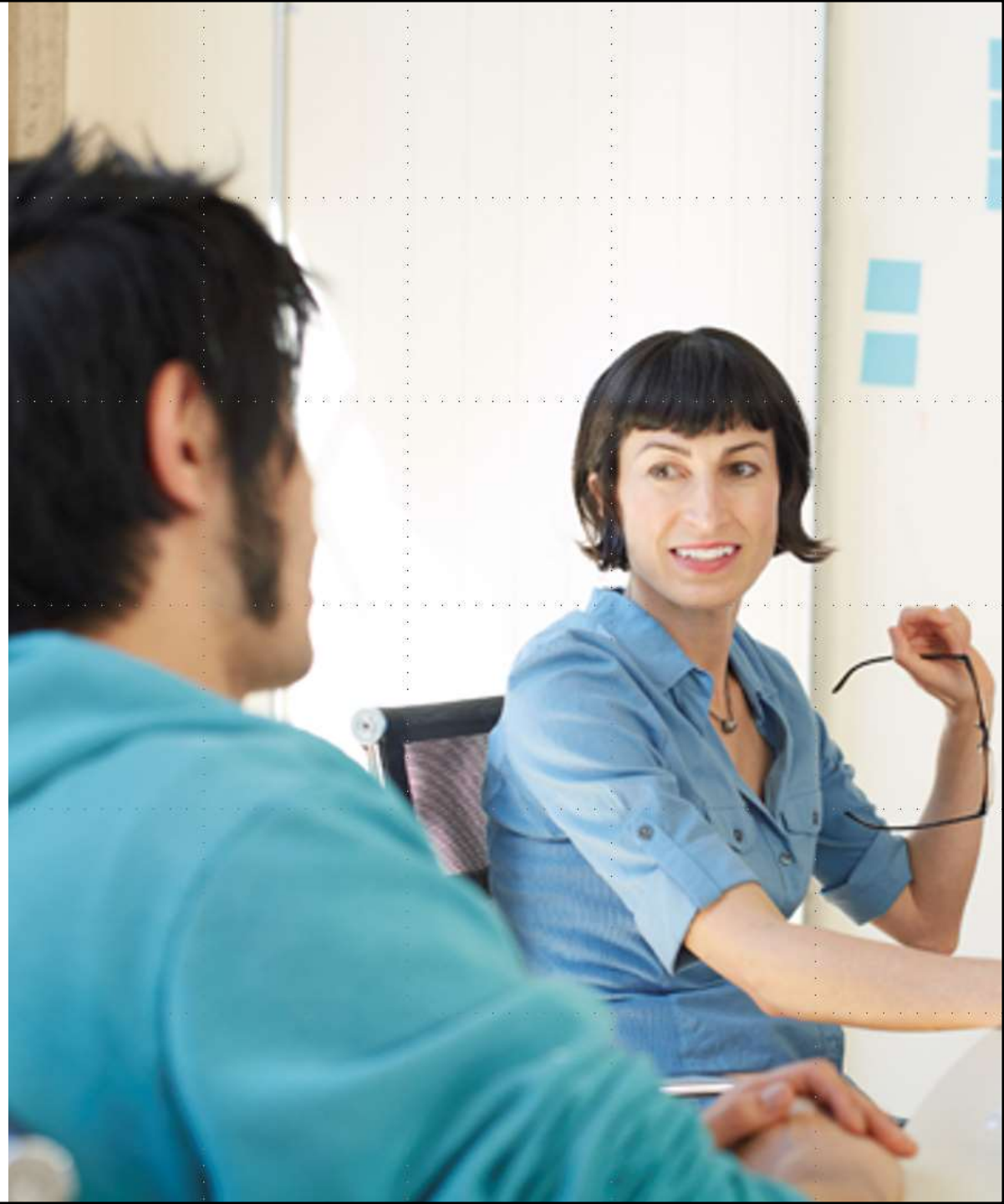
Microsoft

Azure Active Directory

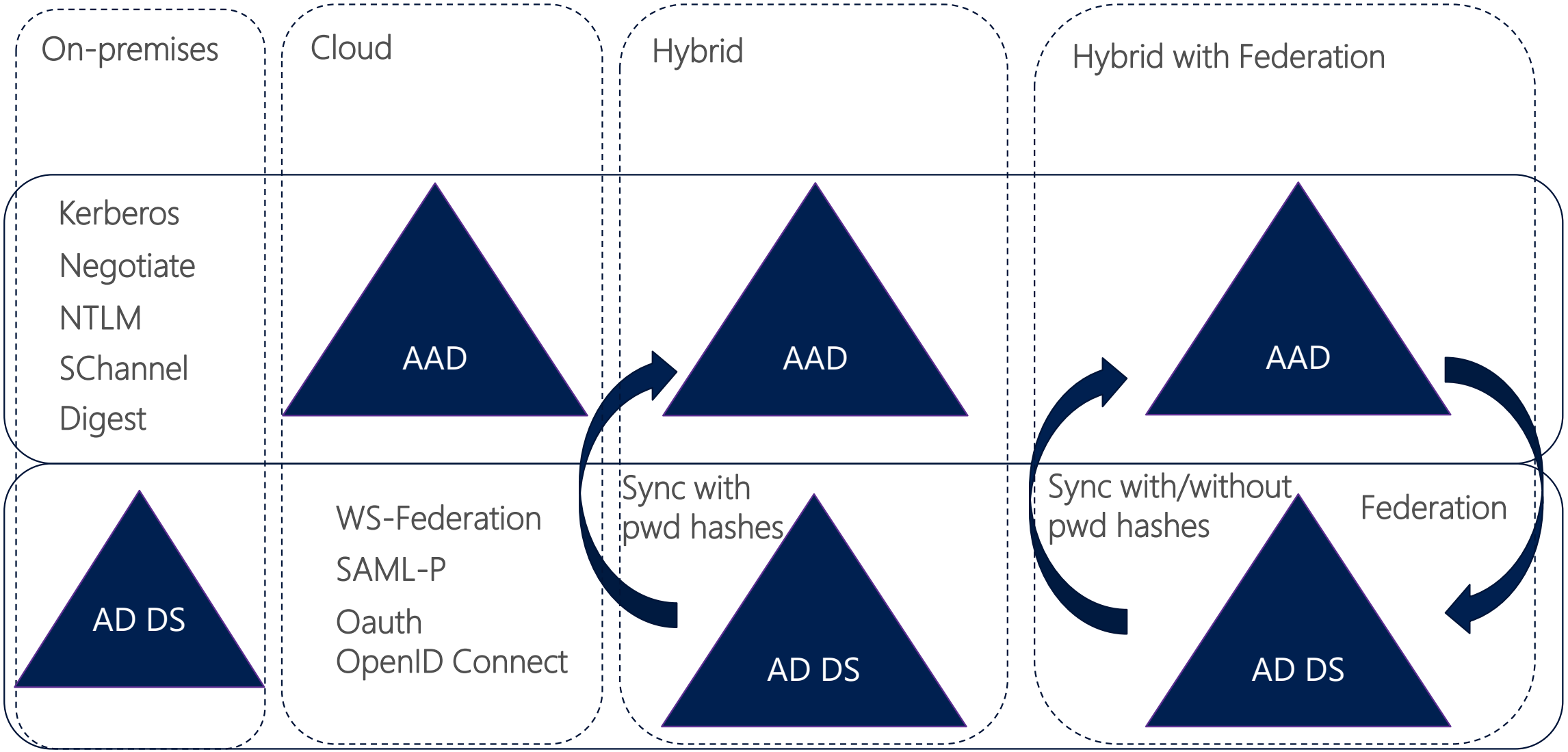
Microsoft Services

Agenda

- Azure AD
- Azure AD Domain Services
- Role Based Access Control (RBAC)
- Azure AD B2B & B2C
- Azure Multi-Factor Authentication
- Azure AD Application Proxy
- Azure AD Conditional Access
- Azure AD Privileged Identity Management



Identity Today



Problem Statement

Traditional directories and cloud workloads

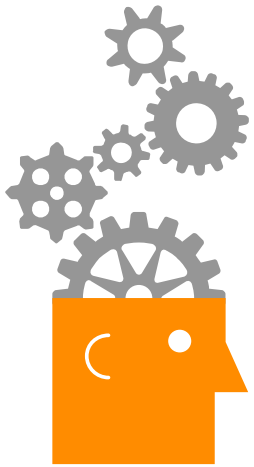
The protocols not designed for cloud

New authentication protocols are better suited for cloud

Connection to the directory is not permanent

Need for interoperable authentication/authorization protocol

Multiple authentication systems break the SSO consolidation



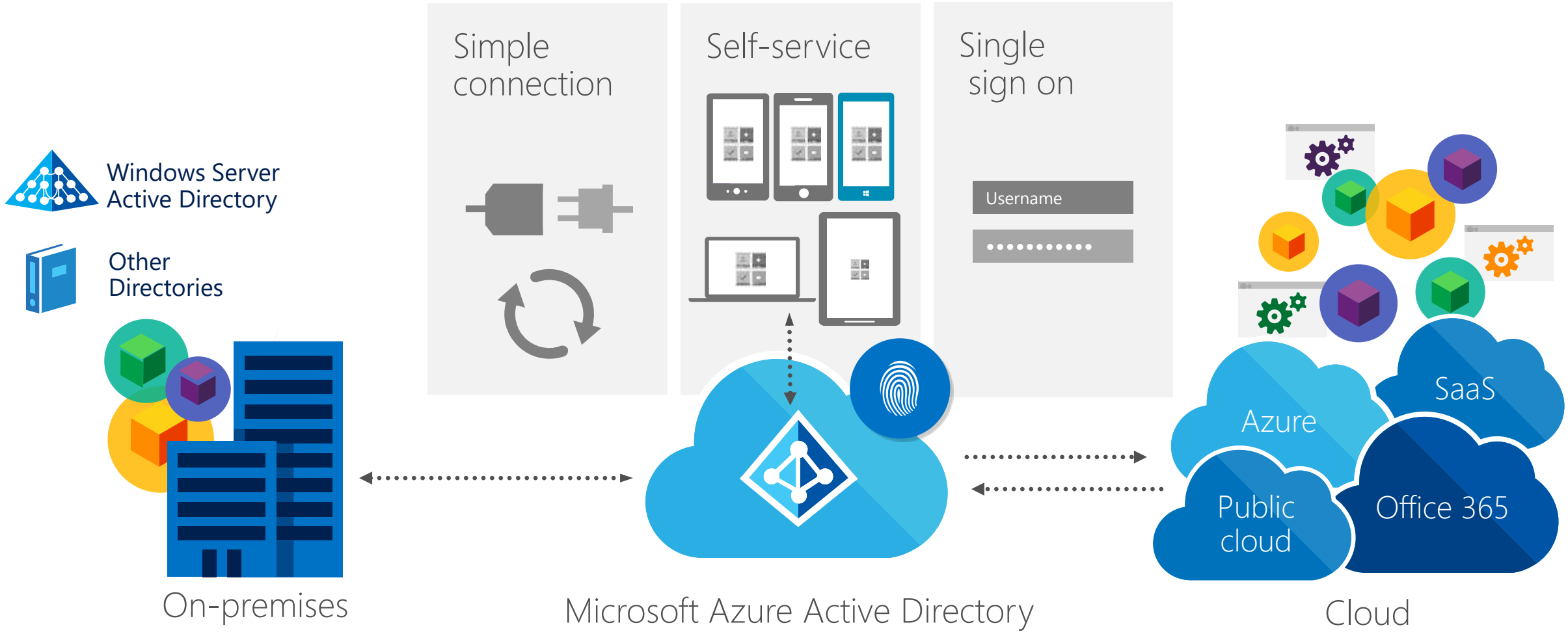
What is Microsoft Azure AD?

A multi-tenant directory in the cloud	Extension of AD DS into the cloud	Designed for cloud applications	Identity as a service	Available in Four Editions

Why Microsoft Azure AD?

Central management of the entities	Allows connecting to the Cloud directory from any platform with any device	Allows identities to be shared with application	Uses standard authentication/authorization protocols	Directory for small orgs with no identity infrastructure

Microsoft Azure Active Directory



Microsoft Azure AD Editions - Free

Manage user accounts

Synchronize with on-premises directories

Get single sign-on across Azure, Office 365, and thousands of SaaS applications

Microsoft Azure AD Editions - Basic

- Company branding
- Group-based application access
- Self-service password reset
- Enterprise SLA of 99.9%
- Azure Active Directory Application Proxy

Azure AD Editions - Premium P1 and P2

Company branding	Group-based application access	Self-service password reset	Enterprise SLA of 99.9%
Identity Protection	Privileged Identity Management	Azure Active Directory Application Proxy	

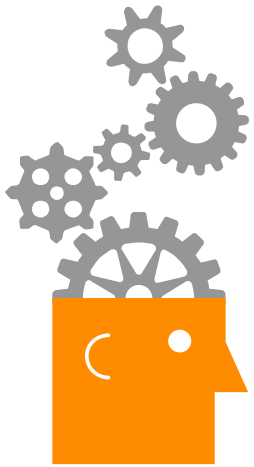
Microsoft

Azure AD Domain Services

Microsoft Services

What is Azure AD Domain Services?

AD DS as a Service	Domain Join, LDAP, NTLM and Kerberos Support	Completely integrated with your Azure AD Tenant
Lift and Shift made easier	Highly Available	Enterprise Scale and SLA



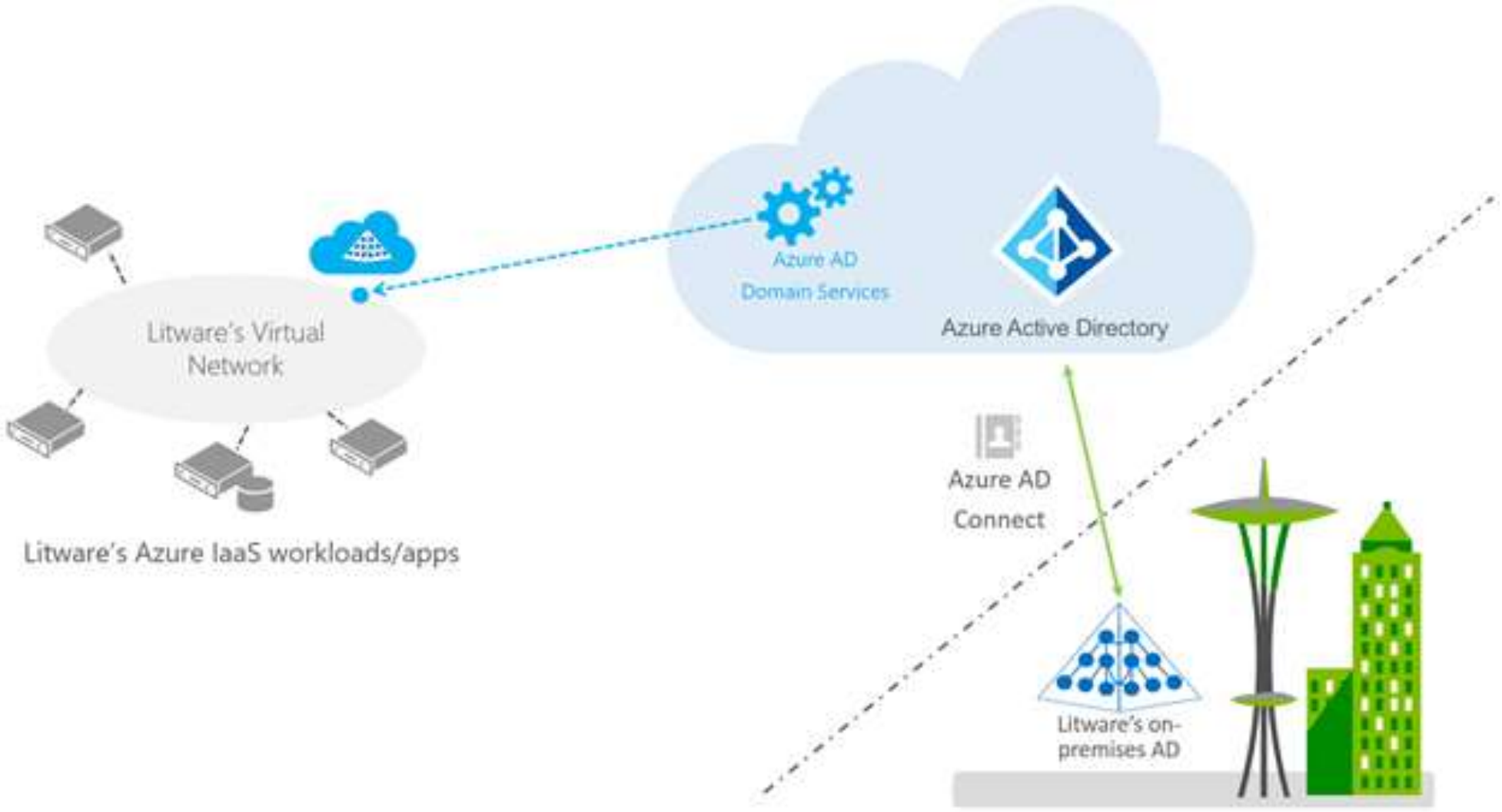
What you can do

- LDAP bind and LDAP read support
- Group Policy*
- Manage DNS
- Custom OUs*
- Deploy to ASM (Classic) VNet today*
- Deploy without VPN or ExpressRoute
- Manage with AD Admin Center and AD PowerShell

What you cannot do today

- AD DS Trusts
- Extend Schema
- Edit Default Domain or Default Domain Controllers Policy
- Domain Admin or Enterprise Admin access
- Deploy to multiple Azure VNet's (Geo Distributed)
- LDAP Write
- Connect to DCs via RDP

Azure AD Domain Services



Microsoft

Role Based Access Control (RBAC)

Microsoft Services

Role Based Access Control

Protecting resources

Secure access with granular permissions

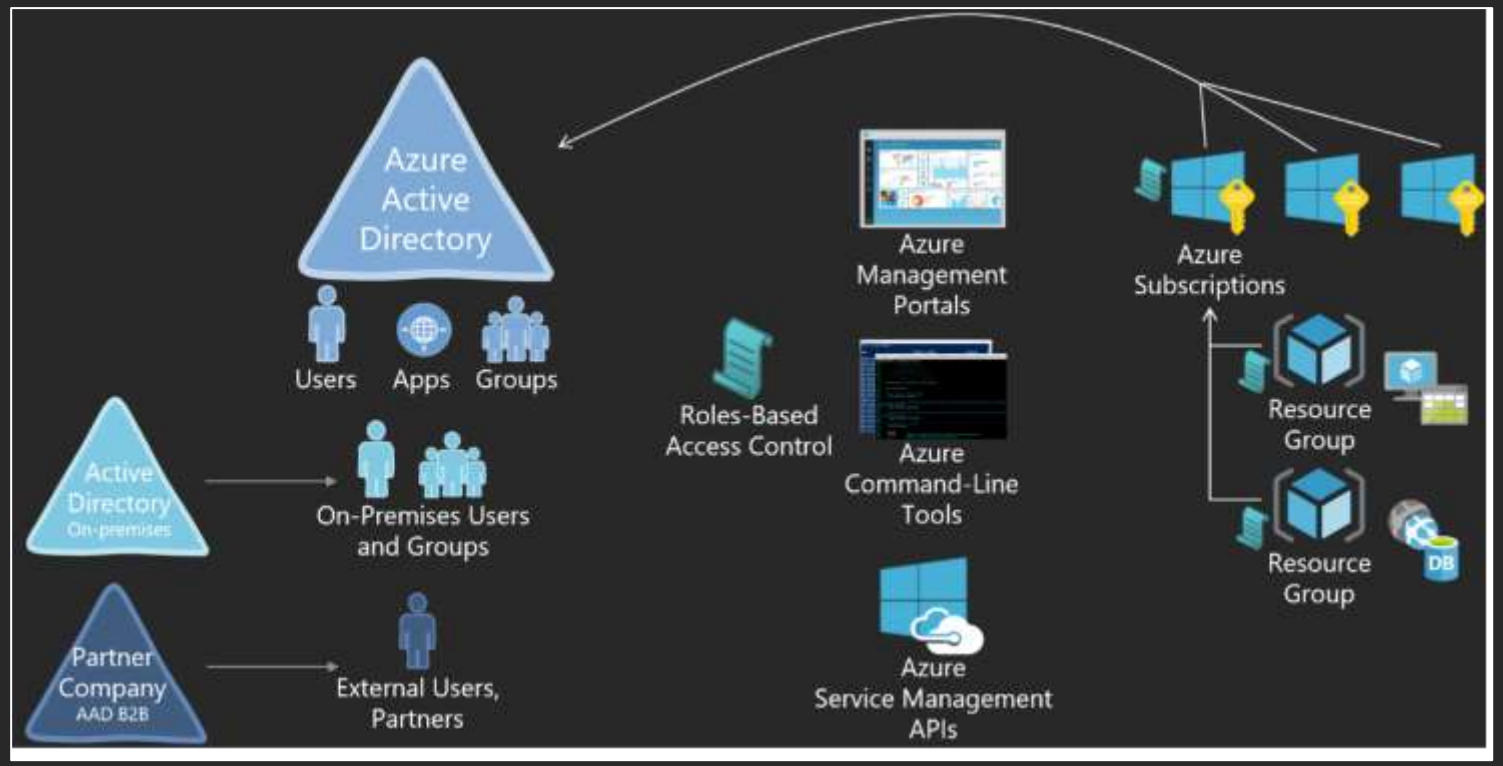
Assignable to users, groups, or service principals

Built-in roles

Custom Roles

Role Based Access Control

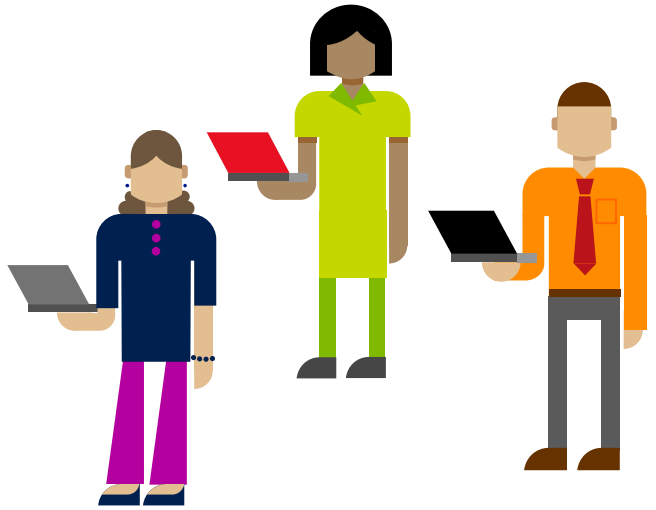
- Used only for Azure administration
  - Manage resources in Azure
  - Azure AD is not an Azure resource
- Roles composed of
  - Actions
  - Not Actions
  - Scopes



RBAC- Concepts

- Role Definitions
  - permissions
  - multiple assignments

- Role Assignments
  - associate role with an identity at a scope
  - always inherited

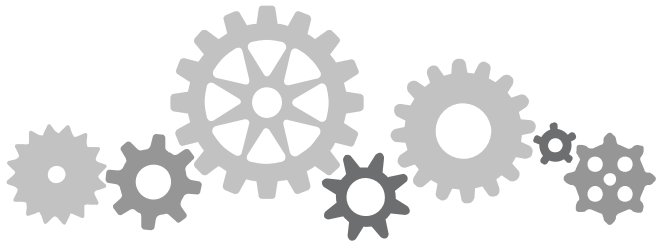


RBAC – Roles

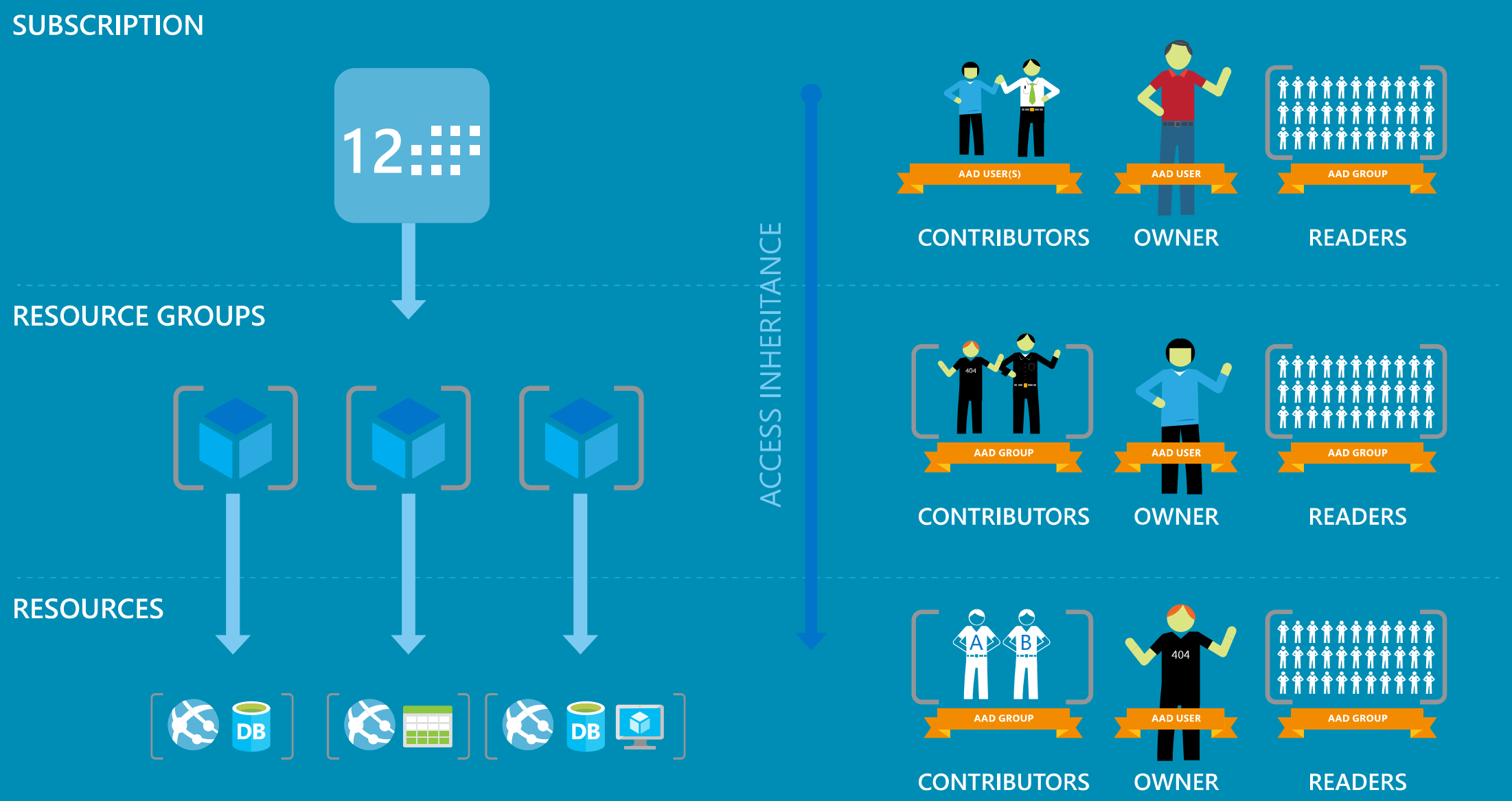
- Build-in roles

BUILT-IN ROLE	ACTIONS	NOT ACTIONS
Owner (allow all actions)	*	
Contributor (allow all actions except writing or deleting role assignments)	*	Microsoft.Authorization/*/Write, Microsoft.Authorization/*/Delete
Reader (allow all read actions)	*/Read	

- Custom roles

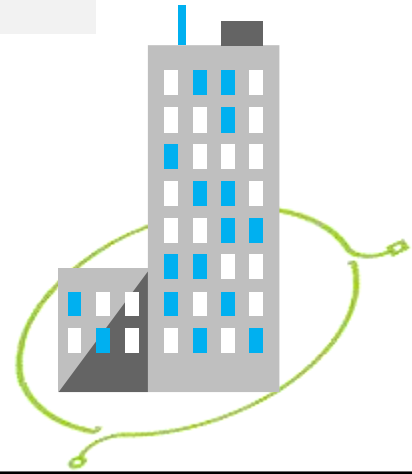


RBAC – Inheritance

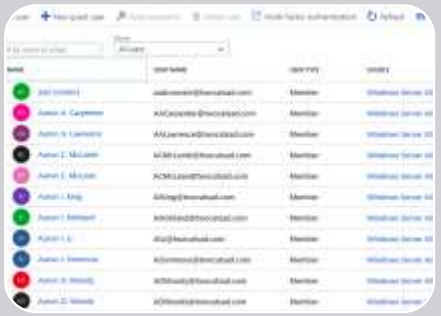


Azure AD Security Principals

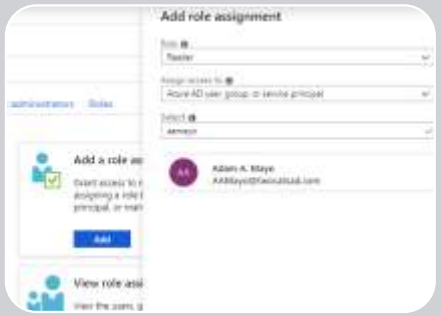
Roles can be assigned to:	Groups	Service Principals
• Users • Organizational users in Azure AD • External Microsoft accounts (@outlook.com)	• Azure AD security groups • Groups can be integrated with on-premises directories	• Service identities are represented as service principals in Azure AD • Assign to roles via Azure PowerShell cmdlets



Basic Process for Adding Access



Create user in Azure AD



Grant user read access to subscription

Browse for Resource or Resource group and add role to it

Add user to role

RBAC – Things you don't expect

Owners

Contributors

Virtual Machine - Write access

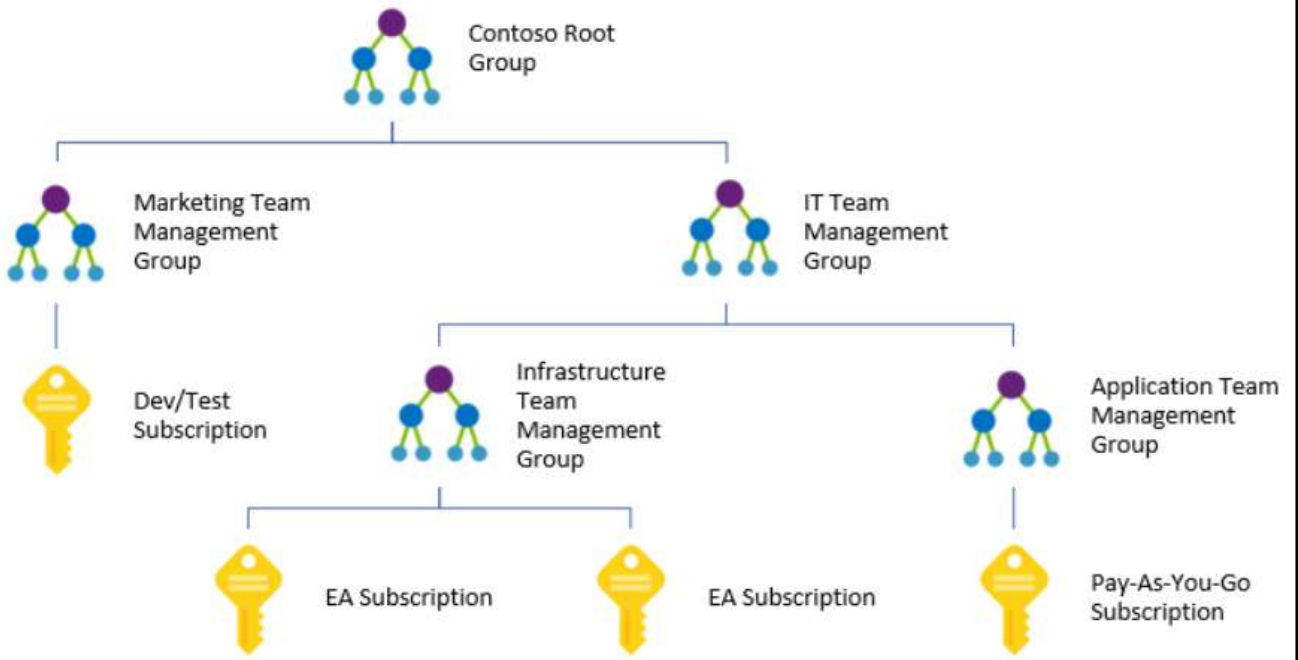
- IP Addresses
- Disks
- Extensions

Virtual Machine and Resource Group Write access:

- Availability Set
- Load balanced sets
- Alert Rules

Management Groups

- Management groups are containers that are used to store multiple subscriptions
- These containers are a level of scope above the subscription level
- Azure Policies and Role Based Access Control can now be applied at the following levels:
  - Management Group
  - Subscription
  - Resource Group
  - Resource



Root Management Group

Each directory is given a single top-level management group called the "Root" management group

This root management group is built into the hierarchy to have all management groups and subscriptions fold up to it

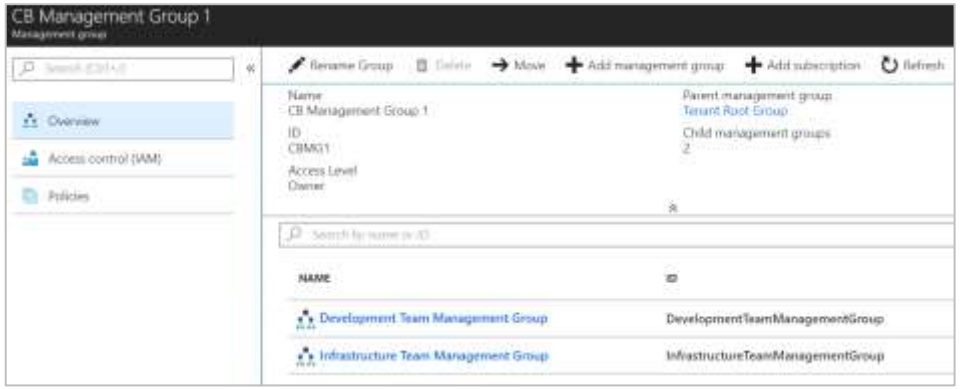
Allows for global policies and RBAC assignments to be applied at the directory level

Azure AD Directory Administrator needs to elevate themselves to be the owner of this root group initially

Once the administrator is the owner of the group, they can assign any RBAC role to other directory users or groups to manage the hierarchy

Management Group Limits

- 10,000 management groups can be supported in a single directory (Azure Active Directory tenant)
- A management group tree can support up to six levels of depth
- This limit doesn't include the Root level or the subscription level
- Each management group and subscription can only support one parent
- All subscriptions and management groups are contained within a single hierarchy in each directory



Demo: Role Based Access Control & Management Groups

Microsoft

Lab: Introduction to RBAC

Microsoft Services

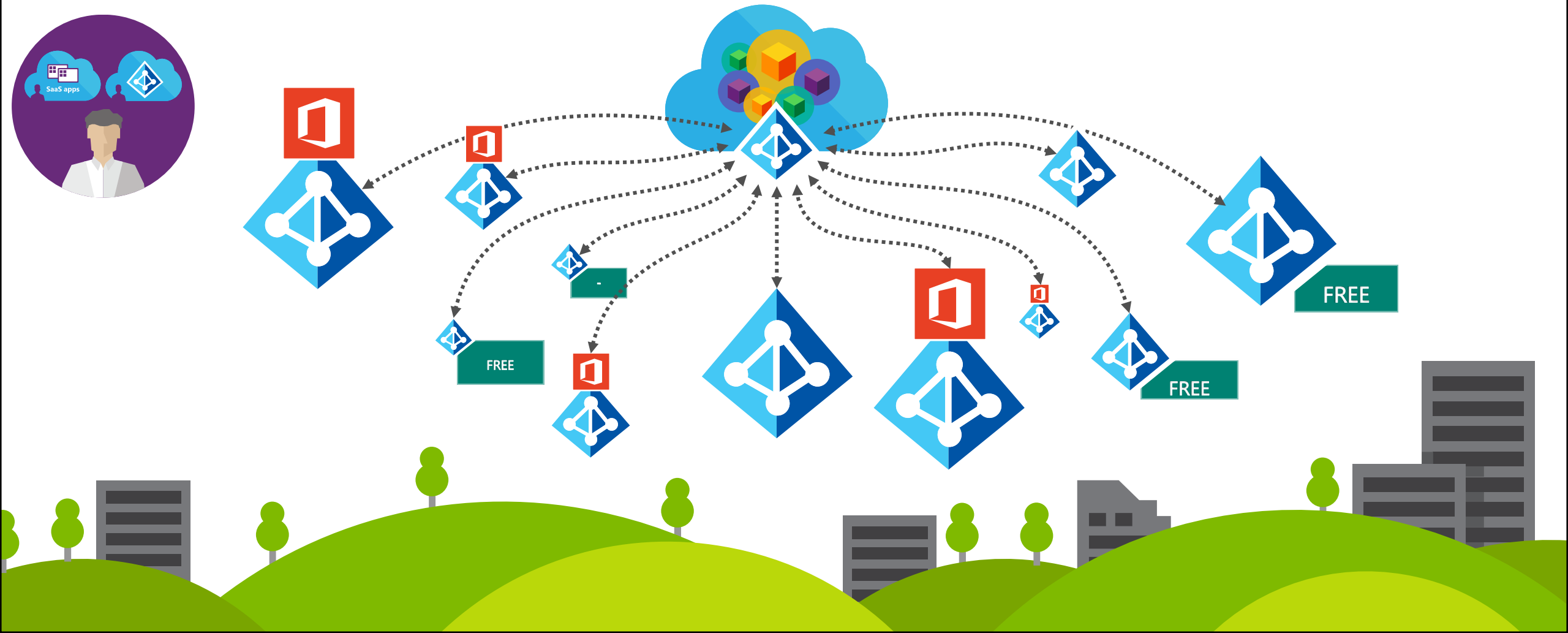
Microsoft

Azure AD B2B & B2C

Microsoft Services

Azure Active Directory B2B

"I need to let my partners access my company's apps by using their own credentials."



Azure Active Directory B2B Concept

Azure AD B2B allows external and authenticated access to key applications and data:

- You do not need a Security Token Service (STS) nor to federate with a partner
- You do not have to create and manage the external accounts in your internal directory
- Partners can use their Azure AD tenant credentials to access your resources and their access is terminated after the user is removed
- If a partner does not already have Azure AD, the B2B collaboration has a streamlined sign-up experience to provide the Azure AD accounts to your business partners
- You can control what partners can access

Provisioned user objects

User object provisioned into inviter's directory

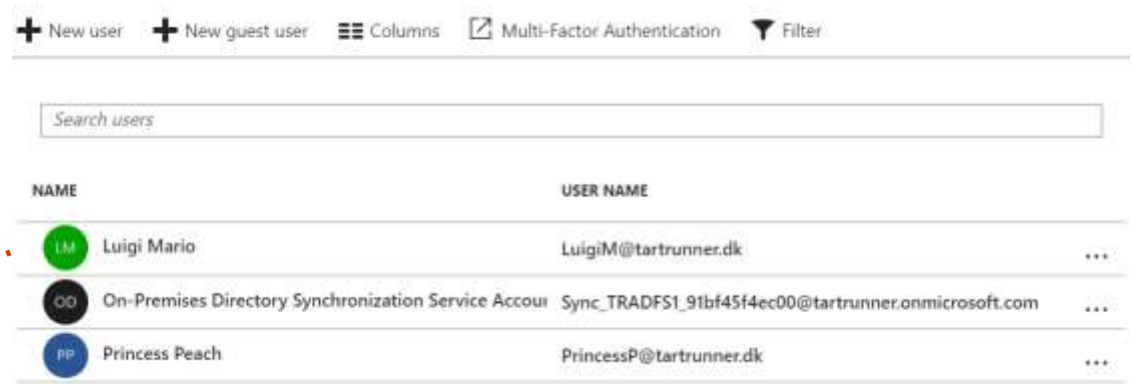
UserType = guest

- Regular user object is provisioned, with UserType attribute set to 'guest'
- Sourced from "Microsoft Azure Active Directory"
- No credentials for user stored in Contoso directory

No direct link between accounts

- If Woodgrove account gets deleted, the guest account in Contoso remains

Soft Linkage



Viral tenant provisioning

When invited partners do not have Azure AD tenants

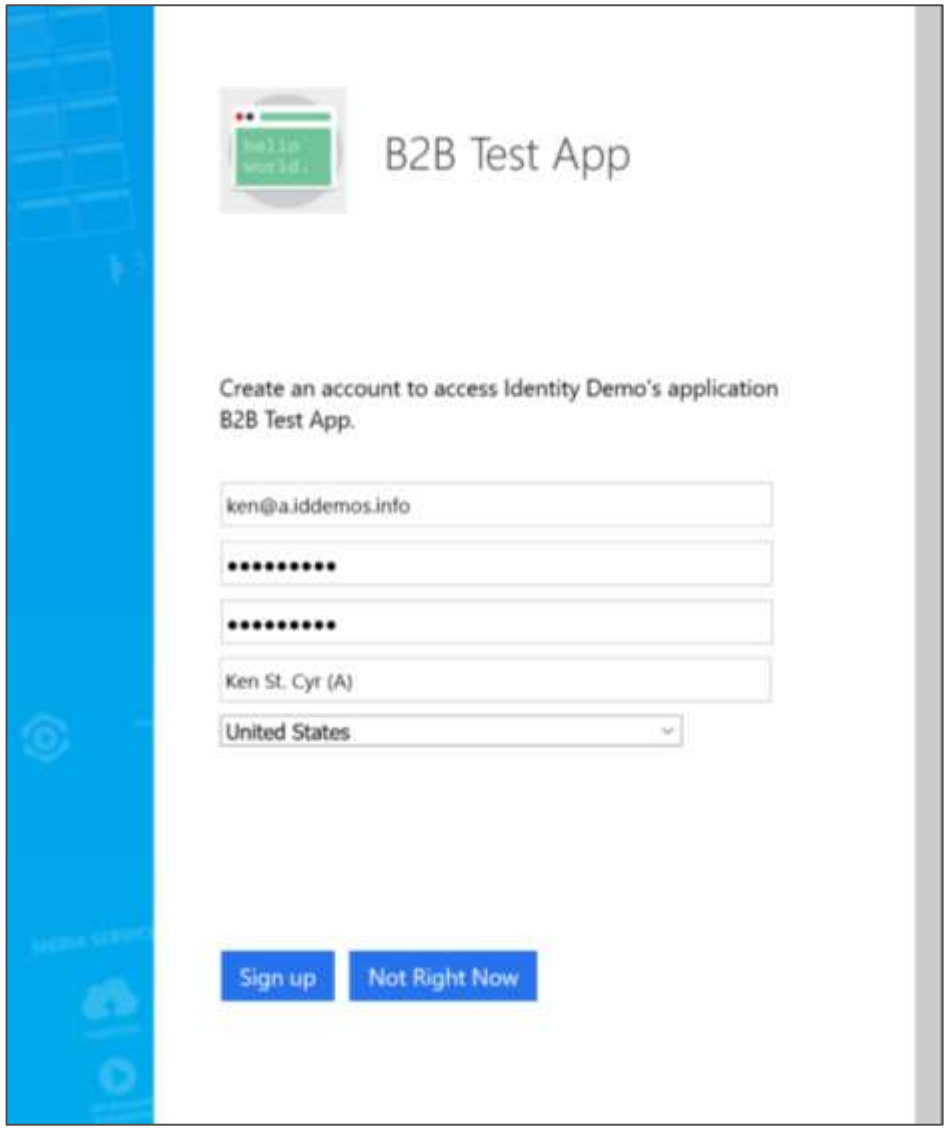
- User is asked to create an account
- Actually creates a “viral” Azure AD tenant without the user knowing

Tenant without a Company Administrator

- Domain has isAdminManaged flag set to **false**
- User has UserType attribute set to **Viral**

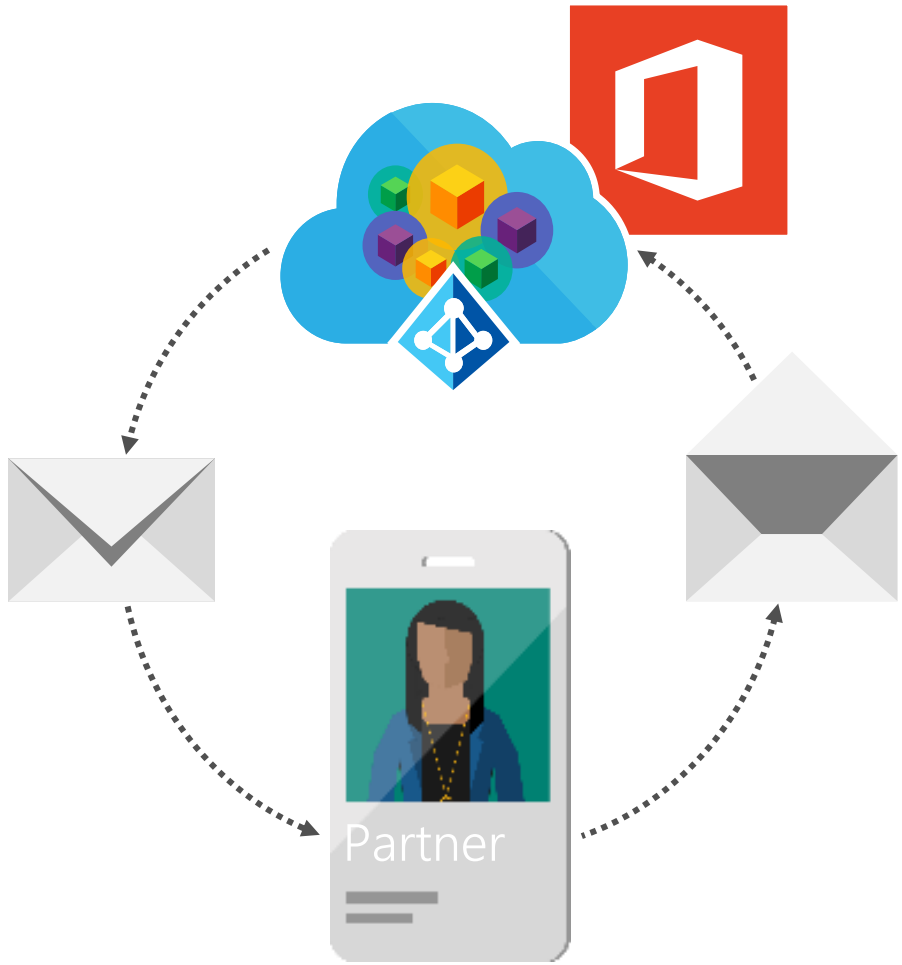
Admin can takeover the tenant

- DNS take over process
- Uses MX or TXT record
- Tenant can be merged into an existing managed tenant



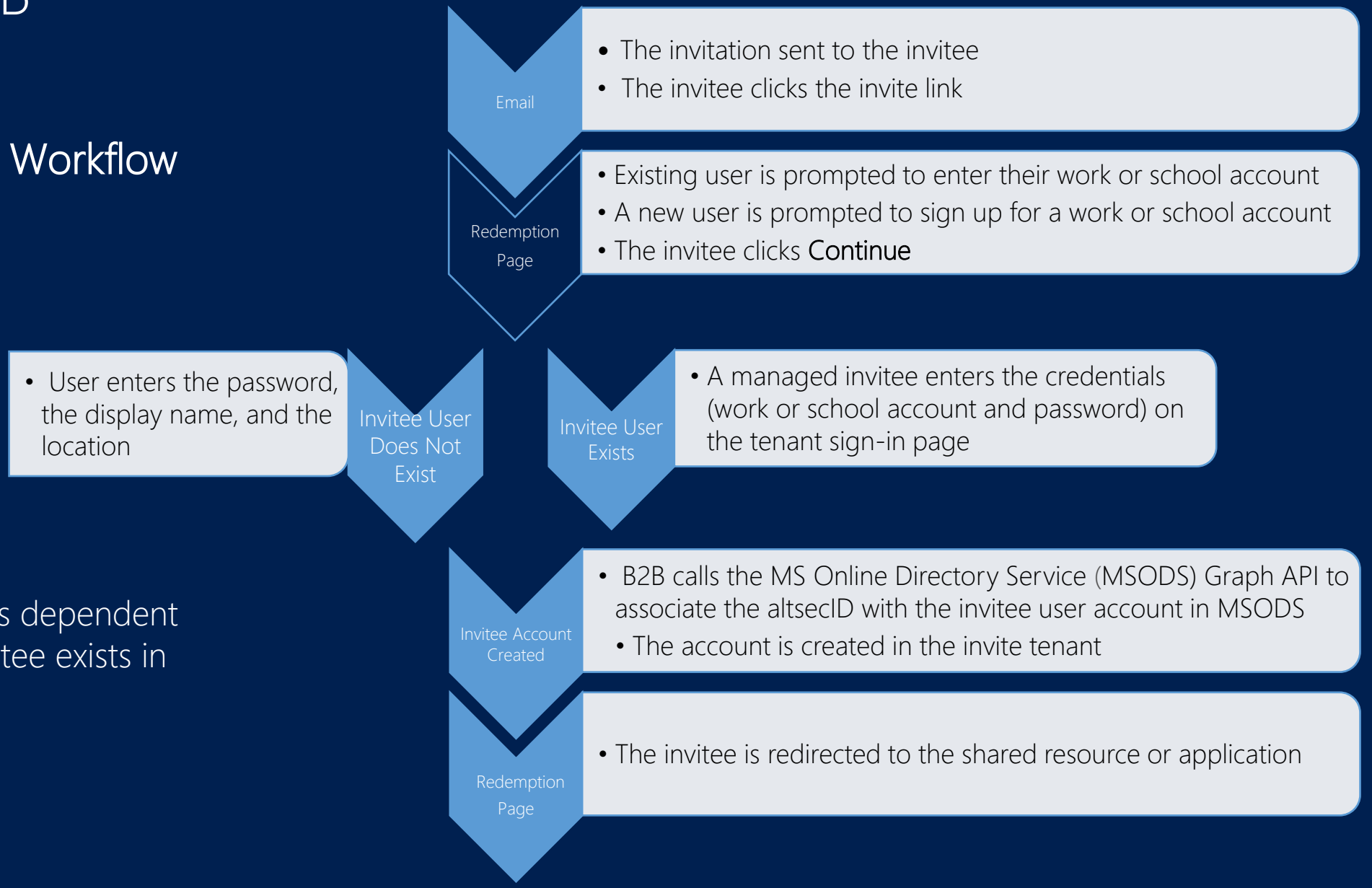
B2B Collaboration – Email Verified Provisioning

- Invitation
  - Uploads a comma separated value (CSV) file containing email addresses of the external users to invite
  - Azure portal creates an external user account in the resource directory, pending acceptance, and sends the branded email invites
- Redeem
  - Partner user receives an email invitation and then clicks the link to accept the invite
  - Partner user signs in to Azure AD to accept the invite
- Authentication
  - Partner user can now authenticate to the resource directory to access the authorized apps



Azure AD B2B

Detailed Redeem Workflow



Redeem workflow is dependent on whether the invitee exists in Azure AD

Provision your B2B users – Build the CSV File

The following sample file will provide B2B access for three users for the SalesForce application:

Email	DisplayName	InviteAppID	InviteReplyUrl	InviteAppResources	InviteGroupResources	InviteContactUsUrl	Language
wharp@contoso.com	Walter Harp	09a8833a-8483-4fc9-8a5b-7f567fa022e8		09a8833a-8483-4fc9-8a5b-7f567fa022e8	bd016fbb-b192-40b5-aef3-11b71ce0176c	http://www.contoso.com	en
jsmith@contoso.com	Jeff Smith	09a8833a-8483-4fc9-8a5b-7f567fa022e8		09a8833a-8483-4fc9-8a5b-7f567fa022e8	bd016fbb-b192-40b5-aef3-11b71ce0176c	http://www.contoso.com	en
bsmith@contoso.com	Ben Smith	09a8833a-8483-4fc9-8a5b-7f567fa022e8		09a8833a-8483-4fc9-8a5b-7f567fa022e8	bd016fbb-b192-40b5-aef3-11b71ce0176c	http://www.contoso.com	en

Use comma as a separator

Required fields:

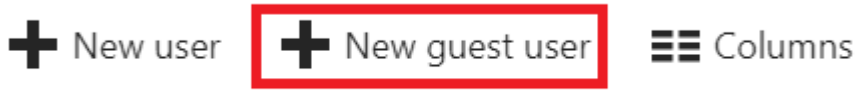
Email: Email address of the invited user
DisplayName: Display name for the invited user (typically, the first and last names)
InviteContactUsUrl: URL to include in email invitations in case the invited user wants to contact your organization

Optional fields:

InviteAppID: The ID for the application to use for branding the email invite and the acceptance pages
InviteAppResources: AppIDs of corporate applications to which you want to assign users
InviteGroupResources: ObjectIDs for the groups to which you want to add users
InviteReplyURL: URL to direct an invited user after invite acceptance. This should be a company-specific URL (such as http://*app.contoso.com*). If this optional field is not specified, the invited user is redirected to the App Access panel from where users can access the corporate apps that you assigned to them
Language: Language for the invitation email and redemption experience, with English as the default when unspecified

Provisioning Your AAD B2B Users

- Use the **New guest user** function on the All users menu



- Bulk users can be added using PowerShell

```
$invitations = import-csv C:\invitations.csv
$messageInfo = New-Object Microsoft.Open.MSGraph.Model.InvitedUserMessageInfo
$messageInfo.customizedMessageBody = "Hey there! Check this out. I created an invitation through PowerShell"
foreach ($email in $invitations) {New-AzureADMSInvitation -InvitedUserEmailAddress $email.InvitedUserEmailAddress -InvitedUserDisplayName $email.Name -InviteRedirectUrl https://wingtiptoysonline-dev-ed.my.salesforce.com -InvitedUserMessageInfo $messageInfo -SendInvitationMessage $true}
```

Azure Active Directory B2C

- Identity management
- Consumer facing applications
- Existing social accounts or local accounts
- Sign-up policies
- Tokens
- Multi Factor Authentication Support
- Customizable user interface

Token flow using Facebook login

Tom

Click “Login with Facebook” at App

Redirect to Facebook Login Page

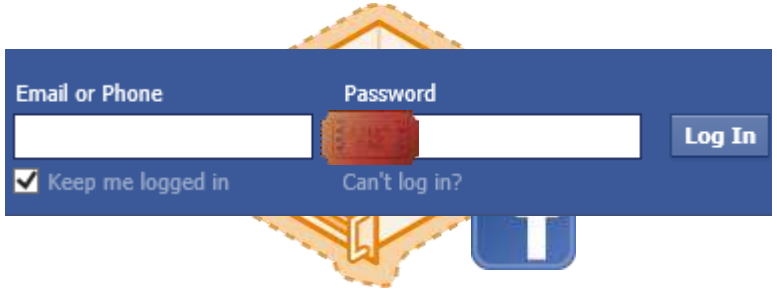
Application

Send Access Token to Graph API and ask for Identity Data

Send Identity Data to App

Graph API

Redirect to App with Access Token



OAuth Server

Identity Store

Azure AD B2C Key Features

Allow users to sign in to your application by using popular social networks such as Facebook or Google, or create accounts with the usernames and passwords specifically for your application

Provides self-service password and profile management and phone-based multi-factor authentication

Sign-up and sign-in experiences are highly customizable

Scalable: can handle hundreds of millions of users

99.9% service level agreement (SLA) in North America*: presence in 17 regions all over the world

Azure AD B2C Key Features

Users only have visibility to their own accounts and profiles

Unique user protection features

Consumers can access all your applications with the same credentials because only one Azure AD B2C tenant is enough for all your consumer online services

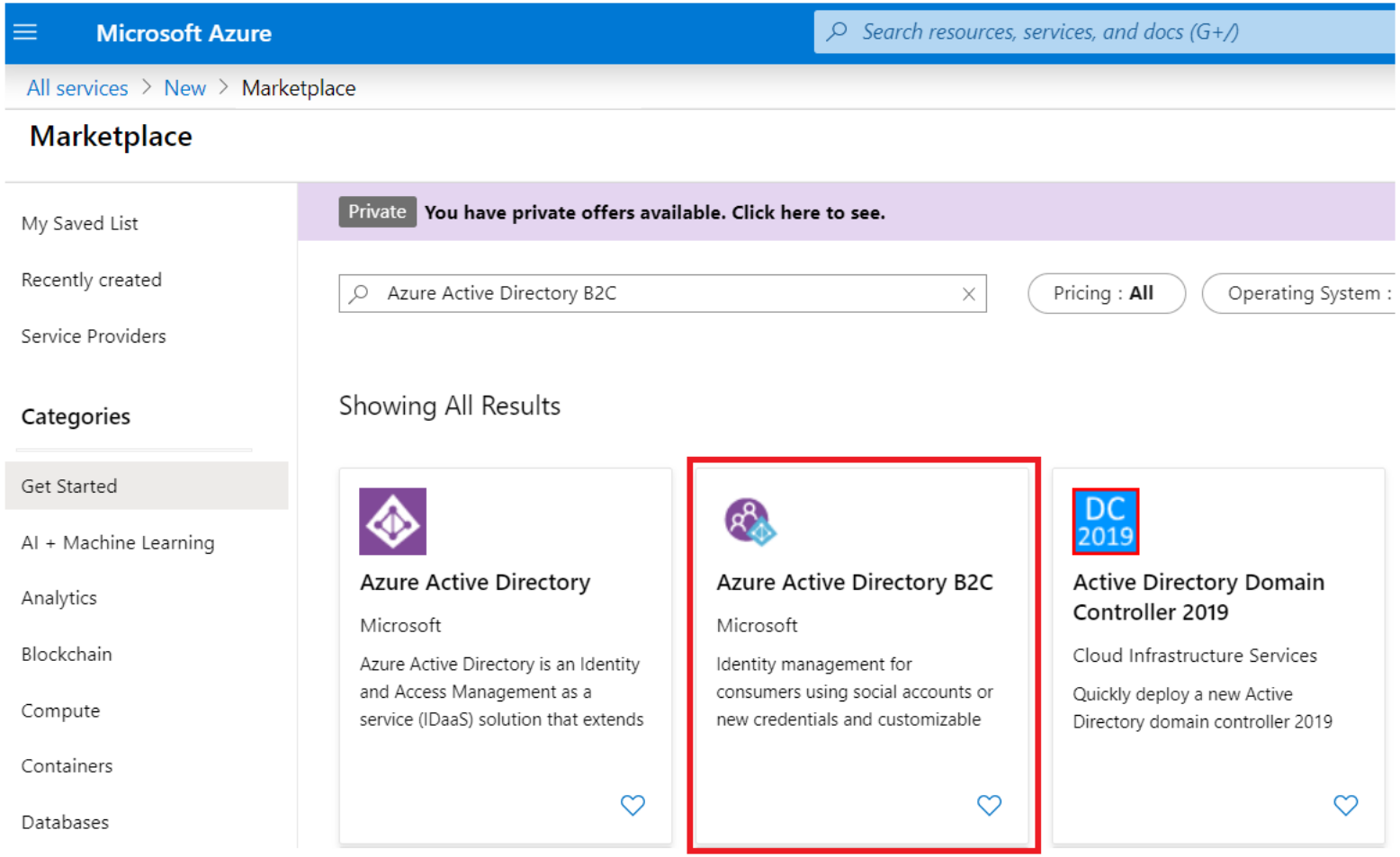
Support for open standards (OAuth and OpenID)

Pay as you go: only pay for the resources that you use

Free tier for up 50,000 users per month and 50,000 authentications per month

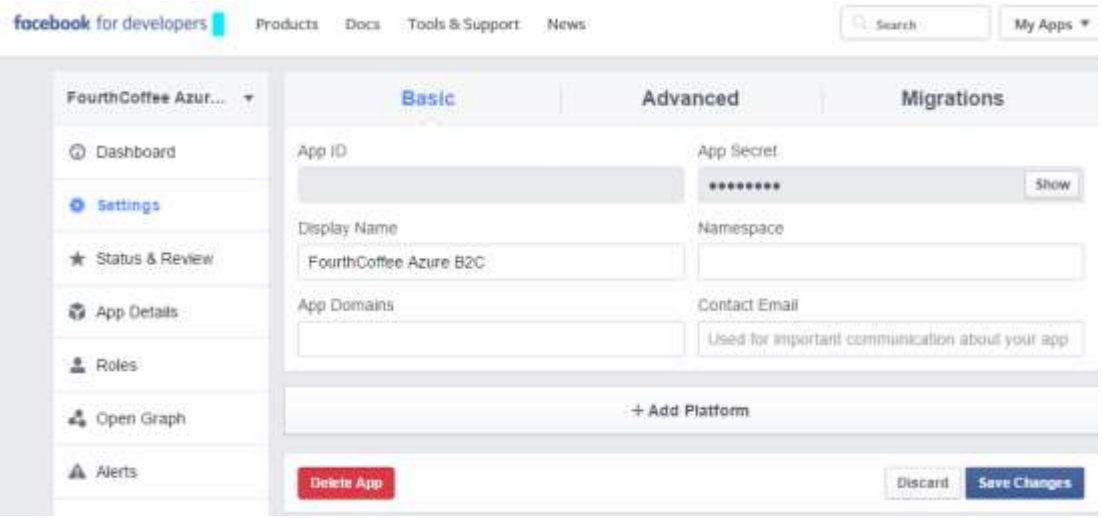
Azure AD B2C – Build the Tenant

- Create and managed in the Azure Portal.



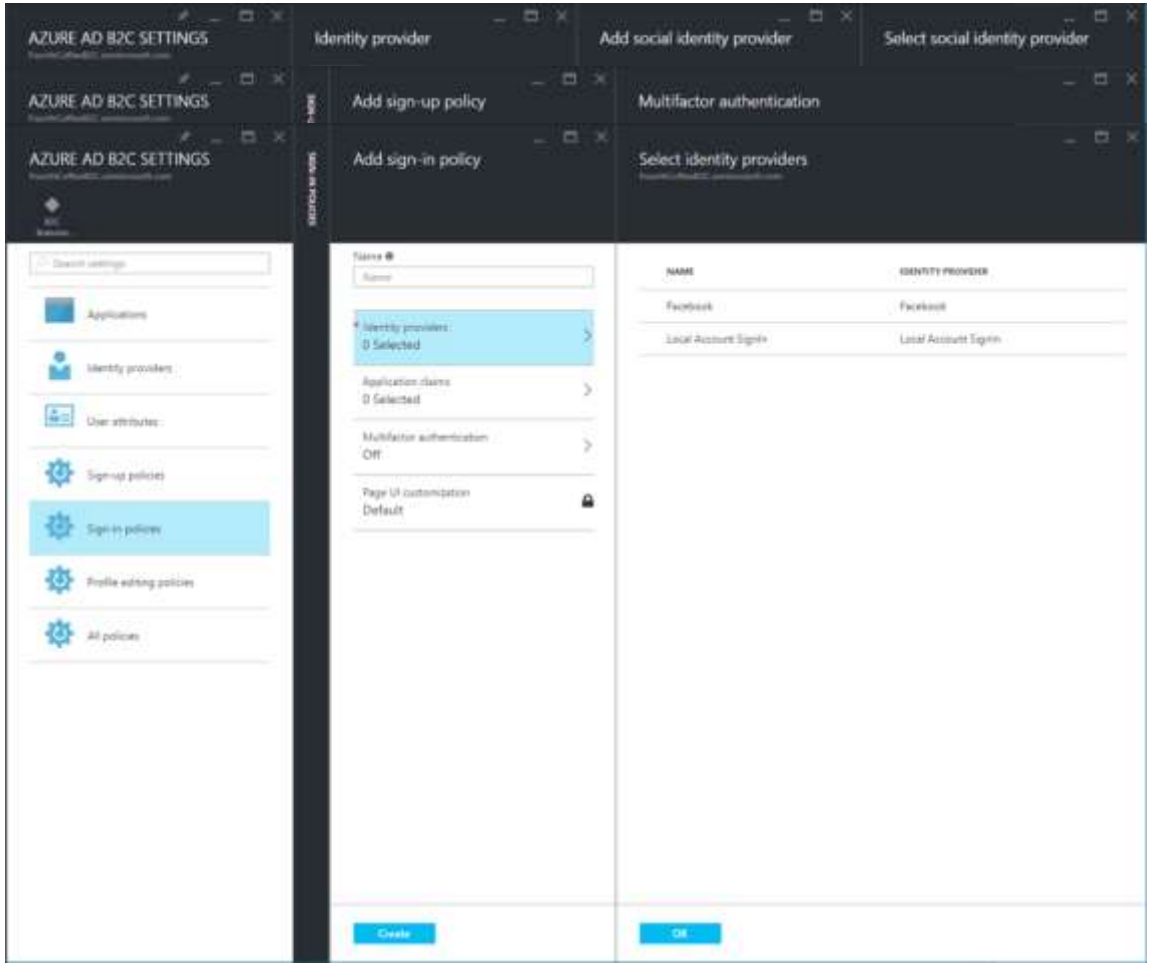
Azure AD B2C – Configure Identity Providers

1. Go to the Provider developers portal
2. Register a new application
3. Provide the application information (Name, description and privacy notice URL)
4. Configure the Redirect URLs field, use OAuth 2.0
5. Copy the values of Client ID and Client secret
6. Configure Identity Provider in the Azure portal



Azure AD B2C – Configure the B2C Directory

1. Select the identity providers
2. Configure the sign-up policy: mandatory attributes during the sign-up
3. Configure the sign-in policy (social accounts or email-named local accounts)



Microsoft

Azure Multi-Factor Authentication

Microsoft Services

What is Multi-Factor Authentication (MFA)

Any two or more of the following factors:

Something you know - a password or PIN

Something you have - a phone, credit card, or hardware token

Something you are - a fingerprint, retinal scan, or other biometric

Stronger when using two different channels (out-of-band)

Types of Multi-Factor Authentication

Hardware OTP tokens

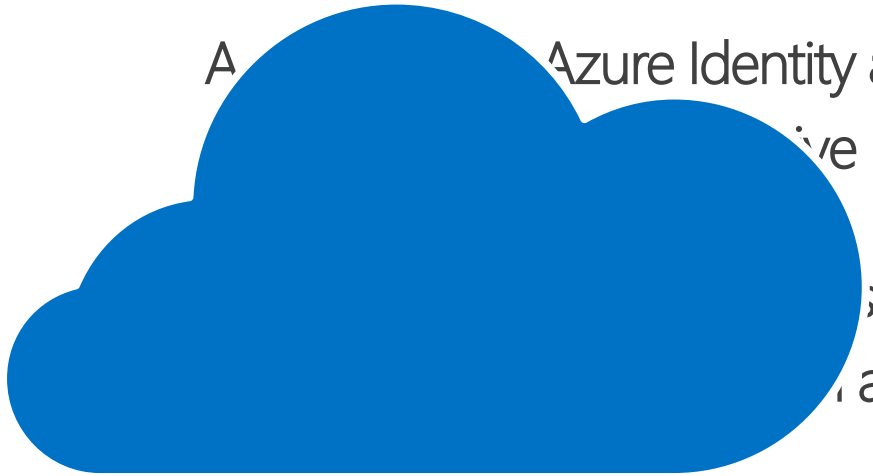
Certificates

Smart cards

Phone-based authentication:

- Phone call, text message, and PushSoftware OTP tokens

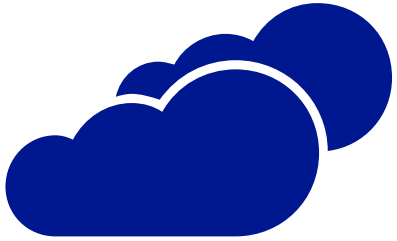
What is Multi-Factor Authentication (MFA)



A Azure Identity and Access management service
ve Directory Premium

; to both on-premises and cloud
additional level of authentication

Trusted by thousands of enterprises to authenticate employee, customer, and partner access



How Azure MFA Works

Mobile Apps

Push Notification

One-Time Passcode (OTP) Token

Phone Calls

Phone Call

Text Messages

Text Message

Choose the MFA Security Solution

Several flavors of Azure MFA	Full version of Azure MFA included with:	Subset of Cloud MFA included for:
• What am I trying to secure? • Where are the users located? • Which feature is required?	• Azure Active Directory Premium • Azure MFA stand alone	• Azure – Azure Administrators • O365 – Licensed Users

Choose the MFA Security Solution

What are you trying to secure	Multi-Factor Authentication in the cloud	Multi-Factor Authentication Server
First party Microsoft apps	*	*
SaaS apps in the app gallery	*	*
IIS applications published through Azure AD App Proxy	*	*
IIS applications not published through Azure AD App Proxy		*
Remote access such as VPN, RDG		*

Choose the MFA Security Solution

User Location	Solution
Azure Active Directory	Multi-Factor Authentication in the cloud
Azure AD and on-premises AD using federation with AD FS	Both MFA in the cloud and MFA Server are available options
Azure AD and on-premises AD using DirSync, Azure AD Sync, Azure AD Connect - no password sync	Both MFA in the cloud and MFA Server are available options
Azure AD and on-premises AD using DirSync, Azure AD Sync, Azure AD Connect - with password sync	Multi-Factor Authentication in the cloud
On-premises Active Directory	Multi-Factor Authentication Server

Azure MFA vs MFA for O365/Azure Admins

	MFA for Office 365/Azure Administrators	Azure Multi-Factor Authentication
Administrators can enable/enforce MFA to users	✓	✓
Use mobile app (online and OTP) as second authentication factor	✓	✓
Use phone call as second authentication factor	✓	✓
Use SMS as second authentication factor	✓	✓
Application passwords for non-browser clients (for example, Outlook, Skype for Business)	✓	✓
Default Microsoft greetings during authentication phone calls	✓	✓
Custom greetings during authentication phone calls		✓
Fraud alert		✓
MFA SDK		✓
Security reports		✓
MFA for on-premises applications/ MFA Server		✓
One-Time Bypass		✓
Block/Unblock Users		✓
Customizable caller ID for authentication phone calls		✓
Event Confirmation		✓

Microsoft

Azure AD Application Proxy

Microsoft Services

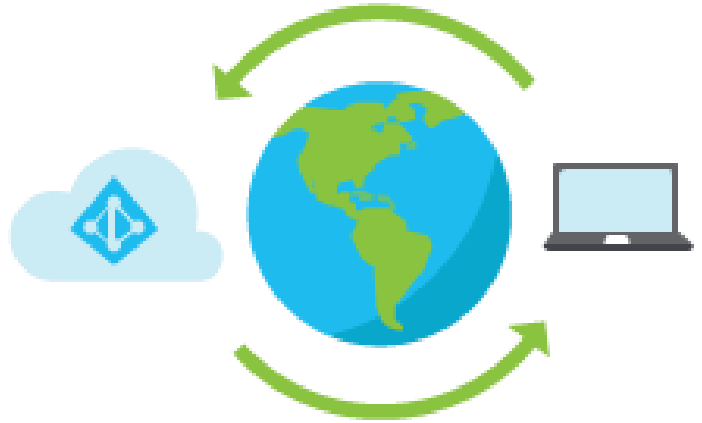
What is Azure AD Application Proxy?

Provide SSO and secure remote access for on-premises or Azure IaaS web applications

Reverse Proxy using an Azure endpoint

No inbound Firewall rules required

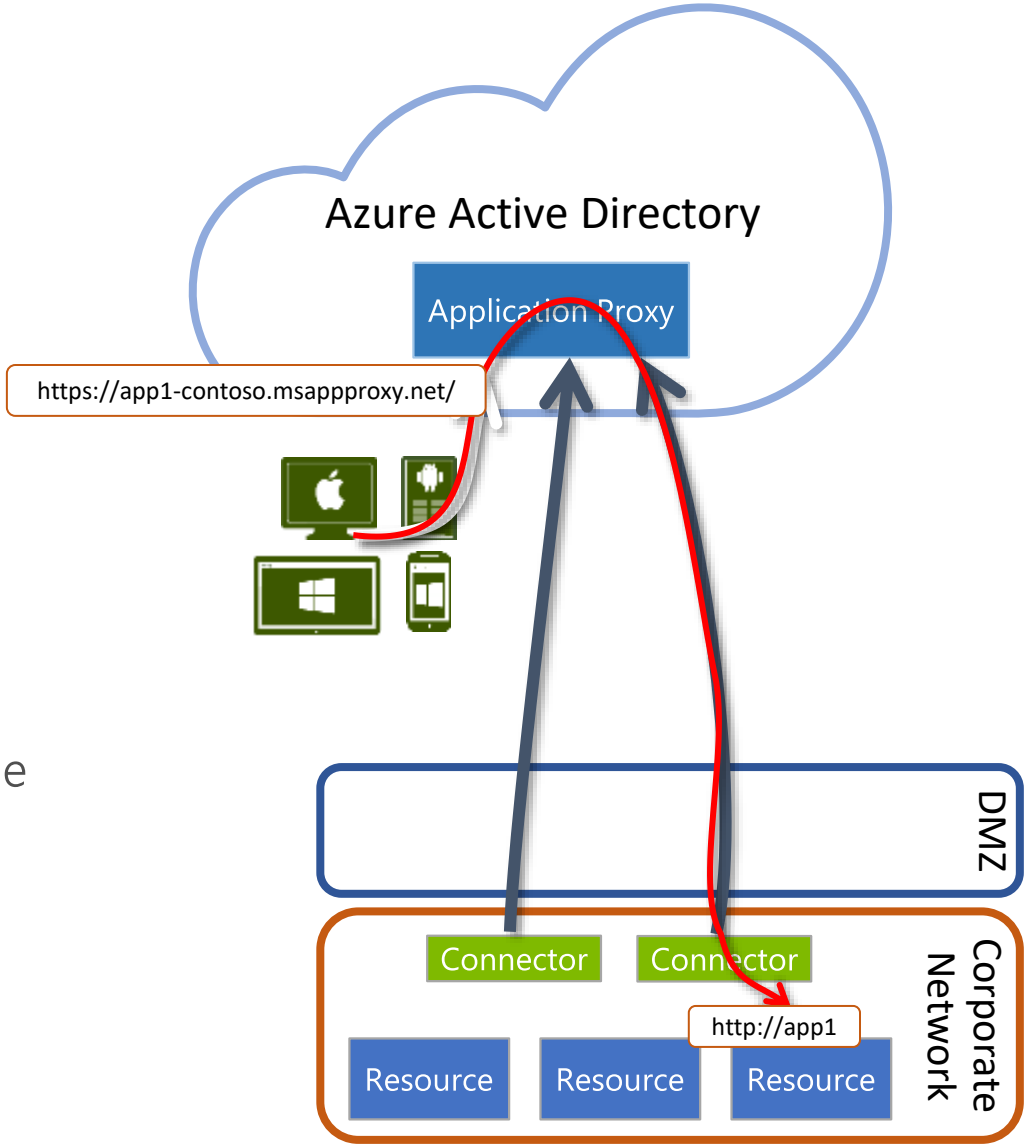
Provide AAD authentication for Kerberos, Claims or Forms based applications



Azure AD Application Proxy

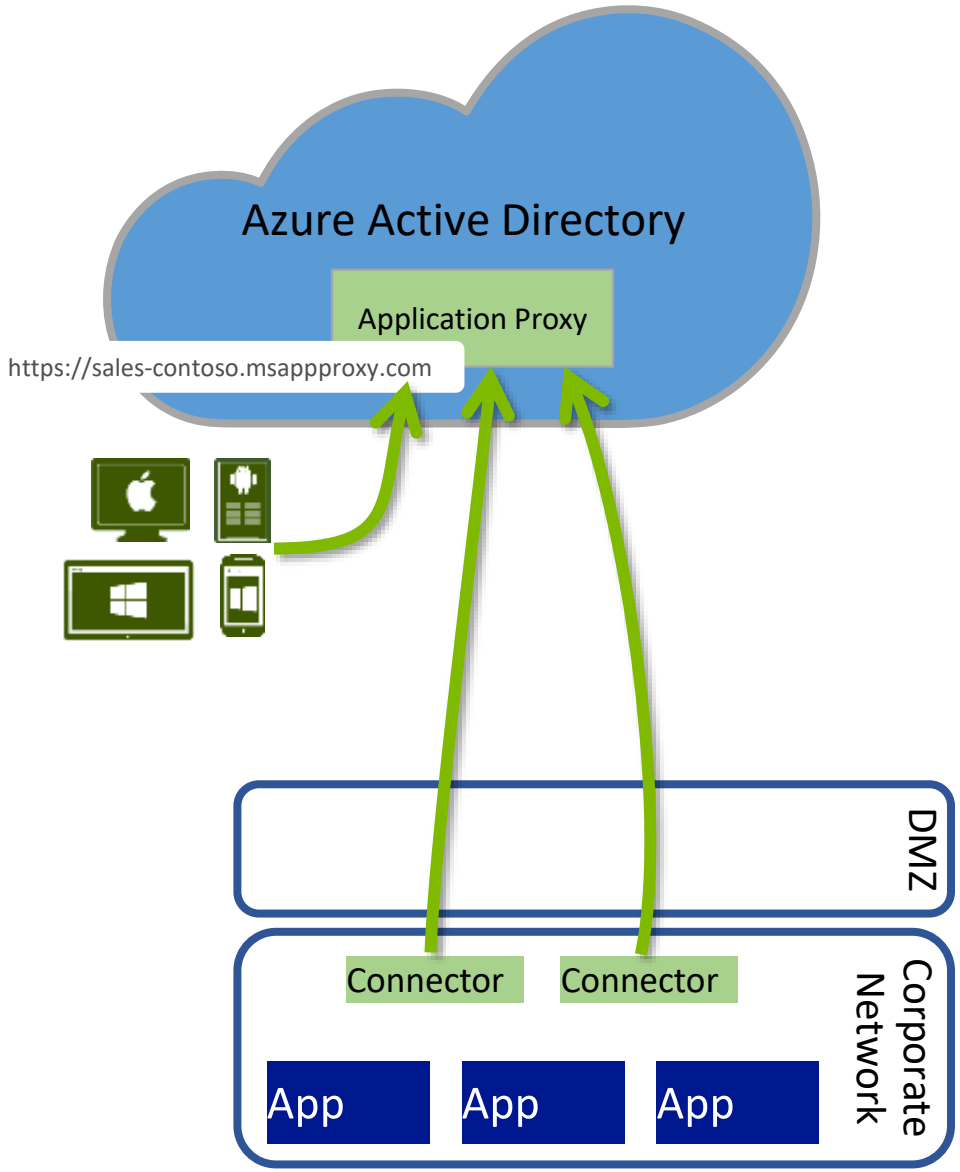
How it works:

- Connectors are deployed usually on corpnet next to resources
- Multiple connectors can be deployed for redundancy, scale, multiple sites and different resources
- The connector auto connects to the cloud service
- User connects to the cloud service that routes their traffic to the resources via the connectors



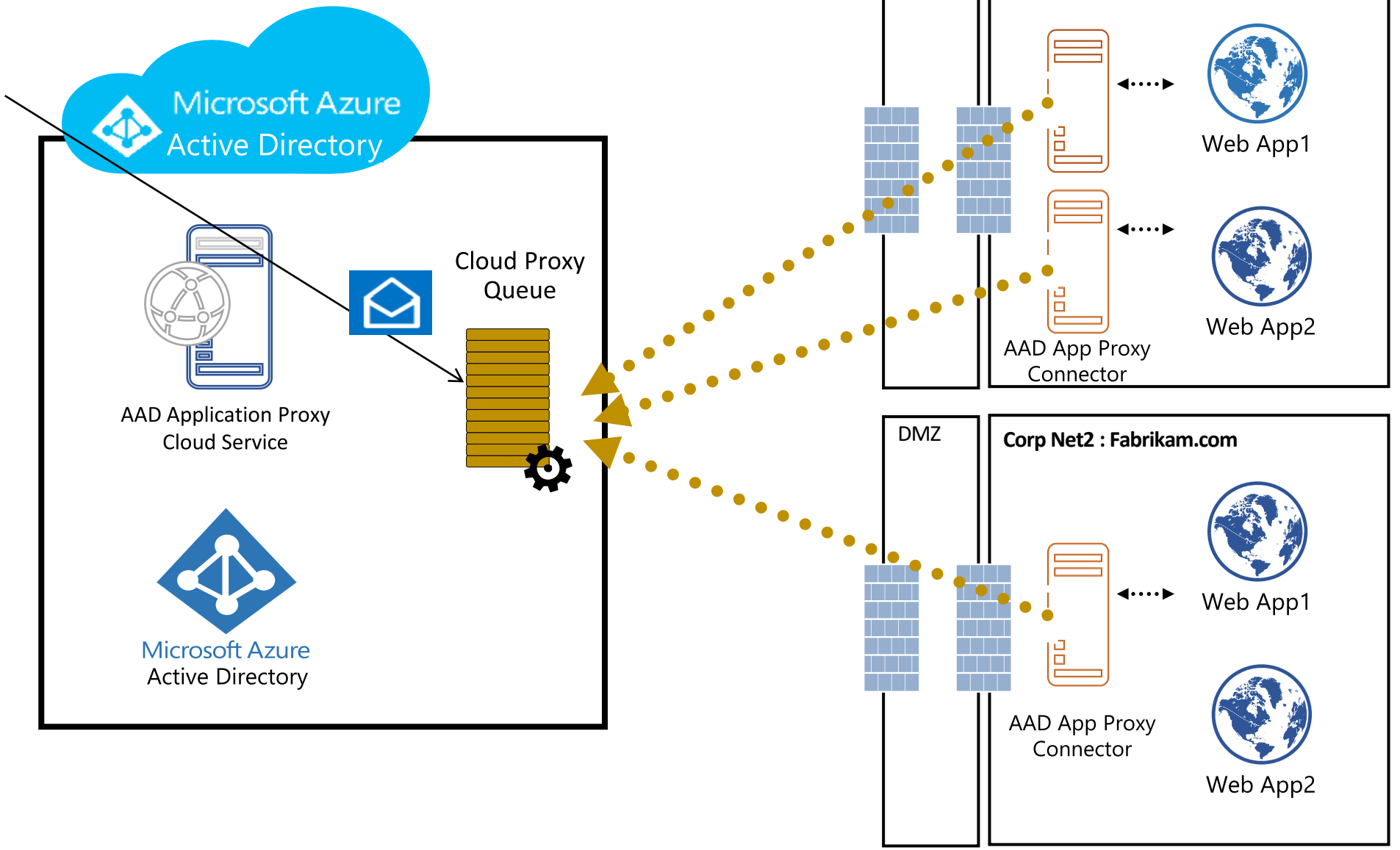
Cloud Scale Security

- All HTTP/S traffic is terminated in the cloud blocking most HTTP level attacks.
- Unauthenticated traffic filtered in the cloud – will not arrive on-prem.
- No incoming connections to the corporate network – only outgoing connection to the Azure AD Application Proxy service
- Internet facing service always up to date with latest security patches and server upgrades
- Login abnormalities detection, reporting and auditing by Azure AD

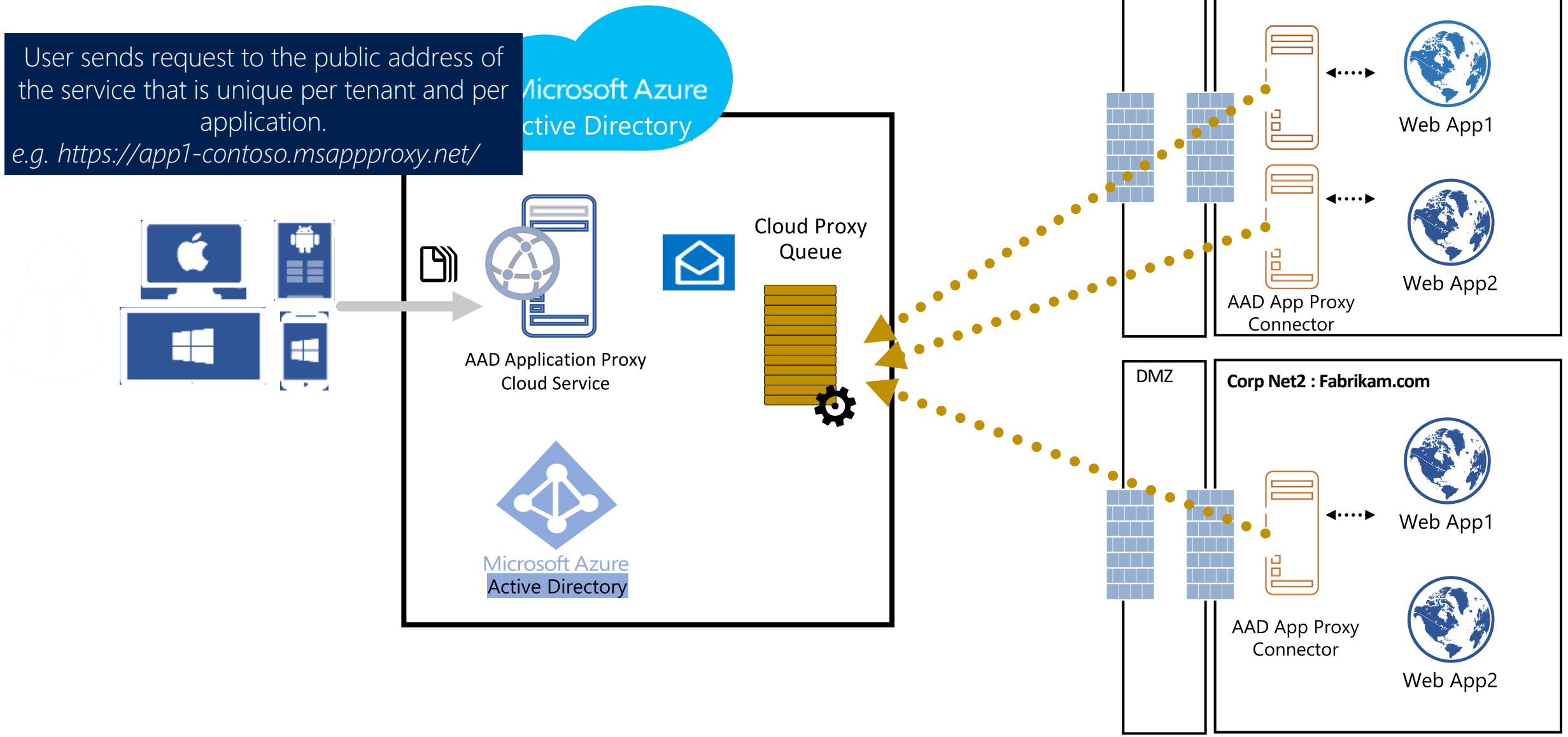


Azure AD Application Proxy Data flow

Once Started, the connector polls the Azure AD Application Proxy service for new client request. The requests remain waiting until user requests arrives or timeout

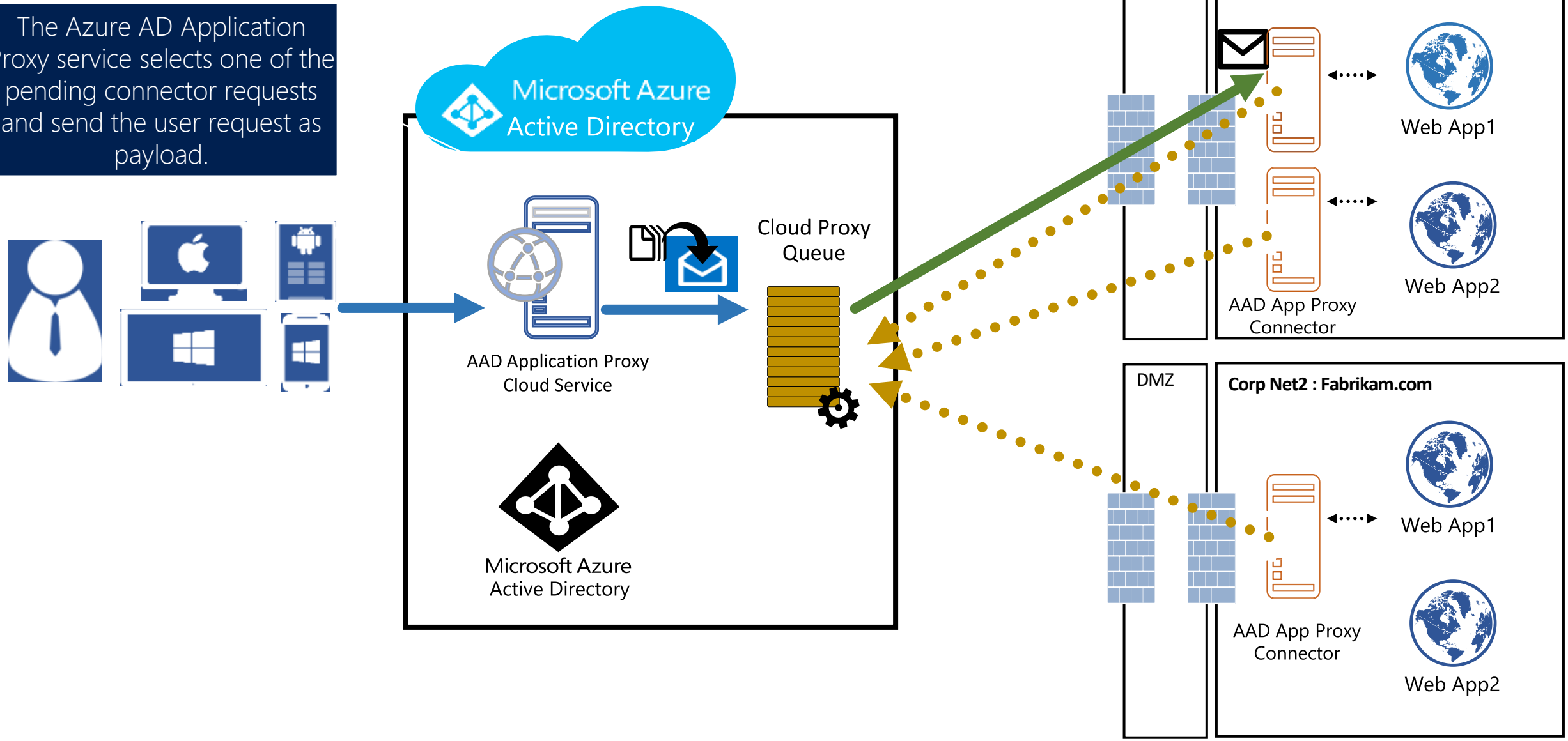


Azure AD Application Proxy Data flow

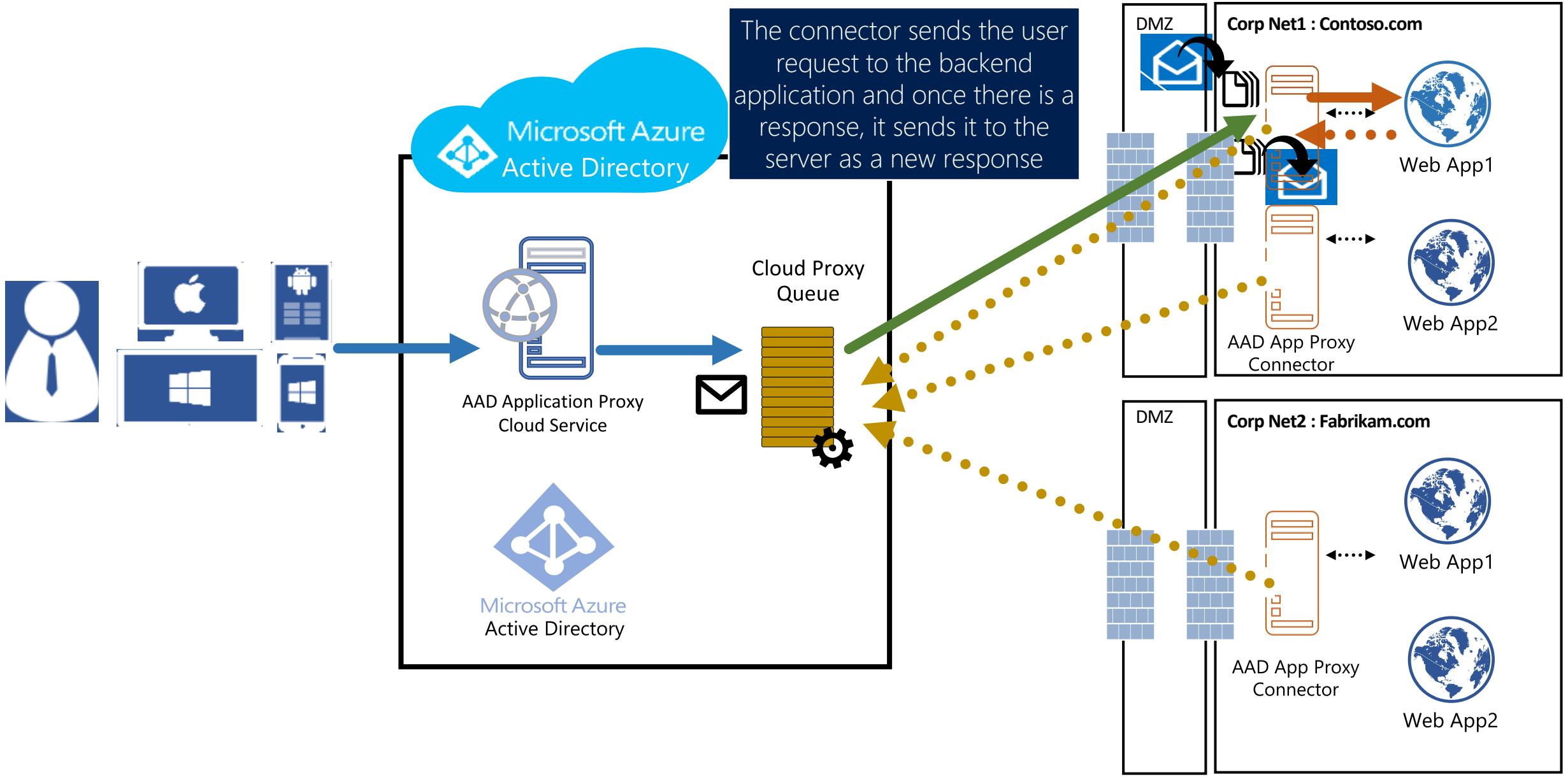


Azure AD Application Proxy Data flow

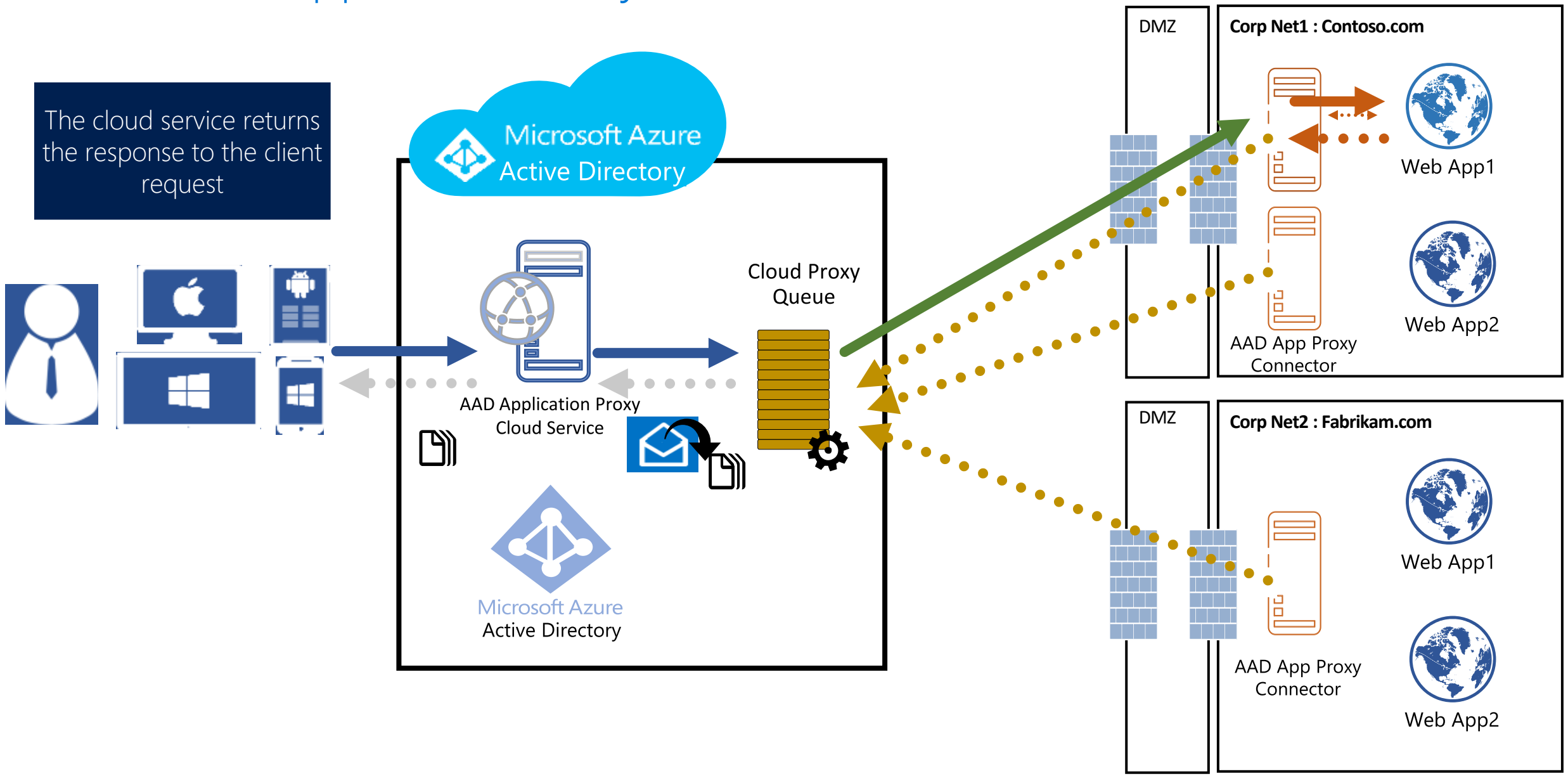
The Azure AD Application Proxy service selects one of the pending connector requests and send the user request as payload.



Azure AD Application Proxy Data flow

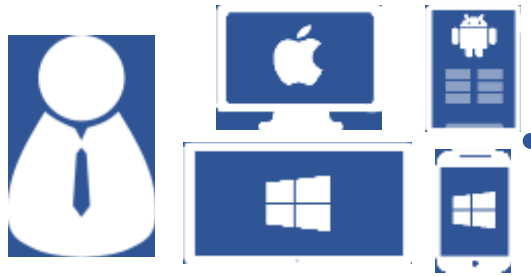


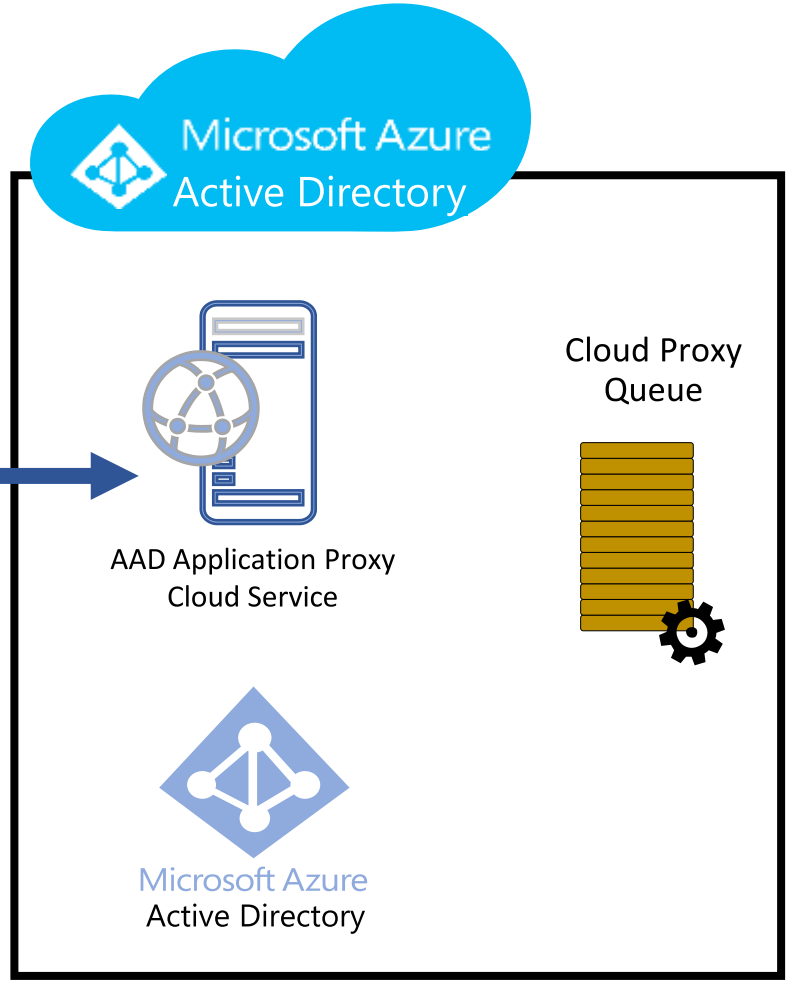
Azure AD Application Proxy Data flow

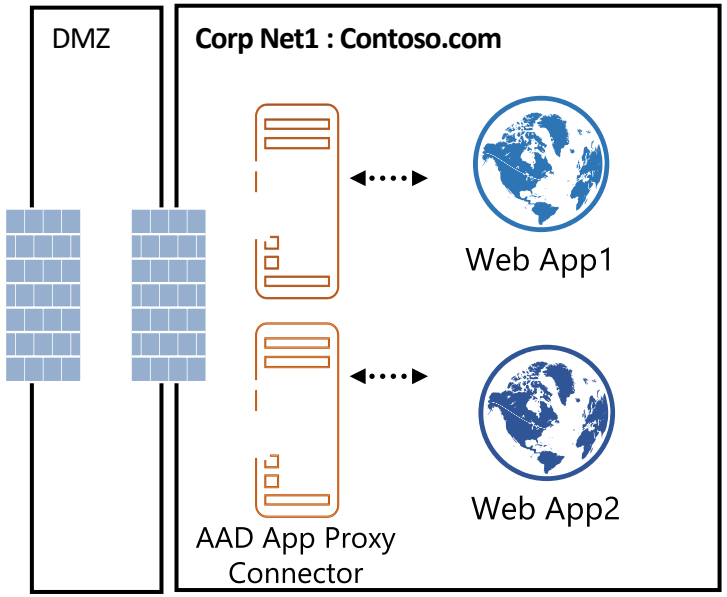


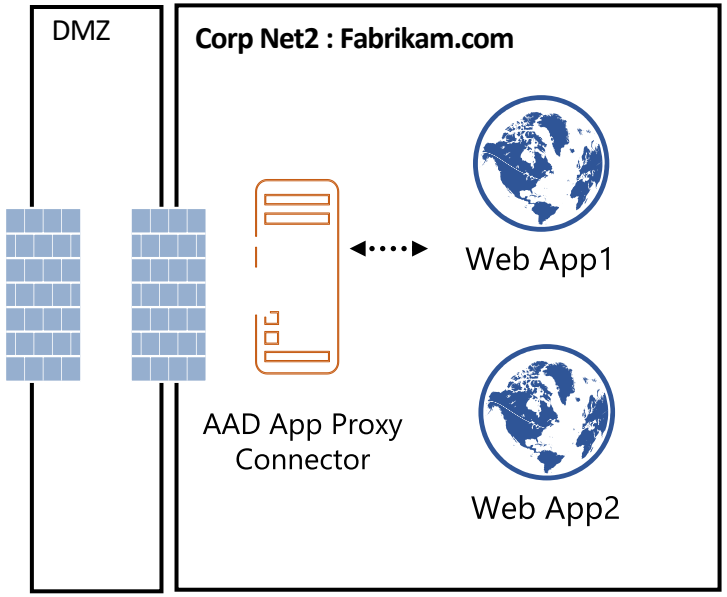
AAD Pre Authentication Scenario

User sends a new unauthenticated request to application that is configured to require pre authentication



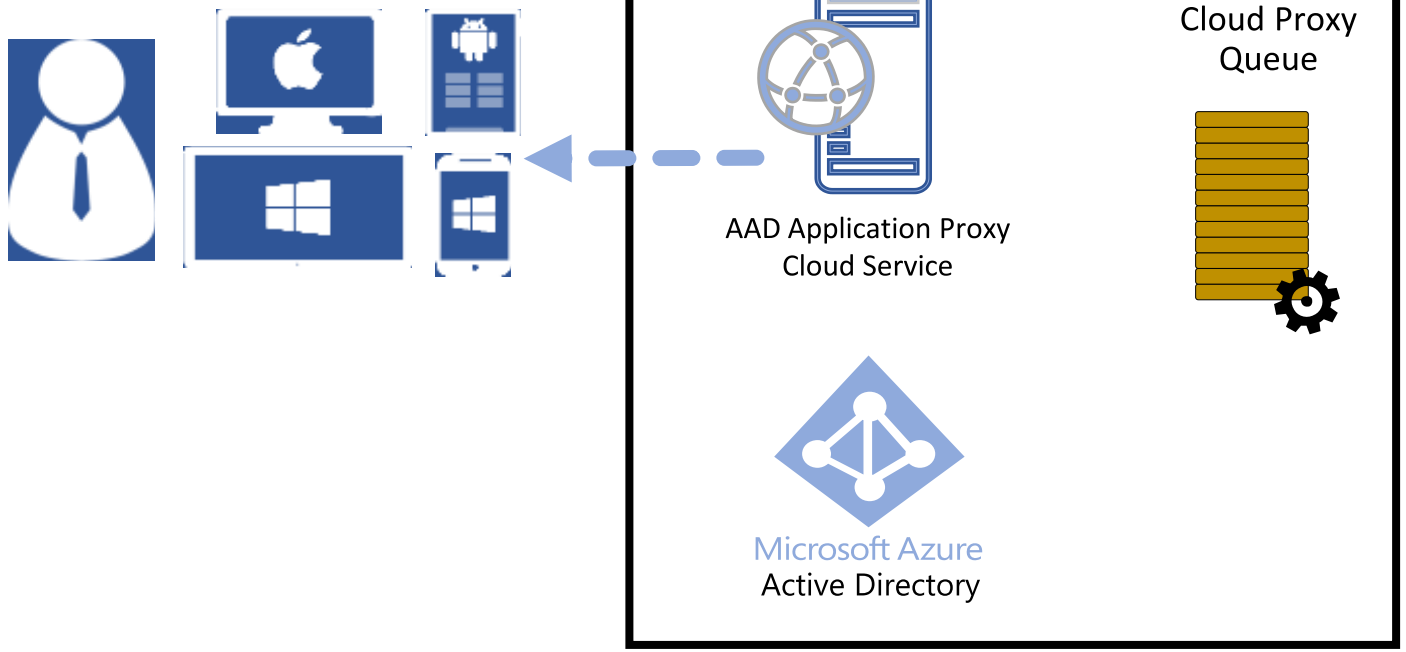


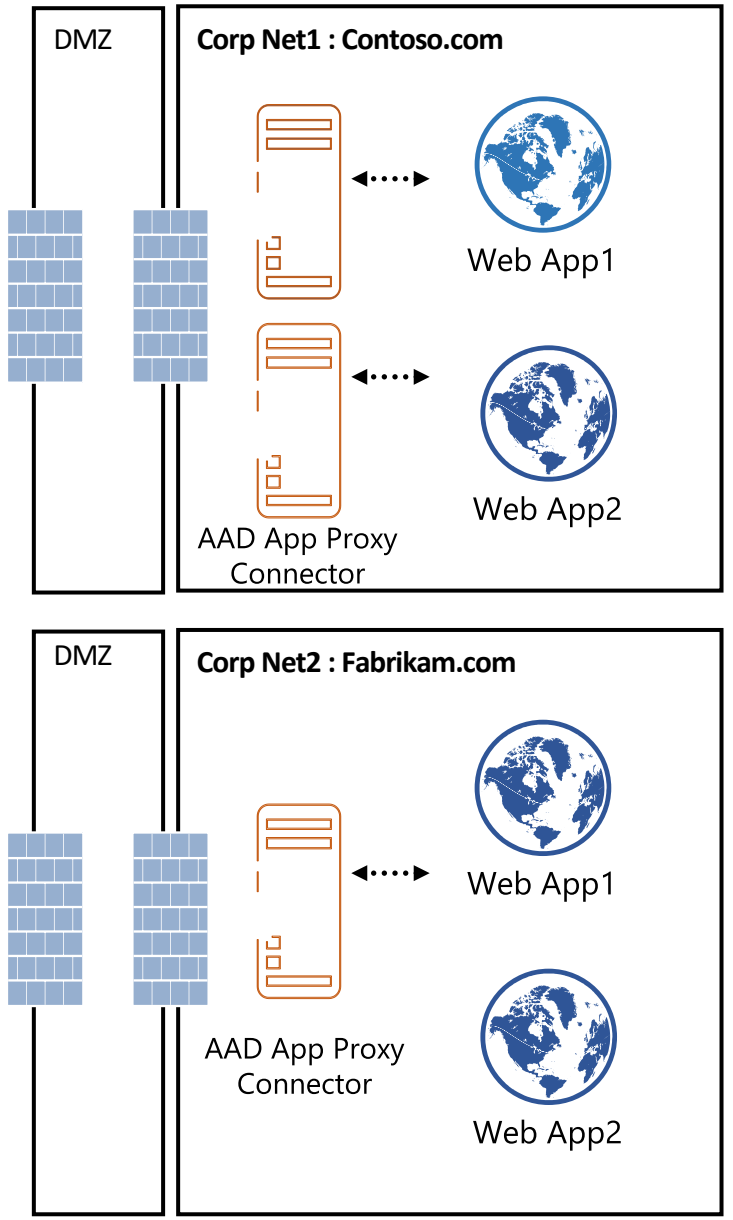




AAD Pre Authentication Scenario

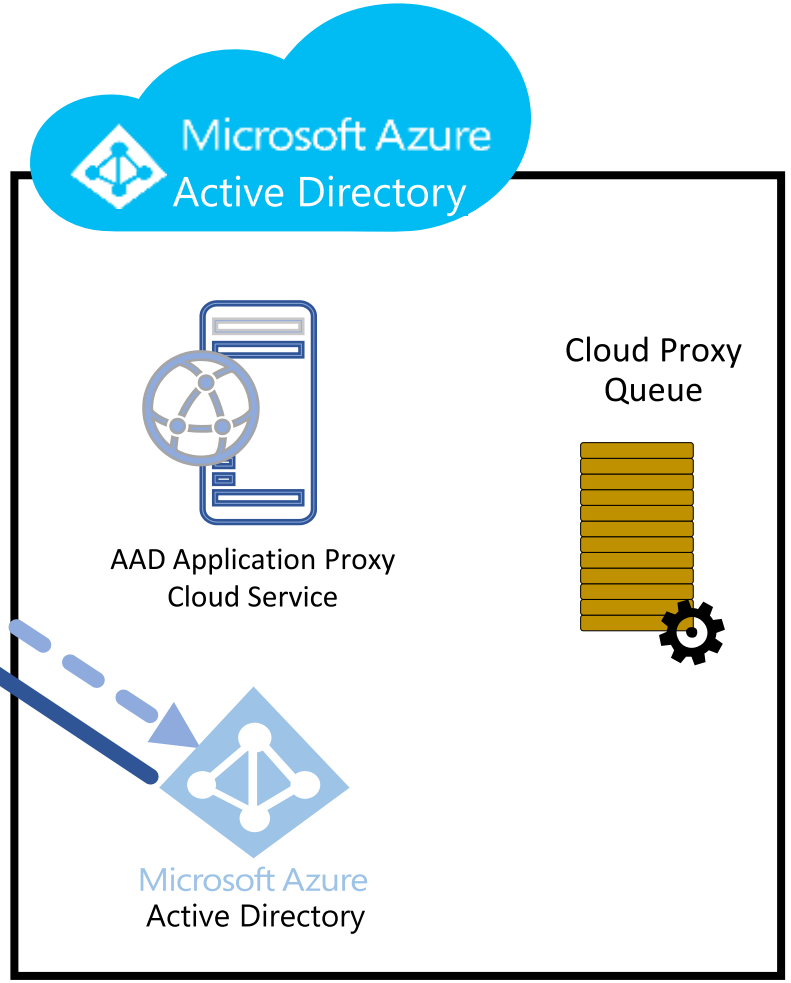
The proxy redirects the user to the Azure AD STS address with information on the application that needs pre authentication. Nothing is sent to the backend

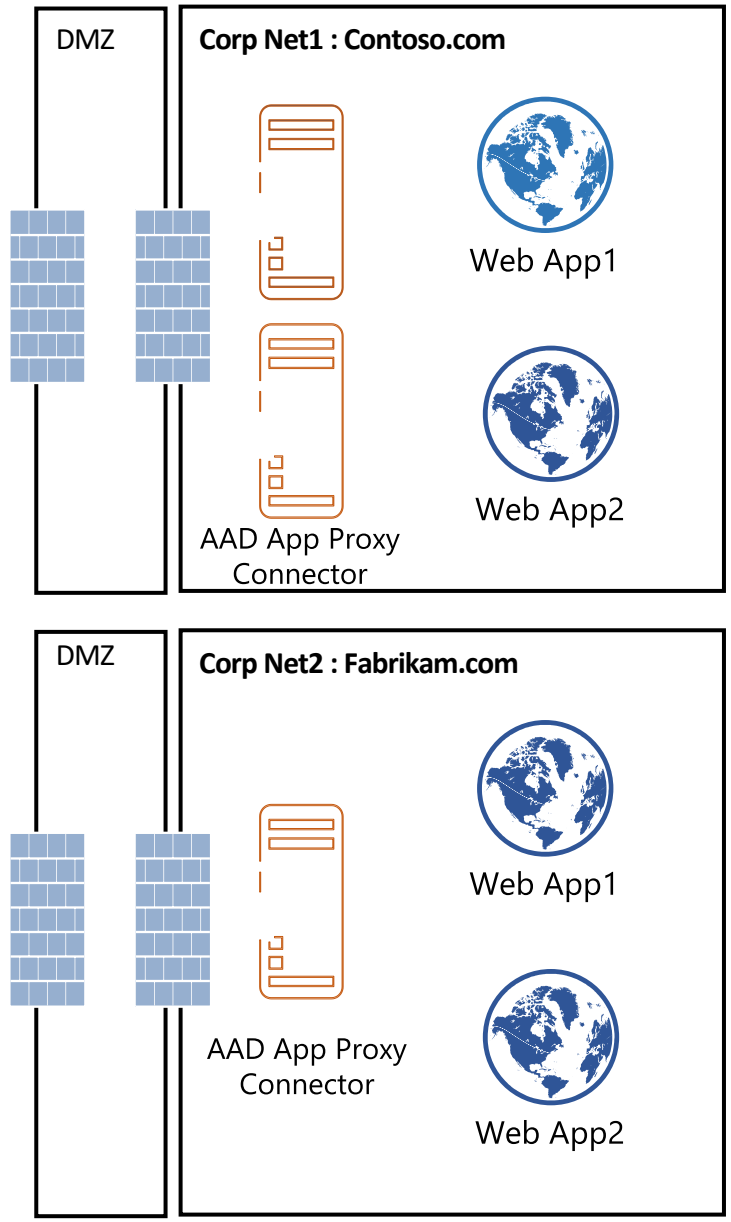




AAD Pre Authentication Scenario

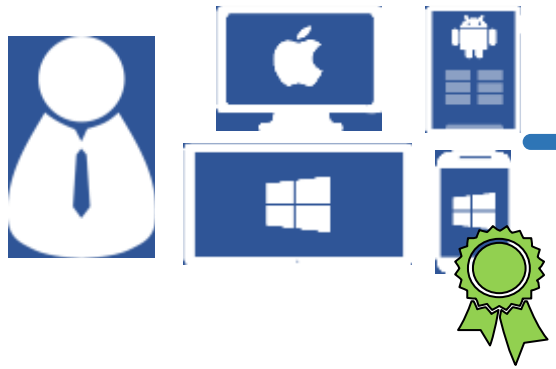
User is authenticating to Azure AD STS. This process may involve other systems depending on tenant configuration. E.g. 2FA Once authenticated, the user is redirected back to the AD Application Proxy service with the acquired token

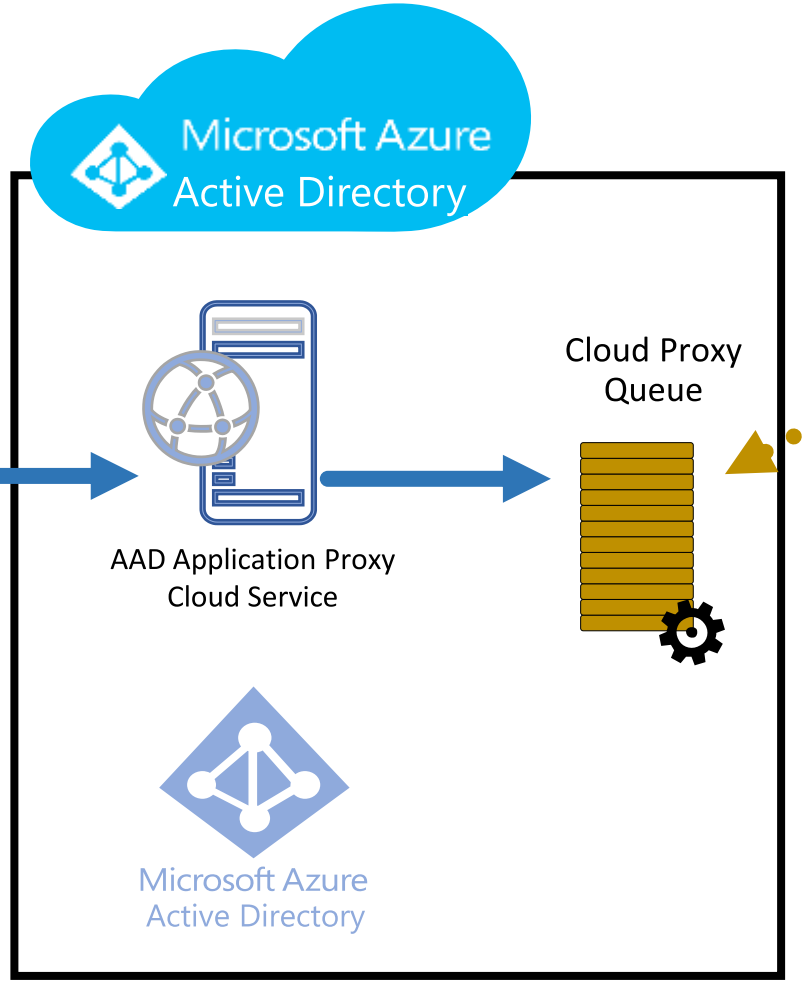


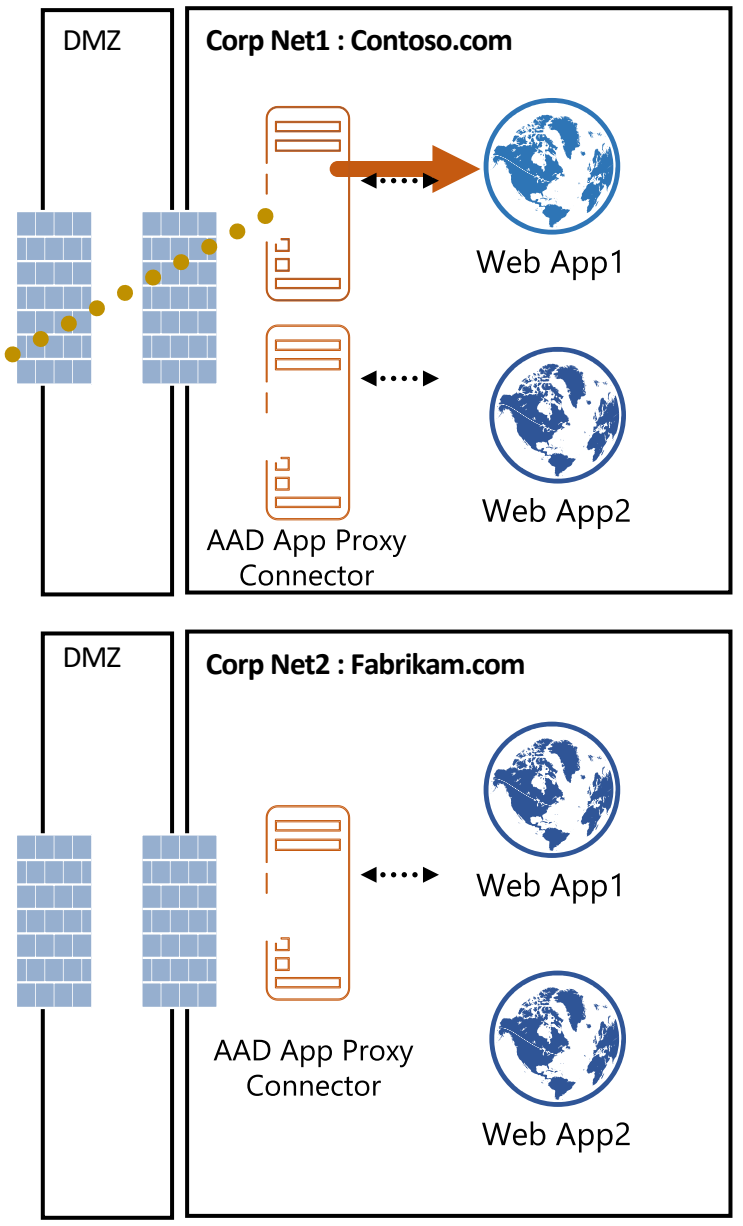


AAD Pre Authentication Scenario

The user request arrives again but now with a valid authentication token. Once the token is validated, the request is sent to the backend application







Other Features

User Your Own Domain:

- Publish applications using one of your own verified domains. Upload a PFX certificate.
- DNS – Create a CNAME record for your custom name to *app-yourtennantname*.msappproxy.com

Connector Groups:

- Group connectors for location (e.g. Azure East US, On premises Data center etc)
- Adds redundancy
- Assign applications to a specific Connector Group

Other Features

SSO for on-premises IWA apps using KCD:

- Configure on-premises application for Kerberos (register SPNs).
- Configure Connector servers for Kerberos Constrained Delegation with Protocol Transition.
- Proxy validates the token (from Azure AD) and retrieves the User Principal Name (UPN) from it, and then sends the request, the UPN, and the Service Principal Name (SPN) to the Connector through a dually authenticated secure channel.
- The Connector performs Kerberos Constrained Delegation (KCD) negotiation with the on-premises AD, impersonating the user to get a Kerberos token to the application.

Microsoft

Azure AD Conditional Access

Microsoft Services

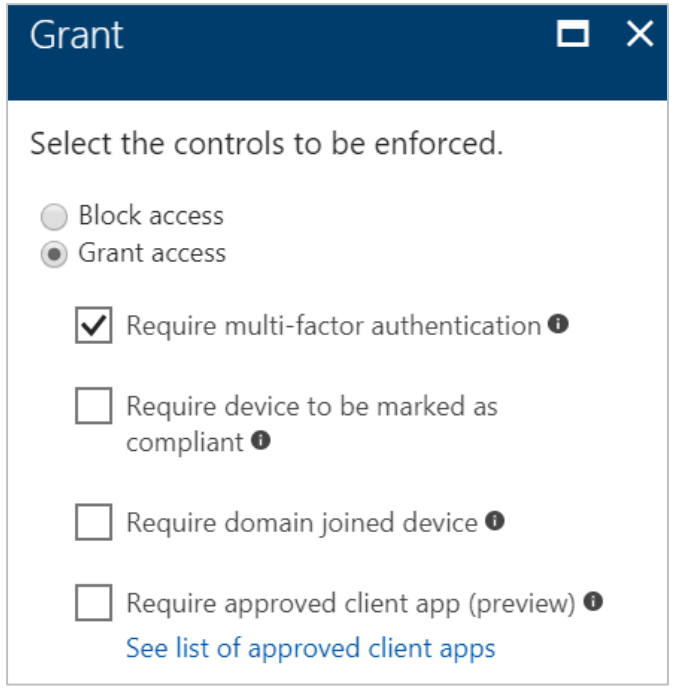
What is Azure AD Conditional Access?

- Conditional access is a feature of Azure Active Directory that allows you to enforce controls on access to apps in your environment based on specific conditions.
- With controls, you can either tie additional requirements to the access or you can block it.
- Conditional access is based on policies.
- Typically, you define your access requirements using statements that are based on the following pattern:

- E.g. when contractors are trying to access our cloud apps from networks that are not trusted, then block access.

Controls

- In a conditional access policy, controls define what should happen when a condition statement has been satisfied.
- The current implementation of Azure Active Directory enables you to configure the following grant control requirements:
  - **Multifactor Authentication** - you can use Azure Multi-Factor or an on-premises multi-factor authentication provider, combined with Active Directory Federation Services (AD FS).
  - **Compliant device** - you can set up a policy to allow only computers that are compliant, or mobile devices that are enrolled in a mobile device management application, to access your organization's resources.
  - **Domain joined device** - you can require the device to be a domain joined device, this policy applies to Windows desktops, laptops, and enterprise tablets.



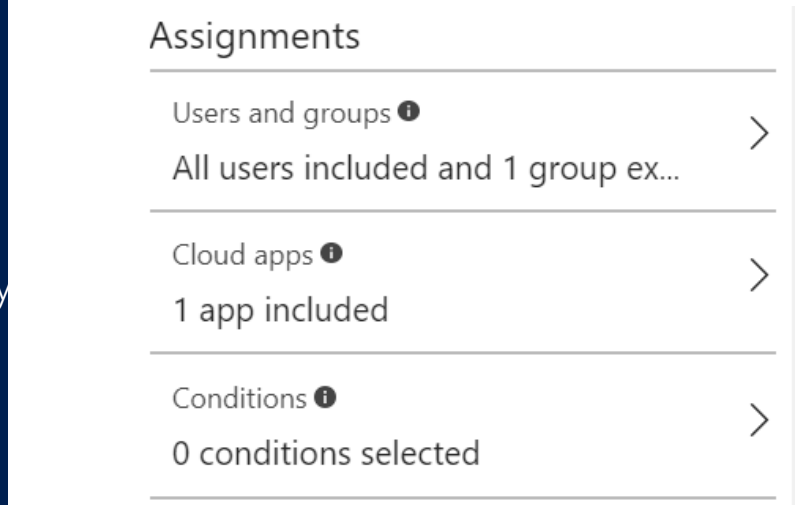
Condition Statements

- In a conditional access policy, you define the criteria that need t
  met for your controls to be applied in the form of a condition
  statement.

- You can include the following assignments into your condition
  statement:
  - Users & Groups - selecting the users and groups your policy applies to, if necessary, you can also explicitly exclude a set of users from your policy by exempting them.

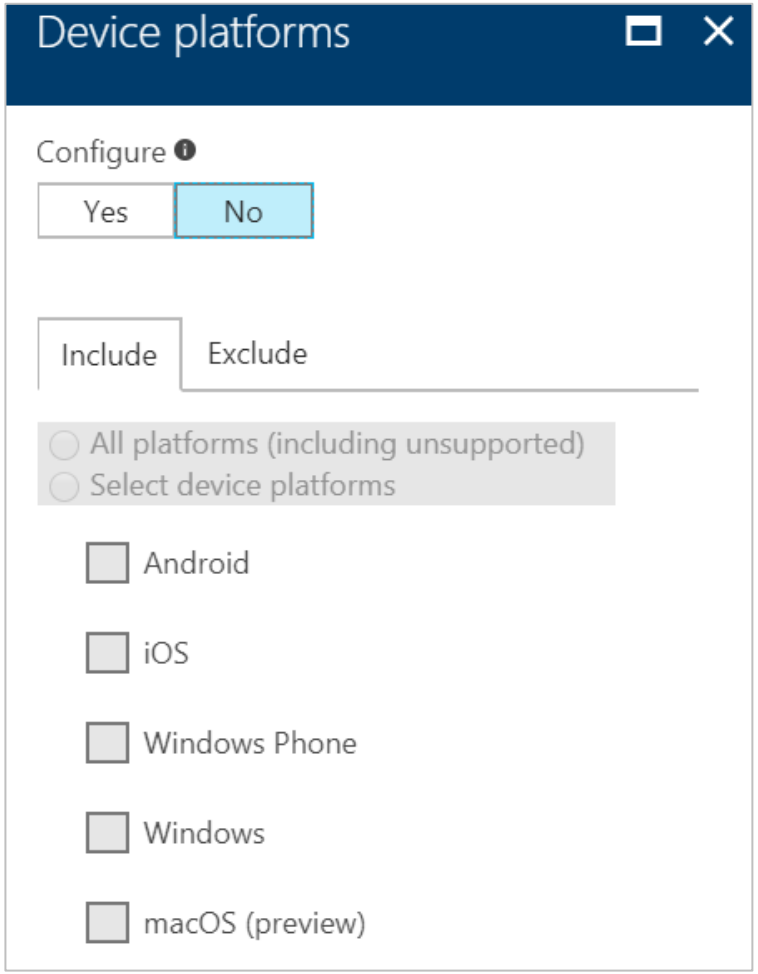
  - Cloud Apps – selecting the cloud apps your policy applies to, if necessary, can also explicitly exclude a set of apps from your policy.

  - Conditions - in a condition statement, you can define additional requireme
    how access to your apps is performed.



Conditions

- The current implementation of Azure Active Directory, allows you to define additional requirements for your condition statements in the following areas:
  - Sign-in risk – uses the risk level attribute value of a users risk event record as a condition e.g. High, Medium or Low.
  - Device platforms - you can define the device platforms that are included as well as device platforms that are exempted from a policy e.g. Android, iOS etc.
  - Locations – you can specify a range of IP addresses that can bypass MFA e.g. for users that are signing in from the company's intranet.
  - Client apps – you can specify the type of app that MFA should apply to e.g. Browser or Mobile apps and desktop clients.
- Conditional access is currently not supported with legacy authentication e.g. basic authentication.



Microsoft

Azure AD Privileged Identity Management

Microsoft Services

What is Azure AD Privileged Identity Management (PIM)?

PIM is a feature of Azure Active Directory that allows you to manage, control, and monitor access within your organization.

Azure AD PIM allows you to:

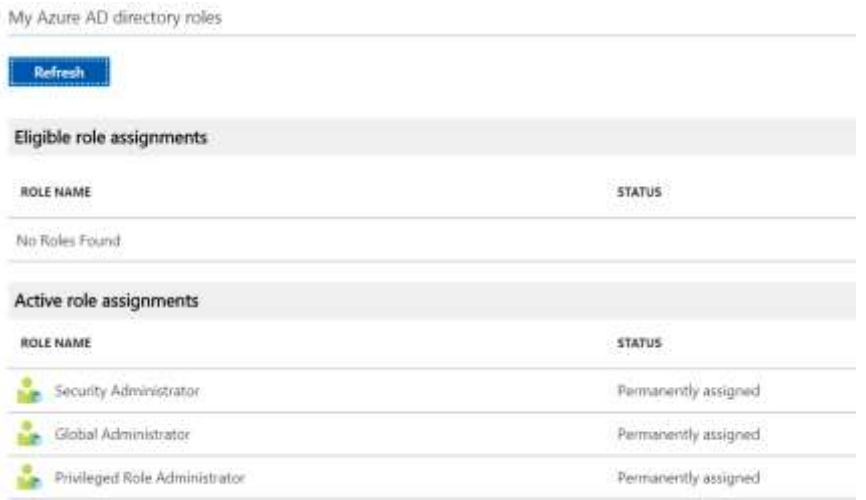
- See which users are Azure AD administrators
- Enable on-demand, "just in time" administrative access to Microsoft Online Services like Office 365 and Intune
- Get reports about administrator access history and changes in administrator assignments
- Get alerts about access to a privileged role

Azure AD PIM can manage the following Azure AD organizational roles, including (but not limited to):

- Global Administrator
- Billing Administrator
- Service Administrator
- User Administrator
- Password Administrator

Just in time Administrator access (JIT)

- Allows you to assign a role permanently or for a predetermined amount of time
- Users who have been assigned a role permanently are known as **permanent admins** and users who have been assigned a role for a period of time are known as **eligible admins**
- An **eligible admins** role is inactive until they require access, they then complete an activation process and become an active admin for a period of time
- User account must be an organizational account
- To configure JIT access:
  - Configure role activation settings e.g. the duration the role is active for
  - Add user or group to the role



PIM Administration

- Requires the Premium P2 edition of Azure AD
- Enable PIM from the Azure portal
- Run the security wizard which walks you through the initial assignment experience
- Access the PIM admin dashboard for an overview of your environment