

Cloud
Computing

Caltech

Center for Technology &
Management Education

Post Graduate Program in Cloud Computing

Cloud Computing

Caltech

**Center for Technology &
Management Education**

**PG CC - Microsoft Azure Architect
Technologies: AZ:303**



Implement Azure Active Directory

Learning Objectives

By the end of this lesson, you will be able to:

- Describe what is Azure Active Directory
- Create Management Groups, Subscriptions, and Resource Groups
- Create User and Group Accounts
- Add and Verify Domains and Custom Domains
- Describe Azure AD Identity Protection



Learning Objectives

By the end of this lesson, you will be able to:

- 🕒 Implement Conditional Access
- 🕒 Configure Fraud Alerts for MFA
- 🕒 Configure Trusted IPs
- 🕒 Configure Guest Users in Azure AD



A Day in the Life of an Azure Architect

You have joined an organization as an Azure administrator that is looking for a user management tool. The tool should not require any on-premise directory input.

- You have been asked for a user management solution as a new employee recently joined your company. The company needs to manage all of its user identity, group memberships, and password management considering access security.
- They are also looking for a solution that can help assign similar access to the users having similar designation. In addition to this, they would need an option to invite any external user to collaborate with their organization as a guest user.

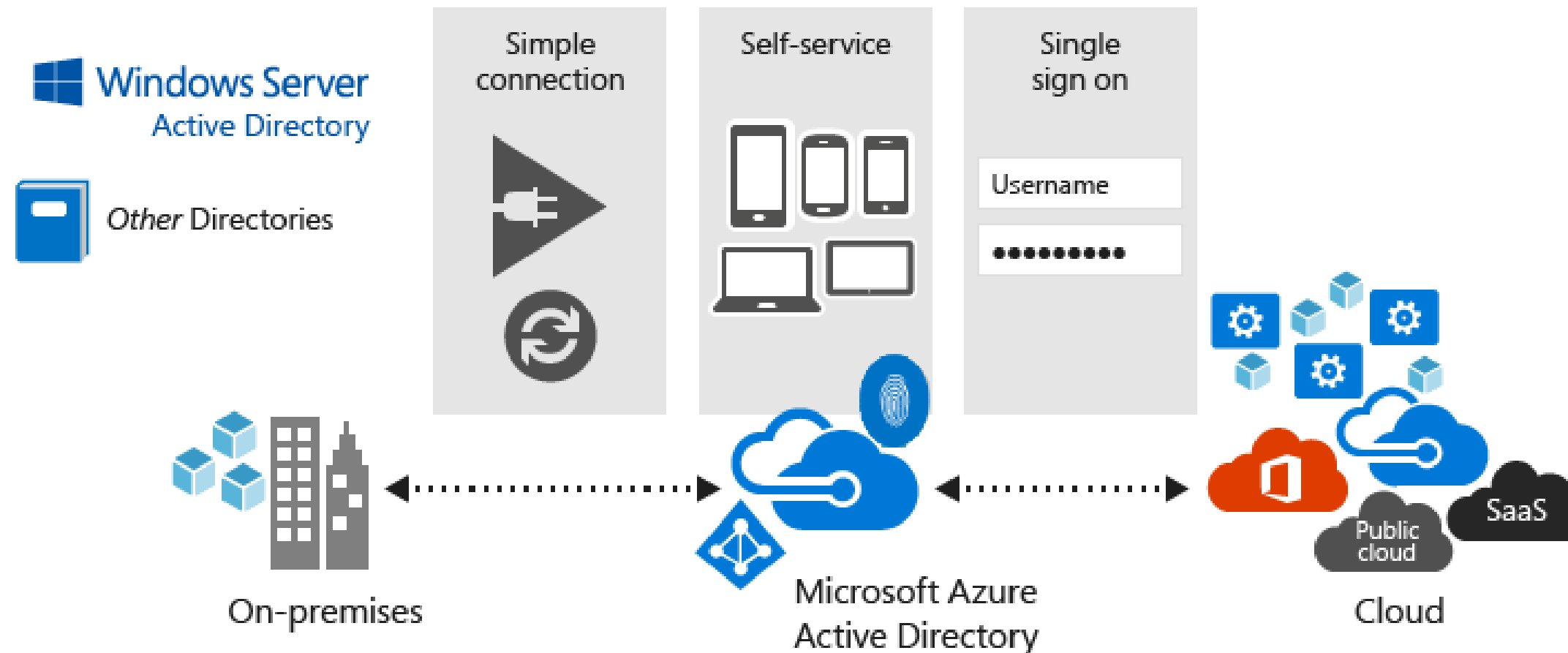
To achieve all of the above along with some additional features, you will be learning a few concepts in this lesson that will help you find a solution for the given scenario.



Azure Active Directory

Azure Active Directory

Azure Active Directory (Azure AD) is Microsoft's cloud-based identity and access management service, which helps employees of an enterprise client to sign in and access resources.



Azure Active Directory

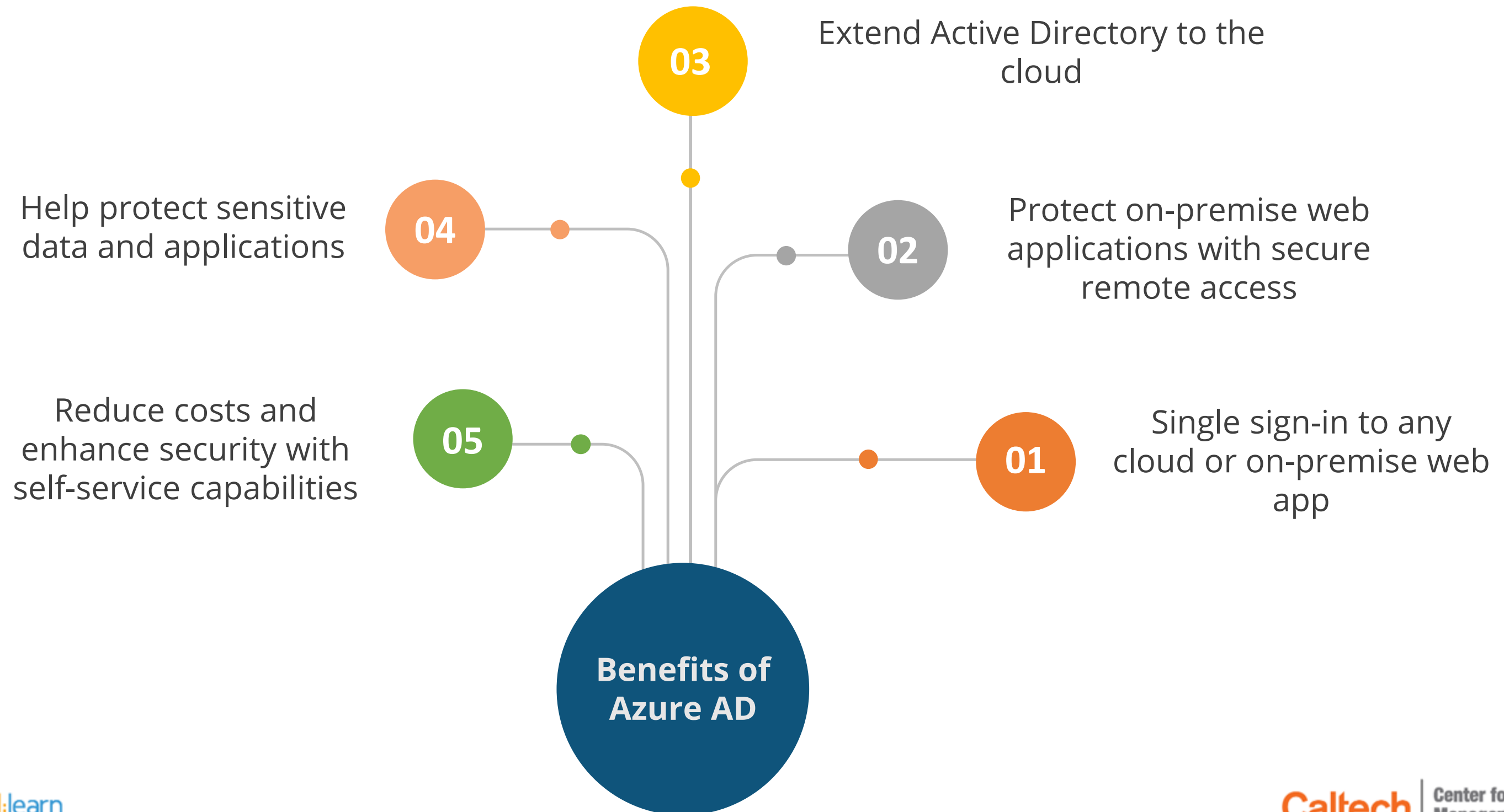


Azure Active
Directory

Features

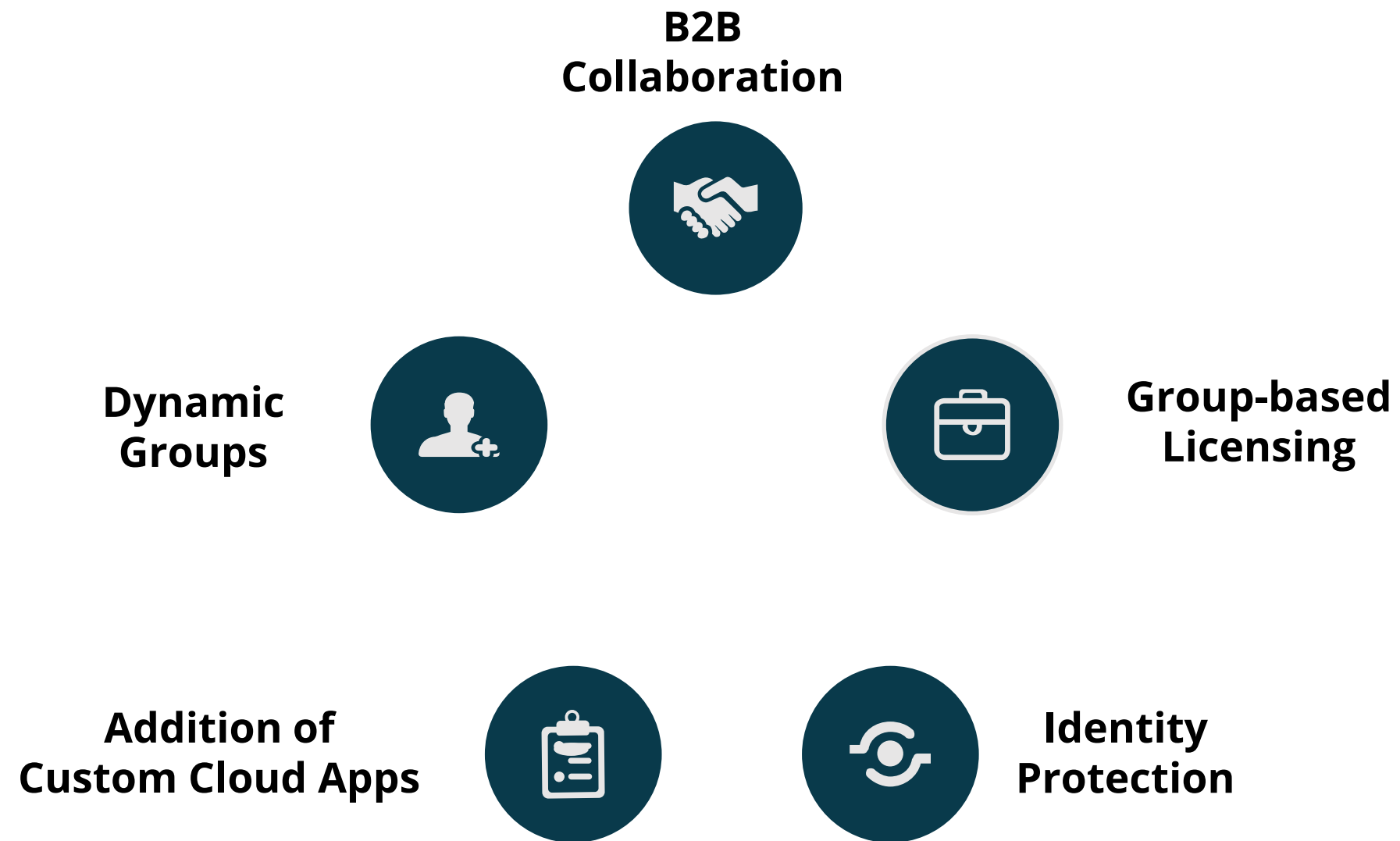
- Single sign-on access to thousands of cloud applications and resources
- Identity management capabilities and integration
- Integration with Windows Server Active Directory
- Facilitates the development of applications with a global scope

Azure Active Directory Benefits



Azure Active Directory Benefits

Some additional benefits include:



Azure Active Directory Concepts

Concepts	Description
Identity	An object that can be authenticated.
Account	An identity that has data associated with it.
Azure AD Account	An identity created through Azure AD or another Microsoft cloud service.
Azure Tenant	A dedicated and trusted instance of Azure AD that is automatically created when an organization signs up for a Microsoft cloud service subscription.
Azure AD Directory	Each Azure tenant has a dedicated and trusted Azure AD.
Azure Subscription	Used to pay for Azure cloud services.

AD Domain Service Vs Azure Active Directory

Azure Active Directory

- Azure AD is primarily an identity solution, and designed for HTTP and HTTPS communications
- Queried using the REST API over HTTP and HTTPS instead of LDAP
- Includes federation services and many third-party services (such as Facebook)

AD Domain Services (AD DS)

- AD DS are the core functions responsible for managing users and computers.
- It allows system administrators to organise data into logical hierarchies.
- It Includes security certificates, Single Sign-On (SSO), LDAP, and rights management.

Azure Active Directory Editions

Azure AD Free

It is designed to introduce system administrators to Azure AD.

Azure AD Premium P2

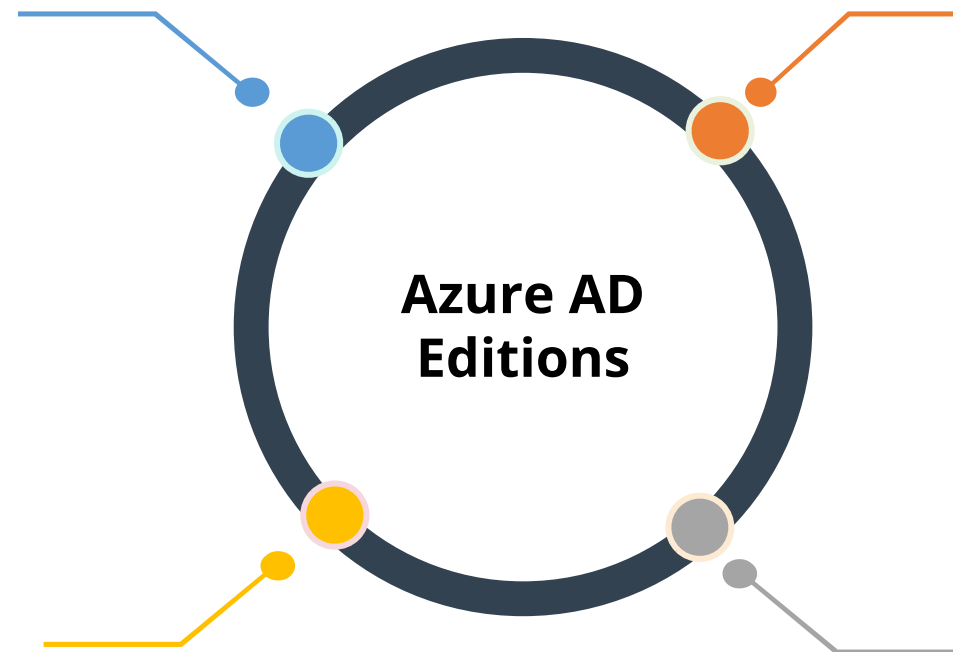
It has all the features of the other editions, including advanced identity protection and privileged identity management.

Microsoft 365

It provides cloud-centric application access and self-service identity management solutions.

Azure AD Premium P1

It is designed to help organizations with demanding identity and access management needs.



Azure Active Directory Editions

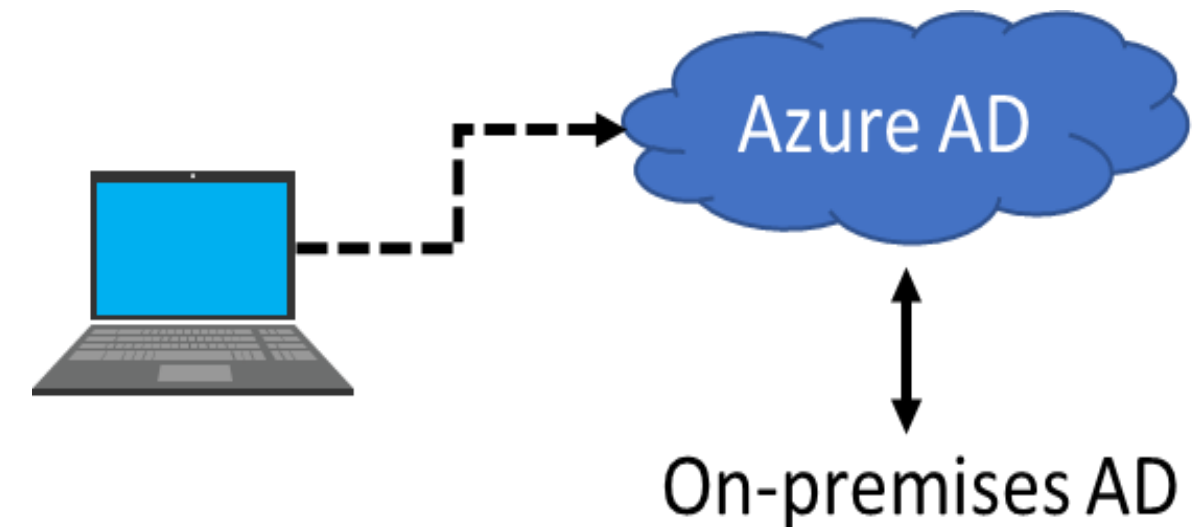
Feature	Free	Microsoft 365 Apps	Premium P1	Premium P2
Directory Objects	500,000 objects	No object limit	No object limit	No object limit
Single Sign-On	Unlimited	Unlimited	Unlimited	Unlimited
Core Identity and Access	X	X	X	X
B2B Collaboration	X	X	X	X
Identity & Access for O365		X	X	X
Premium Features			X	X
Hybrid Identities			X	X
Advanced Group Access			X	X
Conditional Access			X	X
Identity Protection				X
Identity Governance				X

Azure AD Join

Azure AD Joined Devices

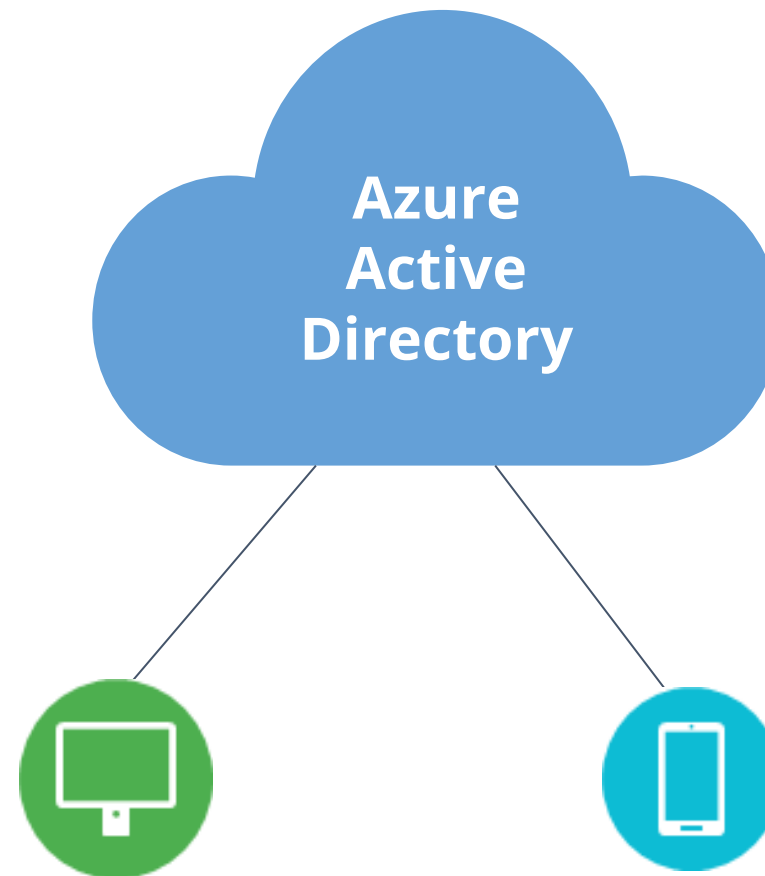
Azure AD join is designed for enterprises that do not have a Windows Server Active Directory infrastructure on-premise.

- Single Sign-On (SSO) to your Azure managed SaaS apps and services
- Enterprise compliant roaming of user settings across joined devices
- Access to Windows Store for business
- Access restriction to apps from only compliant devices



Device Management

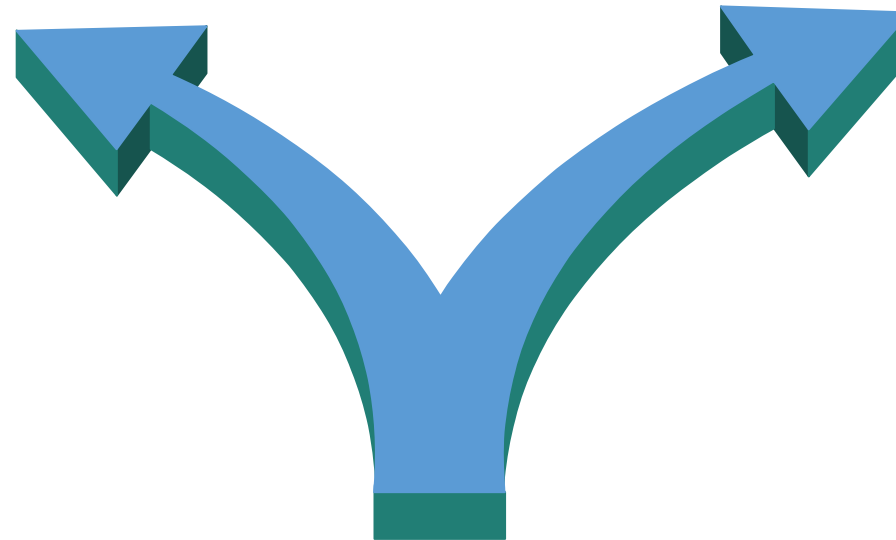
Devices in Azure AD can be managed using Mobile Device Management (MDM) tools like Microsoft Intune, Microsoft Endpoint Configuration Manager, Azure AD join, or other tools.



Device Management

Registering a device

- Enables a registered device to authenticate when the user signs-in
- Disables the device, when needed
- Registers personally owned devices



Azure AD has two options

Joining a device

- Extends the advantages of registration to all registered devices
- Changes the local state of a device
- Sign-in using an organizational account instead of a personal account

Hybrid Azure AD Joined Devices

- Devices joined to both devices on-premise AD and Azure AD
- Central management of work-owned
- Users to sign-in to their devices with their AD work or school accounts

	Registered Devices	Azure AD Joined Devices	Hybrid AD Joined Devices
Device Type	Personal	Organization owned	Organization owned
Registration	Manual	Manual	Automatic
Operating System	Windows 10	Windows 10	Windows 7, 8, and 10

Configuring Azure AD Join

The steps to configure Azure AD join are:

- Select users who can join devices to Azure AD
- Select users that are granted local administrator rights on a device
- Allow Azure AD joined or hybrid Azure AD joined to register with Azure AD

The screenshot displays the Azure AD Join configuration window. At the top, there are 'Save' and 'Discard' buttons. The main configuration area includes several sections:

- Users may join devices to Azure AD:** Includes radio buttons for 'All' (selected), 'Selected', and 'None'. Below this is a section for 'Selected' users, currently showing 'No member selected' with a right arrow.
- Additional local administrators on Azure AD joined devices:** Includes radio buttons for 'Selected' and 'None' (selected). Below this is another 'Selected' section showing 'No member selected' with a right arrow.
- Users may register their devices with Azure AD:** Includes radio buttons for 'All' (selected) and 'None'.
- Require Multi-Factor Auth to join devices:** Includes radio buttons for 'Yes' and 'No' (selected).
- Maximum number of devices per user:** A dropdown menu currently set to '20'.
- Users may sync settings and app data across devices:** Includes radio buttons for 'All' (selected), 'Selected', and 'None'. Below this is a third 'Selected' section showing 'No member selected' with a right arrow.

Configuring Azure AD Join

- Check if required Multi-Factor Authentication (MFA) to join devices
- Enter the maximum number of devices a user can have
- Allow user's settings and app data to sync across their Windows 10 devices

The screenshot shows the 'Configure Azure AD Join' window. At the top, there are 'Save' and 'Discard' buttons. The settings are organized into sections with expandable/collapsible headers.

- Users may join devices to Azure AD**: Radio buttons for 'All' (selected), 'Selected', and 'None'. Below is a header 'Selected' and a list area showing 'No member selected'.
- Additional local administrators on Azure AD joined devices**: Radio buttons for 'Selected' and 'None' (selected). Below is a header 'Selected' and a list area showing 'No member selected'.
- Users may register their devices with Azure AD**: Radio buttons for 'All' (selected) and 'None'.
- Require Multi-Factor Auth to join devices**: Radio buttons for 'Yes' and 'No' (selected).
- Maximum number of devices per user**: A dropdown menu currently set to '20'.
- Users may sync settings and app data across devices**: Radio buttons for 'All' (selected), 'Selected', and 'None'. Below is a header 'Selected' and a list area showing 'No member selected'.

Assisted Practice

Azure AD Join

Duration: 10 Min.

Problem Statement:

Create an Azure AD Join to join devices directly to Azure AD without the need to connect to on-premise Active Directory, keeping your users productive and secure.

Assisted Practice: Guidelines

Steps to create Azure AD Join:

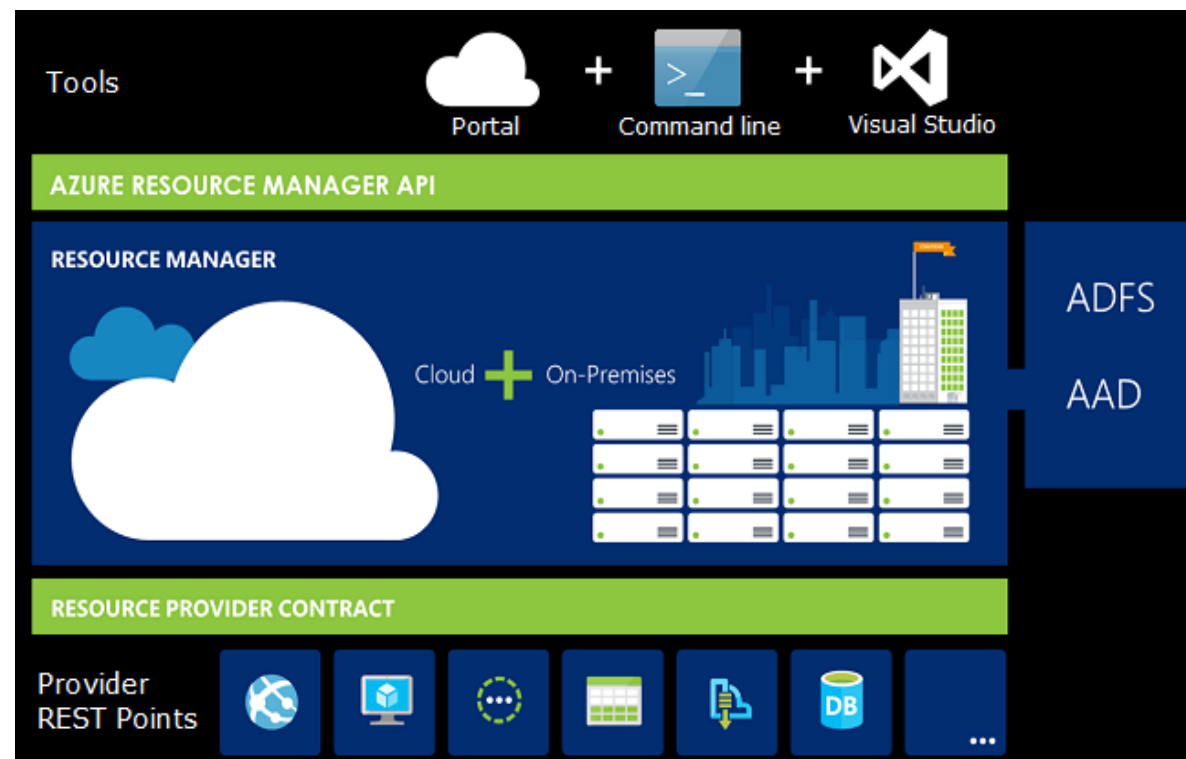
1. Go to the Azure Portal
2. Select Azure Active Directory
3. Create an Azure AD Join



Management Groups, Resource Groups and Subscriptions

Resource Manager

Azure Resource Manager is the service that manages and deploys Azure resources.



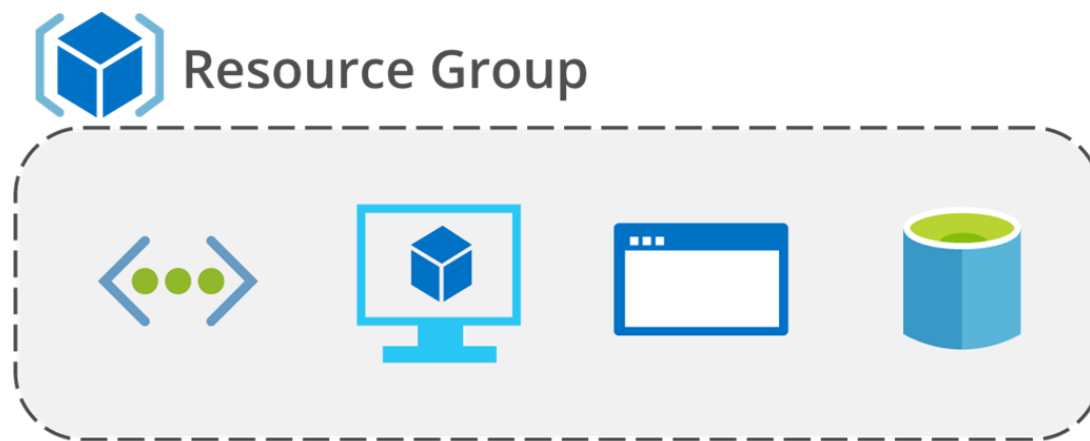
- Renders a consistent management layer.
- Facilitates collaboration with the resources in solution, as a group.
- Enables deployment, updation, or deletion using a single, coordinated operation.
- Provides security, auditing, and tagging features.

Note

Select the tools and APIs that are best suited.

Resource Groups

Resource Group is a logical grouping of resources.



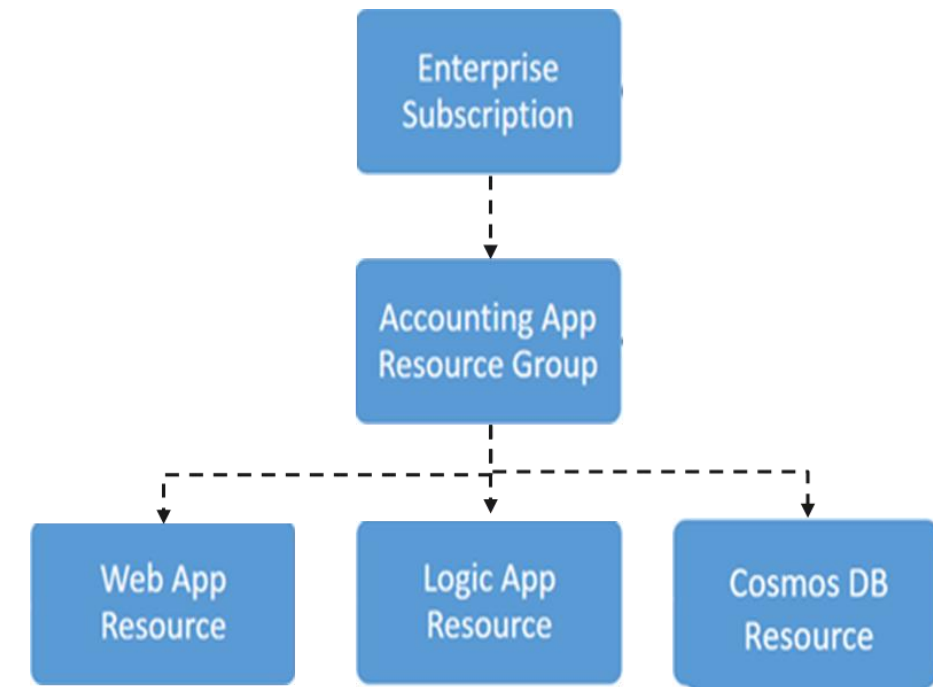
- Fundamental concept of the Azure platform
- Ties to the resource life cycle
- Cannot be nested
- Must be allocated to each resource

Note

A majority of resources can be moved between resource groups.

Resource Groups and Deployments

- There can only be one resource group per resource.
- Renaming resource groups is not possible.
- Groups can have a wide range of resources (services).
- They can also have resources from various regions.
- Deployments are made in stages.



Users can easily add, remove, and modify resources by scoping permissions to a resource group.

Resource Group Organization

Organizing for authorization

Since resource groups fall under the scope of RBAC, users can organise resources by who wants to manage them.

Organizing for life cycle

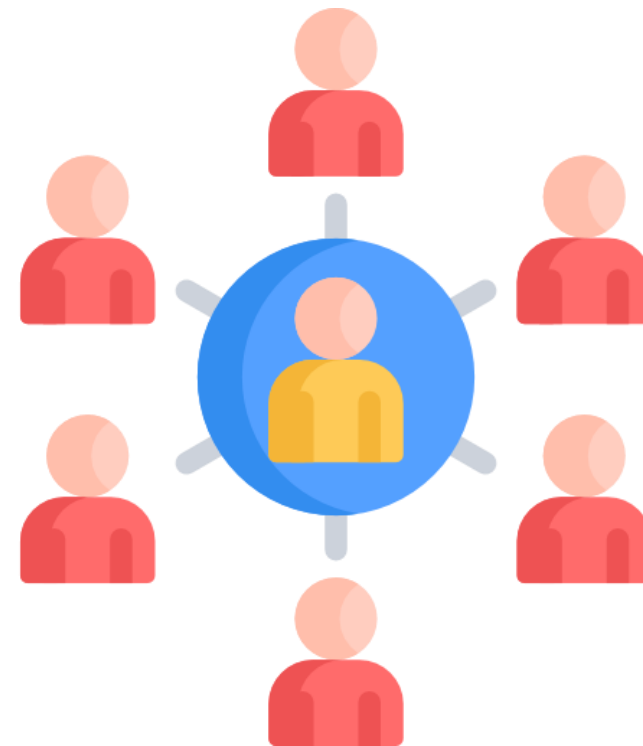
When a user deletes a resource group, all of the resources inside the resource group are also deleted. It is suitable when resources are more disposable, such as in production environments.

Organizing for billing

Putting resources in the same resource group allows them to be grouped together for billing reports.

Management Groups

Azure Management Groups provide an efficient way to manage access, policies, and compliance across an enterprise.



It manages access through a hierarchy made up of management groups and subscriptions

Management Groups

01

Management Groups provide a level of scope above subscriptions

02

Subscriptions can be organized into containers called Management Groups

03

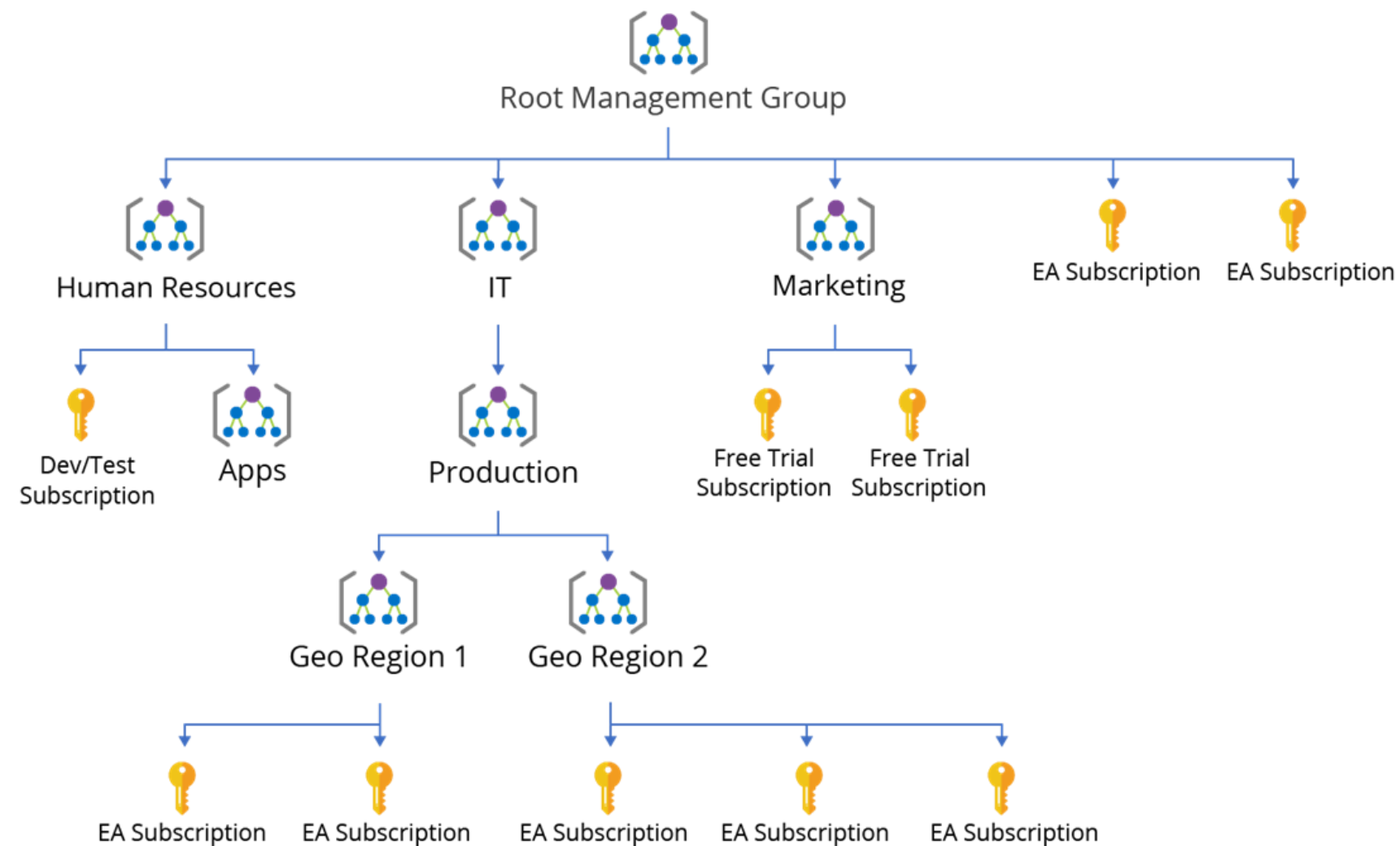
Management Groups are organizationally aligned through custom hierarchies and grouping

04

Management groups provide enterprise-level management on a wide scale, regardless of the sort of subscriptions a user have,

Management Groups

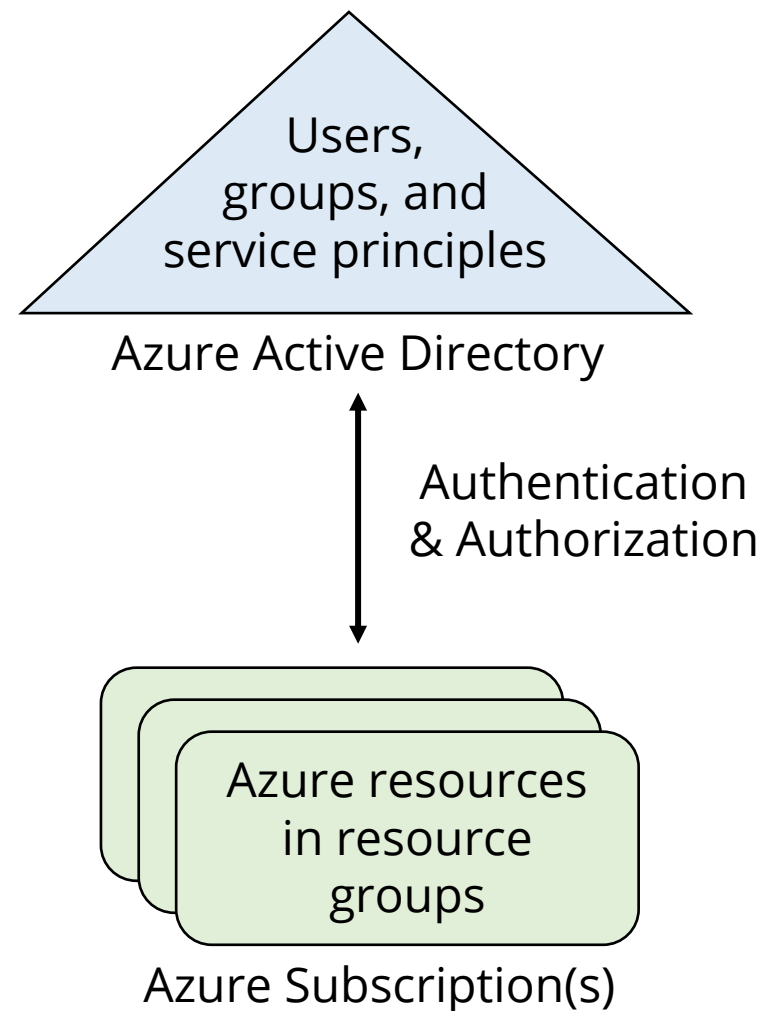
Building a governance hierarchy is shown below.



Source: <https://docs.microsoft.com/>

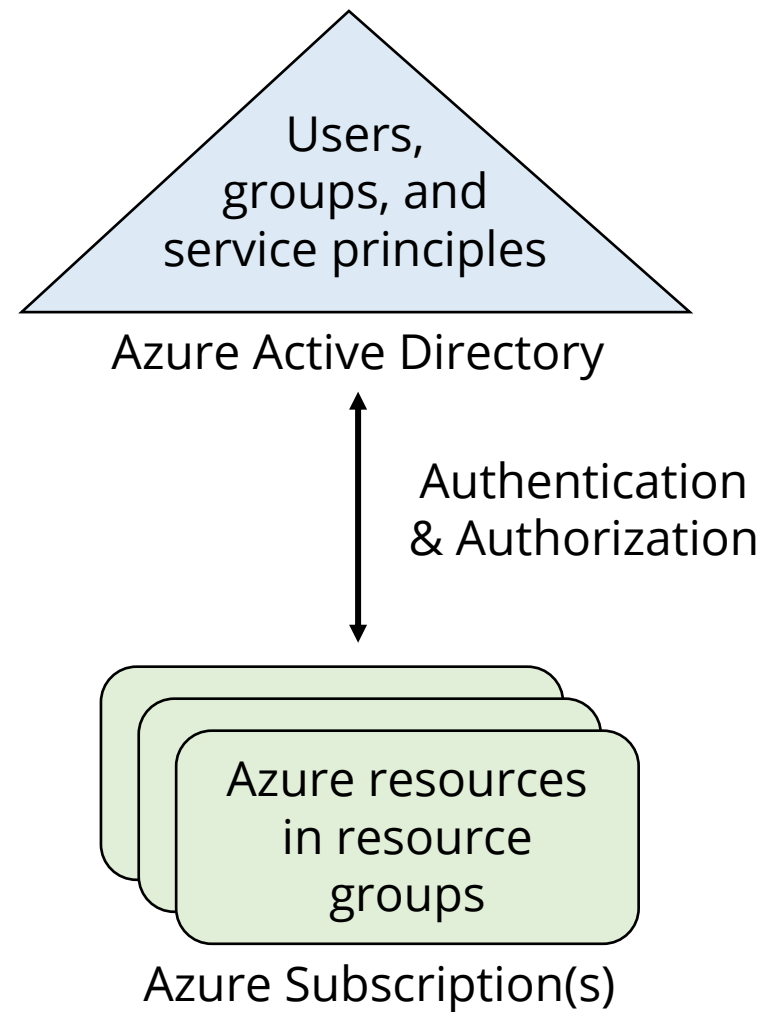
Azure Subscriptions and Accounts

An Azure account is connected to a subscription, which is a logical unit of Azure services.



- Azure services are billed on a per-subscription basis.
- Subscriptions have accounts and are associated with Azure AD.

Azure Subscriptions and Accounts



- An account is an identity in Azure AD or in a directory that is trusted by Azure AD.
- The most common way to allow a user access to Azure services is to add them to the Azure AD directory linked with subscription.

Getting an Azure Subscription

The types of Azure subscriptions are:



- **Enterprise Agreement** - Customer makes an upfront monetary commitment to Azure
- **Reseller** - Open Licensing program
- **Microsoft partner** - Find a partner that can design and implement cloud solution
- **Free trial account** - Customer can use a free Azure credit, to try out different tiers and types of Azure services

Azure Subscriptions and Service Limits

Microsoft Azure limits are also called quotas.

Managing limits

- Some limits apply to the regional level.
- The user can raise soft limits by raising an online customer support request at no charge.
- These limits keeps on changing.
- To check the latest limits, navigate to:
<https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/azure-subscription-service-limits>

Users and Groups

Azure User Accounts

A user account is used for the authentication and authorization during the sign-in process.

Home > Users - All users





Users - All users

microsoft - Azure Active Directory

Search (Ctrl+/)

Show

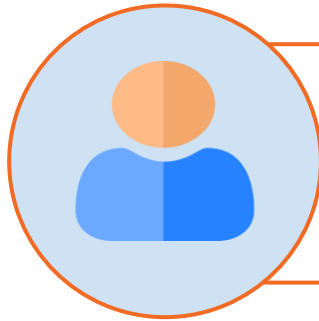
All users

NAME	USER NAME	USER TYPE	SOURCE
 Ziaulla	████████@macoutlook.com	Guest	Azure Active Directory
 Retail Crisis Notifications	████████@microsoft.com	Member	Windows Server AD
 "Planning & Launch Services OEM Inquiries	████████@microsoft.com		Windows Server AD
 Bert	████████@hotmail.com	Guest	Azure Active Directory

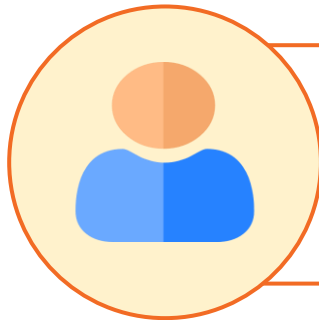
All users must have a user account.

Azure User Accounts

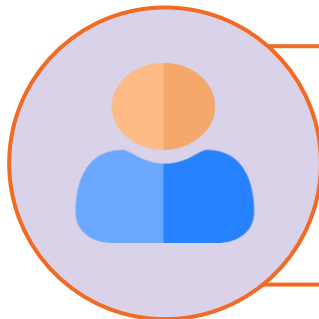
Different sources of user accounts depending on the type of identity are:



Cloud Identities (Azure AD): Users that only exist in Azure AD
Ex: Administrators Account



Directory-synchronized (Windows Server AD): Users brought in using Azure AD Connect



Guest (Azure AD): Users from outside Microsoft Azure
Ex: Google and Microsoft Accounts

Create and Manage Users

How to add users?

1. Synchronize users from Windows Server Active Directory.
2. Manually create users by using the Azure portal.
 - Creating a user
 - Inviting a user

The screenshot shows the Azure portal interface for creating a new user. It is divided into two main sections: 'User' and 'Profile'.

User Section:

- Name:** A text input field with a placeholder example: 'Chris Green'.
- User name:** A text input field with a placeholder example: 'chris@contoso.com'.
- Profile:** A section with a blue header and a right-pointing arrow. Below it, it says 'Not configured'.
- Properties:** A section with a right-pointing arrow. Below it, it says 'Default'.
- Groups:** A section with a right-pointing arrow. Below it, it says '0 groups selected'.
- Directory role:** A section with a right-pointing arrow. Below it, it says 'User'.

Profile Section:

- General:** A section with two text input fields: 'First name' and 'Last name'.
- Work info:** A section with two text input fields: 'Job title' and 'Department'.

Group Accounts

Groups in Azure Active Directory can be used to control access to cloud-based applications, on-premise apps, and resources.

Users and groups - All groups																			
<input type="text" value="Search (Ctrl+/)"/>		<input type="text" value="Search groups"/>																	
<div><div> Overview</div><div>MANAGE</div><div> All users</div><div> All groups</div></div>		<table><tr><th colspan="2">NAME</th><th>GROUP TYPE</th><th>MEMBERSHIP TYPE</th></tr><tr><td></td><td>Group1</td><td>Security</td><td>Assigned</td></tr><tr><td></td><td>Group2</td><td>Security</td><td>Assigned</td></tr><tr><td></td><td>Group23</td><td>Security</td><td>Assigned</td></tr></table>		NAME		GROUP TYPE	MEMBERSHIP TYPE		Group1	Security	Assigned		Group2	Security	Assigned		Group23	Security	Assigned
NAME		GROUP TYPE	MEMBERSHIP TYPE																
	Group1	Security	Assigned																
	Group2	Security	Assigned																
	Group23	Security	Assigned																

Instead of having to provide access permissions one by one, groups allow the resource owner to assign a set of permissions to all members of the group.

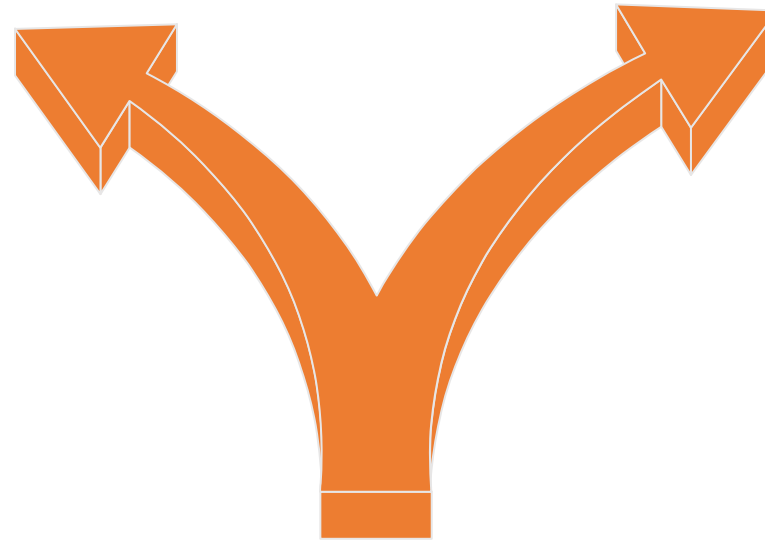
Group Accounts

Security Groups

Security-enabled and used to manage access to different resources and grant permissions.

Distribution groups (Office 365)

They are used by email clients and are not security-enabled.



There are two types of groups:

Group Accounts

There are two ways to add members to group:

Directly assigned

- Users must be manually added

Dynamically assigned

- Dynamic assignment, based on rules
- Requires Azure AD Premium P1 license

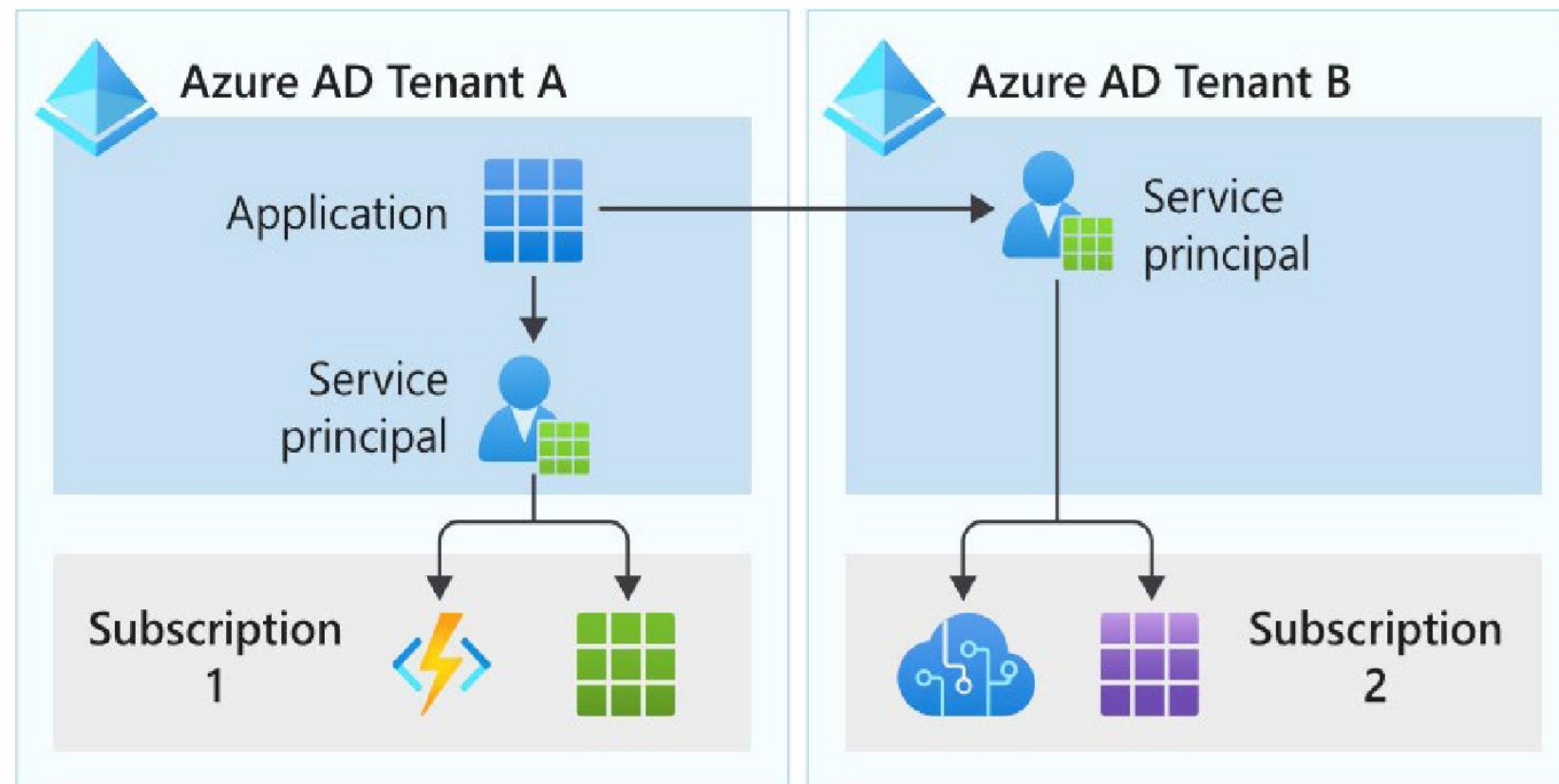
Service Principals

An Azure service principal is an identity that can be used to access Azure resources through applications, hosted services, and automated tools.



- Consider an Azure service principal to be a proxy account, or identity, for an app or service.
- The user can give the service principal permission to access the Azure services as required.

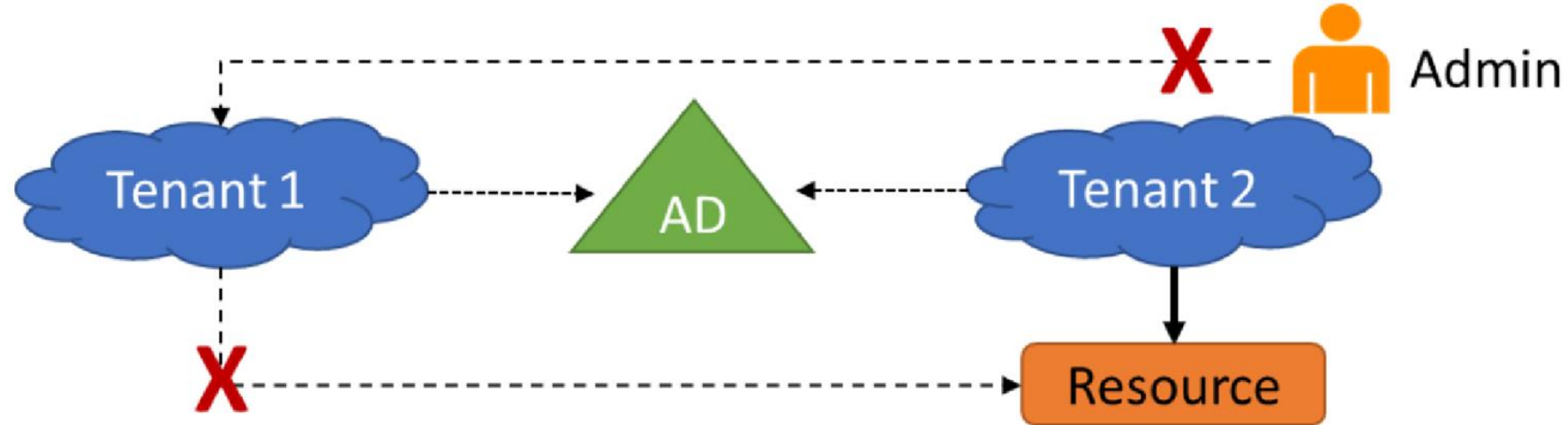
Service Principals



- If all of the services are in the same tenant, only one service principal is needed.
- The user will need a service principal for each tenant if the app requires access to Azure services in a different tenant.

Azure Active Directory Tenants

A tenant is a dedicated instance of an Azure AD directory.



A user may have several tenants for the following:

- Resource independence
- Administrative independence
- Synchronization independence

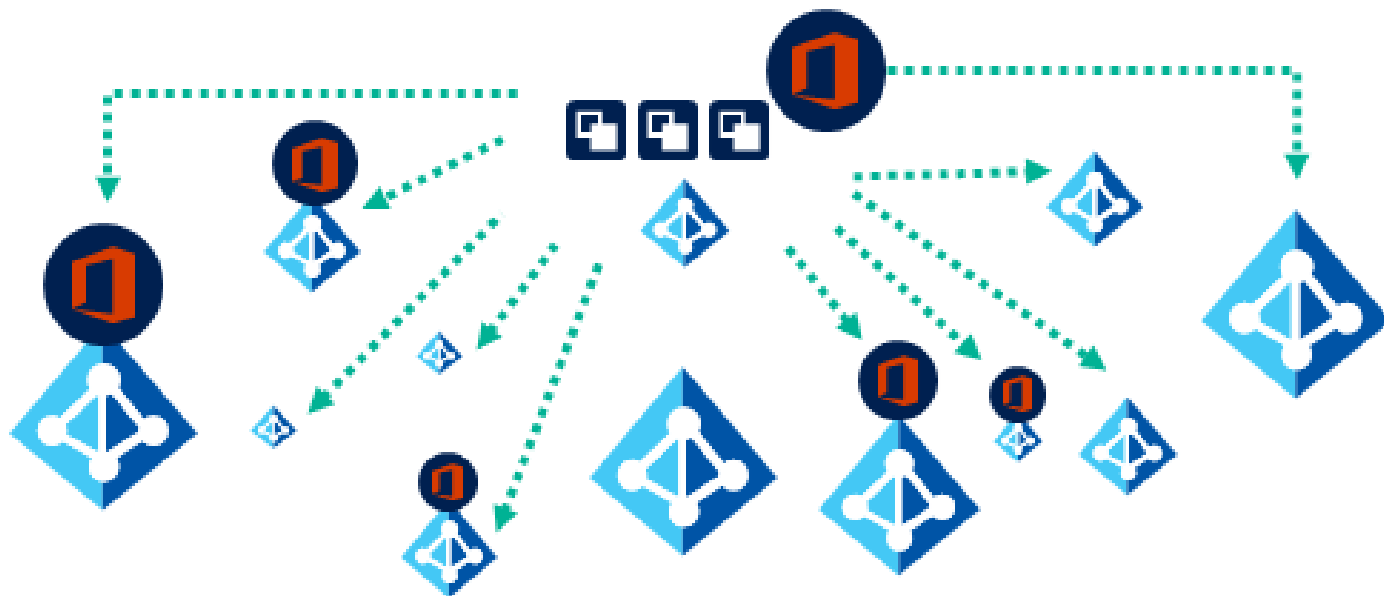
Azure AD B2B

Azure AD B2B allows a user to securely share their company's applications and resources with guests from any other organization, while retaining control of their own corporate data.



Azure AD B2B

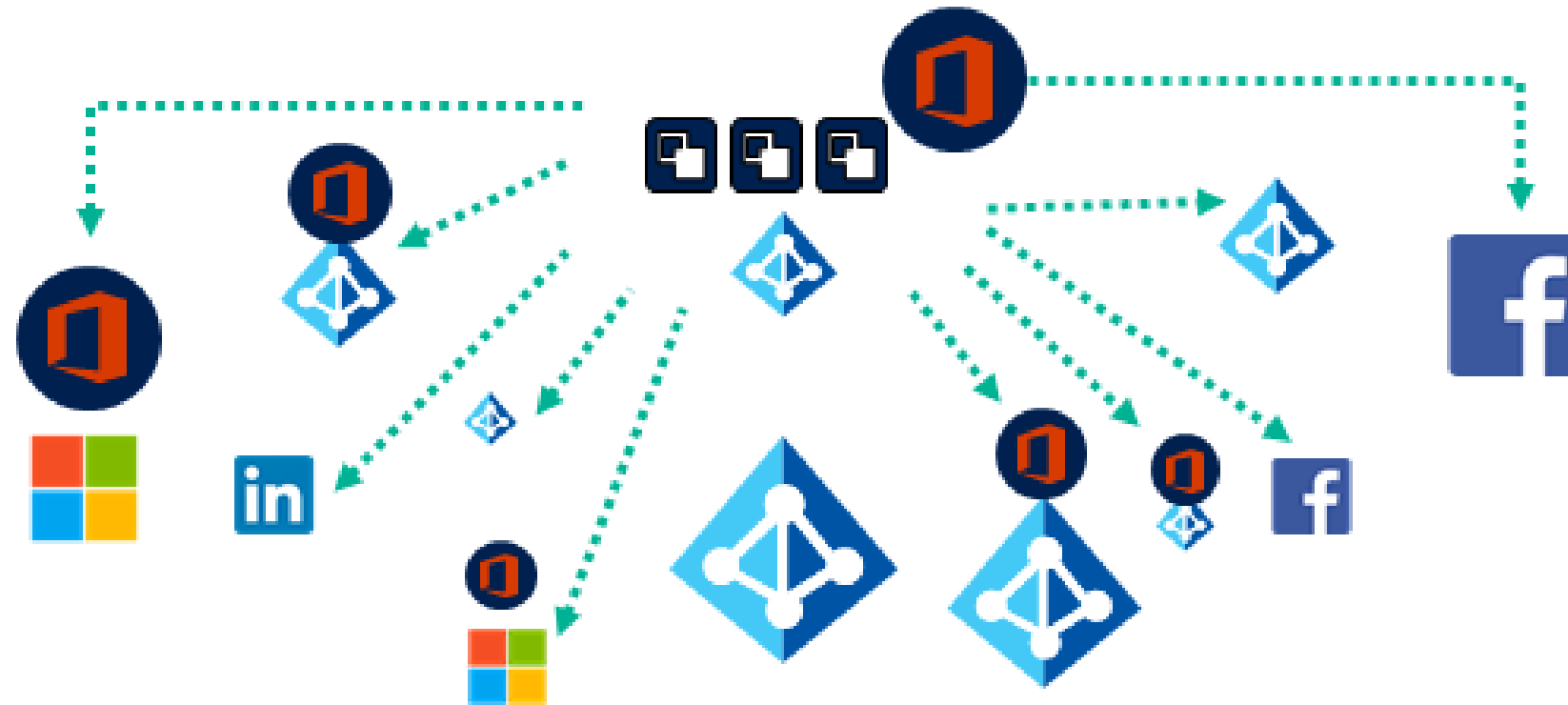
With Azure AD B2B (business-to-business):



- There are no external operating costs for user's business.
- Azure AD is not needed since the partner uses their own identities and credentials.
- The user does not have to worry about passwords or external accounts.
- The user will not have to worry about syncing accounts or managing account lifecycles.

Azure AD B2C

Business-to-customer identity as a service is provided by Azure Active Directory B2C.



To enable single sign-on access to a user's applications and APIs, customers use their preferred social, enterprise, or local account identities.

Azure AD B2C

With Azure AD B2C:

01 Invite users from other social media identity providers into your own organization tenant.

02 User provisioning is done by the invited party.

03 Standards-based authentication protocols are used including OpenID Connect, OAuth 2.0, and SAML.

04 Integration support for most modern applications and commercial off-the-shelf software.

05 The directory can hold 100 custom attributes per user.

06 Collect user data, pass it to a third party system for validation, and then user account creation.

Assisted Practice

Azure AD User Creation
Min.

Duration: 10

Problem Statement:

As an administrator, you've been tasked with creating an Azure AD user for a new employee in your company.

Assisted Practice: Guidelines

Steps to create a user in Azure AD:

1. Login to your azure portal
2. Select Azure Active Directory
3. Select New user and enter required fields



Assisted Practice

Azure AD Group creation
Min

Duration: 10

Problem Statement:

Create a user group in Azure AD to manage access by combining users with similar job roles and assigning them similar rights as an administrator in your organisation.

Assisted Practice: Guidelines

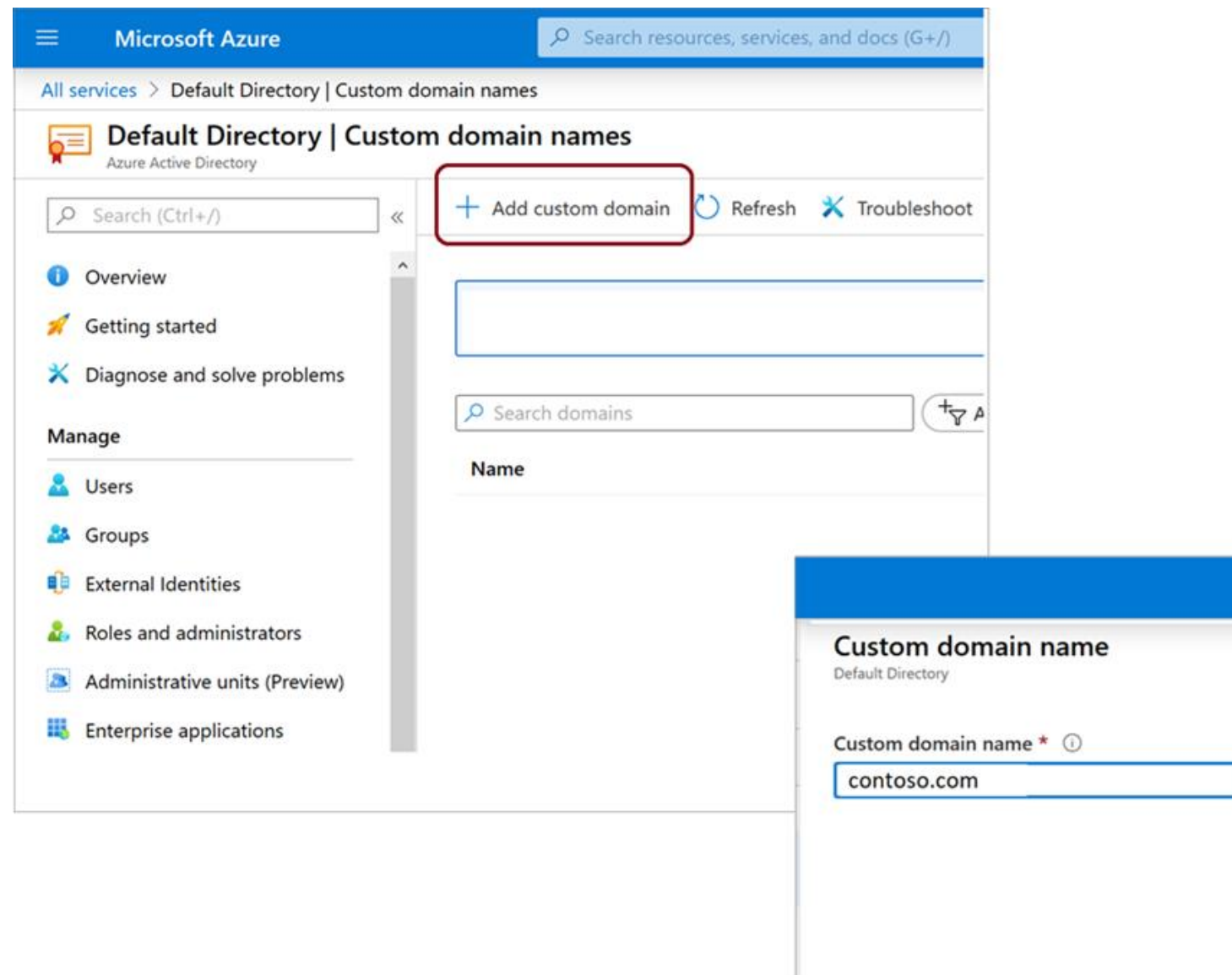
Steps to create a user group in Azure AD:

1. Login to your azure portal
2. Select Azure Active Directory
3. Select New group on the Active Directory page
4. Enter required fields and create the user group

Domains and Custom Domains

Domains and Custom Domains

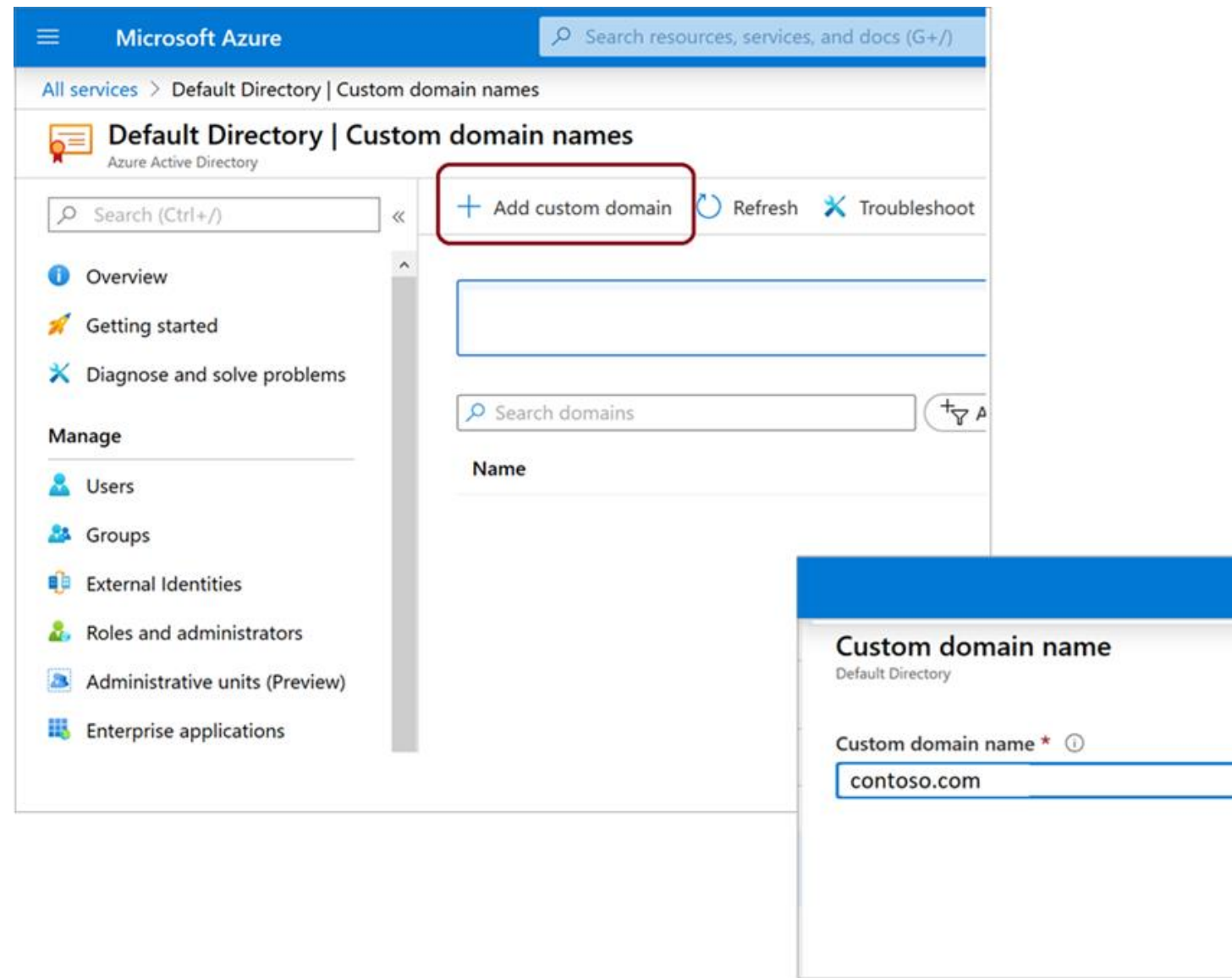
A domain is a unique brand name that identifies a website.



Azure AD tenant domain naming convention:

- Suffix onmicrosoft.com at the initial (mandatory)
Ex: domainname.onmicrosoft.com
- Custom (optional)
Ex: domainname.com

Domains and Custom Domains

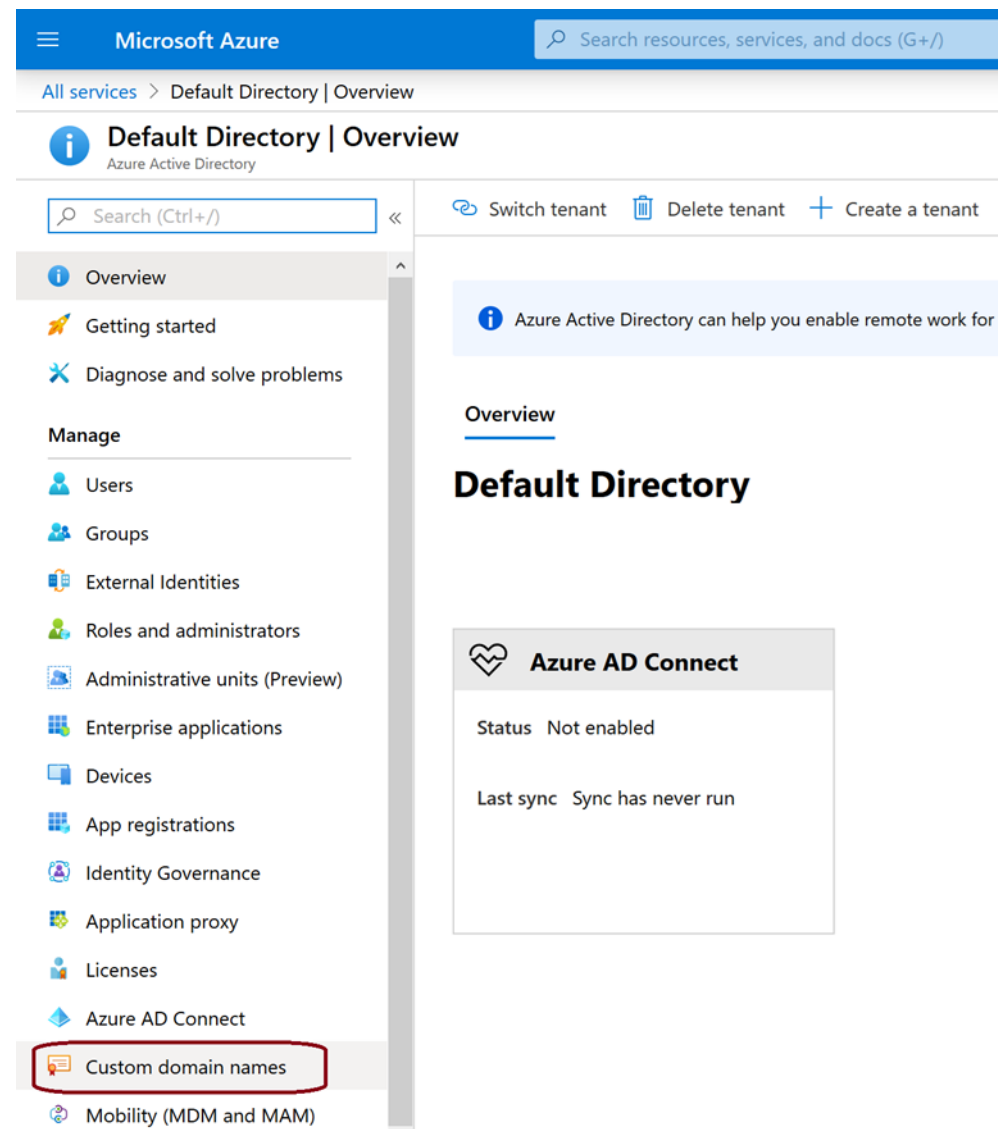


Domain name management:

- Requires global administrator privileges to perform domain management tasks
- Domain names are globally unique
- Custom domain names require verification

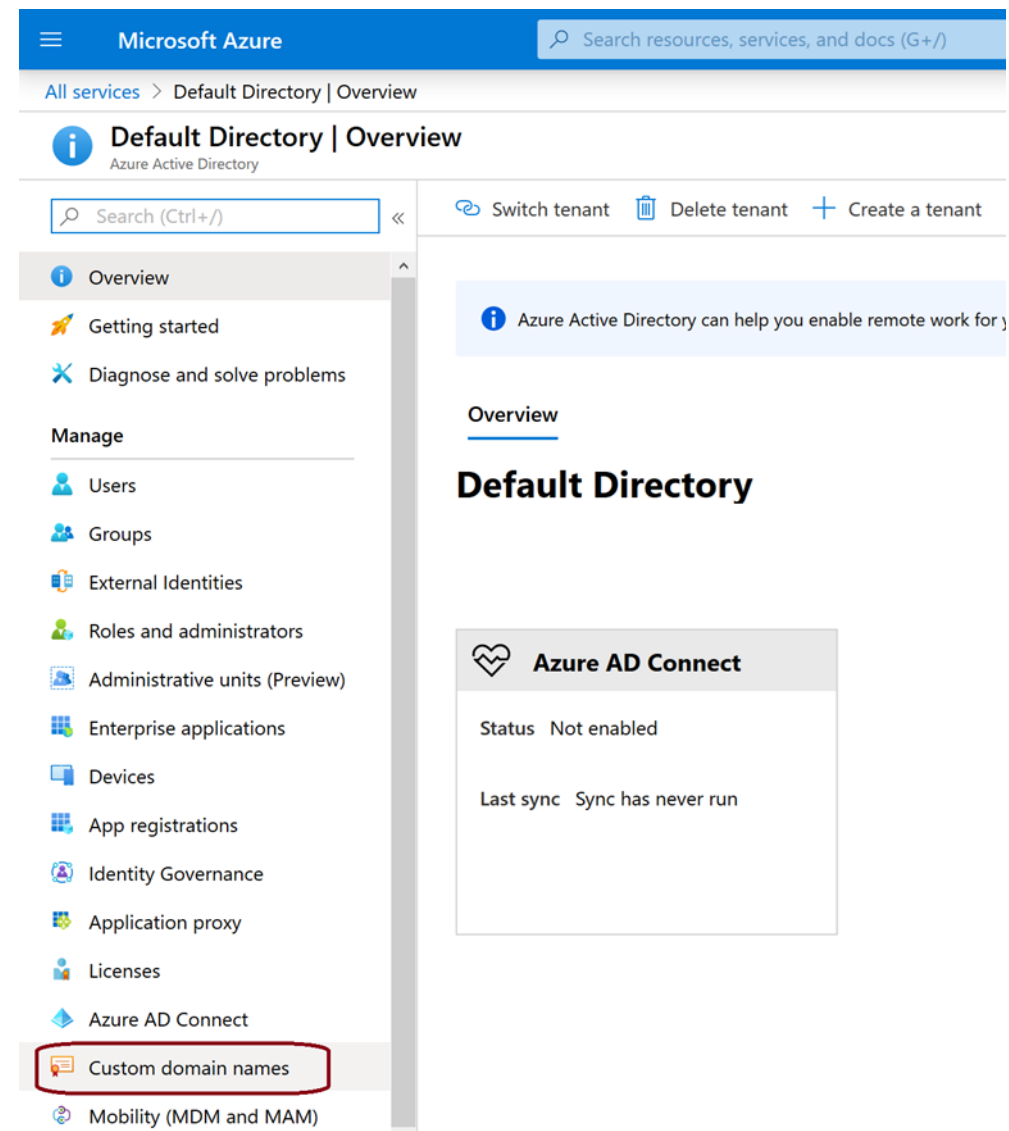
Verifying Custom Domain Name

After adding create user Azure AD tenant, user can add a custom domain name using Azure portal



Verifying Custom Domain Name

A custom domain name is initially in an unverified state



To verify a custom domain

Create a specific TXT or MX DNS record
in the corresponding DNS zone

Assisted Practice

Azure AD - Add a custom Domain

Duration: 10 Min

Problem Statement:

You've been given a project to create a custom domain in Azure AD for a website that your company's developers are working on.

Assisted Practice: Guidelines

Steps to create a custom domain in Azure AD:

1. Login to your azure portal
2. Select Azure Active Directory
3. Select and add custom domain



Azure AD Identity Protection

Azure Active Directory Identity Protection

Protection allows organizations to accomplish three key tasks:



- Automate the detection and remediation of identity-based risks
- Investigate risks using the data presented in the Azure portal
- Export risk detection data to third-party utilities for further analysis

Risk Detection and Remediation

Risk Detection Type	Description
Atypical travel	Sign in from an atypical location based on the user's recent sign-ins.
Anonymous IP address	Sign in from an anonymous IP address (for example: Tor browser, anonymizer VPNs).
Unfamiliar sign-in properties	Sign in with properties which are not seen for the given user recently
Malware linked IP address	Sign in from a malware linked IP address
Leaked credentials	Sign in credentials of the user have been leaked
Azure AD threat intelligence	Microsoft's internal and external threat intelligence sources have identified a known attack pattern

Azure Active Directory Identity Protection

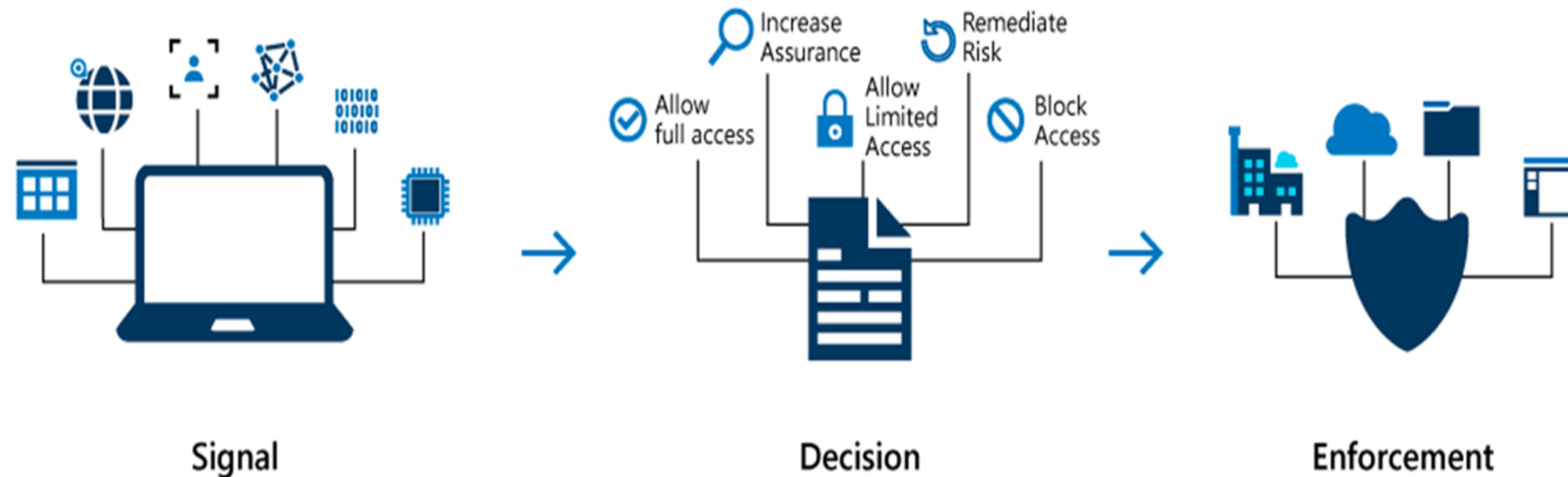
Administrators can review detections and take manual action on them, if needed.



Conditional Access

Conditional Access

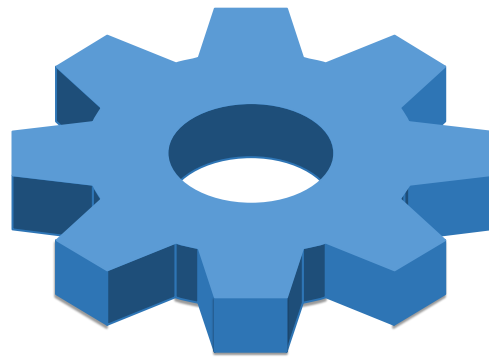
Conditional Access policies are if-then statements, which means that if a user wishes to access a resource, they should first perform an action.



Conditional Access allows a user to apply the appropriate access controls when not required to keep the organization safe and secure.

Conditional Access and Azure Multi-Factor Authentication (MFA)

Azure MFA enables a user to enforce controls on access to apps, based on specific conditions given below:



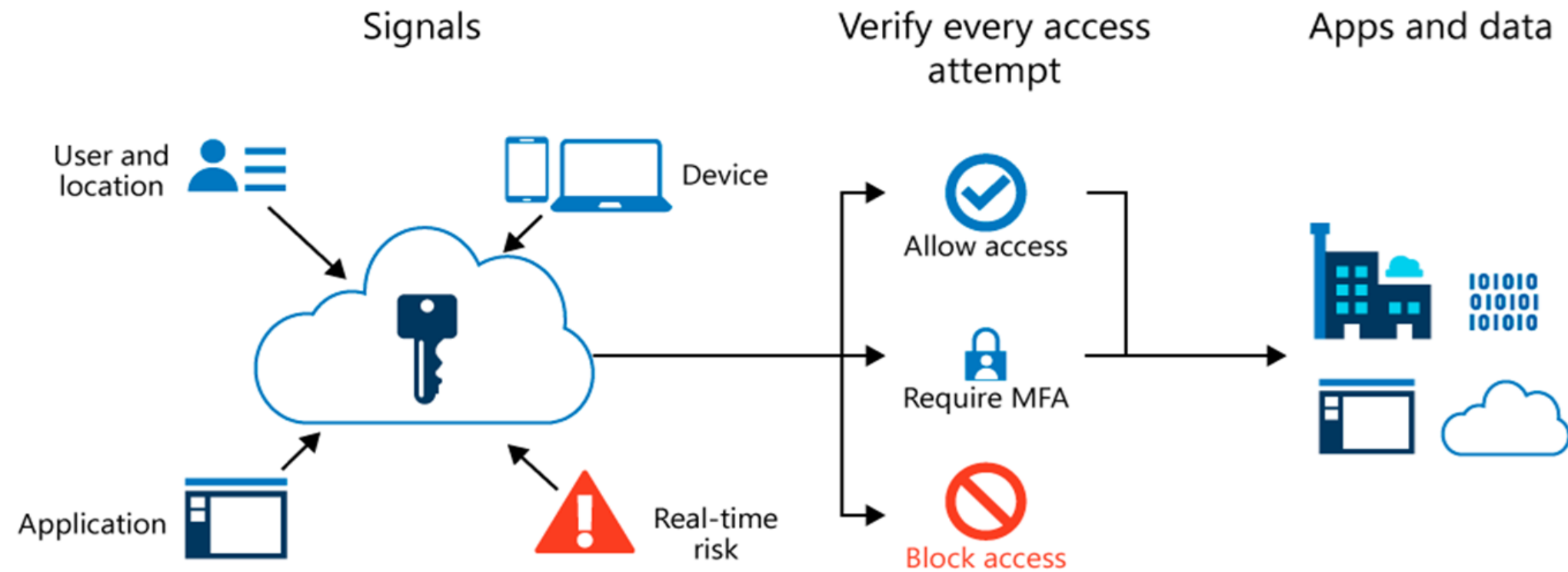
Users and groups can be enabled for MFA to prompt for additional verification during sign-in.



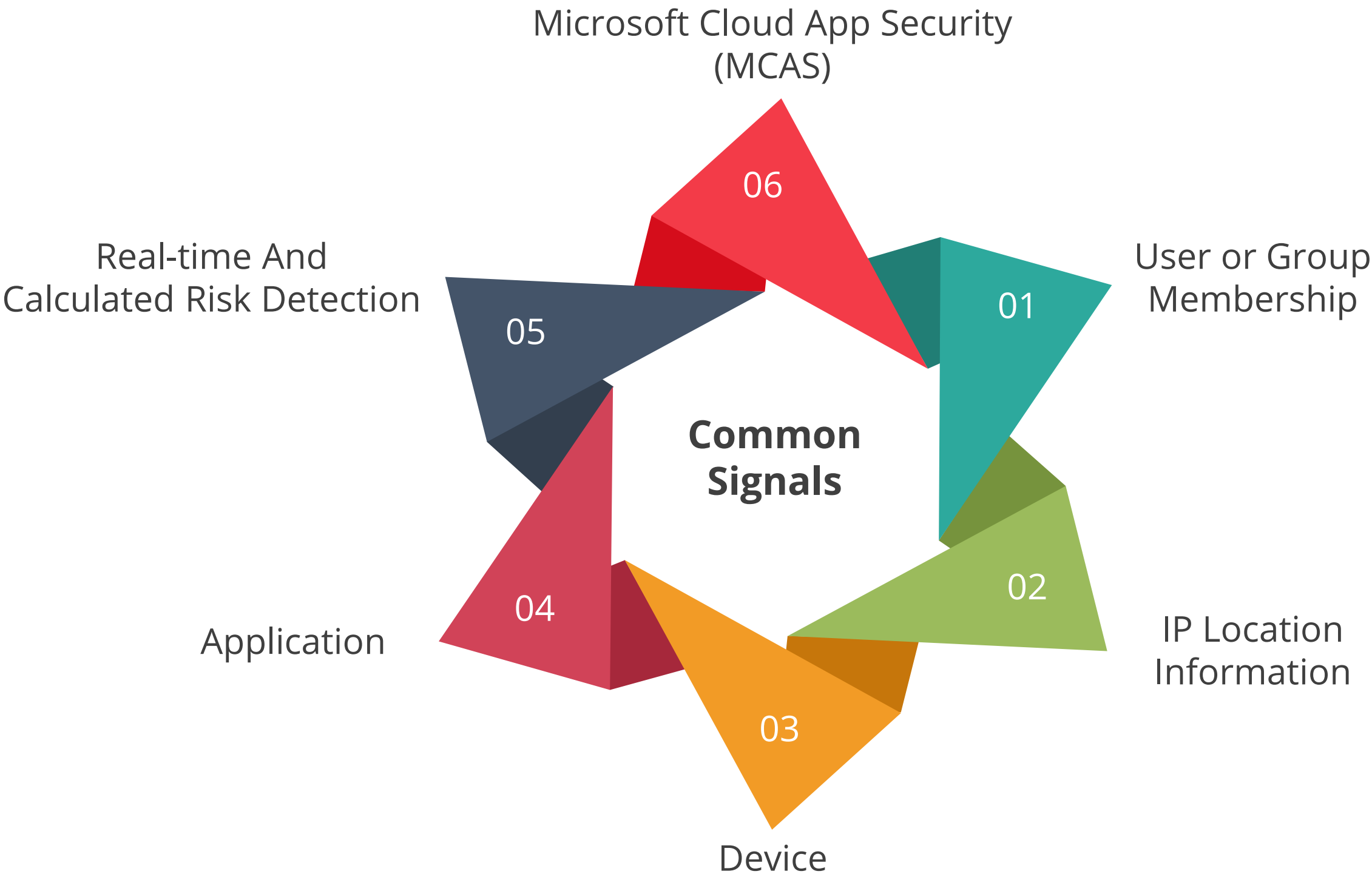
Alternatively, Conditional Access policies can be used to define events or applications that require MFA.

Azure Multi-Factor Authentication

Azure Multi-Factor Authentication provides two-step authentication and verification.



Conditional Access: Signals



Conditional Access: Decisions

The following are the common decisions that Conditional Access should consider while making a policy decision:



Block Access

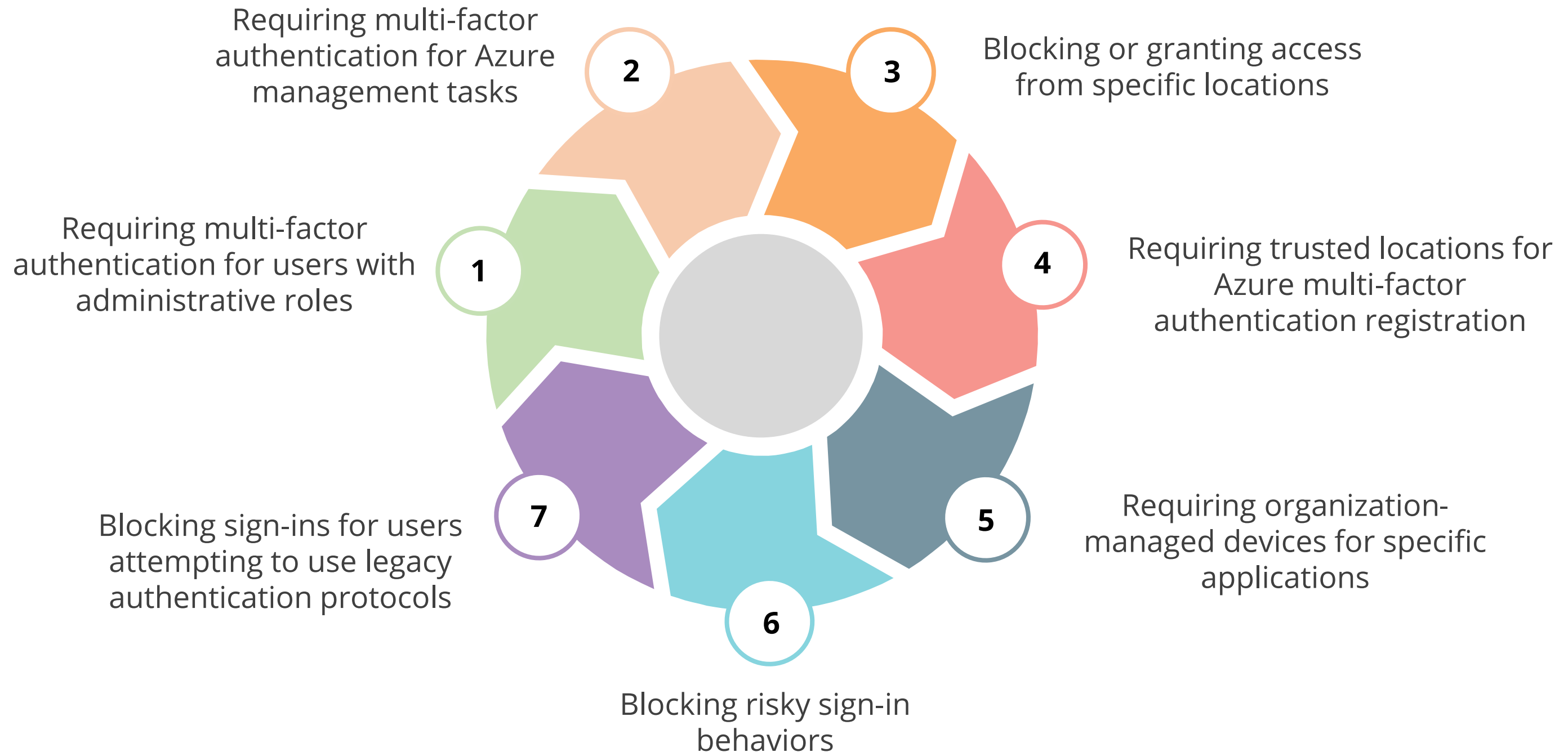
Most restrictive decision



Grant access

Least restrictive decision

Commonly Applied Policies



Multi-Factor Authentication (MFA)

Multi-Factor Authentication (MFA)

Multi-Factor Authentication is a process where a user is prompted during the sign-in process for an additional form of identification, such as to enter a code on their cell phone or to provide a fingerprint scan.

Username
ae@contoso.com

Password

Password



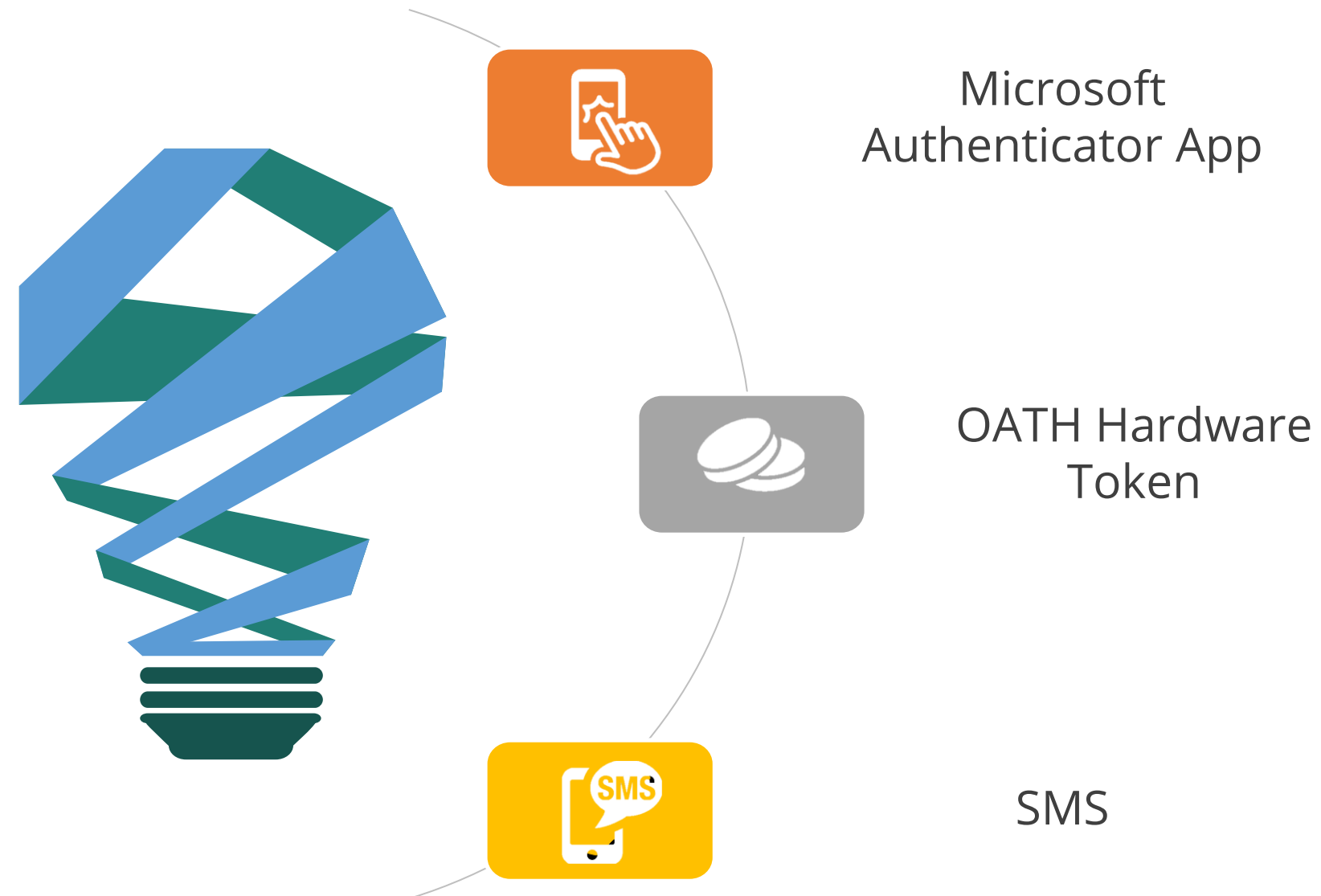
Phone or
hardware key



Biometrics like a
fingerprint or face
scan

MFA Verification Methods

Verification methods for multi-factor authentication:



MFA Authentication Methods



Self-Service Password Reset

Self-Service Password Reset (SSPR) gives users the ability to bypass the helpdesk and reset their own passwords.

Password reset - Properties

MANAGE

- Properties
- Authentication methods
- Registration
- Notifications

Save Discard

Self service password reset enabled ⓘ

None Selected All

Select group

OnPremUsers

Three options of password reset properties:

- None
- Selected
- All

Self-Service Password Reset: Authentication Methods

The methods for authentication of self-service password reset are:

The screenshot shows the 'Password reset - Authentication methods' configuration page in the Azure Active Directory portal. The left sidebar contains navigation links: 'Diagnose and solve problems', 'Manage' (with sub-links for 'Properties', 'Authentication methods', 'Registration', 'Notifications', 'Customization', and 'On-premises integration'), 'Activity' (with 'Audit logs' and 'Usage & insights'), and 'Troubleshooting + Support' (with 'New support request'). The main content area has 'Save' and 'Discard' buttons at the top. Below them, the 'Number of methods required to reset' is set to 1. The 'Methods available to users' section includes checkboxes for 'Mobile app notification' (disabled), 'Mobile app code', 'Email' (checked), 'Mobile phone' (checked), 'Office phone', and 'Security questions' (checked). The 'Number of questions required to register' is set to 5, and the 'Number of questions required to reset' is set to 3. At the bottom, a dashed box indicates '5 security questions selected'.

- Mobile app code
- Email
- Cell phone
- Office phone
- Security questions

Configure Azure MFA Settings

Some of the MFA settings are given in the table below.

Feature	Description
Account lockout	Temporarily lock accounts, in the multi-factor authentication service, if there are too many denied authentication attempts in a row.
Block/unblock users	Used to block specific users from being able to receive MFA requests.
Fraud alert	Configure settings related to user's ability to report fraudulent verification requests
Notifications	Enable notifications of events from MFA Server.
OATH tokens	Used in cloud-based Azure MFA environments to manage OATH tokens for users.
Phone call settings	Configure settings related to phone calls and greetings for cloud and on-premise environments.
Providers	This will show any existing authentication providers that may have associated with an Azure account.

Azure MFA Reports

Azure MFA provides reports that are available in the Azure portal.

Report	Location	Description
Blocked user history	Azure AD > Security > MFA > Block/unblock users	Shows the history of requests to block or unblock users
Usage and fraud alerts	Azure AD > Sign-ins	Provides information on overall usage, user summary, and user details; as well as a history of fraud alerts submitted during the date range specified
Usage for on-premise components	Azure AD > Security > MFA > Activity report	Provides information on overall usage for MFA through the NPS extension, ADFS, and MFA server
Bypassed user history	Azure AD > Security > MFA > One-time bypass	Provides a history of requests to bypass Multi-Factor Authentication for a user
Server status	Azure AD > Security > MFA > Server status	Displays the status of Multi-Factor Authentication servers associated with an Azure account

Azure MFA Reports

Users can view reports from the Azure portal and based on the reports they can answer multiple questions for better user experience.

FAQ

- Was the sign-in challenged with MFA?
- How did the user complete MFA?
- Why was the user unable to complete MFA?
- How many users are challenged for MFA?
- How many users are unable to complete the MFA challenge?
- What are the common MFA issues end users are running into?

Guest Users in Azure AD

Guest Users

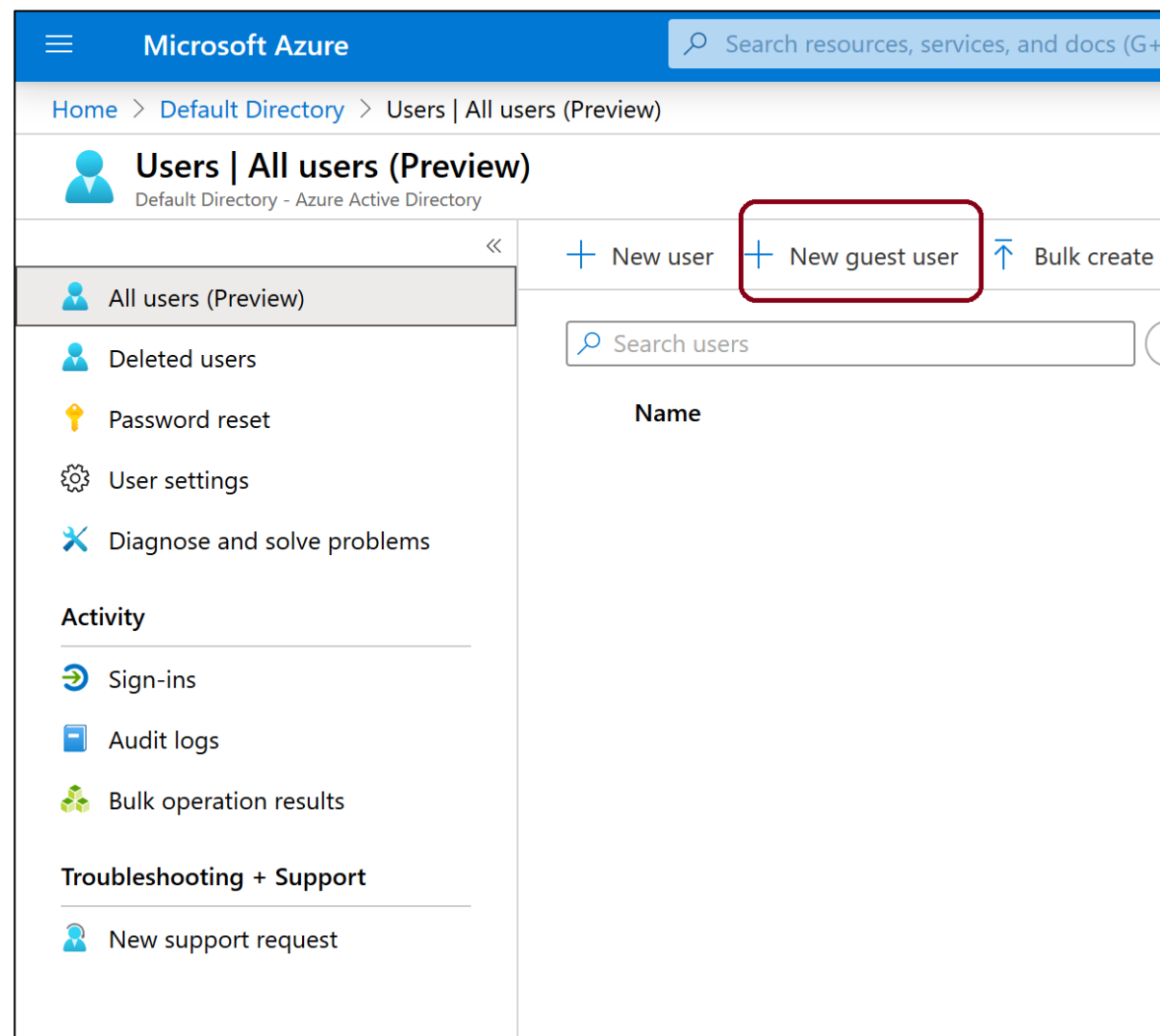
Guest users are those who are not considered as an internal entity, such as an external partner, stakeholder, or a customer.

Prerequisites

- Anyone can be asked to work for a company by adding them as a guest user.
- Guest users can use their own work, education, or social identity to log in.
- An user should have the ability to create user accounts.
- A user should have a working email address.

Adding Guest Users

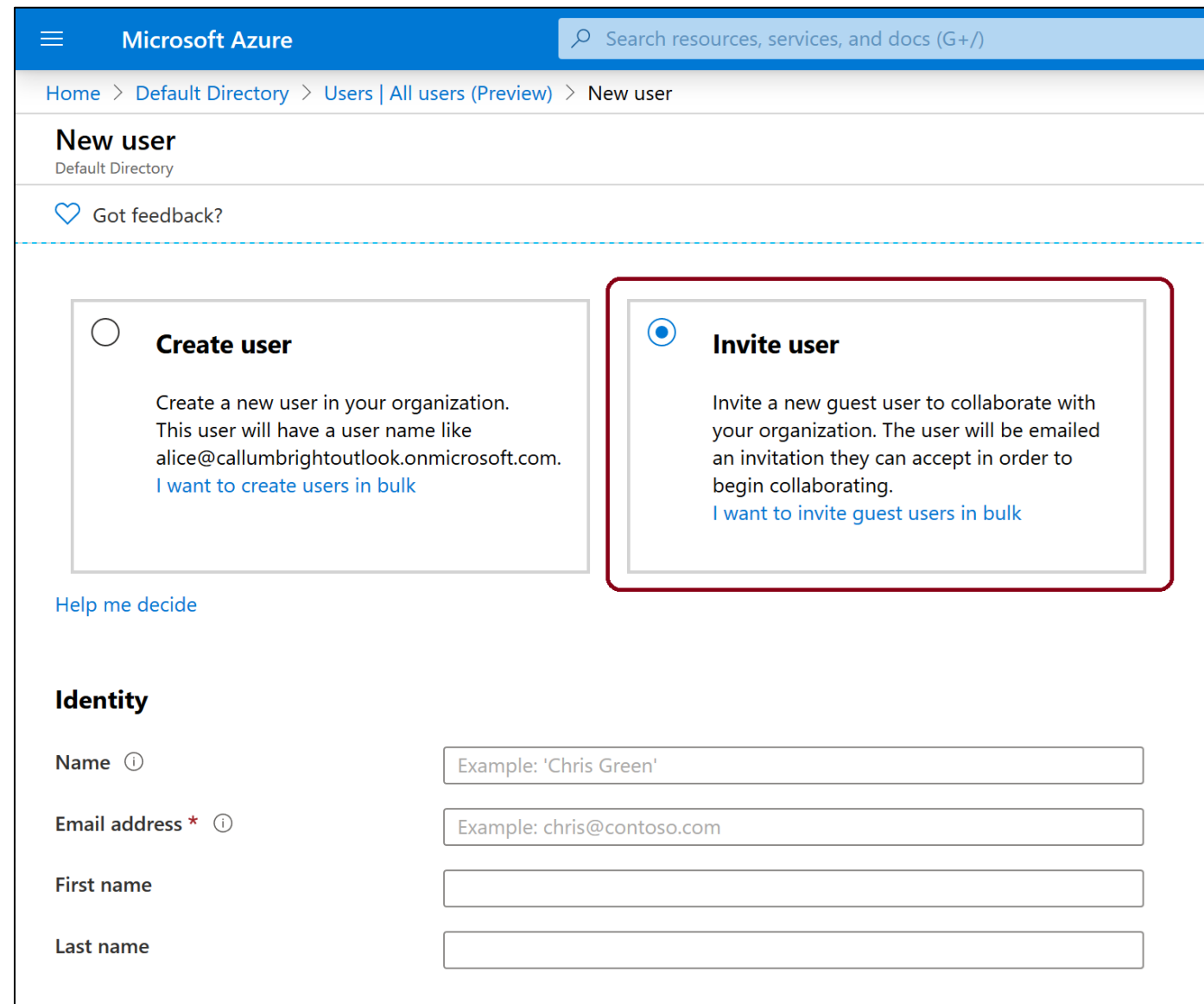
Anyone can work with a company by being added directory as a guest user.



Follow the instructions given below to add a new guest user:

- Log in as an administrator to the Microsoft Azure portal.
- In the left column, click on **All users**.
- Choose **New guest user**.
- After landing on the New user page, click on **Invite user**.

Adding Guest Users



Microsoft Azure

Search resources, services, and docs (G+)

Home > Default Directory > Users | All users (Preview) > New user

New user

Default Directory

Got feedback?

☐ **Create user**
Create a new user in your organization. This user will have a user name like `alice@callumbrightoutlook.onmicrosoft.com`.
[I want to create users in bulk](#)

☒ **Invite user**
Invite a new guest user to collaborate with your organization. The user will be emailed an invitation they can accept in order to begin collaborating.
[I want to invite guest users in bulk](#)

[Help me decide](#)

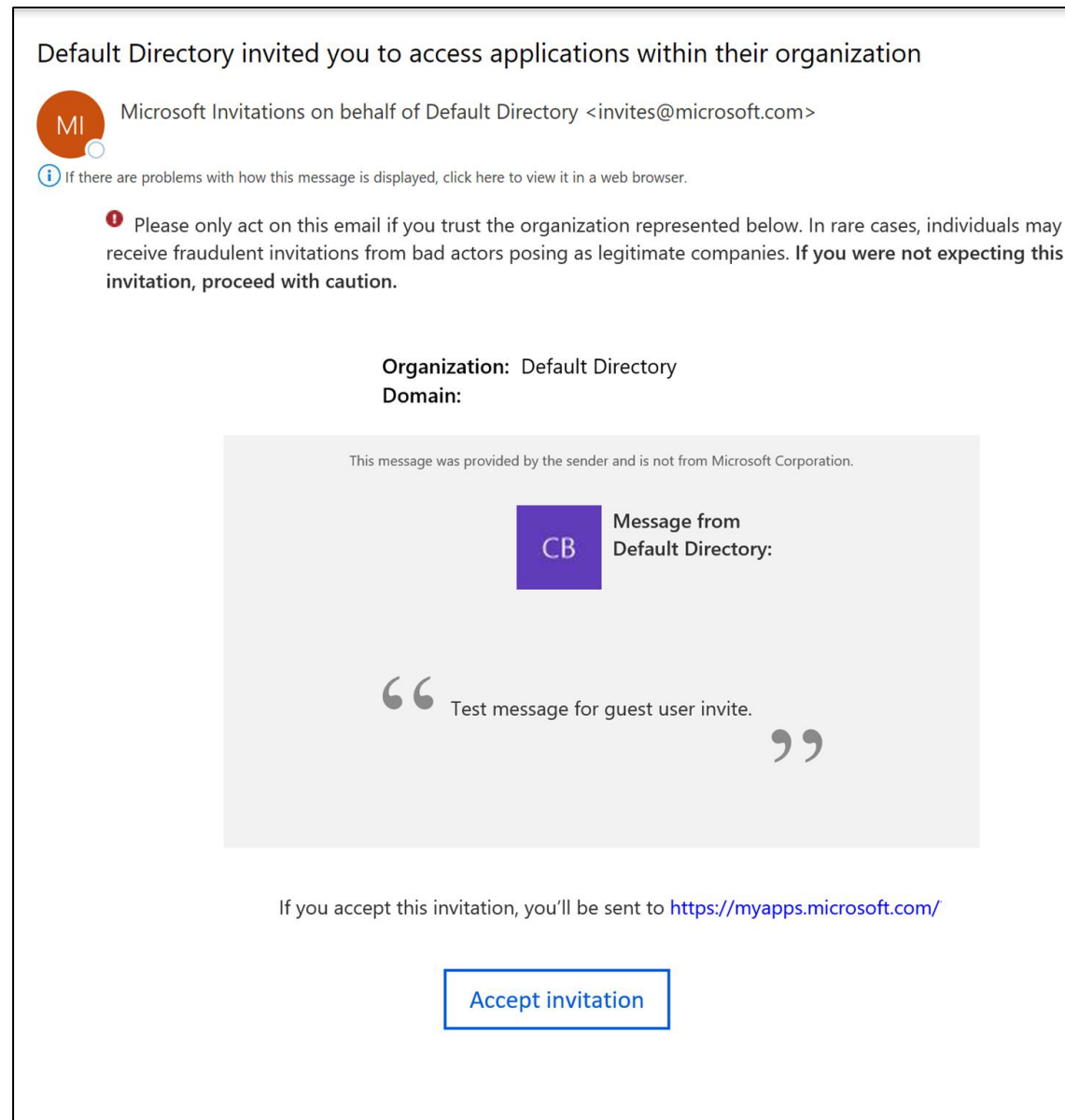
Identity

Name ⓘ	Example: 'Chris Green'
Email address * ⓘ	Example: <code>chris@contoso.com</code>
First name	
Last name	

- Fill out the appropriate fields, such as your **Name**, **Email address**, **Groups**, and **Directory role**.
- Now, click on **Invite** to send the invitation to the user.
- A notification stating **Successfully invited** will appear at the top right of your screen.
- After sending the invitation, the Guest user account is added to the directory.

Accept the Guest User Invite

Follow the instructions to accept a new user invite:



- Log in to your guest user's email account.
- In the inbox, locate the mail having the subject **You're invited**.
- Open the email, and click on **Get started**.
- Select **Accept Invitation**.

Assisted Practice

Azure AD Guest User Creation

Duration: 10 Min

Problem Statement:

You've been given the task of creating a guest user so that you can invite an external user to collaborate with your company by adding the user to your directory as a guest user.

Assisted Practice: Guidelines

Steps to create guest user in Azure AD:

1. Login to your azure portal
2. Select Azure Active Directory
3. Create New guest user from manage



Key Takeaways

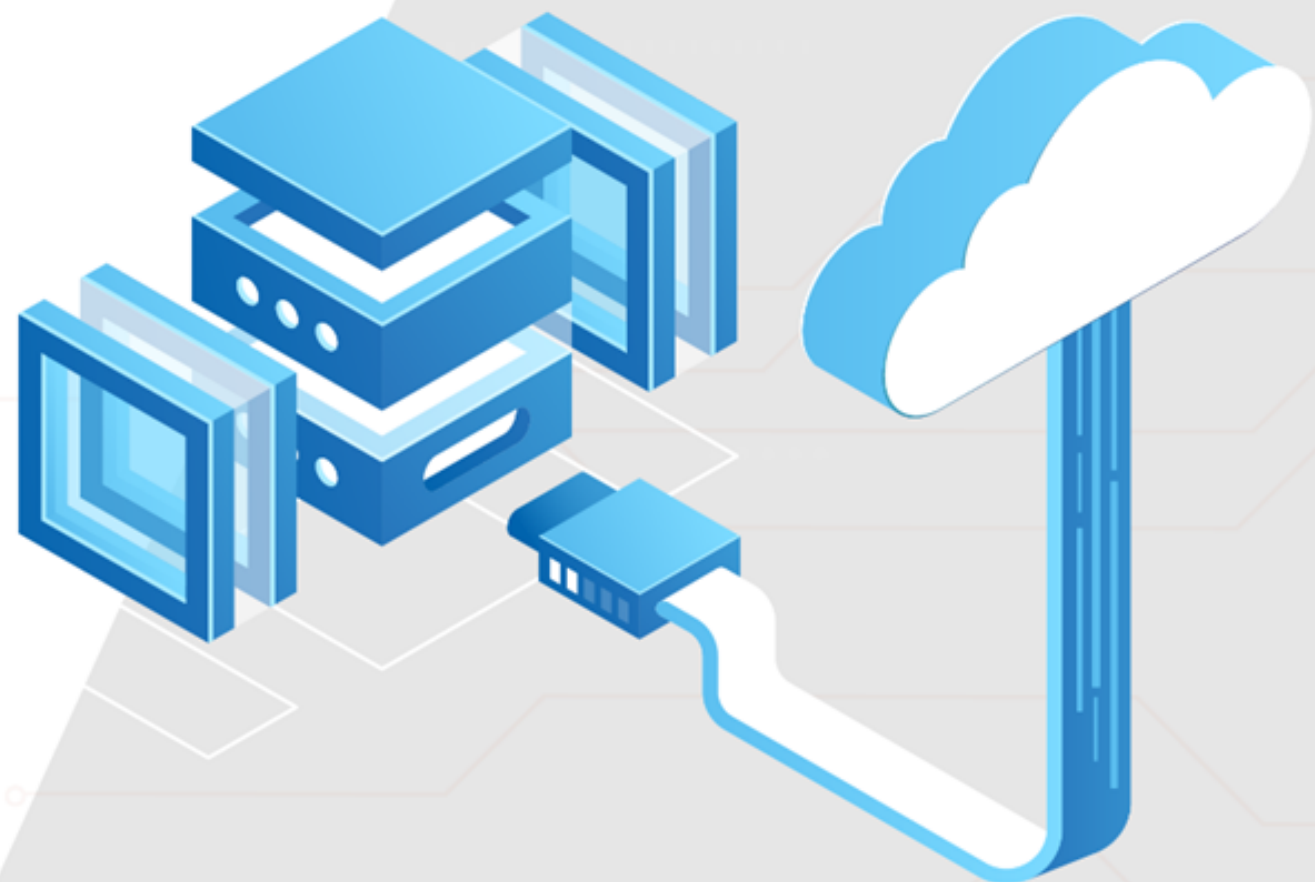
- Azure Active Directory is Microsoft's cloud-based identity and access management service.
- Azure Resource Manager is the service that manages and deploys Azure resources.
- Azure Management Groups provide an efficient way to manage access, policies, and compliance across an enterprise.
- A user account is used for the authentication and authorization during the sign-in process.



Key Takeaways

- An Azure service principal is an identity that can be used to access Azure resources.
- In Conditional Access policies if a user wants to access a resource, then they must complete an action.
- Multi-factor authentication is a process where a user is prompted during the sign-in process for an additional form of identification.





Thank you