



SC-300

# Microsoft Identity and Access Administrator

# SC-300 Agenda



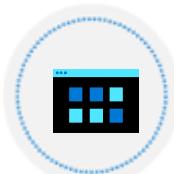
LP1: Implement an Identity Management Solution

Id  
external  
hybrid  
Id  
Id

2x RBAC



LP2: Implement an Authentication and Access Management Solution



LP3: Implement Access Management for Apps



LP4: Plan and Implement an Identity Governance Strategy

# Implement an Identity Management Solution



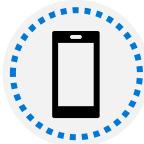
# Outline



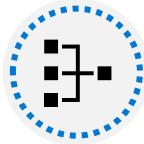
Create, configure, and manage identities



Configure and manage Azure Active Directory

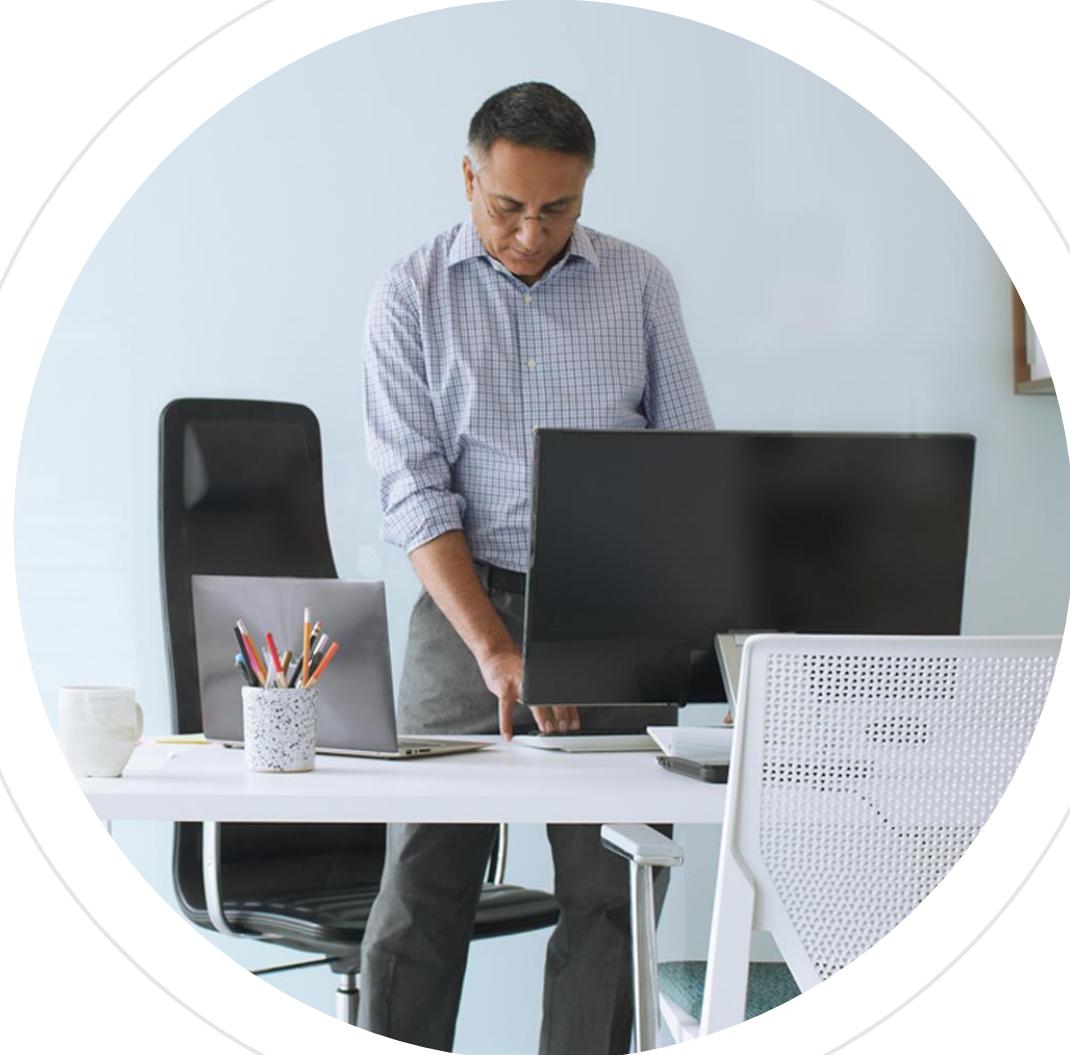


Implement and manage external identities



Implement and manage hybrid identity

# Create, configure, and manage identities



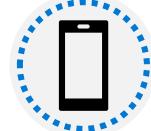
# Objectives



Create, configure, and manage users



Create, configure, and manage groups



Configure and manage device identities



Manage licenses



Custom security attributes



Provisioning using SCIM

# Create, configure, and manage users



# Create, configure, and manage users

- A user account contains all the information needed to authenticate the user during the sign-on process
- You use the **Azure Active Directory** dashboard in the Azure portal to work with user objects
- Three kinds of users:
  - Cloud identities
  - Directory-synchronized identities
  - Guest users

The screenshot shows the Azure Active Directory 'Users | All users' page for the Contoso tenant. The left sidebar includes links for 'All users' (which is highlighted with a red box), 'Deleted users', 'Password reset', 'User settings', and 'Diagnose and solve problems'. The main area displays a table of 35 users with columns for Name, User principal name, User type, Directory synced, Account enabled, and Creation type. The 'User type' column highlights 'Member' for most users, while 'Guest' is shown for Casey Jensen. A red box encloses the 'User type' header, and a red arrow points from the 'All users' link in the sidebar to the 'User type' header in the table.

Name	User principal name	User type	Directory synced	Account enabled	Creation type
Adele Vance	AdeleV	Member	No	Yes	
Alex Wilber	AlexW	Member	No	Yes	
Allan Deyoung	AllanD	Member	No	Yes	
Automate Bot	AutomateB	Member	No	Yes	
Bianca Pisani	BiancaP	Member	No	Yes	
Brian Johnson (TAI...)	BrianJ	Member	No	Yes	
Cameron White	CameronW	Member	No	Yes	
Casey Jensen	caseyj	Guest	No	Yes	Invitation
Christie Cline	ChristieC	Member	No	Yes	
Conf Room Adams	Adams	Member	No	Yes	

# User settings

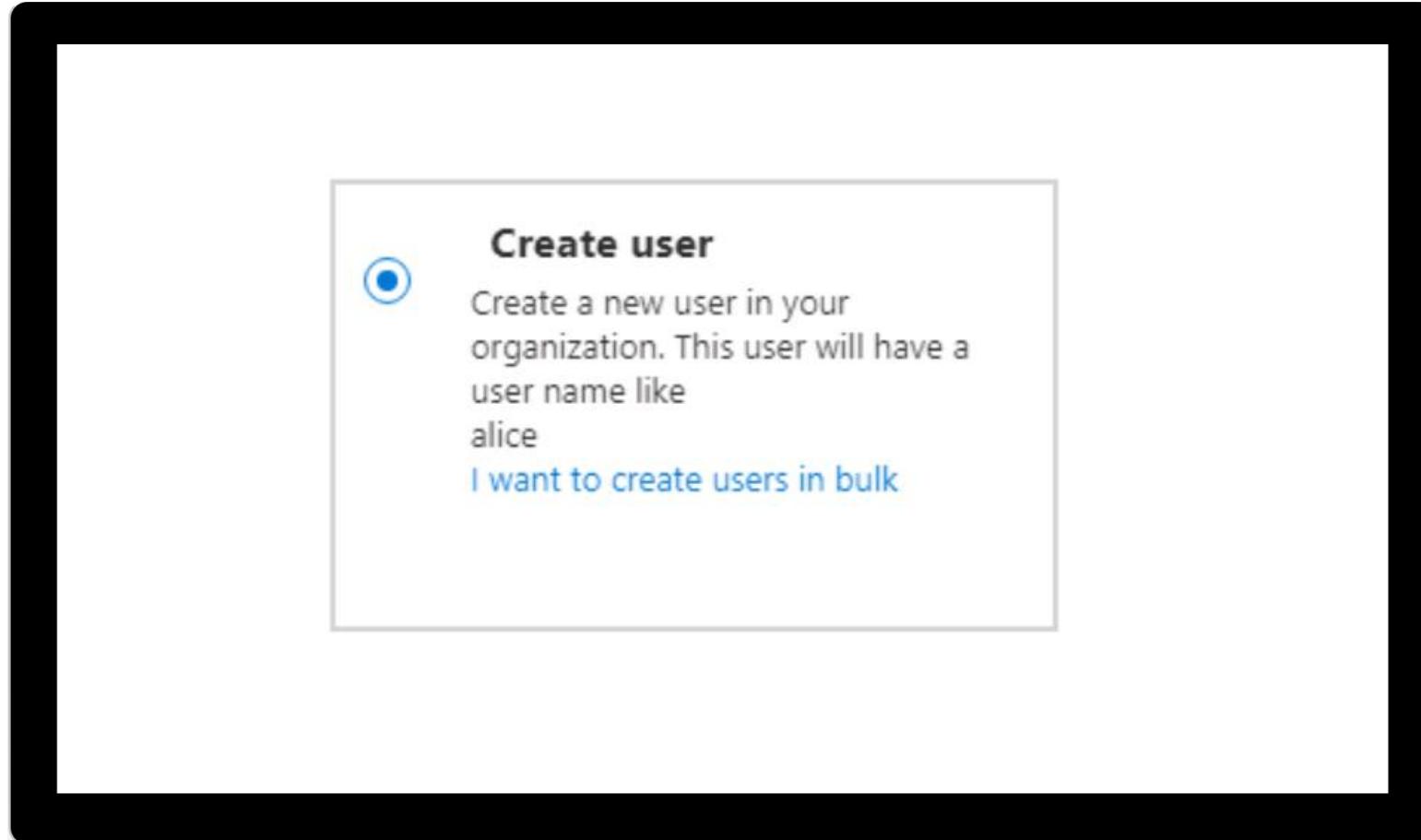
Some  
configurable  
user settings:

- Groups
- Licenses
- Devices
- Location

The screenshot shows the Azure portal interface for managing a user profile. The top navigation bar includes Home, Contoso, Users, and Adele Vance. The main title is "Adele Vance | Profile". On the left, a sidebar titled "Manage" lists several categories: Profile (selected), Custom security attributes (preview), Assigned roles, Administrative units (highlighted with a red box), Groups, Applications, Licenses (highlighted with a red box), Devices (highlighted with a red box), Azure role assignments, and Authentication methods. The main content area displays user details in a grid format. Adele Vance's information includes Name (Adele Vance), First name (Adele), Last name (Vance), User Principal Name (AdeleV), User type (Member), Object ID (redacted), and Issuer (Manage B2B collaboration). In the "Job info" section, Adele's Job title is Retail Manager, Department is Retail, and Manager is Miriam Graham. Under "Settings", Block sign in is set to No, and Usage location is United States (highlighted with a red box).

Name	Value	Manager
Name	Adele Vance	Miriam Graham
First name	Adele	
Last name	Vance	
User Principal Name	AdeleV	
User type	Member	
Object ID	(Redacted)	Manage B2B collaboration
Issuer		
Job title	Retail Manager	Department
Company name	---	Employee ID
---	---	---
Block sign in	No	Usage location
		United States

# Demo – Users



**Create user**

Create a new user in your organization. This user will have a user name like alice

[I want to create users in bulk](#)

# Create, configure, and manage groups



# Create, configure, and manage groups

## Security groups:

- Most common
- Manage access to shared resources for a group

## Microsoft 365 groups:

- Access shared mailbox, calendar, SharePoint, and more
- Give access to external people

Users and groups - All groups

Search (Ctrl+ /)

Search groups

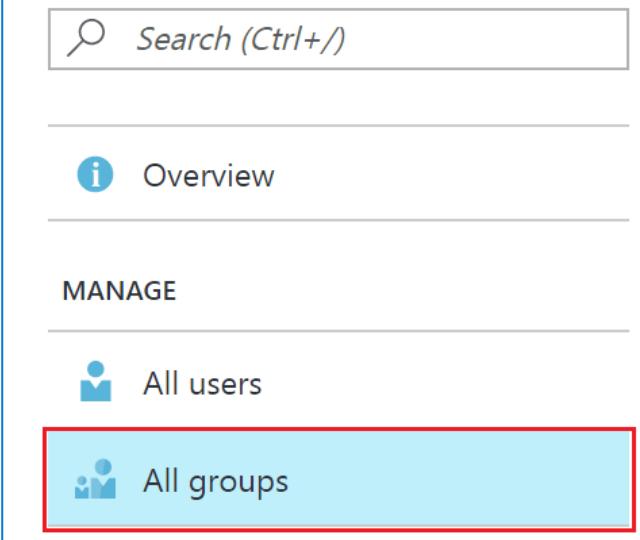
NAME	GROUP TYPE	MEMBERSHIP TYPE	
GR	Group1	Security	Assigned
GR	Group2	Security	Assigned
GR	Group23	Security	Assigned

Overview

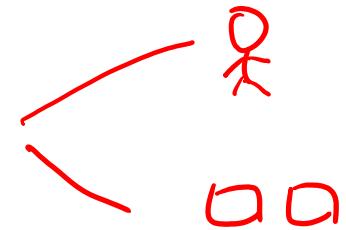
MANAGE

All users

All groups



# Dynamic Groups



- Special type of Security Group
- Membership dynamically generated via Membership Rule
  - UserType, department, region, and other items

Dynamic membership rules

Save Discard Got feedback?

Configure Rules

You can use the rule builder or rule syntax text box to create or edit a dynamic membership rule. [Learn more](#)

And/Or	Property	Operator	Value
And	<Choose a Property>	<Choose an Operat...>	Add a value
+ Add expression		+ Get custom extension properties	

Some items could not be displayed in the rule builder. [Learn more](#)

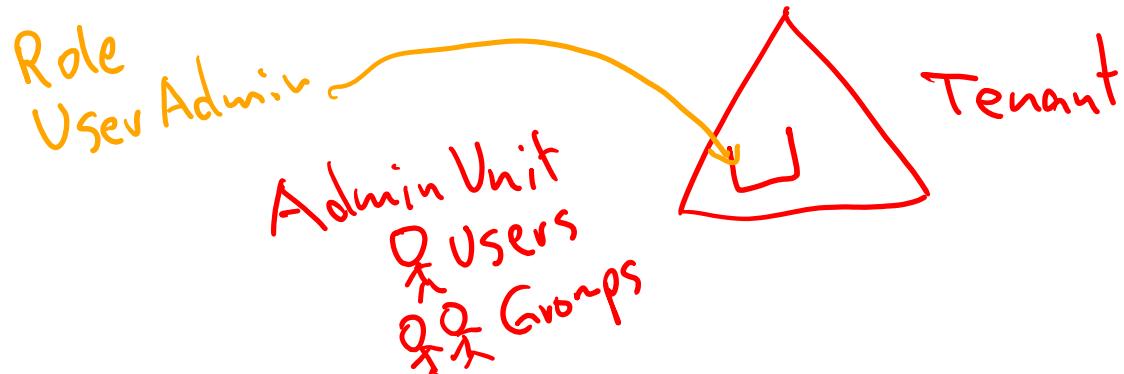
Rule syntax

```
user.ObjectId -ne null
```

# Group configuration options

Some configurable group settings:

- Properties
- Administrative units
- Group membership
- Roles and administrators



Home > Contoso > Groups >

**Legal Team** Group

Delete | Got feedback?

**Legal Team** LT

Membership type

Source

Type

Object Id

Created at

Email

Direct members

2 Total 2 User(s)

Group memberships

0

Overview

Diagnose and solve problems

Manage

Properties

Members

Owners

Roles and administrators

Administrative units

Group memberships

Applications

Azure role assignments

Activity

Access reviews

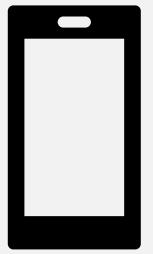
Audit logs

Bulk operation results

Troubleshooting + Support

New support request

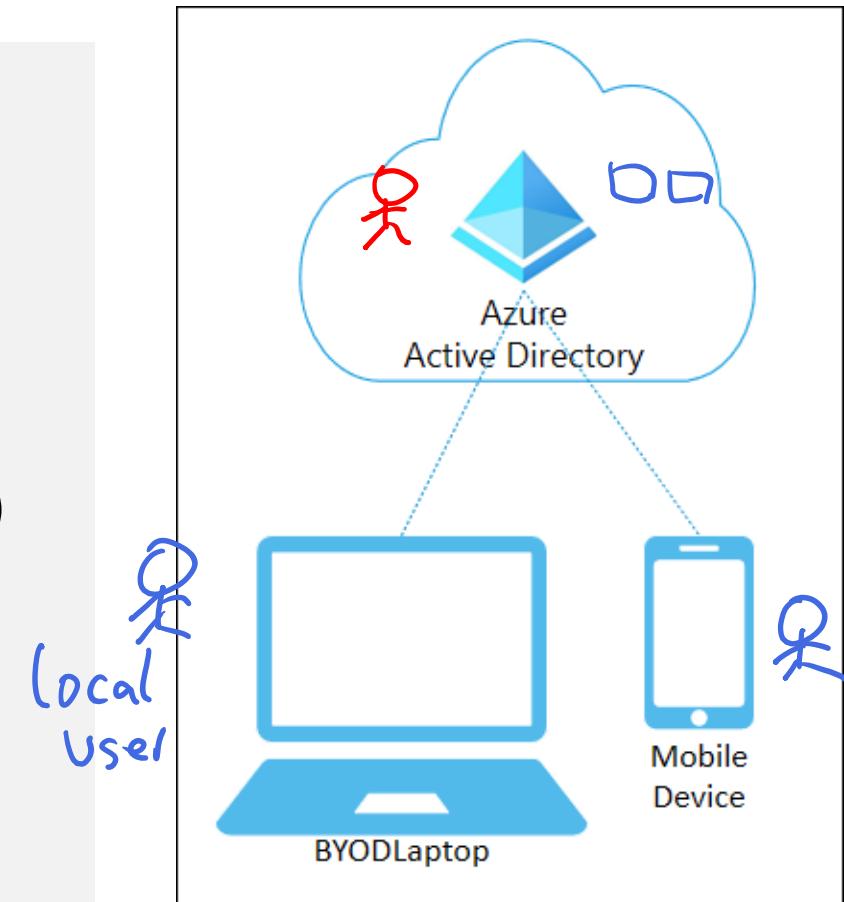
# Configure and mange device identities



# Azure AD registered devices

- Supports “BYOD” (bring your own device)
- Registered devices sign in using a local account
- Also attached to an Azure AD account granting access to organizational resources
- Control using Mobile Device Management (MDM) tools like Microsoft Intune **ME**

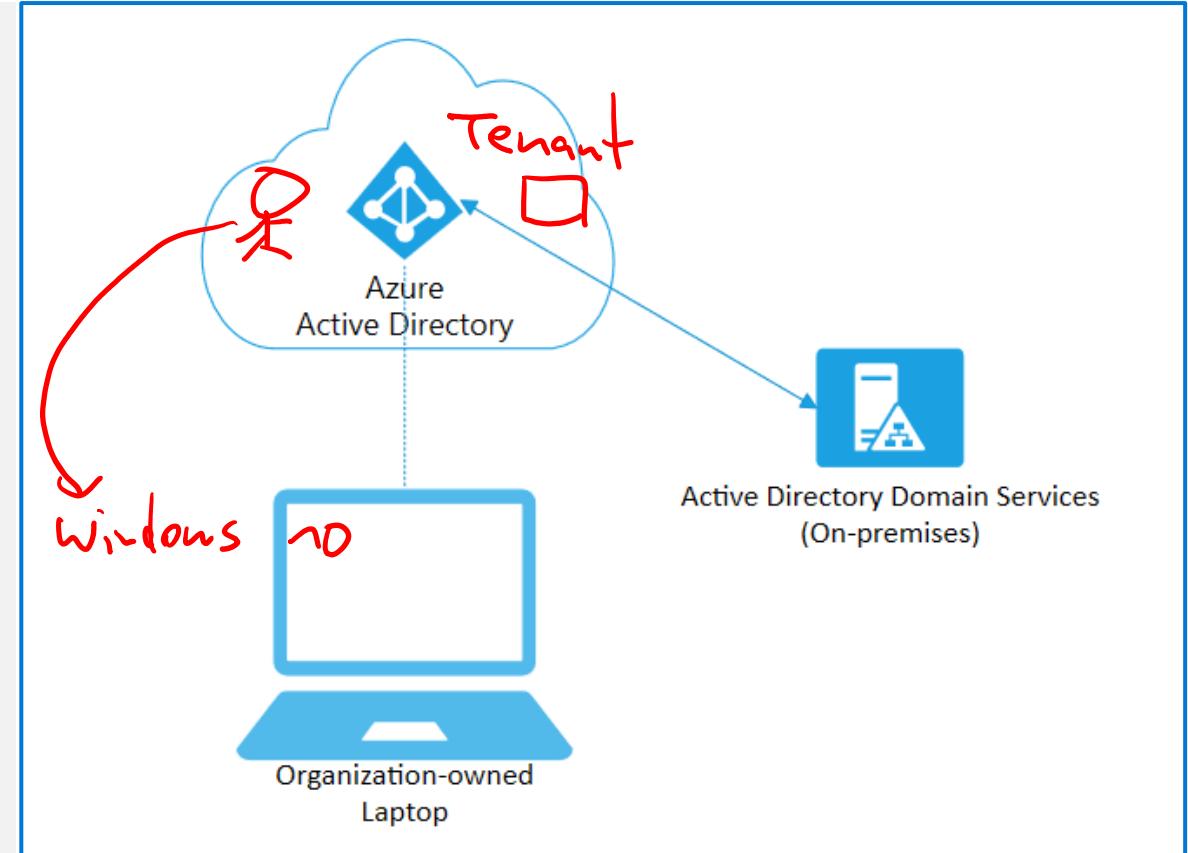
OS – Windows 10/11, iOS, Android, and MacOS



# Azure AD joined devices

- Intended for cloud-first or cloud-only organizations
- Organization-owned devices
- Joined only to Azure AD; organizational account required to sign in
- Conditional Access policies can be applied to the device identity

OS – Windows 10/11 devices (not Home)

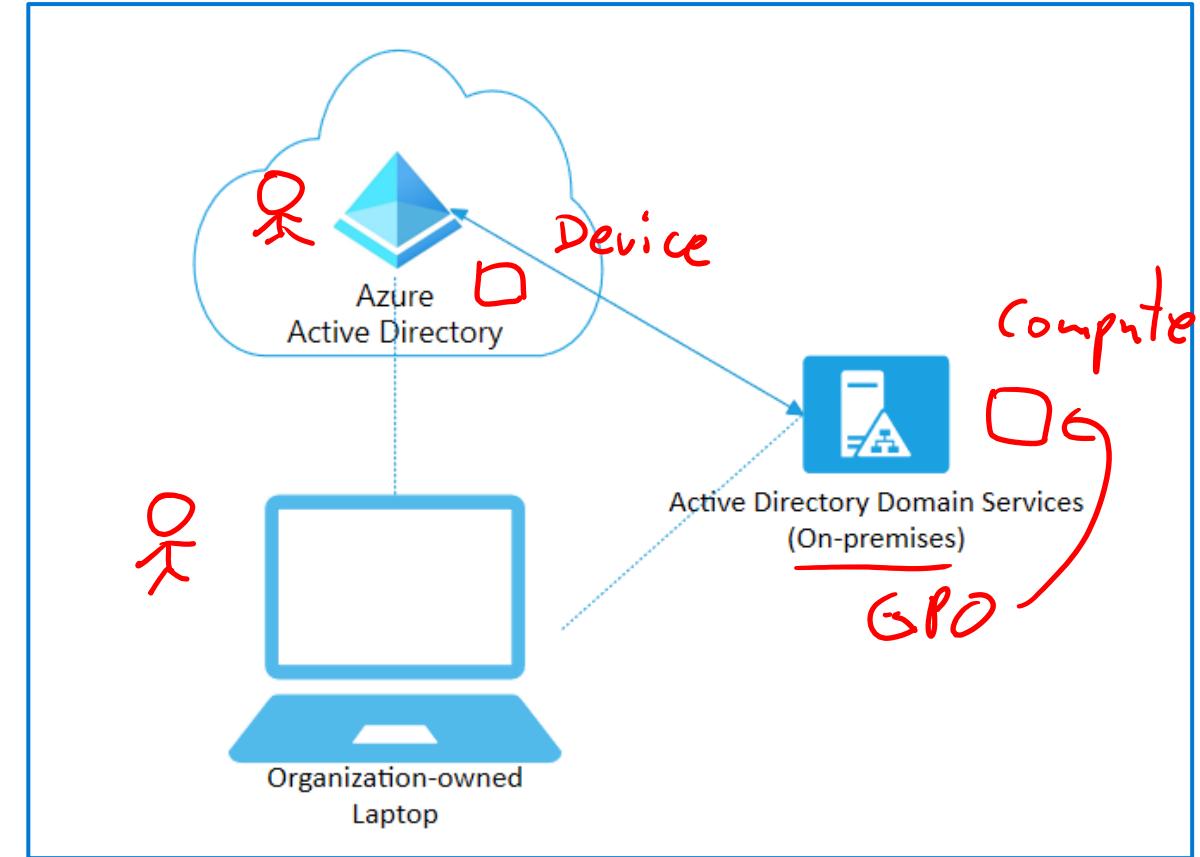


# Hybrid Azure AD joined devices

Use Azure AD hybrid joined devices if:

- You have Win32 apps deployed to these devices using Active Directory machine authentication
- You want to continue to use Group Policy to manage the device
- You want to use existing image solutions to deploy devices

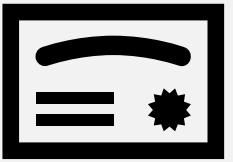
OS - Windows 7 and 8.1 devices in addition to Windows 10



# Device writeback

- Use Azure AD Connect to copy cloud registered device to the on-premises AD.
  - Copied into the **Registered Devices** container
- Used to enable device-based conditional access for ADFS-protected devices
- Provides extra security and assurance that access to applications is granted only to trusted devices
- Synchronizes all devices registered in Azure back to the on-premises Active Directory

# Manage licenses



# About licenses

Microsoft Azure is a cloud service that provides many built-in services for free.

- Azure AD comes as a free service
- Gain additional Azure AD functionality with a P1 or P2 license

Additional Services (like O365 are paid cloud services)

- Microsoft paid cloud services require licenses
- Licenses are assigned to each user who needs access to the services
- Each user requires a separate paid license
- Administrators use management portals and PowerShell cmdlets to manage licenses

# Group-based licensing

- You can assign one or more product licenses to a group
- Azure AD ensures that the licenses are assigned to all members of the group
- New group members are automatically assigned the appropriate licenses
- Licenses are removed from users when they leave the group
- Licenses can be assigned to any security group
- Administrators can disable service plans
- All Microsoft cloud services are supported
- Available only through the Azure portal
- Azure AD automatically modifies licenses based on group membership changes
- A user can be a member of multiple groups with license policies specified
- In some cases, licenses cannot be assigned to a user



# Custom security attributes

IOIO  
IOIO

# Manage custom security attributes (preview)

Business-specific attributes (key-value pairs) that you can define and assign to Azure AD objects.

Azure AD Premium P1 / P2

The screenshot shows the 'Contoso | Custom security attributes (Preview)' page in the Azure Active Directory portal. The left sidebar lists various management options, and the main area is titled 'New attribute'. A red box highlights the 'Custom security attributes (Preview)' option in the sidebar and the 'Add attribute set' button at the top. Another red box highlights the 'New attribute' form, which includes fields for Attribute name, Description, Data type (set to String), and settings for Allow multiple values and Only allow predefined values. The 'Predefined values' section is currently empty.

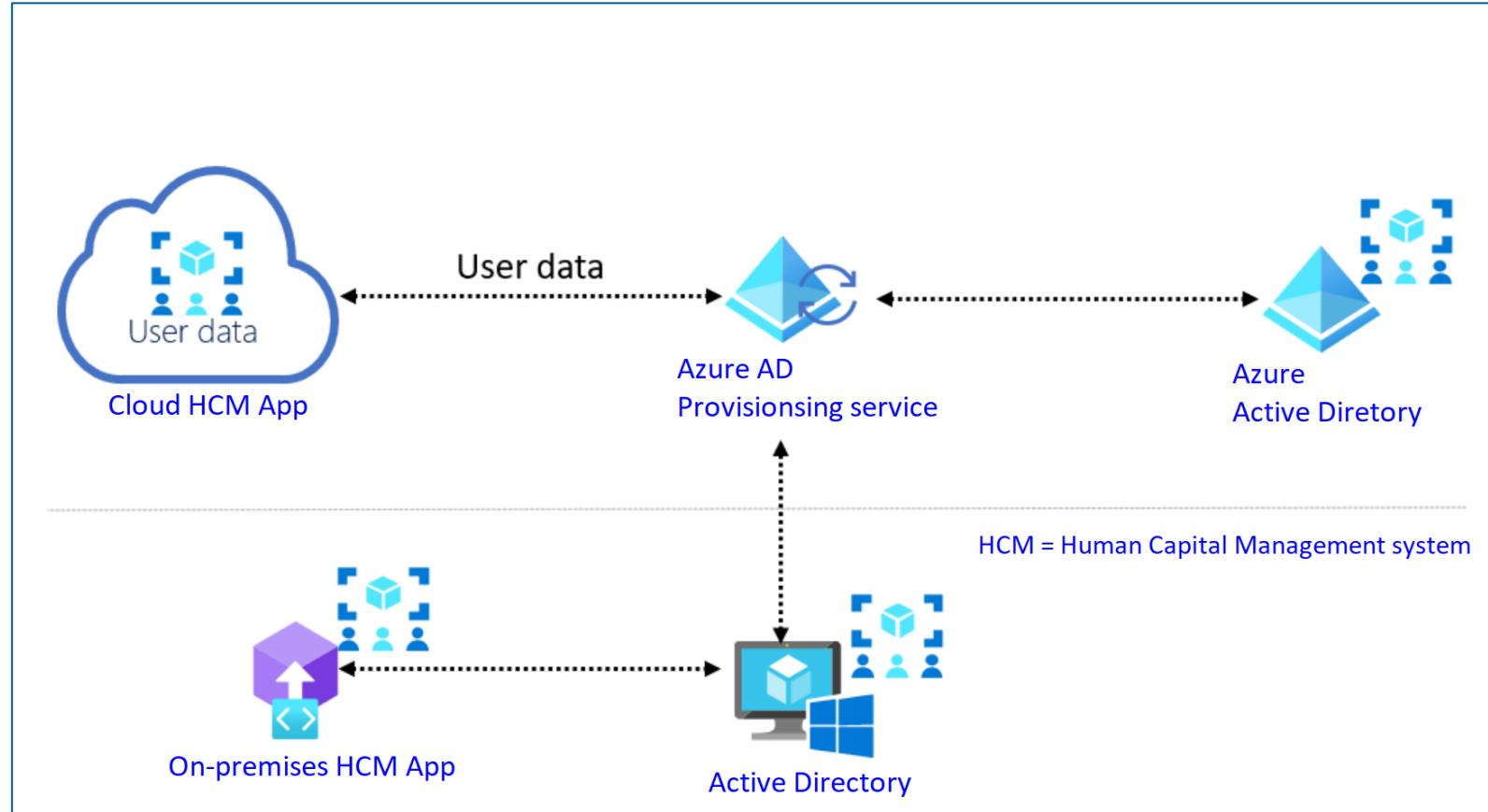
# Provisioning with SCIM



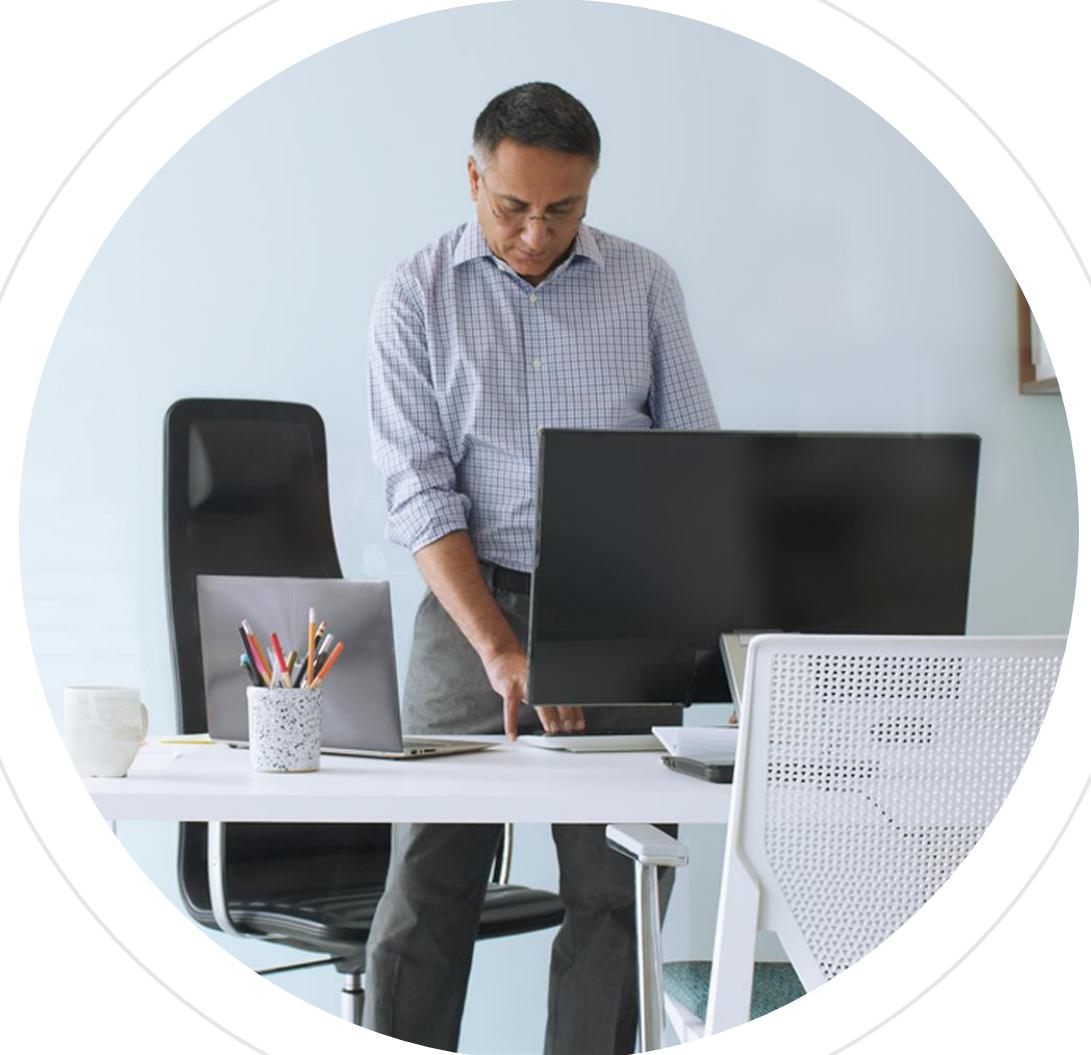
# Identity provisioning from cloud applications by using SCIM

**SCIM – System for Cross-Domain Identity Management**

**Use employee records to provision Azure AD accounts**



# Configure and manage Azure Active Directory tenant



# Objectives



Configure company branding



Configure and manage Azure Active Directory roles

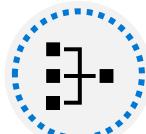
R B A C



Configure and manage custom domains



Configure and manage device registration



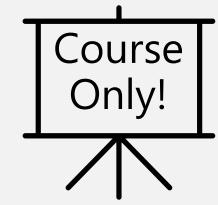
Configure delegation by using administrative units



Configure tenant-wide settings



# Company branding



# Company branding

Customize the Azure AD sign-in pages with company logos and other elements

- Require Azure AD P1/P2, or an M365 license
- Customize by language

Home > Contoso - Company branding > Configure company branding

Configure company branding  
Contoso

Save Discard Delete

Language Default

Sign-in page background image  
Image size: 1920x1080px  
File size: <300KB  
File type: PNG or JPG



Remove Select a file

Banner logo  
Image size: 280x60px  
File size: 10KB  
File type: Transparent PNG or JPG



Remove Select a file

Username hint  
Forgot your username?

Sign-in page text  
If you need help, contact the Help Desk online

This screenshot shows the 'Configure company branding' page for the 'Contoso' tenant in the Azure portal. It displays settings for customizing the Azure AD sign-in page, including a background image featuring two mobile phones with a keyhole icon, a banner logo placeholder for the Microsoft logo, and hints for forgot usernames and sign-in page text.

# Configure and manage Azure Active Directory roles



Global Admin

# Admin access to Azure and Azure AD

Azure Portal – <https://portal.azure.com>

Azure AD Admin Portal – <https://aad.portal.azure.com>

- Note – this portal is still active, but most of its functionality is available in modern portals like the Entra Admin Center and M365 Admin

**Entra Admin Center** – <https://entra.microsoft.com>

M365 Admin Center – <https://admin.microsoft.com>

Microsoft Defender for Cloud Apps Portal – <https://portal.cloudappsecurity.com>

- Formerly – Microsoft Cloud App Security (MCAS)

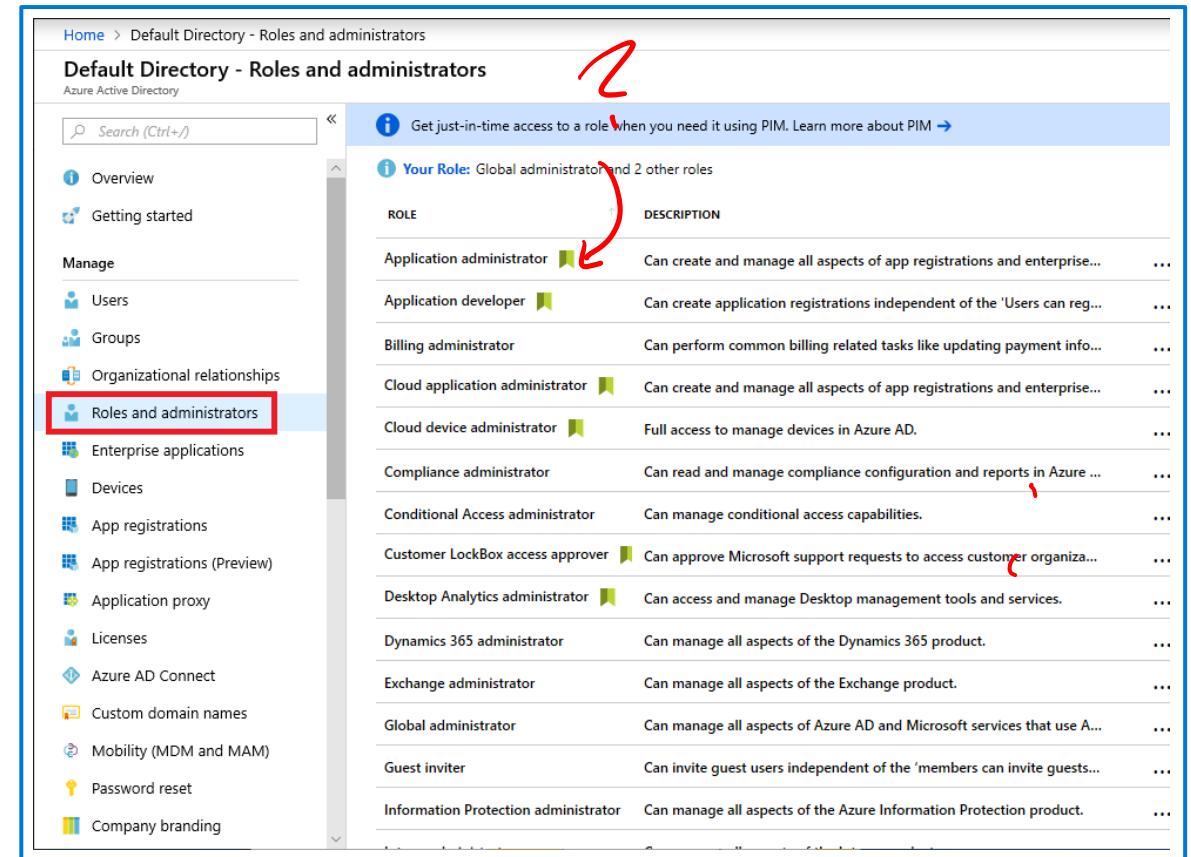
# Azure AD roles

## Intended for:

- IT admins
- App developers
- Microsoft 365, Office 365, Azure, or Dynamics CRM Online subscribers

Control permissions to manage Azure AD resources (vs. Azure roles, which control permissions to manage Azure resources)

Do not overlap with Azure roles by default



ROLE	DESCRIPTION
Application administrator	Can create and manage all aspects of app registrations and enterprise...
Application developer	Can create application registrations independent of the 'Users can reg...
Billing administrator	Can perform common billing related tasks like updating payment info...
Cloud application administrator	Can create and manage all aspects of app registrations and enterprise...
Cloud device administrator	Full access to manage devices in Azure AD.
Compliance administrator	Can read and manage compliance configuration and reports in Azure ...
Conditional Access administrator	Can manage conditional access capabilities.
Customer LockBox access approver	Can approve Microsoft support requests to access customer organizat...
Desktop Analytics administrator	Can access and manage Desktop management tools and services.
Dynamics 365 administrator	Can manage all aspects of the Dynamics 365 product.
Exchange administrator	Can manage all aspects of the Exchange product.
Global administrator	Can manage all aspects of Azure AD and Microsoft services that use A...
Guest inviter	Can invite guest users independent of the 'members can invite guests...
Information Protection administrator	Can manage all aspects of the Azure Information Protection product.

# Custom Roles

Create a custom role to meet your security goals or needs.

Requires an Azure AD premium license

The screenshot shows the 'MSODS Partner | Roles and administrators (Preview)' page in the Azure Active Directory. A red oval highlights the title 'Custom Roles' at the top left. On the left sidebar, under 'Manage', the 'Roles and administrators (Preview)' option is highlighted with a red box. At the top right, there is a red box around the '+ New custom role' button. A callout bubble above it says 'Get just-in-time access to a role when you need it using PIM. Learn more about'. The main area is titled 'New custom role' with tabs for 'Basics', 'Permissions', and 'Review + create'. The 'Basics' tab is selected. It shows fields for 'Name' (with a red box and a circled red arrow pointing to it), 'Description' (with a red box and a circled red arrow pointing to it), and 'Baseline permissions' (with a red box and a circled red arrow pointing to it). In the 'Permissions' tab, a permission 'microsoft.directory/applications/myOrganization/credentials/update' is selected, indicated by a checked checkbox and a red box around it. A red box also highlights the 'PERMISSION' checkbox itself.

# Assigning roles – to a user or group

Assign built-in or custom roles

Assign to a User, Group, Service Principal or Managed Identity

Use principle of Least Privilege when assigning

The screenshot shows the 'Assigned roles' section of the Azure portal for a user named Chris Green. The top navigation bar includes 'Home', 'Default Directory', 'Users', and 'Chris Green'. Below the navigation is a breadcrumb trail: 'Chris Green | Assigned roles'. On the left, there's a sidebar with 'Manage' options: 'Profile', 'Assigned roles' (which is selected and highlighted in grey), 'Administrative units', 'Groups', 'Applications', and 'Licenses'. At the top right, there are buttons for 'Add assignments' (highlighted with a green box), 'Remove assignments', 'Refresh', and 'Got feedback?'. The main content area is titled 'Administrative roles' with a sub-note: 'Administrative roles can be used to grant access to Azure AD and other Microsoft services.' A 'Search by name or description' input field and a 'Add filters' button are available. A table lists the assigned role: 'Application administrator' (with a checkbox icon) and a description: 'Can create and manage all aspects of app registrations'.

Role	Description
<input type="checkbox"/> Application administrator	Can create and manage all aspects of app registrations

# Assign users or groups to a role

Identities can be added to a role

Alternative method to assign roles

Use principle of Least Privilege when assigning

The screenshot shows the Microsoft Azure portal interface. On the left, there's a sidebar with navigation links: Home > Contoso > Billing administrator. Below this, under 'Manage', the 'Assignments' link is highlighted. A green box highlights the '+ Add assignments' button. An info message says 'You can also assign b...' and a search bar says 'Search by name'. The main area shows three user profiles: Adele Vance, Alex Wilber, and Allan Devouna. Underneath them is a section titled 'Selected items' which says 'No items selected'.

Home > Contoso > Billing administrator

Billing administrator | Assignments

All roles

+ Add assignments

Diagnose and solve problems

Manage

Assignments

Description

Activity

Bulk operation results

Troubleshooting + Support

New support request

You can also assign b...

Search by name

Name

No role assignments found

Adele Vance  
AdeleV@ Contoso .OnMicrosoft.com

Alex Wilber  
AlexW@ Contoso OnMicrosoft.com

Allan Devouna

Selected items

No items selected

# Assigning Azure roles to a Subscription or broader-scope

The screenshot shows the Azure portal interface for managing access control (IAM) in a resource group named 'cloud-shell-storage-westus'. The 'Role assignments' tab is active. A modal window titled 'Add role assignment' is open, showing fields for selecting a role and assigning it to a user or service principal. The main blade displays a summary of role assignments for the subscription.

Number of role assignments for this subscription	
0	

Add role assignment

Role: Select a role

Assign access to: User, group, or service principal

Select: Search by name or email address

Assign roles to manage Subscriptions, Management Groups, and Resource Groups

Roles

Policy

Sus

Sub 2

RG

# Using Azure AD roles for Common delegation scenarios

## Delegation scenarios:

- Restrict and manage application creation
- Assigning owners to an application
- Assigning a built-in administrative role that grants access to manage configuration in Azure AD for all applications
- Creating a custom role defining very specific permissions and assigning it to someone

When you delegate administrative tasks, you want to keep a few terms in mind:

**Least Privilege** - **Just in Time** - **Just long enough**

PIM

# Delegating administrative task with built-in roles

## Delegating app administration

- Application Administrator role |
- Cloud Application Administrator role

## Delegating app registration

- Application Developer role

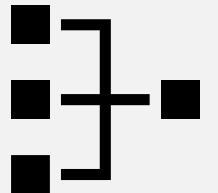
## Delegating app ownership

- Enterprise Application Owner role
- Application Registration Owner role

The screenshot shows the 'Default Directory | Roles and administrators' page in the Azure Active Directory portal. The left sidebar includes links for Overview, Preview features, Diagnose and solve problems, Manage (with options for Users, Groups, External Identities, Roles and administrators, Administrative units, and Enterprise applications), and a search bar. The main area displays 'Administrative roles' with a note about their purpose for granting access to privileged actions. It lists three roles: 'Application administrator' (selected, indicated by a checked checkbox), 'Application developer' (unchecked), and 'Attack payload author' (unchecked). There are also buttons for 'New custom role', 'Delete custom role', 'Refresh', and 'Print'.

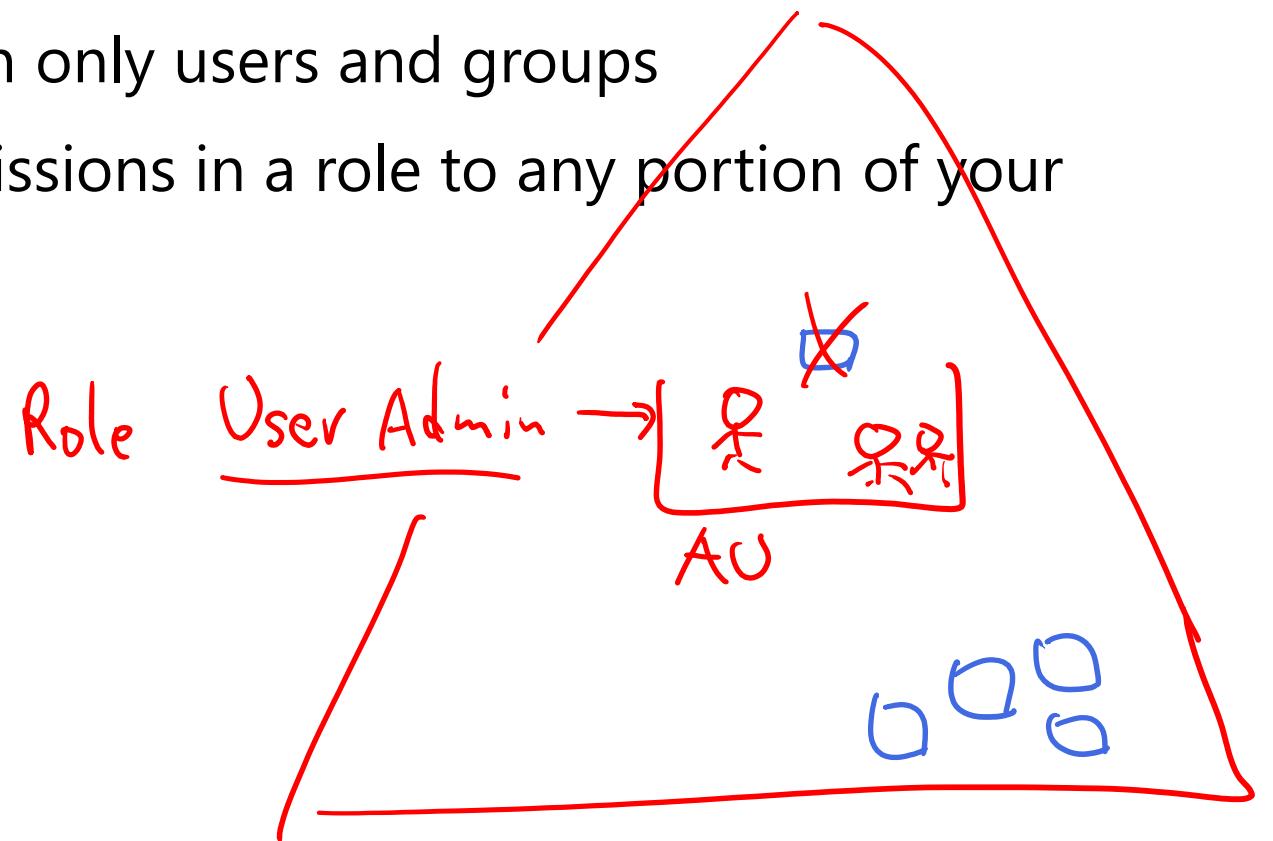
Role
<input checked="" type="checkbox"/> Application administrator
<input type="checkbox"/> Application developer
<input type="checkbox"/> Attack payload author

# Configure delegation by using administrative units



# About administrative units

- Administrative units are Azure Active Directory (Azure AD) resources that can be containers for other Azure AD resources
- An administrative unit can contain only users and groups
- Administrative units restrict permissions in a role to any portion of your organization that you define



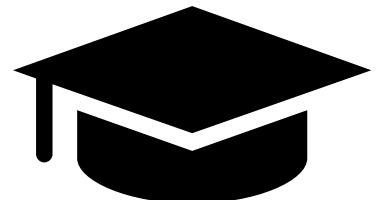
# Deployment scenario

**Large university composed of many autonomous schools (School of Business, School of Engineering, and so on)**

**Each school has a team of IT admins who control access, manage users, and set policies for their school**

**Administrative tasks could include:**

- Creating a role with administrative permissions over only Azure AD users in the business school administrative unit
- Creating an administrative unit for the School of Business
- Populating the administrative unit with only the business school students and staff
- Adding the business school IT team to the role, along with its scope



# Common delegation scenarios for Admin Units

## Delegation scenarios:

- Assigning types of authentication methods
- Creating a dedicated Helpdesk Admin
- Admin to control users and groups within the Admin Unit
- Setup a person that manages the licenses to tools and SaaS apps

**When you delegate administrative tasks, you want to keep a few terms in mind:**

**Least Privilege - Just in Time - Just long enough**

# Delegating administrative task with built-in roles

## Delegating authentication administration

- Authentication Administrator role

## Delegating licensing

- License Administrator

## Delegating user, group, and password management

- User Administrator

The screenshot shows the Azure Active Directory portal with the URL "Home > Default Directory". The main title is "Default Directory | Administrative units" under "Azure Active Directory". On the left, there is a navigation menu with icons for External Identities, Roles and administrators, Administrative units (which is selected and highlighted in grey), Enterprise applications, Devices, and App registrations. To the right of the menu, there is a search bar labeled "Search administrative units" and a form to enter a name, with "School of Engineering" typed into it. There are also "Learn more", "Add", and "Edit" buttons.

# Analyze Azure AD role permissions



# Permissions in Azure AD

**Permission – Consent or authorization to perform a specific action.**

Who / What gets permissions?			
Member Users	Guest Users	Applications	Devices
<b>Example default permissions for each:</b>			
<ul style="list-style-type: none"><li>• Enumerate list of user</li><li>• Invite guest users</li><li>• Change their password</li><li>• Manage Photo</li><li>• Create groups</li><li>• Etc.</li></ul>	<ul style="list-style-type: none"><li>• Read own properties</li><li>• Change their password</li><li>• Search for groups</li><li>• Cannot invite groups</li><li>• Etc.</li></ul>		

\* Augment or restrict permissions with settings and role assignments

# Augment or restrict permissions

The image shows two screenshots from the Azure portal. The left screenshot is titled 'Users | User settings' under 'Default Directory - Azure Active Directory'. It includes sections for 'Enterprise applications', 'App registrations', 'Administration portal', 'LinkedIn account connections', 'External users', and 'User features'. The 'Administration portal' section has two buttons: 'Yes' (highlighted with a red arrow) and 'No'. The 'LinkedIn account connections' section also has two buttons: 'Yes' (highlighted with a red arrow) and 'Selected group' (highlighted with a green circle). The right screenshot is titled 'Roles and administrators | All roles' under 'Default Directory - Azure Active Directory'. It lists various administrative roles: Application administrator, Application developer, Attack payload author, Attack simulation administrator, Attribute assignment administrator, Attribute assignment reader, Attribute definition administrator, and Attribute definition reader. The 'Application administrator' role is highlighted with a green circle.

Portal  
Shareable Links :443 → Bastion Host :3389 VM Q

# Analyze permission

## Role permission

Specific permissions granted when role assigned to a user or group.

## Guest / Service principal

Additional permission given to ensure a basic level of functionality when assigned to guest users or service principals.

The screenshot shows the Azure portal interface for managing roles. On the left, a sidebar menu includes 'Diagnose and solve problems', 'Assignments', and 'Description' (which is selected). Below these are sections for 'Activity' (with 'Bulk operation results') and 'Troubleshooting + Support' (with 'New support request'). The main content area has a title 'Attribute definition reader | Description' and a 'Summary' section. It lists the role's name ('Attribute definition reader'), description ('Users with this role can read the definition of custom security attributes.'), template ID ('1d336d2c-4ae8-42ef-9711-b3604ce3fc2c'), and a related article link ('Assigning administrator roles in Azure Active Directory'). A 'Role permissions' section follows, listing various API permissions and their descriptions:

API Permission	Description
microsoft.directory/attributeSets/allProperties/read	Read all properties of attribute sets.
microsoft.directory/customSecurityAttributeDefinitions/allProperties/read	Read all properties of custom security attribute definitions.
This role also grants the following <a href="#">basic read permissions</a> to guests and service principals	
microsoft.directory/administrativeUnits/standard/read	Read basic properties on administrative units.
microsoft.directory/administrativeUnits/members/read	Read members of administrative units.
microsoft.directory/applications/standard/read	Read standard properties of applications.
microsoft.directory/applications/owners/read	Read owners on all types of applications.
microsoft.directory/applications/policies/read	Read applications.policies property in Azure Active Directory.
microsoft.directory/contacts/standard/read	Read basic properties on contacts in Azure Active Directory.

# Configure and manage custom domains



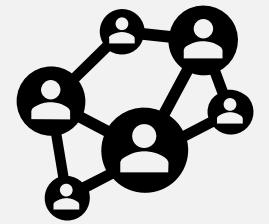
# Adding a custom domain name

- Every new tenant has a default domain name ending in .onmicrosoft.com
- You can add your own custom domain name and make it the primary domain name
- You can add multiple custom domain names for an organization
- You must add a root domain before adding subdomains

The screenshot shows the 'Custom domain names' blade in the Azure Active Directory portal for the 'Fabrikam' tenant. The left sidebar lists various management options, with 'Custom domain names' highlighted by a red box at the bottom. The main area displays a table with one row for 'fabrikam.onmicrosoft.com', which is marked as 'Available'. A red box highlights the '+ Add custom domain' button in the top right corner of the table header.

NAME	STATUS	FEDERATED	PRIMARY
fabrikam.onmicrosoft.com	Available		✓

# Configure tenant-wide setting



# Tenant-wide settings

- Tenant-wide settings apply to the entire tenant when set
- These global values set some default behaviors to be applied to all users and properties
- Manage members and guest users:
  - Register applications
  - Restrict access to Azure AD administrative portal
- Sign in with LinkedIn
- Manage security defaults
- External Collaboration
  - Restricting who can invite guest and other settings

# User settings

Azure Portal → Azure AD → Users → User Settings

- App registrations – users can register applications
- Administration portal – restrict access to the Azure AD administration portal
- LinkedIn account connections – Allow users to connect their work or school account with LinkedIn
- Other

The screenshot shows the 'User settings' section of the Azure Active Directory (Azure AD) portal. The left sidebar lists various administrative options: External Identities, Roles and administrators, Administrative units, Enterprise applications, Devices, App registrations, Identity Governance, Application proxy, Licenses, Azure AD Connect, Custom domain names, Mobility (MDM and MAM), Password reset, Company branding, User settings (which is selected and highlighted in grey), Properties, and Security. The main content area is titled 'Default Directory | User settings'. It includes sections for 'Enterprise applications' (Manage how end users launch and view their applications), 'App registrations' (Users can register applications with Yes selected), 'Administration portal' (Restrict access to Azure AD administration portal with Yes selected), 'LinkedIn account connections' (Allow users to connect their work or school account with LinkedIn, with a note that data sharing is not enabled until users learn more about LinkedIn account connections), and 'External users' (Manage external collaboration settings). At the top right, there are 'Save' and 'Discard' buttons.

# User settings – External Users

Azure Portal → Azure AD → Users → User Settings

- App registrations – users can register applications
- Administration portal – restrict access to the Azure AD administration portal
- LinkedIn account connections – Allow users to connect their work or school account with LinkedIn
- Manage user feature previews
- External Collaboration setting

The screenshot shows the 'External collaboration settings' section of the Azure AD User Settings. At the top, there's a navigation bar with 'Home > Default Directory > External collaboration settings ...'. Below it are 'Save' and 'Discard' buttons. A purple banner at the top right says 'Email one-time passcode for guests has been moved to All Identity Providers.' A note indicates that the 'Guest user access' setting has changed from 'most inclusive' to 'most restrictive'. The 'Guest user access' section shows three options: 'Guest users have the same access as members (most inclusive)', 'Guest users have limited access to properties and memberships of directory objects', and 'Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)', with the third option selected. The 'Guest invite settings' section shows four options: 'Anyone in the organization can invite guest users including guests and non-admins (most inclusive)', 'Member users and users assigned to specific admin roles can invite guest users including guests with member permissions', 'Only users assigned to specific admin roles can invite guest users', and 'No one in the organization can invite guest users including admins (most restrictive)', with the second option selected. The 'Enable guest self-service sign up via user flows' section has a 'Yes' button (disabled) and a 'No' button (selected). A copyright notice at the bottom reads '© Copyright Microsoft Corporation. All rights reserved.'

# Tenant properties

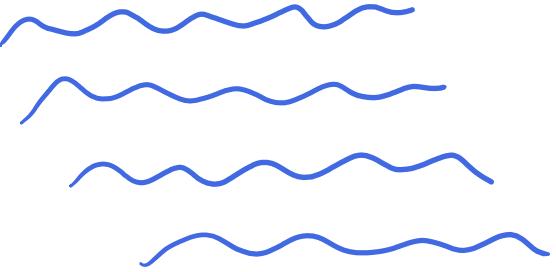
Azure Portal → Azure AD → Properties

- Changing the tenant display name
- Finding the country or region associated with your tenant
- Finding the location associated with your tenant
- Tenant ID and Technical Contact
- Global privacy contact
- Privacy statement URL

The screenshot shows the 'Default Directory | Properties' page in the Azure Active Directory portal. The left sidebar lists various management options: External Identities, Roles and administrators, Administrative units, Enterprise applications, Devices, App registrations, Identity Governance, Application proxy, Licenses, Azure AD Connect, Custom domain names, Mobility (MDM and MAM), Password reset, Company branding, User settings, Properties (which is selected and highlighted in blue), and Security. The main right pane displays the 'Tenant properties' section with the following fields:

- Name: Default Directory
- Country or region: United States
- Location: United States datacenters
- Notification language: English
- Tenant ID: (empty field)
- Technical contact: (empty field)
- Global privacy contact: (empty field)
- Privacy statement URL: (empty field)

At the top right of the main pane, there are 'Save' and 'Discard' buttons.



# Implement and manage external identities



# Objectives



Describe guest users and B2B Accounts



Manage external collaboration



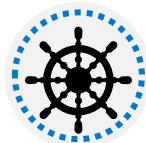
How external users are managed in Microsoft 365



Invite external users – individually or in bulk



Manage external user accounts in Azure Active Directory



Implement cross-tenant access controls

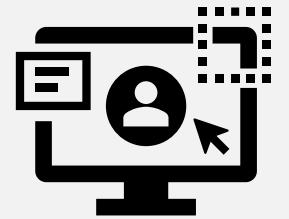


Configure identity providers



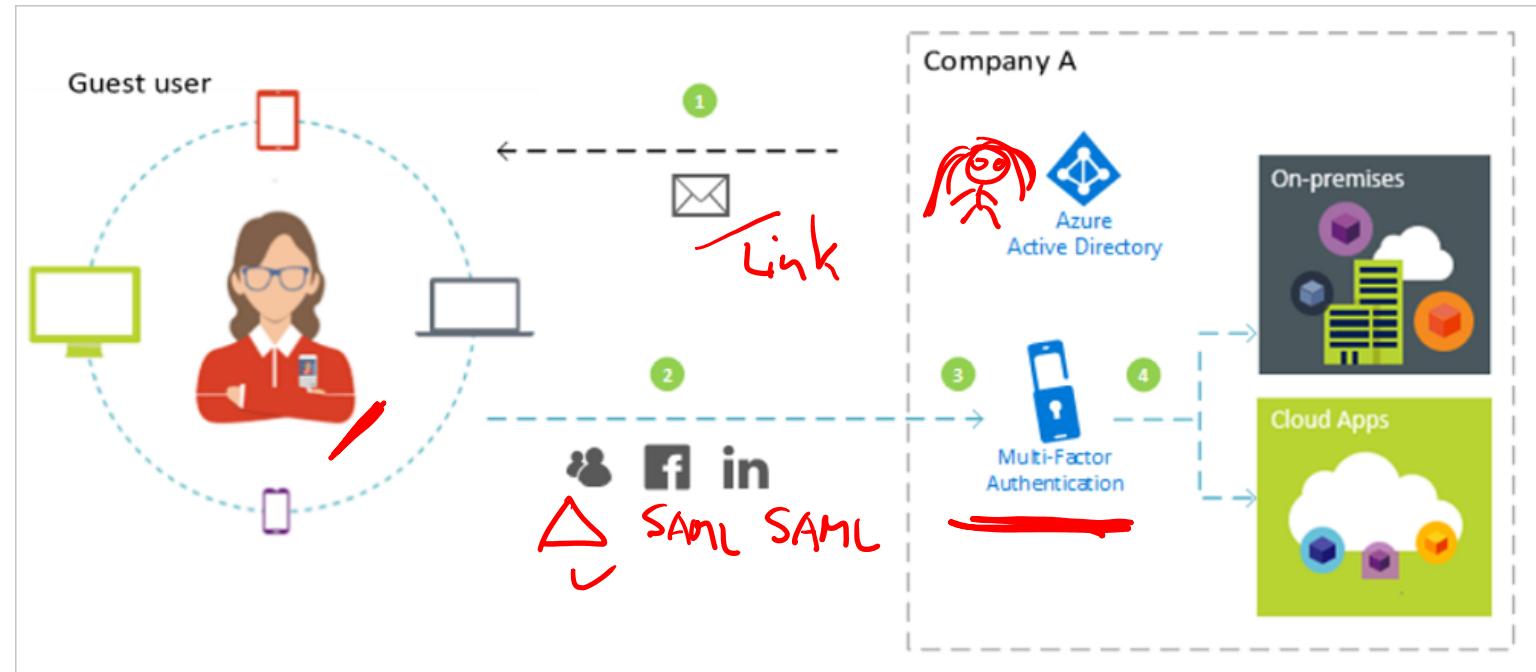
Implement and manage Verified ID

Describe guest user and B2B accounts  
&  
Manage external collaboration



# Azure Active Directory B2B

- Guest user – an external user invited to join your corporate Azure AD.
- Sourced from another AD, Social Media, partners, and other services.
- Secure B2B collaboration projects enabled.



# Collaborating with external users

- Invite external users into your tenant as guests
- External users use their existing credentials for authentication
- They are assigned permissions for authorization
- You can restrict what external users can see and do

# External users from M365 Workloads



# Microsoft 365 admin center

- Manage guest users in the Microsoft 365 admin center.
- Similar process to Azure AD.
- Always use Zero Trust principles when managing.

The screenshot shows the Microsoft 365 admin center interface. The top navigation bar includes the organization name "Contoso Electronics", the title "Microsoft 365 admin center", and a search bar. The left sidebar has a "Guest users" section selected, showing a list of users: Home, Users, Active users, Contacts, Guest users (selected), Deleted users, Teams & groups, Billing, Setup, and Show all. The main content area is titled "Guest users" and displays a message about guest access to Teams. It includes a "Add a guest user" button and a "Refresh" link. A table lists one guest user: Chris Green, with an email address of ChrisG@anexternalemail.com. There are "Display name" and "Email Address" columns, and a "Choose columns" link.

Display name	Email Address	Choose columns
Chris Green	ChrisG@anexternalemail.com	[...]

# External collaboration options in Microsoft 365

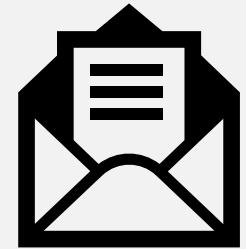
Activity	Account type	Default setting
Authenticated file and folder sharing	Guest account	Enabled
Site sharing	Guest account	Enabled
Team sharing	Guest account	Enabled
Shared channel in Teams	Existing Microsoft 365 external account	Disabled
External chat and meetings	Existing Microsoft 365 external account	Enabled
Anonymous meeting join	None	Enabled
Unauthenticated file and folder sharing	None	Enabled

# Granting / removing guest access

- Configure at the workload admin level.
- Always have a governance process in place.
- Always use Zero Trust principles when managing.

The screenshot shows the Microsoft Teams Admin Center interface for 'Contoso Electronics'. The left sidebar has a dark theme with white icons and text. The 'Guest access' option is highlighted with a purple background. The main content area is titled 'Guest access' and explains that it lets people outside the organization access teams and channels. It includes sections for 'Allow guest access in Teams' (set to 'On'), 'Calling' (with a note about managing calling settings for guests), 'Make private calls' (switched to 'On'), and 'Meeting' (with a note about turning on or off settings for guests in meetings).

**Invite external users – individually or in bulk**



# Inviting users



## Inviting users individually:

- Any user (even a guest) can invite guest users by default
- Inviter sends the guest a direct link to the app being shared
- Application owners can manage their own guest users



## Inviting users in bulk:

- Prepare a .csv file with user information and invitation preferences
- Upload the .csv file to Azure AD

# Manage external user accounts in Azure Active Directory



# Guest Users – restricted by default

Guest users do not have:

- Assigned roles ~~—~~
- Group membership
- Licenses

Or other capabilities by default.  
Grant access as your security  
posture and organization needs  
dictate.

The screenshot shows the Microsoft Azure portal interface for managing user assignments. At the top, the navigation path is Home > Contoso > Users > Sam Oogle. The main title is "Sam Oogle | Assigned roles". Below the title, there is a "User" icon and a "Diagnose and solve problems" link. On the right, there are buttons for "Add assignments", "Refresh", and "Got it". There are two tabs: "Eligible assignments" and "Active assignments", with "Active assignments" being the active tab. A search bar "Search by role" is present. The left sidebar lists several categories: Profile, Assigned roles (which is selected and highlighted in grey), Administrative units, Groups, Applications, Licenses, Devices, Azure role assignments, and Authentication methods. The "Assigned roles" section under "Manage" contains a table with columns for Role, Principal name, and Status. The table shows one row: "No results". The bottom section is titled "Activity" and includes links for Sign-ins and Audit logs.

# Provide the Guest User the least privilege access needed

Add guest to:

- “Assign Roles” just as with normal users.

You can add Guests to groups as well.

Home > Contoso > Users > Sam Oogle >

## Add assignments

Privileged Identity Management | Azure AD roles

Membership    Setting

Resource: Contoso

Resource type: Directory

Select role (i)

Search role

Select member(s) \* (i)  
1 Member(s) selected

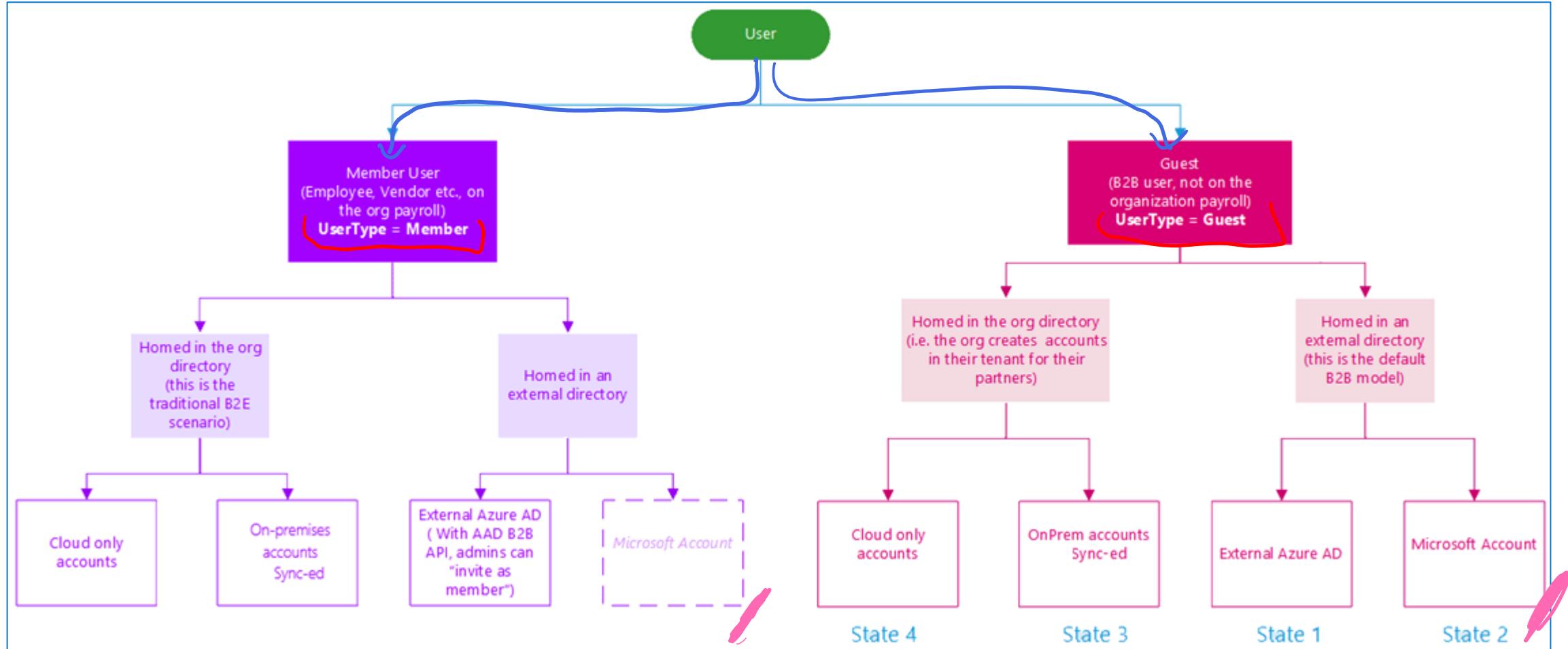
Selected member(s) (i)

Sam Oogle

Search role by name

- Groups Administrator
- Guest Inviter
- Helpdesk Administrator
- Hybrid Identity Administrator
- Identity Governance Administrator
- Insights Administrator
- Insights Business Leader
- Intune Administrator
- Kaizala Administrator
- Knowledge Administrator
- Knowledge Manager

# B2B user states



# Cross-tenant access controls



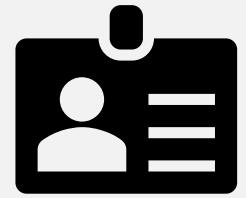
# Configure cross-tenant access controls

- Default – applied to all external collaboration.
- Organizational settings – add rules by specific tenant / tenant-id.
- Microsoft cloud – control access to Azure Government clouds.

The screenshot shows the 'External Identities' blade in the Azure portal for the 'Contoso - Azure Active Directory' tenant. The 'Cross-tenant access settings (Preview)' tab is selected. The page displays two main sections: 'Inbound access settings' and 'Outbound access settings'. Under 'Inbound access settings', there is a table showing default settings for various collaboration types. Under 'Outbound access settings', there is a link to edit defaults.

Type	Applies to	Status
B2B collaboration	External users and groups	All allowed
B2B collaboration	Applications	All allowed
B2B direct connect	External users and groups	All blocked
B2B direct connect	Applications	All blocked
Trust settings	N/A	Disabled

# Configure identity providers



# SAML / WS-Fed

- You can set up direct federation with any organization that supports SAML 2.0 or WS-Fed
- Any new guests will be authenticated using direct federation
- Guest users sign in using their own organizational account

# SAML / WS-Fed identity provider configuration

Home > Contoso > External Identities

## External Identities | All identity providers

Contoso - Azure Active Directory

Search (Ctrl+I)



Google

Facebook

New SAML/WS-Fed IdP

Got feedback?

Overview

Cross-tenant access settings  
(Preview)

All identity providers

External collaboration settings

Diagnose and solve problems

Self-service sign up

Custom user attributes

All API connectors

User flows

Subscriptions

Linked subscriptions

Lifecycle management

### Configured identity providers

Name

Azure Active Directory

Microsoft Account

Email one-time passcode

### SAML/WS-Fed identity providers

Search

Search by domain name

Display name

Configuration

Domains

You have not added a SAML/WS-Fed identity provider

### New SAML/WS-Fed IdP

You must configure the federating identity provider first. →

Display name \*

Select protocol

Identity provider protocol \*

Select protocol

SAML

WS-Fed

Domain name of federating IdP \*

fabrikam.com

Select a method for populating metadata \*

Select method

Select method

Parse metadata file

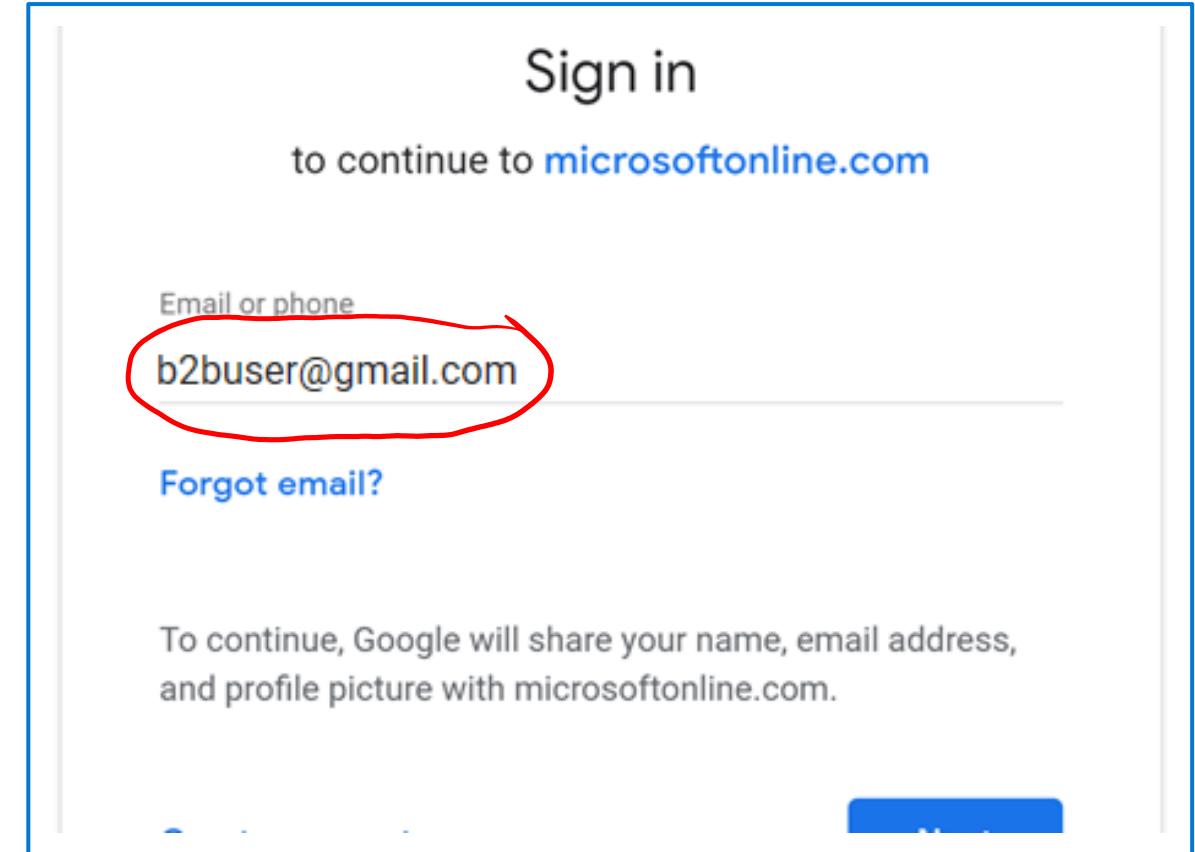
Input metadata manually

Save

Cancel

# Using Google as an identity provider

- Guest users who aren't signed in to Google will be prompted to do so
- Guest users who are already signed in to Google will be prompted to choose the account they want to use
- They must choose the account you used to invite them



# Using Facebook as an identity provider

- To use a Facebook account as an identity provider, you must create an application in the Facebook developers' console
- Set the Facebook client ID and client secret using either the Azure AD portal or PowerShell
- You can test your Facebook configuration by signing up via a user flow on an app enabled for self-service sign-up

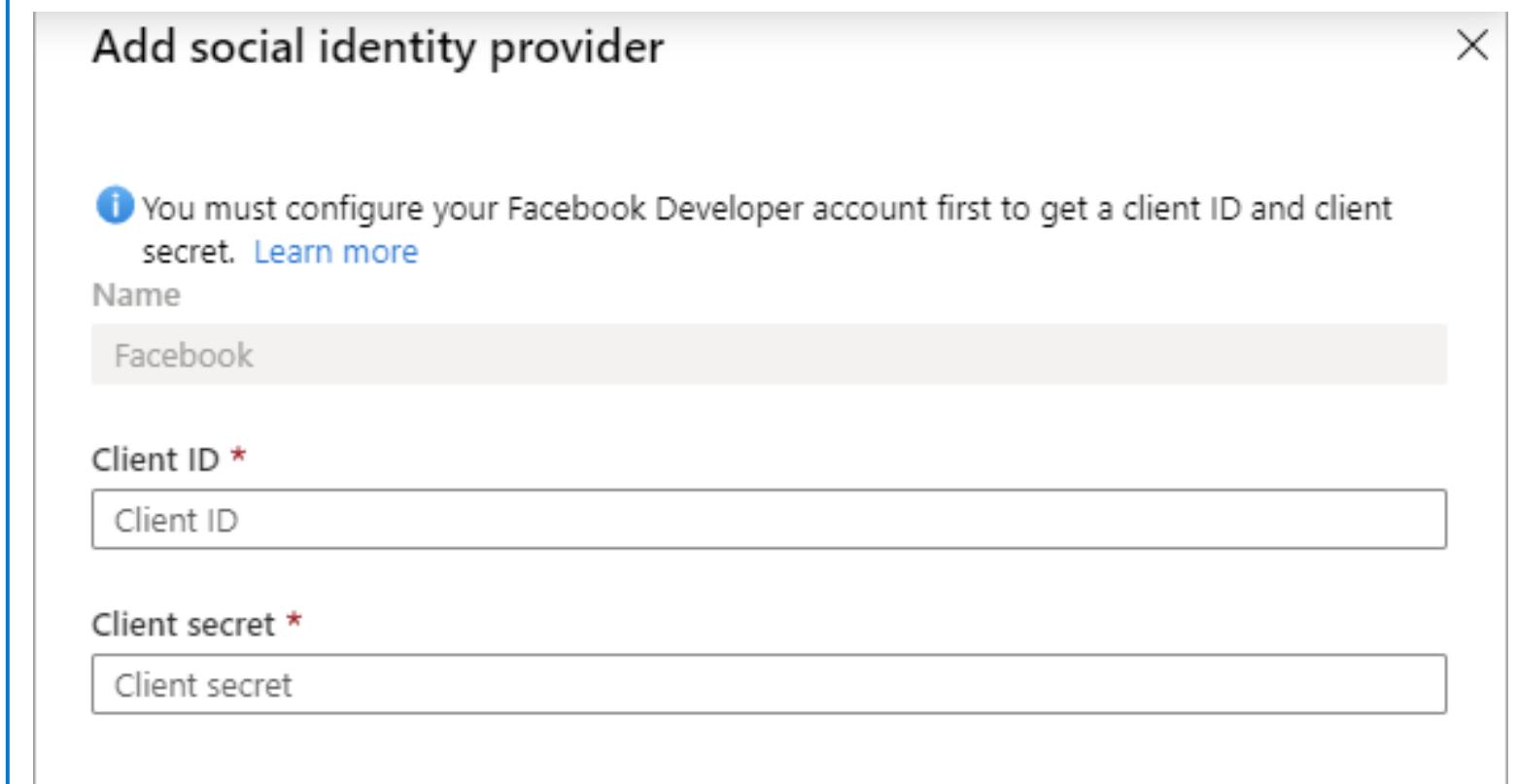
Add social identity provider X

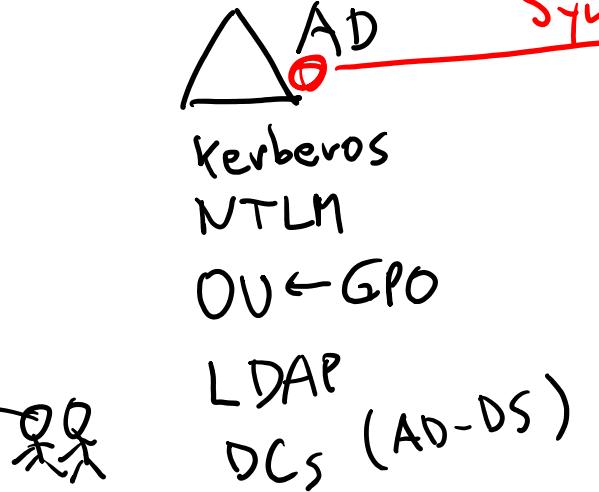
i You must configure your Facebook Developer account first to get a client ID and client secret. [Learn more](#)

Name

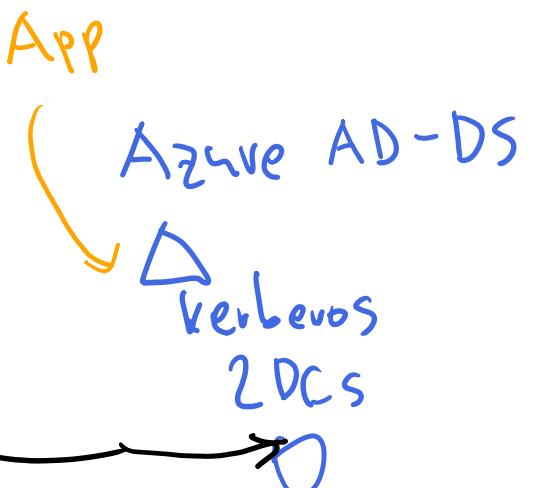
Client ID \*

Client secret \*





# Implement and manage hybrid identity



# Objectives



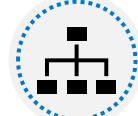
Plan, design, and implement Azure Azure Active Directory Connect (AADC)



Implement and manage password hash synchronization (PHS)



Implement and manage pass-through authentication (PTA)



Implement and manage federation



Troubleshoot synchronization errors



Implement Azure Active Directory Connect Health



Manage Azure Active Directory Connect Health

On Prem server ≠ DC

AD

AAD

✓  
Pass Change

X

✓

X

WS-Fed

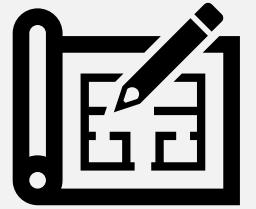
✓

X

Cloud Sync

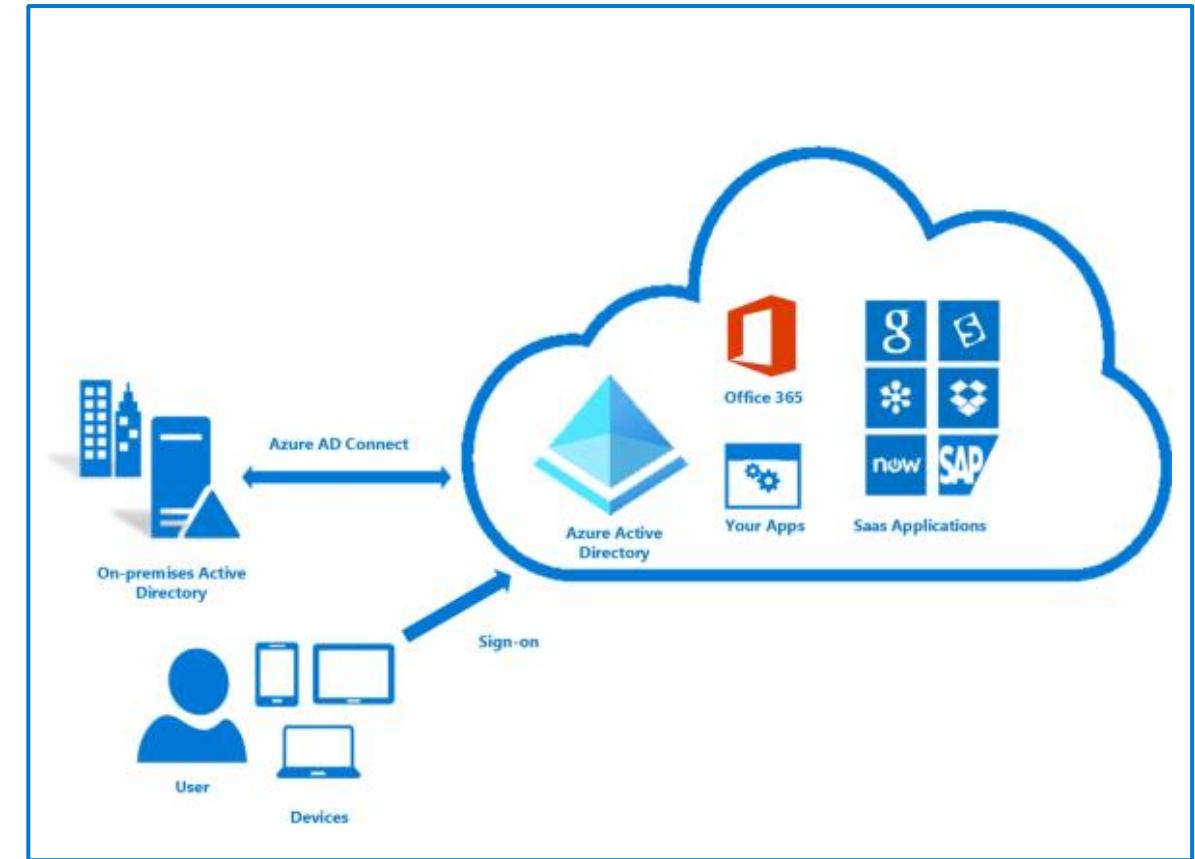
4.

# Plan, design, and implement Azure Active Directory Connect (AADC)

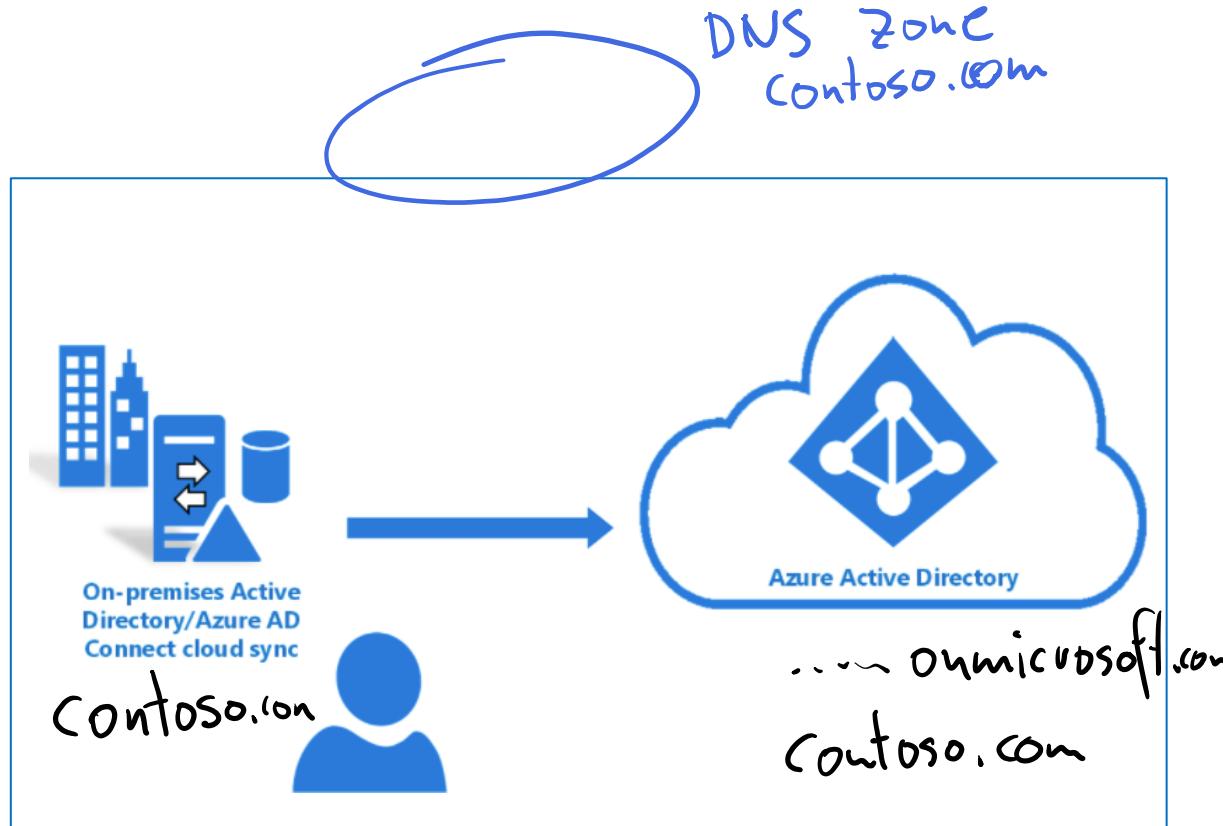


# What is Azure Active Directory Connect?

- Azure AD Connect is a solution that bridges an organizations on-premises Active Directory with your cloud-based Azure Active Directory
- Azure Active Directory Connect provides:
  - Synchronization
  - Password hash synchronization
  - Pass-through authentication
  - Federation integration
  - Health monitoring



# Azure AD Connect cloud sync



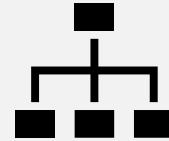
- Azure AD Connect cloud sync is a solution syncs your on-premises AD with Azure AD
- Lightweight provisioning agent required on the on-premises AD
- All sync configuration is managed in the cloud
- Can be used in conjunction with Azure AD Connect

# Authentication methods



## Cloud authentication

- **Azure AD password hash synchronization (PHS)**
  - Users can use the same username and password that they use on premises
- **Azure AD pass-through authentication (PTA)**
  - Simple password validation for Azure AD authentication services using a software agent that runs on one or more on-premises servers

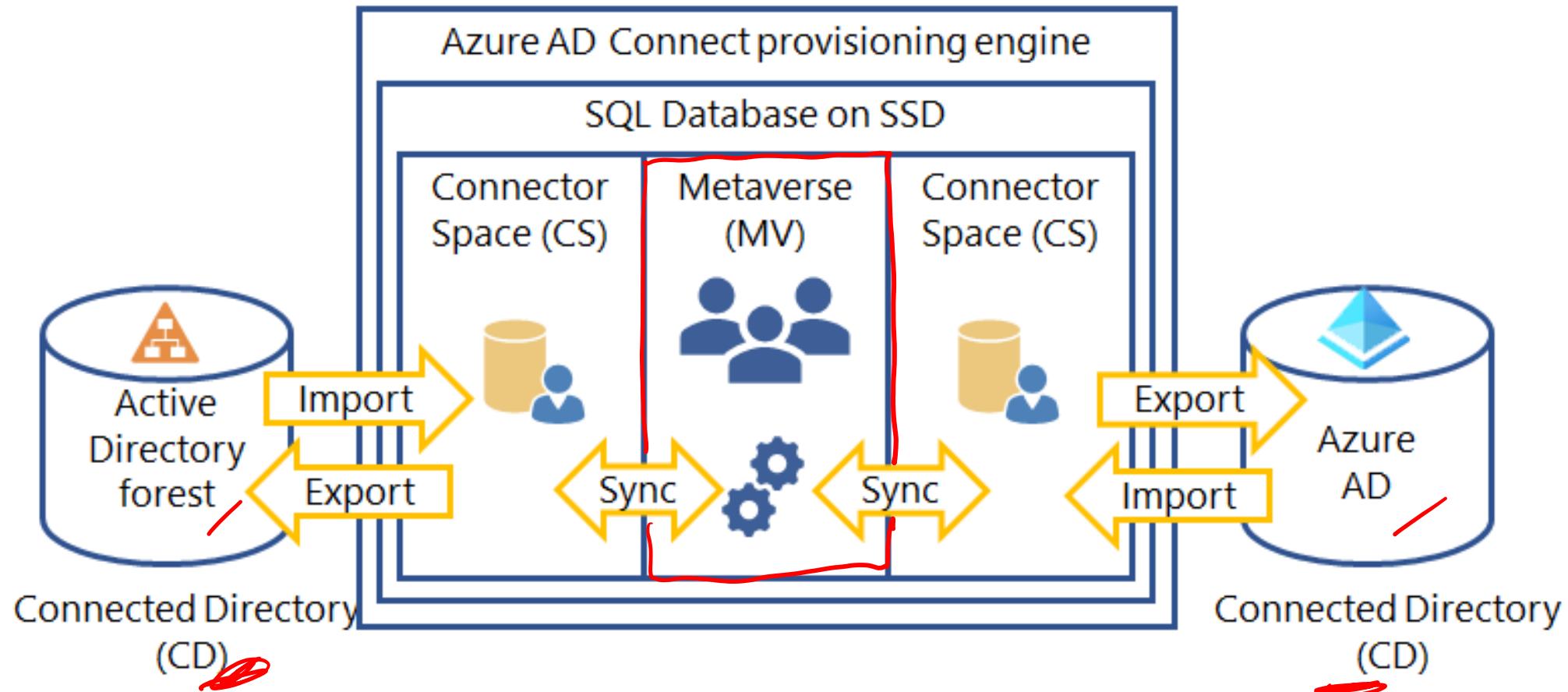


## Federated authentication

- **Handoff to trusted authentication system**
  - Azure AD hands off the authentication process to a separate trusted authentication system to validate the user's password
  - The authentication system can provide additional advanced authentication requirements, such as a smartcard or third-party multifactor authentication

# Azure AD Connect component factors

Min

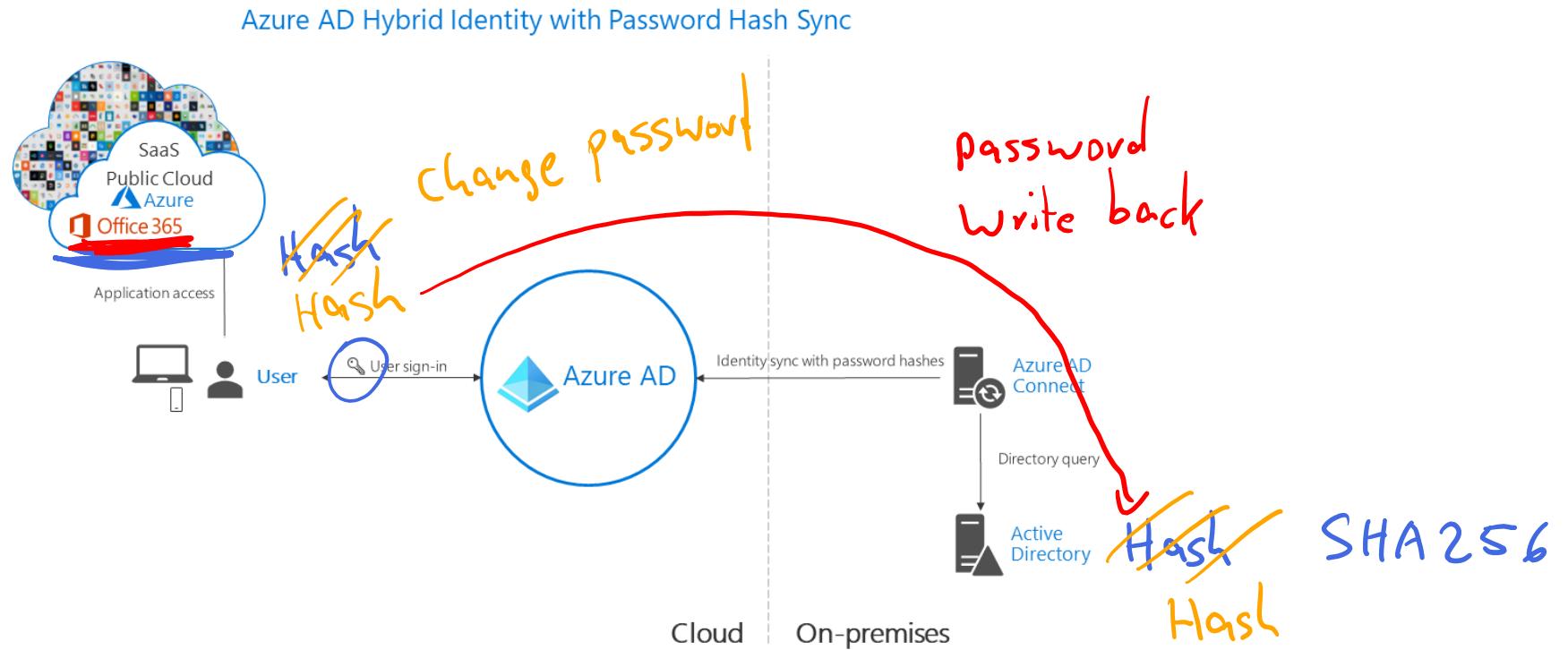


# Implement and manage password hash synchronization (PHS)



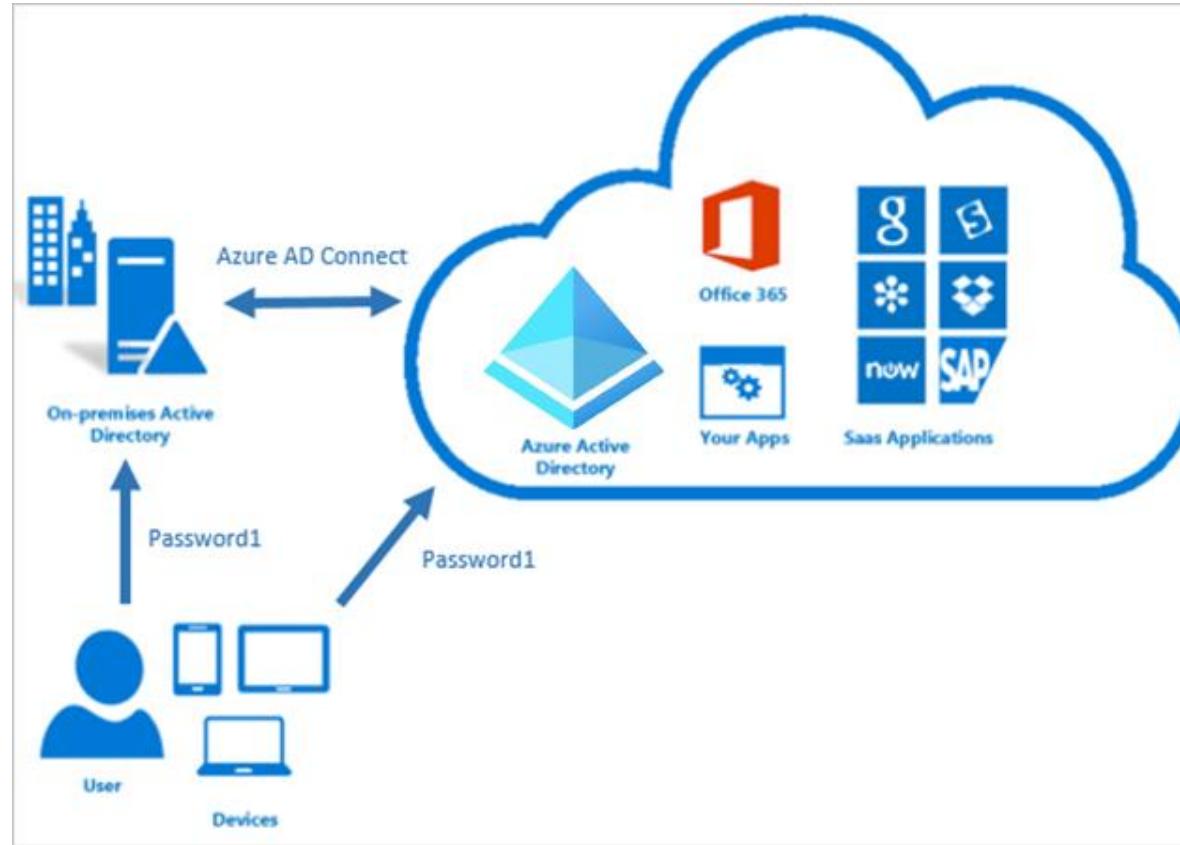
Anton Zeilinger  
QC

# Password hash sync

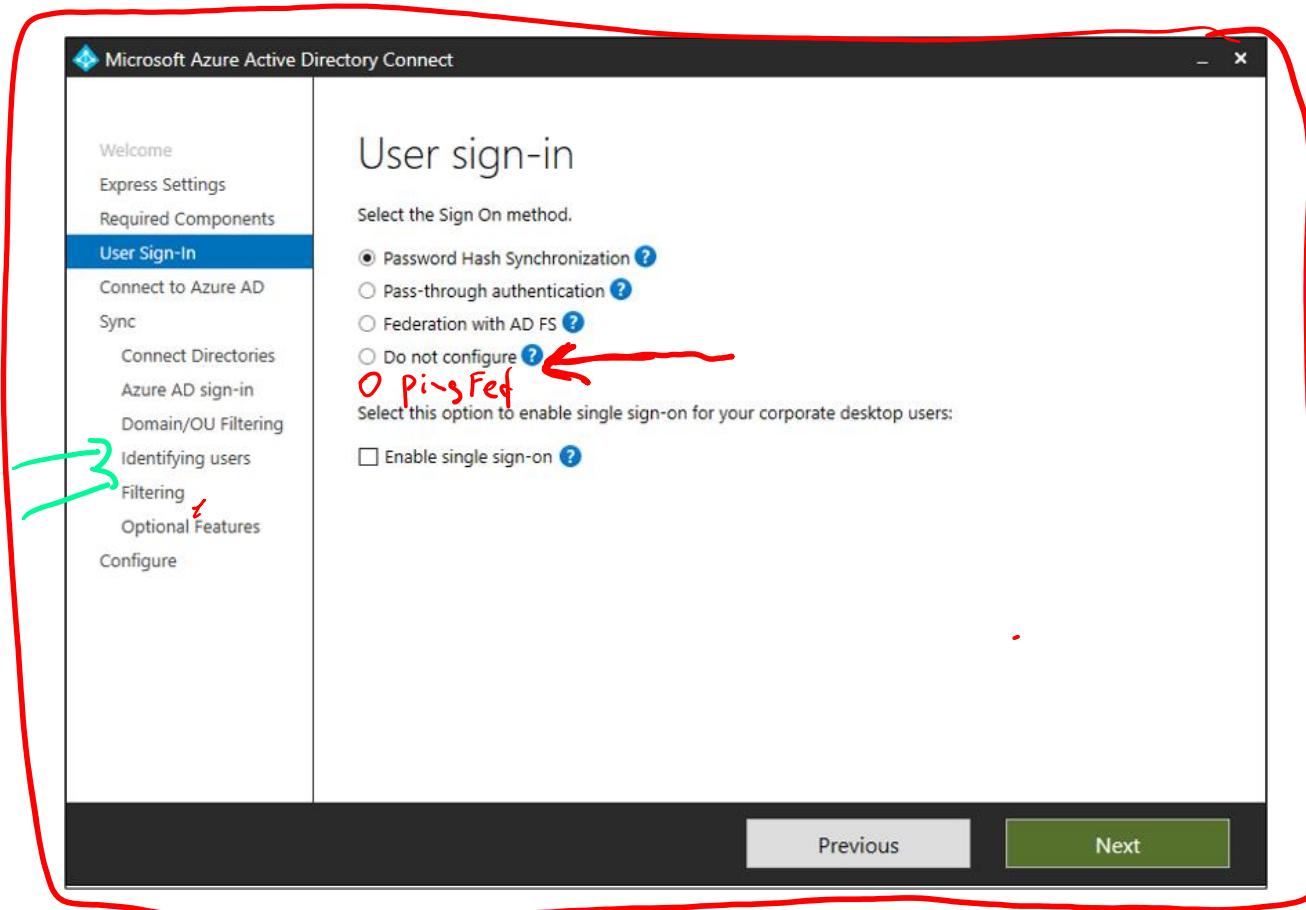


Simplicity of a password hash synchronization solution

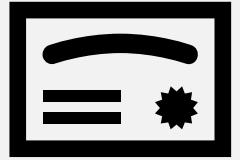
# How password hash synchronization works



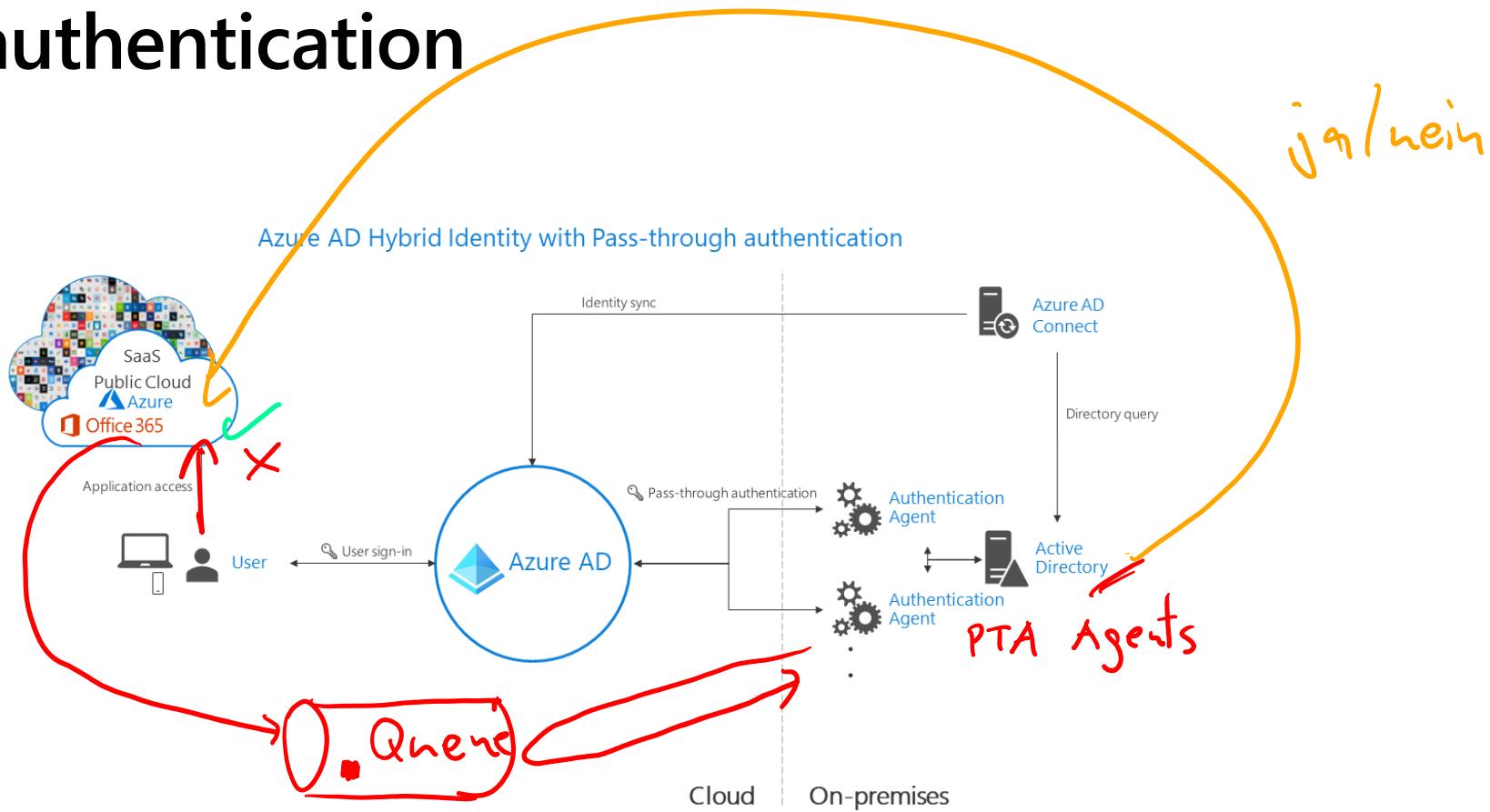
# Enable password hash synchronization



# Implement and manage pass-through authentication (PTA)

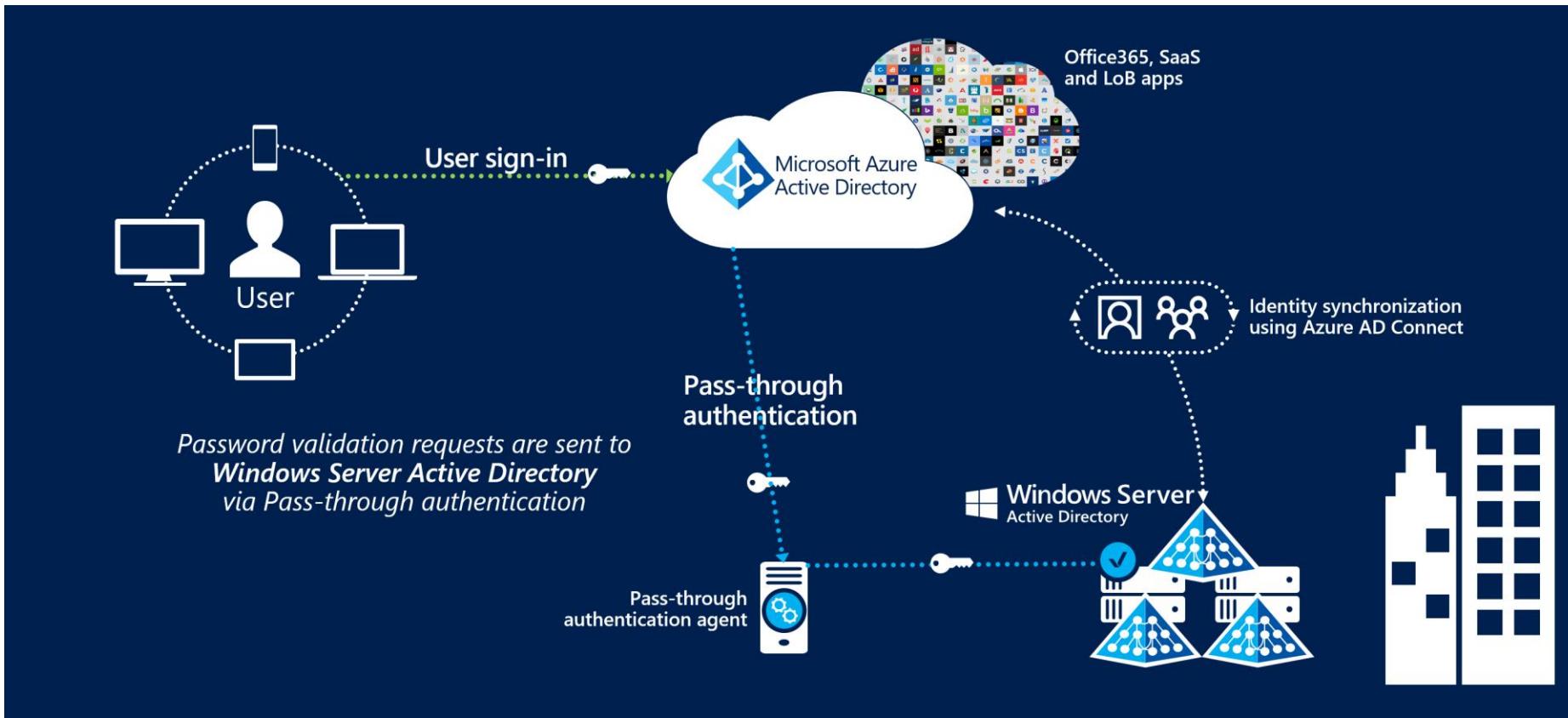


# Pass-through authentication



Agent requirements of pass-through authentication, using two agents for redundancy

# How Azure AD Pass-through Authentication works



# Enable pass-through authentication

**Microsoft Azure Active Directory Connect**

Welcome  
Express Settings  
Required Components  
**User Sign-In**  
Connect to Azure AD  
Sync  
  Connect Directories  
  Azure AD sign-in  
  Domain/OU Filtering  
Identifying users  
Filtering  
Optional Features  
Configure

## User sign-in

Select the Sign On method.

Password Hash Synchronization ?  
 Pass-through authentication ?  
 Federation with AD FS ?  
 Federation with PingFederate ?  
 Do not configure ?

Select this option to enable single sign-on for your corporate desktop users:

Enable single sign-on ?

We recommend that you have a cloud only Company Administrator account so that you are able to manage pass-through authentication in the event of an on-premises failure. [Learn more](#)

Previous      Next

**Microsoft Azure Active Directory Connect**

Welcome  
**Tasks**

## Additional tasks

The required tasks for the scenario have been completed. Choose from the list below to perform additional tasks.

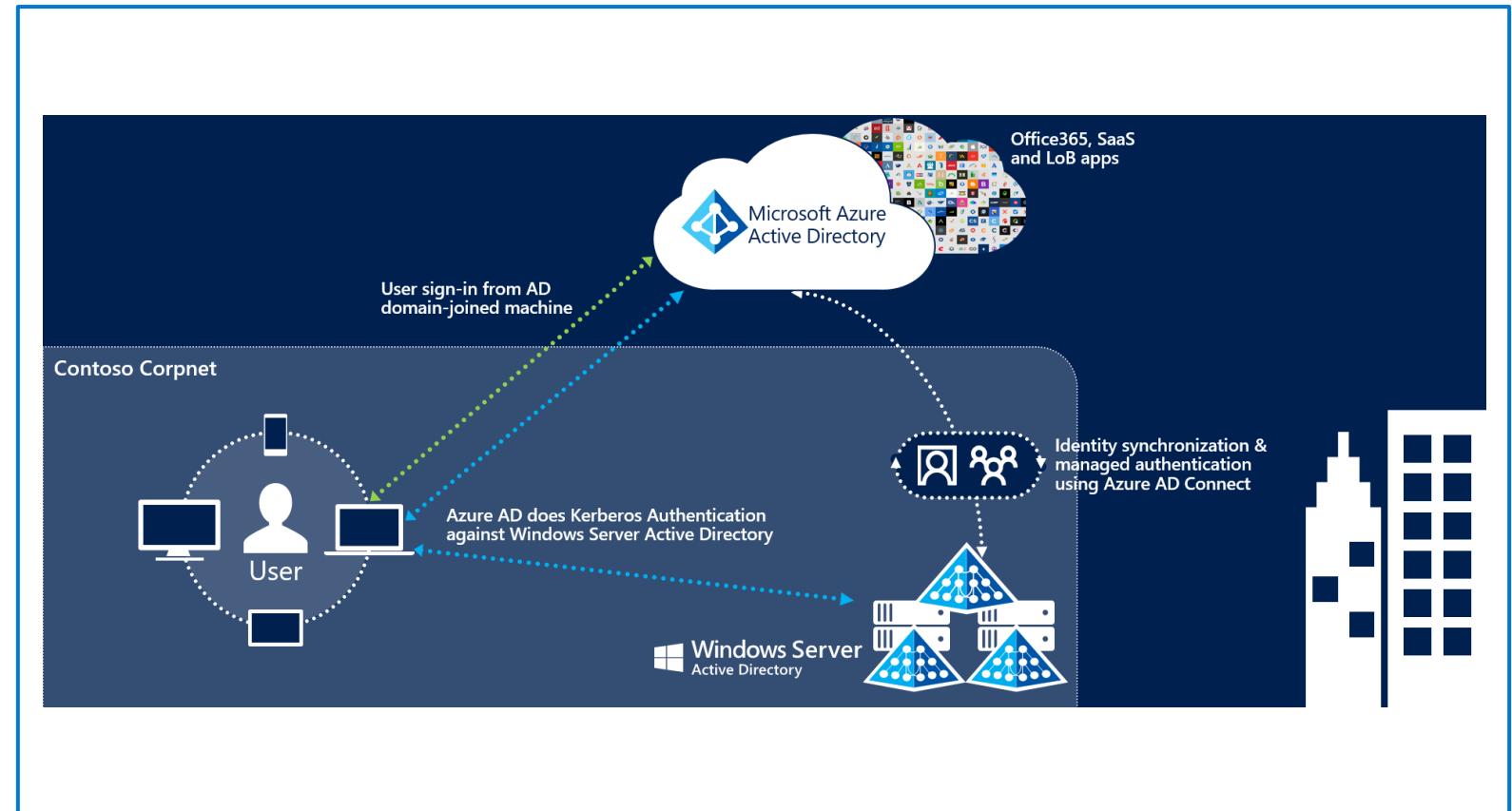
Privacy settings  
View current configuration  
Customize synchronization options  
Configure device options ?  
Refresh directory schema  
Configure staging mode  
**Change user sign-in**  
Configure Source Anchor  
Manage federation ?  
Troubleshoot

Previous      Next

# Seamless single sign-on (SSO)

# Single Sign-On

- User sign-in via on-premises or via Azure AD Connect alternate ID.
- If single sign-in fails, the user is prompted to log in.
- Sign out works, but releases the sign-in so all further access is blocked until sign-in is completed again.
- Supported in browser-based and Office-based clients.

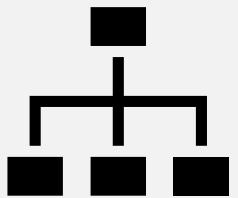


# How Seamless SSO is set up

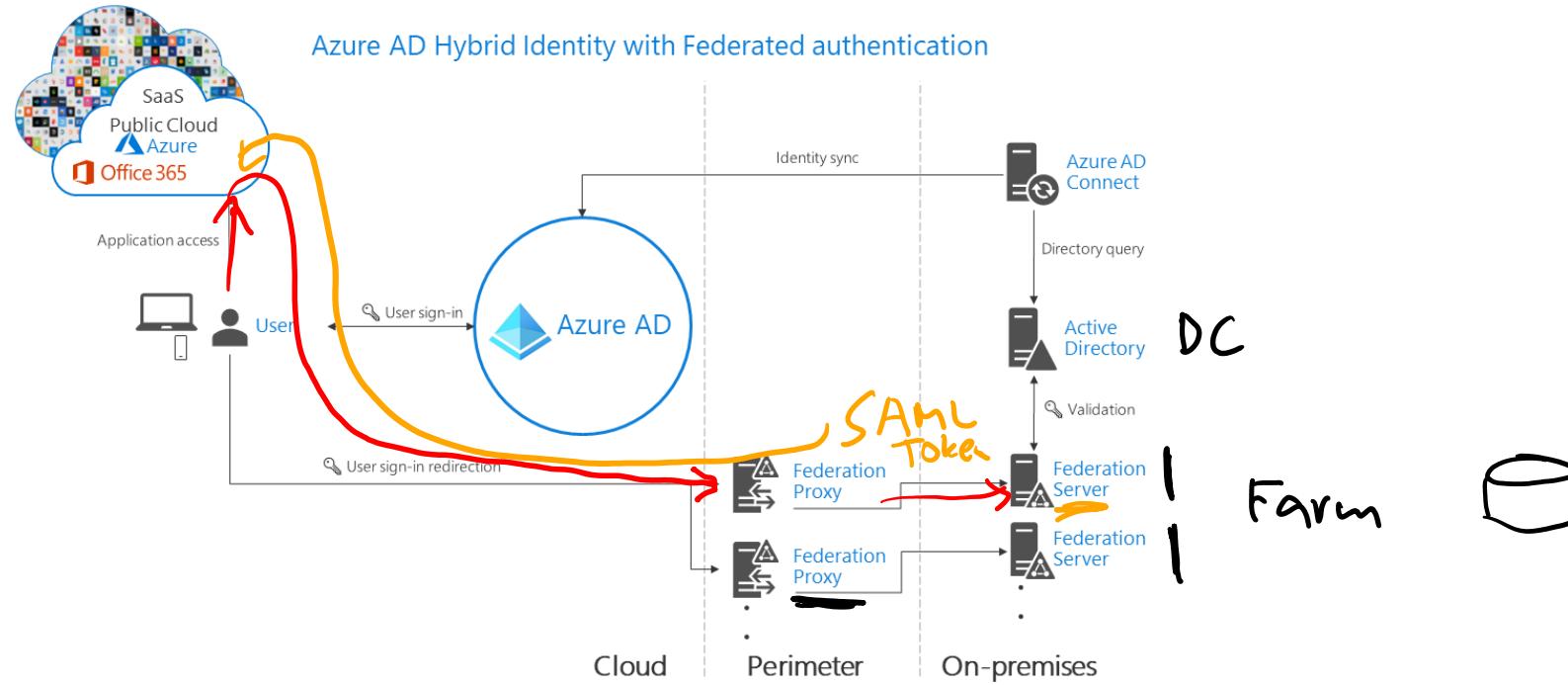
Seamless SSO is enabled using Azure AD Connect. While enabling the SSO, the following steps occur:

- A computer account (AZUREADSSOACC) is created in your on-premises Active Directory (AD) in each AD forest that you synchronize to Azure AD (using Azure AD Connect).
- In addition, a number of Kerberos service principal names (SPNs) are created to be used during the Azure AD sign-in process.
- The computer account's Kerberos decryption key is shared securely with Azure AD. If there are multiple AD forests, each computer account will have its own unique Kerberos decryption key.

# Implement and manage federation



# Federated authentication

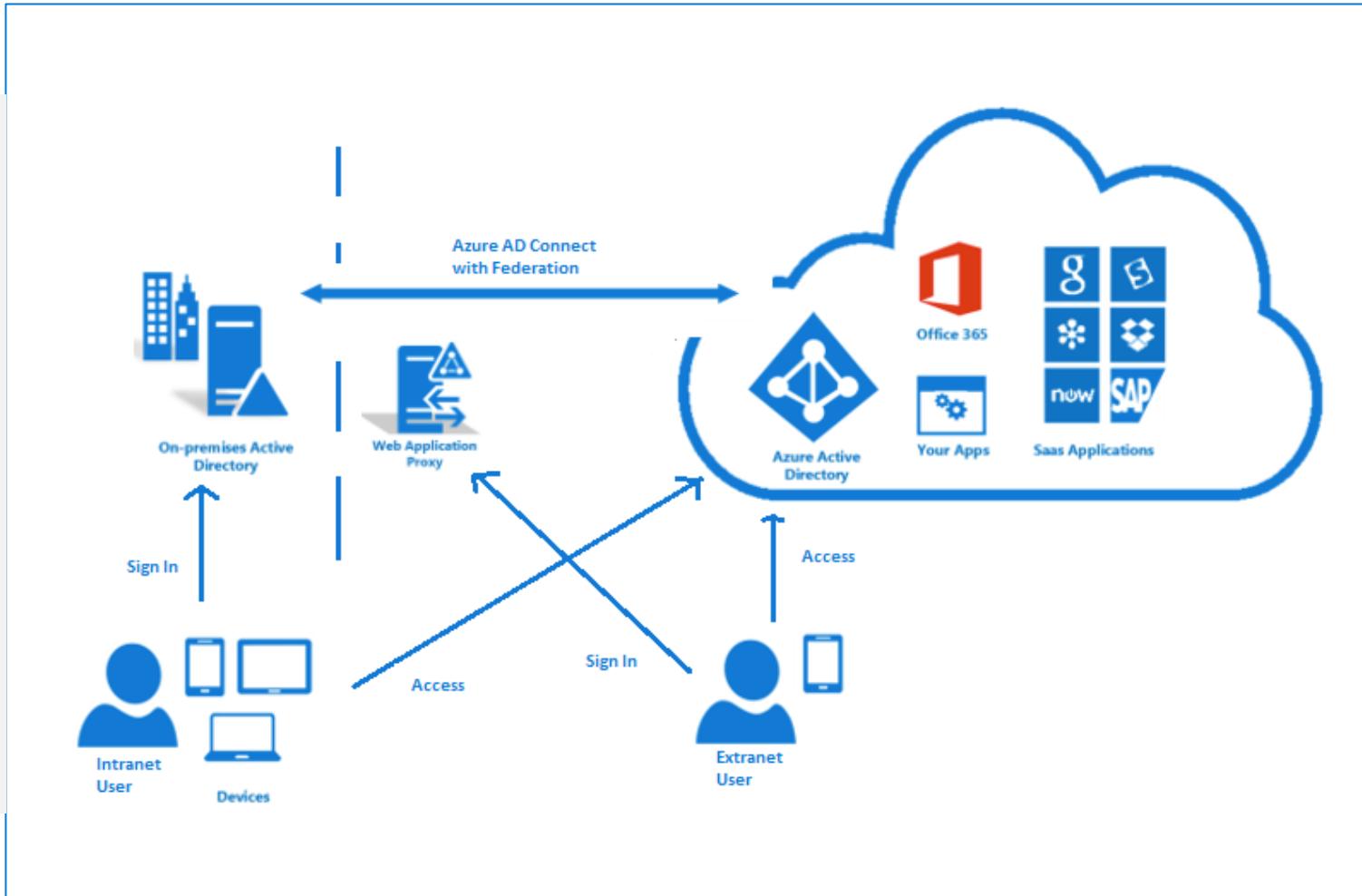


Components required for federation in your perimeter and internal network of your organization

# What is federation?

**Federation uses a new or existing farm with AD FS in Windows Server 2012 R2**

- User sign-in to Azure AD services using their on-premises passwords
- Azure AD Connect configures the trust between Azure AD and on-premises farm



# Deploying a federation with AD FS and Azure AD Connect

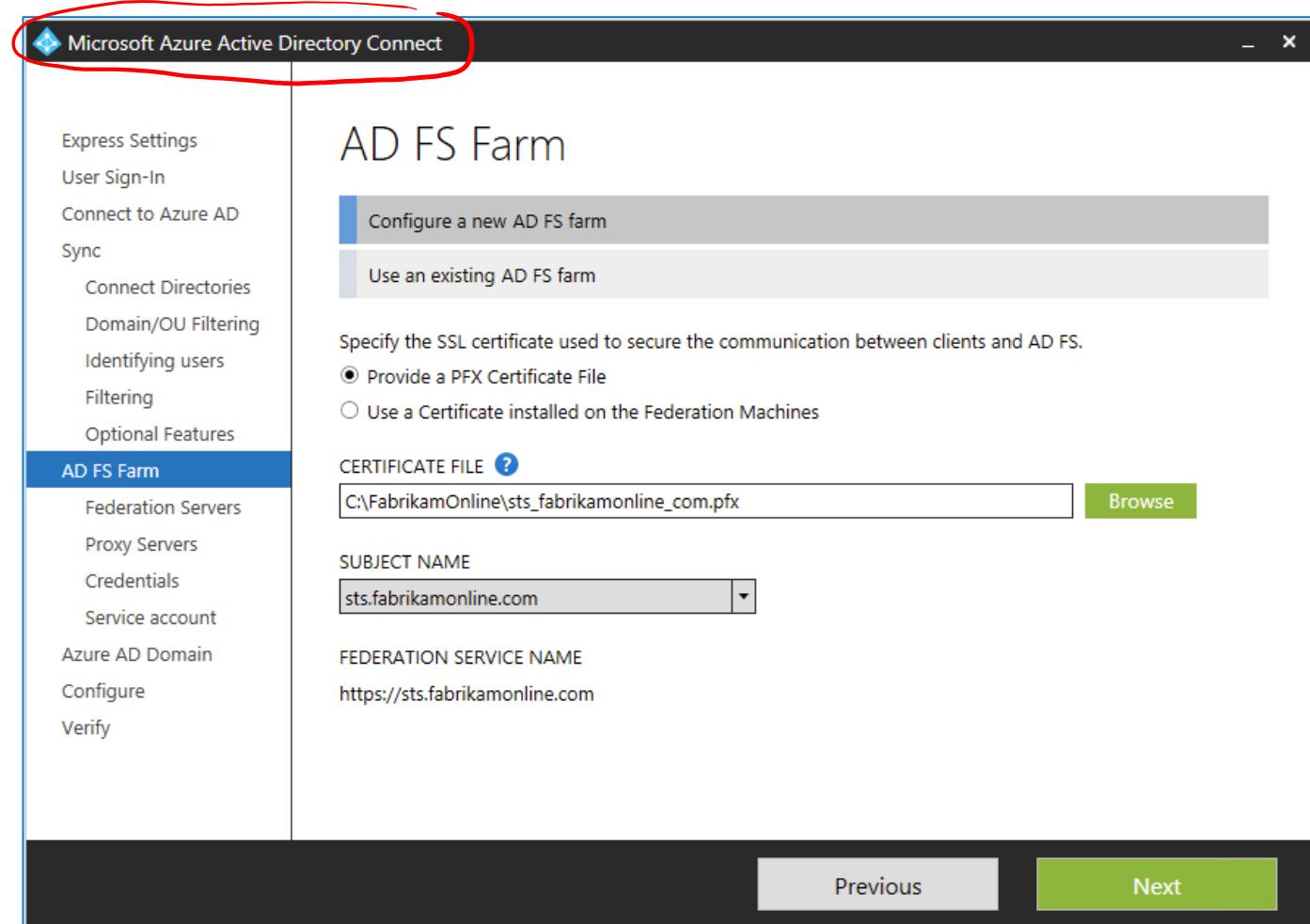
Deploying an AD FS farm, you need:

- Local administrator credentials on your federation servers.
- Local administrator credentials on any workgroup servers (not domain-joined) that you intend to deploy the Web Application Proxy role on.
- The machine that you run the wizard on to be able to connect to any other machines that you want to install AD FS or Web Application Proxy on by using Windows Remote Management.

# Using Azure AD Connect to connect to an AD FS farm

## Primary Steps

- Select AD FS server(s)
- Select Web App Proxy server(s)
- Specify AD FS service account
- Select Azure AD domain to federate



# Managing federation with Azure AD Connect

Manage AD FS feature	What it does
<a href="#">Repair the trust</a>	How to repair the federation trust with Microsoft 365.
<a href="#">Federate with Azure AD using alternate login ID</a>	Configure federation using alternate login ID
<a href="#">Add an AD FS server</a>	How to expand an AD FS farm with an additional AD FS server.
<a href="#">Add an AD FS Web Application Proxy server</a>	How to expand an AD FS farm with an additional Web Application Proxy (WAP) server.
<a href="#">Add a federated domain</a>	How to add a federated domain.

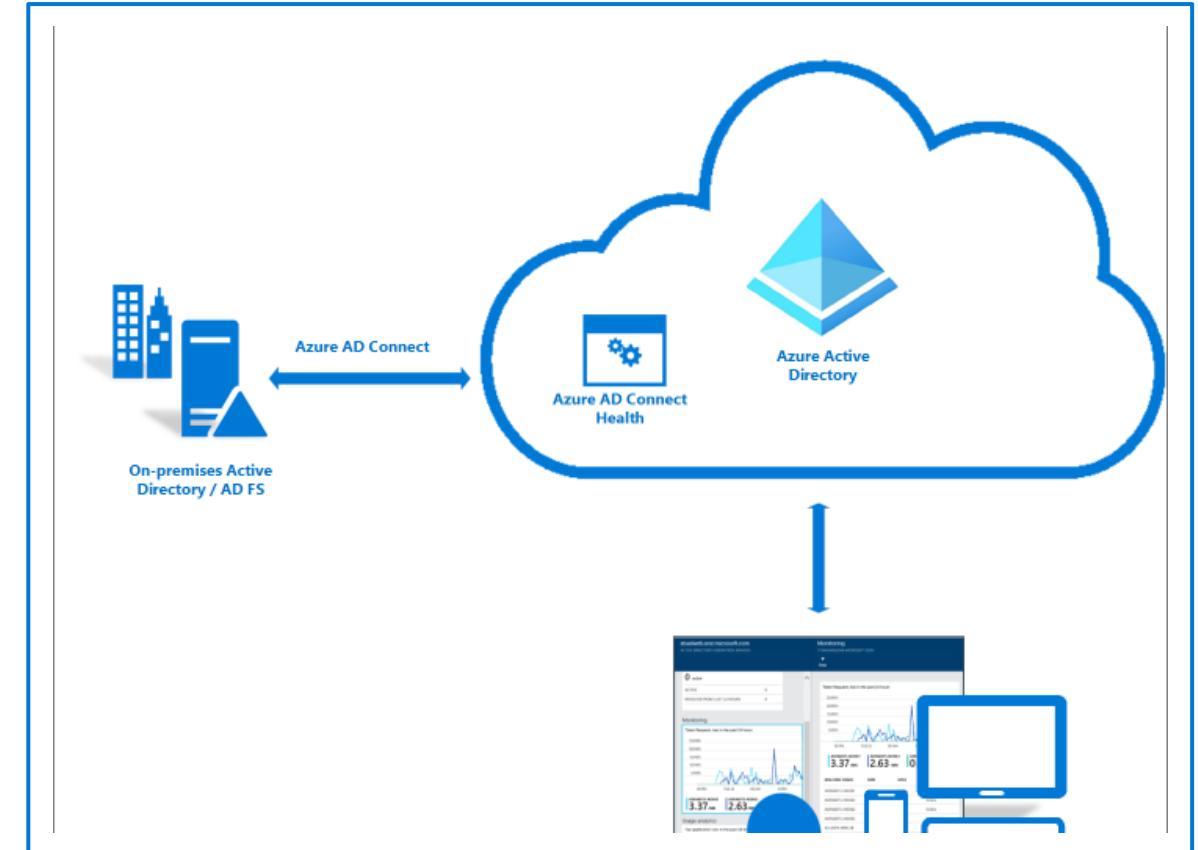
# Implement Azure Active Directory Connect Health



# What is Azure Active Directory Connect Health?

- Provides robust monitoring of your on-premises identity infrastructure
- Enables you to maintain a reliable connection to Microsoft 365 and Microsoft Online Services
- Provides monitoring capabilities for your key identity components.
- Makes the key data points about these components easily accessible.
- Azure AD Health Connect Portal  
(aka.ms/aadconnecthealth)

Start-ADSync Sync Cycle

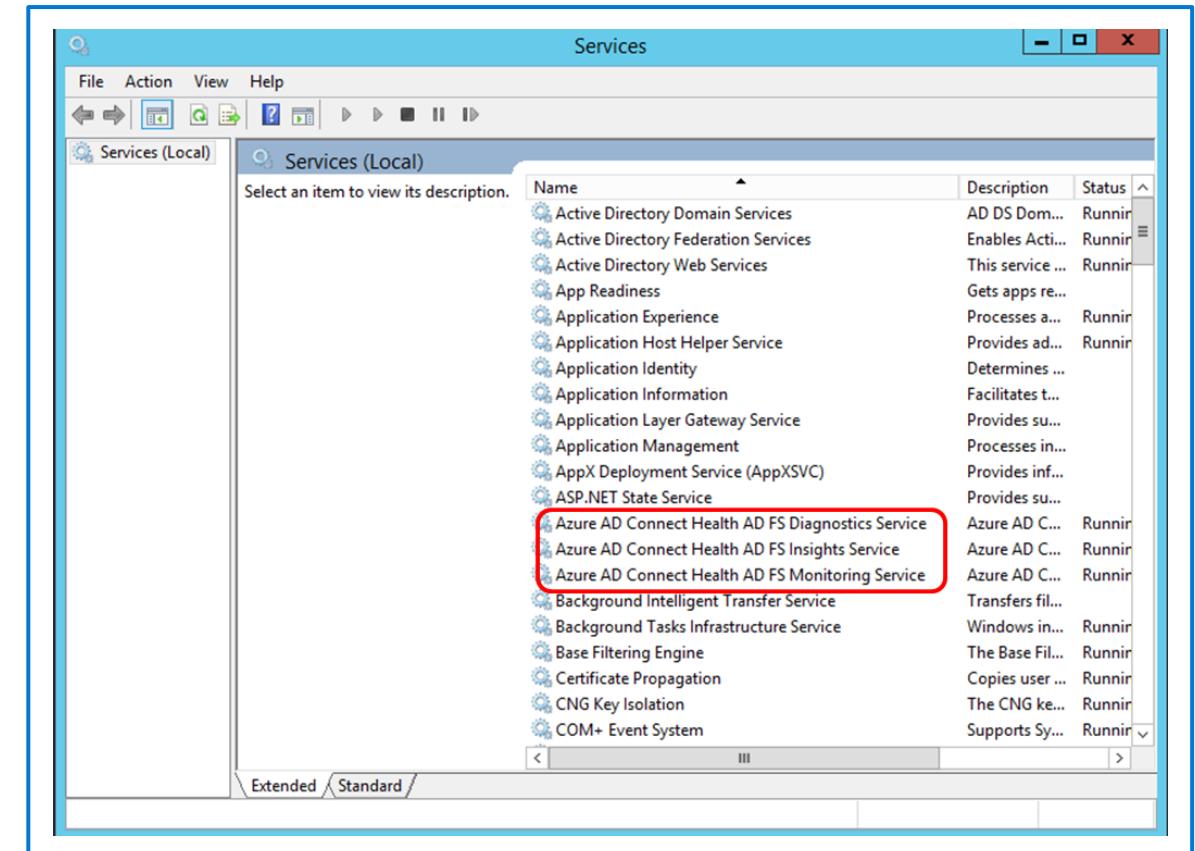


# Considerations for installing Azure AD Connect Health

- Azure AD Premium license required (P1 or P2)
- Only a Global Administrator can deploy and configure
- Azure AD Connect Health Agent – install on each server to collect health data from
  - AD FS server or your Azure AD Domain Services machine or etc.
- Firewall must be opened for specific IP ranges and TCP ports
- TLS inspection can block install or operation
- PowerShell 4.0 or later required
- FIPS compliant encryption must be disabled

# Example – AD Connect Help for AD FS Installation steps

1. Install the agent for Active Directory Federation Service
2. Configure the agent
3. Sign in using an Azure AD account with permission to register the agent
4. Ensure that the Azure AD Connect Health services are installed
5. Install the Azure AD Connect Health agent for Sync



# Manage Azure Active Directory Connect Health



# Enable email notifications

The screenshot shows the Azure Active Directory Connect (Sync) Alerts blade in the Azure portal. On the left, there's a summary card for 'Azure Active Directory Connect Servers' showing 2 servers: FABVM03 (Unhealthy) and FABVM02 (Healthy). Below it is another card for 'Azure Active Directory Connect (Sync) Alerts' showing 1 active alert. On the right, the main pane displays 'Azure Active Directory Connect (Sync) Alerts' for fabtoso.onmicrosoft.com. It includes a 'Time Range' filter, a 'Notification' button (which is highlighted with a red box), and a 'Settings' button. A tooltip says: 'You can provide feedback by doing a right click on any alert.' Below this is a search bar labeled 'Find ...'. The main area lists 'ACTIVE ALERTS' with one entry: 'Azure AD Connect Sync Service is not r...' (Error, FABVM03). Under 'RESOLVED ALERTS', it says 'No items for this.' To the right, there's a 'Notification' section with a toggle switch set to 'ON', a checkbox for 'Notify All Global Administrators', and an 'ADDITIONAL EMAIL RECIPIENTS' field containing 'varun@fabtoso.com' and 'idadmins@fabtoso.com'.

# Additional tasks

## Delete a server or service instance

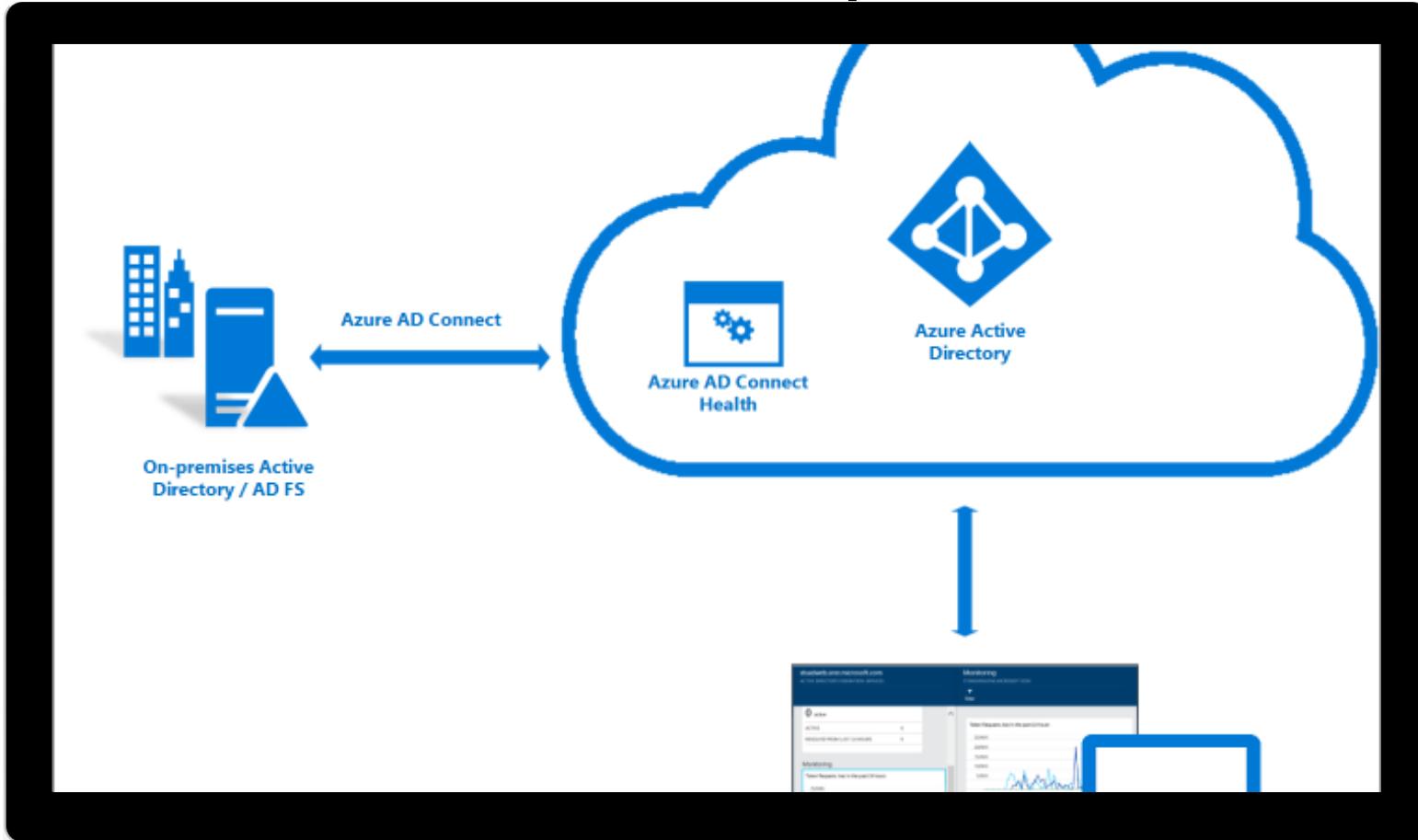
- Delete a server from the Azure AD Connect Health service
- Delete a service instance from Azure AD Connect Health service

## Manage access with Azure Role Based Access Control

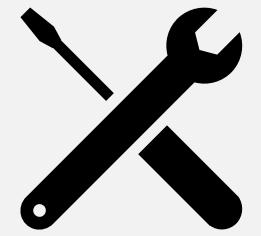
- Allow users or groups access to Azure AD Connect Health
- Remove users or groups

# Demo Video: Azure AD Connect Health monitors on-premises AD Domain Services

[Launch  
Video](#)



# Troubleshoot synchronization errors



# Troubleshooting

## Diagnose and remediate duplicated attribute sync errors

- Duplicate UserPrincipalName or Proxy Addresses
- Orphaned object

## Diagnostic and troubleshooting steps in Connect Health

- Attributes: UserPrincipalName, ProxyAddresses, SipProxyAddress, OnPremiseSecurityIdentifier

# Potential synchronization errors

## Data mismatch errors

- InvalidSoftMatch
- ObjectTypeMismatch

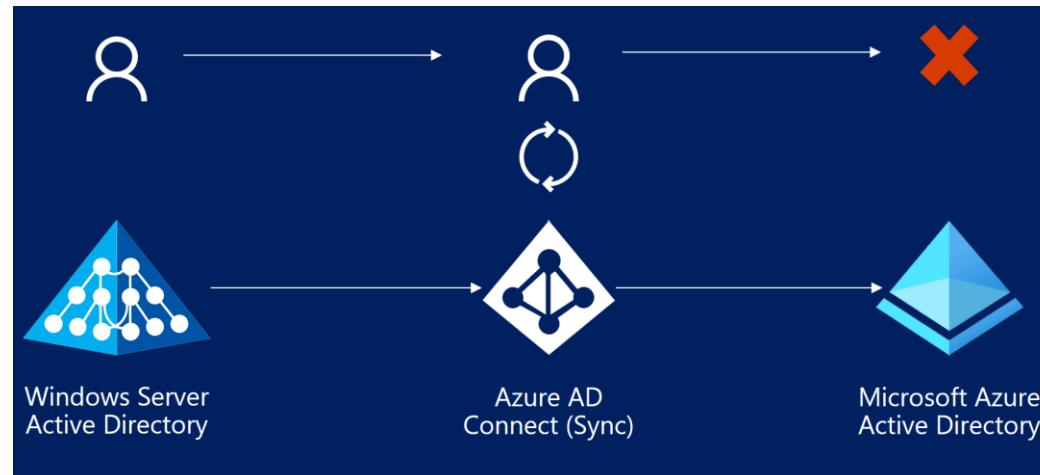
## Duplicate attributes

- AttributeValueMustBeUnique

## Data validation failures

- IdentityDataValidationFailed
- FederatedDomainChangeError

**LargeObject**  
**Admin role conflict**



# Summary

## Initial Azure AD configuration

- Azure AD roles, Custom Roles,
- Custom Domain *Names*
- Administrative Units *UAU*
- Tenant wide settings



## External Identities

*B2B*

- Guests can use your solutions
- External Collaboration
- Invite individually or in bulk
- Use external identity providers (as needed)

## Configure and Manage Identities

- Users
  - Groups
  - Licenses
  - Focus on proper maintenance!
- App
  - Devices

## Hybrid Identity

- Connect to your on-premises AD
- Azure AD Connect
- Implement PHS, PTA, and SSO
- Azure AD Connect Health

# Labs

Lab	Brief description	Length
1. Manage user roles	Create a user account, add a role to it, and remove a role.	10 minutes
2. Working with tenant properties	Set tenant-wide properties such as changing the tenant display name and adding privacy information.	10 minutes
3. Assign licenses to users and groups	Create a user in Azure Active Directory, create a security group, and assign a license to a group.	10 minutes
4. Configure external collaboration	Configure external collaboration settings.	5 minutes
5. Add guest users to the directory	Add users individually to the directory	5 minutes
6. Add a federated identity provider	Configure a new federated identity provider	15 minutes

# References

Implement initial configuration of Azure AD

<https://docs.microsoft.com/learn/modules/implent-initial-configuration-of-azure-active-directory/>

Create, configure, and manage identities

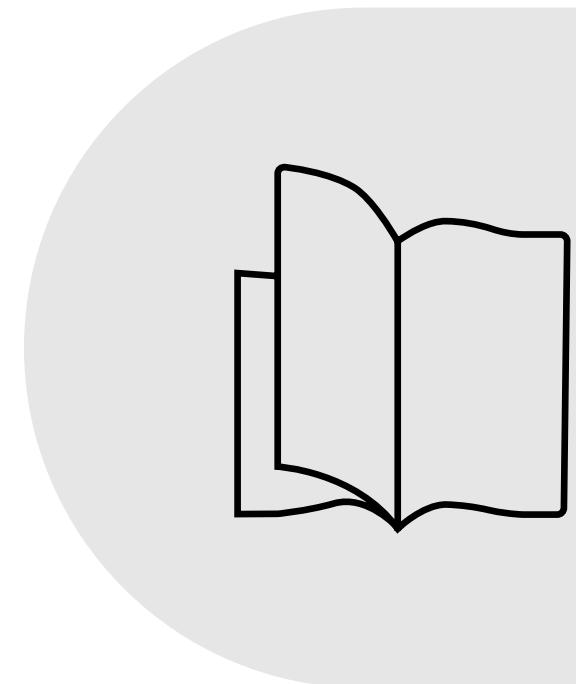
<https://docs.microsoft.com/learn/modules/create-configure-manage-identities/>

Implement and manage external identities

<https://docs.microsoft.com/learn/modules/implent-manage-external-identities/>

Implement and manage hybrid identity

<https://docs.microsoft.com/learn/modules/implent-manage-hybrid-identity/>



**End of presentation**