



SC-300

# Microsoft Identity and Access Administrator



LP 1

# Implement an identity management solution



# Agenda

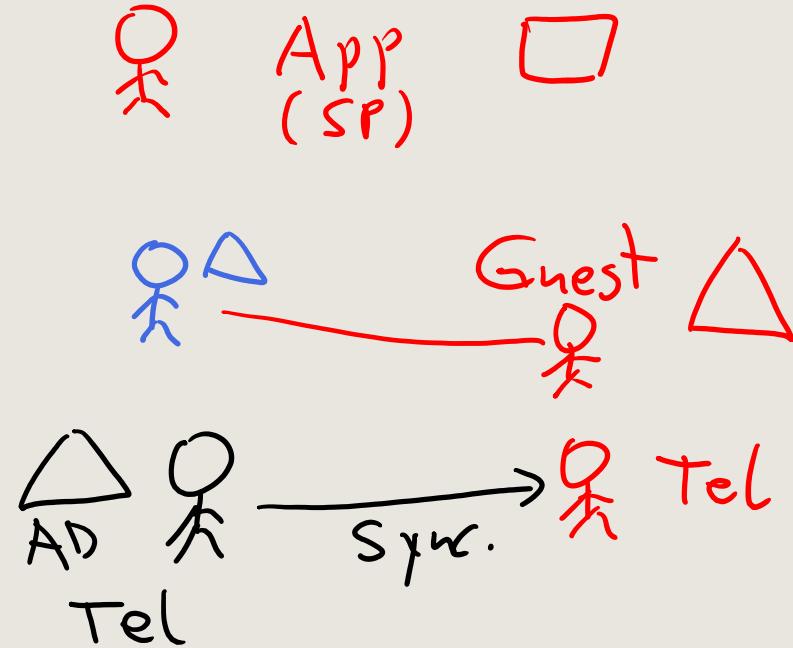
---

- LP 1 Implement an Identity Management Solution ←
- LP 2 Implement an Authentication and Access Management Solution
- LP 3 Implement Access Management for Apps
- LP 4 Plan and Implement an Identity Governance Strategy

# Outline

---

- Create, configure, and manage identities
- Configure and manage Microsoft Entra ID
- Implement and manage external identities
- Implement and manage hybrid identity



# Learning objectives

After completing this module, you will be able to:

- 1** Explain and configure identities for use in your cloud solutions.
- 2** Deploy and manage a Microsoft Entra ID infrastructure.
- 3** Configure and maintain external and hybrid identities.

# Create, configure, and manage identities

# Objectives

- 1** Create, configure, and manage users
- 2** Create, configure, and manage groups
- 3** Configure and manage device identities
- 4** Manage licenses
- 5** Custom security attributes
- 6** 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 **Identity – All users** dashboard in the Microsoft Entra admin center to work with user objects
- Three kinds of users:
  - Cloud identities
  - Directory-synchronized identities
  - External users

The screenshot shows the 'Users' dashboard in the Microsoft Entra admin center. On the left, there's a sidebar with links like 'All users', 'Audit logs', 'Sign-in logs', etc. The main area displays a table of users with columns for 'Display name', 'User principal name', 'User type', and 'On-premises sync'. There are 24 users listed, each with a small profile picture and a checkbox next to their name.

	Display name ↑	User principal name ↑	User type	On-premises sync
<input type="checkbox"/>	Adele Vance	AdeleV	Member	No
<input type="checkbox"/>	Alex Wilber	AlexW	Member	No
<input type="checkbox"/>	Bhogeswar Kalita	BhogeswarK	Member	No
<input type="checkbox"/>	Diego Siciliani	DiegoS	Member	No
<input type="checkbox"/>	Grady Archie	GradyA	Member	No
<input type="checkbox"/>	Henrietta Mueller	HenriettaM	Member	No
<input type="checkbox"/>	Isaiah Langer	IsaiahL	Member	No
<input type="checkbox"/>	Johanna Lorenz	JohannaL	Member	No

# User settings

## Some configurable user settings:

- Groups
- Licenses
- Devices
- Location



The screenshot shows the Azure portal interface for managing a user named Adele Vance. The left sidebar lists various configuration options: Overview, Audit logs, Sign-in logs, Diagnose and solve problems, Custom security attributes, Assigned roles, Administrative units, Groups, Applications, Licenses, Devices, Azure role assignments, and Authentication methods. The 'Groups' option is highlighted with a red box and a red arrow from the previous slide. The main content area displays Adele Vance's basic info, including her profile picture, name (Adele Vance), object ID (AdeleV), member status, and creation date (Apr 24, 2022, 11:56 AM). It also shows her group memberships (7), applications (1), assigned roles (0), and assigned licenses (1).

Setting	Value	Count
Group memberships	AdeleV	7
Applications		1
Assigned roles		0
Assigned licenses		1

# Demo—users

The screenshot shows the 'Users' page in the Microsoft Azure portal. At the top, there is a search bar labeled 'Search' and a navigation bar with icons for 'New user', 'Edit (Preview)', and 'Delete'. Below the navigation bar, a list of user-related actions is displayed:

- All users
- Audit logs
- Sign-in logs
- Diagnose and solve problems
- Deleted users
- Password reset

A dropdown menu is open over the 'New user' button, showing two options:

- Create new user: Create a new internal user in your organization
- Invite external user: Invite an external user to collaborate with your organization

Below the dropdown, two user profiles are listed:

- Adele Vance (selected, indicated by a checked checkbox)
- Alex Wilber

# Create, configure, and manage groups

# Create, configure, and manage groups

## Security groups:

- Most common
- Manage access to shared resources for a group
- Can be nested groups

## Microsoft 365 groups:

- Access shared mailbox, calendar, SharePoint, and more
- Give access to external people
- Unable to nest within groups

The screenshot shows the 'Groups | All groups' page. On the left, there's a sidebar with 'Overview', 'All groups' (which is selected and highlighted in grey), 'Deleted groups', and 'Diagnose and solve problems'. Below that are sections for 'Settings' (General, Expiration, Naming policy) and 'Activity' (Privileged Identity Management, Access reviews). The main area lists 24 groups with columns for Name, Group type, and Membership type. The groups listed are: AAD DC Administrators (Security, Assigned), All Company (Microsoft 365, Assigned), Azure ATP (Security, Assigned), and two entries for Azure ATP (Security, Assigned).

Name	Group type	Membership type
AAD DC Administrators	Security	Assigned
All Company	Microsoft 365	Assigned
Azure ATP	Security	Assigned
Azure ATP	Security	Assigned

# Dynamic groups

- Special type of security group
- Membership dynamically generated via membership rule
  - Property -- example = department, region, and other items

Dynamic membership rules ...

Save Discard | Got feedback?

Configure Rules Validate 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
	<Choose a Property>	<Choose an Operator>	Add a value
And	objectId	Not Equals	null
And	Choose a Property	Choose an Operator	Add a value

+ Add expression + Get custom extension properties [○](#)

Rule syntax

```
(user.ObjectId -ne null)
```

# Group configuration options

## Some configurable group settings:

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

The screenshot shows the 'All Company' group settings page. The left sidebar has sections for Overview, Manage (Properties, Members, Owners, Roles and administrators), and Activity (Privileged Identity Management, Access reviews). The 'Properties' section is highlighted with a red box. The 'Administrative units' and 'Group memberships' sections are also highlighted with red boxes. The main content area displays basic information about the group, including its name ('All Company'), a description ('This is the default group for everyone in the network'), and various statistics like total direct members (1), source (Cloud), type (Microsoft 365), and object ID.

Home > Users > Groups | All groups >

**All Company** Group

Overview

Manage

Properties

Members

Owners

Roles and administrators

Administrative units

Group memberships

Applications

Azure role assignments

Activity

Privileged Identity Management

Access reviews

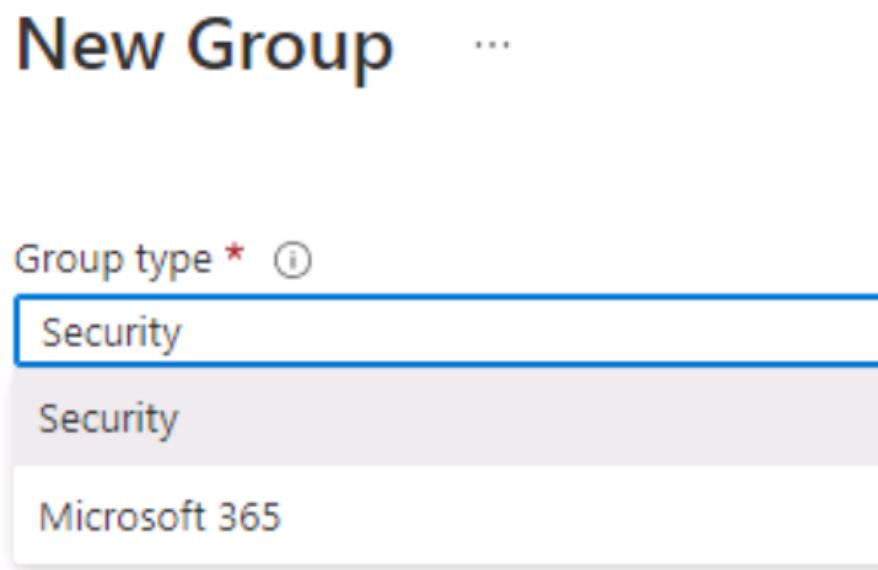
Delete Got feedback?

**All Company**

This is the default group for everyone in the network

Membership type	Assigned	Total direct members	1
Source	Cloud	User(s)	1
Type	Microsoft 365	Group(s)	0
Object ID		Device(s)	0
Created on	4/24/2022, 7:51 AM	Other(s)	0
Email	allcompany		

# Demo—groups

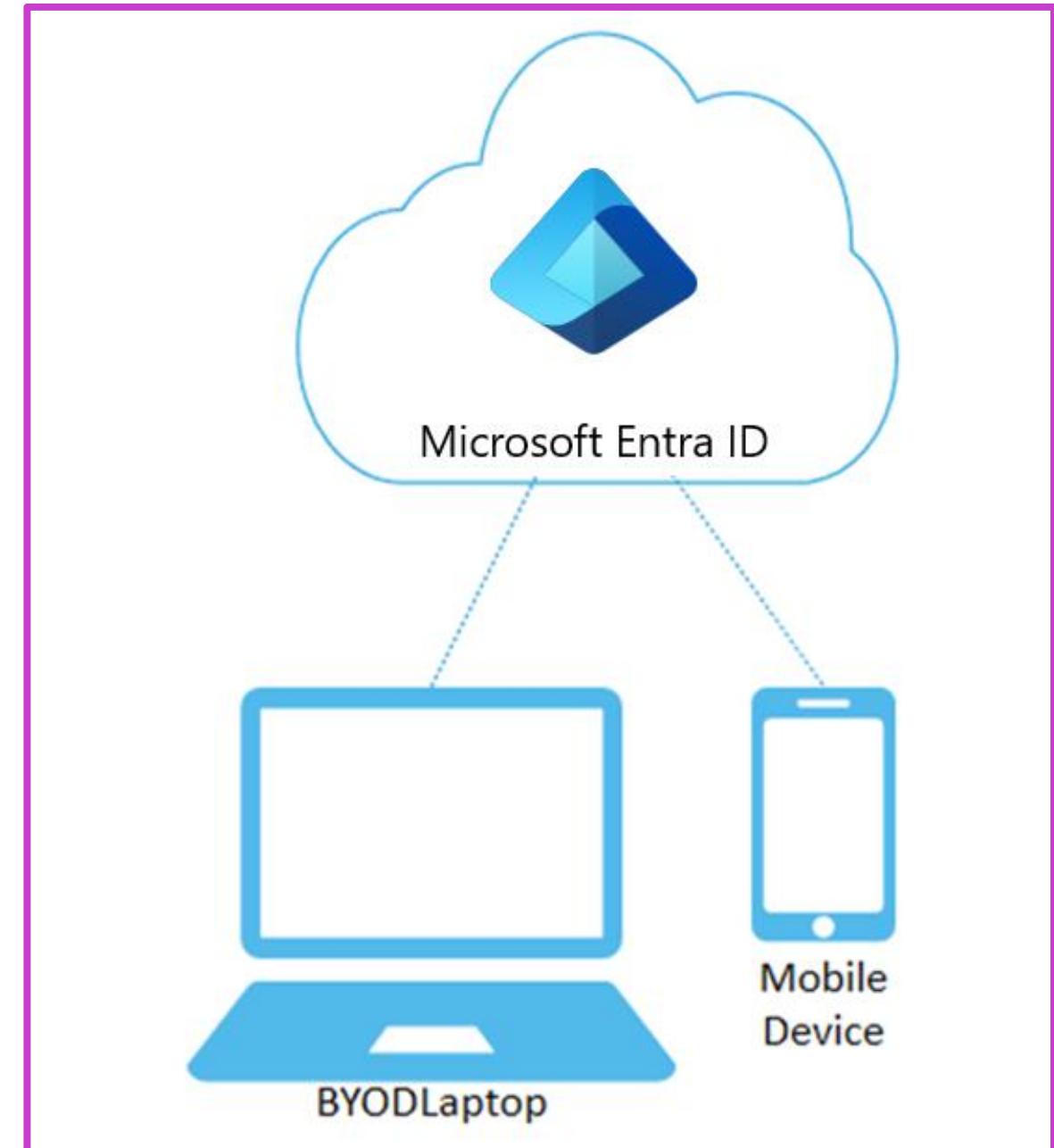


# Configure and manage device identities

# Microsoft Entra ID registered devices

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

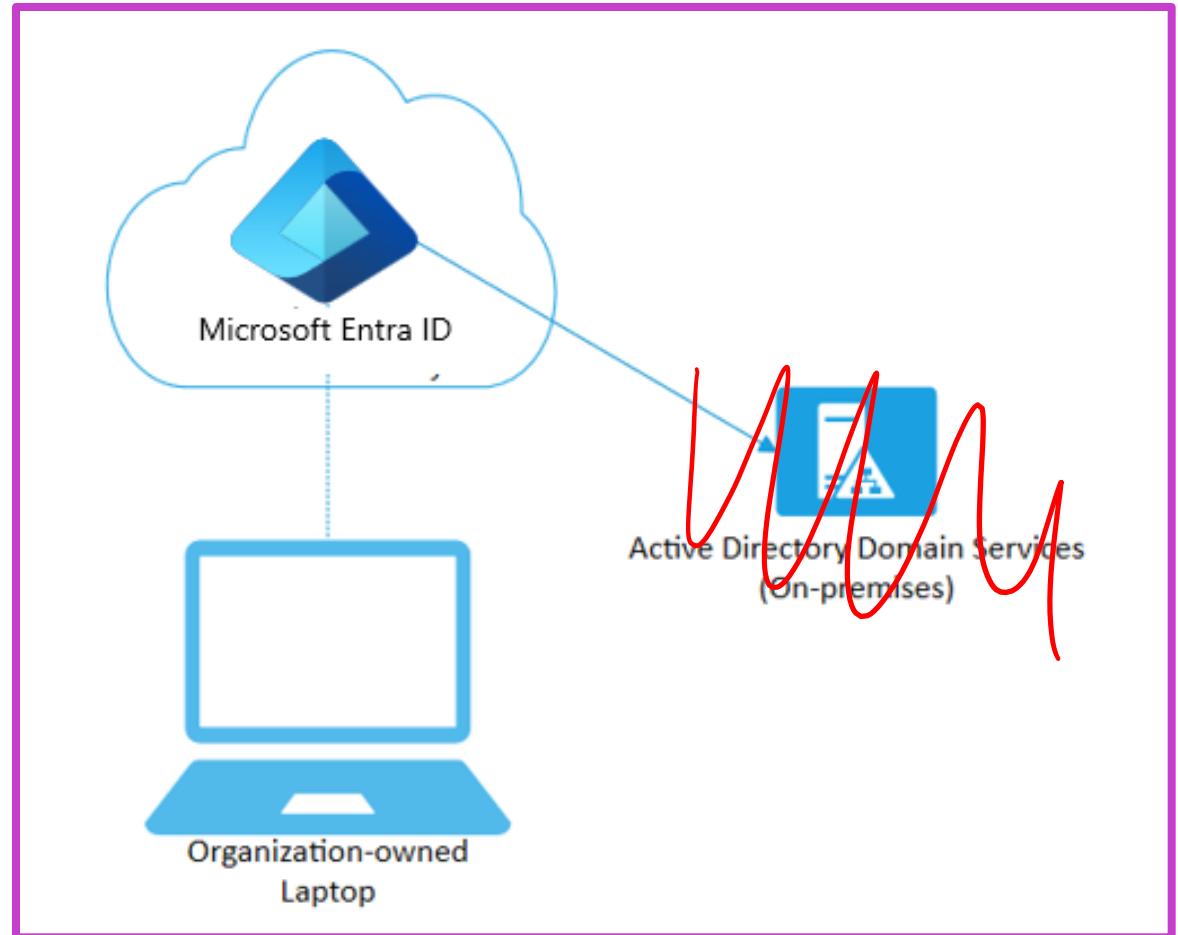
OS: Windows 10/11, iOS, Android, and  
MacOS    *Windows Server*



# Microsoft Entra ID joined devices

- Intended for cloud-first or cloud-only organizations
- Organization-owned devices
- Joined only to Microsoft Entra ID; organizational account required to sign in
- Easy to sign in with an Entra ID account
- Conditional Access policies can be applied to the device identity

OS: Windows 10/11 devices (not Home)

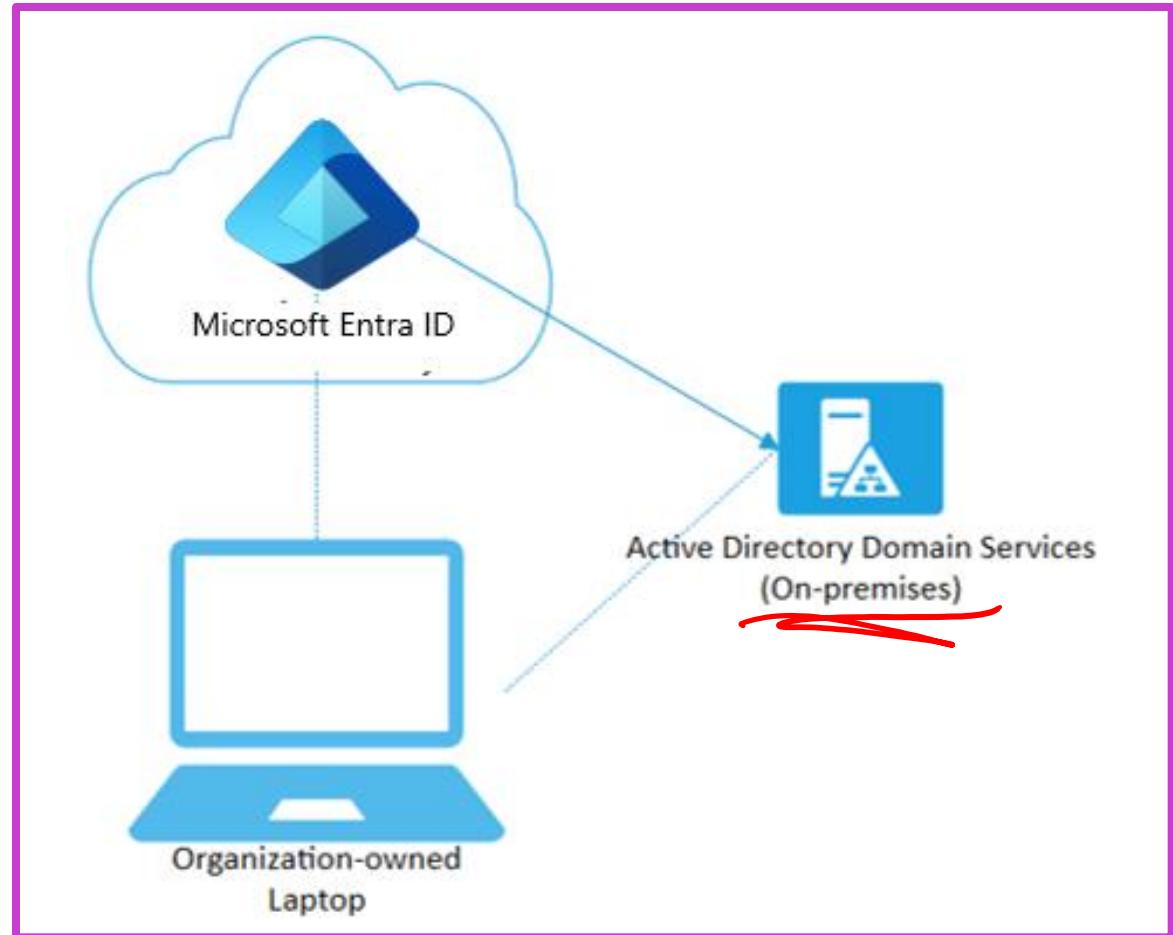


# Microsoft Entra hybrid joined devices

**Use Microsoft Entra hybrid joined devices if:**

- You have Win32 apps deployed to these devices using Microsoft Entra ID 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 8.1 devices in addition to Windows 10/11, plus later Windows Server versions.**



# Device writeback

- Use Microsoft Entra Connect to copy a 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
- Required to Single sign-on to be enabled.

# Manage licenses

# About licenses

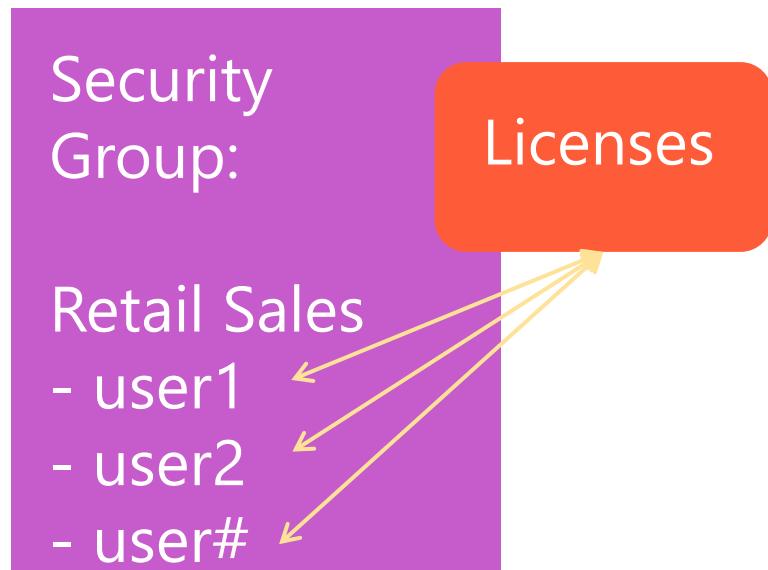
**Microsoft Azure is a cloud service that provides many built-in services for free.**

- Microsoft Entra ID comes as a free service
- Gain additional Microsoft Entra ID functionality with a premium P1 or P2 license
- Microsoft Entra ID Governance license
  - A targeted governance license focused on entitlement related features, lifecycle workflows, access reviews, and PIM.

**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
- Microsoft Entra ID assigns 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

# Demo—licenses

## Licenses | Overview

...  
Got feedback?

### Get started with license management

We are making it easier than ever to manage all your licenses. You can easily:

- Get a trial or purchase license
- See your purchased licenses and see the number of assigned licenses and the product expiry
- Manage licenses to a user or group
- View and delete your self-sign up subscriptions
- See all Microsoft Entra ID features available based on your licenses level

[Users](#)   [Groups](#)   [Self-service sign up products](#)





# Custom security attributes

# Manage custom security attributes

Business-specific attributes (key-value pairs) that you can define and assign to Microsoft Entra ID objects.

Example: Add app1 storage clearance attribute to users who need access; then set a conditional access policy.

The screenshot shows the Microsoft Entra ID 'Custom attributes' management interface. At the top, there's a search bar labeled 'Search attribute set name'. Below it, a table lists two attribute sets: 'Banker' and 'Clerk'. The 'Banker' set has a description 'This person can write checks against the bank' and a maximum of 25 attributes. The 'Clerk' set has a description 'Bank clerk' and a maximum of 25 attributes. To the right of the table, there are two open modal dialogs. The first, 'New attribute set', prompts for an 'Attribute set name' (with a red asterisk), a 'Description', and a 'Maximum number of attributes' (set to 25). The second, 'New attribute', prompts for an 'Attribute name' (with a red asterisk), a 'Description', a 'Data type' (set to 'String'), and several configuration options: 'Allow multiple values to be assigned' (set to 'No'), 'Only allow predefined values to be assigned' (set to 'No'), and a 'Predefined values' section with a '+ Add value' button. The 'Is active?' checkbox is also present.

Microsoft Entra ID P1/P2

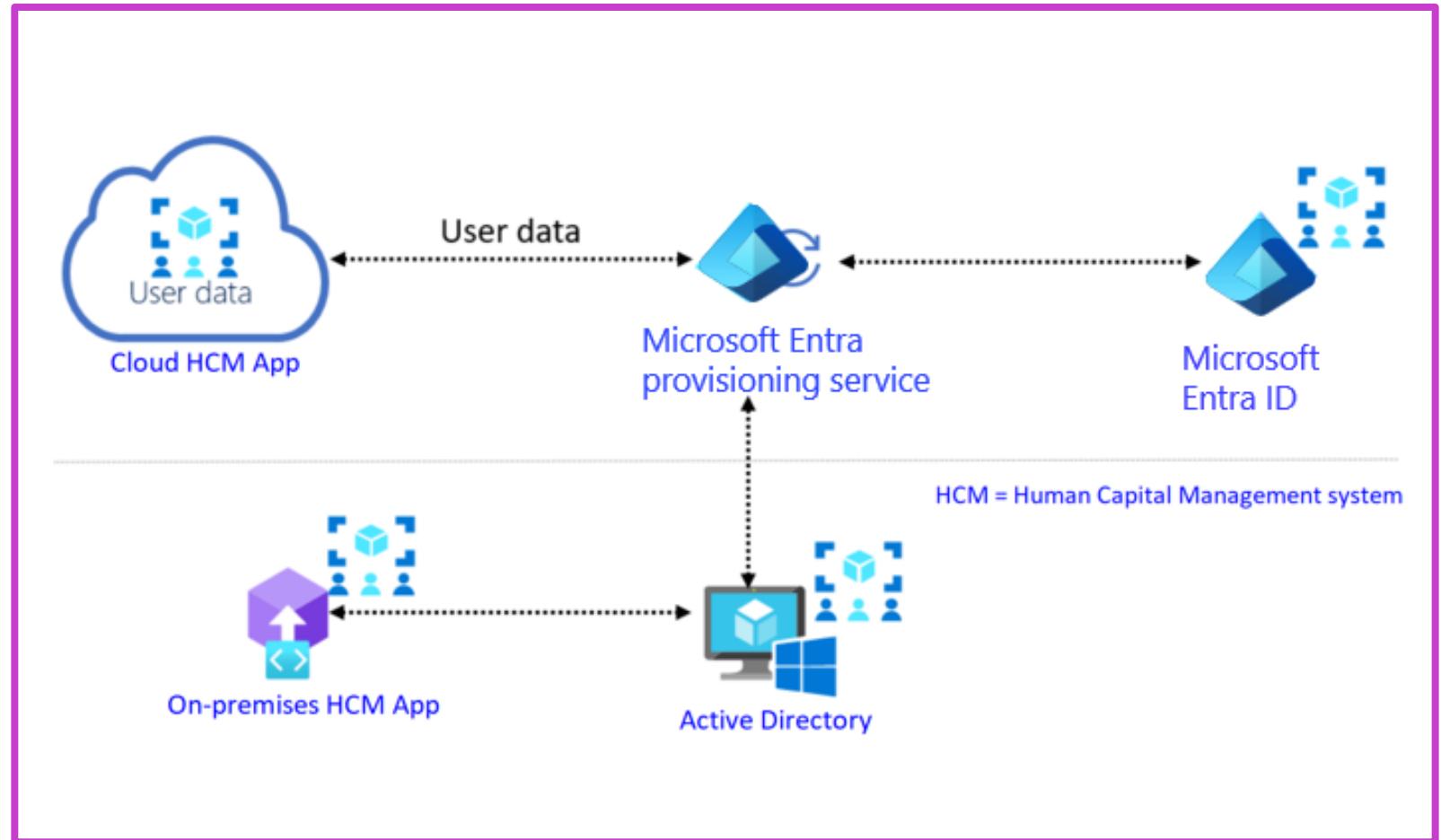
# Provisioning with SCIM

(training only, not on exam OD)

# Identity provisioning from cloud applications by using SCIM

SCIM—System for Cross-Domain Identity Management

Use employee records to provision Microsoft Entra ID accounts



# Configure and manage a Microsoft Entra tenant

# Objectives

- 1** Configure company branding
  - 2** Configure and manage Microsoft Entra roles
  - 3** Configure delegation by using administrative units
  - 4** Evaluate effective permissions
  - 5** Configure and manage domains in Microsoft Entra and Microsoft 365
  - 6** Configure tenant-wide settings
- 

# Company branding

# Company branding

## Customize the Microsoft Entra ID sign-in pages with company logos and other elements

- Requires Microsoft Entra ID P1/P2, or an M365 license
- Customize by language

### Customize default sign-in experience ...

Basics Layout Header Footer Sign-in form Review

Customize the default sign-in experience to personalize the sign-in page for anyone signing-in to your tenant.

#### Background

Upload background image, favicon or choose background color.

Favicon ⓘ

Select file(s)

Browse



Image size: 32x32px  
(resizable)  
Max file size: 5KB  
File Type: PNG (preferred),  
JPG, or JPEG

Background image ⓘ

Select file(s)

Browse

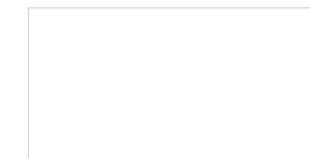


Image size: 1920x1080px  
Max file size: 300KB  
File Type: PNG, JPG, or JPEG

Page background color ⓘ

Not provided



Review + create

< Previous

Next: Layout >

# Configure and manage Microsoft Entra roles

# Admin access to Azure and Microsoft Entra ID

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

Azure portal—<https://portal.azure.com>

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

Microsoft Defender for Cloud Apps Portal—<https://security.microsoft.com/>

# Microsoft Entra roles

## Intended for:

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

Define access to Entra ID resources

Do not overlap with Azure roles by default

The screenshot shows the 'Roles and administrators | All roles' page in the Microsoft Entra admin center. The left sidebar is highlighted with a pink border and features sections for 'All roles', 'Protected actions', 'Diagnose and solve problems', 'Activity' (with 'Access reviews' and 'Audit logs'), and 'Troubleshooting + Support' (with 'New support request'). The 'All roles' section is currently selected. The main content area displays a table of roles with columns for 'Role', 'Description', 'Privileged', and 'Type'. A red vertical line is drawn from the bottom of the sidebar's pink border down to the top of the table, highlighting the sidebar area.

Role	Description	Privileged	Type
AI Administrator	Manage all aspects of Microsoft 365 Copilot and AI-related enterprise services in Microsoft 365.		Built-in
Application Administrator	Can create and manage all aspects of app registrations and enterprise apps.	PRIVILEGED	Built-in
Application Developer	Can create application registrations independent of the 'Users can register applications' setting.	PRIVILEGED	Built-in
Attack Payload Author	Can create attack payloads that an administrator can initiate later.		Built-in
Attack Simulation Administrator	Can create and manage all aspects of attack simulation campaigns.		Built-in

# Custom roles

## Roles and administrators | All roles

- All roles
- Protected actions
- Diagnose and solve problems
- Activity
- Access reviews
- Audit logs
- Troubleshooting + Support
- New support request

[+ New custom role](#) [Delete custom role](#) [Download assignments](#) [Refresh](#) [Preview features](#) [Got feedback?](#)

Get just-in-time access to a role when you need it using PIM. Learn more about PIM →

Your [Basics](#) [Permissions](#) [Review + create](#)

Learn mo

Roles created here will be available for assignment on other resources as well. [Learn more](#)

[Search](#)

Role

App

Description

App

Attrib

Baseline permissions

Start from scratch

Clone from a custom role

Attack Simulation Administrator

Can create and manage all aspects of attack

Attribute Assignment Administrator

Assign custom security attribute keys and va

Attribute Assignment Reader

Read custom security attribute keys and val

Attribute Definition Administrator

Define and manage the definition of custom

Basics [Permissions](#) [Review + create](#)

Add permissions for this custom role. Currently, permissions for Application registrations and Enterprise applications are supported in custom roles. [Learn more](#)

[Search by permission name or description](#)

Permission	Description
<input type="checkbox"/> microsoft.directory/applicationPolicies/allProperties/read	Read all properties (including privileged properties) on application policies
<input type="checkbox"/> microsoft.directory/applicationPolicies/allProperties/update	Update all properties (including privileged properties) on application policies
<input type="checkbox"/> microsoft.directory/applicationPolicies/basic/update	Update standard properties of application policies
<input type="checkbox"/> microsoft.directory/applicationPolicies/create	Create application policies
<input type="checkbox"/> microsoft.directory/applicationPolicies/createAsOwner	Create application policies, and creator is added as the first owner

Create a custom role to meet your security goals or needs

Requires a Microsoft Entra ID premium license

# Assigning roles—to a user or group

Home > Users > Adele Vance

Adele Vance | Assigned roles

User

Search Add assignments Refresh Got feedback?

Overview Audit logs Sign-in logs Diagnose and solve problems

Manage

Custom security attributes Assigned roles Administrative units

Eligible assignments Active assignments Expired assignments

Search by role

Role	Principal name	Scope	Membership
Application Administrator	AdeleV	Directory	Direct

Assign built-in or custom roles

Assign to a user, group, service principal or managed identity

Use principle of least privilege when assigning

# Assign users or groups to a role

The screenshot shows the Microsoft Azure portal interface. On the left, there's a navigation bar with 'Home > Contoso > Billing administrator'. Below it is a sidebar with options like 'Diagnose and solve problems', 'Manage' (which is selected), 'Assignment' (highlighted with a green box), 'Description', 'Activity', 'Bulk operation results', 'Troubleshooting + Support', and 'New support request'. In the main content area, under 'Manage', there's a button labeled '+ Add assignments' with a green box around it. A tooltip says 'You can also assign b...'. Below this is a search bar with 'Search by name' and a 'Name' input field containing 'No role assignments found'. To the right, a modal window titled 'Add assignments' lists three users: Adele Vance, Alex Wilber, and Allan Devouna, each with their email and organization information. At the bottom of the modal, it says 'Selected items' and 'No items selected'.

Identities can be added to a role

Alternative method to assign roles

Use principle of least privilege when assigning

# Exercise—Explore dynamic groups

This exercise teaches students how to create a dynamic group with all users as members.

[Launch this Exercise in GitHub](#)



**Dynamic membership rules**

Save Discard | Got feedback?

Configure Rules Validate Rules (Preview)

You can use the rule builder or rule syntax text box to create or edit a dynamic mem

And/Or	Property
And	<Choose a Property>
+ Add expression	+ Get custom extension properties ⓘ

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

**Rule syntax**

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

# Assigning Azure roles to a subscription or broader scope

The screenshot shows the Azure Access control (IAM) interface for the 'rgBuild' resource group. The 'Role assignments' tab is selected. A red box highlights the '+ Add' button. The 'Add role assignment' dialog is open, showing the 'Members' tab selected. The 'Selected role' is set to 'Azure AI Developer'. The 'Assign access to' section has 'User, group, or service principal' selected. The 'Members' section shows a table with columns: Role, Members\*, Conditions, Assignment type, and Review + assign. The table currently displays one row for 'Azure AI Developer'. The 'Description' field at the bottom is optional.

Assign roles to manage subscriptions, management groups, and resource groups

# Using Microsoft Entra 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 Microsoft Entra ID 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**

# Delegating administrative tasks with built-in roles

## Delegating app administration

- Password administrator role
- Group administrator role

## Delegating app registration

- Application developer role

## Delegating app ownership

- Enterprise application owner role
- Application registration owner role

The screenshot shows the 'Roles and administrators | All roles' page in the Microsoft Entra ID portal. The left sidebar includes links for 'All roles', 'Protected actions', 'Diagnose and solve problems', 'Activity' (with 'Access reviews' and 'Audit logs'), and 'Troubleshooting + Support' (with 'New support request'). The main content area displays information about 'Administrative roles', stating they are used for granting access for privileged actions. It features a search bar ('Application') and a 'Add filters' button. A table lists three built-in roles:

Role	Description	Privileged	Ass...	Type
Application Administrator	Can create and manage all aspects o	PRIVILEGED	0	Built-in
Application Developer	Can create application registrations i	PRIVILEGED	0	Built-in
Attribute Provisioning Administrator	Read and edit the provisioning config	PRIVILEGED	0	Built-in

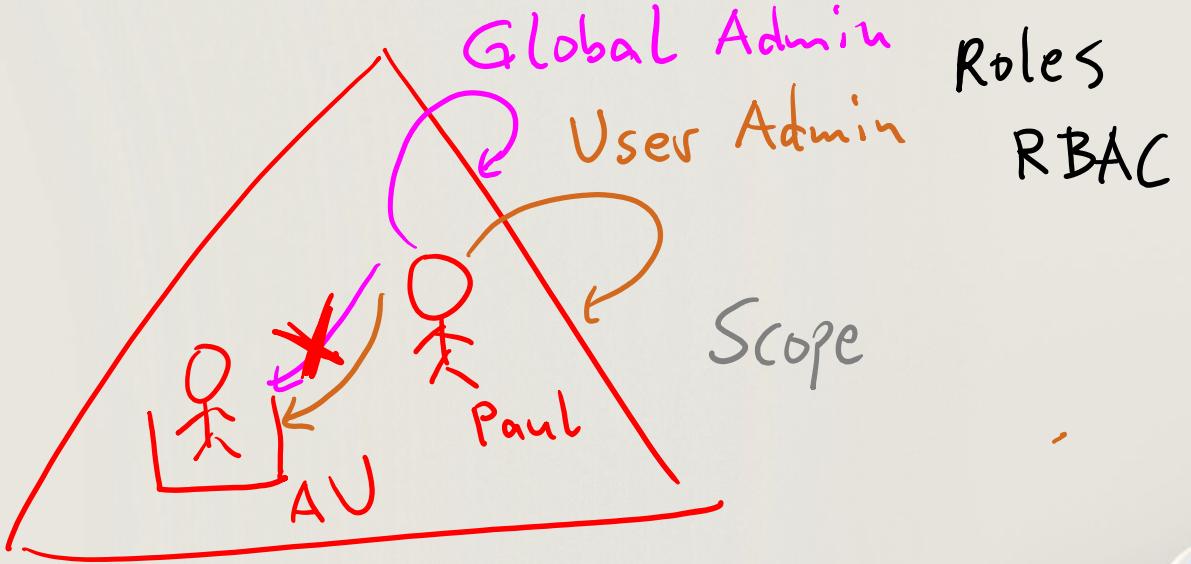
# Demo—assigning roles

Resource type  
Directory

Select role i  
 ▼

Scope type i  
 ▼

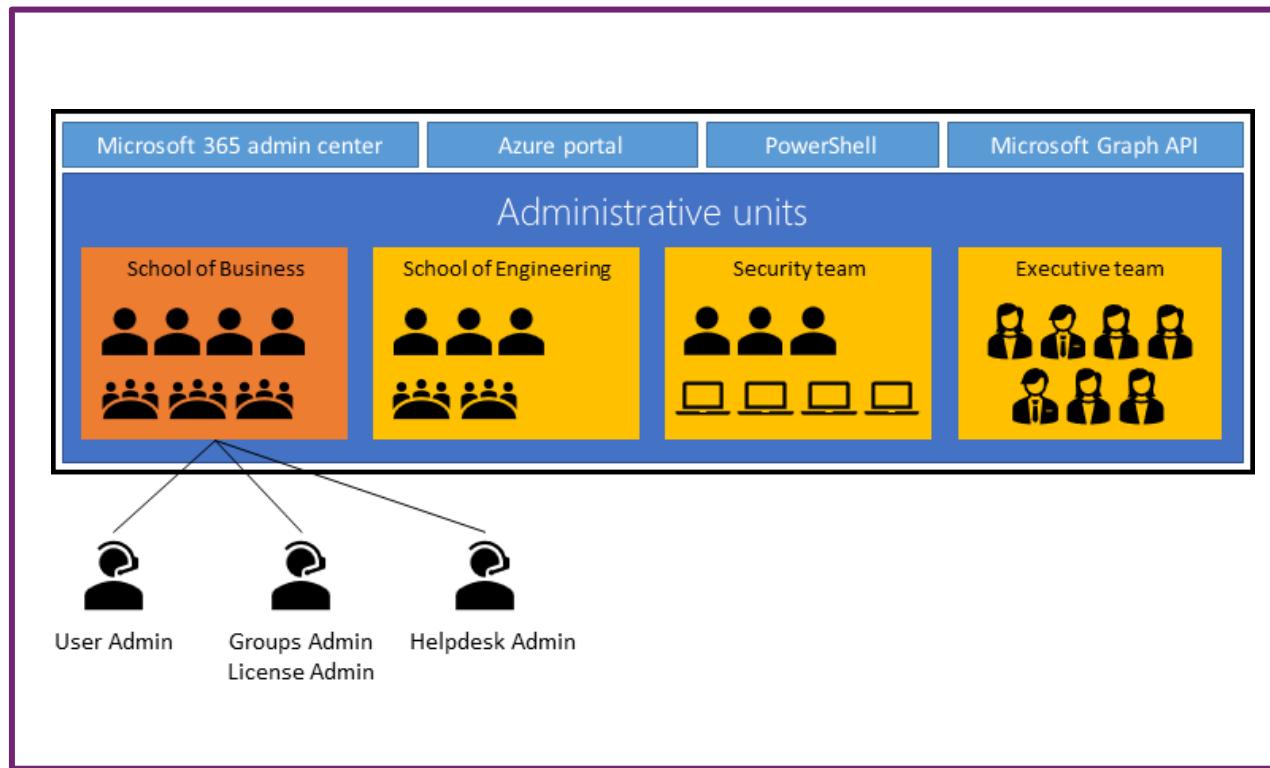
Select member(s) \* i  
No member selected



## When to use Administrative units

# About administrative units

- Administrative units are Microsoft Entra ID resources that can be containers for other Microsoft Entra resources.
- An administrative unit can contain only users, groups, and devices.
- Administrative units restrict permissions in a role to a specific 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 Microsoft Entra 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
- Set up a person who 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**

JIT

JEA

# Administrative Units

## Delegating authentication administration

- Authentication administrator role

## Delegating licensing

- License administrator

## Delegating user, group, and password management

- User administrator

The screenshot shows the Microsoft Entra admin center interface. The top navigation bar is black with the text "Microsoft Entra admin center". Below it, the left sidebar has a dark grey background with white text and icons. The sidebar includes links for "Applications", "Roles & admins", "Admin units" (which is currently selected and highlighted in blue), and "Delegated admin partners". At the bottom of the sidebar is a "Billing" link. To the right of the sidebar, the main content area has a white background. It displays the title "Administrative units" in large bold letters. Below the title are three buttons: "Learn more" (with a blue info icon), "Add" (with a blue plus sign icon), and "Delete" (with a grey trash bin icon). A search bar labeled "Search administrative units" is present. Below the search bar is a table with one row, showing a checkbox next to the name "sc300AU".

# Evaluate effective permissions for Microsoft Entra role

# Permissions in Microsoft Entra ID

Permission—consent or authorization to perform a specific action.

Who gets permissions:

Member Users	External Users	Applications	Devices
--------------	----------------	--------------	---------

Example default permissions for each:

<ul style="list-style-type: none"><li>• <b>Enumerate list of users</b></li><li>• <b>Invite external users</b></li><li>• <b>Change their password</b></li><li>• <b>Manage Photo</b></li><li>• <b>Create groups</b></li><li>• <b>And so on</b></li></ul>	<ul style="list-style-type: none"><li>• <b>Read own properties</b></li><li>• <b>Change their password</b></li><li>• <b>Search for groups</b></li><li>• <b>Cannot invite groups</b></li><li>• <b>And so on</b></li></ul>	<ul style="list-style-type: none"><li>• <b>App must be registered</b></li><li>• <b>API and permissions assigned in registration</b></li><li>• <b>Examples – read, write, verify, and others</b></li></ul>	<ul style="list-style-type: none"><li>• <b>Device must be registered or joined to the Microsoft Entra tenant</b></li></ul>
--	---	---	--

\* Augment or restrict permissions with settings and role assignments

# Augment or restrict permissions

 **Users | User settings**

**Default user role permissions**

[Learn more](#)

Users can register applications  Yes

Restrict non-admin users from creating tenants  No

Users can create security groups  Yes

**Guest user access**

[Learn more](#)

Guest user access restrictions  Guest users have the same access as members (most inclusive)  Guest users have limited access to properties and memberships of directory objects  Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)

**Administration portal**

[Learn more](#)

Restrict access to Microsoft Entra ID administration portal  No

**LinkedIn account connections**

[Learn more](#)

Allow users to connect their work or school account with LinkedIn  Yes  Selected group

 **Roles and administrators | All roles**

[New custom role](#) [Delete custom role](#) [Download assignments](#) [Refresh](#)

**Get just-in-time access to a role when you need it using PIM.** [Learn more about PIM](#)

**Your Role:** Global Administrator and 3 other roles

**Administrative roles**

Administrative roles are used for granting access for privileged actions in Microsoft Entra ID. We can use administrative roles to grant access to manage other parts of Microsoft Entra ID not related to application configuration. [Learn more](#)

[Learn more about Microsoft Entra ID role-based access control](#)

Search by name or description [Add filters](#)

Role	Description
<input type="checkbox"/> AI Administrator	Manage all aspects of Microsoft 365 Copilot
<input type="checkbox"/> Application Administrator	Can create and manage all aspects of app registrations
<input type="checkbox"/> Application Developer	Can create application registrations independently
<input type="checkbox"/> Attack Payload Author	Can create attack payloads that an administrator can use in attacks
<input type="checkbox"/> Attack Simulation Administrator	Can create and manage all aspects of attack simulations
<input type="checkbox"/> Attribute Assignment Administrator	Assign custom security attribute keys and values
<input type="checkbox"/> Attribute Assignment Reader	Read custom security attribute keys and values
<input type="checkbox"/> Attribute Definition Administrator	Define and manage the definition of custom security attributes
<input type="checkbox"/> Attribute Definition Reader	Read the definition of custom security attributes

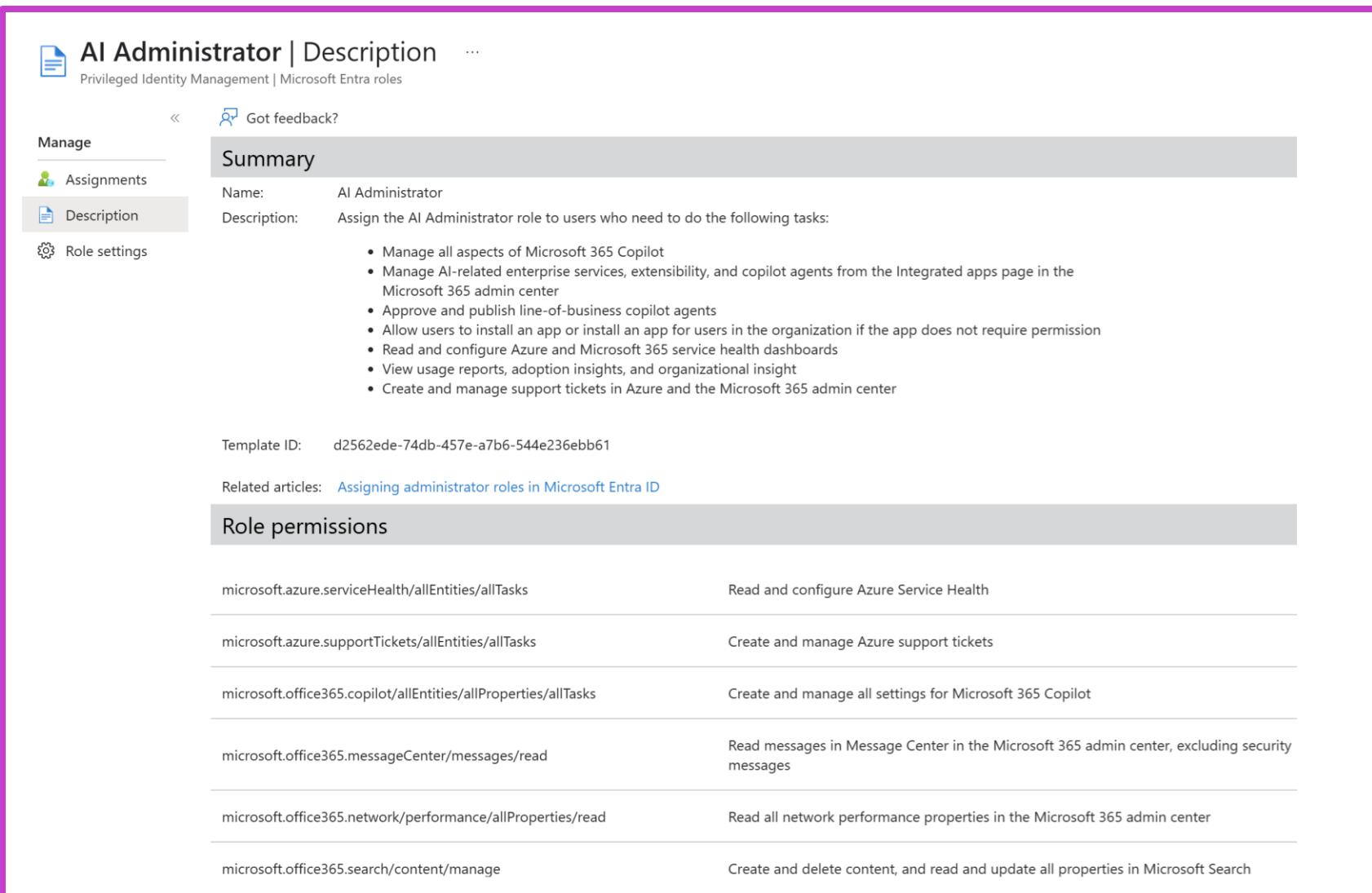
# Analyze permission

## 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 'AI Administrator | Description' page in the Microsoft Entra portal. The 'Summary' section displays the role's name, description, and a list of permissions. The 'Role permissions' section lists specific API permissions and their descriptions.

**Summary**

Name: AI Administrator  
Description: Assign the AI Administrator role to users who need to do the following tasks:

- Manage all aspects of Microsoft 365 Copilot
- Manage AI-related enterprise services, extensibility, and copilot agents from the Integrated apps page in the Microsoft 365 admin center
- Approve and publish line-of-business copilot agents
- Allow users to install an app or install an app for users in the organization if the app does not require permission
- Read and configure Azure and Microsoft 365 service health dashboards
- View usage reports, adoption insights, and organizational insight
- Create and manage support tickets in Azure and the Microsoft 365 admin center

Template ID: d2562ede-74db-457e-a7b6-544e236ebb61

Related articles: [Assigning administrator roles in Microsoft Entra ID](#)

**Role permissions**

microsoft.azure.serviceHealth/allEntities/allTasks	Read and configure Azure Service Health
microsoft.azure.supportTickets/allEntities/allTasks	Create and manage Azure support tickets
microsoft.office365.copilot/allEntities/allProperties/allTasks	Create and manage all settings for Microsoft 365 Copilot
microsoft.office365.messageCenter/messages/read	Read messages in Message Center in the Microsoft 365 admin center, excluding security messages
microsoft.office365.network/performance/allProperties/read	Read all network performance properties in the Microsoft 365 admin center
microsoft.office365.search/content/manage	Create and delete content, and read and update all properties in Microsoft Search

# Configure and manage custom domains

# Adding a custom domain name

- Tenant has a default domain name ending in **onmicrosoft.com**
- Add your custom domain name and make it the primary domain name
- Add multiple custom domain names for an organization
- Add a root domain before adding subdomains

The screenshot shows the Microsoft Entra admin center interface. The left sidebar includes links for Applications, Roles & admins, Billing, Settings, Preview hub, Domain names (which is selected and highlighted in blue), Mobility, and Protection. The main content area is titled "Custom domain names" and displays a list of items: "Custom domain names" (selected and highlighted in gray), "Custom url domains (Preview)", "Troubleshooting + Support", and "New support request". A search bar at the top right contains the text "Contoso.onmicrosoft.com". Handwritten annotations in orange highlight the "Microsoft Entra admin center" header and point to the "Custom domain names" and "Custom url domains (Preview)" links.

# Configure tenant-wide settings

# 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 Microsoft Entra ID administrative portal
- Sign in with LinkedIn
- Manage security defaults ✓
- External collaboration
  - Restricting who can invite guest and other settings ✓

# User settings

Microsoft Entra admin center → Identity → Users → User Settings

- App registrations—users can register applications
- Administration portal – Restrict access to the Microsoft Entra ID administration portal
- LinkedIn account connections – Allow users to connect their work or school account with LinkedIn
- Other

The screenshot shows the 'Users | User settings' page in the Microsoft Entra admin center. On the left, there is a sidebar with icons and labels: All users, Audit logs, Sign-in logs, Diagnose and solve problems, Deleted users, Password reset, User settings (which is highlighted with a gray background), Bulk operation results, and New support request. To the right, under 'Default user role permissions', there are three settings with toggle switches:

- Users can register applications: Yes (blue toggle switch)
- Restrict non-admin users from creating tenants: No (gray toggle switch)
- Users can create security groups: Yes (blue toggle switch)

# User settings—external users

Microsoft Entra ID → Identity → Users → User Settings

- App registrations—users can register applications
- Administration portal—restrict access to the Microsoft Entra ID administration portal
- LinkedIn account connections—allow users to connect their work or school account with LinkedIn
- Manage user feature previews
- External collaboration setting

Home > Default Directory >

## External collaboration settings

Save Discard

Email one-time passcode for guests has been moved to All Identity Providers. →

### Guest user access

Guest user access restrictions ⓘ

[Learn more](#)

- Guest users have the same access as members (most inclusive)
- Guest users have limited access to properties and memberships of directory objects
- Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)

### Guest invite settings

Guest invite restrictions ⓘ

[Learn more](#)

- 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
- No one in the organization can invite guest users including admins (most restrictive)

Enable guest self-service sign up via user flows ⓘ

[Learn more](#)

Yes No

# Tenant properties

Entra Admin Center → Identity → Overview → Properties

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

Home >  
Default Directory

+ Add Manage tenants What's new Preview fe...

*(i)* Azure Active Directory is becoming Microsoft Entra ID. [Learn more](#)

Overview Monitoring Properties Recommendations To...

Name	Contoso
Country or region	United States
Data location	United States datacenters
Notification language	English
Tenant ID	
Technical contact	
Global privacy contact	
Privacy statement URL	

Access management for Azure resources

# Demo—set tenant-wide settings

The screenshot shows a user interface for managing tenant-wide settings. At the top, there is a navigation bar with five tabs: Overview, Monitoring, Properties (which is underlined, indicating it is the active tab), Recommendations, and Tutorials. Below the navigation bar, there are five configuration items, each consisting of a label on the left and a value on the right.

Name	Contoso
Country or region	United States
Data location	United States datacenters
Notification language	English
Tenant ID	(Empty input field)

# References (1 of 2)

**Classic subscription administrator roles, Azure roles, and Microsoft Entra roles**

<https://learn.microsoft.com/azure/role-based-access-control/rbac-and-directory-admin-roles>

**Understand Azure role definitions**

<https://learn.microsoft.com/azure/role-based-access-control/role-definitions>

**Privileged Identity Management**

<https://learn.microsoft.com/entra/id-governance/privileged-identity-management/>

**How To: Configure the Microsoft Entra Multi-Factor Authentication registration policy**

<https://learn.microsoft.com/entra/id-protection/howto-identity-protection-configure-mfa-policy>



# References (2 of 2)

**Conditional Access: Require MFA for administrators**

<https://learn.microsoft.com/entra/identity/conditional-access/howto-conditional-access-policy-admin-mfa>

**Conditional Access: Require MFA for Azure management**

<https://learn.microsoft.com/entra/identity/conditional-access/howto-conditional-access-policy-azure-management>

**Conditional Access: Block legacy authentication**

<https://learn.microsoft.com/entra/identity/conditional-access/howto-conditional-access-policy-block-legacy>

**Conditional Access: Require MFA for all users**

<https://learn.microsoft.com/entra/identity/conditional-access/howto-conditional-access-policy-all-users-mfa>



# Implement and manage external identities

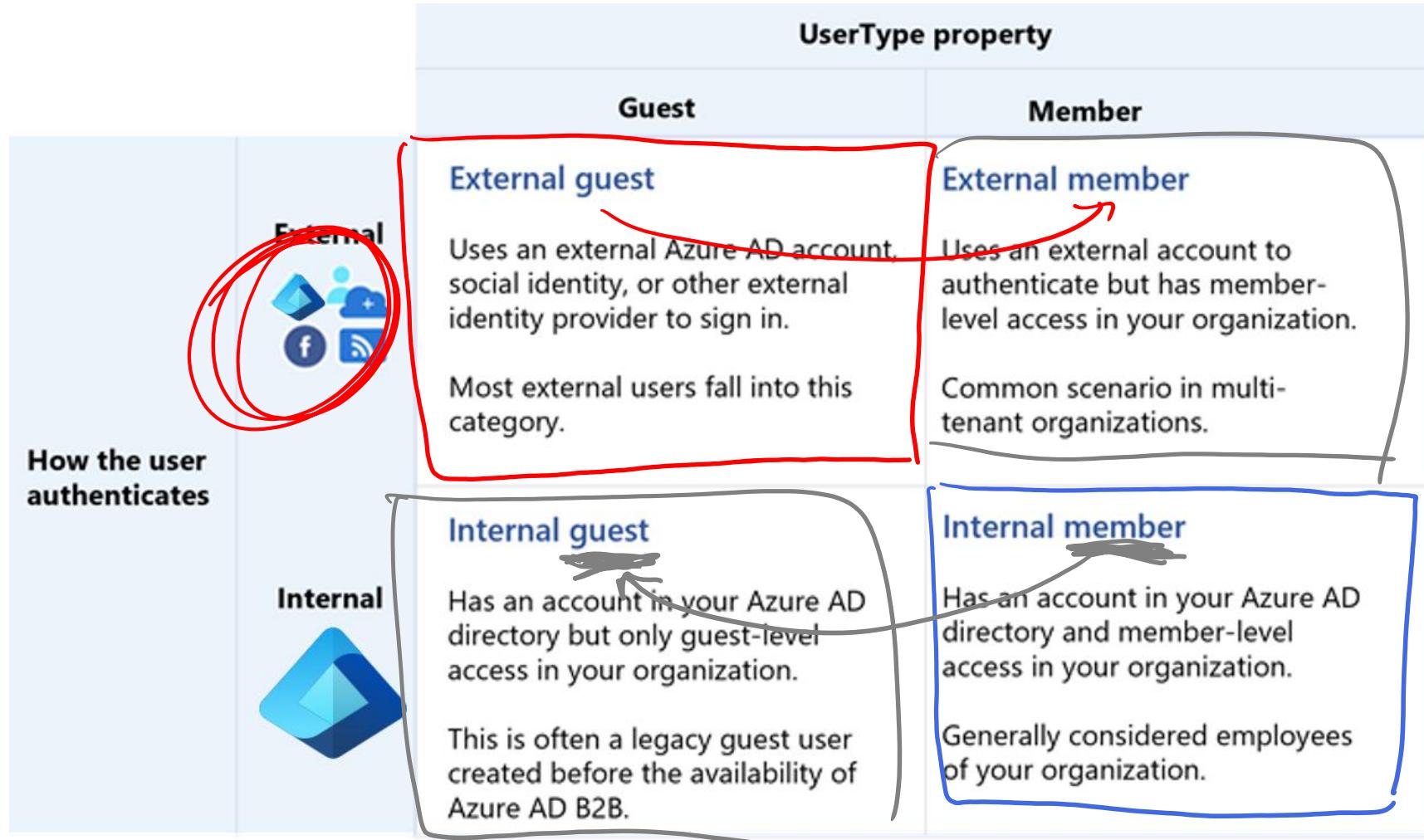
Guest  
Member

# Objectives

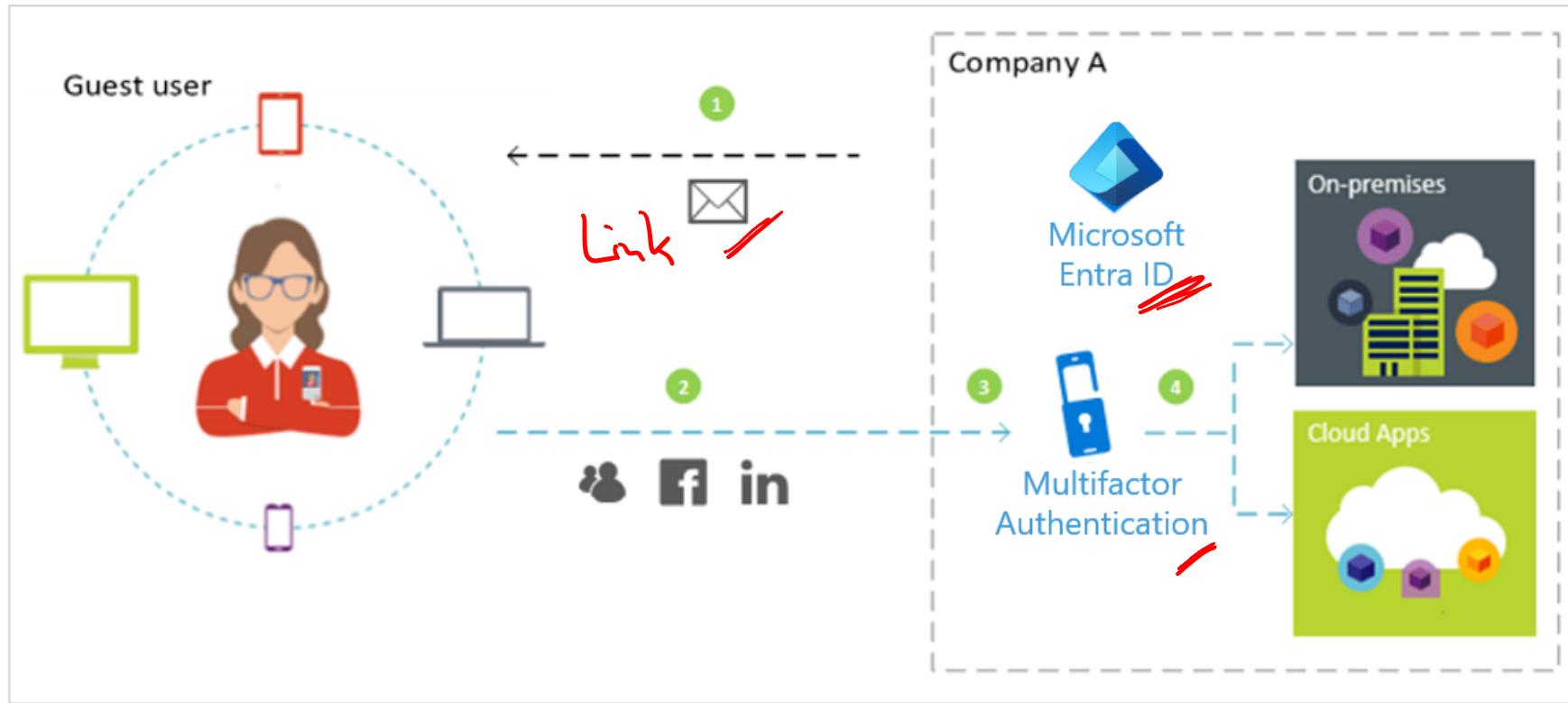
- 1 Describe guest users and B2B accounts
- 2 Manage external collaboration
- 3 How external users are managed in Microsoft 365
- 4 Invite external users—individually or in bulk
- 5 Manage external user accounts in Microsoft Entra ID
- 6 Implement cross-tenant access controls
- 7 Configure identity providers
- 8 Implement and manage Verified ID

Describe external users,  
B2B accounts, and manage  
external collaboration

# Relationship between external and member users



# Microsoft Entra B2B



**Guest user**—a user invited to join your corporate Microsoft Entra ID.

Sourced from another directory, social media, partners, and other services.

Secure B2B collaboration projects enabled.

# Collaborating with external users

- Invite external users into your tenant typically 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

# Exercise—configure external collaboration



This exercise teaches students how to configure external collaboration settings.

[Launch this Exercise in GitHub](#)

Guest invite settings

Guest invite restrictions ⓘ

[Learn more](#)

- 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
- No one in the organization can invite guest users including admins (most restrictive)

Enable guest self-service sign up via user flows ⓘ

# External users from M365 workloads

# Microsoft 365 admin center

The screenshot shows the Microsoft 365 admin center interface. On the left is a navigation sidebar with icons for Home, Copilot, Users (selected), Active users, Contacts, Guest users (selected), Deleted users, and Teams & groups. The main content area is titled "Guest users" and shows a message: "Guests have access to Teams. Manage Teams settings". It includes a "Add a guest user" button and a "Refresh" link. Below is a table with columns for "Display name" and "Choose columns". Two entries are listed: "External User" and "Robert at Google".

Manage guest users in the Microsoft 365 admin center.

Similar process to Microsoft Entra ID.

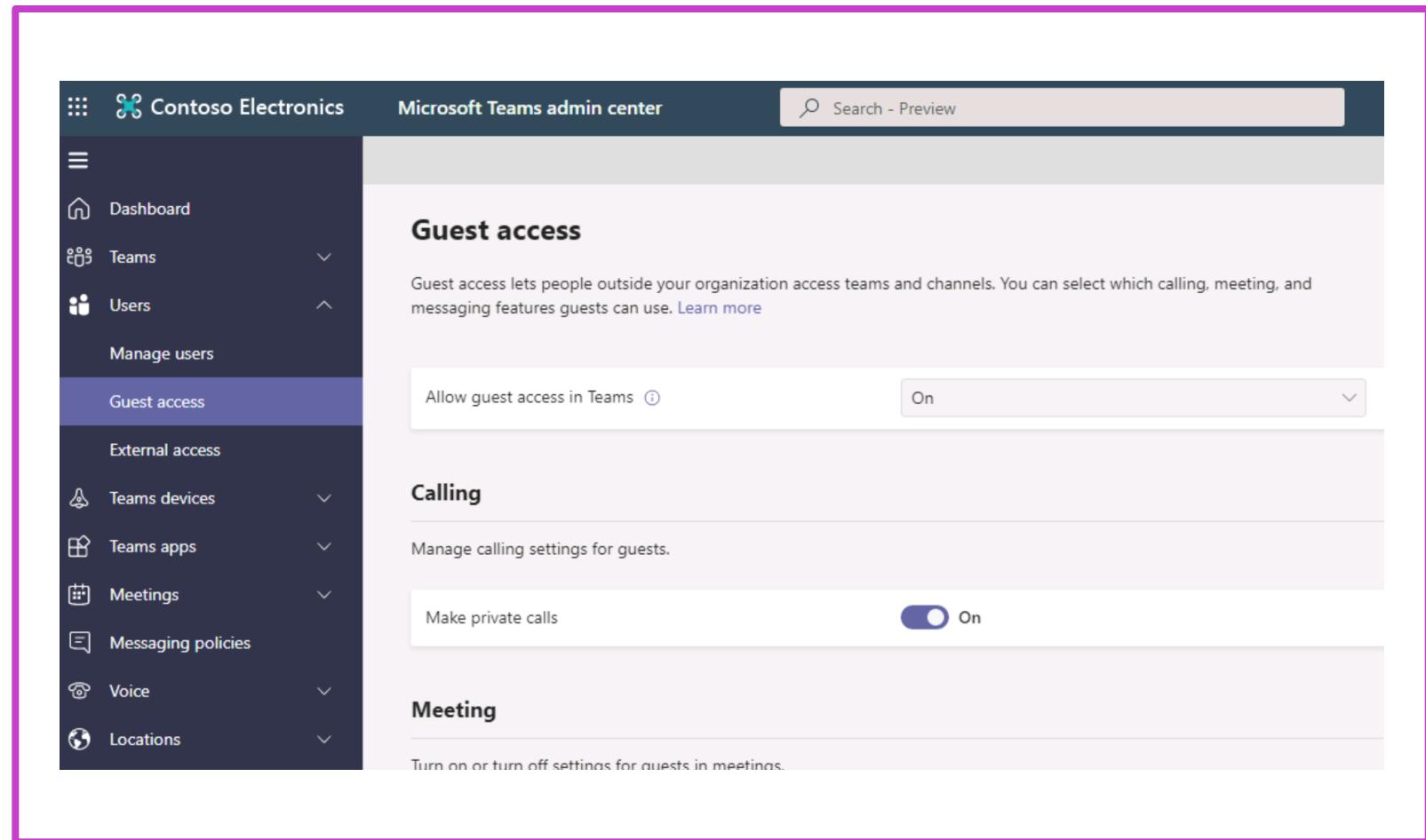
Always use Zero Trust principles when managing.

# 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 external user 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 a section for 'Allow guest access in Teams' which is set to 'On'. Below this are sections for 'Calling' (with a 'Make private calls' toggle switch turned '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 Microsoft Entra ID

# Demo—add external user (single or bulk)

The screenshot shows the Microsoft 365 Admin Center interface for managing users. At the top, there is a navigation bar with several actions: 'New user' (with a dropdown arrow), 'Edit (Preview)' (with a dropdown arrow), 'Delete', 'Download users' (with a downward arrow icon), and 'Bulk operations' (with a clipboard icon and a dropdown arrow). Below this, there are two main sections: 'Create new user' (described as 'Create a new internal user in your organization') and 'Invite external user' (described as 'Invite an external user to collaborate with your organization').

# Manage external user accounts in Microsoft Entra ID

# External users—restricted by default

## External users do not have:

- Assigned roles
- Group membership
- Licenses

Grant access as your security posture and organization needs dictate using Entitlement or Manually.

The screenshot shows the Microsoft Entra ID interface for managing user roles. The top navigation bar includes 'Chris Green | Assigned roles', 'User', 'Search', '+ Add assignments', 'Refresh', and 'Got feedback?'. Below the navigation are tabs for 'Eligible assignments', 'Active assignments' (which is selected), and 'Expired assignments'. A search bar for 'Search by role' is present. The main area displays a table with columns: 'Role', 'Principal name', 'Scope', and 'Membership'. A message 'No results' is shown. On the right, a modal window titled 'Add assignments' is open, with tabs for 'Membership' (selected) and 'Setting'. It shows 'Resource' set to 'qg14', 'Resource type' set to 'Directory', and 'Select role' set to 'Attribute Log Reader'. The 'Scope type' dropdown is set to 'Directory'. Under 'Select member(s)', it says '1 Member(s) selected' and shows 'Selected member(s)' with 'Chris Green' listed. A 'Remove' button is at the bottom right of the modal.

# 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 ⓘ

Search role

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

Selected member(s) ⓘ

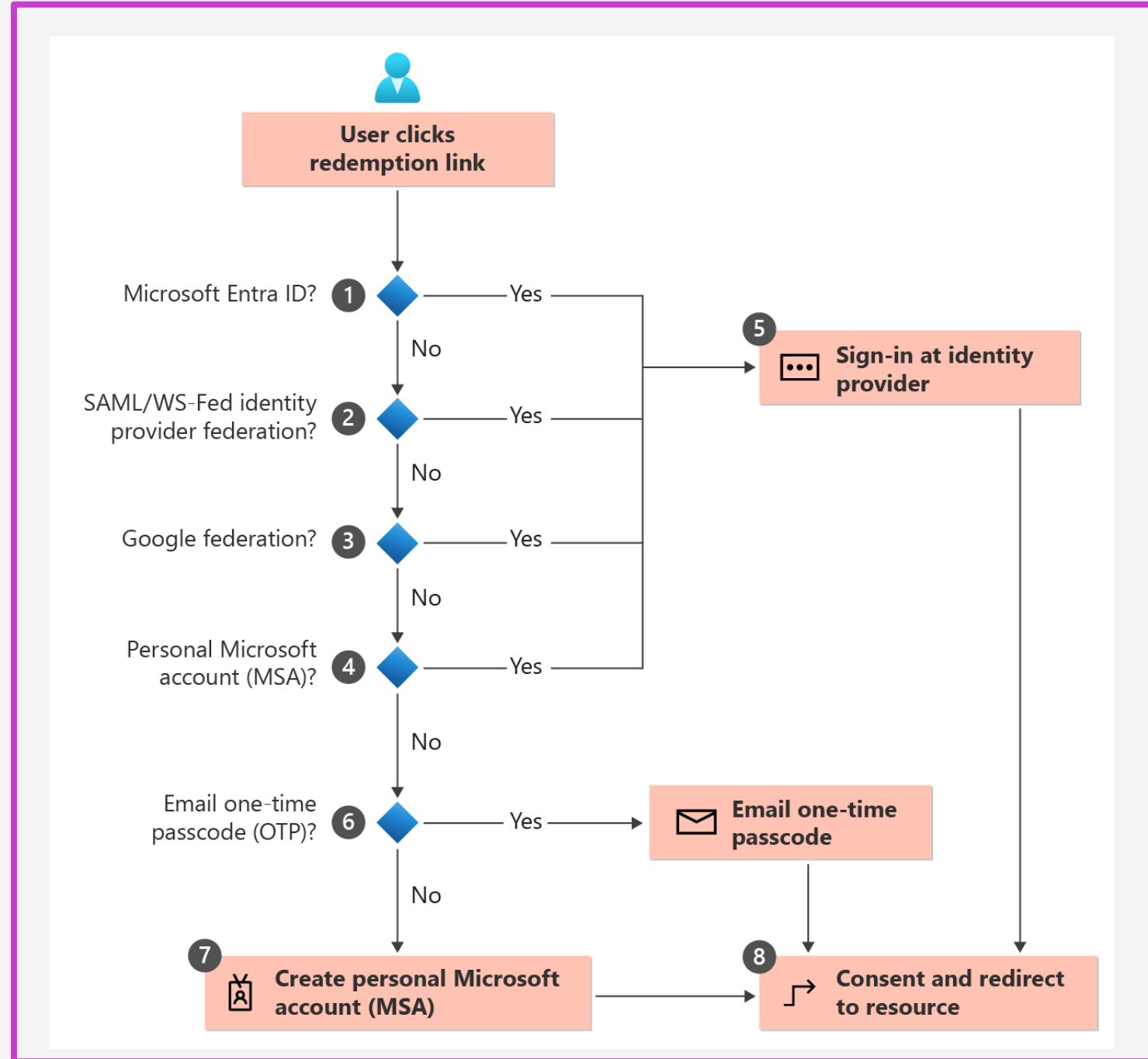
Sam Oogle

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 redemption

## External identity remediation types

- Microsoft Entra ID native
- SAML / WS-Fed
- Google (other social media)
- Personal MSA
- One-time passcode



# 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. The 'Cross-tenant access settings' tab is selected. The left sidebar includes links for Overview, All identity providers, External collaboration settings, Diagnose and solve problems, Self-service sign up (with Custom user attributes, All API connectors, and Custom authentication extensions), Subscriptions (with Linked subscriptions), Lifecycle management (with Terms of use and Access reviews), and Troubleshooting + Support. The main content area has tabs for 'Default settings' (selected), 'Organizational settings', and 'Microsoft cloud settings'. The 'Default settings' tab displays a table of inbound access settings:

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

Below this is a section for 'Outbound access settings' with a 'Edit outbound defaults' link.

# Configure cross-tenant synchronization

## Synchronize users and attributes across organizations

- Automatically create and delete users cross-tenant.
- Move attributes and settings across tenants.
- Synced users benefit from features like Conditional Access and analytics.
- Push only—from source tenant to a destination tenant.

Home > Default 2 | Cross-tenant synchronization > Cross-tenant synchronization | Configurations > Fabrikam | Overview >

### Provisioning

Save Discard

Provisioning Mode

Automatic

Use Azure AD to manage the creation and synchronization of user accounts in Fabrikam based on user and group assignment.

Admin Credentials

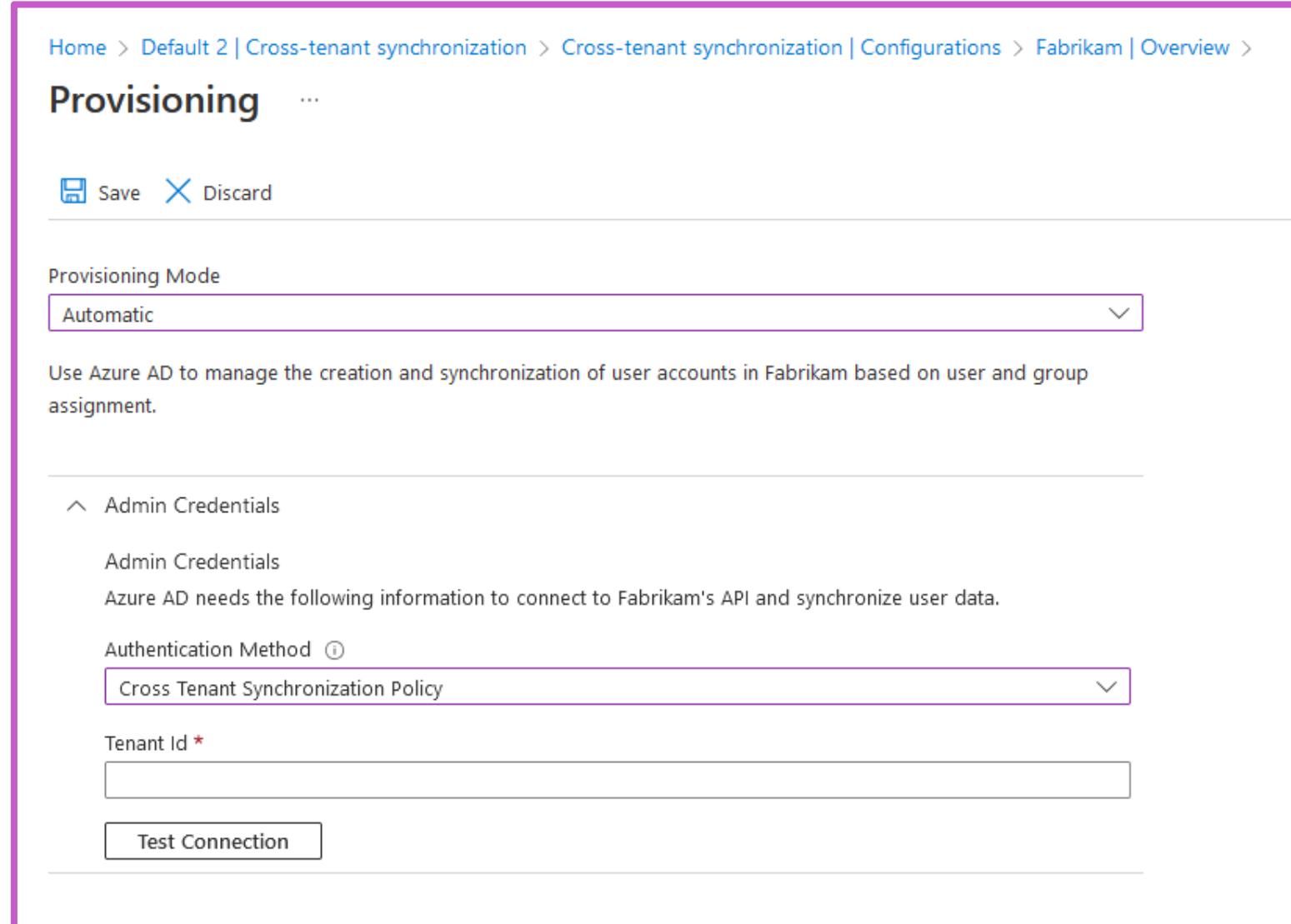
Admin Credentials  
Azure AD needs the following information to connect to Fabrikam's API and synchronize user data.

Authentication Method ⓘ

Cross Tenant Synchronization Policy

Tenant Id \*

Test Connection



# 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
- External users sign in using their own organizational account

# SAML/WS-Fed identity provider configuration

Home > Users > External Identities

## External Identities | All identity providers

Search

Built-in

Custom

Overview

Cross-tenant access settings

All identity providers

External collaboration settings

Diagnose and solve problems

Self-service sign up

Custom user attributes

All API connectors

Custom authentication extensions

User flows

Name	Status
Microsoft Entra ID	Configured
Email one-time passcode	Configured
Microsoft	Configured
Google	Configured
Facebook	Configure

### New SAML/WS-Fed IdP

You must configure the federating identity provider first. →

Display name \*

Identity provider protocol \*

Select protocol

Domain name of federating IdP \*

fabrikam.com

You can add more domains after configuring the SAML/WS-Fed IdP.[Learn more.](#)

Select a method for populating metadata \*

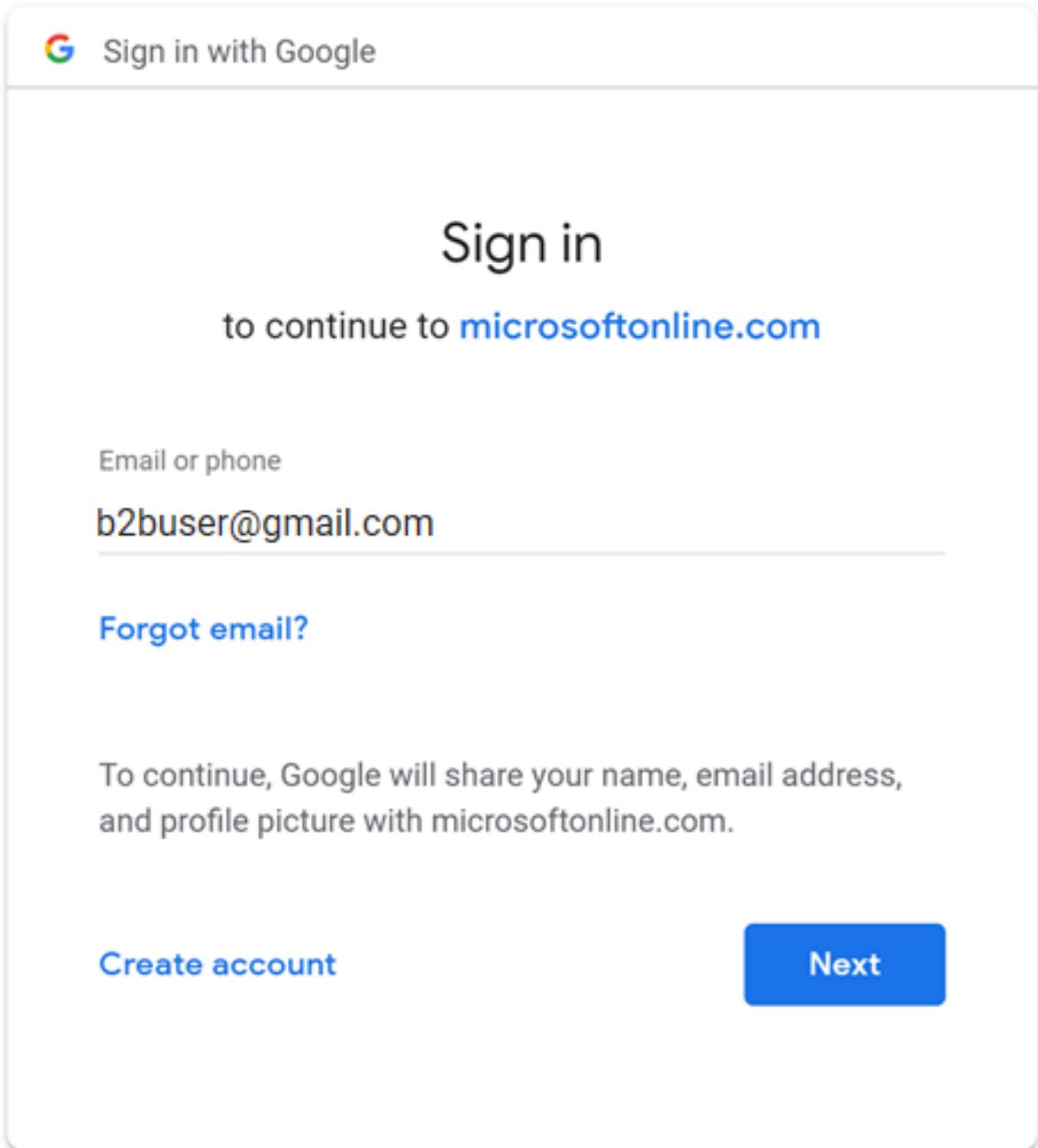
Select method

Save

Cancel

# Using Google as an identity provider

- External users who aren't signed in to Google will be prompted to do so
- External 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 Microsoft Entra ID 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 \*

# Verifiable credentials

# Implement Microsoft Entra Verified ID

## Requirements:

- Azure subscription
- Microsoft Entra ID Premium
- Azure Key Vault

The screenshot shows the Microsoft Entra admin center interface. On the left, a sidebar menu is visible with several sections: Multifactor authentication, Identity Governance, Dashboard, Entitlement management, Access reviews, Privileged Identity Management, Lifecycle workflows, Verified ID, Permissions Management, and Global Secure Access. The 'Verified ID' section is currently selected and expanded, showing three sub-options: Overview, Credentials, and Organization settings. The main content area is titled 'Overview' and features a heading 'Welcome to Entra Verified ID'. It explains that Verified ID enables fast remote onboarding, secure access, and easy account recovery. Below this, there are three numbered steps: 1. Configure organization settings (with a 'Configure' button), 2. Register decentralized ID (with a 'Register' button), and 3. Verify domain ownership (with a 'Verify' button). A search bar at the top right says 'Search resources, services, and docs (G+)'. The overall theme is light blue and white.

# Microsoft Entra Verified ID usage and value

## Value

- **Trust without over sharing**

- Share only the information needed for verification

- **Decentralized / tamper resistant**

- Cryptographically signed and held by the users (not company)

- **Portable Trust**

- Usable across systems and platforms

- **Extends authentication and Authorization**

- Compliments Entra ID existing verifications

## Usage Scenarios

- **Employee verification**

- Temp staff, contractors, shared desks
- Blocks badge cloning / theft

- **B2B Guest support**

- No longer need long lived guest accounts

- **On boarding**

- New hires
- Allow new hires to start with biometrics enabled

- **Secure API and AI access**

- Require biometrics for additional access

# Implement and manage hybrid identity

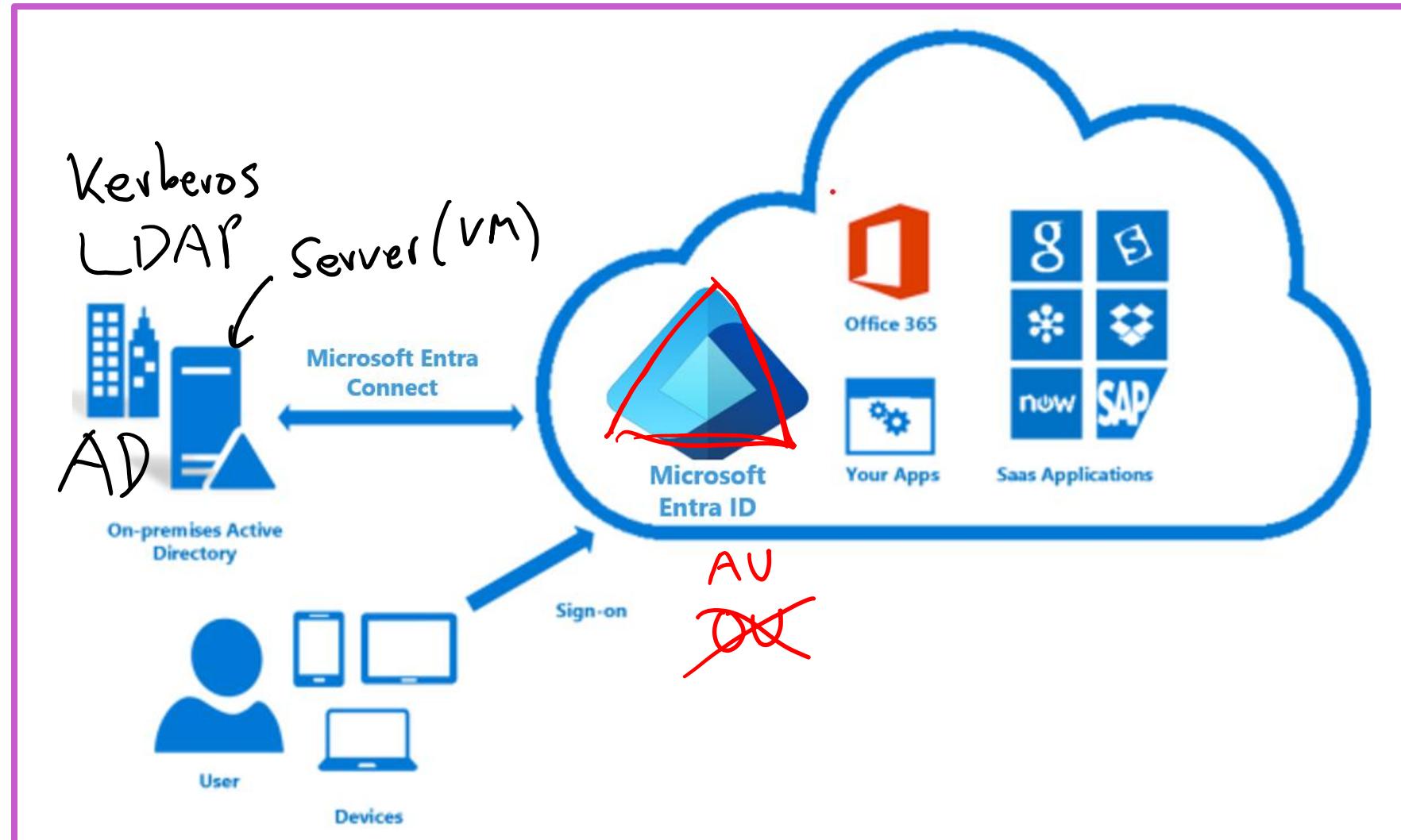
# Objectives

- 1** Plan, design, and implement Microsoft Entra Connect Sync
- 2** Implement and manage password hash synchronization (PHS)
- 3** Implement and manage pass-through authentication (PTA)
- 4** Implement and manage federation
- 5** Troubleshoot synchronization errors
- 6** Implement Microsoft Entra Connect Health
- 7** Manage Microsoft Entra Connect Health

# Plan, design, and implement Microsoft Entra Connect

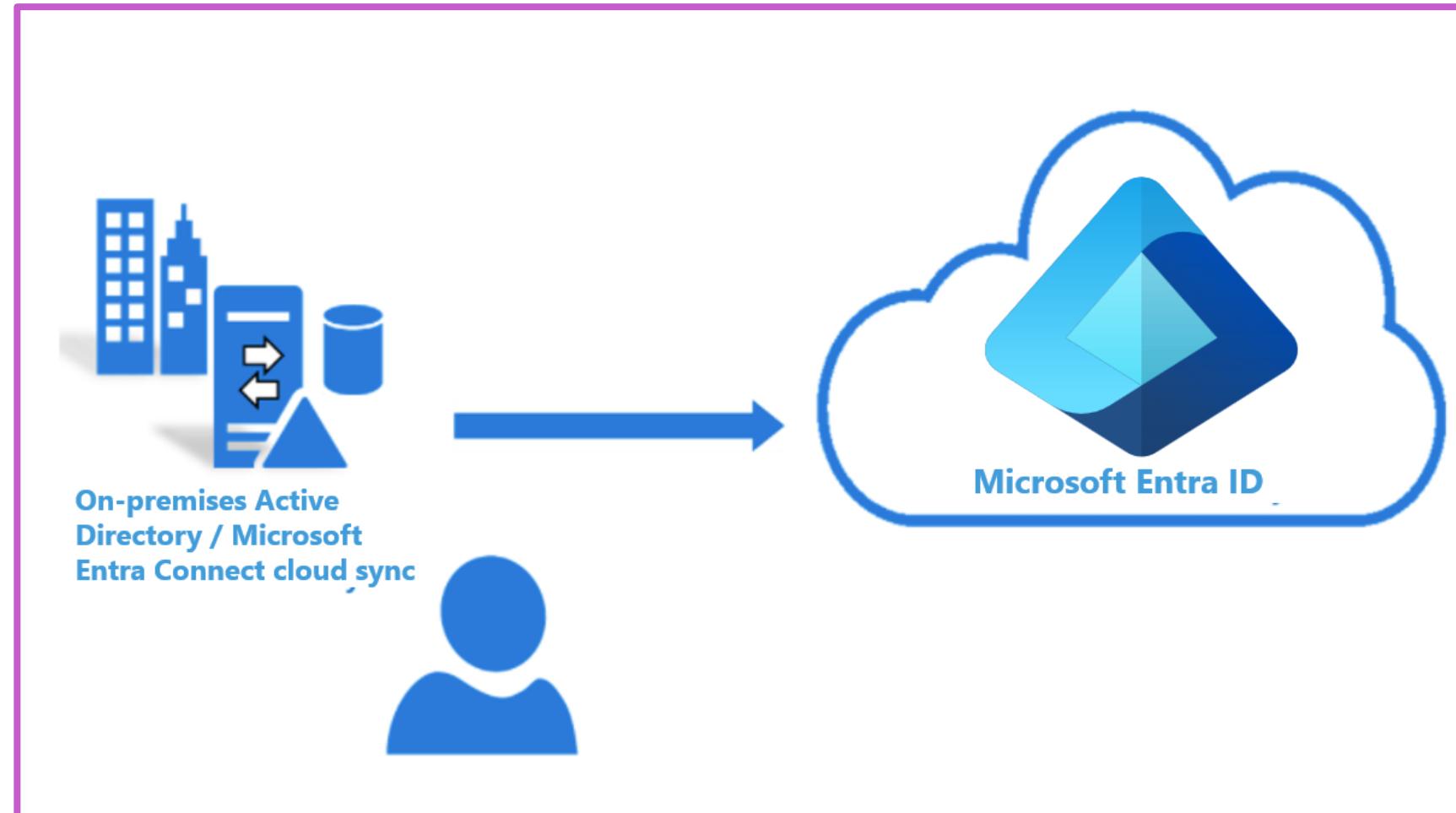
# What is Microsoft Entra Connect?

- Microsoft Entra Connect is a solution that bridges an organization's on-premises Active Directory with your cloud-based Microsoft Entra ID
- Microsoft Entra Connect provides:
  - Synchronization
  - Password hash synchronization
  - Pass-through authentication
  - Federation integration
  - Health monitoring



# Microsoft Entra cloud sync

- Microsoft Entra cloud sync is a solution that syncs your on-premises AD with Microsoft Entra ID
- Lightweight provisioning agent required on the on-premises AD
- All sync configuration is managed in the cloud
- Can be used in conjunction with Microsoft Entra Connect
- **No Device Sync.**



# Authentication methods

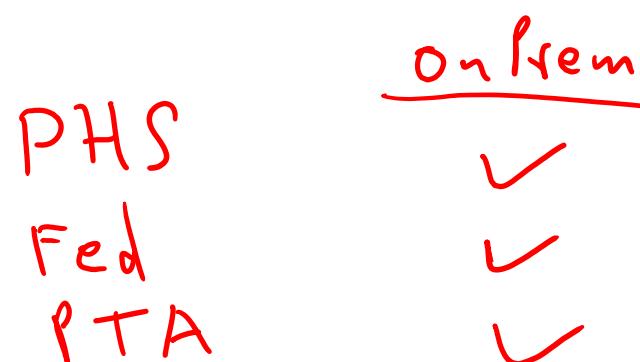
## Cloud authentication

### Microsoft Entra password hash synchronization (PHS)

- Users can use the same username and password that they use on-premises

### Microsoft Entra pass-through authentication (PTA)

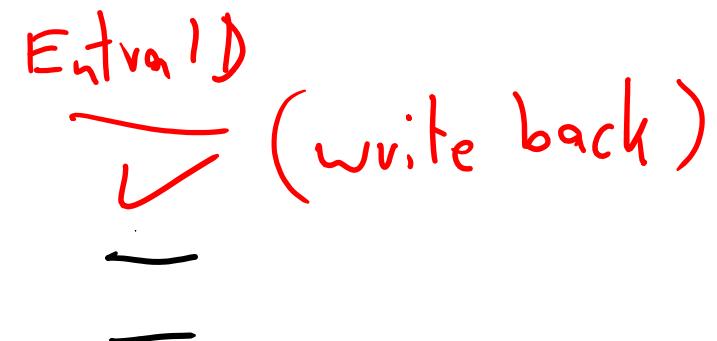
- Simple password validation for Microsoft Entra ID authentication services using a software agent that runs on one or more on-premises servers



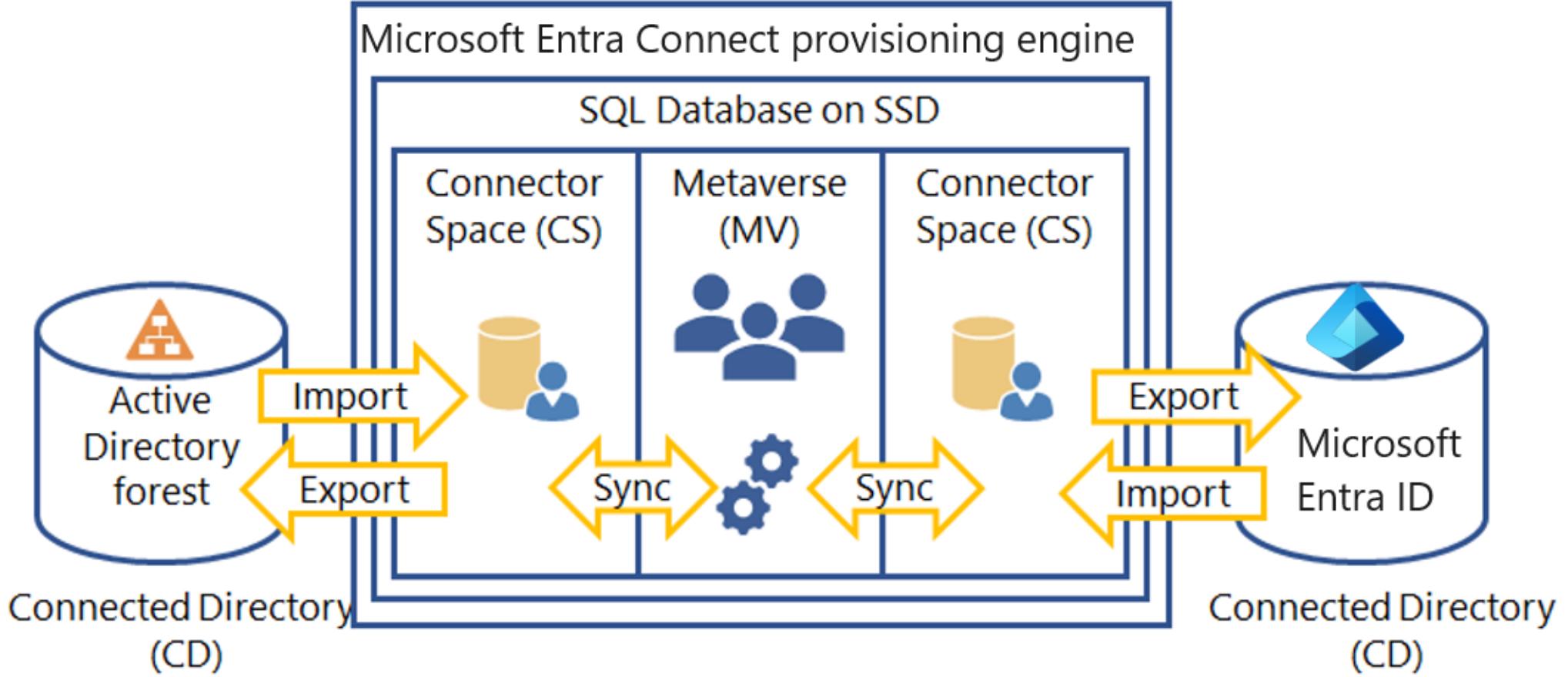
## Federated authentication

### Handoff to trusted authentication system

- Microsoft Entra ID 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

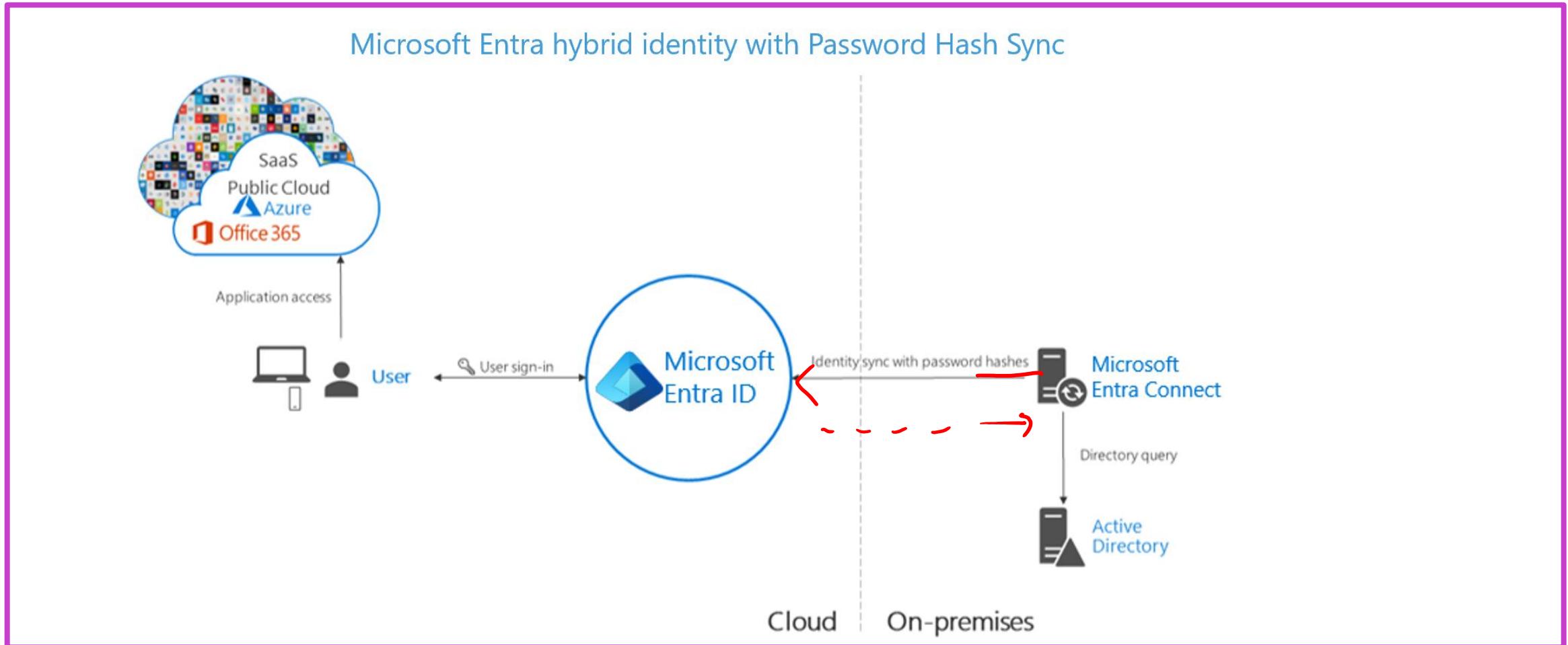


# Microsoft Entra Connect component factors



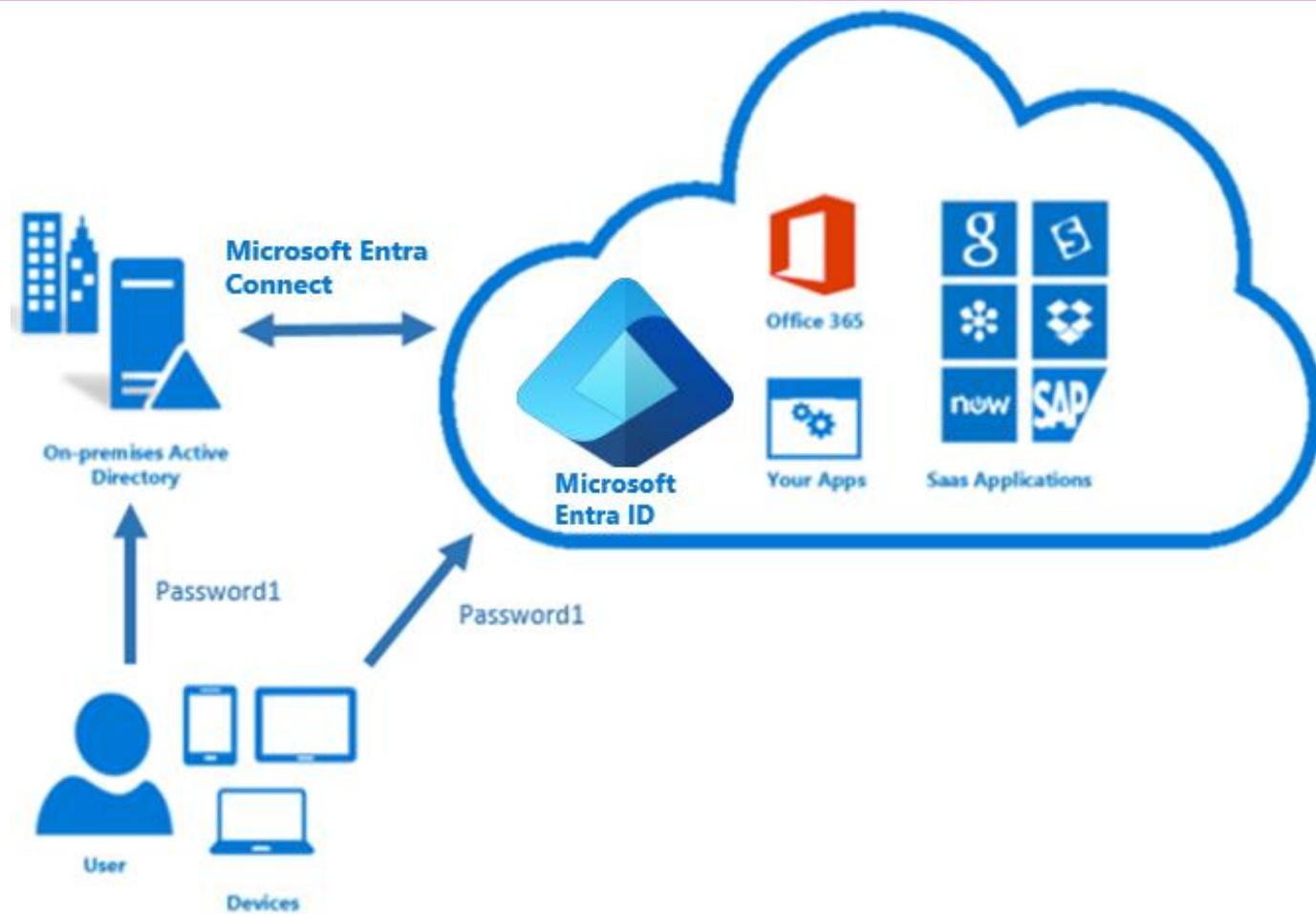
# Implement and manage password hash synchronization (PHS)

# Password hash sync

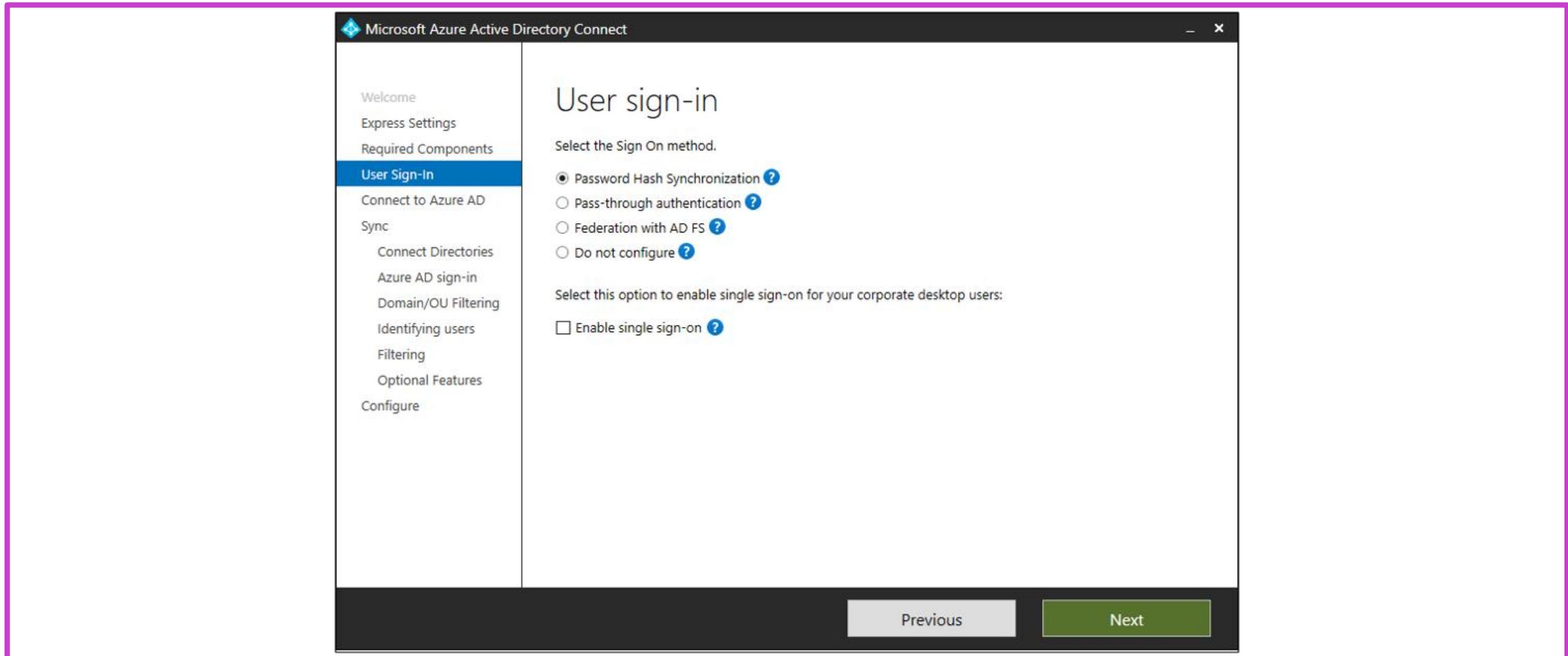


Simplicity of a password hash synchronization solution

# How password hash synchronization works

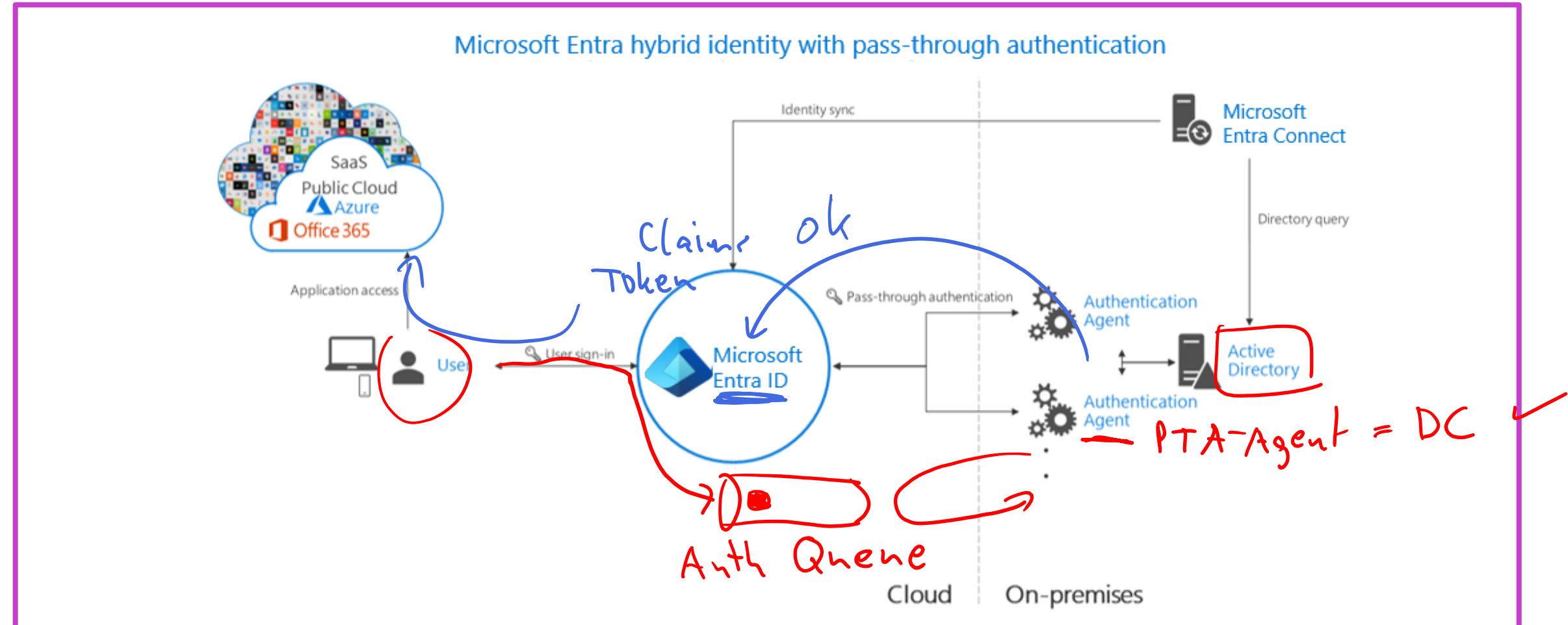


# Enable password hash synchronization



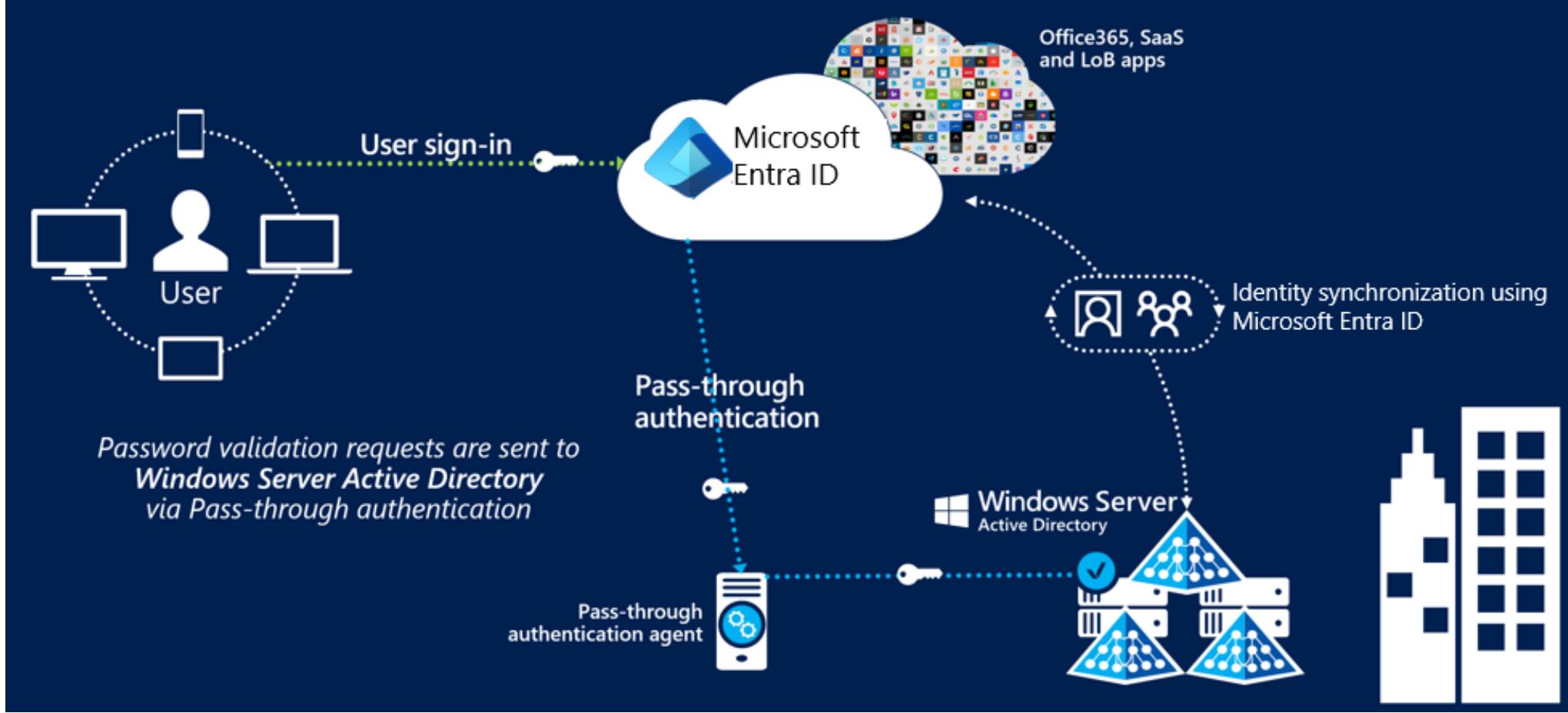
# Implement and manage pass-through authentication (PTA)

# Pass-through authentication PTA



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

# How Microsoft Entra pass-through authentication works



# Enable pass-through authentication

The image displays two side-by-side screenshots of the Microsoft Azure Active Directory Connect wizard, both enclosed in a thick pink border.

**User sign-in Step:**

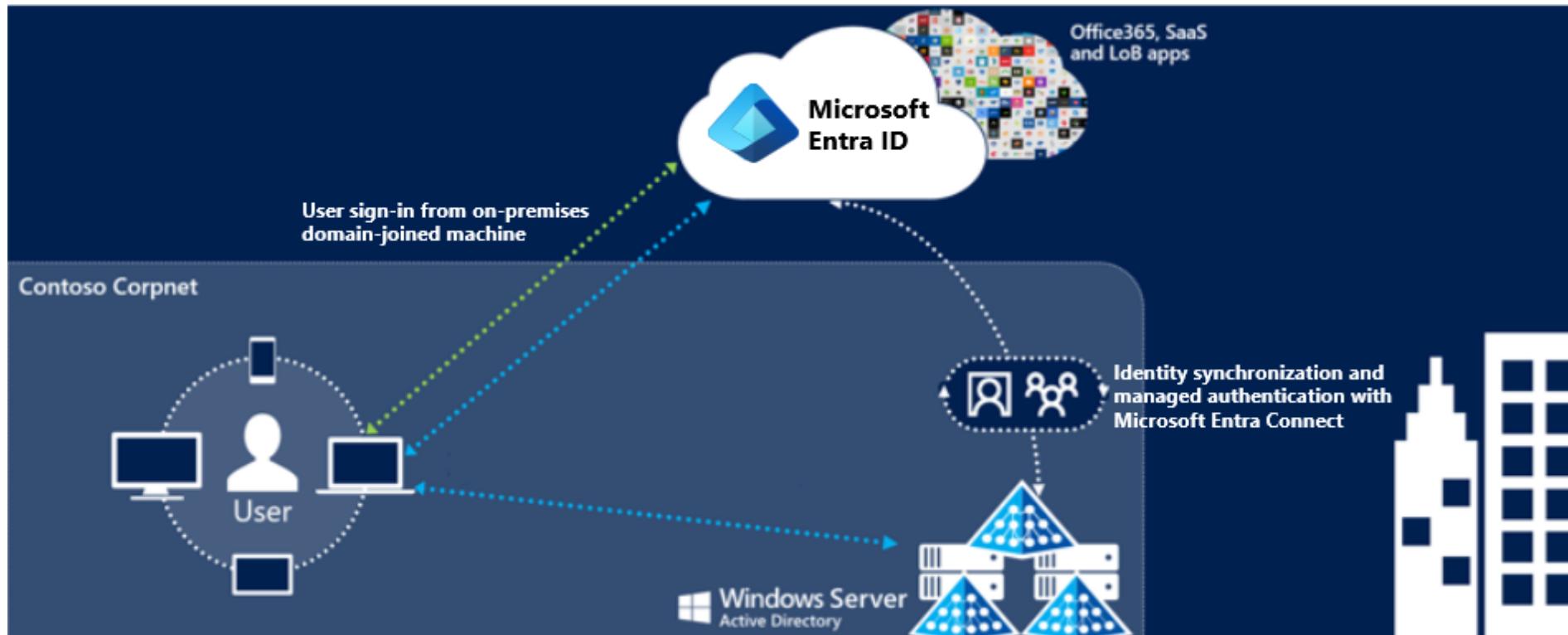
- Left Panel (Navigation):** Shows a sidebar with options: Welcome, Express Settings, Required Components, **User Sign-In** (selected), Connect to Azure AD, Sync, Connect Directories, Azure AD sign-in, Domain/OU Filtering, Identifying users, Filtering, Optional Features, and Configure.
- Right Panel (Content):** Title: User sign-in. Subtitle: Select the Sign On method. Options: Password Hash Synchronization, Pass-through authentication (selected), Federation with AD FS, Federation with PingFederate, and Do not configure. A checkbox for Enable single sign-on is present. A note at the bottom states: "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](#)".

**Additional tasks Step:**

- Left Panel (Navigation):** Shows a sidebar with options: Welcome, **Tasks** (selected).
- Right Panel (Content):** Title: Additional tasks. Subtitle: The required tasks for the scenario have been completed. Choose from the list below to perform additional tasks. A list of tasks includes: Privacy settings, View current configuration, Customize synchronization options, Configure device options, Refresh directory schema, Configure staging mode, **Change user sign-in** (selected), Configure Source Anchor, Manage federation, and Troubleshoot.

# Seamless single sign-on (SSO)

# Single sign-on



User sign-in via on-premises or via Microsoft Entra Connect alternate ID.

If single sign-in fails, the user is prompted to log in.

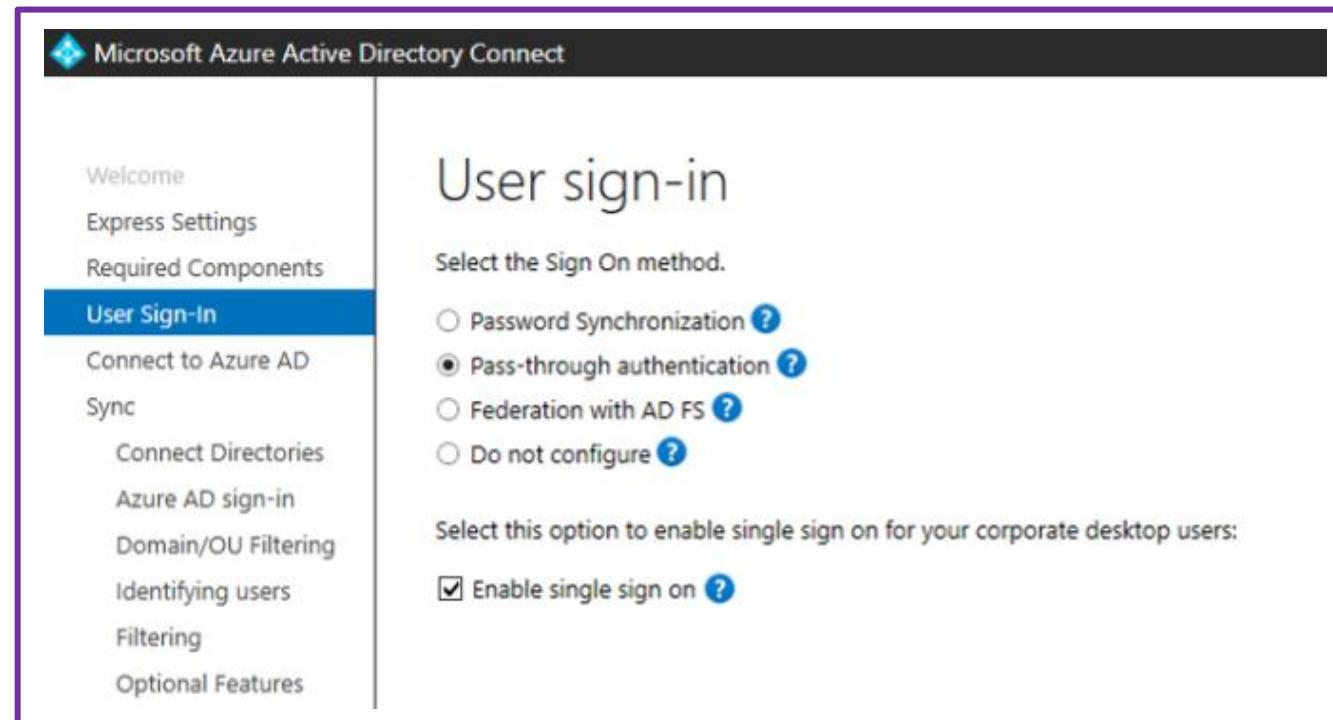
Sign out works, but releases the sign-in so all further access is blocked until sign-in is completed again.

Supported in browser-based and Office-based clients.

# How seamless SSO is set up

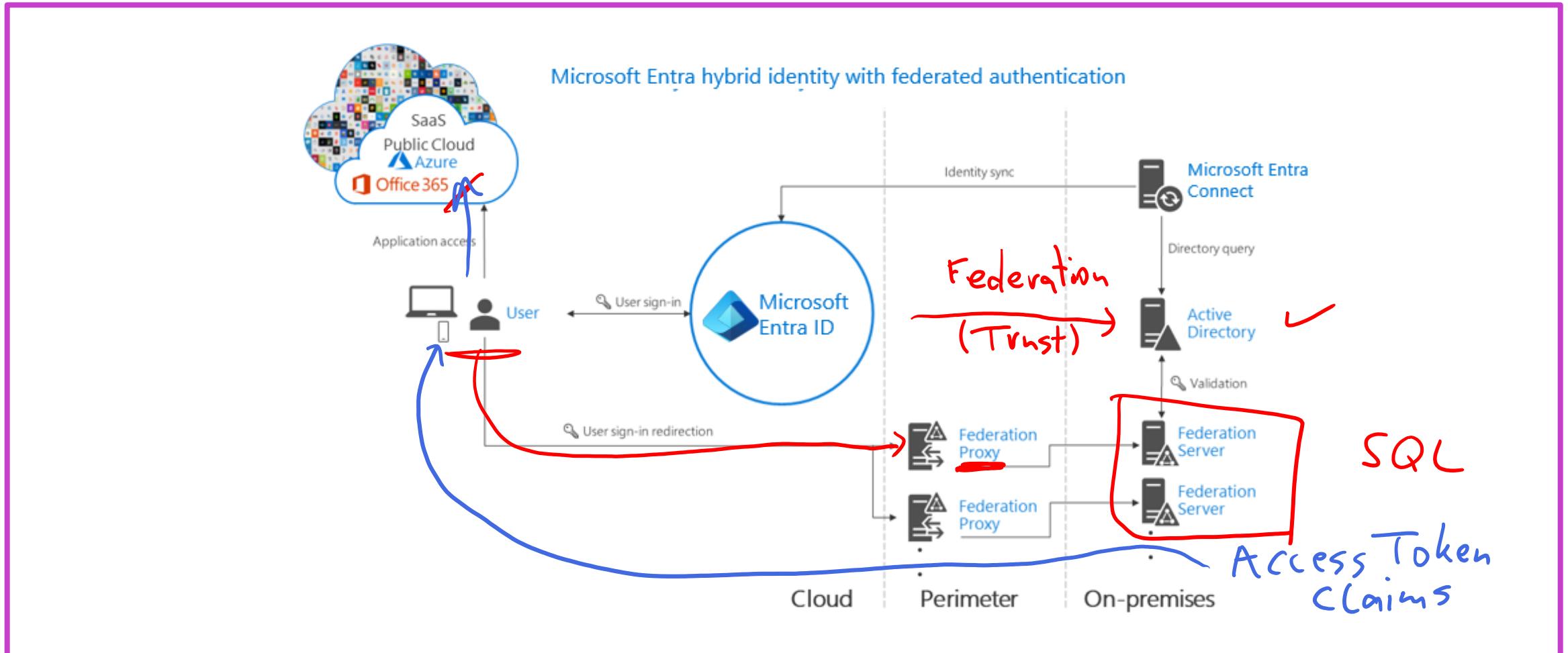
Seamless SSO is enabled using Microsoft Entra Connect. While enabling the SSO, the following steps occur:

1. A computer account (AZUREADSSOACC) is created in your on-premises Active Directory (AD).
2. A set of Kerberos service principal names (SPNs) are created to be used during the Microsoft Entra ID sign-in process.
3. Kerberos decryption key is shared securely with Microsoft Entra ID.



# Implement and manage federation

# Federated authentication

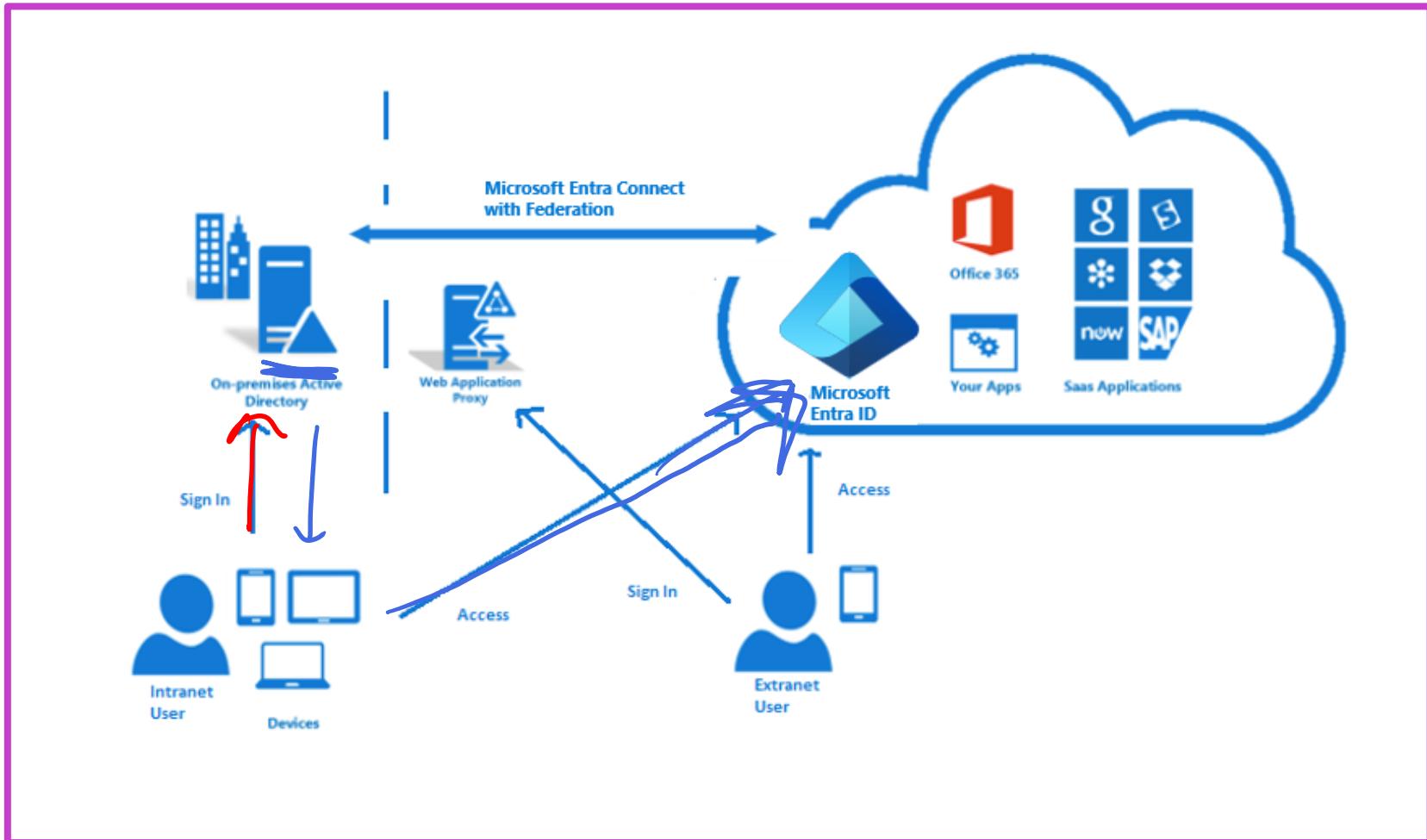


Components required for federation in the perimeter and internal network of your organization

# What is federation?

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

- Users sign in to Microsoft Entra ID services using their on-premises passwords
- Microsoft Entra Connect configures the trust between Microsoft Entra ID and the on-premises farm



# Deploying a federation with AD FS and Microsoft Entra Connect

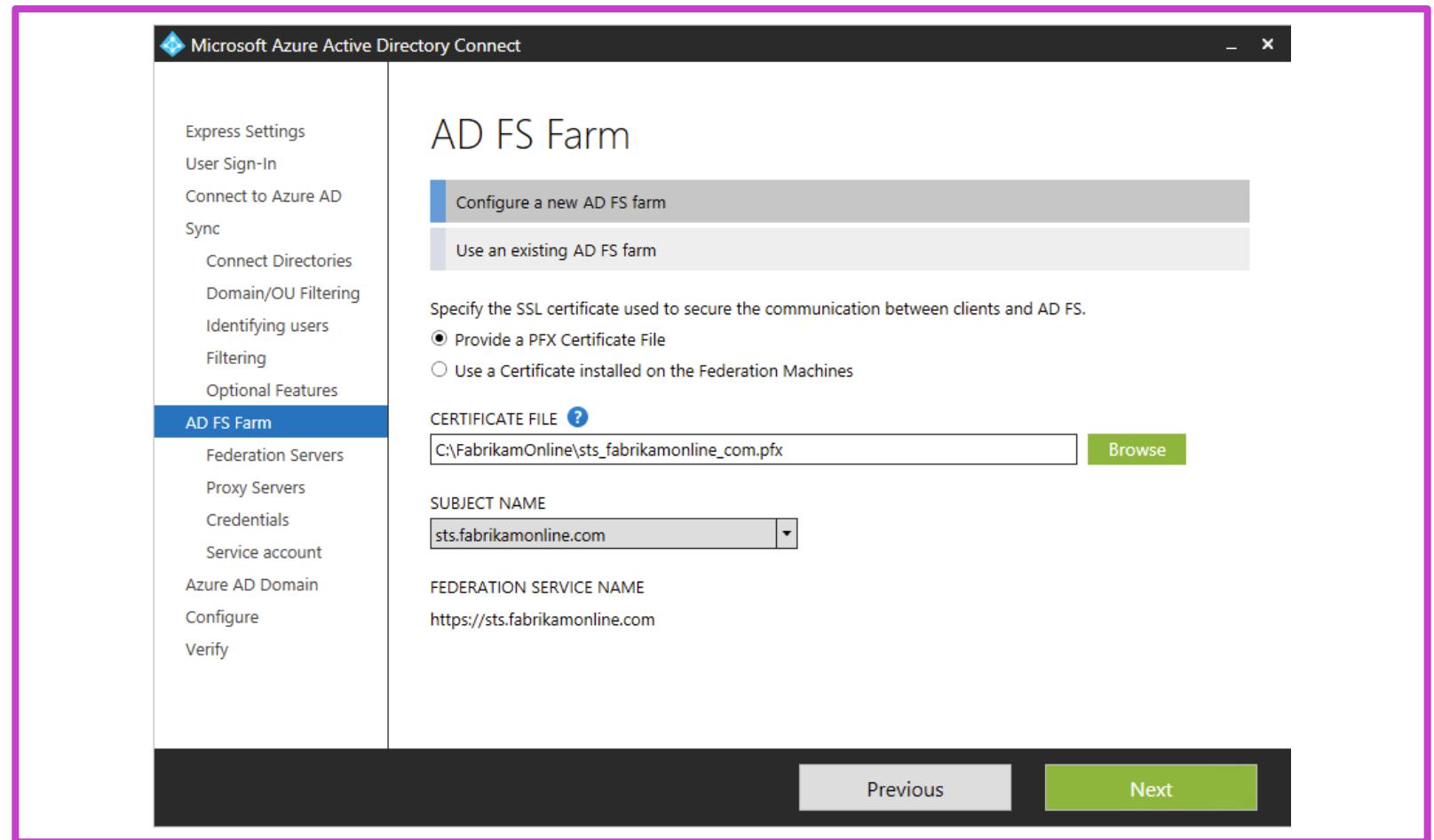
**To deploy an AD FS farm, you need:**

- 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 Microsoft Entra 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 Microsoft Entra domain to federate



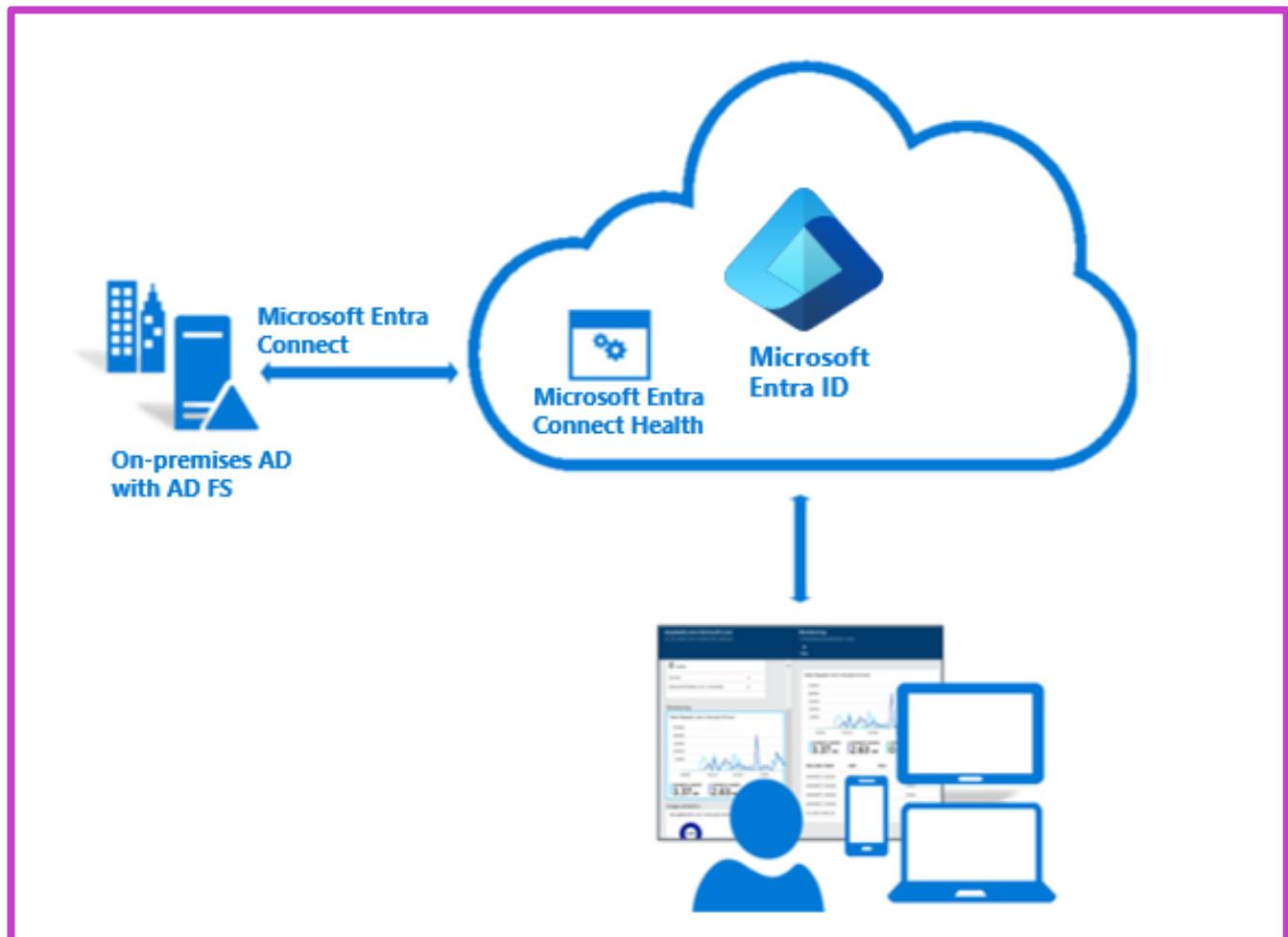
# Managing federation with Microsoft Entra Connect

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

# Implement Microsoft Entra Connect Health

# What is Microsoft Entra 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
- Microsoft Entra Health Connect portal (aka.ms/aadconnecthealth)

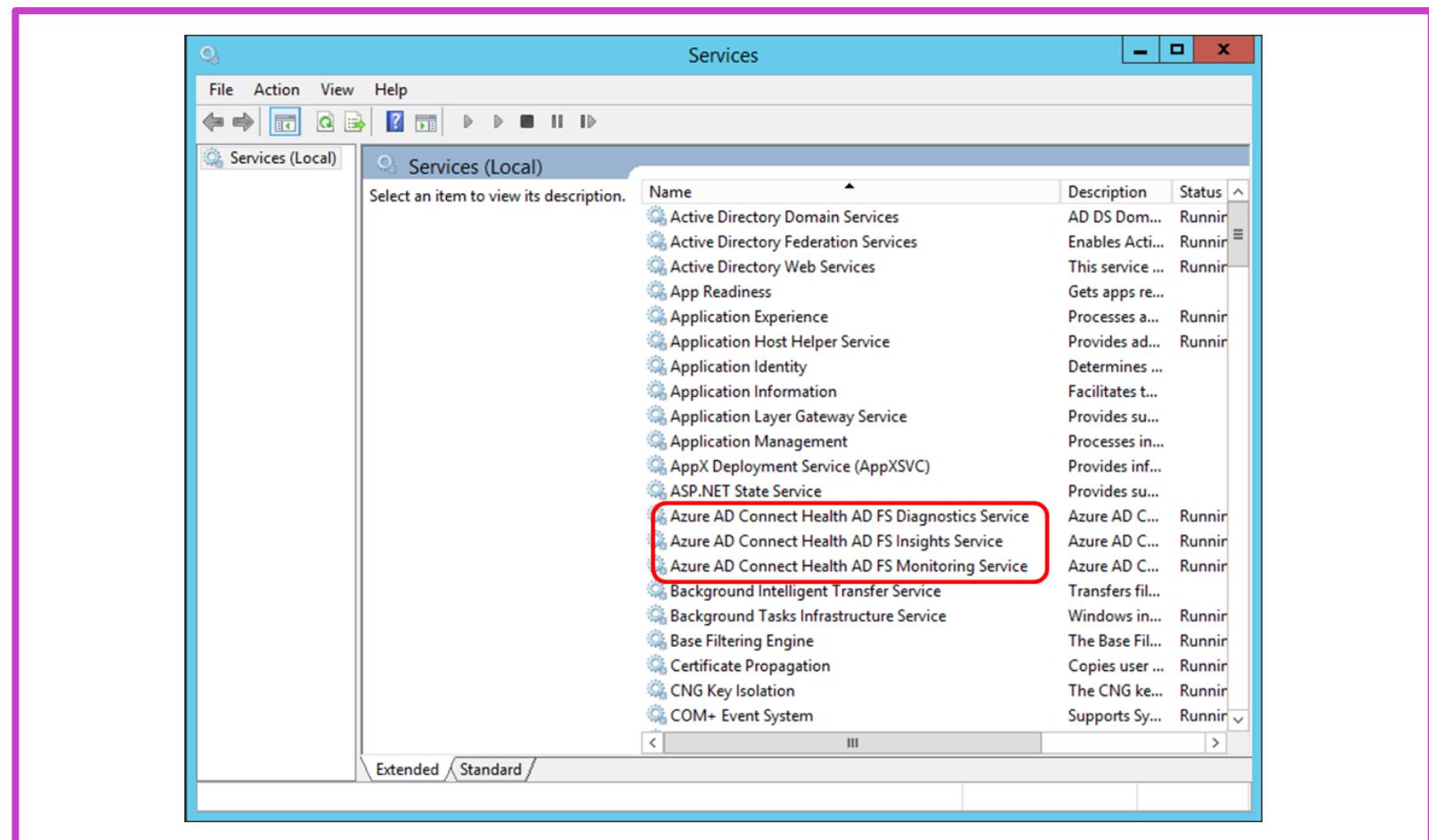


# Considerations for installing Microsoft Entra Connect Health

- Microsoft Entra ID premium license required (P1 or P2)
- Only a global administrator can deploy and configure
- Microsoft Entra Connect Health Agent—install on each server to collect health data from
  - AD FS server or your Active Directory Domain Services machine
- 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—Microsoft Entra Connect Help for AD FS installation steps

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



# Manage Microsoft Entra 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 of Azure Active Directory Connect Servers: FABVM03 is Unhealthy and FABVM02 is Healthy. Below that, the Azure Active Directory Connect (Sync) Alerts section shows 1 active alert, all of which are Active. A red box highlights the 'Azure Active Directory Connect (Sync) Alerts' tile.

**Azure Active Directory Connect (Sync) Alerts**

fabtoso.onmicrosoft.com

Time Range Notificati... Settings

**NAME** **TYPE** **SCOPE**

**ACTIVE ALERTS**

Azure AD Connect Sync Service is not r...	! Error	FABVM03
---	---------	---------

**RESOLVED ALERTS**

No items for this.

**Notification**  
fabtoso.onmicrosoft.com

Save Discard

You can provide feedback by doing a right click on any alert.

Find ...

OFF ON

Notify All Global Administrators

ADDITIONAL EMAIL RECIPIENTS

varun@fabtoso.com  
idadmins@fabtoso.com

# Additional tasks

## Delete a server or service instance

- Delete a server from the Microsoft Entra Connect Health service
- Delete a service instance from Microsoft Entra Connect Health service

## Manage access with Azure role based access control

- Allow users or groups access to Microsoft Entra Connect Health
- Remove users or groups

# Troubleshoot synchronization errors

# Troubleshooting

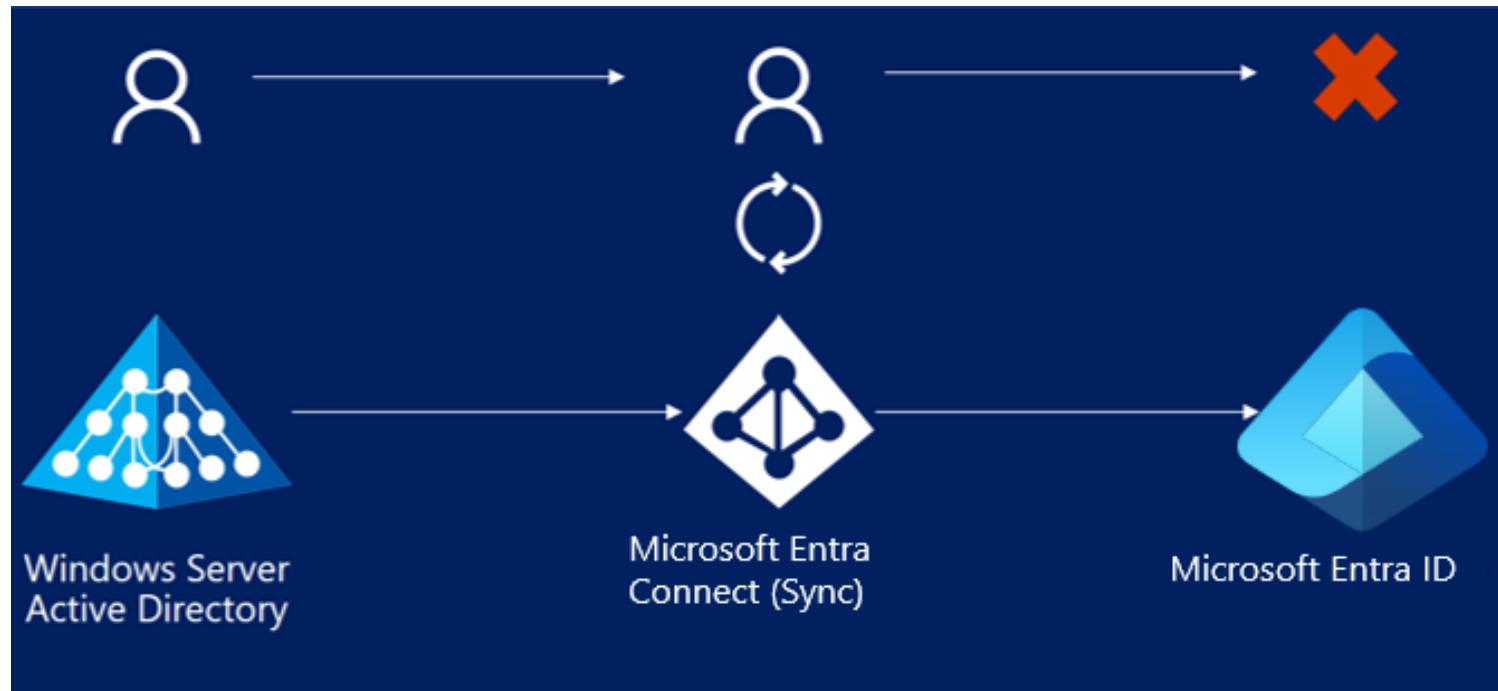
## Diagnose and remediate duplicated attribute sync errors

- 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 Microsoft Entra ID configuration

- Microsoft Entra roles, custom roles
- Custom domain
- Administrative units
- Tenant-wide settings

## Configure and manage identities

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

## External Identities

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

## Hybrid Identity

- Connect to your on-premises AD
- Microsoft Entra Connect
- Implement PHS, PTA, and SSO
- Microsoft Entra 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 Microsoft Entra ID, 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 Microsoft Entra ID**

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

**Create, configure, and manage identities**

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

**Implement and manage external identities**

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

**Implement and manage hybrid identity**

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



# Learning path recap

## In this learning path, we:

Explained and configured identities for use in your cloud solutions.

Deployed and managed a Microsoft Entra ID infrastructure.

Configured and maintained external and hybrid identities.

