Microsoft

SC-300

Microsoft Identity and Access Administrator

Microsoft

LP 1

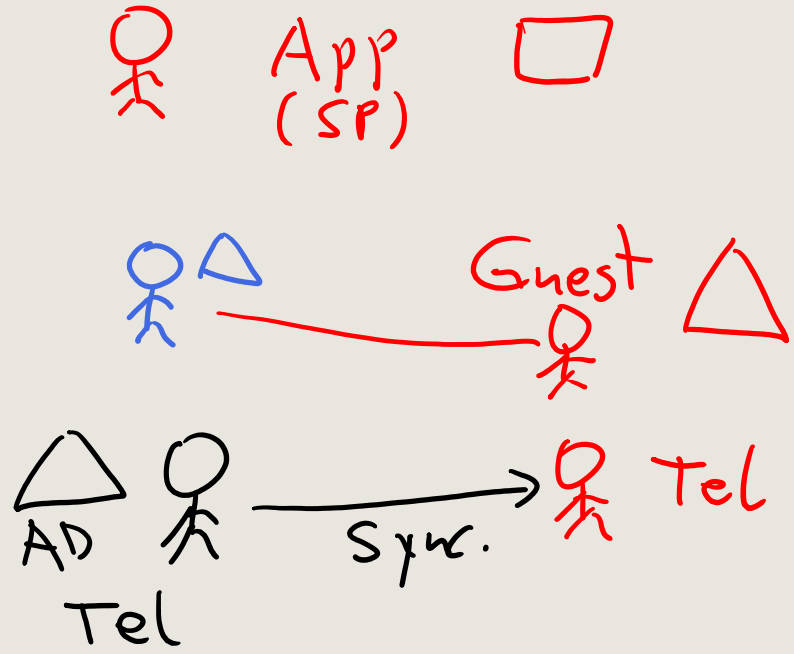
Implement an identity management solution

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

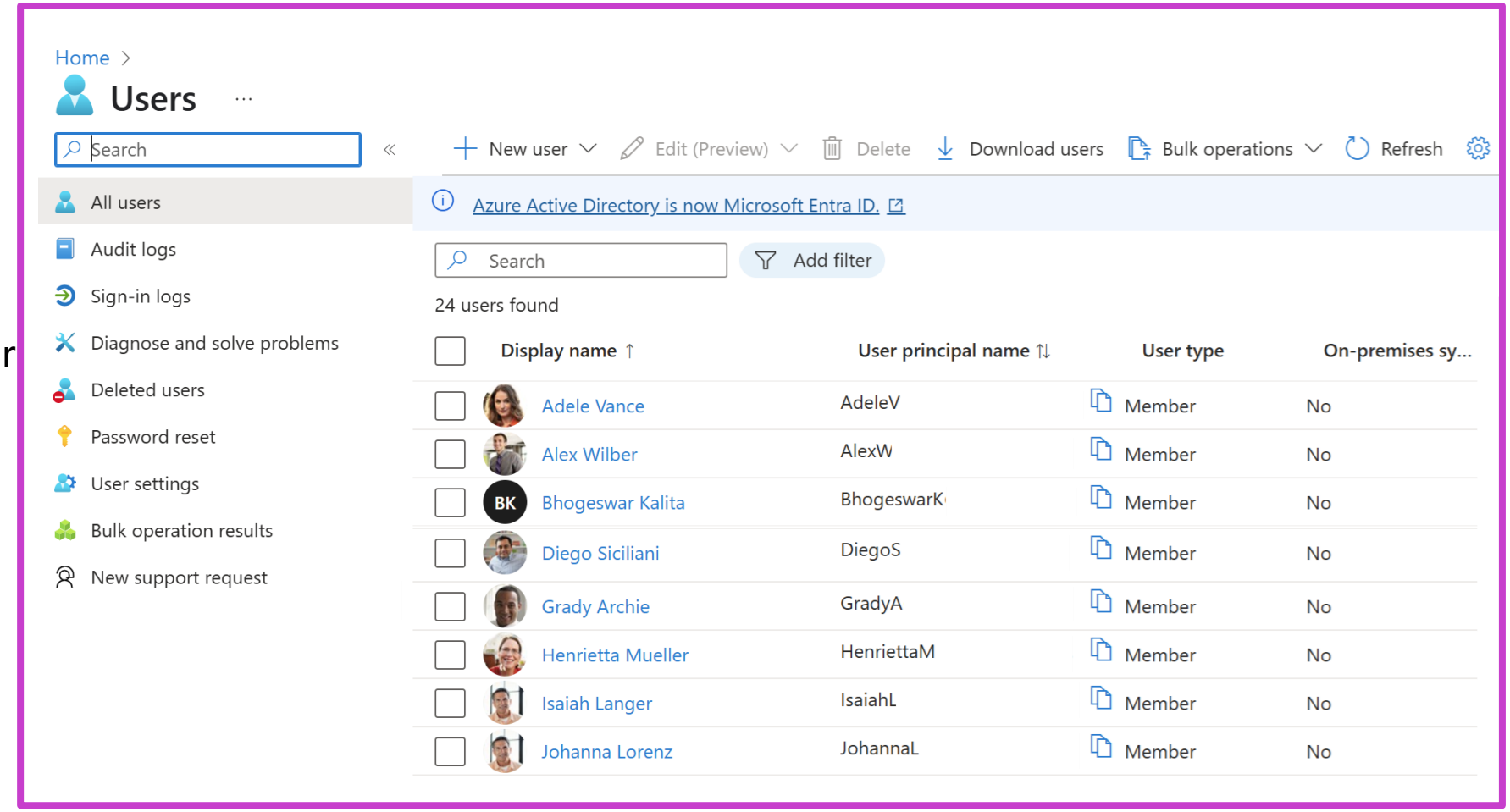
Objectives

1. Create, configure, and manage users
2. Create, configure, and manage groups
3. Configure and mange device identities
4. Manage licenses
5. Custom security attributes
6. Provisioning using SCIM

Create, configure, and manage users

Create, configure, and manage users

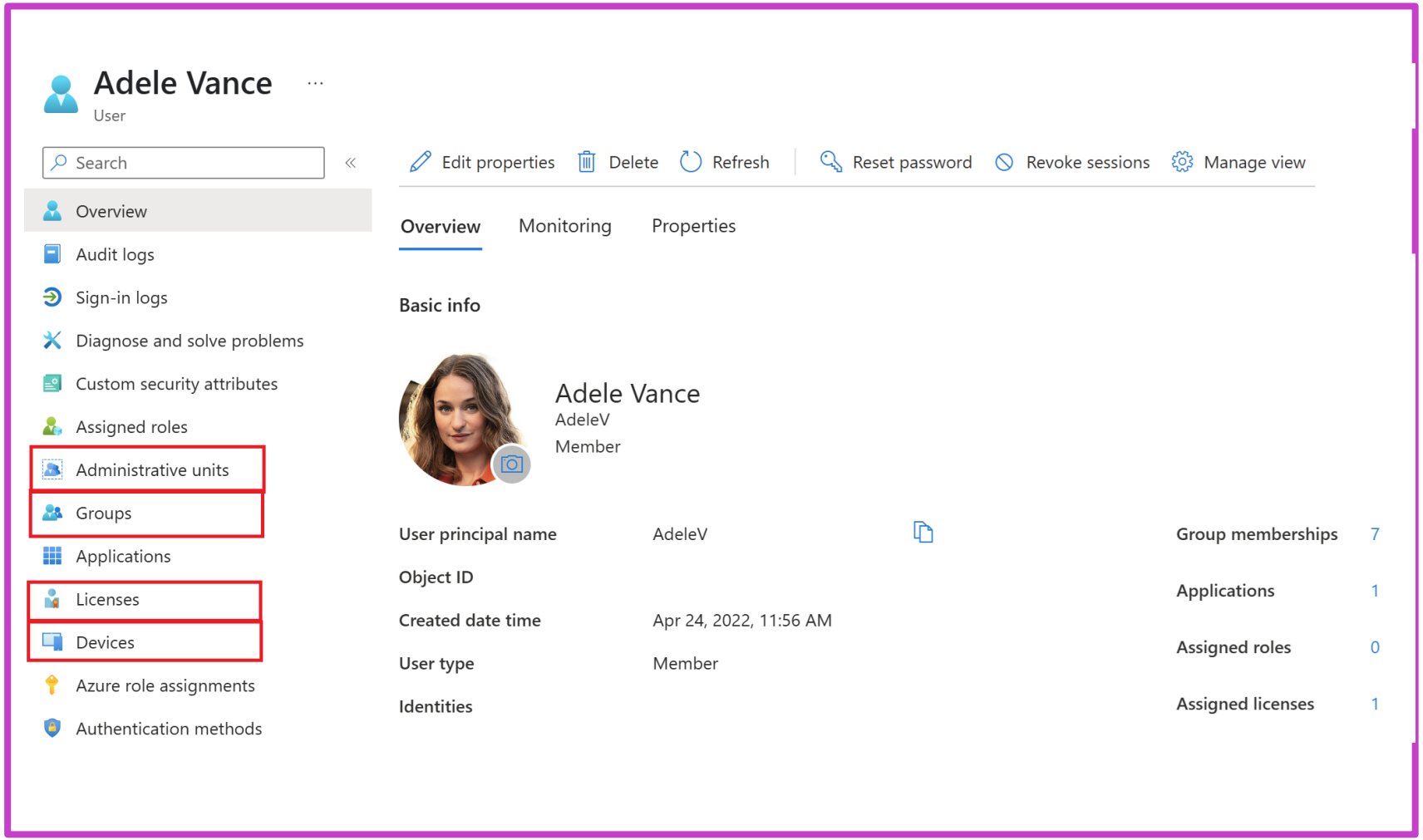
- A user account contains all the information needed to authenticate the user during the sign-on process
- You use the **Identity – All users** dashboard in the Microsoft Entra admin center to work with user objects
- Three kinds of users:
  - Cloud identities
  - Directory-synchronized identities
  - External users



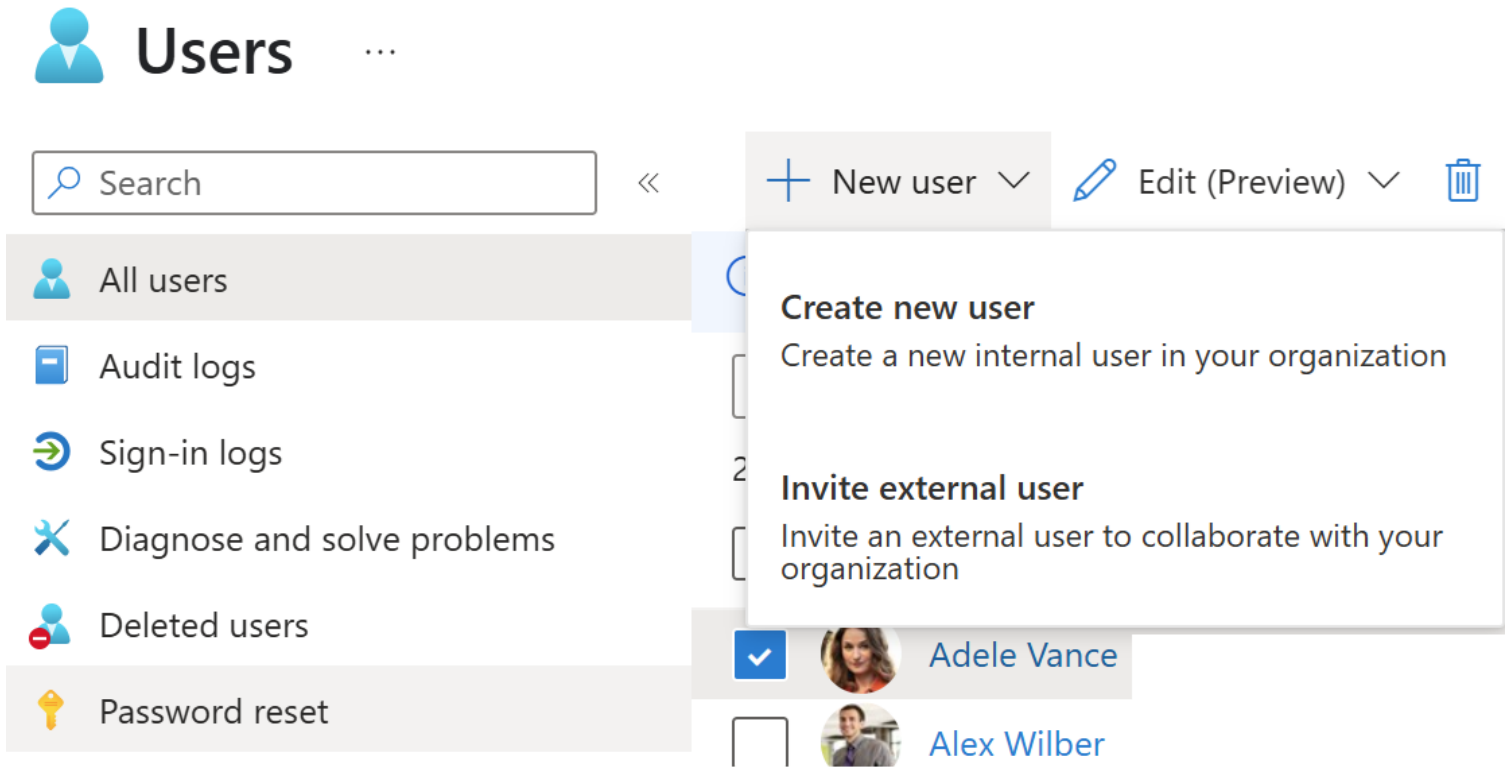
User settings

Some configurable user settings:

- Groups
- Licenses
- Devices
- Location



Demo—users



Create, configure, and manage groups

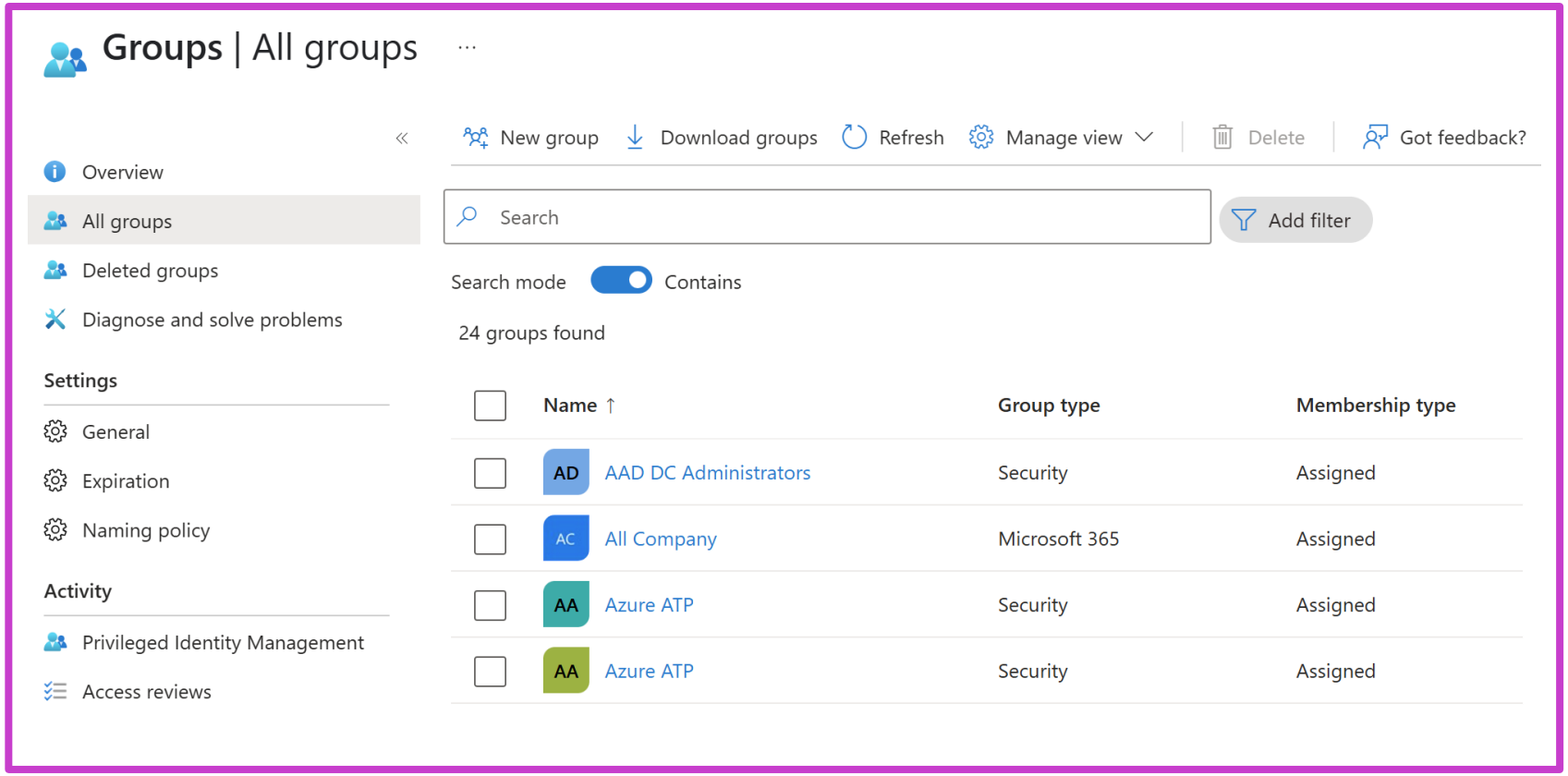
Create, configure, and manage groups

Security groups:

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

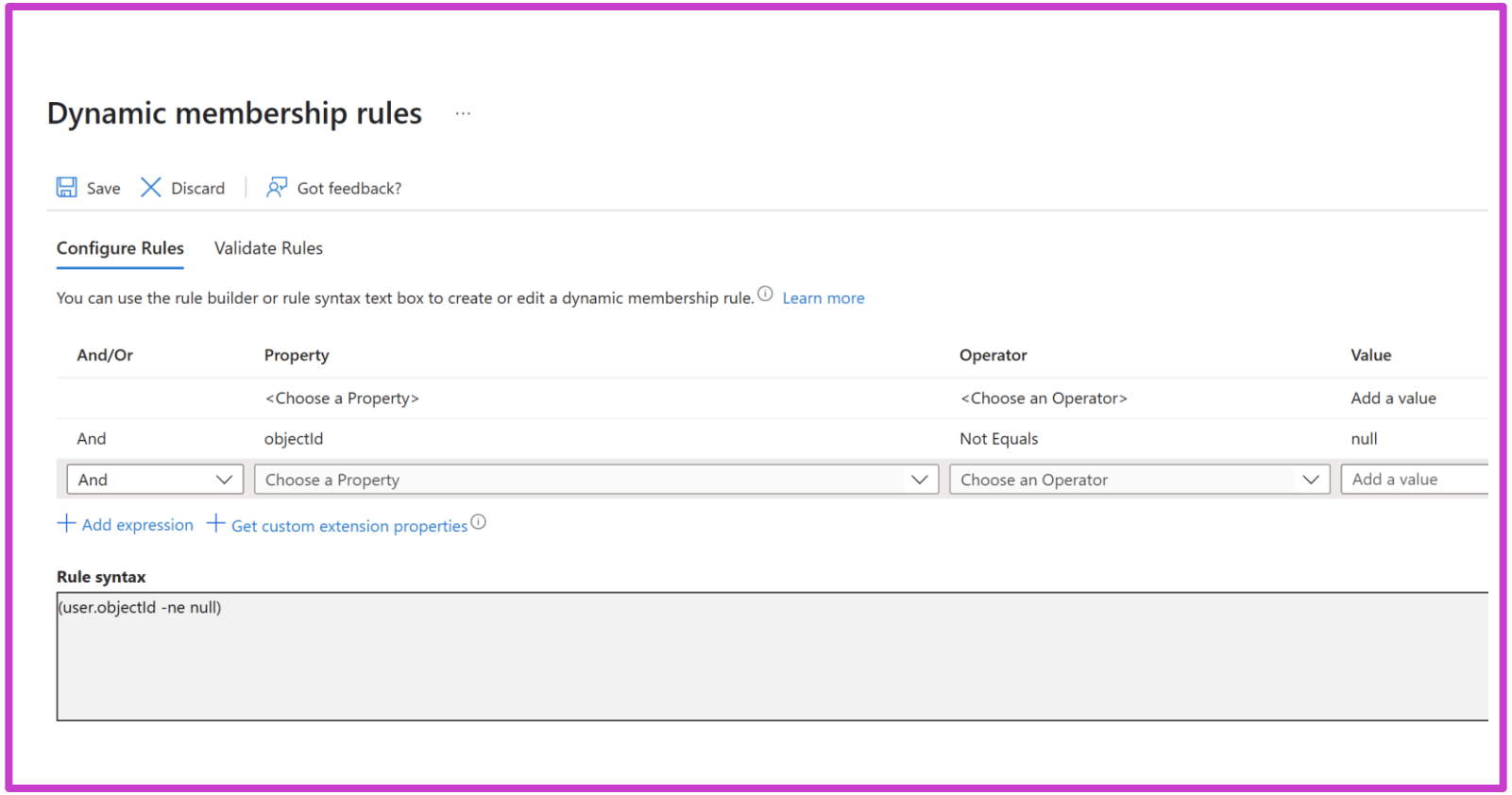
Microsoft 365 groups:

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



Dynamic groups

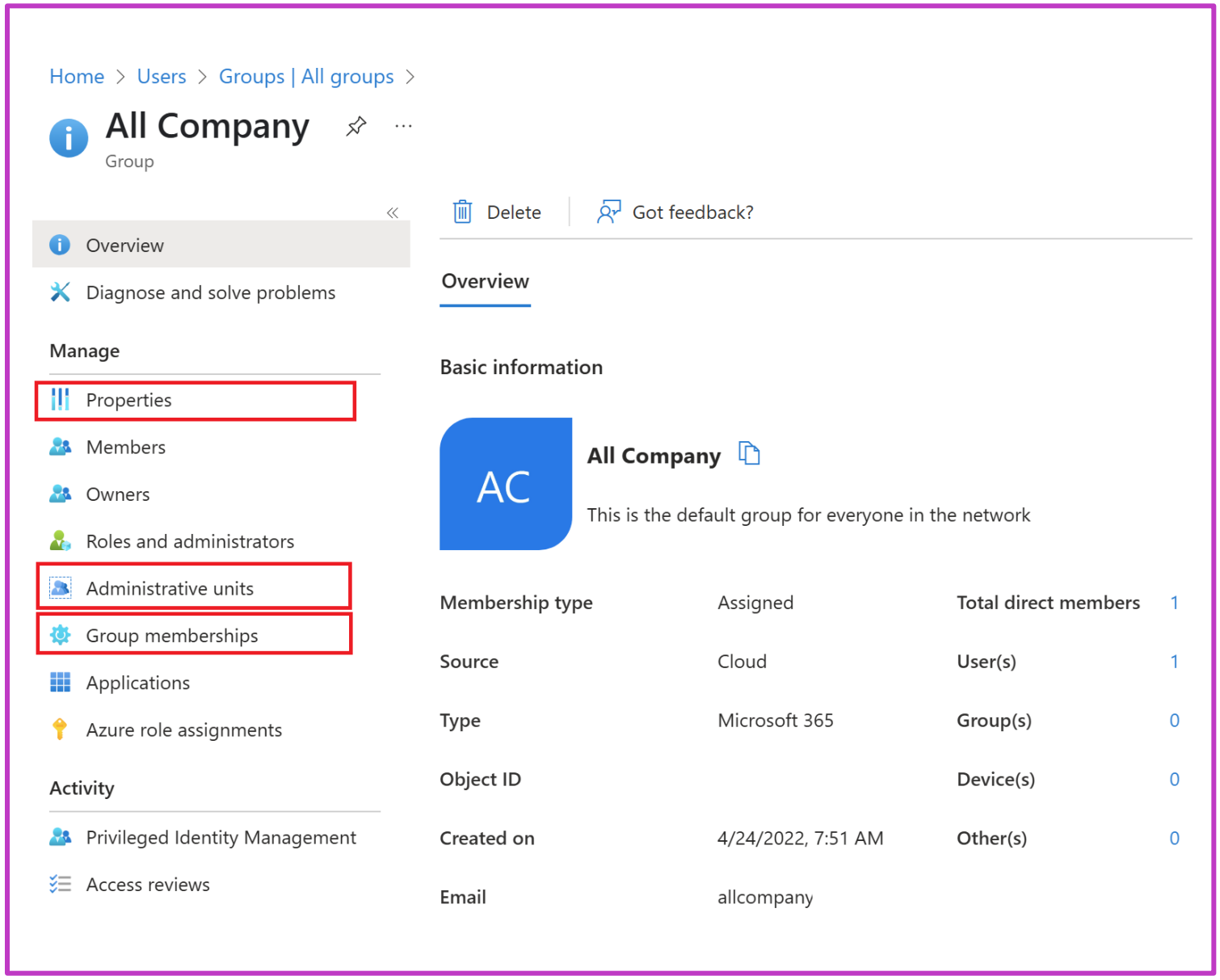
- Special type of security group
- Membership dynamically generated via membership rule
  - Property -- example = department, region, and other items



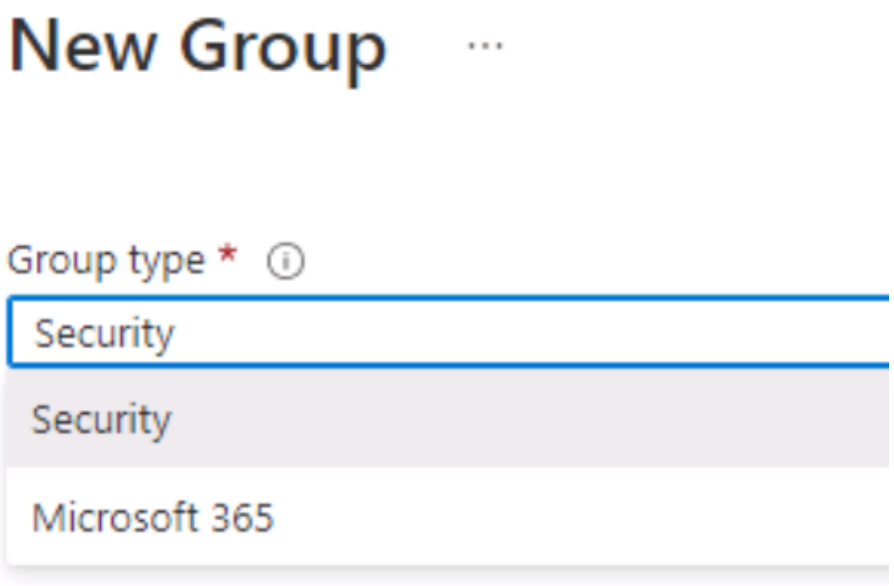
Group configuration options

Some configurable group settings:

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



Demo—groups

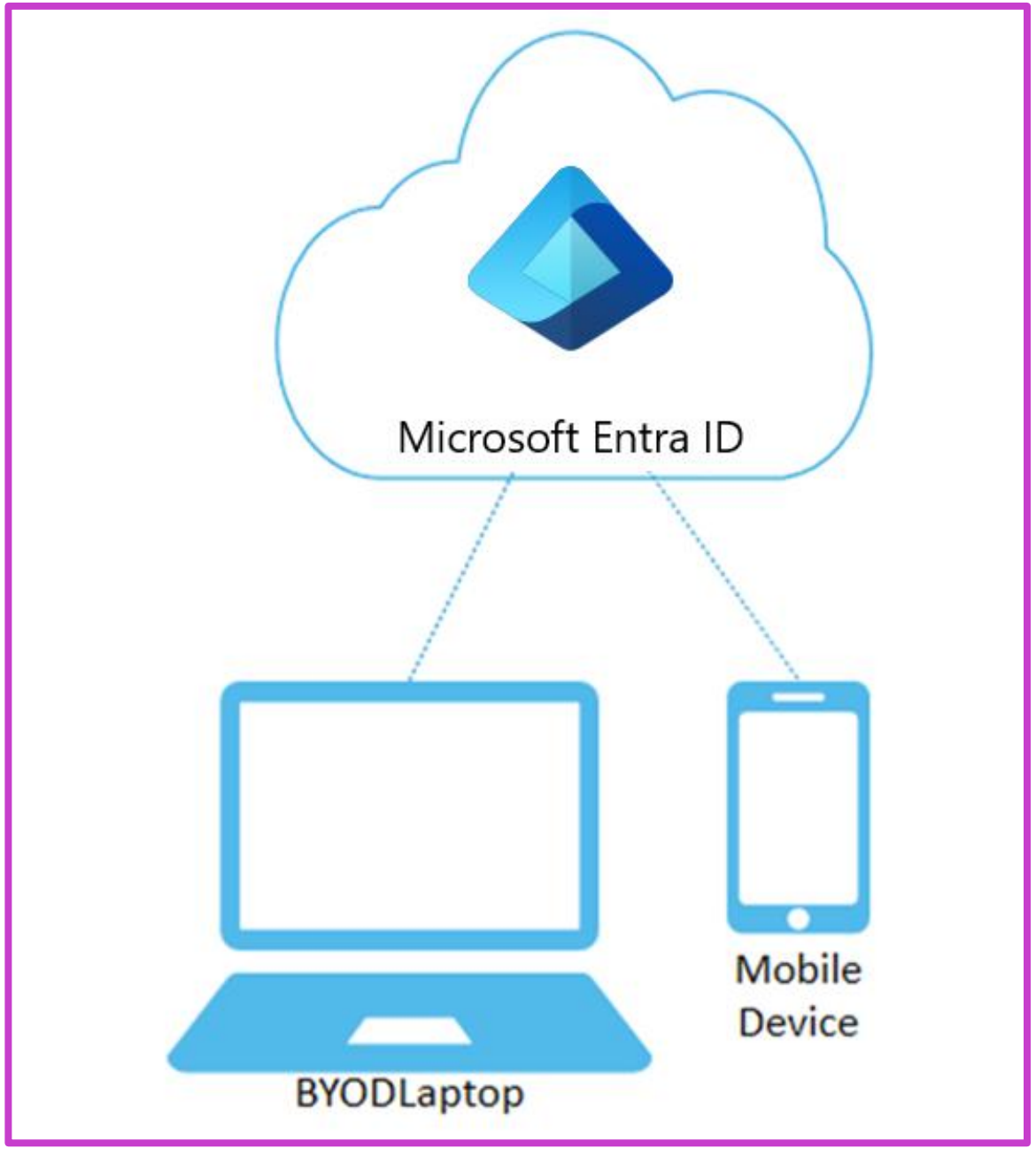


Configure and manage device identities

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

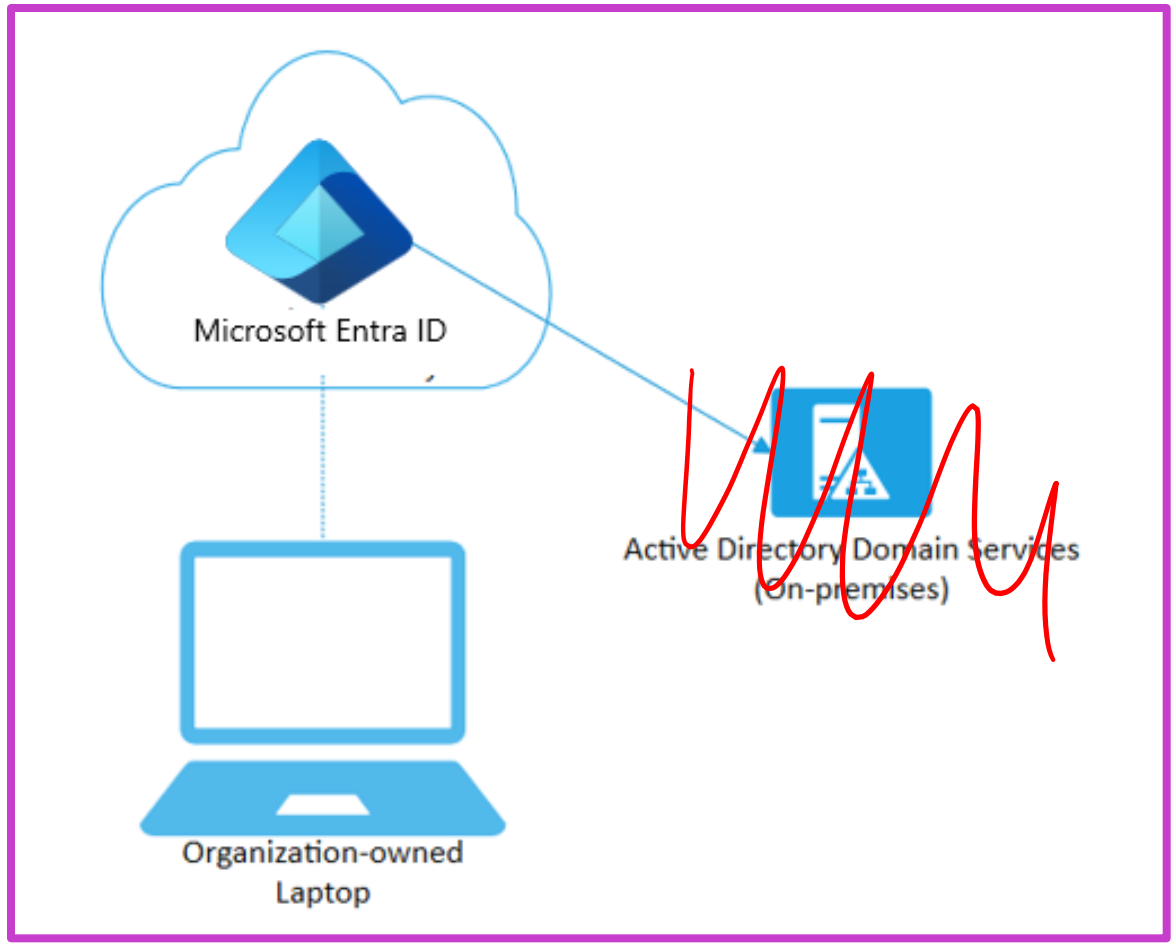
OS: Windows 10/11, iOS, Android, and MacOS Windows Server



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)

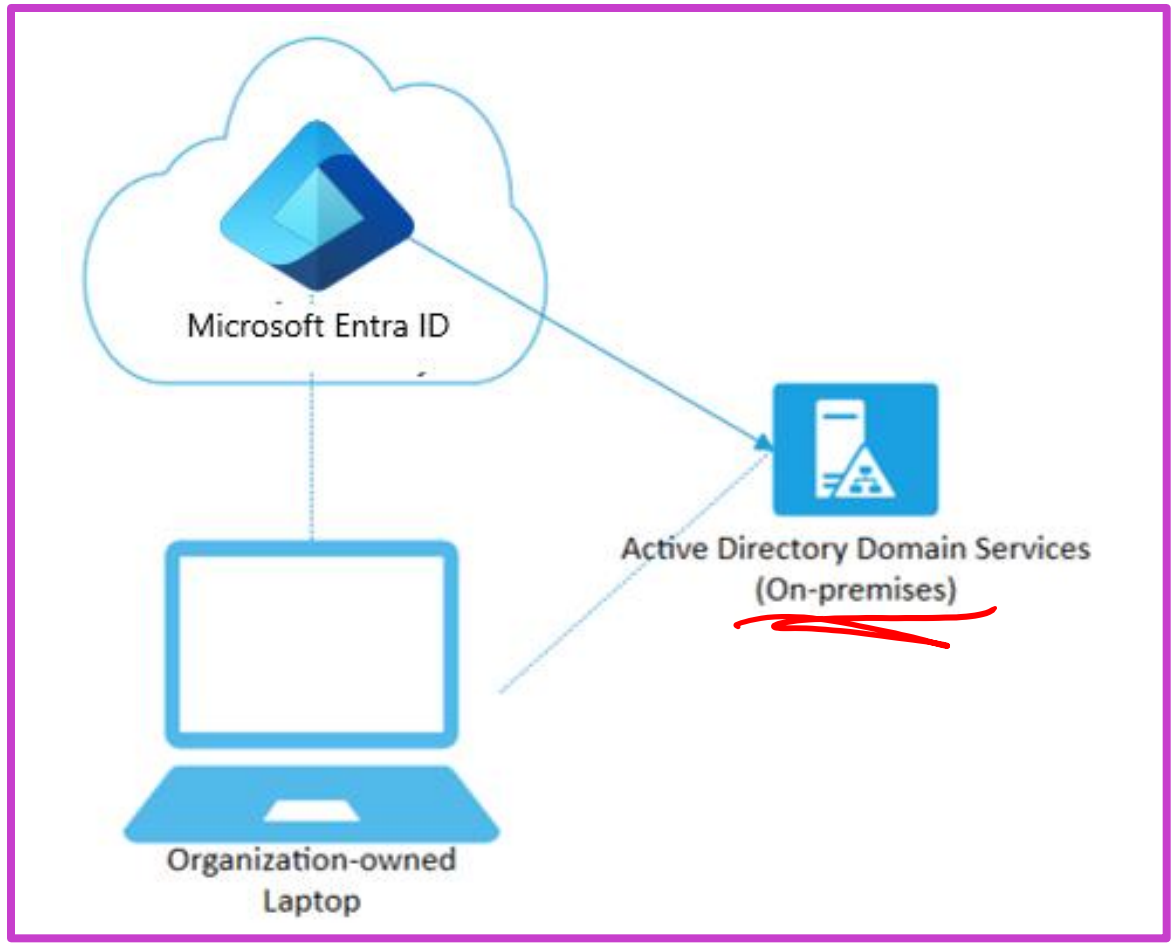


Microsoft Entra hybrid joined devices

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

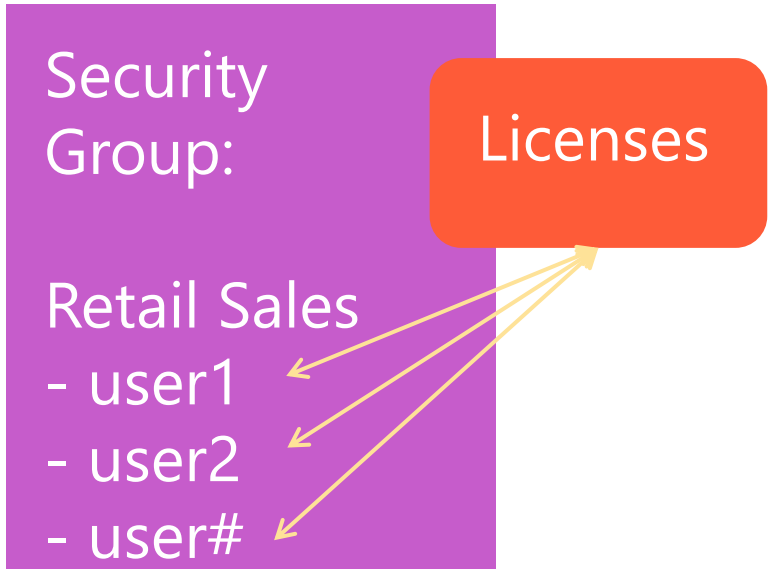
Microsoft Azure is a cloud service that provides many built-in services for free.

- 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)

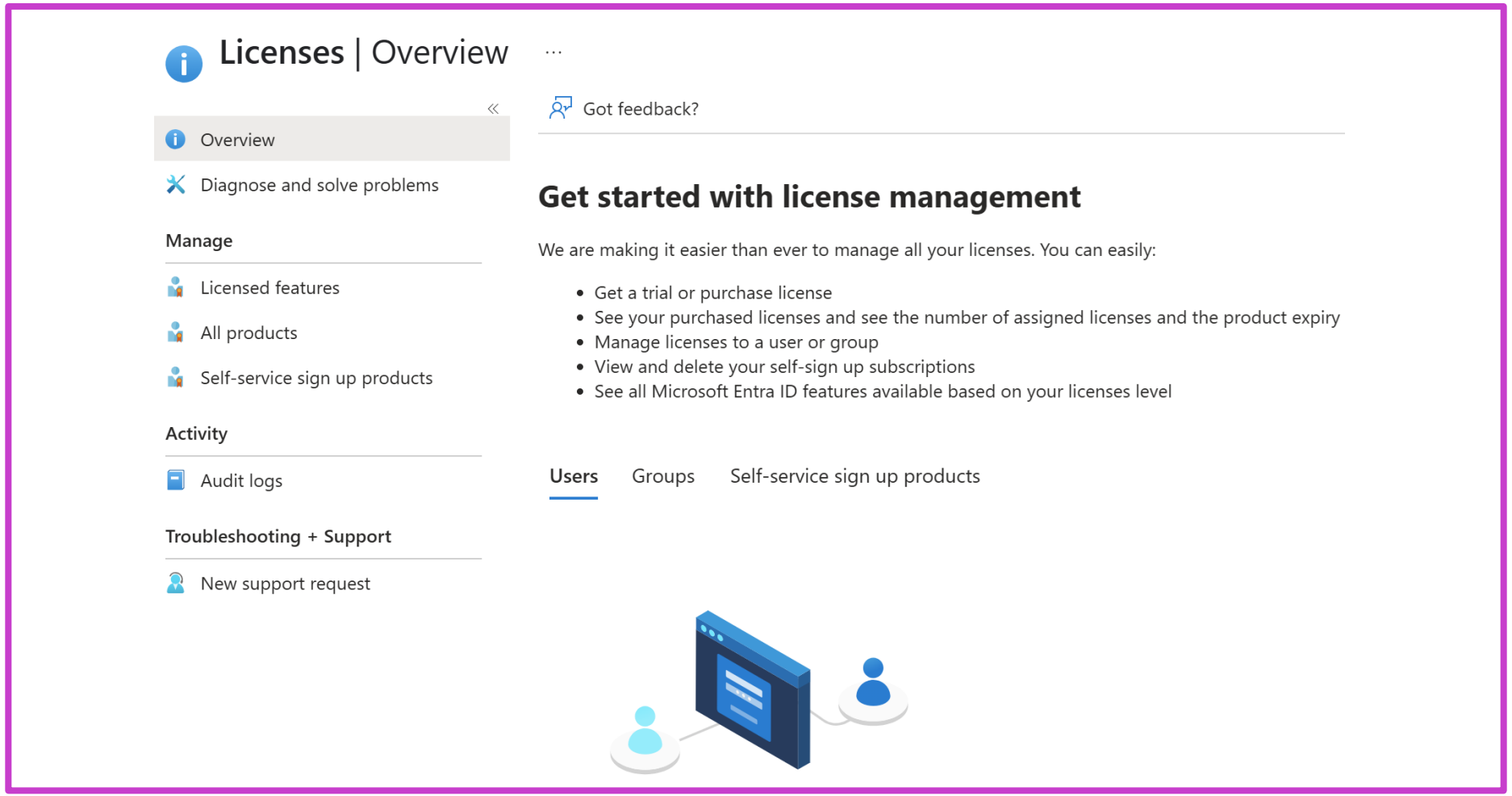
- Microsoft paid cloud services require licenses
- Licenses are assigned to each user who needs access to the services
- Each user requires a separate paid license
- Administrators use management portals and PowerShell cmdlets to manage licenses

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



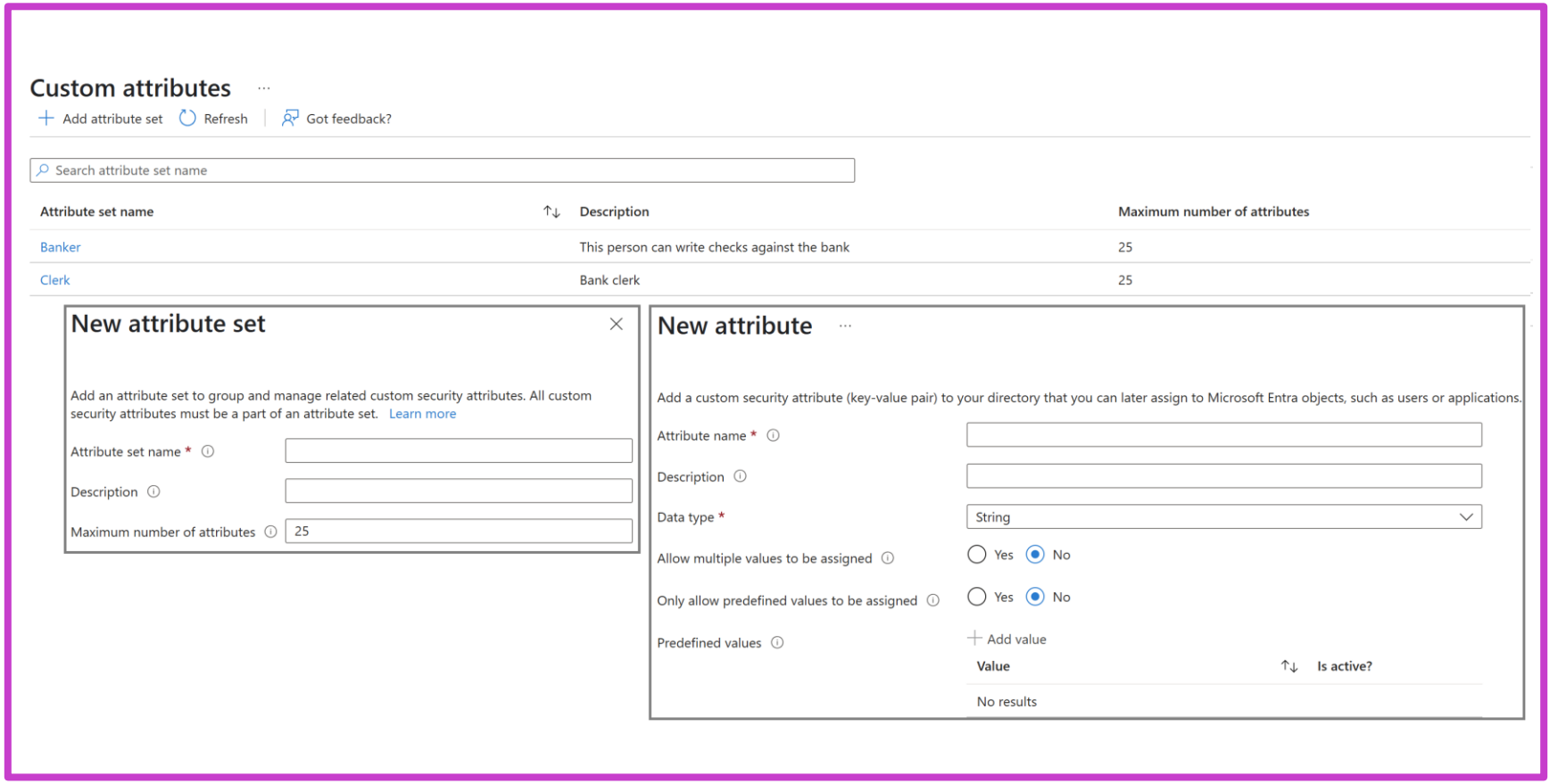
Custom security attributes

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.

Microsoft Entra ID P1/P2



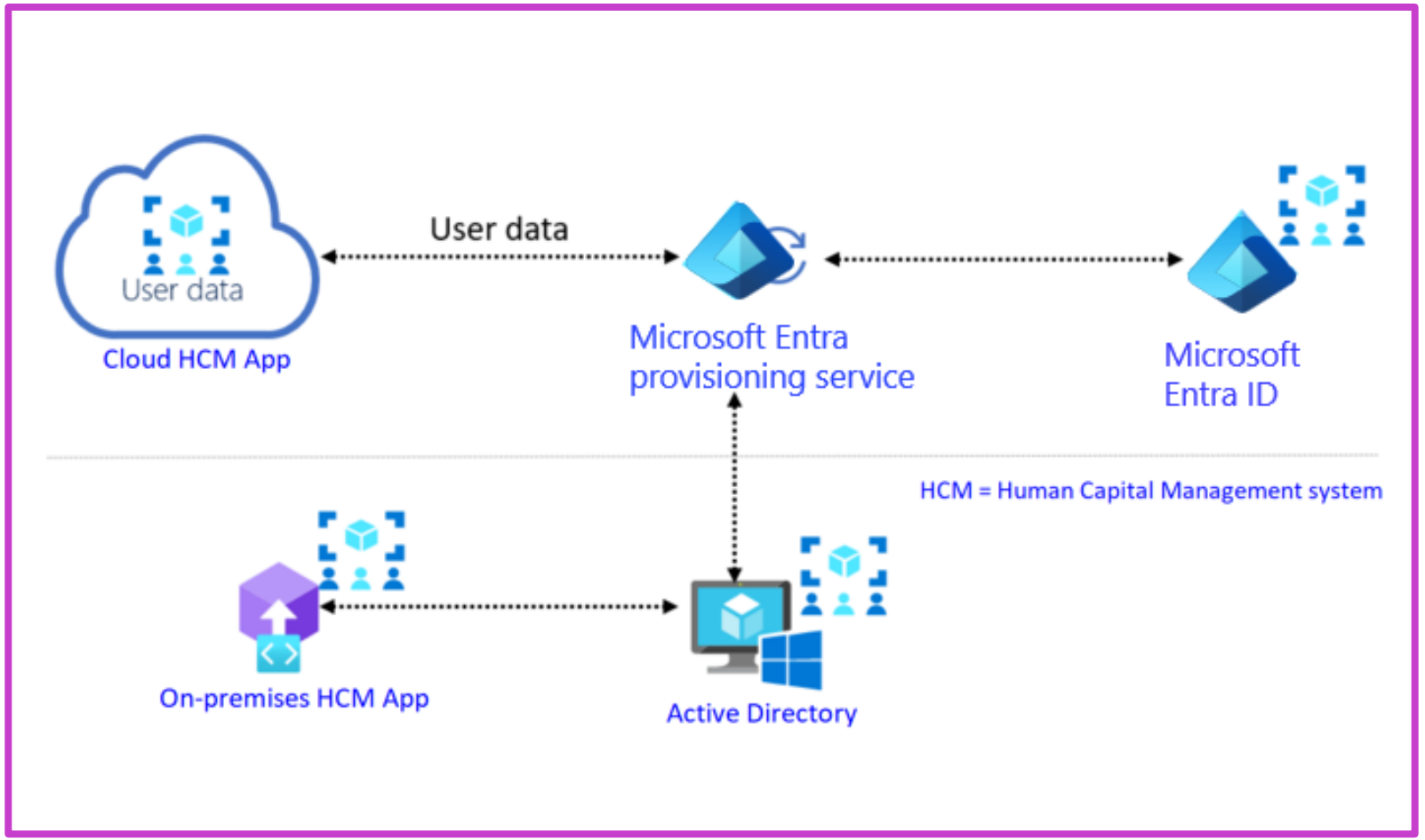
Provisioning with SCIM

(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

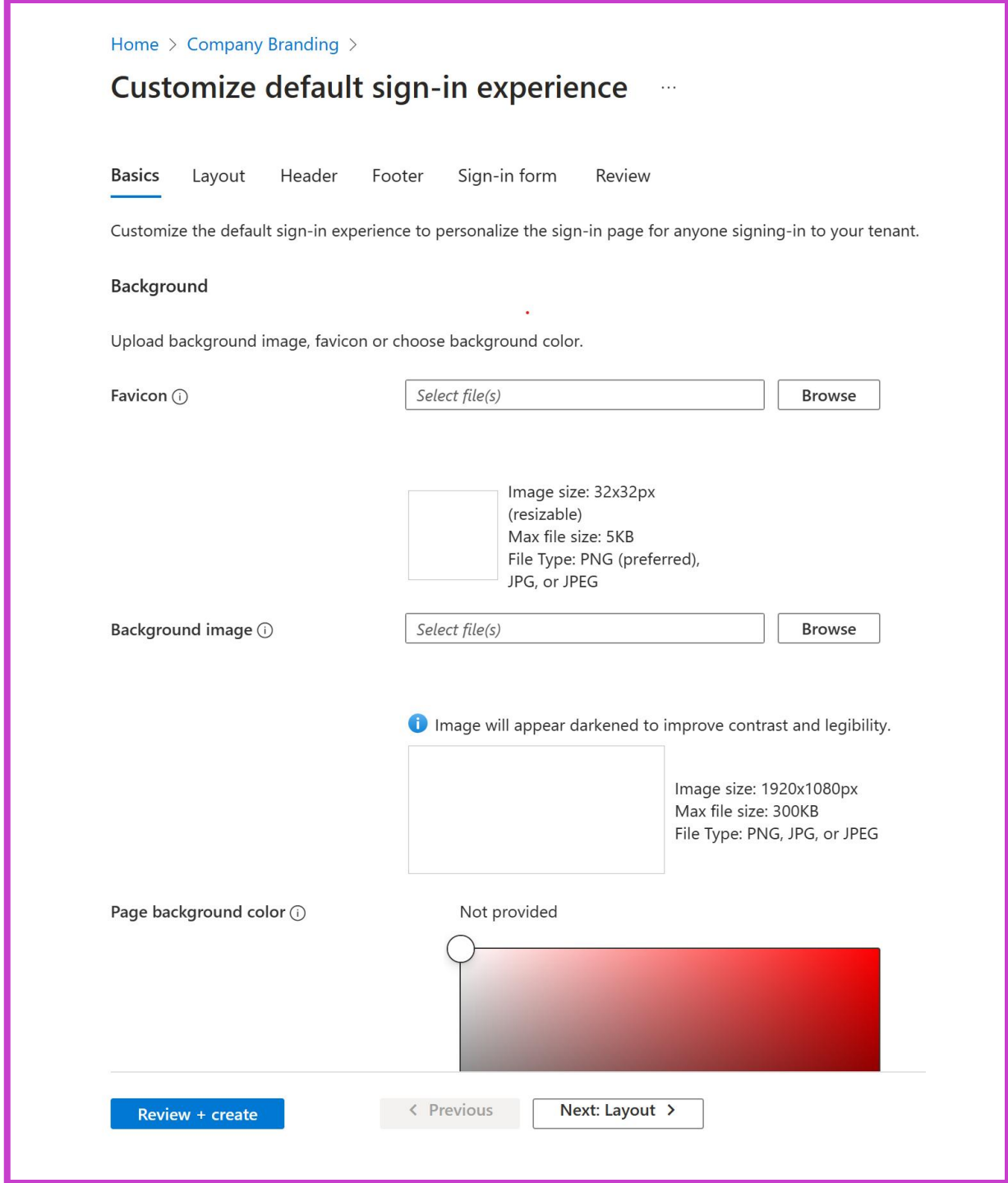
1. Configure company branding
2. Configure and manage Microsoft Entra roles
3. Configure delegation by using administrative units
4. Evaluate effective permissions
5. Configure and manage domains in Microsoft Entra and Microsoft 365
6. Configure tenant-wide settings

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



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/

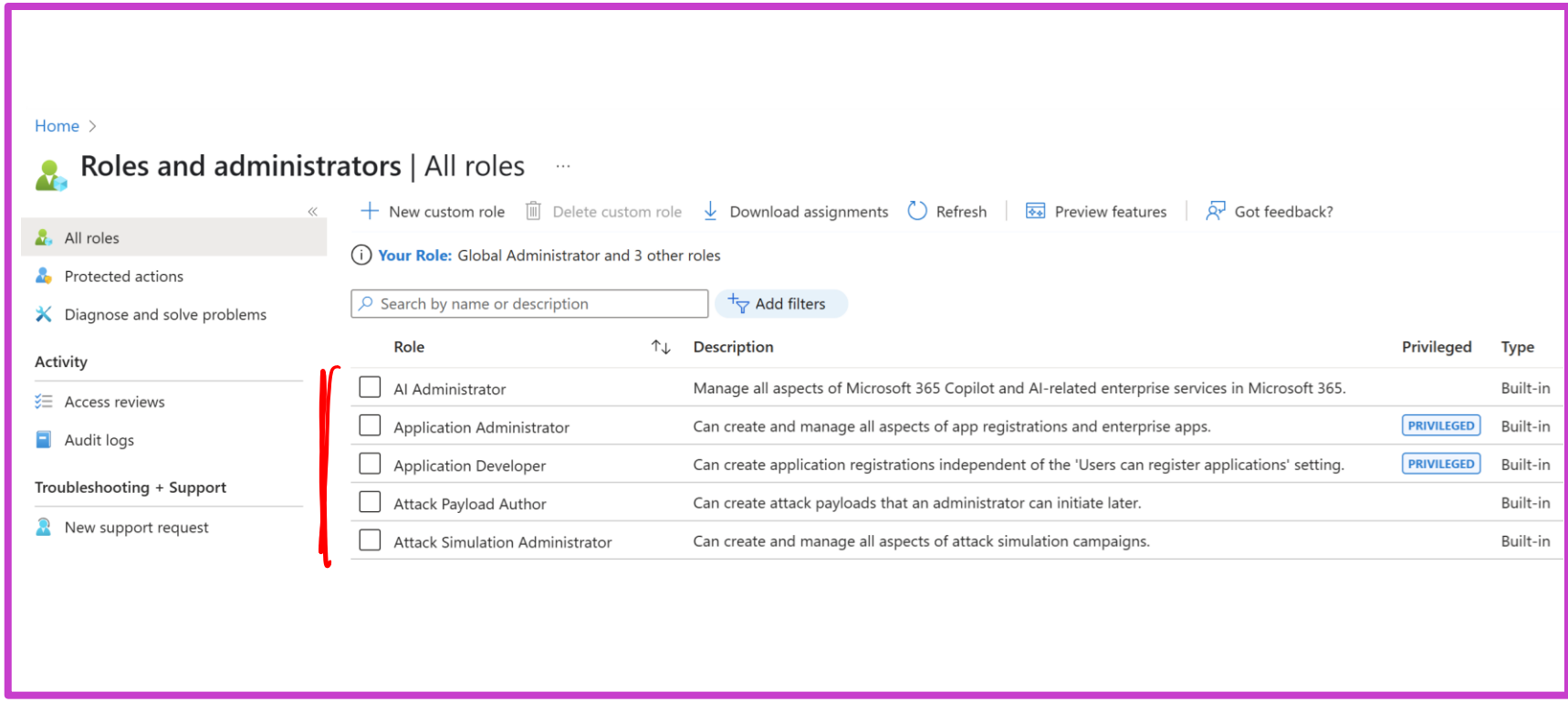
Microsoft Entra roles

Intended for:

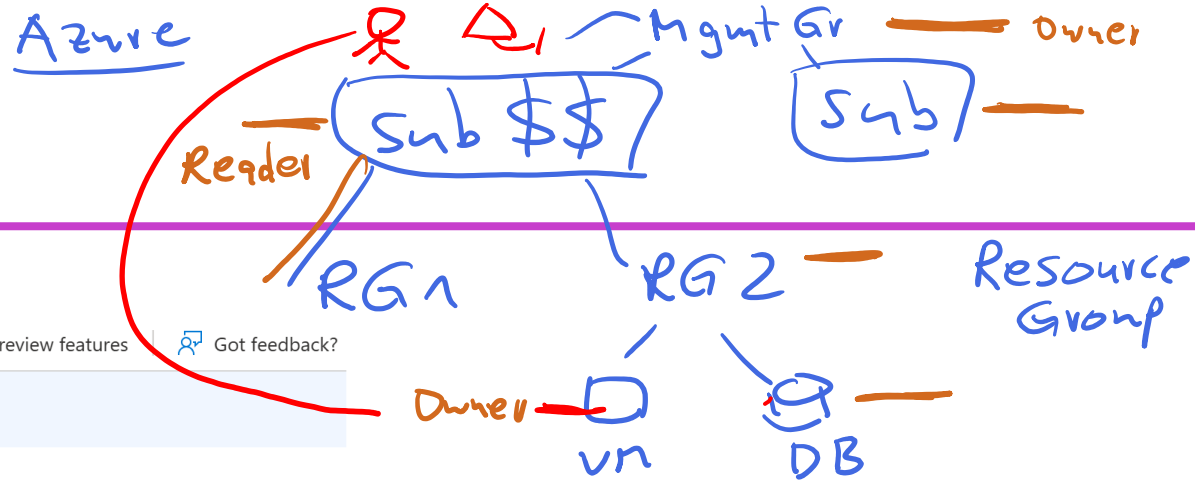
- IT admins
- App developers
- Microsoft 365, Office 365, Azure, or Dynamics CRM Online subscribers

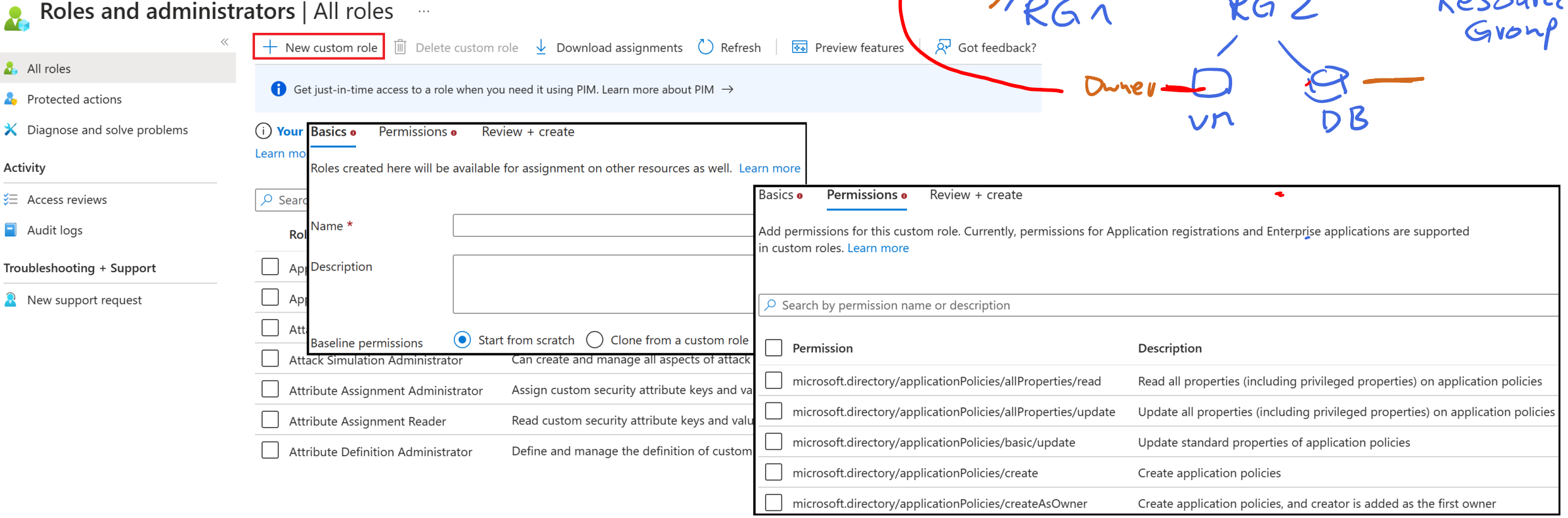
Define access to Entra ID resources

Do not overlap with Azure roles by default



Custom roles

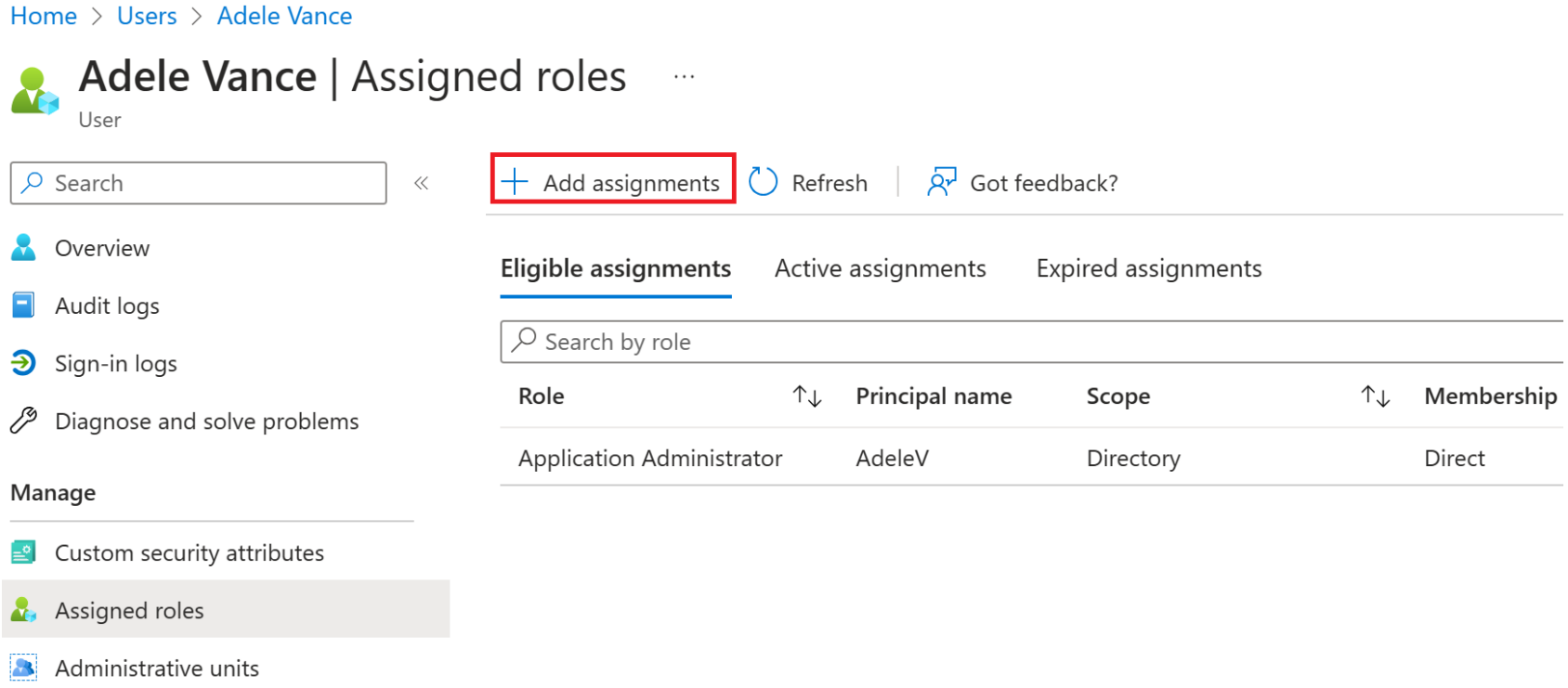




Create a custom role to meet your security goals or needs

Requires a Microsoft Entra ID premium license

Assigning roles—to a user or group

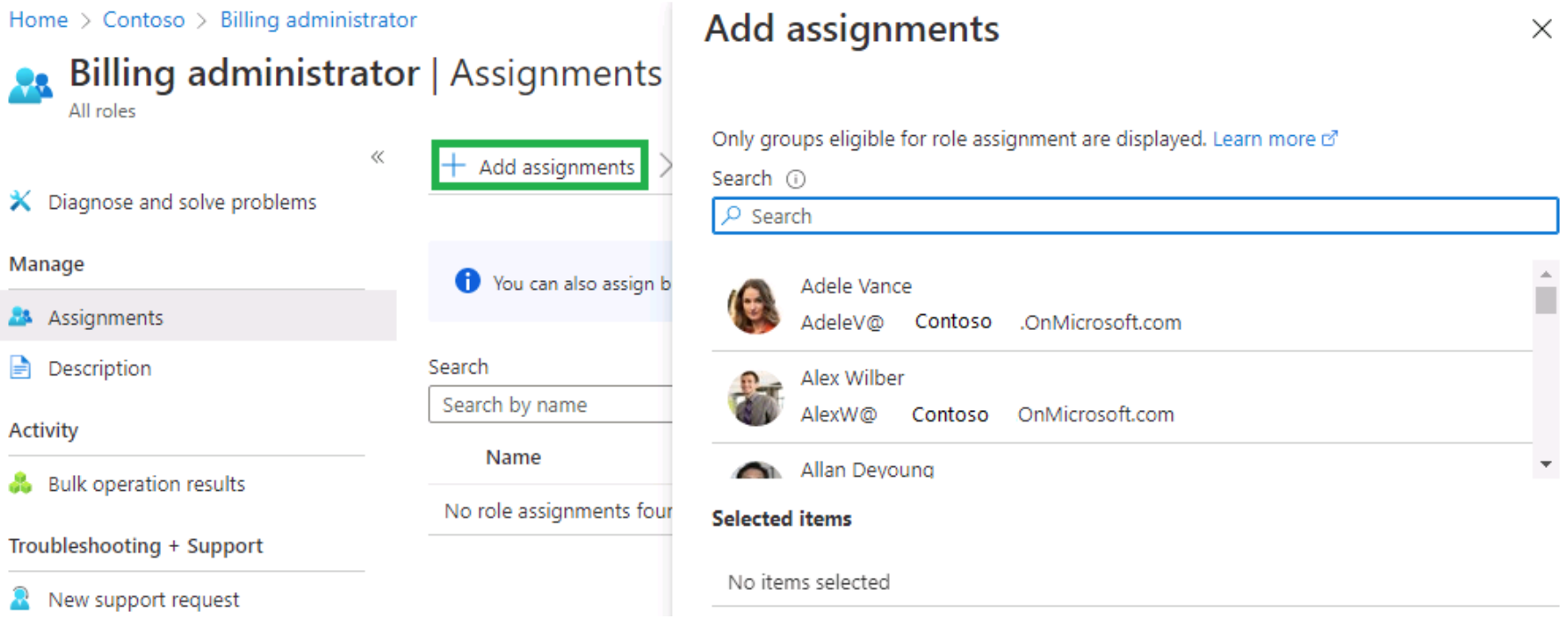


Assign built-in or custom roles

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

Use principle of least privilege when assigning

Assign users or groups to a role



Identities can be added to a role

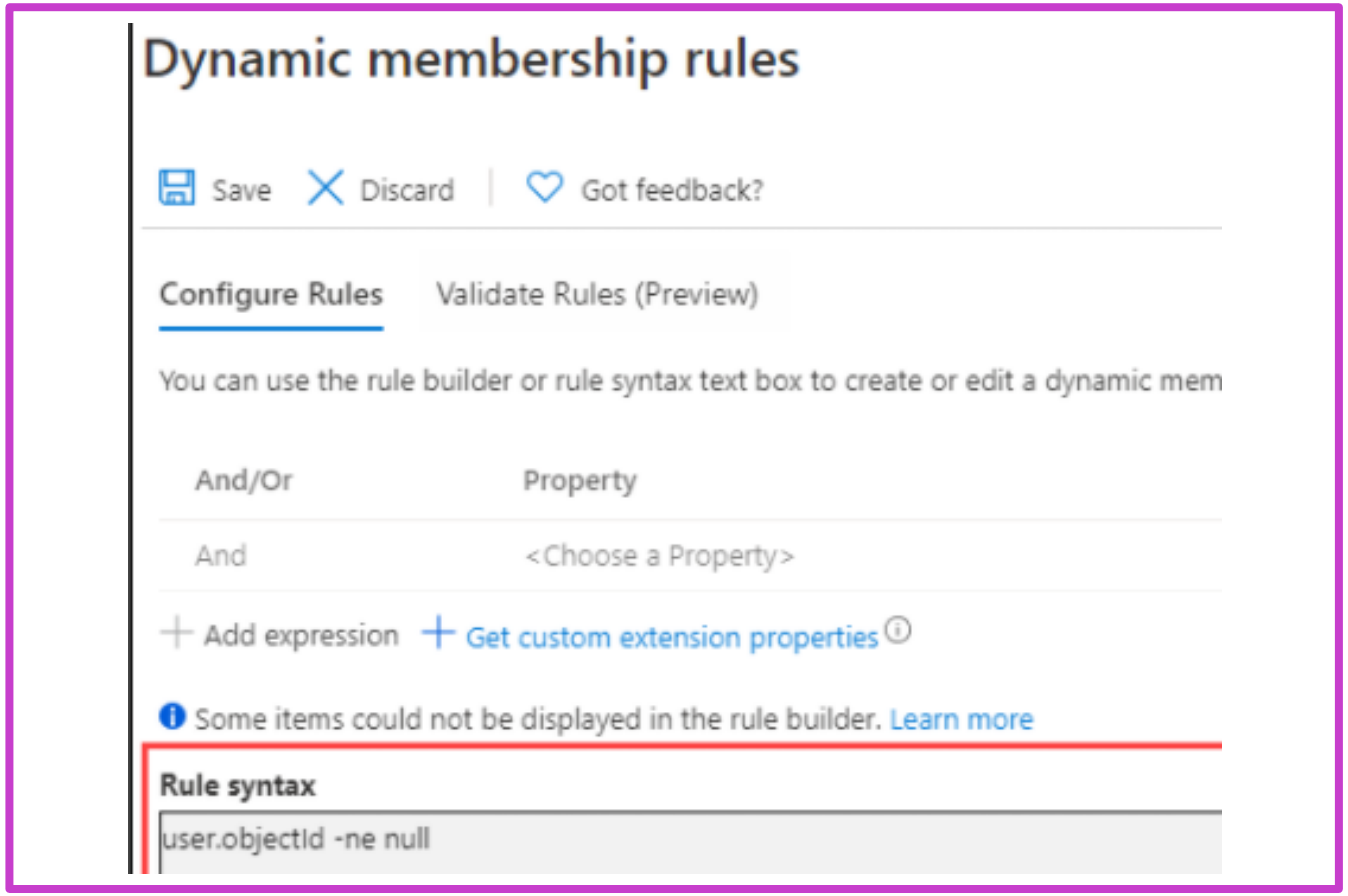
Alternative method to assign roles

Use principle of least privilege when assigning

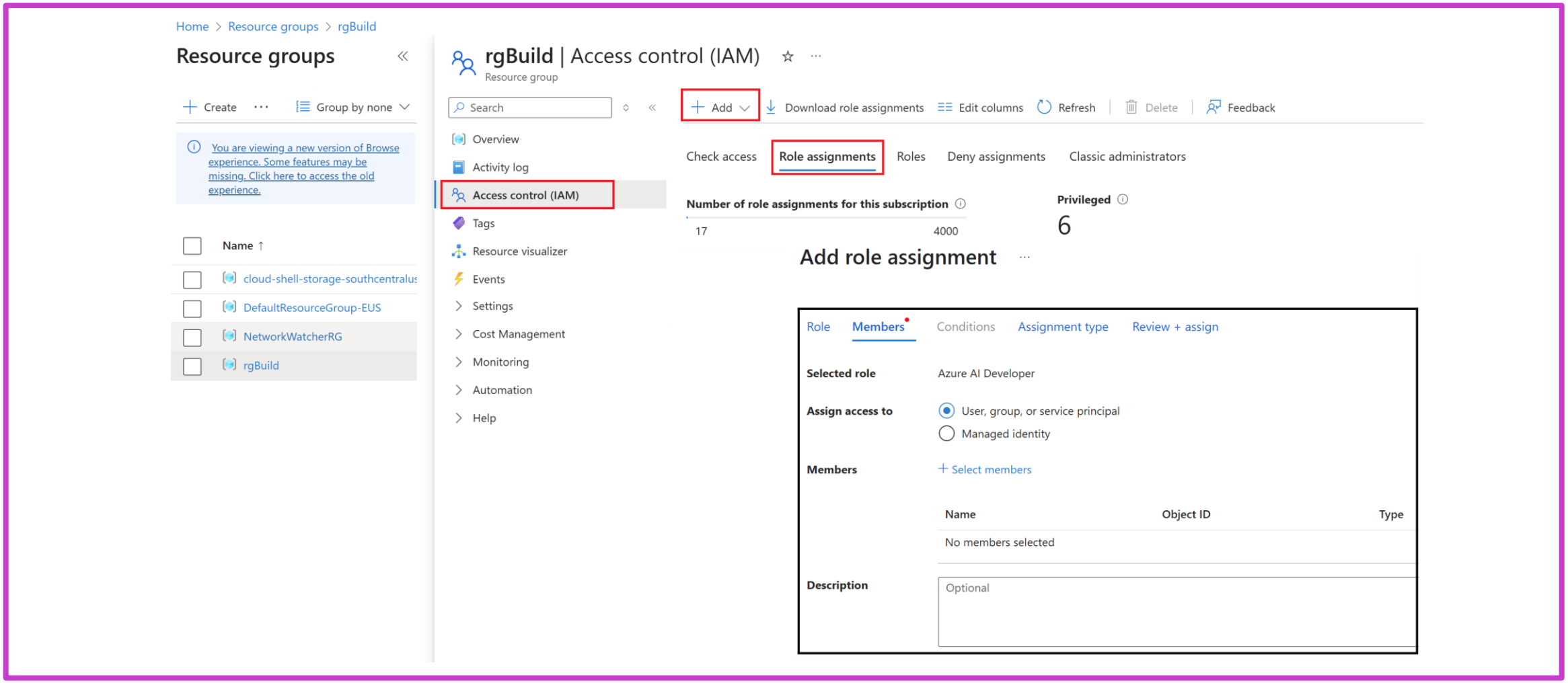
Exercise—Explore dynamic groups

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

[Launch this Exercise in GitHub]



Assigning Azure roles to a subscription or broader scope



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

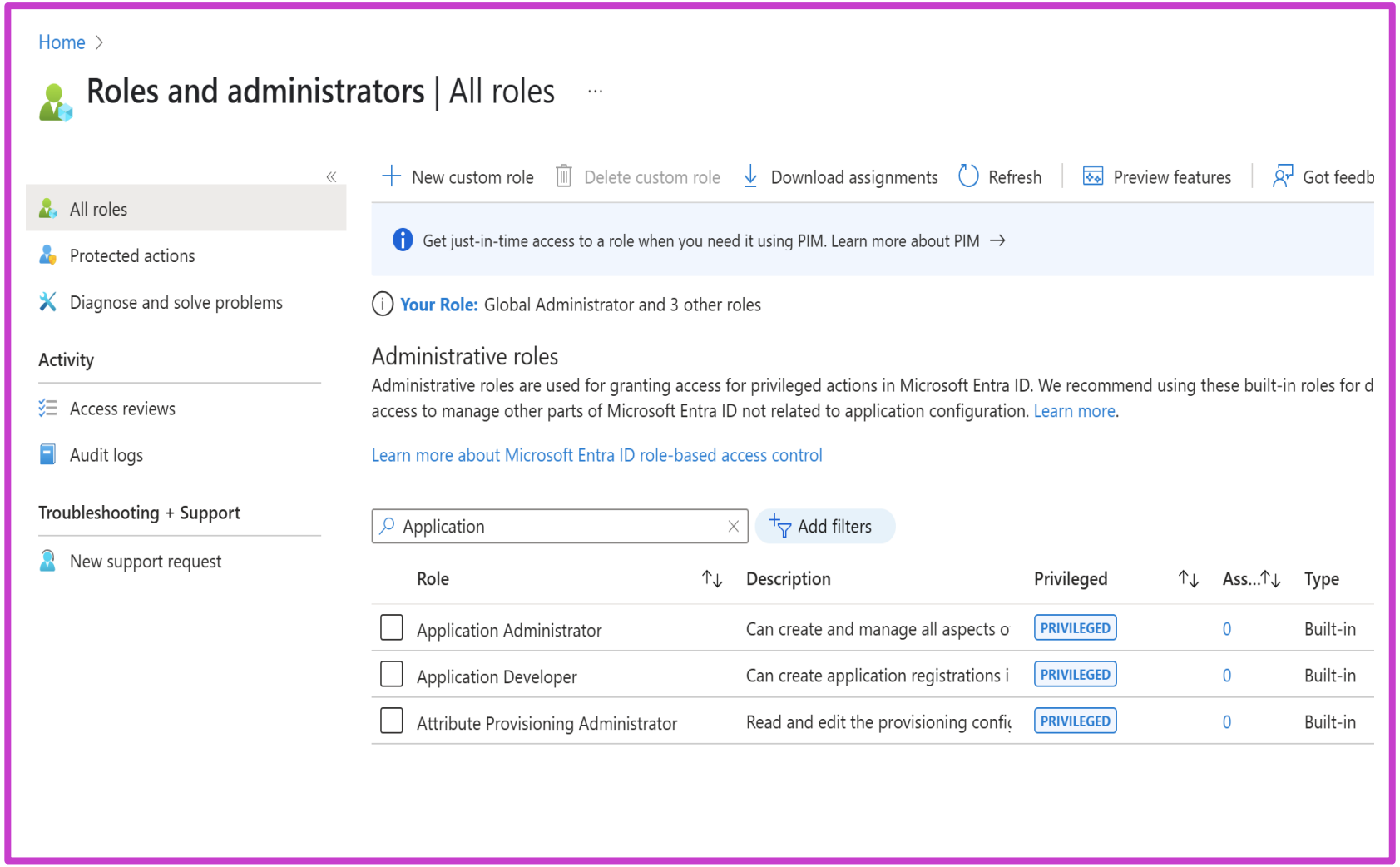
- Password administrator role
- Group administrator role

Delegating app registration

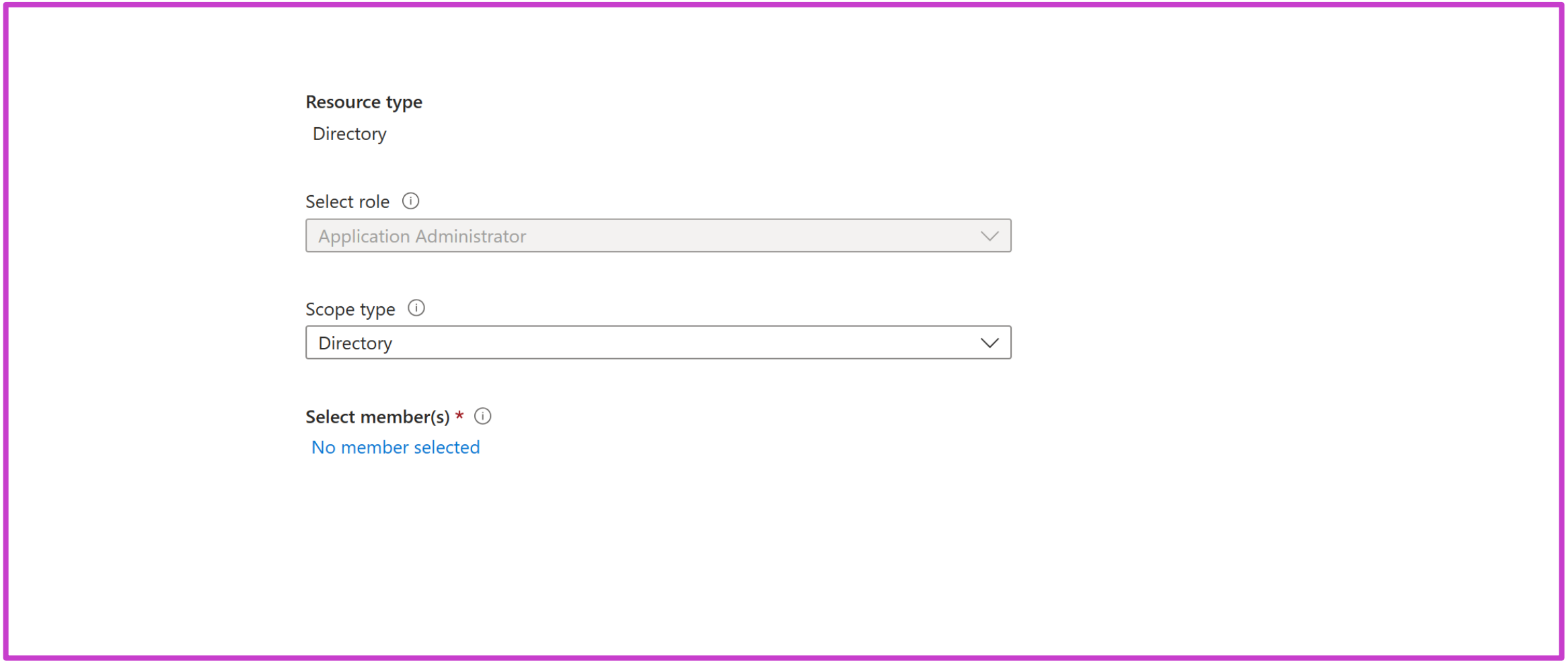
- Application developer role

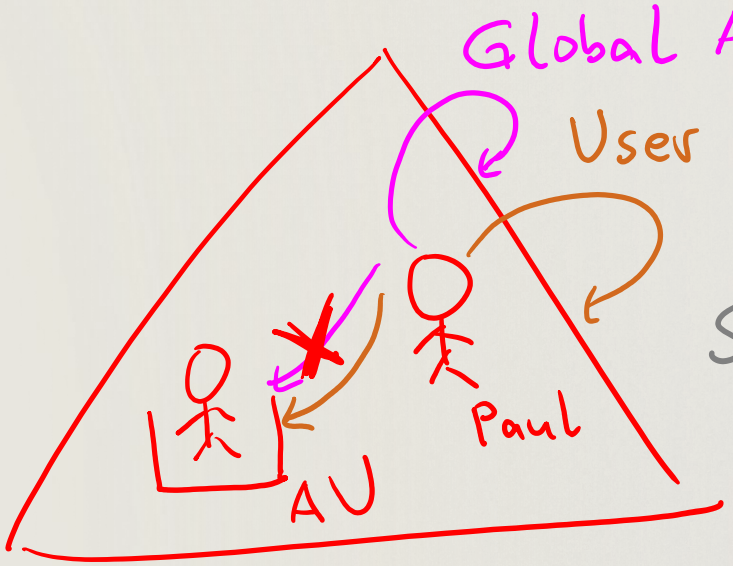
Delegating app ownership

- Enterprise application owner role
- Application registration owner role



Demo—assigning roles



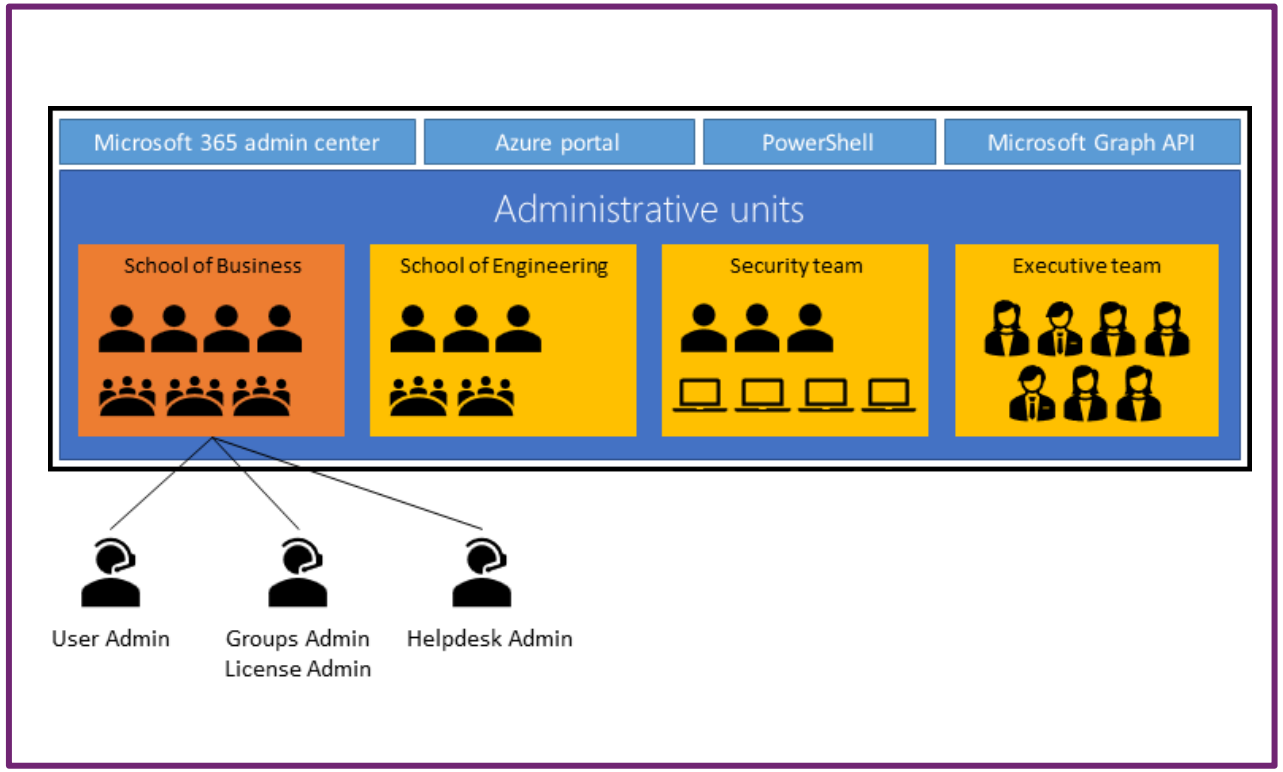


Roles
RBAC

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

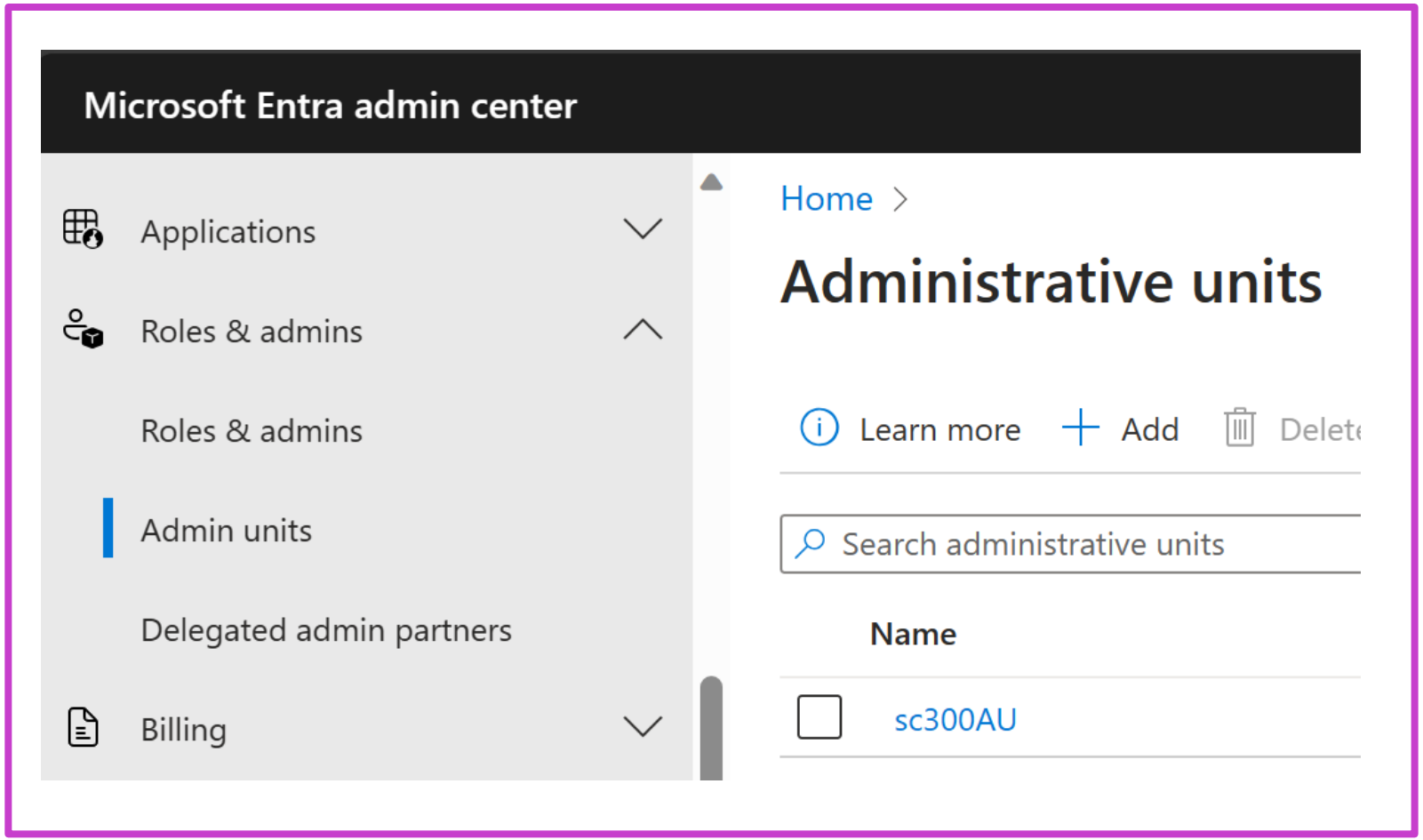
- Authentication administrator role

Delegating licensing

- License administrator

Delegating user, group, and password management

- User administrator



Evaluate effective permissions for Microsoft Entra role

Permissions in Microsoft Entra ID

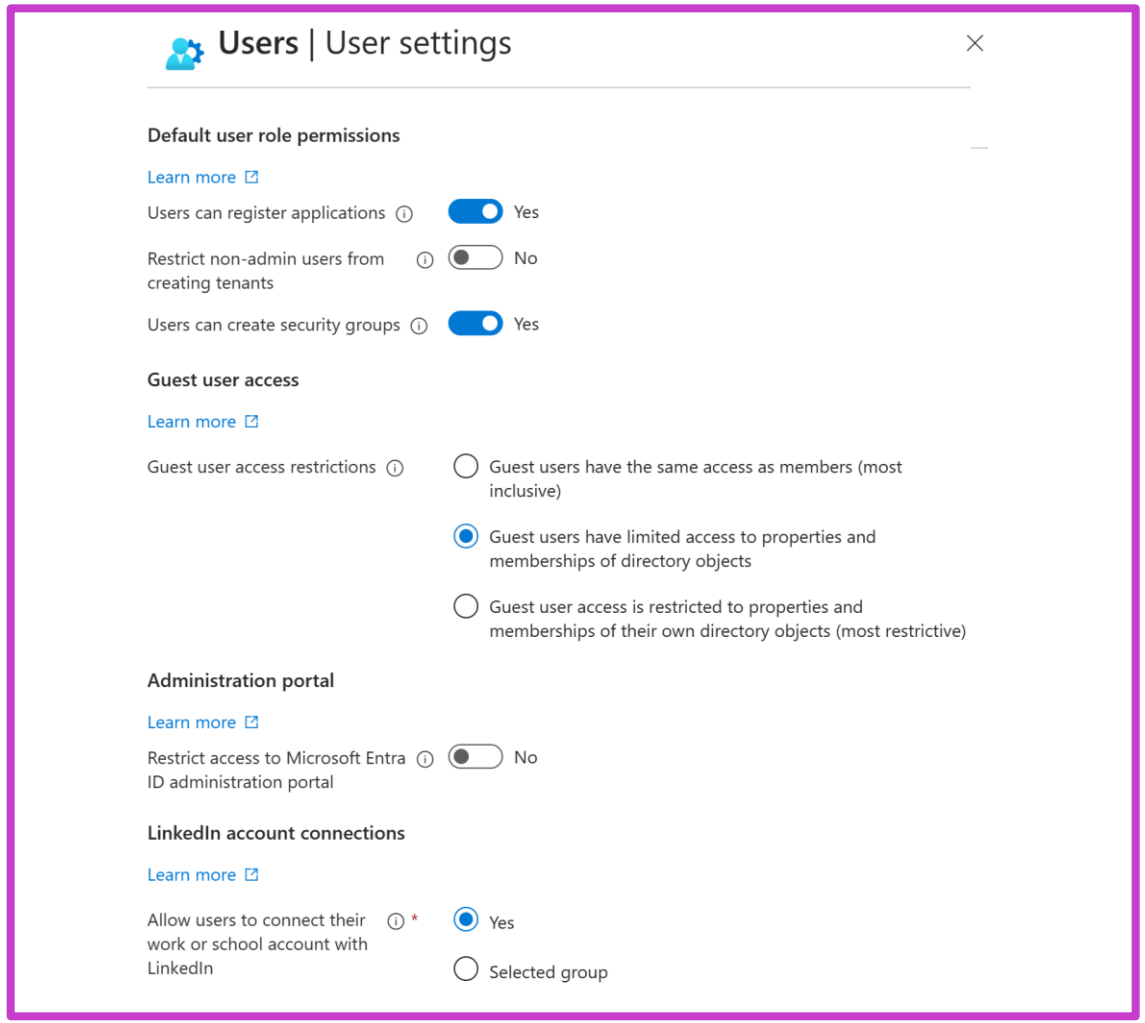
Permission—consent or authorization to perform a specific action.

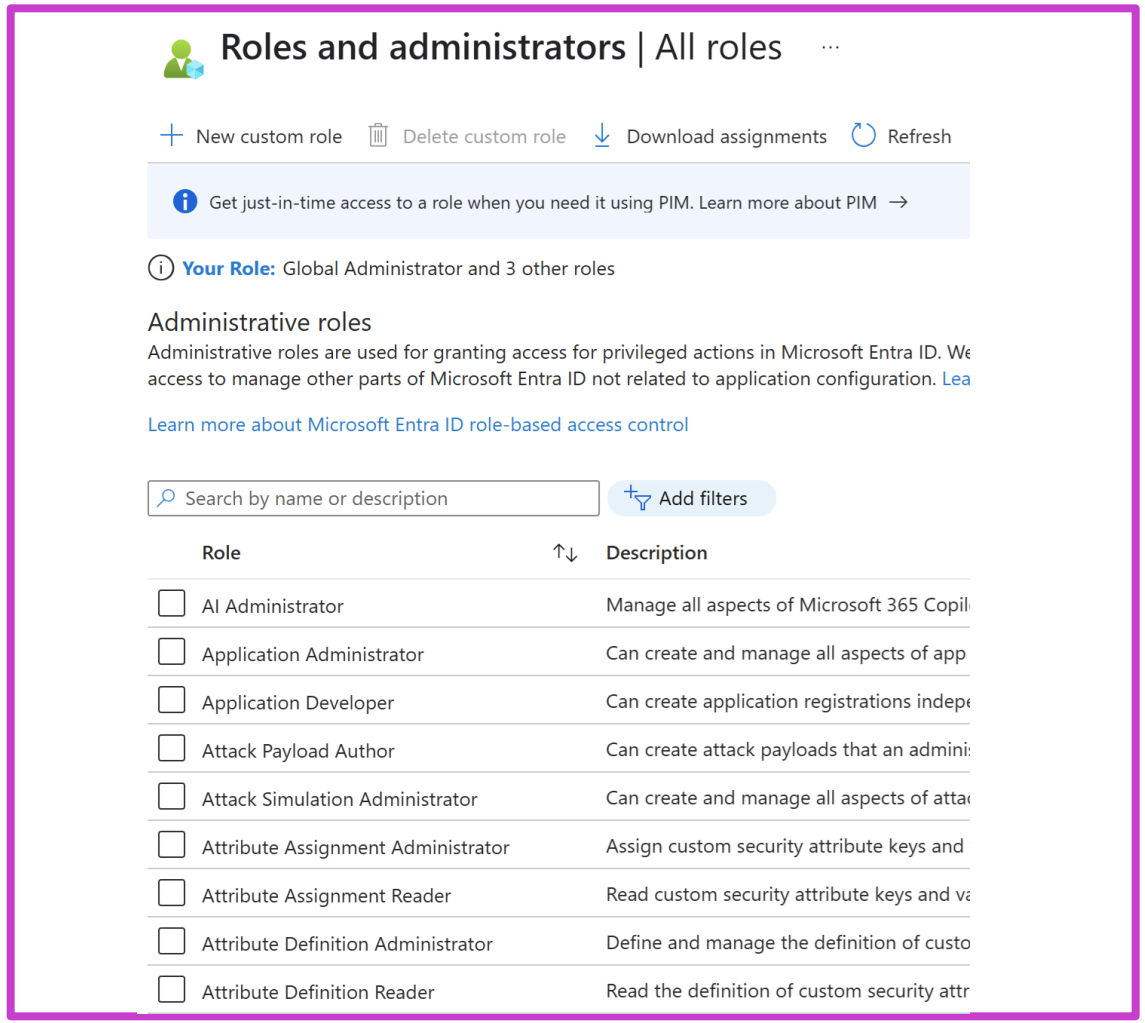
Who gets permissions:

Member Users	External Users	Applications	Devices
Example default permissions for each:			
• Enumerate list of users • Invite external users • Change their password • Manage Photo • Create groups • And so on	• Read own properties • Change their password • Search for groups • Cannot invite groups • And so on	• App must be registered • API and permissions assigned in registration • Examples – read, write, verify, and others	• Device must be registered or joined to the Microsoft Entra tenant

* Augment or restrict permissions with settings and role assignments

Augment or restrict permissions





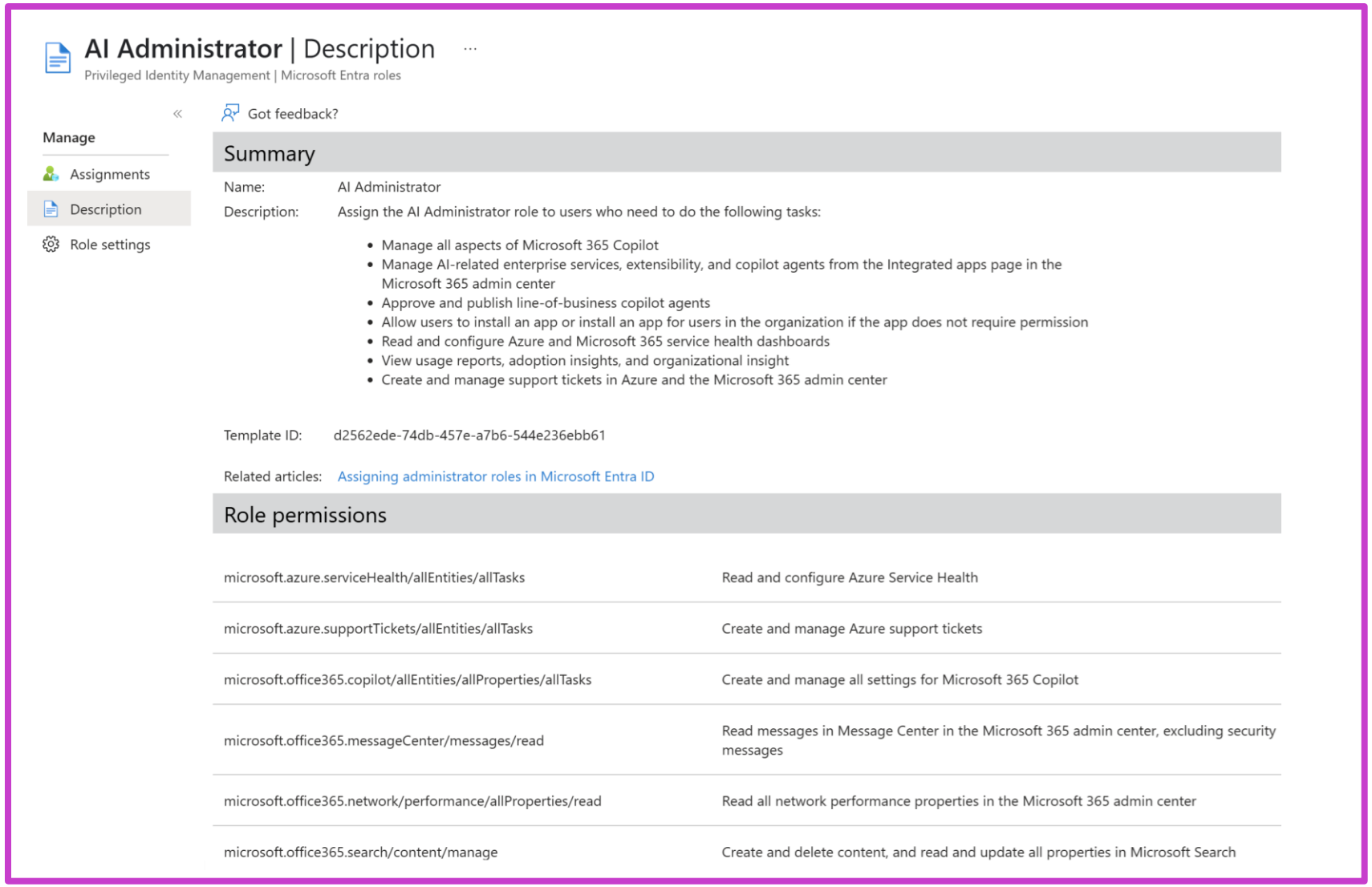
Analyze permission

Role permission

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

Guest/service principal

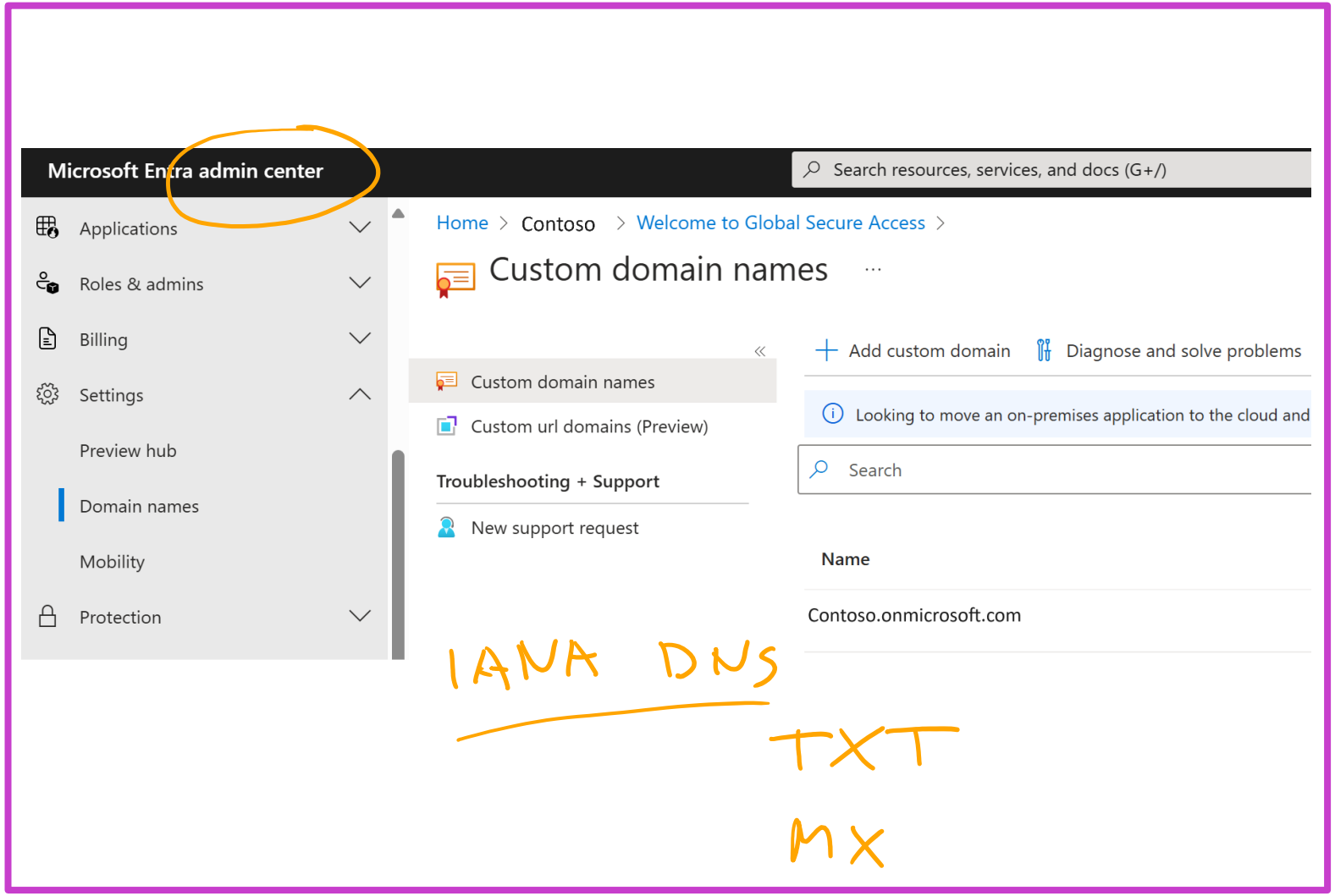
Additional permission given to ensure a basic level of functionality when assigned to guest users or service principals.



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



Configure tenant-wide settings

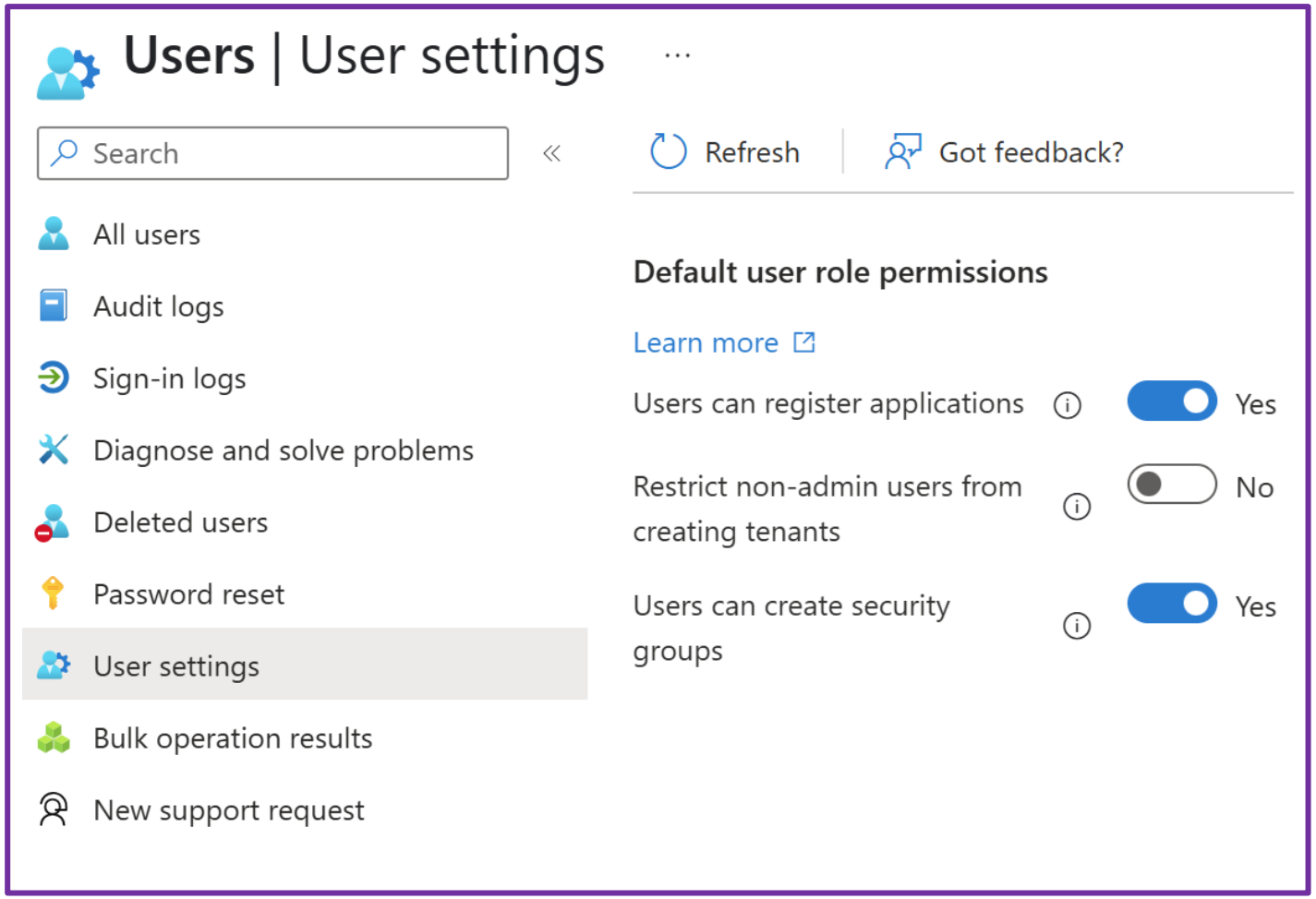
Tenant-wide settings

- **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

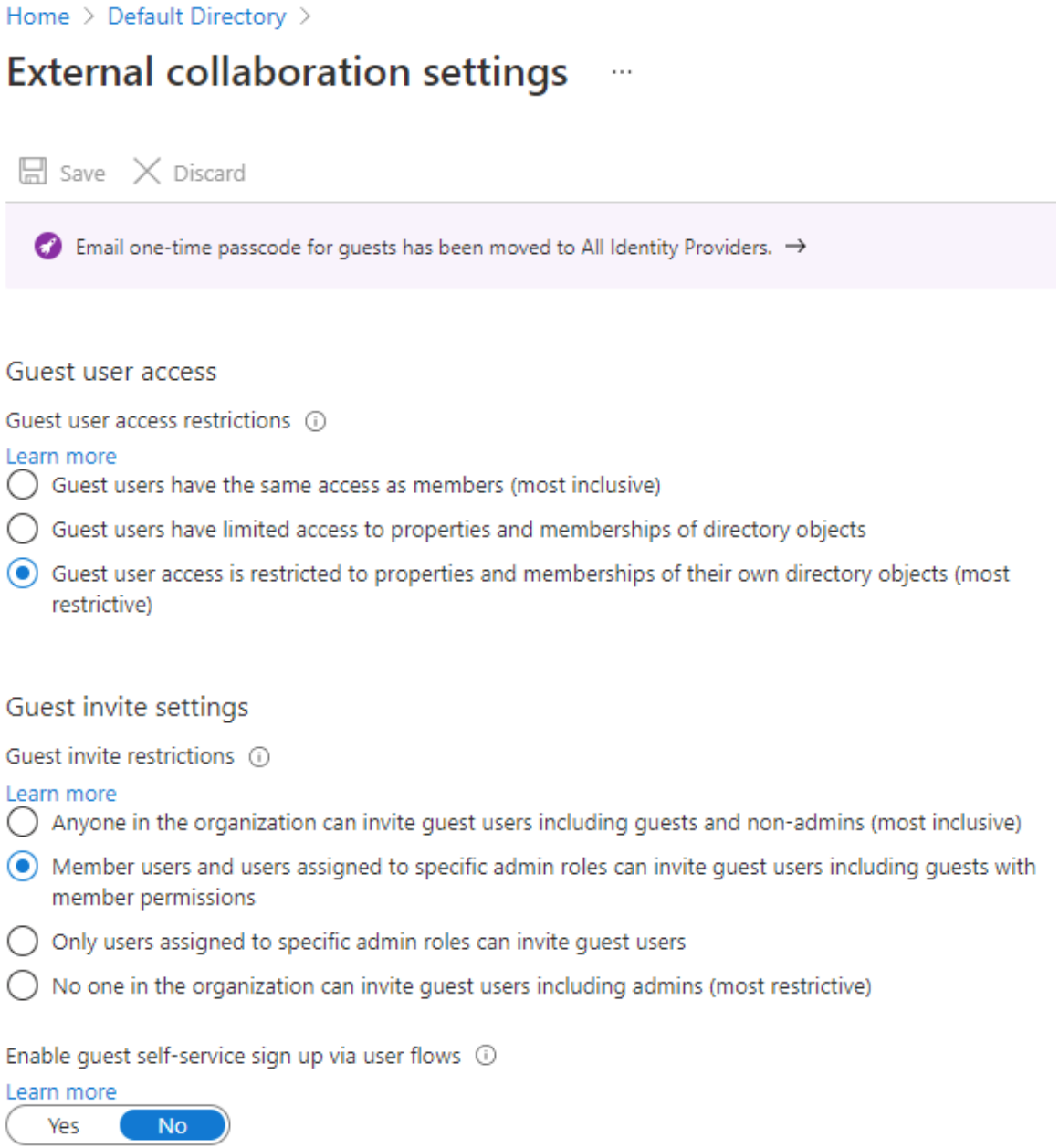
- App registrations—users can register applications
- Administration portal – Restrict access to the Microsoft Entra ID administration portal
- LinkedIn account connections – Allow users to connect their work or school account with LinkedIn
- Other



User settings—external users

Microsoft Entra ID → Identity → Users → User Settings

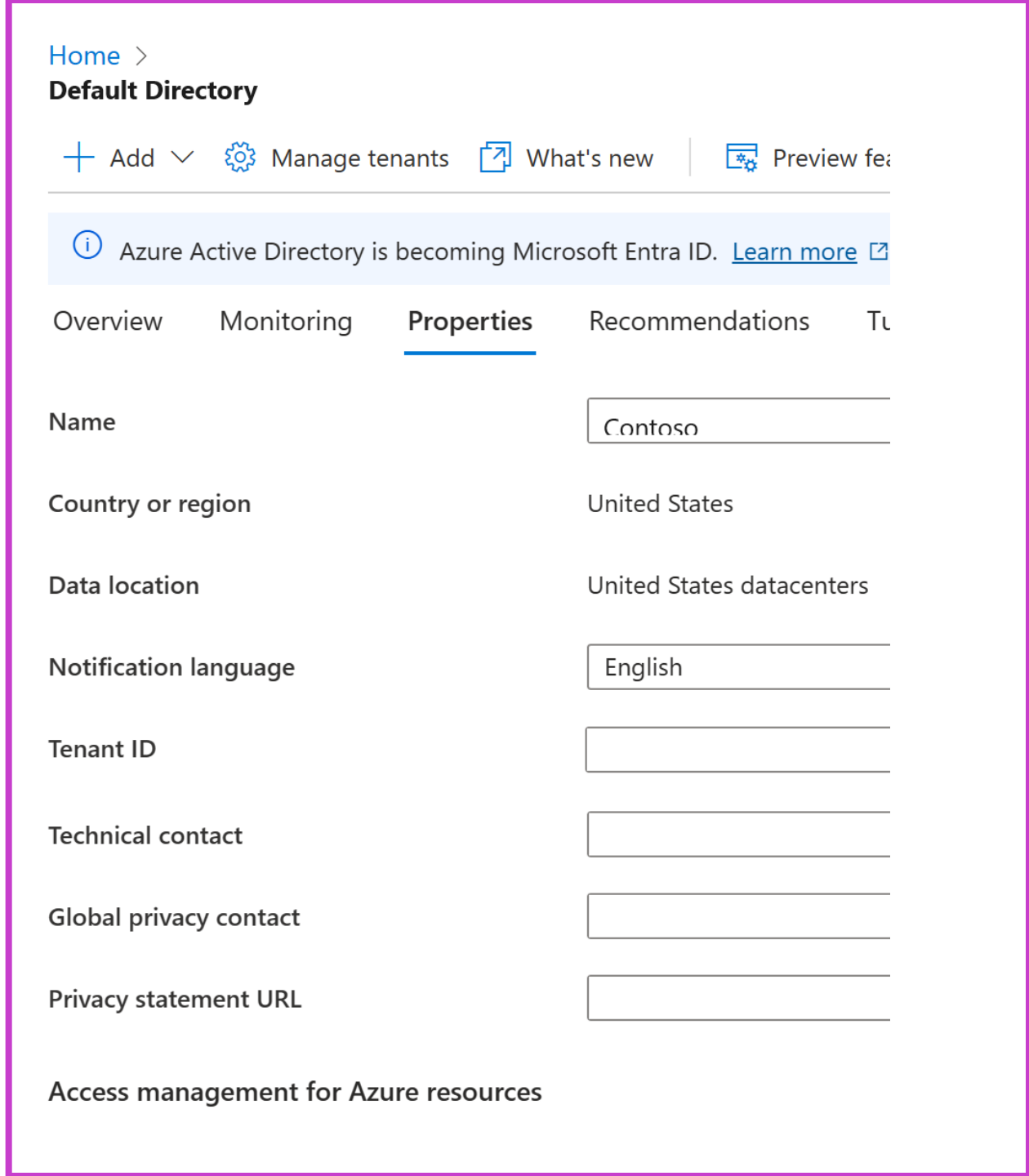
- App registrations—users can register applications
- Administration portal—restrict access to the Microsoft Entra ID administration portal
- LinkedIn account connections—allow users to connect their work or school account with LinkedIn
- Manage user feature previews
- External collaboration setting



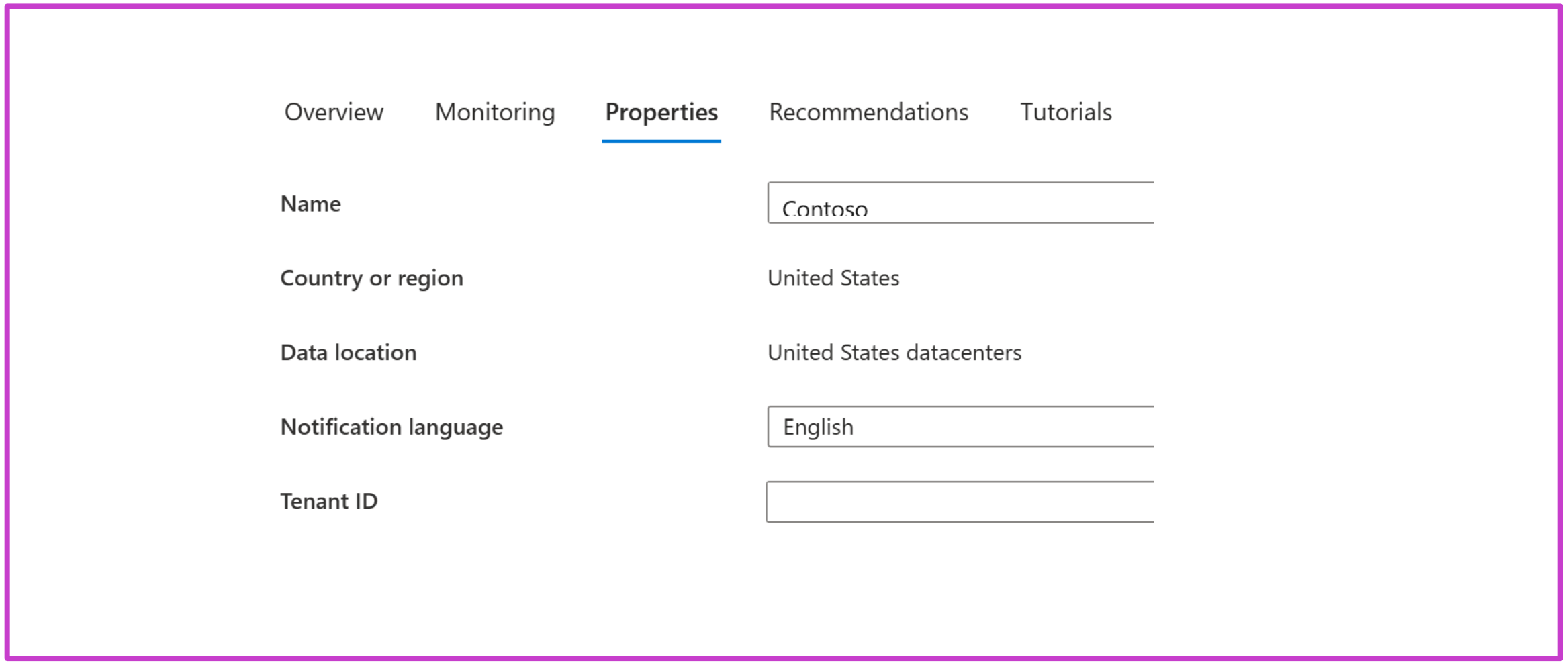
Tenant properties

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



Demo—set tenant-wide settings



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

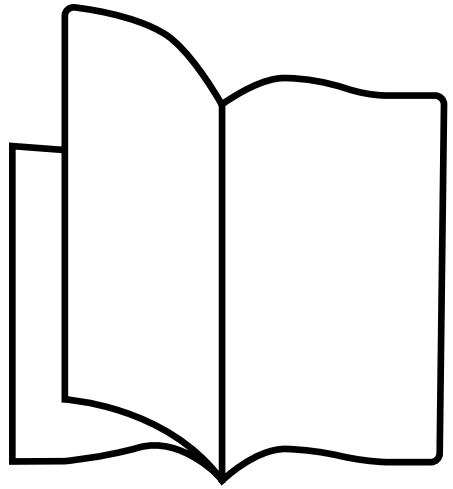
https://learn.microsoft.com/azure/role-based-access-control/role-definitions

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

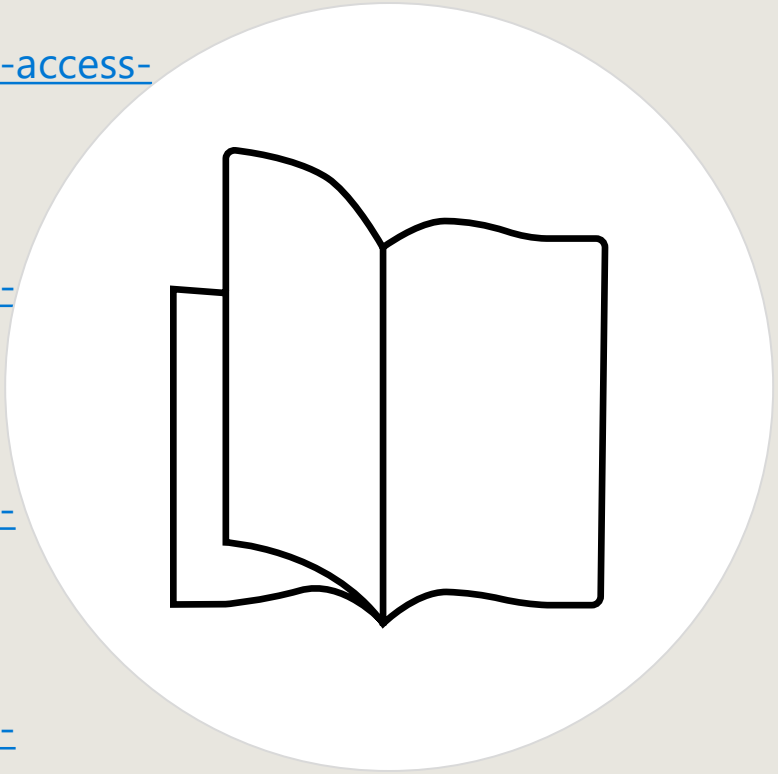
https://learn.microsoft.com/entra/identity/conditional-access/howto-conditional-policy-azure-management

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

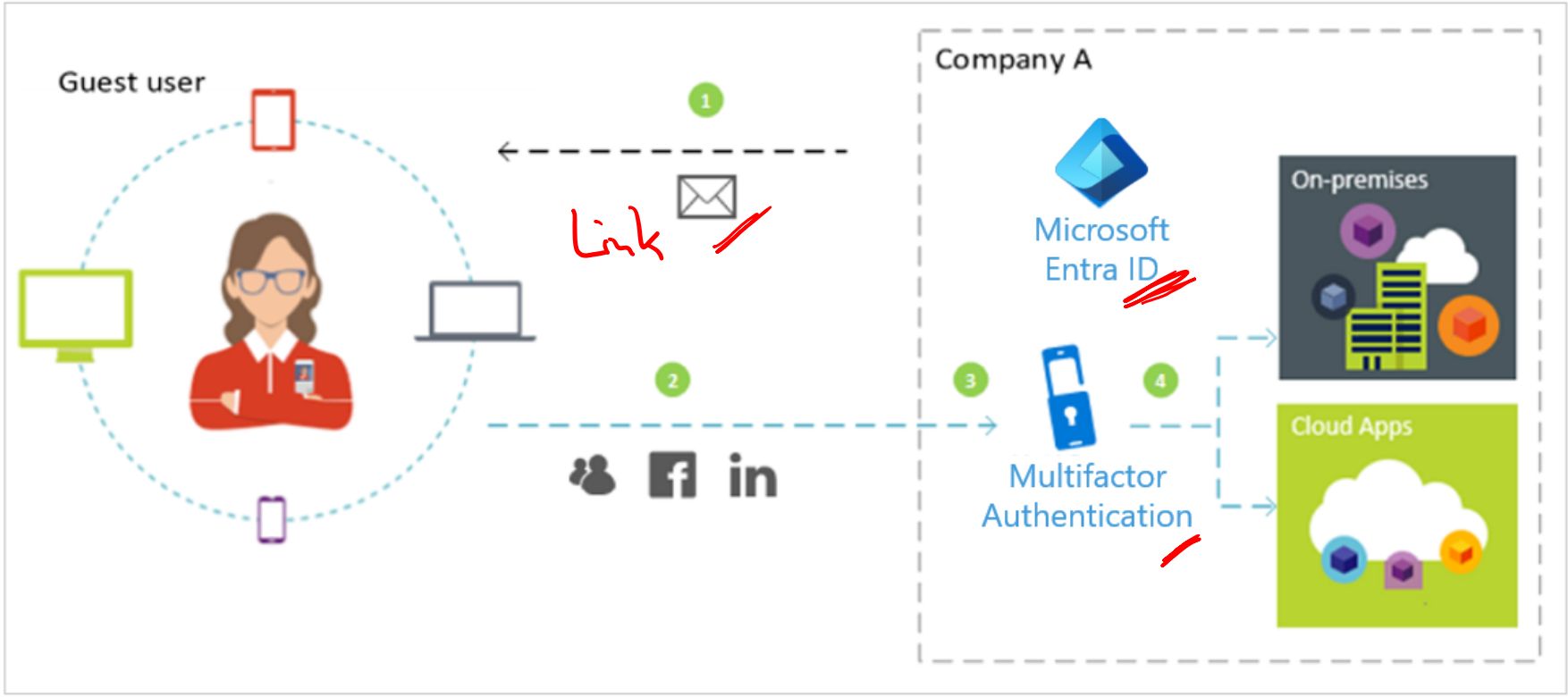
1. Describe guest users and B2B accounts
2. Manage external collaboration
3. How external users are managed in Microsoft 365
4. Invite external users—individually or in bulk
5. Manage external user accounts in Microsoft Entra ID
6. Implement cross-tenant access controls
7. Configure identity providers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

Describe external users, B2B accounts, and manage external collaboration

Relationship between external and member users

How the user authenticates	UserType property: Guest	UserType property: Member
External	**External guest** Uses an external Azure AD account, social identity, or other external identity provider to sign in. Most external users fall into this category.	**External member** Uses an external account to authenticate but has member-level access in your organization. Common scenario in multi-tenant organizations.
Internal	**Internal guest** Has an account in your Azure AD directory but only guest-level access in your organization. This is often a legacy guest user created before the availability of Azure AD B2B.	**Internal member** Has an account in your Azure AD directory and member-level access in your organization. Generally considered employees of your organization.

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.

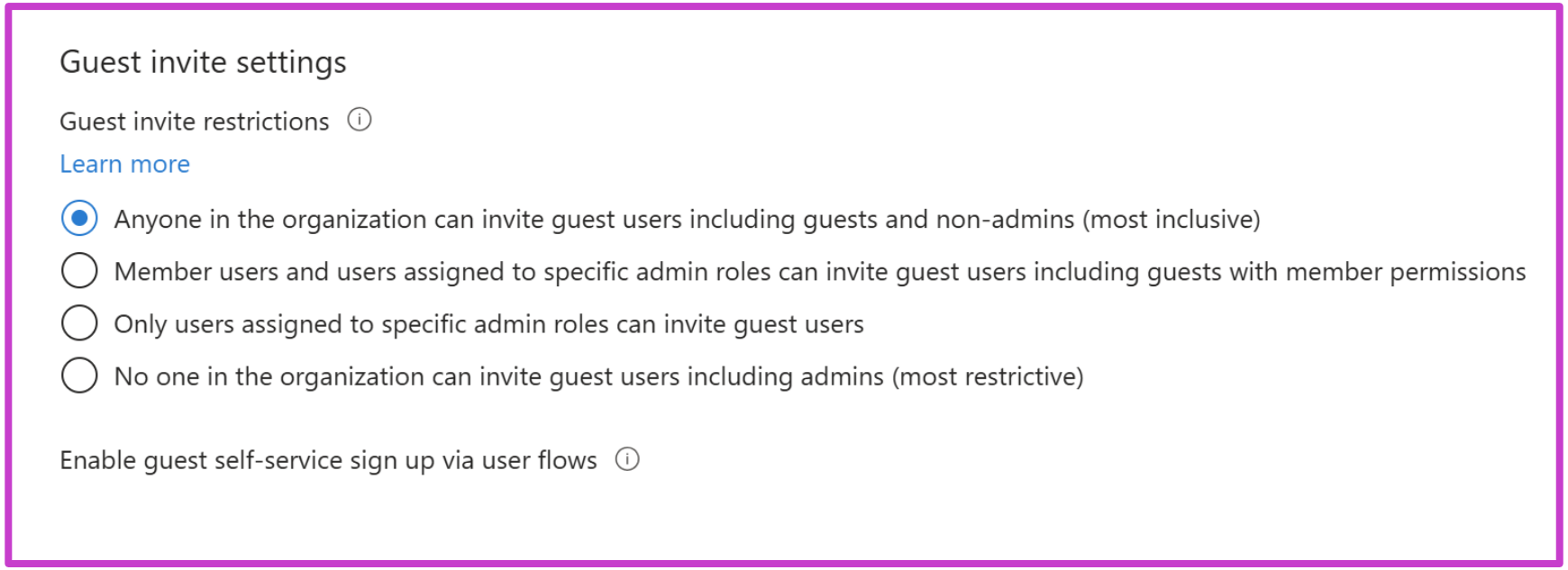
Collaborating with external users

- 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

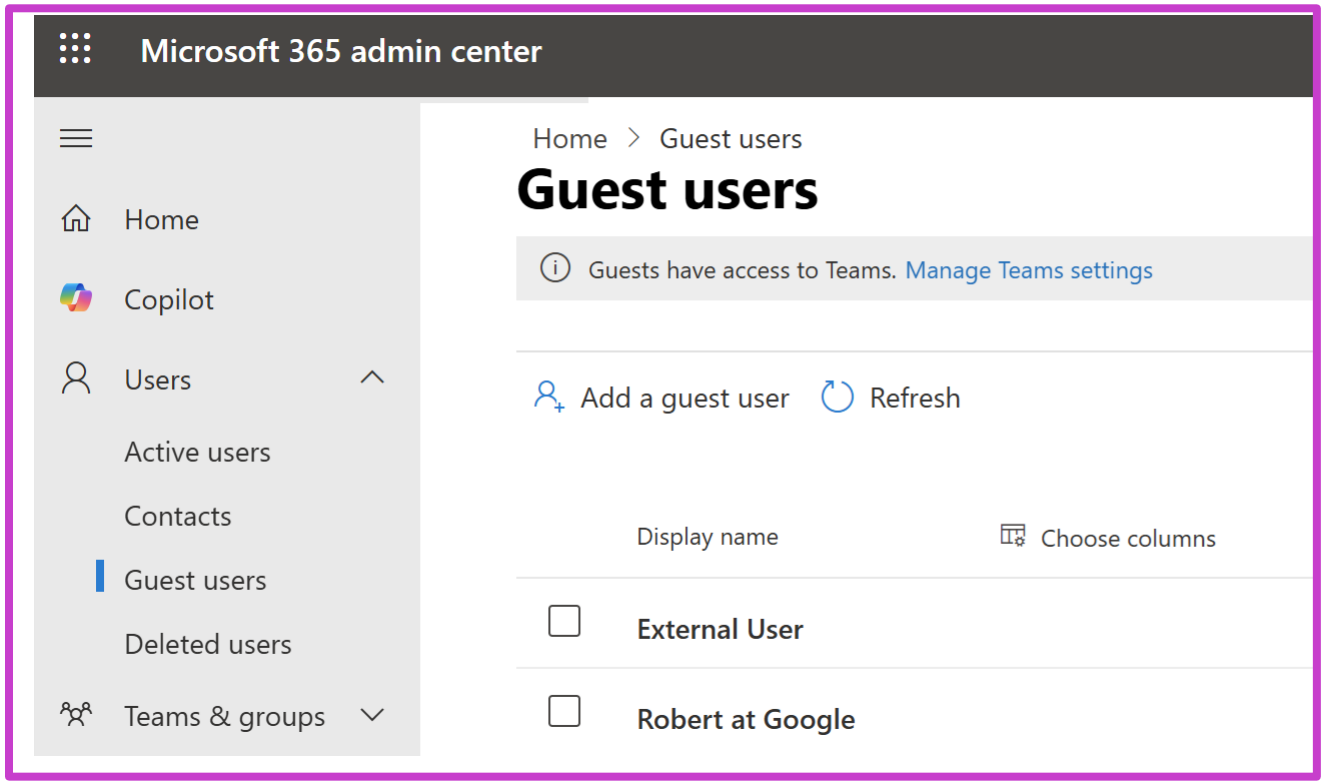
This exercise teaches students how to configure external collaboration settings.

[Launch this Exercise in GitHub]



External users from M365 workloads

Microsoft 365 admin center



Manage guest users in the Microsoft 365 admin center.

Similar process to Microsoft Entra ID.

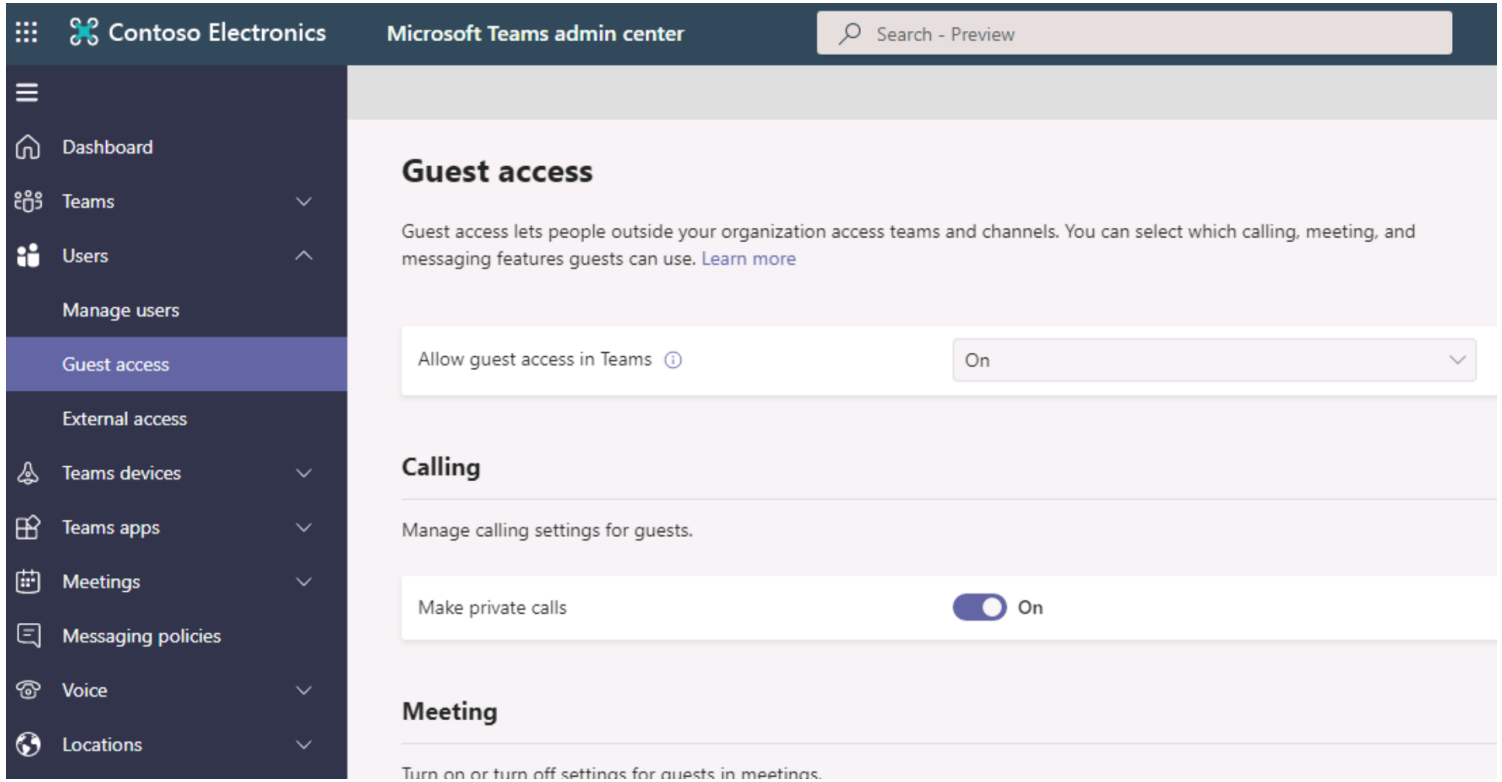
Always use Zero Trust principles when managing.

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



Invite external users—Individually or in bulk

Inviting users

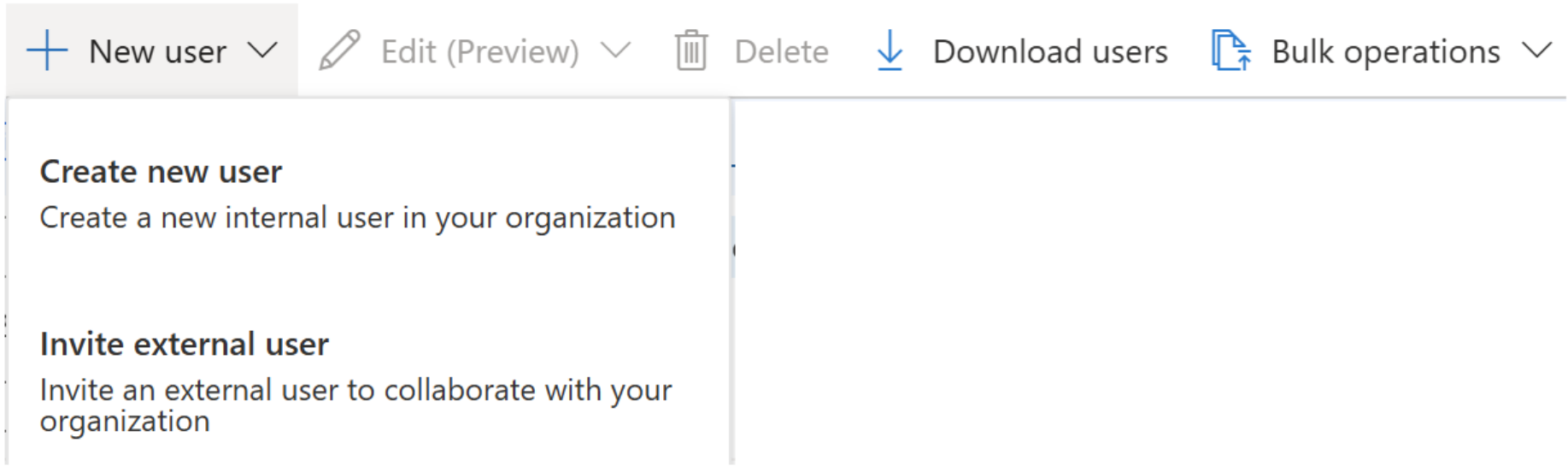
Inviting users individually:

- 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)



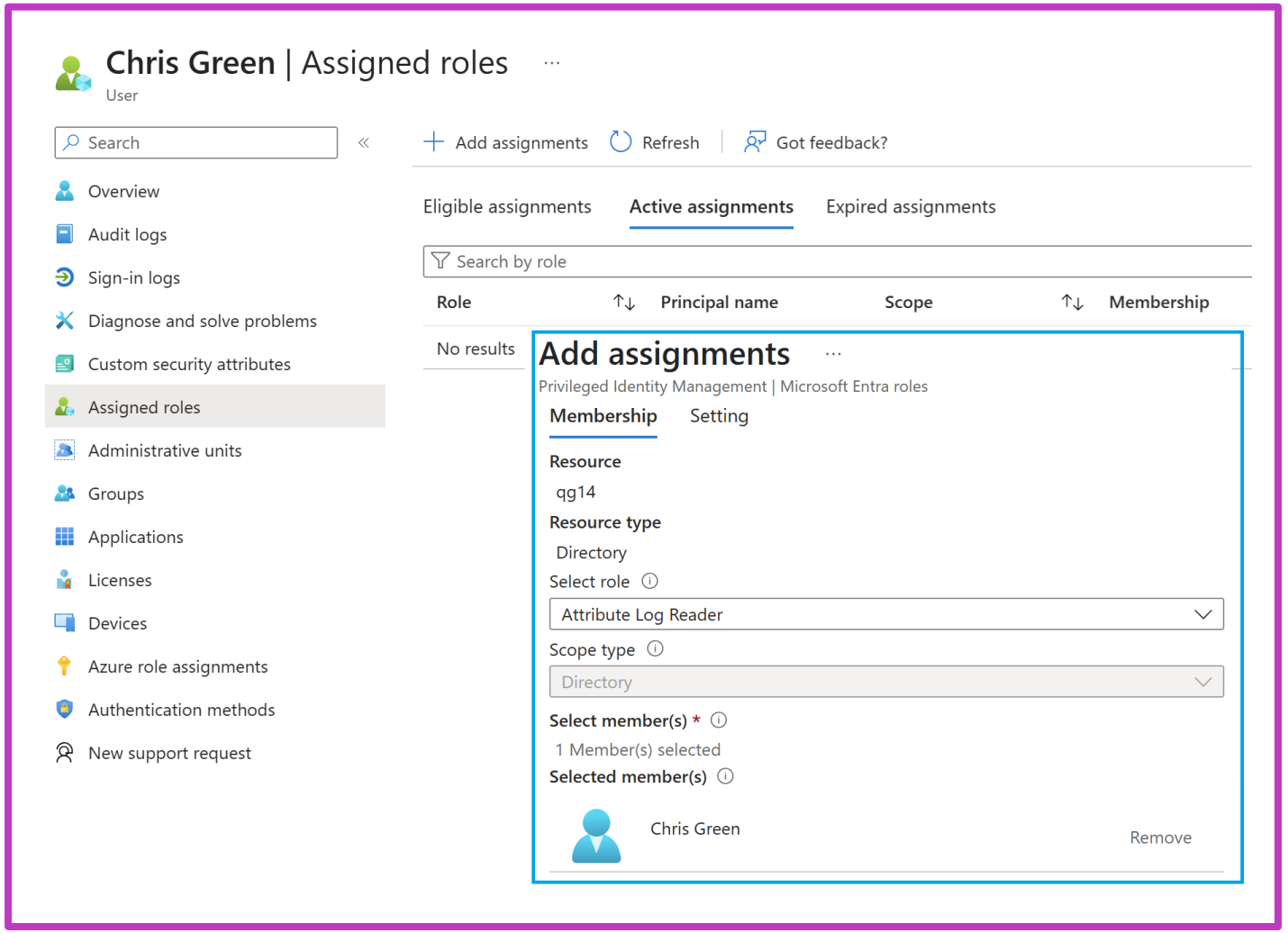
Manage external user accounts in Microsoft Entra ID

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.

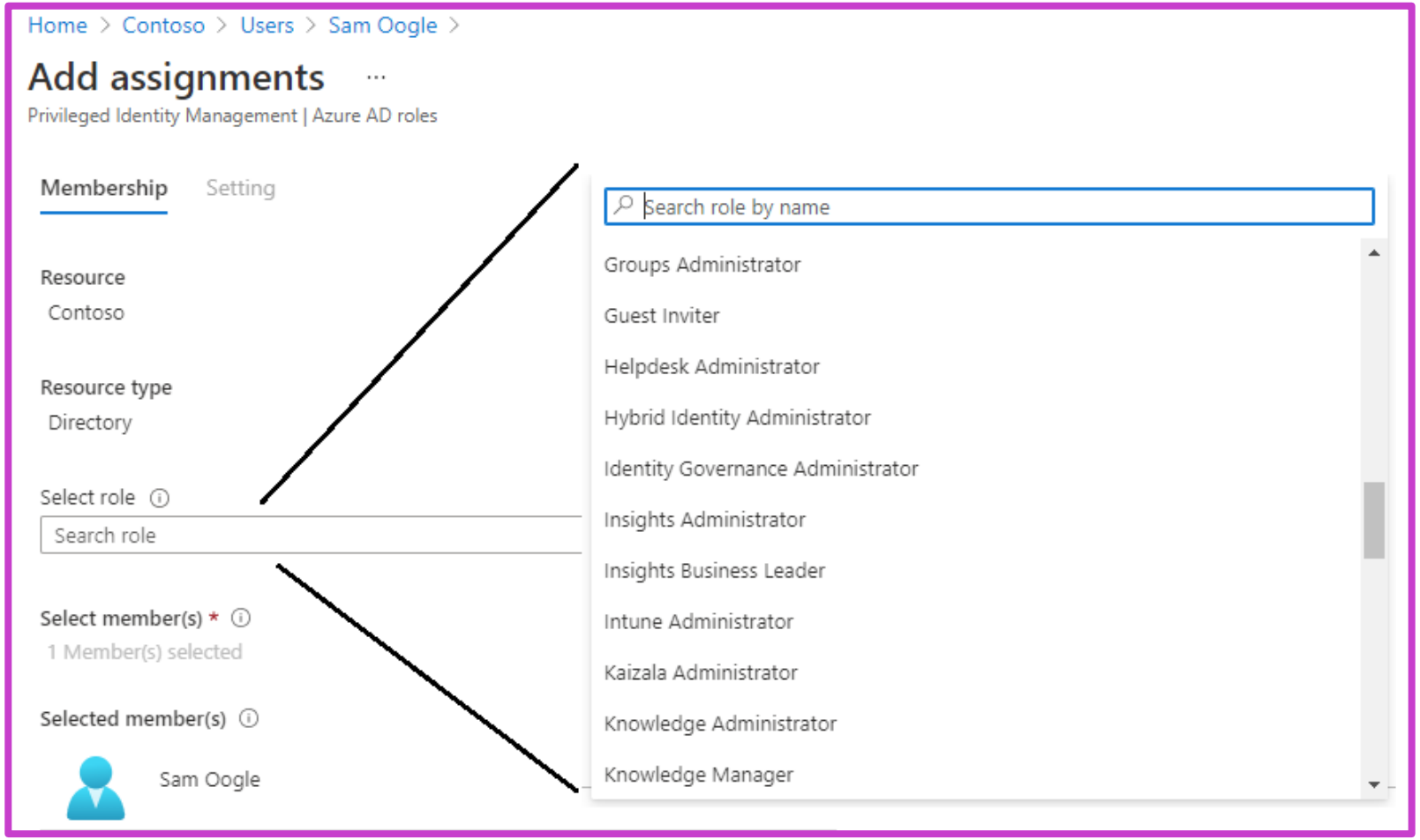


Provide the guest user the least privilege access needed

Add guest to:

- “Assign roles” just as with normal users.

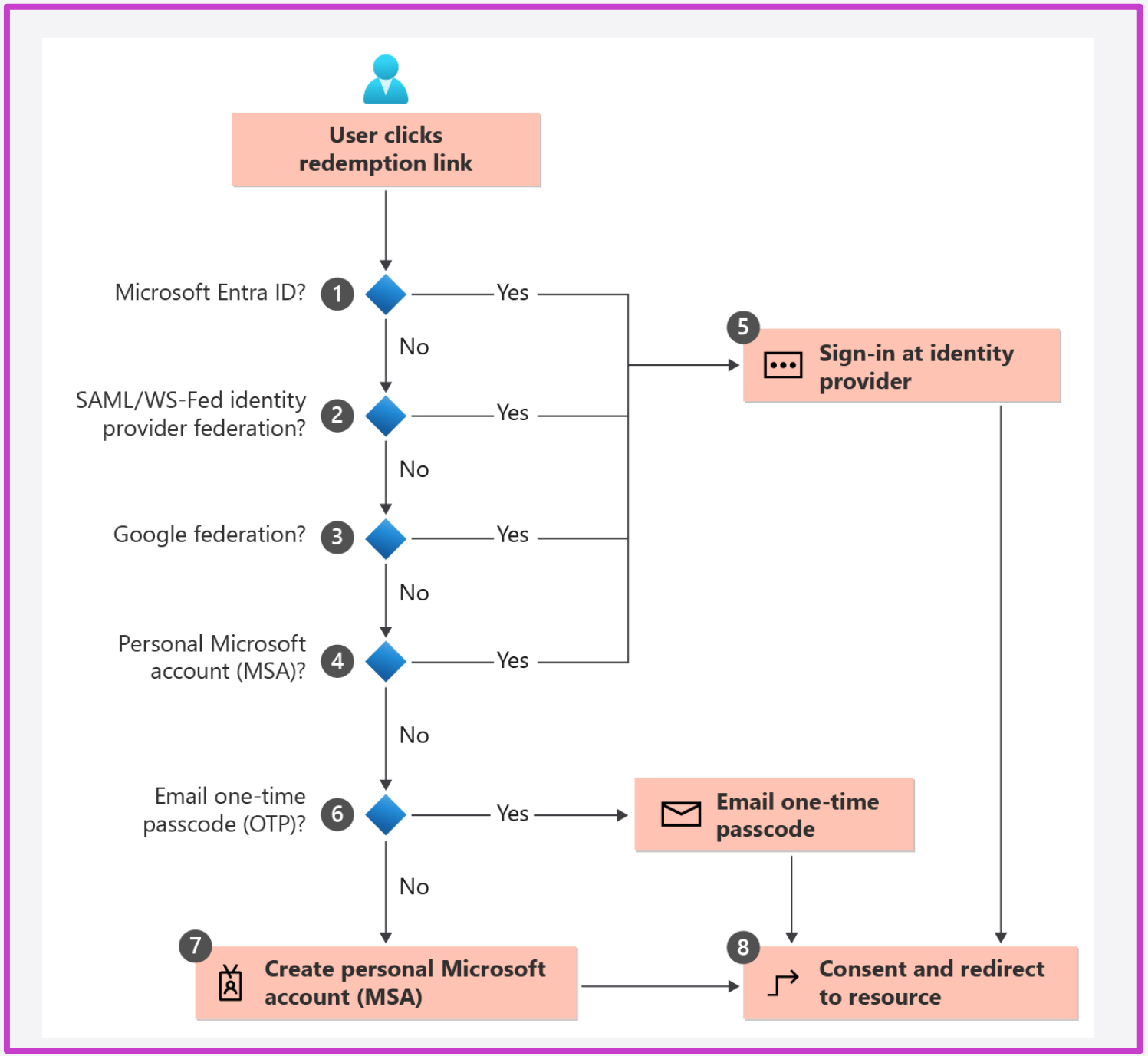
You can add Guests to groups as well.



B2B user redemption

External identity remediation types

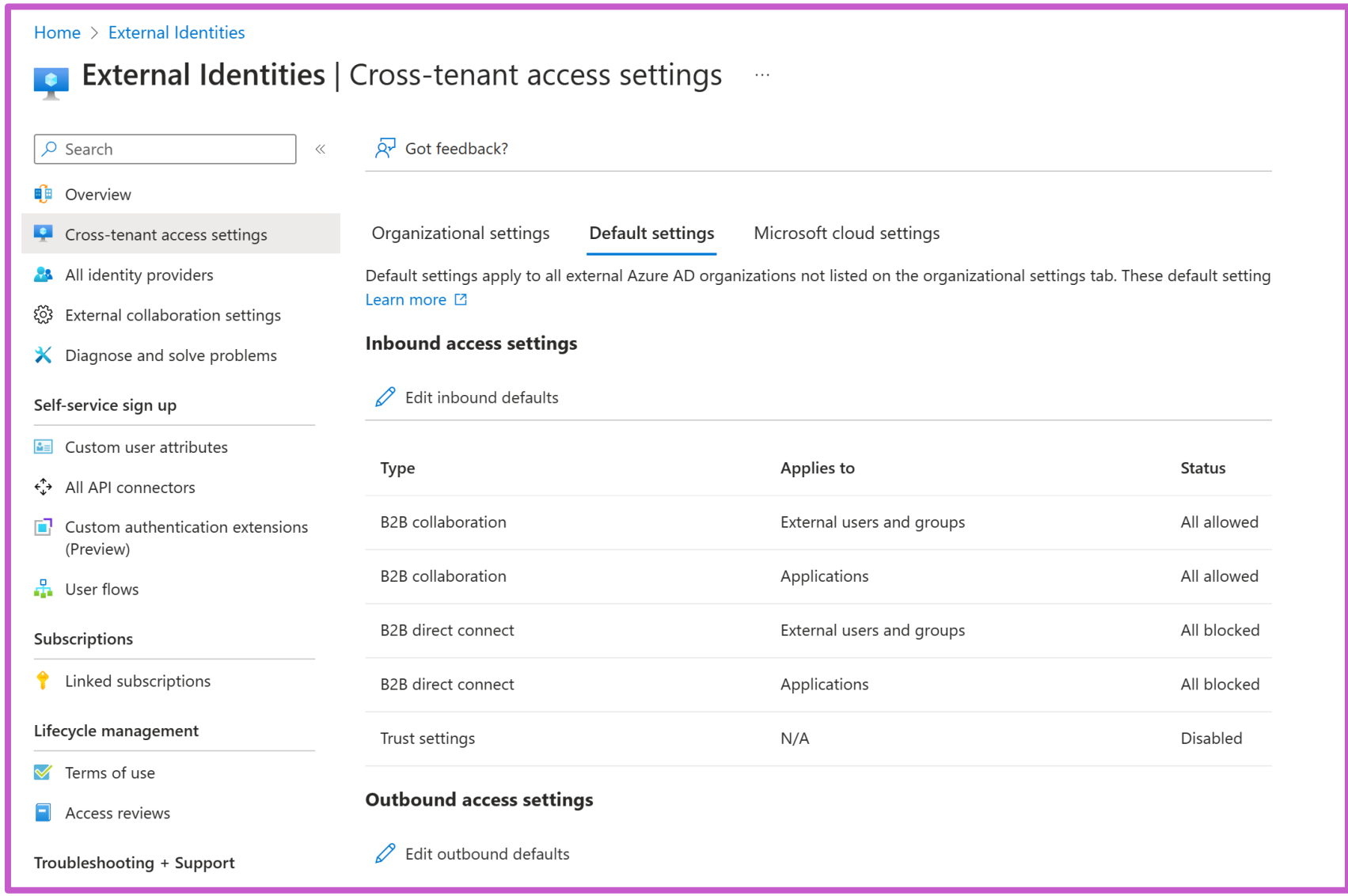
- Microsoft Entra ID native
- SAML / WS-Fed
- Google (other social media)
- Personal MSA
- One-time passcode



Cross-tenant access controls

Configure cross-tenant access controls

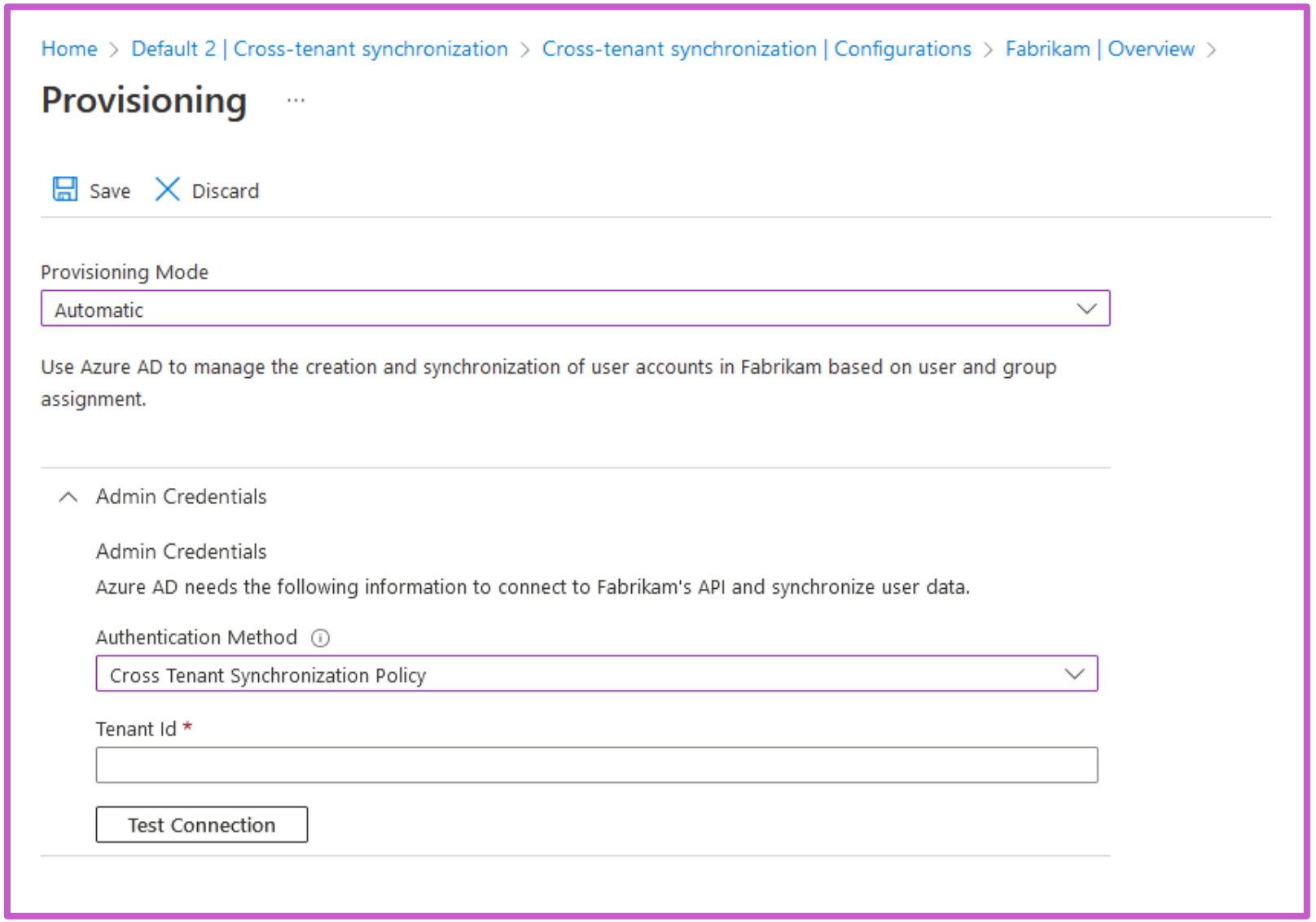
- Default—applied to all external collaboration.
- Organizational settings—add rules by specific tenant/tenant-id.
- Microsoft cloud—control access to Azure Government clouds.



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.

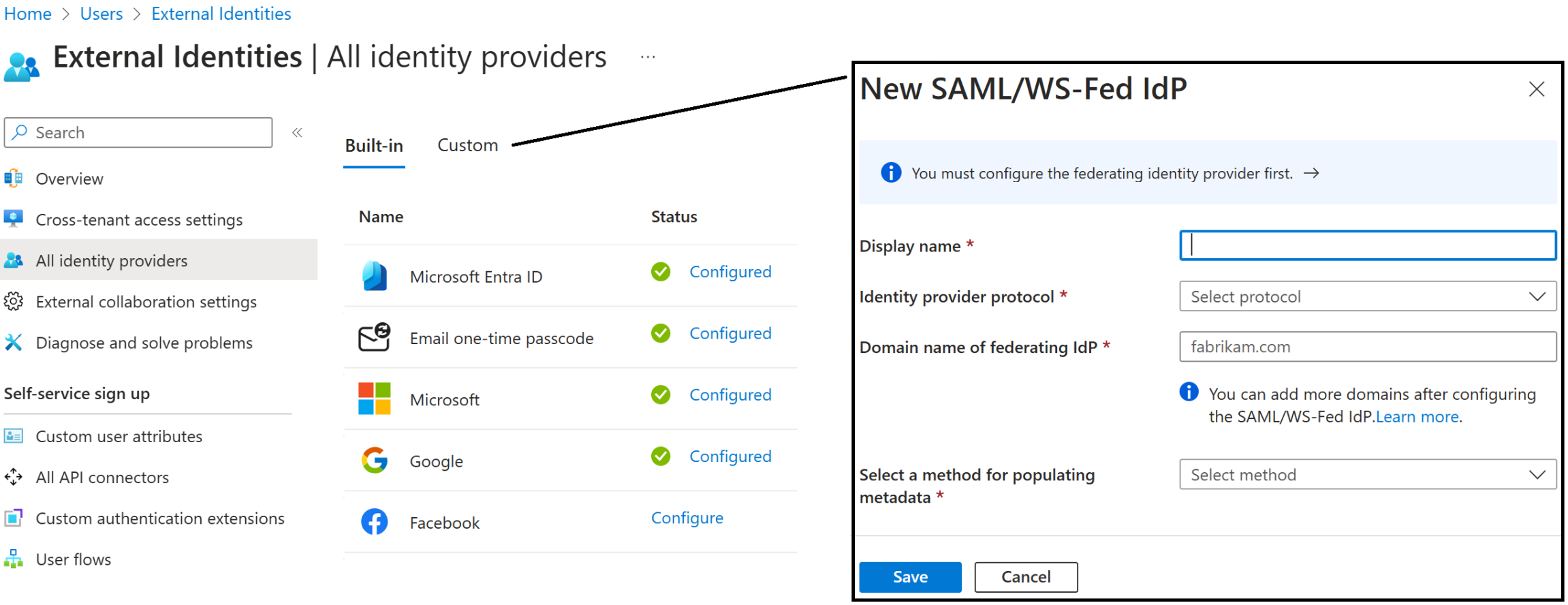


Configure identity providers

SAML/WS-Fed

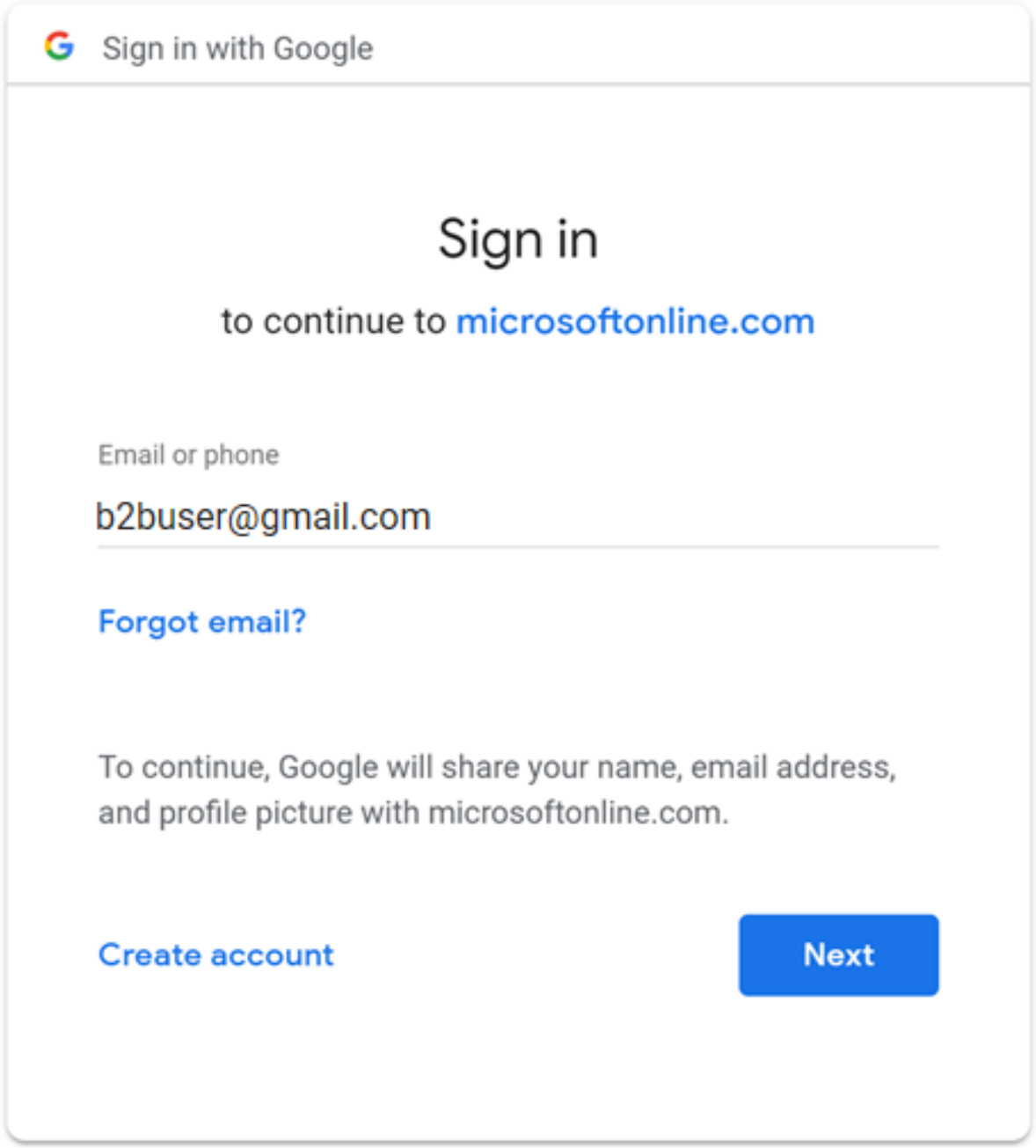
- You can set up direct federation with any organization that supports SAML 2.0 or WS-Fed
- Any new guests will be authenticated using direct federation
- External users sign in using their own organizational account

SAML/WS-Fed identity provider configuration



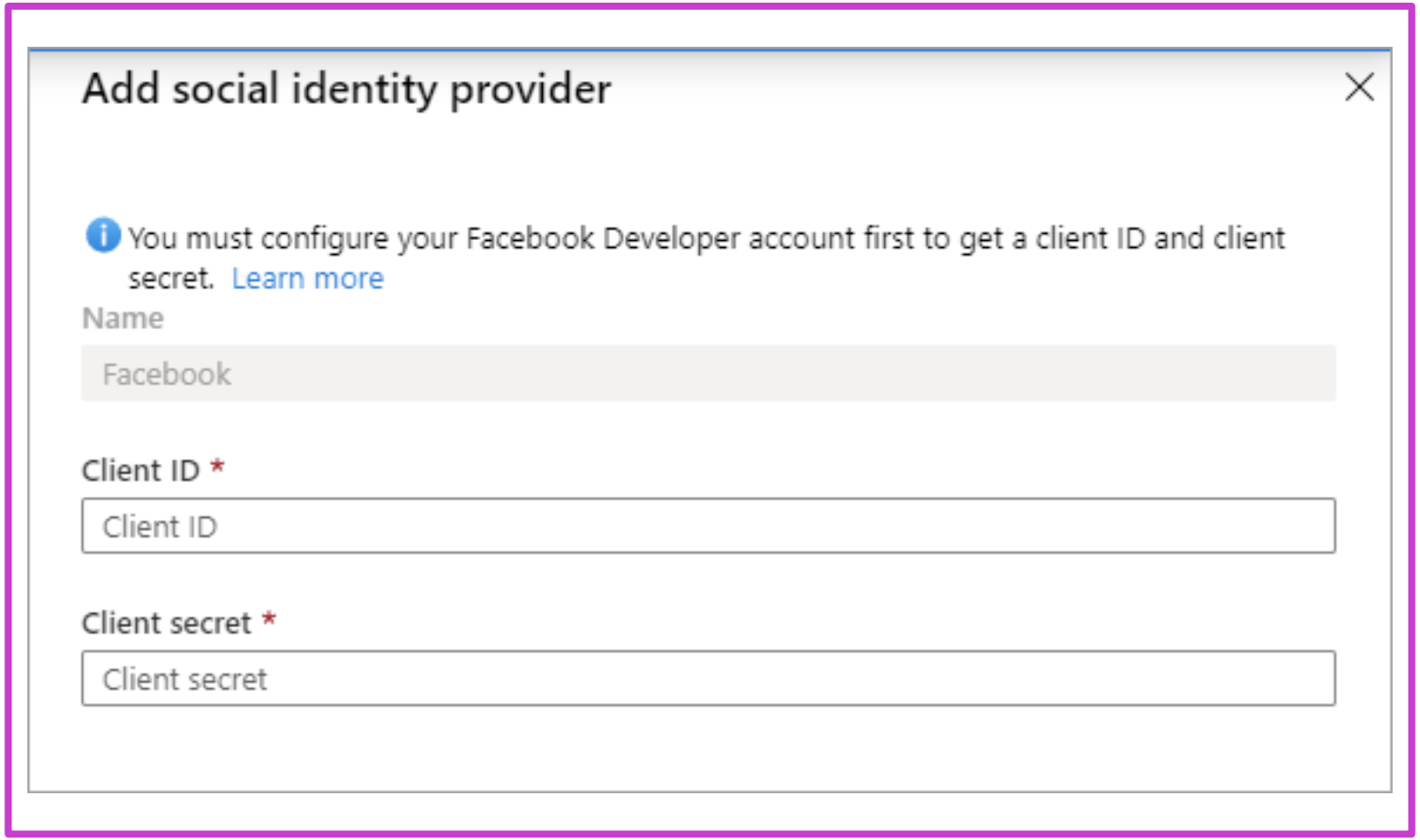
Using Google as an identity provider

- 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

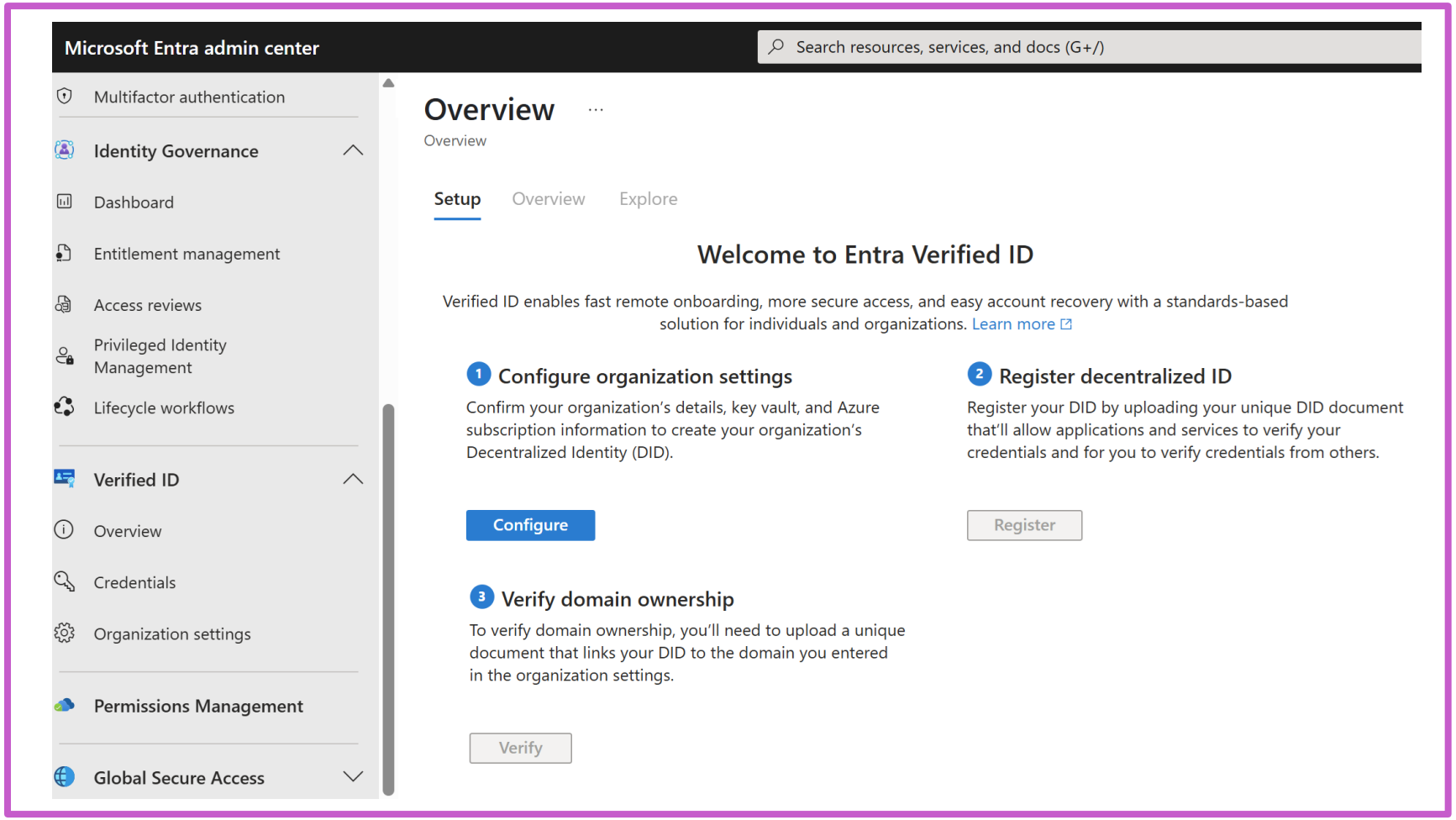


Verifiable credentials

Implement Microsoft Entra Verified ID

Requirements:

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



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

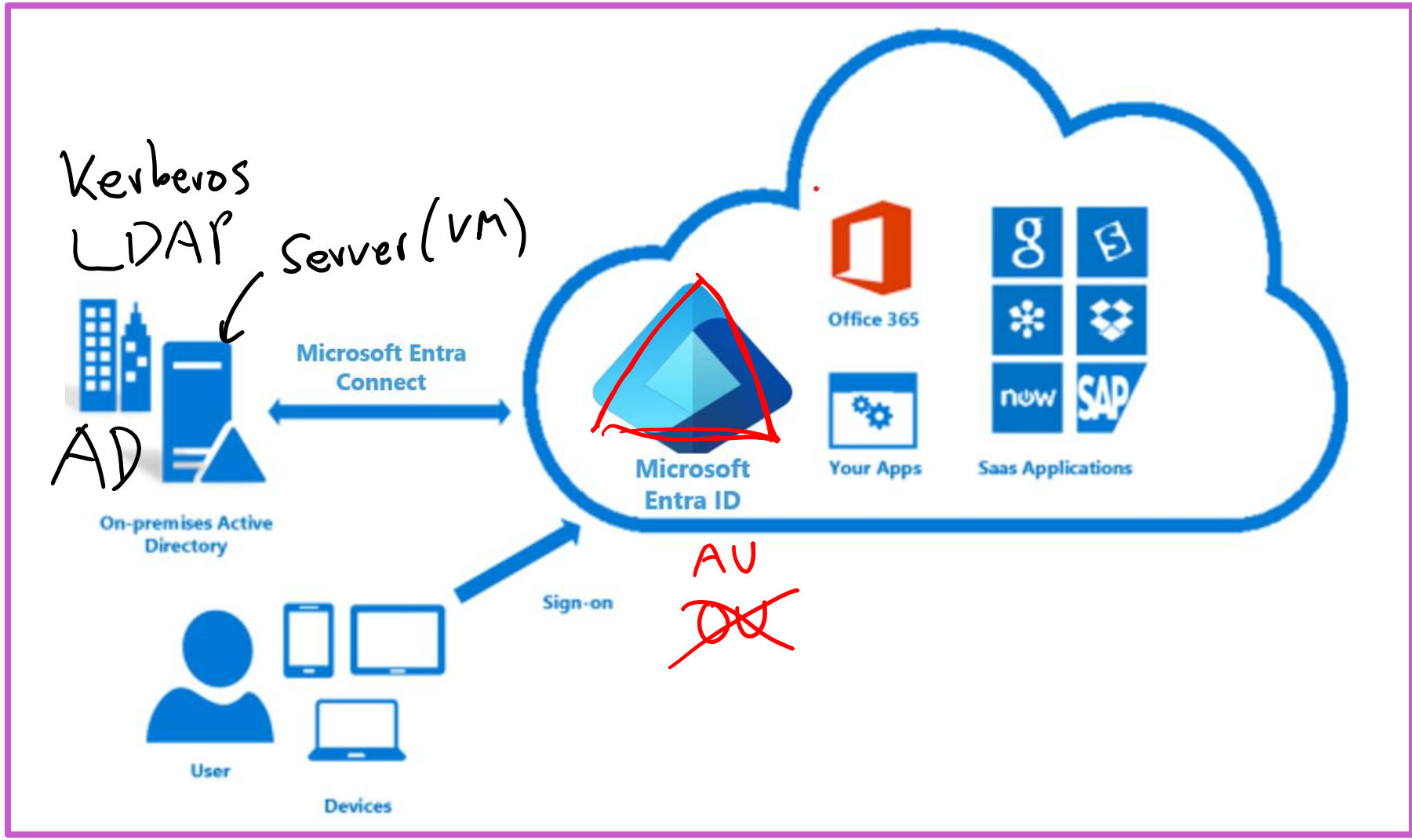
Objectives

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?

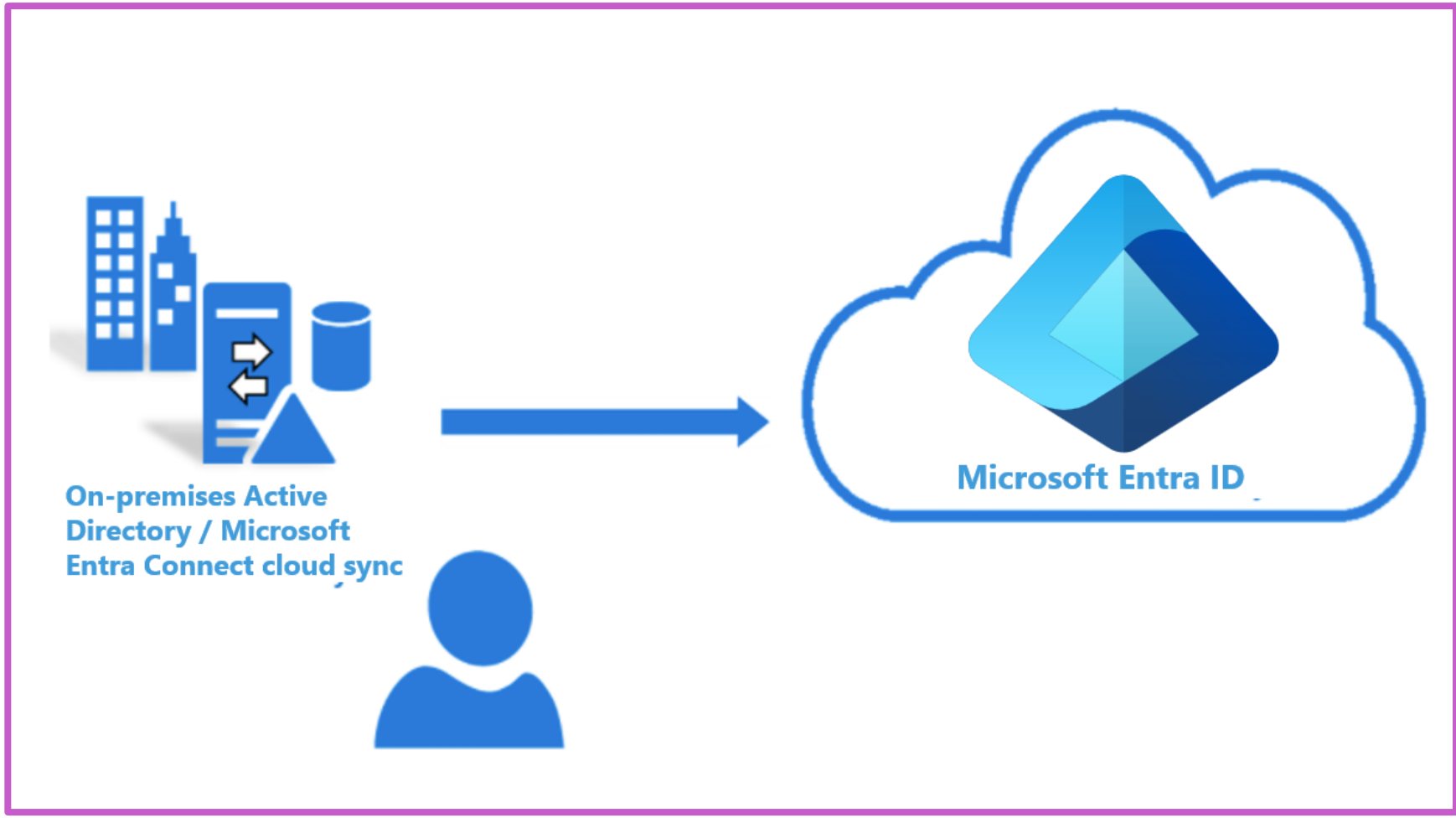
- Microsoft Entra Connect is a solution that bridges an organization's on-premises Active Directory with your cloud-based Microsoft Entra ID
- Microsoft Entra Connect provides:
  - Synchronization
  - Password hash synchronization
  - Pass-through authentication
  - Federation integration
  - Health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

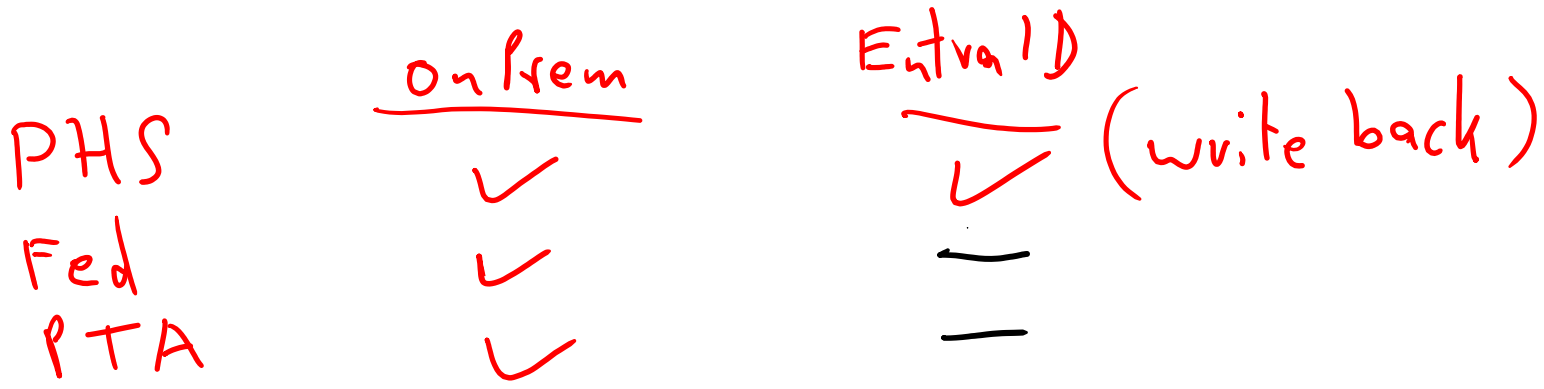
Microsoft Entra pass-through authentication (PTA)

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

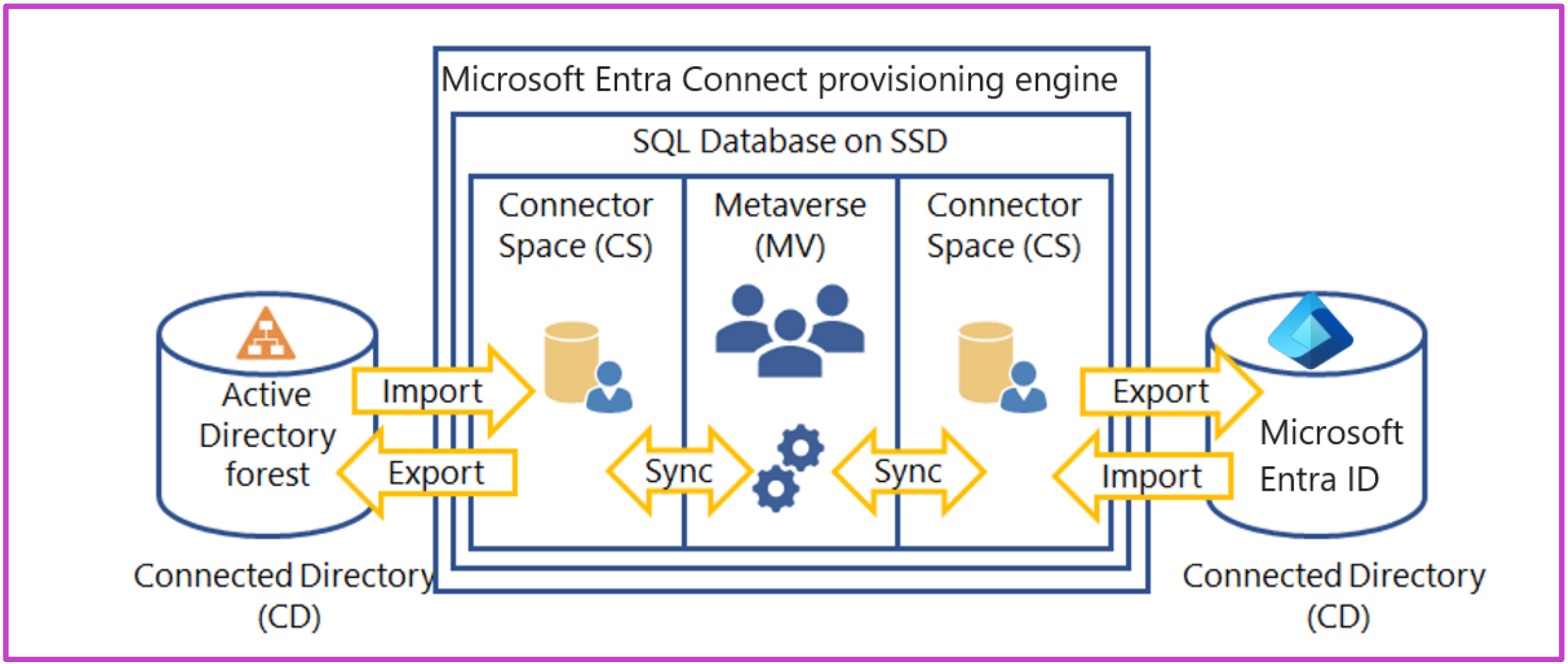
Federated authentication

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

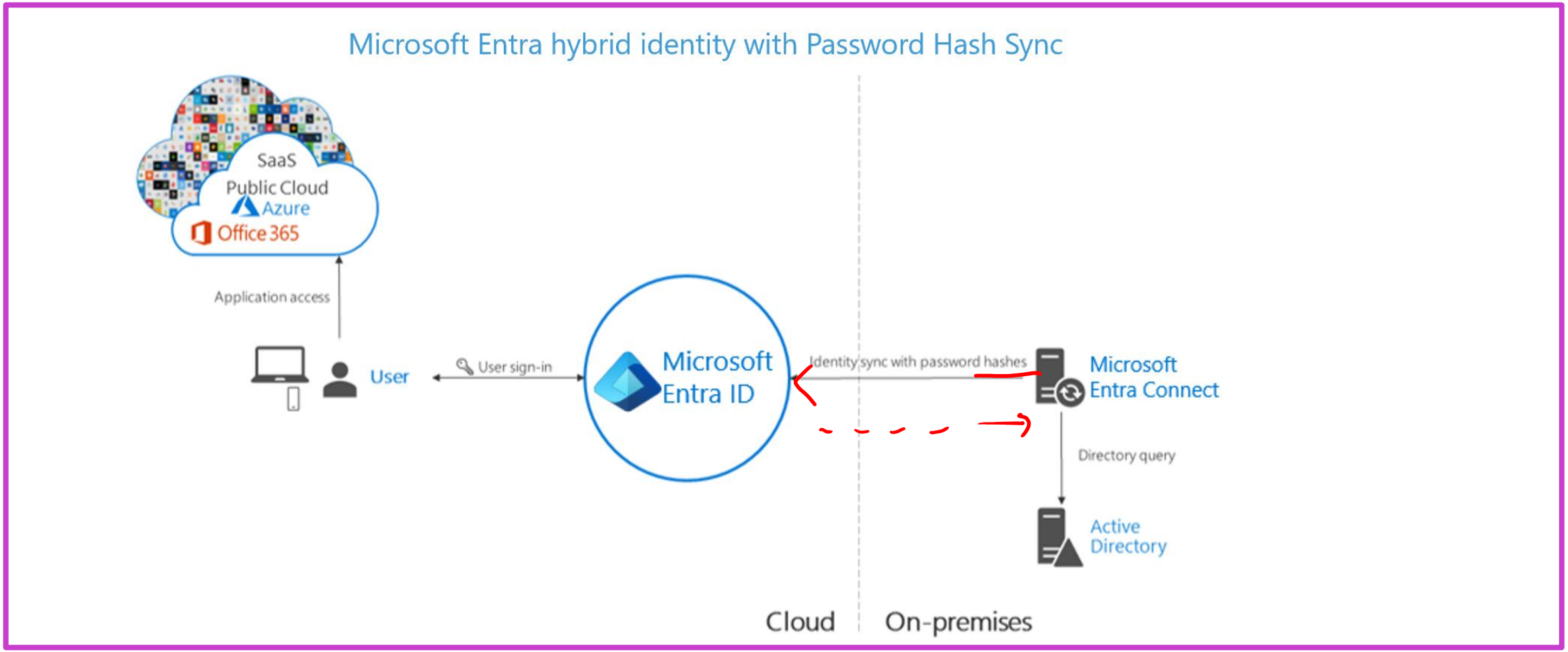


Microsoft Entra Connect component factors



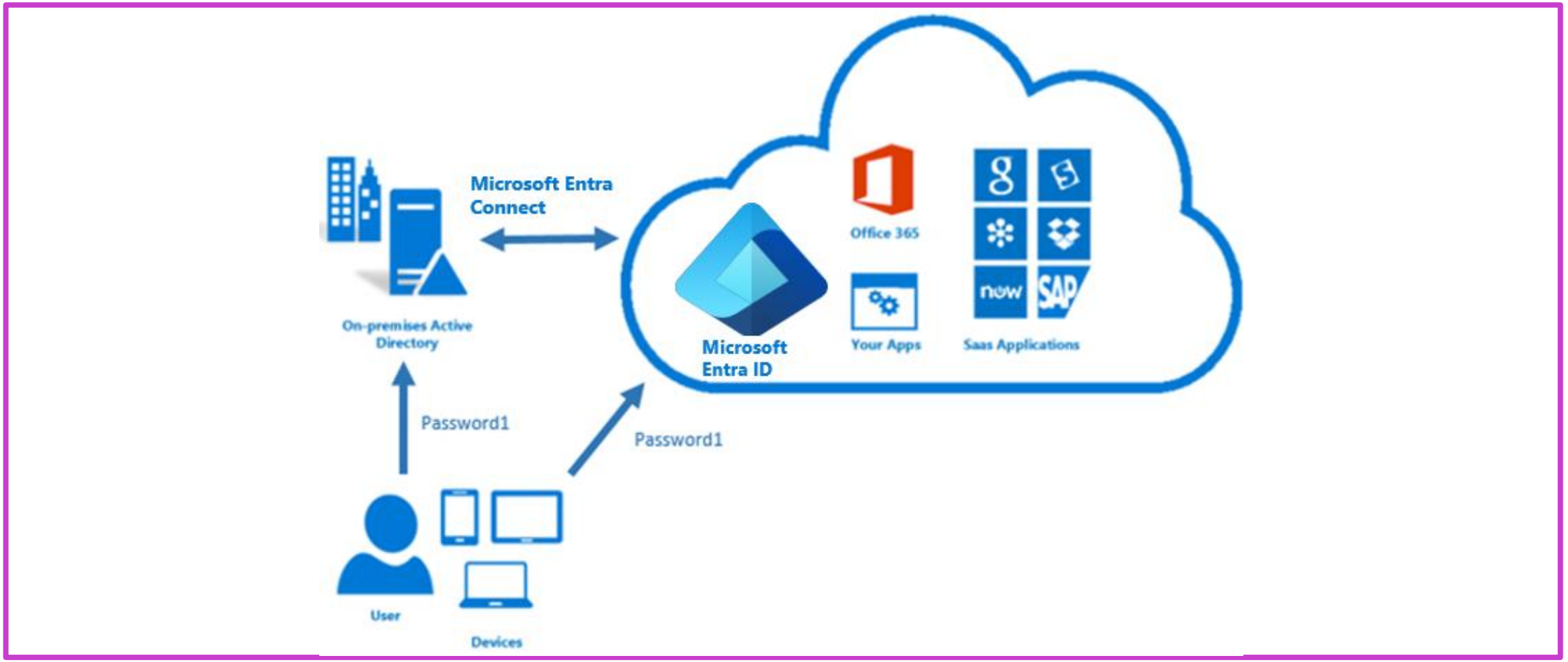
Implement and manage password hash synchronization (PHS)

Password hash sync

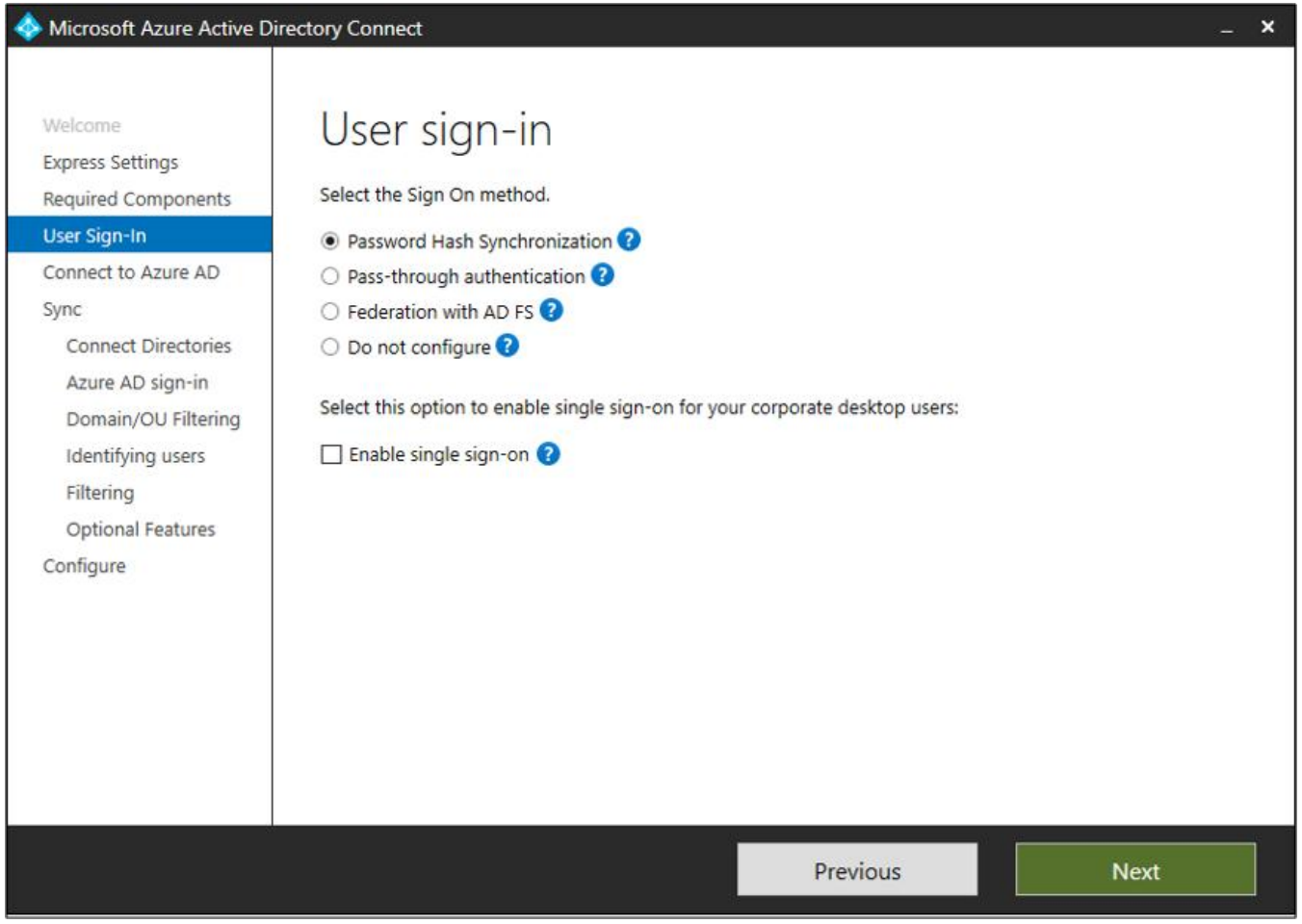


Simplicity of a password hash synchronization solution

How password hash synchronization works

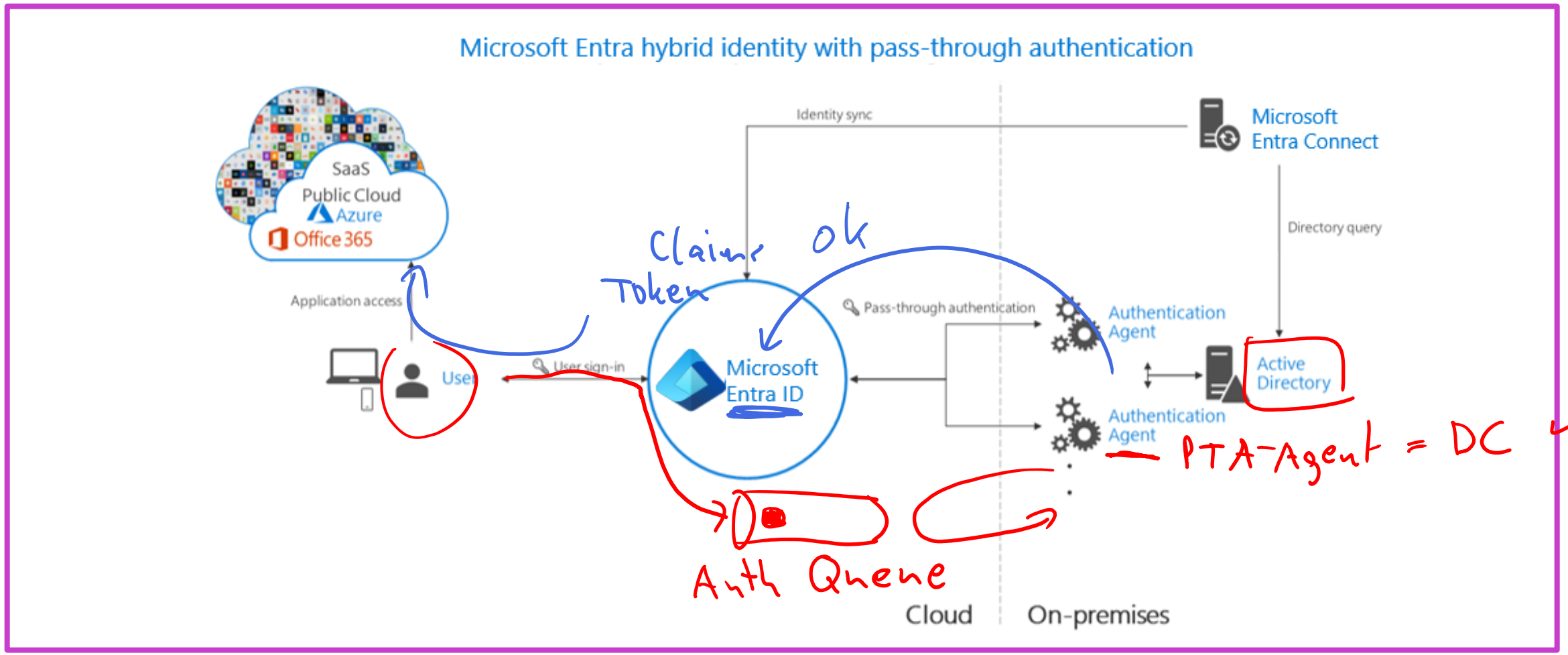


Enable password hash synchronization



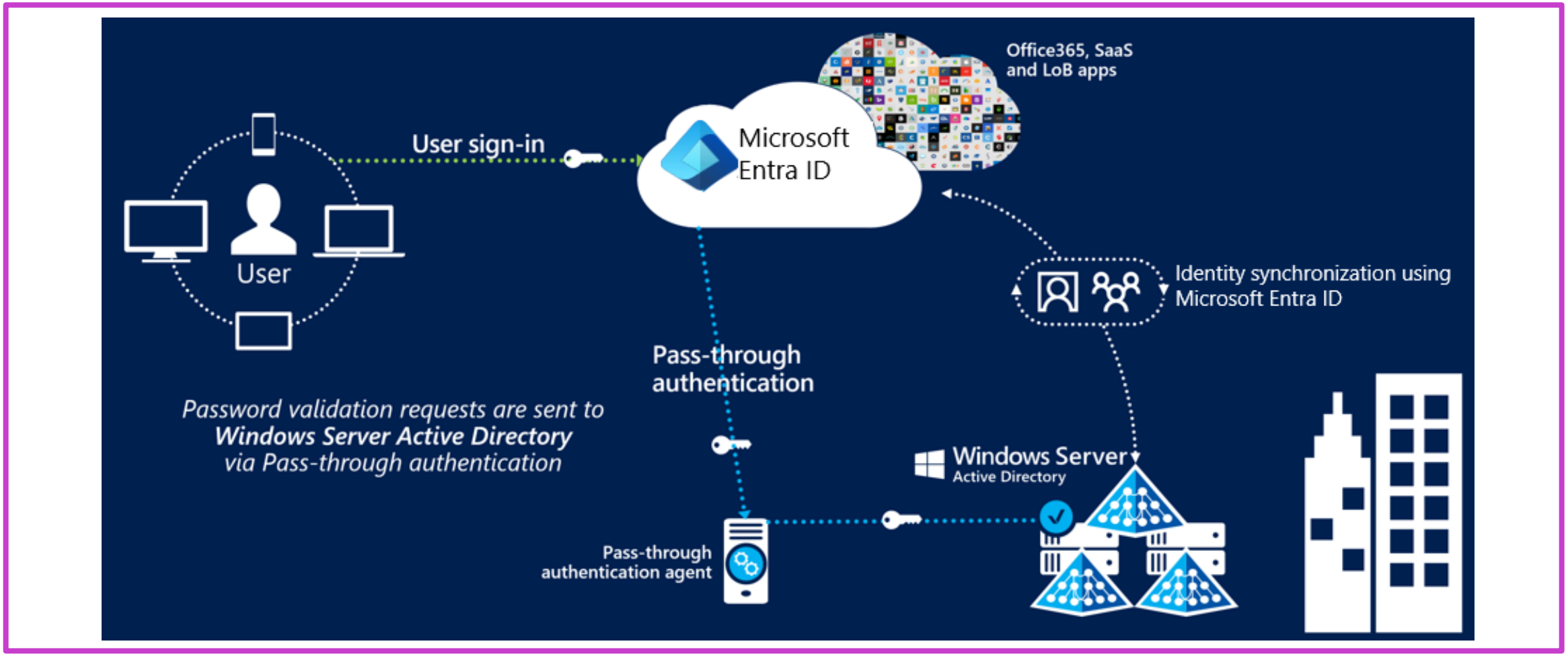
Implement and manage pass-through authentication (PTA)

Pass-through authentication

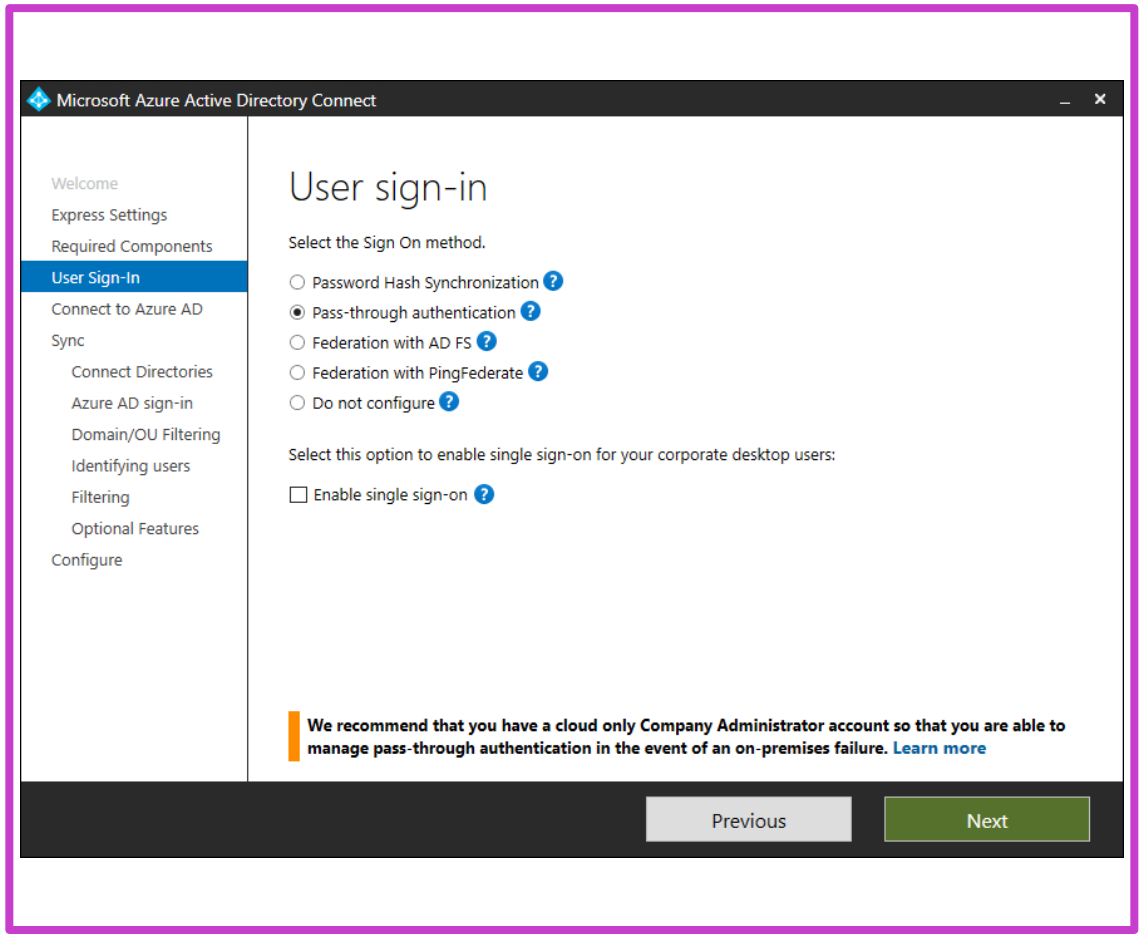


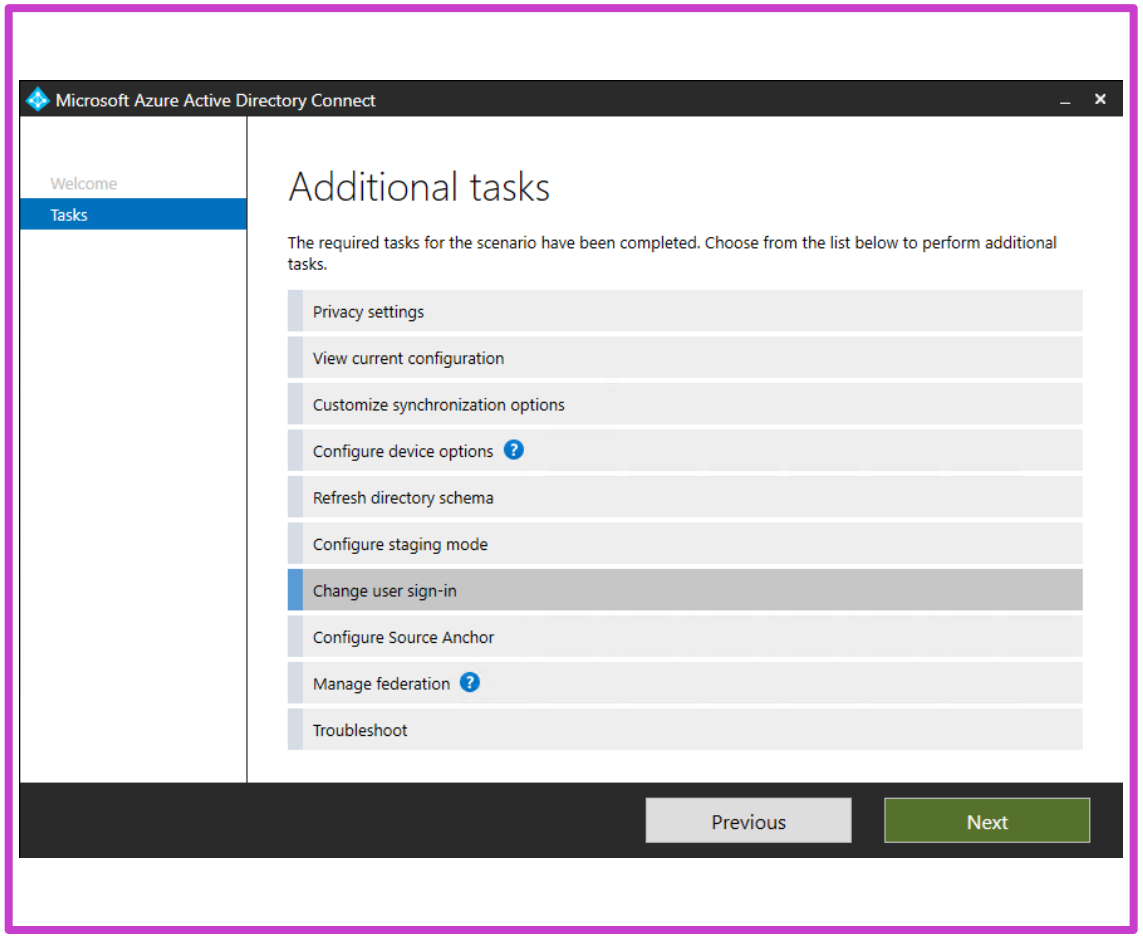
Agent requirements of pass-through authentication, using two agents for redundancy

How Microsoft Entra pass-through authentication works



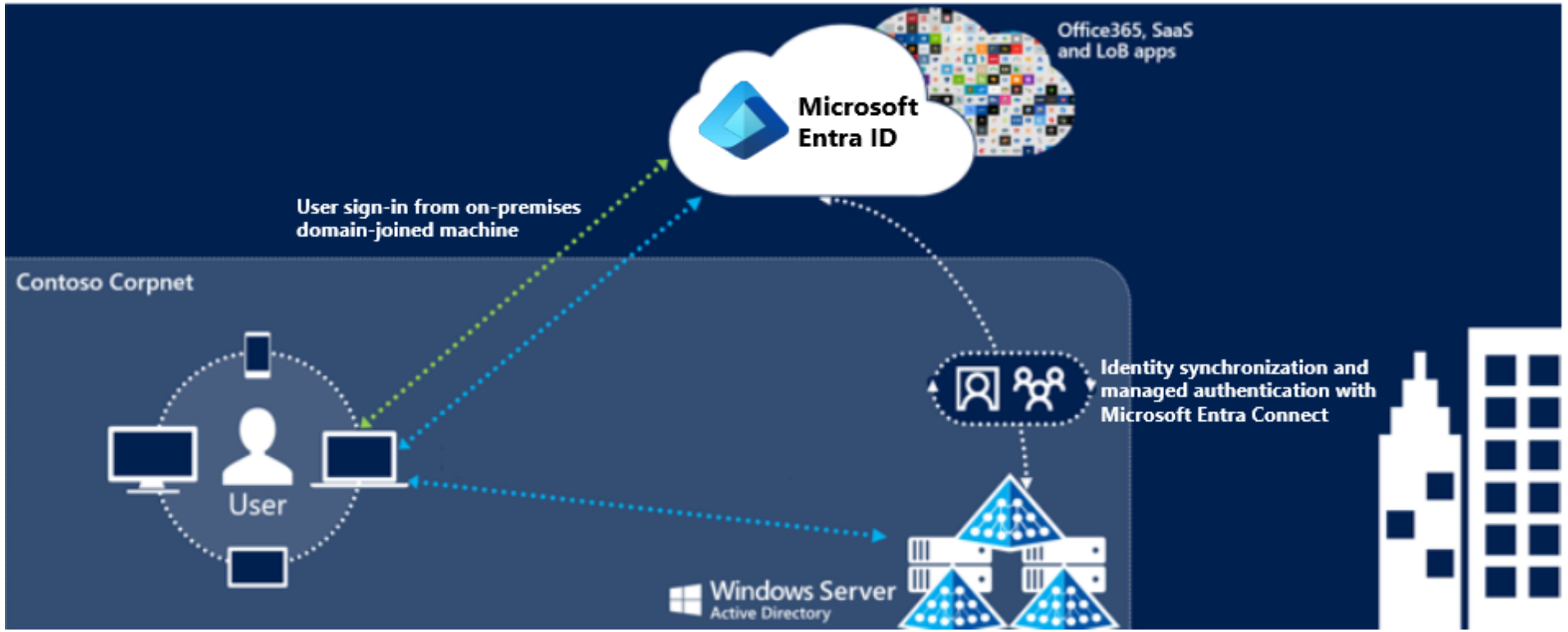
Enable pass-through authentication





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.

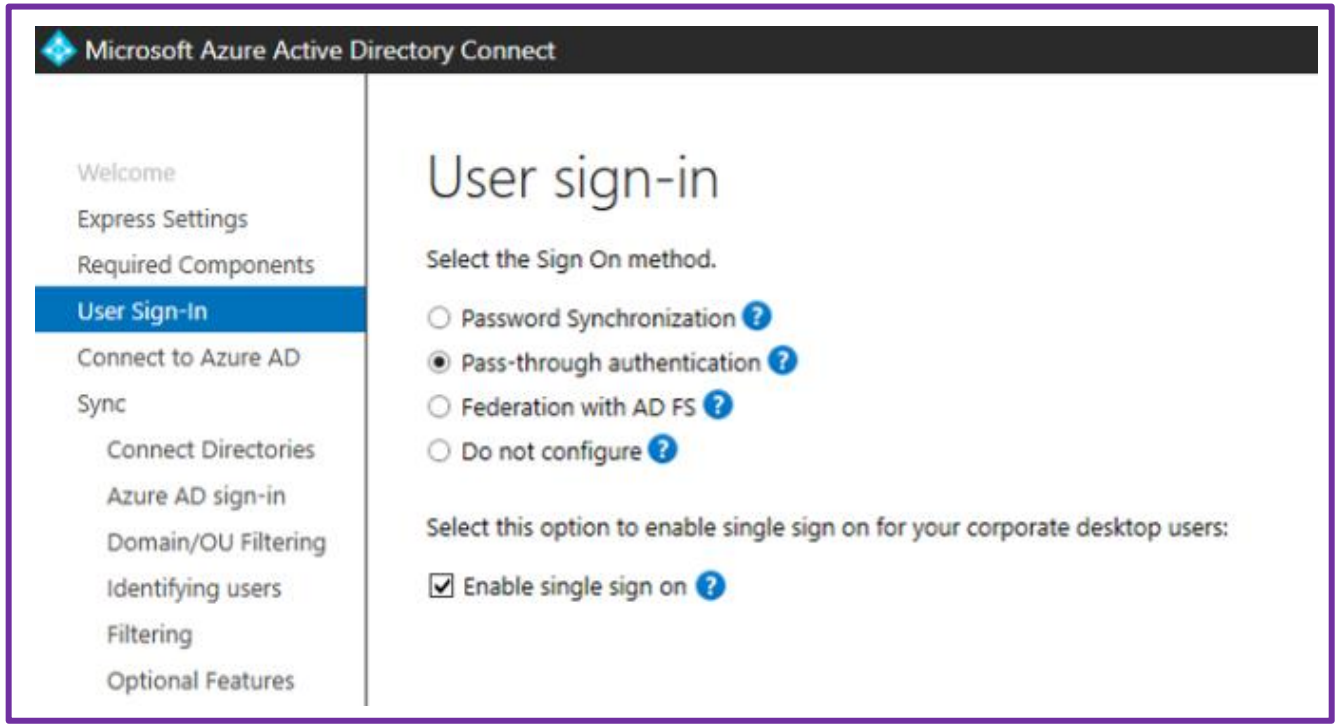
Sign out works, but releases the sign-in so all further access is blocked until sign-in is completed again.

Supported in browser-based and Office-based clients.

How seamless SSO is set up

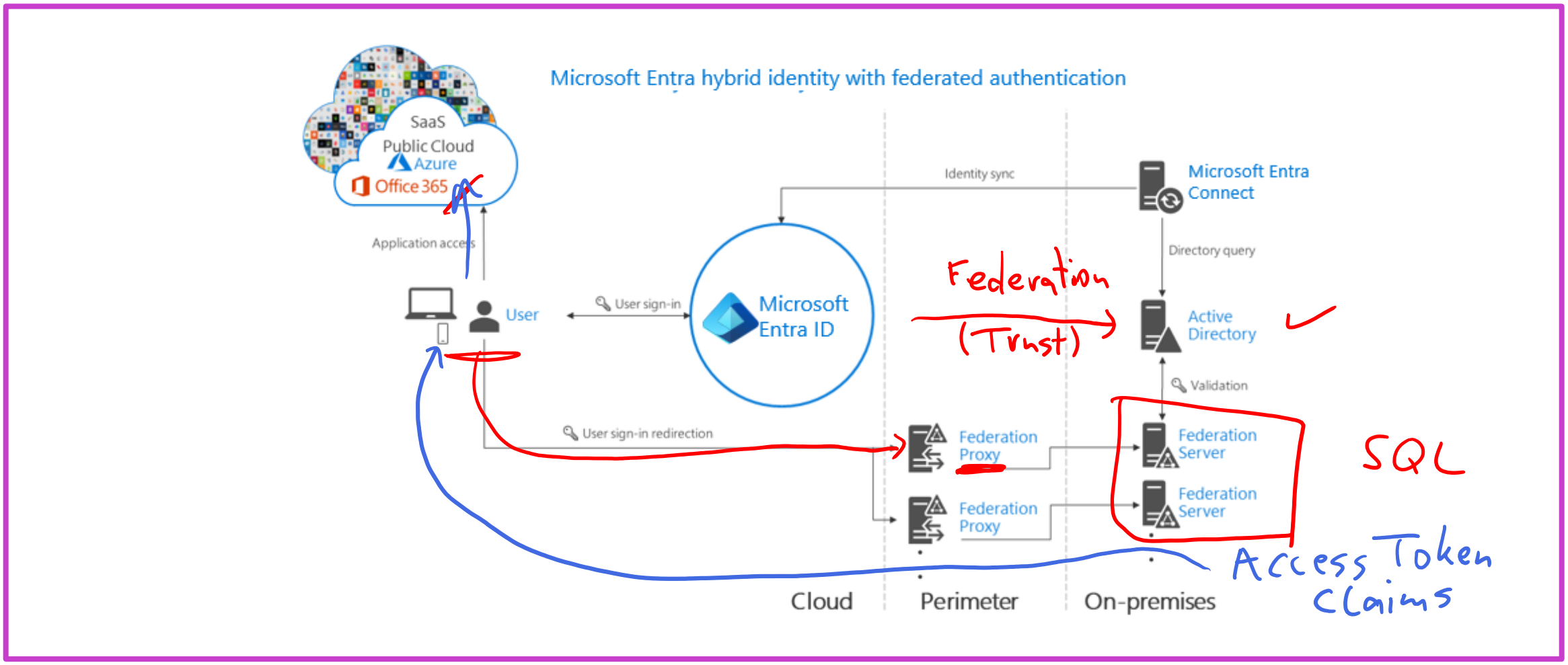
Seamless SSO is enabled using Microsoft Entra Connect. While enabling the SSO, the following steps occur:

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

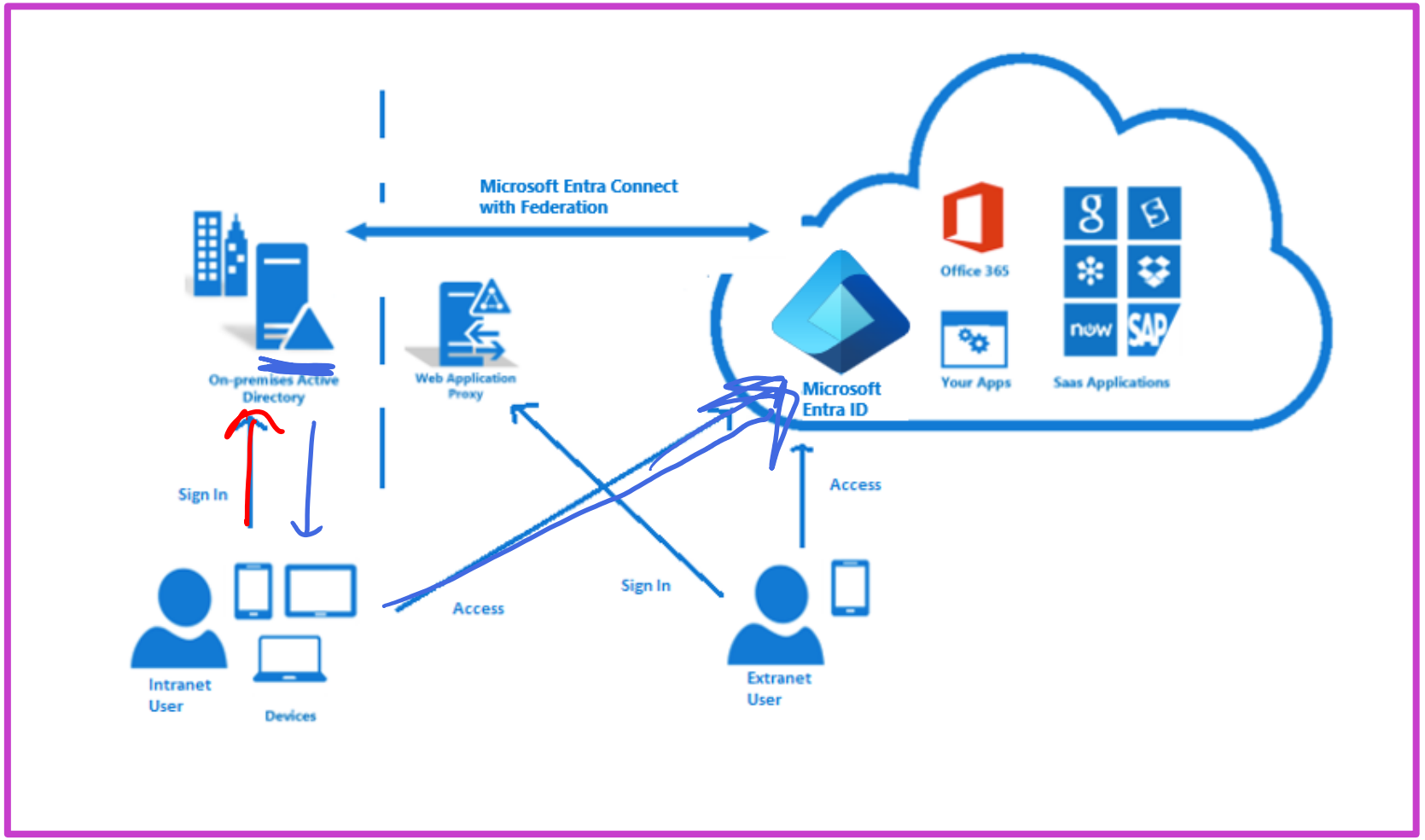


Components required for federation in the perimeter and internal network of your organization

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

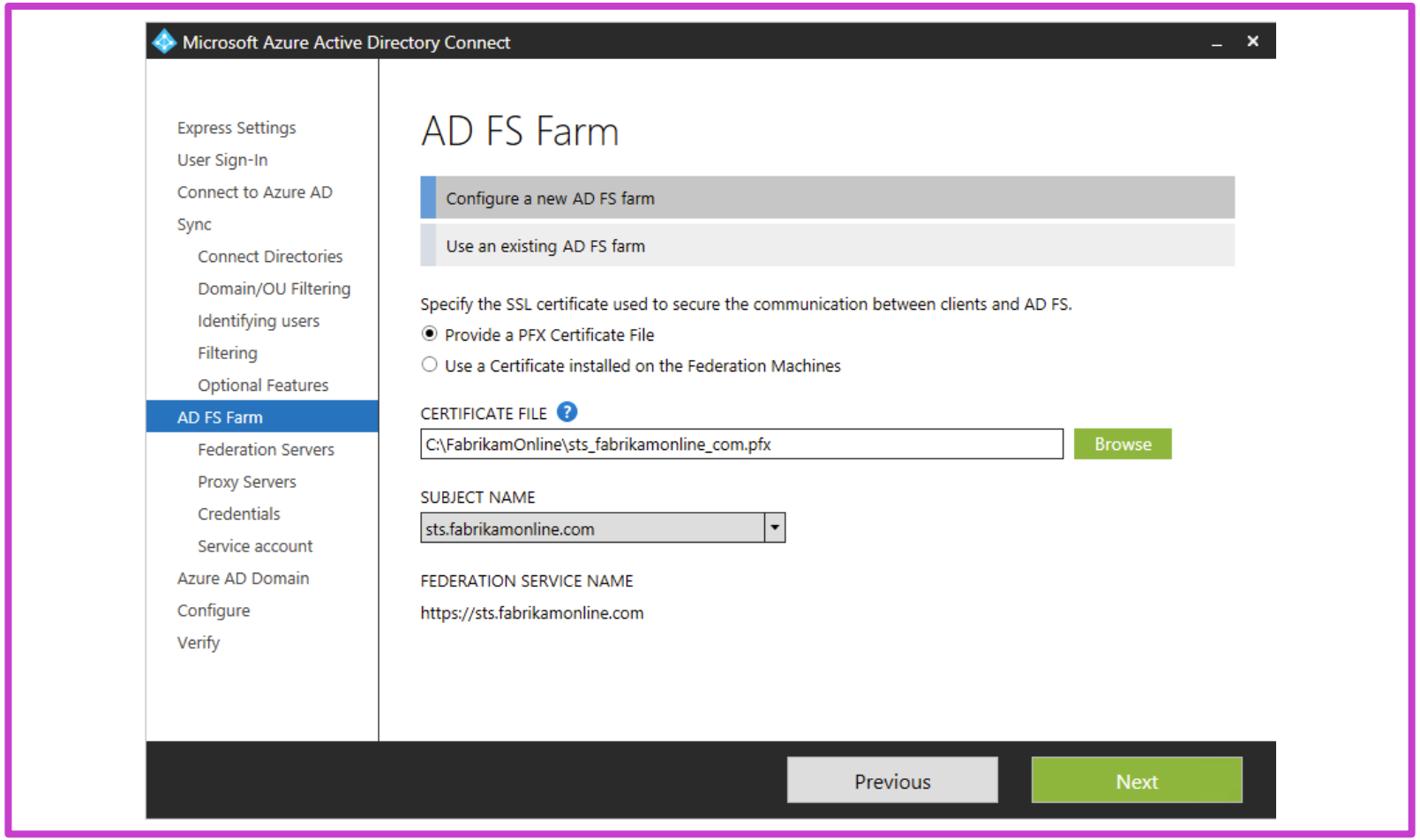
To deploy an AD FS farm, you need:

- 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



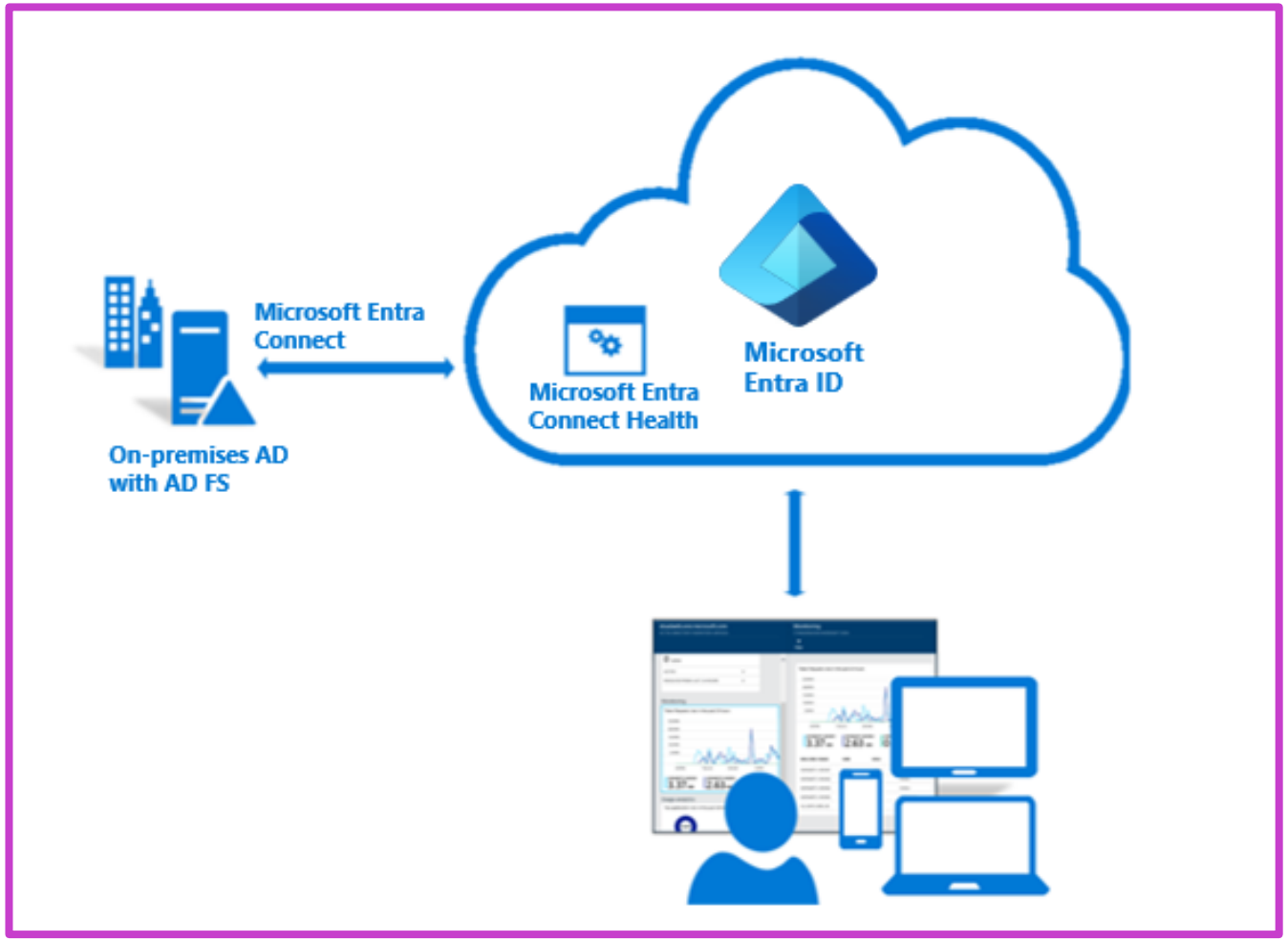
Managing federation with Microsoft Entra Connect

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

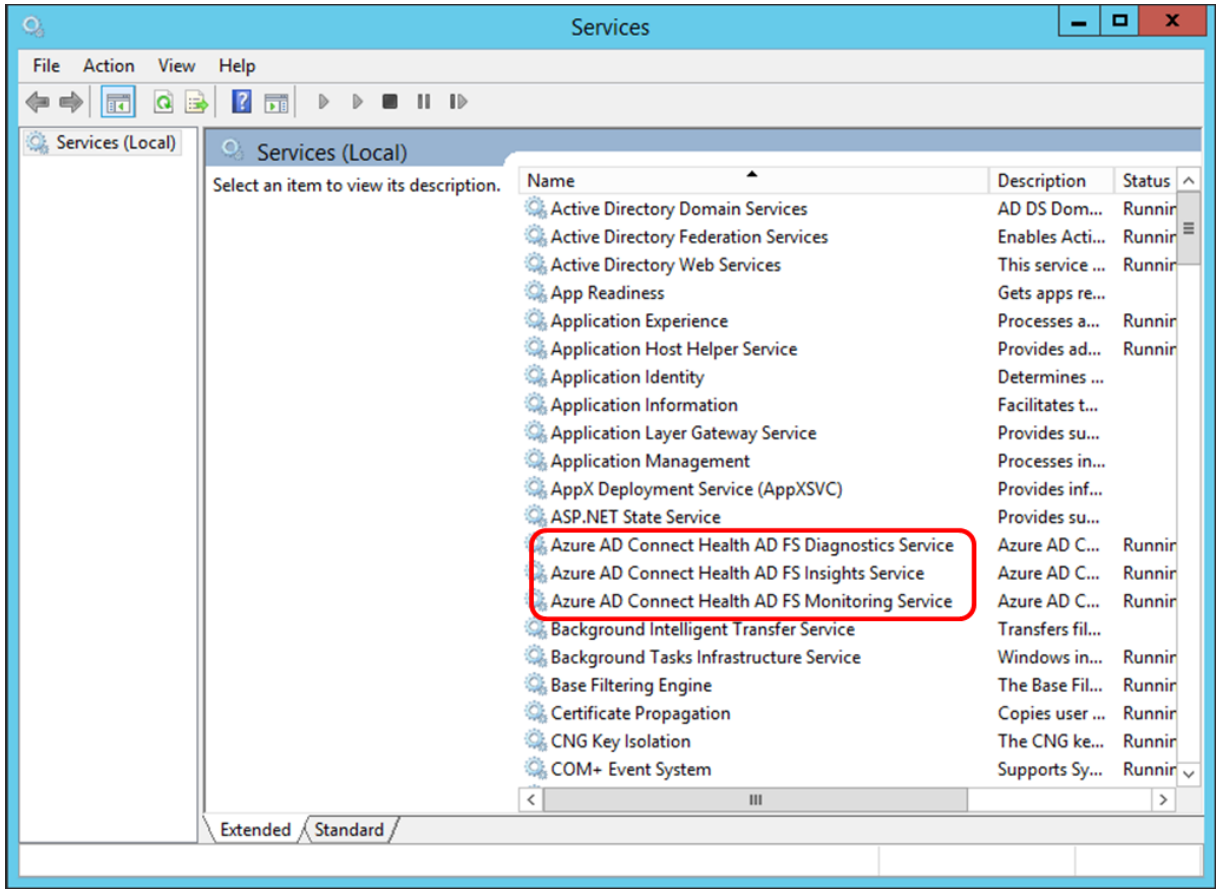


Considerations for installing Microsoft Entra Connect Health

- 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

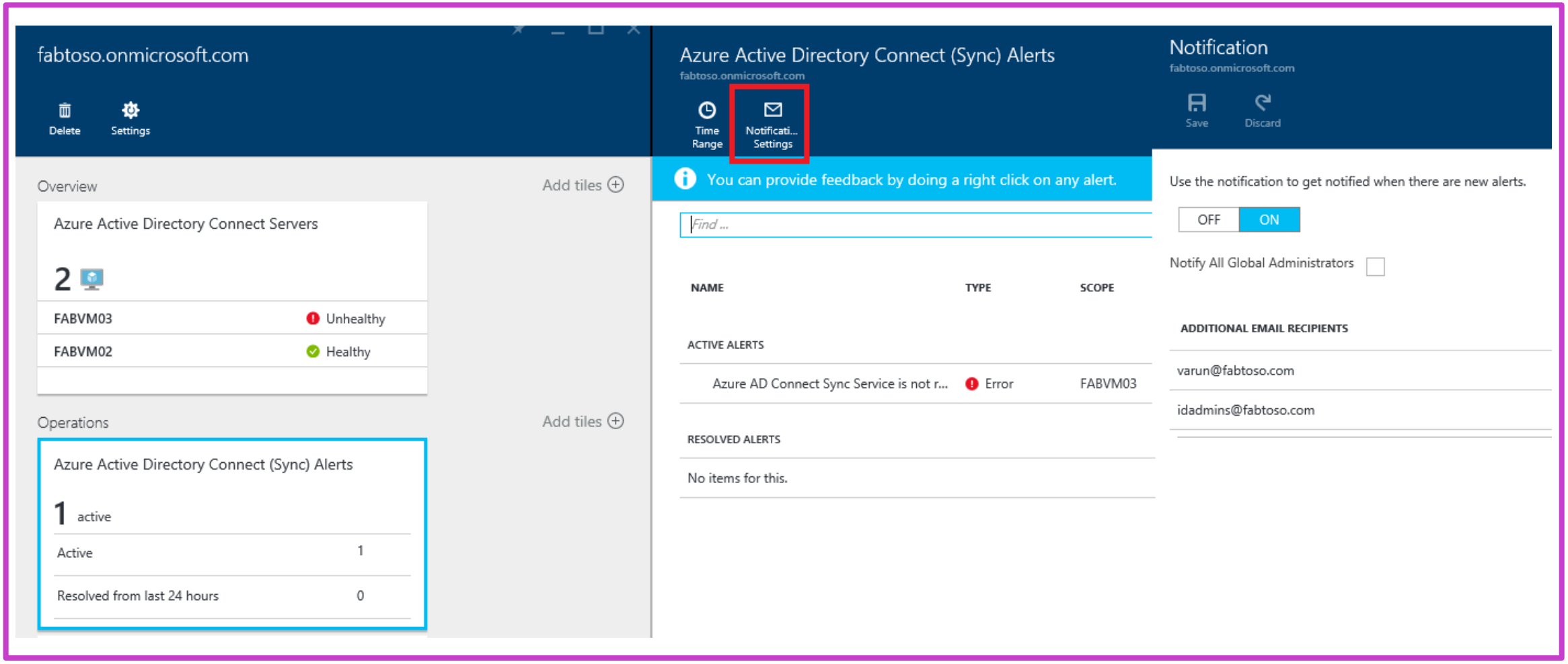
Example—Microsoft Entra Connect Help for AD FS installation steps

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



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

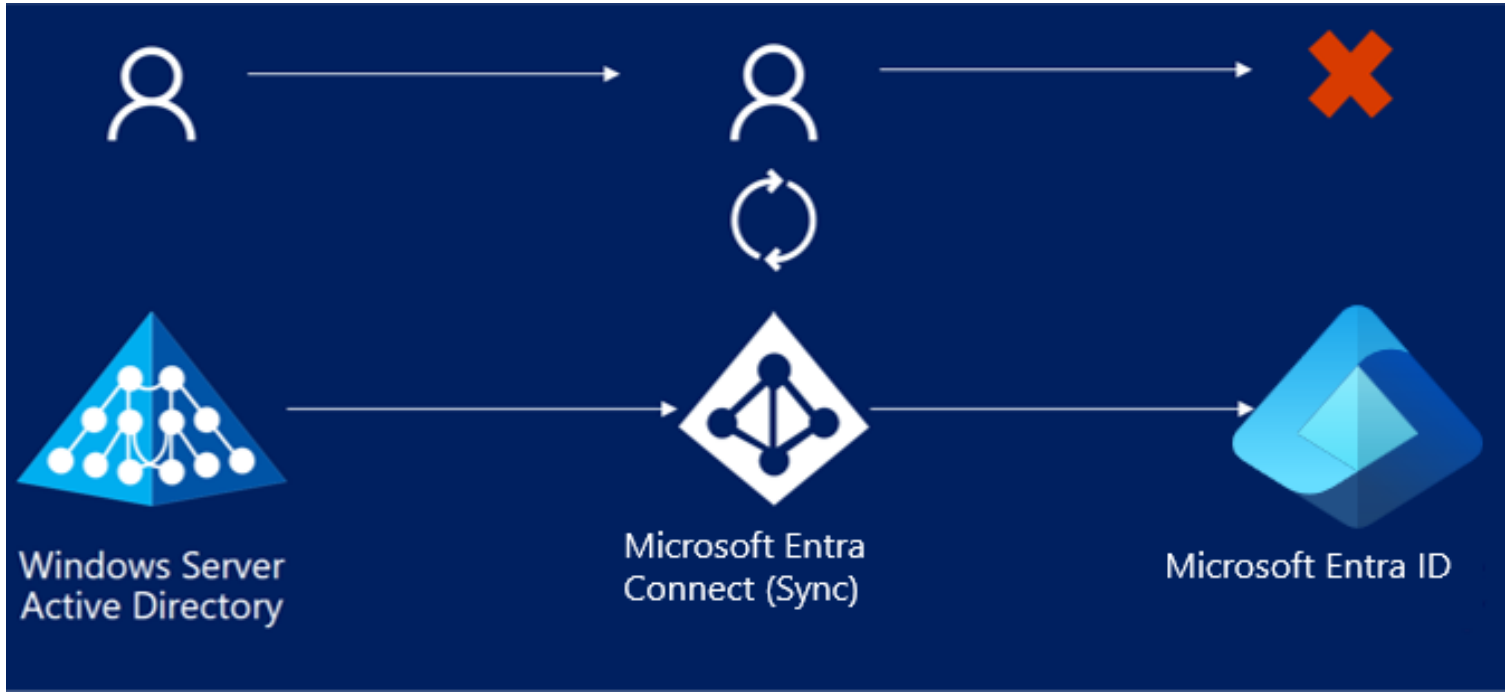
Diagnose and remediate duplicated attribute sync errors

- Duplicate UserPrincipleName 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.