Microsoft Security

SC-300

Microsoft Identity and Access Administrator

SC-300 Agenda

LP1: Implement an Identity Management Solution

Id
external Id
hybrid Id

2x RBAC

LP2: Implement an Authentication and Access Management Solution

LP3: Implement Access Management for Apps

LP4: Plan and Implement an Identity Governance Strategy

Microsoft Security

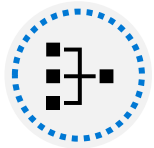
Implement an Identity Management Solution

Outline

Create, configure, and manage identities

Configure and manage Azure Active Directory

Implement and manage external identities

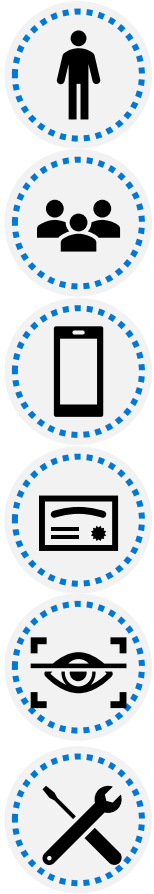


Implement and manage hybrid identity

Microsoft Security

Create, configure, and manage identities

Objectives



Create, configure, and manage users

Create, configure, and manage groups

Configure and mange device identities

Manage licenses

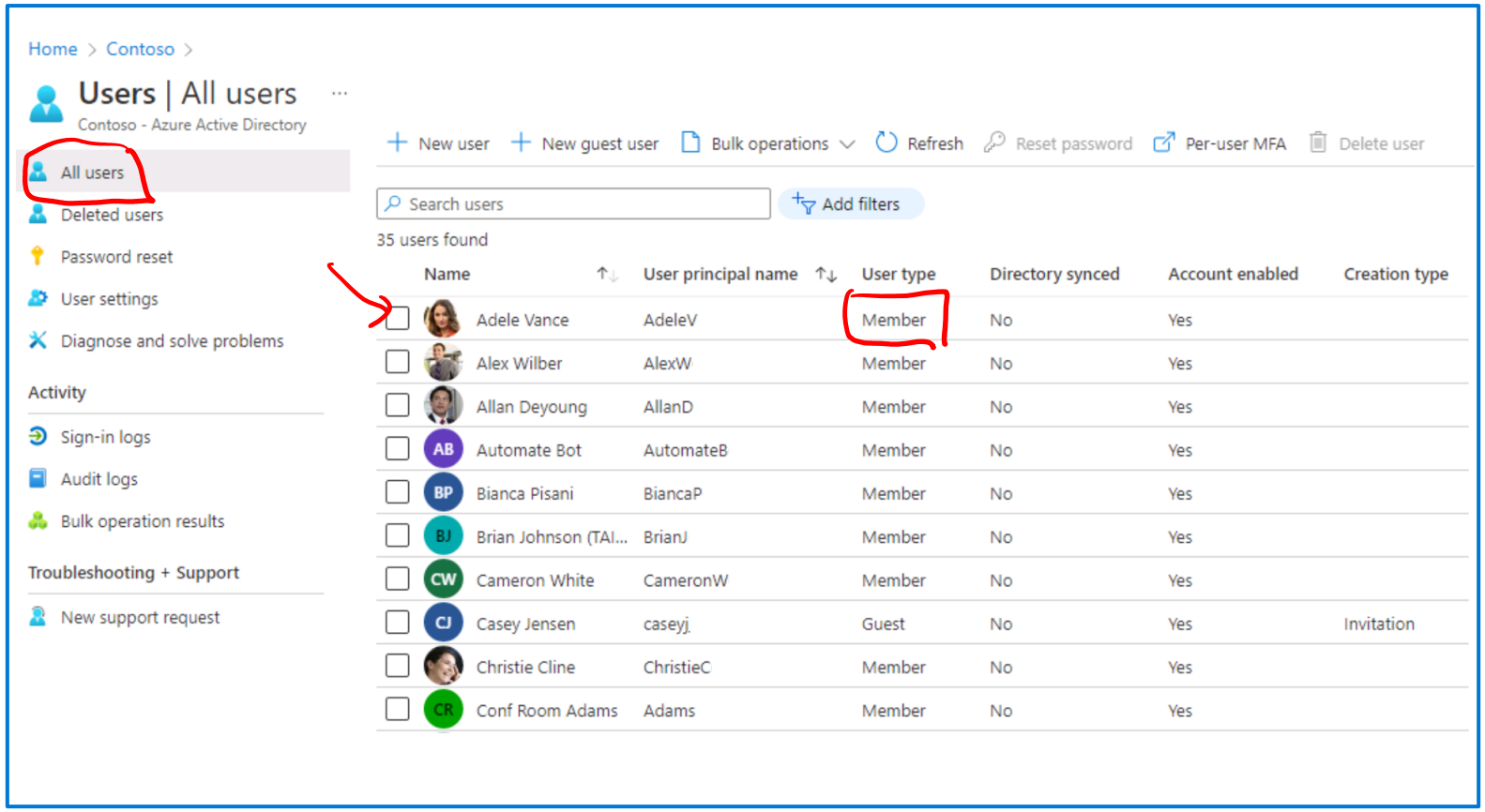
Custom security attributes

Provisioning using SCIM

Create, configure, and manage users

Create, configure, and manage users

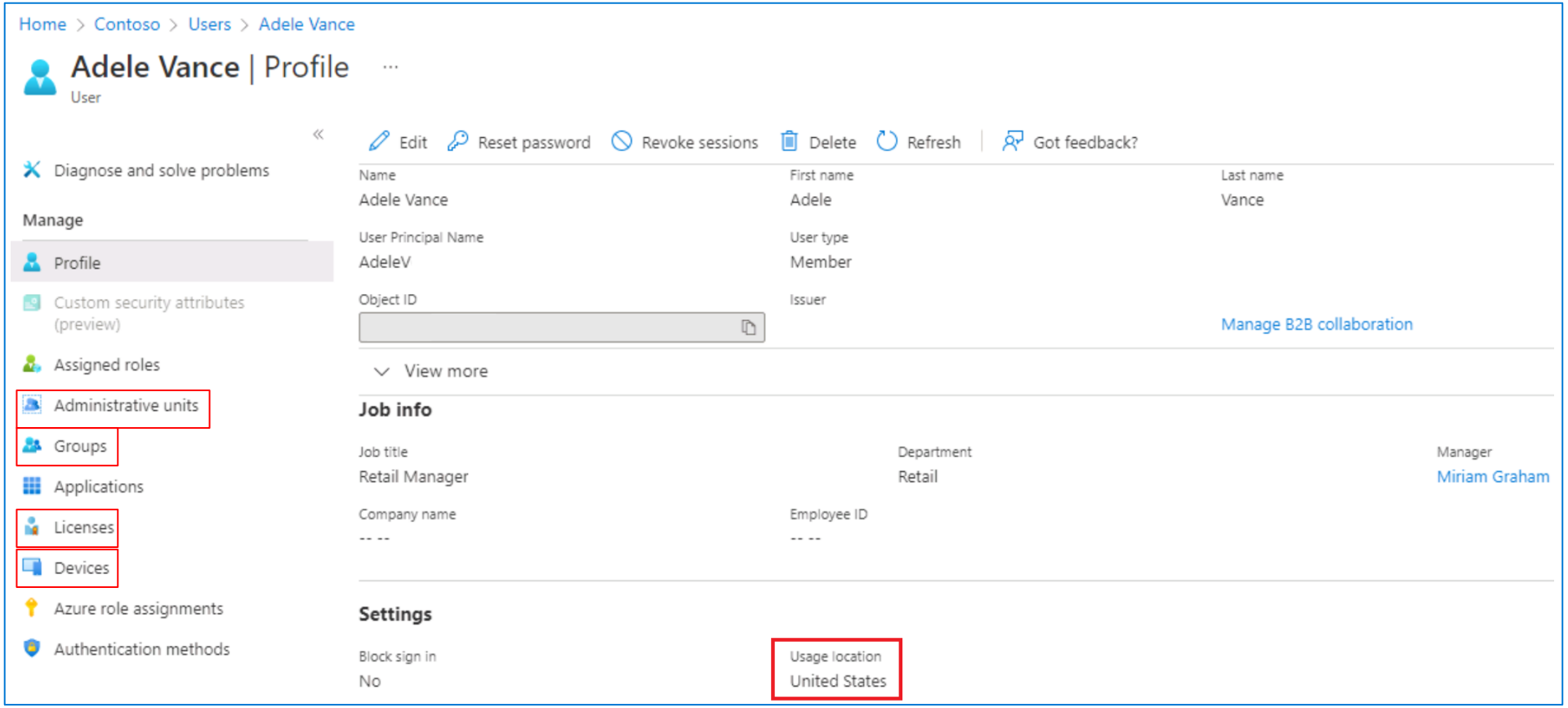
- A user account contains all the information needed to authenticate the user during the sign-on process
- You use the **Azure Active Directory** dashboard in the Azure portal to work with user objects
- Three kinds of users:
  - Cloud identities
  - Directory-synchronized identities
  - Guest users



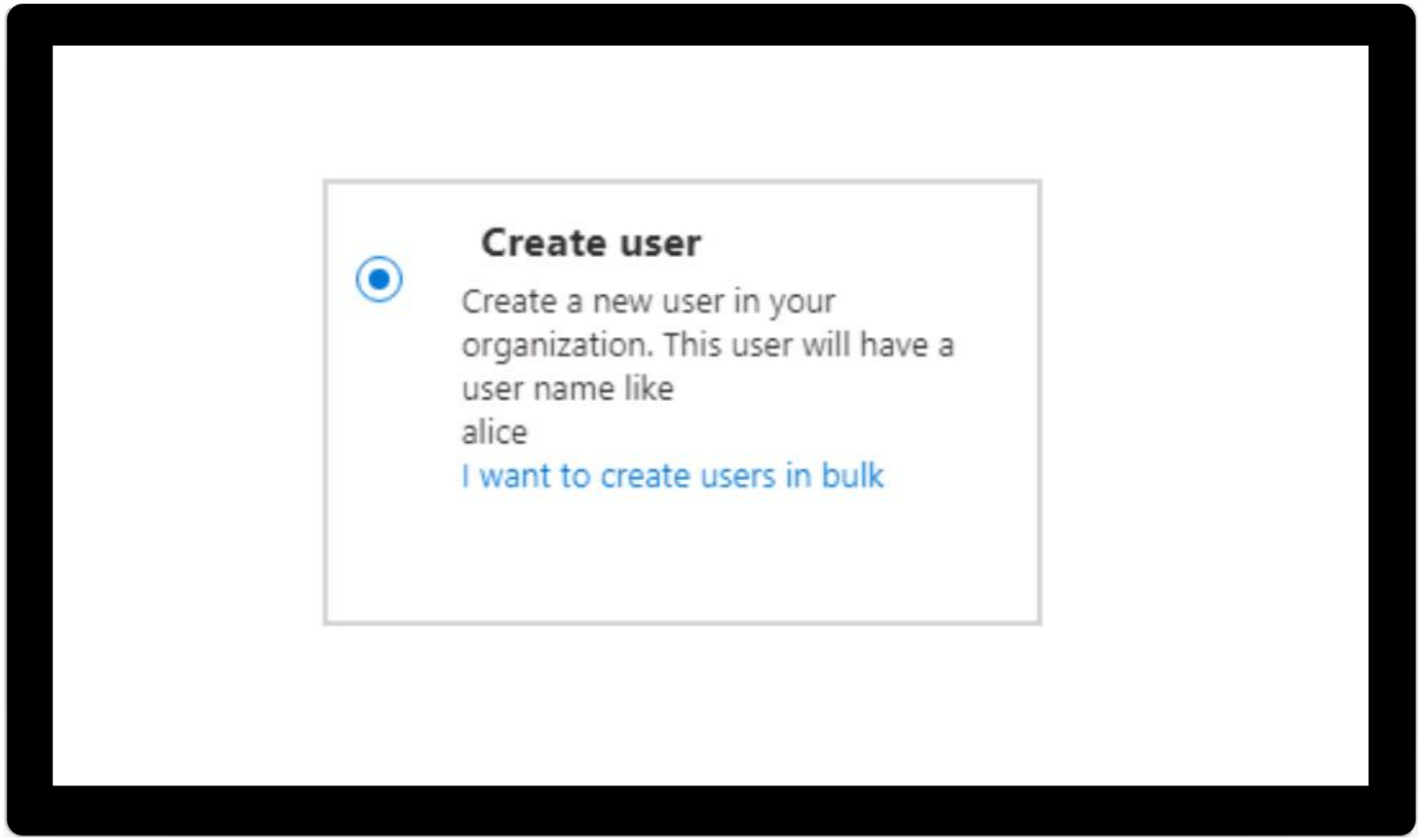
User settings

Some configurable user settings:

- Groups
- Licenses
- Devices
- Location



Demo – Users



Create, configure, and manage groups

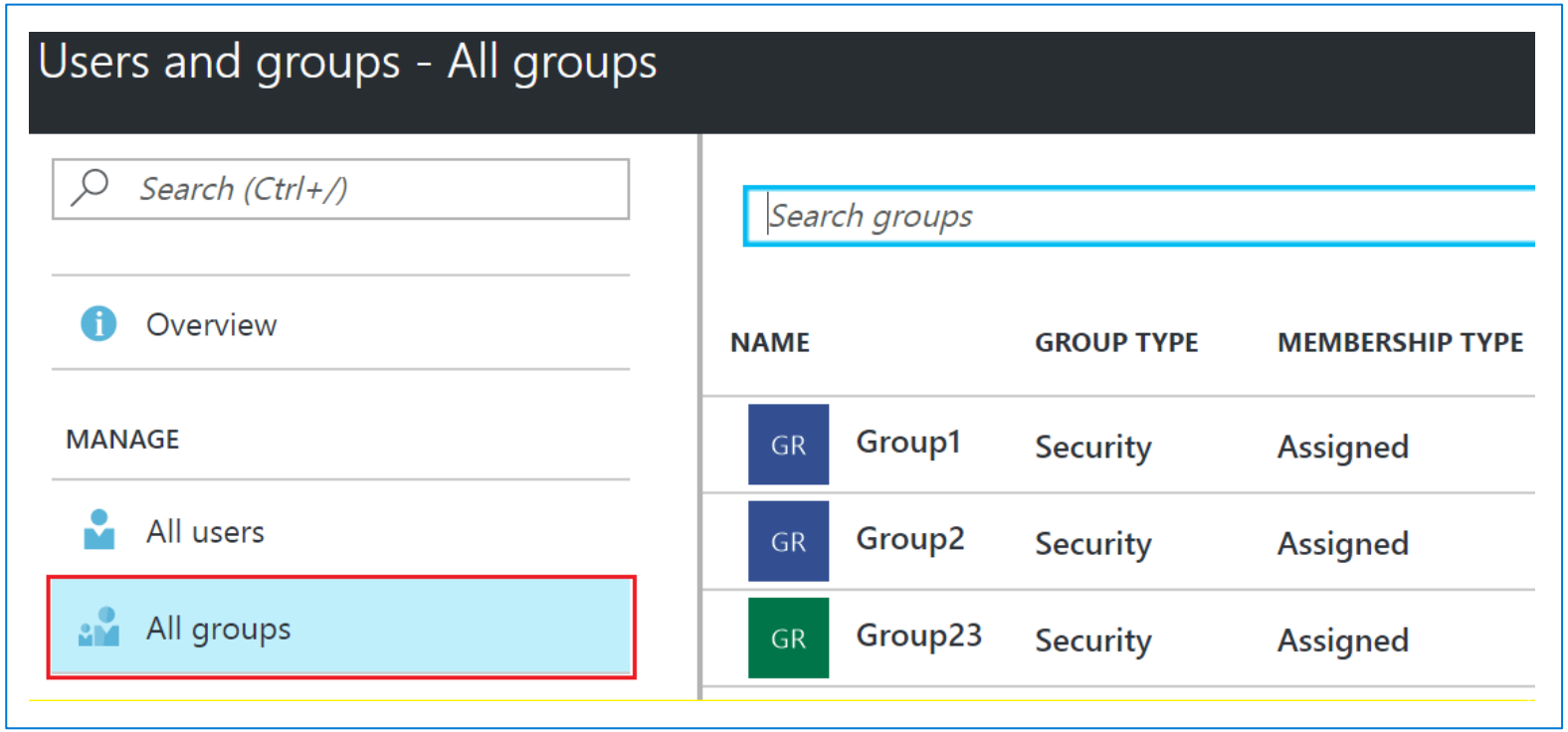
Create, configure, and manage groups

Security groups:

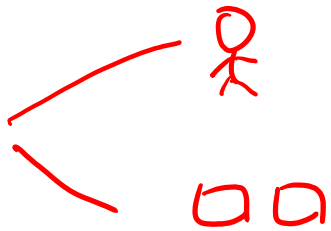
- Most common
- Manage access to shared resources for a group

Microsoft 365 groups:

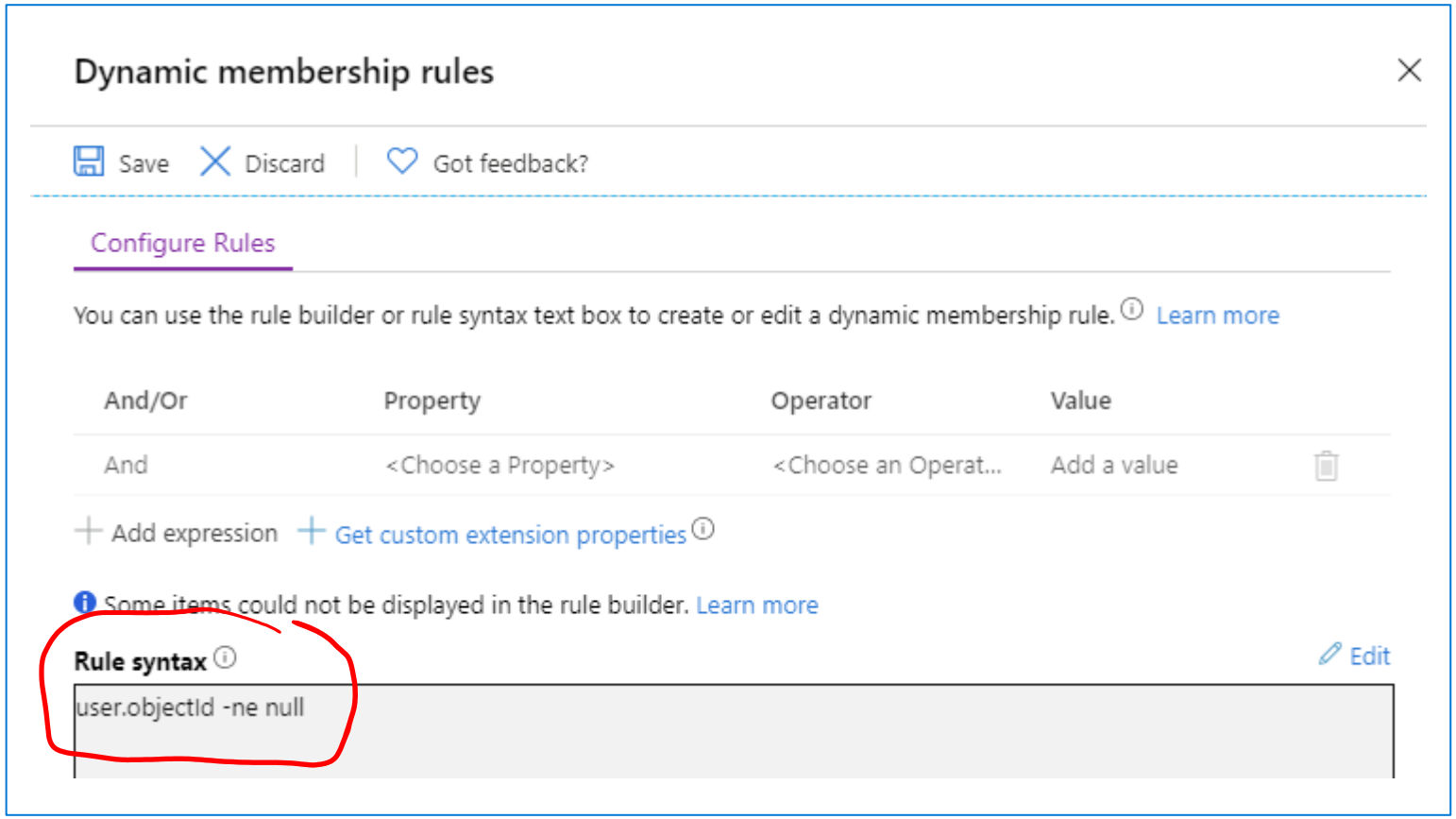
- Access shared mailbox, calendar, SharePoint, and more
- Give access to external people



Dynamic Groups



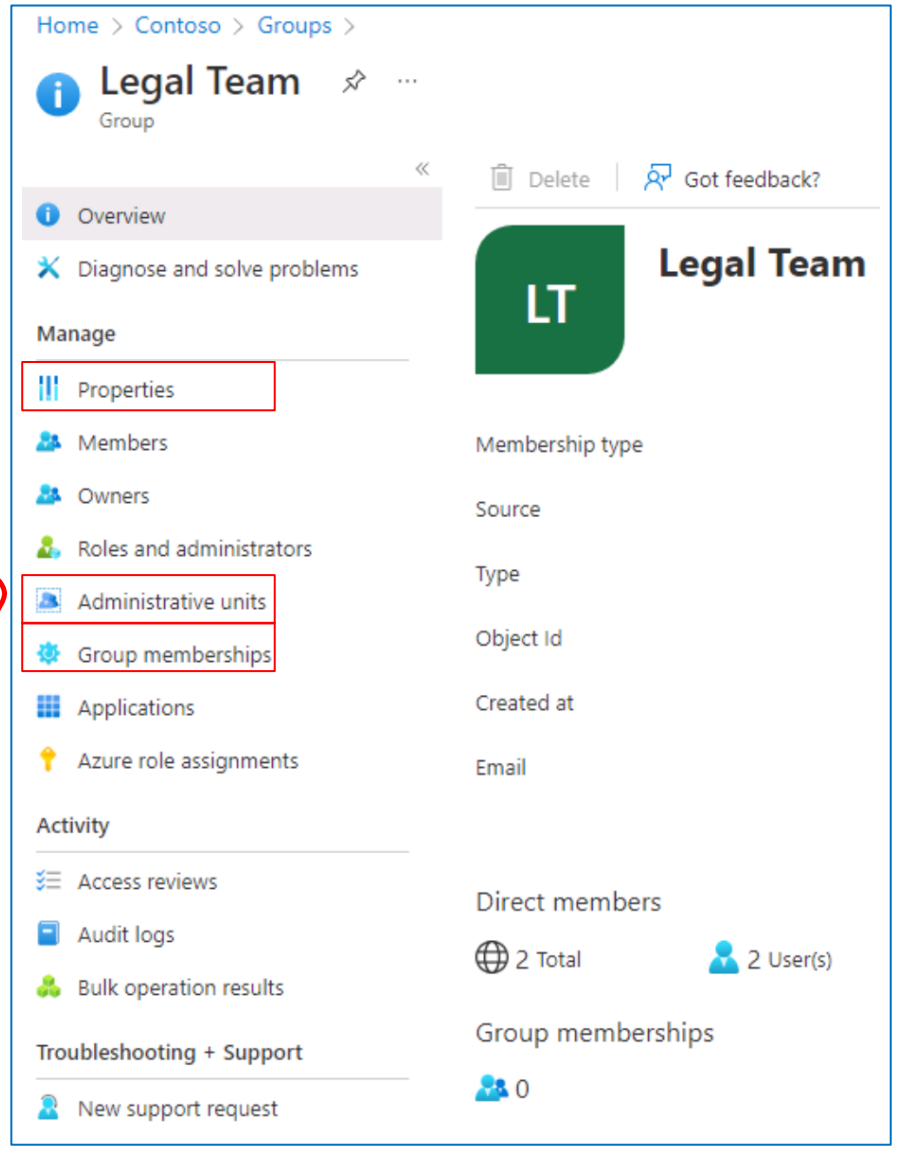
- Special type of Security Group
- Membership dynamically generated via Membership Rule
  - UserType, department, region, and other items



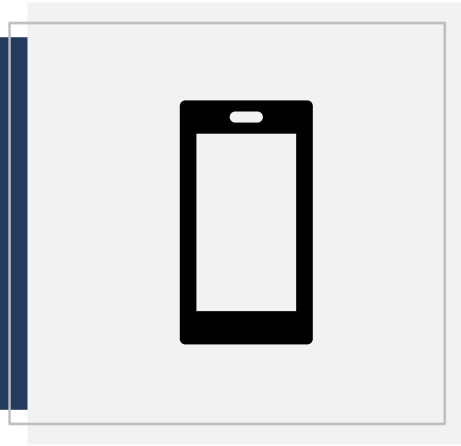
Group configuration options

Some configurable group settings:

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



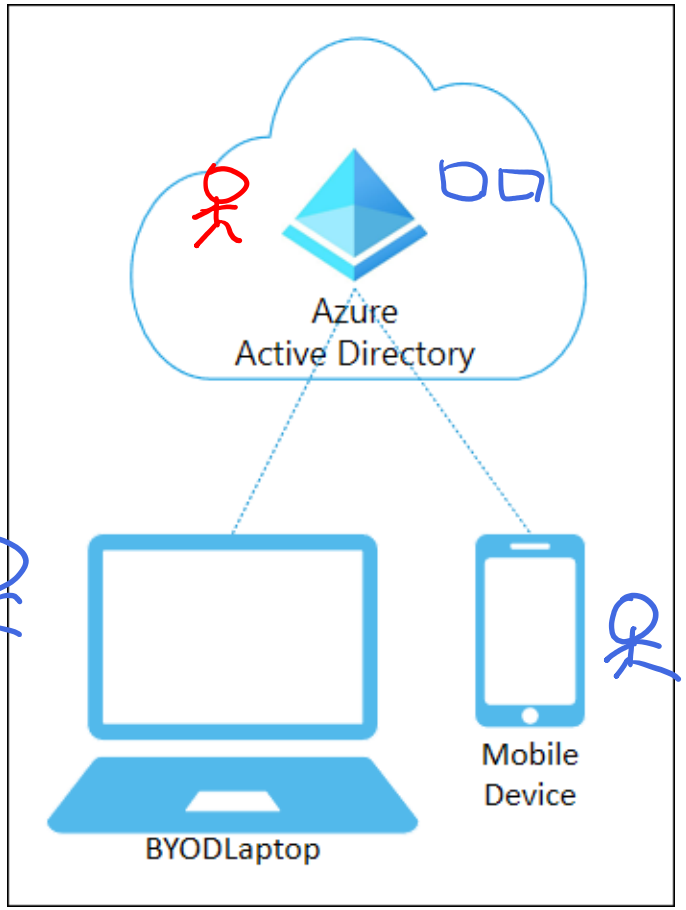
Configure and mange device identities



Azure AD registered devices

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

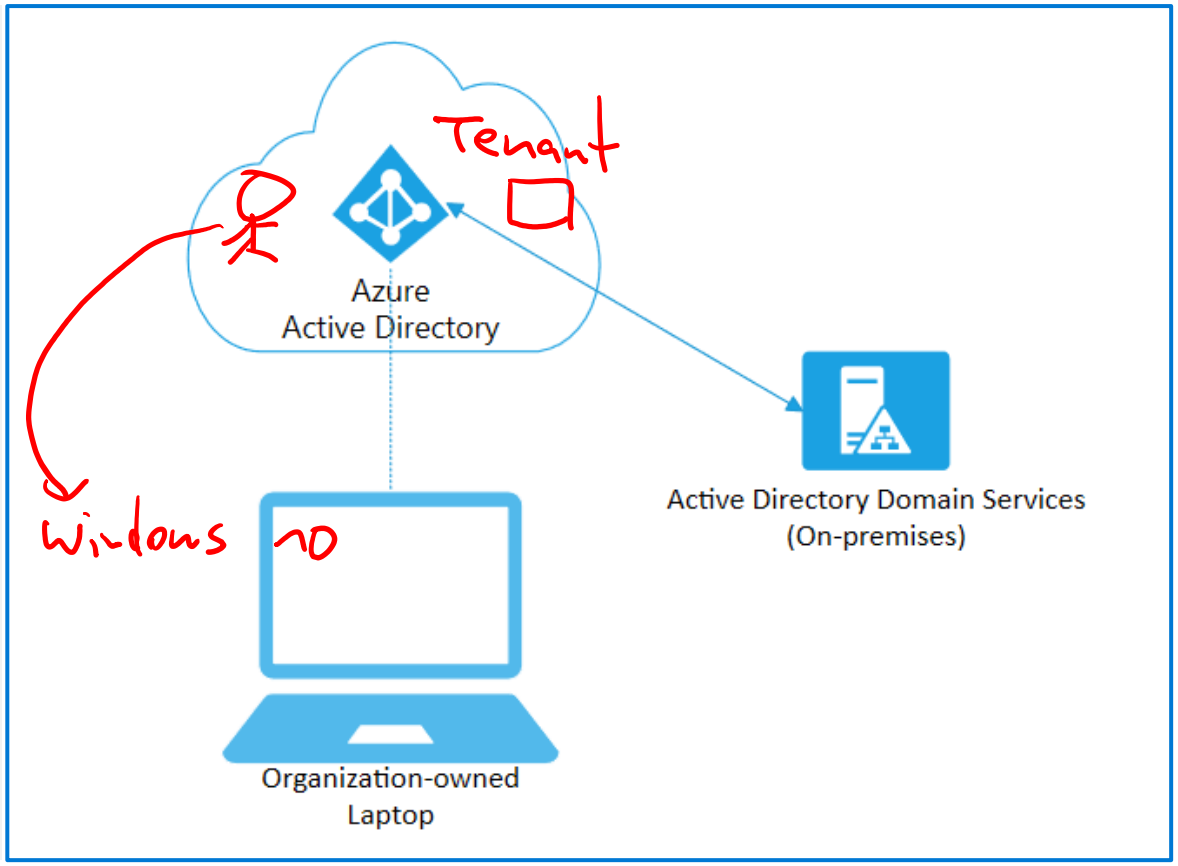
OS – Windows 10/11, iOS, Android, and MacOS



Azure AD joined devices

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

OS – Windows 10/11 devices (not Home)

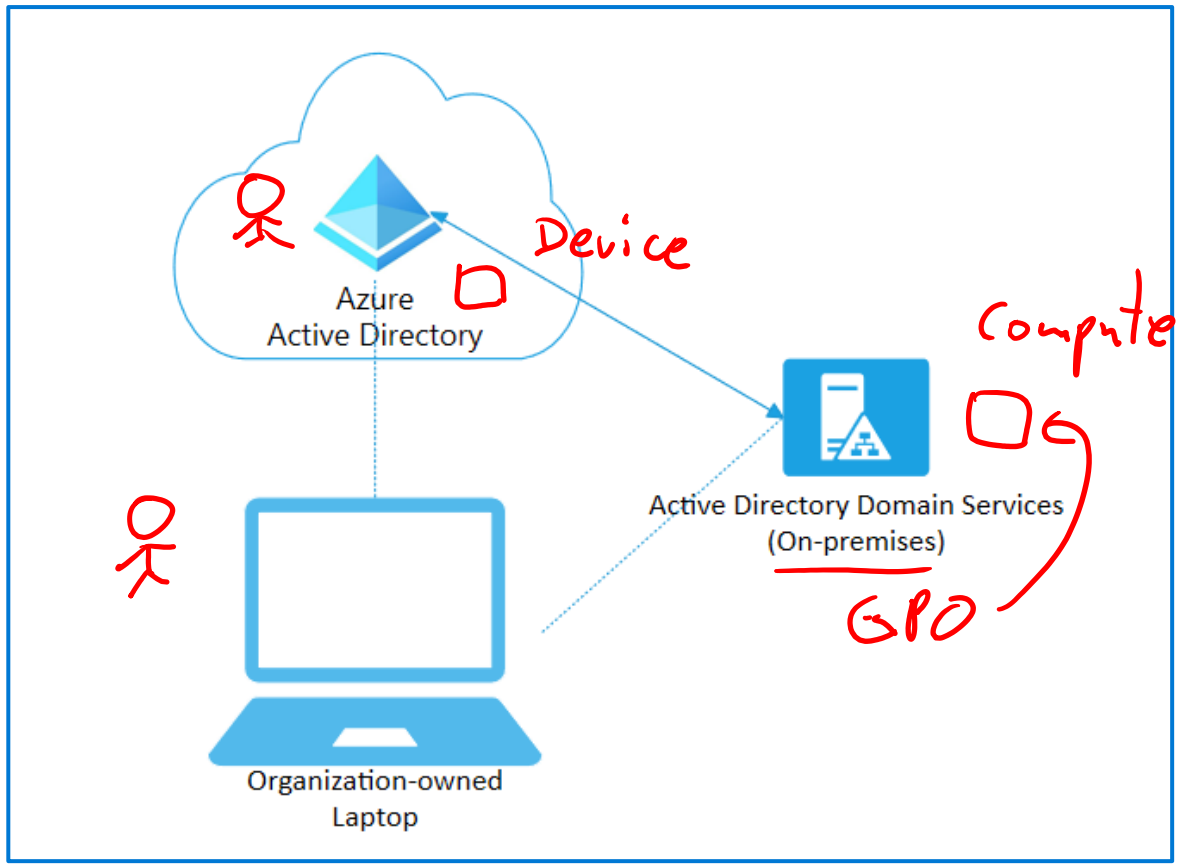


Hybrid Azure AD joined devices

Use Azure AD hybrid joined devices if:

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

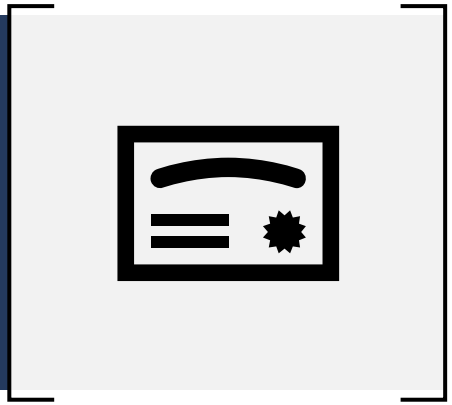
OS - Windows 7 and 8.1 devices in addition to Windows 10



Device writeback

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

Manage licenses



About licenses

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

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

Additional Services (like O365 are paid cloud services)

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

Group-based licensing

- You can assign one or more product licenses to a group
- Azure AD ensures that the licenses are assigned to all members of the group
- New group members are automatically assigned the appropriate licenses
- Licenses are removed from users when they leave the group
- Licenses can be assigned to any security group

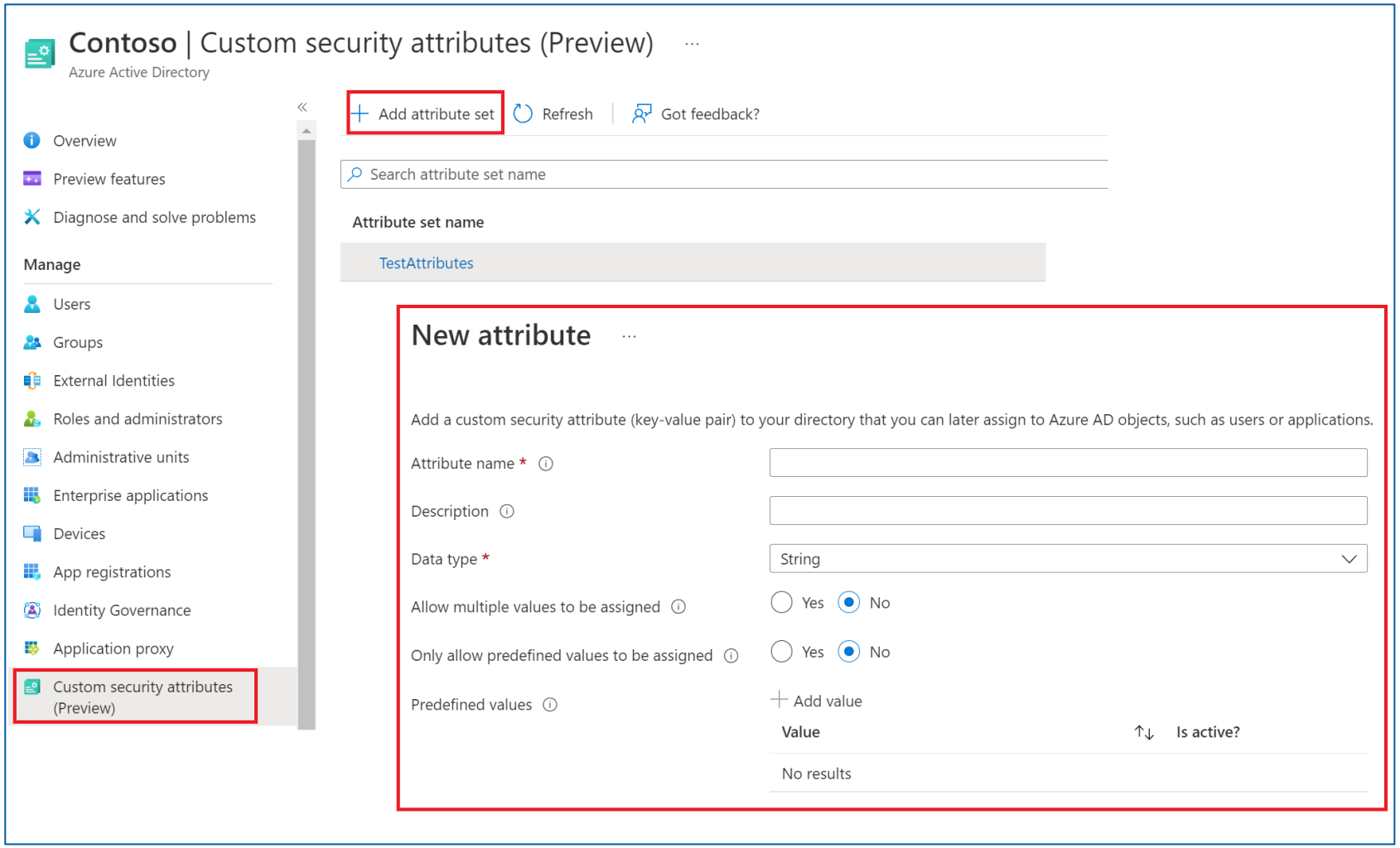
- Administrators can disable service plans
- All Microsoft cloud services are supported
- Available only through the Azure portal
- Azure AD automatically modifies licenses based on group membership changes
- A user can be a member of multiple groups with license policies specified
- In some cases, licenses cannot be assigned to a user

Custom security attributes

Manage custom security attributes (preview)

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

Azure AD Premium P1 / P2

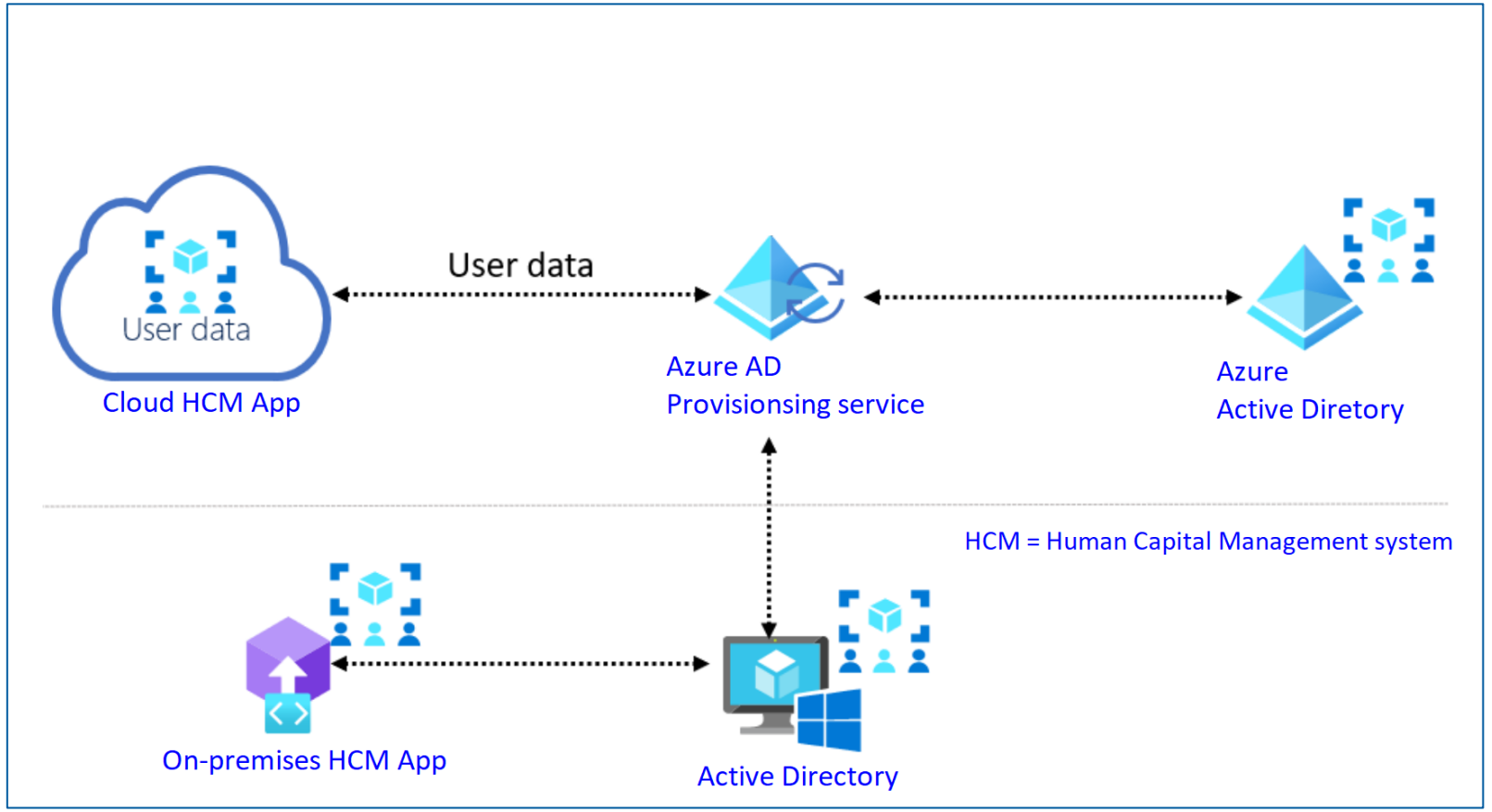


Provisioning with SCIM

Identity provisioning from cloud applications by using SCIM

SCIM – System for Cross-Domain Identity Management

Use employee records to provision Azure AD accounts



Microsoft Security

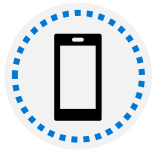
Configure and manage Azure Active Directory tenant

Objectives

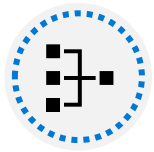
Configure company branding

Configure and manage Azure Active Directory roles

Configure and manage custom domains



Configure and manage device registration



Configure delegation by using administrative units

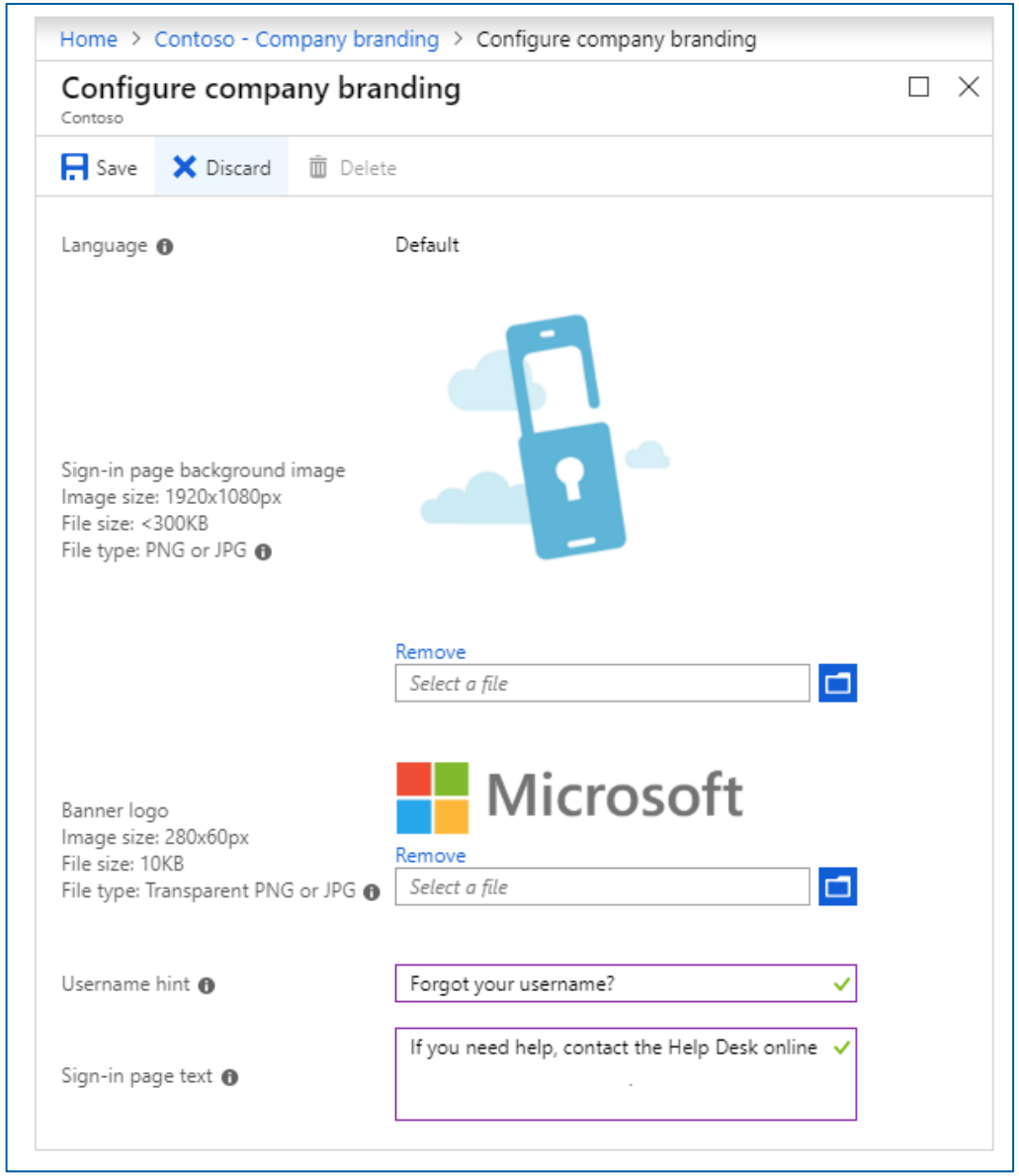
Configure tenant-wide settings

Company branding

Company branding

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

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



Configure and manage Azure Active Directory roles

Global Admin

Admin access to Azure and Azure AD

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

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

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

Entra Admin Center – https://entra.microsoft.com

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

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

- Formerly – Microsoft Cloud App Security (MCAS)

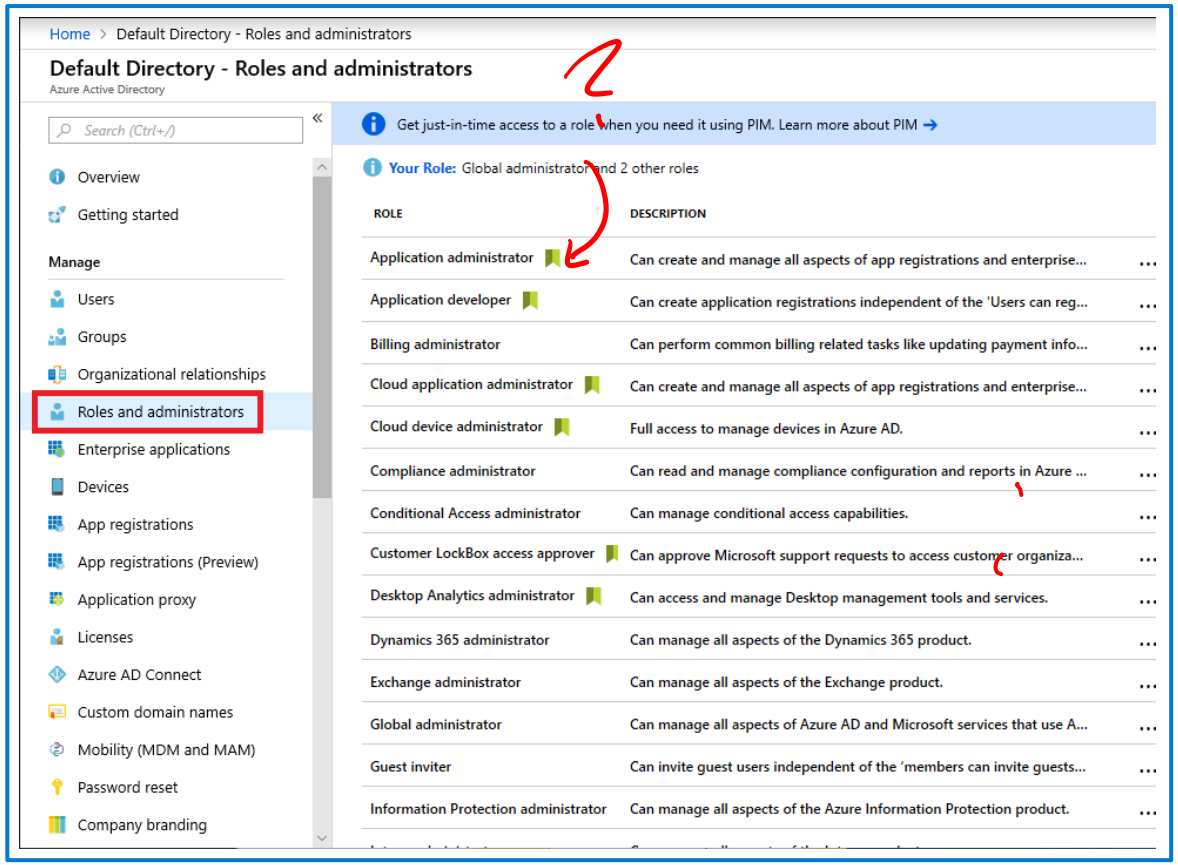
Azure AD roles

Intended for:

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

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

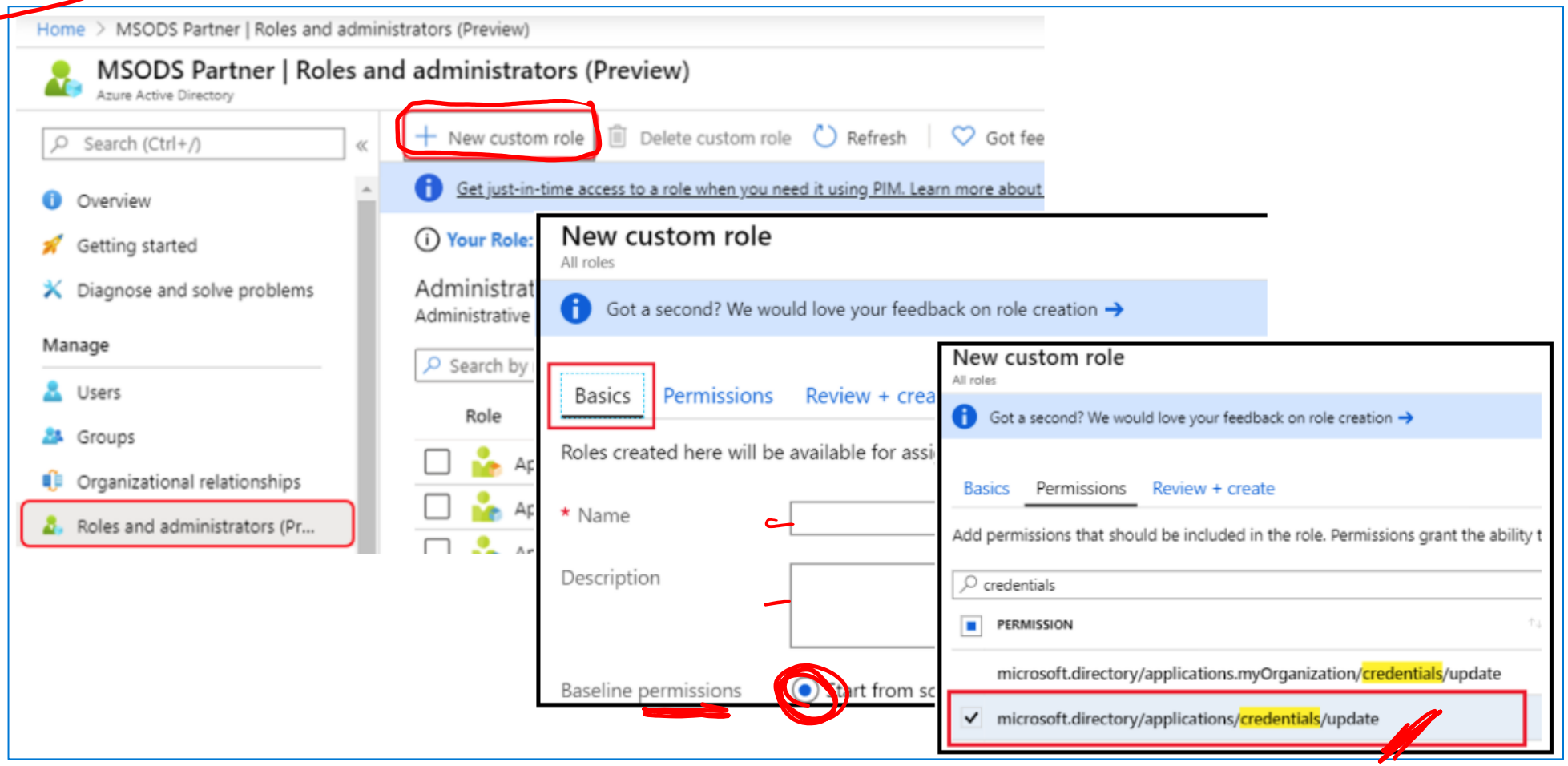
Do not overlap with Azure roles by default



Custom Roles

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

Requires an Azure AD premium license

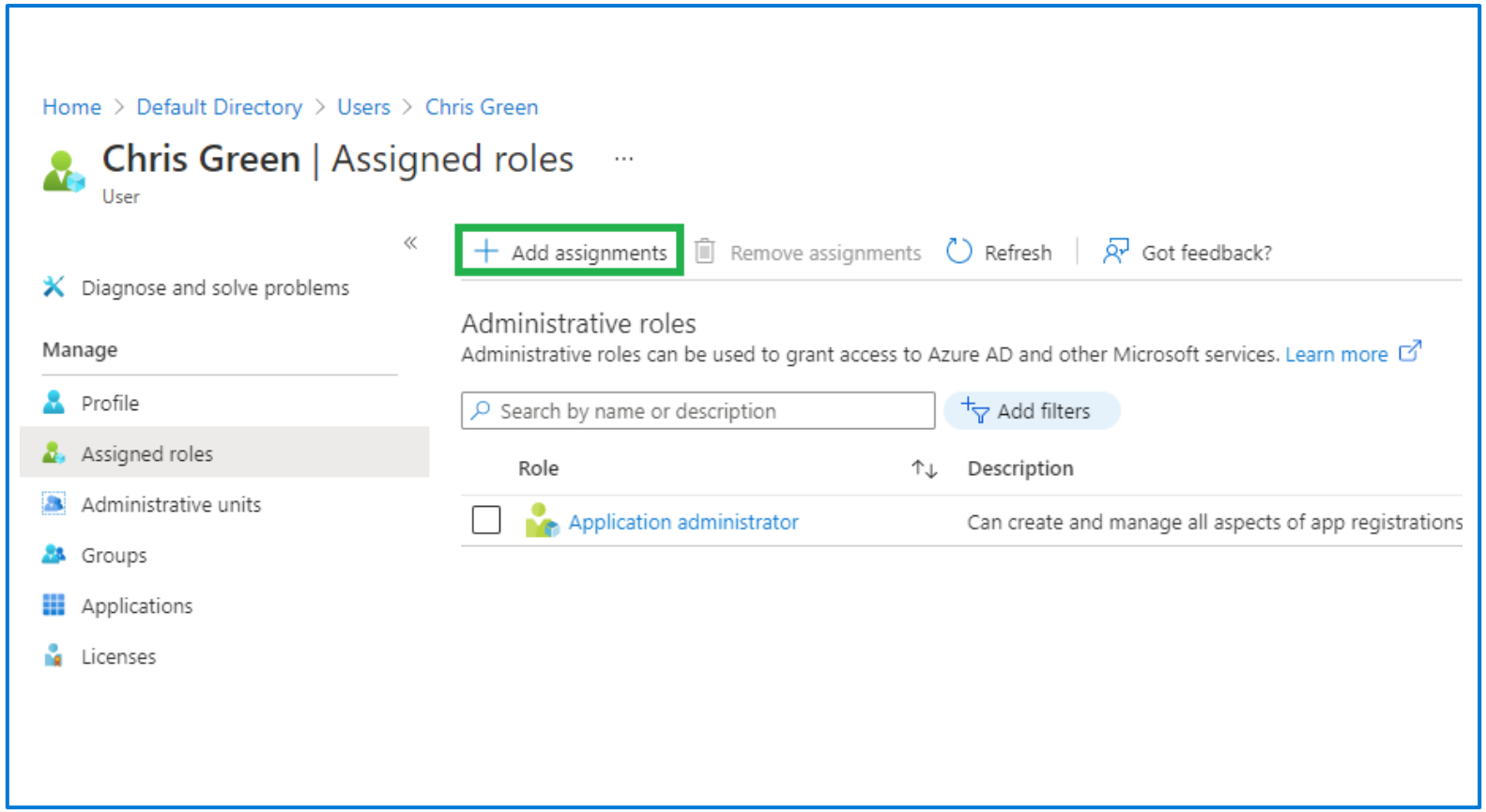


Assigning roles – to a user or group

Assign built-in or custom roles

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

Use principle of Least Privilege when assigning

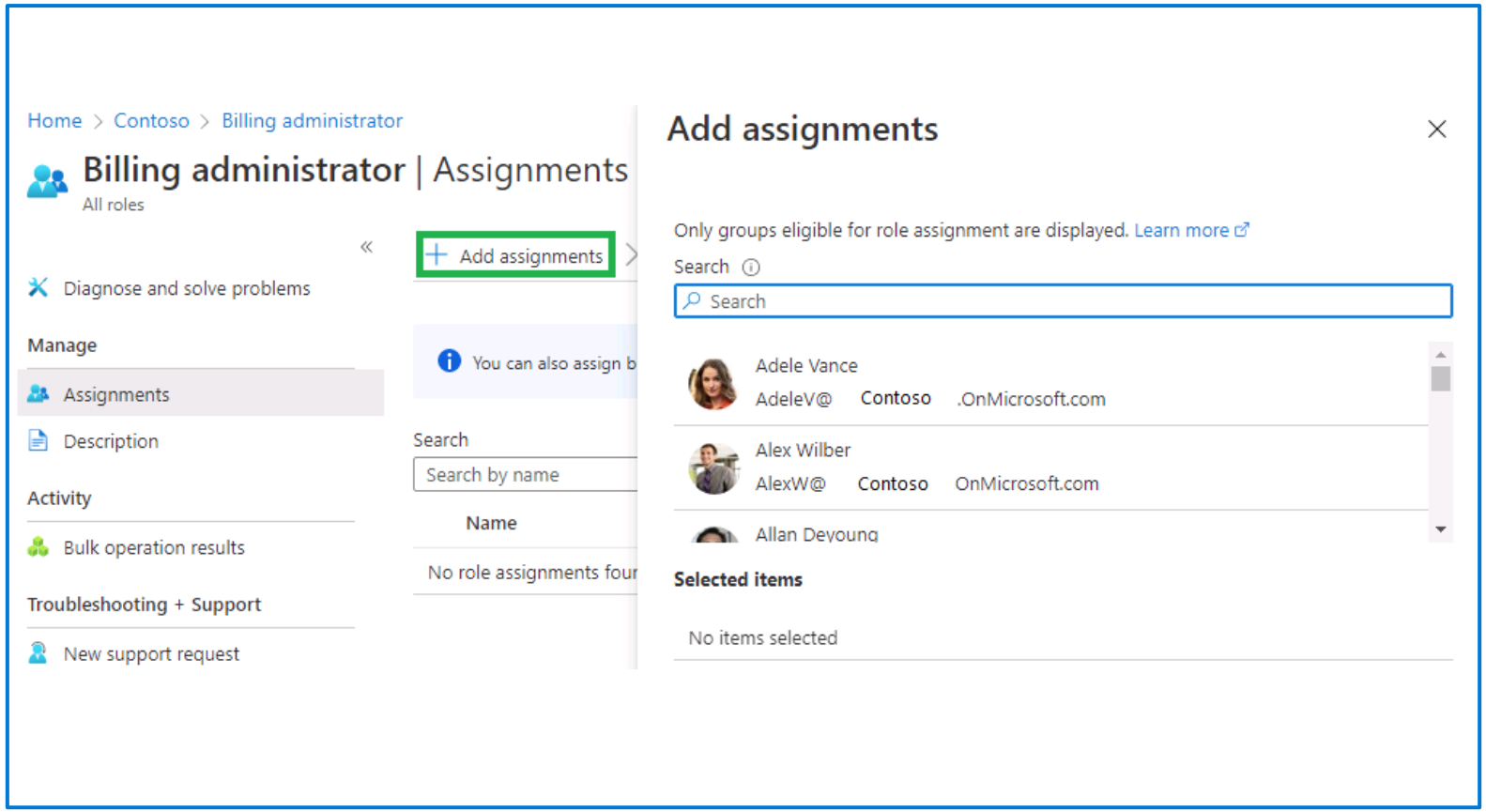


Assign users or groups to a role

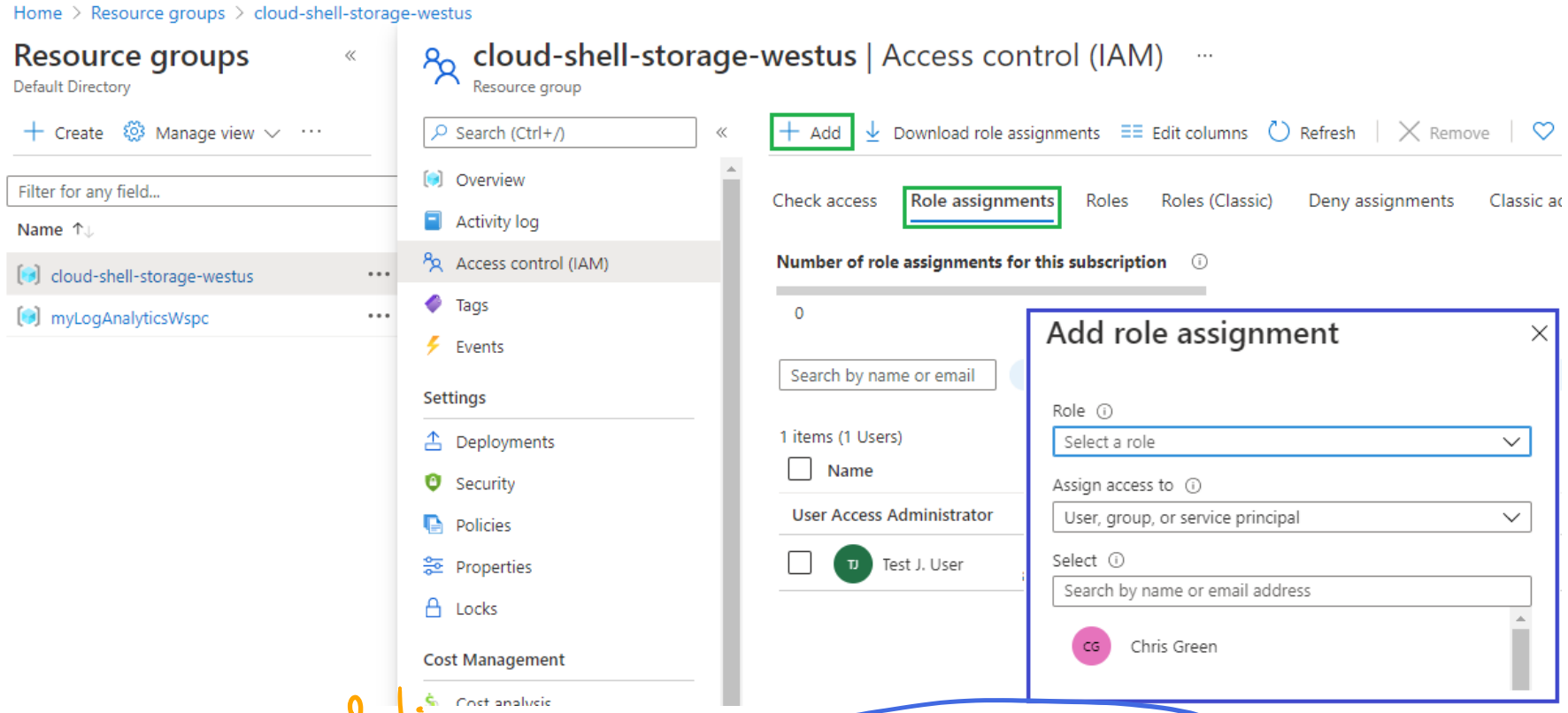
Identities can be added to a role

Alternative method to assign roles

Use principle of Least Privilege when assigning



Assigning Azure roles to a Subscription or broader-scope



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

Using Azure AD roles for Common delegation scenarios

Delegation scenarios:

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

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

Least Privilege - Just in Time - Just long enough

PIM

Delegating administrative task with built-in roles

Delegating app administration

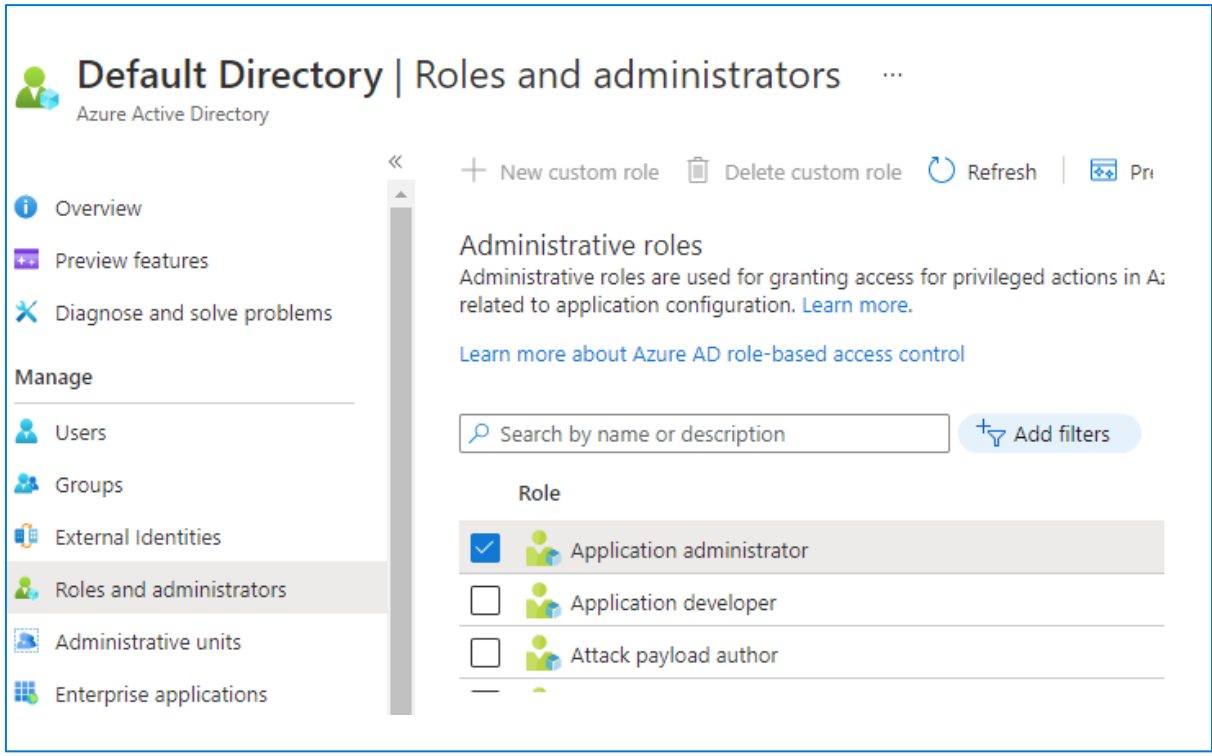
- Application Administrator role
- Cloud Application Administrator role

Delegating app registration

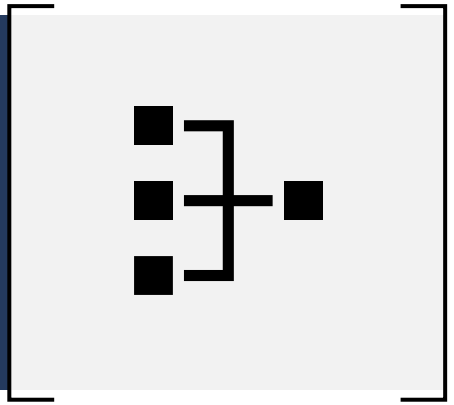
- Application Developer role

Delegating app ownership

- Enterprise Application Owner role
- Application Registration Owner role

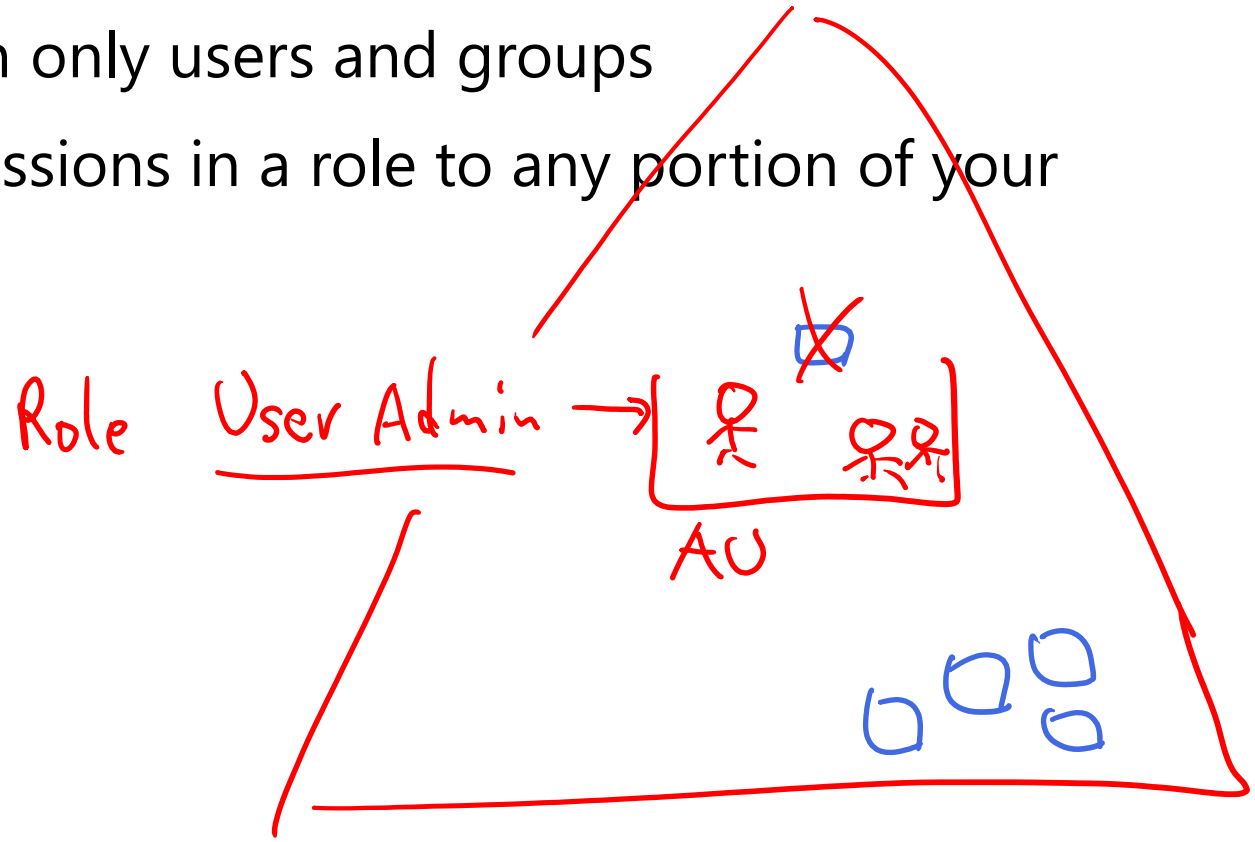


Configure delegation by using administrative units



About administrative units

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



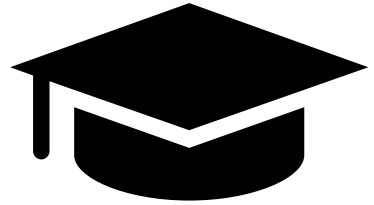
Deployment scenario

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

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

Administrative tasks could include:

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



Common delegation scenarios for Admin Units

Delegation scenarios:

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

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

Least Privilege - Just in Time - Just long enough

Delegating administrative task with built-in roles

Delegating authentication administration

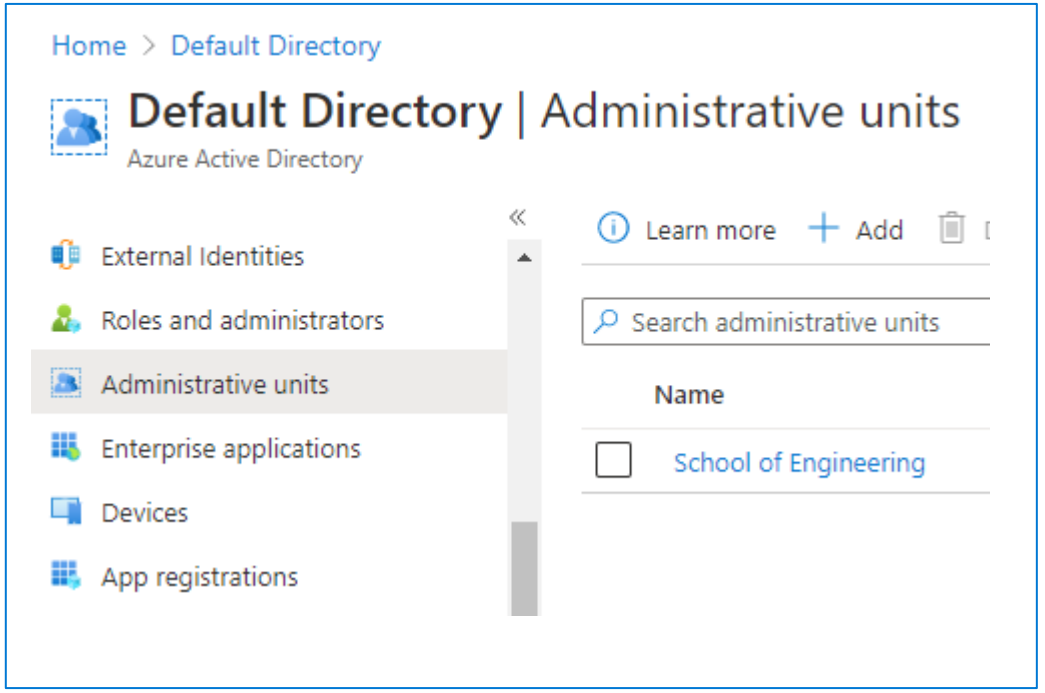
- Authentication Administrator role

Delegating licensing

- License Administrator

Delegating user, group, and password management

- User Administrator



Analyze Azure AD role permissions

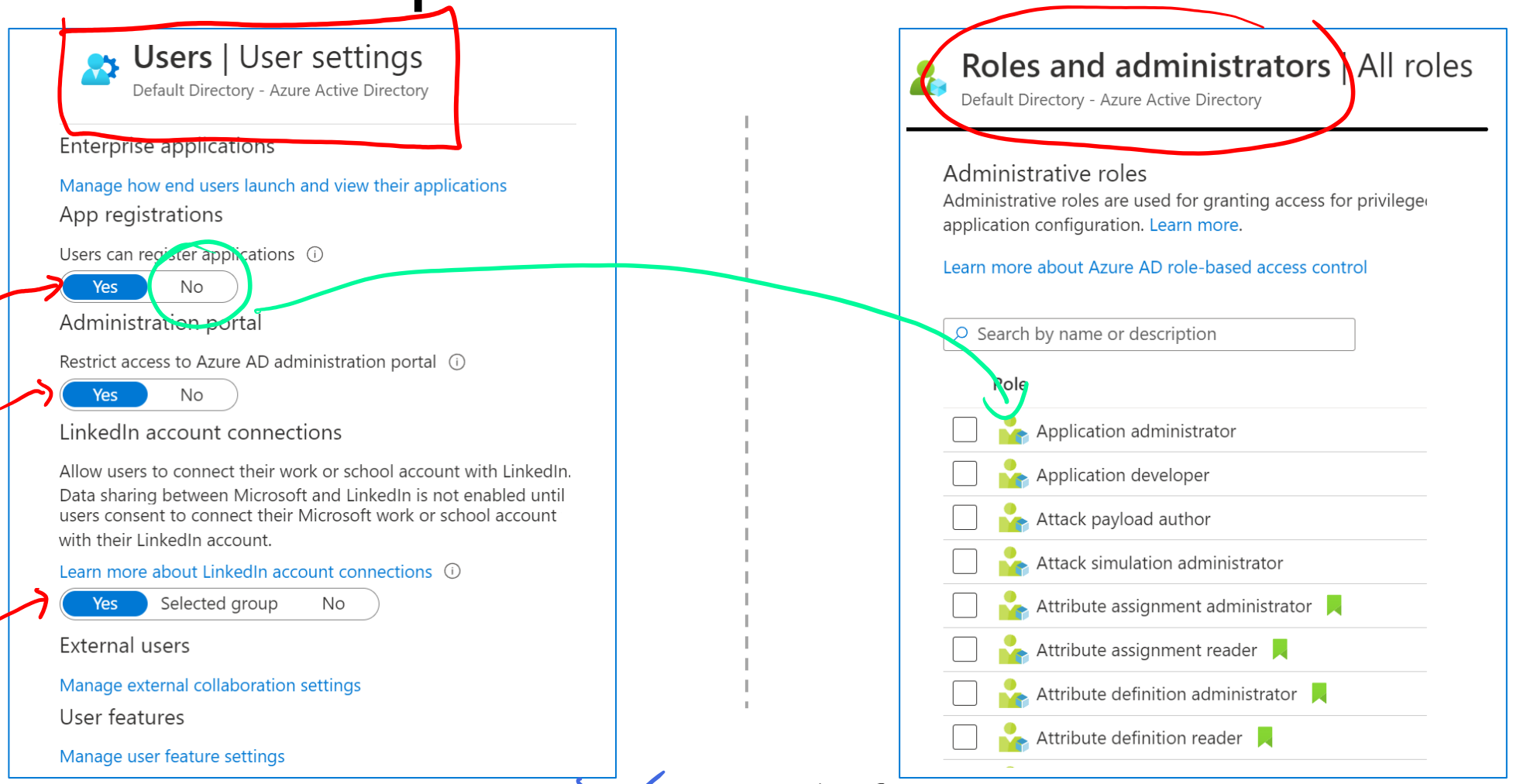
Permissions in Azure AD

Permission – Consent or authorization to perform a specific action.

Who / What gets permissions?			
Member Users	Guest Users	Applications	Devices
Example default permissions for each:			
• Enumerate list of user • Invite guest users • Change their password • Manage Photo • Create groups • Etc.	• Read own properties • Change their password • Search for groups • Cannot invite groups • Etc.		

* Augment or restrict permissions with settings and role assignments

Augment or restrict permissions



Portal
Shareable Links
:443
Bastion Host
:3389
VM

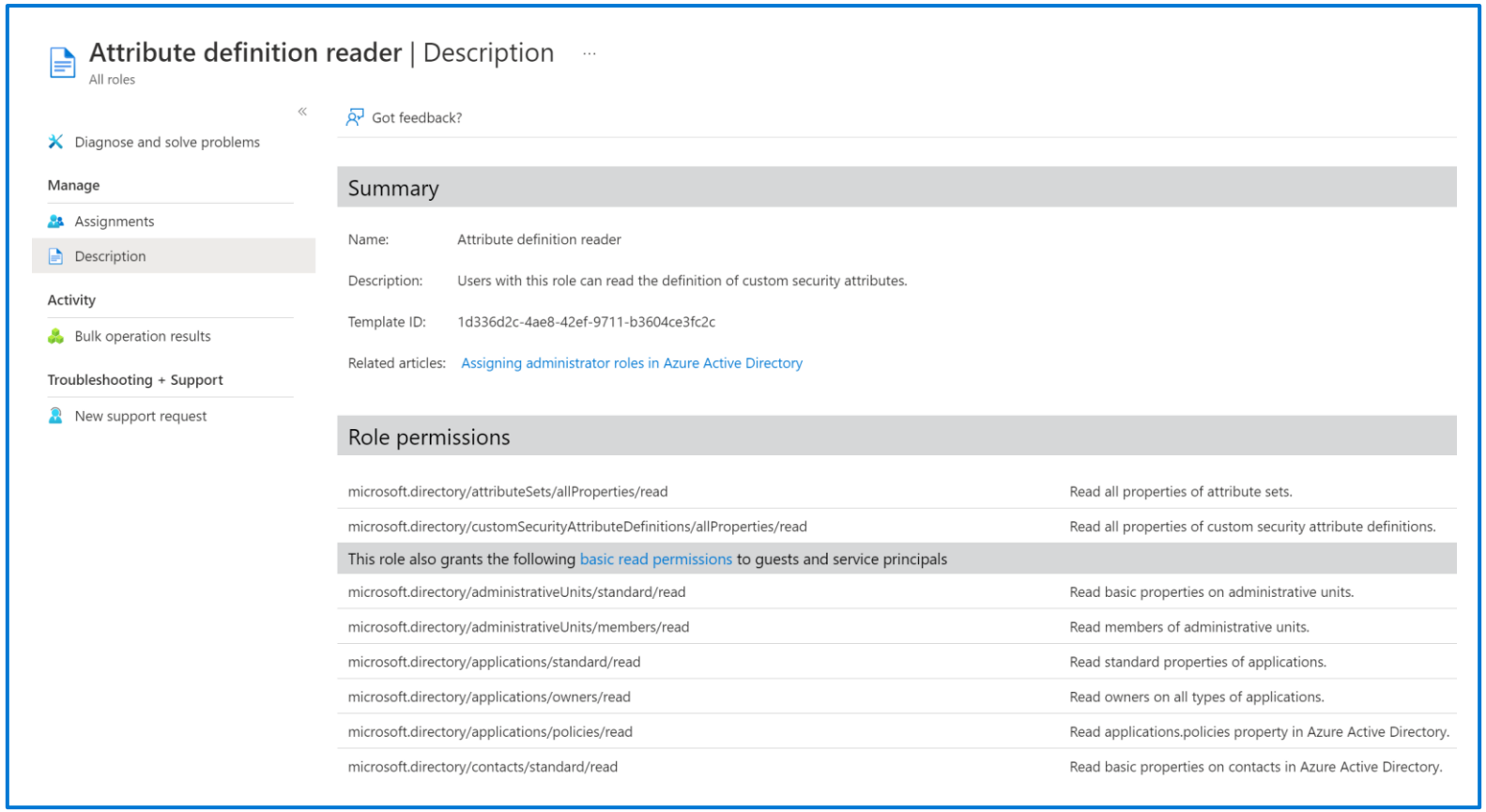
Analyze permission

Role permission

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

Guest / Service principal

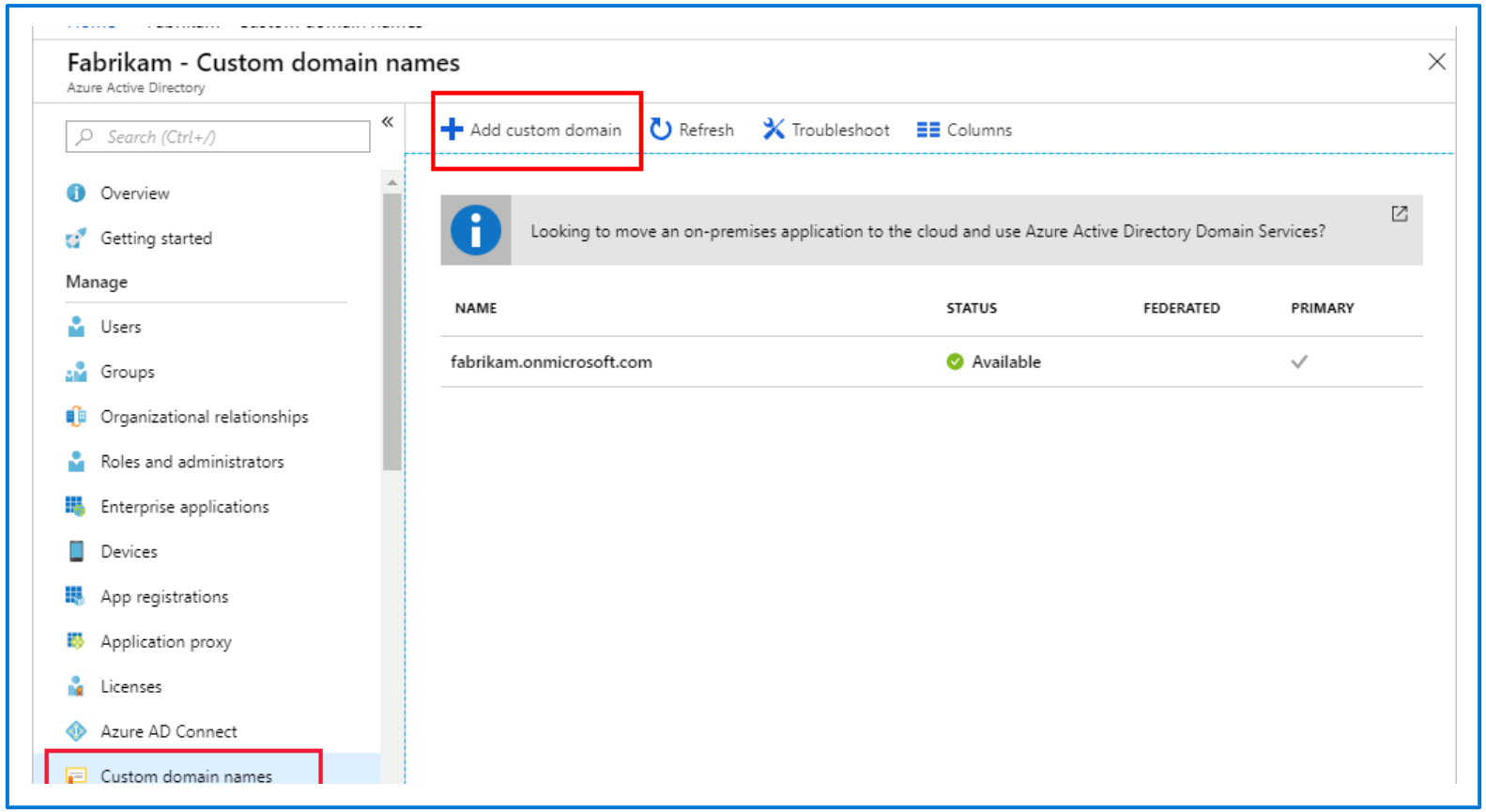
Additional permission given to ensure a basic level of functionality when assigned to guest users or service principals.



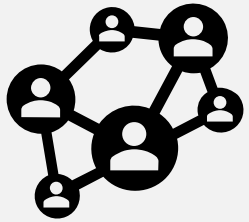
Configure and manage custom domains

Adding a custom domain name

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



Configure tenant-wide setting



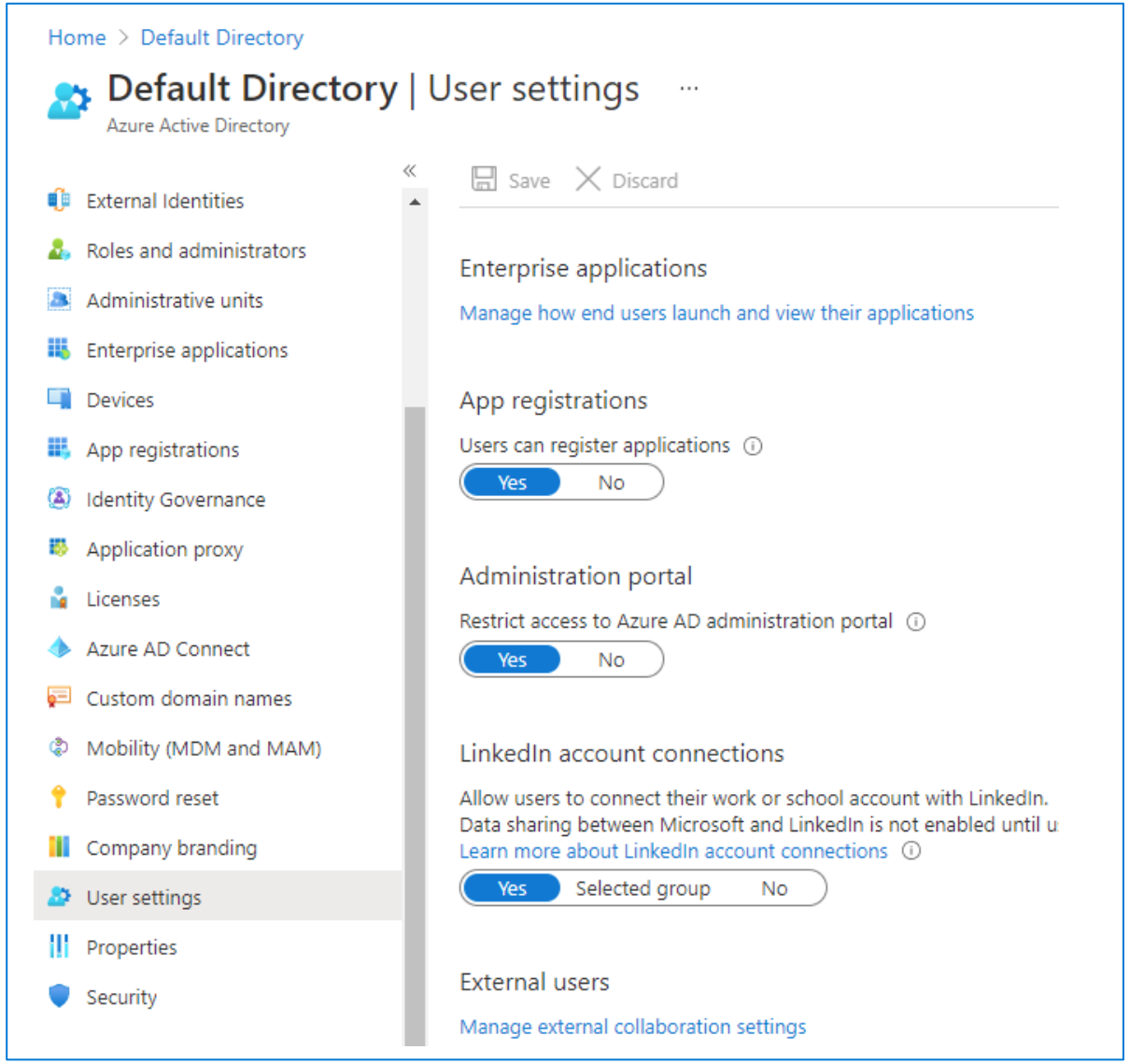
Tenant-wide settings

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

User settings

Azure Portal → Azure AD → Users → User Settings

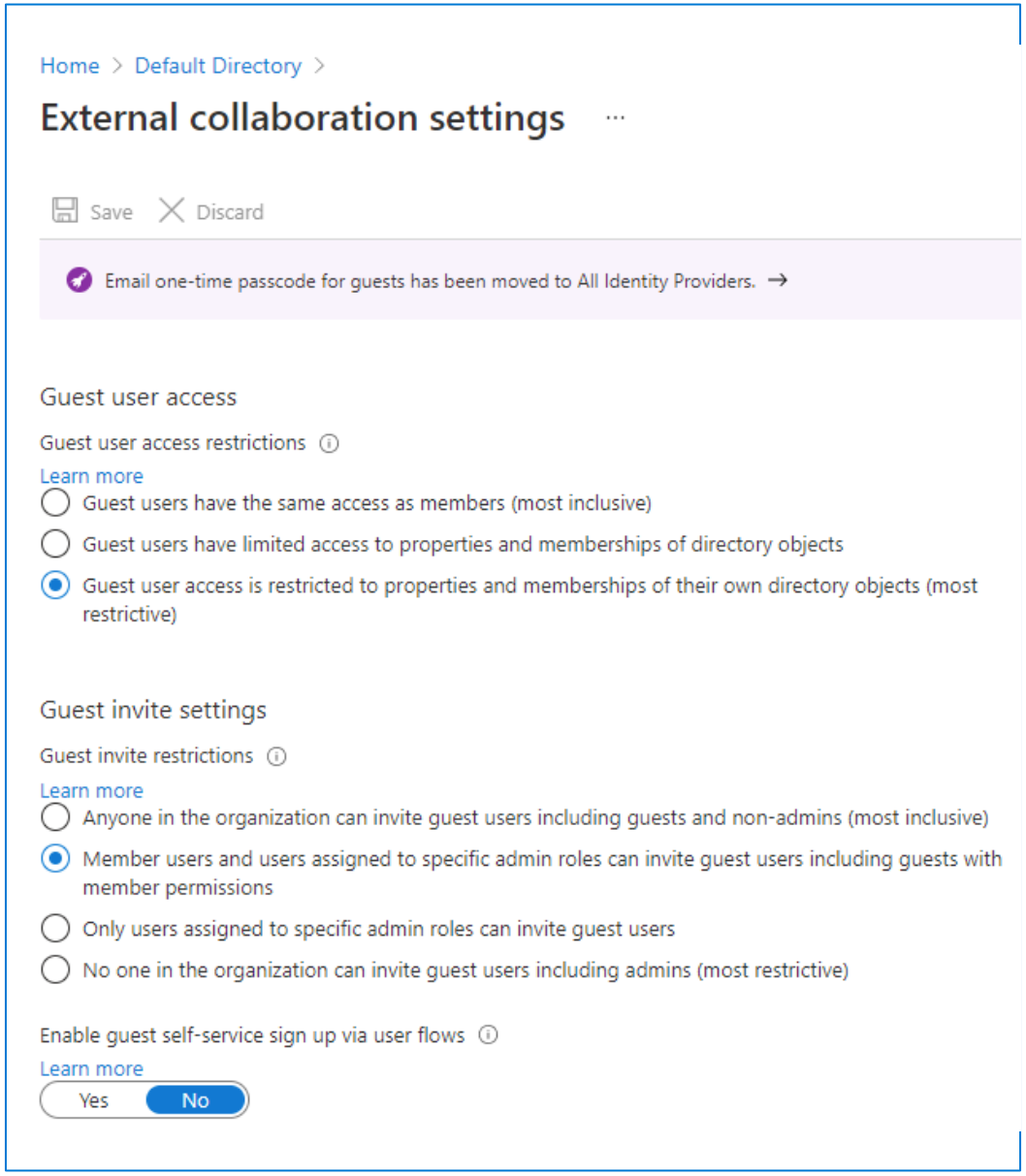
- App registrations – users can register applications
- Administration portal – restrict access to the Azure AD administration portal
- LinkedIn account connections – Allow users to connect their work or school account with LinkedIn
- Other



User settings – External Users

Azure Portal → Azure AD → Users → User Settings

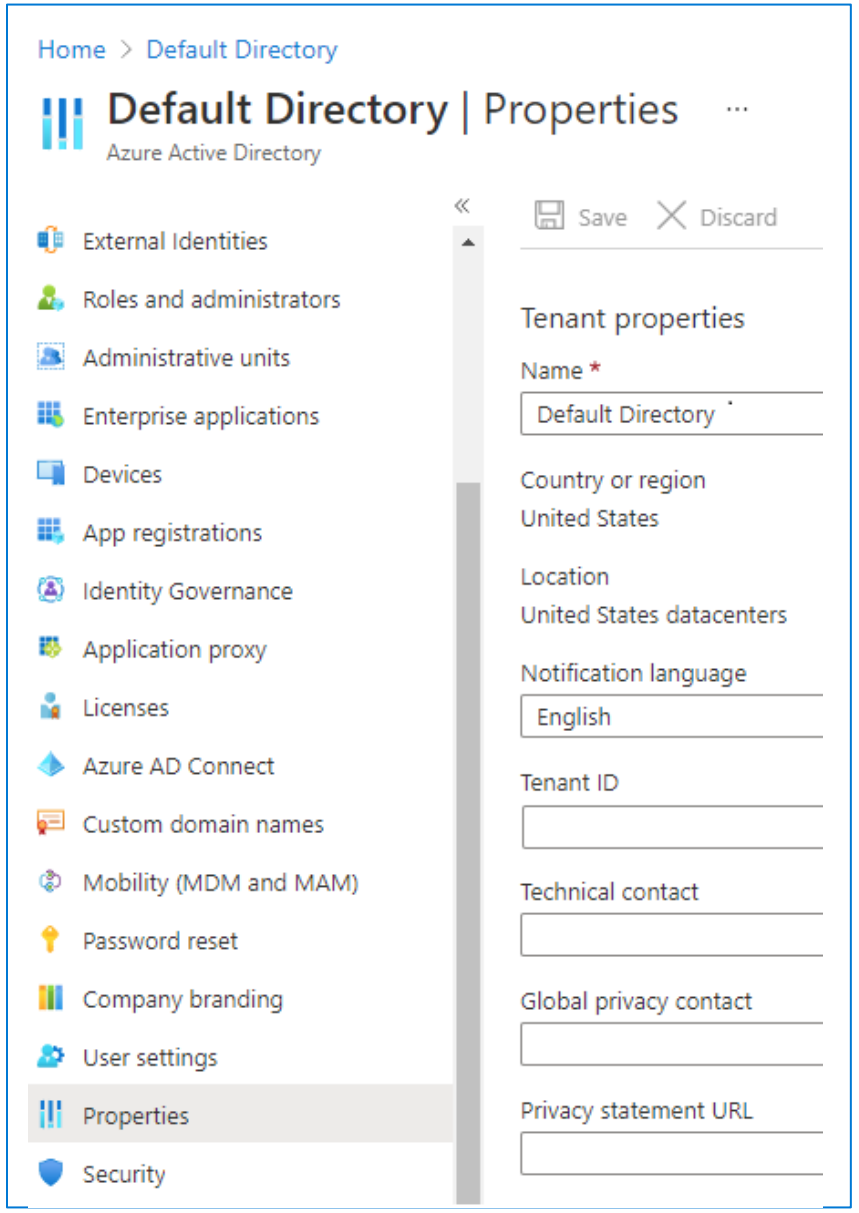
- App registrations – users can register applications
- Administration portal – restrict access to the Azure AD administration portal
- LinkedIn account connections – Allow users to connect their work or school account with LinkedIn
- Manage user feature previews
- External Collaboration setting



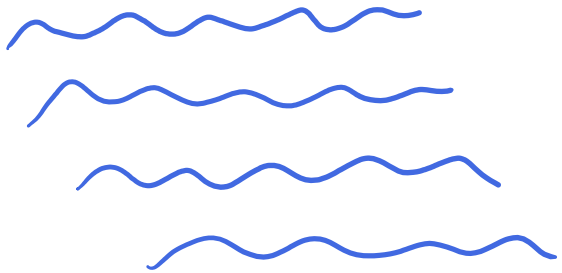
Tenant properties

Azure Portal → Azure AD → Properties

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



Microsoft Security



Implement and manage external identities

Guest B2B Firma - Firma
MS Account
Social media

Tenant B2C App

B2E Firma

Objectives

Describe guest users and B2B Accounts

Manage external collaboration

How external users are managed in Microsoft 365

Invite external users – individually or in bulk

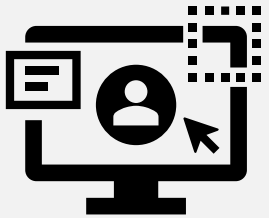
Manage external user accounts in Azure Active Directory

Implement cross-tenant access controls

Configure identity providers

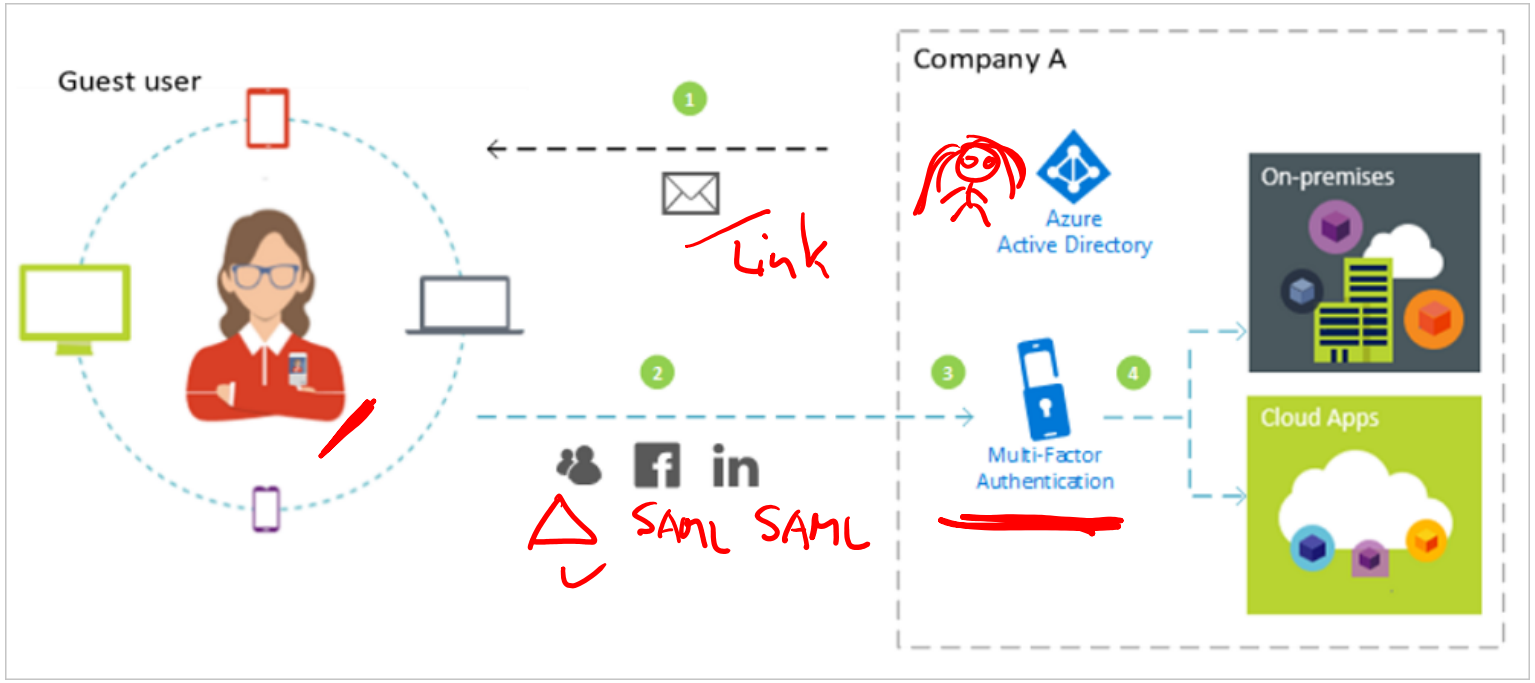
Implement and manage Verified ID

Describe guest user and B2B accounts
&
Manage external collaboration



Azure Active Directory B2B

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



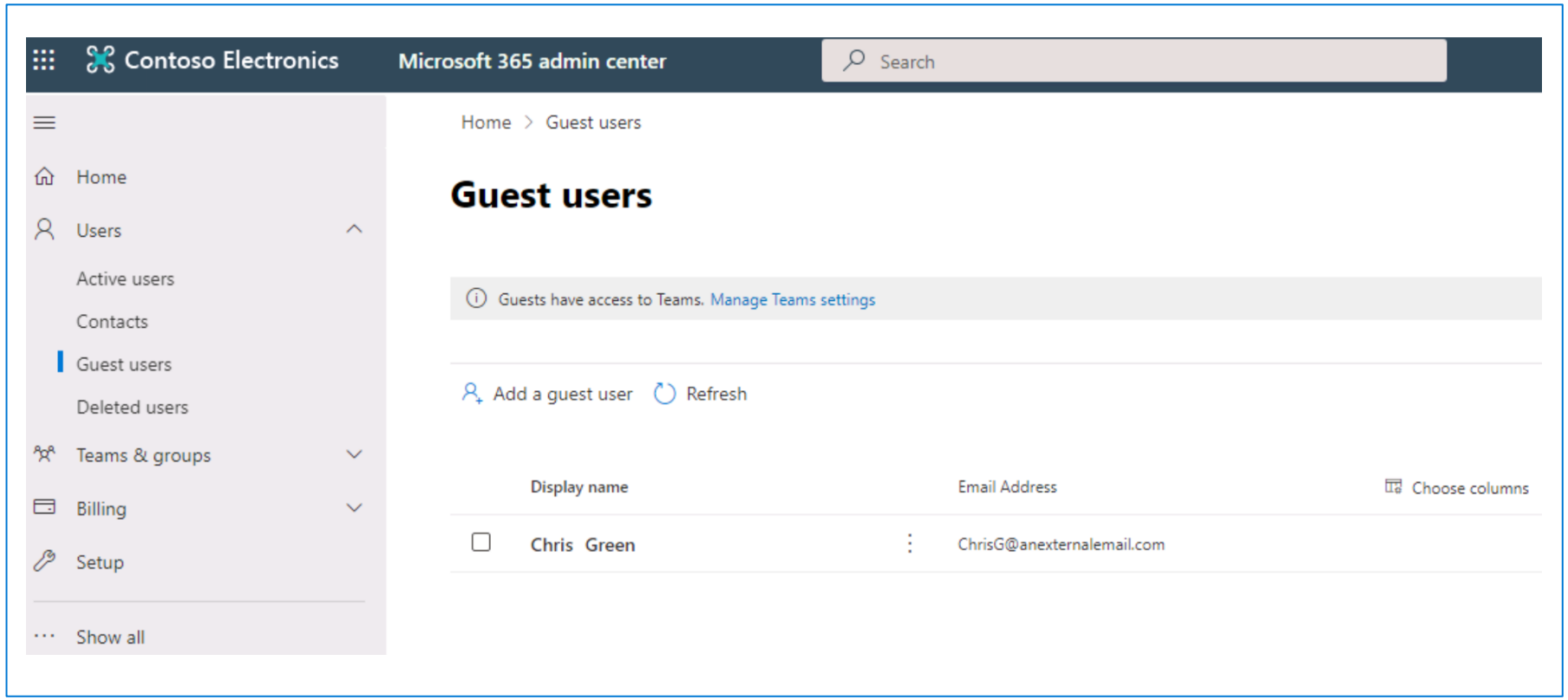
Collaborating with external users

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

External users from M365 Workloads

Microsoft 365 admin center

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

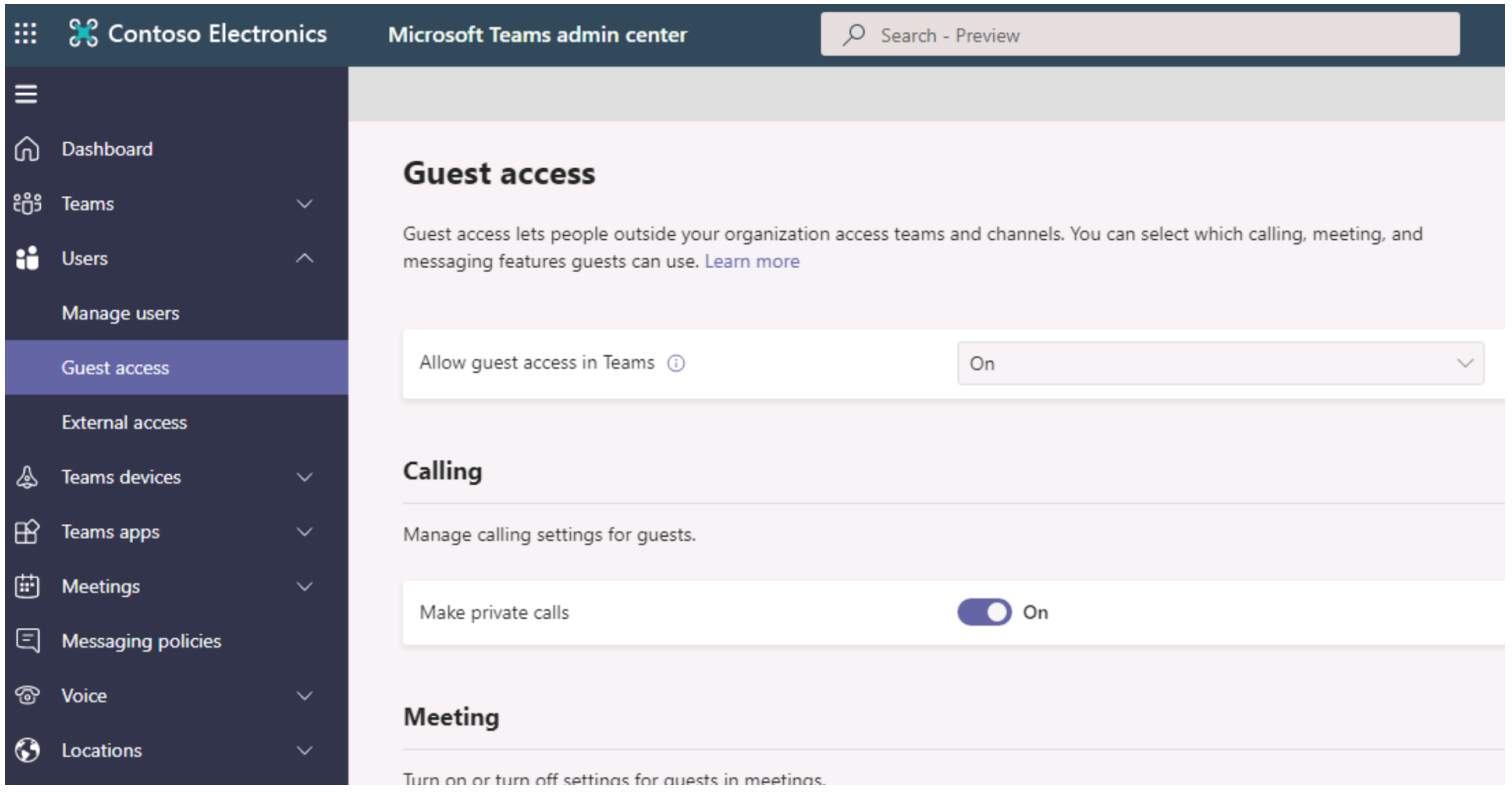


External collaboration options in Microsoft 365

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

Granting / removing guest access

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



Invite external users – individually or in bulk

Inviting users

Inviting users individually:

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

Inviting users in bulk:

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

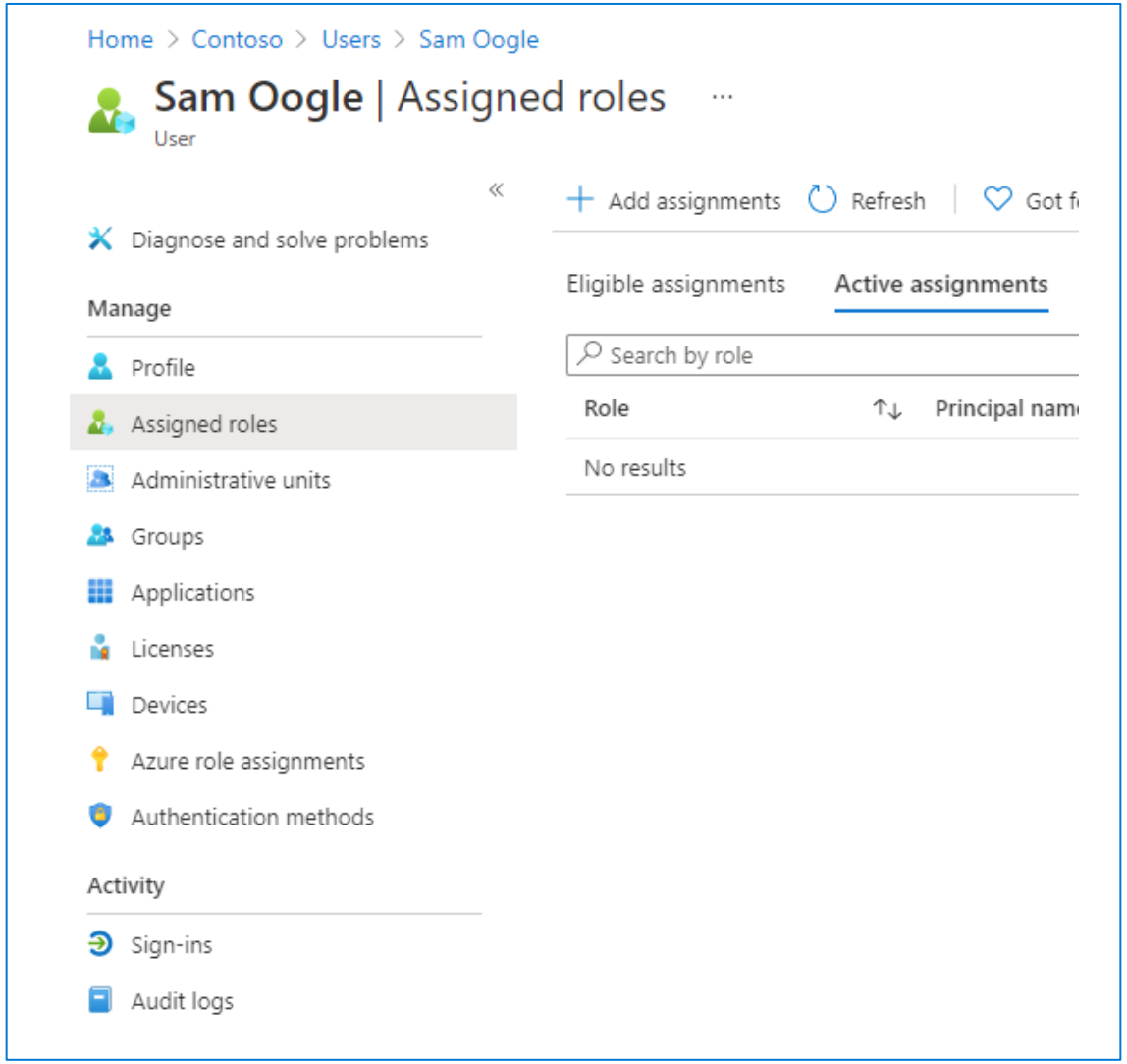
Manage external user accounts in Azure Active Directory

Guest Users – restricted by default

Guest users do not have:

- Assigned roles
- Group membership
- Licenses

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

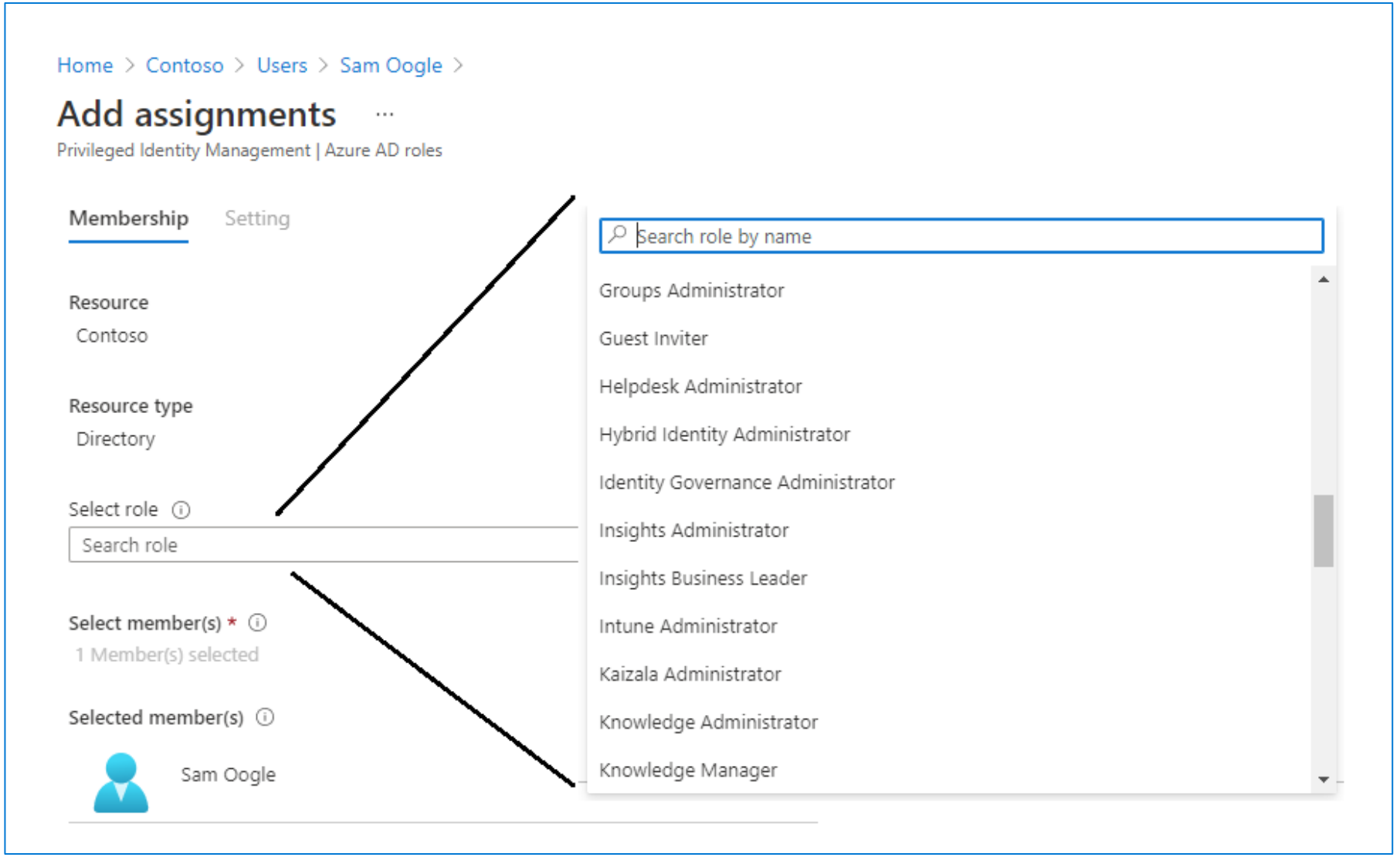


Provide the Guest User the least privilege access needed

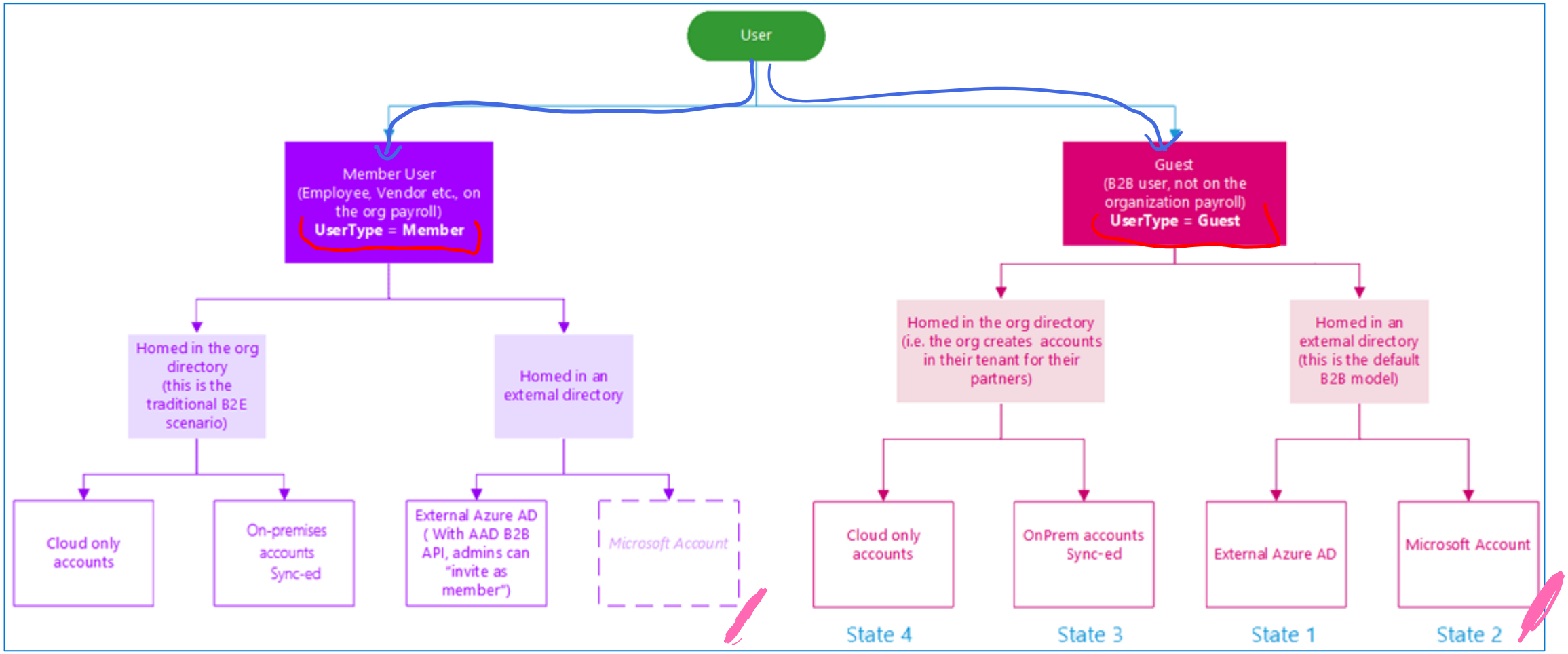
Add guest to:

- "Assign Roles" just as with normal users.

You can add Guests to groups as well.



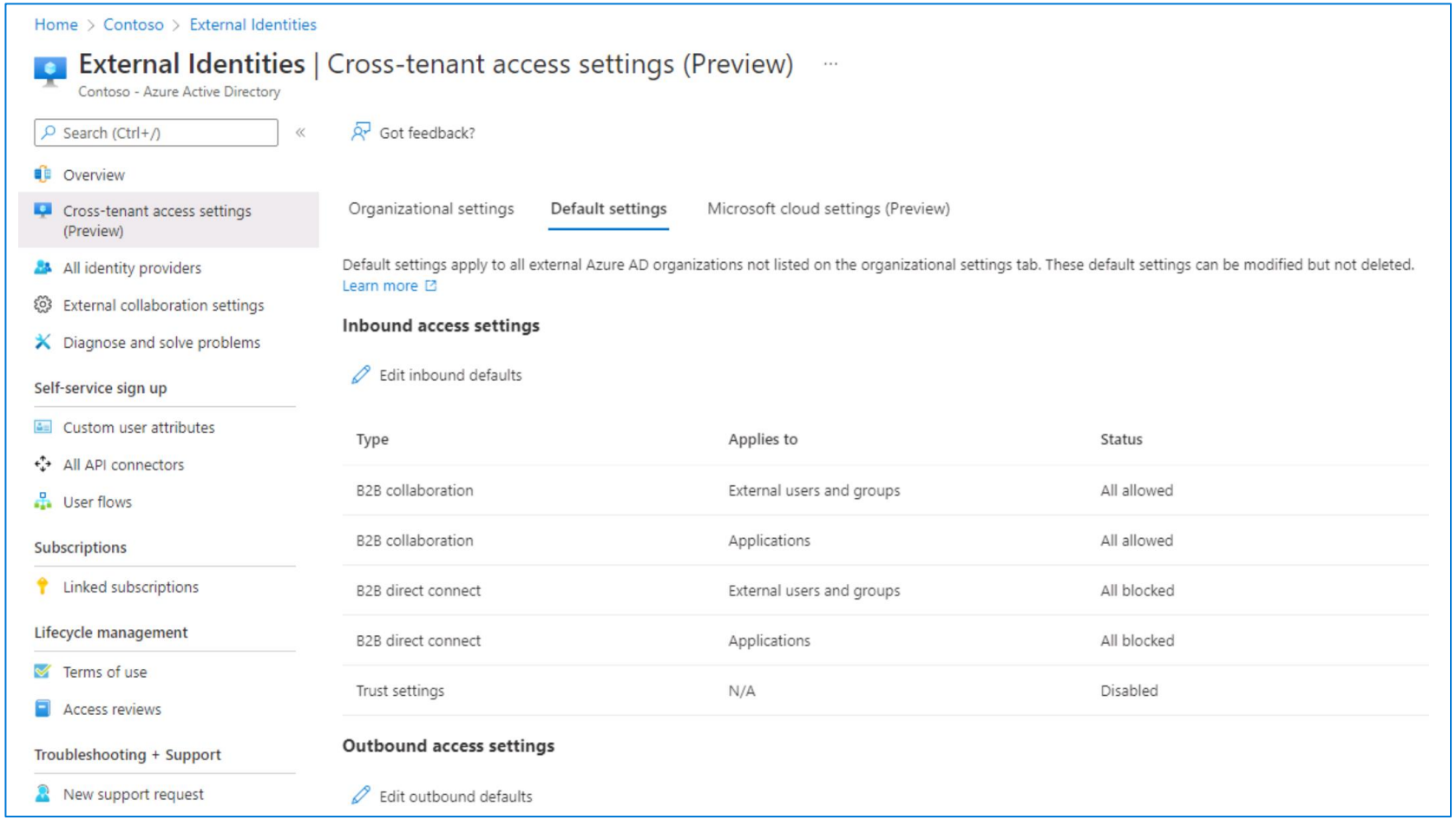
B2B user states



Cross-tenant access controls

Configure cross-tenant access controls

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

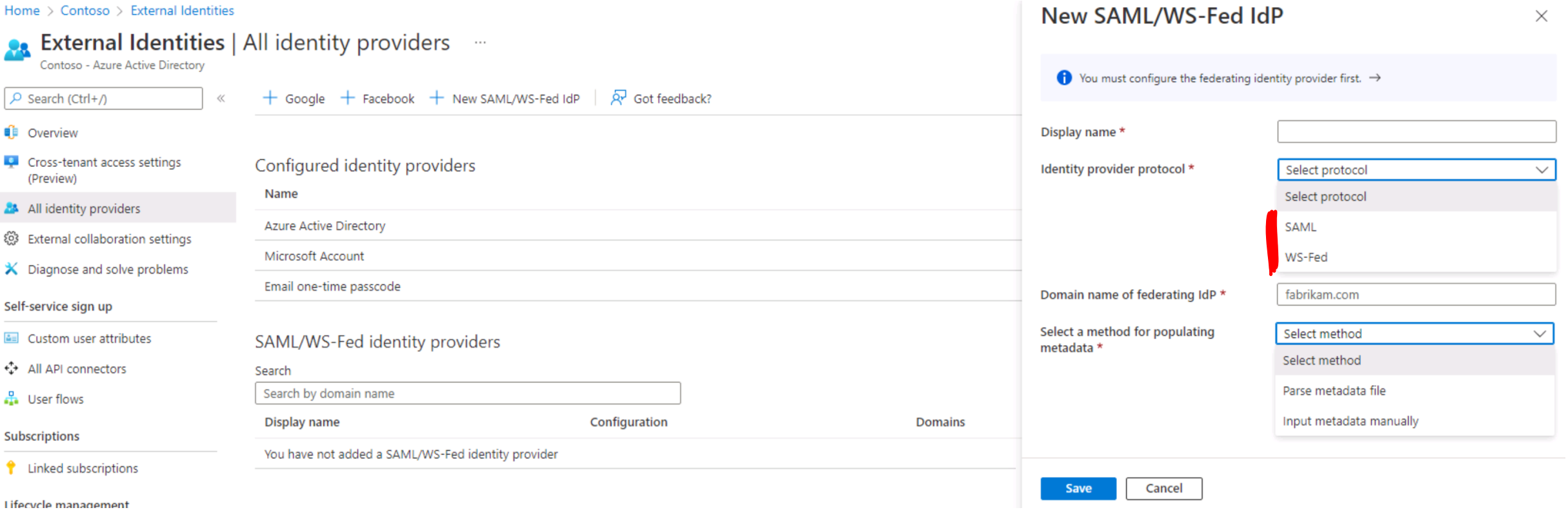


Configure identity providers

SAML / WS-Fed

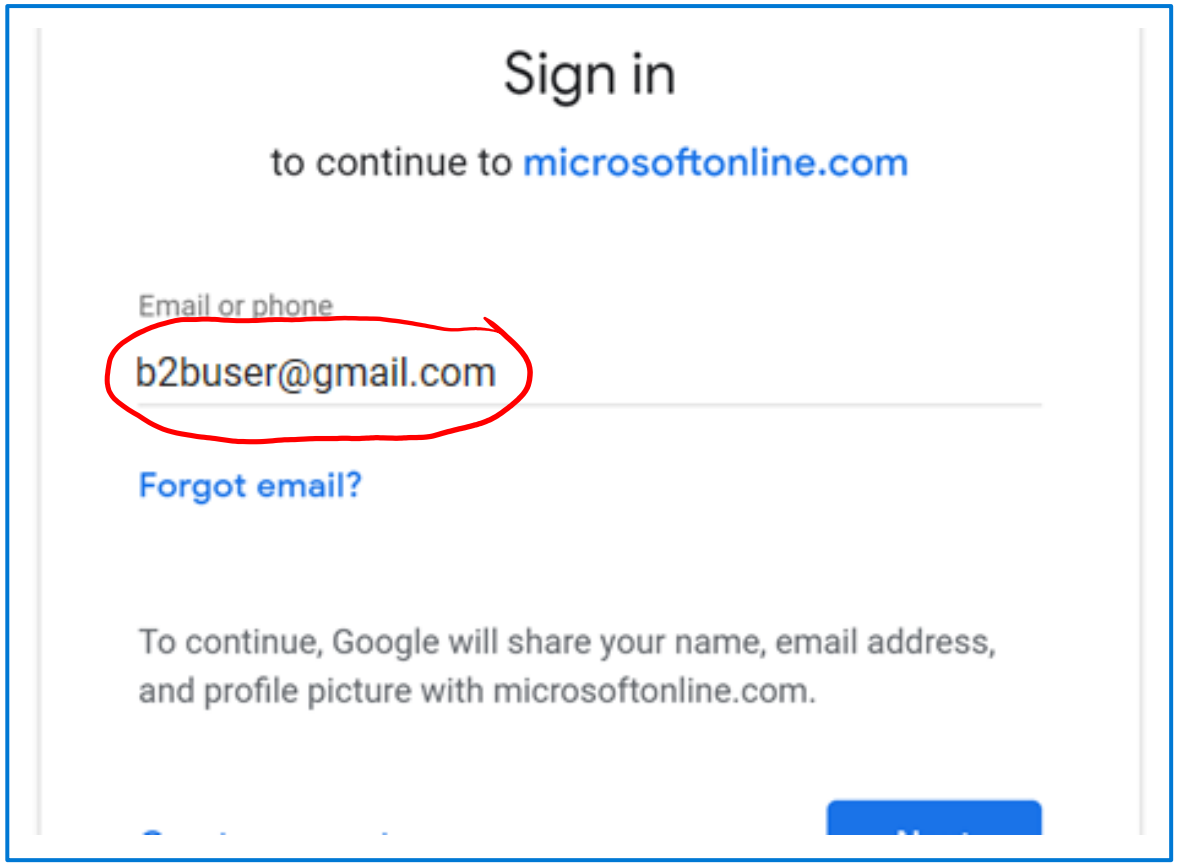
- You can set up direct federation with any organization that supports SAML 2.0 or WS-Fed
- Any new guests will be authenticated using direct federation
- Guest users sign in using their own organizational account

SAML / WS-Fed identity provider configuration



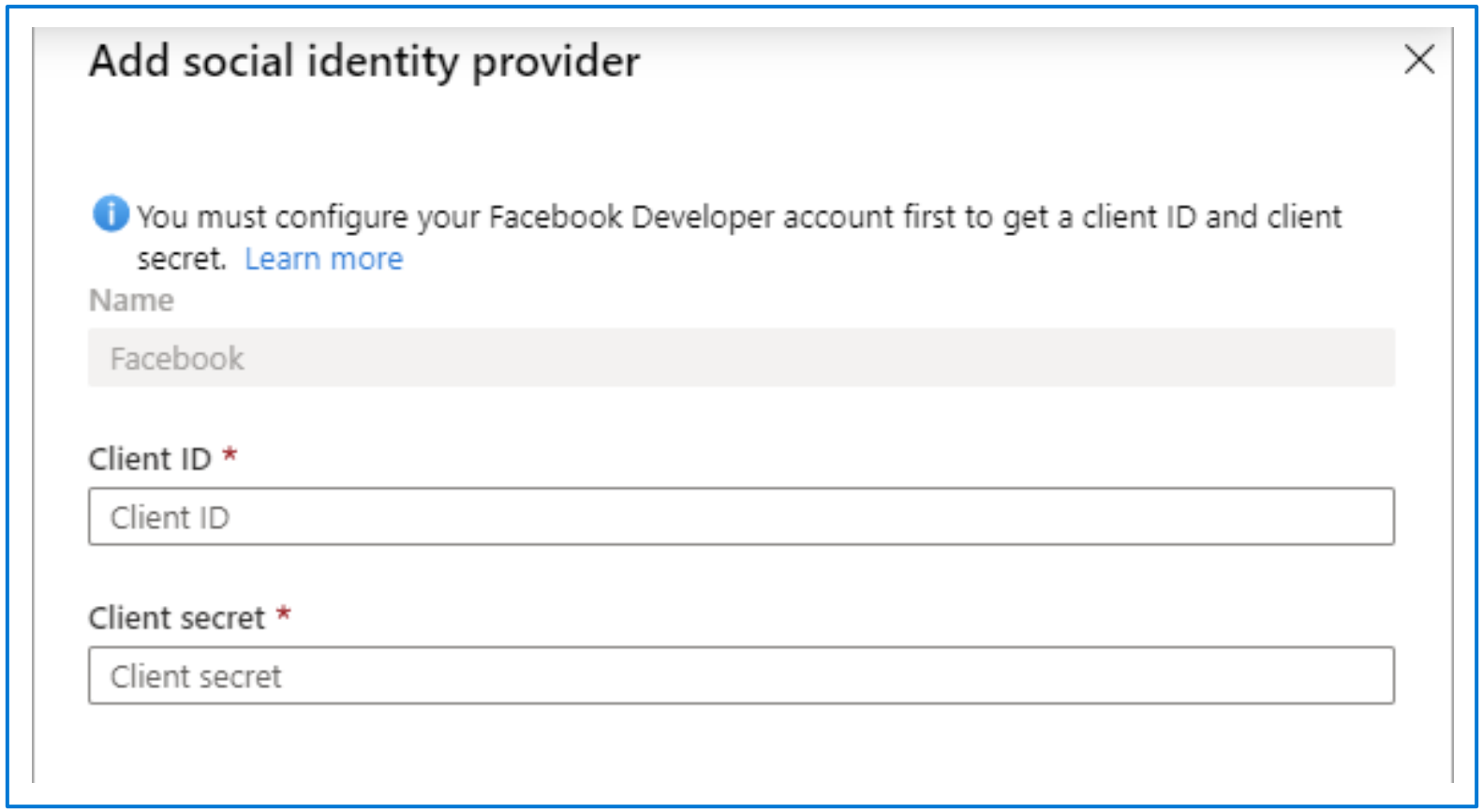
Using Google as an identity provider

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



Using Facebook as an identity provider

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



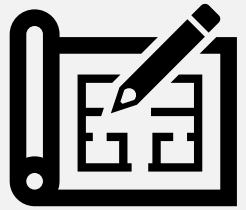
Microsoft Security

Implement and manage hybrid identity

Objectives

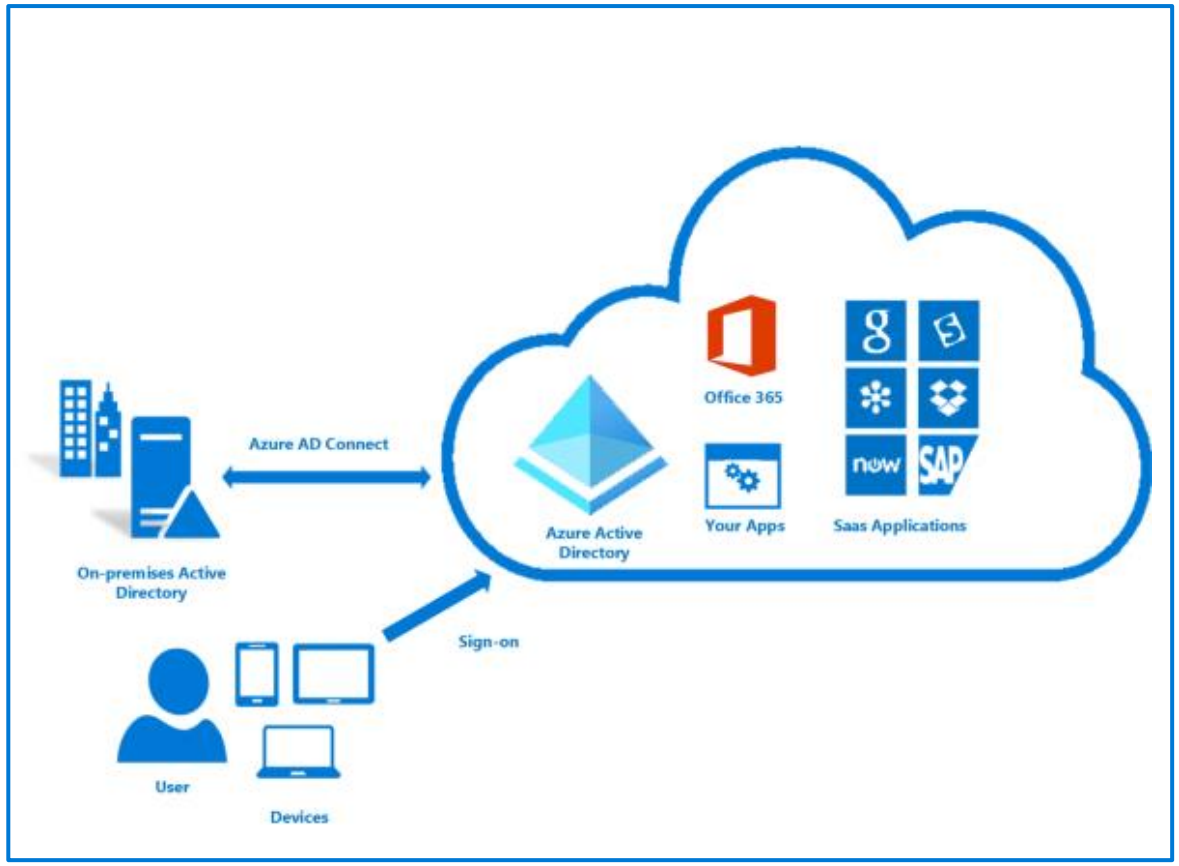
- Plan, design, and implement Azure Active Directory Connect (AADC)
- Implement and manage password hash synchronization (PHS)
- Implement and manage pass-through authentication (PTA)
- Implement and manage federation
- Troubleshoot synchronization errors
- Implement Azure Active Directory Connect Health
- Manage Azure Active Directory Connect Health

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

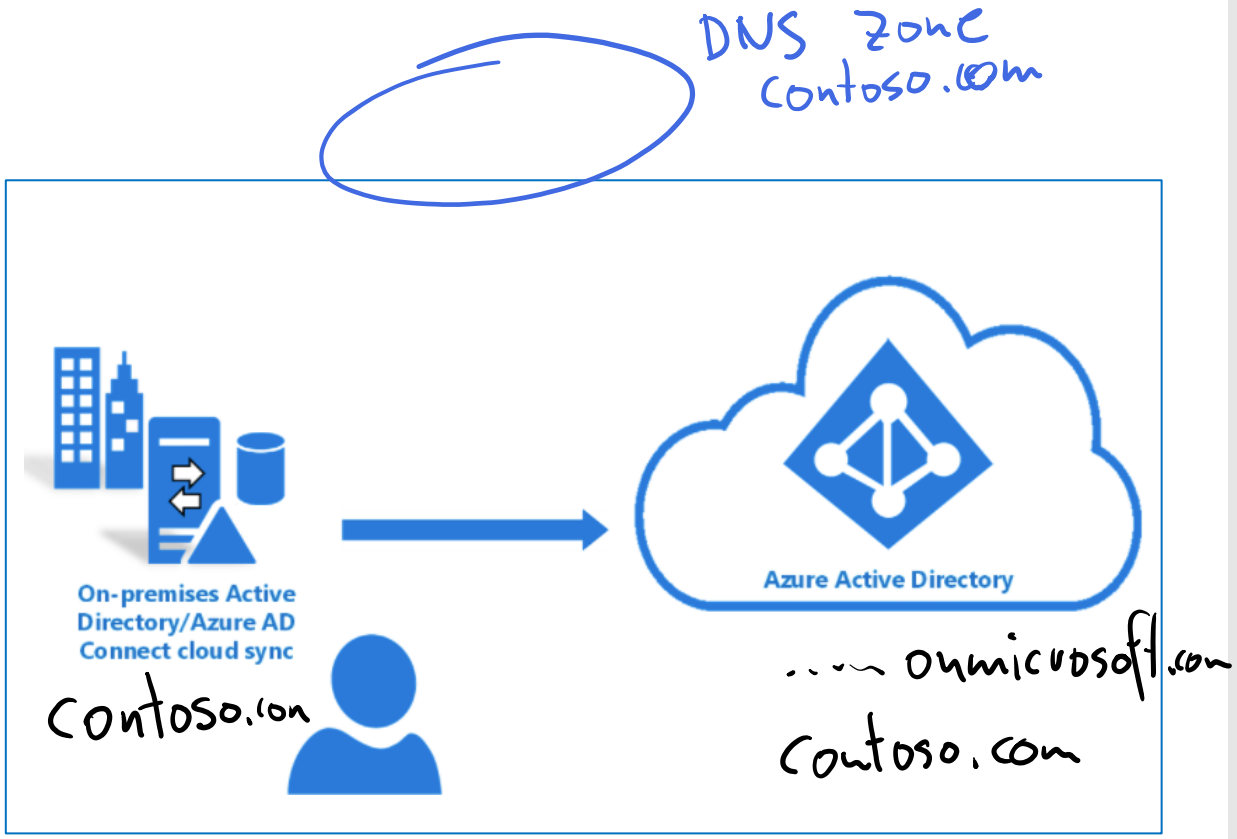


What is Azure Active Directory Connect?

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



Azure AD Connect cloud sync

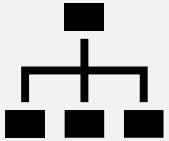


- Azure AD Connect cloud sync is a solution syncs your on-premises AD with Azure AD
- Lightweight provisioning agent required on the on-premises AD
- All sync configuration is managed in the cloud
- Can be used in conjunction with Azure AD Connect

Authentication methods

Cloud authentication

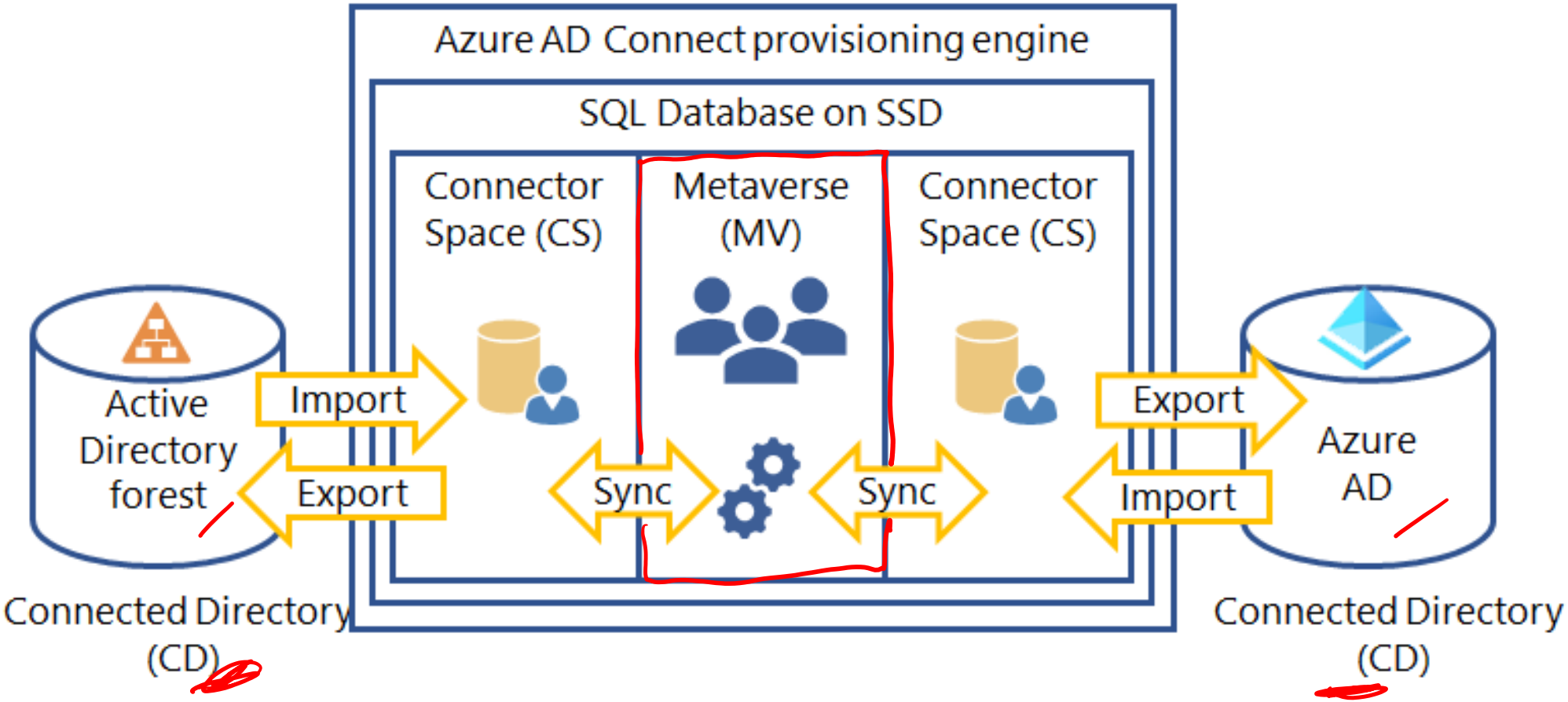
- **Azure AD password hash synchronization (PHS)**
  - Users can use the same username and password that they use on premises
- **Azure AD pass-through authentication (PTA)**
  - Simple password validation for Azure AD authentication services using a software agent that runs on one or more on-premises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



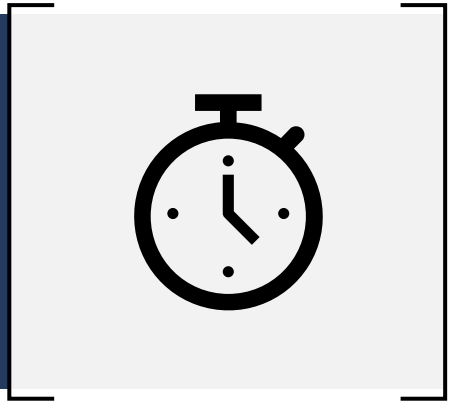
Federated authentication

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

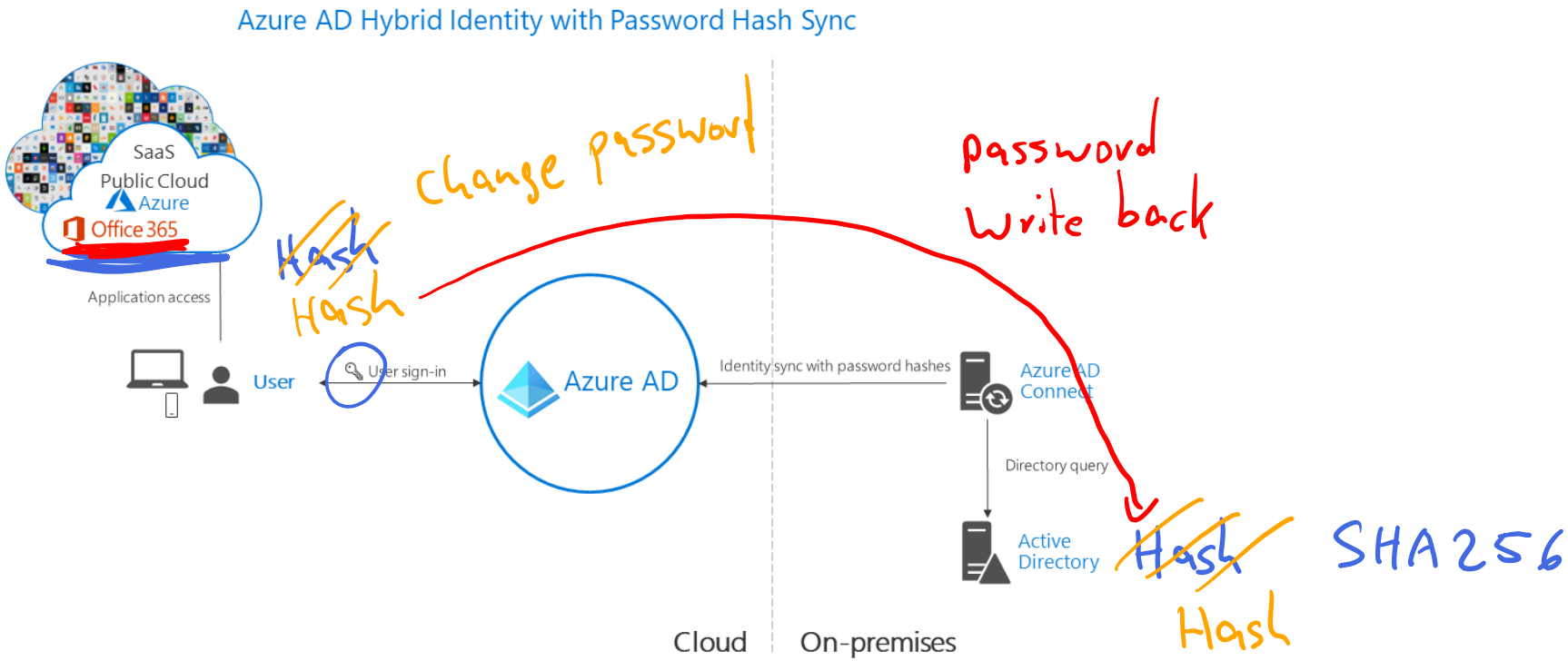
Azure AD Connect component factors



Implement and manage password hash synchronization (PHS)

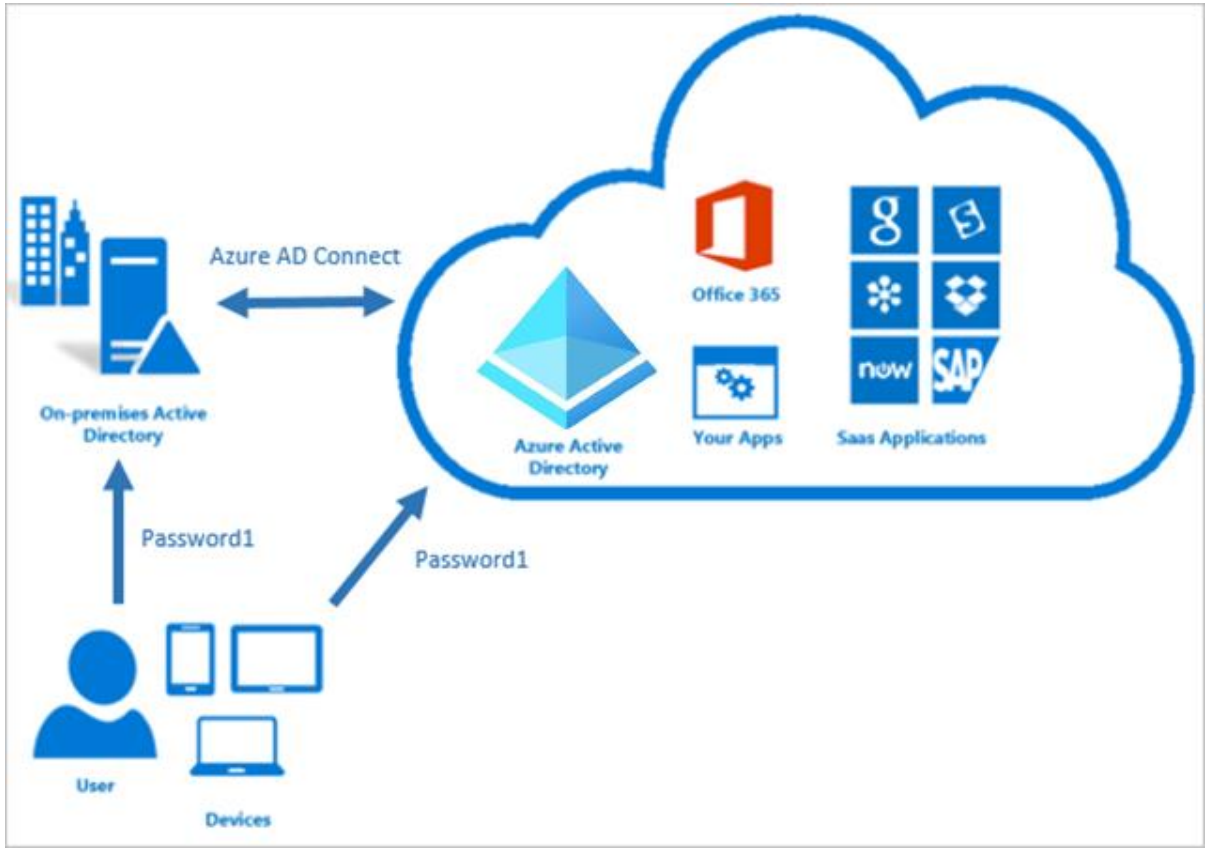


Password hash sync

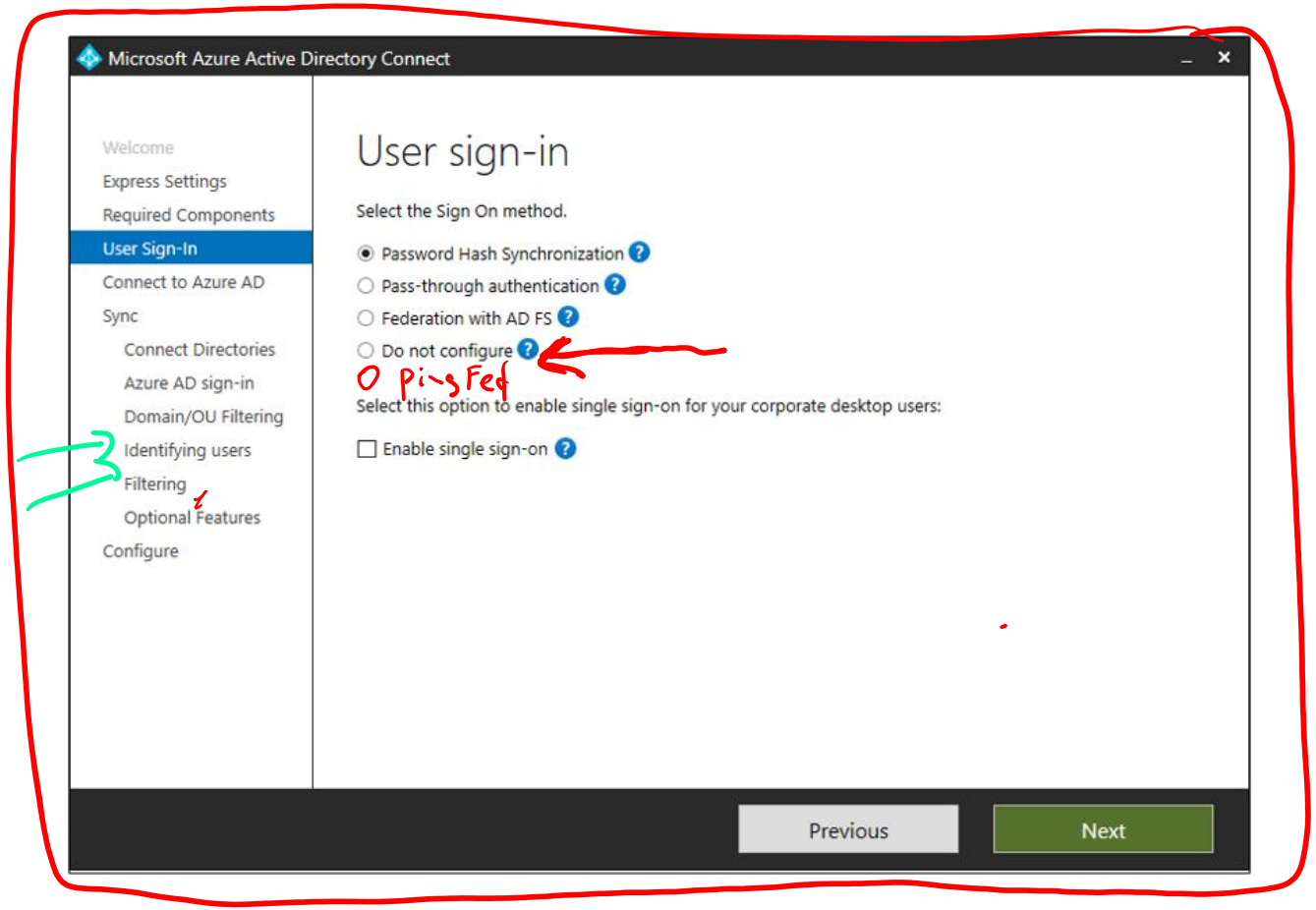


Simplicity of a password hash synchronization solution

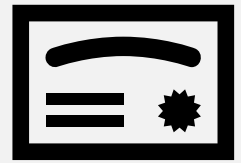
How password hash synchronization works



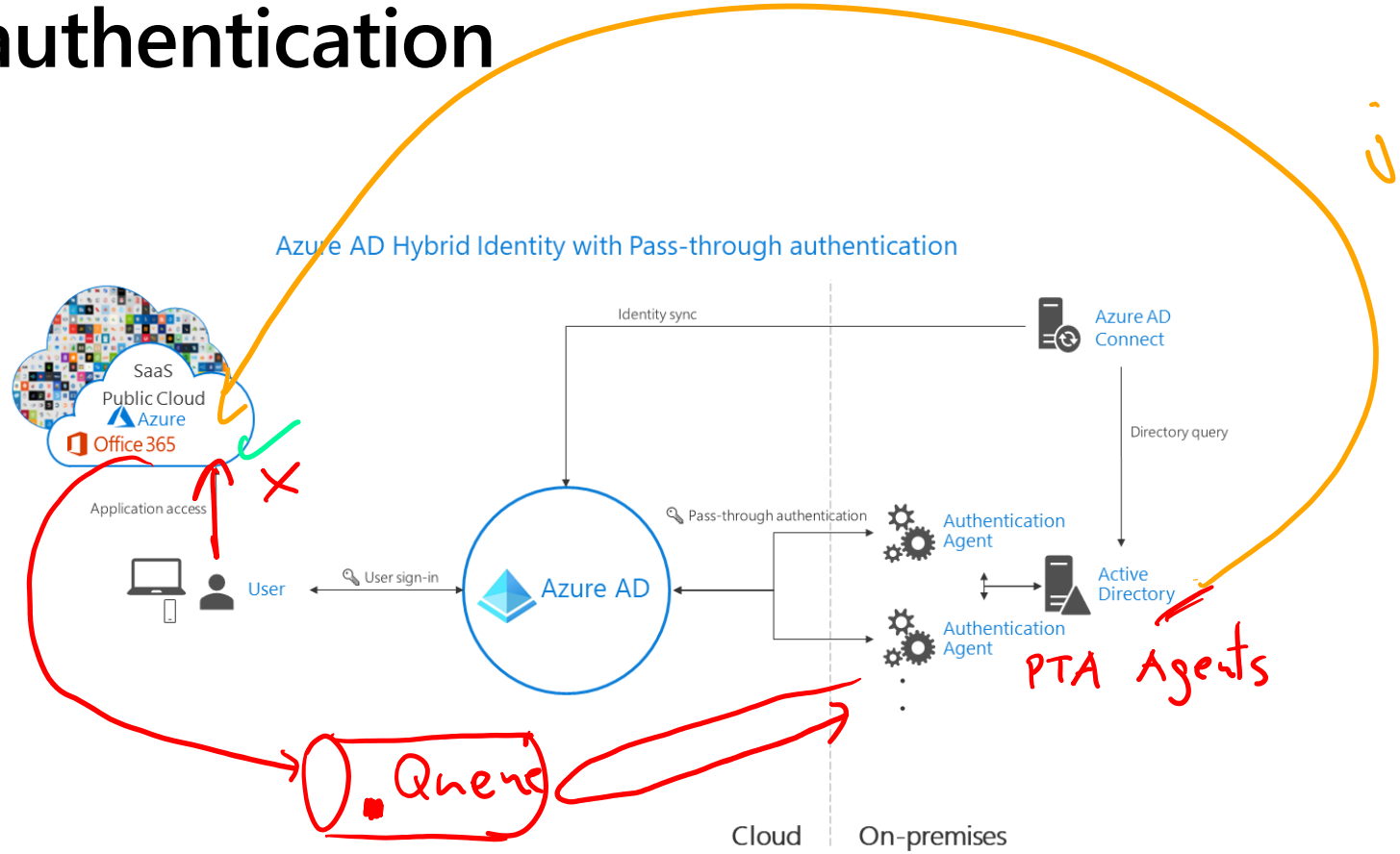
Enable password hash synchronization



Implement and manage pass-through authentication (PTA)

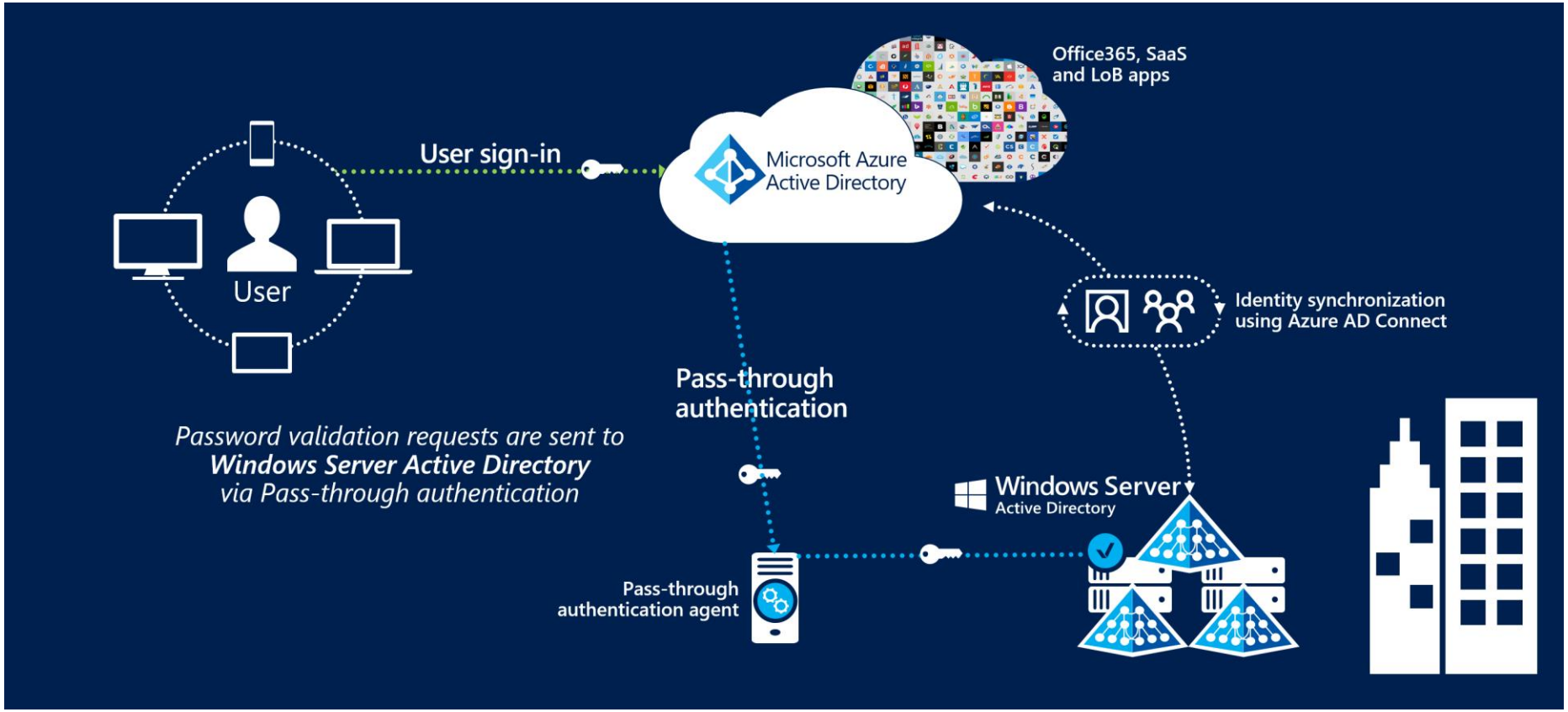


Pass-through authentication

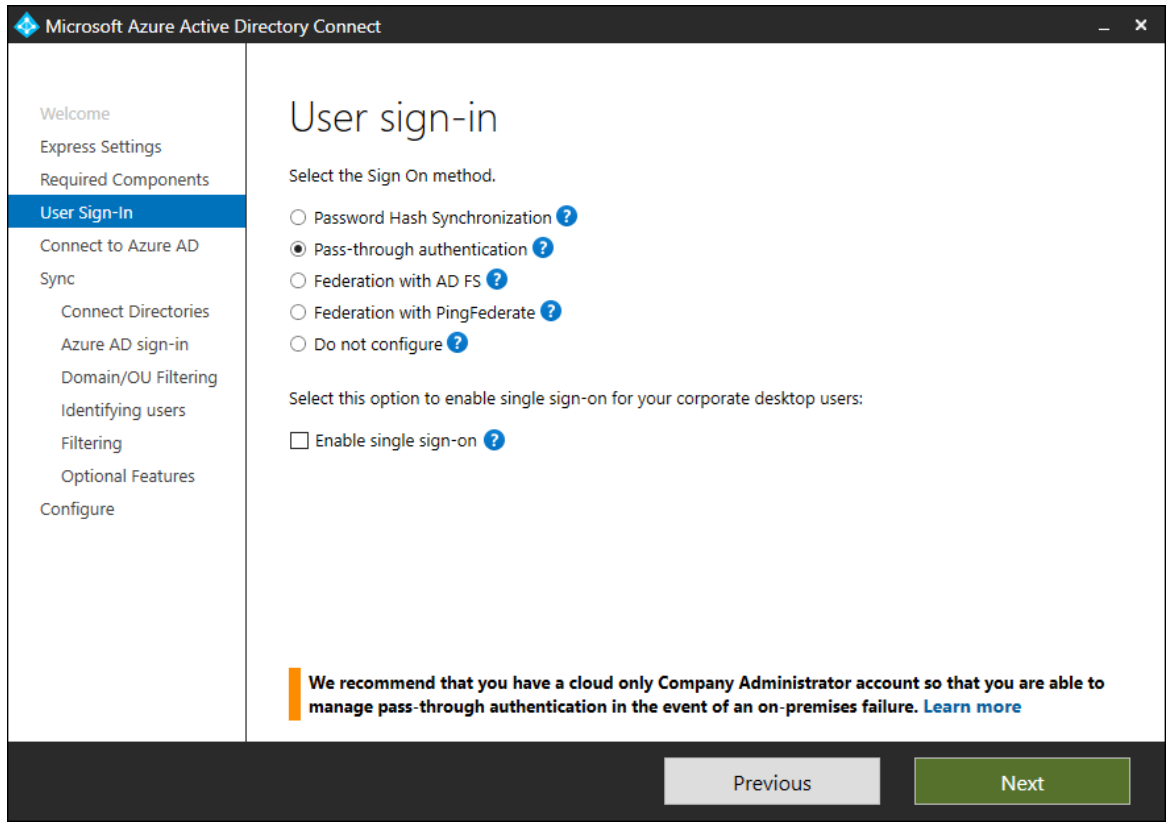


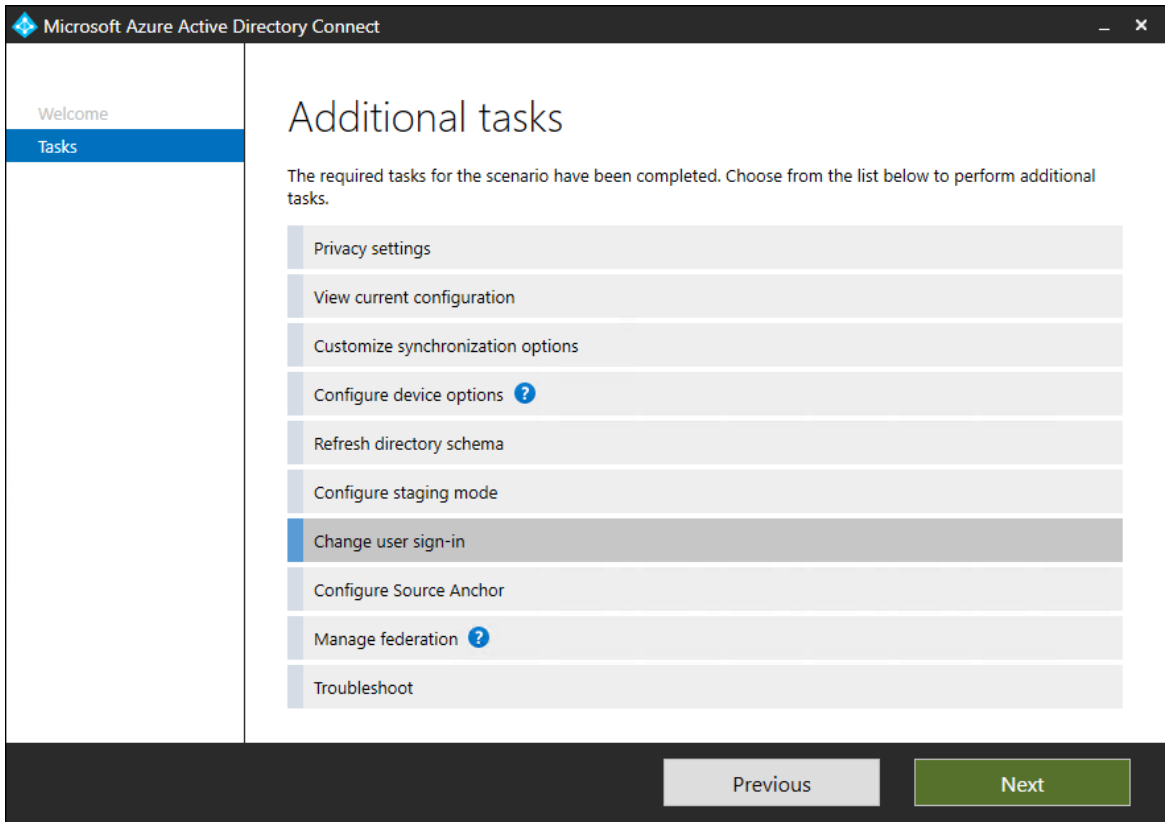
Agent requirements of pass-through authentication, using two agents for redundancy

How Azure AD Pass-through Authentication works



Enable pass-through authentication

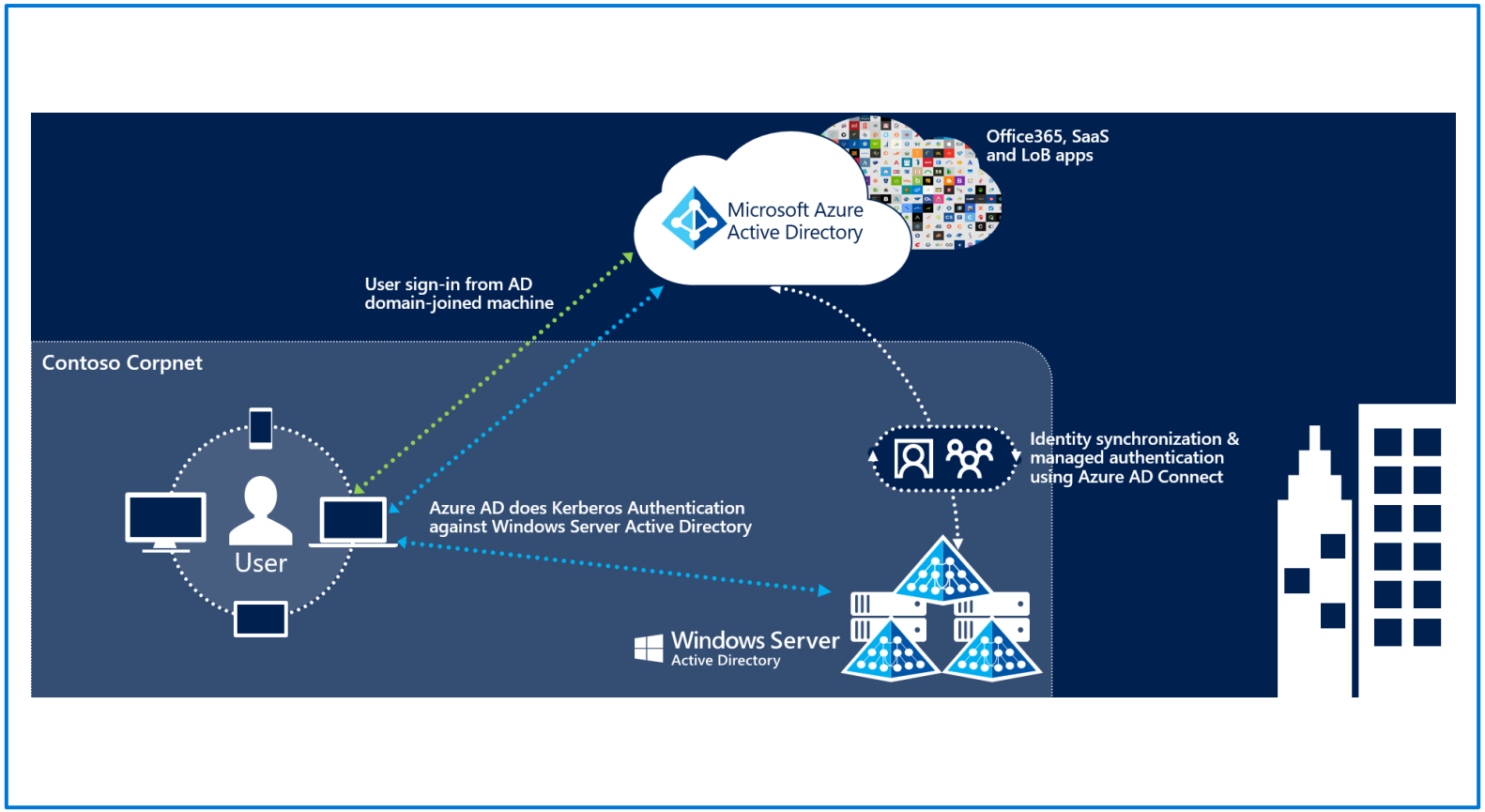




Seamless single sign-on (SSO)

Single Sign-On

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

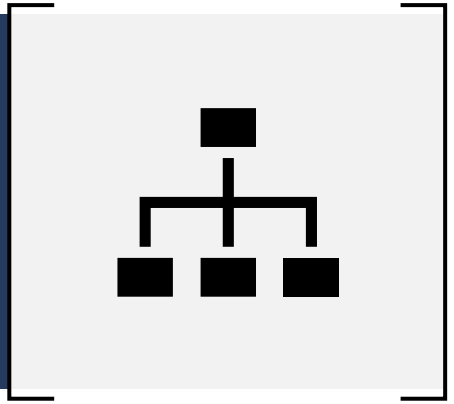


How Seamless SSO is set up

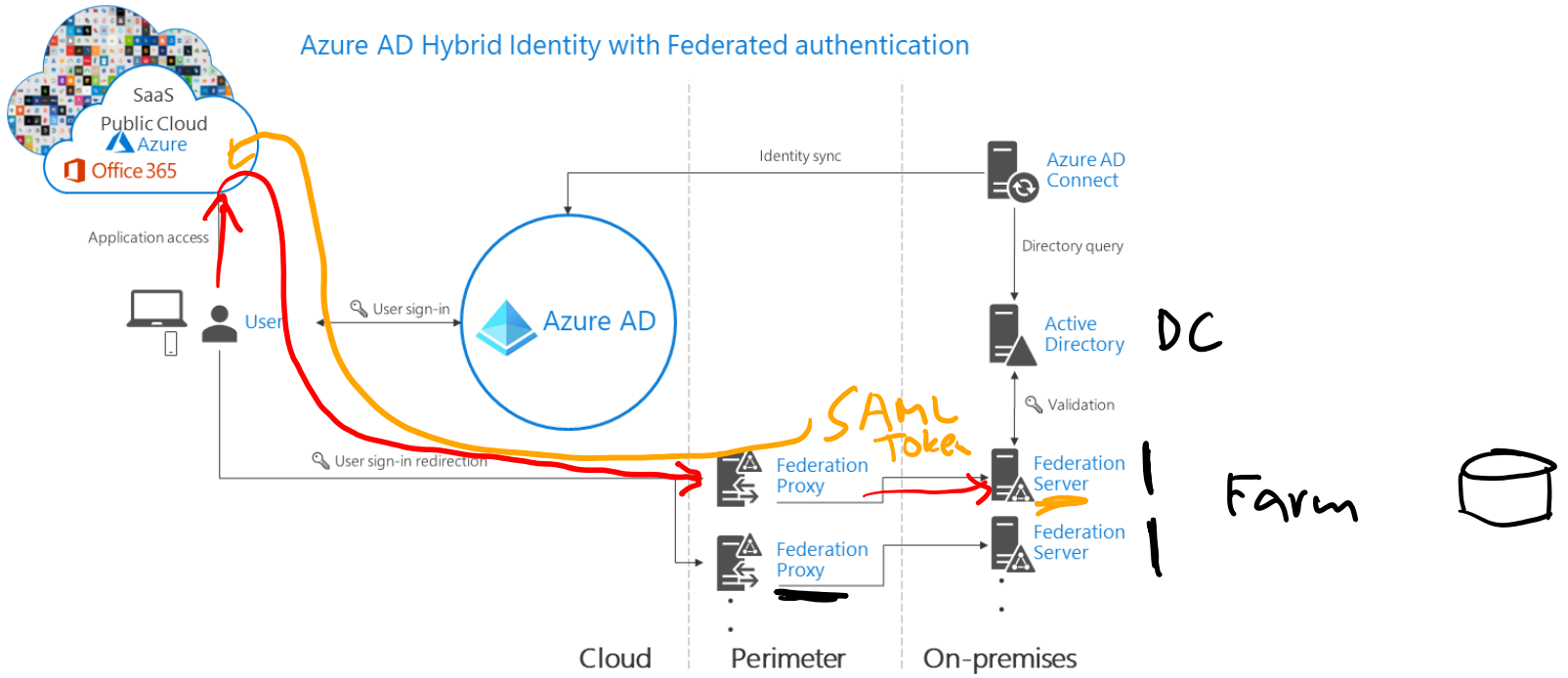
Seamless SSO is enabled using Azure AD Connect. While enabling the SSO, the following steps occur:

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

Implement and manage federation



Federated authentication

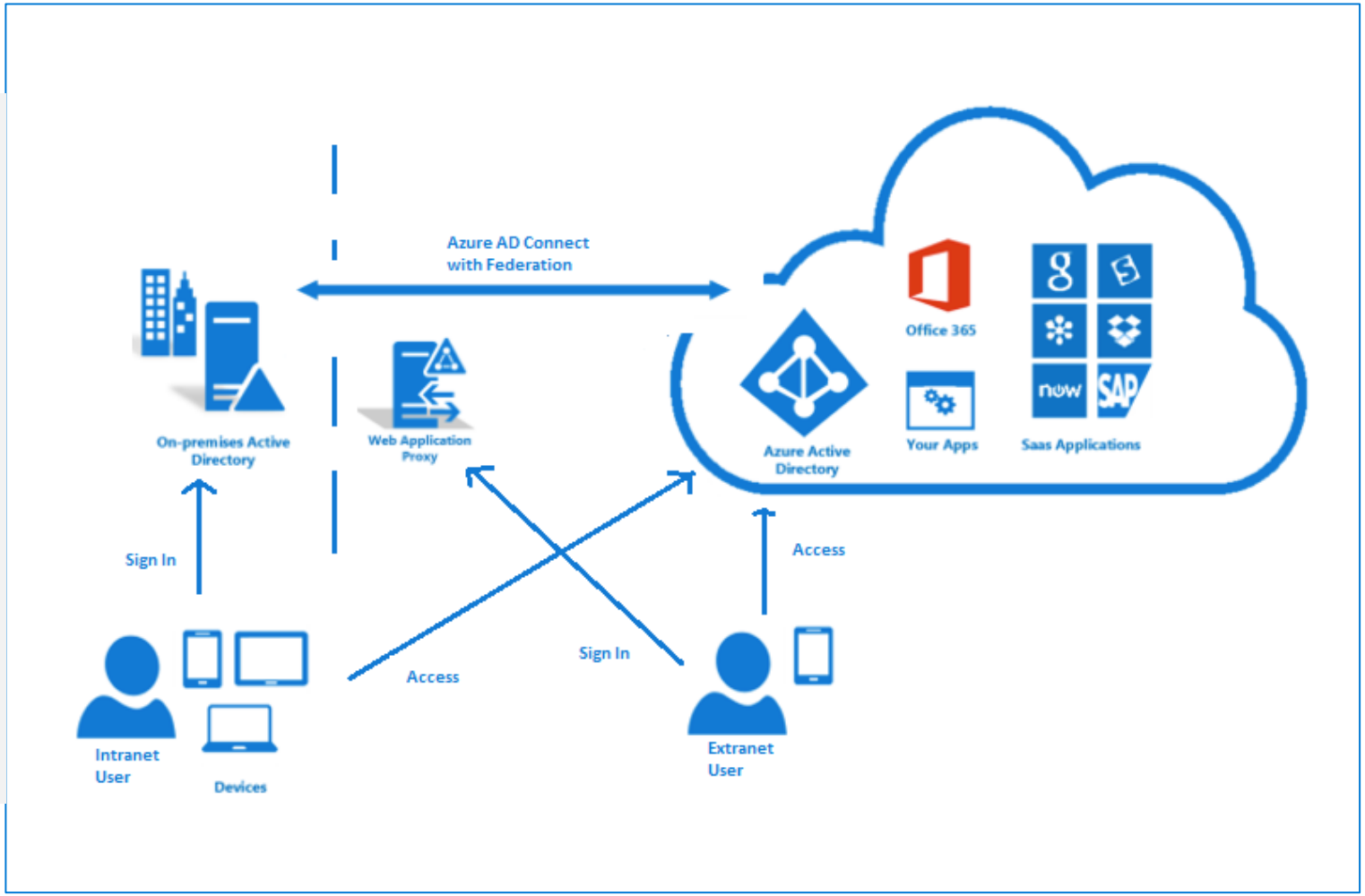


Components required for federation in your perimeter and internal network of your organization

What is federation?

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

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



Deploying a federation with AD FS and Azure AD Connect

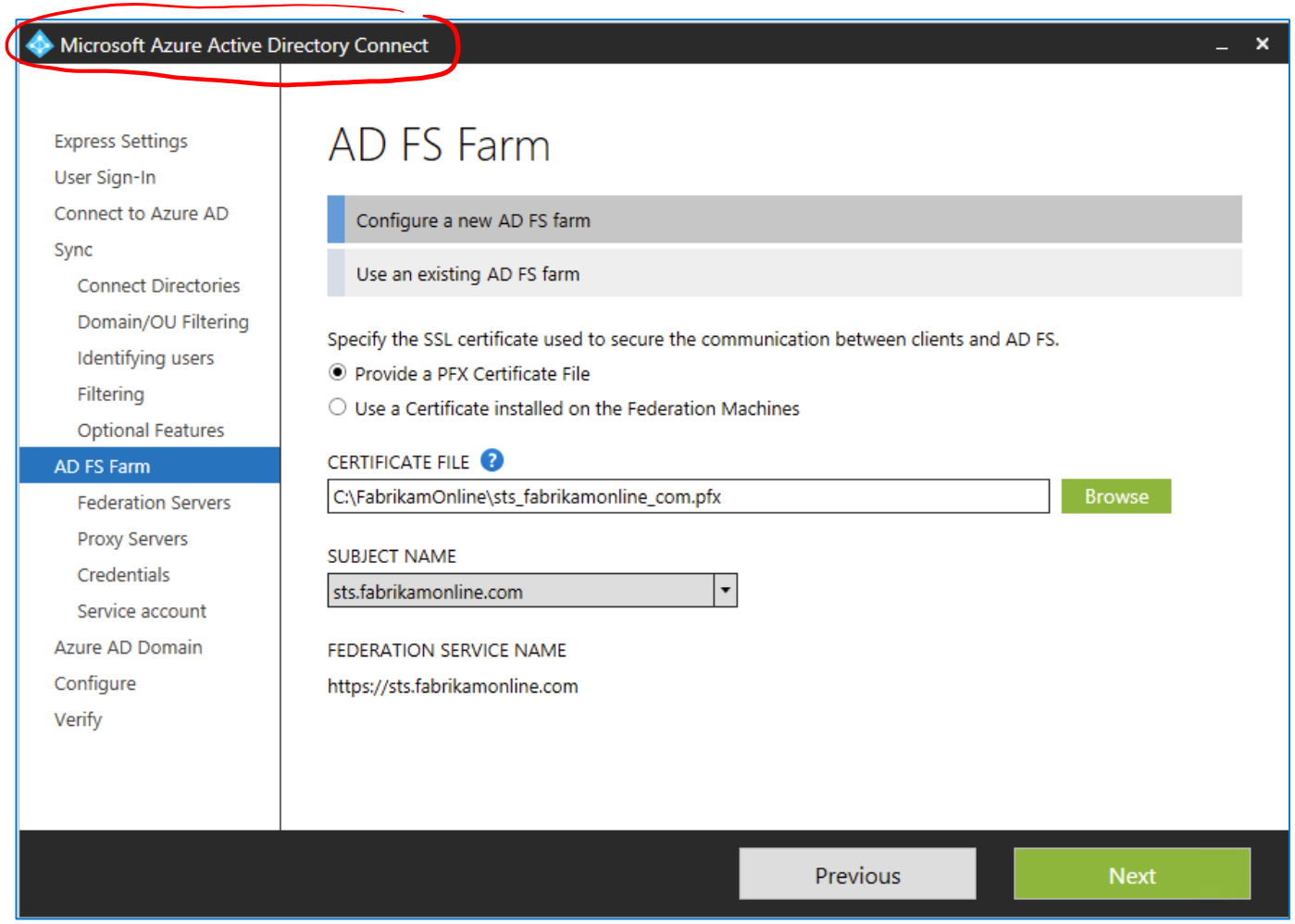
Deploying an AD FS farm, you need:

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

Using Azure AD Connect to connect to an AD FS farm

Primary Steps

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



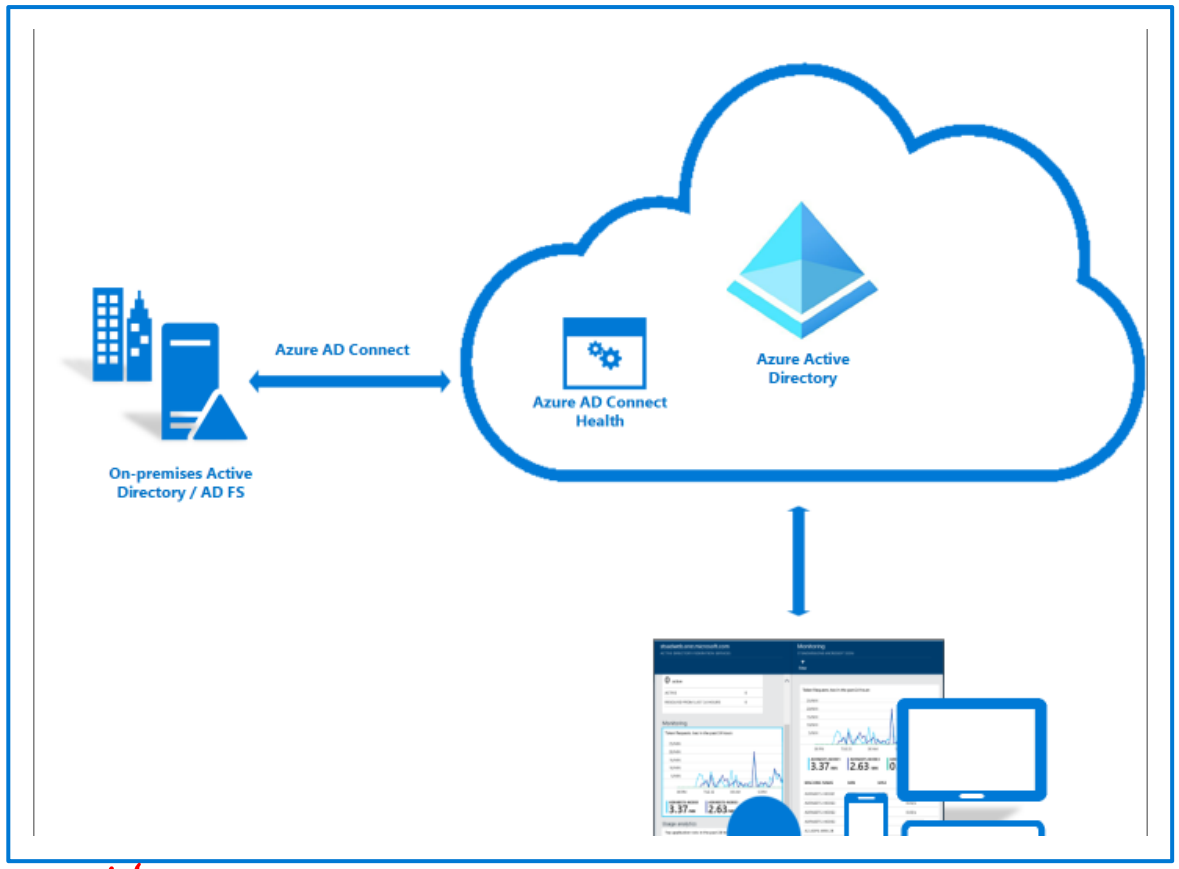
Managing federation with Azure AD Connect

Manage AD FS feature	What it does
Repair the trust	How to repair the federation trust with Microsoft 365.
Federate with Azure AD 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 Azure Active Directory Connect Health

What is Azure Active Directory Connect Health?

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



Start-ADSyncSyncCycle

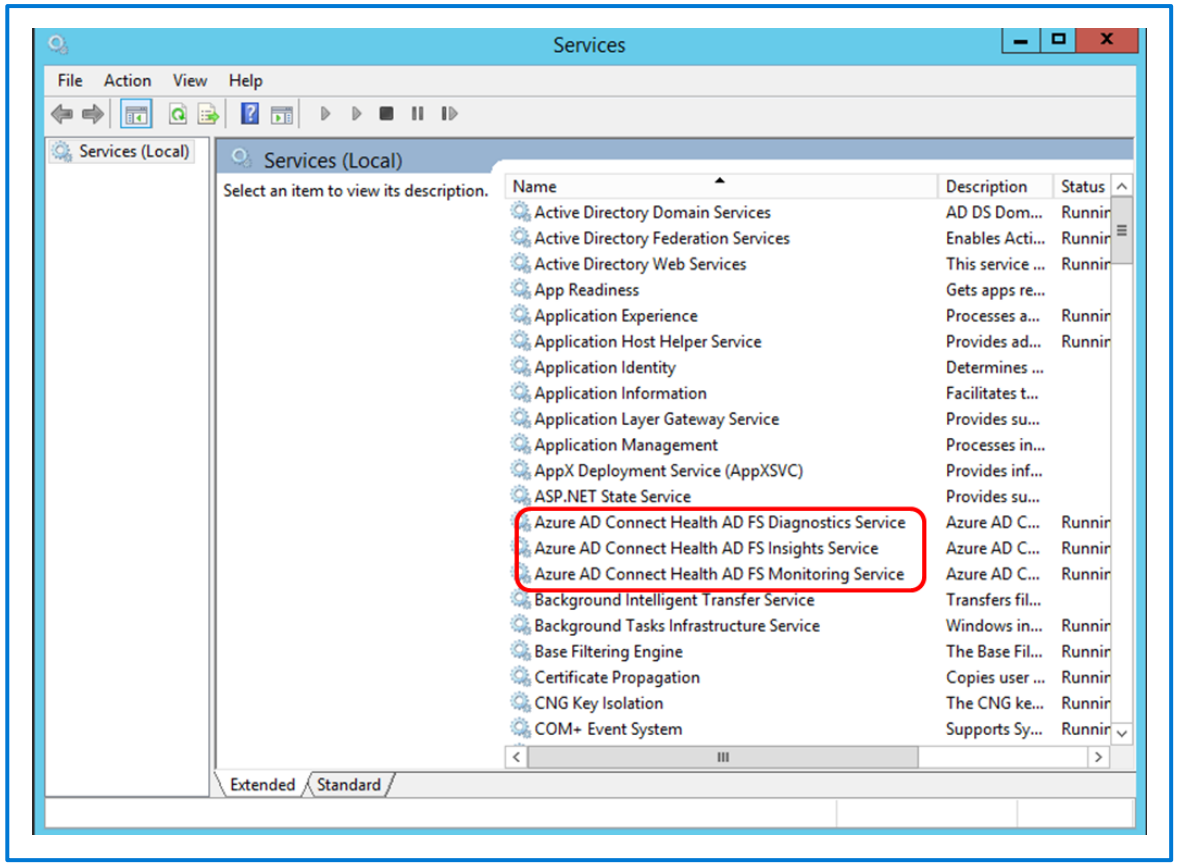
Delta
Full

Considerations for installing Azure AD Connect Health

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

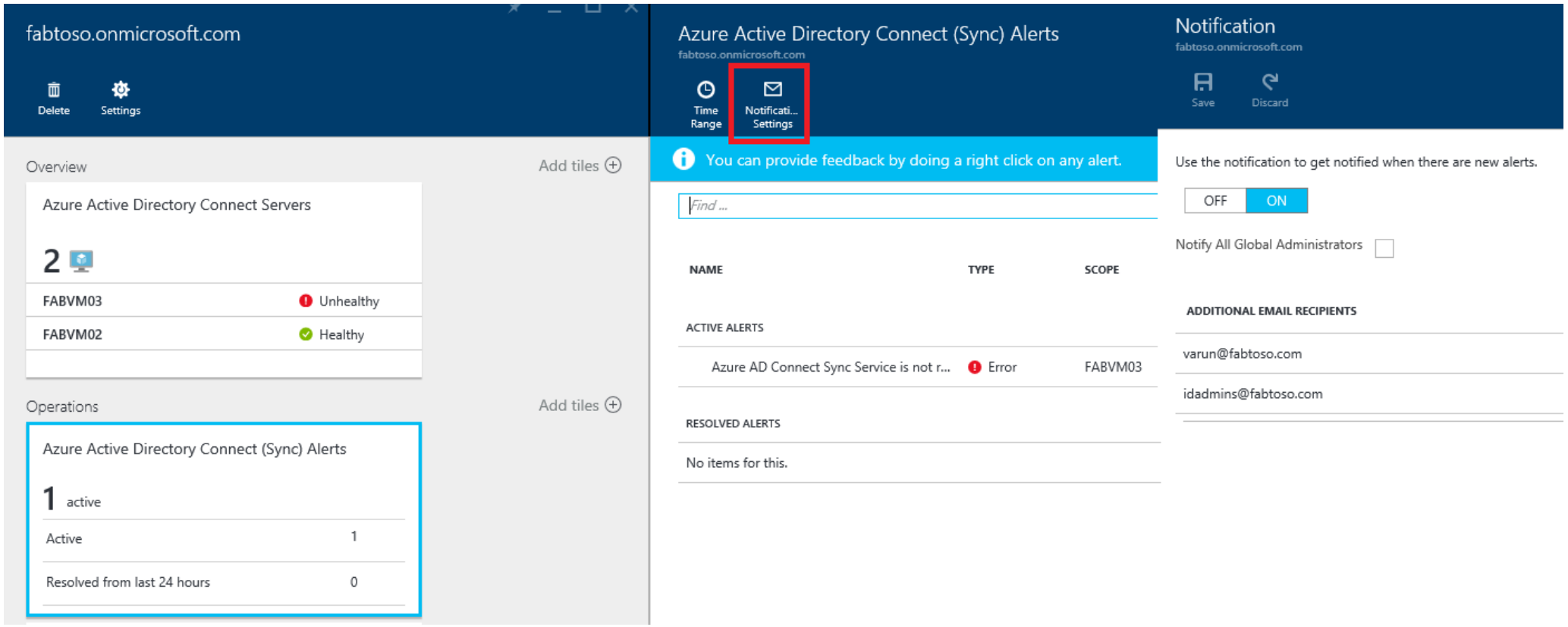
Example – AD Connect Help for AD FS Installation steps

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



Manage Azure Active Directory Connect Health

Enable email notifications



Additional tasks

Delete a server or service instance

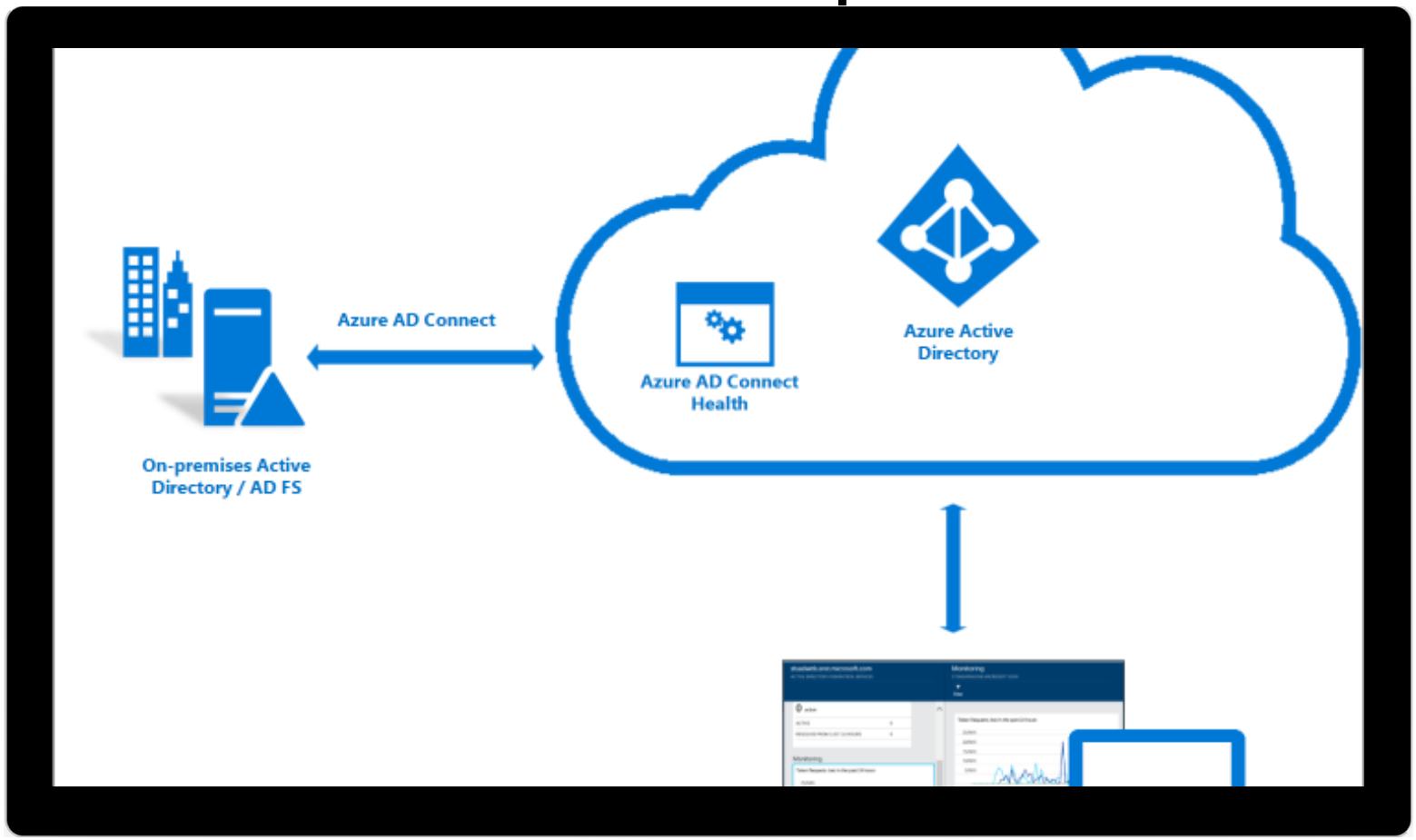
- Delete a server from the Azure AD Connect Health service
- Delete a service instance from Azure AD Connect Health service

Manage access with Azure Role Based Access Control

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

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

Launch Video



Troubleshoot synchronization errors

Troubleshooting

Diagnose and remediate duplicated attribute sync errors

- Duplicate 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

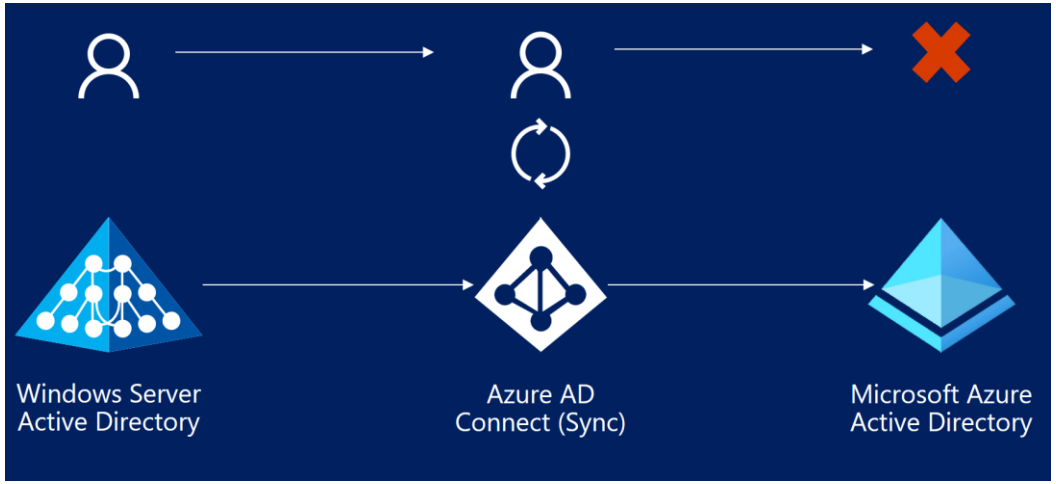
- AttributeValueMustBeUnique

Data validation failures

- IdentityDataValidationFailed
- FederatedDomainChangeError

LargeObject

Admin role conflict



Summary

Initial Azure AD configuration

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

Configure and Manage Identities

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

  - App
  - Devices

External Identities B2B

- 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
- Azure AD Connect
- Implement PHS, PTA, and SSO
- Azure AD Connect Health

Labs

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

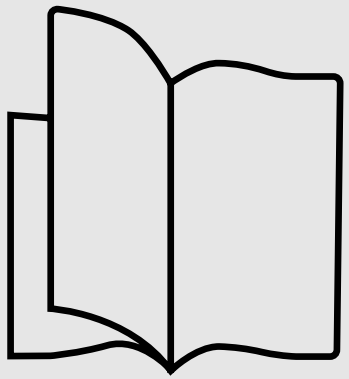
References

Implement initial configuration of Azure AD
https://docs.microsoft.com/learn/modules/implement-initial-configuration-of-azure-active-directory/

Create, configure, and manage identities
https://docs.microsoft.com/learn/modules/create-configure-manage-identities/

Implement and manage external identities
https://docs.microsoft.com/learn/modules/implement-manage-external-identities/

Implement and manage hybrid identity
https://docs.microsoft.com/learn/modules/implement-manage-hybrid-identity/



End of presentation