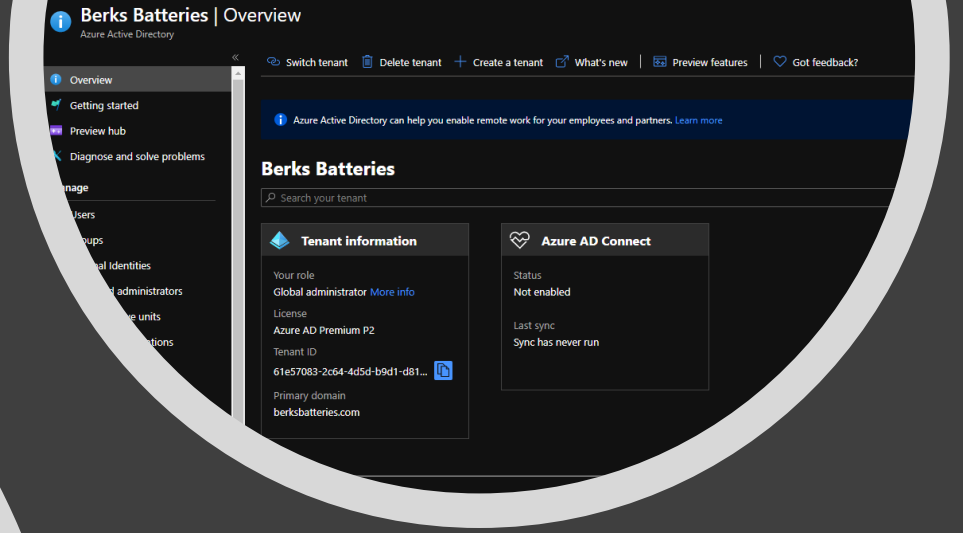


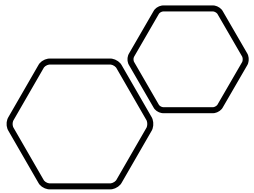
Course Intro

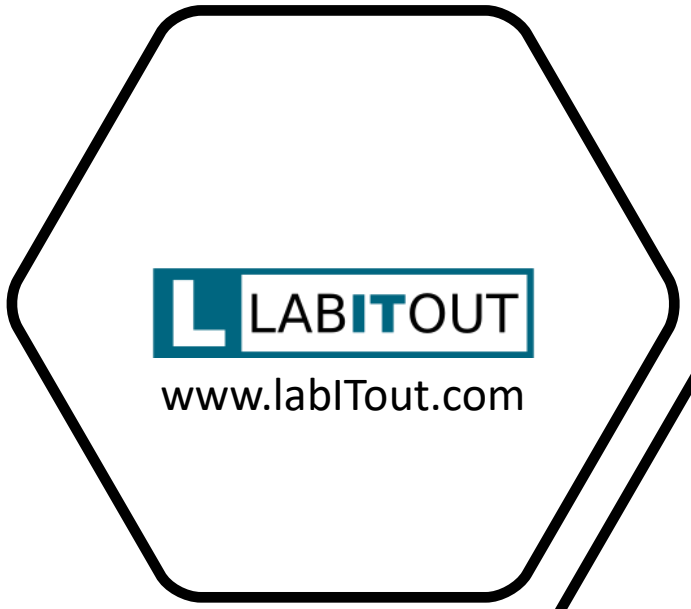
Thomas Mitchell

Thomas Mitchell

I’m a 25-year veteran of the IT industry.

I posses significant cloud experience.





I am the founder…

Thomas Mitchell

https://www.linkedin.com/in/thomas-j-mitchell/

Intro to Azure Active Directory

Learn what Azure AD is, and what it offers.

Learn about the differences between **Azure AD**, **traditional Active Directory**, and **Azure AD Domain Services**.

Azure AD Authentication

Learn about the different Azure AD authentication options, including **self-service password reset** and **multi-factor authentication**.

Managing Users and Groups

Learn how to **create users and groups**, and how to **manage users and groups**. We'll also cover different **roles** that are used to control access to Azure resources.

Azure AD B2B and Azure AD B2C

Learn what Azure AD B2B is and what Azure AD B2C is. Learn what each offering is used for.

Azure AD Domain Services

Learn what Azure AD Domain Services is and what it offers. We'll also compare the different identity solutions that are available as well.

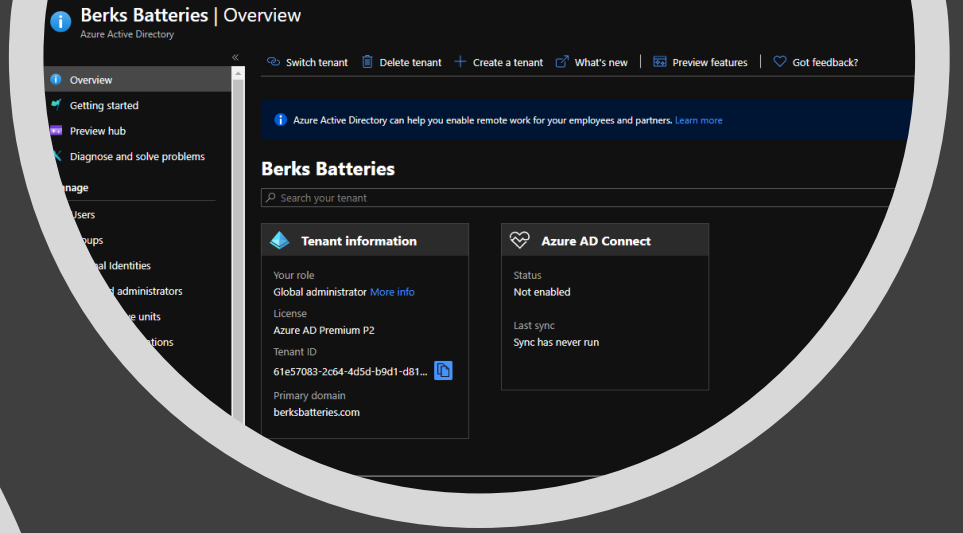
Hybrid Identities

Learn what hybrid identities are, and what the role of **Azure AD Connect** is.

Learn about **Password Hash Sync**, **Pass-Through Authentication**, **Federation**, and **Single Sign-On**.

Please give this a rating when you’re finished!

Let’s Get Started!

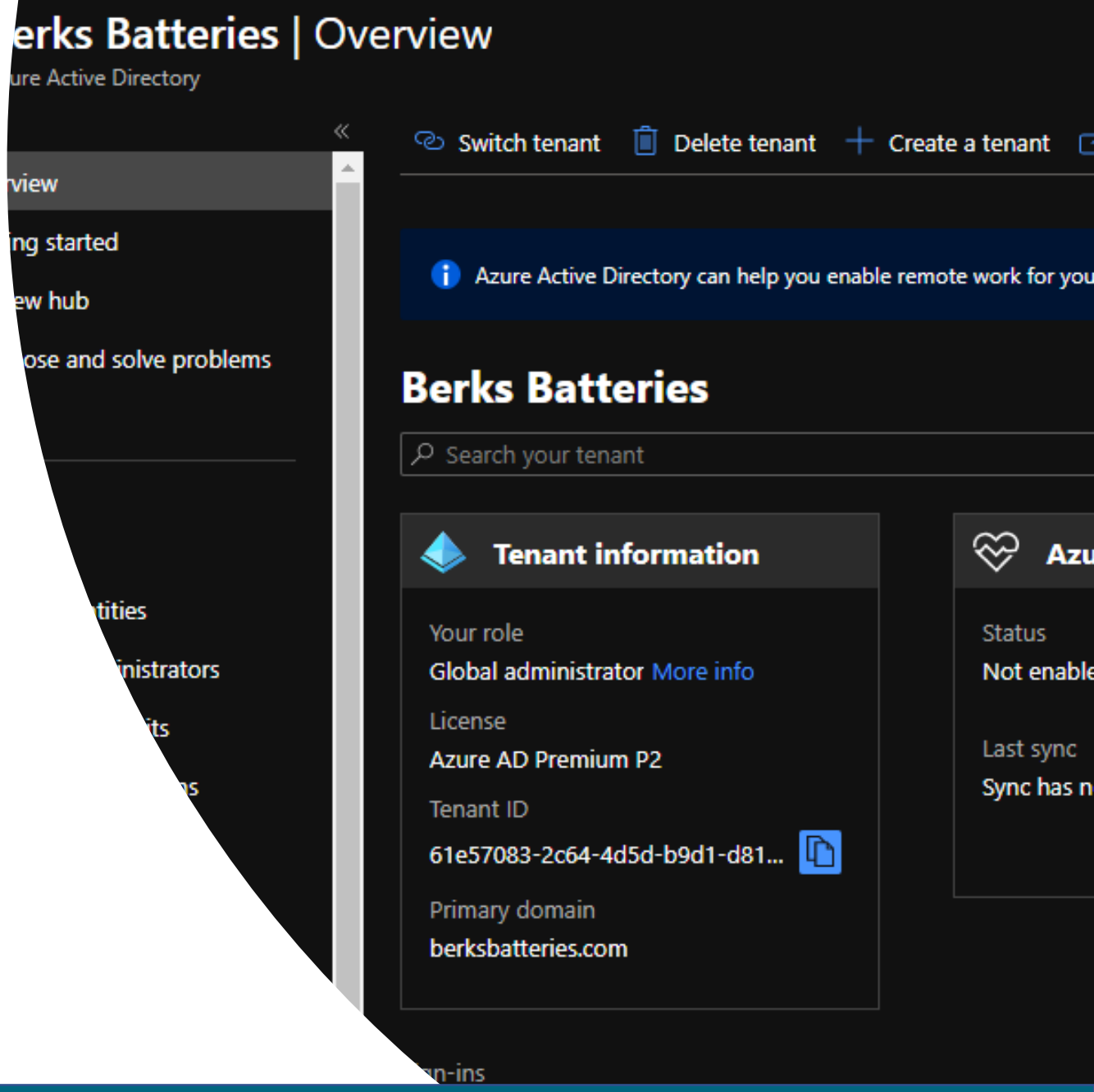


What is Azure Active Directory?

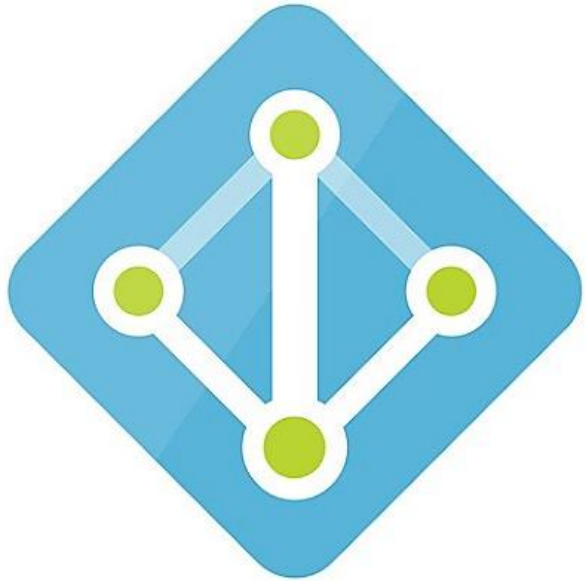
Azure AD

Azure AD is a cloud-based identity and access management service.

- Allows users to sign in and access resources:
  - Provides access to internal resources
  - Provides access to external resources
- Who Uses Azure AD?
  - IT Administrators
  - Application Developers
  - Subscribers



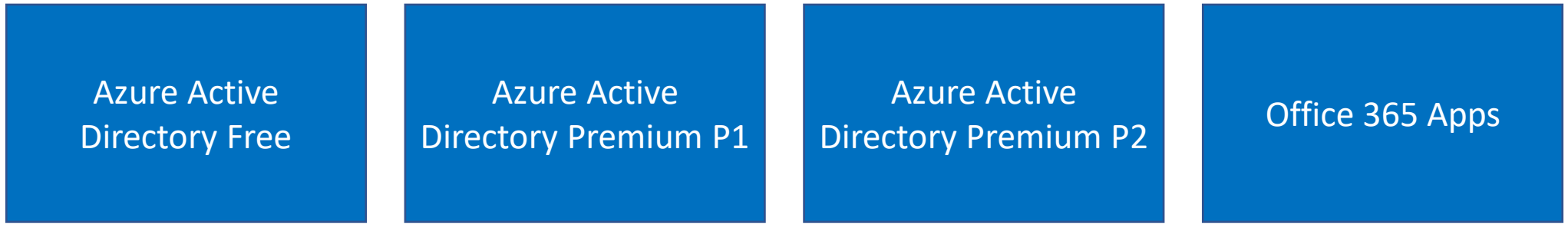
Who Uses Azure AD?



- IT Administrators
  - Use Azure AD to control access to apps and resources
  - Enforce multifactor authentication
  - Automate user provisioning
- Application Developers
  - Adding single sign-on to applications
  - Allow applications to work with the existing credentials for users
- Subscribers
  - Microsoft 365 & Office 365 subscriptions are already automatically Azure AD tenants because user access to these apps are controlled by Azure AD

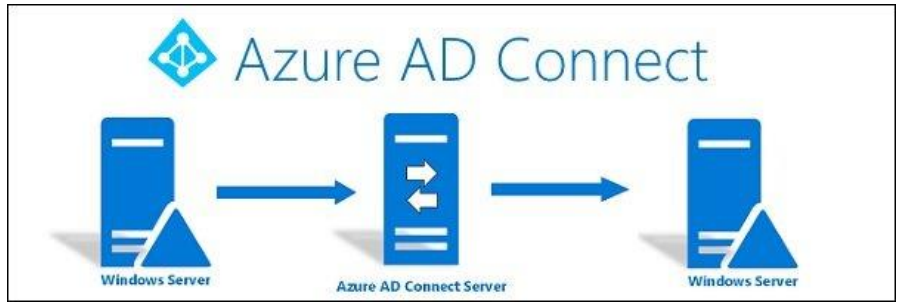
Azure AD Licenses

- Azure AD is offered in a free version and paid versions
- Paid Azure AD licenses provide additional benefits:
  - Self-service
  - Enhanced monitoring
  - Security
  - Reporting
  - Secure access for mobile users



Azure Active Directory Free

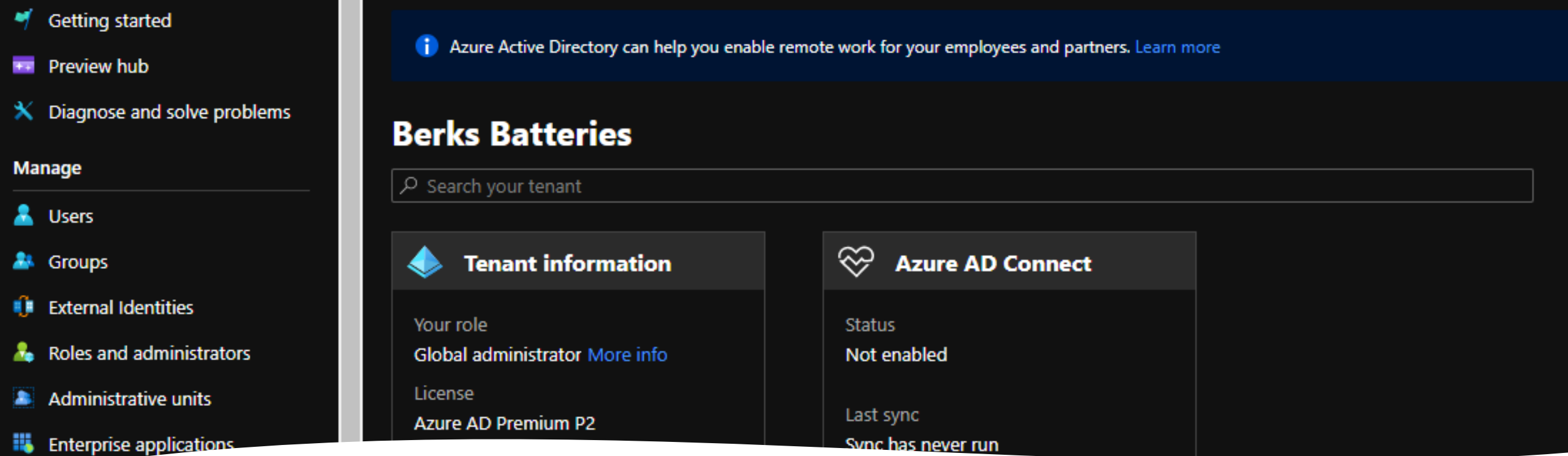
- Offers User & Group Management
- Offers On-Prem Directory Synchronization



- Offers Some Basic Reporting Functionality
- Self-Service Password Change for Cloud-Only Users
- Single Sign-On for Azure, Office 365, and Other SaaS Apps

Azure Active Directory Premium P1

- Offers everything the free version offers
- Also offers some advanced administration capabilities
  - Dynamic groups
  - Self-service group management
  - Self-service password reset for on-prem users
  - Microsoft Identity Manager

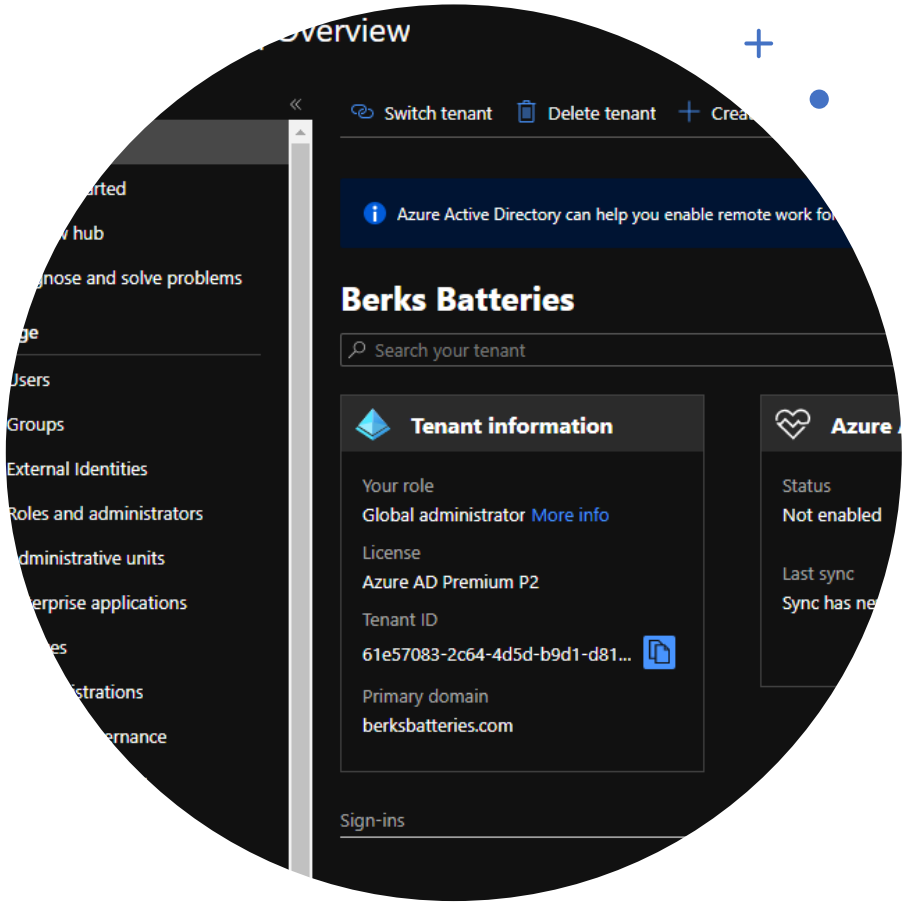


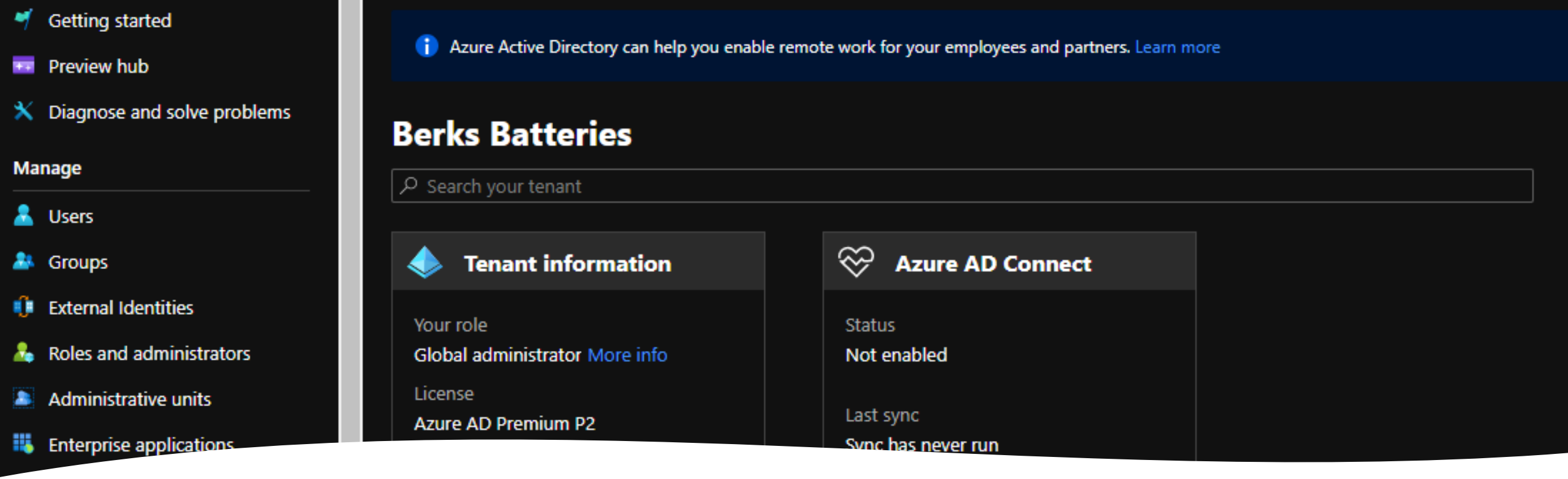
Azure AD Premium P2

- Builds off the free version and Premium P1
- Offers Azure Active Directory Identity Protection
  - Used to leverage risk-based conditional access to applications & data
- Privileged identity management
  - Restrict and monitor the access and activities of administrators
  - Just-in-time access

Office 365 Apps

- Offers user and group management, user-based provisioning, device registration, user-based access management and provisioning, and basic security and usage reports.
- Limited single sign-on capabilities, along with self-service password reset for cloud-only users

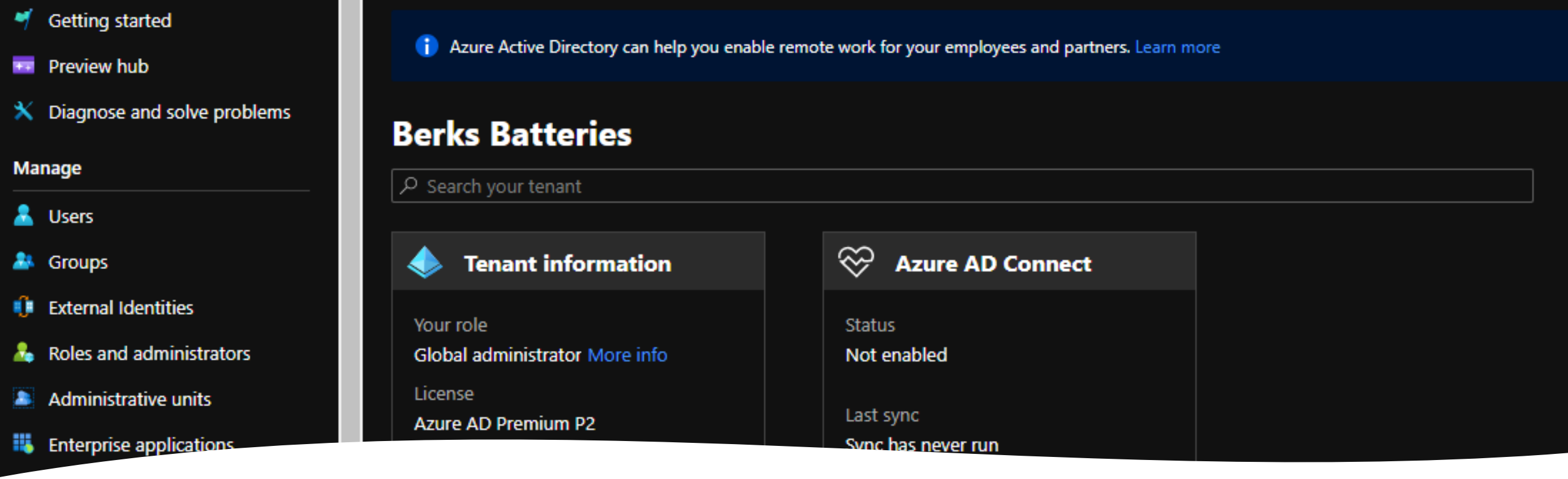




https://azure.microsoft.com/en-us/pricing/details/active-directory

Key Terms

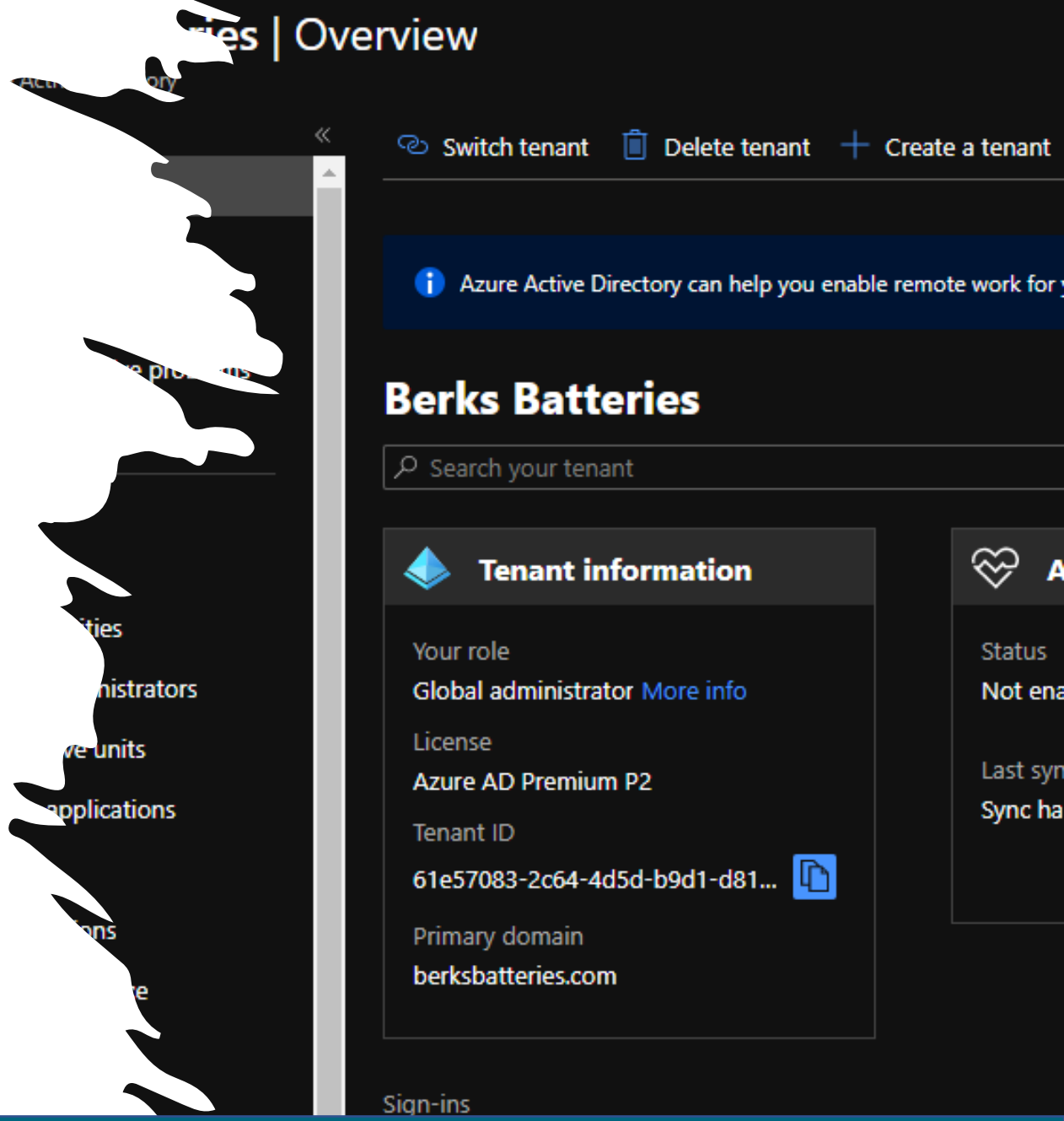
Term or Concept	Description
Identity	A thing that can get authenticated. An identity can be a user with a username and password. Identities also include applications or other servers that might require authentication through secret keys or certificates.
Azure AD Account	An identity created through Azure AD or another Microsoft cloud service, such as Microsoft 365. Identities are stored in Azure AD and accessible to your organization's cloud service subscriptions. Sometimes called a Work or school account.
Azure AD Directory	Each Azure tenant has a dedicated and trusted Azure AD directory. The Azure AD directory includes the tenant's users, groups, and apps and is used to perform identity and access management functions for tenant resources.
Azure AD Global Administrator	This administrator role is automatically assigned to whomever created the Azure AD tenant. Global administrators can do all of the administrative functions for Azure AD and any services that federate to Azure AD, such as Exchange Online, SharePoint Online, and Skype for Business Online. You can have multiple Global administrators, but only Global administrators can assign administrator roles.



https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis#terminology

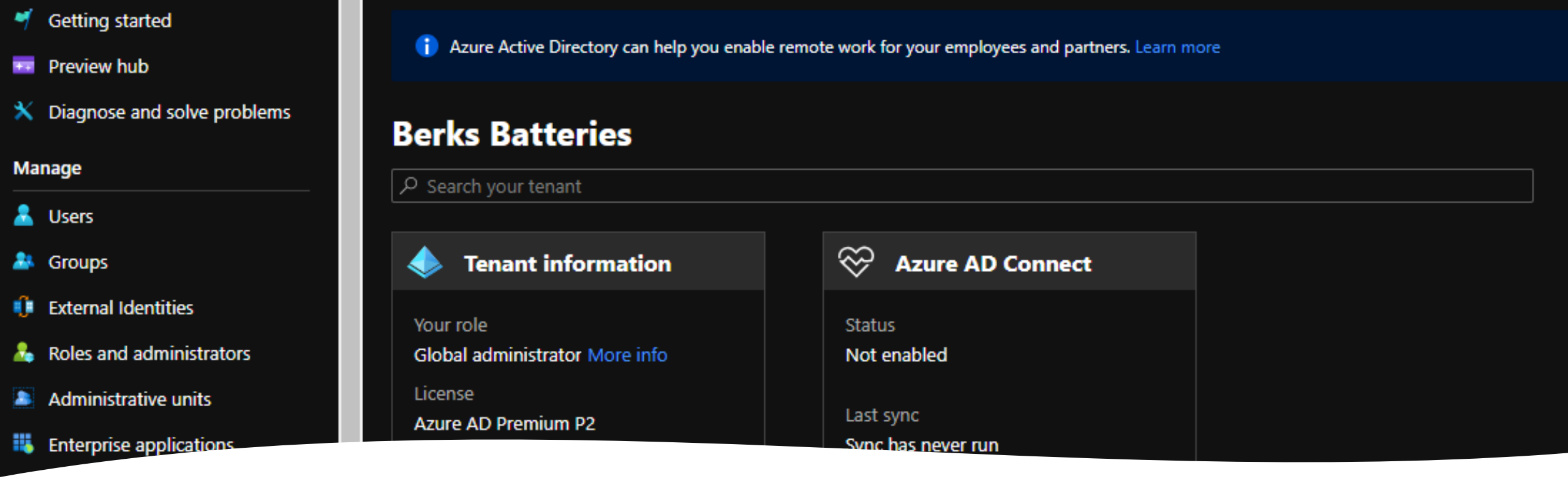
Azure AD Features

- Application management features
  - Application proxy
  - Single sign-on
  - My apps portal
- Authentication features
  - Self-service password reset
  - Multifactor authentication
  - Banned password lists
  - Smart lockout

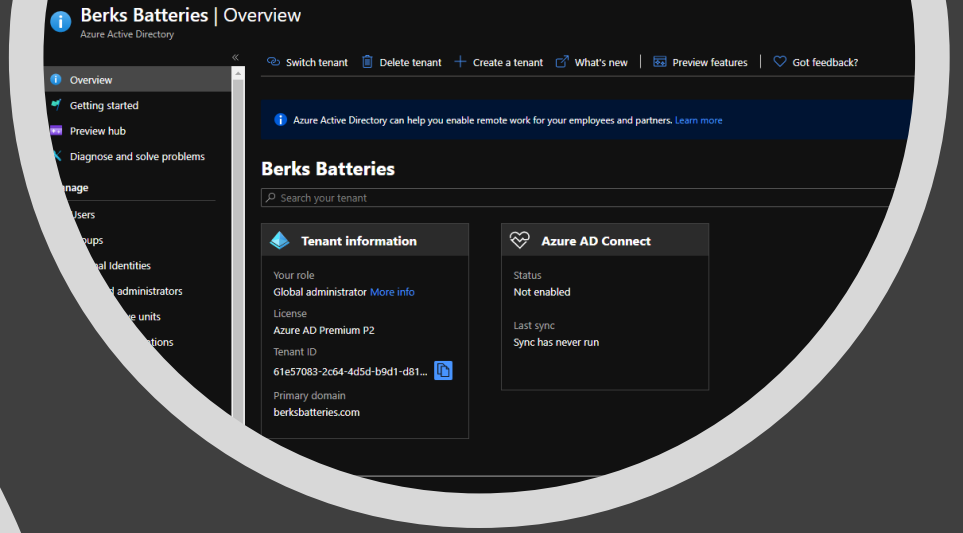


More Azure AD Features

- Hybrid identity features
  - Azure Active Directory Connect & Connect Health
    - Used to provide a single user identity that each user can use for authentication and authorization to your resources
- Various reporting and monitoring features
  - Provide insights into the security and usage patterns within your organization
- Privileged Identity Management (PIM)
  - Manage, control, and monitor access to resources



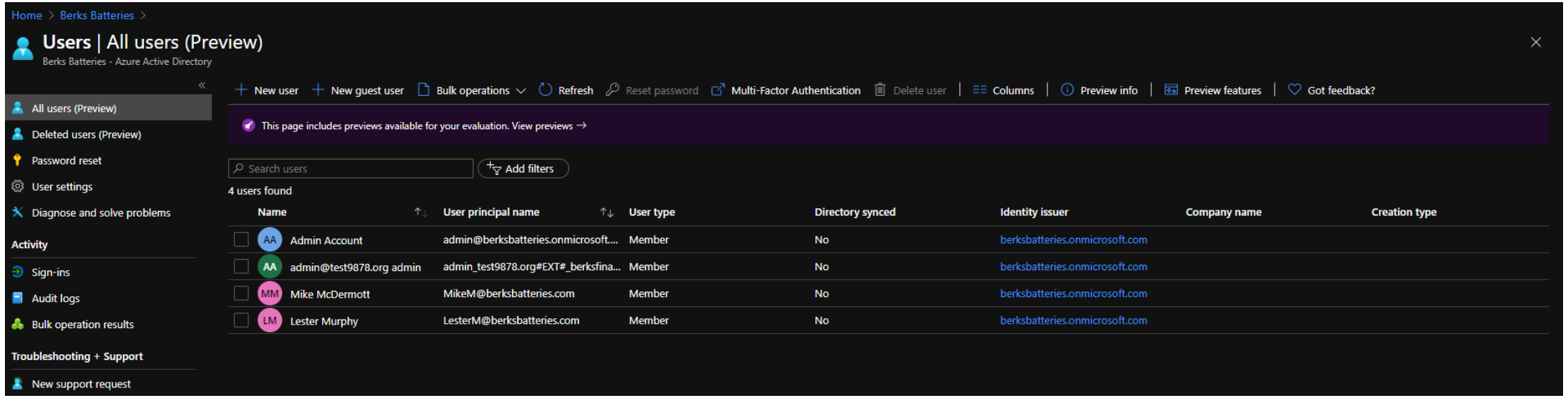
https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis#which-features-work-in-azure-ad

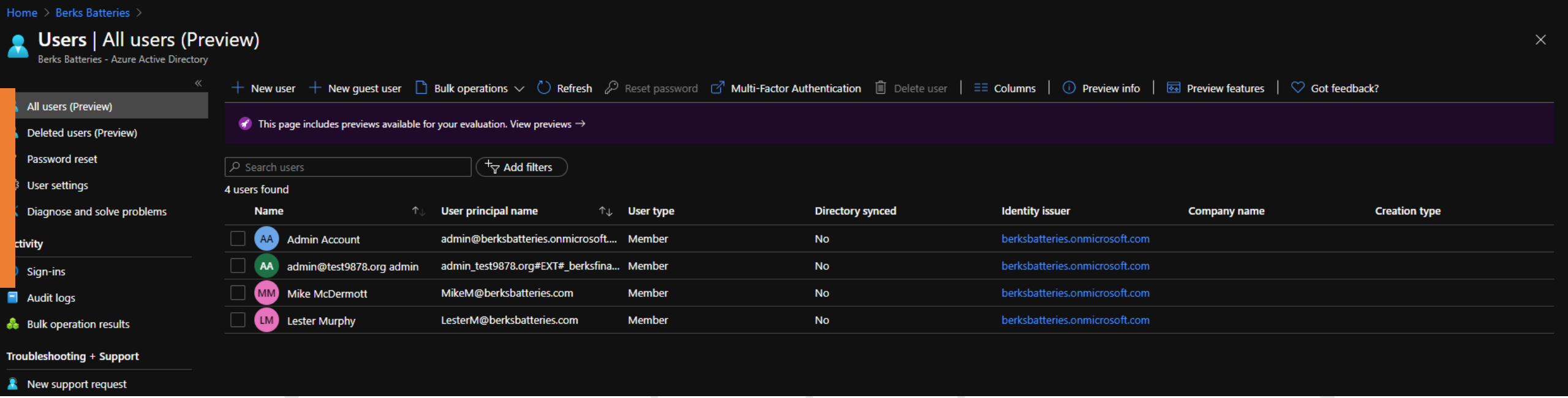


Creating and Managing Users

Creating and Managing Users

- Azure account is needed to access Azure resources
- Users are **authenticated** using their accounts
  - Allows users to sign on
- Once authenticated, Azure AD will **authorize** the user
  - Determines what resources that user can access

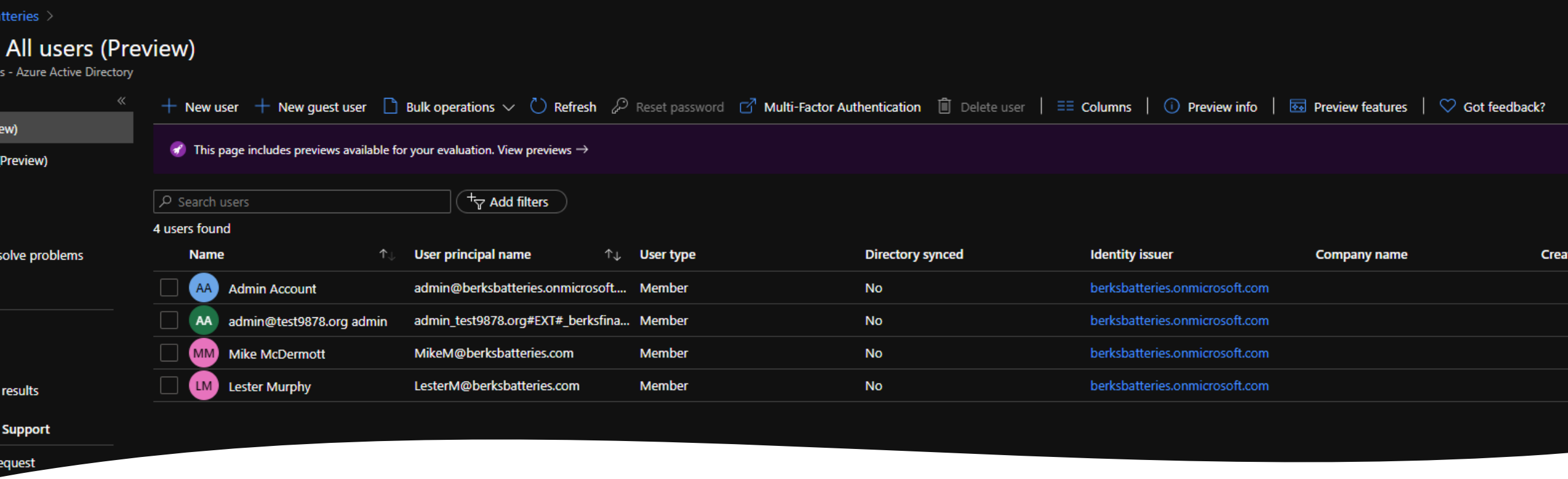




Defining Users in Azure AD

Users in Azure Active Directory can be defined in **THREE** ways:

- Cloud Identities
- Directory Synchronized Identities
- Guest Users



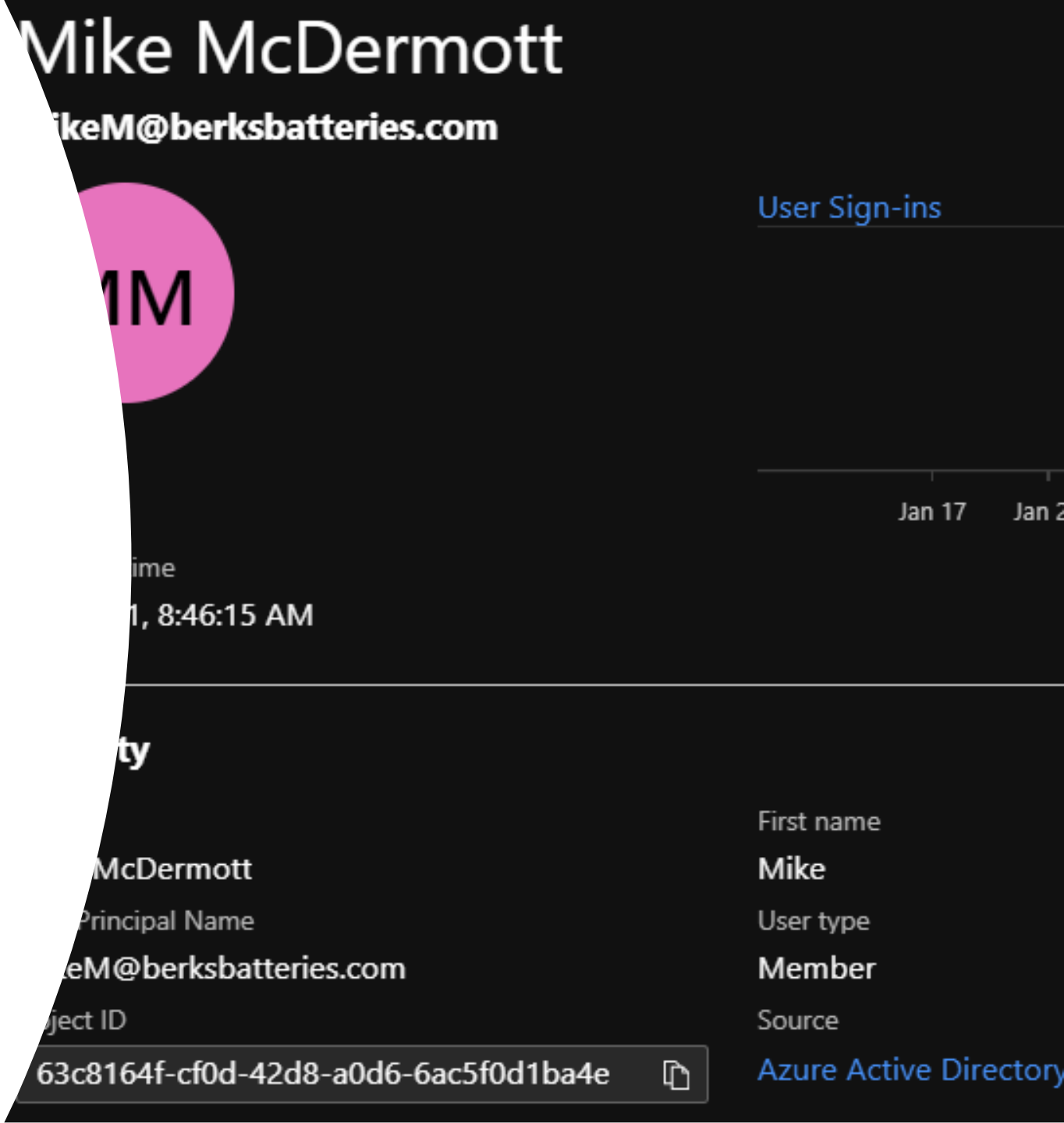
Cloud Identities

Show up in the Azure AD Portal as **Azure Active Directory** users or **External Azure Active Directory** users.

- Members of local Azure AD = Azure Active Directory users
- Users defined in another Azure AD = External Azure AD users

Cloud Identities

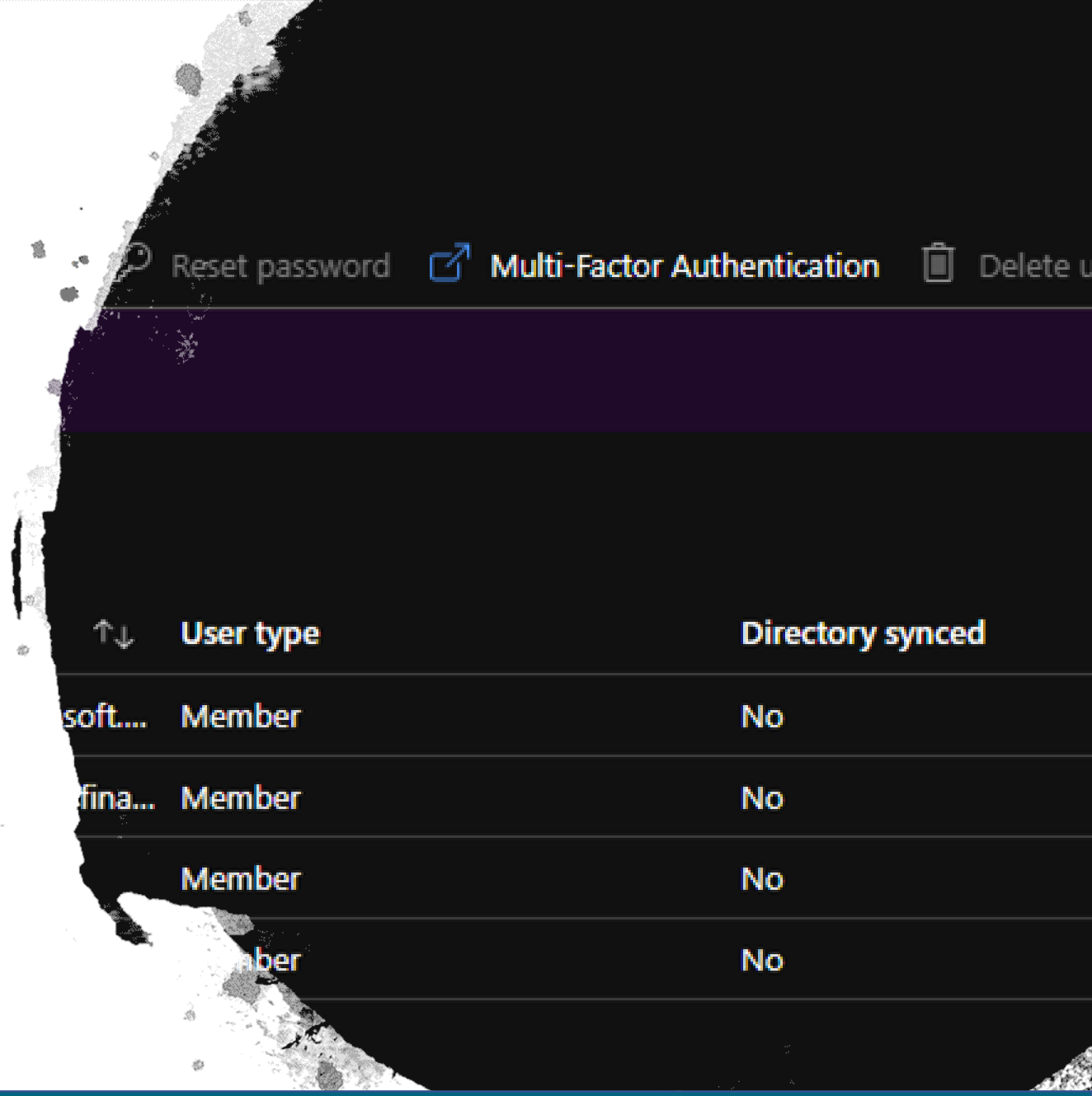
- Cloud Identities show up in the Azure AD Portal as **Azure Active Directory** users or **External Azure Active Directory** users.
- Members of local Azure AD are called Azure Active Directory users.
- Users defined in another Azure AD are called External Azure AD users.



Directory Synchronized Identities

Directory Synchronized Identities show up in the Azure AD Portal as **Windows Server AD** users.

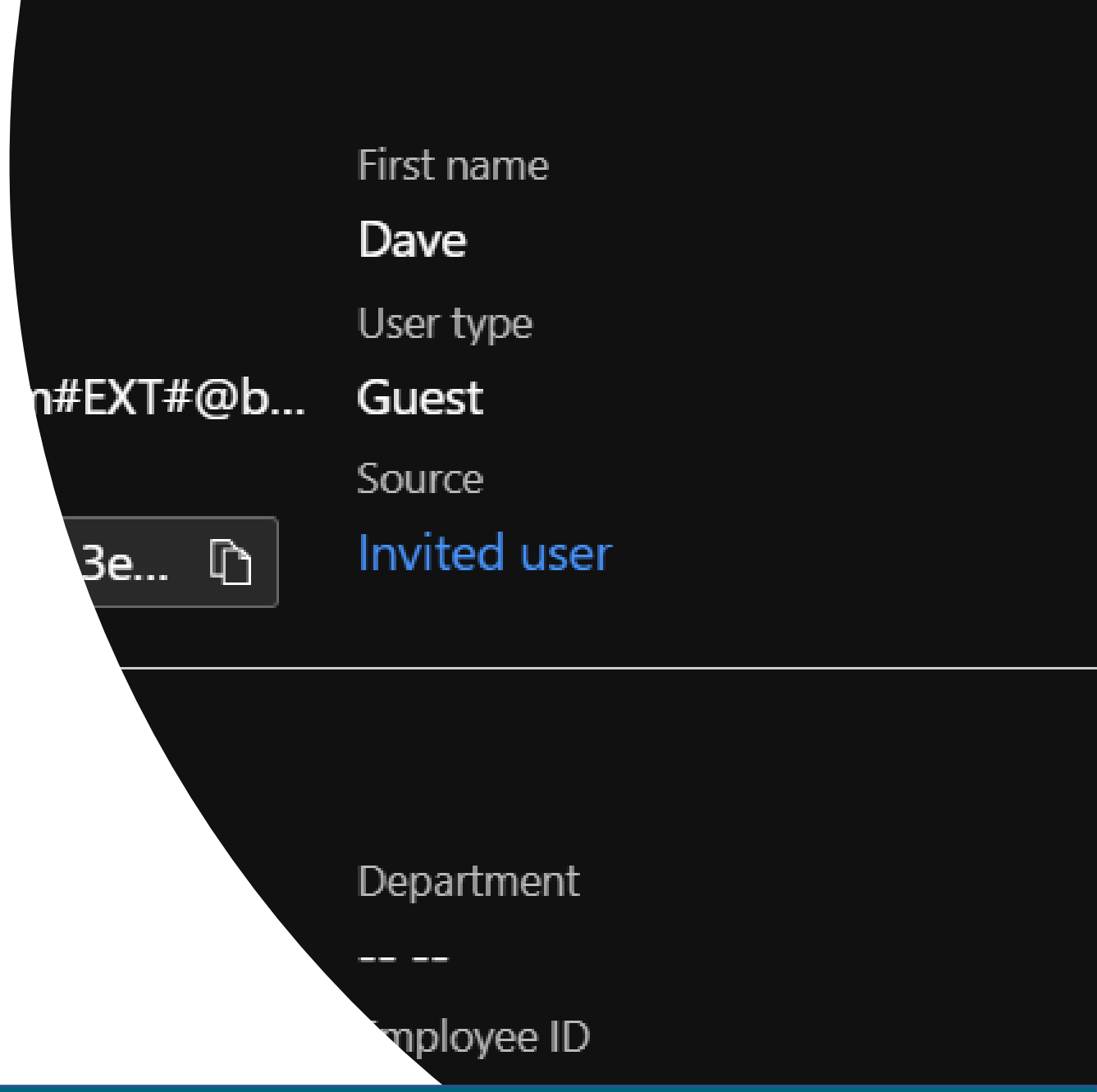
- Users that have been synchronized to Azure AD from an on-prem active directory via Azure AD connect.



Guest Users

Guest users are Azure AD users that exist outside of the Azure Active Directory.

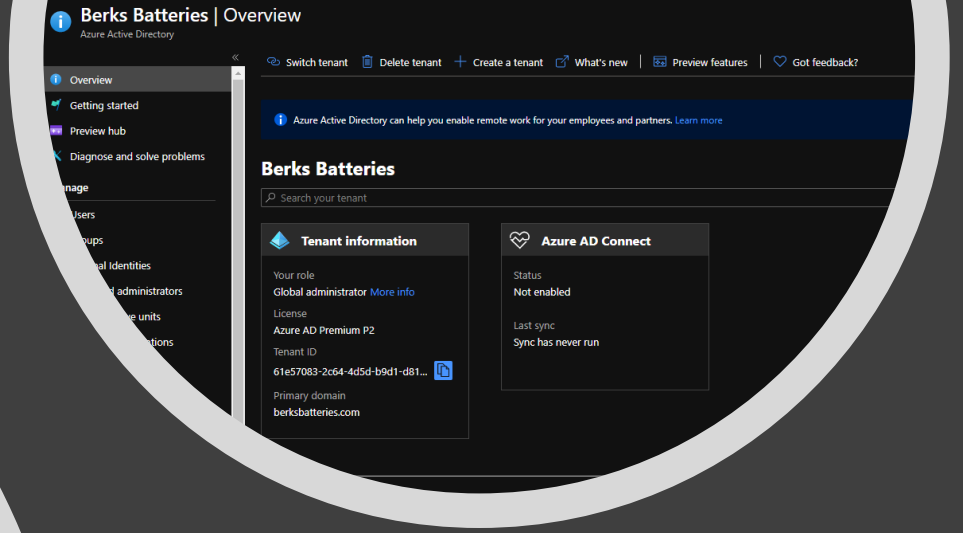
- Guest users are accounts in Azure AD from other cloud providers.
- Users with Microsoft accounts.
- Will show up in the Azure AD users list as **invited users.**



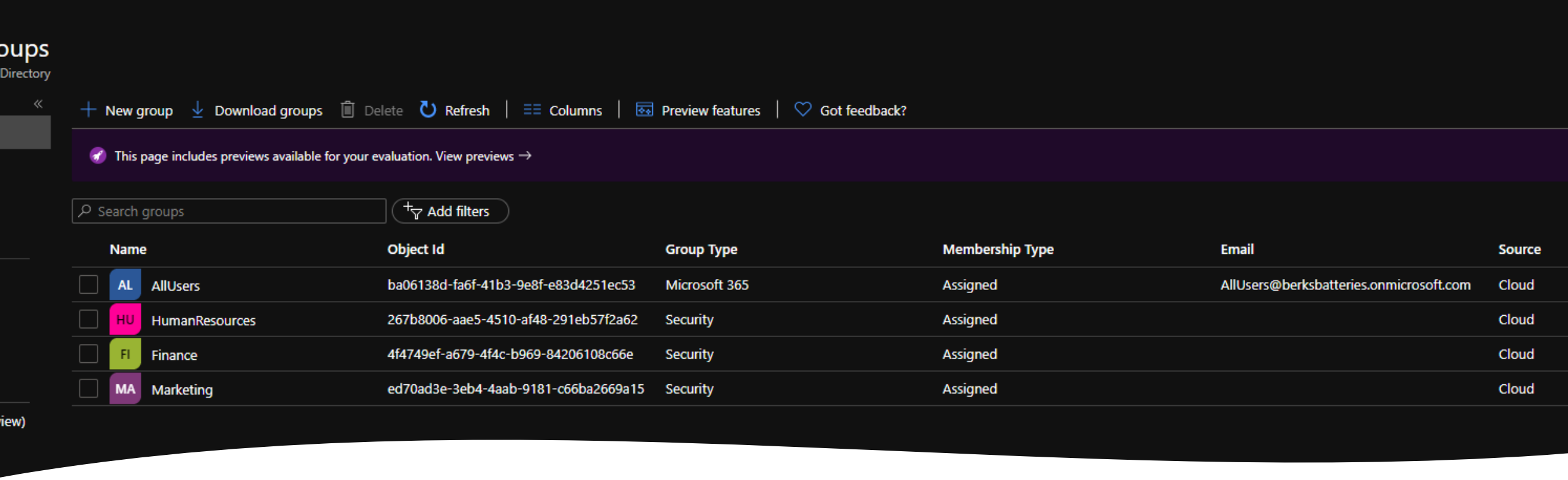
Adding Cloud Identities to Azure AD

Several ways to add cloud identities in Azure Active Directory

- Sync users from an on-prem Active Directory
- Use the Azure portal to manually add new users
- Use the command line
  - Azure PowerShell
  - Azure CLI
- Create users from a CSV file in PowerShell
- Azure AD graph API
- Office 365 admin center
- Microsoft InTune admin console



Creating and Managing Groups

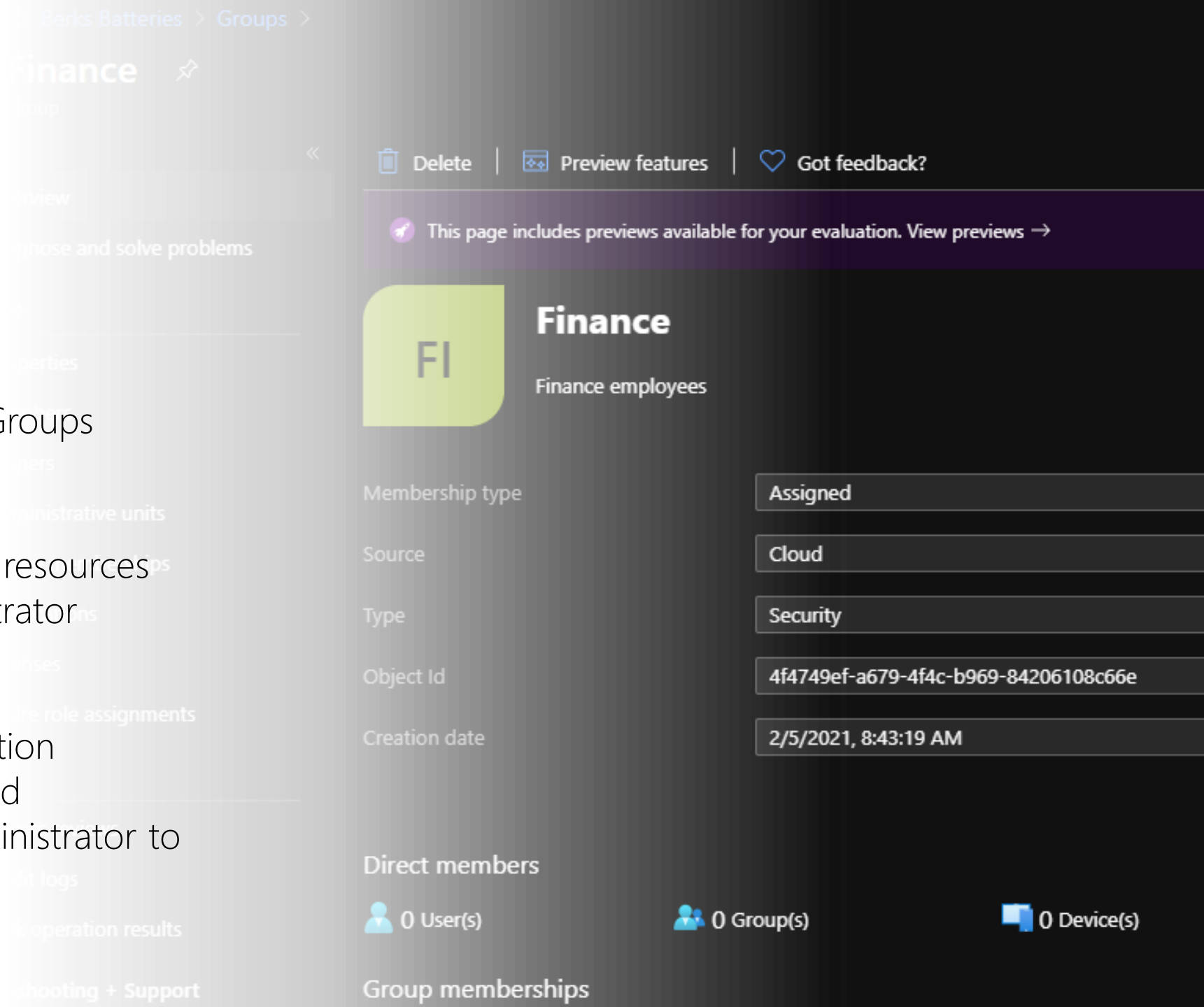


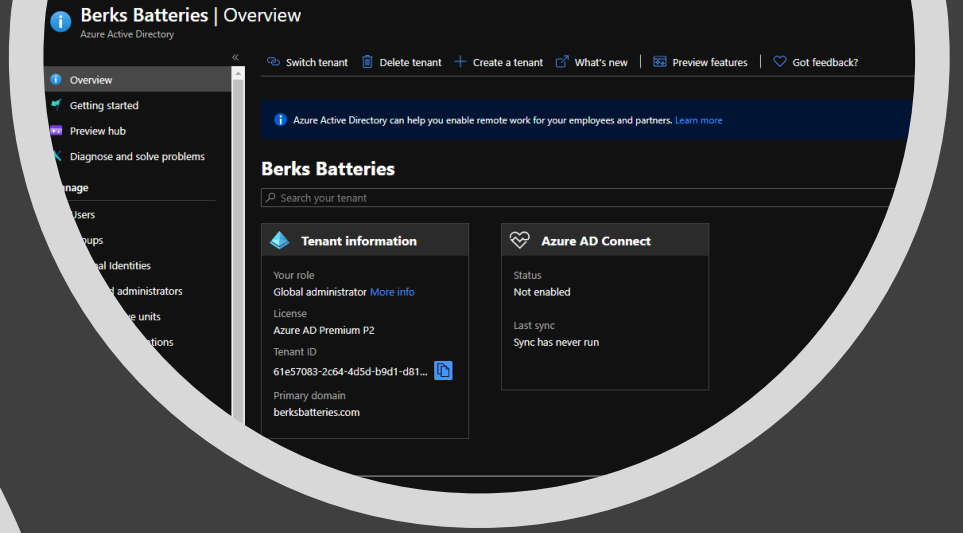
Creating and Managing Groups

- Azure AD groups are used to organize users & manage permissions
  - Assigning permissions to a group simplifies permissions mgmt
  - Allows you to grant permissions for multiple users
- Dynamic Groups
  - Define membership based on certain rules
  - Users are automatically added to the group

Two Types of Azure AD Groups

- Security Groups vs Office 365 Groups
- Security Groups
  - Most commonly used
  - Used to manage access to resources
  - Require Azure AD administrator privileges to manage
- Office 365 Groups
  - Used to facilitate collaboration
  - External users can be added
  - Do not need to be an administrator to use Office 365 groups

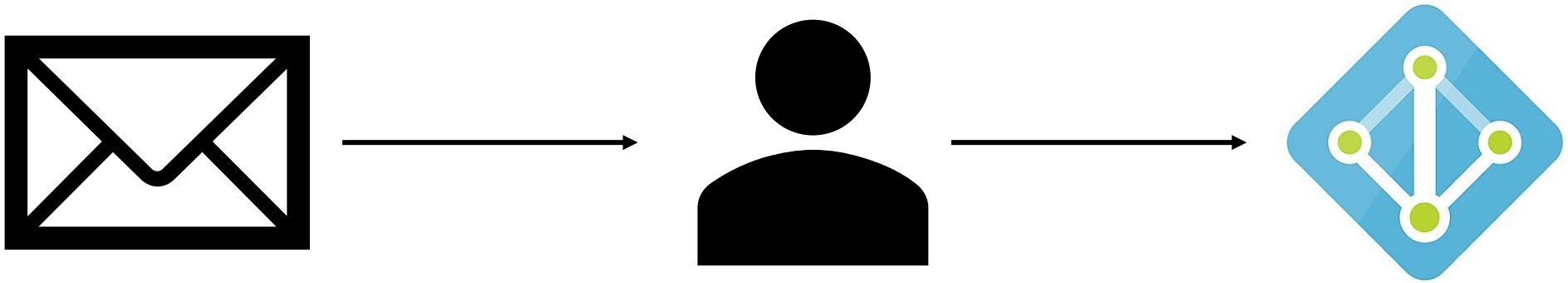




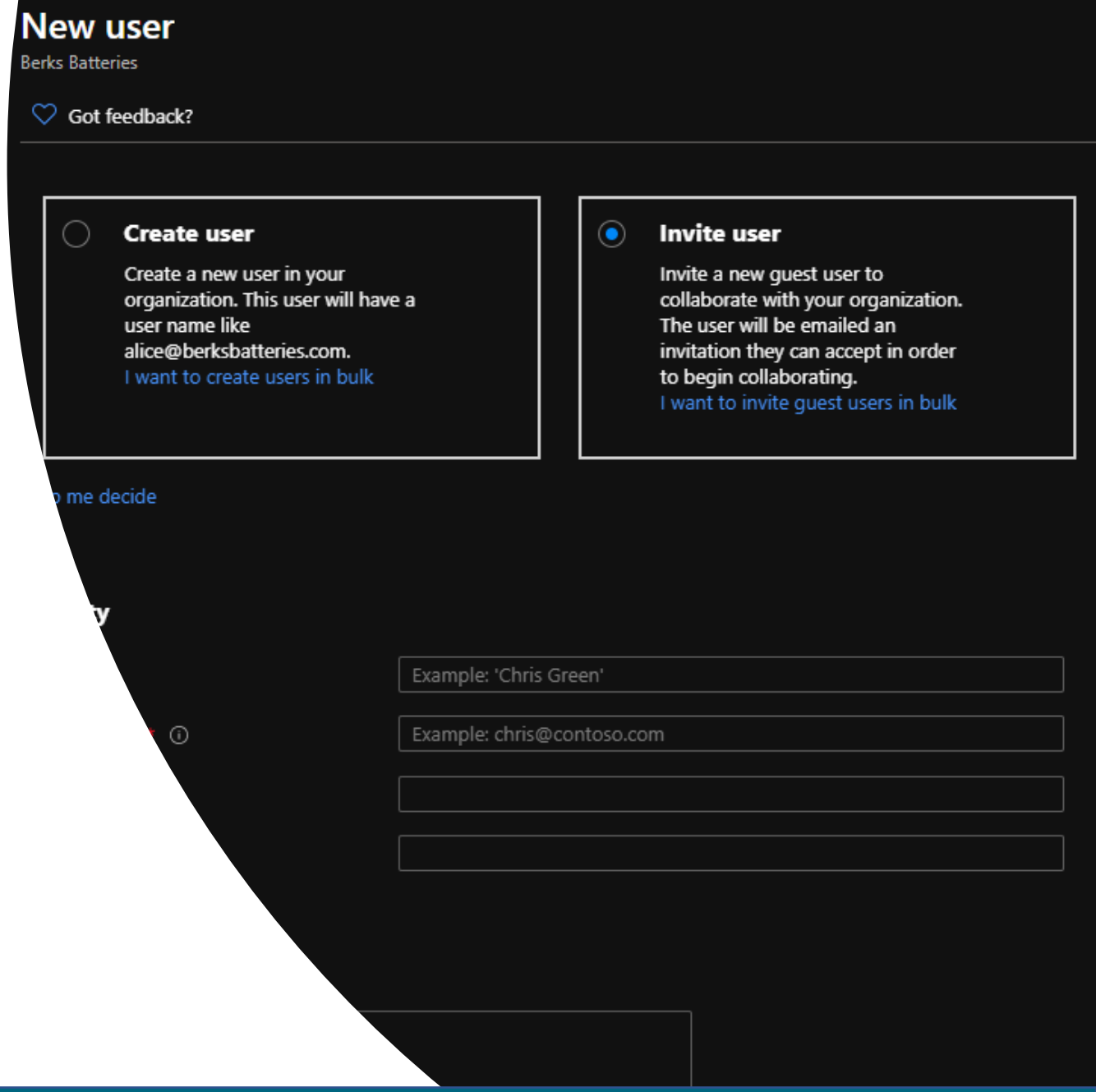
Azure Active Directory B2B

What is Azure Active Directory B2B?

- Used to share applications and services with guest users
- External org doesn't need to have Azure Active Directory
- B2B uses an invitation and redemption process
- No need to manage external accounts or external passwords



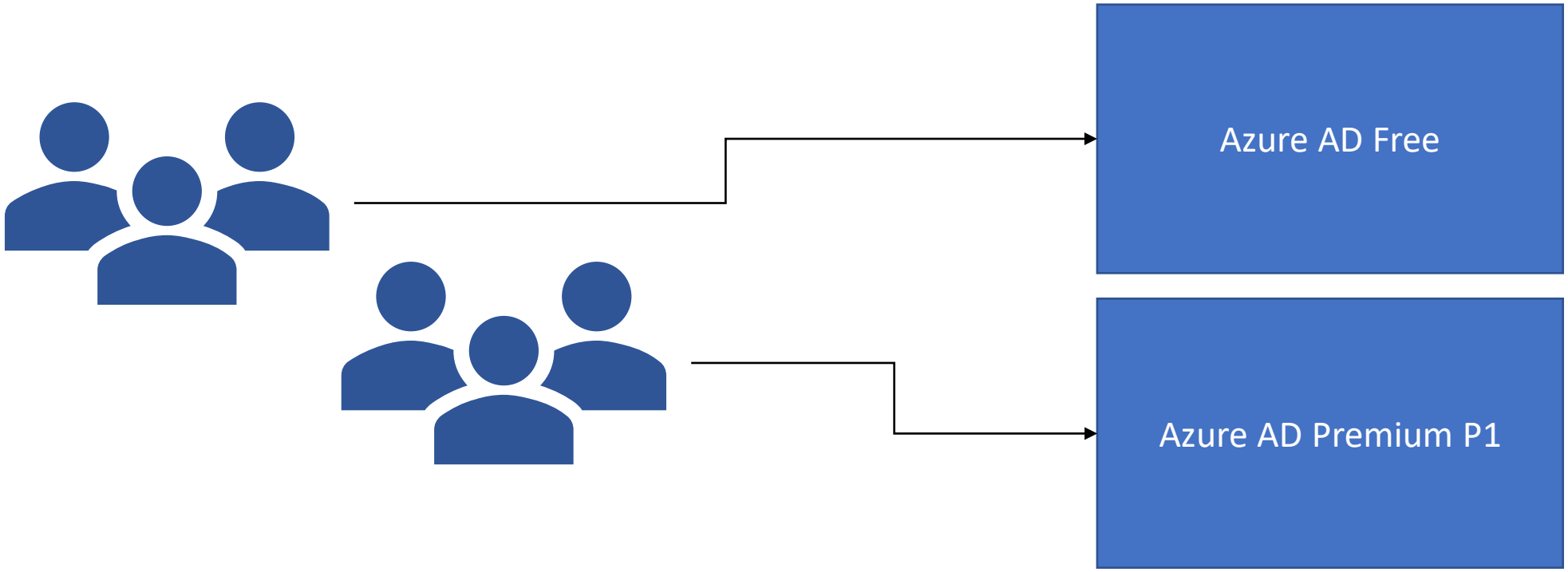
Azure AD B2B

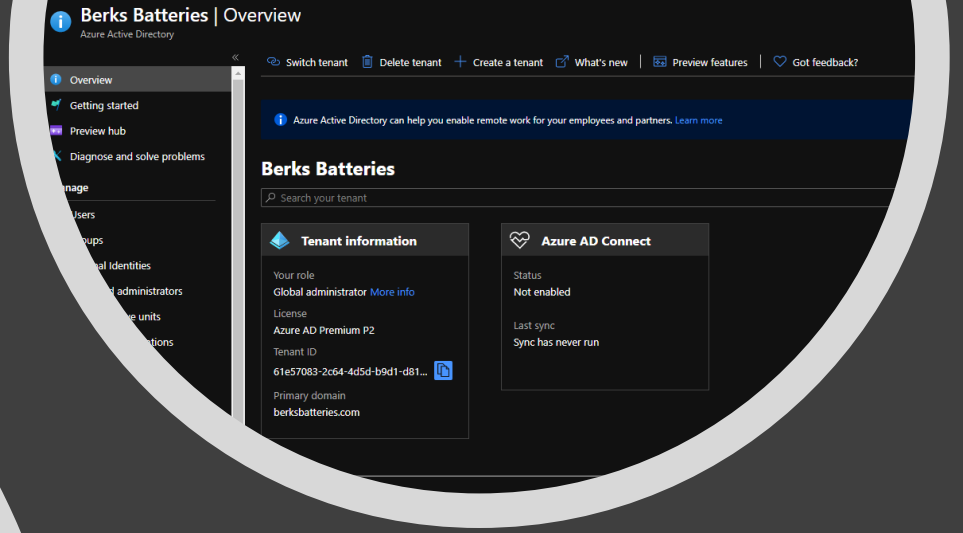


- You can add guest users through the Azure AD portal
- Process is similar to that of adding an internal user
- App owners and group owners can manage their own guest users

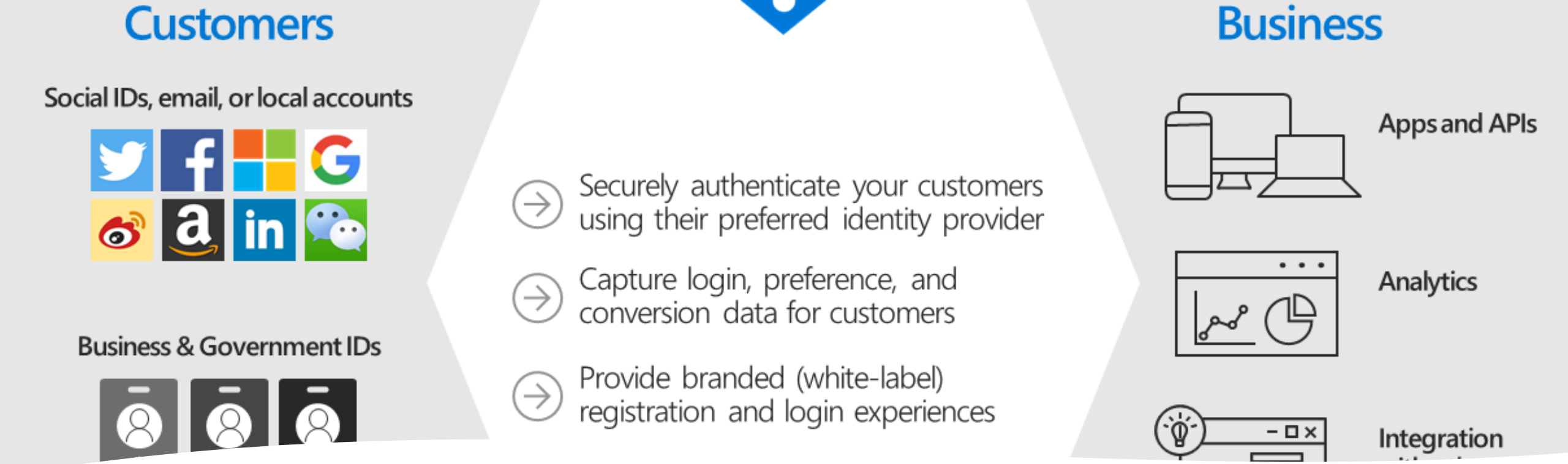
Azure AD B2B Licensing

- Guest users can use free Azure AD features without any additional licensing requirements
- You can invite up to five guest users for each paid Azure AD edition license that you are own





Azure Active Directory B2C



Azure Active Directory B2C

A business to consumer identity service.

- Sign on to apps with social accounts, enterprise accounts, or local accounts
- **EXAMPLE:** a website that allows users to login using their Facebook or LinkedIn accounts.
- You can customize your user experience with your own brand

Customers

Social IDs, email, or local accounts

Business & Government IDs

- Securely authenticate your customers using their preferred identity provider
- Capture login, preference, and conversion data for customers
- Provide branded (white-label) registration and login experiences

Business

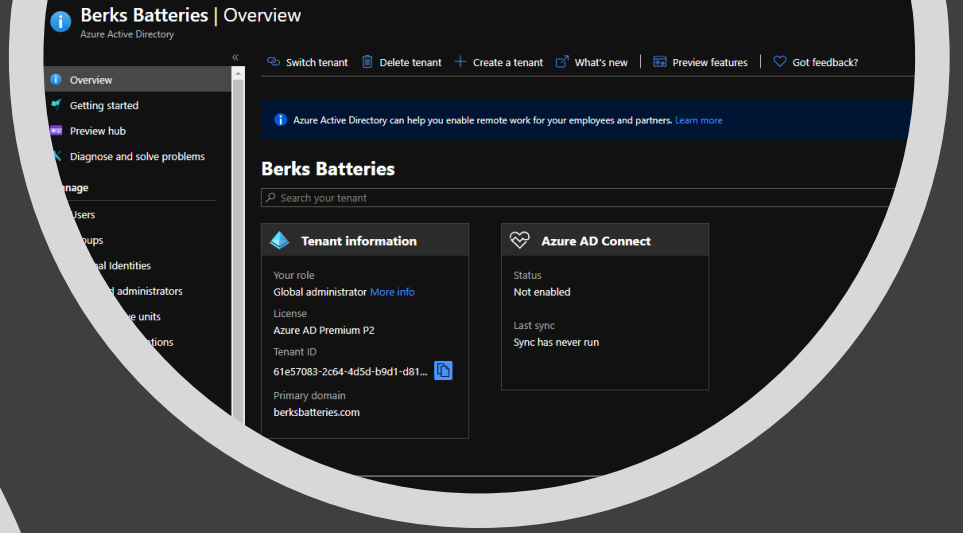
Apps and APIs

Analytics

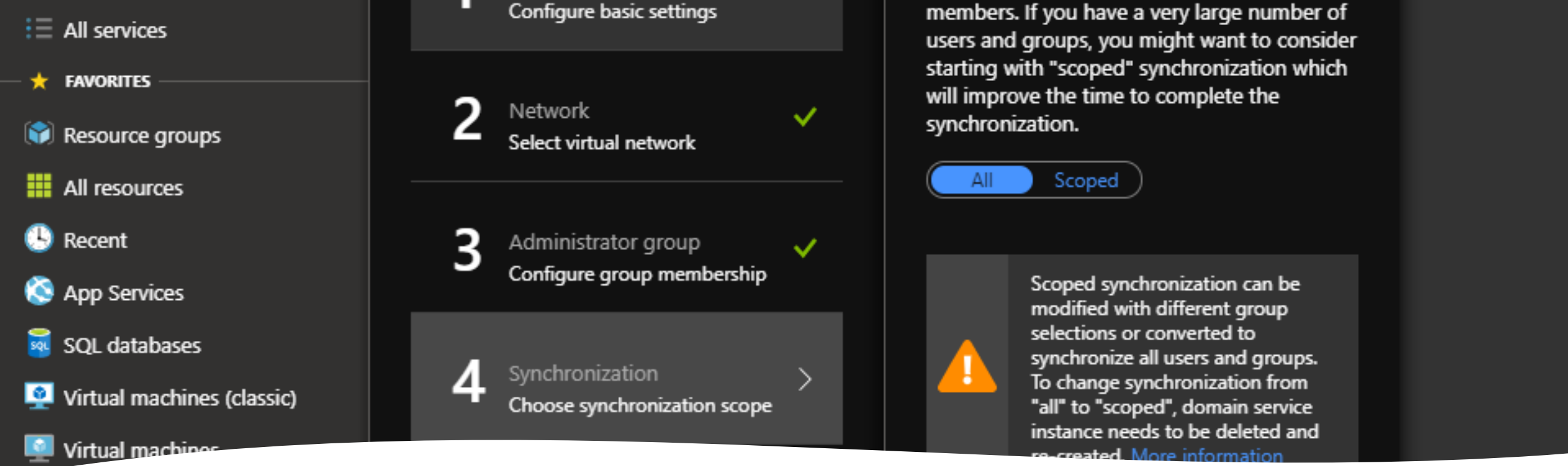
Integration with other systems

Azure AD B2C Authentication

- Standards-based protocols: OpenID Connect, OAuth 2.0, and SAML
- Azure AD B2C works with most modern apps & off-the-shelf apps
- Azure AD B2C free tier allows 50,000 active users per month



Azure AD Domain Services



What is Azure AD Domain Services?

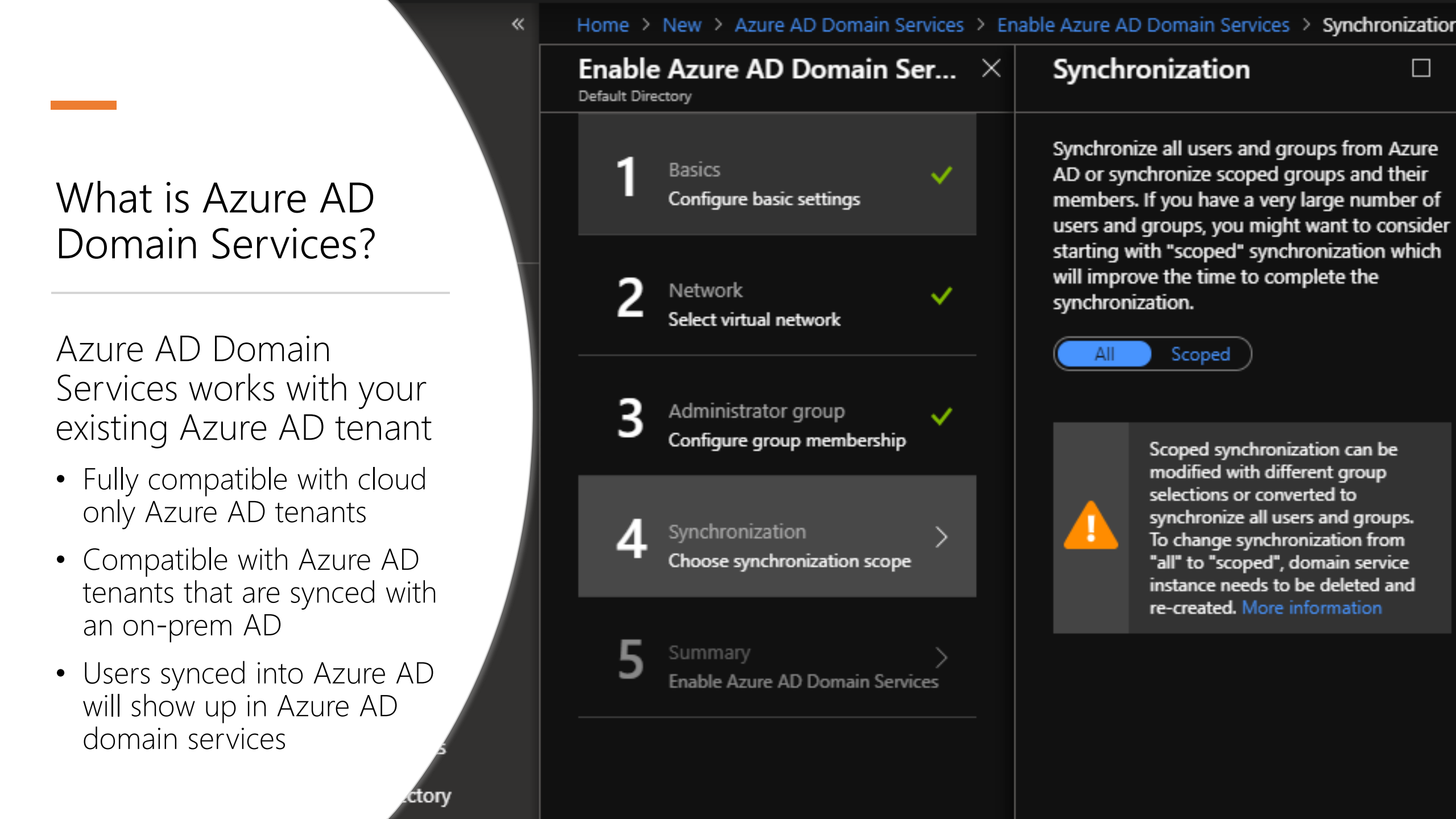
Azure AD domain services is essentially a **managed version** of a traditional on-prem Active Directory

- Offers Domain Join, Group Policy, LDAP, Kerberos, and NTLM authentication
- Does not require deployment or management of DCs

What is Azure AD Domain Services?

Azure AD Domain Services works with your existing Azure AD tenant

- Fully compatible with cloud only Azure AD tenants
- Compatible with Azure AD tenants that are synced with an on-prem AD
- Users synced into Azure AD will show up in Azure AD domain services



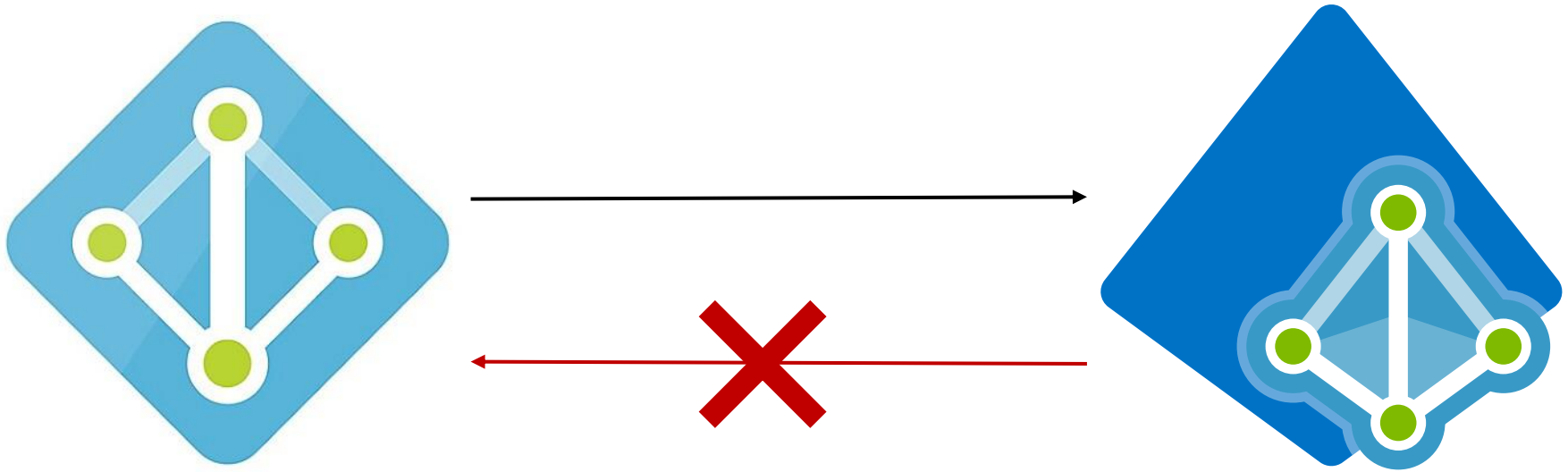
How does Azure ADDS Work?

When Azure ADDS is deployed, a managed domain is created on the virtual network that you specify.

- Azure spins up two Windows server domain controllers that run on VMs
- You cannot manage, or even access, the domain controllers
- Azure performs all management of the domain controllers

How does Azure ADDS Work?

- The managed domain that is spun up is configured for one-way synchronization from Azure AD



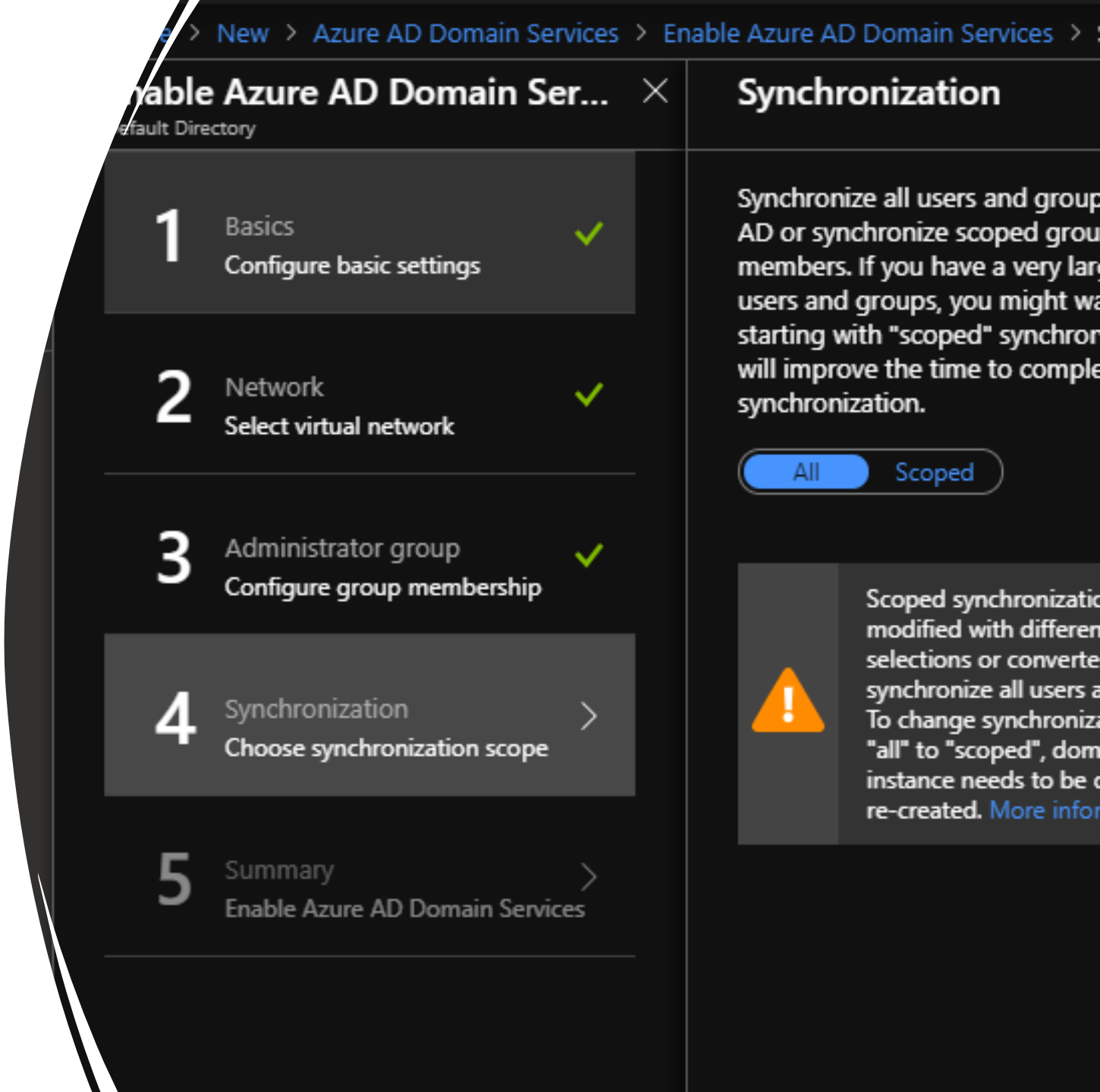
Azure ADDS Best Practices

CLOUD-ONLY BEST PRACTICE:

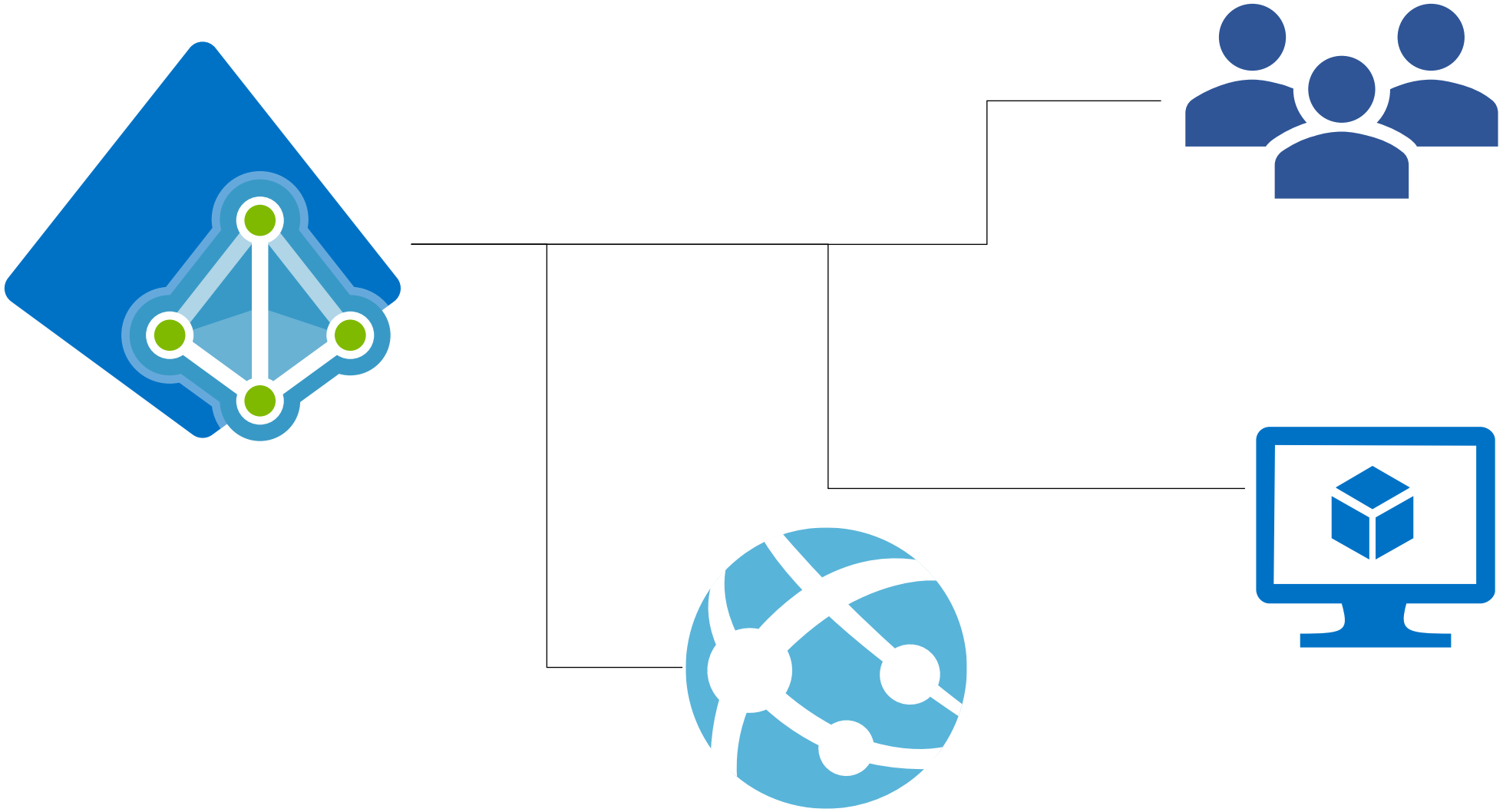
- Create resources in Azure Active Directory and let them sync over to the managed domain service.

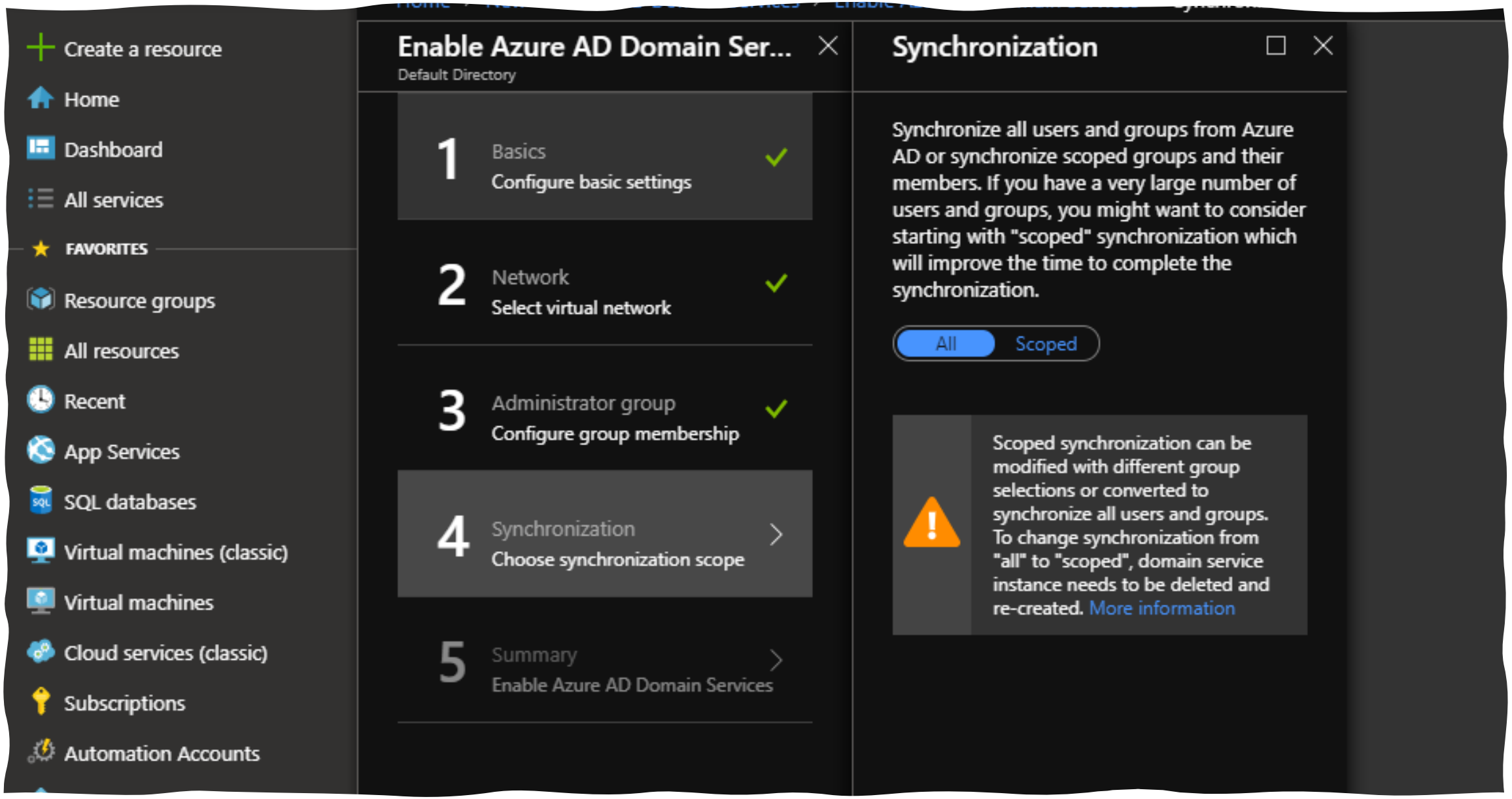
HYBRID BEST PRACTICE:

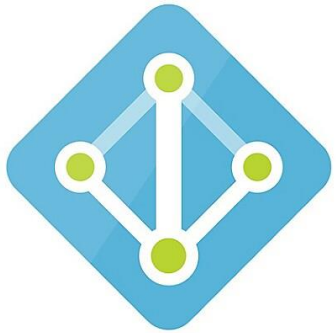
- Create users in the on-prem AD so they synchronize over to Azure Active Directory with Azure AD connect.
- After syncing to Azure AD, they will sync to Azure AD domain services



How does Azure ADDS Work?



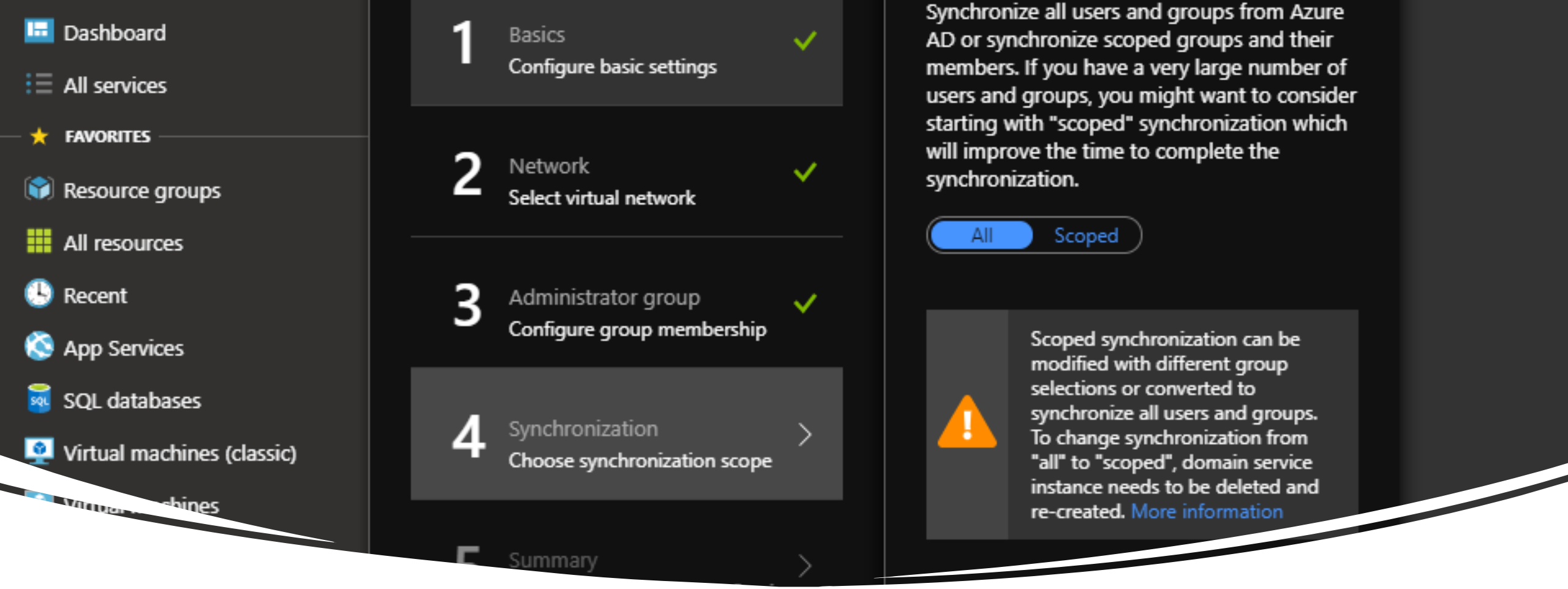

Create a resource
Home
Dashboard
All services
FAVORITES
Resource groups
All resources
Recent
App Services
SQL databases
Virtual machines (classic)
Virtual machines
Cloud services (classic)
Subscriptions
Automation Accounts
Enable Azure AD Domain Ser...
Default Directory
1 Basics
Configure basic settings
2 Network
Select virtual network
3 Administrator group
Configure group membership
4 Synchronization
Choose synchronization scope
5 Summary
Enable Azure AD Domain Services
Synchronization
Synchronize all users and groups from Azure AD or synchronize scoped groups and their members. If you have a very large number of users and groups, you might want to consider starting with "scoped" synchronization which will improve the time to complete the synchronization.
All
Scoped
Scoped synchronization can be modified with different group selections or converted to synchronize all users and groups. To change synchronization from "all" to "scoped", domain service instance needs to be deleted and re-created. More information



How Does Azure ADDS Work?

Azure AD Domain Services is tightly integrated with Azure Active Directory.

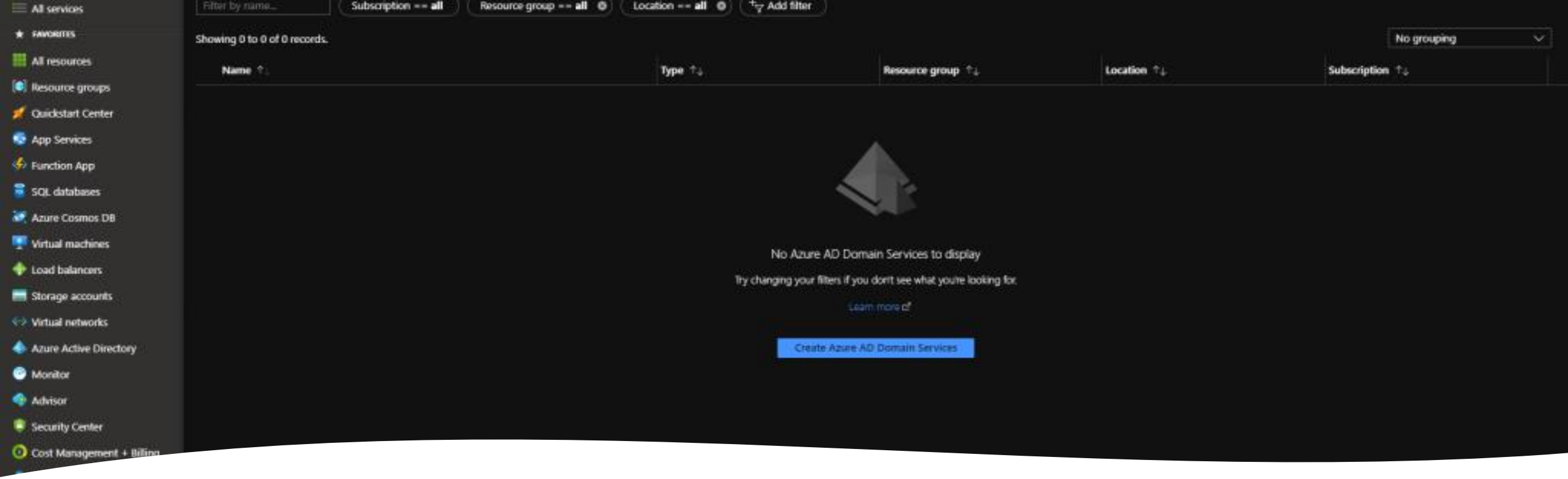
- Accounts in external directories that are linked to your Azure AD will not be available in Azure Active Directory domain services
- Because users and their credentials are synchronized from Azure Active Directory into Azure Active Directory domain services, users only have to remember one set of credentials to sign in and to authenticate against Azure Active Directory domain services.



Azure ADDS Authentication

Azure ADDS supports Kerberos & NTLM authentication.

- Allows you to deploy applications that rely on Windows integrated authentication
- Simplifies lift and shift of applications to Azure

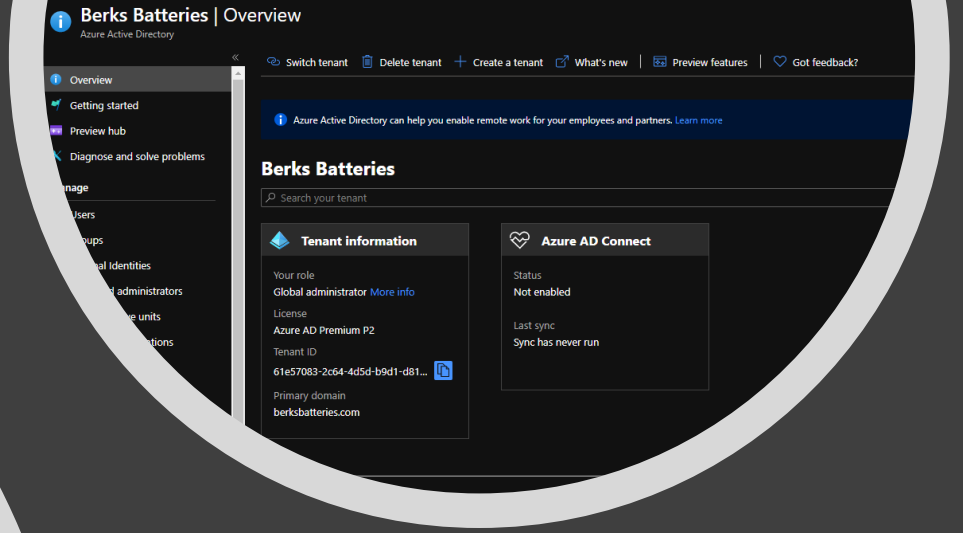


Azure ADDS Availability

Because Azure Active Directory domain services includes multiple domain controllers, the managed domain is always available.

IMPORTANT NOTE!

- An Azure Active Directory domain services managed domain is a **standalone** domain.
- Azure Active Directory domain services managed domain **IS NOT** an extension of an. on-prem Active Directory domain

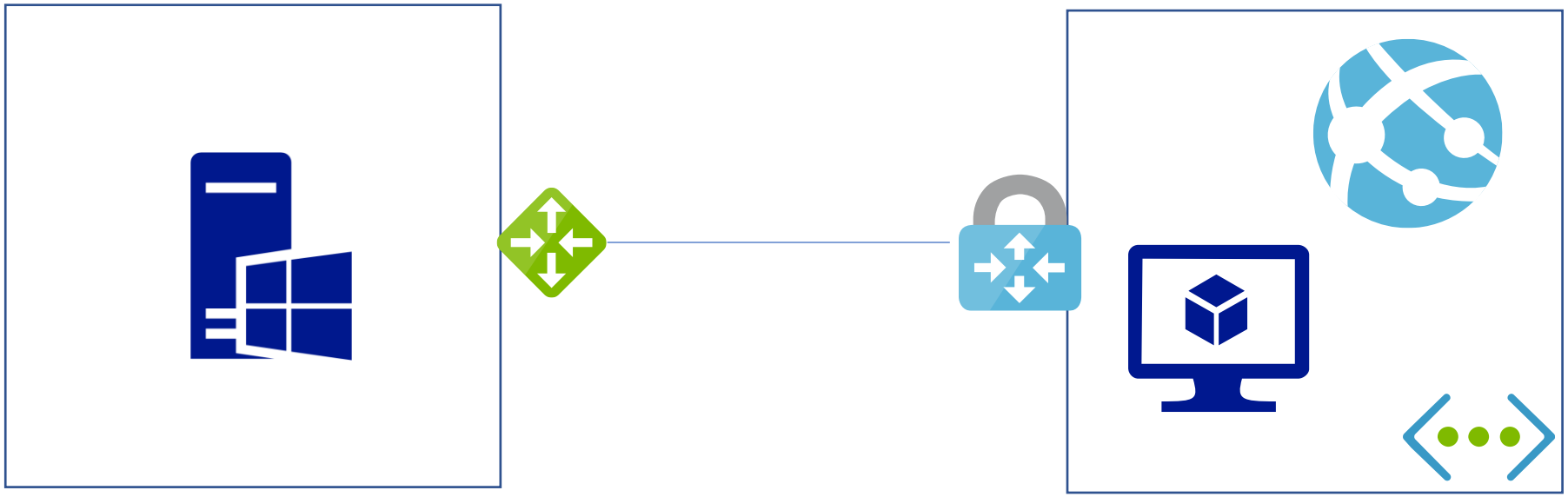


Comparing Identity Solutions

Comparing Identity Solutions

There are several ways that IT administrators can provide identity services to applications that they wish to run in Azure.

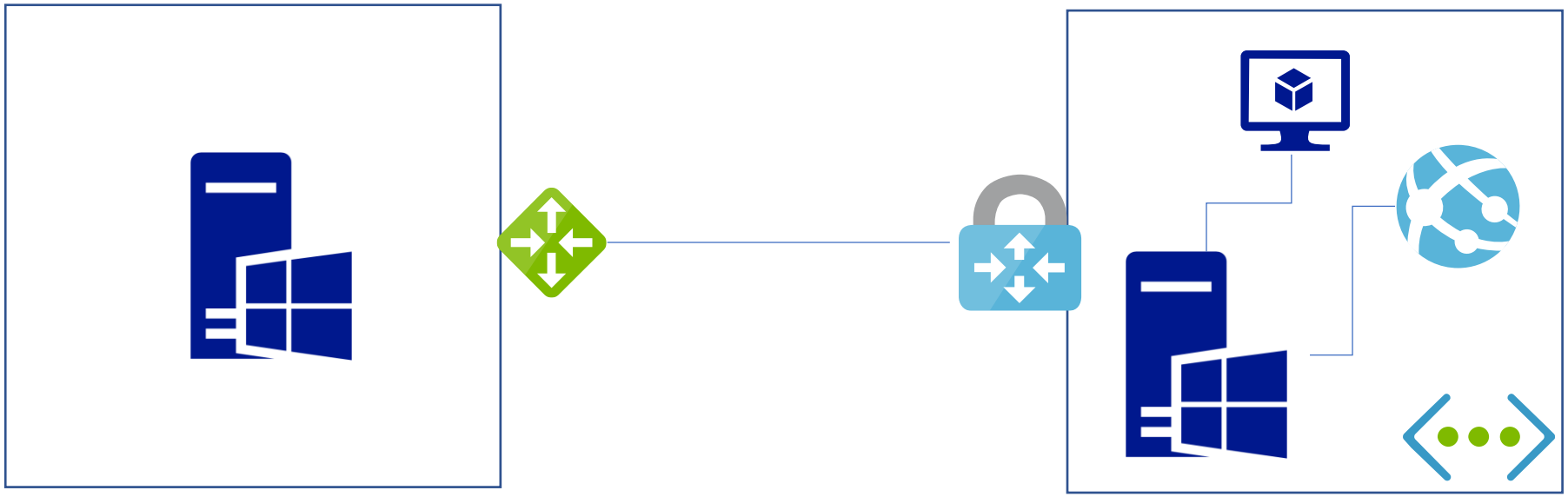
Site-to-Site VPN Between On-Prem Network and Azure



Comparing Identity Solutions

There are several ways that IT administrators can provide identity services to applications that they wish to run in Azure.

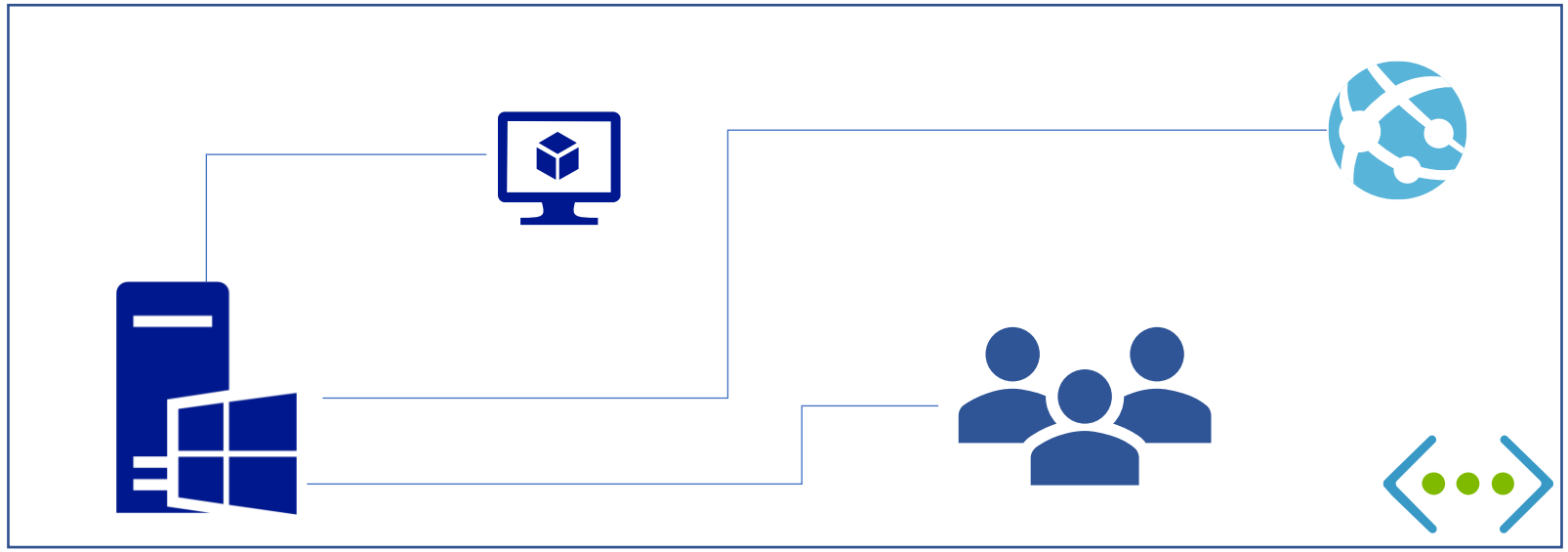
Create Replica Domain Controllers in Azure

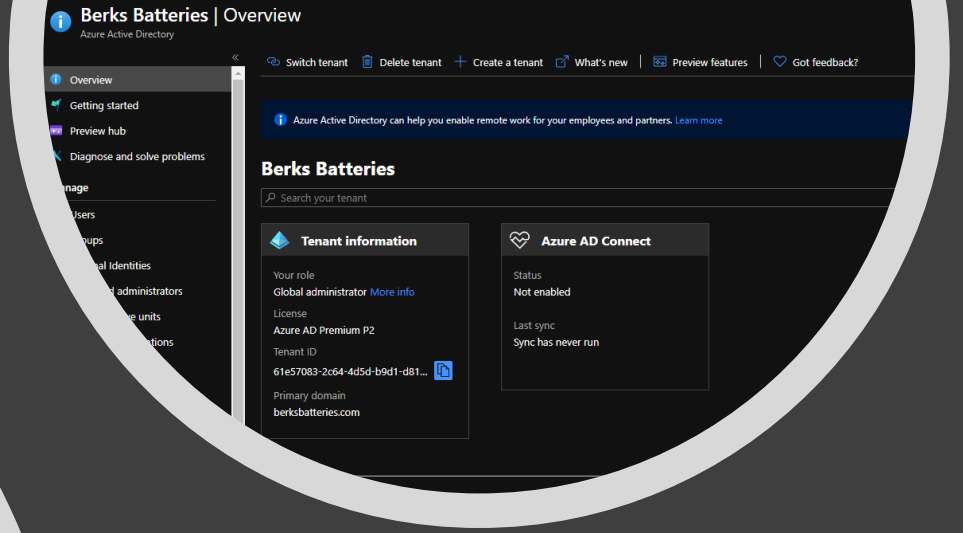


Comparing Identity Solutions

There are several ways that IT administrators can provide identity services to applications that they wish to run in Azure.

Standalone Active Directory Environment in Azure



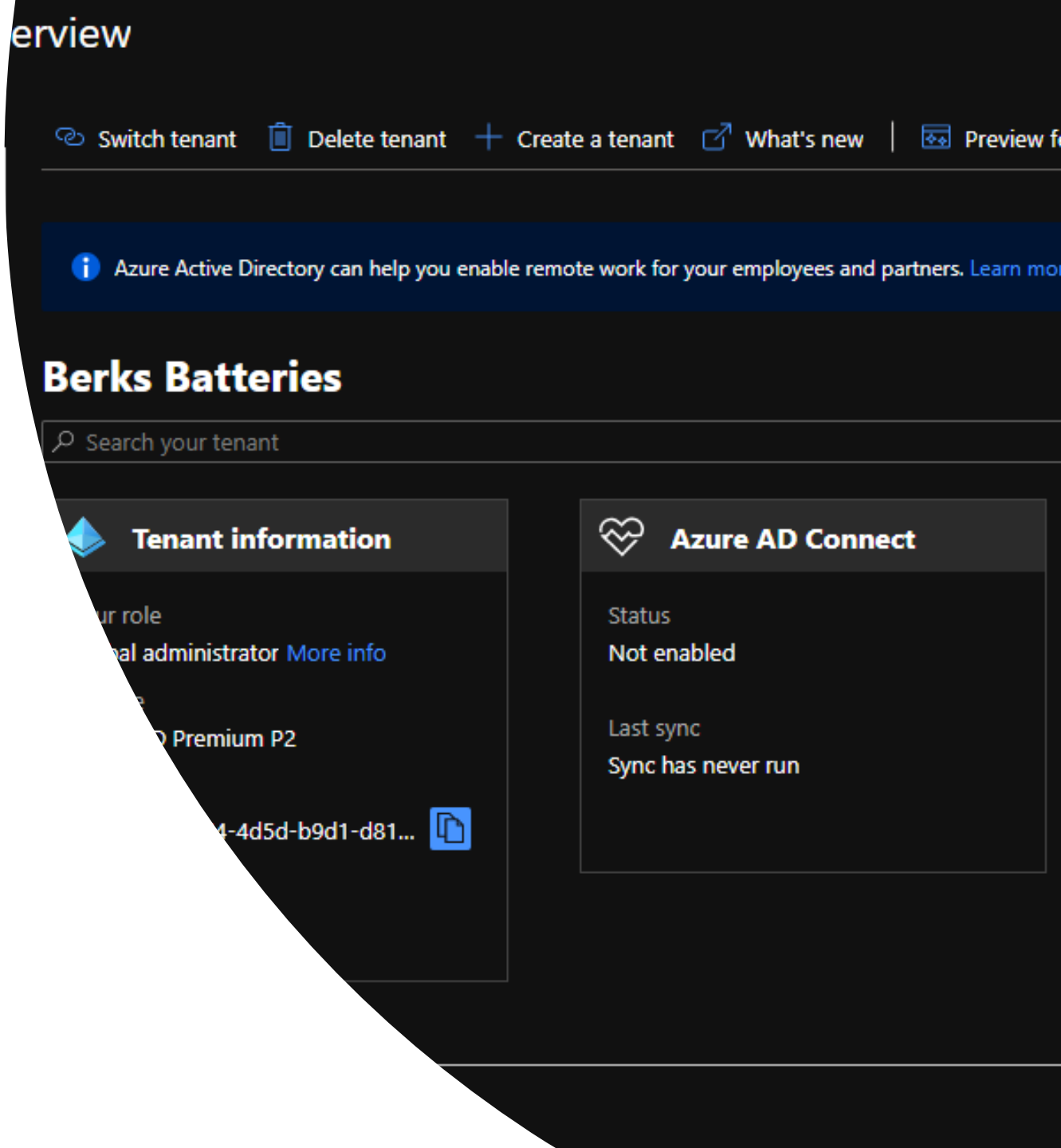


Hybrid Identities

What is Hybrid Identity?

Because organizations are relying more and more on a mixture of on-prem solutions and cloud solutions, it has become necessary to ensure users have access to both those on-prem solutions and those cloud solutions.

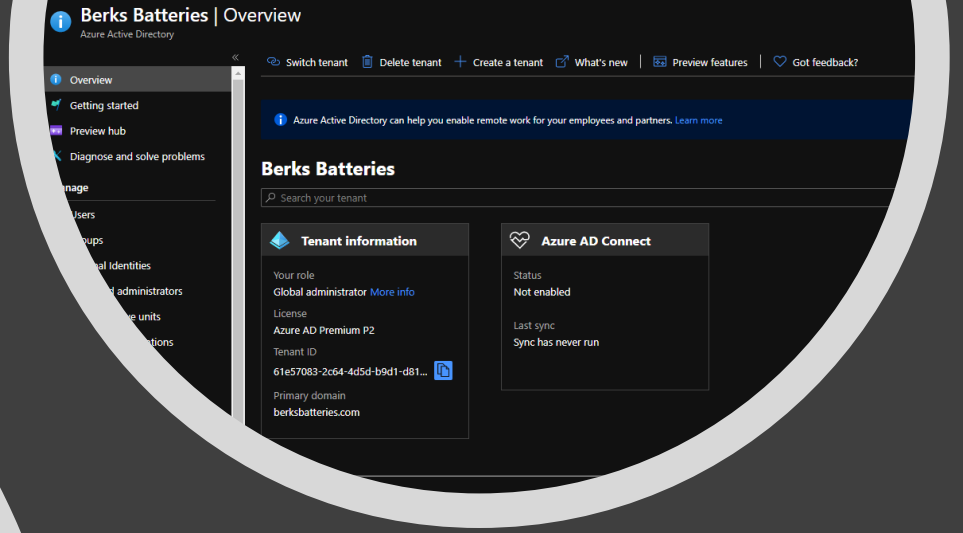
Hybrid Identity is Microsoft's identity solution that can span on-prem and cloud. It creates common user identities that are used for authentication and authorization, regardless of where the user is located.



The 3 Hybrid Identity Methods

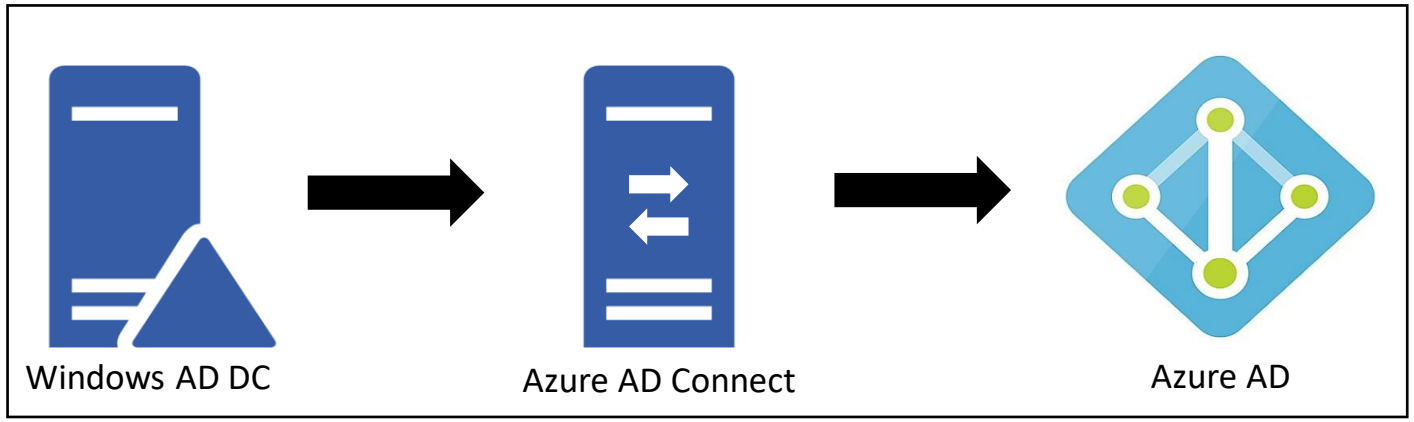
There are **three** methods available that make hybrid identities possible in Azure Active Directory:

- Password hash synchronization (PHS)
- Pass-through authentication (PTA)
- Federation



Intro to Azure AD Connect

Azure AD Connect



Azure AD connect is a software tool that is used to facilitate hybrid identities. It is used to configure:

- Password Hash Synchronization
- Pass-through Authentication
- Federation Integration
- Synchronization
- Health Monitoring

Azure AD Connect

Password Hash Synchronization:

- Synchronizes a hash of your on-prem AD user passwords with Azure AD
- Allows your users to sign into cloud solutions using their on-prem passwords

Pass-through Authentication:

- Allows users to use their on-prem passwords in the cloud
- Does not require the infrastructure of a federated environment

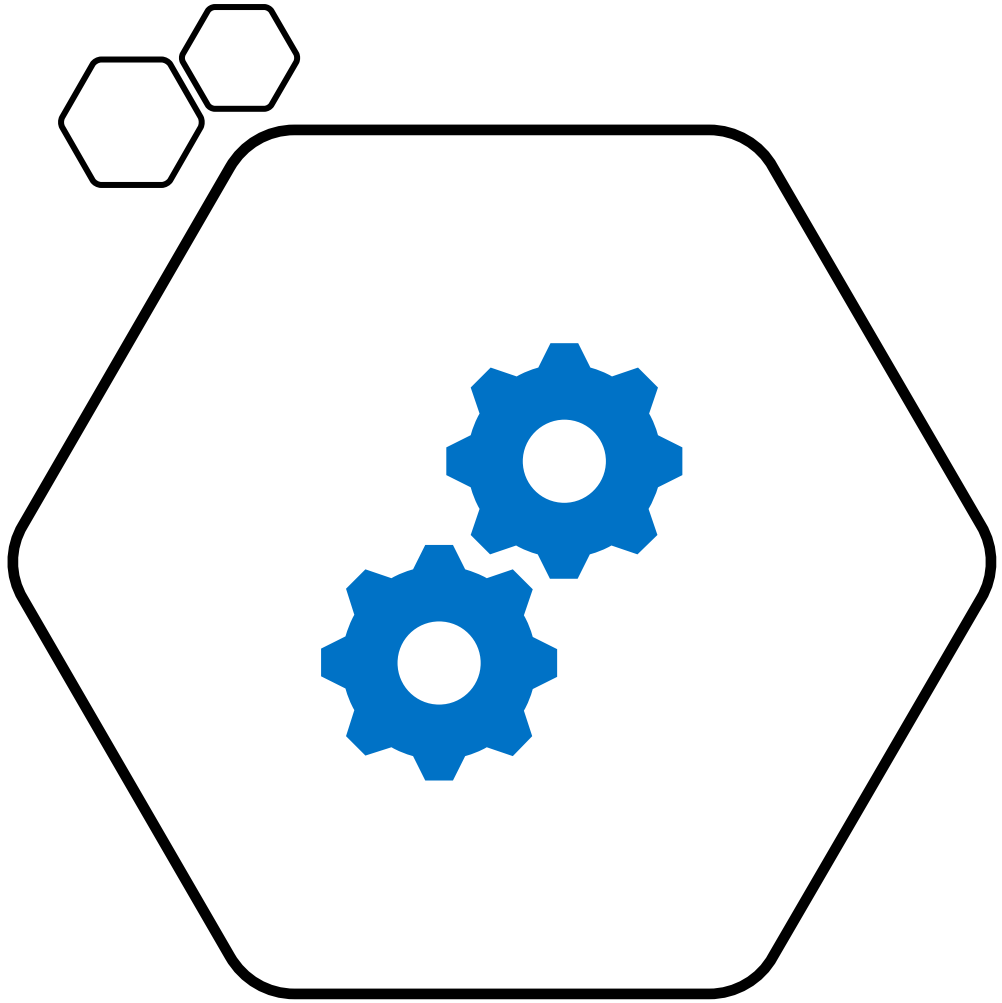
Azure AD Connect

Federation Integration:

- An optional feature included with Azure AD connect
- Used to leverage an on-prem ADFS infrastructure to configure a hybrid environment

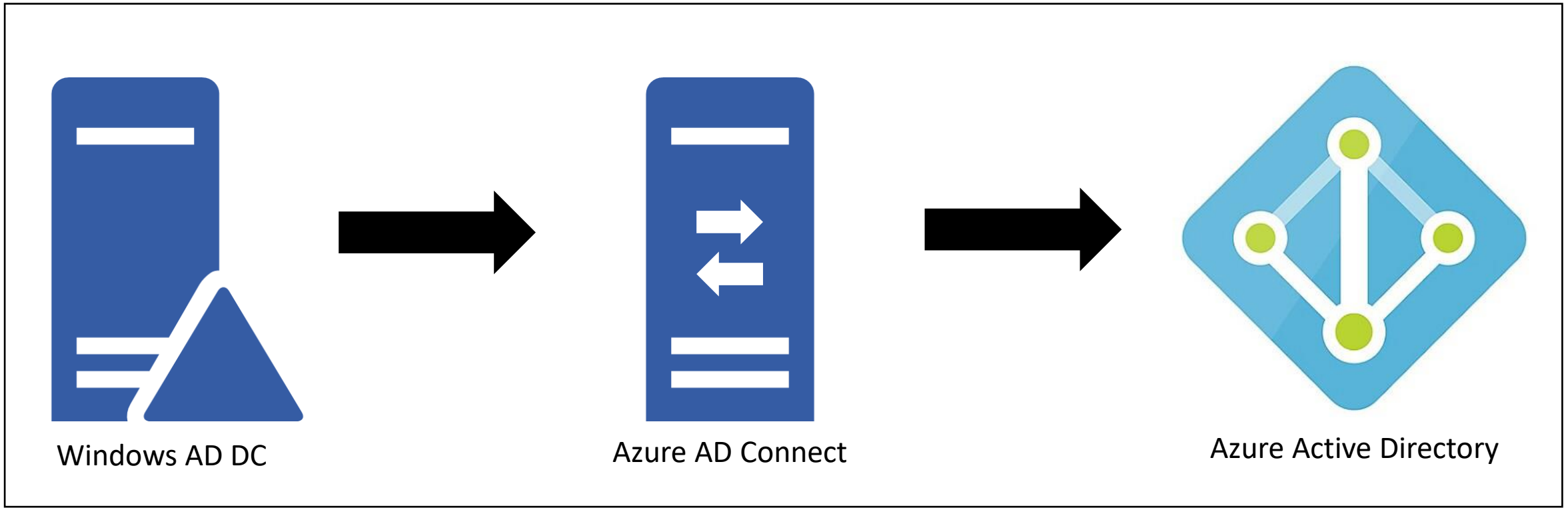
Health Monitoring:

- Provides robust monitoring of the Azure AD connect deployment
- Provides a central location in your Azure portal to view the health of Azure AD connect



Azure AD Connect

- Organizations typically deploy Azure AD connect so that their users can use the same identity to access not only the on-prem applications but also cloud services like Office 365.
- Azure AD connect is free and included in all Azure subscriptions



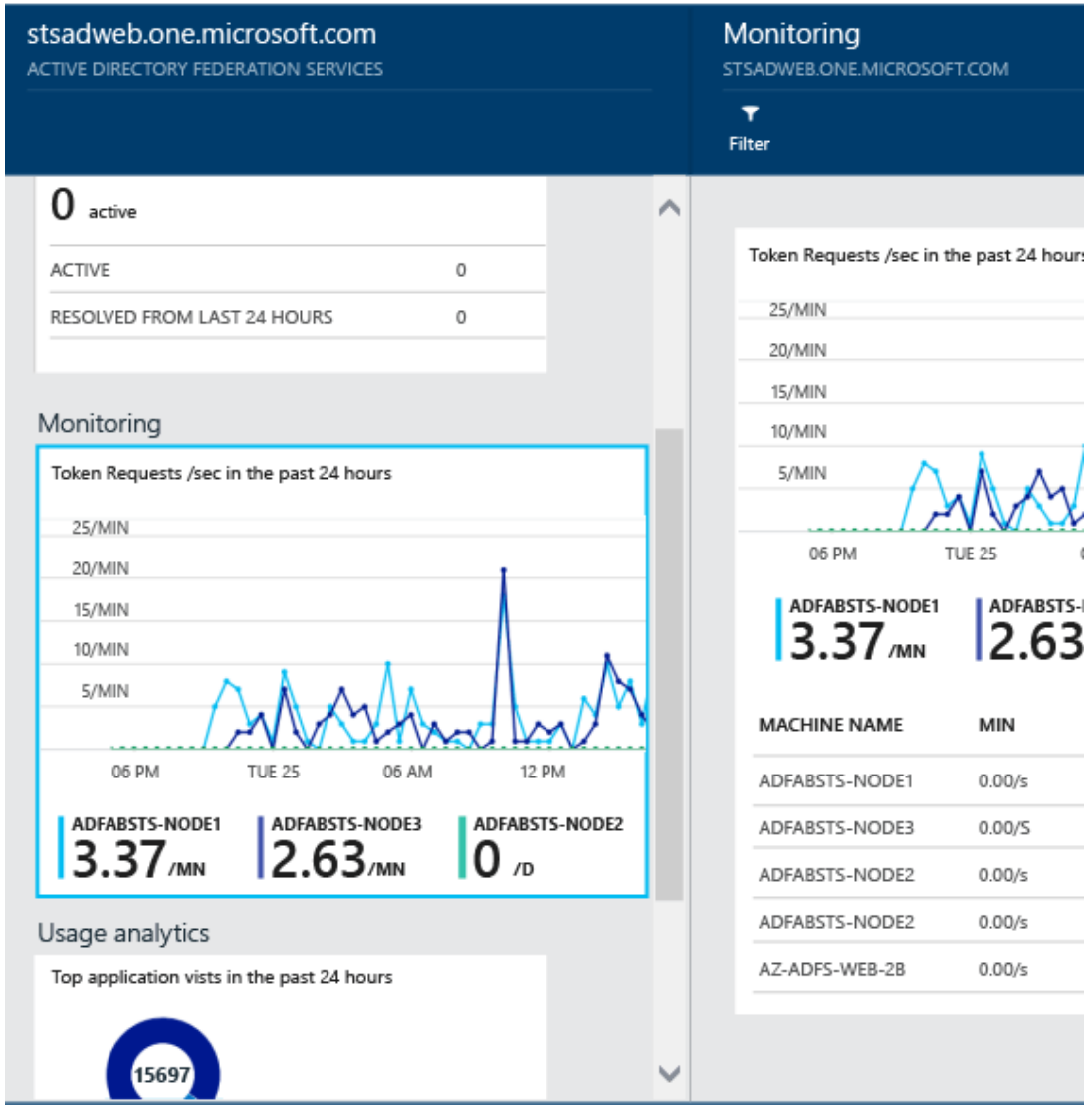
Azure AD Connect Health

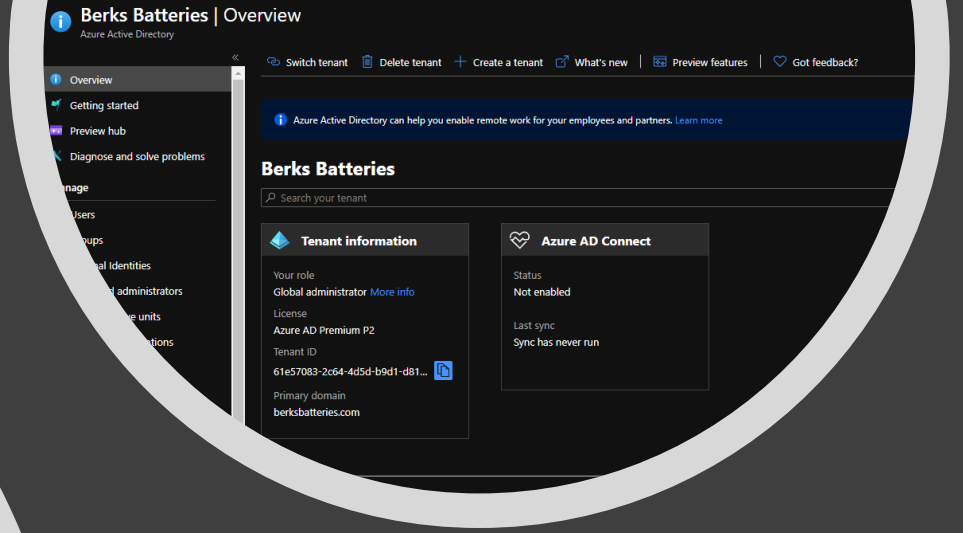
Offers robust monitoring of the on-prem identity infrastructure:

- Helps maintain a reliable connection to Microsoft online services
- View monitoring data in the Azure AD connect health portal

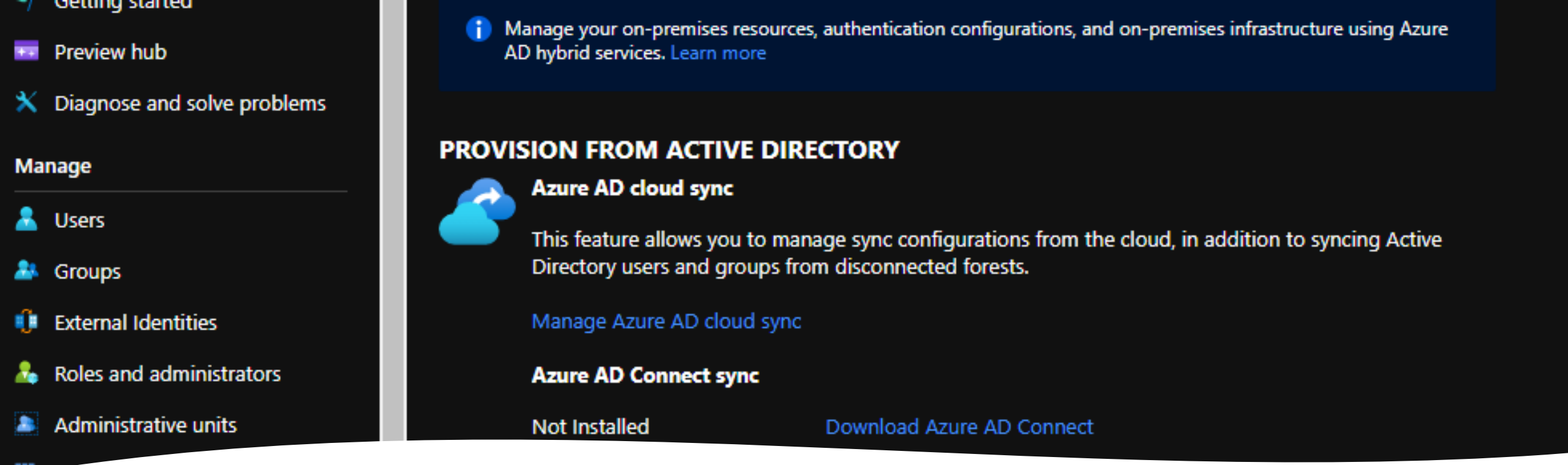
Requires installation of an agent on each on-prem domain controller.

Azure AD connect health requires an Azure AD Premium P1 license.





PHS vs PTA Authentication



Password Hash Synchronization

Password hash synchronization is probably still the most common sign-in method used when hybrid identities are required.

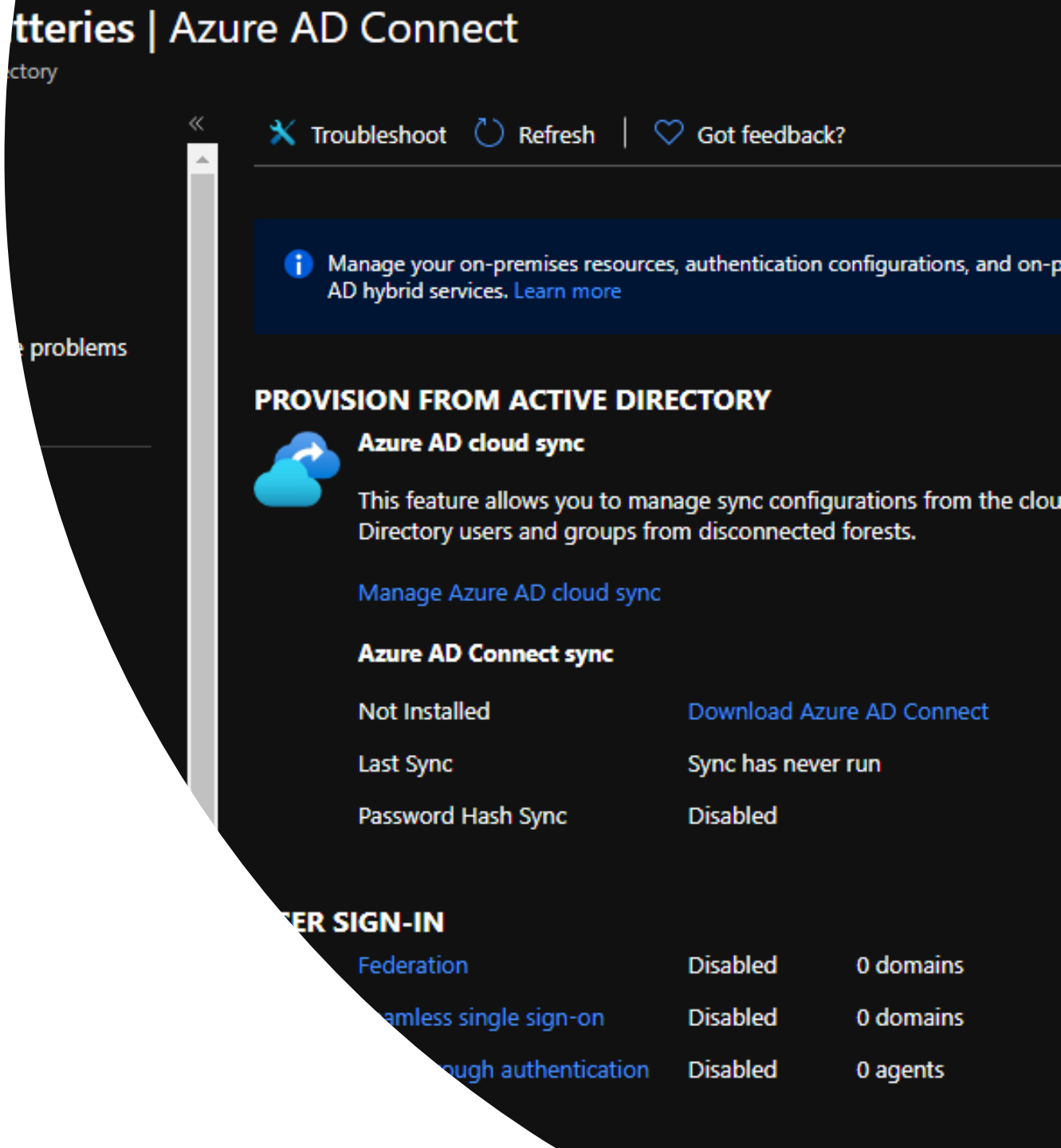
- Azure AD connect synchronizes a hash of the hash of user passwords
- Simplifies sign-on to services like Office 365
- Password hash synchronization helps reduce helpdesk costs
- A good backup to federation with Active Directory federation services

Password Hash Synchronization

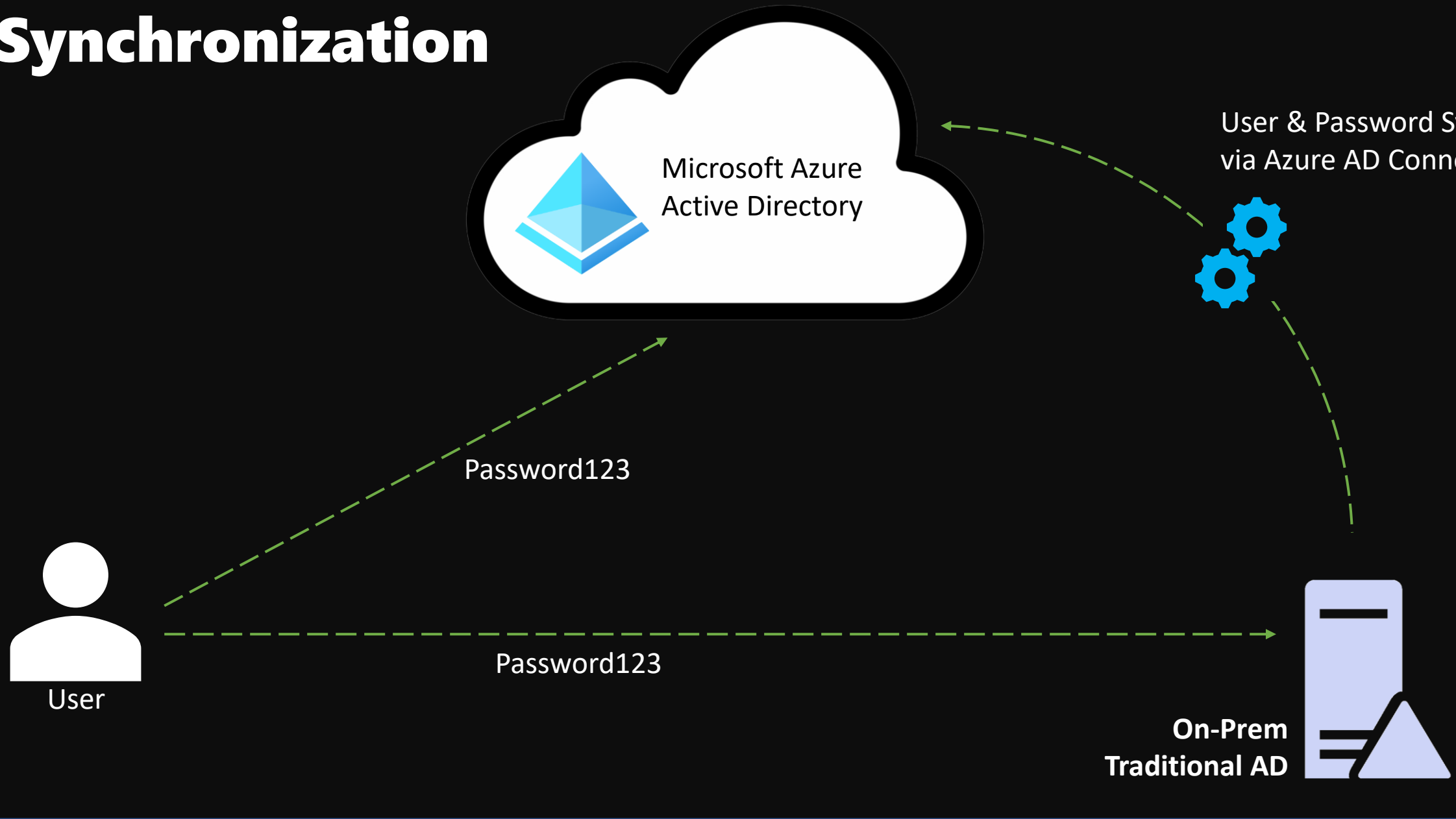
Deploying password hash synchronization is straightforward:

- Deploy Azure AD connect
- Set up synchronization
- Select the password hash synchronization sign in method

Azure AD connect will synchronize on-prem users to Azure Active Directory, along with the hash of the hash of their passwords.



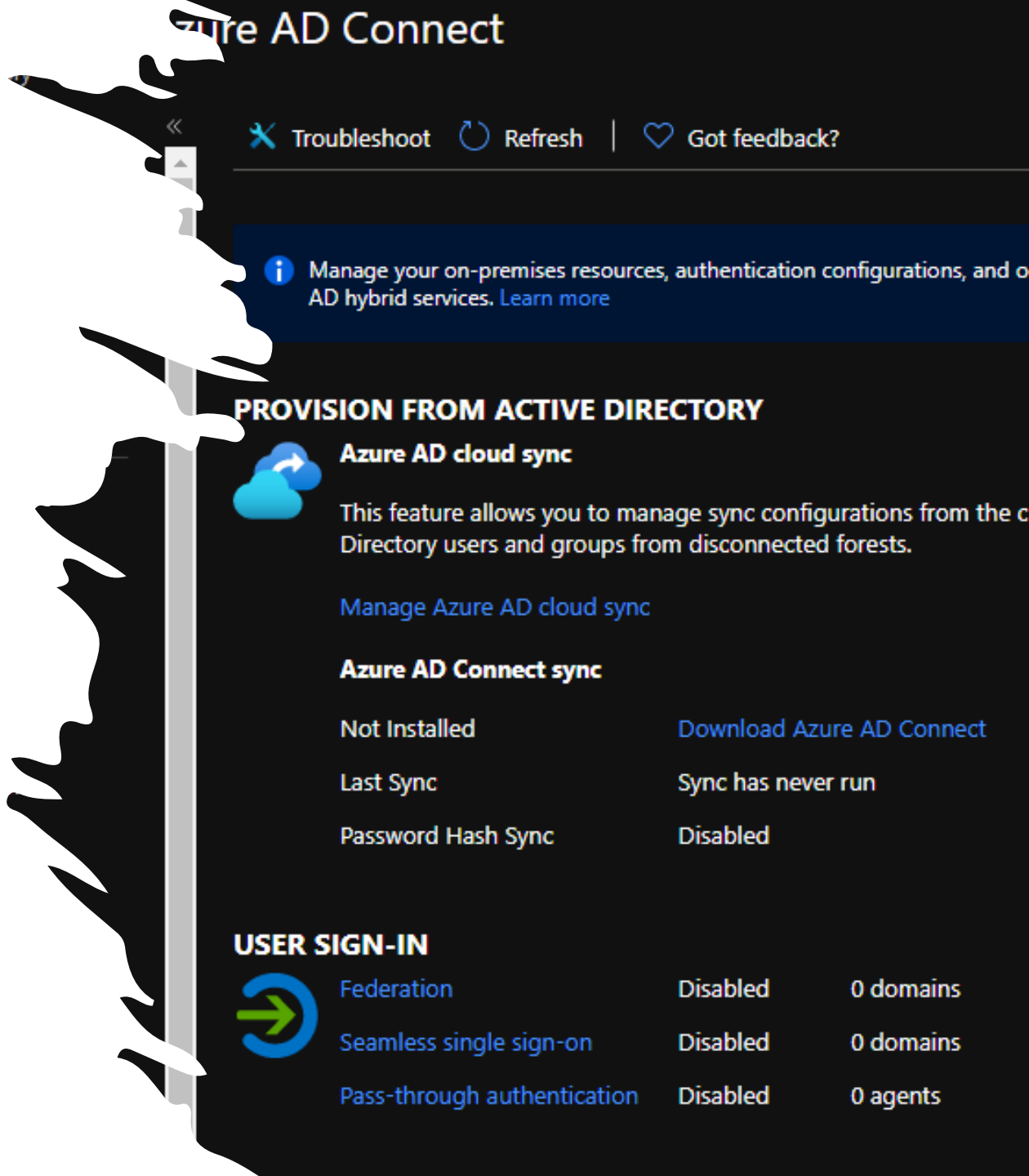
Password Hash Synchronization

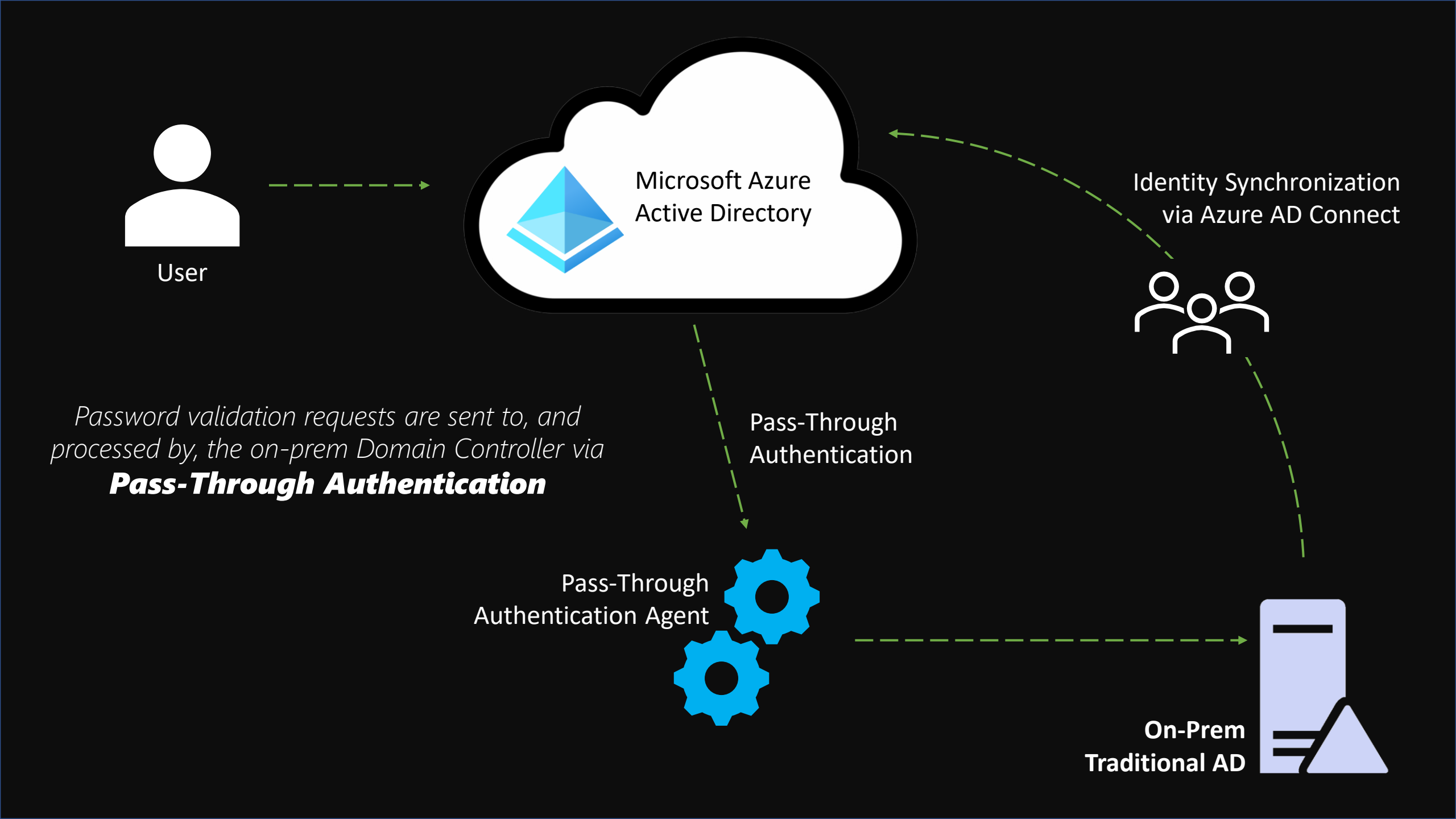


Pass Through Authentication

Pass through authentication provides the same benefit of cloud authentication that password hash synchronization offers, but in a much different way.

- Provides password validation against the on-prem environment
- Requires software agents to be installed on the on-prem domain controllers
- The on-prem servers validate users directly with the on-prem AD
- Password validation is not performed in the cloud



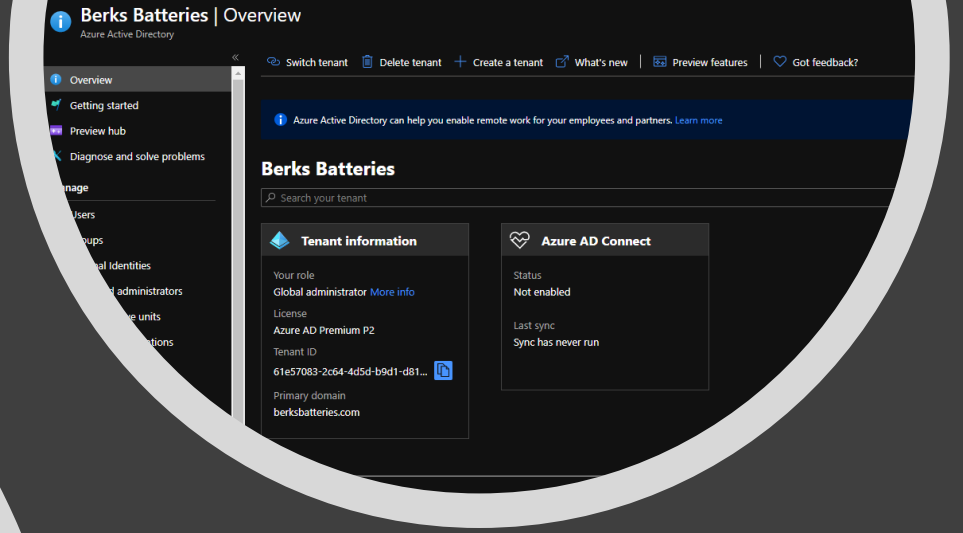

User
Microsoft Azure
Active Directory
Identity Synchronization
via Azure AD Connect
Password validation requests are sent to, and
processed by, the on-prem Domain Controller via
Pass-Through Authentication
Pass-Through
Authentication
Pass-Through
Authentication Agent
On-Prem
Traditional AD

Pass-Through Authentication

Pass through authentication is the solution of choice for organizations with security requirements that mandate immediate enforcement of on-prem user account states, password policies, and sign in hours.

Pass through authentication can be used with the seamless single sign-on feature as well.

Pass through authentication allows users to access applications from their corporate machines inside the corporate network without the need to retype their passwords.



Federation with Azure AD

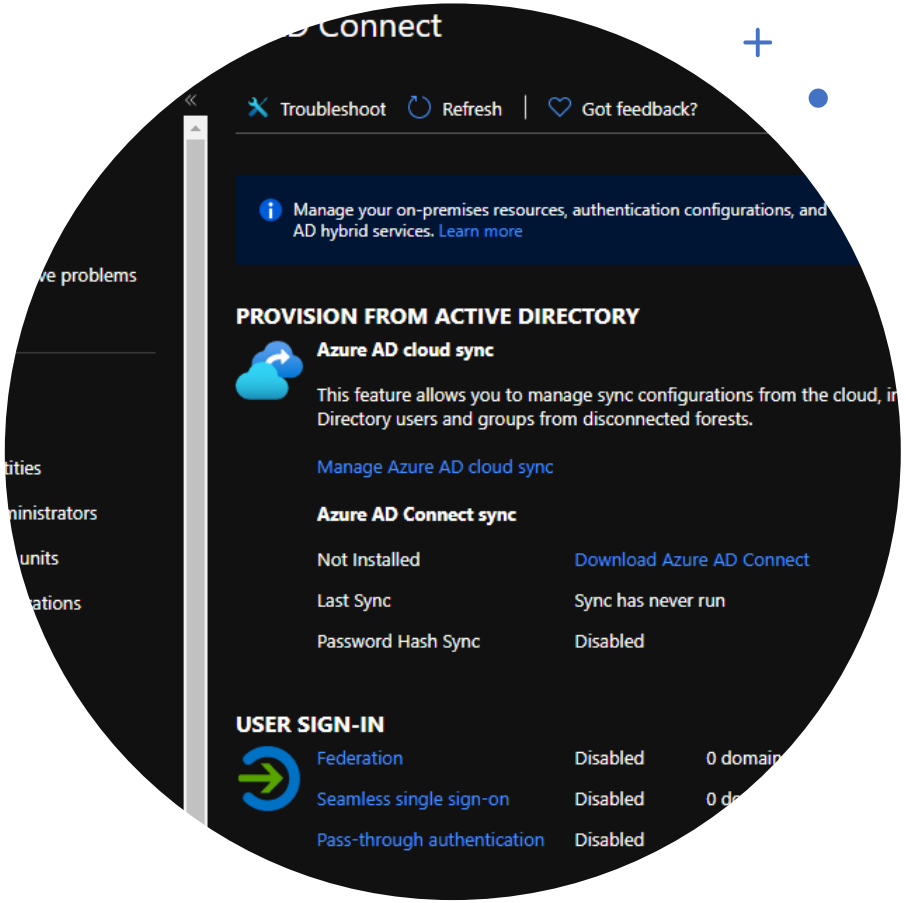
Federation with Azure AD

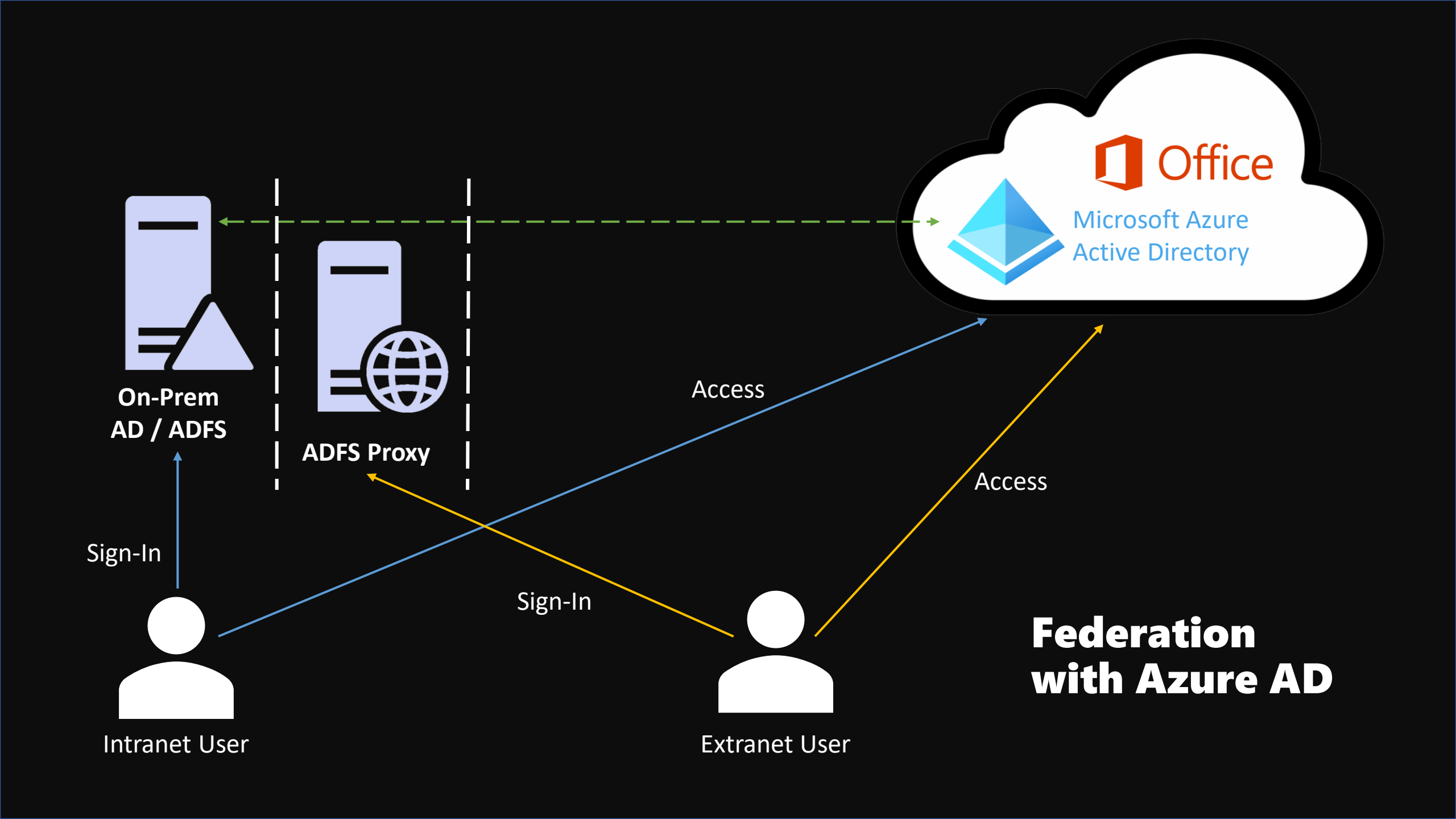
Federation is a collection of domains that trust each other.

- Typically involves one or more organizations
- Used for authentication and for authorization

To Federate an on-prem Active Directory Federation service with Azure AD, you can use Azure AD connect.

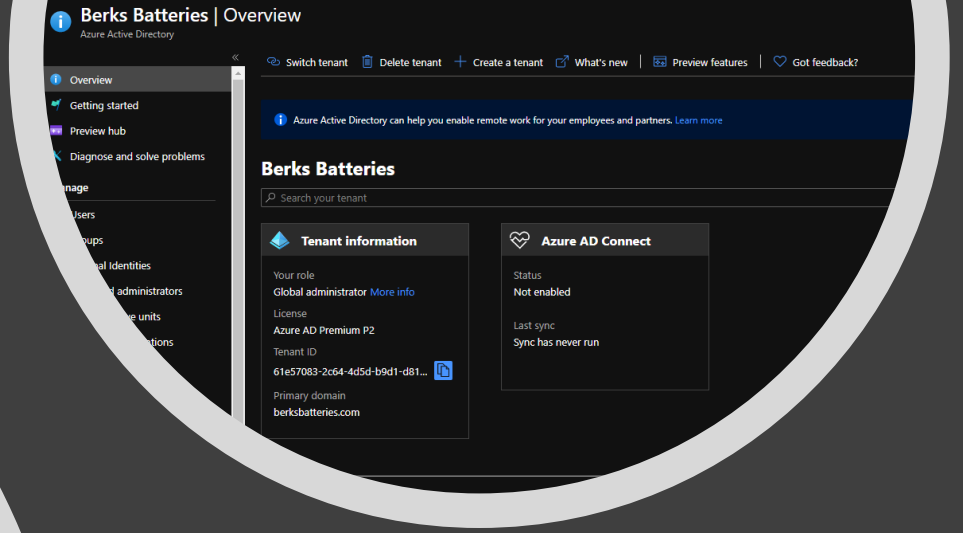
- Users can sign-in to Azure AD based services using on-prem passwords
- Users don't have to re-enter their passwords if on the corporate network



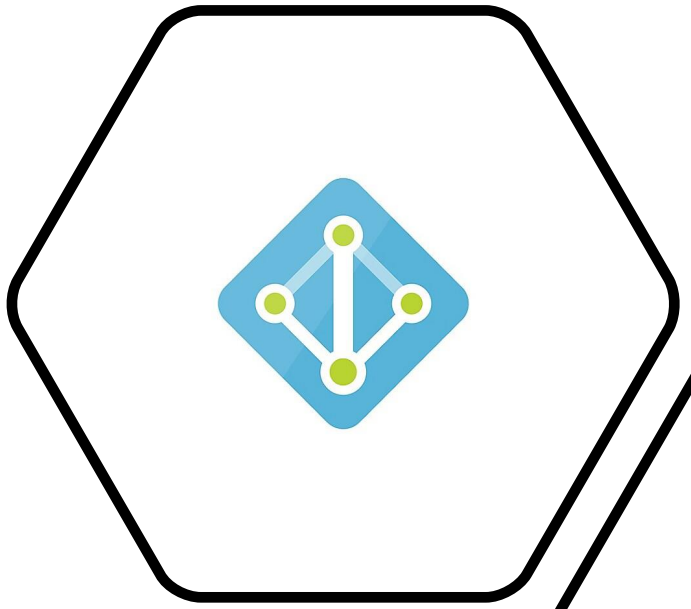

Office
Microsoft Azure
Active Directory
On-Prem
AD / ADFS
ADFS Proxy
Access
Access
Sign-In
Sign-In
Intranet User
Extranet User
Federation
with Azure AD

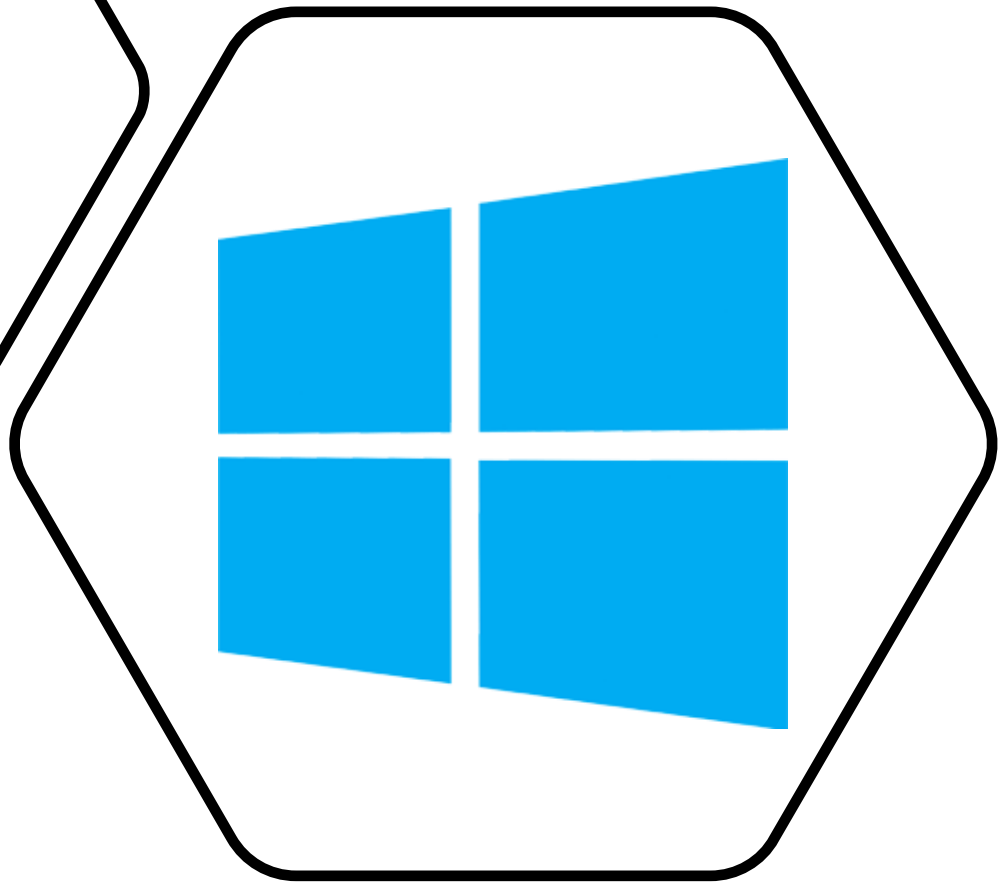
While **Federation** does offer enhanced control, it does involve quite a bit of additional hardware. The hardware required is used to configure an ADFS farm that Azure Active Directory will federate with.

https://docs.Microsoft.com/en-us/Azure/active-directory/hybrid/how-to-connect-fed-whatis



Azure AD vs Traditional AD





Azure AD vs Traditional AD

Azure Active Directory is essentially Microsoft's next iteration of identity and access management for the cloud.

- Identity-as-a-Service solution
- Key differences between traditional AD and Azure Active Directory

User Management: Azure AD vs Traditional AD

Task	Traditional AD	Azure AD
Provision Users		
External Users		
Resource Access		
Admin Management		
Authentication		

User Management: Azure AD vs Traditional AD

Task	Traditional AD	Azure AD
Provision Users	manually or through automated provisioning systems that are hosted in-house	
External Users		
Resource Access		
Admin Management		
Authentication		

User Management: Azure AD vs Traditional AD

Task	Traditional AD	Azure AD
Provision Users	manually or through automated provisioning systems that are hosted in-house	synchronize on-prem user identities into Azure AD OR automatically created in Azure AD through the use of cloud HR systems and through SCIM-enabled software
External Users		
Resource Access		
Admin Management		
Authentication		

User Management: Azure AD vs Traditional AD

Task	Traditional AD	Azure AD
Provision Users	manually or through automated provisioning systems that are hosted in-house	synchronize on-prem user identities into Azure AD OR automatically created in Azure AD through the use of cloud HR systems and through SCIM-enabled software
External Users	Created manually in a dedicated external Active Directory forest	
Resource Access		
Admin Management		
Authentication		

User Management: Azure AD vs Traditional AD

Task	Traditional AD	Azure AD
Provision Users	manually or through automated provisioning systems that are hosted in-house	synchronize on-prem user identities into Azure AD OR automatically created in Azure AD through the use of cloud HR systems and through SCIM-enabled software
External Users	Created manually in a dedicated external Active Directory forest	Azure AD B2B used to manage links to external user identities
Resource Access		
Admin Management		
Authentication		

User Management: Azure AD vs Traditional AD

Task	Traditional AD	Azure AD
Provision Users	manually or through automated provisioning systems that are hosted in-house	synchronize on-prem user identities into Azure AD OR automatically created in Azure AD through the use of cloud HR systems and through SCIM-enabled software
External Users	Created manually in a dedicated external Active Directory forest	Azure AD B2B used to manage links to external user identities
Resource Access	create groups which are granted permissions to resources and then add users to groups	
Admin Management		
Authentication		

User Management: Azure AD vs Traditional AD

Task	Traditional AD	Azure AD
Provision Users	manually or through automated provisioning systems that are hosted in-house	synchronize on-prem user identities into Azure AD OR automatically created in Azure AD through the use of cloud HR systems and through SCIM-enabled software
External Users	Created manually in a dedicated external Active Directory forest	Azure AD B2B used to manage links to external user identities
Resource Access	create groups which are granted permissions to resources and then add users to groups	Access to resources granted through Azure AD groups can OR via the entitlement management feature OR via time-based criteria
Admin Management		
Authentication		

User Management: Azure AD vs Traditional AD

Task	Traditional AD	Azure AD
Provision Users	manually or through automated provisioning systems that are hosted in-house	synchronize on-prem user identities into Azure AD OR automatically created in Azure AD through the use of cloud HR systems and through SCIM-enabled software
External Users	Created manually in a dedicated external Active Directory forest	Azure AD B2B used to manage links to external user identities
Resource Access	create groups which are granted permissions to resources and then add users to groups	Access to resources granted through Azure AD groups can OR via the entitlement management feature OR via time-based criteria
Admin Management	domains, OUs, and groups used to delegate admin privileges	
Authentication		

User Management: Azure AD vs Traditional AD

Task	Traditional AD	Azure AD
Provision Users	manually or through automated provisioning systems that are hosted in-house	synchronize on-prem user identities into Azure AD OR automatically created in Azure AD through the use of cloud HR systems and through SCIM-enabled software
External Users	Created manually in a dedicated external Active Directory forest	Azure AD B2B used to manage links to external user identities
Resource Access	create groups which are granted permissions to resources and then add users to groups	Access to resources granted through Azure AD groups can OR via the entitlement management feature OR via time-based criteria
Admin Management	domains, OUs, and groups used to delegate admin privileges	built-in roles, RBAC, and custom roles used to delegate admin privileges. PIM can also be used.
Authentication		

User Management: Azure AD vs Traditional AD

Task	Traditional AD	Azure AD
Provision Users	manually or through automated provisioning systems that are hosted in-house	synchronize on-prem user identities into Azure AD OR automatically created in Azure AD through the use of cloud HR systems and through SCIM-enabled software
External Users	Created manually in a dedicated external Active Directory forest	Azure AD B2B used to manage links to external user identities
Resource Access	create groups which are granted permissions to resources and then add users to groups	Access to resources granted through Azure AD groups can OR via the entitlement management feature OR via time-based criteria
Admin Management	domains, OUs, and groups used to delegate admin privileges	built-in roles, RBAC, and custom roles used to delegate admin privileges. PIM can also be used.
Authentication	credentials based on passwords, certificates, smart cards, and are managed with password policies	

User Management: Azure AD vs Traditional AD

Task	Traditional AD	Azure AD
Provision Users	manually or through automated provisioning systems that are hosted in-house	synchronize on-prem user identities into Azure AD OR automatically created in Azure AD through the use of cloud HR systems and through SCIM-enabled software
External Users	Created manually in a dedicated external Active Directory forest	Azure AD B2B used to manage links to external user identities
Resource Access	create groups which are granted permissions to resources and then add users to groups	Access to resources granted through Azure AD groups can OR via the entitlement management feature OR via time-based criteria
Admin Management	domains, OUs, and groups used to delegate admin privileges	built-in roles, RBAC, and custom roles used to delegate admin privileges. PIM can also be used.
Authentication	credentials based on passwords, certificates, smart cards, and are managed with password policies	uses intelligent password protection, MFA, and self-service password reset

Applications: Azure AD vs Traditional AD

Task	Traditional AD	Azure AD
SaaS		
Services		

Applications: Azure AD vs Traditional AD

Task	Traditional AD	Azure AD
SaaS	Not supported natively; require ADFS federation; more administrative overhead and additional hardware costs	
Services		

Applications: Azure AD vs Traditional AD

Task	Traditional AD	Azure AD
SaaS	Not supported natively; require ADFS federation; more administrative overhead and additional hardware costs	allows SaaS applications to be integrated, provided they support OAuth2, SAML, or WS-* authentication
Services		

Applications: Azure AD vs Traditional AD

Task	Traditional AD	Azure AD
SaaS	Not supported natively; require ADFS federation; more administrative overhead and additional hardware costs	allows SaaS applications to be integrated, provided they support OAuth2, SAML, or WS-* authentication
Services	Usually require Active Directory service accounts to run; creates a security hole	

Applications: Azure AD vs Traditional AD

Task	Traditional AD	Azure AD
SaaS	Not supported natively; require ADFS federation; more administrative overhead and additional hardware costs	allows SaaS applications to be integrated, provided they support OAuth2, SAML, or WS-* authentication
Services	Usually require Active Directory service accounts to run; creates a security hole	leverages managed identities that are managed by Azure AD and are tied to the resource provider; can't be used to gain backdoor access

Devices: Azure AD vs Traditional AD

Task	Traditional AD	Azure AD
Mobile Devices		
Windows Desktops		
Windows Servers		
Linux Workloads		
Authentication		

Devices: Azure AD vs Traditional AD

Task	Traditional AD	Azure AD
Mobile Devices	does not natively support them	
Windows Desktops		
Windows Servers		
Linux Workloads		
Authentication		

Devices: Azure AD vs Traditional AD

Task	Traditional AD	Azure AD
Mobile Devices	does not natively support them	provides integration with Microsoft InTune
Windows Desktops		
Windows Servers		
Linux Workloads		
Authentication		

Devices: Azure AD vs Traditional AD

Task	Traditional AD	Azure AD
Mobile Devices	does not natively support them	provides integration with Microsoft InTune
Windows Desktops	Can be joined to the domain and managed with group policy	
Windows Servers		
Linux Workloads		
Authentication		

Devices: Azure AD vs Traditional AD

Task	Traditional AD	Azure AD
Mobile Devices	does not natively support them	provides integration with Microsoft InTune
Windows Desktops	Can be joined to the domain and managed with group policy	Can be joined to the domain and managed with Microsoft InTune
Windows Servers		
Linux Workloads		
Authentication		

Devices: Azure AD vs Traditional AD

Task	Traditional AD	Azure AD
Mobile Devices	does not natively support them	provides integration with Microsoft InTune
Windows Desktops	Can be joined to the domain and managed with group policy	Can be joined to the domain and managed with Microsoft InTune
Windows Servers	Can be joined to the domain and managed with group policy	
Linux Workloads		
Authentication		

Devices: Azure AD vs Traditional AD

Task	Traditional AD	Azure AD
Mobile Devices	does not natively support them	provides integration with Microsoft InTune
Windows Desktops	Can be joined to the domain and managed with group policy	Can be joined to the domain and managed with Microsoft InTune
Windows Servers	Can be joined to the domain and managed with group policy	cannot be joined to an Azure Active Directory
Linux Workloads		
Authentication		

Devices: Azure AD vs Traditional AD

Task	Traditional AD	Azure AD
Mobile Devices	does not natively support them	provides integration with Microsoft InTune
Windows Desktops	Can be joined to the domain and managed with group policy	Can be joined to the domain and managed with Microsoft InTune
Windows Servers	Can be joined to the domain and managed with group policy	cannot be joined to an Azure Active Directory
Linux Workloads	does not support Linux workloads natively	
Authentication		

Devices: Azure AD vs Traditional AD

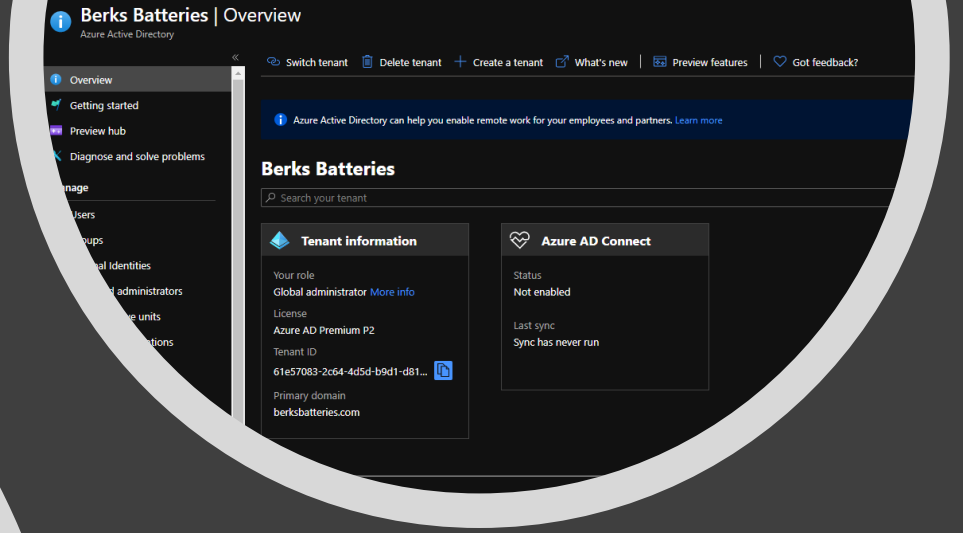
Task	Traditional AD	Azure AD
Mobile Devices	does not natively support them	provides integration with Microsoft InTune
Windows Desktops	Can be joined to the domain and managed with group policy	Can be joined to the domain and managed with Microsoft InTune
Windows Servers	Can be joined to the domain and managed with group policy	cannot be joined to an Azure Active Directory
Linux Workloads	does not support Linux workloads natively	Linux and UNIX virtual machines in Azure can leverage managed identities to access resources
Authentication		

Devices: Azure AD vs Traditional AD

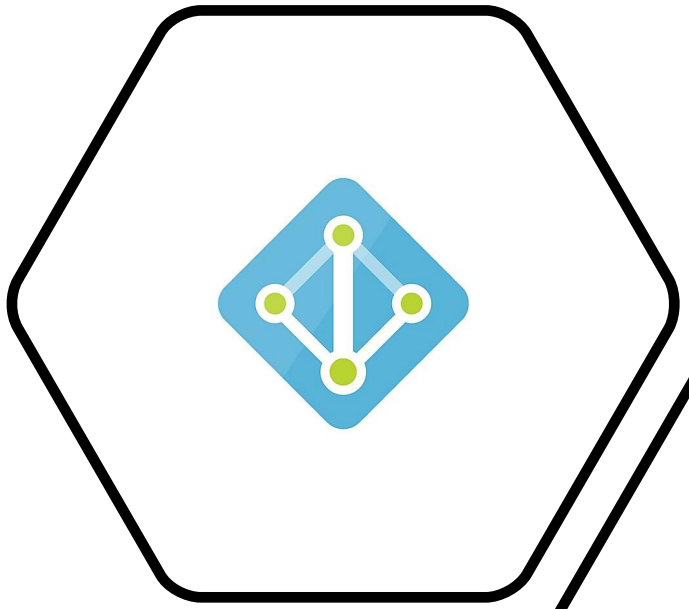
Task	Traditional AD	Azure AD
Mobile Devices	does not natively support them	provides integration with Microsoft InTune
Windows Desktops	Can be joined to the domain and managed with group policy	Can be joined to the domain and managed with Microsoft InTune
Windows Servers	Can be joined to the domain and managed with group policy	cannot be joined to an Azure Active Directory
Linux Workloads	does not support Linux workloads natively	Linux and UNIX virtual machines in Azure can leverage managed identities to access resources
Authentication	credentials based on passwords, certificates, smart cards, and are managed with password policies	

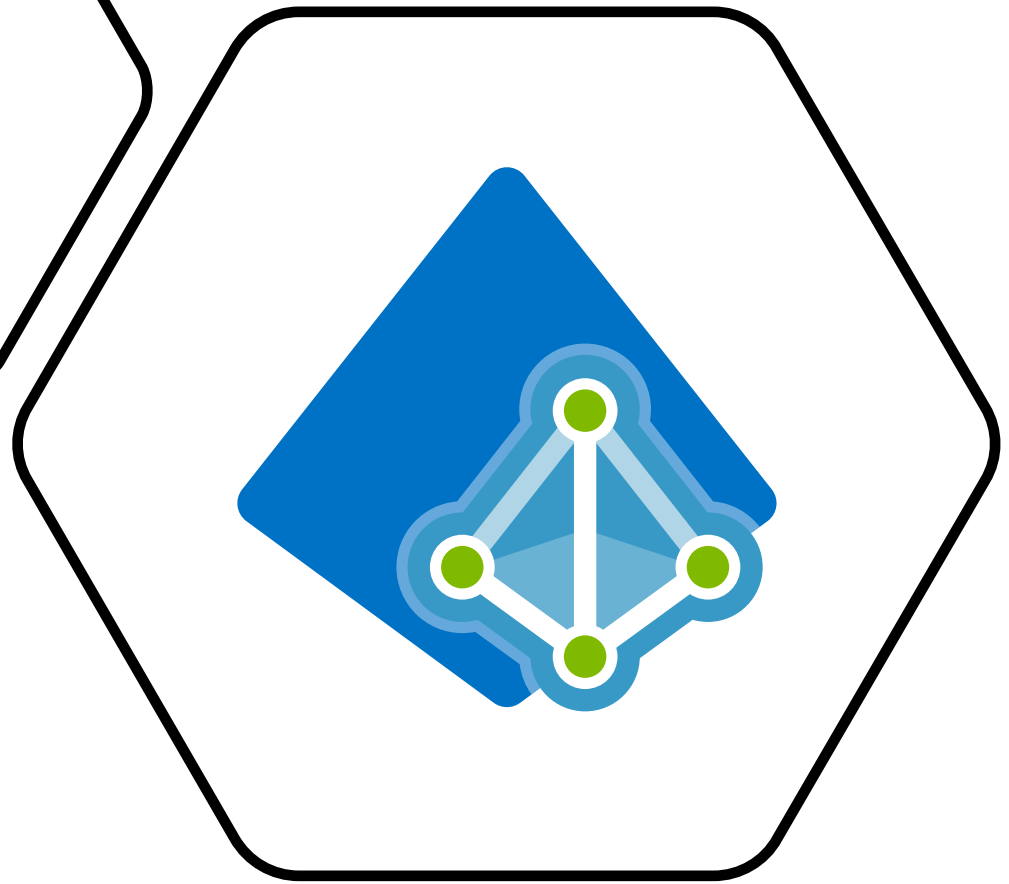
Devices: Azure AD vs Traditional AD

Task	Traditional AD	Azure AD
Mobile Devices	does not natively support them	provides integration with Microsoft InTune
Windows Desktops	Can be joined to the domain and managed with group policy	Can be joined to the domain and managed with Microsoft InTune
Windows Servers	Can be joined to the domain and managed with group policy	cannot be joined to an Azure Active Directory
Linux Workloads	does not support Linux workloads natively	Linux and UNIX virtual machines in Azure can leverage managed identities to access resources
Authentication	credentials based on passwords, certificates, smart cards, and are managed with password policies	uses intelligent password protection, MFA, and self-service password reset



Azure AD vs Azure ADDS





Azure AD vs Azure ADDS

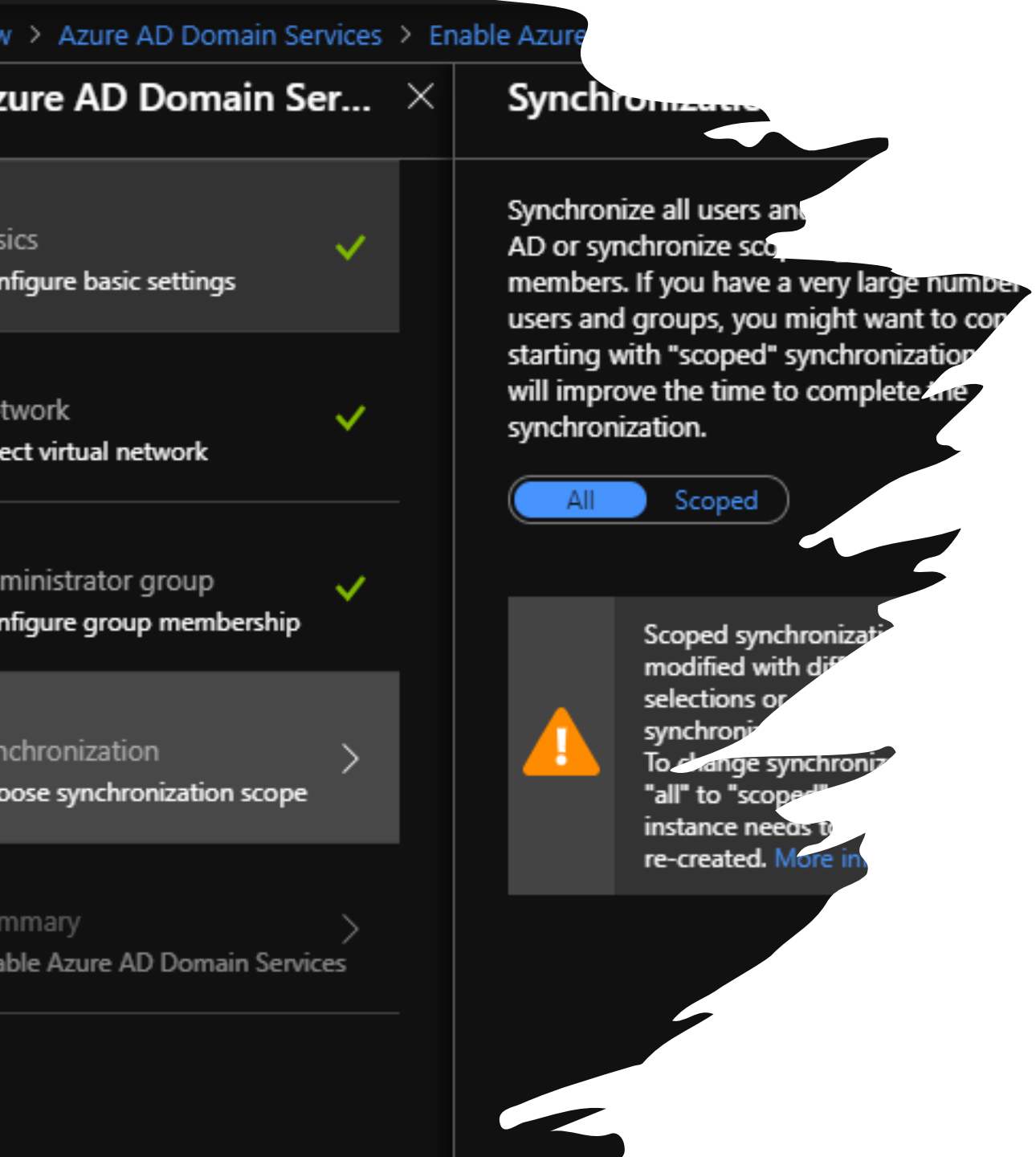
Azure Active Directory and Azure AD domain services share common names and technologies but are really are two different offerings that are designed to provide different services.

Azure Active Directory

Azure Active Directory is a cloud-based identity and mobile device management solution.

Provides user account and authentication services.

Synchronize traditional on-prem AD to Azure AD to provide a single identity solution.

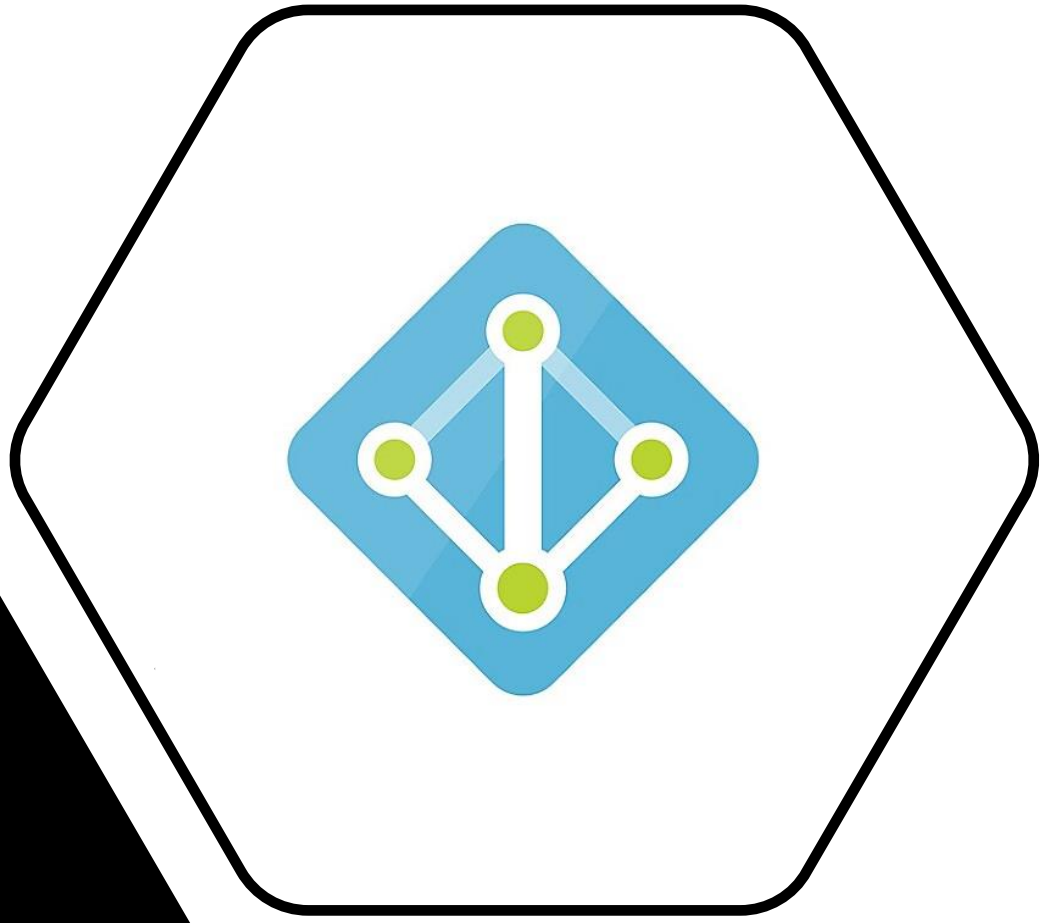


Azure AD Domain Services

Azure AD Domain Services is a fully-managed domain services offering.

- Includes a fully-compatible subset of features found in a traditional AD
  - Domain Join
  - Group Policy
  - LDAP
  - Kerberos & NTLM Authentication
- Integrates with Azure AD
- Can be synchronized with Azure AD

Azure AD
vs Azure AD DS



When you deploy Azure Active Directory, it allows you to manage the identity of the devices that are used by the organization and to control access to resources from such devices.

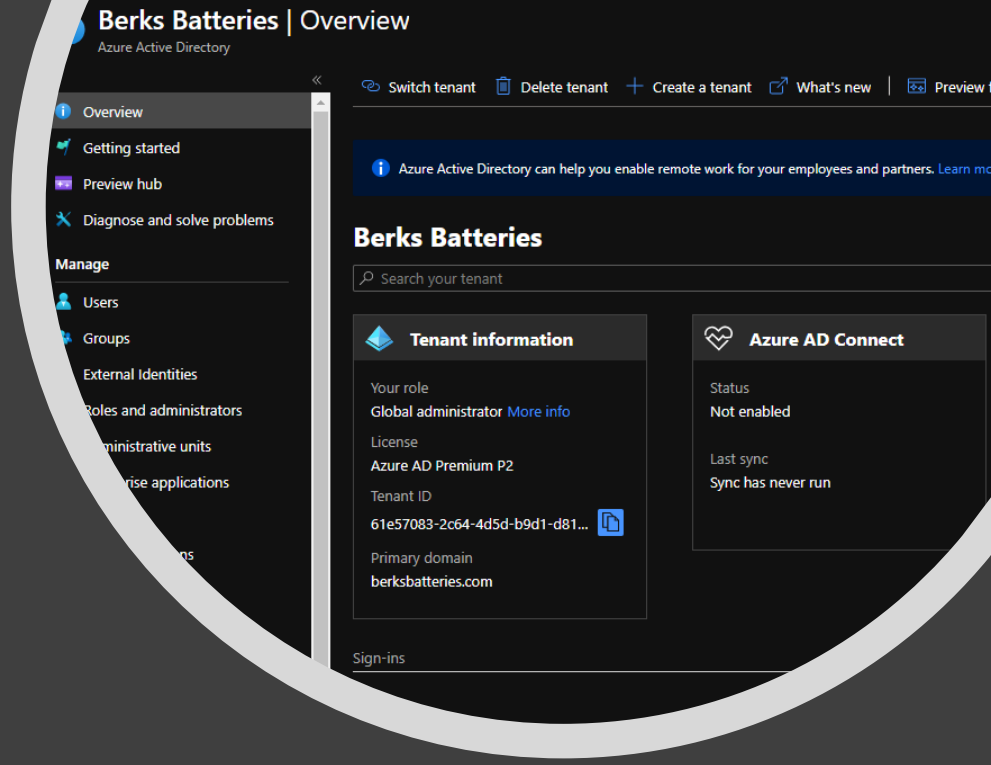
Azure AD vs Azure AD DS

Azure Active Directory allows users to register their personal devices with the directory.

- Creates identities for devices that can be authenticated by Azure AD
- Device management is performed via MDM software like Microsoft InTune

Computers & laptops can be joined to Azure AD.

- Provides the same benefits as registering personal devices with Azure AD
- Secure applications with single sign-on
- Leverage enterprise policy compliant roaming of user settings across different devices

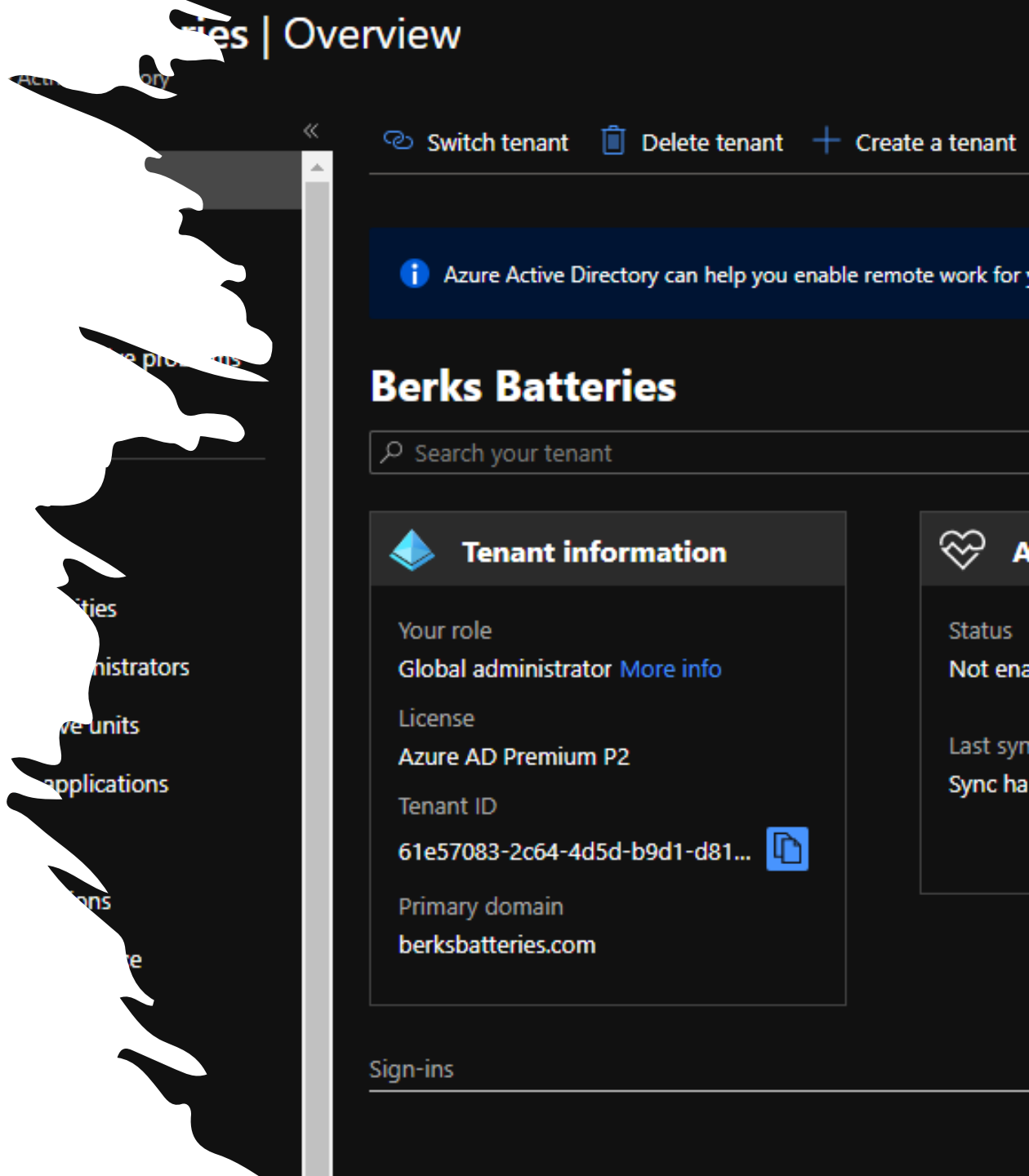


Azure AD
vs Azure AD DS

When a user with an Azure AD joined or Azure AD register device authenticates, that authentication is performed via modern OAuth or open ID connect based protocols.

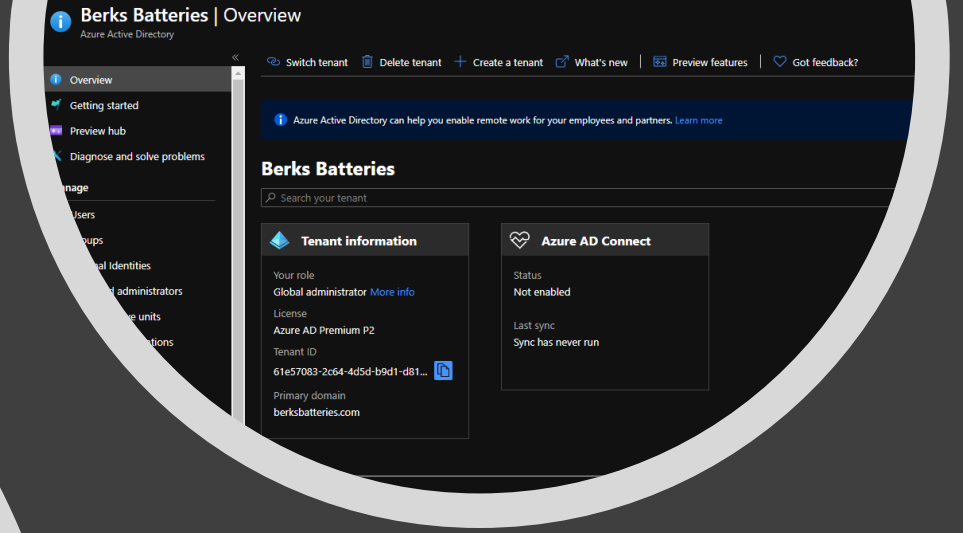
HOWEVER...

When a user authenticates from an Azure AD domain services joined device, applications can use Kerberos and NTLM protocols for authentication instead.

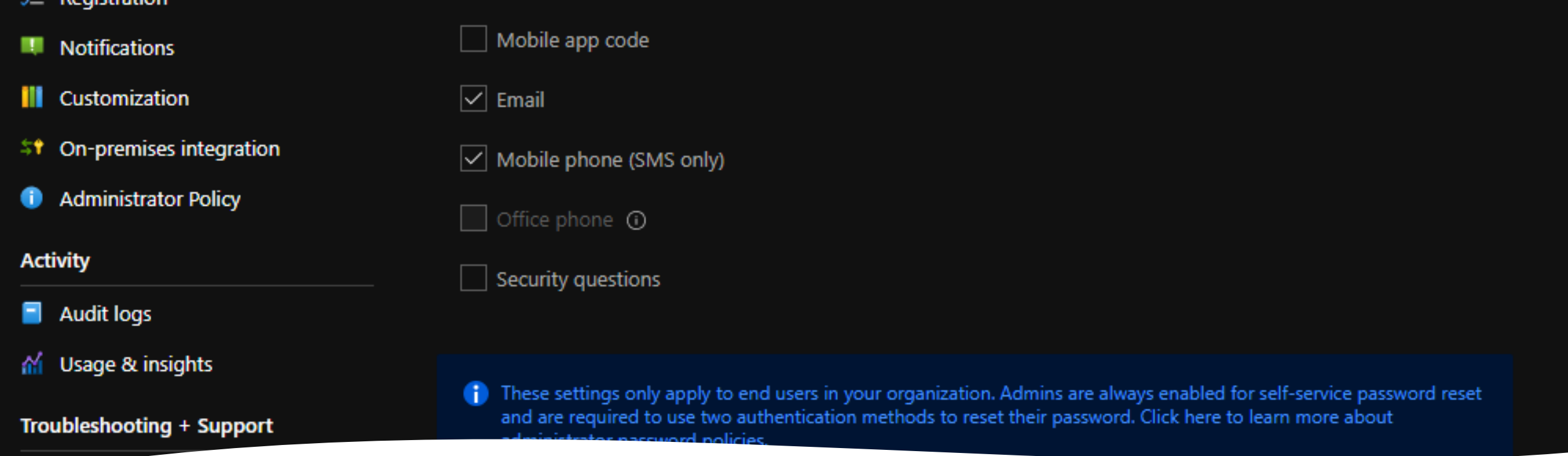


Azure AD vs Azure AD DS

Aspect	**Azure AD-joined**	**Azure AD DS-joined**
Device controlled by	Azure AD	Azure AD DS managed domain
Representation in the directory	Device objects in the Azure AD directory	Computer objects in the Azure AD DS managed domain
Authentication	OAuth / OpenID Connect based protocols	Kerberos and NTLM protocols
Management	Mobile Device Management (MDM) software like InTune	Group Policy
Networking	Works over the internet	Must be connected to, or peered with, the virtual network where the managed domain is deployed



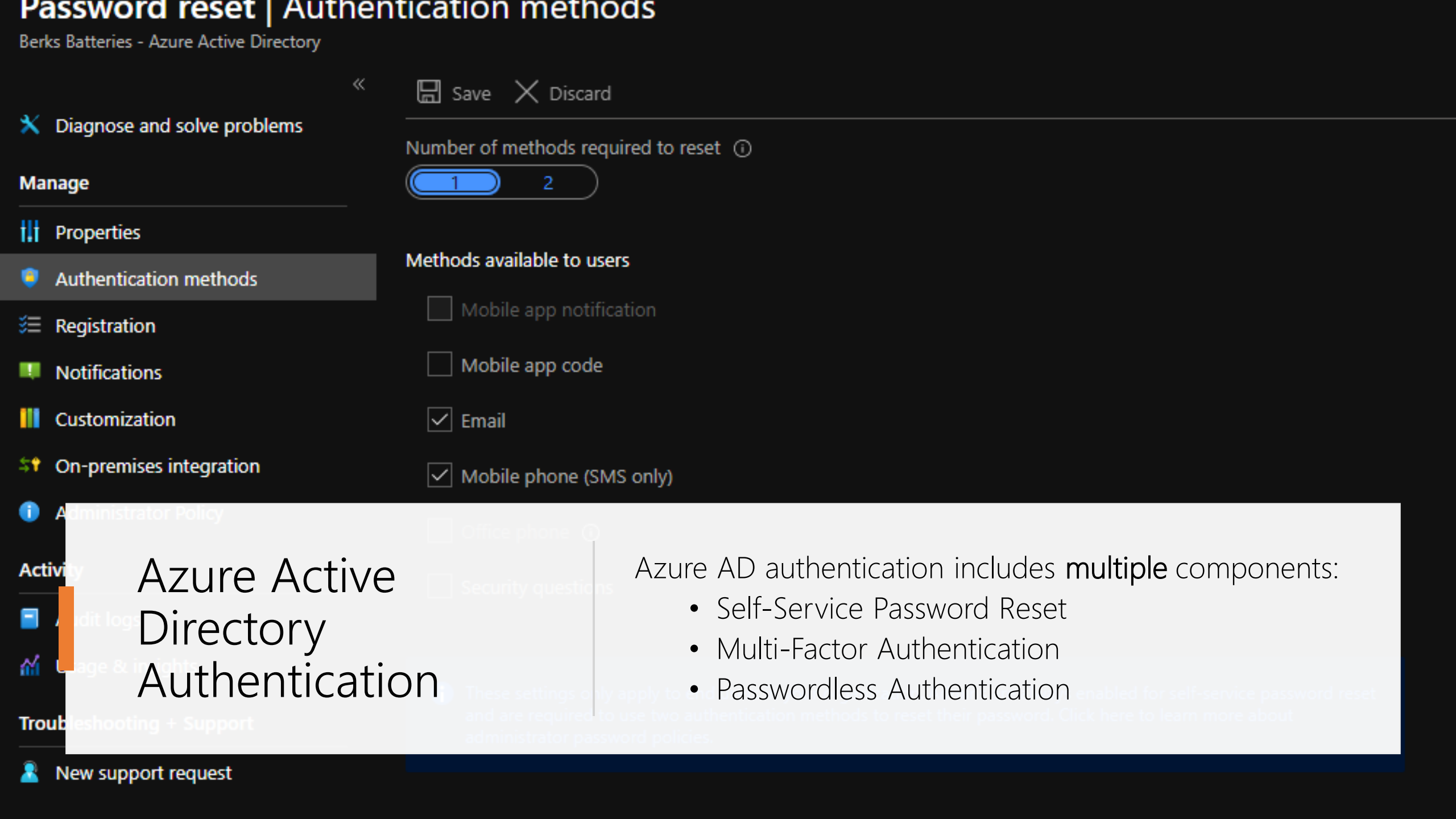
Azure AD Authentication



Azure Active Directory Authentication

The main function of Azure Active Directory is the verification or authentication of credentials any time an end user signs into a device, service, or application.

Authentication involves more than just a username and password in Azure AD.



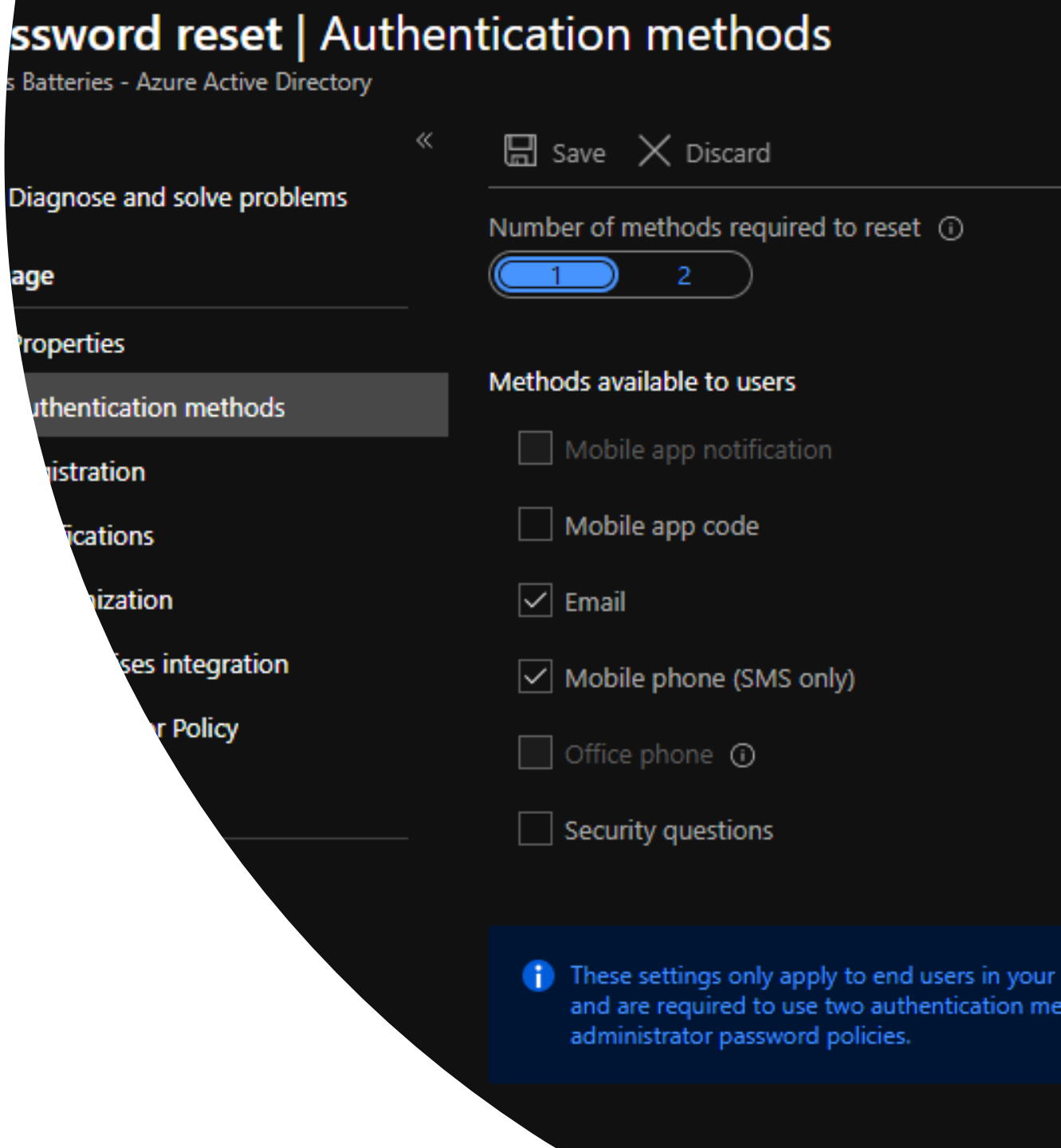
Azure Active Directory Authentication

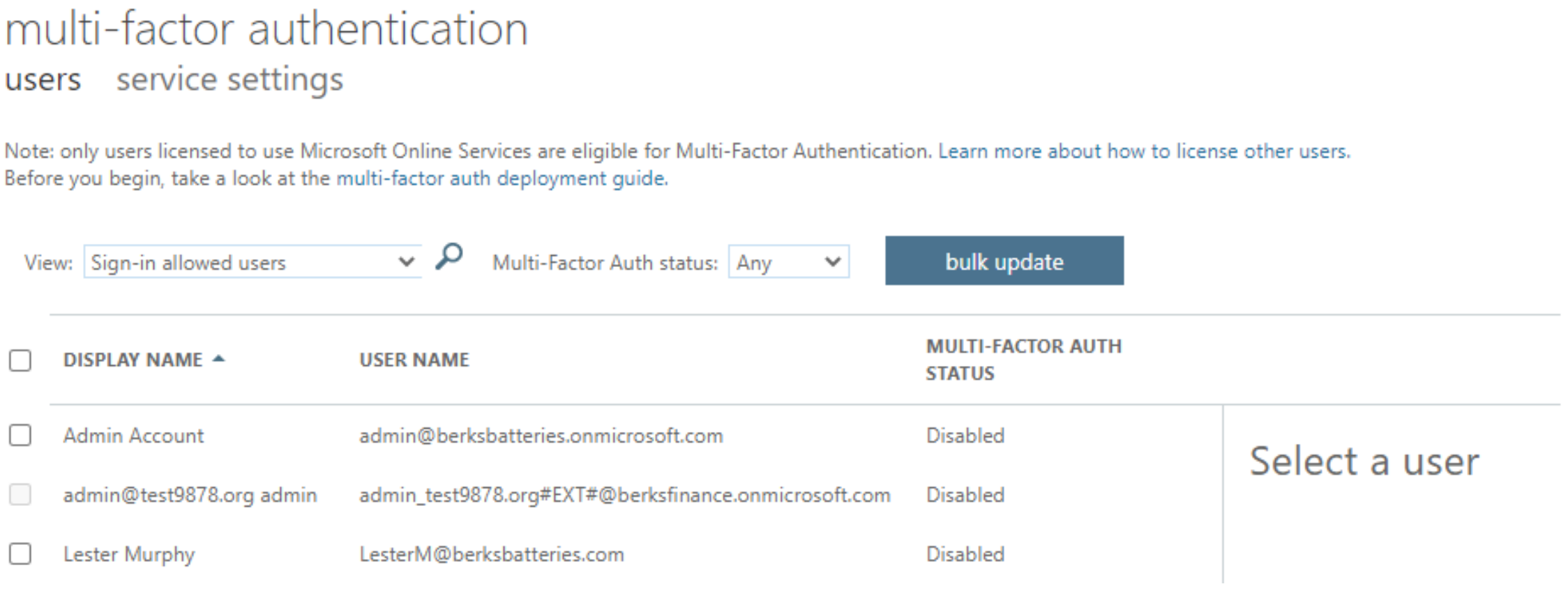
Azure AD authentication includes **multiple** components:

- Self-Service Password Reset
- Multi-Factor Authentication
- Passwordless Authentication

Self-Service Password Reset

Azure Active Directory's self-service password reset feature allows users to change their passwords via a web browser from virtually any device.





Multi-Factor Authentication

Azure MFA requires users to provide a second form of authentication during sign-in.

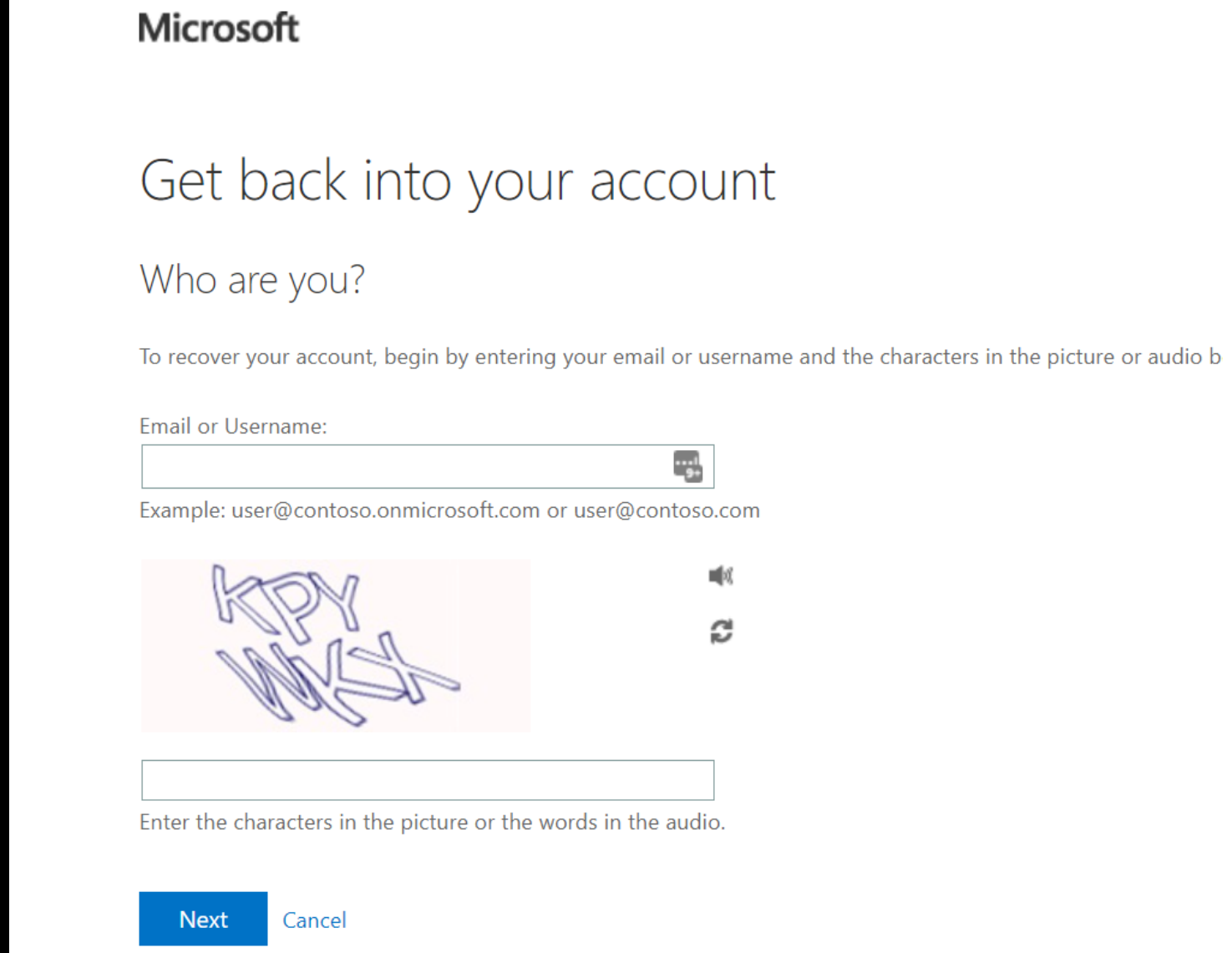
- Phone Call
- SMS Text Message
- Mobile App Notification

Passwordless Authentication

Passwordless authentication makes it possible for end users to authenticate **without the need for a password**.

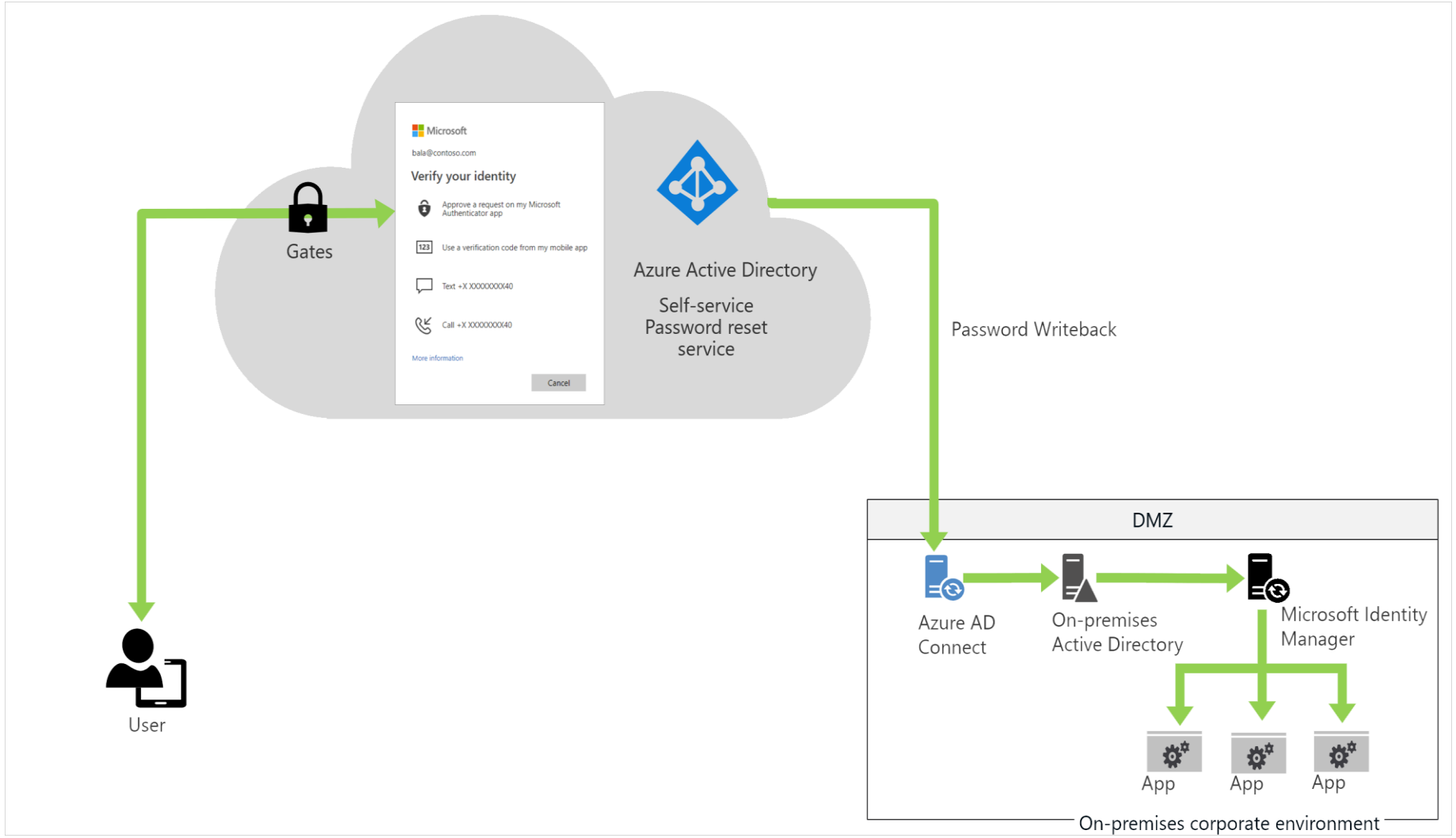
Self-Service Password Reset

Allows users to change their passwords, reset their passwords, and unlock their accounts.



https://aka.ms/sspr

How SSPR Works



Azure Multi-Factor Authentication

To ensure a user is who they say they are, Azure multi-factor authentication requires a **combination** of:

- Something the User Knows
- Something the User Has
- Something the User Is

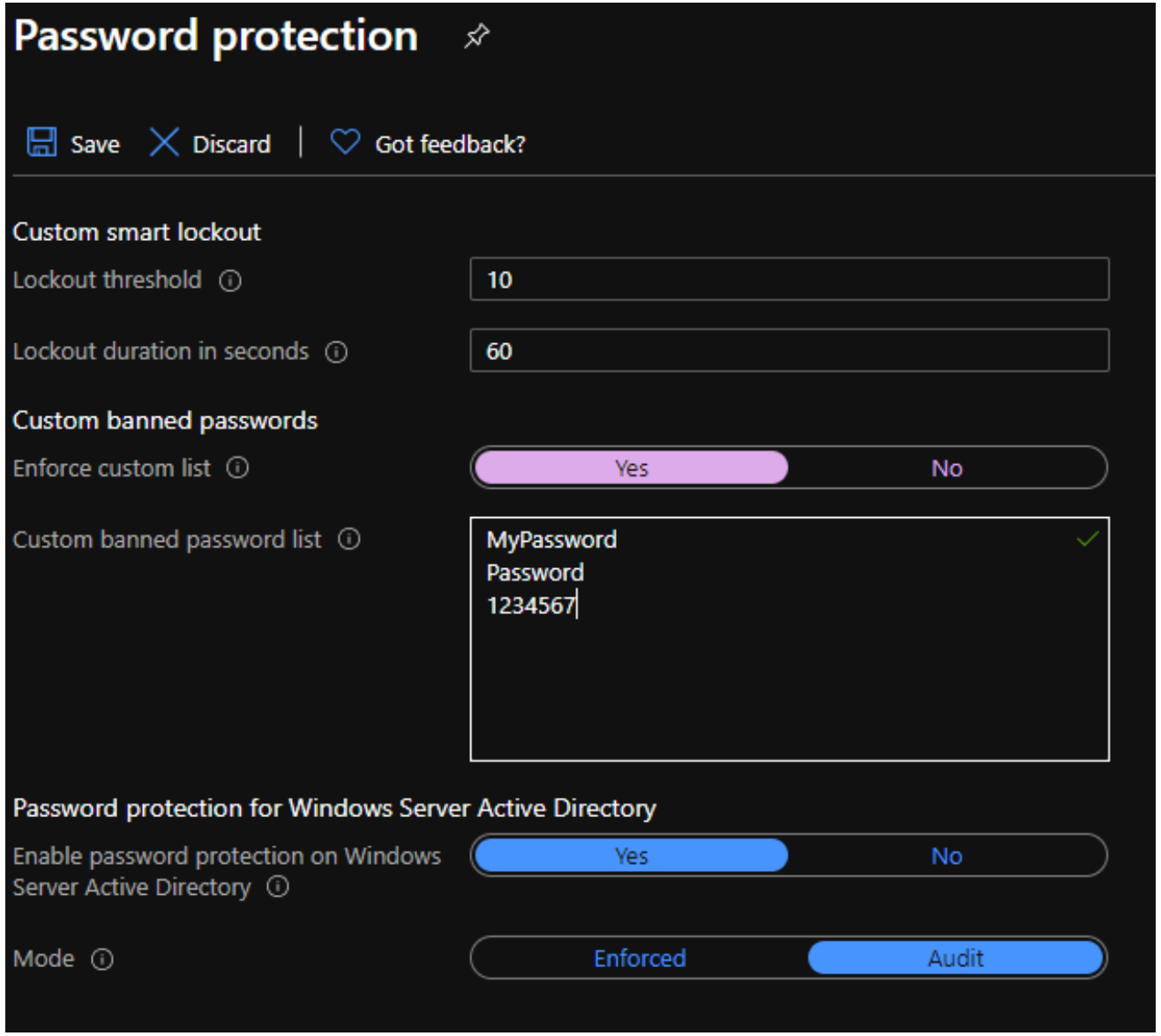
The user needs to provide at least **2** of these authentication factors.

Password Protection

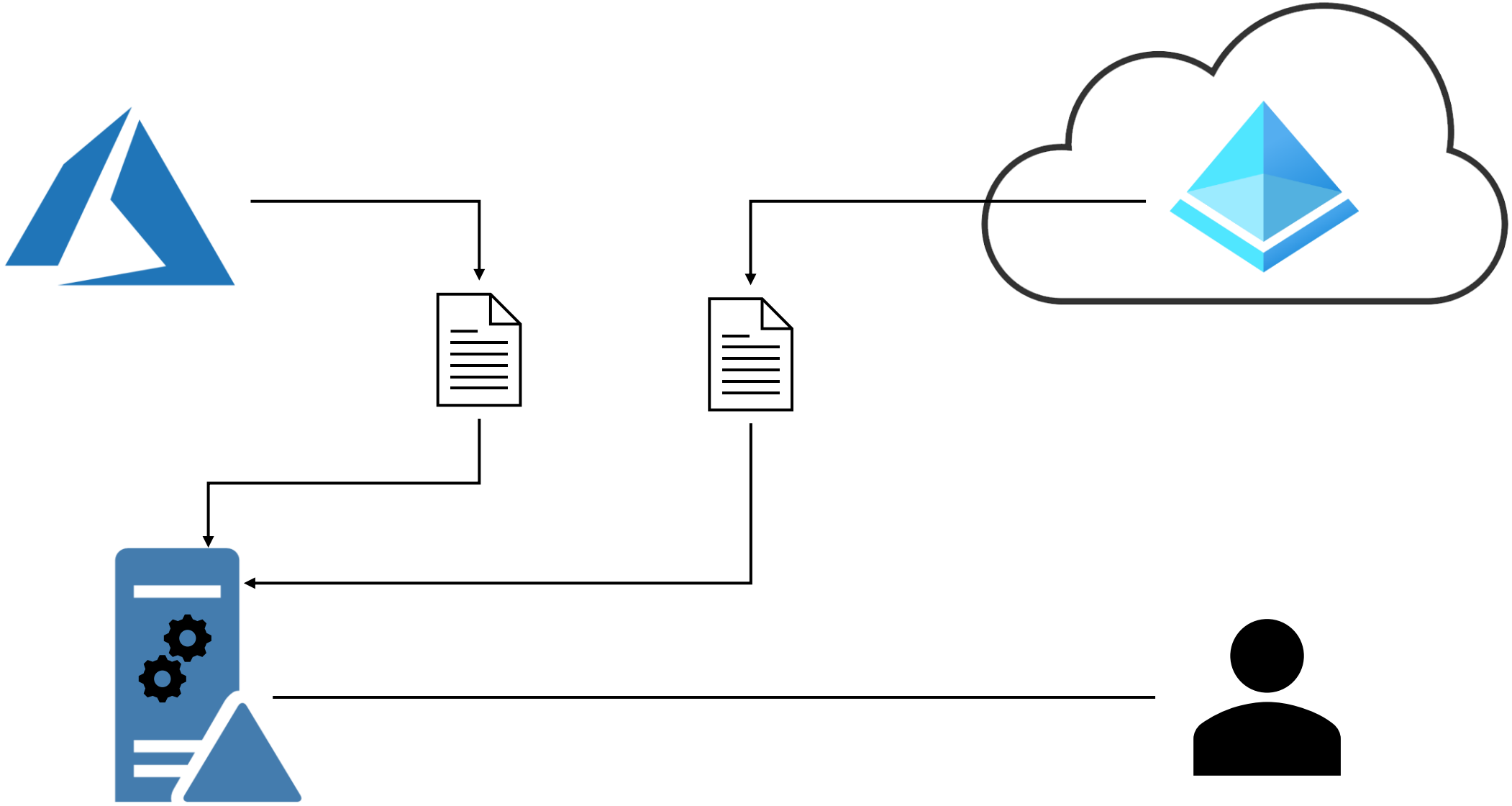
Microsoft Azure maintains a global banned password list that is updated on a regular basis.

Custom password protection policies can be used to further protect against the use of insecure passwords.

Azure AD password protection can be integrated with on-prem Active Directory environments.

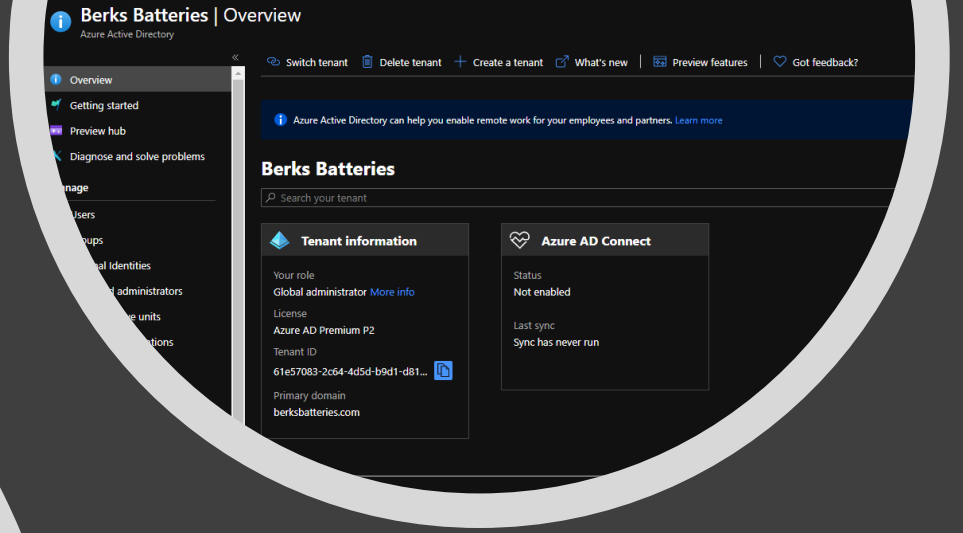


Password Protection



Passwordless Authentication

When a user signs in through a passwordless method, instead of providing a username and password, the user's credentials are provided via methods like biometrics through **Windows Hello for Business**, or through a **FIDO2 security key**.

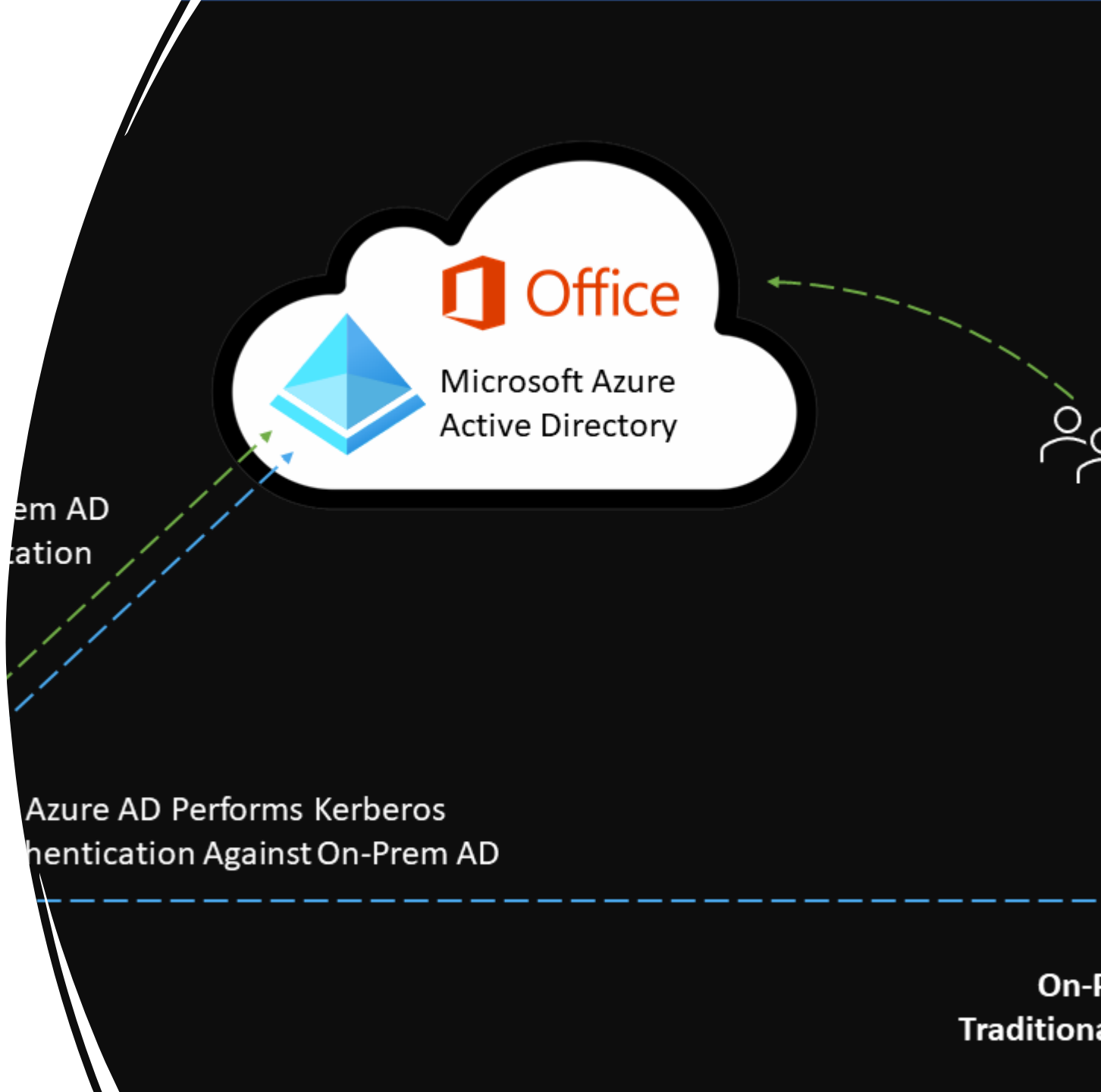


Seamless Single Sign-On

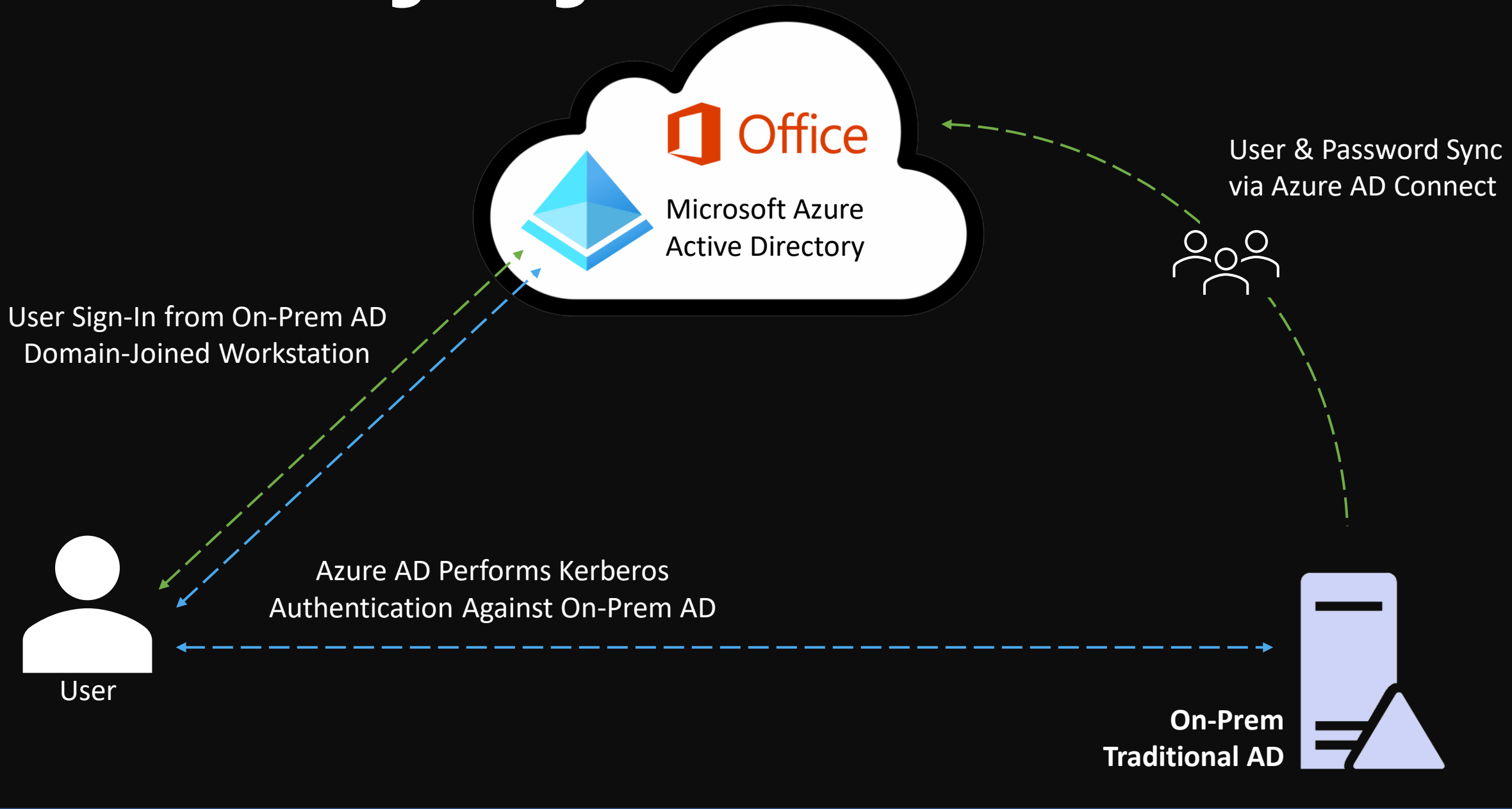
Seamless Single Sign-On

Automatically signs users in when using a corporate device while connected to corporate network.

- Users don't have enter passwords to sign into Azure AD
- Makes it easier for end-users to access cloud-based applications



Seamless Single Sign-On



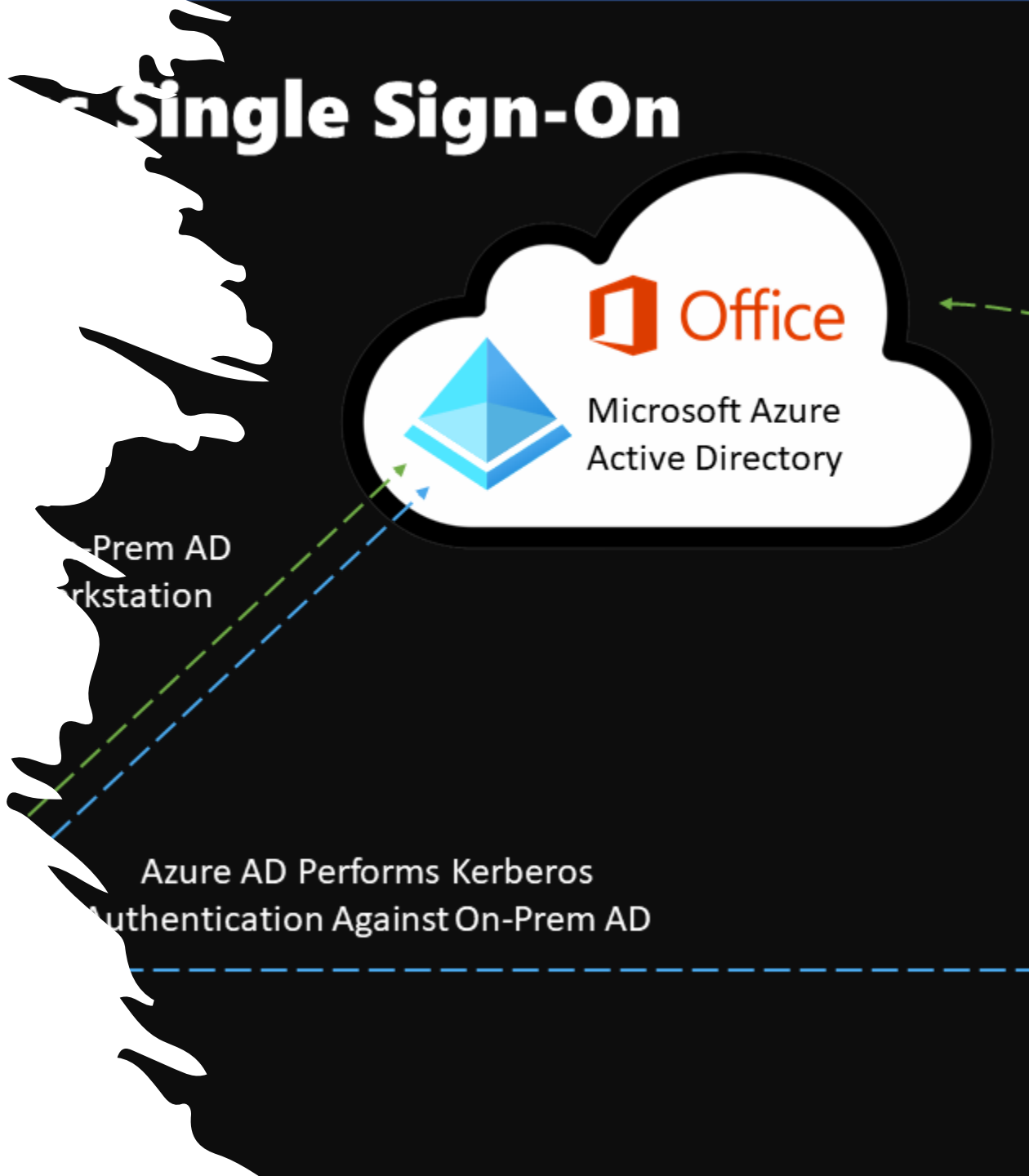
Single Sign-On

Single Sign-On can be achieved via **Primary Refresh Token** OR via **Seamless SSO.**

When using Windows 10, Microsoft recommends using SSO via primary refresh token. If you are still using Windows 7 or Windows 8.1, Microsoft recommends using Seamless SSO.

Seamless SSO

- Seamless SSO requires the user's device to be domain-joined.
- Seamless SSO is NOT used on Windows 10 Azure AD-joined devices or ON hybrid Azure AD-joined devices.
- Azure AD-joined, Hybrid Azure AD-joined, and Azure AD registered devices use the Primary Refresh Token option.



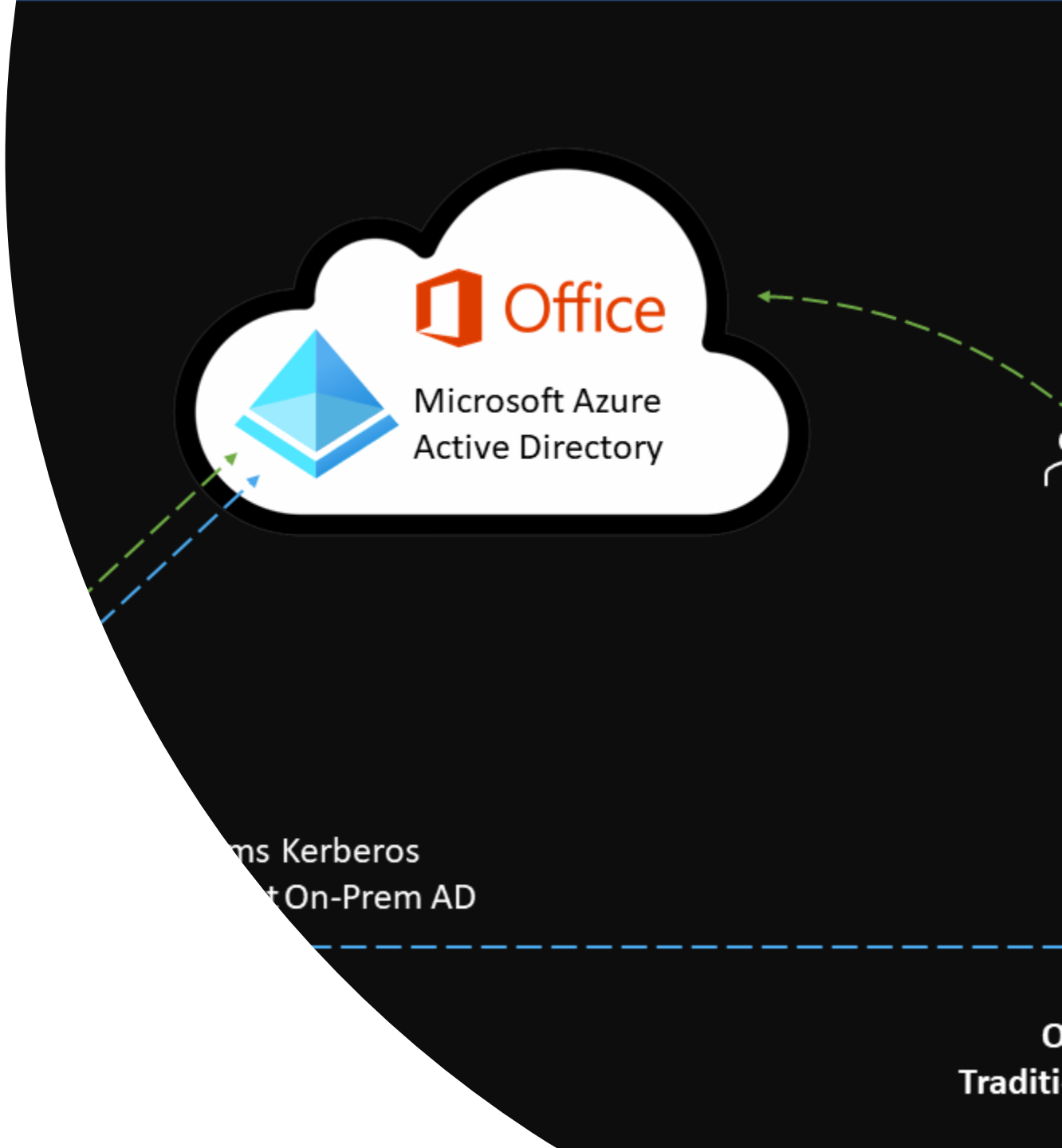
Seamless SSO

Because users are automatically signed into both on-prem apps and cloud-based apps, they don't have to enter their passwords repeatedly.

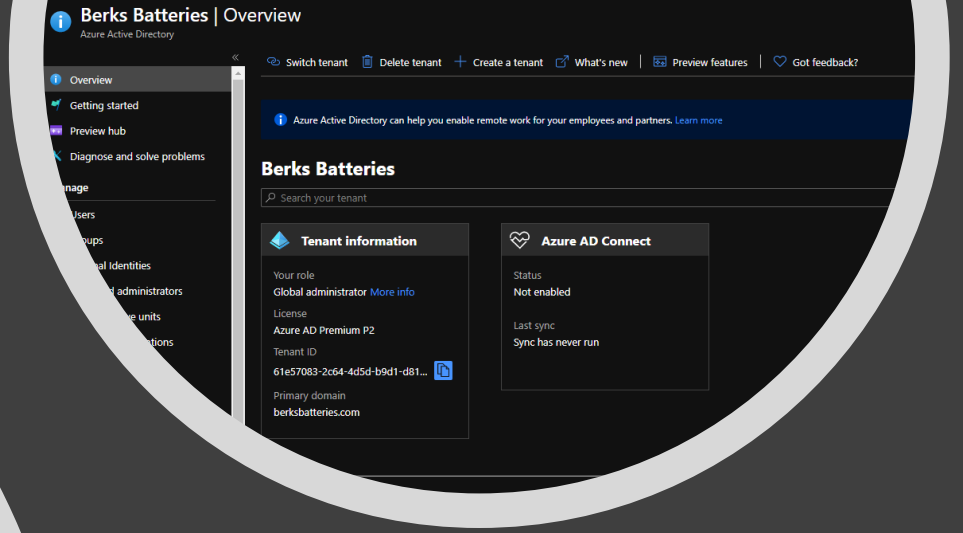
Easy to deploy and manage.

Can be rolled out via Group Policy.

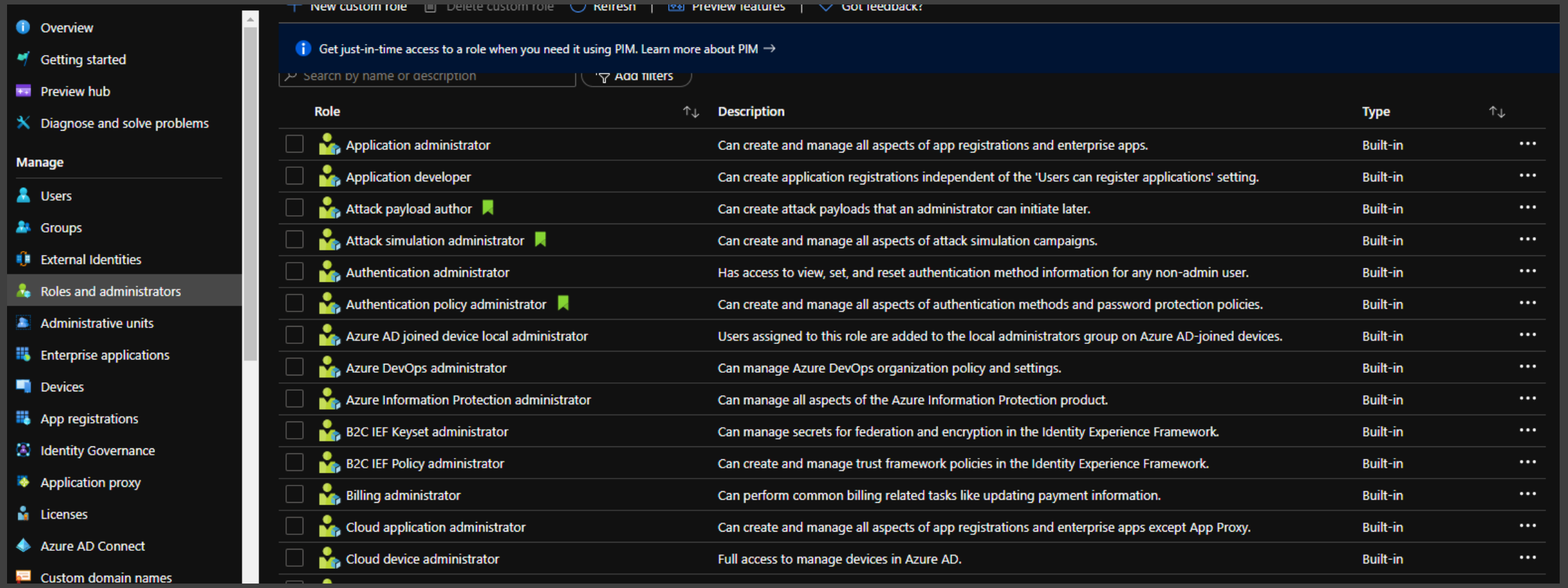
Register non-Windows 10 devices with Azure AD without the need for an ADFS infrastructure.



https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sso-how-it-works



Role-Based Access Control in Azure AD



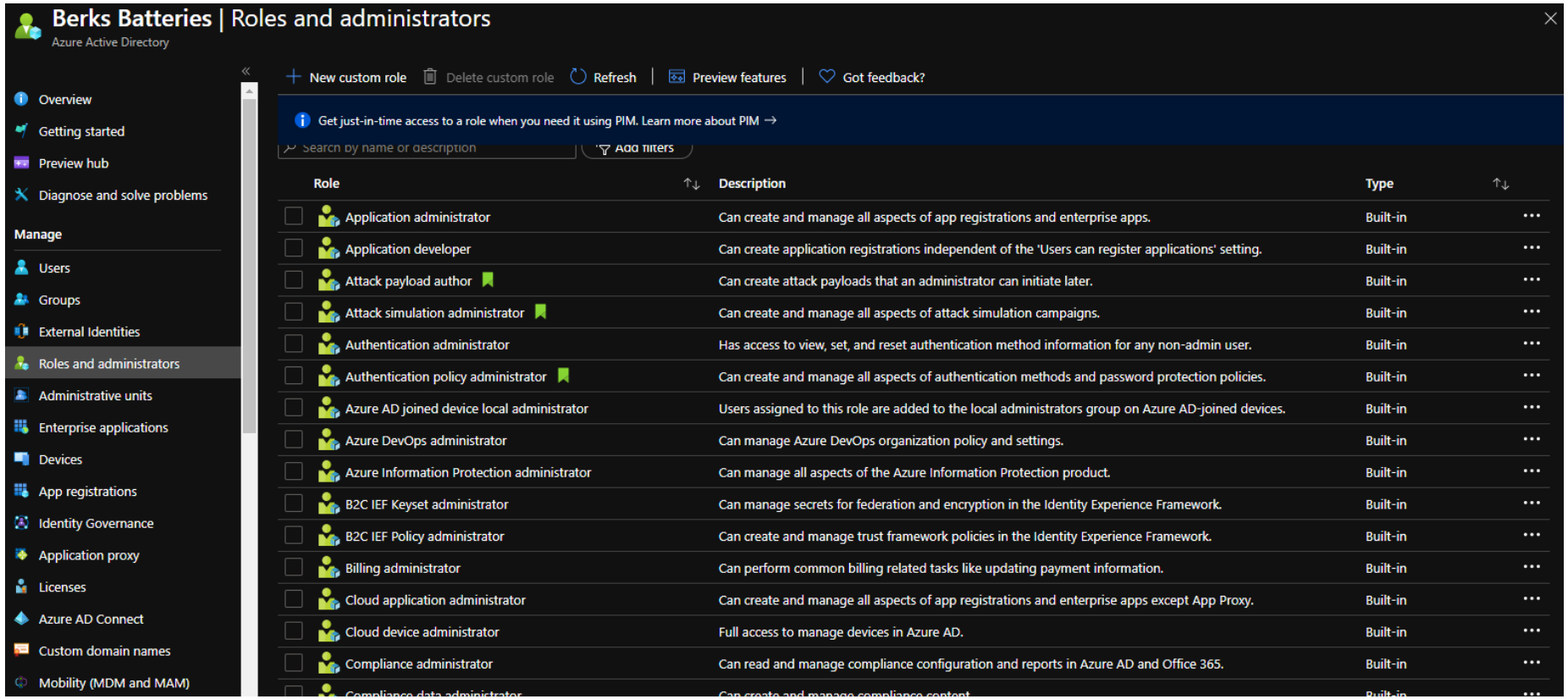
Role-Based Access Control

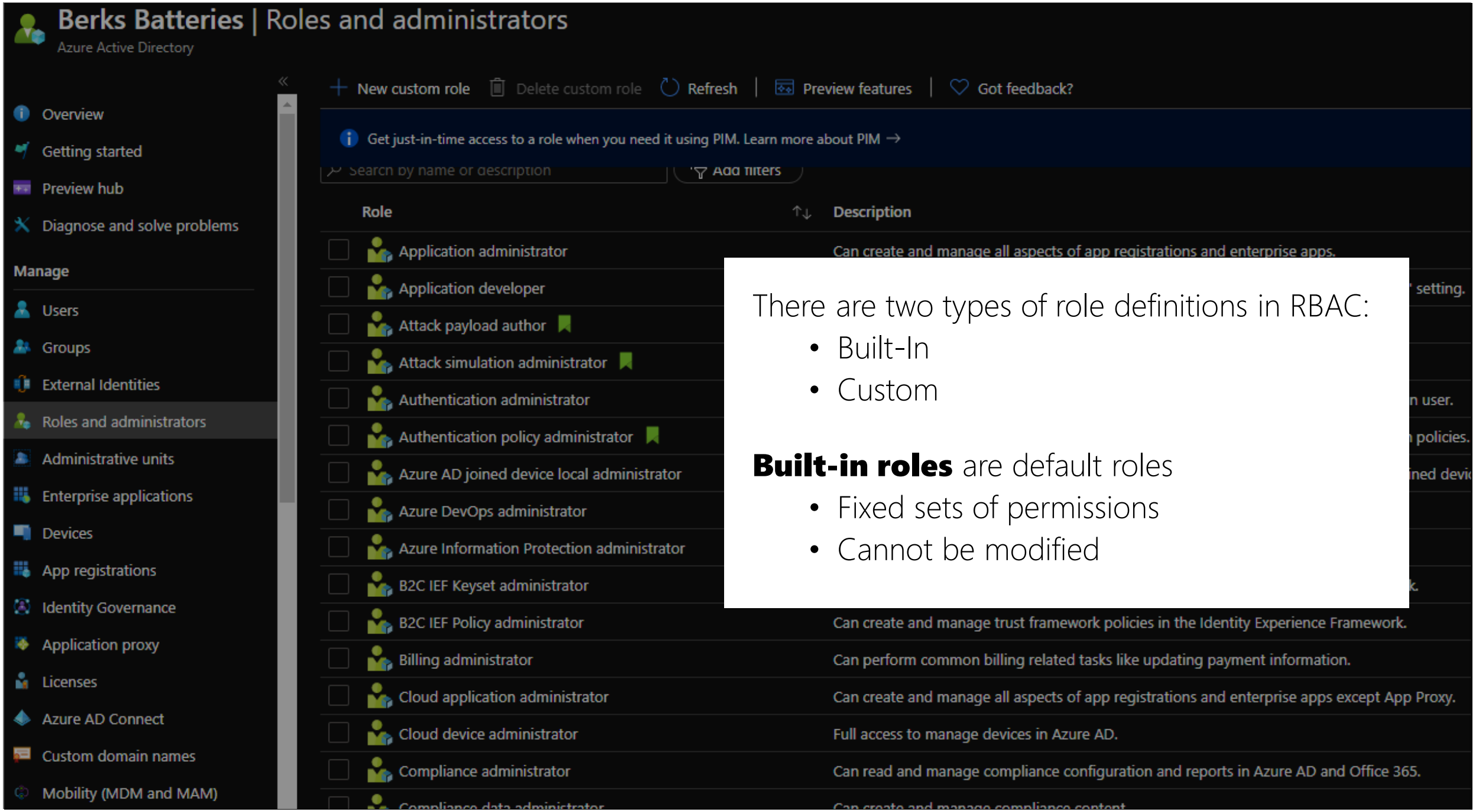
There are **2** RBAC systems in play in Azure:

- Azure RBAC
- Azure AD RBAC

Role-Based Access Control

The **Azure RBAC** system controls access to Azure resources, like virtual machines, vNets, and such, while the **Azure AD RBAC** system allows you to grant granular permissions to admins.





There are two types of role definitions in RBAC:

- Built-In
- Custom

Built-in roles are default roles

- Fixed sets of permissions
- Cannot be modified

Azure AD RBAC Roles

https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference

Azure AD RBAC Custom Roles

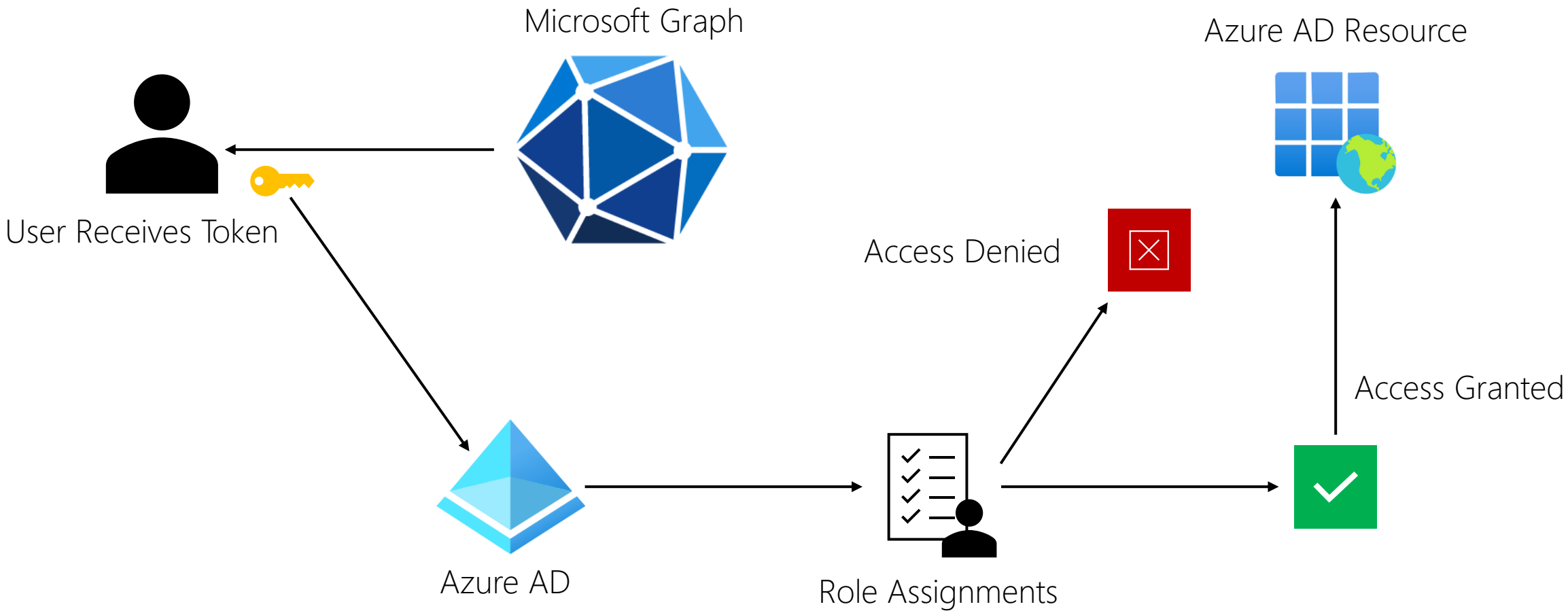
Custom roles are useful when you have a need for a combination of permissions that's not offered by a built-in role.

How to use a custom role:

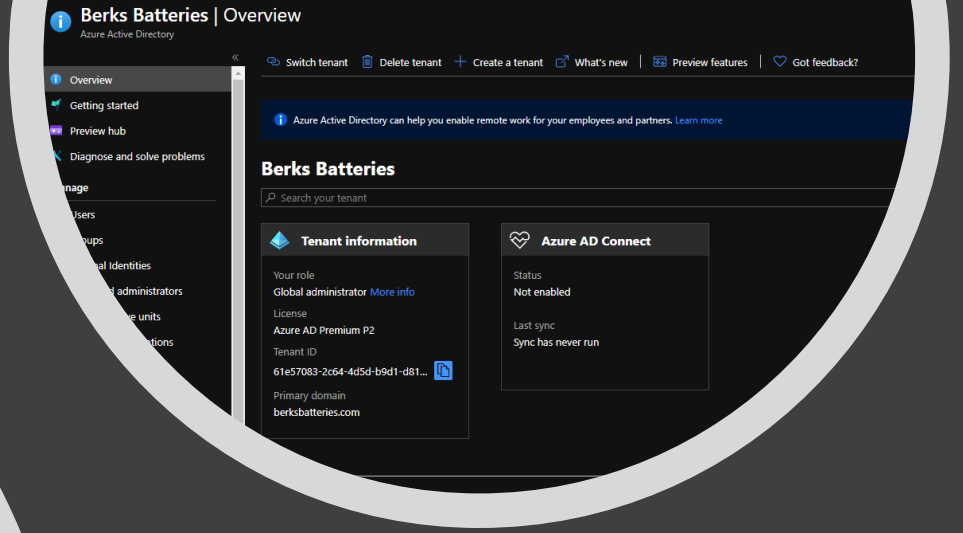
- Create the custom role definition
- Define the permissions for the role
- Assign the role to users

Role assignments are assigned a specific scope that defines the set of Azure AD resources that the role member should have access to.

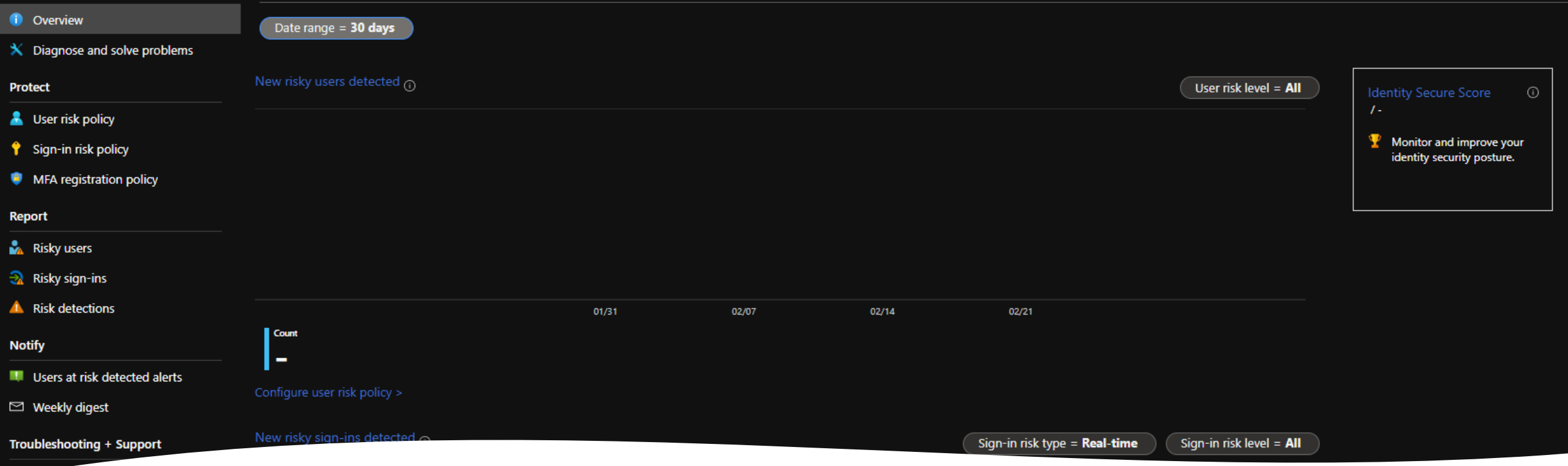
How Azure AD Determines Access



https://docs.microsoft.com/en-us/azure/active-directory/roles/concept-understand-roles



What is Azure Identity Protection?



Azure Identity Protection

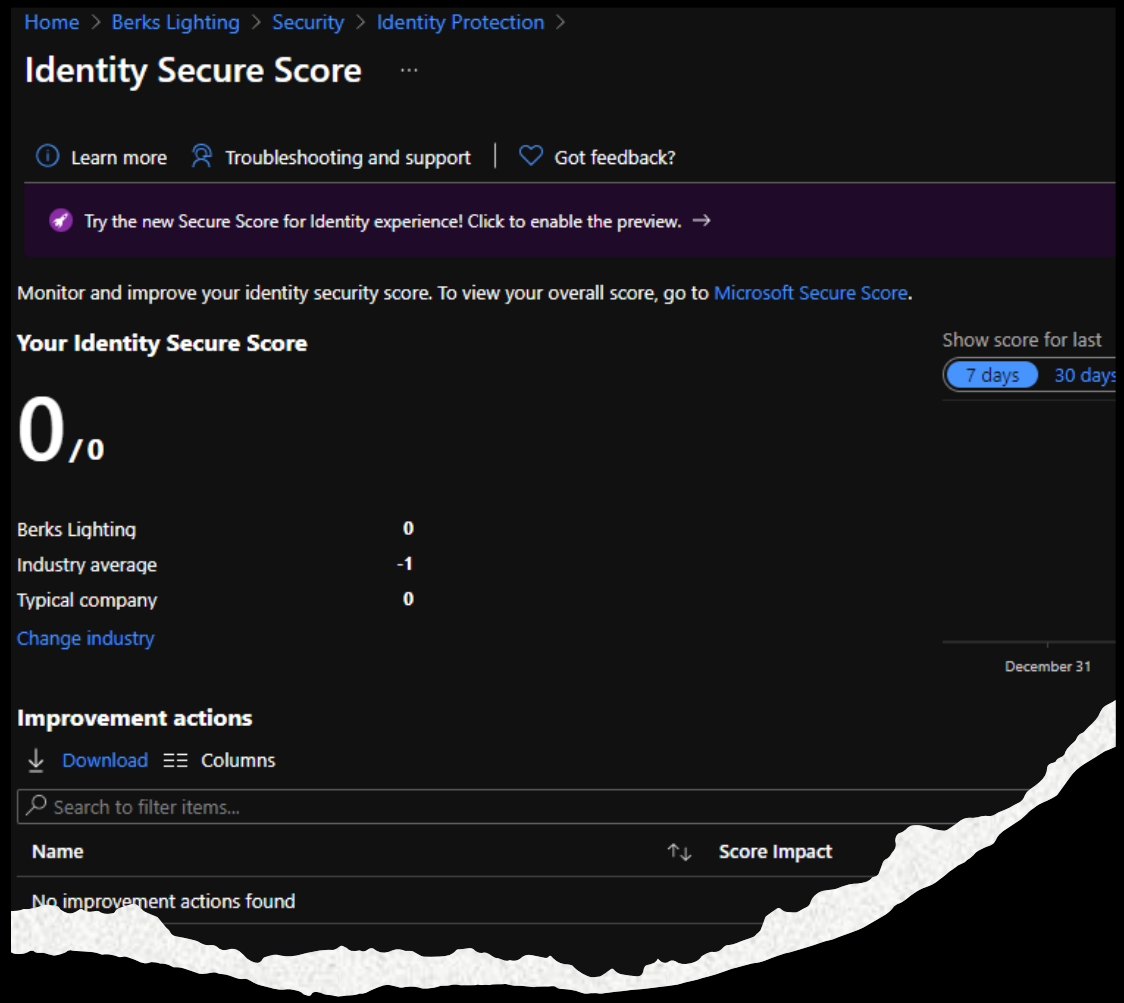
Azure Identity Protection is a tool that allows organizations to accomplish several tasks:

- Automate detection & remediation of identity-based risks
- Investigate risks using data in the portal
- Export risk detection data to third-party tools

Azure Identity Protection

Identifies the following types of risks:

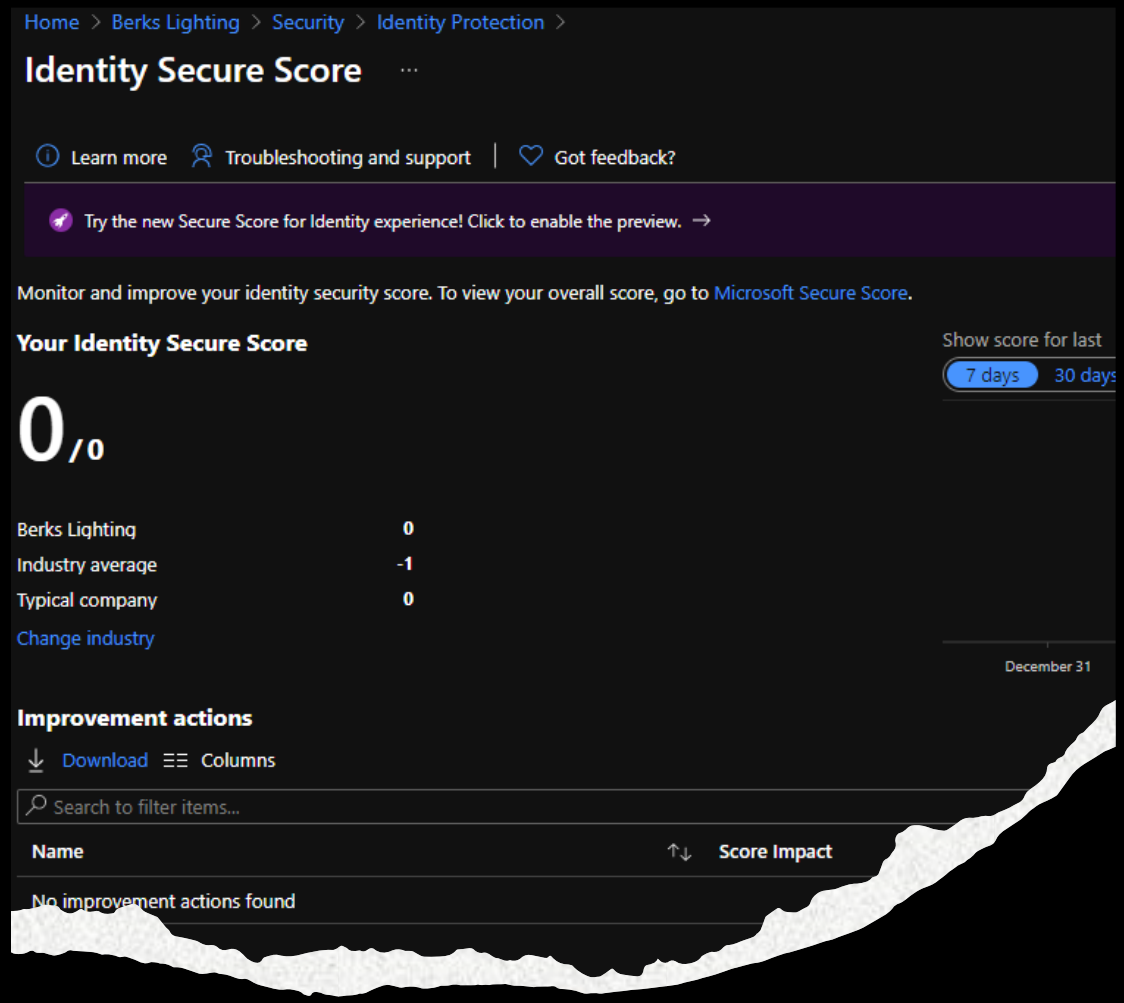
- Anonymous IP address
- Atypical travel
- Malware linked IP address
- Unfamiliar sign-in properties
- Leaked Credentials
- Password spray
- New country
- Activity from anonymous IP address
- Suspicious inbox forwarding



Azure Identity Protection

Identifies the following types of risks:

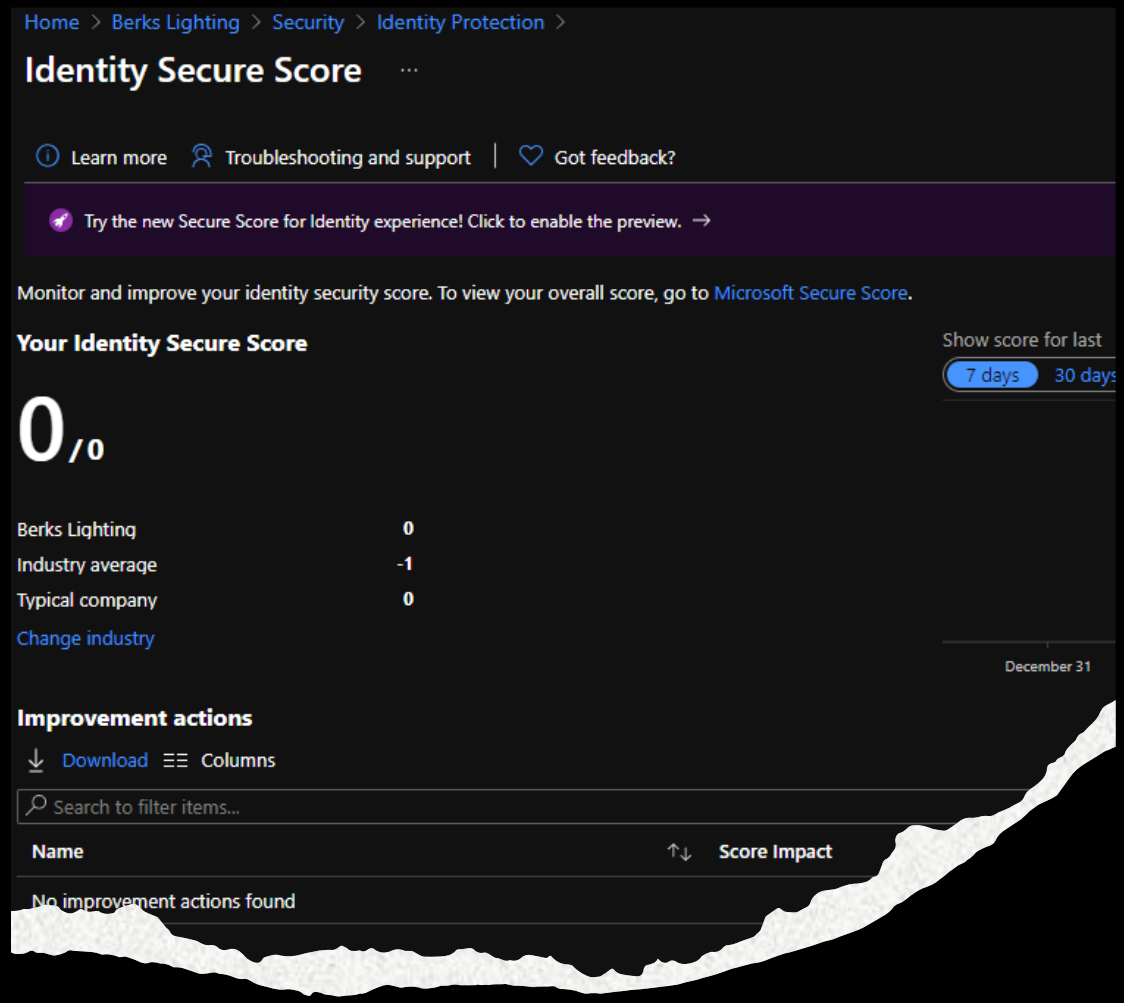
- **Anonymous IP address**
- Atypical travel
- Malware linked IP address
- Unfamiliar sign-in properties
- Leaked Credentials
- Password spray
- New country
- Activity from anonymous IP address
- Suspicious inbox forwarding



Azure Identity Protection

Identifies the following types of risks:

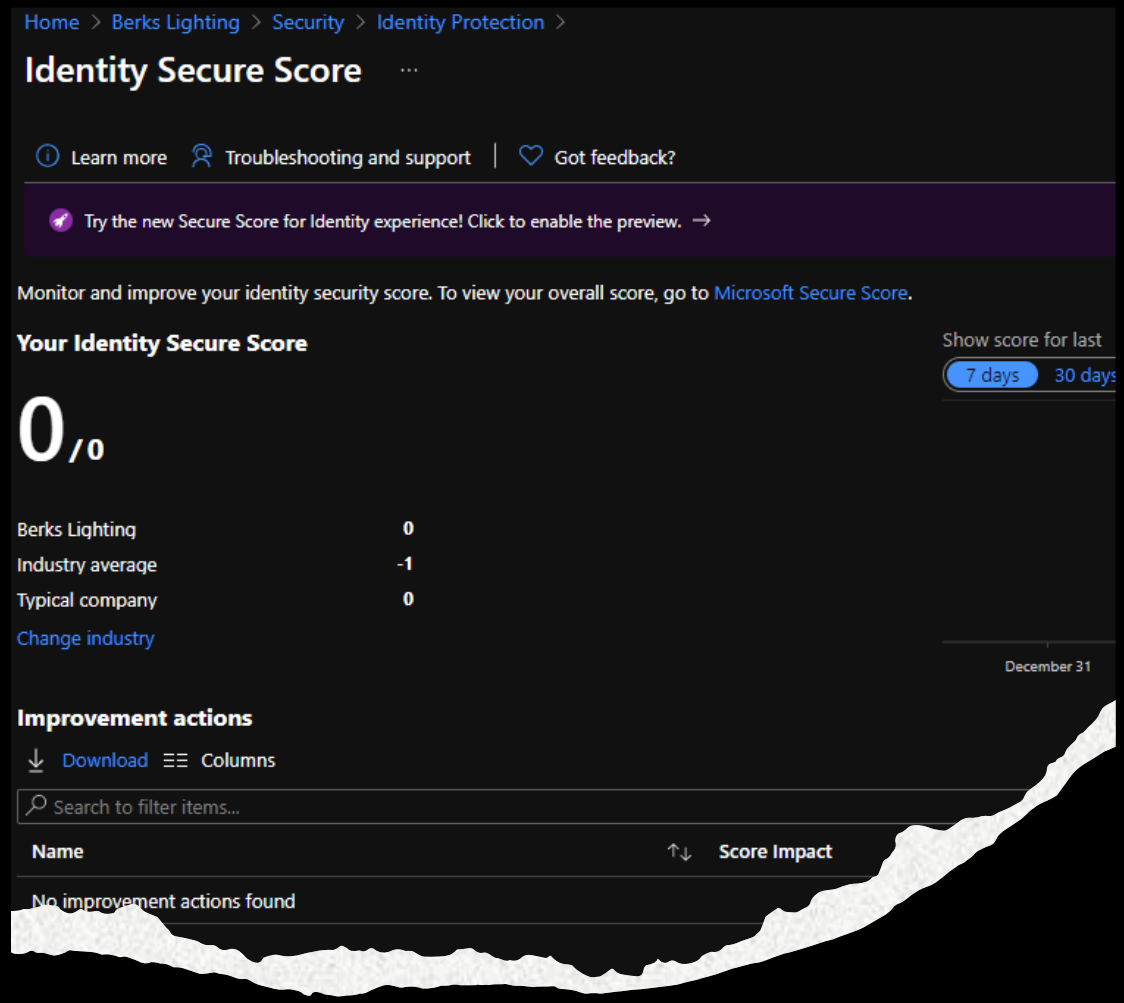
- Anonymous IP address
- **Atypical travel**
- Malware linked IP address
- Unfamiliar sign-in properties
- Leaked Credentials
- Password spray
- New country
- Activity from anonymous IP address
- Suspicious inbox forwarding



Azure Identity Protection

Identifies the following types of risks:

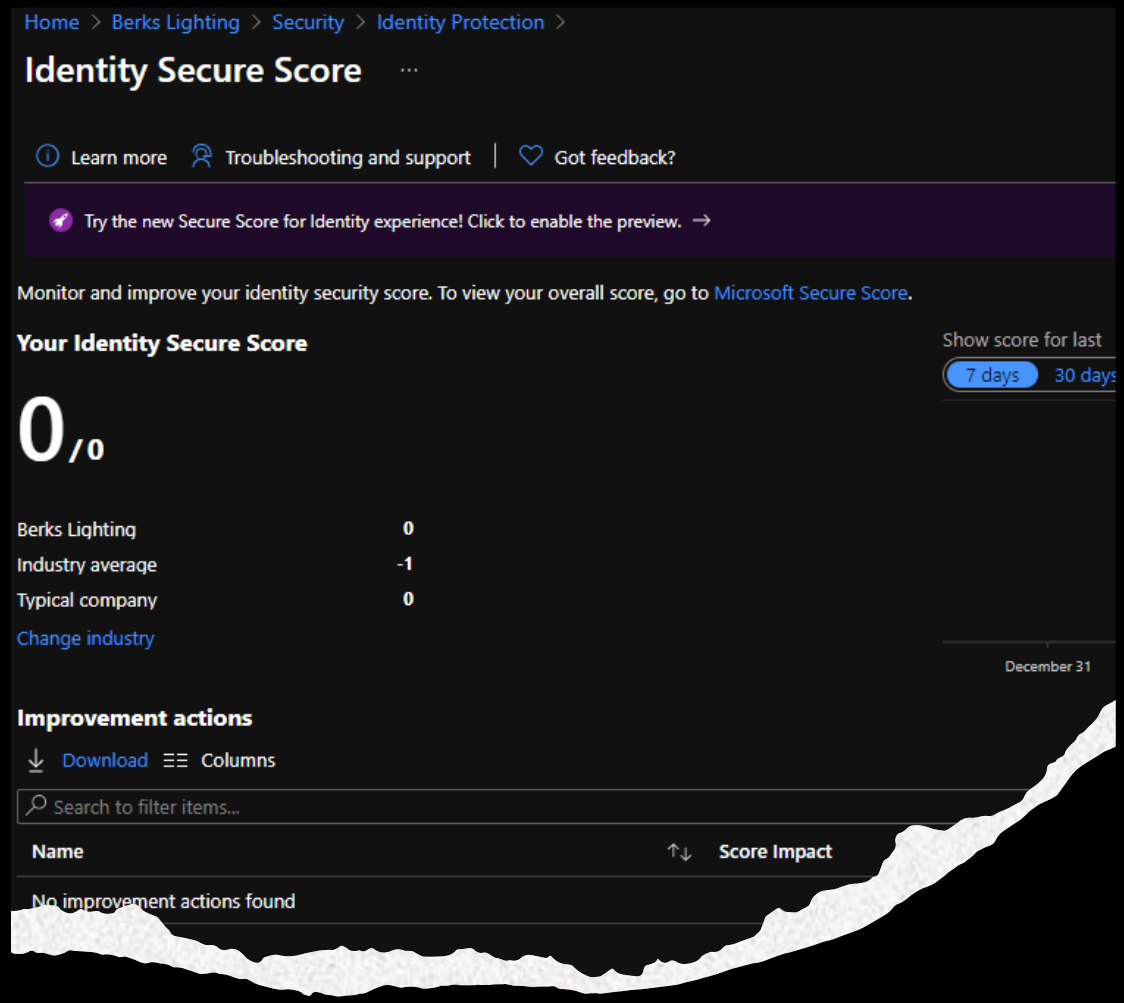
- Anonymous IP address
- Atypical travel
- **Malware linked IP address**
- Unfamiliar sign-in properties
- Leaked Credentials
- Password spray
- New country
- Activity from anonymous IP address
- Suspicious inbox forwarding



Azure Identity Protection

Identifies the following types of risks:

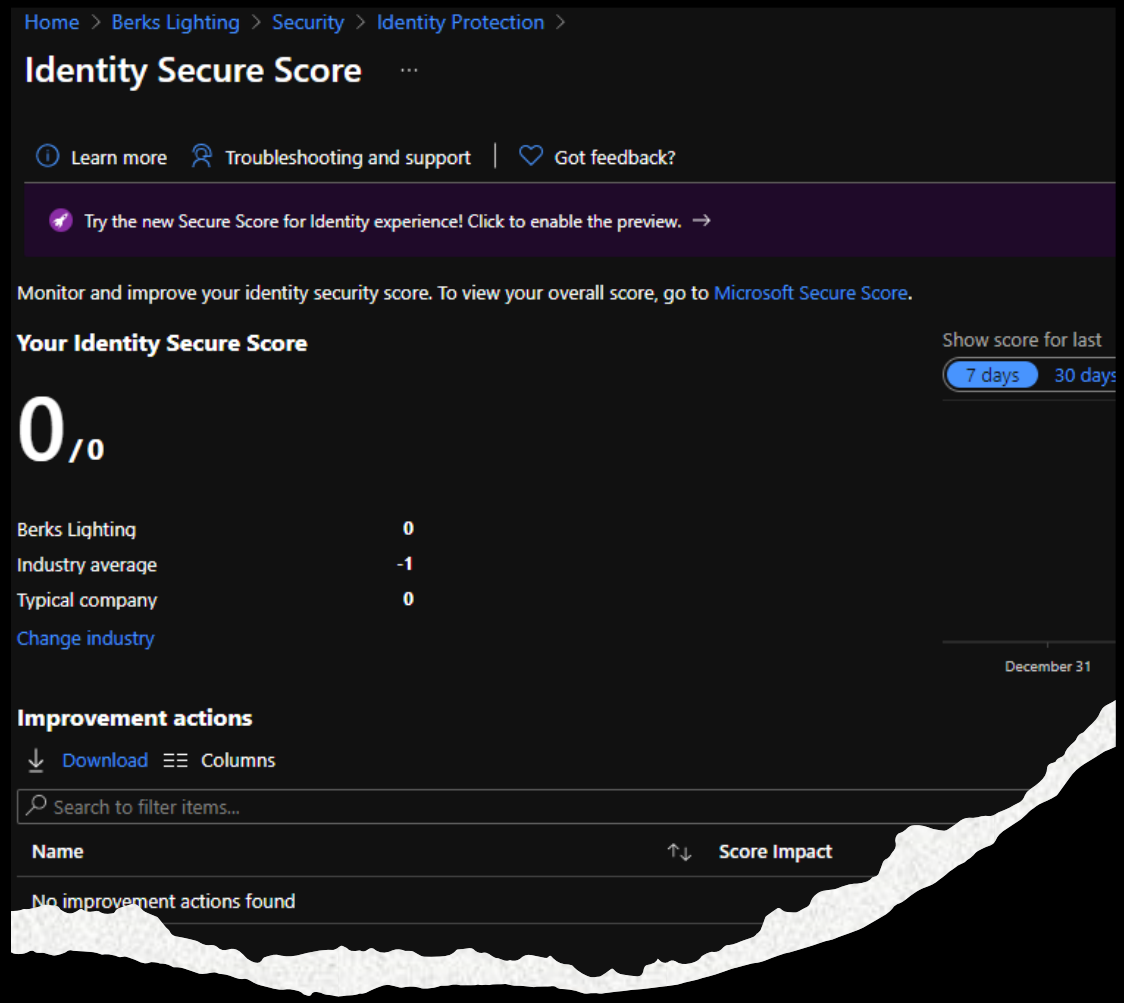
- Anonymous IP address
- Atypical travel
- Malware linked IP address
- **Unfamiliar sign-in properties**
- Leaked Credentials
- Password spray
- New country
- Activity from anonymous IP address
- Suspicious inbox forwarding



Azure Identity Protection

Identifies the following types of risks:

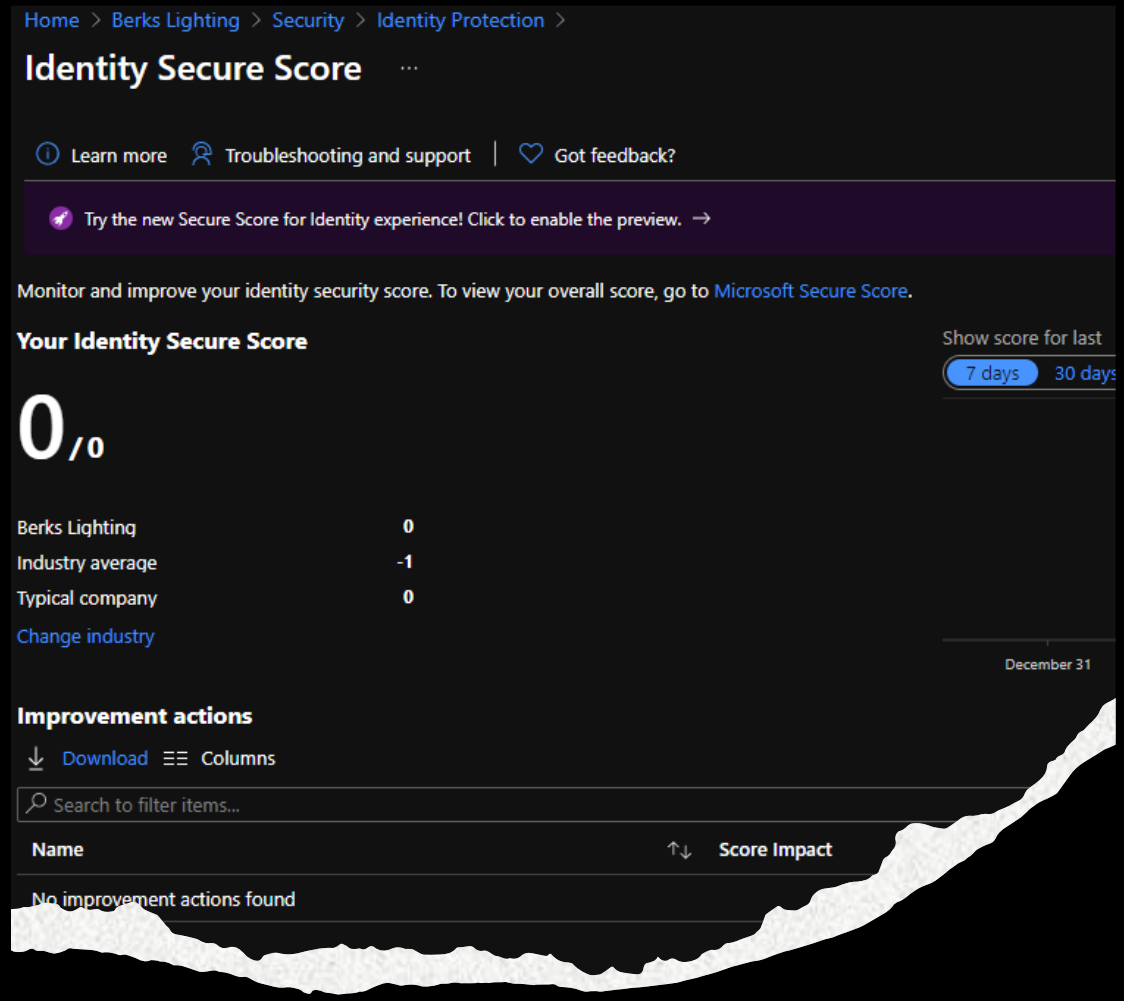
- Anonymous IP address
- Atypical travel
- Malware linked IP address
- Unfamiliar sign-in properties
- **Leaked Credentials**
- Password spray
- New country
- Activity from anonymous IP address
- Suspicious inbox forwarding



Azure Identity Protection

Identifies the following types of risks:

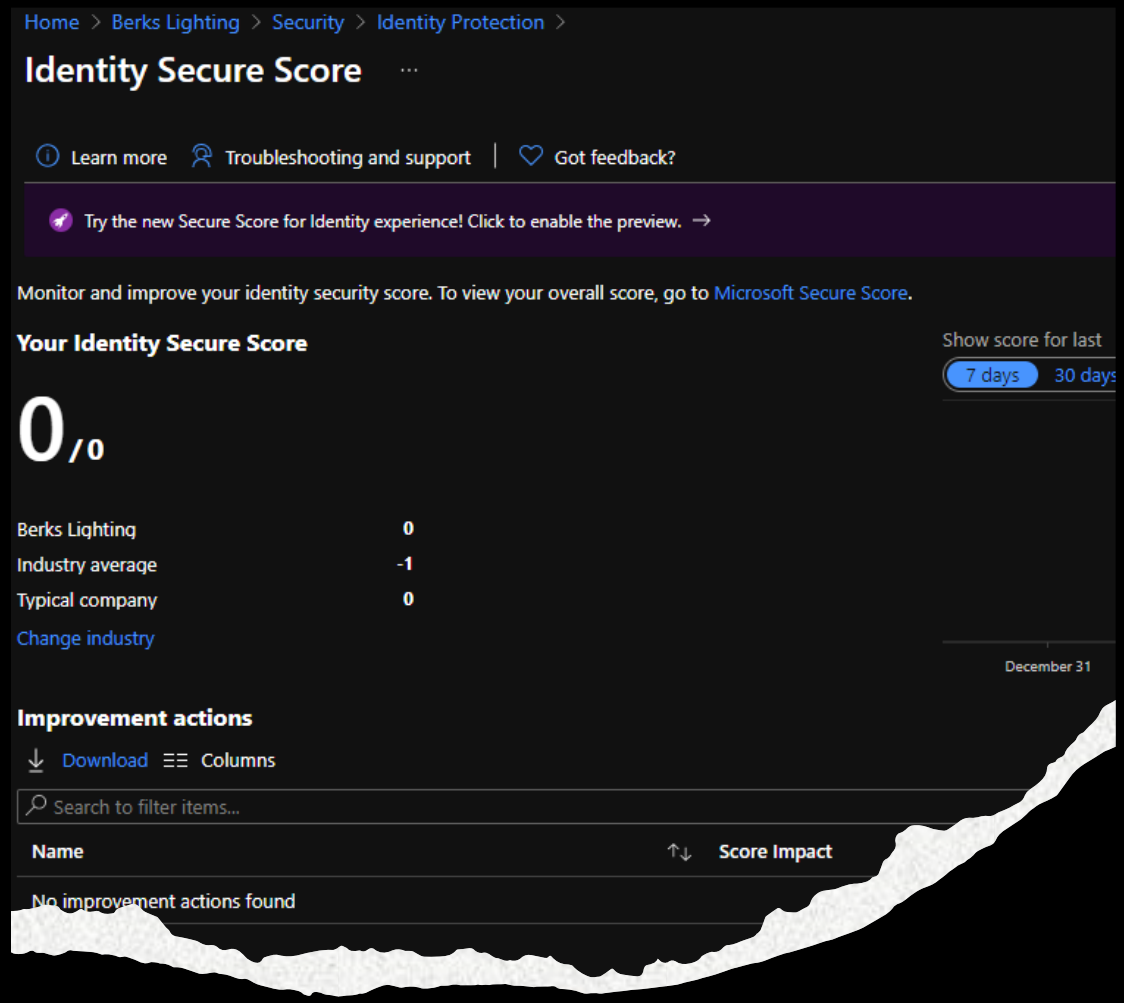
- Anonymous IP address
- Atypical travel
- Malware linked IP address
- Unfamiliar sign-in properties
- Leaked Credentials
- **Password spray**
- New country
- Activity from anonymous IP address
- Suspicious inbox forwarding



Azure Identity Protection

Identifies the following types of risks:

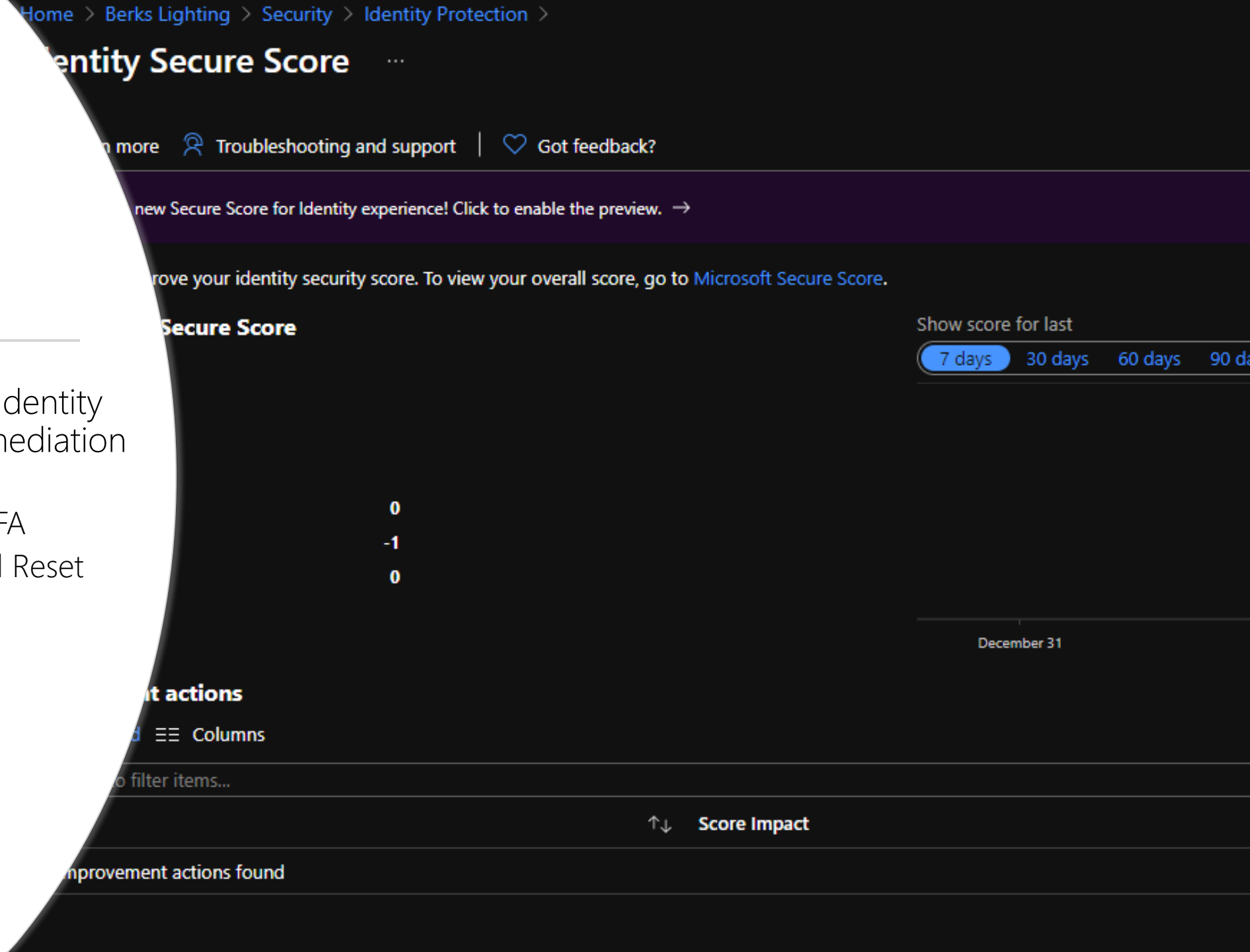
- Anonymous IP address
- Atypical travel
- Malware linked IP address
- Unfamiliar sign-in properties
- Leaked Credentials
- Password spray
- New country
- Activity from anonymous IP address
- Suspicious inbox forwarding

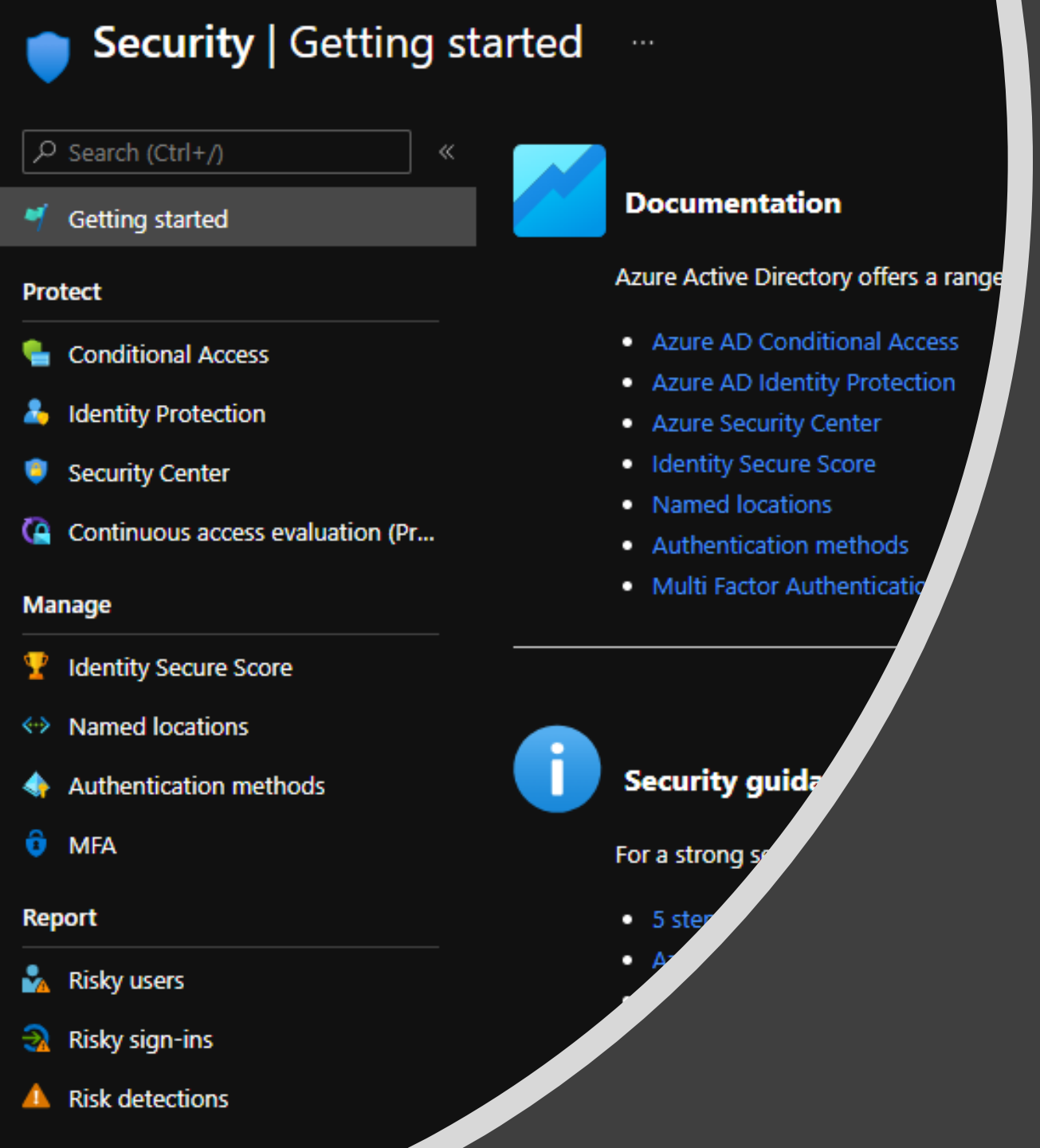


Azure Identity Protection

Risk signals picked up by Identity Protection can trigger remediation efforts:

- Perform Azure AD MFA
- Self-Service Password Reset
- Account Blocking



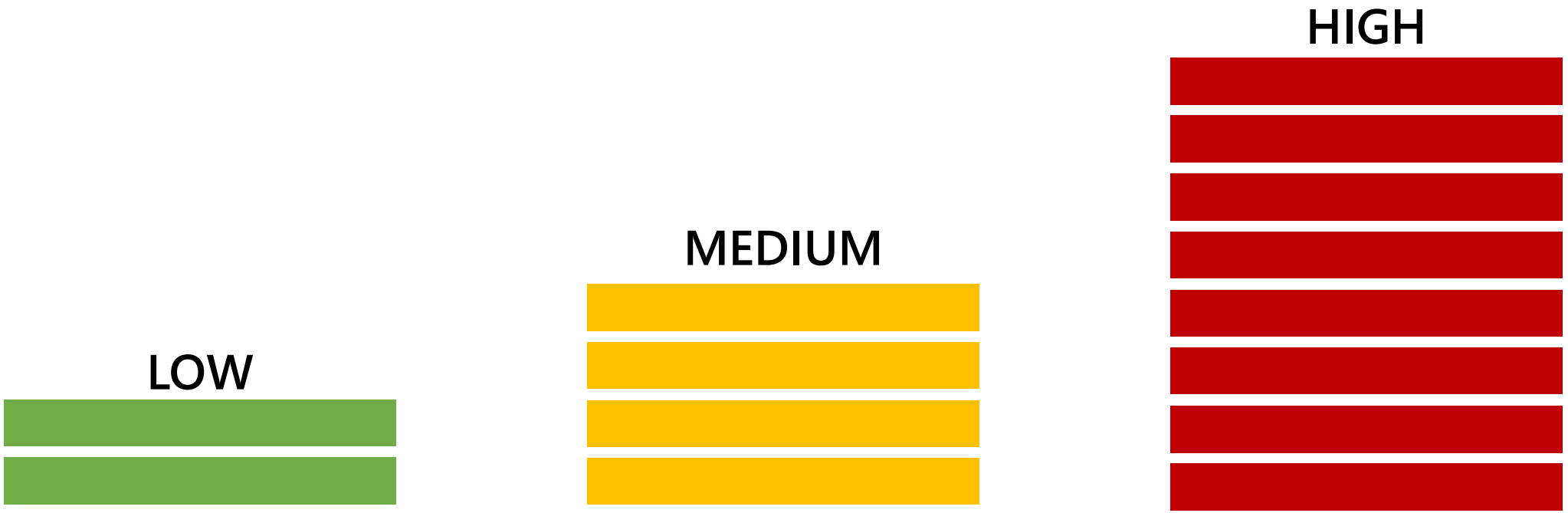


Azure Identity Protection

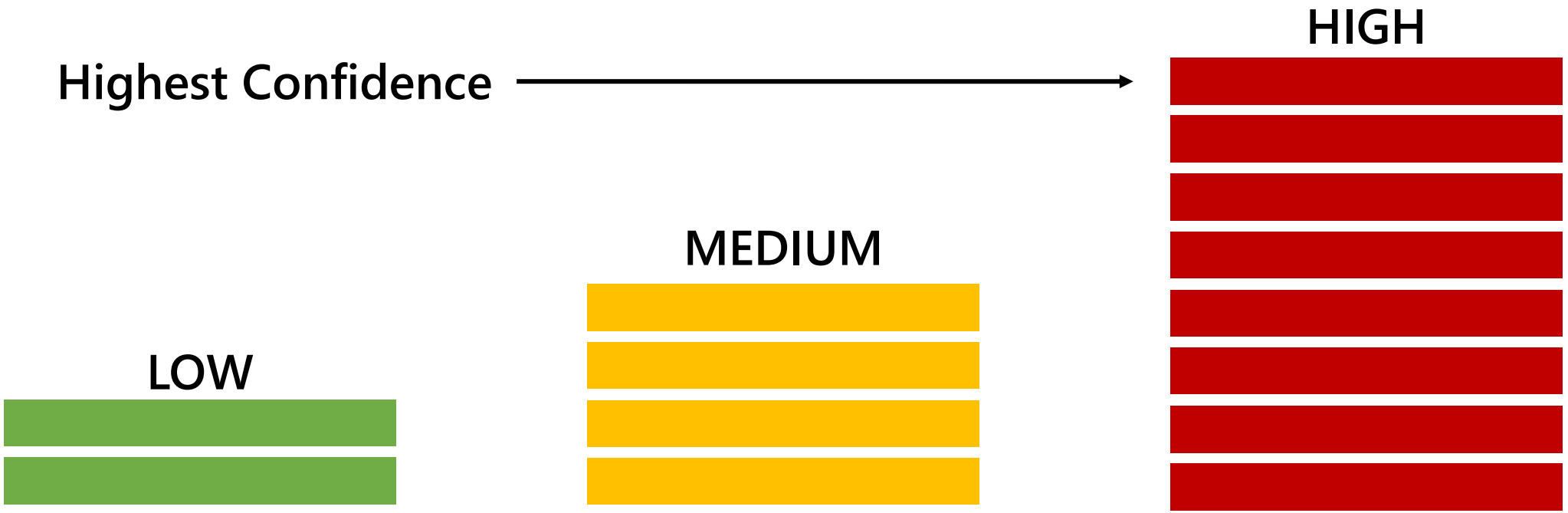
There are **3** key reports that administrators can use for investigations in Identity Protection:

- Risky users
- Risky sign-ins
- Risk detections

Risk Levels



Risk Levels



Unfamiliar Sign-In Properties

<

Leaked Credentials

Azure Identity Protection

- Security Reader
- Security Operator
- Security Administrator
- Global Reader
- Global Administrator

Role	Can do	Can't do
Global administrator	Full access to Identity Protection	
Security administrator	Full access to Identity Protection	Reset password for a user
Security operator	View all Identity Protection reports and Overview blade Dismiss user risk, confirm safe sign-in, confirm compromise	Configure or change policies Reset password for a user Configure alerts
Security reader	View all Identity Protection reports and Overview blade	Configure or change policies Reset password for a user Configure alerts Give feedback on detections

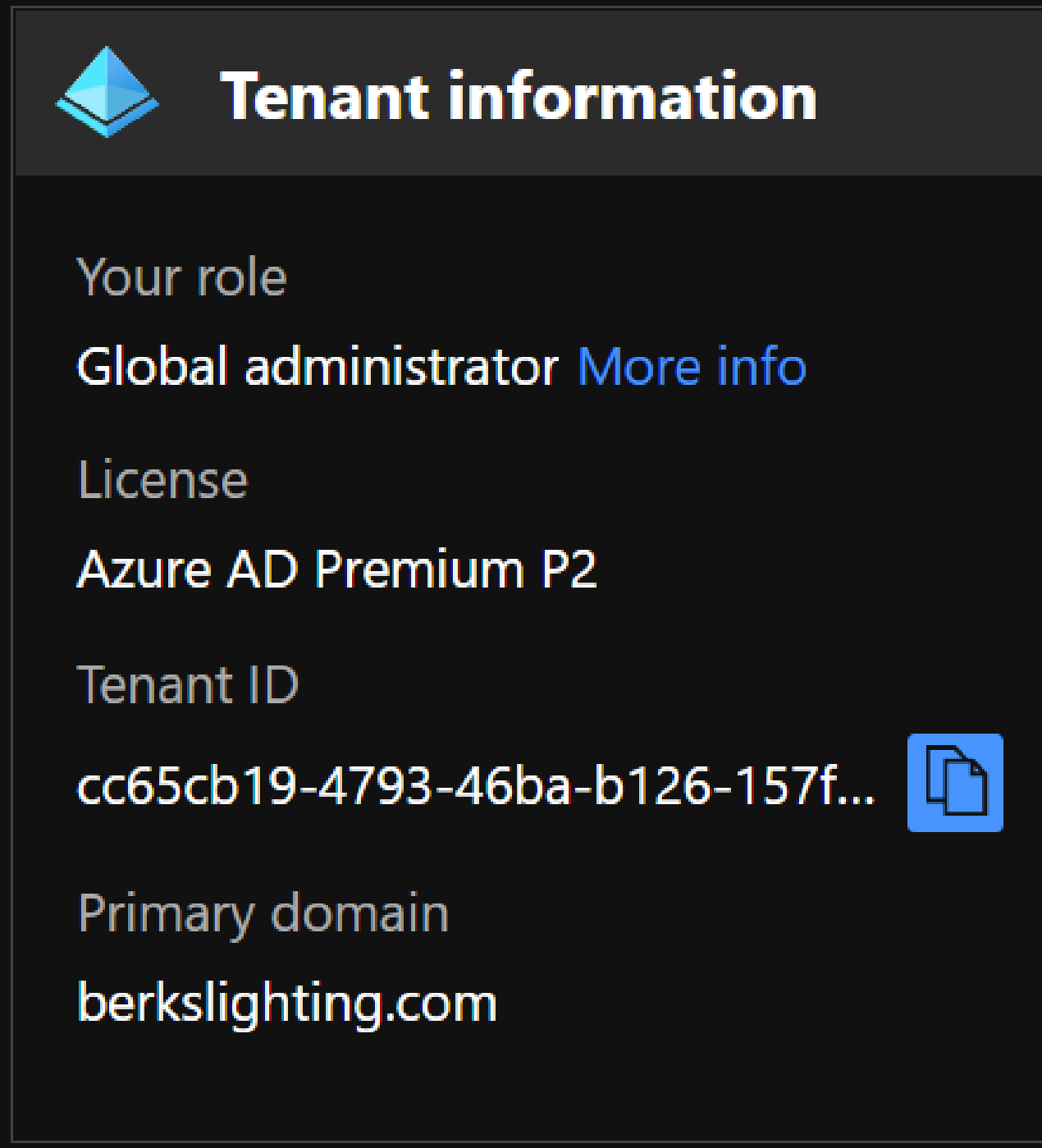
Azure Identity Protection

Role	Can do	Can't do
Global administrator	Full access to Identity Protection	
Security administrator	Full access to Identity Protection	Reset password for a user
Security operator	View all Identity Protection reports and Overview blade Dismiss user risk, confirm safe sign-in, confirm compromise	Configure or change policies Reset password for a user Configure alerts
Security reader	View all Identity Protection reports and Overview blade	Configure or change policies Reset password for a user Configure alerts Give feedback on detections

The **Security Operator** role cannot access the Risky sign-ins report.
Conditional Access Administrators can also create policies that factor in sign-in risk as a condition.

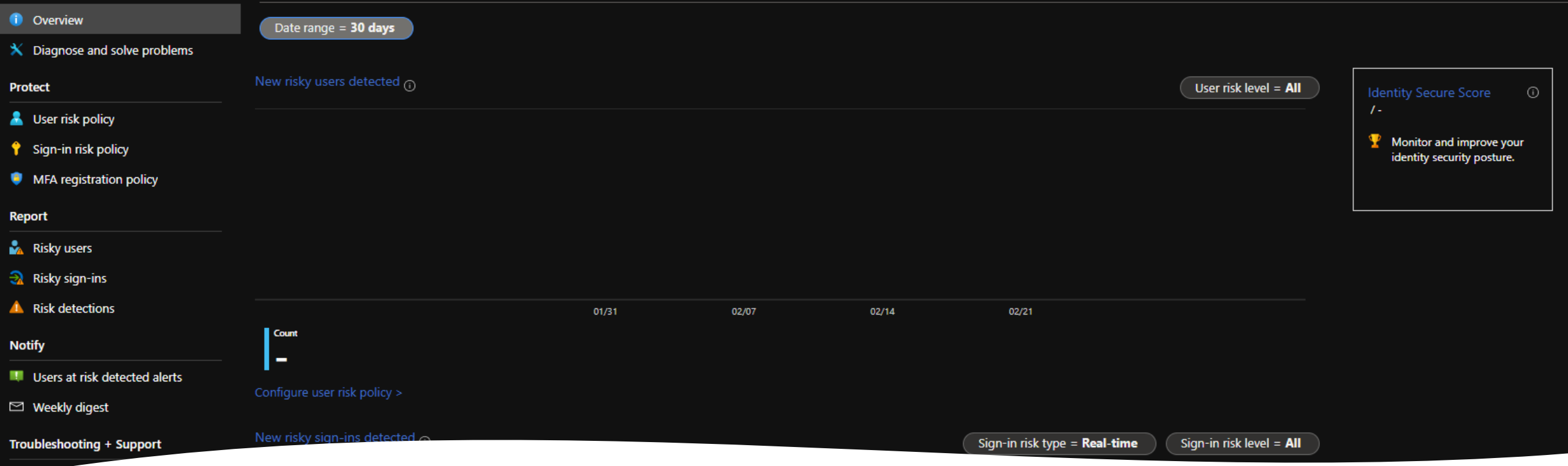
Azure Identity Protection

Identity Protection requires an Azure AD Premium P2 license



LICENSE REQUIREMENTS				
Capability	**Details**	**Azure AD Free / Microsoft 365 Apps**	**Azure AD Premium P1**	**Azure AD Premium P2**
Risk policies	User risk policy (via Identity Protection)	No	No	Yes
Risk policies	Sign-in risk policy (via Identity Protection or Conditional Access)	No	No	Yes
Security reports	Overview	No	No	Yes
Security reports	Risky users	Limited Information. Only users with medium and high risk are shown. No details drawer or risk history.	Limited Information. Only users with medium and high risk are shown. No details drawer or risk history.	Full access
Security reports	Risky sign-ins	Limited Information. No risk detail or risk level is shown.	Limited Information. No risk detail or risk level is shown.	Full access
Security reports	Risk detections	No	Limited Information. No details drawer.	Full access
Notifications	Users at risk detected alerts	No	No	Yes
Notifications	Weekly digest	No	No	Yes
	MFA registration policy	No	No	Yes

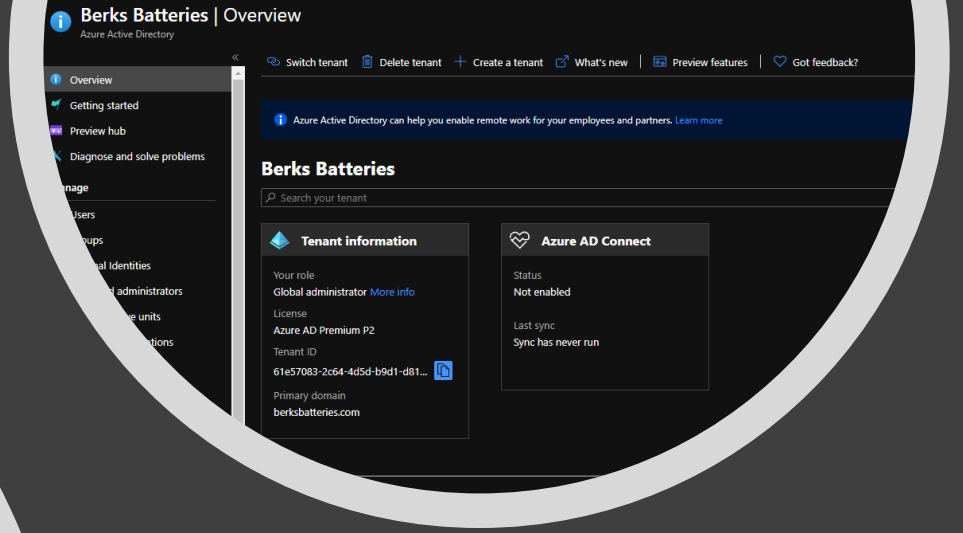
Azure Identity Protection



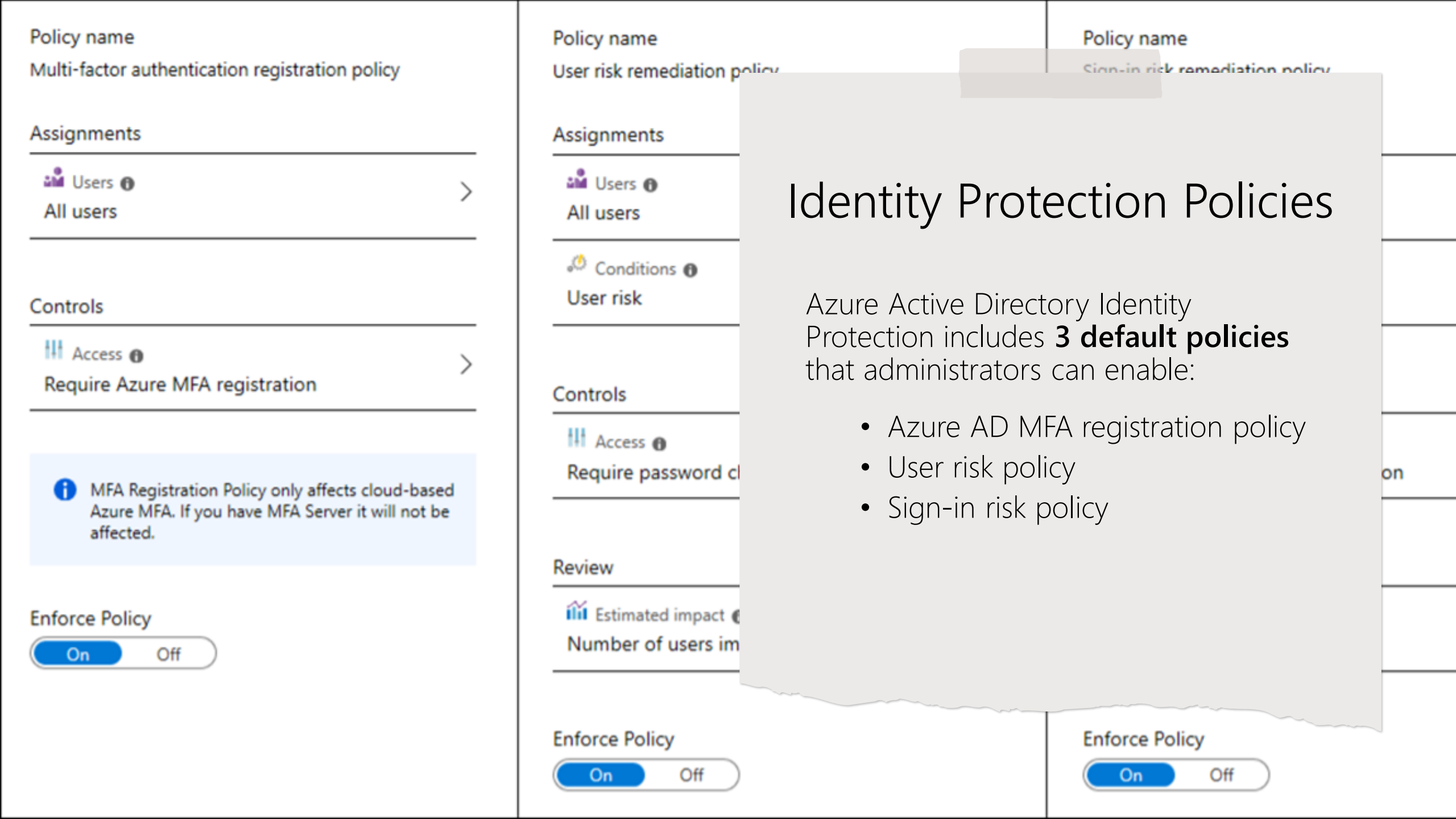
Azure Identity Protection

Azure Identity Protection is a tool that allows organizations to accomplish several tasks:

- Automate detection & remediation of identity-based risks
- Investigate risks using data in the portal
- Export risk detection data to third-party tools



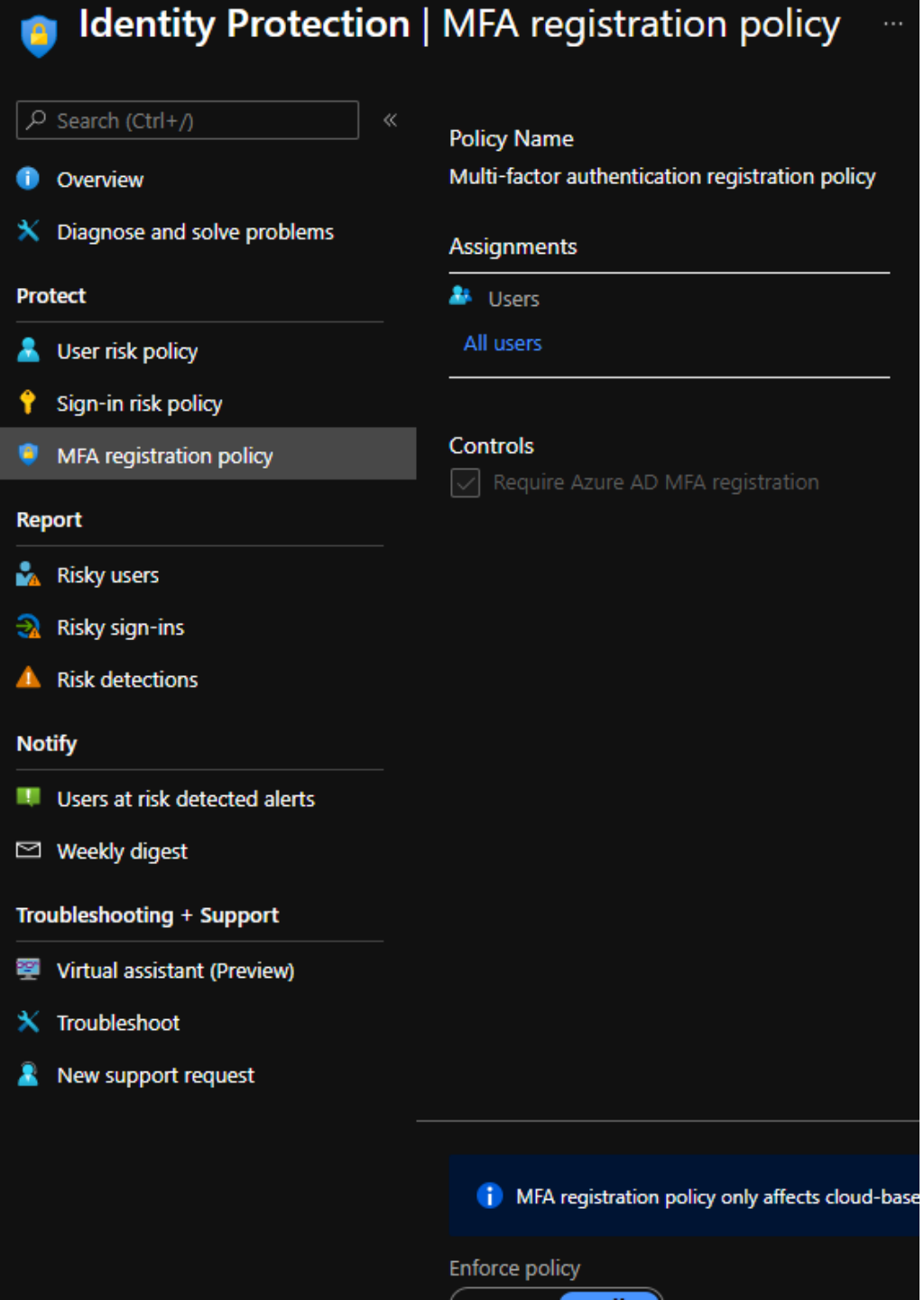
Identity Protection Policies



Identity Protection Policies

Azure Active Directory Identity Protection includes **3 default policies** that administrators can enable:

- Azure AD MFA registration policy
- User risk policy
- Sign-in risk policy



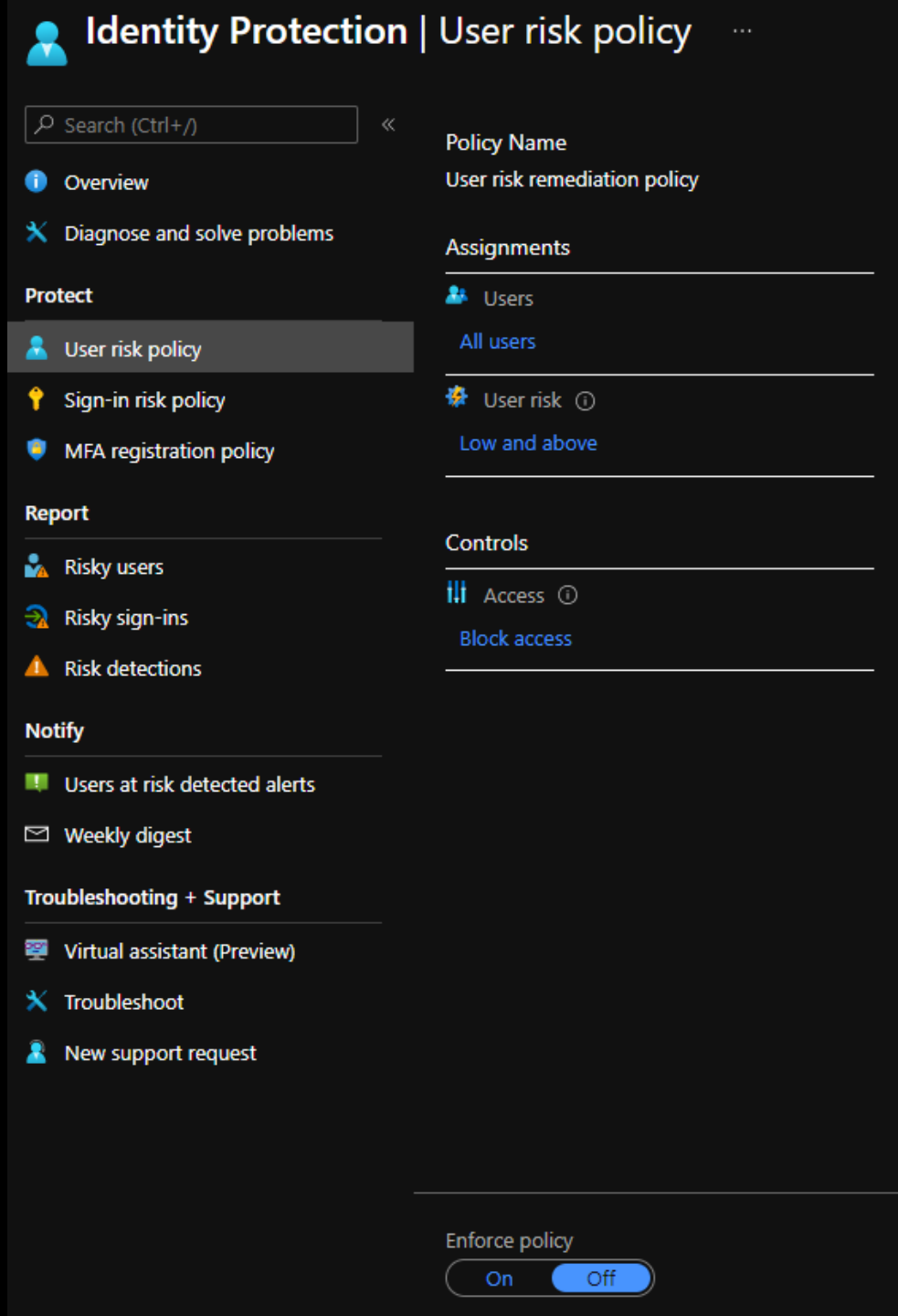
Azure AD MFA Registration Policy

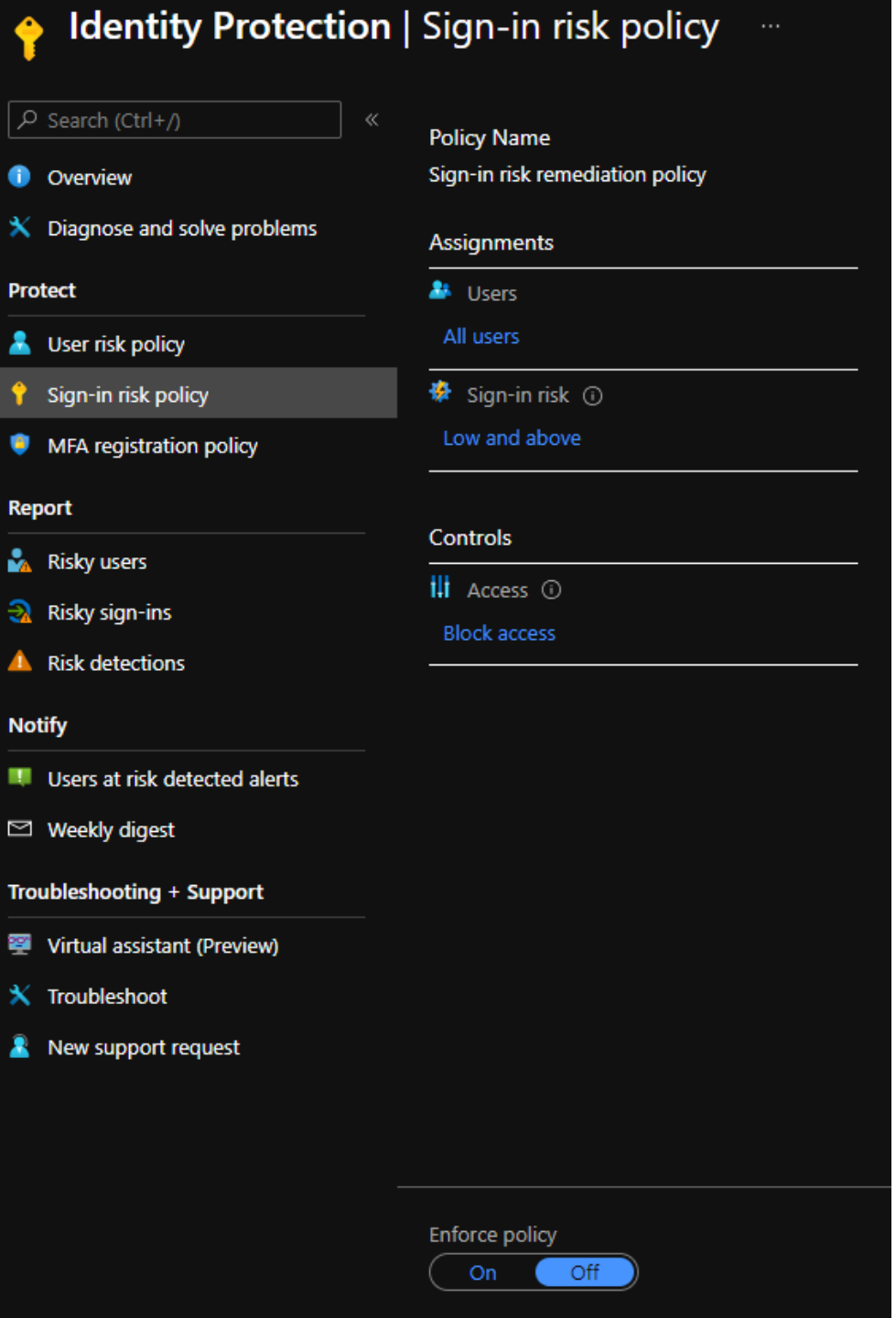
The **Azure AD MFA Registration Policy** ensures new users have registered for MFA on their first day.

- Multi-factor authentication is a self-remediation method for risk events within Identity Protection that allows users to take action on their own to reduce helpdesk call volume.

User Risk Policy

- Used to calculate what Identity Protection believes is normal behavior for a user.
- Calculates probability that an identity has been compromised.
- Administrator can make a decision based on this risk score signal.
  - Block access
  - Allow access
  - Allow access / require password change via SSPR
- Users can perform self-service password reset to self-remediate.





Sign-In Risk Policy

Identity Protection analyzes signals from each sign-in, both real-time and offline.

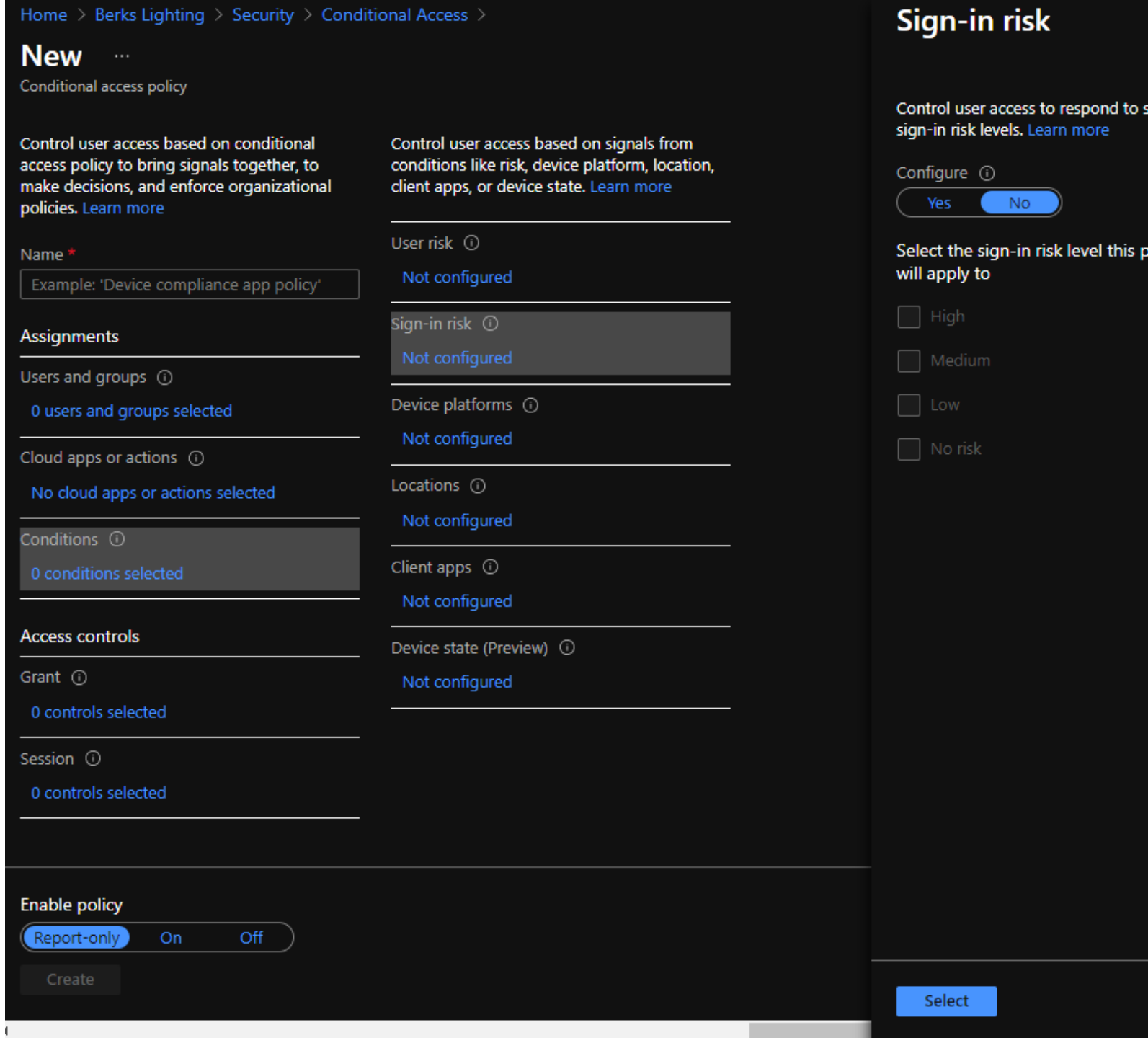
- Calculates a risk score based on the probability that a specific sign-in wasn't performed by the actual user.

Administrators can choose to:

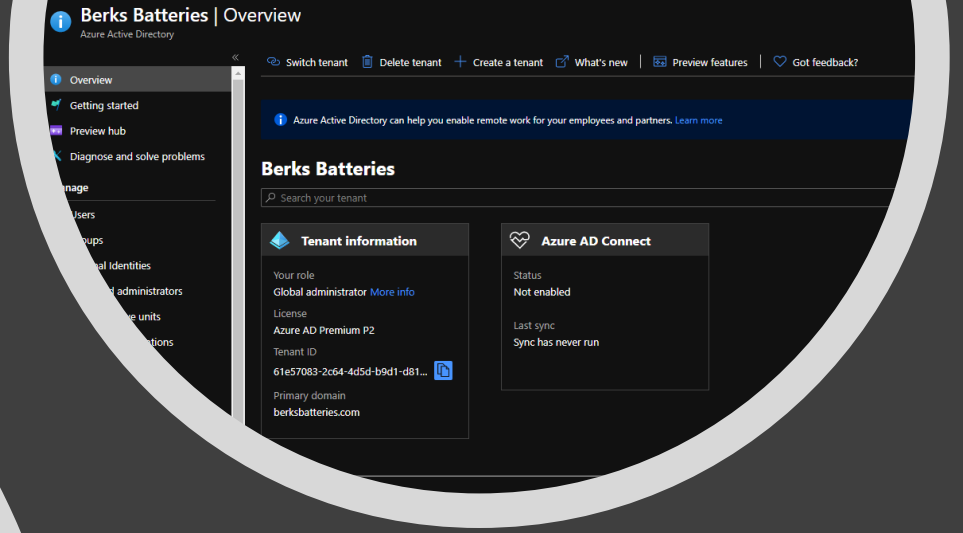
- Block access
- Allow access
- Allow access but require MFA

Custom Conditional Access Policy

Administrators can create custom Conditional Access policies that include sign-in risk as an assignment condition.



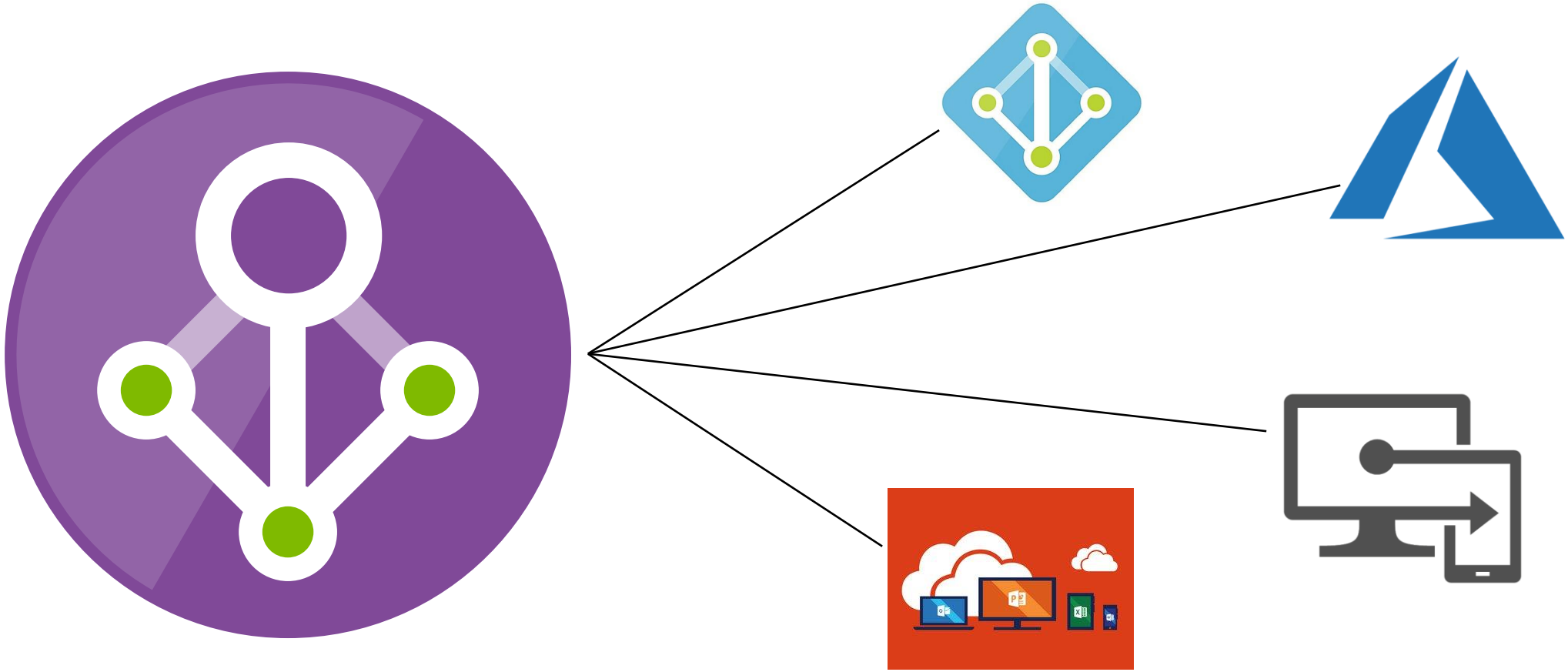
HANDS-ON LAB!


Berks Batteries | Overview
Azure Active Directory
Switch tenant
Delete tenant
Create a tenant
What's new
Preview features
Got feedback?
Overview
Getting started
Preview hub
Diagnose and solve problems
Azure Active Directory can help you enable remote work for your employees and partners. Learn more
Berks Batteries
Search your tenant
Tenant information
Your role
Global administrator More info
License
Azure AD Premium P2
Tenant ID
61e57083-2c64-4d5d-b9d1-d81...
Primary domain
berksbatteries.com
Azure AD Connect
Status
Not enabled
Last sync
Sync has never run

Azure AD PIM

Privileged Identity Management

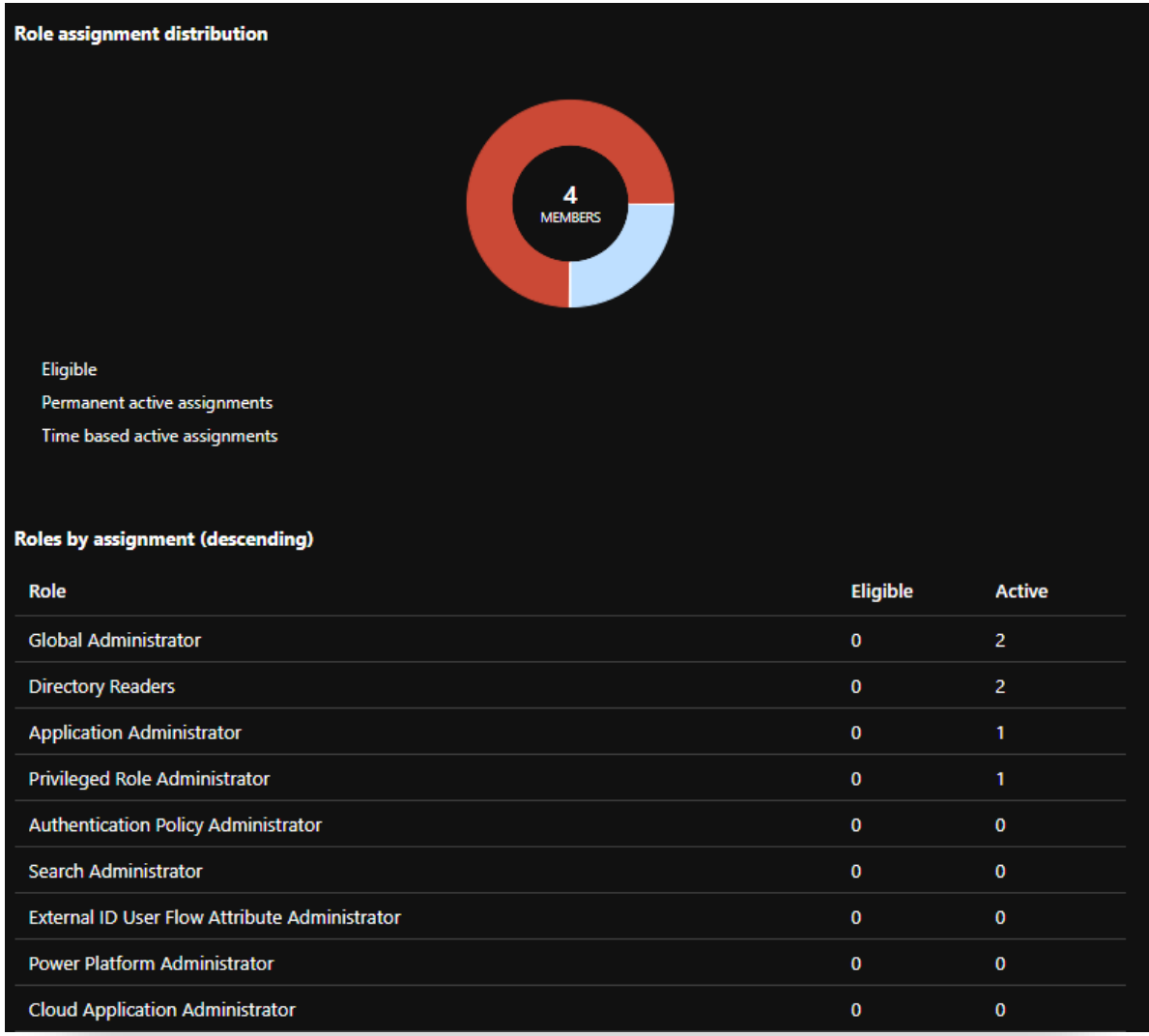
Privileged Identity Management is an Azure AD service that is used to manage, control, and monitor access to critical resources.



PIM Use Cases

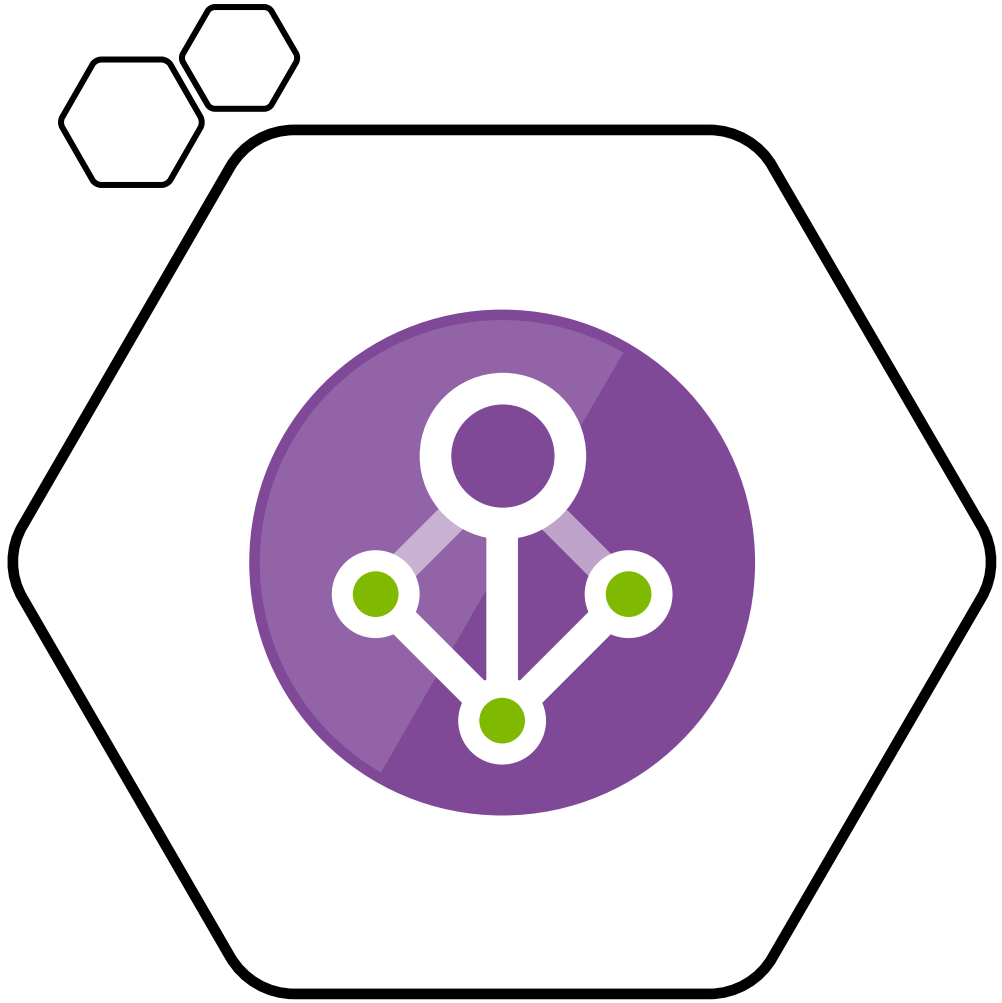
PIM is useful to organizations that want to minimize the number of people who have access to critical information or resources.

- Reduces the chance of a malicious actor getting that access
- Reduces chances of an authorized user impacting a sensitive resource
- Allows just-in-time privileged access to Azure resources and Azure AD
- Provides oversight for what users are doing with admin privileges



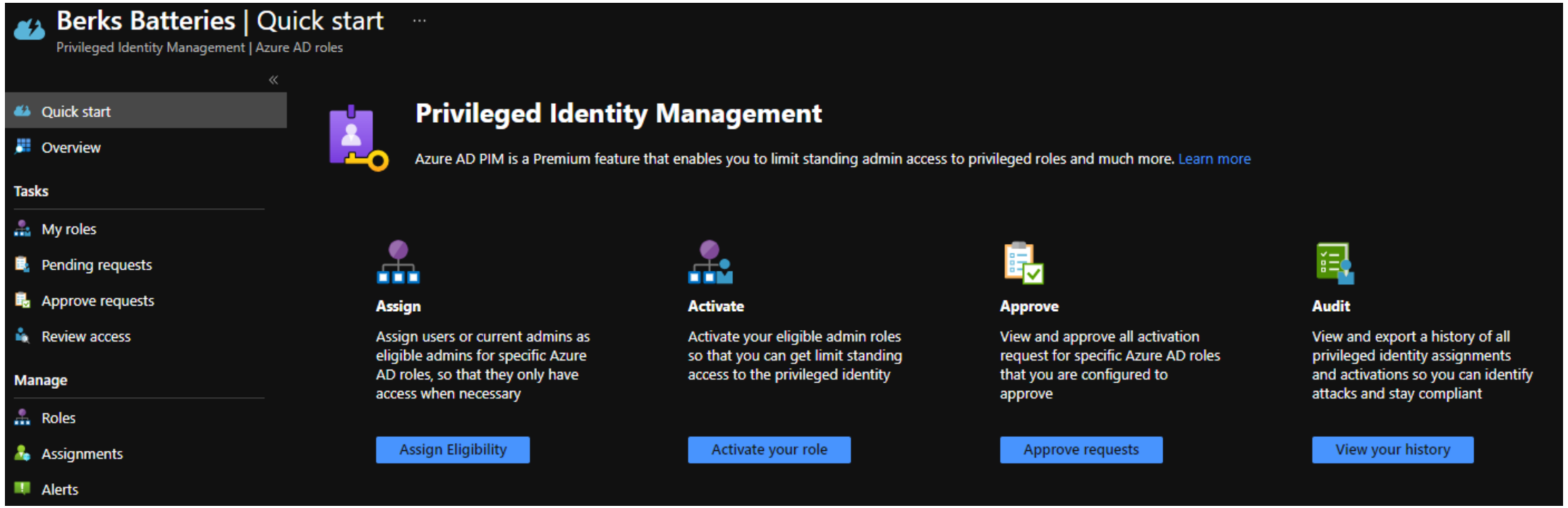
Key Features of PIM:

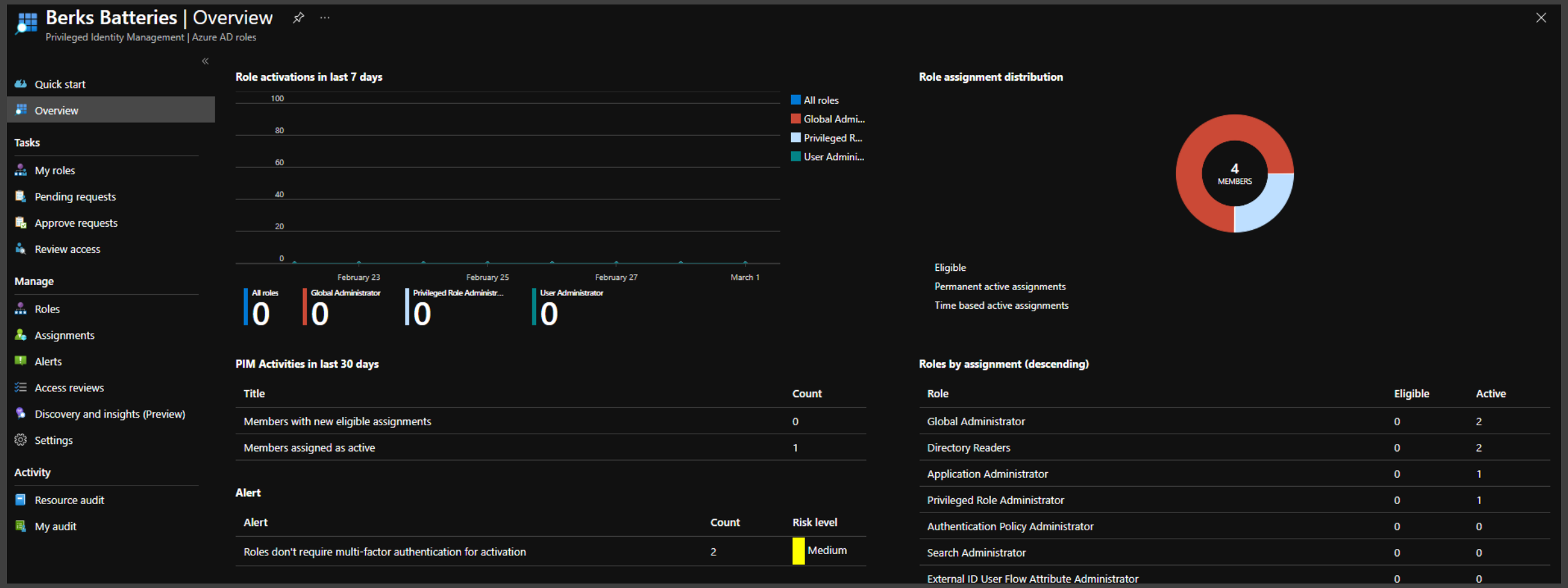
- Provide just-in-time privileged access to Azure AD and Azure resources
- Assign time-bound access to resources
- Require approval to activate privileged roles
- Enforce MFA to activate any role
- Use justification to understand activations
- Notifications when privileged roles activated
- Conduct access reviews
- Download audit history



Privileged Identity Management

As an administrator, you can choose to manage Azure AD roles, Azure resource roles, or privileged access groups.

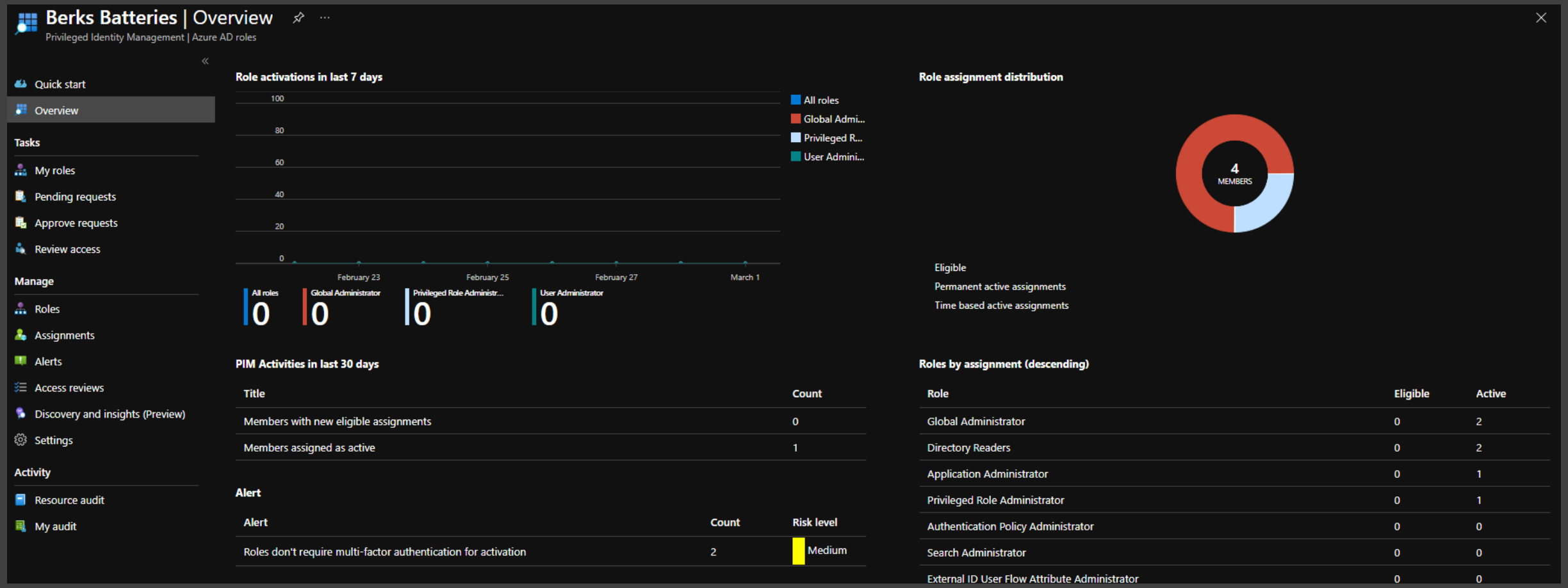




Privileged Identity Management

Privileged Role Administrator Permissions:

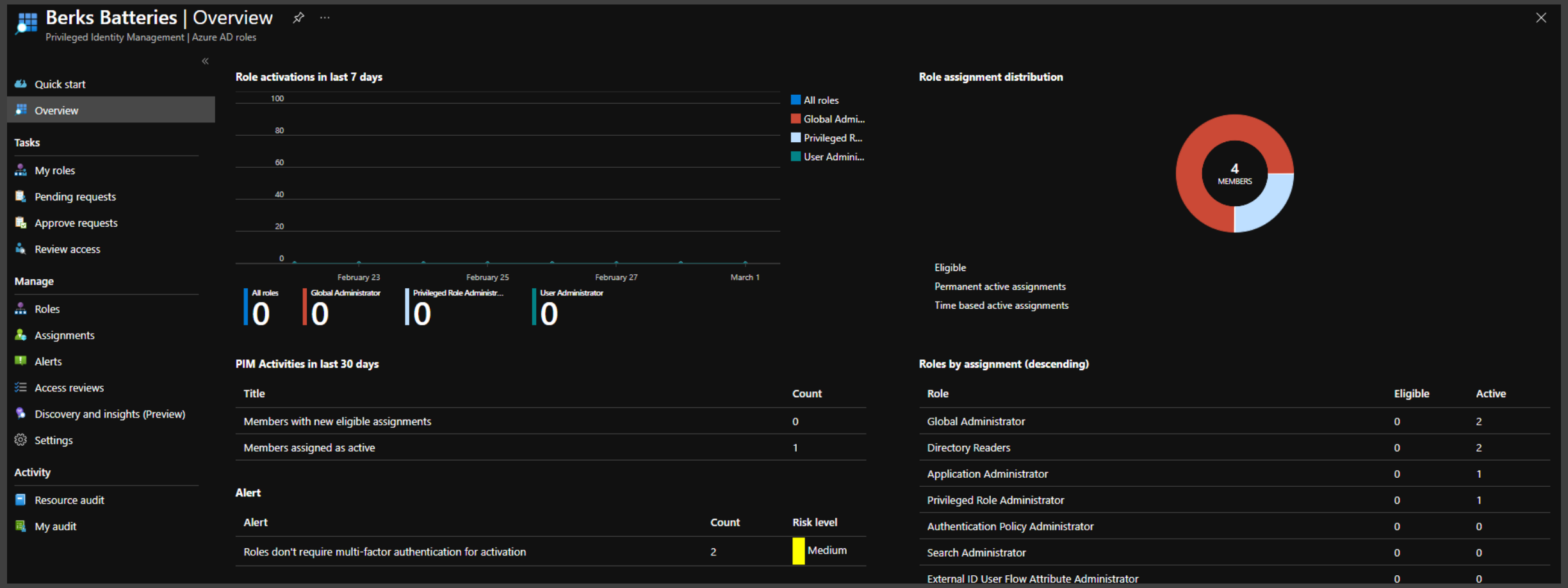
- Enable approval for specific roles
- Specify approver users or groups to approve requests
- View request and approval history for all privileged roles



Privileged Identity Management

Approver Permissions:

- View pending approvals
- Approve or reject requests for role elevation
- Provide justification for my approval or rejection

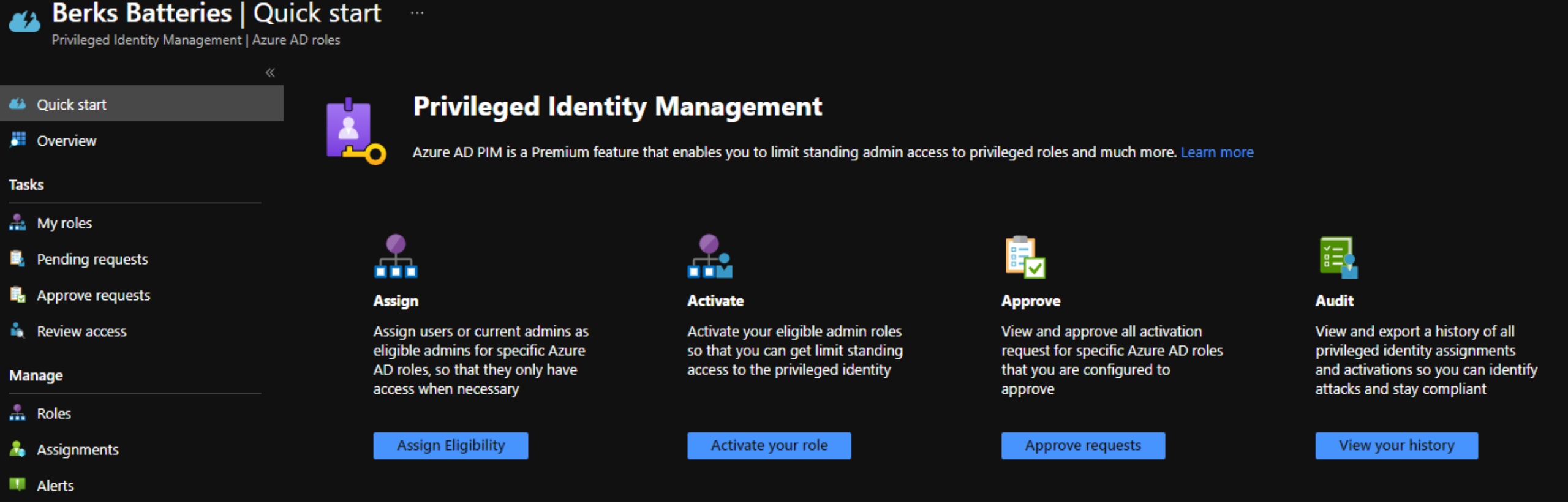


Privileged Identity Management

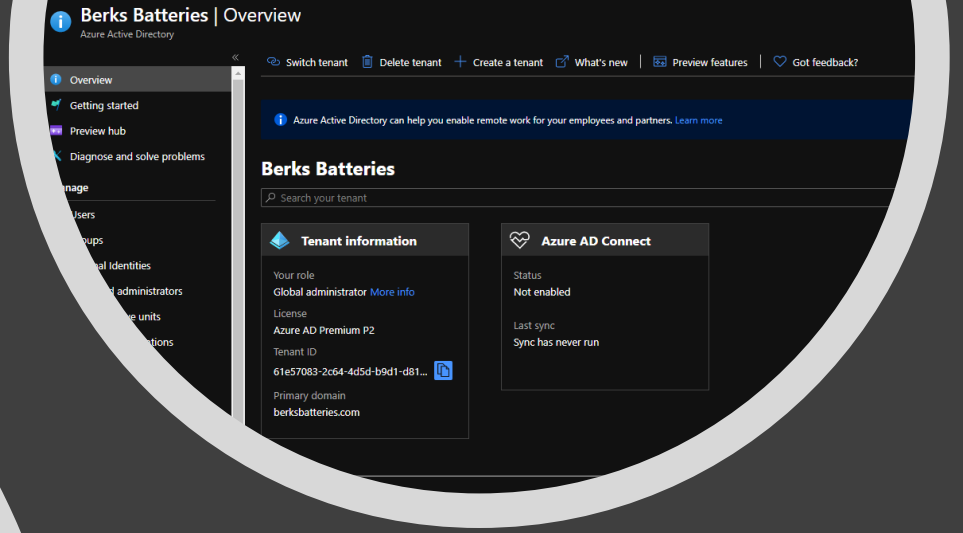
Eligible Role User Permissions:

- Request activation of a role that requires approval
- View the status of your request to activate
- Complete task in Azure AD if activation approved

Term or concept	Role assignment category	Description
eligible	Type	A role assignment that requires a user to perform one or more actions to use the role. If a user has been made eligible for a role, that means they can activate the role when they need to perform privileged tasks. There's no difference in the access given to someone with a permanent versus an eligible role assignment. The only difference is that some people don't need that access all the time.
active	Type	A role assignment that doesn't require a user to perform any action to use the role. Users assigned as active have the privileges assigned to the role.
activate		The process of performing one or more actions to use a role that a user is eligible for. Actions might include performing a multi-factor authentication (MFA) check, providing a business justification, or requesting approval from designated approvers.
assigned	State	A user that has an active role assignment.
activated	State	A user that has an eligible role assignment, performed the actions to activate the role, and is now active. Once activated, the user can use the role for a preconfigured period-of-time before they need to activate again.
permanent eligible	Duration	A role assignment where a user is always eligible to activate the role.
permanent active	Duration	A role assignment where a user can always use the role without performing any actions.
expire eligible	Duration	A role assignment where a user is eligible to activate the role within a specified start and end date.
expire active	Duration	A role assignment where a user can use the role without performing any actions within a specified start and end date.
just-in-time (JIT) access		A model in which users receive temporary permissions to perform privileged tasks, which prevents malicious or unauthorized users from gaining access after the permissions have expired. Access is granted only when users need it.
principle of least privilege access		A recommended security practice in which every user is provided with only the minimum privileges needed to accomplish the tasks they are authorized to perform. This practice minimizes the number of Global Administrators and instead uses specific administrator roles for certain scenarios.



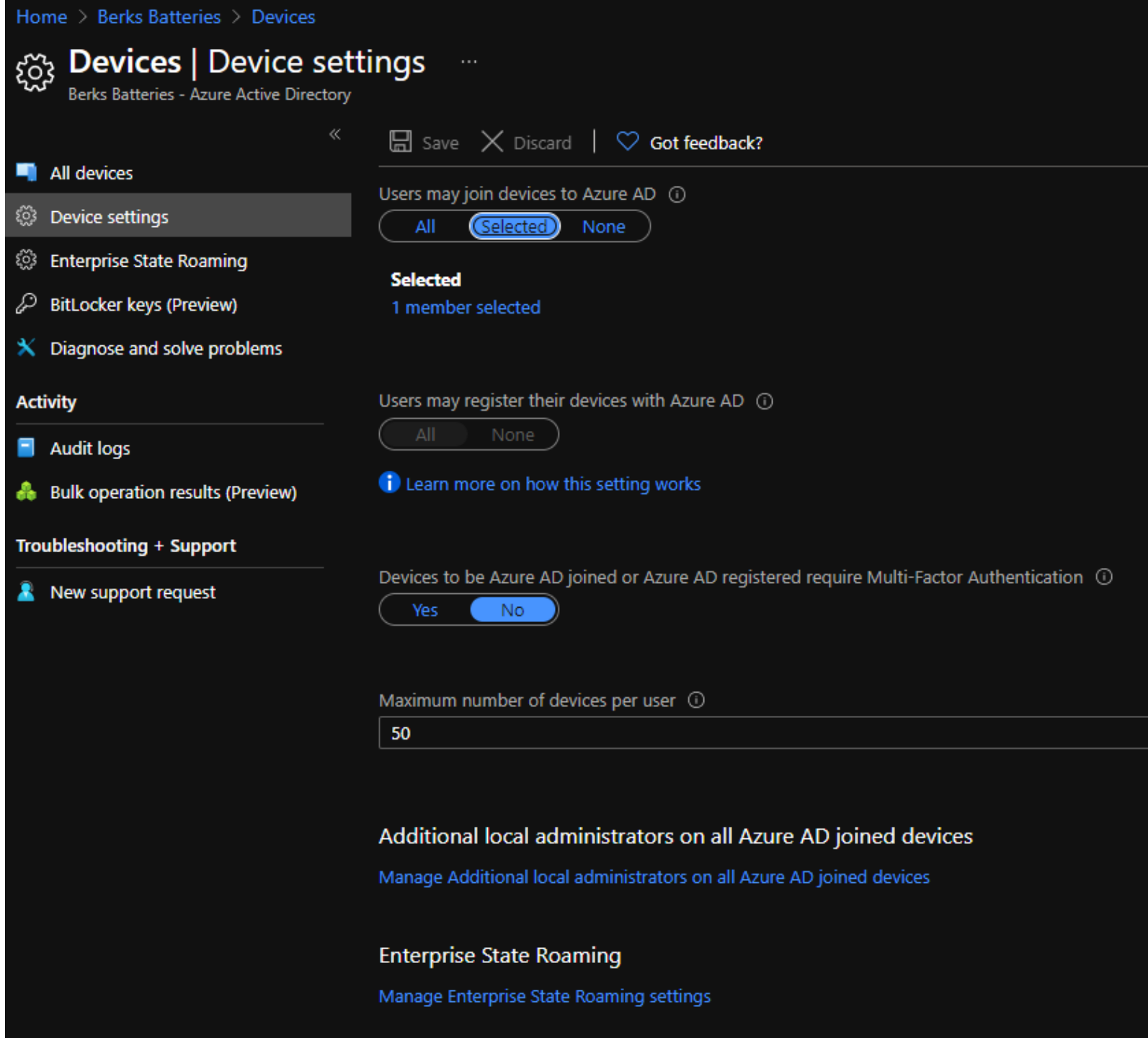
https://docs.microsoft.com/azure/active-directory/privileged-identity-management/subscription-requirements



Configuring & Managing Device Registration

Configure & Manage Device Registration

With the advent of BYOD, organizations want to allow end-users to be productive wherever they are located and whenever they are working, while also protecting their assets.



Configure & Manage Device Registration

Organizations can use tools like Microsoft InTune to ensure that devices meet corporate security standards and compliance.

Leveraging Azure active directory enables single sign-on for devices, applications, and services from anywhere in the world, through these devices.

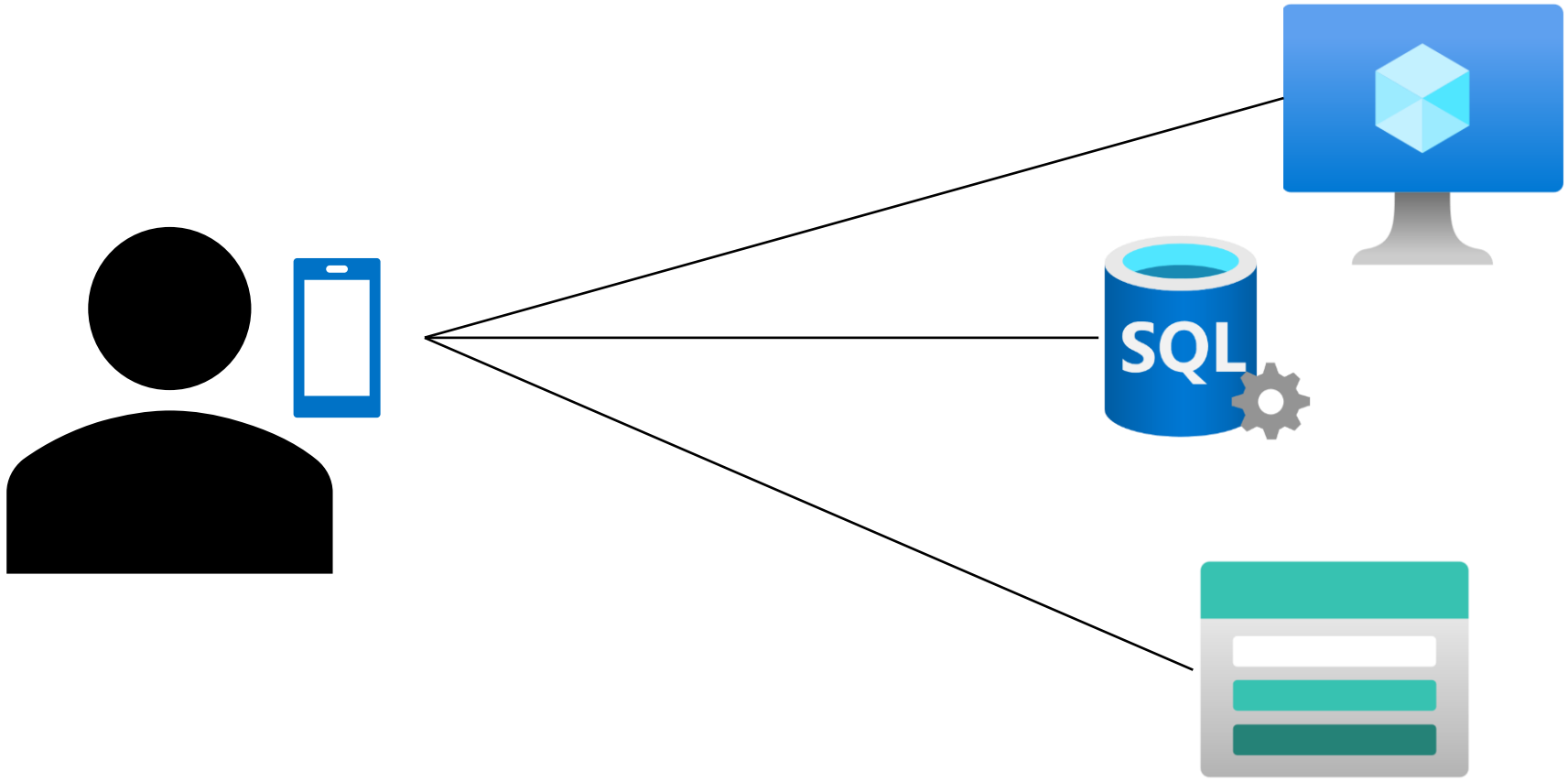
Configure & Manage Device Registration

There are two ways to manage devices in Azure AD:

- Azure AD Registered Devices
- Azure AD Joined Devices (including Hybrid Join)

Azure AD Registered Devices

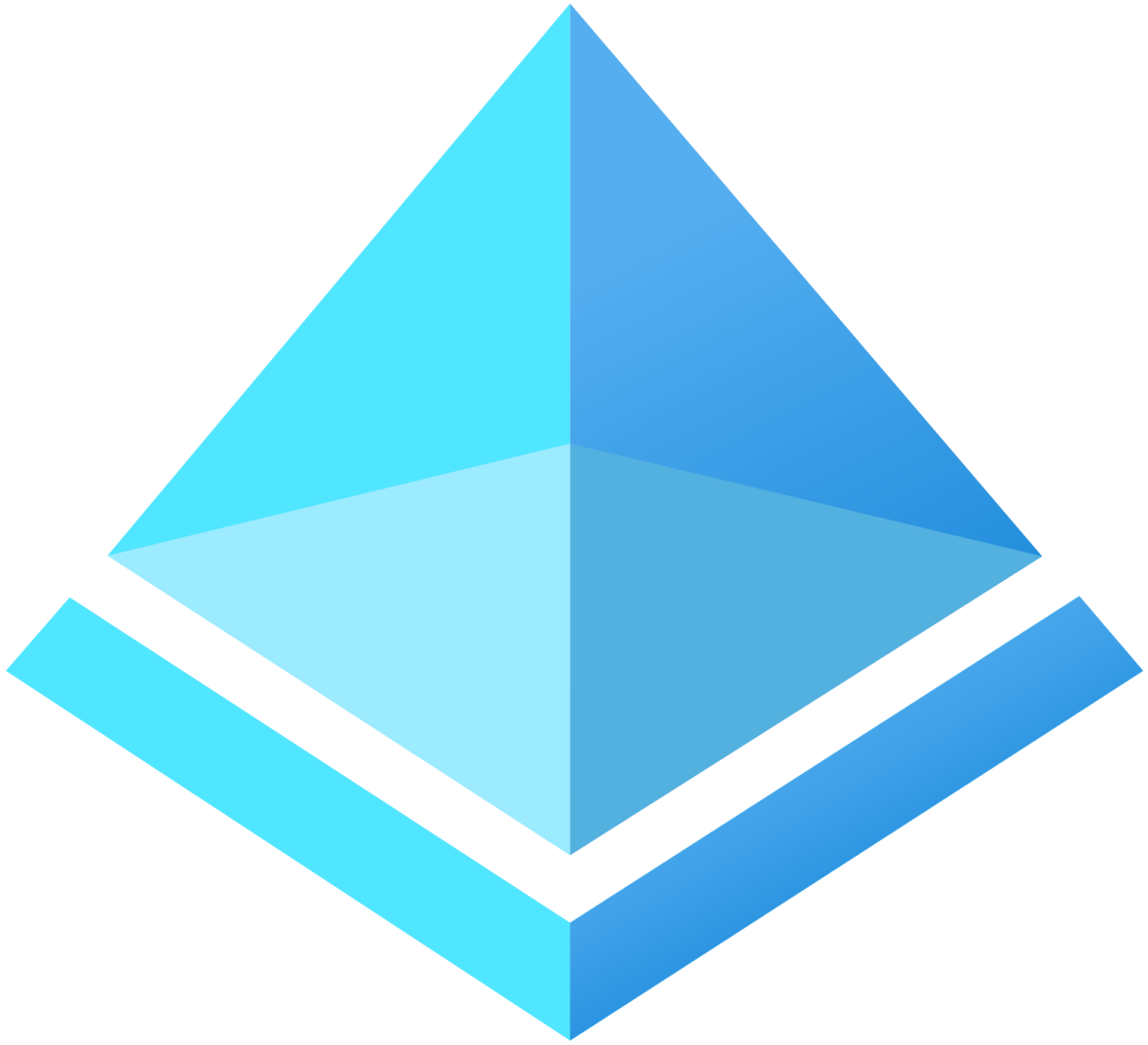
Azure AD Registered devices allow organizations to support BYOD scenarios.

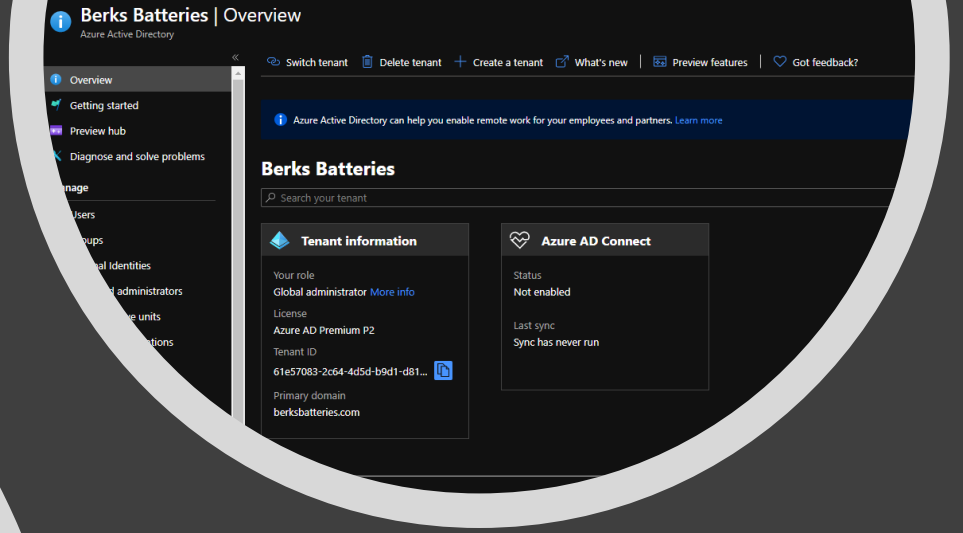


Azure AD Joined Devices

Azure AD Join is designed for organizations that prefer to be cloud first or even cloud only.

Intended for organizations who wish to have a very small on-prem footprint or no on-prem footprint.



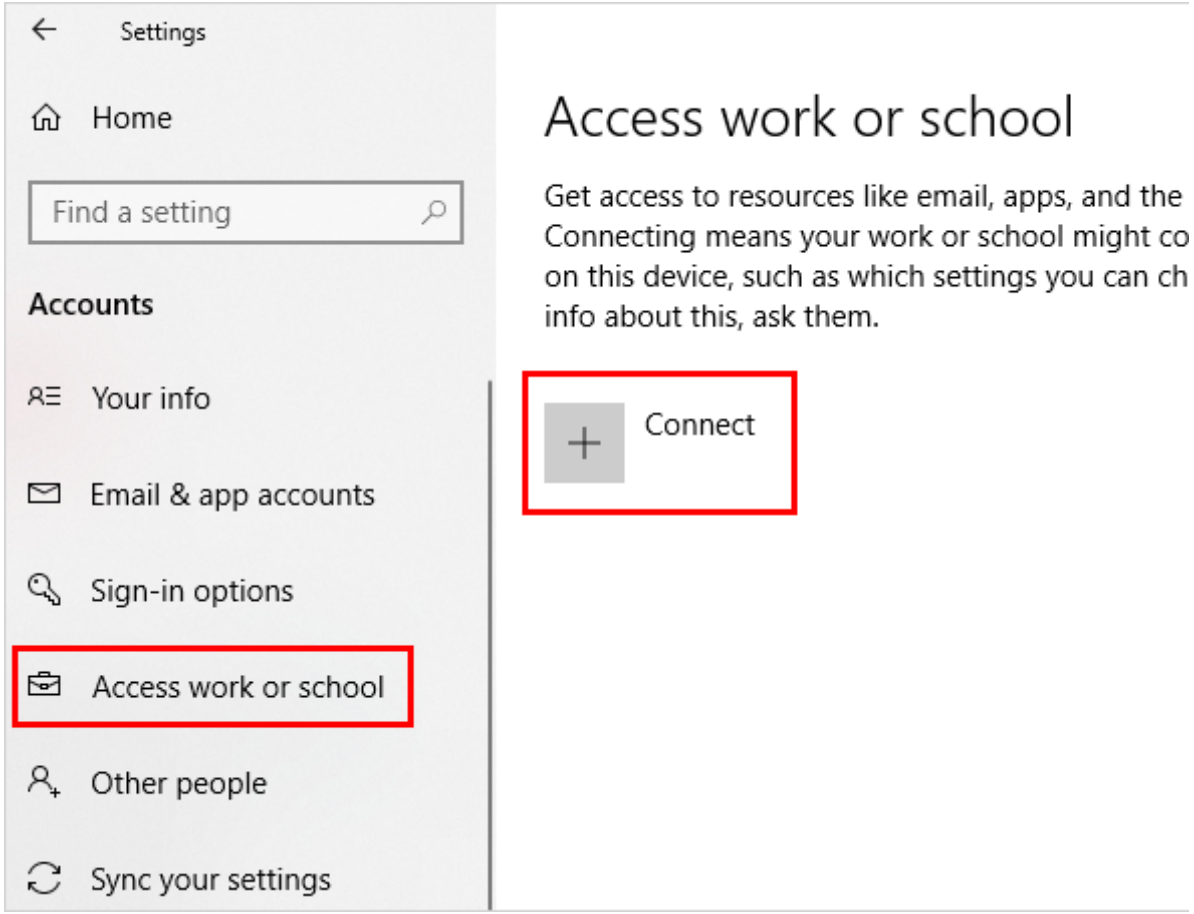


Azure AD Registered Devices

Azure AD Registered Devices

Azure AD registered devices allow organizations to support BYOD scenarios.

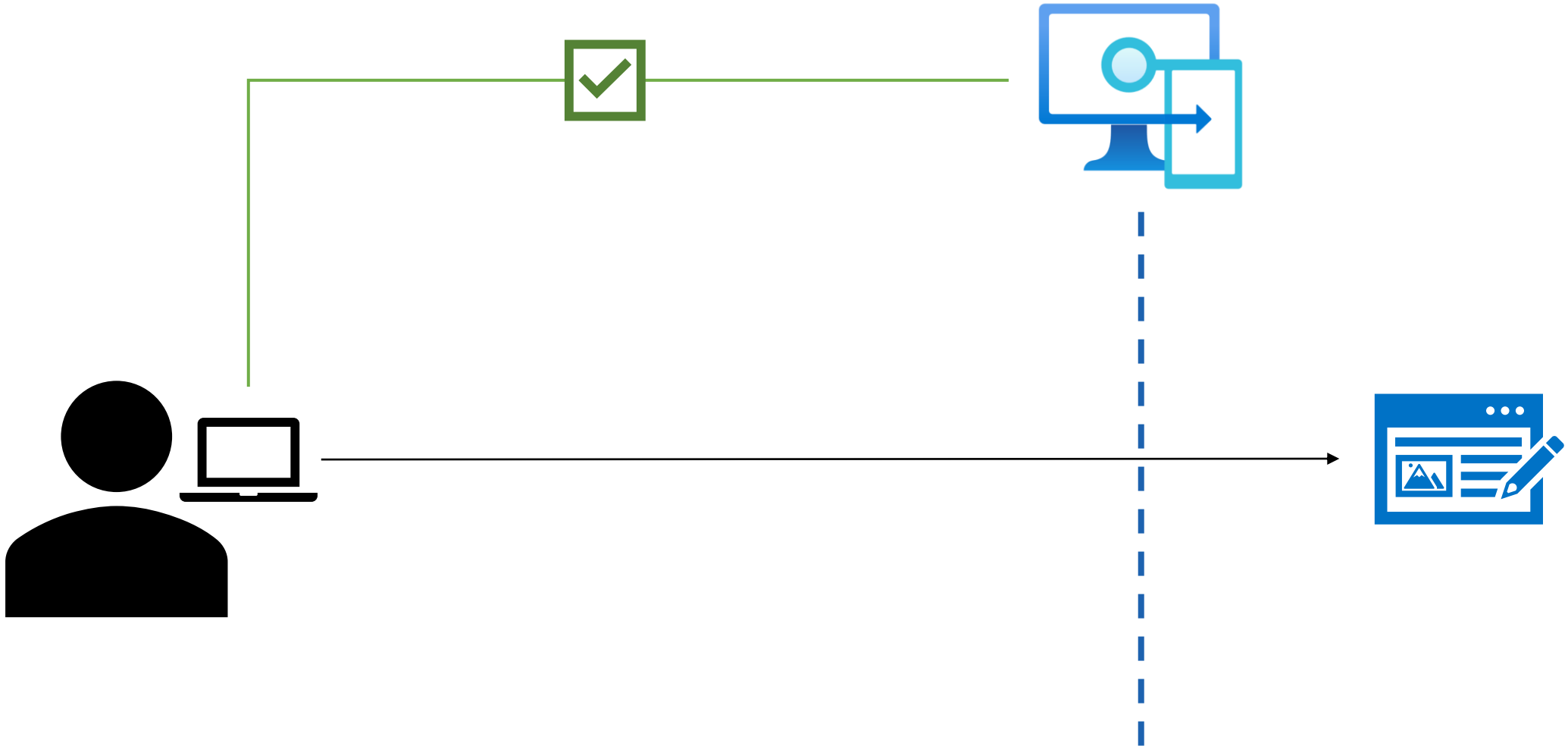
Allows users to access Azure AD-controlled resources while using their own personal devices.

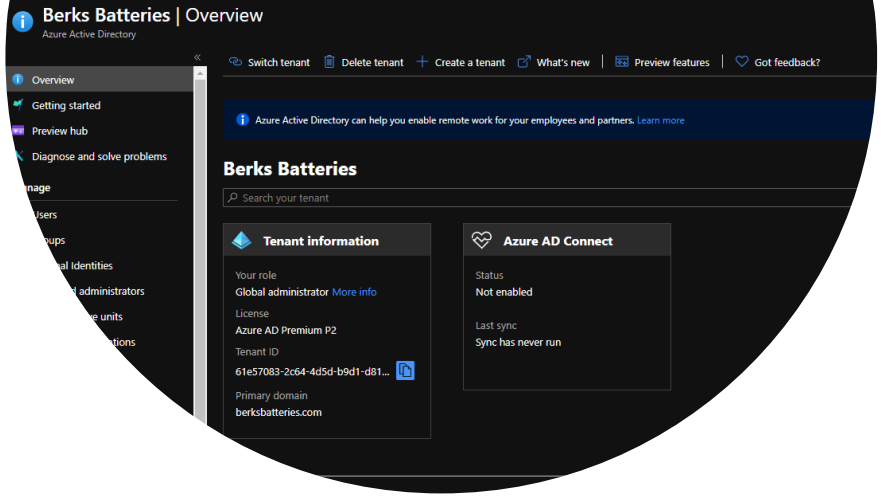


Azure AD Registered Devices

Definition	Registered to Azure AD without requiring organizational account to sign in to the device
Primary audience	• Applicable to all users with the following criteria: • --Bring your own device (BYOD) & Mobile devices
Device ownership	User or Organization
Operating systems	Windows 10, iOS, Android, and macOS
Provisioning	• Windows 10 – Settings • iOS/Android – Company Portal or Microsoft Authenticator app • macOS – Company Portal
Device sign in options	• End-user local credentials • Password • Windows Hello • PIN • Biometrics or Pattern for other devices
Device management	• Mobile Device Management (example: Microsoft Intune) / Mobile Application Management
Key capabilities	• SSO to cloud resources • Conditional Access when enrolled into Intune • Conditional Access via App protection policy • Enables Phone sign in with Microsoft Authenticator app

Azure AD Registered Devices



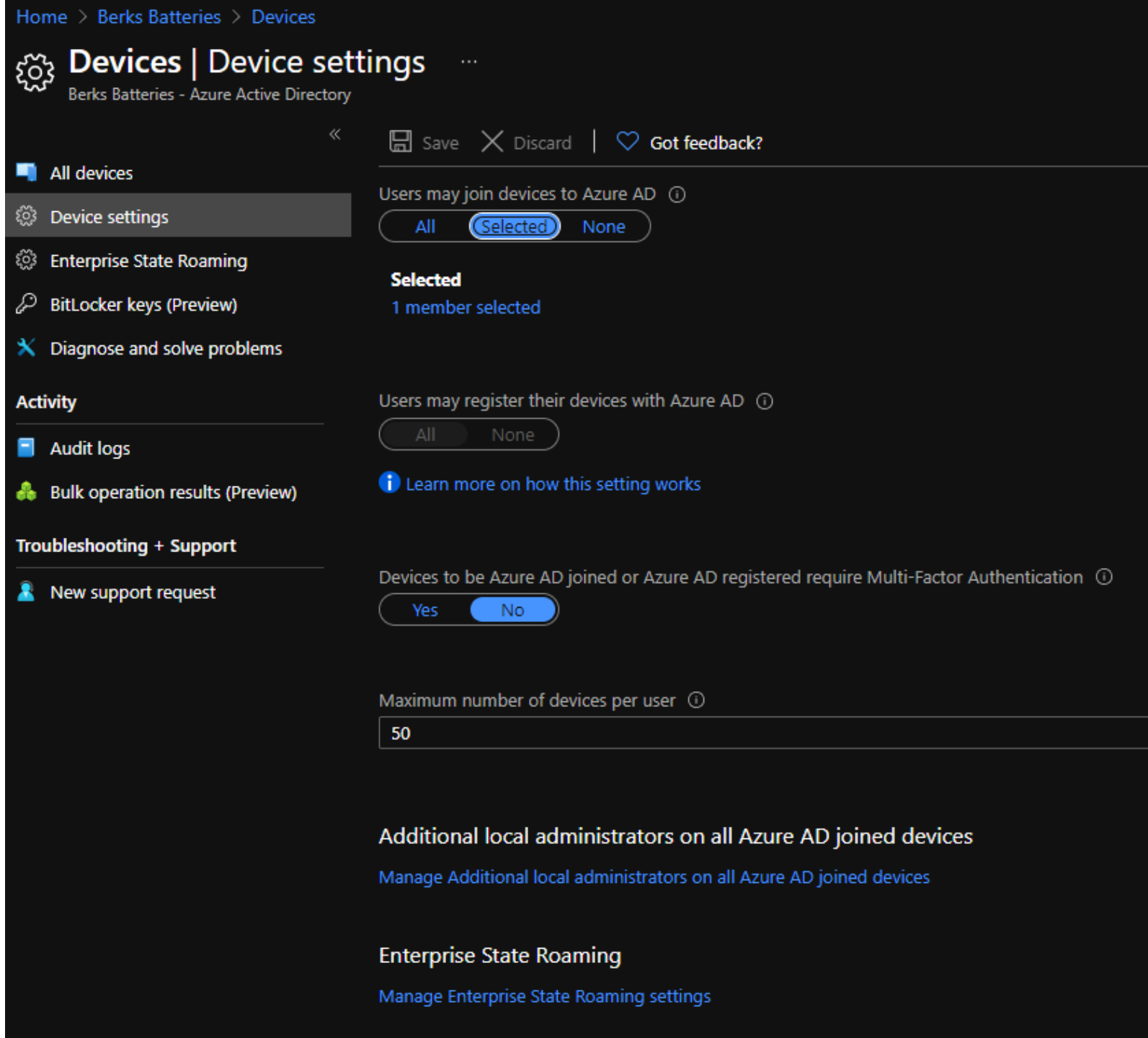


Azure AD Joined Devices

Azure AD Joined Devices

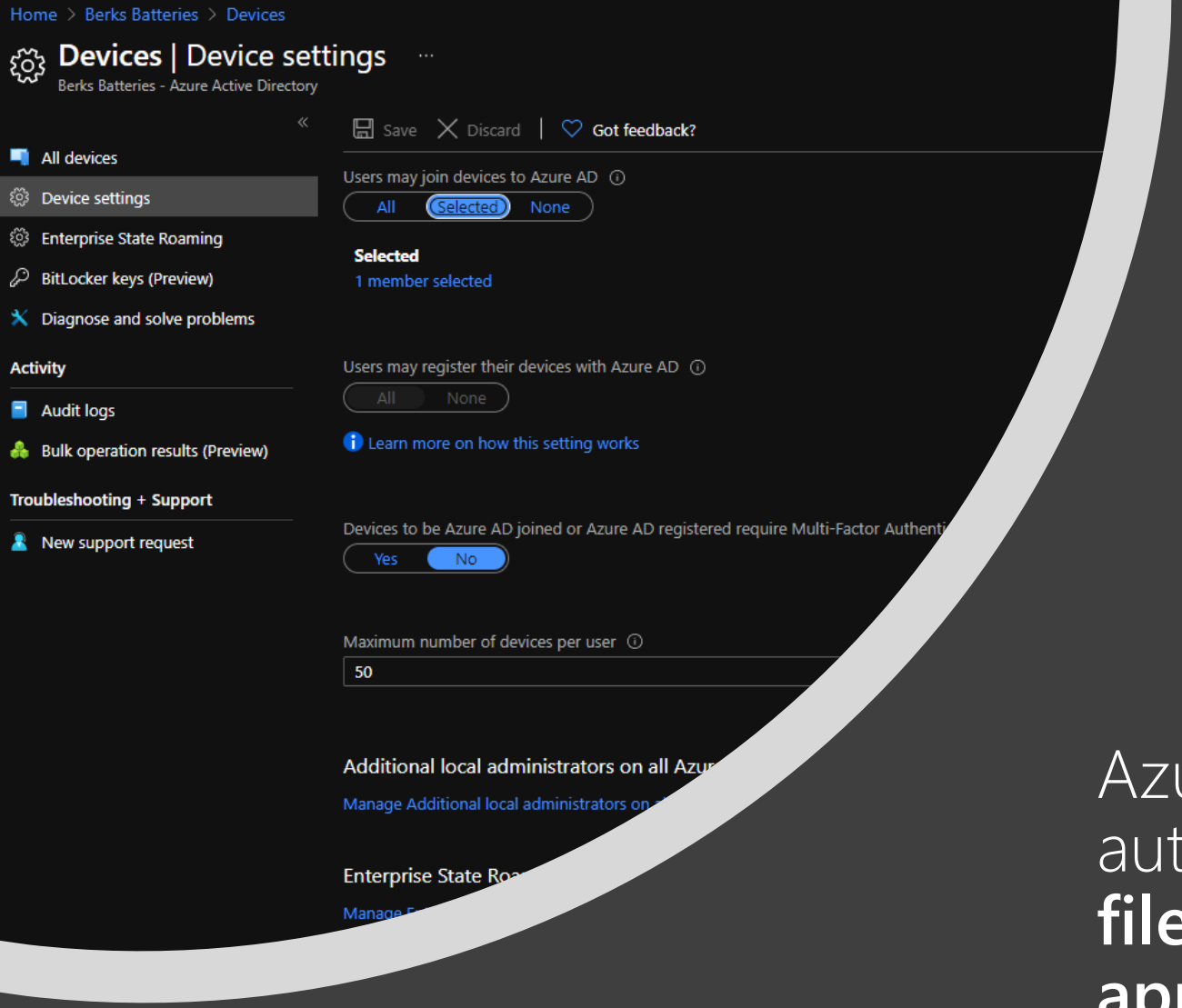
Designed for organizations that prefer to be cloud first or even cloud only.

For organizations who wish to have a very small on-prem footprint or no on-prem footprint at all.



Azure AD Joined Devices

Definition	Joined only to azure AD requiring organizational account to sign into the device
Primary audience	• Suitable for both cloud-only and hybrid organizations • Applicable to all users in an organization
Device ownership	Organization
Operating systems	• All Windows 10 devices except Windows 10 Home • Windows Server 2019 Virtual Machines running in Azure (Server core is not supported)
Provisioning	• Self-service: Windows OOBE or Settings • Bulk enrollment • Windows Autopilot
Device sign in options	• Organizational accounts using: • --Password, Windows Hello for Business, FIDO2.0 security keys (preview)
Device management	• Mobile Device Management (example: Microsoft Intune) • Co-management with Microsoft Intune and Microsoft Endpoint Configuration Manager
Key capabilities	• SSO to both cloud and on-premises resources • Conditional Access through MDM enrollment and MDM compliance evaluation • Self-service Password Reset and Windows Hello PIN reset on lock screen • Enterprise State Roaming across devices

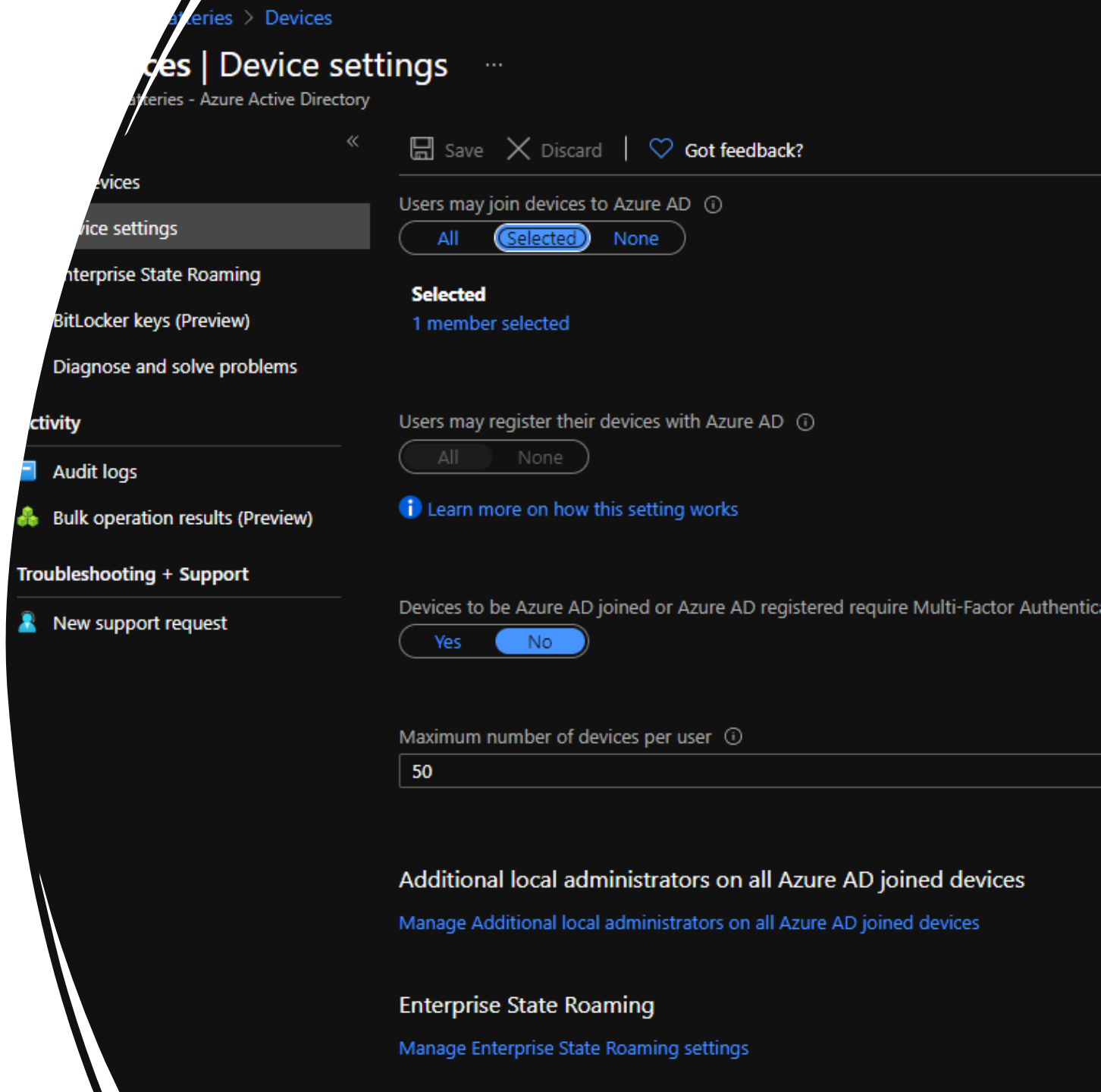


Azure AD Joined devices can still authenticate to on-prem servers like **file servers**, **print servers**, and **application servers**.

Use Cases for Azure AD Joined Devices

Transition to a cloud-based infrastructure using Azure AD and Microsoft InTune.

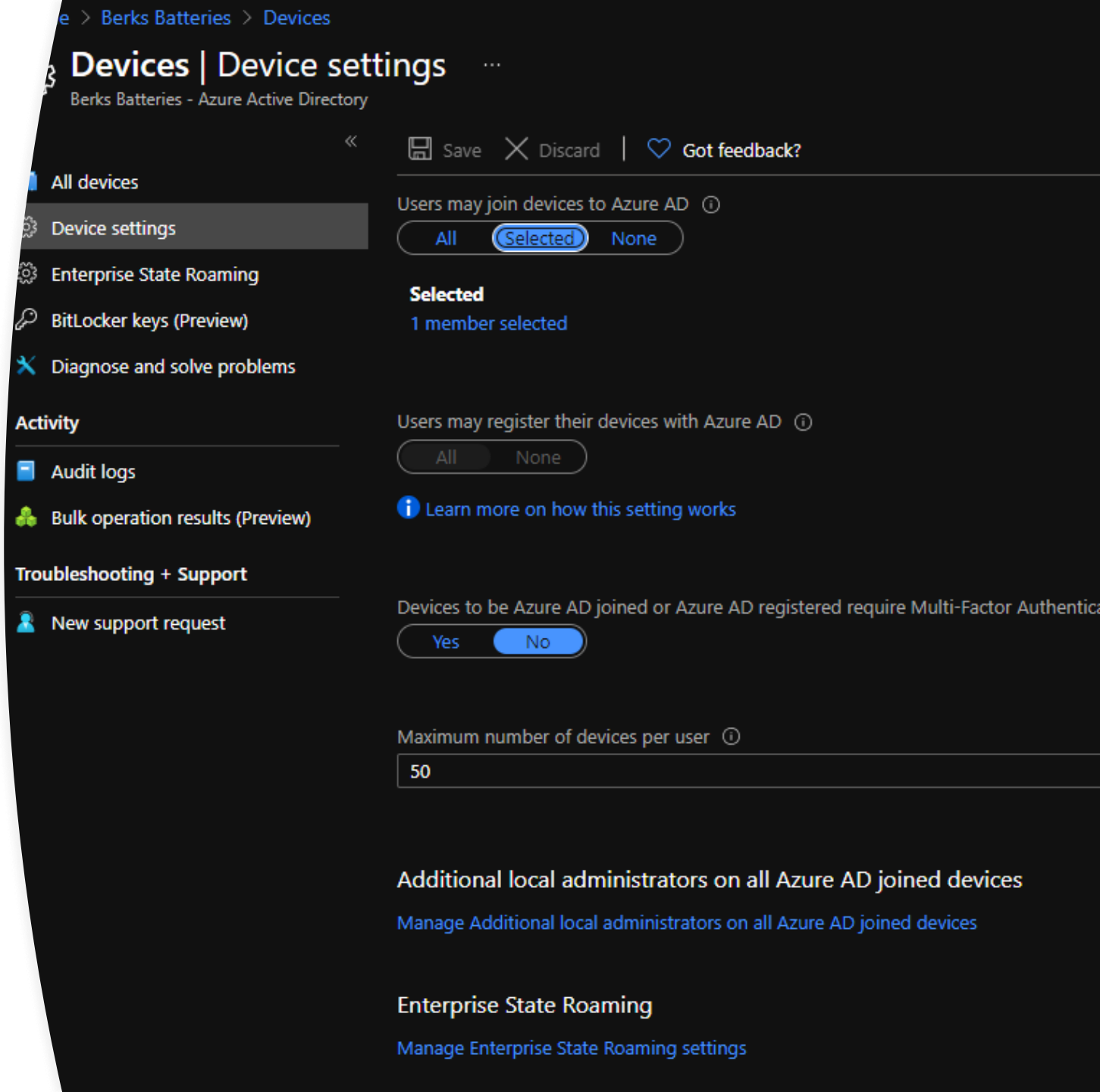
Can’t use an on-prem domain-join, but still need to get a handle on mobile devices, tablets, and phones.



Azure AD Joined Devices

Azure AD Join supports all Windows 10 devices except for those running Windows 10 home.

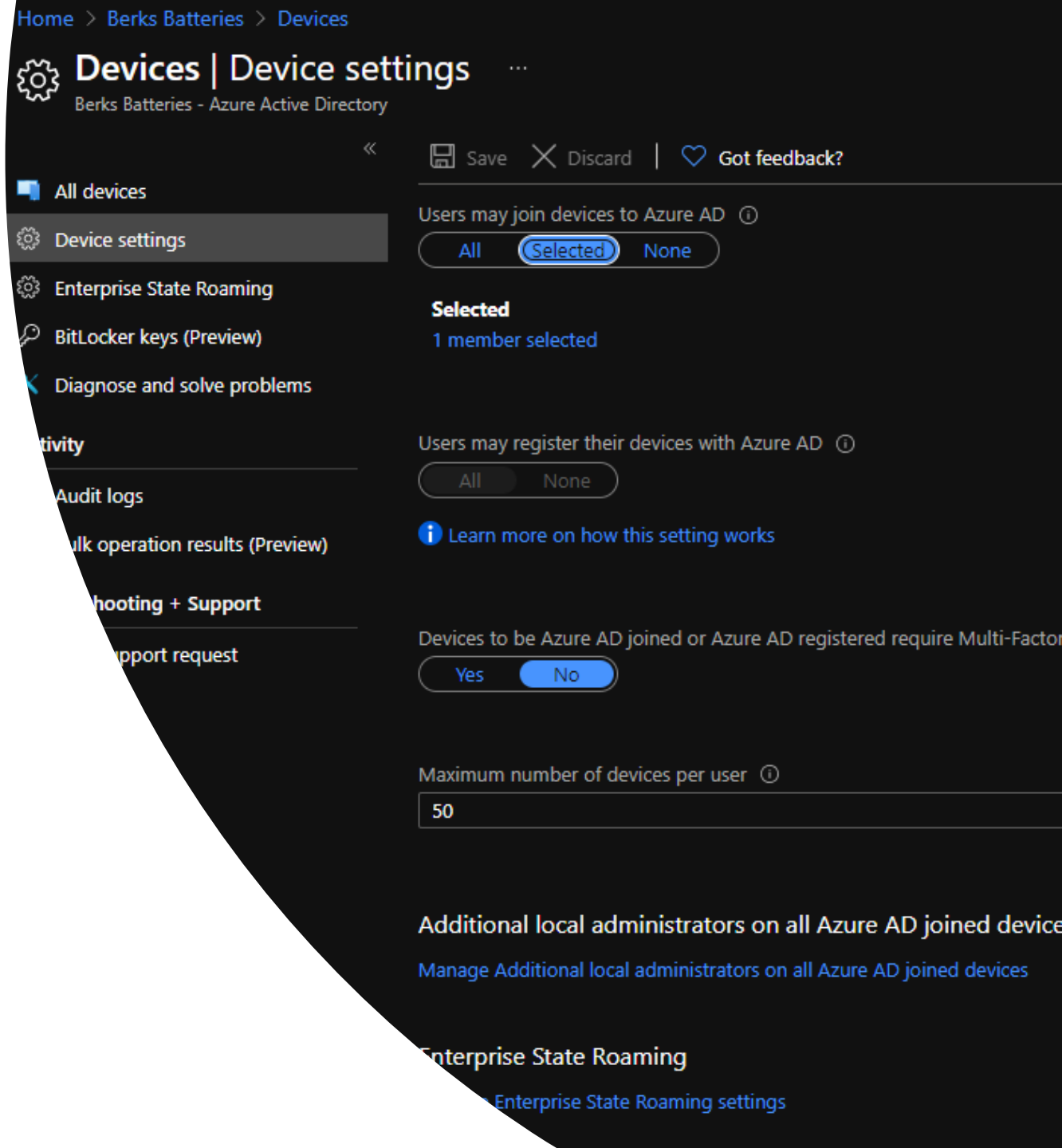
- Simplifies windows deployments of work-owned devices
- Simplifies access to organizational apps and resources
- Simplifies cloud-based management of work-owned devices
- Simplifies the sign in process for users to their devices

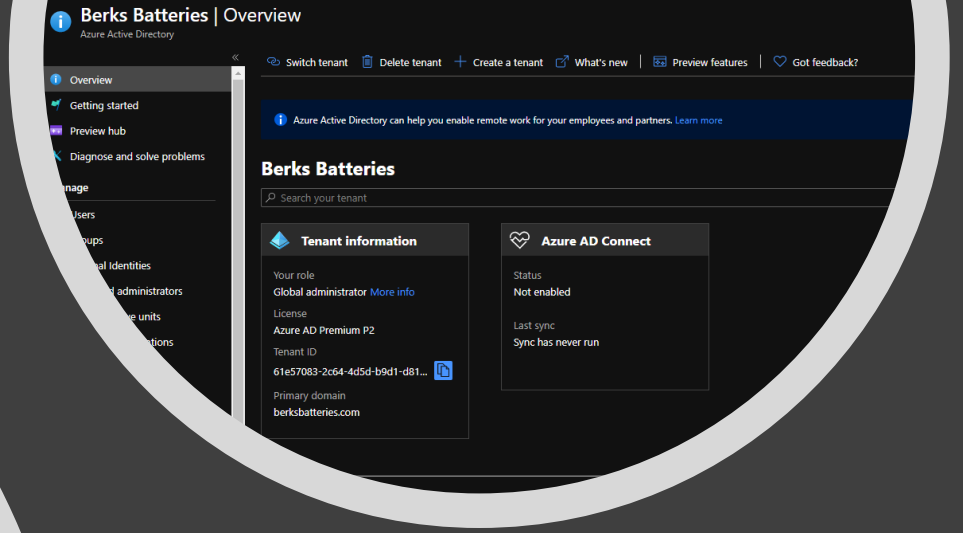


Azure AD Joined Devices

Users can take advantage of self-service to join new Windows 10 devices to Azure AD during the first run experience when the machine is booted up for the first time.

- Device registration service must be configured
- Permissions must be configured
- Fewer devices registered than configured maximum





Hybrid Azure AD Joined Devices

Hybrid Azure AD Joined Devices

Hybrid Azure AD joined devices are joined to an on-prem Active Directory, and are registered with Azure AD.

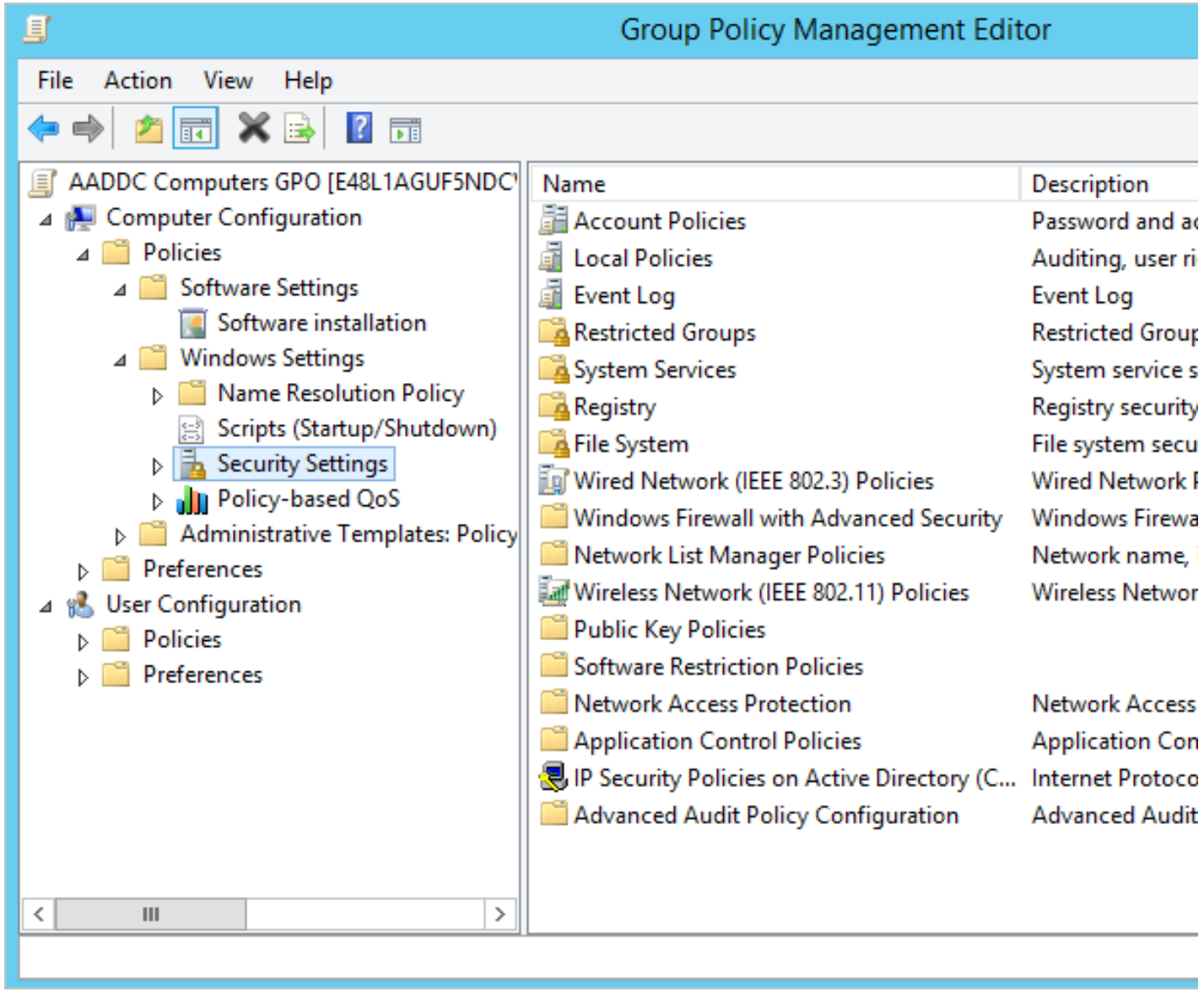
- An organizational account is required to sign into a Hybrid Azure AD joined device.
- Organizations that have an on-prem Active Directory footprint will often use Hybrid Azure AD joined devices.

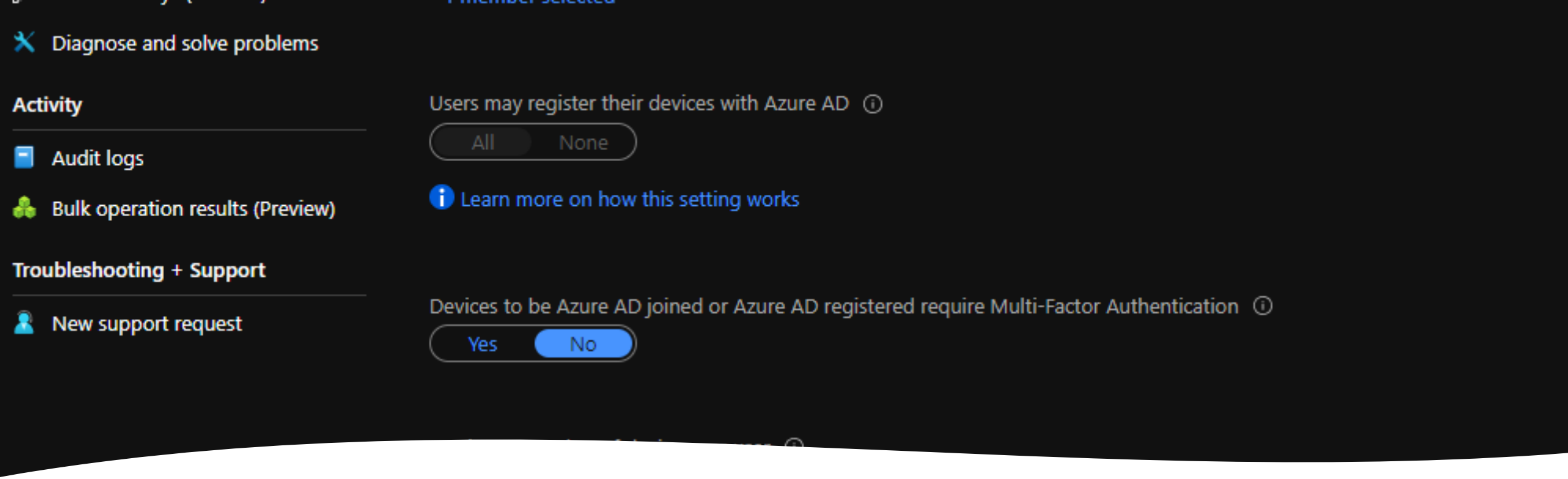
Hybrid Azure AD Joined Devices

DEFINITION	JOINED TO ON-PREMISES AD AND AZURE AD REQUIRING ORGANIZATIONAL ACCOUNT TO SIGN INTO THE DEVICE
Primary audience	• Suitable for hybrid organizations with existing on-premises AD infrastructure • Applicable to all users in an organization
Device ownership	Organization
Operating systems	• Windows 10, 8.1 and 7 • Windows Server 2008/R2, 2012/R2, 2016 and 2019
Provisioning	• Windows 10, Windows Server 2016/2019 • Domain join by IT and autojoin via Azure AD Connect or ADFS config • Domain join by Windows Autopilot and autojoin via Azure AD Connect or ADFS config • Windows 8.1, Windows 7, Windows Server 2012 R2, Windows Server 2012, and Windows Server 2008 R2 - Require MSI
Device sign in options	• Organizational accounts using: • --Password / Windows Hello for Business for Win10
Device management	• Group Policy • Configuration Manager standalone or co-management with Microsoft Intune
Key capabilities	• SSO to both cloud and on-premises resources • Conditional Access through Domain join or through Intune if co-managed • Self-service Password Reset and Windows Hello PIN reset on lock screen • Enterprise State Roaming across devices

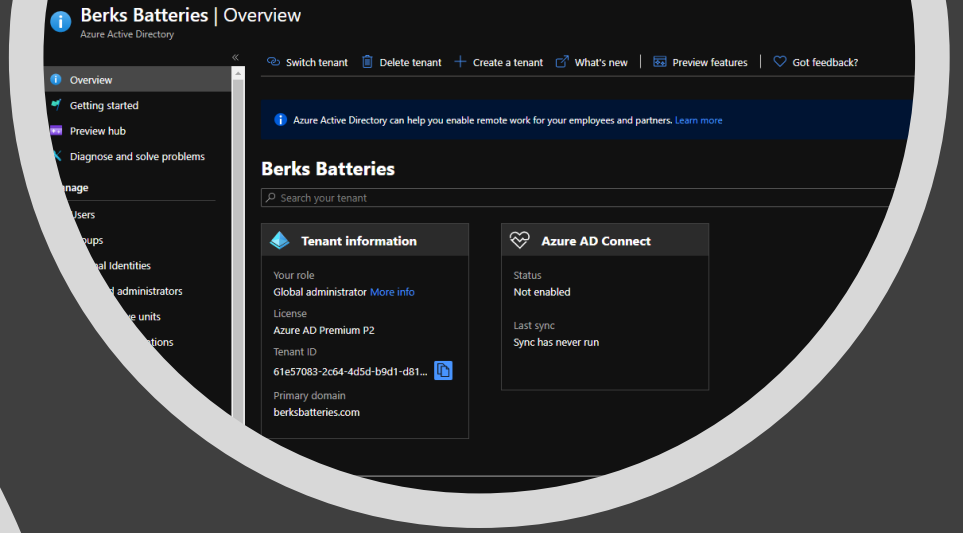
Windows 8.1

Windows 7





If you already have an on-prem AD footprint that you still need, using Hybrid Azure AD Joined devices will allow you to also benefit from the capabilities that are provided by Azure Active Directory.



Course Conclusion

Intro to Azure Active Directory

Learn what Azure AD is, and what it offers.

Learn about the differences between **Azure AD**, **traditional Active Directory**, and **Azure AD Domain Services**.

Azure AD Authentication

Learn about the different Azure AD authentication options, including **self-service password reset** and **multi-factor authentication**.

Managing Users and Groups

Learn how to **create users and groups**, and how to **manage users and groups**. We'll also cover different **roles** that are used to control access to Azure resources.

Azure AD B2B and Azure AD B2C

Learn what Azure AD B2B is and what Azure AD B2C is. Learn what each offering is used for.

Azure AD Domain Services

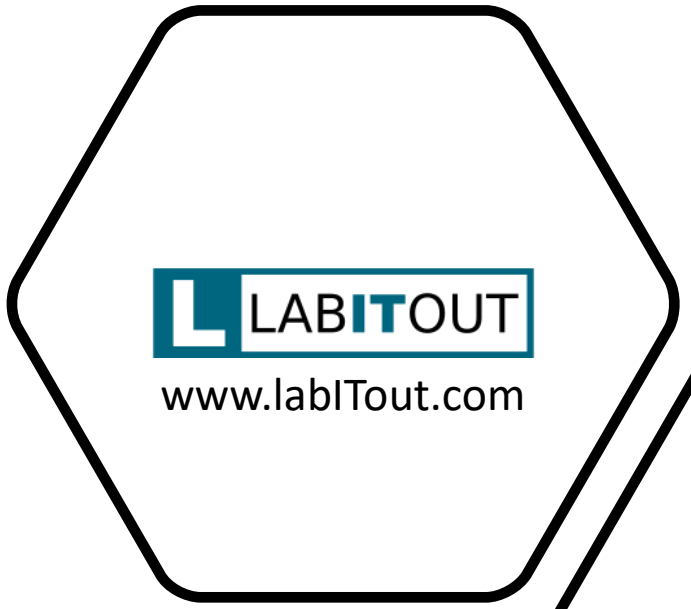
Learn what Azure AD Domain Services is and what it offers. We'll also compare the different identity solutions that are available as well.

Hybrid Identities

Learn what hybrid identities are, and what the role of **Azure AD Connect** is.

Learn about **Password Hash Sync**, **Pass-Through Authentication**, **Federation**, and **Single Sign-On**.

Don’t forget to leave a course rating!



Be sure to visit!