



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

Image Users Groups External identities Global administrators Delegated administrators Delegated units Applications

**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... [Edit](#)  
Primary domain: berksbatteries.com

**Azure AD Connect**

Status: Not enabled  
Last sync: Sync has never run

# Course Intro

Thomas  
Mitchell

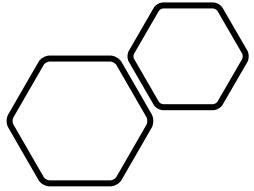


# Thomas Mitchell

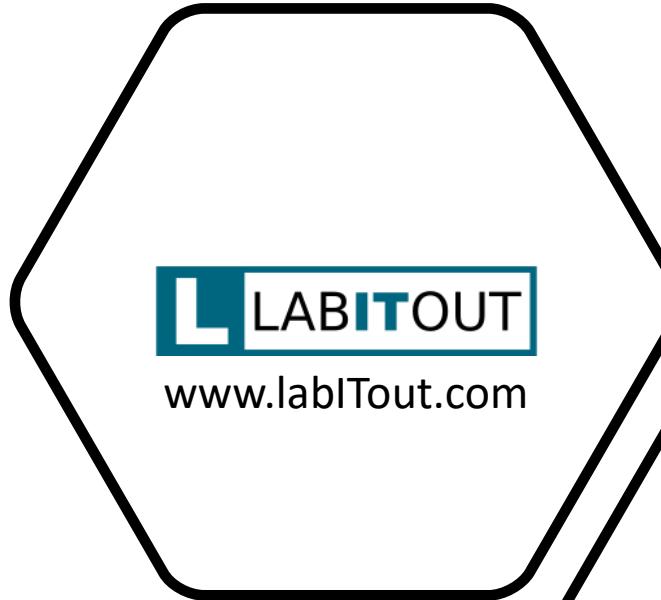
I'm a 25-year veteran  
of the IT industry.

I posses significant  
cloud experience.





I am the founder...



# Thomas Mitchell

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



# Intro to Azure Active Directory

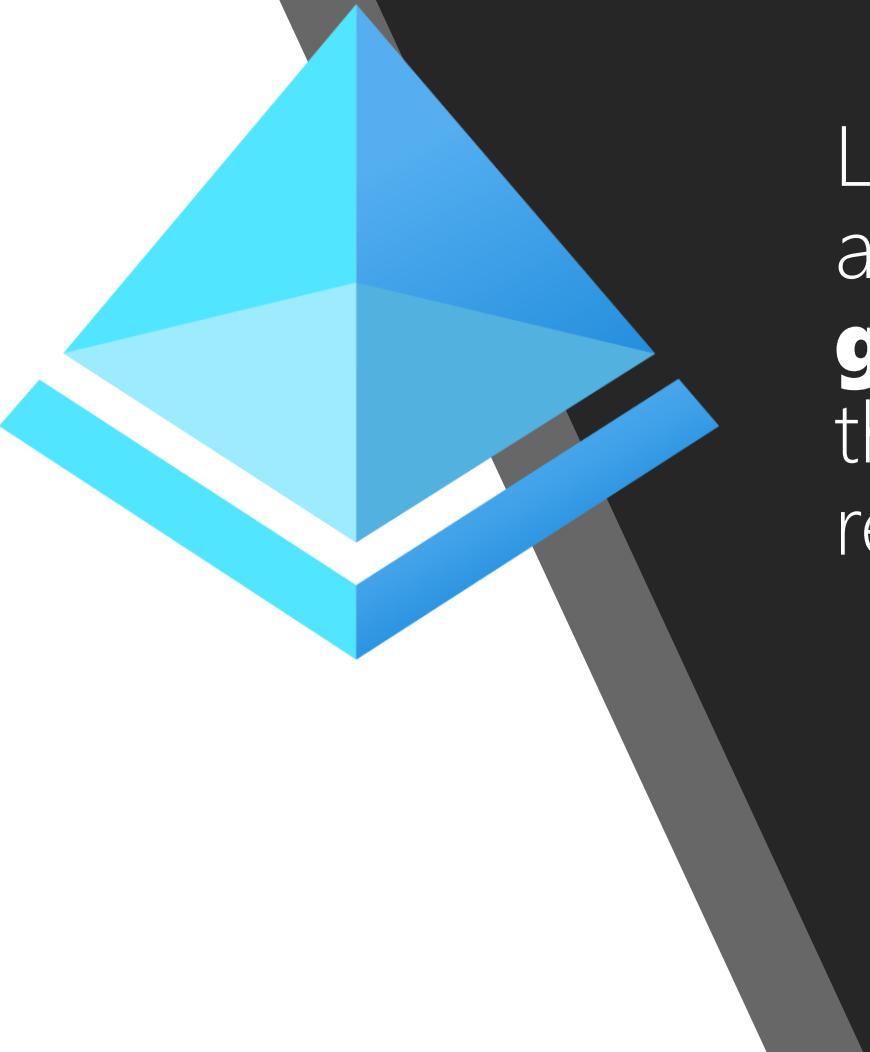
Learn what Azure AD is, and what it offers.

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!



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

Image Users Groups External identities Global administrators Delegated administrators Delegated units Applications

**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... [Edit](#)  
Primary domain: berksbatteries.com

**Azure AD Connect**

Status: Not enabled  
Last sync: Sync has never run

# 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

Berks Batteries | Overview

Switch tenant Delete tenant Create a tenant

View Getting started New hub Choose and solve problems

Berks Batteries

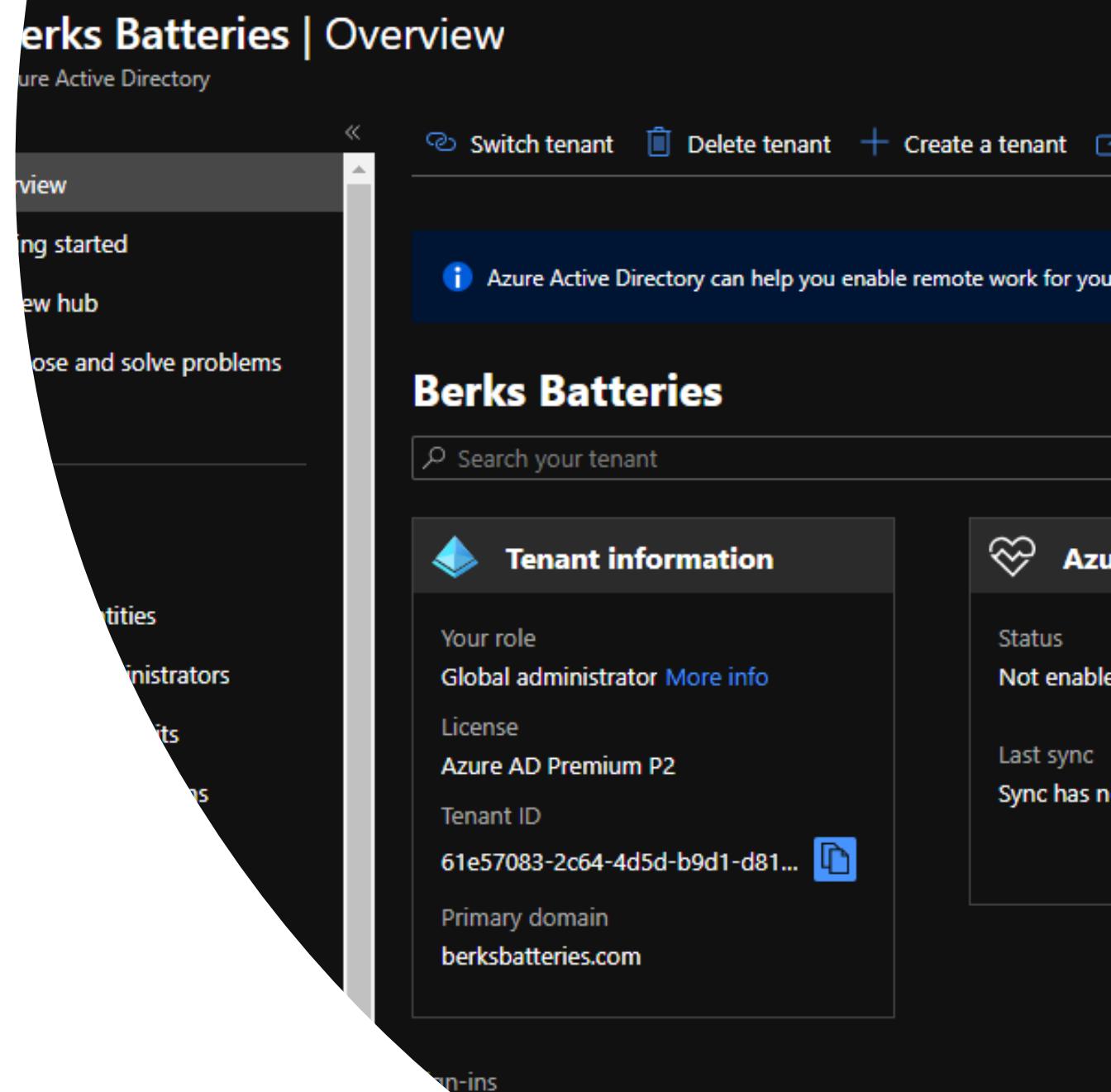
Search your tenant

Tenant information

Your role	Global administrator	More info
License	Azure AD Premium P2	
Tenant ID	61e57083-2c64-4d5d-b9d1-d81...	
Primary domain	berksbatteries.com	

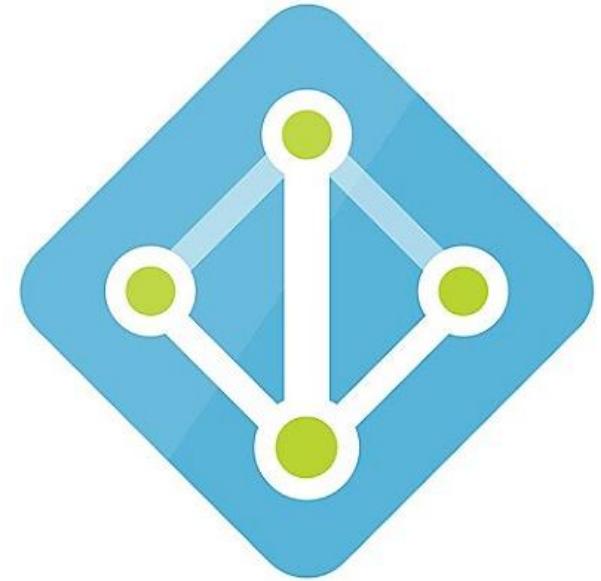
Status Not enabled

Last sync Sync has n



# 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

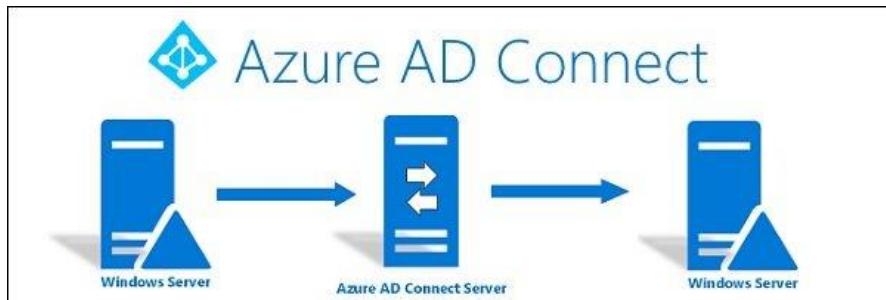
Azure Active  
Directory Premium P1

Azure Active  
Directory Premium P2

Office 365 Apps

# 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



[Getting started](#)[Preview hub](#)[Diagnose and solve problems](#)

## Manage

[Users](#)[Groups](#)[External identities](#)[Roles and administrators](#)[Administrative units](#)[Enterprise applications](#)

# Azure AD Premium P2

## Berks Batteries

 Search your tenant

### Tenant information

Your role

Global administrator [More info](#)

License

Azure AD Premium P2



### Azure AD Connect

Status

Not enabled

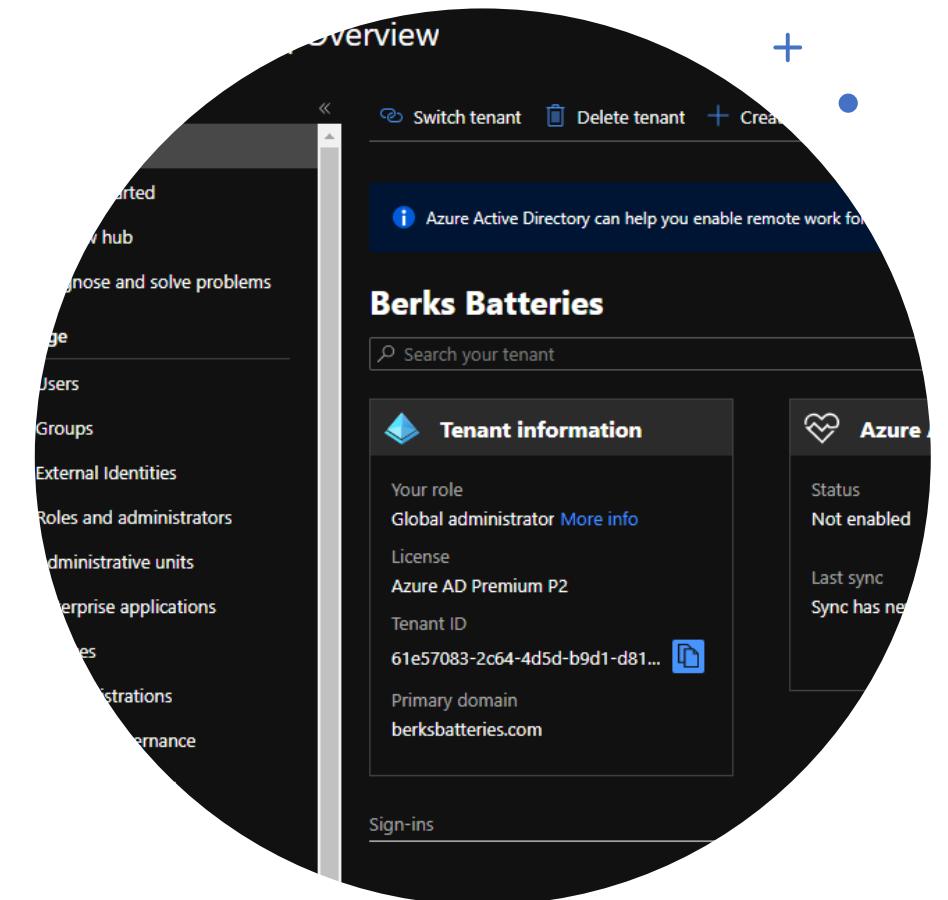
Last sync

Sync has never run

- 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



Getting started

Preview hub

Diagnose and solve problems

## Manage

Users

Groups

External Identities

Roles and administrators

Administrative units

Enterprise applications

**i** 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



### Azure AD Connect

Status

Not enabled

Last sync

Sync has never run

<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.

[Getting started](#)[Preview hub](#)[Diagnose and solve problems](#)**Manage**[Users](#)[Groups](#)[External Identities](#)[Roles and administrators](#)[Administrative units](#)[Enterprise applications](#)

**i** 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



### Azure AD Connect

Status

Not enabled

Last sync

Sync has never run

<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

The screenshot shows the Azure Active Directory Overview page. At the top, there are navigation links: 'Switch tenant', 'Delete tenant', and 'Create a tenant'. A sidebar on the left lists 'Properties', 'Administrators', 'Active units', 'Applications', 'Groups', and 'Sign-ins'. The main content area displays a message: 'Azure Active Directory can help you enable remote work for your organization'. Below this is a section titled 'Berks Batteries' with a search bar. A 'Tenant information' card provides details: 'Your role' (Global administrator), 'License' (Azure AD Premium P2), 'Tenant ID' (61e57083-2c64-4d5d-b9d1-d81...), and 'Primary domain' (berksbatteries.com). On the right, a vertical sidebar shows 'Status' (Not enabled) and 'Last sync' (Sync hasn't run yet).

# 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

[Getting started](#)[Preview hub](#)[Diagnose and solve problems](#)

## Manage

[Users](#)[Groups](#)[External Identities](#)[Roles and administrators](#)[Administrative units](#)[Enterprise applications](#)

**i** 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



### Azure AD Connect

Status

Not enabled

Last sync

Sync has never run

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



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

Image Users Groups External identities Global administrators Delegated administrators Delegated units Applications

**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... [Edit](#)  
Primary domain: berksbatteries.com

**Azure AD Connect**

Status: Not enabled  
Last sync: Sync has never run

# 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

The screenshot shows the 'Users | All users (Preview)' page in the Azure Active Directory portal. The left sidebar includes links for 'All users (Preview)', 'Deleted users (Preview)', 'Password reset', 'User settings', 'Diagnose and solve problems', 'Activity', 'Sign-ins', 'Audit logs', 'Bulk operation results', 'Troubleshooting + Support', and 'New support request'. The main content area displays a table with the following data:

Name	User principal name	User type	Directory synced	Identity issuer	Company name	Creation type
AA Admin Account	admin@berksbatteries.onmicrosoft.com	Member	No	berksbatteries.onmicrosoft.com		
AA admin@test9878.org admin	admin_test9878.org#EXT#_berksfina...	Member	No	berksbatteries.onmicrosoft.com		
MM Mike McDermott	MikeM@berksbatteries.com	Member	No	berksbatteries.onmicrosoft.com		
LM Lester Murphy	LesterM@berksbatteries.com	Member	No	berksbatteries.onmicrosoft.com		

 All users (Preview) Deleted users (Preview) Password reset User settings Diagnose and solve problems Activity Sign-ins Audit logs Bulk operation results Troubleshooting + Support New support request

# Defining Users in Azure AD

 New user  New guest user  Bulk operations  Refresh  Reset password  Multi-Factor Authentication  Delete user  Columns  Preview info  Preview features  Got feedback? This page includes previews available for your evaluation. View previews → Search users Add filters

4 users found

Name	User principal name	User type	Directory synced	Identity issuer	Company name	Creation type
 AA Admin Account	admin@berksbatteries.onmicrosoft.com	Member	No	berksbatteries.onmicrosoft.com		
 AA admin@test9878.org admin	admin_test9878.org#EXT#_berksfin...	Member	No	berksbatteries.onmicrosoft.com		
 MM Mike McDermott	MikeM@berksbatteries.com	Member	No	berksbatteries.onmicrosoft.com		
 LM Lester Murphy	LesterM@berksbatteries.com	Member	No	berksbatteries.onmicrosoft.com		

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

- Cloud Identities
- Directory Synchronized Identities
- Guest Users

## All users (Preview)

s - Azure Active Directory

ew)

Preview)

This screenshot shows the 'All users (Preview)' page in the Azure Active Directory portal. The page displays a list of four users found. Each user entry includes a checkbox, a profile icon, the user name, the user principal name, the user type (all listed as Member), the directory sync status (all listed as No), the identity issuer (all listed as berksbatteries.onmicrosoft.com), and the company name (all listed as berksbatteries). There are also buttons for 'New user', 'New guest user', 'Bulk operations', 'Refresh', 'Reset password', 'Multi-Factor Authentication', 'Delete user', 'Columns', 'Preview info', 'Preview features', and 'Got feedback?'.

Name	User principal name	User type	Directory synced	Identity issuer	Company name	Create
<input type="checkbox"/> AA Admin Account	admin@berksbatteries.onmicrosoft...	Member	No	berksbatteries.onmicrosoft.com	berksbatteries	
<input type="checkbox"/> AA admin@test9878.org admin	admin_test9878.org#EXT#_berksfina...	Member	No	berksbatteries.onmicrosoft.com	berksbatteries	
<input type="checkbox"/> MM Mike McDermott	MikeM@berksbatteries.com	Member	No	berksbatteries.onmicrosoft.com	berksbatteries	
<input type="checkbox"/> LM Lester Murphy	LesterM@berksbatteries.com	Member	No	berksbatteries.onmicrosoft.com	berksbatteries	

# 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

# Mike McDermott

MikeM@berksbatteries.com

User Sign-ins

# 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.

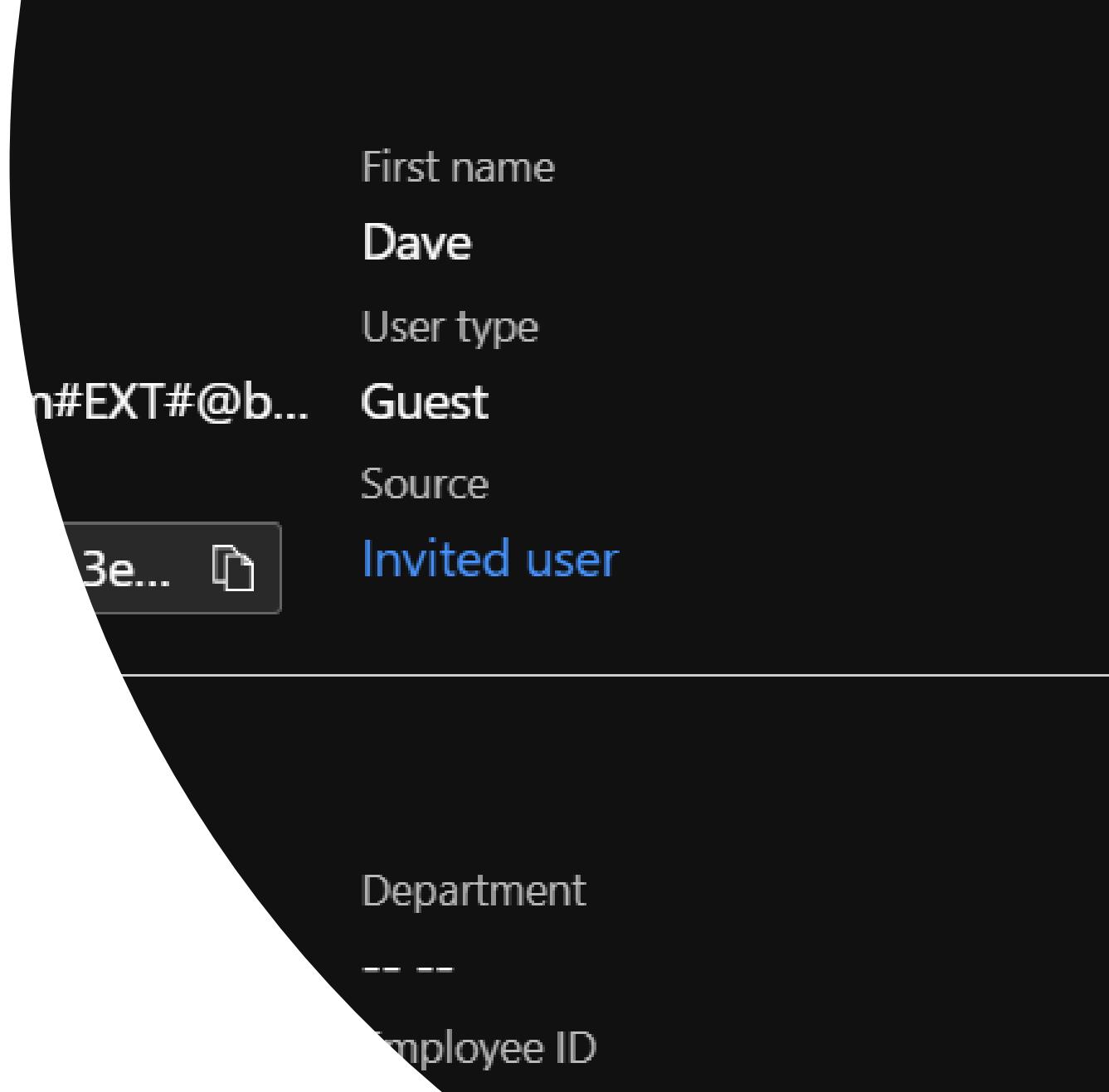
User type	Directory synced
soft... Member	No
fina... Member	No
Member	No
Member	No

# Guest Users

---

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

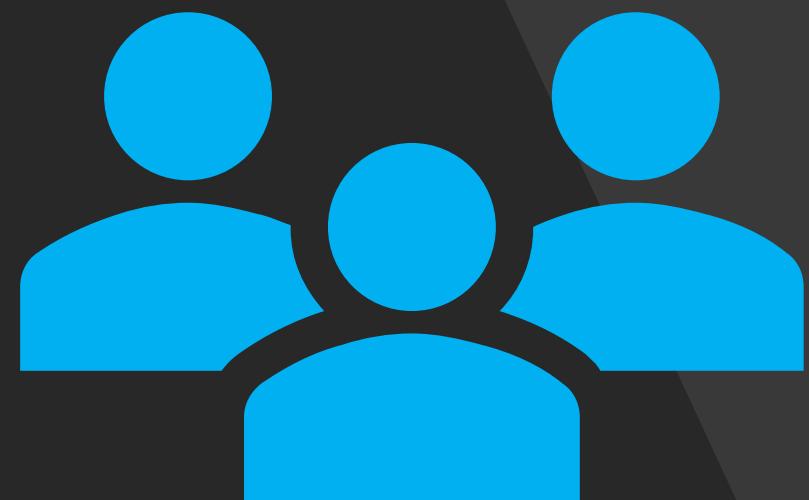
- Guest users are accounts in Azure AD from other cloud providers.
- Users with Microsoft accounts.
- Will show up in the Azure AD users list as **invited users**.



# 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





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

Image Users Groups Global identities Local administrators Delegated units Applications

**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... [Edit](#)  
Primary domain: berksbatteries.com

**Azure AD Connect**

Status: Not enabled  
Last sync: Sync has never run

# Creating and Managing Groups

This page includes previews available for your evaluation. View previews →

Search groups [+ Add filters](#)

Name	Object Id	Group Type	Membership Type	Email	Source
<input type="checkbox"/> AL AllUsers	ba06138d-fa6f-41b3-9e8f-e83d4251ec53	Microsoft 365	Assigned	AllUsers@berksbatteries.onmicrosoft.com	Cloud
<input type="checkbox"/> HU HumanResources	267b8006-aae5-4510-af48-291eb57f2a62	Security	Assigned		Cloud
<input type="checkbox"/> FI Finance	4f4749ef-a679-4f4c-b969-84206108c66e	Security	Assigned		Cloud
<input type="checkbox"/> MA Marketing	ed70ad3e-3eb4-4aab-9181-c66ba2669a15	Security	Assigned		Cloud

# 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

**Finance**

View

Choose and solve problems

Properties

Members

Administrative units

Role assignments

Logs

Operation results

Shooting + Support

Delete | Preview features | Got feedback?

This page includes previews available for your evaluation. View previews →

**Finance**

Finance employees

Membership type	Assigned
Source	Cloud
Type	Security
Object Id	4f4749ef-a679-4f4c-b969-84206108c66e
Creation date	2/5/2021, 8:43:19 AM

**Direct members**

0 User(s) 0 Group(s) 0 Device(s)

**Group memberships**



Berks Batteries | Overview  
Azure Active Directory

Switch tenant Delete tenant + Create a tenant What's new Preview features Got feedback?

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... [Edit](#)  
Primary domain: berksbatteries.com

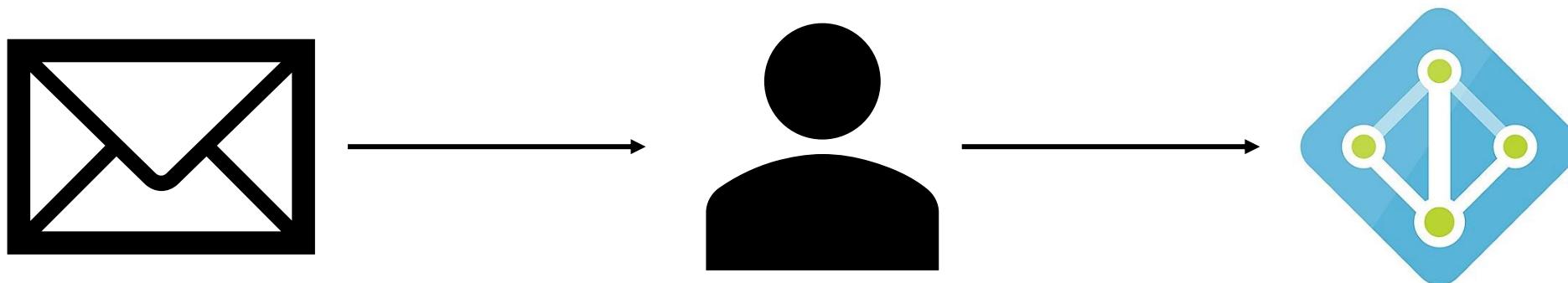
**Azure AD Connect**

Status: Not enabled  
Last sync: Sync has never run

# Azure Active Directory B2B

# What is Azure Active Directory B2B?

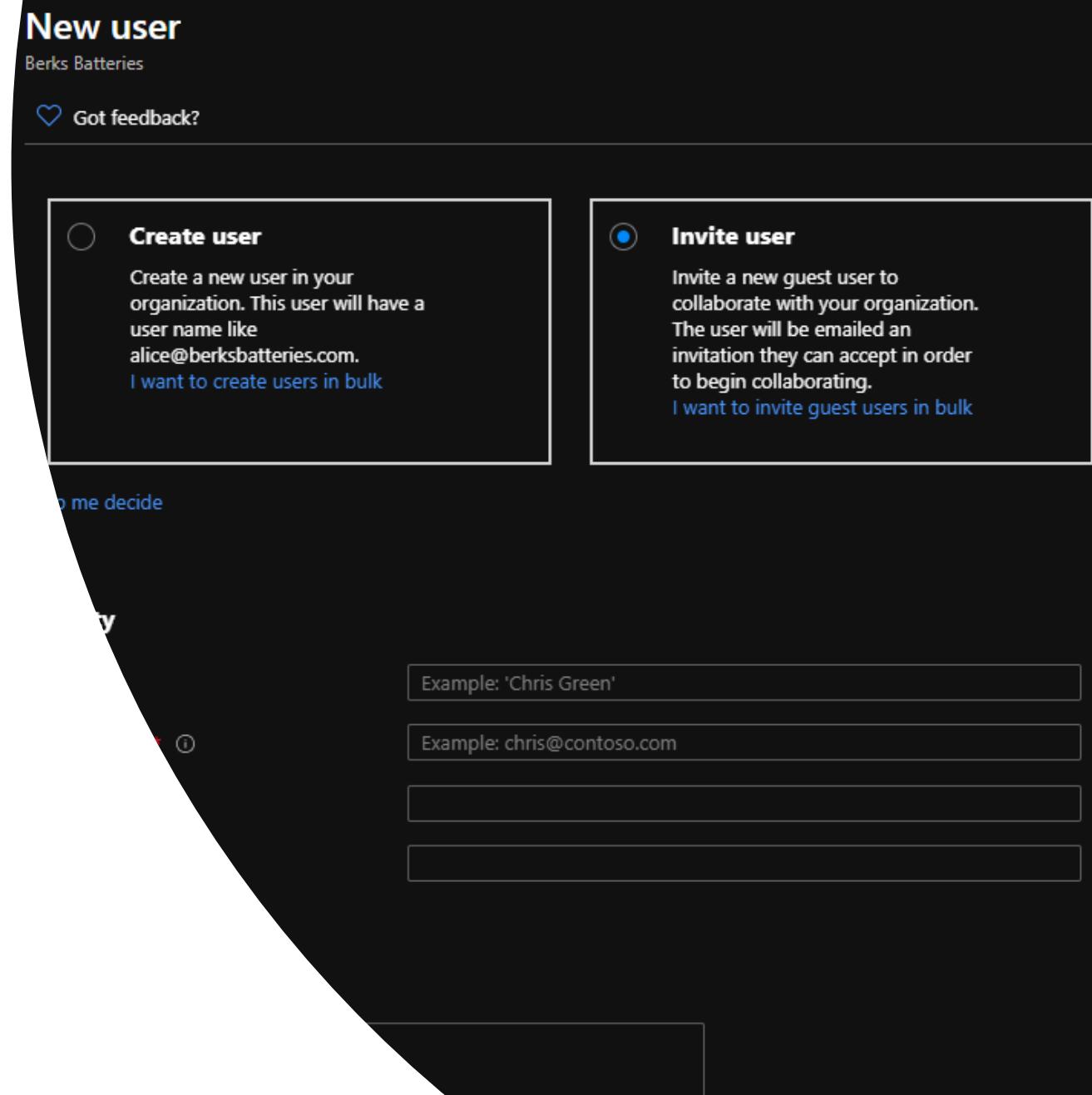
- Used to share applications and services with guest users
- External org doesn't need to have Azure Active Directory
- B2B uses an invitation and redemption process
- No need to manage external accounts or external passwords



# Azure AD B2B

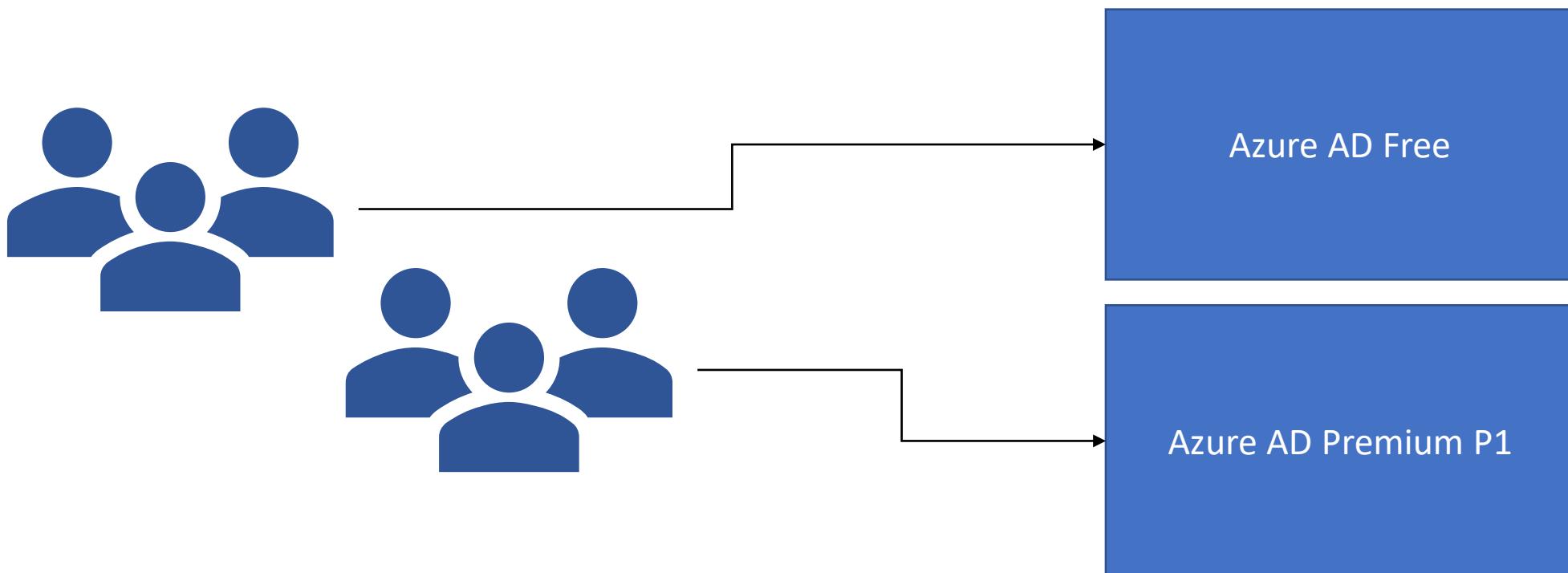
---

- 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 own





Berks Batteries | Overview  
Azure Active Directory

Switch tenant Delete tenant + Create a tenant What's new Preview features Got feedback?

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... [Edit](#)  
Primary domain: berksbatteries.com

**Azure AD Connect**

Status: Not enabled  
Last sync: Sync has never run

# Azure Active Directory B2C

# Customers

Social IDs, email, or local accounts



Business & Government IDs



# Azure Active Directory B2C

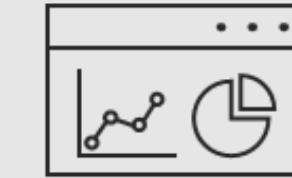
A business to consumer identity service.

- 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

# Business



Apps and APIs



Analytics



Integration

# Azure AD B2C Authentication

Social IDs, email, or local accounts



Business & Government IDs



## Customers



- 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

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



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

Image Users Groups External identities Global administrators Delegated administrators Delegated units Applications

**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... [Copy]  
Primary domain: berksbatteries.com

**Azure AD Connect**

Status: Not enabled  
Last sync: Sync has never run

# Azure AD Domain Services

All services

FAVORITES

Resource groups

All resources

Recent

App Services

SQL databases

Virtual machines (classic)

Virtual machines

Configure basic settings

2 Network  
Select virtual network ✓

3 Administrator group  
Configure group membership ✓

4 Synchronization  
Choose synchronization scope >

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](#)

# 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

## Enable Azure AD Domain Ser... X

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?

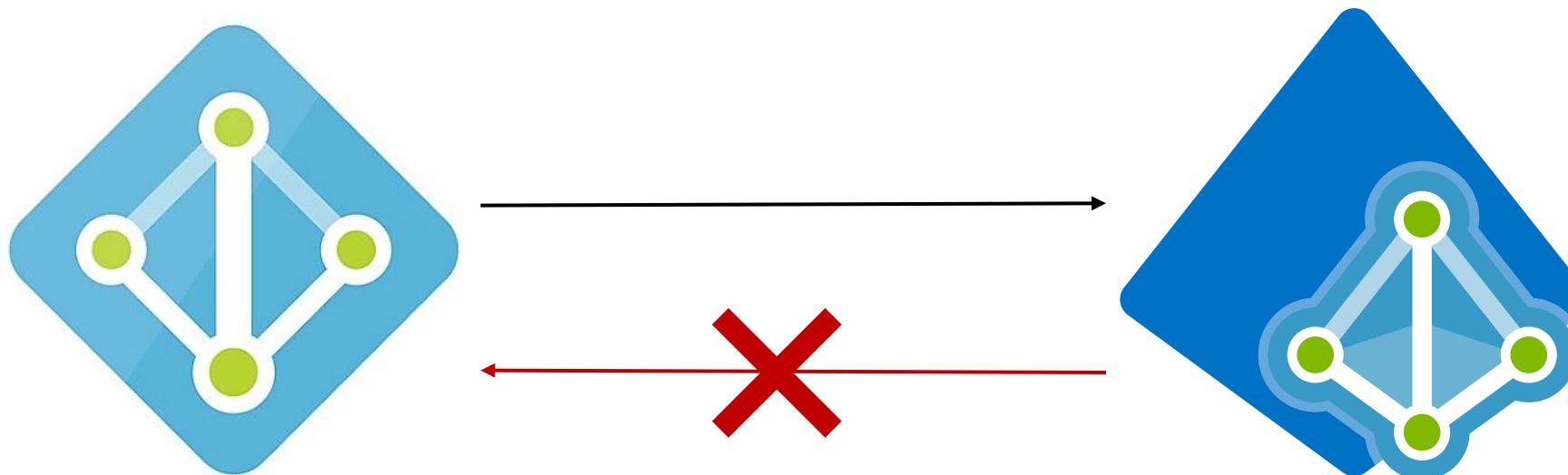


When Azure ADDS is deployed, a managed domain is created on the virtual network that you specify.

- 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

The screenshot shows the 'Enable Azure AD Domain Services' wizard. The current step is '4 Synchronization > Choose synchronization scope'. To the right, there is a 'Synchronization' panel with the following content:

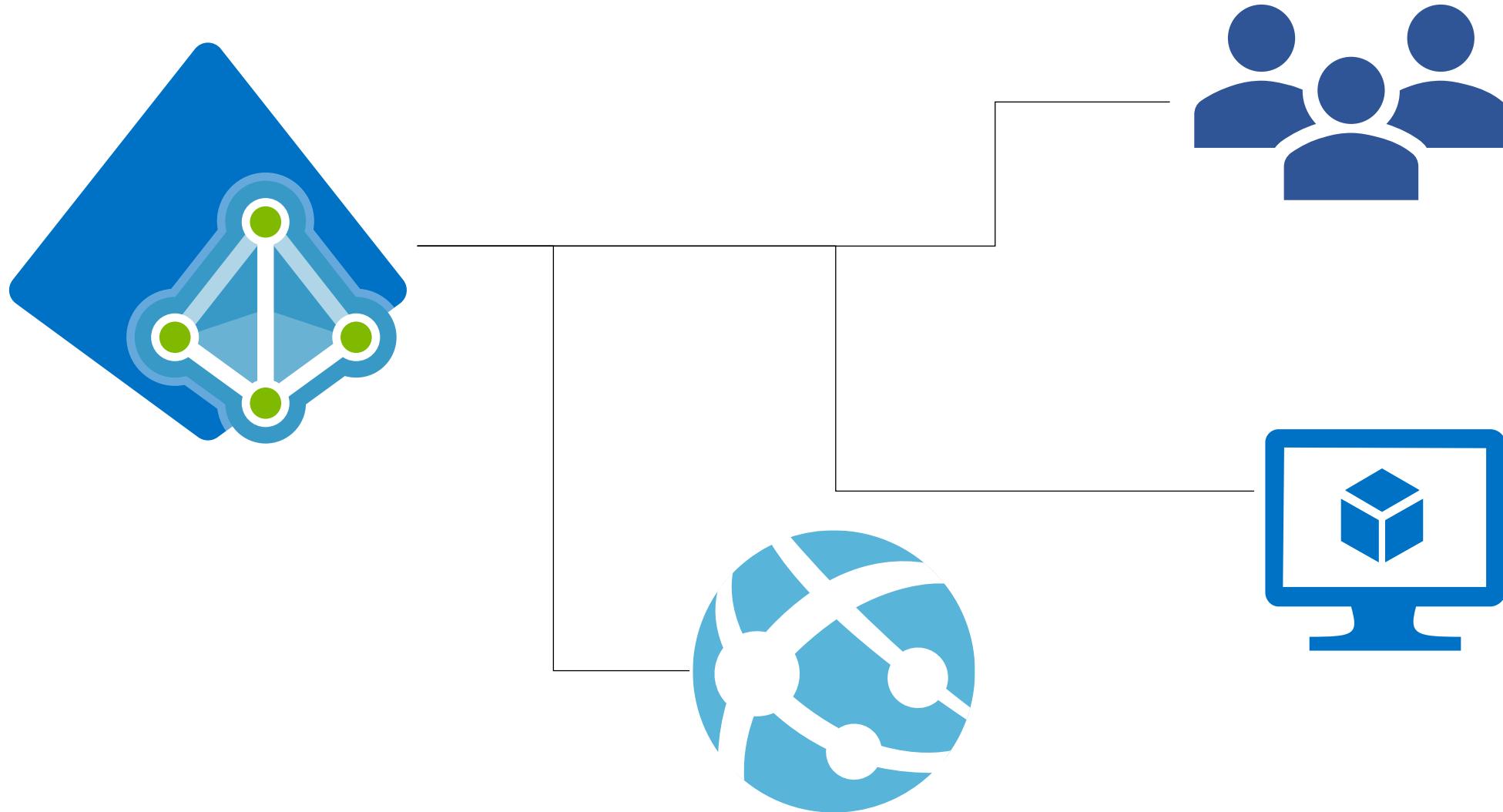
**Synchronization**

Synchronize all users and groups in your on-premises AD or synchronize scoped groups and their members. If you have a very large number of users and groups, you might want to start with "scoped" synchronization. This will improve the time to complete synchronization.

**All**   **Scoped**

**! Warning** Scoped synchronization was modified with different settings or converted from "all" to "scoped". To change synchronization scope from "all" to "scoped", domain controller instance needs to be re-created. [More information](#)

# How does Azure ADDS Work?



HOME > ADD A NEW SERVICE > AZURE AD DOMAIN SERVICES > ENABLE AZURE AD DOMAIN SERVICES

**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 Services**

**Synchronization**

Default Directory

1 Basics Configure basic settings ✓

2 Network Select virtual network ✓

3 Administrator group Configure group membership ✓

4 Synchronization Choose synchronization scope >

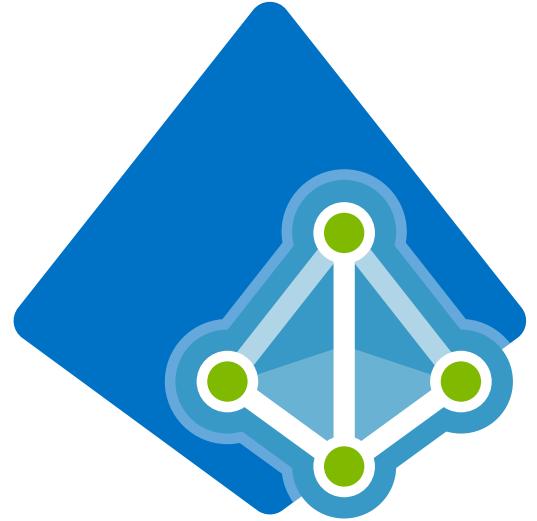
5 Summary Enable Azure AD Domain Services >

**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**

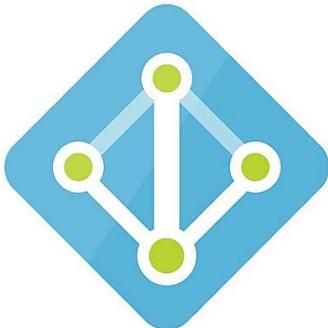
**!** Scoped synchronization can be modified with different group selections or converted to synchronize all users and groups. To change synchronization from "all" to "scoped", domain service instance needs to be deleted and re-created. [More information](#)



# 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.



 Dashboard

 All services

 FAVORITES

 Resource groups

 All resources

 Recent

 App Services

 SQL databases

 Virtual machines (classic)

 Virtual machines

**1** Basics 

Configure basic settings

**2** Network 

Select virtual network

**3** Administrator group 

Configure group membership

**4** Synchronization 

Choose synchronization scope

Summary 

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](#)

# 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

All services

Filter by name... Subscription == all Resource group == all Location == all Add filter

Favorites

No grouping

All resources

Name ↑ Type ↑ Resource group ↑ Location ↑ Subscriptions ↑

Showing 0 to 0 of 0 records.

Resource groups

Quickstart Center

App Services

Function App

SQL databases

Azure Cosmos DB

Virtual machines

Load balancers

Storage accounts

Virtual networks

Azure Active Directory

Monitor

Advisor

Security Center

Cost Management + Billing



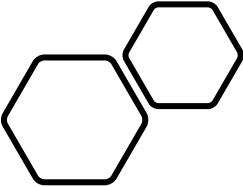
No Azure AD Domain Services to display  
Try changing your filters if you don't see what you're looking for.  
[Learn more ↗](#)

Create Azure AD Domain Services

# 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





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

Image Users Groups External identities Global administrators Delegated administrators Delegated units Applications

**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... [Copy]  
Primary domain: berksbatteries.com

**Azure AD Connect**

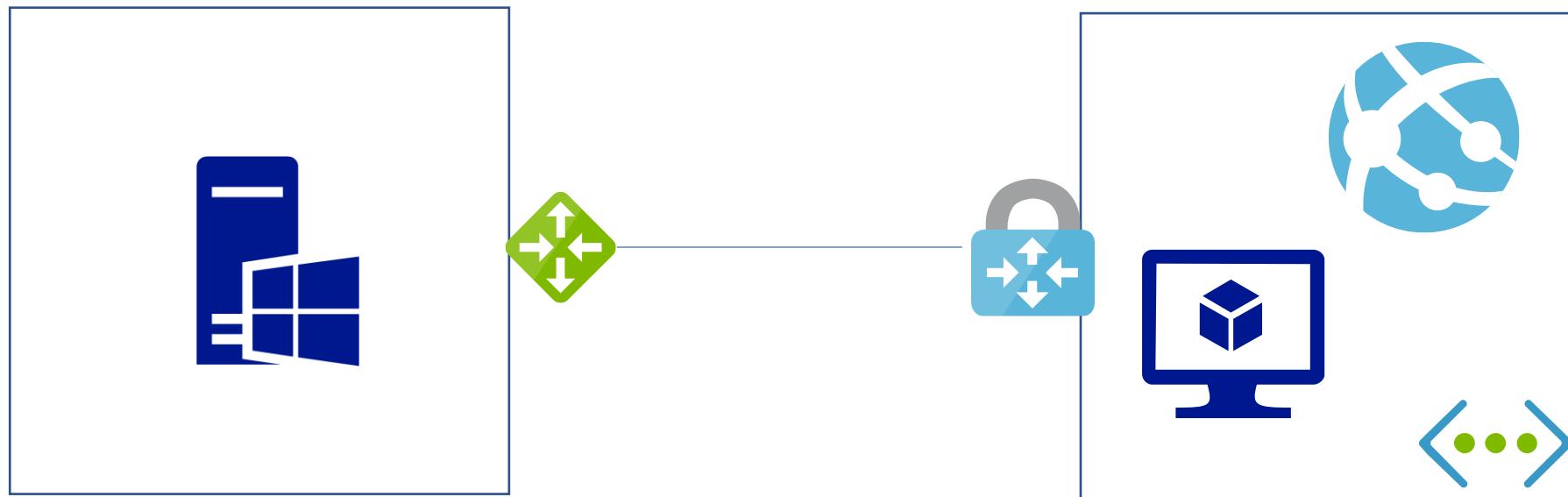
Status: Not enabled  
Last sync: Sync has never run

# 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.

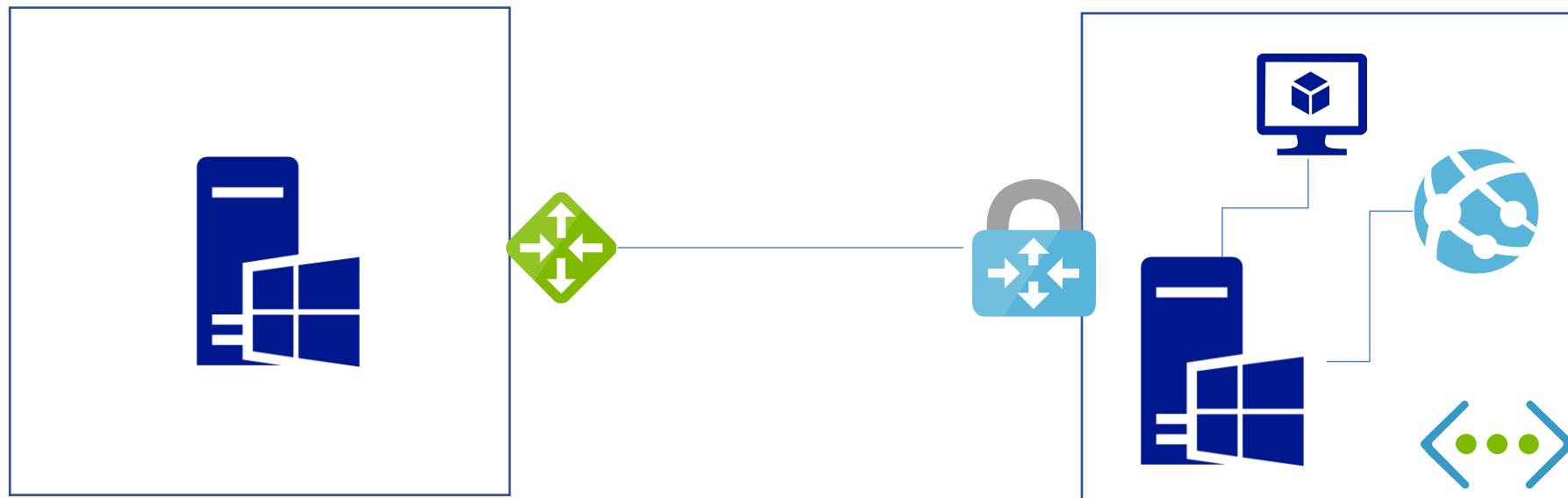
## Site-to-Site VPN Between On-Prem Network and Azure



# Comparing Identity Solutions

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

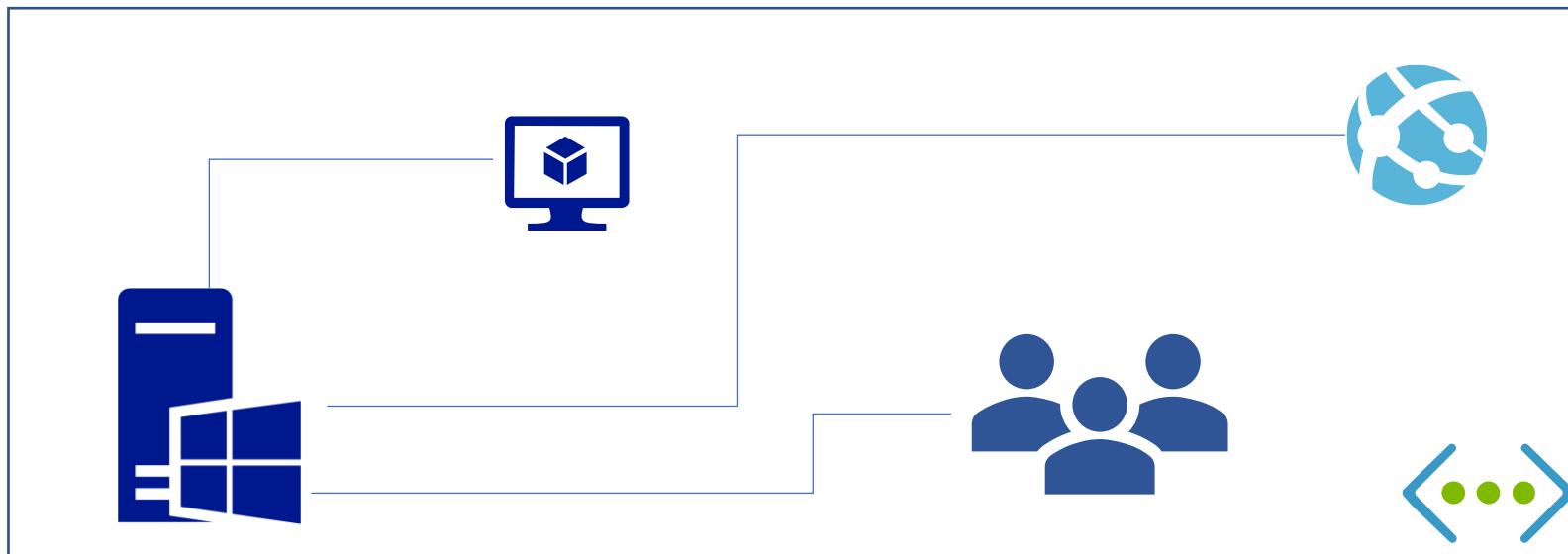
## Create Replica Domain Controllers in Azure



# 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





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

Image Users Groups Global identities Local administrators Delegated units Applications

**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... [Edit](#)  
Primary domain: berksbatteries.com

**Azure AD Connect**

Status: Not enabled  
Last sync: Sync has never run

# 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 screenshot shows the Azure Active Directory tenant overview page for the tenant "Berks Batteries". The top navigation bar includes links for "Switch tenant", "Delete tenant", "Create a tenant", "What's new", and "Preview features". A banner at the top states: "Azure Active Directory can help you enable remote work for your employees and partners. Learn more". The main content area displays "Tenant information" and "Azure AD Connect" status. The "Tenant information" section shows the tenant name "Berks Batteries", role "Global administrator", and license "Premium P2". The "Azure AD Connect" section shows "Status: Not enabled" and "Last sync: Sync has never run".



# 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



Berks Batteries | Overview  
Azure Active Directory

Switch tenant Delete tenant + Create a tenant What's new Preview features Got feedback?

Azure Active Directory can help you enable remote work for your employees and partners. [Learn more](#)

## Berks Batteries

Search your tenant

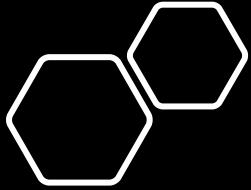
**Tenant information**

Your role: Global administrator [More info](#)  
License: Azure AD Premium P2  
Tenant ID: 61e57083-2c64-4d5d-b9d1-d81... [Edit](#)  
Primary domain: berksbatteries.com

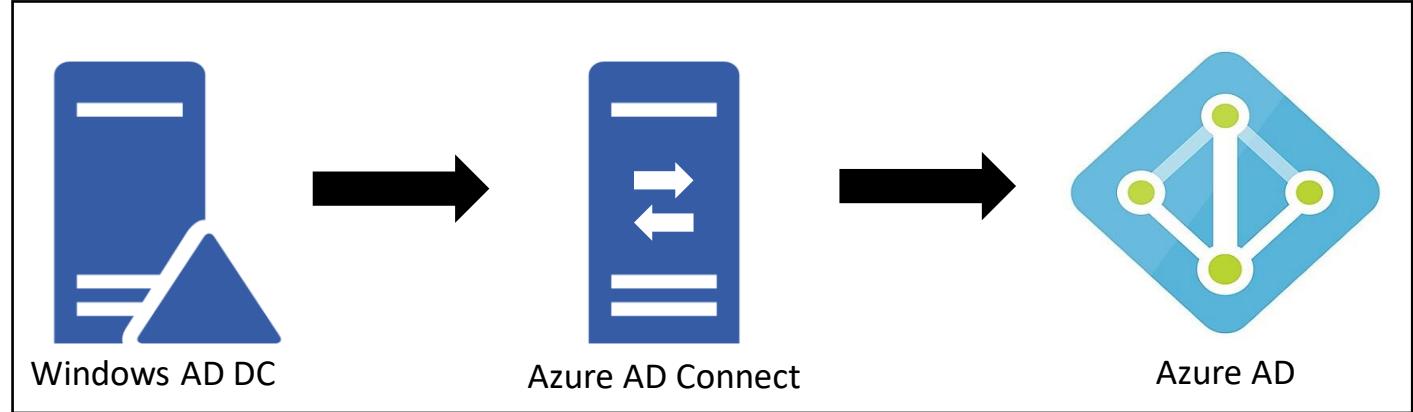
**Azure AD Connect**

Status: Not enabled  
Last sync: Sync has never run

# 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



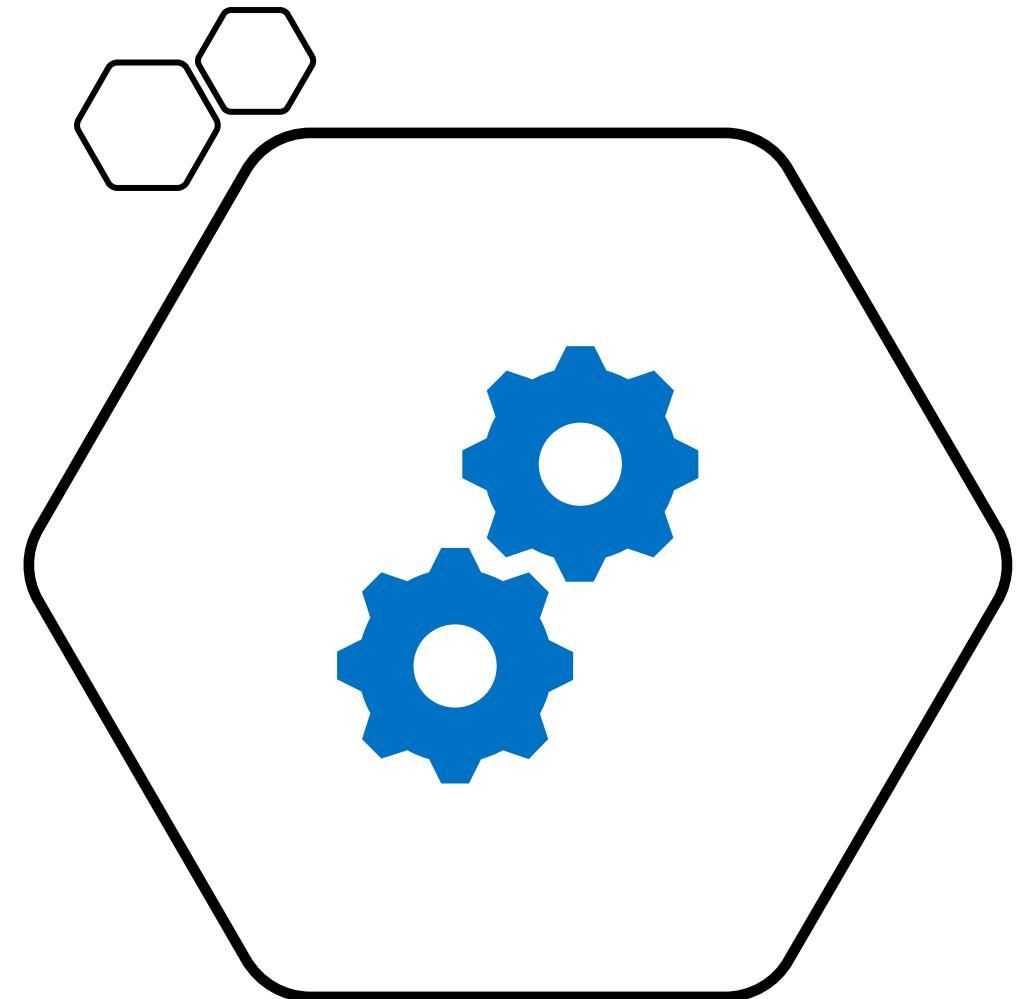
# Azure AD Connect

## Federation Integration:

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

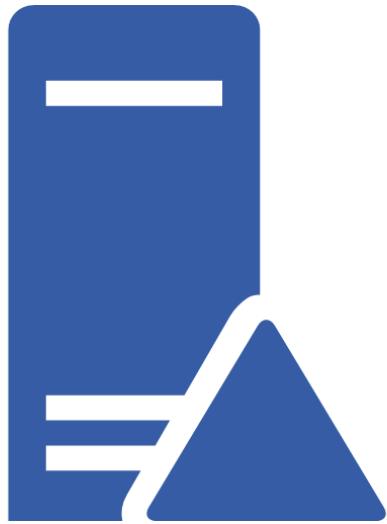
## Health Monitoring:

- 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

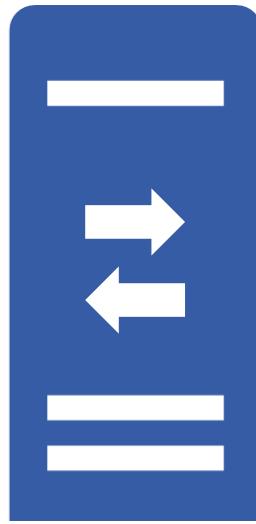


# Azure AD Connect

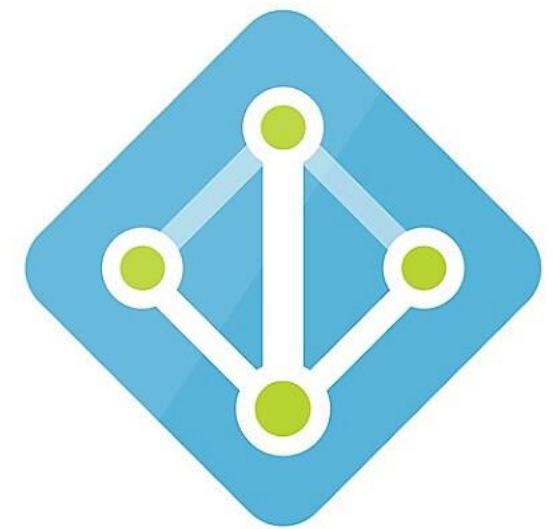
- Organizations typically deploy Azure AD connect so that their users can use the same identity to access not only the on-prem applications but also cloud services like Office 365.
- Azure AD connect is free and included in all Azure subscriptions



Windows AD DC



Azure AD Connect



Azure Active Directory

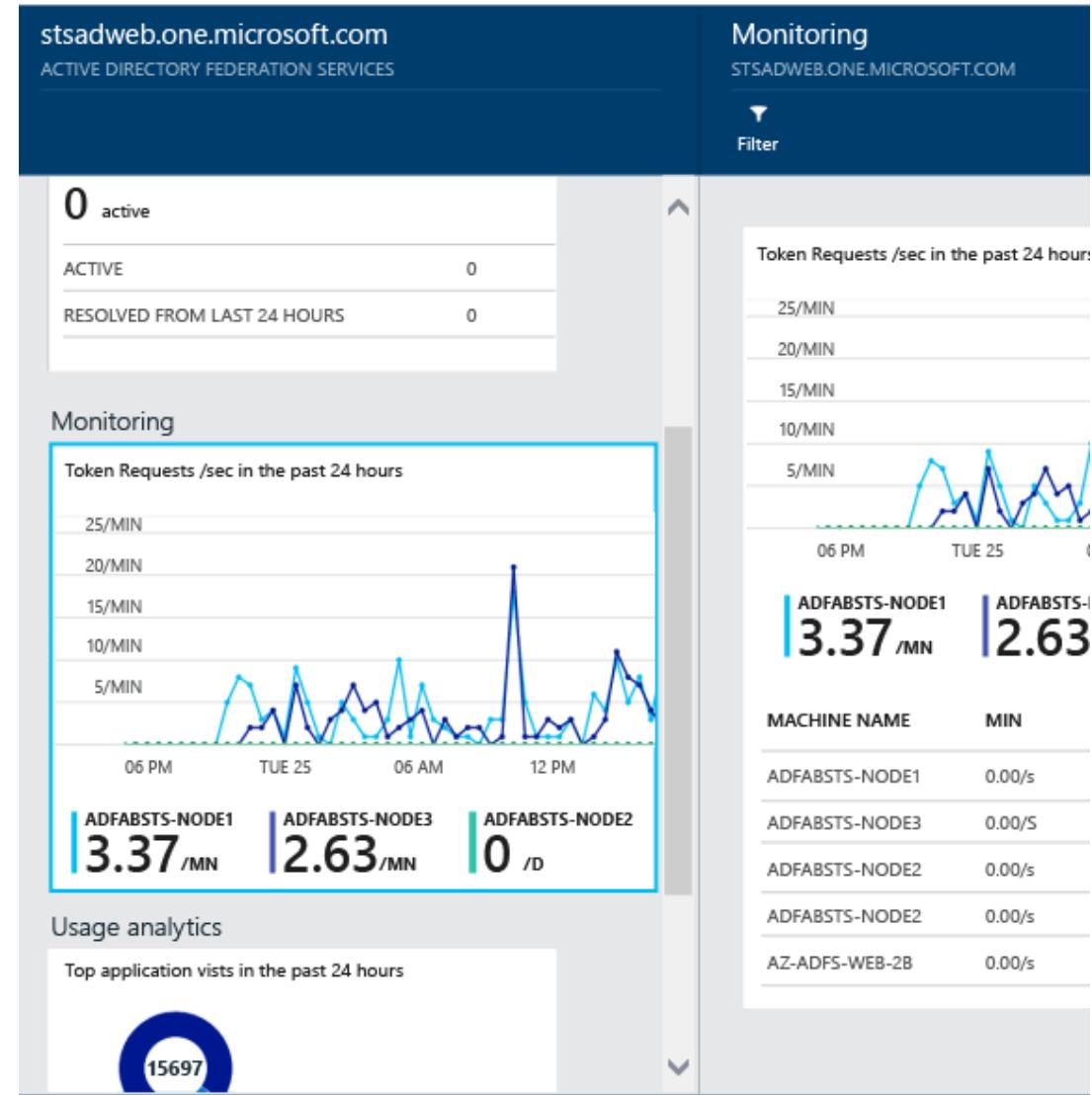
# Azure AD Connect Health

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.





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

User Groups External identities Conditional access units Applications

**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... [Edit](#)

Primary domain berksbatteries.com

**Azure AD Connect**

Status Not enabled

Last sync Sync has never run

# PHS vs PTA Authentication

**Manage** Users Groups External Identities Roles and administrators Administrative units

# Password Hash Synchronization

 Manage your on-premises resources, authentication configurations, and on-premises infrastructure using Azure AD hybrid services. [Learn more](#)

## PROVISION FROM ACTIVE DIRECTORY



### Azure AD cloud sync

This feature allows you to manage sync configurations from the cloud, in addition to syncing Active Directory users and groups from disconnected forests.

[Manage Azure AD cloud sync](#)

### Azure AD Connect sync

Not Installed

[Download Azure AD Connect](#)

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:

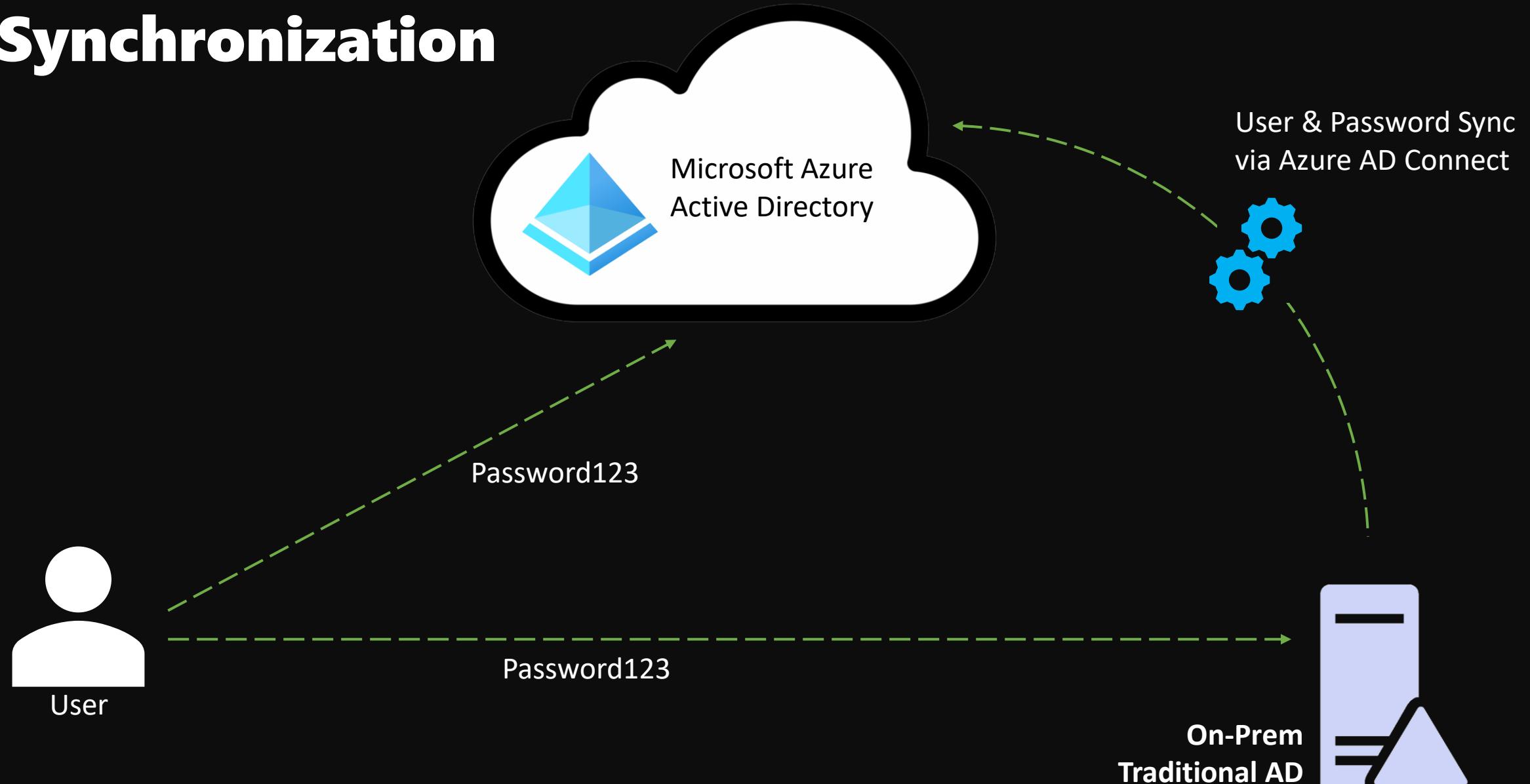
- Deploy Azure AD connect
- Set up synchronization
- Select the password hash synchronization sign in method

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

The screenshot shows the Azure AD Connect blade in the Azure portal. At the top, there's a navigation bar with 'Azure AD Connect' and other options like 'Problems' and 'Logs'. Below the navigation is a banner with an info icon and text: 'Manage your on-premises resources, authentication configurations, and on-premises AD hybrid services. [Learn more](#)'. The main area is titled 'PROVISION FROM ACTIVE DIRECTORY' and contains two sections: 'Azure AD cloud sync' and 'Azure AD Connect sync'. Under 'Azure AD cloud sync', there's a blue cloud icon with a sync arrow, followed by the text 'This feature allows you to manage sync configurations from the cloud' and a link 'Manage Azure AD cloud sync'. Under 'Azure AD Connect sync', there are two rows of information: 'Not Installed' and 'Last Sync' (Sync has never run), and 'Password Hash Sync' (Disabled). At the bottom, there's a section titled 'USER SIGN-IN' with three rows: 'Federation' (Disabled, 0 domains), 'Seamless single sign-on' (Disabled, 0 domains), and 'Single sign-on through authentication' (Disabled, 0 agents).

Setting	Status	Details
Azure AD cloud sync	Manage sync configurations from the cloud	<a href="#">Manage Azure AD cloud sync</a>
Azure AD Connect sync	Not Installed	<a href="#">Download Azure AD Connect</a>
Azure AD Connect sync	Last Sync	Sync has never run
Azure AD Connect sync	Password Hash Sync	Disabled
USER SIGN-IN		
Federation	Disabled	0 domains
Seamless single sign-on	Disabled	0 domains
Single sign-on through authentication	Disabled	0 agents

# 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

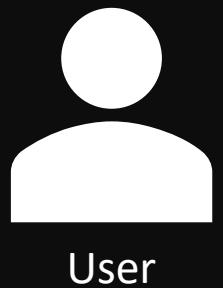
The screenshot shows the Azure AD Connect interface. At the top, there's a navigation bar with 'Azure AD Connect' and icons for 'Troubleshoot', 'Refresh', and 'Got feedback?'. Below the navigation bar, a banner says 'Manage your on-premises resources, authentication configurations, and other AD hybrid services. Learn more'. The main content area is divided into two sections: 'PROVISION FROM ACTIVE DIRECTORY' and 'USER SIGN-IN'.

**PROVISION FROM ACTIVE DIRECTORY**

Azure AD cloud sync	
This feature allows you to manage sync configurations from the cloud. Sync users and groups from disconnected forests.	<a href="#">Manage Azure AD cloud sync</a>
Azure AD Connect sync	
Not Installed	<a href="#">Download Azure AD Connect</a>
Last Sync	Sync has never run
Password Hash Sync	Disabled

**USER SIGN-IN**

Federation	Disabled	0 domains
Seamless single sign-on	Disabled	0 domains
Pass-through authentication	Disabled	0 agents



User



Microsoft Azure  
Active Directory

Identity Synchronization  
via Azure AD Connect



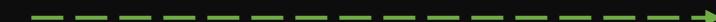
*Password validation requests are sent to, and processed by, the on-prem Domain Controller via*

### **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.



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

Image Users Groups External identities Global administrators Delegated administrators Delegated units Applications

**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... [Copy]  
Primary domain: berksbatteries.com

**Azure AD Connect**

Status: Not enabled  
Last sync: Sync has never run

# Federation with Azure AD

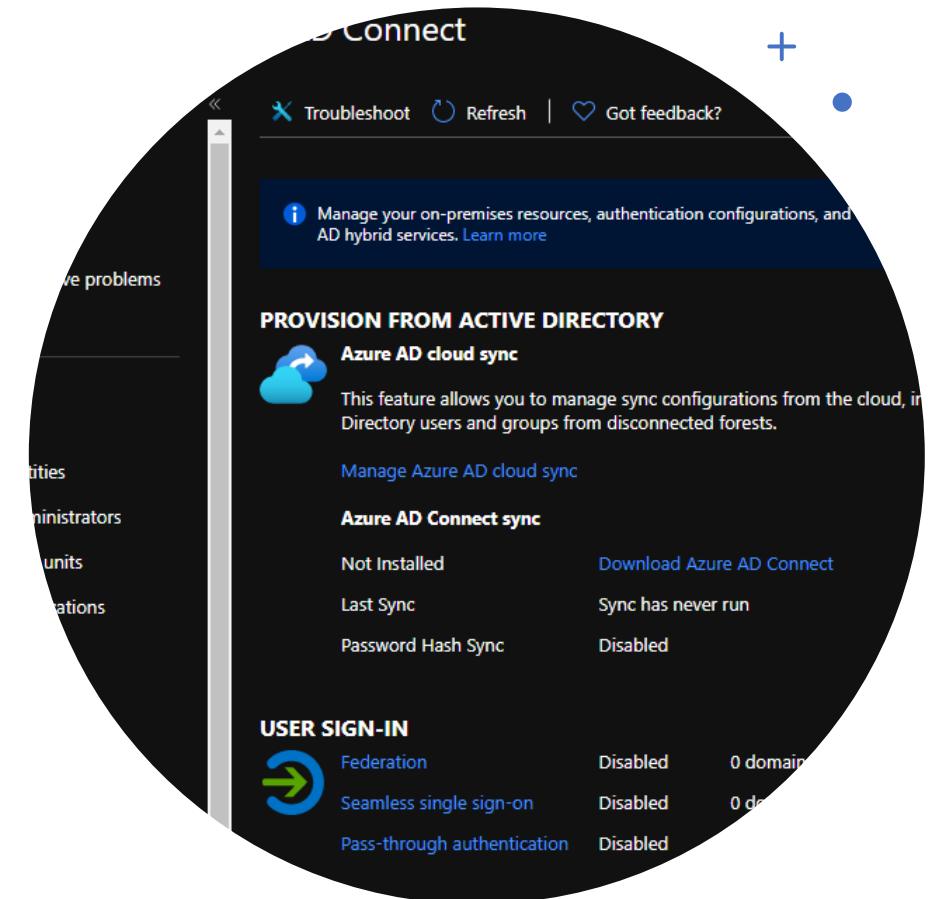
# Federation with Azure AD

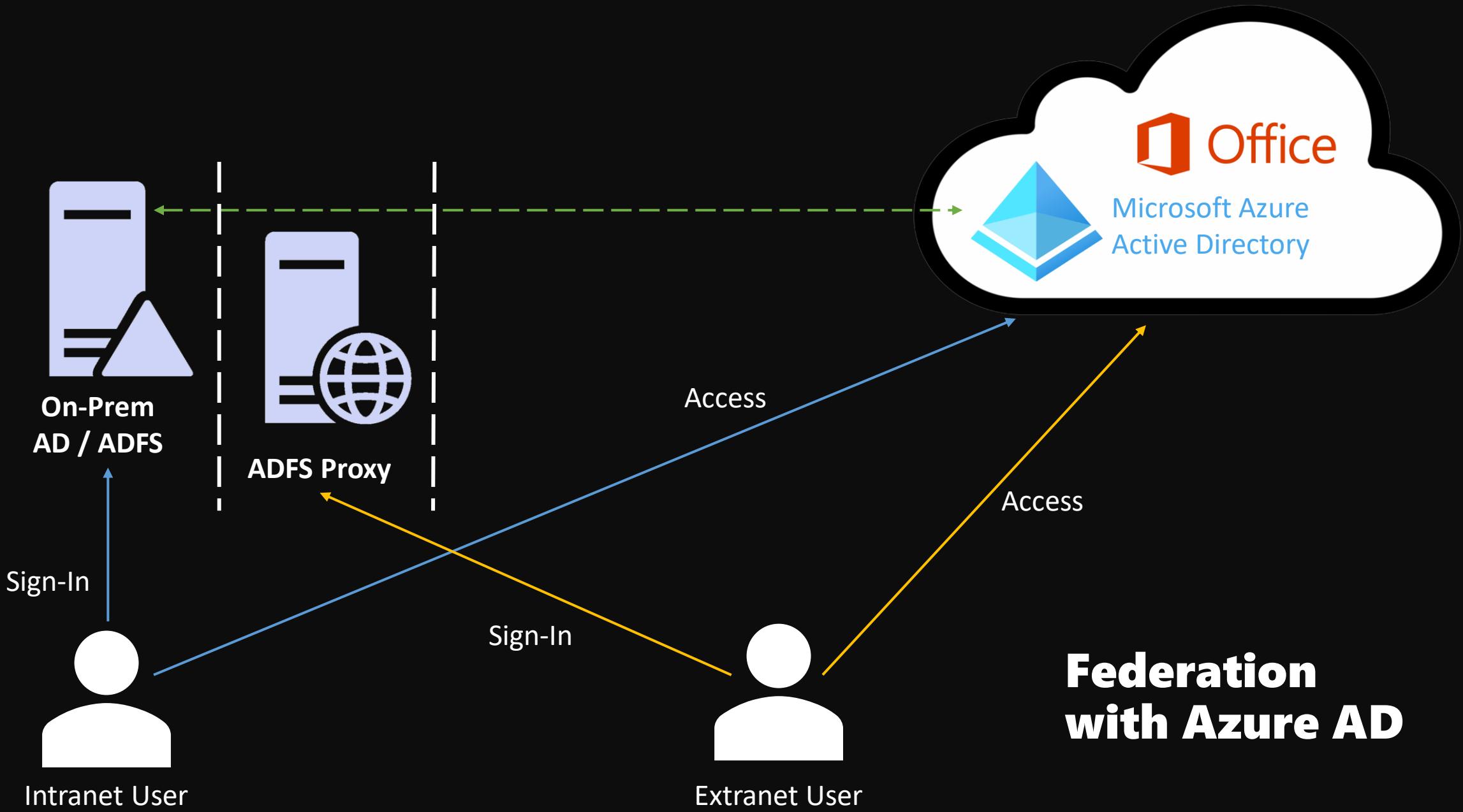
Federation is a collection of domains that trust each other.

- 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





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>



Berks Batteries | Overview  
Azure Active Directory

Switch tenant Delete tenant + Create a tenant What's new Preview features Got feedback?

Azure Active Directory can help you enable remote work for your employees and partners. [Learn more](#)

## Berks Batteries

Search your tenant

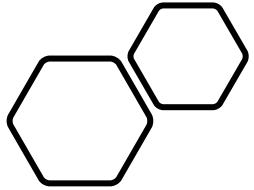
**Tenant information**

Your role: Global administrator [More info](#)  
License: Azure AD Premium P2  
Tenant ID: 61e57083-2c64-4d5d-b9d1-d81... [Edit](#)  
Primary domain: berksbatteries.com

**Azure AD Connect**

Status: Not enabled  
Last sync: Sync has never run

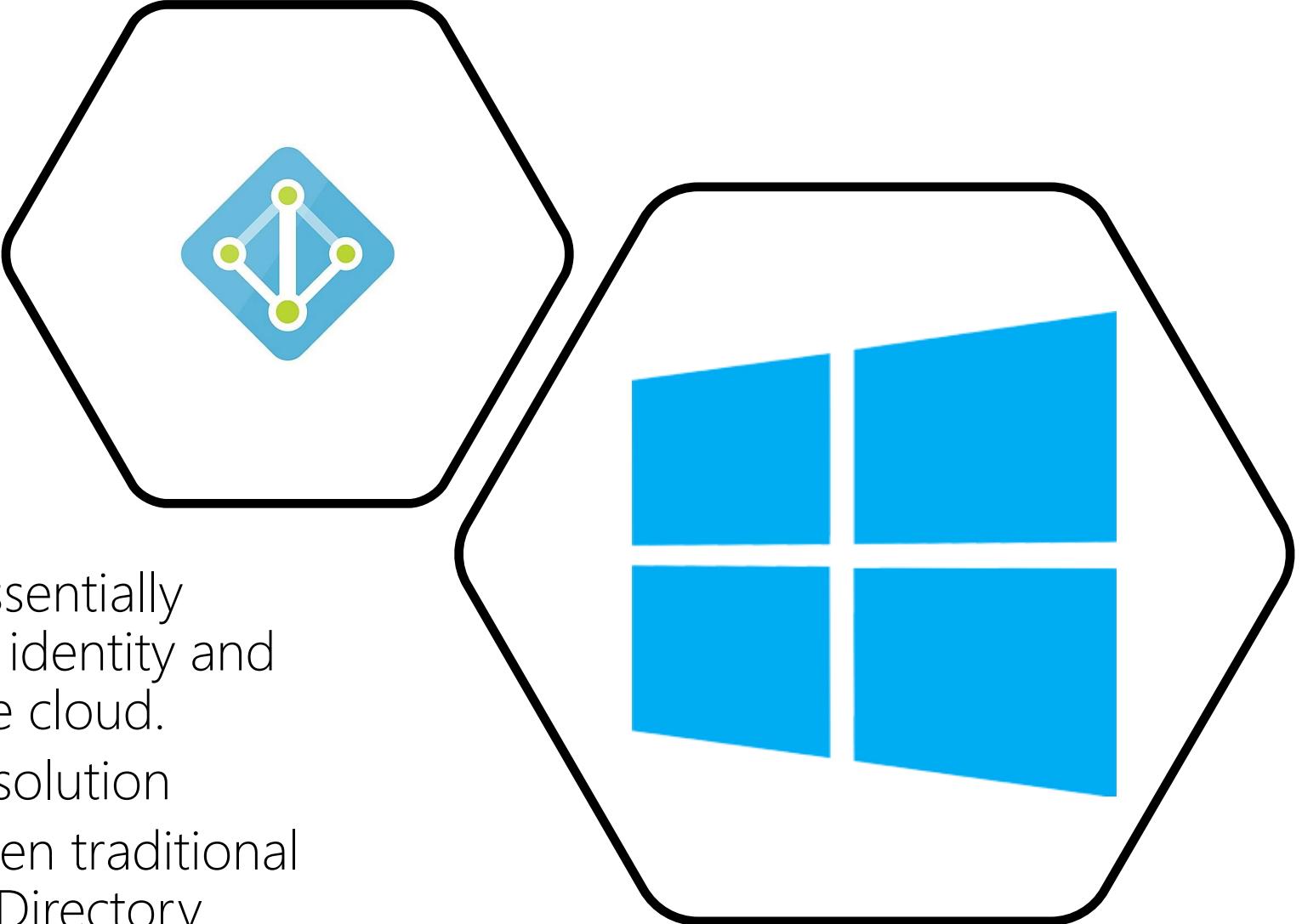
# Azure AD vs Traditional AD



## 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
<b>Provision Users</b>		
<b>External Users</b>		
<b>Resource Access</b>		
<b>Admin Management</b>		
<b>Authentication</b>		

# User Management: Azure AD vs Traditional AD

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

# User Management: Azure AD vs Traditional AD

Task	Traditional AD	Azure AD
<b>Provision Users</b>	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
<b>External Users</b>		
<b>Resource Access</b>		
<b>Admin Management</b>		
<b>Authentication</b>		

# User Management: Azure AD vs Traditional AD

Task	Traditional AD	Azure AD
<b>Provision Users</b>	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
<b>External Users</b>	Created manually in a dedicated external Active Directory forest	
<b>Resource Access</b>		
<b>Admin Management</b>		
<b>Authentication</b>		

# User Management: Azure AD vs Traditional AD

Task	Traditional AD	Azure AD
<b>Provision Users</b>	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
<b>External Users</b>	Created manually in a dedicated external Active Directory forest	Azure AD B2B used to manage links to external user identities
<b>Resource Access</b>		
<b>Admin Management</b>		
<b>Authentication</b>		

# User Management: Azure AD vs Traditional AD

Task	Traditional AD	Azure AD
<b>Provision Users</b>	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
<b>External Users</b>	Created manually in a dedicated external Active Directory forest	Azure AD B2B used to manage links to external user identities
<b>Resource Access</b>	create groups which are granted permissions to resources and then add users to groups	
<b>Admin Management</b>		
<b>Authentication</b>		

# User Management: Azure AD vs Traditional AD

Task	Traditional AD	Azure AD
<b>Provision Users</b>	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
<b>External Users</b>	Created manually in a dedicated external Active Directory forest	Azure AD B2B used to manage links to external user identities
<b>Resource Access</b>	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
<b>Admin Management</b>		
<b>Authentication</b>		

# User Management: Azure AD vs Traditional AD

Task	Traditional AD	Azure AD
<b>Provision Users</b>	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
<b>External Users</b>	Created manually in a dedicated external Active Directory forest	Azure AD B2B used to manage links to external user identities
<b>Resource Access</b>	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
<b>Admin Management</b>	domains, OUs, and groups used to delegate admin privileges	
<b>Authentication</b>		

# User Management: Azure AD vs Traditional AD

Task	Traditional AD	Azure AD
<b>Provision Users</b>	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
<b>External Users</b>	Created manually in a dedicated external Active Directory forest	Azure AD B2B used to manage links to external user identities
<b>Resource Access</b>	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
<b>Admin Management</b>	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.
<b>Authentication</b>		

# User Management: Azure AD vs Traditional AD

Task	Traditional AD	Azure AD
<b>Provision Users</b>	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
<b>External Users</b>	Created manually in a dedicated external Active Directory forest	Azure AD B2B used to manage links to external user identities
<b>Resource Access</b>	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
<b>Admin Management</b>	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.
<b>Authentication</b>	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
<b>Provision Users</b>	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
<b>External Users</b>	Created manually in a dedicated external Active Directory forest	Azure AD B2B used to manage links to external user identities
<b>Resource Access</b>	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
<b>Admin Management</b>	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.
<b>Authentication</b>	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
<b>Mobile Devices</b>		
<b>Windows Desktops</b>		
<b>Windows Servers</b>		
<b>Linux Workloads</b>		
<b>Authentication</b>		

# 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
<b>Mobile Devices</b>	does not natively support them	provides integration with Microsoft InTune
<b>Windows Desktops</b>	Can be joined to the domain and managed with group policy	
<b>Windows Servers</b>		
<b>Linux Workloads</b>		
<b>Authentication</b>		

# Devices: Azure AD vs Traditional AD

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

# Devices: Azure AD vs Traditional AD

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

# Devices: Azure AD vs Traditional AD

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

# Devices: Azure AD vs Traditional AD

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

# Devices: Azure AD vs Traditional AD

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

# Devices: Azure AD vs Traditional AD

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

# Devices: Azure AD vs Traditional AD

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



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

Image Users Groups External identities Global administrators Delegated administrators Delegated units Applications

**Berks Batteries**

Search your tenant

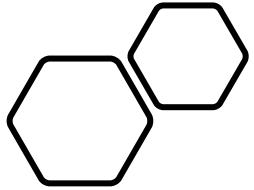
**Tenant information**

Your role: Global administrator More info  
License: Azure AD Premium P2  
Tenant ID: 61e57083-2c64-4d5d-b9d1-d81... [Copy]  
Primary domain: berksbatteries.com

**Azure AD Connect**

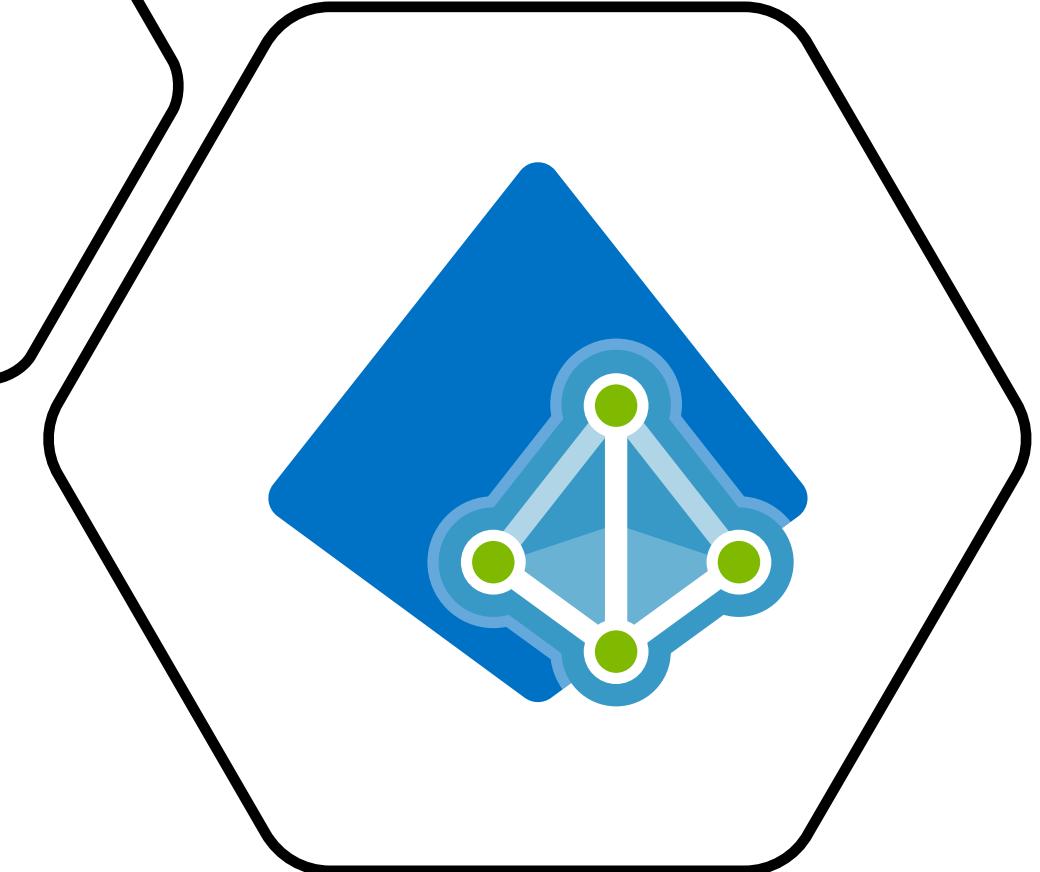
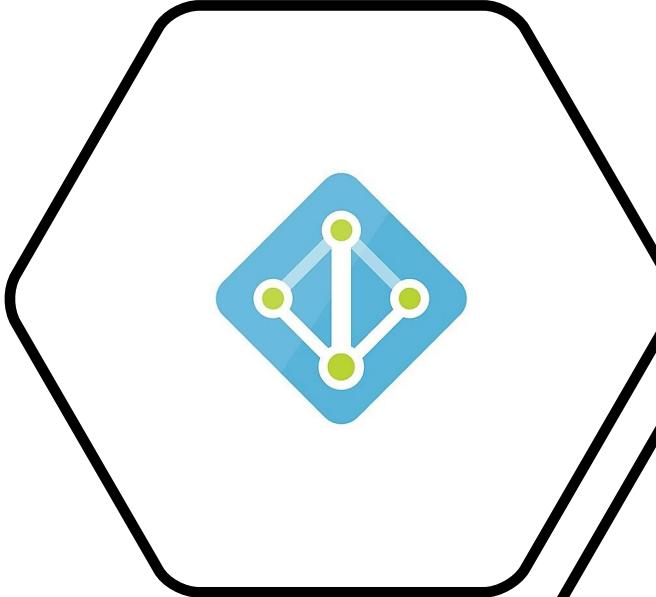
Status: Not enabled  
Last sync: Sync has never run

# 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 Ser... X

ics  
Configure basic settings

twork  
ect virtual network

ministrator group  
nfigure group membership

nchronization  
oose synchronization scope

mmary  
able Azure AD Domain Services

## Synchronization

Synchronize all users and groups in your entire Active Directory or synchronize specific users and groups. If you have a very large number of users and groups, you might want to consider starting with "scoped" synchronization. This will improve the time to complete the synchronization.

All      Scoped



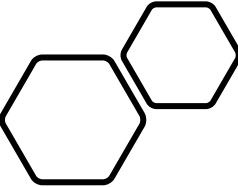
Scoped synchronization has been modified with different selections or configurations.  
To change synchronization from "all" to "scoped", the instance needs to be re-created. [More info](#)

# Azure AD Domain Services

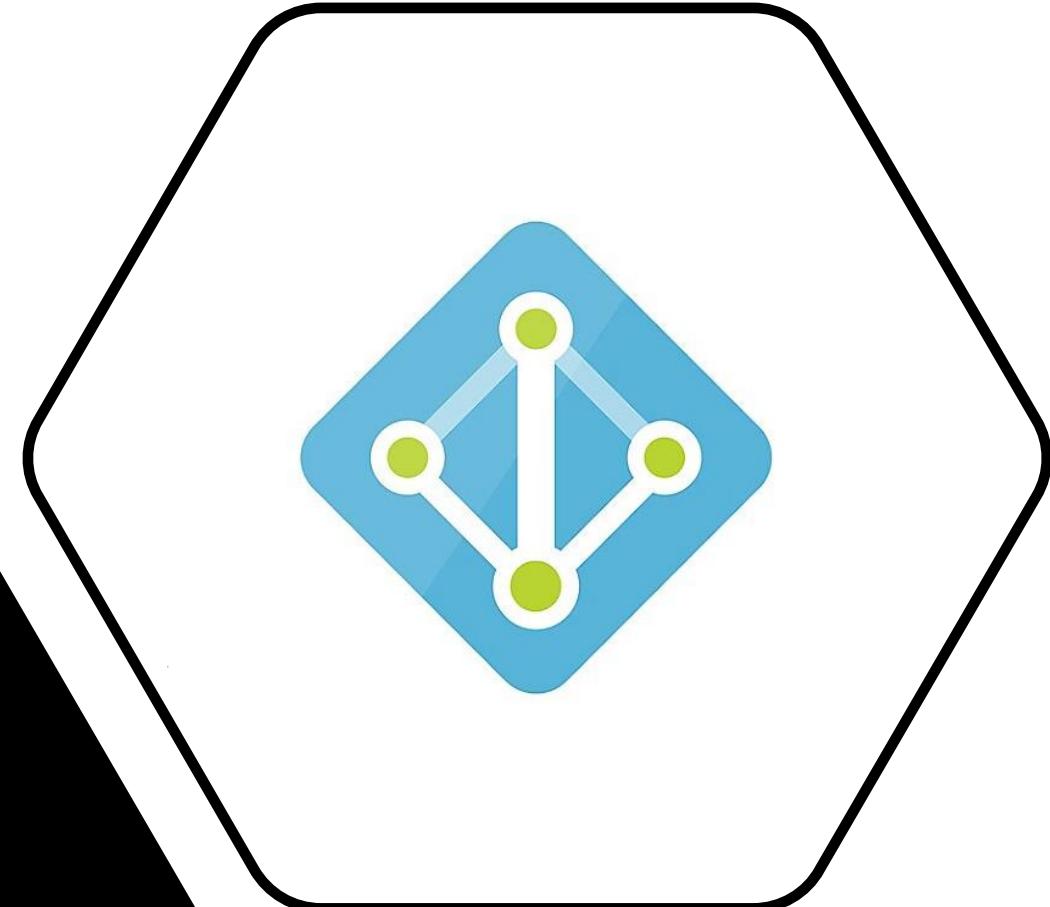
Azure AD Domain Services is a fully-managed domain services offering.

- 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

The screenshot shows the Azure Active Directory Overview page for the tenant "Berks Batteries". The left sidebar has a dark theme with white text and icons. It includes links for Overview, Getting started, Preview hub, Diagnose and solve problems, Manage (with sub-links for Users, Groups, External Identities, Roles and administrators, Administrative units, and Enterprise applications), and Sign-ins. The main content area has a light blue header with the tenant name and a message about enabling remote work. Below the header, there are two sections: "Tenant information" and "Azure AD Connect". The "Tenant information" section displays the Global administrator role, Azure AD Premium P2 license, Tenant ID (61e57083-2c64-4d5d-b9d1-d81...), and the primary domain (berksbatteries.com). The "Azure AD Connect" section shows that it is not enabled, with the last sync status indicating "Sync has never run".



# 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.

The screenshot shows the Azure Active Directory Overview page. At the top, there are navigation links: 'Switch tenant', 'Delete tenant', and 'Create a tenant'. Below this, a banner states: 'Azure Active Directory can help you enable remote work for your organization'. The main area displays the tenant name 'Berks Batteries' in large, bold letters. A search bar is present. On the left, a sidebar lists 'Properties', 'Administrators', 'Groups', 'Applications', and 'Sign-ins'. The 'Tenant information' section contains the following details:

Tenant information	
Your role	Global administrator <a href="#">More info</a>
License	Azure AD Premium P2
Tenant ID	61e57083-2c64-4d5d-b9d1-d81... <a href="#">Copy</a>
Primary domain	berksbatteries.com

At the bottom, there is a 'Sign-ins' section.

# Azure AD vs Azure AD DS

<b>Aspect</b>	<b>Azure AD-joined</b>	<b>Azure AD DS-joined</b>
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



Berks Batteries | Overview  
Azure Active Directory

Switch tenant Delete tenant + Create a tenant What's new Preview features Got feedback?

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... [Copy](#)  
Primary domain: berksbatteries.com

**Azure AD Connect**

Status: Not enabled  
Last sync: Sync has never run

# Azure AD Authentication

Registration

Notifications

Customization

On-premises integration

Administrator Policy

Activity

Audit logs

Usage & insights

Troubleshooting + Support

- Mobile app code
- Email
- Mobile phone (SMS only)
- Office phone ⓘ
- Security questions

**i** These settings only apply to end users in your organization. Admins are always enabled for self-service password reset and are required to use two authentication methods to reset their password. Click here to learn more about administrator password policies.

# 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.

# Password reset | Authentication methods

Berks Batteries - Azure Active Directory

Diagnose and solve problems

Manage

Properties

Authentication methods

Registration

Notifications

Customization

On-premises integration

Administrator Policy

Activity

Audit log

Usage & insights

Troubleshooting + Support

New support request

« Save Discard

Number of methods required to reset ⓘ

1

2

Methods available to users

Mobile app notification

Mobile app code

Email

Mobile phone (SMS only)

Office phone ⓘ

Security questions

## Azure Active Directory Authentication

These settings only apply to users who have not yet enabled self-service password reset and are required to use two authentication methods to reset their password. Click here to learn more about administrator password policies.

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.

ssword reset | Authentication methods

Batteries - Azure Active Directory

« Save Discard

Diagnose and solve problems

age

Properties

Authentication methods

Registration

Notifications

Localization

Devices integration

User Policy

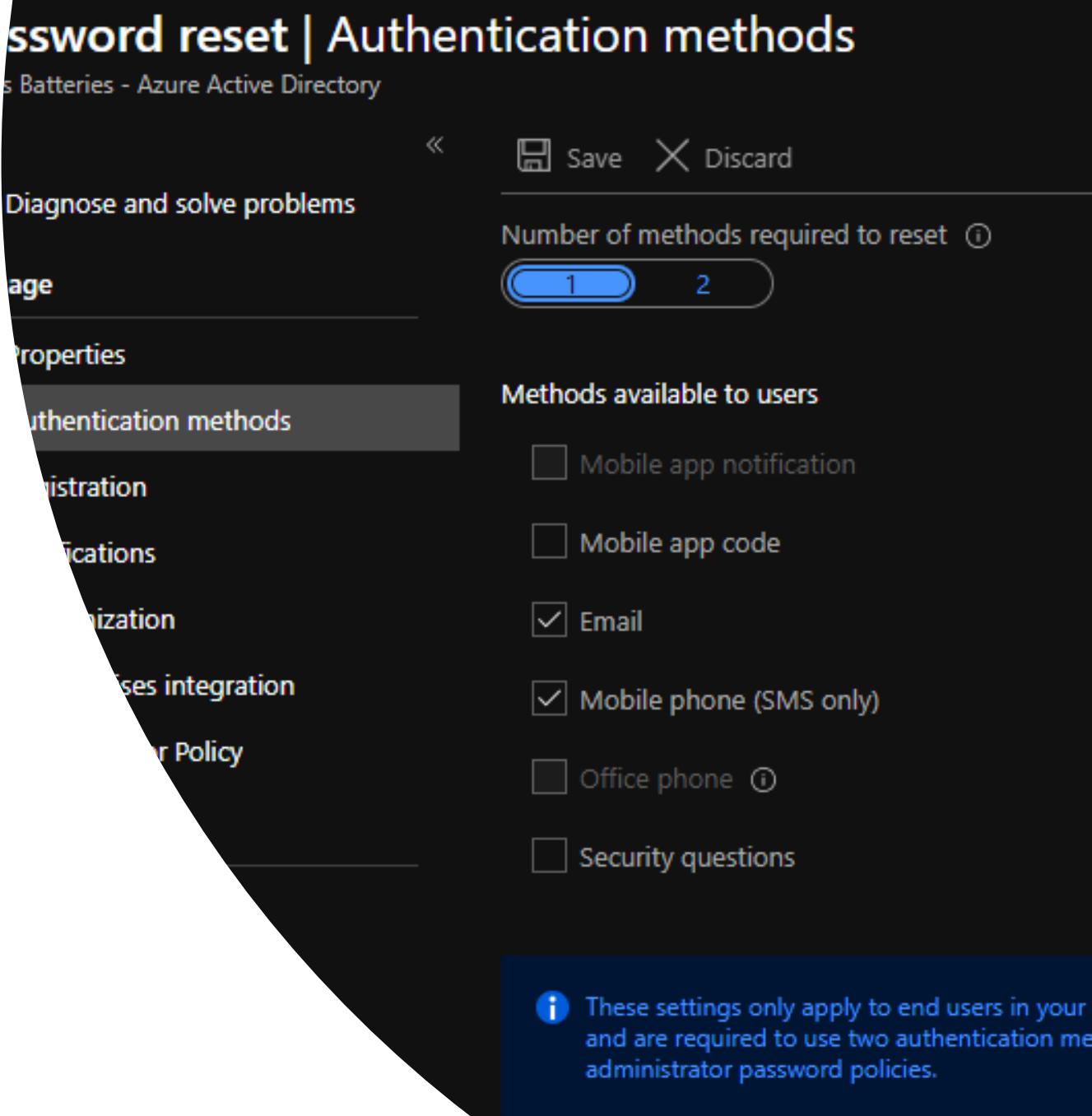
Number of methods required to reset ⓘ

1 2

Methods available to users

- Mobile app notification
- Mobile app code
- Email
- Mobile phone (SMS only)
- Office phone ⓘ
- Security questions

**i** These settings only apply to end users in your organization and are required to use two authentication methods for administrator password policies.



# multi-factor authentication

## users service settings

Note: only users licensed to use Microsoft Online Services are eligible for Multi-Factor Authentication. [Learn more about how to license other users.](#)  
Before you begin, take a look at the [multi-factor auth deployment guide](#).

View: [Sign-in allowed users](#)  Multi-Factor Auth status: [Any](#) [bulk update](#)

---

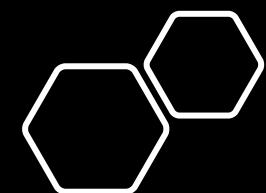
<input type="checkbox"/> DISPLAY NAME ▲	USER NAME	MULTI-FACTOR AUTH STATUS	
<input type="checkbox"/> Admin Account	admin@berksbatteries.onmicrosoft.com	Disabled	
<input type="checkbox"/> admin@test9878.org admin	admin_test9878.org#EXT#@berksfinance.onmicrosoft.com	Disabled	
<input type="checkbox"/> Lester Murphy	LesterM@berksbatteries.com	Disabled	

Select a user

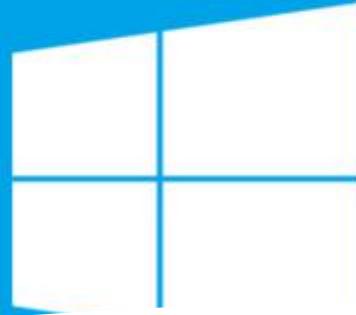
## Multi-Factor Authentication

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

- Phone Call
- SMS Text Message
- Mobile App Notification



# Hello



# Windows 10

## 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.

Microsoft

## Get back into your account

### Who are you?

To recover your account, begin by entering your email or username and the characters in the picture or audio b

Email or Username:

Example: user@contoso.onmicrosoft.com or user@contoso.com



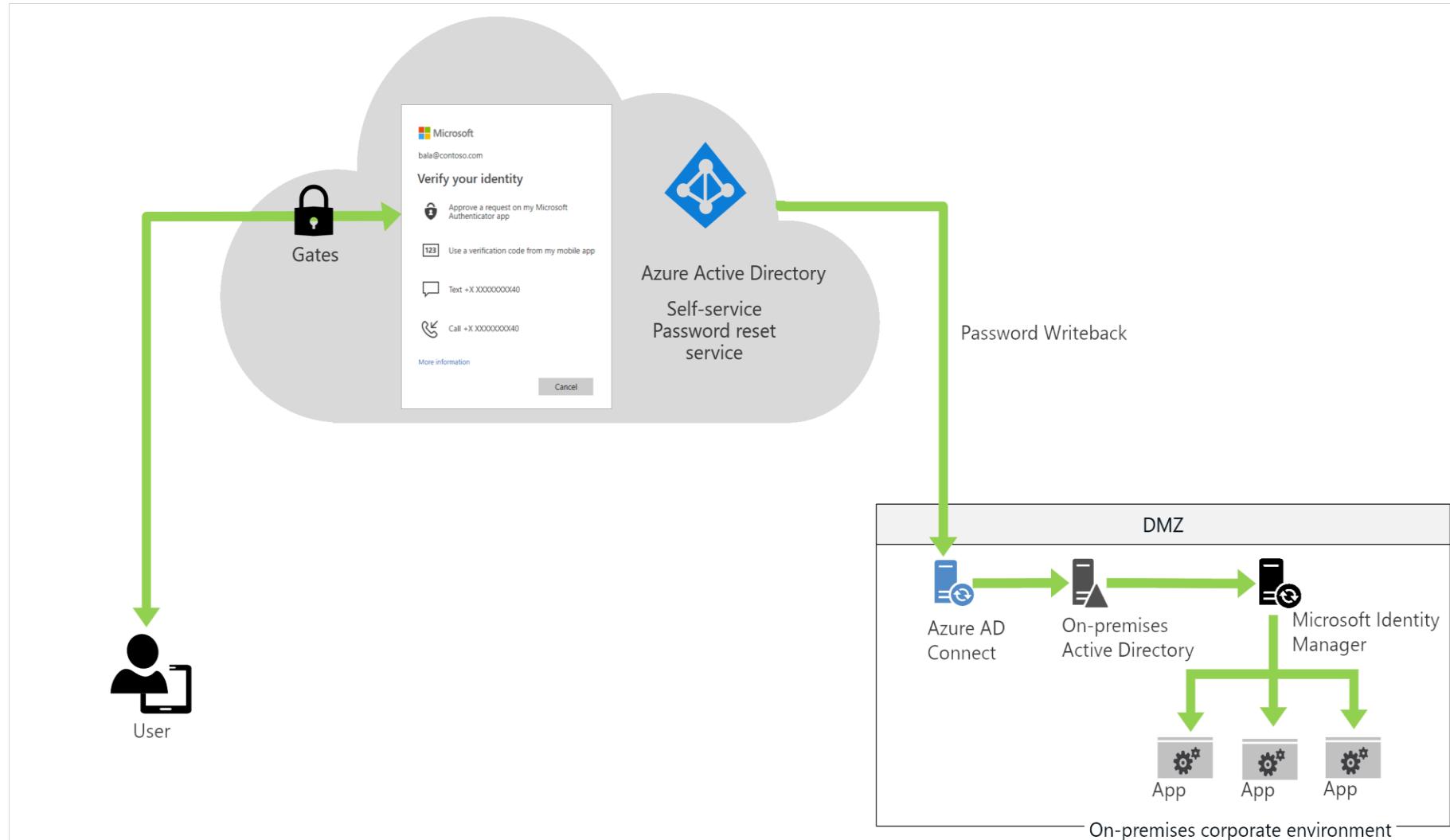
Enter the characters in the picture or the words in the audio.

Next

Cancel

**<https://aka.ms/sspr>**

# How SSPR Works

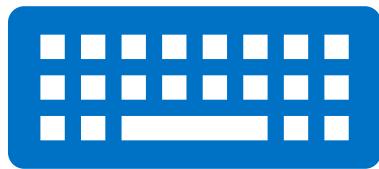


# Azure Multi-Factor Authentication

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.

The screenshot shows the 'Password protection' settings page in the Azure portal. At the top, there are 'Save' and 'Discard' buttons, and a 'Got feedback?' link. Below this, under 'Custom smart lockout', the 'Lockout threshold' is set to 10 and the 'Lockout duration in seconds' is set to 60. Under 'Custom banned passwords', the 'Enforce custom list' switch is turned 'Yes'. A list of banned passwords is shown, including 'MyPassword' (selected), 'Password', and '1234567'. Below this, under 'Password protection for Windows Server Active Directory', the 'Enable password protection on Windows Server Active Directory' switch is turned 'Yes'. The 'Mode' is set to 'Enforced'.

Custom smart lockout

Lockout threshold ⓘ 10

Lockout duration in seconds ⓘ 60

Custom banned passwords

Enforce custom list ⓘ Yes No

Custom banned password list ⓘ

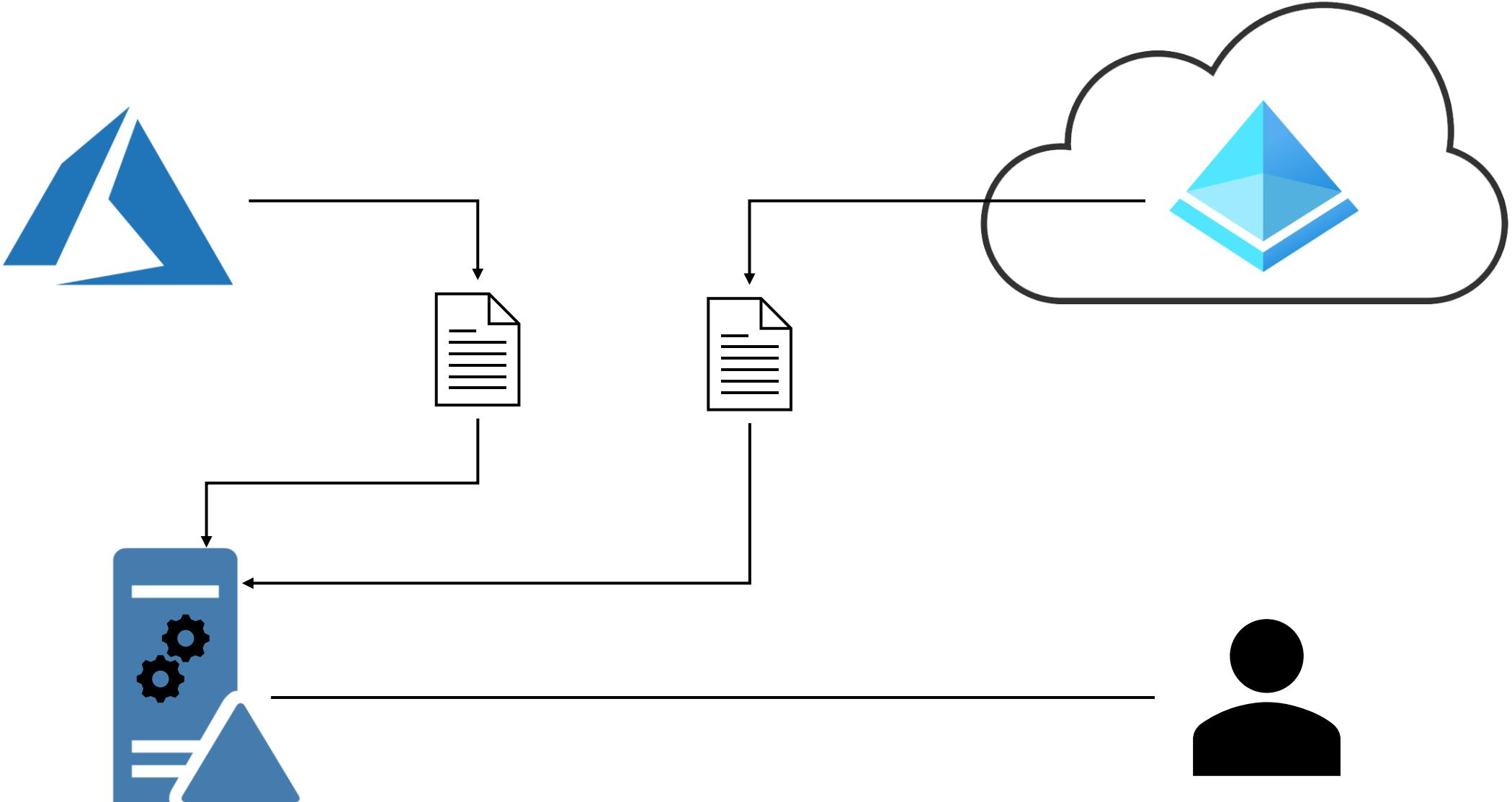
MyPassword ✓  
Password  
1234567

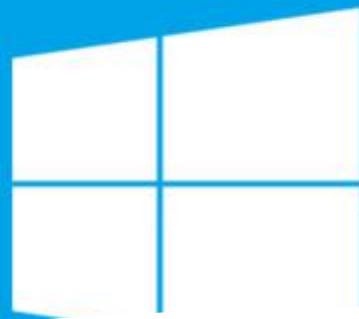
Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory ⓘ Yes No

Mode ⓘ Enforced Audit

# Password Protection





# Hello

# Windows 10

## 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**.



Berks Batteries | Overview  
Azure Active Directory

Switch tenant Delete tenant + Create a tenant What's new Preview features Got feedback?

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

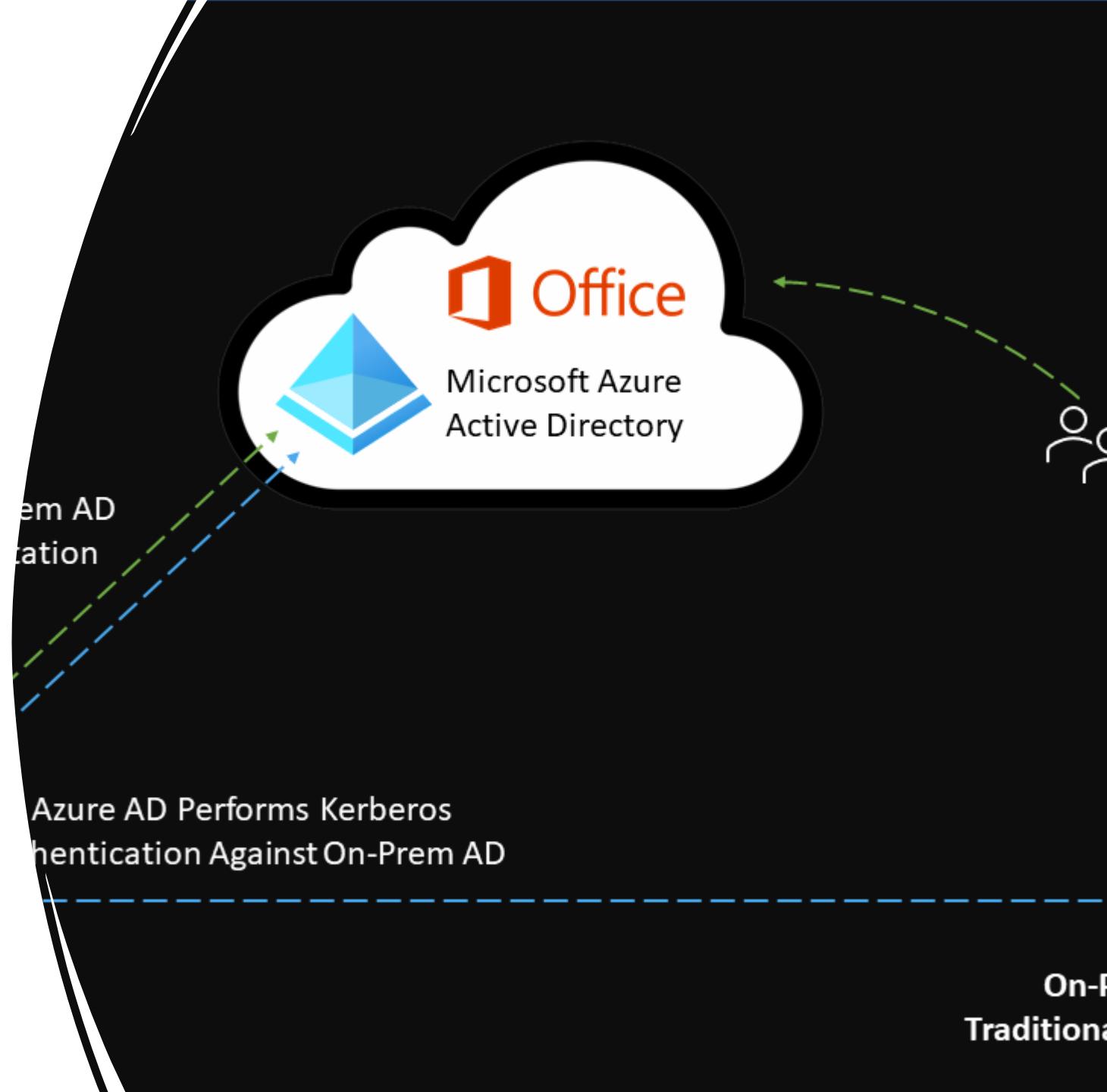
- Status: Not enabled
- Last sync: Sync has never run

# Seamless Single Sign-On

# Seamless Single Sign-On

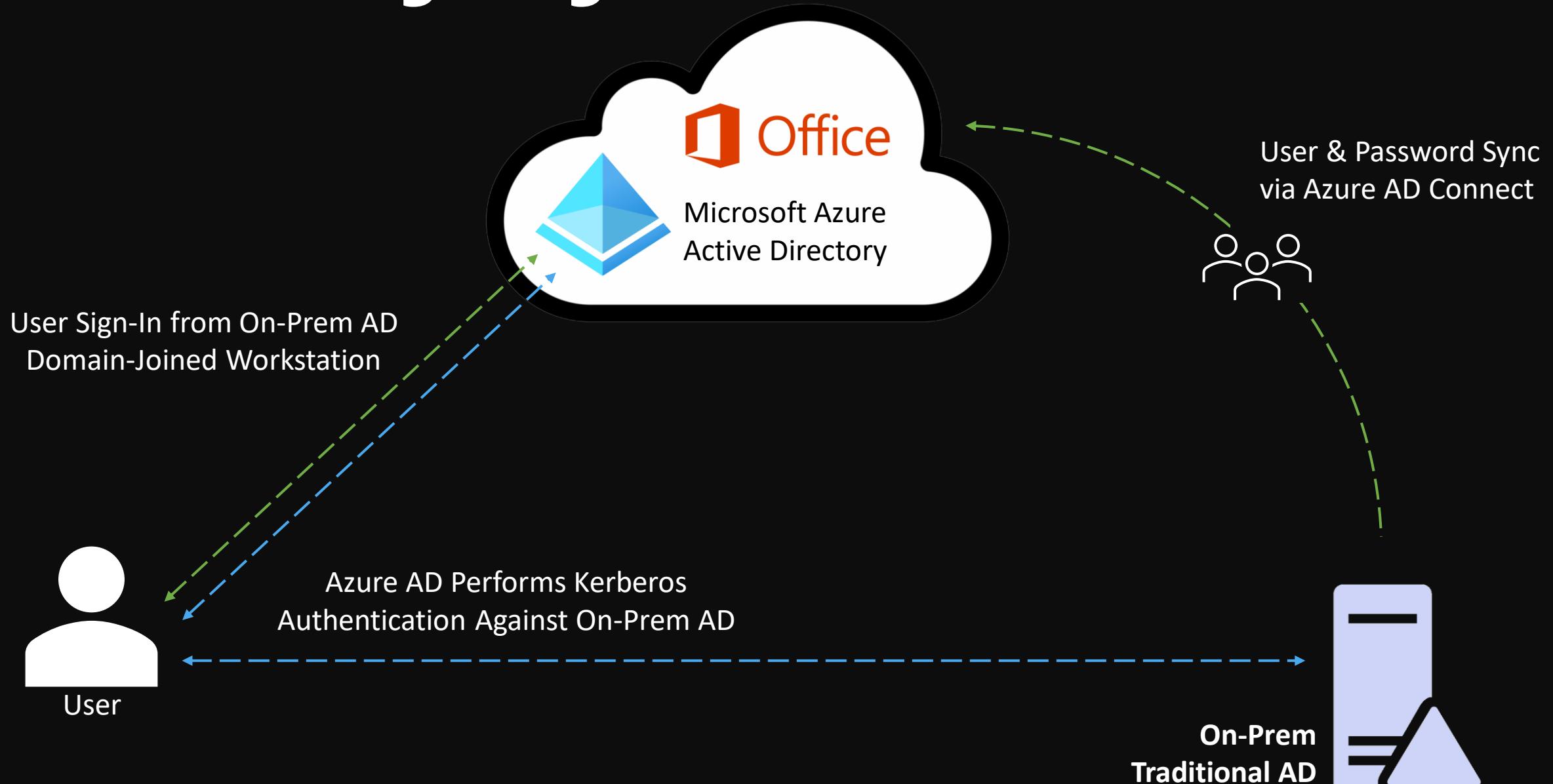
Automatically signs users in when using a corporate device while connected to corporate network.

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



On-Prem  
Traditional

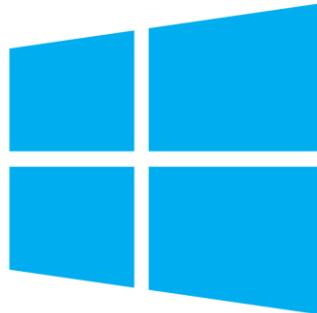
# Seamless Single Sign-On



# Single Sign-On

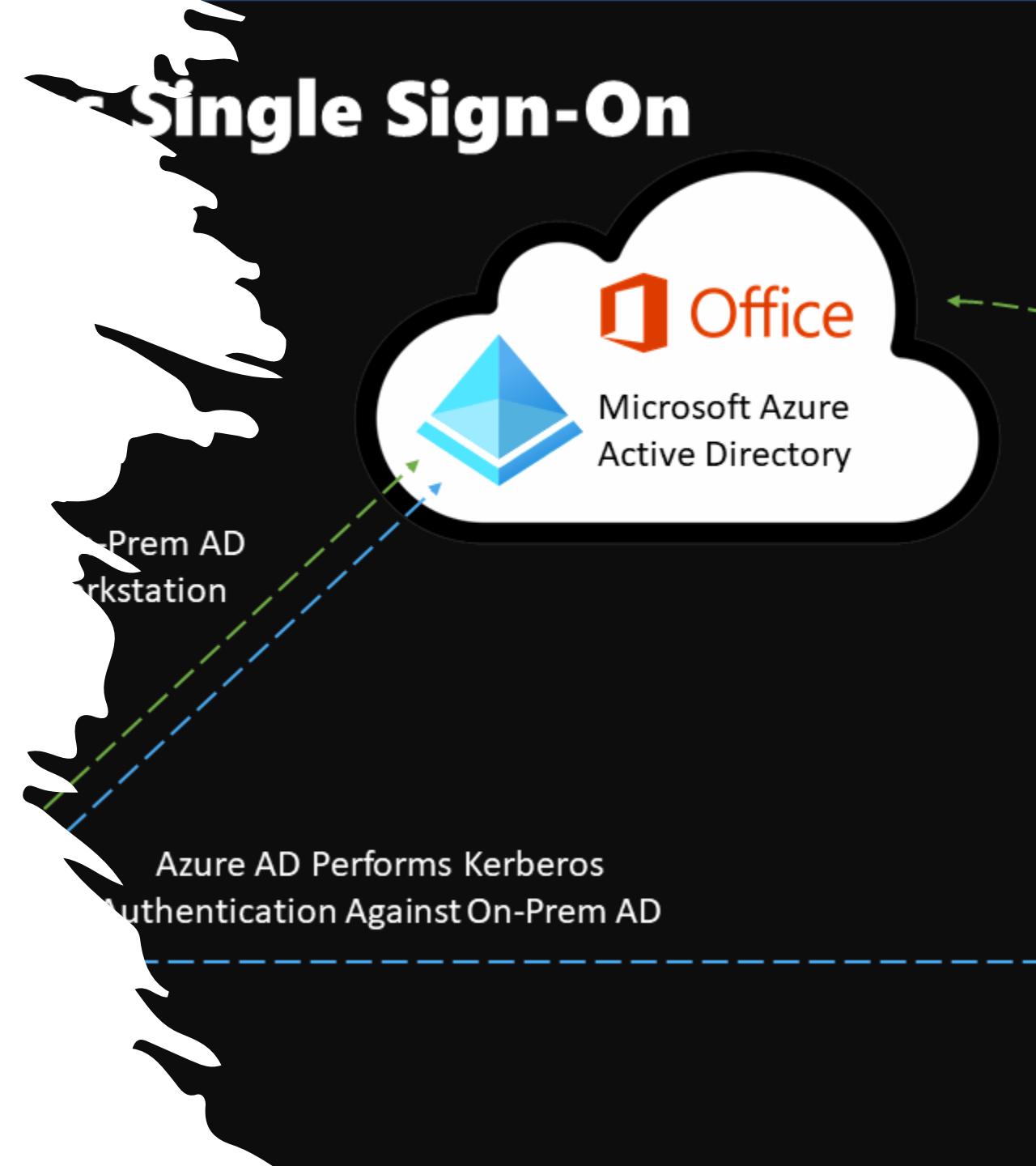
Single Sign-On can be achieved via **Primary Refresh Token** OR via **Seamless SSO**.

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

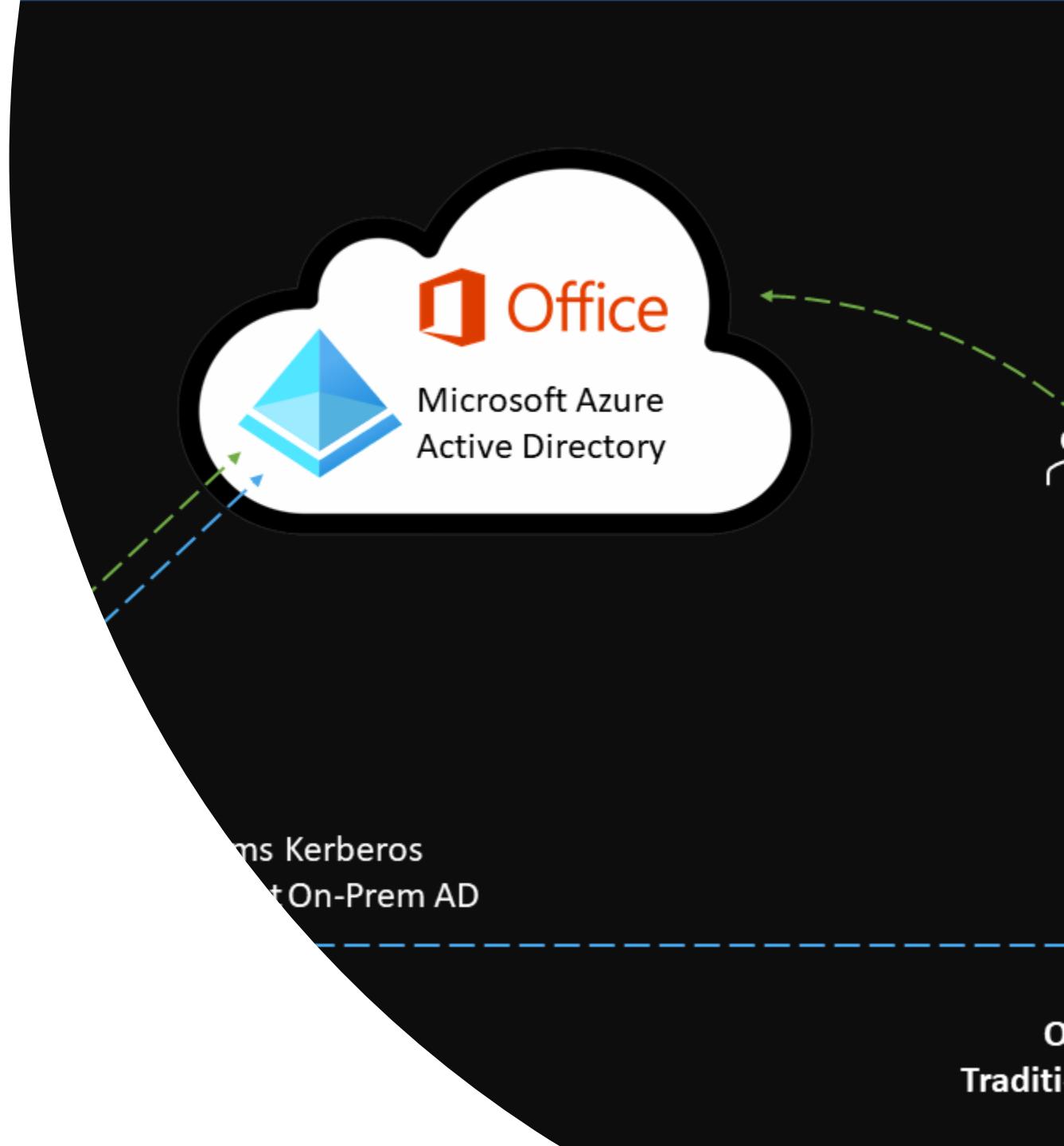
---

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>



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

Image Users Groups External identities Global administrators Delegated administrators Delegated units Applications

## Berks Batteries

Search your tenant

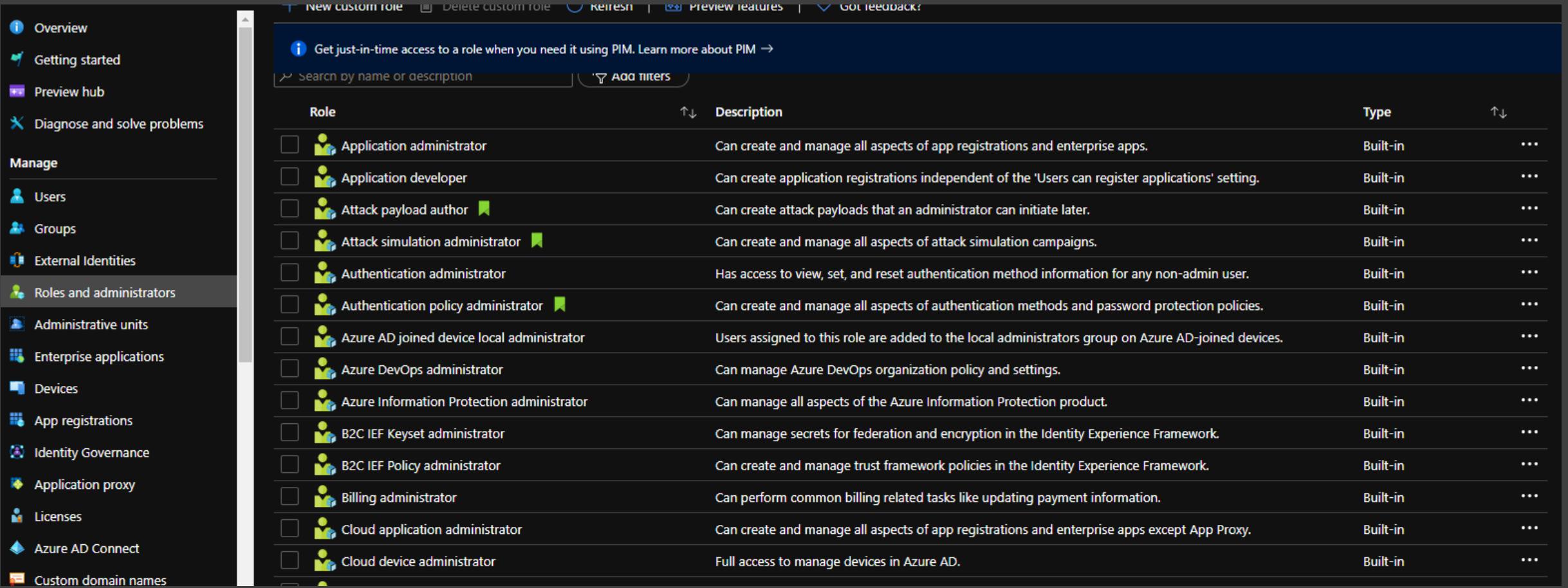
**Tenant information**

Your role: Global administrator [More info](#)  
License: Azure AD Premium P2  
Tenant ID: 61e57083-2c64-4d5d-b9d1-d81... [Edit](#)  
Primary domain: berksbatteries.com

**Azure AD Connect**

Status: Not enabled  
Last sync: Sync has never run

# Role-Based Access Control in Azure AD



The screenshot shows the 'New custom role' page in the Azure portal. The top navigation bar includes 'New custom role', 'Delete custom role', 'Refresh', 'Preview features', and 'Got feedback?'. On the left, a sidebar under 'Manage' lists various Azure services: Users, Groups, External Identities, Roles and administrators (which is selected), Administrative units, Enterprise applications, Devices, App registrations, Identity Governance, Application proxy, Licenses, Azure AD Connect, and Custom domain names. The main content area displays a table of built-in roles:

Role	Description	Type
Application administrator	Can create and manage all aspects of app registrations and enterprise apps.	Built-in
Application developer	Can create application registrations independent of the 'Users can register applications' setting.	Built-in
Attack payload author	Can create attack payloads that an administrator can initiate later.	Built-in
Attack simulation administrator	Can create and manage all aspects of attack simulation campaigns.	Built-in
Authentication administrator	Has access to view, set, and reset authentication method information for any non-admin user.	Built-in
Authentication policy administrator	Can create and manage all aspects of authentication methods and password protection policies.	Built-in
Azure AD joined device local administrator	Users assigned to this role are added to the local administrators group on Azure AD-joined devices.	Built-in
Azure DevOps administrator	Can manage Azure DevOps organization policy and settings.	Built-in
Azure Information Protection administrator	Can manage all aspects of the Azure Information Protection product.	Built-in
B2C IEF Keyset administrator	Can manage secrets for federation and encryption in the Identity Experience Framework.	Built-in
B2C IEF Policy administrator	Can create and manage trust framework policies in the Identity Experience Framework.	Built-in
Billing administrator	Can perform common billing related tasks like updating payment information.	Built-in
Cloud application administrator	Can create and manage all aspects of app registrations and enterprise apps except App Proxy.	Built-in
Cloud device administrator	Full access to manage devices in Azure AD.	Built-in

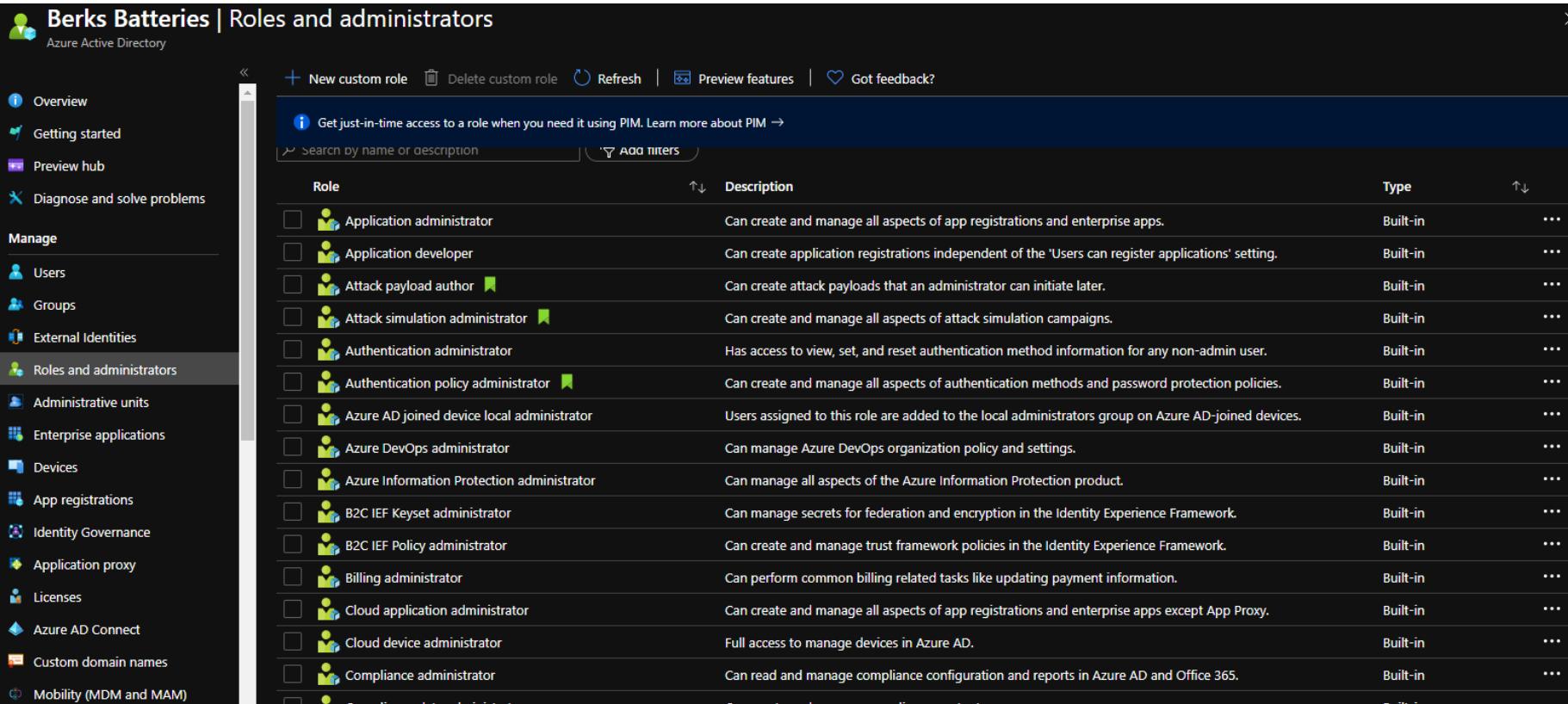
# Role-Based Access Control

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.



The screenshot shows the 'Berks Batteries' Azure Active Directory interface. The left sidebar lists various management categories: Overview, Getting started, Preview hub, Diagnose and solve problems, Manage (with sub-options: Users, Groups, External Identities, Roles and administrators, Administrative units, Enterprise applications, Devices, App registrations, Identity Governance, Application proxy, Licenses, Azure AD Connect, Custom domain names, Mobility (MDM and MAM)), and a preview feature for PIM. The 'Roles and administrators' option is selected. The main content area displays a table of built-in roles:

Role	Description	Type
Application administrator	Can create and manage all aspects of app registrations and enterprise apps.	Built-in
Application developer	Can create application registrations independent of the 'Users can register applications' setting.	Built-in
Attack payload author	Can create attack payloads that an administrator can initiate later.	Built-in
Attack simulation administrator	Can create and manage all aspects of attack simulation campaigns.	Built-in
Authentication administrator	Has access to view, set, and reset authentication method information for any non-admin user.	Built-in
Authentication policy administrator	Can create and manage all aspects of authentication methods and password protection policies.	Built-in
Azure AD joined device local administrator	Users assigned to this role are added to the local administrators group on Azure AD-joined devices.	Built-in
Azure DevOps administrator	Can manage Azure DevOps organization policy and settings.	Built-in
Azure Information Protection administrator	Can manage all aspects of the Azure Information Protection product.	Built-in
B2C IEF Keyset administrator	Can manage secrets for federation and encryption in the Identity Experience Framework.	Built-in
B2C IEF Policy administrator	Can create and manage trust framework policies in the Identity Experience Framework.	Built-in
Billing administrator	Can perform common billing related tasks like updating payment information.	Built-in
Cloud application administrator	Can create and manage all aspects of app registrations and enterprise apps except App Proxy.	Built-in
Cloud device administrator	Full access to manage devices in Azure AD.	Built-in
Compliance administrator	Can read and manage compliance configuration and reports in Azure AD and Office 365.	Built-in
Compliance data administrator	Can create and manage compliance content.	Built-in

 Overview
 Getting started
 Preview hub
 Diagnose and solve problems
<b>Manage</b>
 Users
 Groups
 External Identities
 Roles and administrators
 Administrative units
 Enterprise applications
 Devices
 App registrations
 Identity Governance
 Application proxy
 Licenses
 Azure AD Connect
 Custom domain names
 Mobility (MDM and MAM)

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

Search by name or description  Add filters

Role	Description
 Application administrator	Can create and manage all aspects of app registrations and enterprise apps.
 Application developer	
 Attack payload author 	
 Attack simulation administrator 	
 Authentication administrator	
 Authentication policy administrator 	
 Azure AD joined device local administrator	
 Azure DevOps administrator	
 Azure Information Protection administrator	
 B2C IEF Keyset administrator	
 B2C IEF Policy administrator	
 Billing administrator	Can perform common billing related tasks like updating payment information.
 Cloud application administrator	Can create and manage all aspects of app registrations and enterprise apps except App Proxy.
 Cloud device administrator	Full access to manage devices in Azure AD.
 Compliance administrator	Can read and manage compliance configuration and reports in Azure AD and Office 365.
 Compliance data administrator	Can create and manage compliance content.

There are two types of role definitions in RBAC:

- Built-In
- Custom

## Built-in roles

- Fixed sets of permissions
- Cannot be modified

Can create and manage trust framework policies in the Identity Experience Framework.

Can perform common billing related tasks like updating payment information.

Can create and manage all aspects of app registrations and enterprise apps except App Proxy.

Full access to manage devices in Azure AD.

Can read and manage compliance configuration and reports in Azure AD and Office 365.

Can create and manage compliance content.

# Azure AD RBAC Roles

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

 Overview Getting started Preview hub Diagnose and solve problems Manage Users Groups External identities Roles and assignments Administrative units Enterprise applications Devices App registrations Identity Governance Application Licenses Azure AD Connect Custom domain names Mobility (MDM and MAM)

# Azure AD RBAC Custom Roles

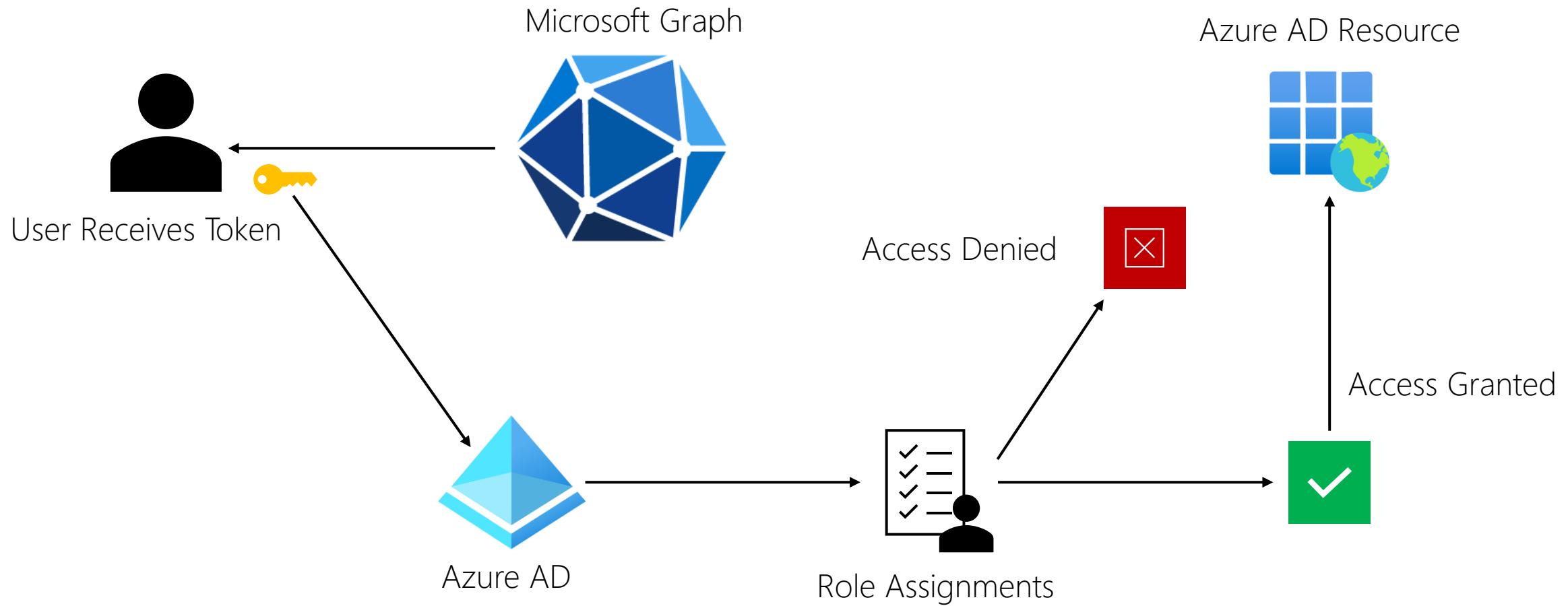
**Custom roles** are useful when you have a need for a combination of permissions that's not offered by a built-in role.

## 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>



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

Image Users Groups Global identities Local administrators Delegated units Applications

**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... [Edit](#)  
Primary domain: berksbatteries.com

**Azure AD Connect**

Status: Not enabled  
Last sync: Sync has never run

# What is Azure Identity Protection?

The screenshot shows the Azure Identity Protection portal interface. On the left, there's a navigation sidebar with sections like Overview, Diagnose and solve problems, Protect, Report, Notify, and Troubleshooting + Support. The main area has three main sections: 'Protect' (User risk policy, Sign-in risk policy, MFA registration policy), 'Report' (Risky users, Risky sign-ins, Risk detections), and 'Notify' (Users at risk detected alerts, Weekly digest). At the top, there are date range filters (Date range = 30 days) and user risk level filters (User risk level = All). A callout box on the right says 'Identity Secure Score /-' and 'Monitor and improve your identity security posture.'

# Azure Identity Protection

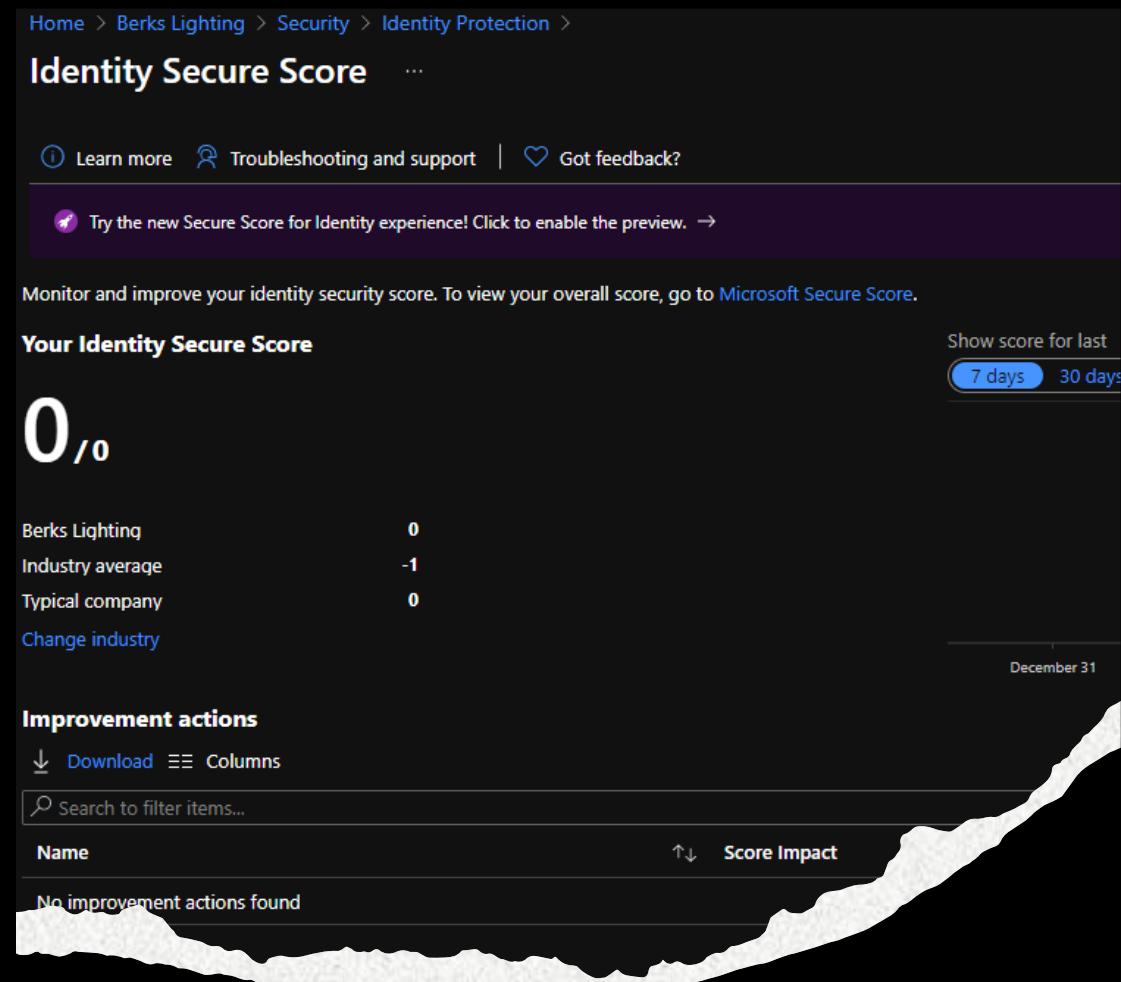
**Azure Identity Protection** is a tool that allows organizations to accomplish several tasks:

- 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:

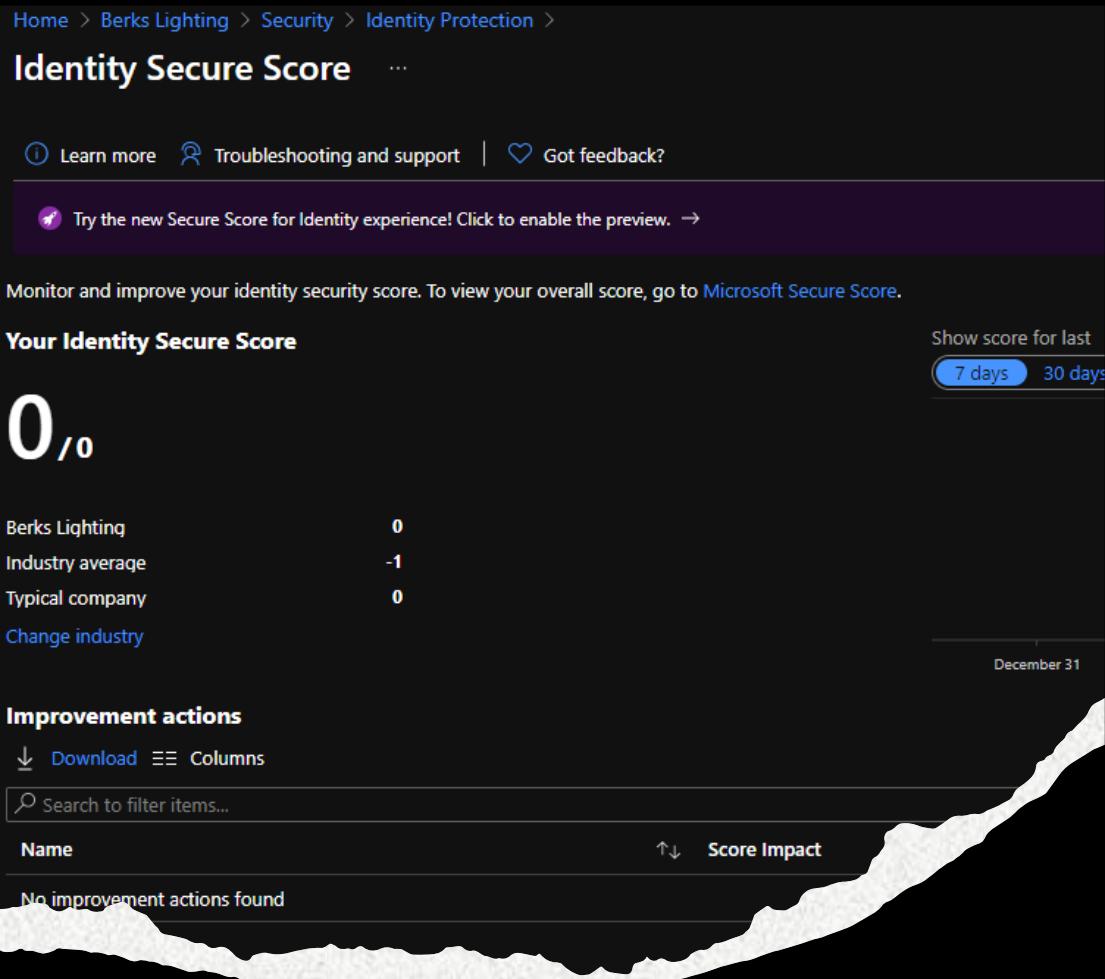
- Anonymous IP address
- Atypical travel
- Malware linked IP address
- Unfamiliar sign-in properties
- Leaked Credentials
- Password spray
- New country
- Activity from anonymous IP address
- Suspicious inbox forwarding



# Azure Identity Protection

Identifies the following types of risks:

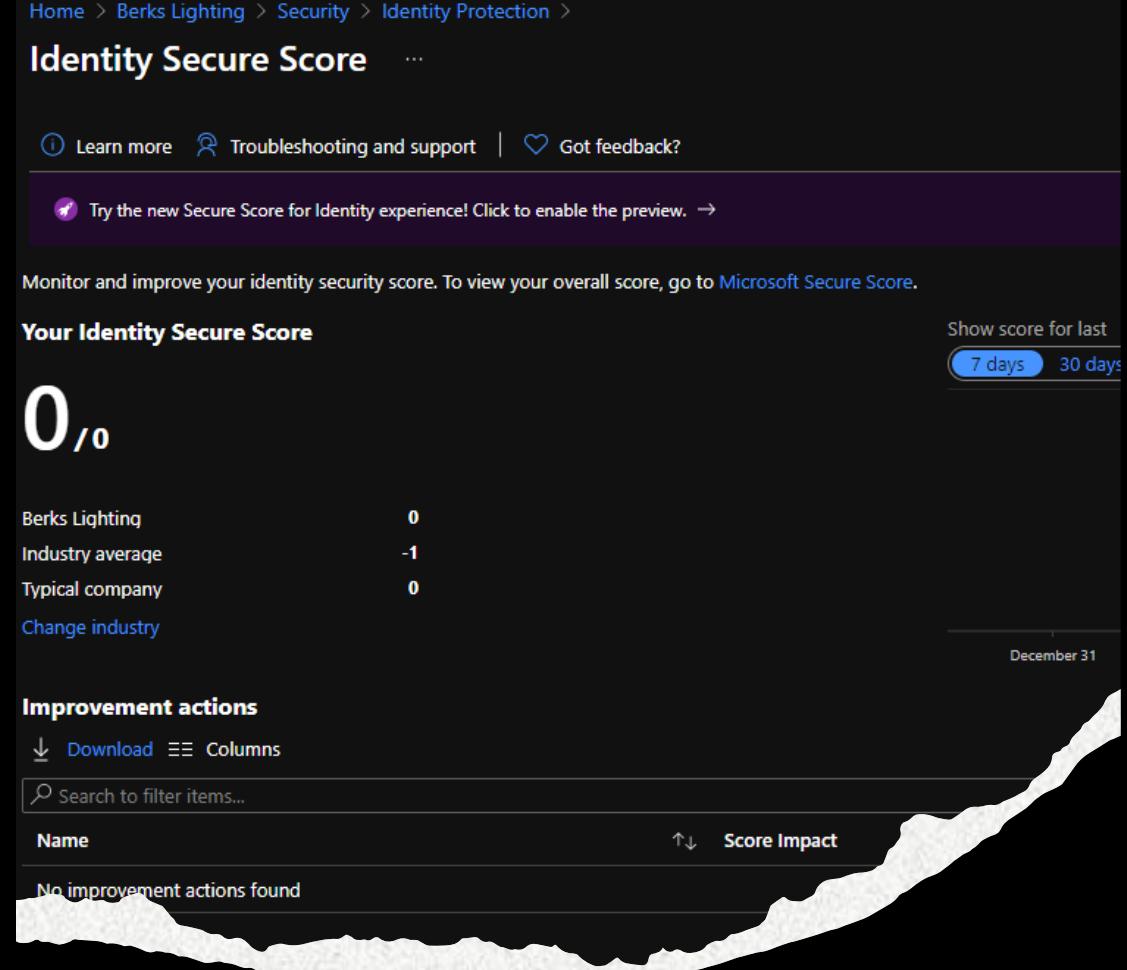
- **Anonymous IP address**
- Atypical travel
- Malware linked IP address
- Unfamiliar sign-in properties
- Leaked Credentials
- Password spray
- New country
- Activity from anonymous IP address
- Suspicious inbox forwarding



# Azure Identity Protection

Identifies the following types of risks:

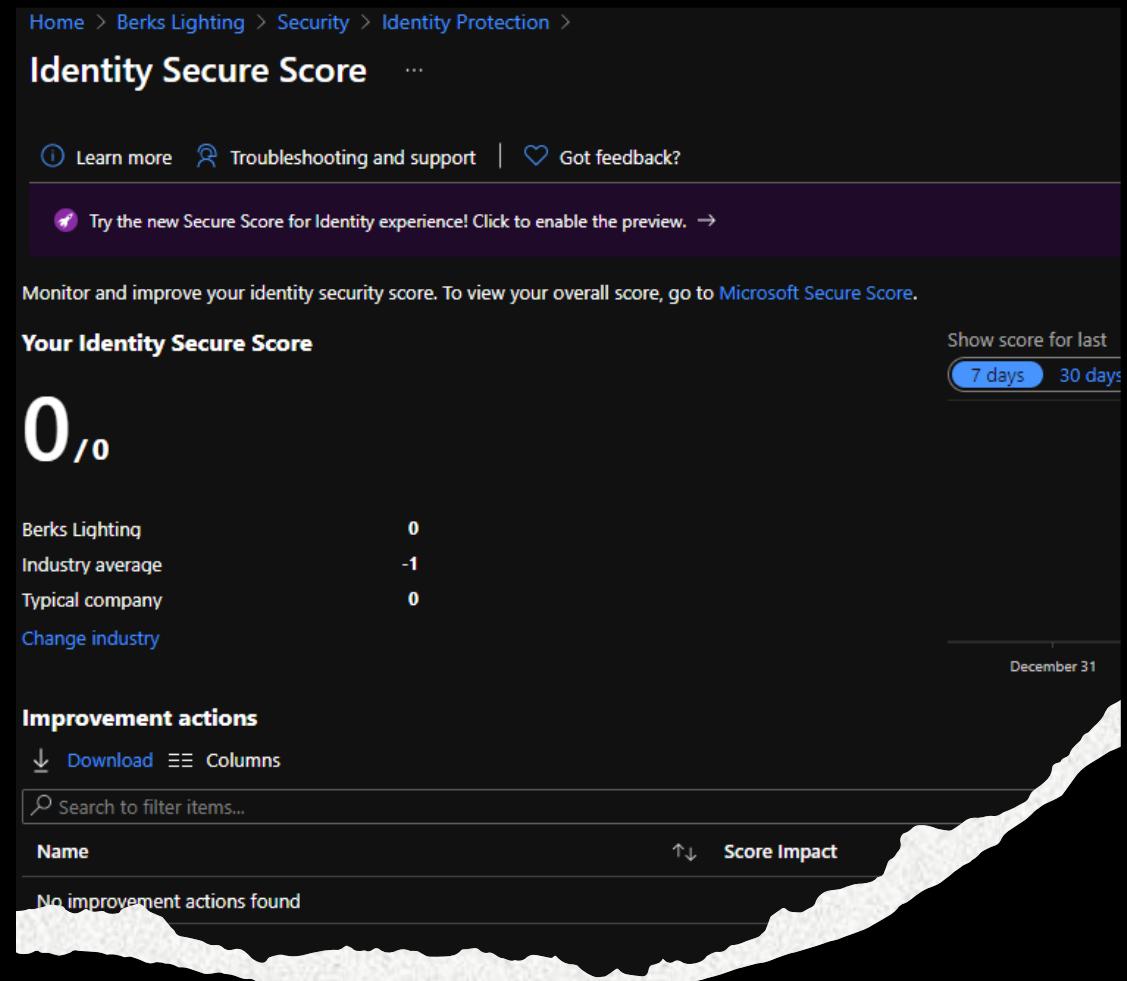
- Anonymous IP address
- **Atypical travel**
- Malware linked IP address
- Unfamiliar sign-in properties
- Leaked Credentials
- Password spray
- New country
- Activity from anonymous IP address
- Suspicious inbox forwarding



# Azure Identity Protection

Identifies the following types of risks:

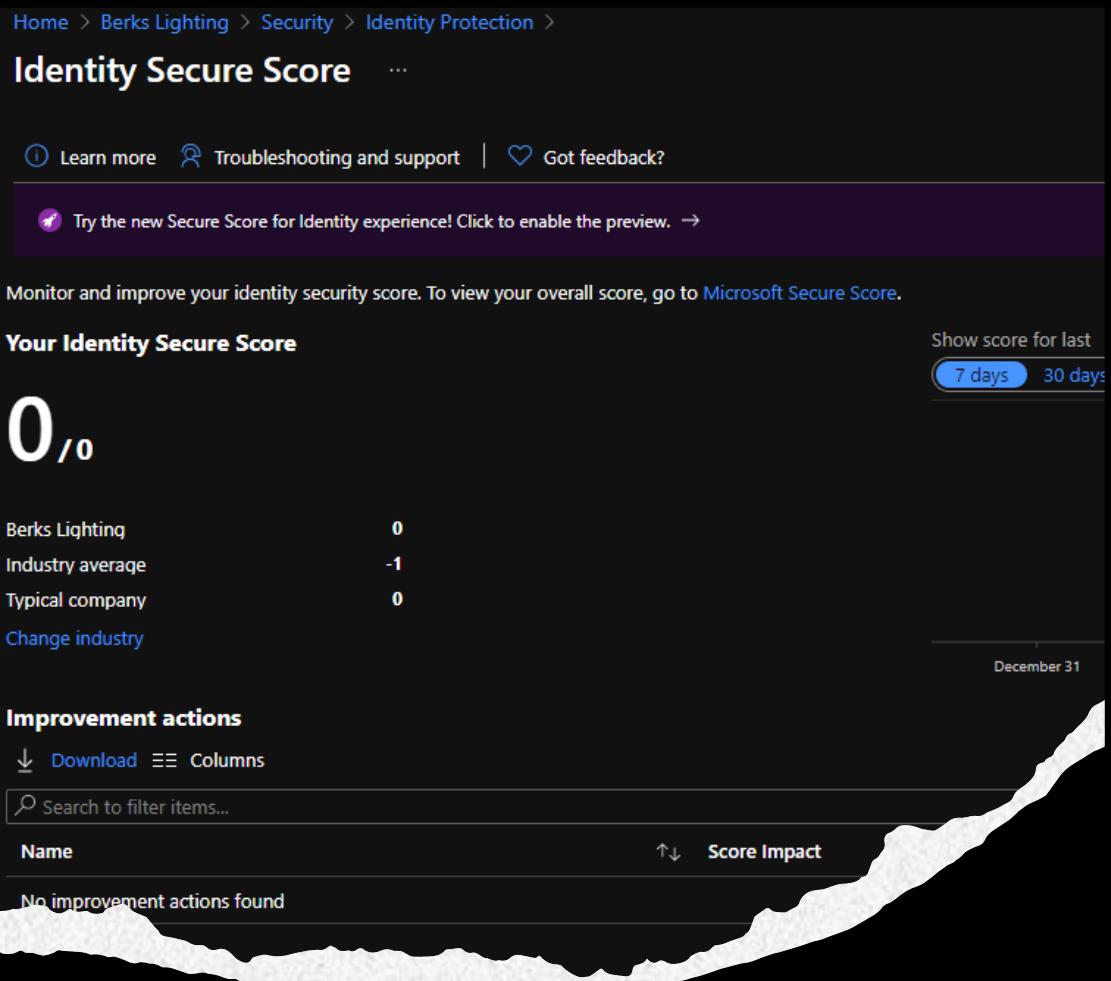
- Anonymous IP address
- Atypical travel
- **Malware linked IP address**
- Unfamiliar sign-in properties
- Leaked Credentials
- Password spray
- New country
- Activity from anonymous IP address
- Suspicious inbox forwarding



# Azure Identity Protection

Identifies the following types of risks:

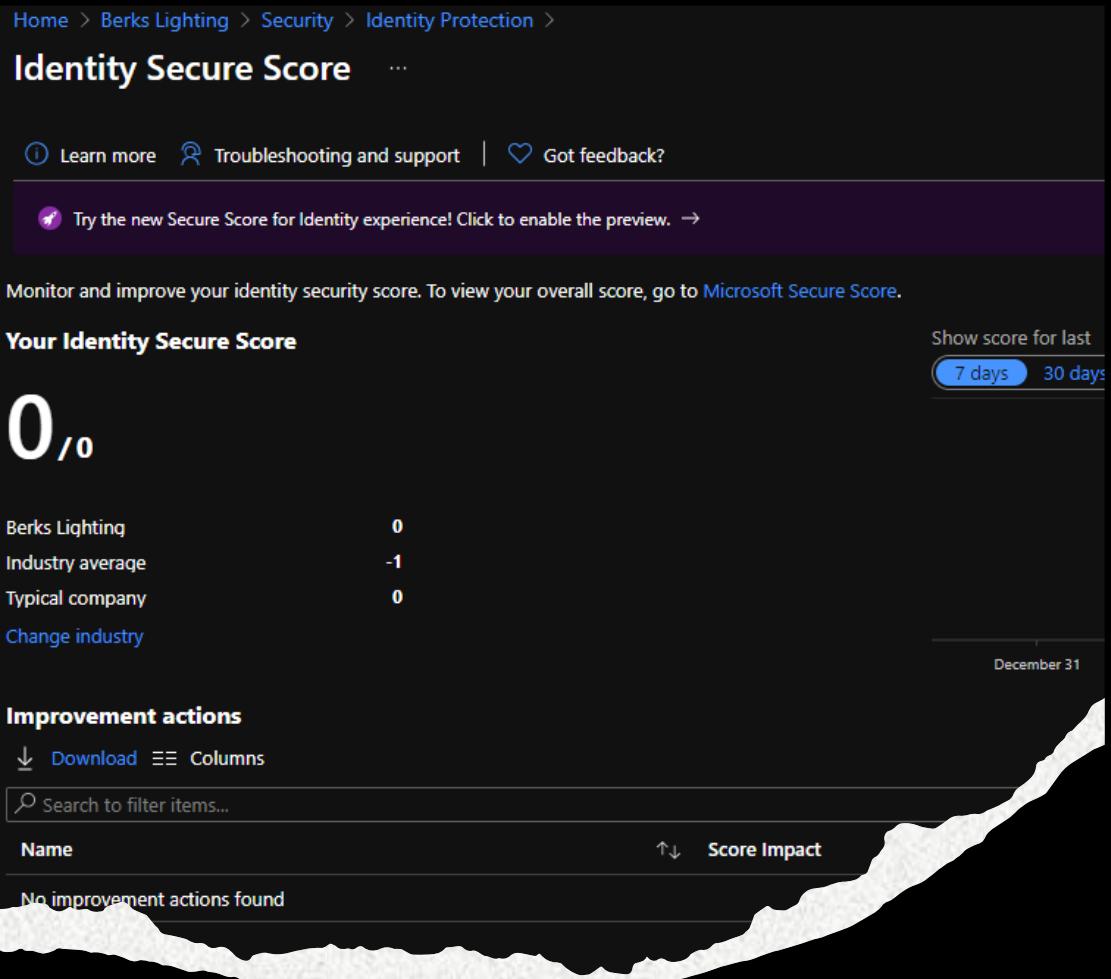
- Anonymous IP address
- Atypical travel
- Malware linked IP address
- **Unfamiliar sign-in properties**
- Leaked Credentials
- Password spray
- New country
- Activity from anonymous IP address
- Suspicious inbox forwarding



# Azure Identity Protection

Identifies the following types of risks:

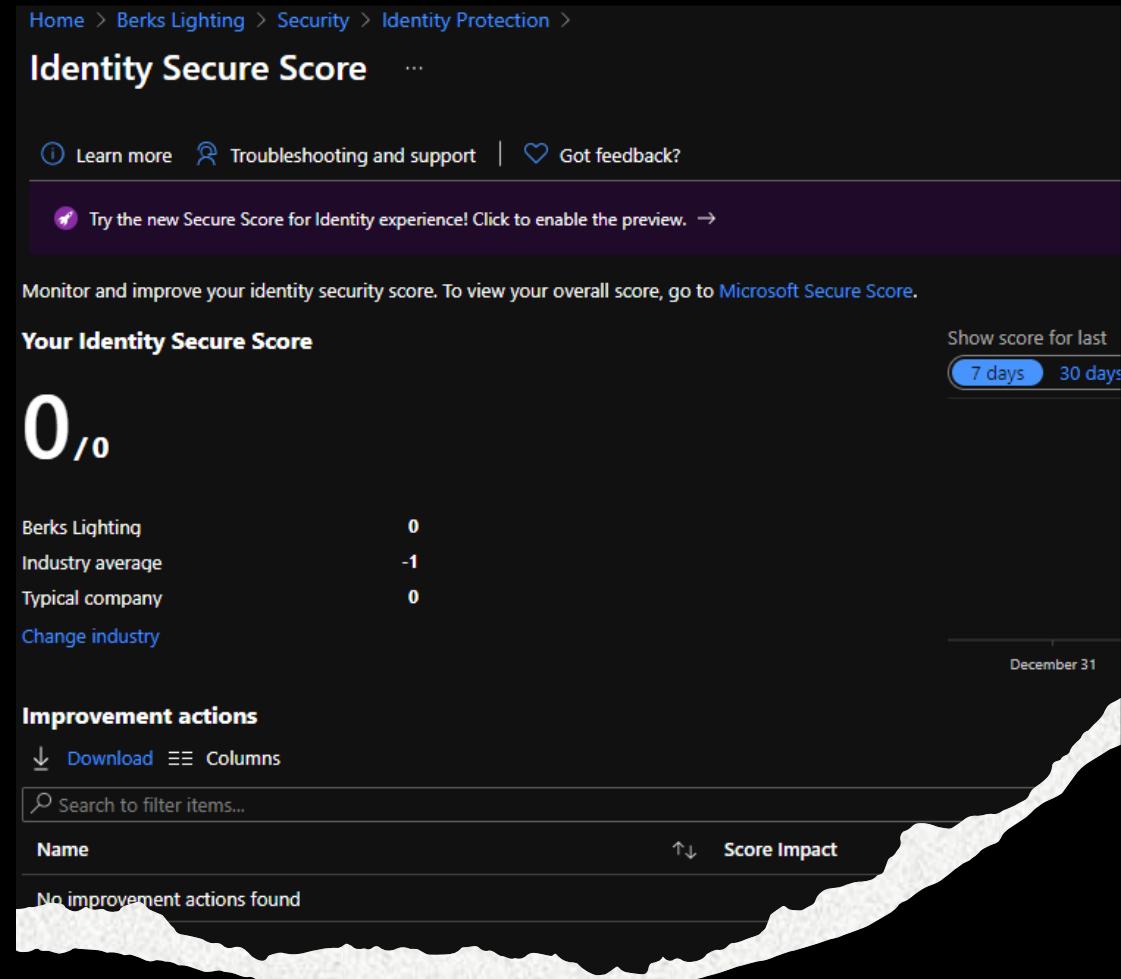
- Anonymous IP address
- Atypical travel
- Malware linked IP address
- Unfamiliar sign-in properties
- **Leaked Credentials**
- Password spray
- New country
- Activity from anonymous IP address
- Suspicious inbox forwarding



# Azure Identity Protection

Identifies the following types of risks:

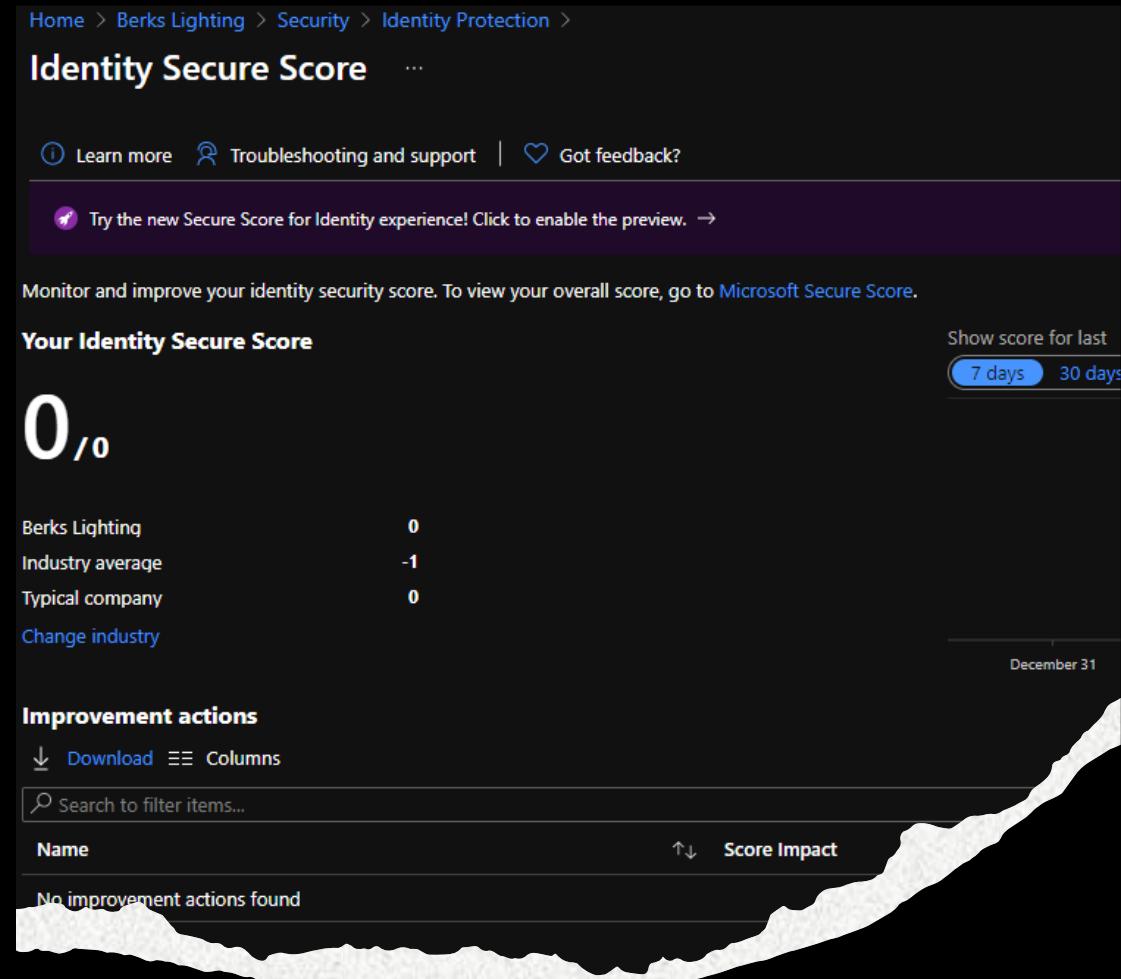
- Anonymous IP address
- Atypical travel
- Malware linked IP address
- Unfamiliar sign-in properties
- Leaked Credentials
- **Password spray**
- New country
- Activity from anonymous IP address
- Suspicious inbox forwarding



# 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



## Identity Secure Score

... more [Troubleshooting and support](#) | [Got feedback?](#)

New Secure Score for Identity experience! Click to enable the preview. →

Improve your identity security score. To view your overall score, go to [Microsoft Secure Score](#).

### Secure Score

Show score for last

7 days 30 days 60 days 90 days

# Azure Identity Protection

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

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

0  
-1  
0

December 31

### Next actions

... Columns

No filter items...

↑↓ Score Impact

Improvement actions found

Search (Ctrl+ /)

## Documentation

Azure Active Directory offers a range

- Azure AD Conditional Access
- Azure AD Identity Protection
- Azure Security Center
- Identity Secure Score
- Named locations
- Authentication methods
- Multi Factor Authentication



## Security guides

For a strong se

- 5 step
- A

# Azure Identity Protection

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

- Risky users
- Risky sign-ins
- Risk detections

## Protect

Conditional Access

Identity Protection

Security Center

Continuous access evaluation (Pr...)

## Manage

Identity Secure Score

Named locations

Authentication methods

MFA

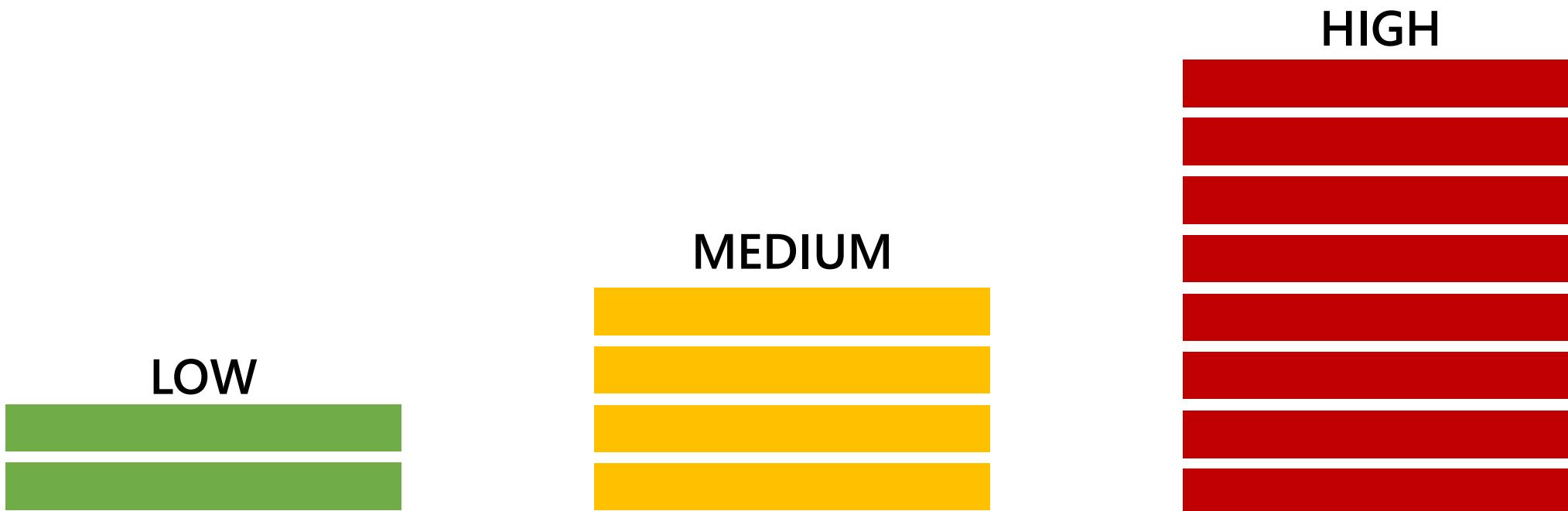
## Report

Risky users

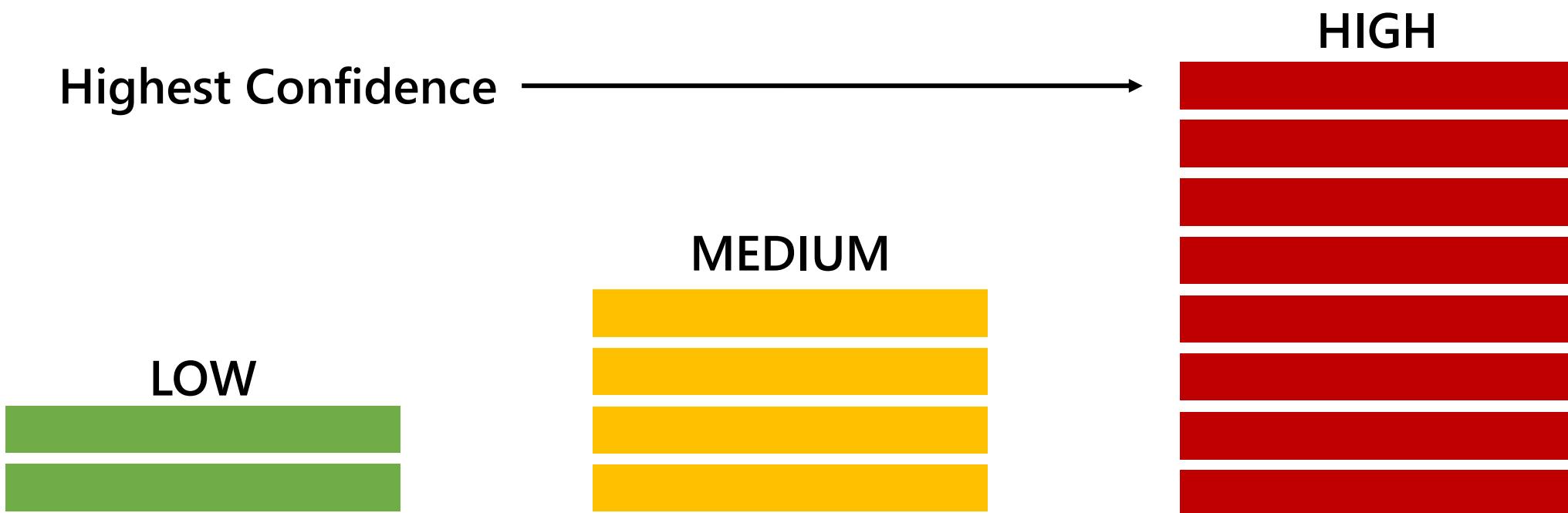
Risky sign-ins

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
<b>Global administrator</b>	Full access to Identity Protection	
<b>Security administrator</b>	Full access to Identity Protection	Reset password for a user
<b>Security operator</b>	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
<b>Security reader</b>	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
<b>Global administrator</b>	Full access to Identity Protection	
<b>Security administrator</b>	Full access to Identity Protection	Reset password for a user
<b>Security operator</b>	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
<b>Security reader</b>	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



## Tenant information

Your role

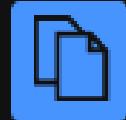
Global administrator [More info](#)

License

Azure AD Premium P2

Tenant ID

cc65cb19-4793-46ba-b126-157f...



Primary domain

berkslighting.com

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

[Overview](#)

Date range = **30 days**

[Diagnose and solve problems](#)

**Protect**

New risky users detected <sup>1</sup>

User risk level = **All**

Identity Secure Score <sup>1</sup>  
/-

[User risk policy](#)

[Sign-in risk policy](#)

[MFA registration policy](#)

**Report**

[Risky users](#)

[Risky sign-ins](#)

[Risk detections](#)

**Notify**

[Users at risk detected alerts](#)

[Weekly digest](#)

**Troubleshooting + Support**

New risky sign-ins detected <sup>0</sup>

Sign-in risk type = **Real-time**

Sign-in risk level = **All**

This screenshot shows the Azure Identity Protection portal. It includes sections for Protect (with a count of 1 new risky user), Report (listing Risky users, Risky sign-ins, and Risk detections), Notify (listing Users at risk detected alerts and Weekly digest), and Troubleshooting + Support (listing New risky sign-ins detected). The main area displays a chart titled 'Count' with four data points: 01/31 (blue bar), 02/07 (orange bar), 02/14 (green bar), and 02/21 (yellow bar). A callout box highlights the 'Identity Secure Score' with a value of '1/-'. The 'Sign-in risk type' is set to 'Real-time' and 'Sign-in risk level' is set to 'All'.

# 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



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

Image Users Groups Global identities Local administrators Delegated units Applications

## 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... [Edit](#)  
Primary domain: berksbatteries.com

**Azure AD Connect**

Status: Not enabled  
Last sync: Sync has never run

# Identity Protection Policies

## Policy name

Multi-factor authentication registration policy

## Assignments



All users



## Controls



Require Azure MFA registration



MFA Registration Policy only affects cloud-based Azure MFA. If you have MFA Server it will not be affected.

## Enforce Policy

On

Off

## Policy name

User risk remediation policy

## Assignments



All users



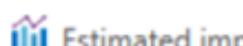
User risk

## Controls



Require password ch

## Review



Number of users im

## Enforce Policy

On

Off

## Policy name

Sign-in risk remediation policy

## Enforce Policy

On

Off

# 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

Search (Ctrl+ /) <

Overview

Diagnose and solve problems

**Protect**

User risk policy

Sign-in risk policy

**MFA registration policy**

**Report**

Risky users

Risky sign-ins

Risk detections

**Notify**

Users at risk detected alerts

Weekly digest

Troubleshooting + Support

Virtual assistant (Preview)

Troubleshoot

New support request

Policy Name  
Multi-factor authentication registration policy

Assignments

Users

All users

Controls

Require Azure AD MFA registration

**i** MFA registration policy only affects cloud-based services

Enforce 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.

Identity Protection | User risk policy

Search (Ctrl+ /) <>

Policy Name  
User risk remediation policy

Assignments

Users  
All users

User risk ①  
Low and above

Protect

User risk policy (selected)

Sign-in risk policy

MFA registration policy

Report

Risky users

Risky sign-ins

Risk detections

Notify

Users at risk detected alerts

Weekly digest

Troubleshooting + Support

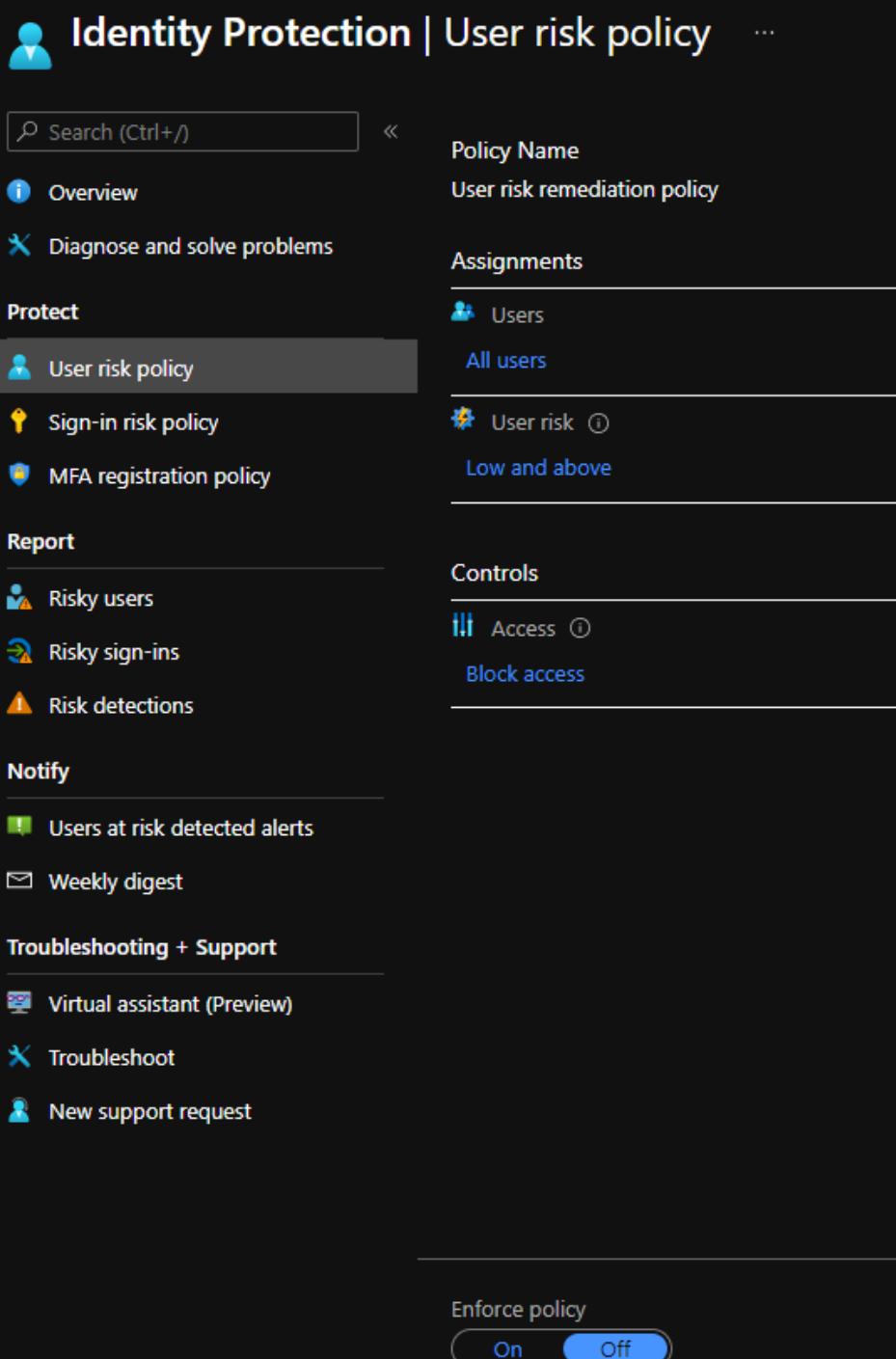
Virtual assistant (Preview)

Troubleshoot

New support request

Enforce policy

On Off



Search (Ctrl+ /) <

**Overview**

**Diagnose and solve problems**

**Protect**

User risk policy

**Sign-in risk policy**

MFA registration policy

**Report**

Risky users

Risky sign-ins

Risk detections

**Notify**

Users at risk detected alerts

Weekly digest

**Troubleshooting + Support**

Virtual assistant (Preview)

Troubleshoot

New support request

Policy Name  
Sign-in risk remediation policy

Assignments

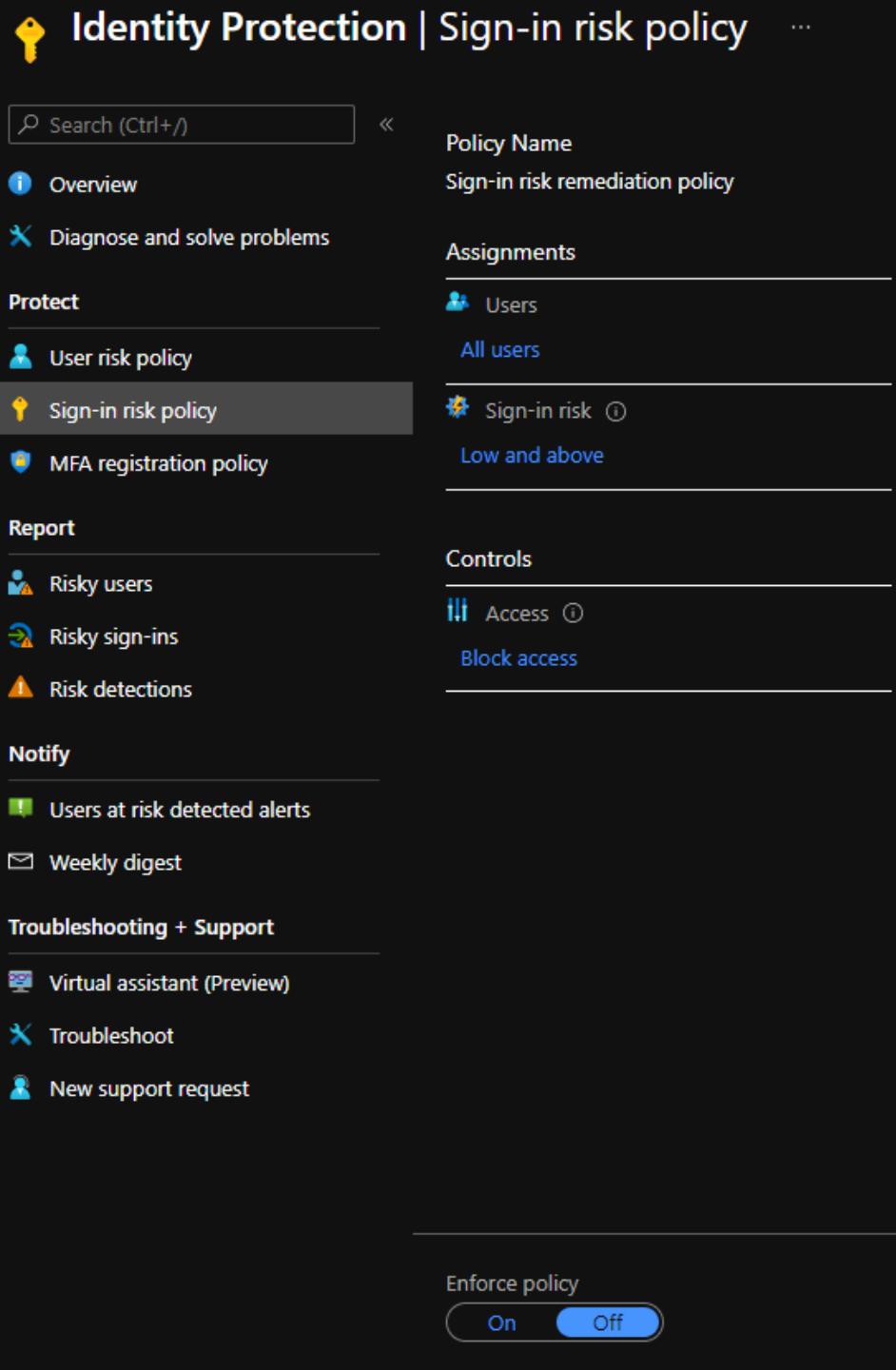
Users  
All users

Sign-in risk  
Low and above

Controls

Access  
Block access

Enforce policy  
**On** Off



# 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

Control user access to respond to sign-in risk levels. [Learn more](#)

Configure ⓘ

Yes

No

Select the sign-in risk level this policy will apply to

High

Medium

Low

No risk

# Custom Conditional Access Policy

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

## New

Conditional access policy

Control user access based on conditional access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name \*

Example: 'Device compliance app policy'

### Assignments

Users and groups ⓘ

0 users and groups selected

Cloud apps or actions ⓘ

No cloud apps or actions selected

Conditions ⓘ

0 conditions selected

### Access controls

Grant ⓘ

0 controls selected

Session ⓘ

0 controls selected

### Enable policy

Report-only

On

Off

Create

Control user access based on signals from conditions like risk, device platform, location, client apps, or device state. [Learn more](#)

User risk ⓘ

Not configured

Sign-in risk ⓘ

Not configured

Device platforms ⓘ

Not configured

Locations ⓘ

Not configured

Client apps ⓘ

Not configured

Device state (Preview) ⓘ

Not configured

Select

# 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

Image Users Groups External identities Global administrators Delegated administrators Delegated units Applications

**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... [Edit](#)  
Primary domain: berksbatteries.com

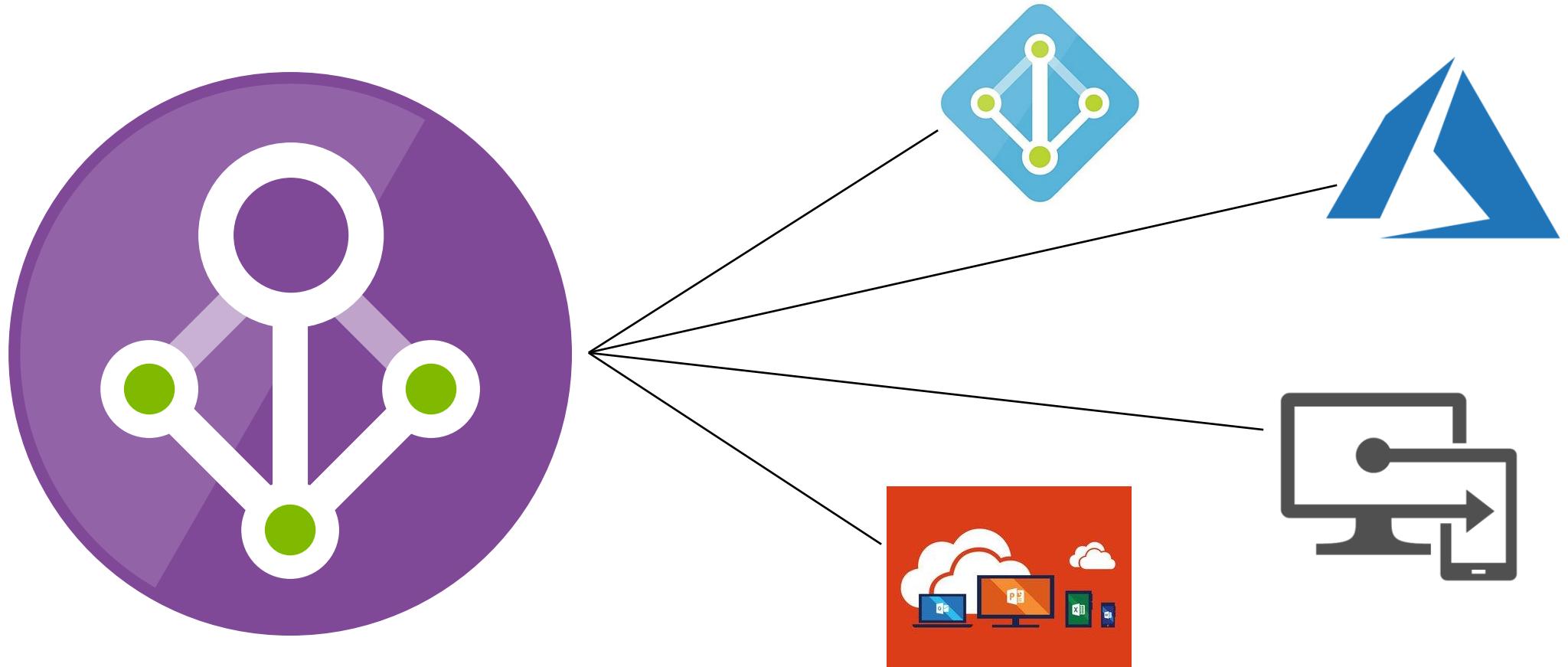
**Azure AD Connect**

Status: Not enabled  
Last sync: Sync has never run

# Azure AD PIM

# Privileged Identity Management

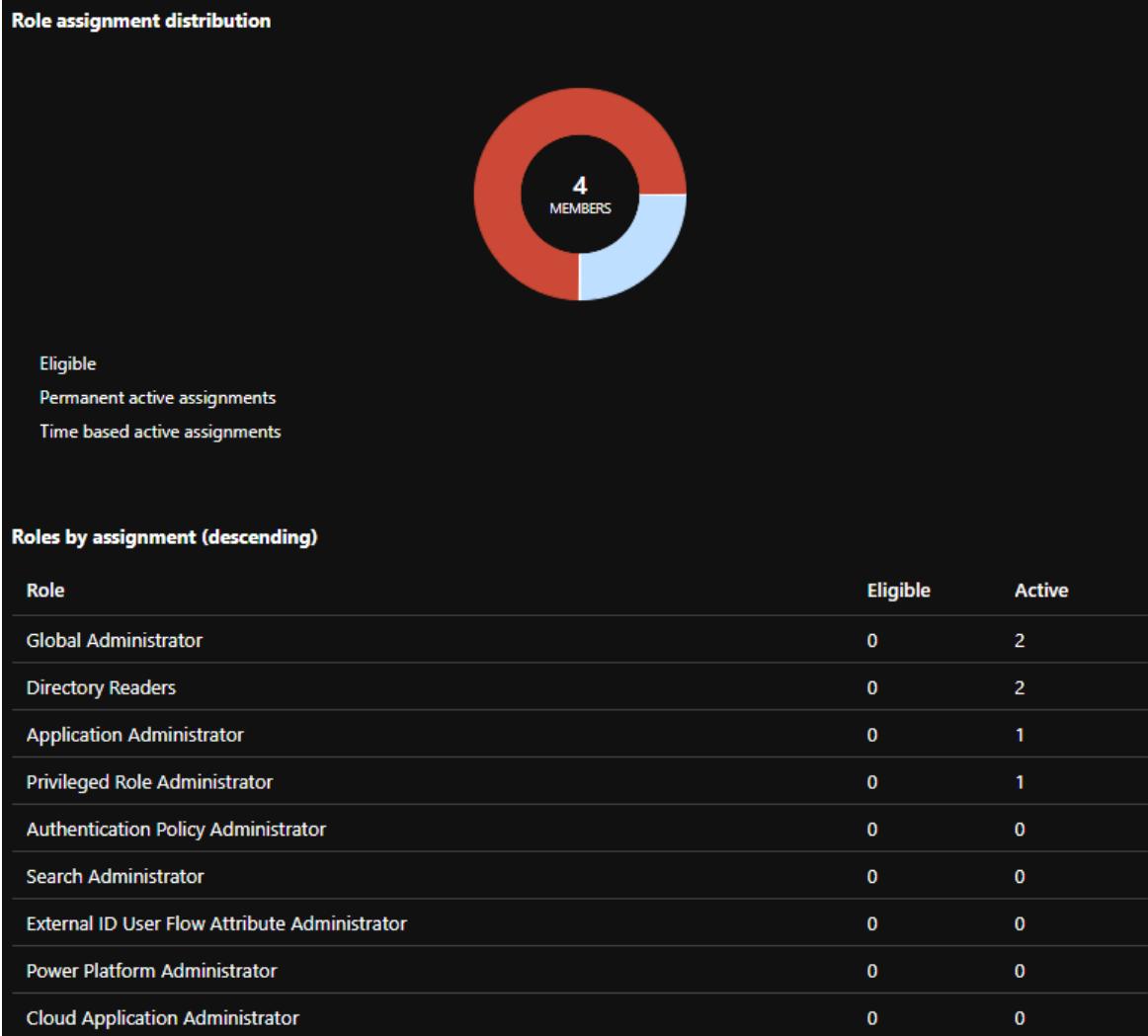
Privileged Identity Management is an Azure AD service that is used to manage, control, and monitor access to critical resources.



# PIM Use Cases

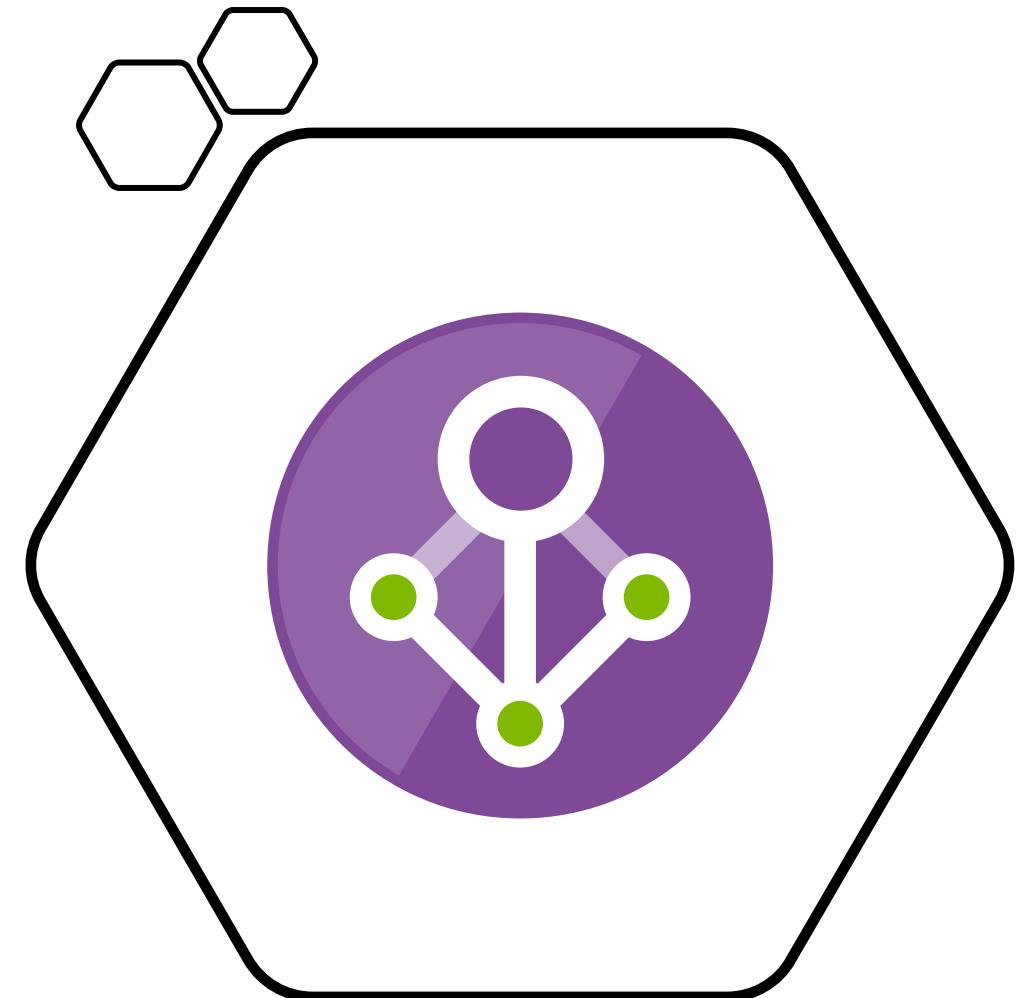
PIM is useful to organizations that want to minimize the number of people who have access to critical information or resources.

- 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



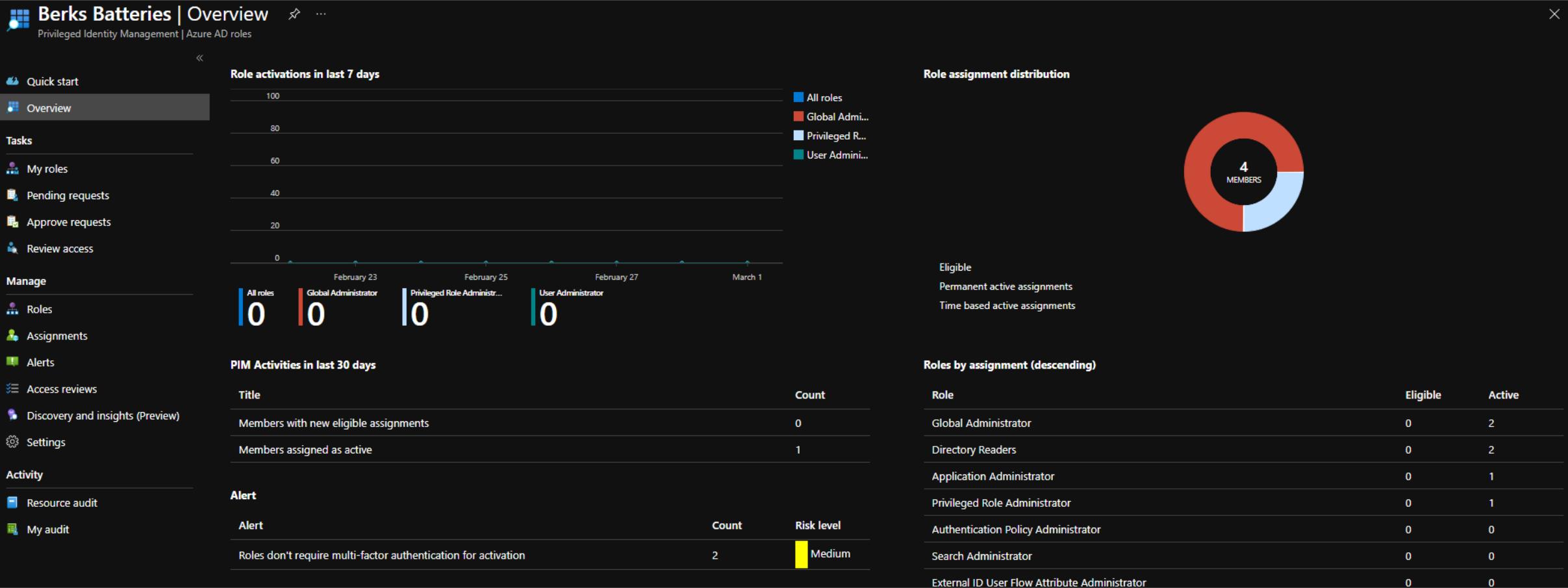
# Privileged Identity Management

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

The screenshot shows the 'Berks Batteries | Quick start' page for Azure AD PIM. The left sidebar has 'Quick start' selected. The main area title is 'Privileged Identity Management'. It includes a sub-header: 'Azure AD PIM is a Premium feature that enables you to limit standing admin access to privileged roles and much more. [Learn more](#)'. Below this are four cards:

- Assign**: Assign users or current admins as eligible admins for specific Azure AD roles, so that they only have access when necessary.
- Activate**: Activate your eligible admin roles so that you can get limit standing access to the privileged identity.
- Approve**: View and approve all activation request for specific Azure AD roles that you are configured to approve.
- Audit**: View and export a history of all privileged identity assignments and activations so you can identify attacks and stay compliant.

At the bottom are four buttons: 'Assign Eligibility', 'Activate your role', 'Approve requests', and 'View your history'.



# 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

Quick start

Overview

Tasks

My roles

Pending requests

Approve requests

Review access

Manage

Roles

Assignments

Alerts

Access reviews

Discovery and insights (Preview)

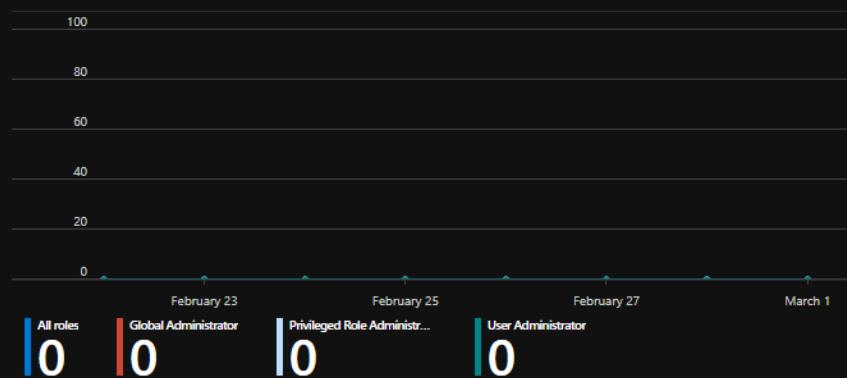
Settings

Activity

Resource audit

My audit

## Role activations in last 7 days



## Role assignment distribution

- All roles
- Global Adminstr...
- Privileged R...
- User Administr...



Eligible

Permanent active assignments

Time based active assignments

## PIM Activities in last 30 days

Title	Count
Members with new eligible assignments	0
Members assigned as active	1

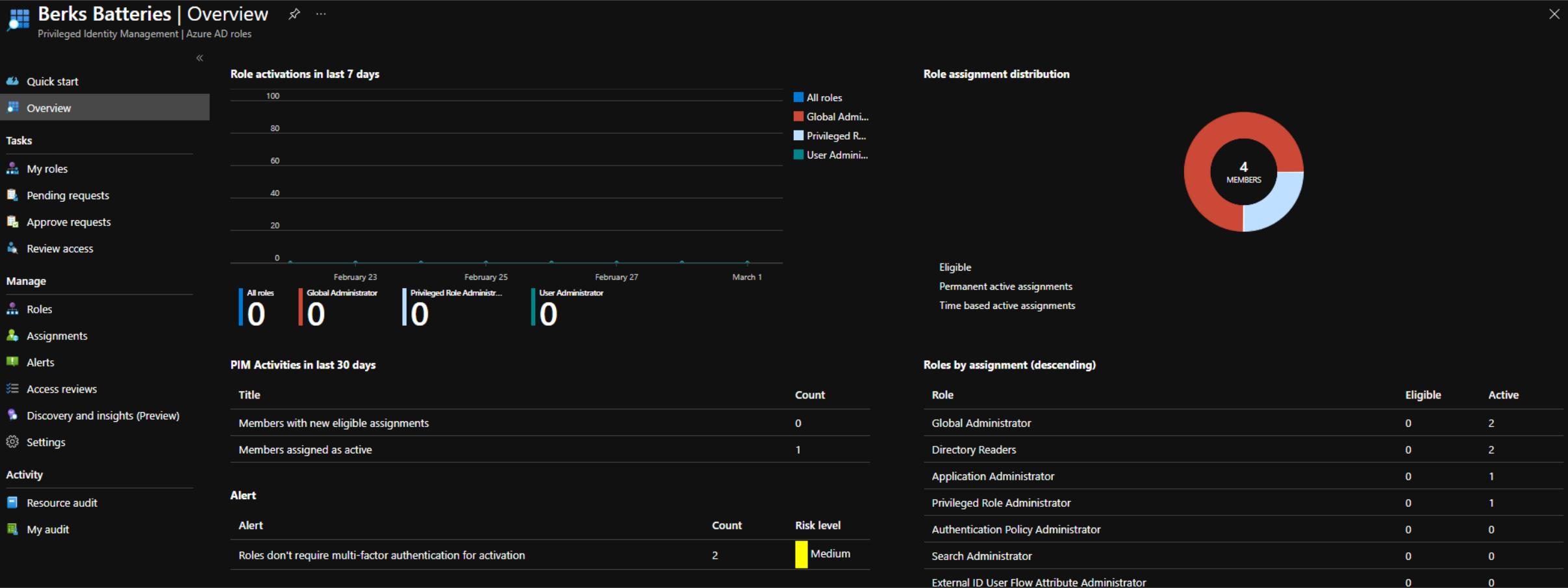
## Roles by assignment (descending)

Role	Eligible	Active
Global Administrator	0	2
Directory Readers	0	2
Application Administrator	0	1
Privileged Role Administrator	0	1
Authentication Policy Administrator	0	0
Search Administrator	0	0
External ID User Flow Attribute Administrator	0	0

## 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
<b>eligible</b>	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.
<b>active</b>	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.
<b>activate</b>		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.
<b>assigned</b>	State	A user that has an active role assignment.
<b>activated</b>	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.
<b>permanent eligible</b>	Duration	A role assignment where a user is always eligible to activate the role.
<b>permanent active</b>	Duration	A role assignment where a user can always use the role without performing any actions.
<b>expire eligible</b>	Duration	A role assignment where a user is eligible to activate the role within a specified start and end date.
<b>expire active</b>	Duration	A role assignment where a user can use the role without performing any actions within a specified start and end date.
<b>just-in-time (JIT) access</b>		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.
<b>principle of least privilege access</b>		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.

&lt;&lt;

Quick start

Overview

## Tasks

My roles

Pending requests

Approve requests

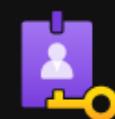
Review access

## Manage

Roles

Assignments

Alerts



## Privileged Identity Management

Azure AD PIM is a Premium feature that enables you to limit standing admin access to privileged roles and much more. [Learn more](#)



### Assign

Assign users or current admins as eligible admins for specific Azure AD roles, so that they only have access when necessary



### Activate

Activate your eligible admin roles so that you can get limit standing access to the privileged identity



### Approve

View and approve all activation request for specific Azure AD roles that you are configured to approve



### Audit

View and export a history of all privileged identity assignments and activations so you can identify attacks and stay compliant

[Assign Eligibility](#)[Activate your role](#)[Approve requests](#)[View your history](#)

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



Berks Batteries | Overview  
Azure Active Directory

Switch tenant Delete tenant + Create a tenant What's new Preview features Got feedback?

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... [Copy](#)  
Primary domain: berksbatteries.com

**Azure AD Connect**

Status: Not enabled  
Last sync: Sync has never run

# 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.

Home > Berks Batteries > Devices

## Devices | Device settings

Berks Batteries - Azure Active Directory

« Save X Discard | Got feedback?

All devices

Device settings (Selected)

Enterprise State Roaming

BitLocker keys (Preview)

Diagnose and solve problems

Activity

Audit logs

Bulk operation results (Preview)

Troubleshooting + Support

New support request

Users may join devices to Azure AD ⓘ

All Selected None

Selected  
1 member selected

Users may register their devices with Azure AD ⓘ

All None

i Learn more on how this setting works

Devices to be Azure AD joined or Azure AD registered require Multi-Factor Authentication ⓘ

Yes No

Maximum number of devices per user ⓘ

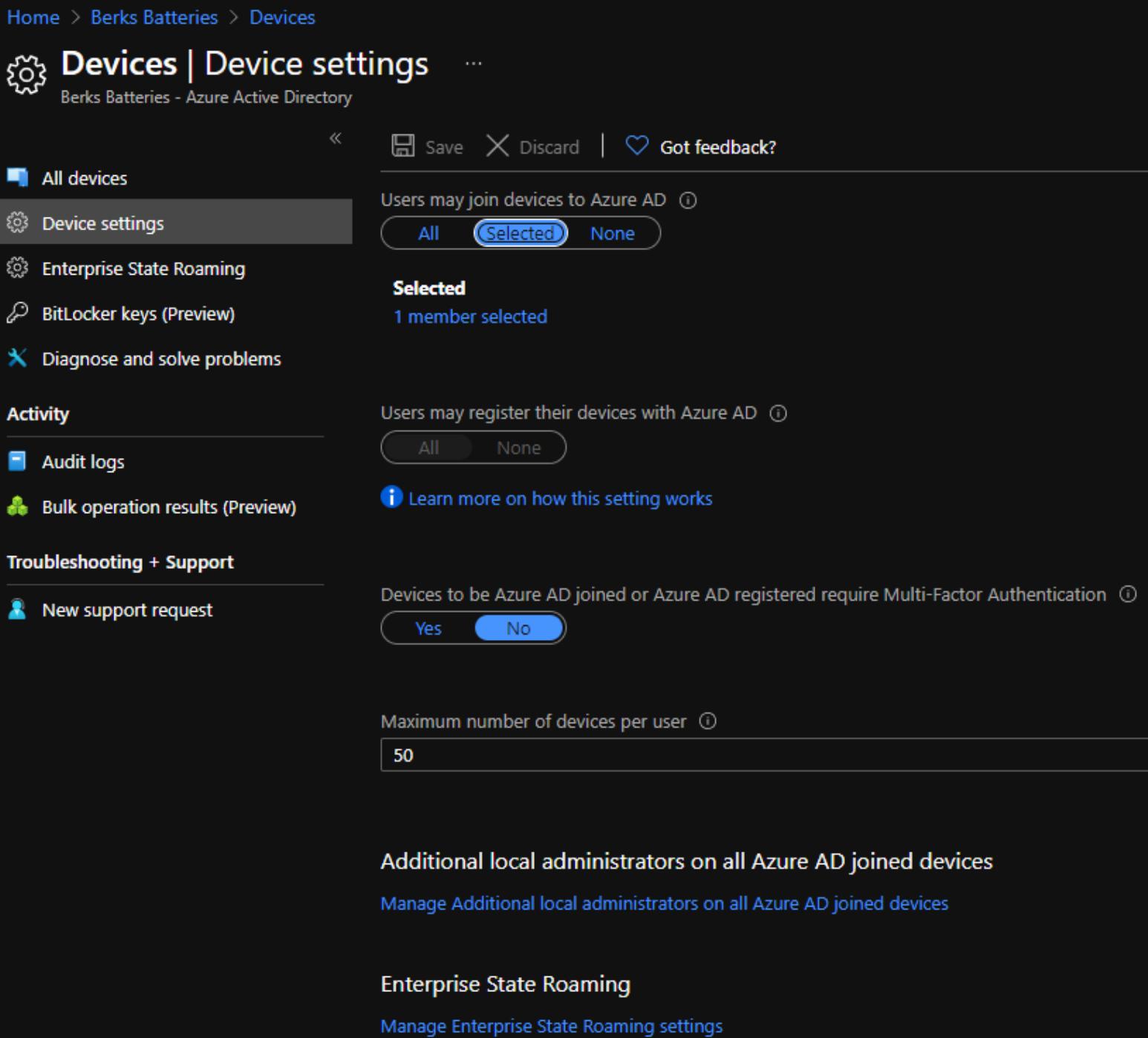
50

Additional local administrators on all Azure AD joined devices

Manage Additional local administrators on all Azure AD joined devices

Enterprise State Roaming

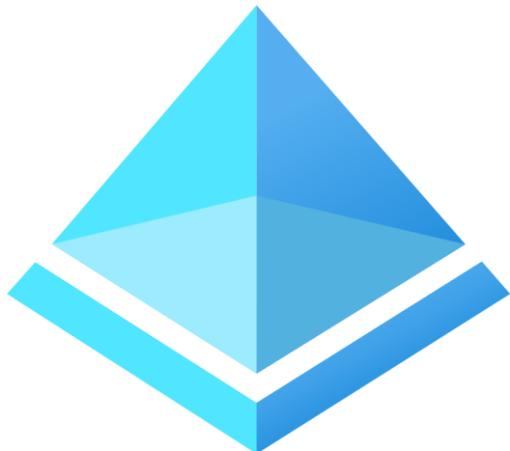
Manage Enterprise State Roaming settings



# 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

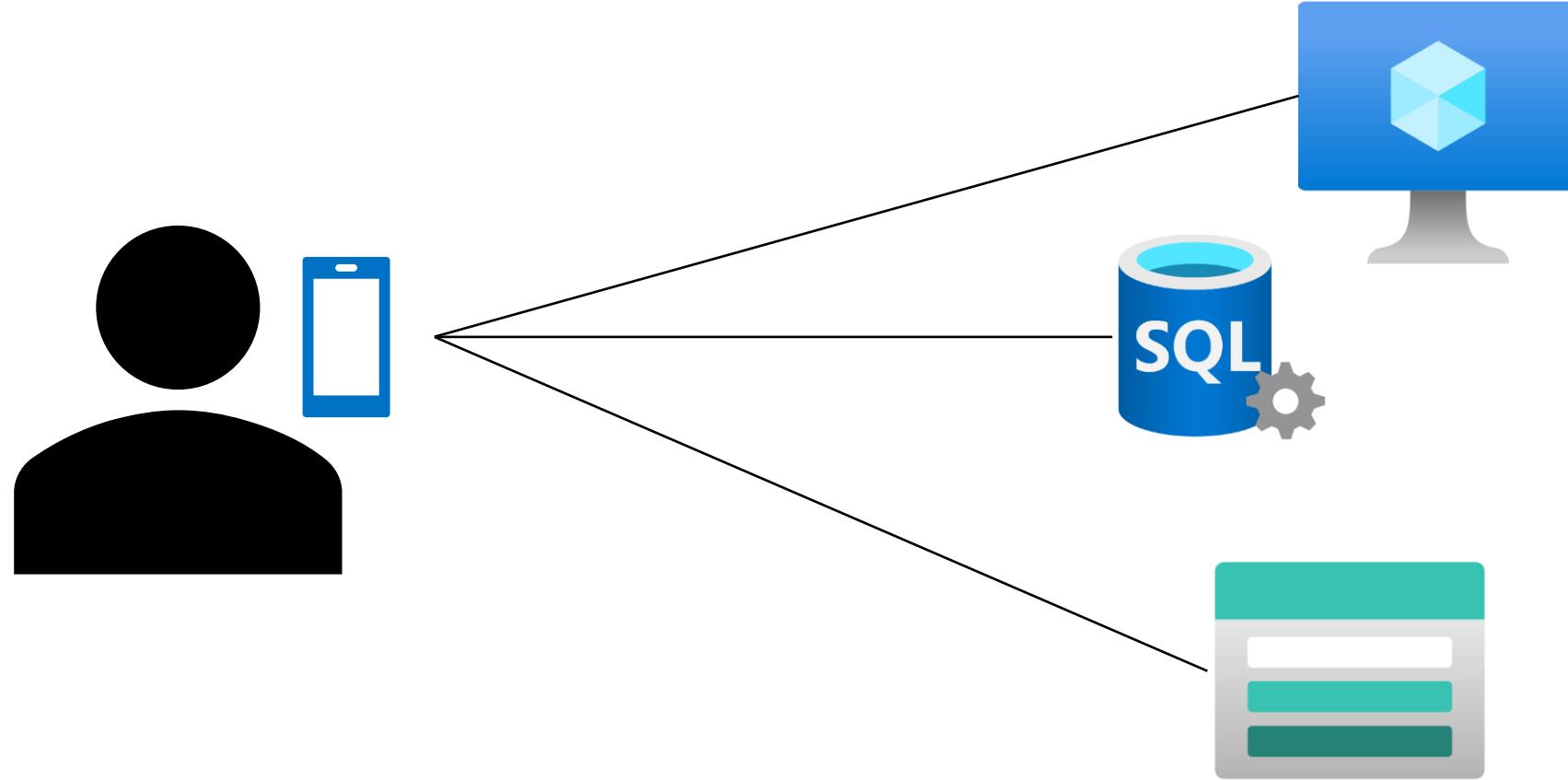
**There are two ways to manage  
devices in Azure AD:**

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



# Azure AD Registered Devices

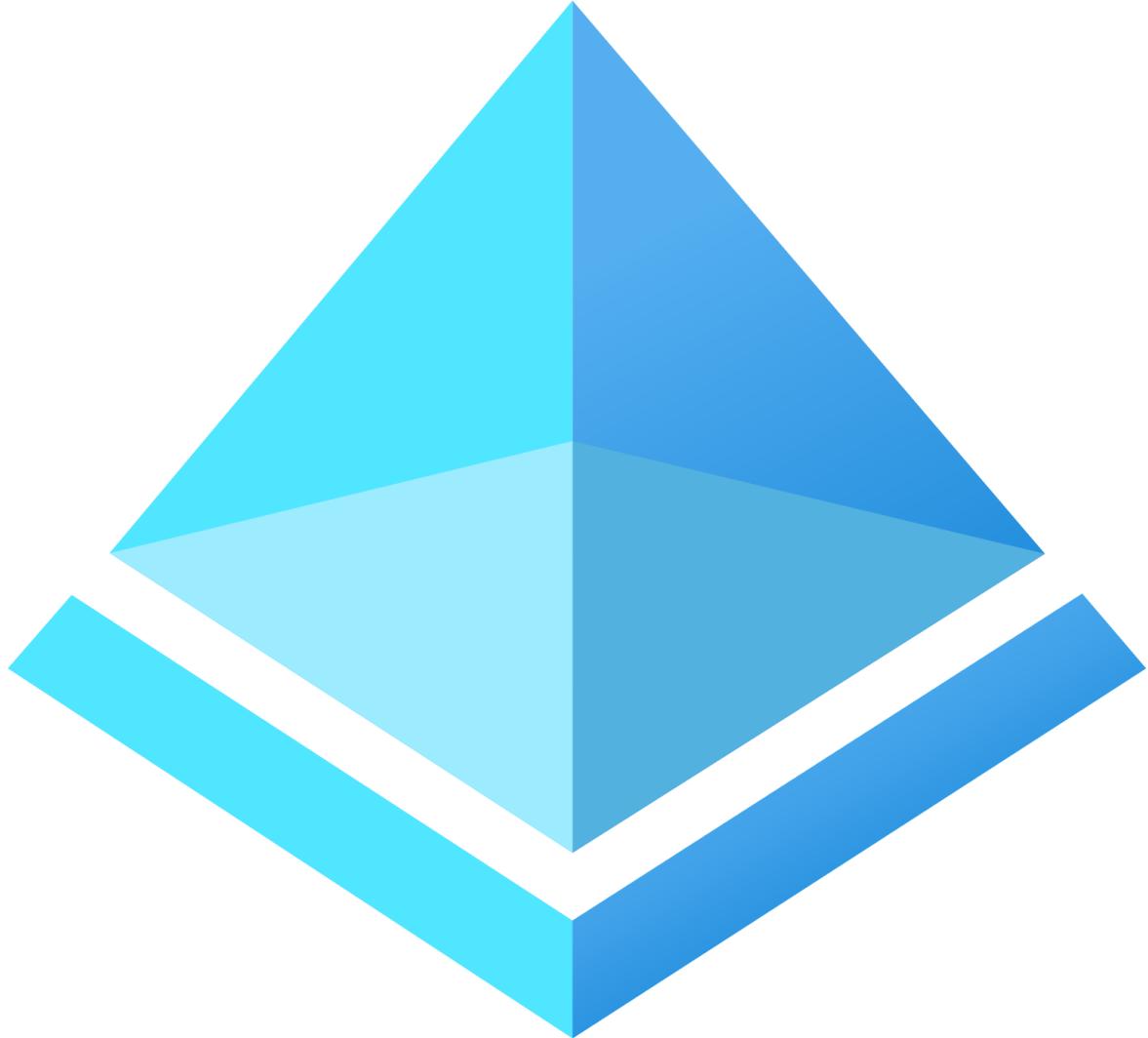
Azure AD Registered devices allow organizations to support BYOD scenarios.



# 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.





Berks Batteries | Overview  
Azure Active Directory

Switch tenant Delete tenant + Create a tenant What's new Preview features Got feedback?

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... [Edit](#)  
Primary domain: berksbatteries.com

**Azure AD Connect**

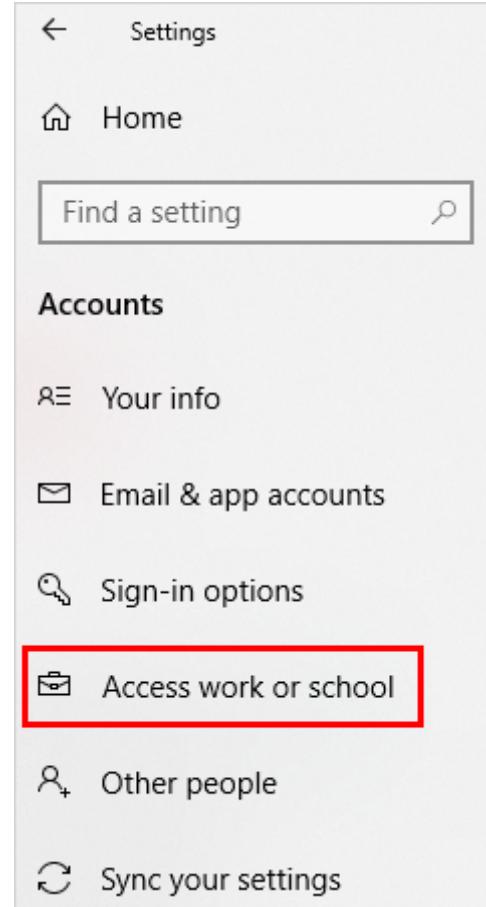
Status: Not enabled  
Last sync: Sync has never run

# Azure AD Registered Devices

# Azure AD Registered Devices

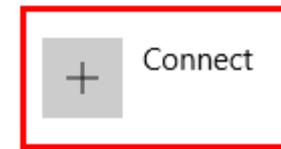
Azure AD registered devices allow organizations to support BYOD scenarios.

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



## Access work or school

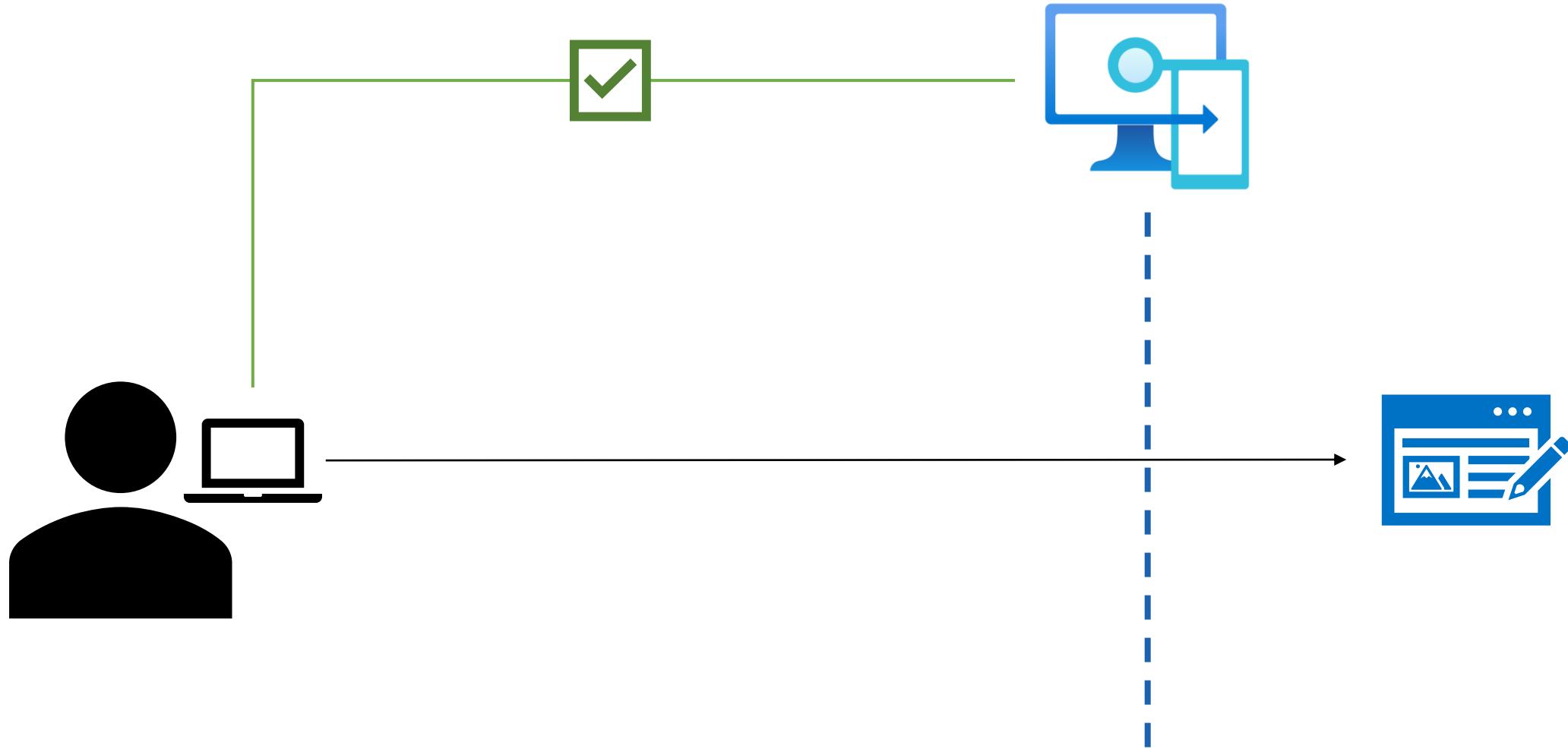
Get access to resources like email, apps, and the  
Connecting means your work or school might co  
on this device, such as which settings you can ch  
info about this, ask them.



# Azure AD Registered Devices

<b>Definition</b>	Registered to Azure AD without requiring organizational account to sign in to the device
<b>Primary audience</b>	<ul style="list-style-type: none"><li>• Applicable to all users with the following criteria:</li><li>• --Bring your own device (BYOD) &amp; Mobile devices</li></ul>
<b>Device ownership</b>	User or Organization
<b>Operating systems</b>	Windows 10, iOS, Android, and macOS
<b>Provisioning</b>	<ul style="list-style-type: none"><li>• Windows 10 – Settings</li><li>• iOS/Android – Company Portal or Microsoft Authenticator app</li><li>• macOS – Company Portal</li></ul>
<b>Device sign in options</b>	<ul style="list-style-type: none"><li>• End-user local credentials</li><li>• Password</li><li>• Windows Hello</li><li>• PIN</li><li>• Biometrics or Pattern for other devices</li></ul>
<b>Device management</b>	<ul style="list-style-type: none"><li>• Mobile Device Management (example: Microsoft Intune) / Mobile Application Management</li></ul>
<b>Key capabilities</b>	<ul style="list-style-type: none"><li>• SSO to cloud resources</li><li>• Conditional Access when enrolled into Intune</li><li>• Conditional Access via App protection policy</li><li>• Enables Phone sign in with Microsoft Authenticator app</li></ul>

# Azure AD Registered Devices





Berks Batteries | Overview  
Azure Active Directory

Switch tenant Delete tenant + Create a tenant What's new Preview features Got feedback?

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... [Edit](#)  
Primary domain: berksbatteries.com

**Azure AD Connect**

Status: Not enabled  
Last sync: Sync has never run

# 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.

Home > Berks Batteries > Devices

## Devices | Device settings

Berks Batteries - Azure Active Directory

« Save X Discard | Got feedback?

All devices

Device settings (Selected)

Enterprise State Roaming

BitLocker keys (Preview)

Diagnose and solve problems

Activity

Audit logs

Bulk operation results (Preview)

Troubleshooting + Support

New support request

Users may join devices to Azure AD ⓘ

All Selected None

Selected  
1 member selected

Users may register their devices with Azure AD ⓘ

All None

i Learn more on how this setting works

Devices to be Azure AD joined or Azure AD registered require Multi-Factor Authentication ⓘ

Yes No

Maximum number of devices per user ⓘ

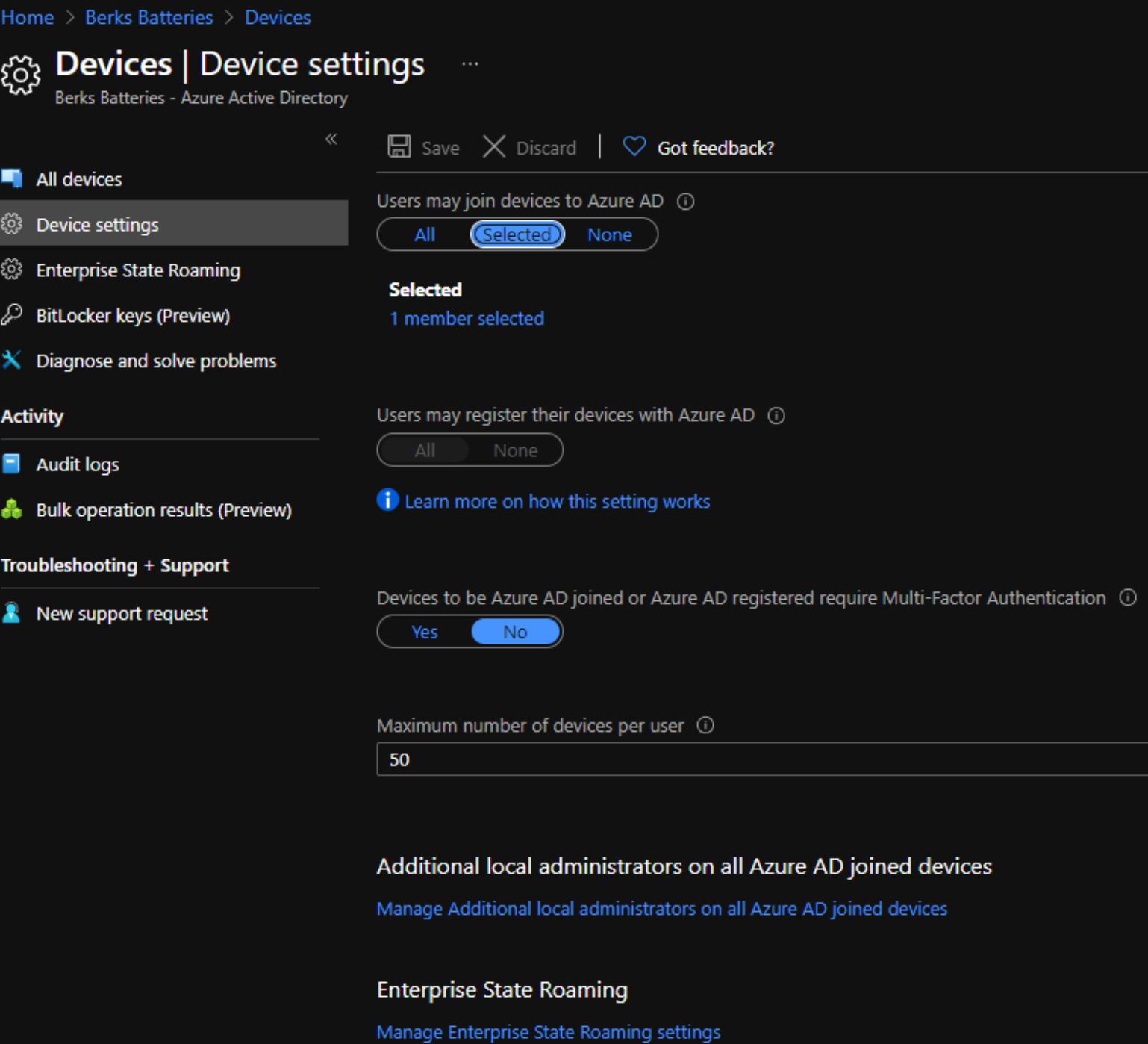
50

Additional local administrators on all Azure AD joined devices

Manage Additional local administrators on all Azure AD joined devices

Enterprise State Roaming

Manage Enterprise State Roaming settings



# Azure AD Joined Devices

---

<b>Definition</b>	Joined only to Azure AD requiring organizational account to sign into the device
<b>Primary audience</b>	<ul style="list-style-type: none"><li>• Suitable for both cloud-only and hybrid organizations</li><li>• Applicable to all users in an organization</li></ul>
<b>Device ownership</b>	Organization
<b>Operating systems</b>	<ul style="list-style-type: none"><li>• All Windows 10 devices except Windows 10 Home</li><li>• Windows Server 2019 Virtual Machines running in Azure (Server core is not supported)</li></ul>
<b>Provisioning</b>	<ul style="list-style-type: none"><li>• Self-service: Windows OOBE or Settings</li><li>• Bulk enrollment</li><li>• Windows Autopilot</li></ul>
<b>Device sign in options</b>	<ul style="list-style-type: none"><li>• Organizational accounts using:<ul style="list-style-type: none"><li>--Password, Windows Hello for Business, FIDO2.0 security keys (preview)</li></ul></li></ul>
<b>Device management</b>	<ul style="list-style-type: none"><li>• Mobile Device Management (example: Microsoft Intune)</li><li>• Co-management with Microsoft Intune and Microsoft Endpoint Configuration Manager</li></ul>
<b>Key capabilities</b>	<ul style="list-style-type: none"><li>• SSO to both cloud and on-premises resources</li><li>• Conditional Access through MDM enrollment and MDM compliance evaluation</li><li>• Self-service Password Reset and Windows Hello PIN reset on lock screen</li><li>• Enterprise State Roaming across devices</li></ul>

 **Devices | Device settings** ...

Berks Batteries - Azure Active Directory

Save Discard Got feedback?

All devices

 **Device settings**

Selected

Users may join devices to Azure AD ⓘ

All Selected None

1 member selected

Enterprise State Roaming

BitLocker keys (Preview)

Diagnose and solve problems

---

**Activity**

 Audit logs

 Bulk operation results (Preview)

---

**Troubleshooting + Support**

New support request

Devices to be Azure AD joined or Azure AD registered require Multi-Factor Authentication.

Yes No

Maximum number of devices per user ⓘ

50

Additional local administrators on all Azure AD joined devices.

Manage Additional local administrators on all Azure AD joined devices

Enterprise State Roaming

Manage Enterprise State Roaming

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.

The screenshot shows the 'Device settings' page in the Azure Active Directory portal. The left sidebar lists several sections: 'Devices' (selected), 'Device settings' (highlighted in grey), 'Enterprise State Roaming', 'BitLocker keys (Preview)', and 'Diagnose and solve problems'. The main content area has three main sections:

- Users may join devices to Azure AD**: A button group with 'All' (greyed out), 'Selected' (blue outline), and 'None'.
- Selected**: Shows '1 member selected'.
- Users may register their devices with Azure AD**: A button group with 'All' (greyed out) and 'None'.

A callout box points to the 'Selected' button with the text: 'Learn more on how this setting works'.

Below these sections, there's a note: 'Devices to be Azure AD joined or Azure AD registered require Multi-Factor Authentication'. A button group shows 'Yes' (greyed out) and 'No' (blue outline).

Other settings include:

- Maximum number of devices per user**: Set to 50.
- Additional local administrators on all Azure AD joined devices**: A link to 'Manage Additional local administrators on all Azure AD joined devices'.
- Enterprise State Roaming**: A link to 'Manage Enterprise State Roaming settings'.

# 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

The screenshot shows the 'Devices | Device settings' page in the Azure Active Directory portal. The left sidebar lists several options: 'All devices' (selected), 'Device settings' (highlighted in grey), 'Enterprise State Roaming', 'BitLocker keys (Preview)', and 'Diagnose and solve problems'. Below these are sections for 'Activity' (Audit logs, Bulk operation results (Preview)) and 'Troubleshooting + Support' (New support request). At the top right, there are buttons for 'Save' and 'Discard', and a 'Got feedback?' link. A message at the top states 'Users may join devices to Azure AD' with three buttons: 'All' (greyed out), 'Selected' (highlighted in blue), and 'None'. To the right of this is a section titled 'Selected' showing '1 member selected'. Further down, another message says 'Users may register their devices with Azure AD' with 'All' and 'None' buttons. A link 'Learn more on how this setting works' is present. At the bottom, there's a note about Multi-Factor Authentication requirements, a 'Yes' button, and a 'No' button. The 'Maximum number of devices per user' is set to 50. At the very bottom, there are links for 'Additional local administrators on all Azure AD joined devices' and 'Manage Additional local administrators on all Azure AD joined devices'. Finally, there are sections for 'Enterprise State Roaming' and 'Manage Enterprise State Roaming settings'.

# 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

The screenshot shows the 'Devices | Device settings' page in the Azure Active Directory portal. The left sidebar lists several sections: 'All devices' (selected), 'Device settings' (highlighted in blue), 'Enterprise State Roaming', 'BitLocker keys (Preview)', and 'Diagnose and solve problems'. The main content area has three main sections: 1) 'Users may join devices to Azure AD' with a status of 'Selected' and '1 member selected'. 2) 'Users may register their devices with Azure AD' with a status of 'None'. 3) 'Devices to be Azure AD joined or Azure AD registered require Multi-Factor' with a status of 'No'. Below these are sections for 'Audit logs', 'Bulk operation results (Preview)', 'Shooting + Support', and 'Support request'. At the bottom, there are sections for 'Maximum number of devices per user' (set to 50), 'Additional local administrators on all Azure AD joined devices' (with a link to 'Manage Additional local administrators on all Azure AD joined devices'), and 'Enterprise State Roaming' (with a link to 'View Enterprise State Roaming settings').



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

Image Users Groups External identities Global administrators Delegated administrators Delegated units Applications

**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... [Edit](#)  
Primary domain: berksbatteries.com

**Azure AD Connect**

Status: Not enabled  
Last sync: Sync has never run

# Hybrid Azure AD Joined Devices

# Hybrid Azure AD Joined Devices

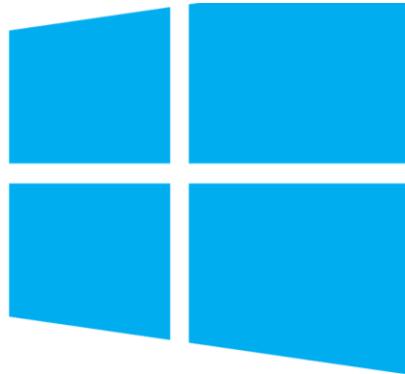
Hybrid Azure AD joined devices are joined to an on-prem Active Directory, and are registered with Azure AD.

- 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

<b>DEFINITION</b>	JOINED TO ON-PREMISES AD AND AZURE AD REQUIRING ORGANIZATIONAL ACCOUNT TO SIGN INTO THE DEVICE
<b>Primary audience</b>	<ul style="list-style-type: none"><li>• Suitable for hybrid organizations with existing on-premises AD infrastructure</li><li>• Applicable to all users in an organization</li></ul>
<b>Device ownership</b>	Organization
<b>Operating systems</b>	<ul style="list-style-type: none"><li>• Windows 10, 8.1 and 7</li><li>• Windows Server 2008/R2, 2012/R2, 2016 and 2019</li></ul>
<b>Provisioning</b>	<ul style="list-style-type: none"><li>• Windows 10, Windows Server 2016/2019</li><li>• Domain join by IT and autojoin via Azure AD Connect or ADFS config</li><li>• Domain join by Windows Autopilot and autojoin via Azure AD Connect or ADFS config</li><li>• Windows 8.1, Windows 7, Windows Server 2012 R2, Windows Server 2012, and Windows Server 2008 R2 - Require MSI</li></ul>
<b>Device sign in options</b>	<ul style="list-style-type: none"><li>• Organizational accounts using:</li><li>• --Password / Windows Hello for Business for Win10</li></ul>
<b>Device management</b>	<ul style="list-style-type: none"><li>• Group Policy</li><li>• Configuration Manager standalone or co-management with Microsoft Intune</li></ul>
<b>Key capabilities</b>	<ul style="list-style-type: none"><li>• SSO to both cloud and on-premises resources</li><li>• Conditional Access through Domain join or through Intune if co-managed</li><li>• Self-service Password Reset and Windows Hello PIN reset on lock screen</li><li>• Enterprise State Roaming across devices</li></ul>



Group Policy Management Editor

File Action View Help

AADDC Computers GPO [E48L1AGUF5NDC]

- Computer Configuration
  - Policies
    - Software Settings
      - Software installation
    - Windows Settings
      - Name Resolution Policy
      - Scripts (Startup/Shutdown)
      - Security Settings
      - Policy-based QoS
      - Administrative Templates: Policy
    - Preferences
  - User Configuration
    - Policies
    - Preferences

Name	Description
Account Policies	Password and ac
Local Policies	Auditing, user ri
Event Log	Event Log
Restricted Groups	Restricted Group
System Services	System service s
Registry	Registry security
File System	File system secu
Wired Network (IEEE 802.3) Policies	Wired Network F
Windows Firewall with Advanced Security	Windows Firewa
Network List Manager Policies	Network name, i
Wireless Network (IEEE 802.11) Policies	Wireless Networ
Public Key Policies	
Software Restriction Policies	
Network Access Protection	Network Access
Application Control Policies	Application Con
IP Security Policies on Active Directory (C...)	Internet Protoco
Advanced Audit Policy Configuration	Advanced Audit

 Diagnose and solve problems

## Activity

Users may register their devices with Azure AD 

All

None

 Audit logs Bulk operation results (Preview) Learn more on how this setting works

## Troubleshooting + Support

 New support requestDevices to be Azure AD joined or Azure AD registered require Multi-Factor Authentication 

Yes

No

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.



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

Image Users Groups External identities Global administrators Delegated administrators Delegated units Applications

**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... [Edit](#)  
Primary domain: berksbatteries.com

**Azure AD Connect**

Status: Not enabled  
Last sync: Sync has never run

# Course Conclusion



# Intro to Azure Active Directory

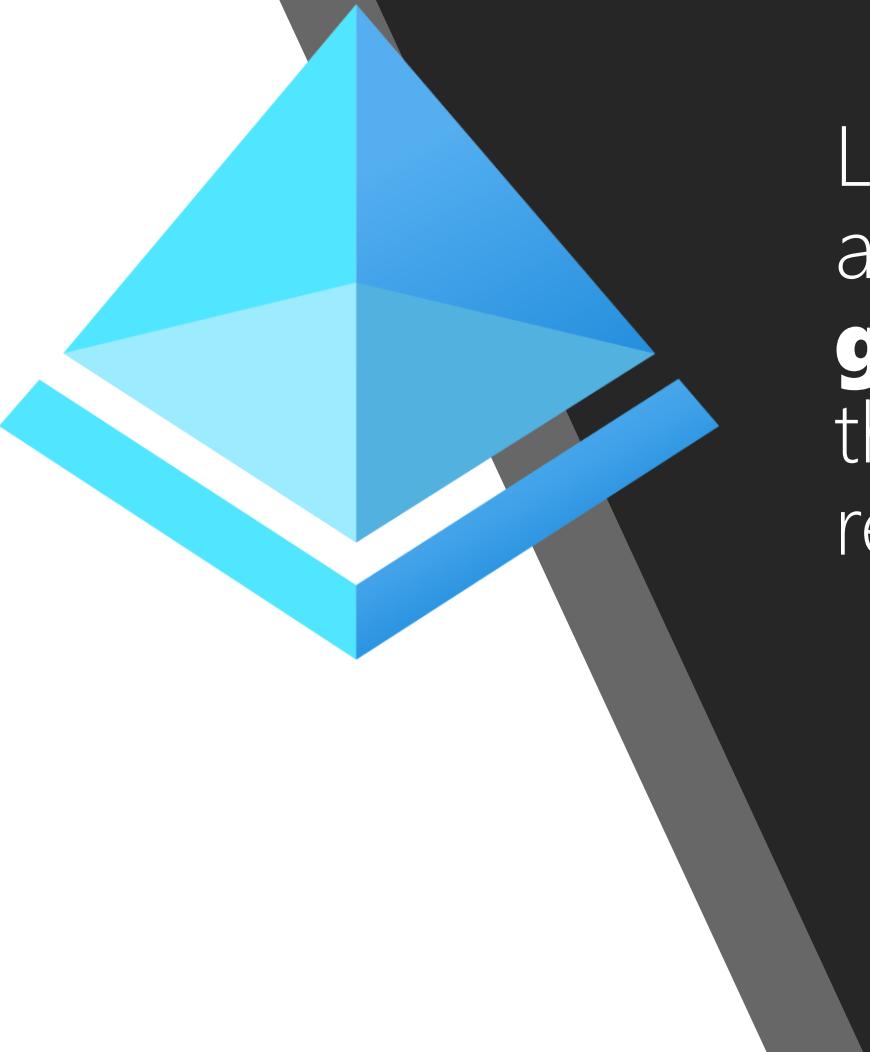
Learn what Azure AD is, and what it offers.

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

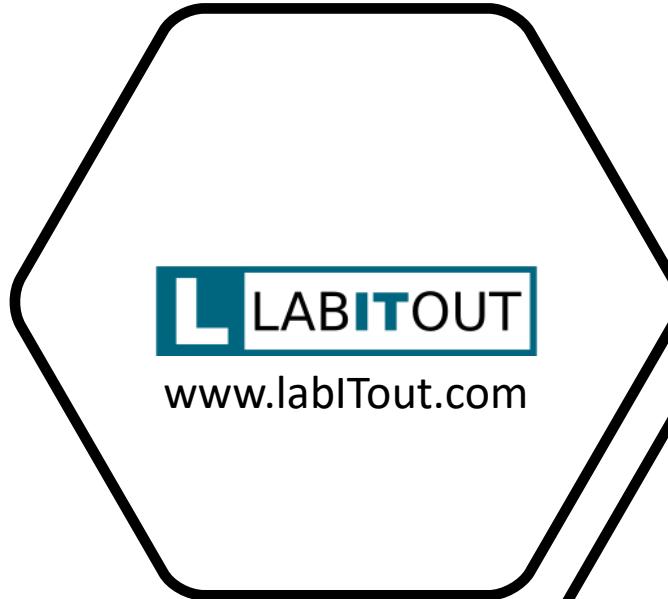
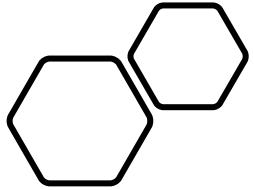


Learn what hybrid identities are, and what the role of **Azure AD Connect** is.

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!