

# Active Directory

## **Secure Access with Azure Active Directory**

---

### **Project Overview**

This project focused on identity and access management using Microsoft Azure Active Directory (Azure AD). It provided hands-on understanding of how modern organizations secure user identities, manage authentication, and control access to cloud and hybrid environments.

The training simulated real-world enterprise identity systems used to protect applications, enforce security policies, and enable secure access across organizational resources.

---

### **Project Objectives**

- Understand Azure Active Directory architecture and services
  - Manage users, groups, and administrative units in cloud environments
  - Implement authentication and security policies
  - Configure Multi-Factor Authentication (MFA) for secure access
  - Explore hybrid identity solutions using Azure AD Connect
  - Understand Single Sign-On (SSO) in enterprise systems
- 

### **Tools & Technologies**

- Microsoft Azure Active Directory (Azure AD)
  - Azure AD Domain Services
  - Azure AD Connect (Hybrid Identity Tooling)
  - Multi-Factor Authentication (MFA) systems
  - Identity & Access Management (IAM) frameworks
  - Microsoft cloud security services
-

# Active Directory

## Core Components & Implementation

### User & Group Management

Configured and managed user identities within Azure AD, including:

- Creation and organization of user accounts
  - Group-based access control
  - Assignment of roles and permissions
  - Administrative unit structuring for scalable management
- 

### Authentication & Security Controls

Explored and implemented identity protection mechanisms such as:

- Password policies and protection mechanisms
  - Multi-Factor Authentication (MFA) setup and enforcement
  - Secure sign-in methods and verification processes
  - Risk-based authentication concepts
- 

### Hybrid Identity Integration

Studied how on-premises Active Directory environments integrate with cloud systems using Azure AD Connect:

- Synchronization of user identities between local and cloud directories
  - Centralized identity management across hybrid environments
  - Improved scalability and security for enterprise infrastructure
- 

### Single Sign-On (SSO)

Configured and analyzed SSO functionality, allowing users to:

- Access multiple applications with one secure login
- Reduce password fatigue
- Improve enterprise user experience and productivity

# Active Directory

---



## Key Skills Demonstrated

- Identity and Access Management (IAM)
  - Cloud Security Architecture (Azure)
  - User Authentication Systems
  - Multi-Factor Authentication (MFA) Implementation
  - Hybrid Cloud Identity Solutions
  - Active Directory Administration
  - Security Policy Configuration
  - Enterprise Access Control Design
- 



## What I Learned

This project strengthened my understanding of how enterprise environments manage secure access at scale. It highlighted the importance of identity as the foundation of cybersecurity and demonstrated how Azure AD enables centralized control over authentication, authorization, and user lifecycle management.

I gained practical insight into how organizations reduce security risks through MFA, enforce access policies, and integrate hybrid infrastructure for scalable identity management.

# Active Directory

## 1. Create 3 users, named John, Jeff and Dave

**Users** Kevandcoperation

Search

+ New user Edit (Preview) Delete Download users Bulk operations Refresh

**Create new user**  
Create a new internal user in your organization

**Invite external user**  
Invite an external user to collaborate with your organization

	User principal name	User type	On-premises sy...	Identities
<input type="checkbox"/>	DaveE@Kevandcoperatio...	Member	No	Kevandcoperation
<input type="checkbox"/>	JeffE@Kevandcoperation...	Member	No	Kevandcoperation
<input type="checkbox"/>	JohnE@Kevandcoperation...	Member	No	Kevandcoperation

## 2. Add the three users into a group named DevSupport

### Overview

### Basic information



**DevSupport**

Membership type	Assigned	Total direct members	3
Source	Cloud	User(s)	3
Type	Security	Group(s)	0
Object ID	5a1a57b7-c609-4f25-ba98-ff40ffc43a24	Device(s)	0
Created on	4/20/2025, 4:38 PM	Other(s)	0

# Active Directory

## 3. Turn on self password reset for the members of the groups

**Password reset | Administrator Policy** ...  
Kevandcooperation

Diagnose and solve problems <<

Is self-service password reset enabled?  
Yes

Manage

Properties

Authentication methods

Registration

Notifications

Number of methods required to reset:  
1

Methods available to administrators:  
Email  
Mobile phone (SMS only)  
Mobile app code

**Password reset | Properties** ...  
Kevandcooperation

Save Discard

Diagnose and solve problems

Manage

Properties

Authentication methods

Registration

Self service password reset enabled ⓘ  
None Selected All

Select group ⓘ  
DevSupport

## 4. Sign in with a User and reset password

### Update your password

You need to update your password because this is the first time you are signing in, or because your password has expired.

.....

Passwords can't contain your user ID, and need to be at least 8 characters long, with at least 3 of the following: uppercase letters, lowercase letters, numbers, and symbols. [View details](#)

.....

.....

**Sign in**

# Active Directory

## Enter password

Your account or password is incorrect. If you don't remember your password, [reset it now](#).

Password

[Forgot my password](#)

Sign in

## Microsoft

### Get back into your account

We're sorry

You can't reset your own password because you haven't registered for password reset.

If you can't sign in, you must [contact your administrator](#) to reset your password for you.

After you can sign in again, [register for self-service password reset](#), to make sure that you're able to reset your own password in the future.

Hide additional details

SSPR\_0014: You haven't registered the necessary security information to perform password reset. If you're an administrator, you can get more information from the [B successfully roll out password reset](#) articles. If you're not an administrator, you can provide this information when you contact your administrator.

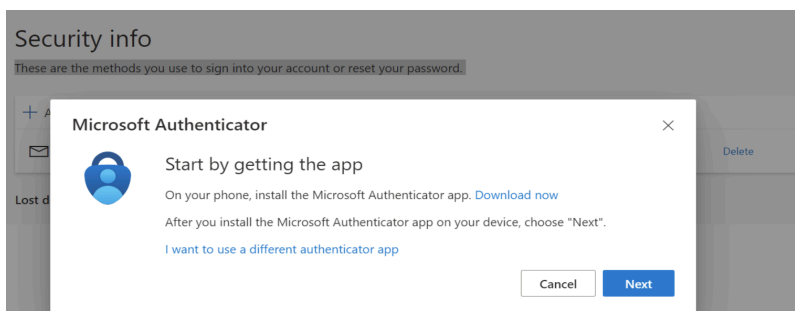
## Microsoft

### Get back into your account

Your admin has been notified

**Only your admin can reset your password.** To assist you, we've sent an email to your admin requesting a password reset.

Note that this request could take some time to complete, depending on your organization's support policies. Contact your admin or helpdesk for any further assistance.



# Active Directory

Microsoft

## Get back into your account

✓ Your password has been reset

To sign in with your new password, [click here](#).

### 5. Enable MFA for all the users

## Per-user multifactor authentication

 Bulk update |  Got feedback?

**Users** | Service settings

Use multifactor authentication (MFA) to protect your users and data. Our recommended approach to enforce MFA is to use adaptive Conditional Access.

Before you begin, take a look at the [multifactor authentication deployment guide](#).

✓ Enable MFA |  Disable MFA |  Enforce MFA |  User MFA settings

Status : All View : Sign-in allowed users  Reset filters

<input type="checkbox"/>	Name ↕	UPN	Status
<input type="checkbox"/>	Dave	DaveE@Kevandcoperation.onmicrosoft.com	enabled
<input type="checkbox"/>	Jeff	JeffE@Kevandcoperation.onmicrosoft.com	enabled
<input type="checkbox"/>	John	JohnE@Kevandcoperation.onmicrosoft.com	enabled