📄 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

💡

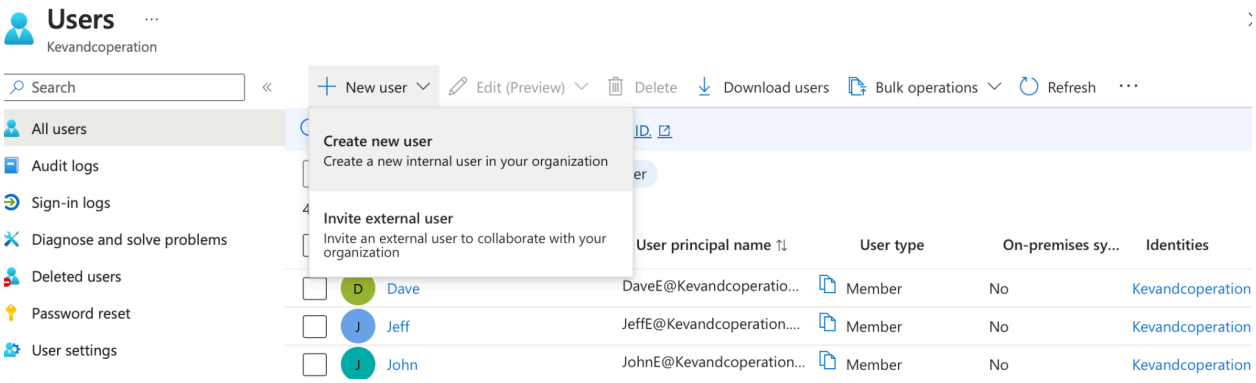
What I Learned

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.

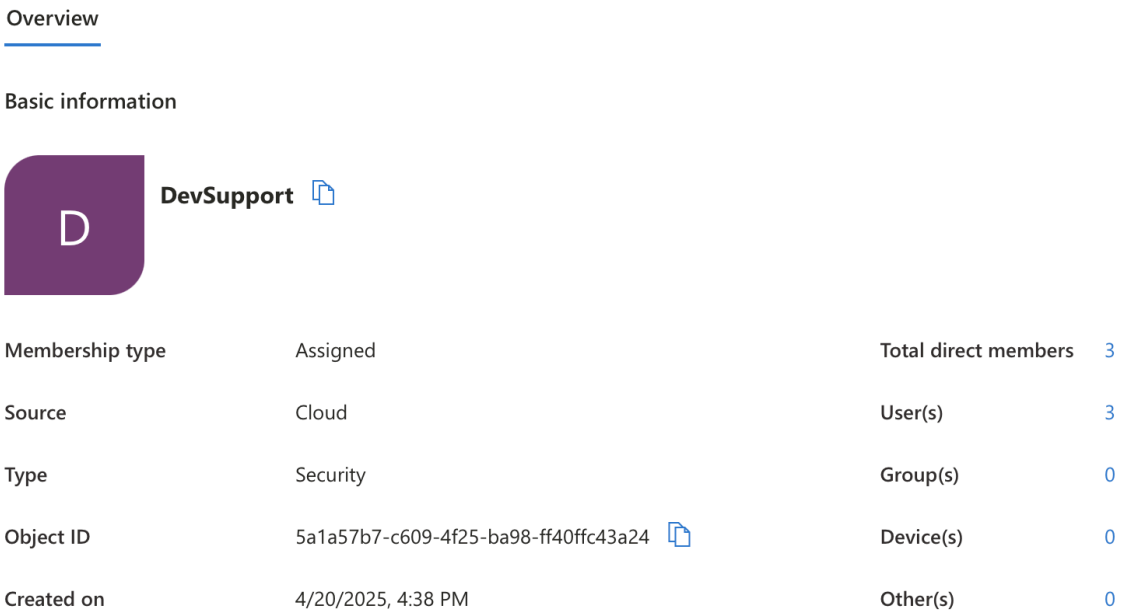
I gained practical insight into how organizations reduce security risks through MFA, enforce access policies, and integrate hybrid infrastructure for scalable identity management.

Active Directory

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

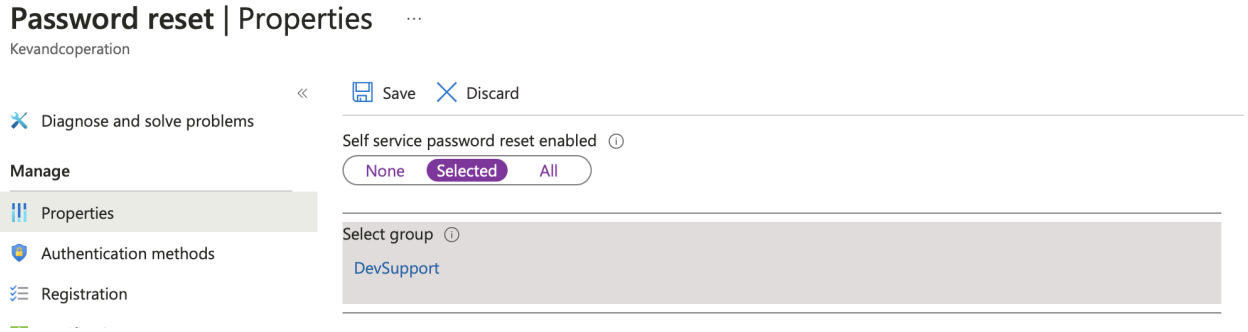


2. Add the three users into a group named DevSupport

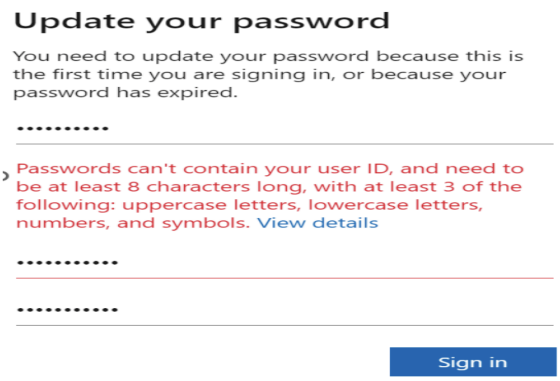


Active Directory

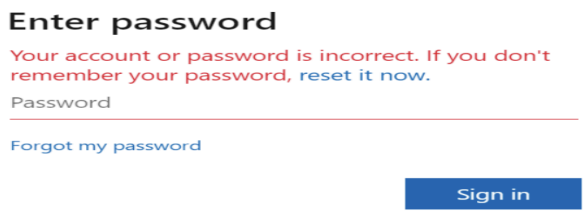
3. Turn on self password reset for the members of the groups

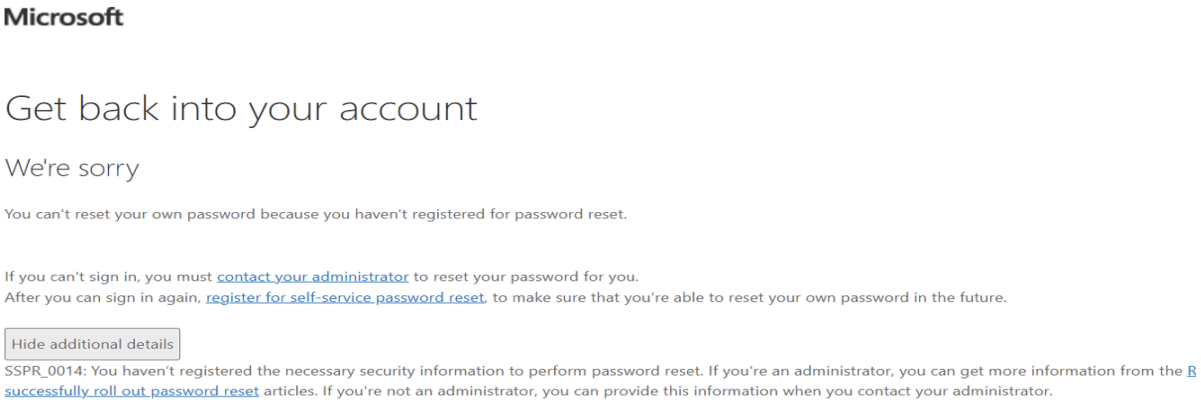


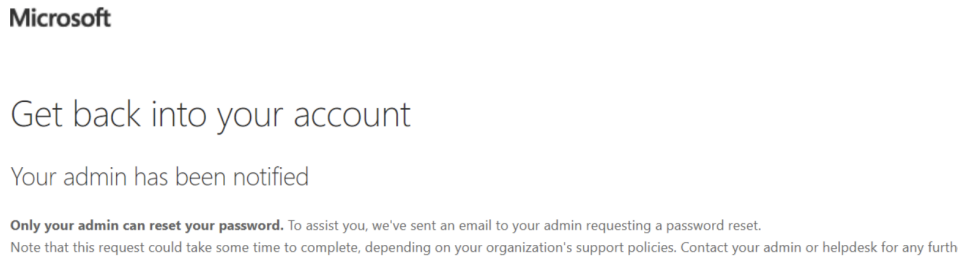
4. Sign in with a User and reset password

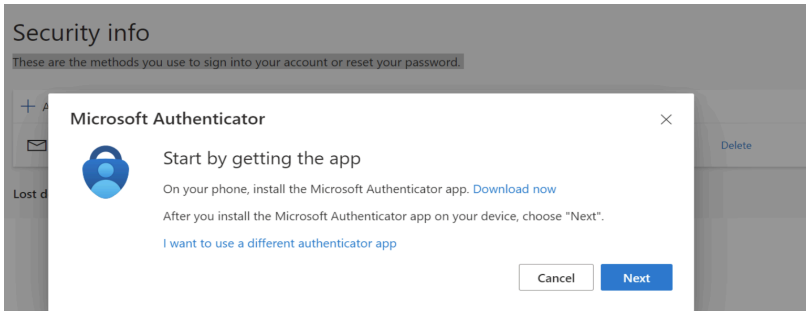


Active Directory

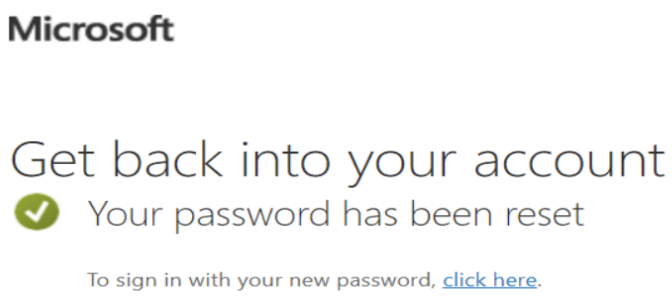








Active Directory



5. Enable MFA for all the users