Documentation: Enabling Multi-Factor Authentication (MFA) and Managing User Access in Microsoft Entra ID

Introduction

This project highlights the implementation of **Multi-Factor Authentication (MFA)**. The focus is on ensuring secure user authentication while balancing operational requirements and security protocols.

Multi-Factor Authentication (MFA)

What is MFA?

MFA is a security enhancement that requires users to authenticate using multiple factors. It is a more secure but slightly less convenient authentication method compared to traditional username and password authentication. After entering their username and password, users are prompted for an additional authentication method such as:

- **Mail OTP**: A one-time passcode sent to the user's email.
- **Authenticator App**: A code generated by a mobile application such as Microsoft Authenticator or Google Authenticator.

Benefits of MFA

1. **Increased Security**: Adds an additional layer of protection against unauthorized access.
2. **Flexibility**: Users can select a preferred secondary authentication method.
3. **Compliance**: Meets security standards and regulatory requirements for sensitive data protection.

User Status in MFA

Microsoft Entra ID defines three MFA user statuses:

1. **Disabled**: The user has not been assigned MFA.
2. **Enabled**: The user has been assigned MFA but has not completed the registration process.
3. **Enforced**: The user has been assigned MFA and has completed the registration process successfully.

Implementation Steps

1. Enabling Multi-Factor Authentication

1. Navigate to **Microsoft Entra ID** in the Azure Portal.
2. Select **Users** and choose the user to configure MFA.
3. Assign the desired MFA policy:
    a. Set the user status to **Enabled**.
    b. Monitor and guide users to complete MFA registration, transitioning them to **Enforced** status.

Project Video Documentation

Video Description

To provide a clear understanding of the project’s functionality, a step-by-step video has been recorded showcasing:

Conclusion

This project showcases essential skills in securing and managing user access using Microsoft Entra ID. By implementing Multi-Factor Authentication and leveraging access management capabilities, administrators can effectively balance security and operational needs.