Azure Identity and Access Management (IAM) Showcase

This project demonstrates my skills in Azure Identity and Access Management (IAM), covering user provisioning, role assignments, security configurations, and MFA implementations.

1. Bulk User Creation in Azure Active Directory

This screenshot demonstrates creating users in Azure Active Directory using bulk upload with a CSV file.

- Excel File: Lists user details (UserPrincipalName, passwords, and attributes).
- Azure Portal: Displays created users (TestUser1 to TestUser5).

Importance: Bulk user creation is a key feature for onboarding users efficiently in a large organization.

2. Setting Up Microsoft Authenticator for MFA

This screenshot shows the setup process for Microsoft Authenticator as part of Multi-Factor Authentication (MFA). Users are prompted to add an account and secure it.

Importance: Enabling MFA is critical for securing user accounts against unauthorized access.

3. Action Required: MFA Enforcement

When a user logs in, Azure AD enforces MFA by requiring additional security information to enable Microsoft Authenticator.

Importance: This ensures that user authentication adheres to strict security policies, enhancing organizational security.

4. User Overview: sadea_luv

This screenshot shows the sadea_luv user's profile in Azure:

- Account Status: Enabled
- Attributes: UserPrincipalName, Object ID, Created Date.

Importance: Reviewing user attributes helps manage user identity and validate account configurations.

5. Account Disabled Example

The sadea_luv account has been disabled to demonstrate lifecycle management. The account can no longer be accessed.

Importance: Disabling unused or compromised accounts is crucial for maintaining a secure environment.

6. Account Lockout for Security

Shows an account (sadea_luv) locked after security thresholds were triggered. The user cannot log in without administrator intervention.

Importance: Account lockouts protect against brute-force attacks and suspicious activity.

7. Role Assignment for Users

The sadea_luv user has been assigned the following roles:

- Desktop Analytics Administrator: Manage desktop services.
- Helpdesk Administrator: Reset passwords for non-admins.

Importance: Role-based access control (RBAC) ensures users have the least privileges necessary for their tasks.

8. MFA Configuration: Per-User Settings

This screenshot shows the per-user MFA configuration:

- Verification Options: Call, SMS, Mobile app notification, and Hardware token.
- Trusted IPs: Optional settings to skip MFA for trusted networks.

Importance: MFA adds an additional layer of security for user sign-ins, preventing unauthorized access.

9. Test User3: User Lifecycle Management

Details of the Test User3 profile:

- Account Status: Disabled.
- Object ID: Used for tracking in Azure AD.

Importance: Demonstrates lifecycle management by disabling accounts no longer in use.

Conclusion

This documentation serves as a comprehensive showcase of my Azure IAM skills. It demonstrates best practices for:

- User Lifecycle Management
- Role-Based Access Control (RBAC)
- Multi-Factor Authentication (MFA)
- Security Enforcement