Configuring and managing Azure Multifactor Authentication (MFA) and self-service password reset involves several steps to enhance the security of your Azure Active Directory (Azure AD). Here's a comprehensive guide covering these aspects:

1. Configure & Manage Azure Multifactor Authentication (MFA)

Step 1: Enable Azure MFA
1. Sign in to Azure Portal: [Azure Portal](https://portal.azure.com)
2. Navigate to Azure AD:
- Go to "Azure Active Directory" next "Security" next "Multi-Factor Authentication".
3. Configure MFA:
- Click on "MFA" under "Security" and then select "Additional cloud-based MFA settings".
- Enable the settings as needed (e.g., app passwords, trusted IPs, verification options).

Step 2: Configure User Settings for MFA
1. User Management:
- Go to "Azure Active Directory" next "Users".
- Select a user, then click on "Authentication methods" next "Require re-register MFA".
- This forces the user to set up MFA at the next sign-in.

2. Two-Factor Authentication

Azure MFA supports multiple methods for two-factor authentication:

Different Methods of Two-Factor Authentication
1. Mobile App:
- Microsoft Authenticator: Users receive a notification or use a verification code.
2. Phone Call:
- Users receive a call and press a key to authenticate.
3. Text Message:
- Users receive a verification code via SMS.
4. Hardware Tokens:
- Physical devices that generate time-based codes.

3. Setup Self-Service Password Reset

Step 1: Enable Self-Service Password Reset (SSPR)
1. Navigate to Azure AD:
- Go to "Azure Active Directory" next "Password reset".
2. Configuration:

- Select "Self-service password reset" and choose the desired scope (e.g., All users or Selected groups).
- Click on "Save".

Step 2: Configure Authentication Methods for SSPR

1. Authentication Methods:
- Go to "Password reset" next "Authentication methods".
- Choose the methods users can use to reset their passwords (e.g., email, mobile phone, security questions).

4. Configure MFA

This involves the same steps as described in section 1, focusing on enforcing MFA across the organization.

5. Configure and Deploy Self-Service Password Reset

This involves the steps described in section 3, ensuring that users are aware of the SSPR functionality and have registered their authentication methods.

6. Implement and Manage Azure MFA Settings

1. Conditional Access Policies:
- Go to "Azure Active Directory" next "Security" next "Conditional Access".
- Create policies that require MFA for certain conditions (e.g., risky sign-ins, access to specific applications).

2. User Registration:
- Ensure users have registered their MFA methods by checking "Azure Active Directory" next "Security" next "Identity Protection" next "MFA Registration".

7. Account Lockout

1. Azure AD Smart Lockout:
- Azure AD has a built-in smart lockout mechanism that locks accounts for a certain period after multiple failed sign-in attempts.
- Configure the settings in "Azure Active Directory" next "Security" next "Authentication methods" next "Password protection".

8. Manage MFA Settings for Users

1. User-Specific Settings:
- Go to "Azure Active Directory" next "Users" next select a user next "Authentication methods".

- Reset MFA registration, enforce MFA, and manage phone numbers.

9. Extend Azure AD MFA to Third-Party and On-Premises Devices

1. Azure AD Application Proxy:
- Use Azure AD Application Proxy to extend Azure AD MFA to on-premises applications.
- Configure the application in "Azure Active Directory" next "Application proxy".

2. Third-Party Integration:
- Use Conditional Access policies to enforce MFA for third-party applications integrated with Azure AD.

10. Monitor Azure AD MFA Activity

1. Sign-in Logs:
- Go to "Azure Active Directory" next "Sign-ins".
- Filter logs by "MFA required" to monitor MFA usage.

2. Reports:
- Use "Azure Active Directory" next "Reports" to get detailed insights into MFA-related activities.

11. OAuth Tokens

OAuth tokens are used to authorize access to resources. Azure AD supports OAuth 2.0 for secure access delegation.

1. Application Registration:
- Register applications in "Azure Active Directory" next "App registrations".
- Configure API permissions and grant admin consent.

2. Token Configuration:
- Use OAuth tokens to authenticate and authorize users against Azure AD-secured resources.