Self-Service Password Reset (SSPR) in Microsoft Entra ID (Azure AD)

What is SSPR?

Self-Service Password Reset (SSPR) is a Microsoft Entra ID feature that empowers users to reset or unlock their passwords without needing to contact the IT helpdesk. This reduces support costs, improves productivity, and enhances user experience by minimizing downtime due to password-related issues.

Why is SSPR Important?

- **Reduce Helpdesk Tickets:** Password reset requests are among the most common IT support calls. SSPR reduces this burden.
- **Improve Security:** With proper verification (multi-factor authentication, email, SMS), unauthorized password resets can be prevented.
- **Increase User Productivity:** Users regain access faster without waiting for manual intervention.
- **Support Hybrid Environments:** SSPR works both for cloud-only and hybrid Azure AD environments with on-premises synchronization.

How SSPR Works

1. **User initiates password reset:** Via a portal (https://passwordreset.microsoftonline.com), users can start the reset process.

2. **Identity verification:** Users verify their identity by responding to registered authentication methods, such as:
    - Mobile phone SMS or call
    - Email verification
    - Security questions
    - Microsoft Authenticator app notification or verification code
3. **Reset password:** Upon successful verification, the user is allowed to create a new password.
4. **Unlock account (optional):** Users can also unlock their accounts if locked due to failed sign-in attempts.

Prerequisites & Setup

- **Licensing:** SSPR is available in Microsoft Entra ID Free, but enhanced features require Premium P1 or P2.
- **User registration:** Users must register their authentication methods before using SSPR.
- **Admin configuration:** SSPR must be enabled and configured in the Microsoft Entra admin portal.

How to Enable and Configure SSPR

Step 1: Enable SSPR in the Azure Portal

1. Sign in to the Azure Portal.
2. Navigate to **Azure Active Directory** > **Password reset**.
3. Under **Properties**, set **Self service password reset enabled** to:

    - **None** (disabled)
    - **Selected** (enable for specific groups)
    - **All** (enable for all users)

4. Save your changes.

Step 2: Configure Authentication Methods

1. In the **Password reset** pane, go to **Authentication methods**.
2. Select which methods users can use to verify their identity (e.g., email, mobile phone, security questions).
3. Define the number of methods required to reset the password (recommended at least 2).

Step 3: Inform Users to Register

- Direct users to https://aka.ms/ssprsetup to register their authentication methods.
- Users must complete registration before they can reset their passwords.

Demo Scenario (Example Use Case)

Imagine an employee forgets their password on a Monday morning and cannot log in. Instead of calling the IT helpdesk and waiting, the employee:

- Navigates to https://passwordreset.microsoftonline.com
- Enters their username/email
- Verifies identity via SMS code sent to their registered phone
- Creates a new password
- Regains access immediately, minimizing downtime

Monitoring and Reporting

Admins can monitor SSPR usage and failures via:

- **Azure AD sign-in logs**
- **Password reset audit logs**
- Alerts for unusual activities such as multiple failed resets

Best Practices

- Enforce multi-factor authentication for password resets.
- Require at least two authentication methods.
- Educate users on registering authentication methods.
- Regularly monitor logs and alerts.
- Integrate SSPR with on-premises Active Directory if using hybrid identity.