

How to Reset a Password in Microsoft Azure

Introduction

This guide provides step-by-step instructions for resetting user passwords in Microsoft Azure Active Directory (now called Microsoft Entra ID). Whether you're an administrator helping a user or setting up self-service password reset, this guide covers the essential methods.

Method 1: Reset Password via Azure Portal (Admin)

Administrators can reset passwords for users directly through the Azure Portal. Follow these steps:

Step 1: Sign in to the **Azure Portal** at <https://portal.azure.com> with your administrator credentials.

Step 2: In the left navigation menu, click on **Microsoft Entra ID** (formerly Azure Active Directory).

Step 3: Select **Users** from the Manage section in the left sidebar.

Step 4: Search for and click on the user whose password needs to be reset.

Step 5: Click the **Reset password** button in the top toolbar.

Step 6: Choose whether to **Auto-generate password** or manually enter a new password.

Step 7: Optionally, check **Require this user to change their password when they first sign in** for added security.

Step 8: Click **Reset** to complete the process.

Step 9: Securely share the new temporary password with the user.

Note: You need Global Administrator, Password Administrator, or User Administrator role to reset passwords.

Method 2: Self-Service Password Reset (SSPR)

If your organization has enabled Self-Service Password Reset, users can reset their own passwords without admin intervention:

Step 1: Navigate to <https://passwordreset.microsoftonline.com> or click 'Forgot my password' on the sign-in page.

Step 2: Enter your **User ID** (email address) and complete the CAPTCHA verification.

Step 3: Click **Next** to proceed to identity verification.

Step 4: Complete the verification method(s) configured for your account (e.g., phone, email, security questions, or authenticator app).

Step 5: Once verified, enter and confirm your **new password**.

Step 6: Click **Finish** to complete the password reset.

Step 7: Sign in with your new password.

Method 3: Reset Password via PowerShell

For bulk operations or automation, administrators can use PowerShell to reset passwords:

```
# Connect to Azure AD
Connect-AzureAD

# Reset password for a specific user
$newPassword = ConvertTo-SecureString "TempP@ssw0rd123!" -AsPlainText -Force
Set-AzureADUserPassword -ObjectId "user@domain.com" -Password $newPassword
-ForceChangePasswordNextLogin $true
```

Best Practices & Security Tips

- **Use Strong Passwords:** Require passwords with at least 12 characters, including uppercase, lowercase, numbers, and special characters.
- **Enable MFA:** Always enable Multi-Factor Authentication for additional security.
- **Force Password Change:** When resetting passwords for users, require them to change it on first login.
- **Communicate Securely:** Never send passwords via unencrypted email. Use secure channels or have users set their own.
- **Enable SSPR:** Configure Self-Service Password Reset to reduce helpdesk burden and improve user experience.
- **Monitor Sign-ins:** Regularly review Azure AD sign-in logs for suspicious activity after password resets.

- **Configure Password Policies:** Set appropriate password expiration and complexity requirements in Azure AD.

Troubleshooting Common Issues

User cannot access SSPR: Ensure SSPR is enabled for the user's group and they have registered authentication methods.

Password reset fails: Check if password meets complexity requirements. Azure AD requires 8+ characters by default.

Admin cannot reset password: Verify you have the appropriate role (Global Admin, Password Admin, or User Admin).

Synced user password issues: For users synced from on-premises AD, password writeback must be enabled in Azure AD Connect.

*For more information, visit the official Microsoft documentation at
<https://learn.microsoft.com/azure/active-directory/>*