

AZURE AD PASSWORD POLICIES

Property	Requirements
Characters allowed	<ul style="list-style-type: none"> • A – Z • a - z • 0 – 9 • @ # \$ % ^ & * - _ ! + = [] { } \ : ' , . ? / ` ~ " () ; • blank space
Characters not allowed	Unicode characters.
Password restrictions	<ul style="list-style-type: none"> • A minimum of 8 characters and a maximum of 256 characters. • Requires three out of four of the following: <ul style="list-style-type: none"> ○ Lowercase characters. ○ Uppercase characters. ○ Numbers (0-9). ○ Symbols (see the previous password restrictions).
Password expiry duration (Maximum password age)	<ul style="list-style-type: none"> • Default value: 90 days. • The value is configurable by using the Set-MsolPasswordPolicy cmdlet from the Azure Active Directory Module for Windows PowerShell.
Password expiry notification (When users are notified of password expiration)	<ul style="list-style-type: none"> • Default value: 14 days (before password expires). • The value is configurable by using the Set-MsolPasswordPolicy cmdlet.
Password expiry (Let passwords never expire)	<ul style="list-style-type: none"> • Default value: false (indicates that password's have an expiration date). • The value can be configured for individual user accounts by using the Set-MsolUser cmdlet.
Password change history	The last password <i>can't</i> be used again when the user changes a password.
Password reset history	The last password <i>can</i> be used again when the user resets a forgotten password.
Account lockout	After 10 unsuccessful sign-in attempts with the wrong password, the user is locked out for one minute. Further incorrect sign-in attempts lock out the user for increasing durations of time. Smart lockout tracks the last three bad password hashes to avoid incrementing the lockout counter for the same password. If someone enters the same bad password multiple times, this behavior will not cause the account to lock out.