# Office 365-Kennwortrichtlinie

Office 365 unterstützt zwei Identitätstypen:

1. **Microsoft Online Services-Cloud-ID**: Die Benutzer können sich mit ihren Cloud-Anmeldeinformationen bei den Office 365-Diensten anmelden. Diese Anmeldeinformationen unterscheiden sich von allen anderen Desktop- oder Unternehmensanmeldeinformationen. Office 365 erstellt diese Identitäten und authentifiziert daher auch die Benutzer. In diesem Fall wird die Kennwortrichtlinie in der Cloud mit dem Office 365-Dienst gespeichert.
2. **Identitätsverbund**: Die Benutzer melden sich mit den AD-Anmeldeinformationen für ihr Unternehmen bei den Office 365-Diensten an. In diesem Fall authentifiziert das Unternehmens-AD den Benutzer, während die Kennwortrichtlinie im lokalen AD kontrolliert und gespeichert wird.

In diesem Artikel werden die Kennwortrichtlinien und -optionen für die Microsoft Online Services-Cloud-IDs beschrieben.

## Kennwortrichtlinie

|  |  |
| --- | --- |
| **Eigenschaft** | **Beschreibung** |
| Kennwortbeschränkungen | mindestens 8 Zeichen, höchstens 16 Zeichen  **Erlaubte Zeichen:**   * A-Z * a-z * 0-9 * ! @ # $ % ^ & \* - \_ + = [ ] { } | \ : ‘ , . ? / ` ~ “ < > ( ) ; * kein Unicode   darf nicht den Alias des Benutzernamens enthalten (Teil vor dem @-Symbol) |
| Gültigkeit des Kennworts | Ein Kennwort ist 90 Tage lang gültig. Dieser Zeitraum kann nicht geändert werden. |
| Ablaufen des Kennworts | Die Ablaufzeit des Kennworts ist standardmäßig aktiviert. In diesem Fall müssen die Benutzer ihr Kennwort nach 90 Tagen ändern. Die Benutzer erhalten zurzeit noch keine Benachrichtigung darüber, dass ihr Kennwort abläuft.  **Ab dem Zeitpunkt der allgemeinen Verfügbarkeit** sind Administratoren berechtigt, diese Einstellung auf Benutzerebene mithilfe des PowerShell-Clients (Microsoft Online Services-Modul für Windows PowerShell) zu aktivieren oder zu deaktivieren. |

|  |  |
| --- | --- |
| **Eigenschaft** | **Beschreibung** |
| Kennwortsicherheit | Sichere Kennwörter müssen drei der folgenden vier Zeichenkategorien enthalten:   * Kleinbuchstaben * Großbuchstaben * Zahlen (0-9) * Symbole (siehe Kennwortbeschränkungen oben)   Sobald die neue Kennwortrichtlinie in Kraft tritt, sind in BPOS sichere Kennwörter zwingend erforderlich.  In Office 365 gibt es eine Einstellung, mit der Sie die Forderung nach einem sicheren Kennwort umgehen können. Diese Einstellung können Sie jedoch erst nach dem Wechsel von BPOS zu Office 365 aktivieren.  **Ab dem Zeitpunkt der allgemeinen Verfügbarkeit** sind Administratoren berechtigt, diese Einstellung auf Benutzerebene über das Microsoft Online Services-Modul zu aktivieren oder zu deaktivieren. |
| Kennwortverlauf | Das letzte Kennwort kann nicht wieder verwendet werden. |
| Kennwortverlaufsdauer | Keine |
| Kontosperrung | Nach zehn erfolglosen Anmeldeversuchen mit einem falschen Kennwort muss der Benutzer einen CAPTCHA-Dialog lösen, um sich anmelden zu können.  Nach weiteren zehn erfolglosen Anmeldeversuchen mit einem falschen Kennwort und der richtigen Lösung des CAPTCHA-Dialogs wird der Benutzer für eine bestimmte Zeit gesperrt. Bei erneuter Eingabe eines falschen Kennworts wird die Sperrzeit entsprechend verlängert. |