

Wie man das WGS 365 Passwort ändert/zurücksetzt (einschließlich E-Mail, Teams, OneDrive und SharePoint)

Ihr Passwort muss alle 180 Tage geändert werden und sollte mindestens 12 Zeichen enthalten, einschließlich Symbole, alphanumerische Zeichen, Zahlen und Sonderzeichen (3 von 4 Kategorien müssen erfüllt sein).

Schritt 1: Wählen Sie die erhaltene E-Mail aus (Betreff: IT-Information: Ihr Passwort läuft in 28 Tagen ab!) oder klicken Sie auf den folgenden Link:

[wgsinstructions - Würth IT GmbH - ONE IT -](#)

Schritt 2: Wählen Sie "WGS Passwort ändern", wenn Ihr Passwort abgelaufen ist. (Wenn Sie Ihr Passwort vergessen haben, wählen Sie bitte "WGS Passwort zurücksetzen". Voraussetzung dafür ist das WSL-Token.)

Würth Global Services - Passwort Self-Service

WGS Passwort ändern

Verwenden Sie "WGS Passwort ändern", wenn Sie Ihr aktuelles WGS Passwort noch kennen und dieses ändern möchten.

WGS Passwort zurücksetzen

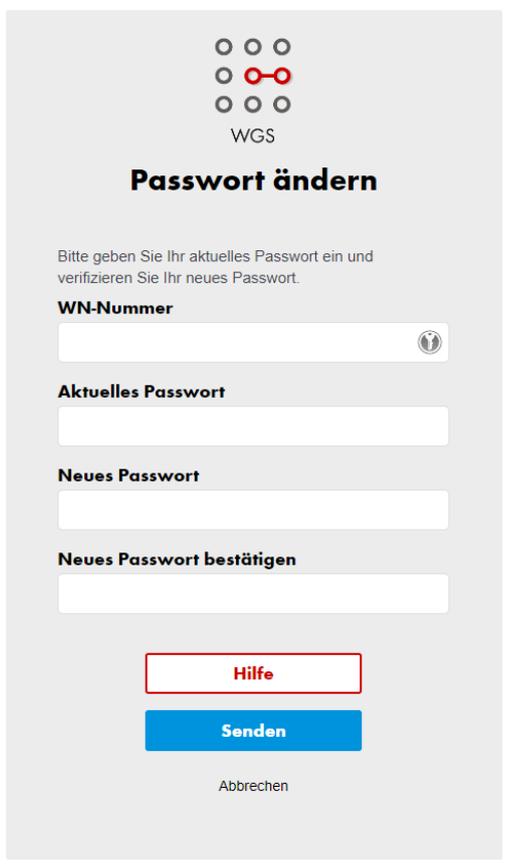
Verwenden Sie "WGS Passwort zurücksetzen", wenn Sie Ihr WGS Passwort vergessen haben und dieses zurücksetzen möchten. **Voraussetzung: WSL-Token**

Bitte beachten Sie die seit 04/2023 gültige neue Passwort-Richtlinie:

- > Die Kennwortlänge muss mindestens 12 Zeichen betragen
(bei privilegierten LA-/CA-Accounts: 15 Zeichen)
- > Passwörter müssen aus den Kategorien Groß- und Kleinbuchstaben, Ziffern sowie Sonderzeichen bestehen (3 von 4 Kategorien müssen erfüllt sein).

Darüber hinaus gelten weiterhin die bereits bestehenden  [Richtlinien](#).

Schritt 3: Füllen Sie Ihre Daten gemäß dem Titel jedes Feldes aus. Bitte beachten Sie, dass die WN-Nummer mit WN***** beginnen sollte, gefolgt von Ihrem WGS-Passwort.



WGS

Passwort ändern

Bitte geben Sie Ihr aktuelles Passwort ein und verifizieren Sie Ihr neues Passwort.

WN-Nummer

Aktuelles Passwort

Neues Passwort

Neues Passwort bestätigen

[Hilfe](#)

[Senden](#)

[Abbrechen](#)

Schritt 4: Klicken Sie auf "Absenden" und Sie sollten eine Bestätigung erhalten, dass die Änderung erfolgreich war.

WICHTIG:

Nach einigen Minuten werden einige Systeme Sie nach dem neuen Passwort fragen.

Option 1: Wenn Sie sich im Würth-Netzwerk befinden (verbunden mit LAN oder WiFi), sollte Ihr Benutzername in diesem Format sein: wn*****@wgs.wuerth.com, gefolgt von dem neuen WGS-Passwort, das Sie erstellt haben.

Option 2: Wenn Sie sich außerhalb des Würth-Netzwerks befinden (Arbeiten von zu Hause oder mobile Daten), sollte Ihre Benutzer-ID in diesem Format sein: wn*****, gefolgt von Ihrem WSL-Passcode. Sobald Sie eingeloggt sind, wird Ihre WSL-Token-APP auf Ihrem Handy Sie auffordern, die Anmeldung zu bestätigen, um sich erfolgreich im System anzumelden.

Richtlinien für Ihr WGS-Passwort

Bitte beachten Sie die folgenden Passwort-Richtlinien, wenn Sie Ihr Passwort ändern:

- Alle 180 Tage werden Sie aufgefordert, Ihr Passwort zu ändern.
- Die letzten 24 Passwörter dürfen nicht wiederverwendet werden.
- Passwörter müssen mindestens 12 Zeichen lang sein (15 Zeichen für privilegierte Konten) und aus den Kategorien Groß- und Kleinbuchstaben, Zahlen sowie Sonderzeichen bestehen (3 von 4 Kategorien müssen erfüllt sein).
- Das Passwort wird gegen eine Passwort-Blacklist überprüft, Passwörter wie "herbst2018" oder "PW4WGS1234" sind nicht erlaubt. Bestimmte Zeichenfolgen, wie "1234", "würth" oder "aaaa", dürfen generell nicht in einem Passwort erscheinen, unabhängig davon, wie komplex die anderen Teile des Passworts sind.
- Namen, firmenbezogene Bezeichnungen, Geburtsdaten, Telefonnummern oder Ähnliches dürfen nicht verwendet werden.
- Das Passwort muss mindestens einen Tag alt sein, bevor es erneut geändert werden kann.
- Wenn das Passwort innerhalb von 30 Minuten 5 Mal falsch eingegeben wird, wird das Konto aus Sicherheitsgründen für 30 Minuten gesperrt.
- Für jedes verwendete System, jede Anwendung, jedes Portal usw. muss ein anderes Passwort verwendet werden.

Info: Wenn ein Passwort nicht akzeptiert wird, überprüfen Sie die Einhaltung der oben genannten Regeln. Wenn ein Passwort aufgrund der Passwort-Blacklist nicht akzeptiert wird, verwenden Sie ein völlig neues Passwort. Die Einhaltung der Passwort-Richtlinien, insbesondere der Passwort-Blacklist, soll verhindern, dass öffentlich bekannte Passwörter, Standardpasswörter und sehr schwache Passwörter verwendet werden. Die technische Überprüfung durch die oben genannten Regeln ersetzt jedoch nicht zu 100 % die persönliche Verantwortung für die Wahl eines sicheren Passworts.