

Passwoerter selbst aendern

Passwoerter selbst aendern

Du kannst SSH-/SFTP- und Datenbank-Passwoerter jederzeit selbst rotieren — direkt aus deinem Container per CLI. Kein Ticket, keine Wartezeit.

Der Befehl ist `webunit-password`. Rotation ist **sofort wirksam** und das neue Passwort wird **einmalig** angezeigt — kopieren und speichern.

SSH-/SFTP-Passwort

```
$ webunit-password ssh
```

Das aktuelle SSH-Passwort wird sofort unguelteig. Bestehende Sitzungen bleiben offen, aber neue Logins brauchen das neue Passwort.

Wichtig: vorher eine zweite SSH-Sitzung mit dem neuen Passwort aufmachen und pruefen, dass Login klappt, BEVOR diese Sitzung geschlossen wird. So kommst du nicht versehentlieh aus.

Fortfahren? [j/N] j

Neues SSH-Passwort:

8f3aK2q7mZpxN4Rtv9LcJhBw

Jetzt in einer zweiten Sitzung testen. Erst wenn Login mit dem neuen Passwort klappt, diese Sitzung schliessen.

Wichtig: deine aktuelle SSH-Sitzung laeuft nach der Rotation weiter, SSH prueft das Passwort nur beim Login. Bevor du die Sitzung schliesst, oeffne eine **zweite** SSH-Verbindung mit dem neuen Passwort und pruefe, dass Login klappt. Erst dann die erste Sitzung beenden. Sonst kannst du dich aussperren.

Datenbank-Passwort

Das Label ist der Datenbank-Name aus dem Admin-Panel (meist `main` oder ein Kunden-Name — im Zweifel: Datenbank-Kachel in der Subscription-Ansicht).

```
$ webunit-password db main
```

Das aktuelle Datenbank-Passwort fuer 'main' wird sofort unguelteig.

Deine Anwendung wird die Datenbank nicht mehr erreichen, bis du das neue Passwort in deiner Config eingetragen und die Anwendung neu geladen hast.

Fortfahren? [j/N] j

Neues Datenbank-Passwort (Label: main):

Q7pX2mkV9fLcNhZa8Bwry3Ju

Trage das Passwort in die Config-Datei deiner Anwendung ein und starte die Anwendung neu.

Wichtig: das alte Passwort ist mit der Rotation **weg** — keine Uebergangsphase. Ab dem Moment schlaegt jeder DB-Zugriff mit dem alten Passwort fehl. Direkt danach das neue Passwort in die Konfigurations- Datei deiner Anwendung eintragen und die Anwendung neu laden.

Wo genau das Passwort in deiner Anwendung eingetragen wird, weisst du selbst am besten — je nach Anwendung eine Config-Datei, eine Environment-Variable oder ein Secret-Manager. Nach dem Eintragen die Anwendung neu starten oder ihre Konfiguration neu einlesen lassen.

Was passiert im Hintergrund

Die CLI ruft unseren Node-Dienst auf, der:

1. ein neues Zufalls-Passwort erzeugt (24 Zeichen),
2. es lokal setzt (SSH: `chpasswd`; DB: `ALTER USER ... IDENTIFIED BY`),
3. es an unser Admin-Panel meldet, damit es dauerhaft ist und beim naechsten Sync nicht ueberschrieben wird,
4. es dir einmalig ausgibt.

Das neue Passwort landet nirgends in Logs. Wenn du es verlierst, musst du erneut rotieren.

Alternative: SSH-Key statt Passwort

Sicherer als Passwort-Rotation ist ein SSH-Key. Public-Key einmalig in `~/.ssh/authorized_keys` deines Containers ablegen, danach kannst du den Passwort-Login im Admin-Panel komplett abschalten. Keys ueberleben Container-Recreate automatisch (werden von uns synchronisiert).

Revision #7

Created 5 September 2026 08:34:53 by webunitadmin

Updated 7 September 2026 15:16:16 by webunitadmin