

PASSWORD MANAGER > ENTWICKLERTOOLS

# CLI Authentifizierungsherausforderu

Ansicht im Hilfezentrum:  
<https://bitwarden.com/help/cli-auth-challenges/>

## CLI Authentifizierungsherausforderungen

Die August 2021 Veröffentlichung von Bitwarden (2021-09-21) führte [Captcha](#) Anforderungen ein, um die Sicherheit gegen Bot-Traffic zu erhöhen. Auf der CLI werden CAPTCHA-Herausforderungen durch Authentifizierungsherausforderungen ersetzt, die mit dem [persönlichen API-Schlüssel](#) Ihres Kontos `client_secret` validiert werden können.

### Tip

Für automatisierte Arbeitsabläufe oder die Bereitstellung des Zugriffs auf eine externe Anwendung empfehlen wir die Verwendung der Methode `bw login --apikey`. Diese Methode folgt einem vorhersehbareren Authentifizierungsfluss und das Widerrufen des Zugriffs einer Anwendung oder Maschine kann durch Erneuern des [API-Schlüssels](#) erreicht werden.

## Holen Sie sich Ihren persönlichen API-Schlüssel

Um Ihren persönlichen API-Schlüssel zu erhalten:

1. In der Bitwarden-Web-App navigieren Sie zu **Einstellungen** → **Sicherheit** → **Schlüssel**:

The screenshot shows the Bitwarden web application interface. On the left is a dark blue sidebar with navigation options: Password Manager, Vaults, Send, Tools, Reports, Settings, My account, Security (highlighted), Preferences, Subscription, Domain rules, Emergency access, and Free Bitwarden Famili... The main content area is titled 'Security' and has three tabs: 'Master password', 'Two-step login', and 'Keys' (selected). Under the 'Keys' tab, there is a section for 'Encryption key settings'. A yellow warning box states: 'Warning: Proceeding will log you out of all active sessions. You will need to log back in and complete two-step login, if any. We recommend exporting your vault before changing your encryption settings to prevent data loss.' Below this, text explains that higher KDF iterations protect the master password from brute force attacks, but higher values may cause performance issues on older devices. Two input fields are shown: 'KDF algorithm (required)' set to 'PBKDF2 SHA-256' and 'KDF iterations' set to '600000'. A note below the iterations field says 'We recommend 600,000 or more'. A 'Change KDF' button is present. Below the encryption settings is the 'API Key' section, which states 'Your API key can be used to authenticate in the Bitwarden CLI.' and contains two buttons: 'View API key' and 'Rotate API key'.

Schlüssel

2. Wählen Sie die Schaltfläche **API-Schlüssel anzeigen** und geben Sie Ihr Master-Passwort ein, um den Zugriff zu bestätigen.

3. Aus dem **API-Schlüssel** Dialogfeld, kopieren Sie den Wert von **client\_secret**, der eine zufällige Zeichenfolge wie **efrbgT9C6BogEfXi5pZc48XyJjfpR** ist.

## Herausforderungen beantworten

Abhängig von Ihren Präferenzen können Sie [eine Umgebungsvariable speichern](#), um Authentifizierungsherausforderungen automatisch zu bestehen, oder Ihr **client\_secret** bei jeder Herausforderung **manuell eingeben**:

### Beantworte Herausforderungen mit einer Umgebungsvariable

Authentifizierungsherausforderungen suchen nach einer nicht-leeren Umgebungsvariable **BW\_CLIENTSECRET**, bevor Sie aufgefordert werden, eine manuell einzugeben. Das Speichern dieser Variablen mit dem [abgerufenen client\\_secret Wert](#) ermöglicht es Ihnen, Authentifizierungsherausforderungen automatisch zu bestehen. Um diese Umgebungsvariable zu speichern:

 Bash

*Bash*

```
export BW_CLIENTSECRET="client_secret"
```

 PowerShell

*Bash*

```
env: BW_CLIENTSECRET="client_secret"
```

#### Warning

Wenn Ihr **client\_secret** falsch ist, erhalten Sie einen Fehler. In den meisten Fällen liegt dies daran, dass Sie Ihren **API-Schlüssel erneuert** haben, seitdem Sie die Variable gespeichert haben. [Führen Sie die oben genannten Schritte aus](#), um den korrekten Wert abzurufen.

### Beantworte Herausforderungen manuell

Wenn eine Authentifizierungsaufforderung gestellt wird und kein **BW\_CLIENTSECRET** Wert gefunden wird, werden Sie aufgefordert, Ihren **client\_secret** Wert manuell einzugeben:

