VR Headset Meta Account Relinking Anleitung

Zweck & Kontext

Diese Anleitung behandelt den Prozess der Wiederverbindung eines VR-Headsets mit seinem zugehörigen Meta-Konto, wenn die Verbindung unterbrochen oder verloren gegangen ist. Konto-Relinking wird notwendig, wenn Headsets ihre Verbindung zu Metas Authentifizierungsservern verlieren, was nach längeren Offline-Perioden, System-Updates oder Konto-Sicherheitsänderungen auftreten kann.

⚠ **Meta**: Meta Hardware und Software (einschließlich MQDH) liegen außerhalb der Kontrolle von WPS. Meta-Updates können unerwartete Funktionalitätsänderungen in VR-Systemen verursachen. WPS überwacht Meta-Veröffentlichungen, um Benutzer über potenzielle Auswirkungen und Änderungen zu informieren.

Voraussetzungen

- Stabile Internetverbindung für sowohl Computer als auch VR-Headset
- E-Mail-Konto-Anmeldedaten, die mit Ihrem VR-Setup verbunden sind *(können von WPS bereitgestellt werden)*
- Meta-Konto-Passwort *(kann von WPS bereitgestellt werden)*
- **Wenn Sie die "Meta Account Access and Security Setup Guide" abgeschlossen haben:**
  - Smartphone mit konfigurierter 2FA-Authenticator-App
  - Zugang zu Ihrem zuvor konfigurierten Authentifizierungsgerät
- **Wenn Sie die "Meta Account Access and Security Setup Guide" NICHT abgeschlossen haben:**
  - Sofortige Koordination mit WPS-Personal für Echtzeit-2FA-Code-Bereitstellung
  - Geplante Zeit mit WPS-Support für geführten Authentifizierungsprozess

Schneller Überblick (für erfahrene Benutzer)

1. Zu `meta.com/device` navigieren und mit Meta-Konto-Anmeldedaten authentifizieren
2. 2FA-Überprüfung mit Ihrem konfigurierten Gerät oder WPS-bereitgestelltem Code abschließen
3. Den achtstelligen Verifikationscode eingeben, der in der VR-Headset-Schnittstelle angezeigt wird
4. Erfolgreiches Relinking bestätigen und kontoabhängige Funktionen testen

Detaillierte Schritte

Zugriff auf Metas Geräteverwaltungsschnittstelle

1. **Zum Geräteverwaltungsportal navigieren**
   - Webbrowser öffnen und direkt zu `meta.com/device` gehen
   - *Diese spezialisierte URL führt Sie direkt zu Metas Geräteverwaltungsschnittstelle*
   - *Vermeiden Sie die Verwendung der allgemeinen meta.com-Seite, da sie zusätzliche Navigationsschritte erfordert*
2. **Konto-Authentifizierung einleiten**
   - **"Continue with email"** aus den verfügbaren Anmeldeoptionen auswählen
   - *Diese Methode bietet den zuverlässigsten Authentifizierungsweg für Kontoverwaltungsaufgaben*

3. **Primäre Authentifizierung abschließen**
    - Die E-Mail-Adresse eingeben, die mit Ihrem VR-Setup verbunden ist
    - **"Next"** klicken, um zur Passwort-Überprüfung zu gelangen
    - **"Enter password instead"** wählen *(einfacher als E-Mail-Code)*
    - Ihr Meta-Konto-Passwort eingeben *(kann von WPS bereitgestellt werden)*
    - **"Log in"** klicken, um zur Zwei-Faktor-Authentifizierung zu gelangen

Zwei-Faktor-Authentifizierung abschließen

4. **2FA-Überprüfung durchführen**

    - System zeigt Dropdown-Menü für verfügbare 2FA-Methoden
    - Die Methode auswählen, die Sie zuvor konfiguriert haben oder wie von WPS-Personal angewiesen
    - **"Next"** klicken, um zur Code-Eingabe zu gelangen
    - Den sechsstelligen Authentifizierungscode aus Ihrer Authenticator-App eingeben
    - *Wenn Sie keine persönliche 2FA konfiguriert haben, verwenden Sie den Code, der von WPS-Personal während Ihrer geplanten Support-Sitzung bereitgestellt wird*
    - **"Next"** klicken, um die Authentifizierung abzuschließen

5. **Anmelde-Persistenz verwalten (optional)**

    - Wählen, ob Anmeldedaten auf diesem Computer gespeichert werden sollen
    - *Das Speichern von Anmeldedaten speichert nur E-Mail- und Passwort-Informationen*
    - *2FA-Überprüfung wird weiterhin für zukünftige Anmeldesitzungen erforderlich sein*
    - *Sicherheitsimplikationen gespeicherter Anmeldedaten auf gemeinsam genutzten Computern berücksichtigen*

6. **Headset-Verifikationscode lokalisieren**

    - VR-Headset aufsetzen oder dessen Display überprüfen
    - *Wenn ein Relink-Code benötigt wird, wird normalerweise nichts anderes im Headset angezeigt*
    - *Dieser Code ist einzigartig für diese Sitzung und läuft nach einer angemessenen Zeit ab*
    - *Den Code sorgfältig notieren, da er groß-/kleinschreibungssensitiv ist und genau eingegeben werden muss*

7. **Verifikationscode eingeben**

    - Zur Meta-Geräteverwaltungsschnittstelle auf Ihrem Computer zurückkehren
    - Bestätigen, dass die korrekten Meta-Konto-Informationen angezeigt werden
    - Den achtstelligen Code von Ihrem Headset in das dafür vorgesehene Feld eingeben
    - *Jeden Buchstaben doppelt überprüfen, bevor Sie fortfahren, da eine falsche Eingabe erfordert, von vorne zu beginnen*
    - **"Continue"** klicken, um den Relinking-Prozess zu starten

8. **Erfolgreiche Verbindung überprüfen**
    - System sollte Bestätigung anzeigen, dass Ihr Gerät wieder verbunden wurde
    - Das Headset sollte aktualisierte Konto-Statusinformationen anzeigen
    - Meta-Konto-Funktionen sollten sofort in der Headset-Schnittstelle verfügbar werden

Fehlerbehebung

Authentifizierung schlägt wiederholt fehl:

- Gmail-Adresse mit VR-Setup-Konto abgleichen
- Passwort-Genauigkeit mit WPS-Personal bestätigen
- Überprüfen, dass Konto Entwicklerrechte aktiviert hat
- Sicherstellen, dass 2FA-Codes aktuell sind (30-Sekunden-Ablauf)

Achtstelliger Code wird von Meta-Schnittstelle nicht akzeptiert:

- Überprüfen, dass Web- und Headset-Meta-Konten übereinstimmen
- Bestätigen, dass achtstelliger Code korrekt eingegeben wurde
- Headset neu starten, um Code zu aktualisieren

Relinking erscheint erfolgreich, aber Konto-Funktionen bleiben unverfügbar:

- Zeit für Konto-Relinking einräumen
- Das Headset neu starten

Wichtige Hinweise

⚠ **Passwort-Koordination**: Niemals versuchen, Meta-Konto-Passwörter eigenständig zu ändern. Passwort-Änderungen immer mit WPS-Personal koordinieren, um technische Support-Aussperrungen zu verhindern und sicherzustellen, dass alle verwandten Systeme notwendige Updates erhalten.

⚠ **Konto-Konsistenz**: Das für das Relinking verwendete Meta-Konto muss exakt mit dem ursprünglich auf dem Headset konfigurierten Konto übereinstimmen. Die Verwendung verschiedener Konten, auch wenn sie zur gleichen Organisation gehören, wird persistente Zugriffsprobleme verursachen.

⚠ **Sicherheits-Timing**: 2FA-Codes sind zeitkritisch. 2FA-Codes laufen alle 30 Sekunden ab.