Meta Account Access and Security Setup Anleitung

Zweck & Kontext

Diese Anleitung bietet vollständigen Zugang zu Ihrem WPS-verwalteten Meta-Konto und richtet sichere Zwei-Faktor-Authentifizierung (2FA) ein. Meta-Konten sind für alle Quest-Headsets erforderlich und können benötigt werden, um Verbindungsprobleme zu lösen, Geräteeinstellungen zu verwalten oder VR-Anwendungen zu troubleshooten.

⚠ **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

- Eine Internetverbindung
- E-Mail-Konto-Anmeldedaten, die mit Ihrem VR-Setup verbunden sind *(können von WPS bereitgestellt werden)*
- Meta-Konto-Passwort *(kann von WPS bereitgestellt werden)*
- Smartphone mit 2FA-App-Funktionalität
- Erste Koordination mit WPS-Personal für erstmalige Anmeldung

Schneller Überblick (für erfahrene Benutzer)

1. Zu `meta.com` navigieren und sich mit WPS-bereitgestellten Anmeldedaten anmelden
2. 2FA-Überprüfung mit WPS-bereitgestelltem Code abschließen
3. Authenticator-App für laufende Sicherheit einrichten
4. **Accounts Center** für Profilverwaltung aufrufen

Detaillierte Schritte

Erster Kontozugang

1. **Zu Meta navigieren**
    - Webbrowser öffnen und zu `meta.com` gehen
2. **Anmeldung aufrufen**
    - **Account-Symbol** *(Personensilhouette)* oben rechts klicken
    - **"Sign up or log into a Meta account"** auswählen
    - **"Continue with email"** wählen

3. **Anmeldedaten eingeben**
    - E-Mail-Adresse eingeben, die mit Ihrem VR-Setup verbunden ist
    - **"Next"** klicken
    - **"Enter password instead"** wählen *(einfacher als E-Mail-Code)*
    - Ihr Meta-Konto-Passwort eingeben *(kann von WPS bereitgestellt werden)*
    - **"Log in"** klicken

Zwei-Faktor-Authentifizierung

4. **Erste 2FA abschließen**

    - 2FA-Methode aus Dropdown auswählen *(WPS wird spezifizieren, welche)*
    - **"Next"** klicken
    - 6-stelligen Code eingeben, der von WPS-Personal bereitgestellt wird
    - **"Next"** klicken

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. **Konto-Dashboard aufrufen**

    - Sie kehren zur `meta.com` Hauptseite zurück
    - **Account-Symbol** erneut klicken, um auf Kontofunktionen zuzugreifen *(Symbol ist jetzt ein Kreis mit einem Buchstaben oder Logo)*
    - **"Accounts Center"** für Haupt-Dashboard auswählen

Ihr eigenes 2FA-Gerät einrichten

Dieser Abschnitt ermöglicht es Personal, ihre eigenen 2FA-Codes zu generieren

7. **Authenticator-App installieren (Empfohlen)**

    - *Eine Authenticator-Anwendung ermöglicht Verwaltung durch mehrere Personen*
    - **Google Authenticator** *(empfohlen)* oder **Authy** herunterladen
    - *Verfügbar sowohl auf iOS als auch Android*
    - *Mehrere Mitarbeiter können denselben Authenticator für gemeinsames Konto verwenden*
    - *SMS- oder WhatsApp-Authentifizierung ist nur für eine Telefonnummer verfügbar*

8. **Zu Sicherheitseinstellungen navigieren**

    - Im **Accounts Center** auf **"Password and security"** klicken
    - **"Two-factor authentication"** auswählen
    - Ihr Profil wählen
    - **"Authentication app"** auswählen und zu Schritt 9 weitergehen *(empfohlen)*
    - **"SMS or WhatsApp"** auswählen und zu Schritt 12 weitergehen

2FA über Authentication App

9. **Neues Gerät hinzufügen**
    - **"Add"**-Schaltfläche klicken
    - *QR-Code und Setup-Schlüssel erscheinen*
    - *Zu Ihrem Telefon für die nächsten Schritte wechseln*
10. **Authenticator-App konfigurieren**
    - Authenticator-App auf dem Telefon öffnen
    - Neues Konto hinzufügen *(+ Symbol)*
    - **"Scan QR code"** oder **"Enter setup key"** wählen
    - QR-Code von der Meta-Website scannen
11. **Setup abschließen**
    - Beschreibenden Namen für dieses Gerät eingeben *(z.B. WPSVR GAuth oder Alex's GAuth)*
    - 6-stelligen Code aus der Authenticator-App eingeben
    - **"Done"** klicken
    - *Gerät erscheint jetzt in der 2FA-Geräteliste*

2FA über SMS oder WhatsApp

12. **Telefonnummer hinzufügen**
    - Ländercode bei Bedarf ändern *(standardmäßig Vereinigte Staaten)*
    - Telefonnummer eingeben
    - **"Next"** klicken
    - Den 6-stelligen Code eingeben, der an das Gerät gesendet wurde
    - **"Done"** klicken

Kontoverwaltungsoptionen

13. **Profilverwaltung**
    - **"Profiles"** in der linken Seitenleiste aufrufen
    - Name, Benutzername, Profilbild oder Avatar bearbeiten
    - *Änderungen wirken sich auf die VR-Headset-Anzeige aus*
14. **Passwort-Änderungen**
    - In **"Password and security" "Change password"** auswählen
    - ⚠ Niemals Passwörter ohne WPS-Koordination ändern. Dies verhindert technische Support-Aussperrungen.

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)

"Add"-Schaltfläche für 2FA ausgegraut:

- Konto hat möglicherweise maximale Anzahl verknüpfter Geräte
- WPS kontaktieren, um ungenutzte Geräte zu entfernen
- Einige Kontotypen haben Gerätebegrenzungen

Kann Profil/Einstellungen nicht sehen:

- Sicherstellen, dass Sie im korrekten Konto angemeldet sind
- Versuchen, sich ab- und wieder anzumelden
- Browser-Cache leeren, wenn Problem anhält

Änderungen werden nicht gespeichert oder mit Headset synchronisiert:

- Einige Minuten für vollständige Synchronisation einräumen
- Headset neu starten, um Konto-Aktualisierung zu erzwingen
- Stabile Internetverbindung auf beiden Geräten überprüfen

Wichtige Sicherheitshinweise

⚠ **Passwort-Koordination**: Niemals Passwörter ohne WPS-Koordination ändern. Dies verhindert technische Support-Aussperrungen.

⚠ **2FA-Methodenwahl**: Wenn SMS oder WhatsApp als 2FA-Methode ausgewählt wurde, hat WPS keinen Zugang zu diesen Nachrichten, um bei Konto-Anmeldung, Geräteverknüpfung oder Konto-Wiederherstellung zu helfen.

⚠ **2FA-Gerätfreigabe**: Mehrere Mitarbeiter können sicher Authenticator-Apps für dasselbe Konto verwenden. Jedes Gerät erhält einen eindeutigen Namen.

⚠ **Zeitempfindlichkeit**: 2FA-Codes laufen alle 30 Sekunden ab. Countdown-Timer in der Authenticator-App beobachten.

2FA-Sicherheit verstehen

Warum 2FA erforderlich ist:

- Meta macht 2FA für die meisten Konten obligatorisch
- Schützt vor unbefugtem Zugang

Wie Codes funktionieren:

- Apps generieren zeitbasierte Codes
- Codes synchronisieren sich mit Metas Servern

Nächste Schritte

Mit etabliertem Meta-Kontozugang:

- VR-Headset-Verbindung und -Kopplung testen
- Überprüfen, dass Profilinformationen korrekt im Headset erscheinen
- 2FA-Setup für andere Mitarbeiter dokumentieren
- Backup-Zugangsverfahren mit WPS etablieren