Meta Account Access and Security Setup Guide

Purpose & Context

This guide provides complete access to your WPS-managed Meta account and sets up secure two-factor authentication (2FA). Meta accounts are required for all Quest headsets and may be needed to resolve connection issues, manage device settings, or troubleshoot VR applications.

⚠ **Meta**: Meta hardware and software (including MQDH) are outside WPS control. Meta updates may cause unexpected functionality changes in VR systems. WPS monitors Meta releases to inform users of potential impacts and changes.

Prerequisites

- An internet connection
- Email account credentials associated with your VR setup *(may be provided by WPS)*
- Meta account password *(may be provided by WPS)*
- Smartphone with 2FA app capability
- Initial coordination with WPS staff for first-time login

Quick Overview (for experienced users)

1. Navigate to `meta.com` and log in with WPS-provided credentials
2. Complete 2FA verification using WPS-provided code
3. Set up authenticator app for ongoing security
4. Access **Accounts Center** for profile management

Detailed Steps

Initial Account Access

1. **Navigate to Meta**
    - Open web browser and go to `meta.com`
2. **Access login**
    - Click **account icon** *(person silhouette)* in upper right
    - Select **"Sign up or log into a Meta account"**
    - Choose **"Continue with email"**
3. **Enter credentials**
    - Enter Email address associated with your VR setup
    - Click **"Next"**
    - Choose **"Enter password instead"** *(easier than email code)*
    - Enter your Meta account password *(may be provided by WPS)*
    - Click **"Log in"**

Two-Factor Authentication

4. **Complete initial 2FA**
    - Select 2FA method from dropdown *(WPS will specify which)*
    - Click **"Next"**
    - Enter 6-digit code provided by WPS staff
    - Click **"Next"**
5. **Manage login persistence (optional)**
    - Choose whether to save login credentials on this computer
    - *Saving credentials only stores email and password information*
    - *2FA verification will still be required for future login sessions*
    - *Consider security implications of saved credentials on shared computers*
6. **Access account dashboard**
    - You'll return to `meta.com` main page
    - Click **account icon** again to access account features *(icon is now a circle with a letter or Logo)*
    - Select **"Accounts Center"** for main dashboard

Setting Up Your Own 2FA Device

This section enables staff to generate their own 2FA codes

7. **Install authenticator app (Recommended)**
    - *An authenticator application allows management by multiple people*
    - Download **Google Authenticator** *(recommended)* or **Authy**
    - *Available on both iOS and Android*
    - *Multiple staff can use same authenticator for shared account*
    - *SMS or WhatsApp authentication is available to only one phone number*
8. **Navigate to security settings**
    - In **Accounts Center**, click **"Password and security"**
    - Select **"Two-factor authentication"**
    - Choose your profile
    - Select **"Authentication app"** and continue to step 9 *(recommended)*
    - Select **"SMS or WhatsApp"** and continue to step 12

2FA via Authentication App

9. **Add new device**
    - Click **"Add"** button
    - *QR code and setup key will appear*
    - *Switch to your phone for next steps*

10. **Configure authenticator app**
    - Open authenticator app on phone
    - Add new account *(+ icon)*
    - Choose **"Scan QR code"** or **"Enter setup key"**
    - Scan QR code from Meta website
11. **Complete setup**
    - Enter descriptive name for this device *(eg WPSVR GAuth or Alex's GAuth)*
    - Input 6-digit code from authenticator app
    - Click **"Done"**
    - *Device now appears in 2FA devices list*

2FA via SMS or WhatsApp

12. **Add Phone Number**
    - Change Country code if needed *(defaults to United States)*
    - Enter Phone Number
    - Click **"Next"**
    - Input the 6-digit code sent to the device
    - Click **"Done"**

Account Management Options

13. **Profile management**
    - Access **"Profiles"** in left sidebar
    - Edit name, username, profile picture, or avatar
    - *Changes affect VR headset display*
14. **Password changes**
    - In **"Password and security"**, select **"Change password"**
    - ⚠ Never change passwords without WPS coordination. This prevents technical support lockouts.

Troubleshooting

Authentication fails repeatedly:

- Verify Gmail address matches VR setup account
- Confirm password accuracy with WPS staff
- Check that account has developer privileges enabled
- Ensure 2FA codes are current (30-second expiration)

"Add" button greyed out for 2FA:

- Account may have maximum devices linked
- Contact WPS to remove unused devices
- Some account types have device limits

Cannot see profile/settings:

- Ensure you're logged into correct account
- Try logging out and back in
- Clear browser cache if persistent

Changes not saving or syncing to headset:

- Allow several minutes for synchronization to complete
- Restart the headset to force account refresh
- Verify stable internet connection on both devices

Important Security Notes

⚠ **Password Coordination**: Never change passwords without WPS coordination. This prevents technical support lockouts.

⚠ **2FA Method Choice**: If SMS or WhatsApp was selected as 2FA method, WPS will not have access to these messages to assist with account login, device linking, or account recovery.

⚠ **2FA Device Sharing**: Multiple staff can safely use authenticator apps for same account. Each device gets unique name.

⚠ **Time Sensitivity**: 2FA codes expire every 30 seconds. Watch countdown timer in authenticator app.

Understanding 2FA Security

Why 2FA is required:

- Meta mandates 2FA for most accounts
- Protects against unauthorized access

How codes work:

- Apps generate time-based codes
- Codes sync with Meta's servers

Next Steps

With Meta account access established:

- Test VR headset connection and pairing
- Verify profile information appears correctly in headset
- Document 2FA setup for other staff members
- Establish backup access procedures with WPS