Guía de Configuración de Acceso y Seguridad de Cuenta Meta

Propósito y Contexto

Esta guía proporciona acceso completo a tu cuenta Meta gestionada por WPS y configura autenticación segura de dos factores (2FA). Las cuentas Meta son requeridas para todos los visores Quest y pueden ser necesarias para resolver problemas de conexión, gestionar configuraciones del dispositivo o solucionar problemas de aplicaciones VR.

⚠ **Meta**: El hardware y software de Meta (incluyendo MQDH) están fuera del control de WPS. Las actualizaciones de Meta pueden causar cambios inesperados en la funcionalidad de los sistemas VR. WPS monitorea los lanzamientos de Meta para informar a los usuarios sobre posibles impactos y cambios.

Prerrequisitos

- Una conexión a internet
- Credenciales de cuenta de email asociadas con tu configuración VR *(pueden ser proporcionadas por WPS)*
- Contraseña de cuenta Meta *(puede ser proporcionada por WPS)*
- Smartphone con capacidad de aplicación 2FA
- Coordinación inicial con personal de WPS para primer inicio de sesión

Resumen Rápido (para usuarios experimentados)

1. Navegar a `meta.com` e iniciar sesión con credenciales proporcionadas por WPS
2. Completar verificación 2FA usando código proporcionado por WPS
3. Configurar aplicación autenticadora para seguridad continua
4. Acceder a **Accounts Center** para gestión de perfil

Pasos Detallados

Acceso Inicial a la Cuenta

1. **Navegar a Meta**
    - Abrir navegador web e ir a `meta.com`
2. **Acceder al inicio de sesión**
    - Hacer clic en **ícono de cuenta** *(silueta de persona)* en la parte superior derecha
    - Seleccionar **"Sign up or log into a Meta account"**
    - Elegir **"Continue with email"**

3. **Ingresar credenciales**
    - Ingresar dirección de Email asociada con tu configuración VR
    - Hacer clic en **"Next"**
    - Elegir **"Enter password instead"** *(más fácil que código de email)*
    - Ingresar tu contraseña de cuenta Meta *(puede ser proporcionada por WPS)*
    - Hacer clic en **"Log in"**

Autenticación de Dos Factores

4. **Completar 2FA inicial**

    - Seleccionar método 2FA del menú desplegable *(WPS especificará cuál)*
    - Hacer clic en **"Next"**
    - Ingresar código de 6 dígitos proporcionado por personal de WPS
    - Hacer clic en **"Next"**

5. **Gestionar persistencia de inicio de sesión (opcional)**

    - Elegir si guardar credenciales de inicio de sesión en esta computadora
    - *Guardar credenciales solo almacena información de email y contraseña*
    - *La verificación 2FA aún será requerida para futuras sesiones de inicio de sesión*
    - *Considerar implicaciones de seguridad de credenciales guardadas en computadoras compartidas*

6. **Acceder al panel de cuenta**

    - Regresarás a la página principal de `meta.com`
    - Hacer clic en **ícono de cuenta** nuevamente para acceder a características de cuenta *(el ícono ahora es un círculo con una letra o Logo)*
    - Seleccionar **"Accounts Center"** para el panel principal

Configurando Tu Propio Dispositivo 2FA

Esta sección permite al personal generar sus propios códigos 2FA

7. **Instalar aplicación autenticadora (Recomendado)**

    - *Una aplicación autenticadora permite gestión por múltiples personas*
    - Descargar **Google Authenticator** *(recomendado)* o **Authy**
    - *Disponible tanto en iOS como Android*
    - *Múltiples miembros del personal pueden usar el mismo autenticador para cuenta compartida*
    - *La autenticación SMS o WhatsApp está disponible solo para un número de teléfono*

8. **Navegar a configuraciones de seguridad**

    - En **Accounts Center**, hacer clic en **"Password and security"**
    - Seleccionar **"Two-factor authentication"**
    - Elegir tu perfil
    - Seleccionar **"Authentication app"** y continuar al paso 9 *(recomendado)*
    - Seleccionar **"SMS or WhatsApp"** y continuar al paso 12

2FA vía Aplicación de Autenticación

9. **Agregar nuevo dispositivo**
    - Hacer clic en el botón **"Add"**
    - *Aparecerán código QR y clave de configuración*
    - *Cambiar a tu teléfono para los siguientes pasos*

10. **Configurar aplicación autenticadora**
    - Abrir aplicación autenticadora en teléfono
    - Agregar nueva cuenta *(ícono +)*
    - Elegir **"Scan QR code"** o **"Enter setup key"**
    - Escanear código QR del sitio web Meta

11. **Completar configuración**
    - Ingresar nombre descriptivo para este dispositivo *(ej WPSVR GAuth o GAuth de Alex)*
    - Ingresar código de 6 dígitos de la aplicación autenticadora
    - Hacer clic en **"Done"**
    - *El dispositivo ahora aparece en la lista de dispositivos 2FA*

2FA vía SMS o WhatsApp

12. **Agregar Número de Teléfono**
    - Cambiar código de País si es necesario *(por defecto Estados Unidos)*
    - Ingresar Número de Teléfono
    - Hacer clic en **"Next"**
    - Ingresar el código de 6 dígitos enviado al dispositivo
    - Hacer clic en **"Done"**

Opciones de Gestión de Cuenta

13. **Gestión de perfil**
    - Acceder a **"Profiles"** en la barra lateral izquierda
    - Editar nombre, nombre de usuario, foto de perfil o avatar
    - *Los cambios afectan la visualización del visor VR*

14. **Cambios de contraseña**
    - En **"Password and security"**, seleccionar **"Change password"**
    - ⚠ Nunca cambiar contraseñas sin coordinación con WPS. Esto previene bloqueos de soporte técnico.

Solución de Problemas

La autenticación falla repetidamente:

- Verificar que la dirección Gmail coincida con la cuenta de configuración VR
- Confirmar precisión de contraseña con personal de WPS
- Verificar que la cuenta tenga privilegios de desarrollador habilitados
- Asegurar que los códigos 2FA sean actuales (expiración de 30 segundos)

Botón "Add" deshabilitado para 2FA:

- La cuenta puede tener el máximo de dispositivos vinculados
- Contactar WPS para remover dispositivos no utilizados
- Algunos tipos de cuenta tienen límites de dispositivos

No se puede ver perfil/configuraciones:

- Asegurar que estés conectado a la cuenta correcta
- Intentar cerrar sesión y volver a iniciar
- Limpiar caché del navegador si persiste

Los cambios no se guardan o sincronizan al visor:

- Permitir varios minutos para que la sincronización se complete
- Reiniciar el visor para forzar actualización de cuenta
- Verificar conexión estable a internet en ambos dispositivos

Notas Importantes de Seguridad

⚠ **Coordinación de Contraseña**: Nunca cambiar contraseñas sin coordinación con WPS. Esto previene bloqueos de soporte técnico.

⚠ **Elección de Método 2FA**: Si se seleccionó SMS o WhatsApp como método 2FA, WPS no tendrá acceso a estos mensajes para asistir con inicio de sesión de cuenta, vinculación de dispositivos o recuperación de cuenta.

⚠ **Compartir Dispositivo 2FA**: Múltiples miembros del personal pueden usar aplicaciones autenticadoras de forma segura para la misma cuenta. Cada dispositivo obtiene un nombre único.

⚠ **Sensibilidad al Tiempo**: Los códigos 2FA expiran cada 30 segundos. Observar el temporizador de cuenta regresiva en la aplicación autenticadora.

Entendiendo la Seguridad 2FA

Por qué se requiere 2FA:

- Meta exige 2FA para la mayoría de las cuentas
- Protege contra acceso no autorizado

Cómo funcionan los códigos:

- Las aplicaciones generan códigos basados en tiempo
- Los códigos se sincronizan con los servidores de Meta

Siguientes Pasos

Con acceso a cuenta Meta establecido:

- Probar conexión y emparejamiento del visor VR
- Verificar que la información del perfil aparezca correctamente en el visor
- Documentar configuración 2FA para otros miembros del personal
- Establecer procedimientos de acceso de respaldo con WPS