Guia de Configuração de Acesso e Segurança da Conta Meta

Propósito e Contexto

Este guia fornece acesso completo à sua conta Meta gerenciada pela WPS e configura autenticação segura de dois fatores (2FA). Contas Meta são necessárias para todos os headsets Quest e podem ser necessárias para resolver problemas de conexão, gerenciar configurações do dispositivo ou solucionar problemas de aplicações VR.

⚠ **Meta**: Hardware e software da Meta (incluindo MQDH) estão fora do controle da WPS. Atualizações da Meta podem causar mudanças inesperadas de funcionalidade em sistemas VR. A WPS monitora lançamentos da Meta para informar usuários sobre potenciais impactos e mudanças.

Pré-requisitos

- Uma conexão com a internet
- Credenciais de conta de email associadas com sua configuração VR *(podem ser fornecidas pela WPS)*
- Senha da conta Meta *(pode ser fornecida pela WPS)*
- Smartphone com capacidade de aplicativo 2FA
- Coordenação inicial com equipe WPS para primeiro login

Visão Geral Rápida (para usuários experientes)

1. Navegar para `meta.com` e fazer login com credenciais fornecidas pela WPS
2. Completar verificação 2FA usando código fornecido pela WPS
3. Configurar app autenticador para segurança contínua
4. Acessar **Accounts Center** para gerenciamento de perfil

Passos Detalhados

Acesso Inicial à Conta

1. **Navegar para Meta**
    - Abrir navegador web e ir para `meta.com`
2. **Acessar login**
    - Clicar **ícone da conta** *(silhueta de pessoa)* no canto superior direito
    - Selecionar **"Sign up or log into a Meta account"**
    - Escolher **"Continue with email"**

3. **Inserir credenciais**
    - Inserir endereço de Email associado com sua configuração VR
    - Clicar **"Next"**
    - Escolher **"Enter password instead"** *(mais fácil que código de email)*
    - Inserir sua senha da conta Meta *(pode ser fornecida pela WPS)*
    - Clicar **"Log in"**

Autenticação de Dois Fatores

4. **Completar 2FA inicial**

    - Selecionar método 2FA do dropdown *(WPS especificará qual)*
    - Clicar **"Next"**
    - Inserir código de 6 dígitos fornecido pela equipe WPS
    - Clicar **"Next"**

5. **Gerenciar persistência de login (opcional)**

    - Escolher se salvar credenciais de login neste computador
    - *Salvar credenciais armazena apenas informações de email e senha*
    - *Verificação 2FA ainda será necessária para futuras sessões de login*
    - *Considere implicações de segurança de credenciais salvas em computadores compartilhados*

6. **Acessar painel da conta**

    - Você retornará à página principal `meta.com`
    - Clicar **ícone da conta** novamente para acessar funcionalidades da conta *(ícone agora é um círculo com uma letra ou Logo)*
    - Selecionar **"Accounts Center"** para painel principal

Configurando Seu Próprio Dispositivo 2FA

Esta seção permite que equipe gere seus próprios códigos 2FA

7. **Instalar app autenticador (Recomendado)**

    - *Uma aplicação autenticadora permite gerenciamento por múltiplas pessoas*
    - Baixar **Google Authenticator** *(recomendado)* ou **Authy**
    - *Disponível tanto no iOS quanto Android*
    - *Múltipla equipe pode usar mesmo autenticador para conta compartilhada*
    - *Autenticação SMS ou WhatsApp está disponível para apenas um número de telefone*

8. **Navegar para configurações de segurança**

    - No **Accounts Center**, clicar **"Password and security"**
    - Selecionar **"Two-factor authentication"**
    - Escolher seu perfil
    - Selecionar **"Authentication app"** e continuar para passo 9 *(recomendado)*
    - Selecionar **"SMS or WhatsApp"** e continuar para passo 12

2FA via App de Autenticação

9. **Adicionar novo dispositivo**
    - Clicar botão **"Add"**
    - *Código QR e chave de configuração aparecerão*
    - *Mudar para seu telefone para próximos passos*
10. **Configurar app autenticador**
    - Abrir app autenticador no telefone
    - Adicionar nova conta *(ícone +)*
    - Escolher **"Scan QR code"** ou **"Enter setup key"**
    - Escanear código QR do site Meta
11. **Completar configuração**
    - Inserir nome descritivo para este dispositivo *(ex WPSVR GAuth ou GAuth do Alex)*
    - Inserir código de 6 dígitos do app autenticador
    - Clicar **"Done"**
    - *Dispositivo agora aparece na lista de dispositivos 2FA*

2FA via SMS ou WhatsApp

12. **Adicionar Número de Telefone**
    - Mudar código do País se necessário *(padrão é Estados Unidos)*
    - Inserir Número de Telefone
    - Clicar **"Next"**
    - Inserir o código de 6 dígitos enviado para o dispositivo
    - Clicar **"Done"**

Opções de Gerenciamento de Conta

13. **Gerenciamento de perfil**
    - Acessar **"Profiles"** na barra lateral esquerda
    - Editar nome, nome de usuário, foto de perfil ou avatar
    - *Mudanças afetam exibição do headset VR*
14. **Mudanças de senha**
    - Em **"Password and security"**, selecionar **"Change password"**
    - ⚠ Nunca mude senhas sem coordenação WPS. Isso previne bloqueios de suporte técnico.

Solução de Problemas

Autenticação falha repetidamente:

- Verificar se endereço Gmail corresponde à conta de configuração VR
- Confirmar precisão da senha com equipe WPS
- Verificar se conta tem privilégios de desenvolvedor habilitados
- Garantir que códigos 2FA estão atuais (expiração de 30 segundos)

Botão "Add" acinzentado para 2FA:

- Conta pode ter número máximo de dispositivos vinculados
- Contatar WPS para remover dispositivos não utilizados
- Alguns tipos de conta têm limites de dispositivos

Não consegue ver perfil/configurações:

- Garantir que está logado na conta correta
- Tentar fazer logout e login novamente
- Limpar cache do navegador se persistir

Mudanças não salvam ou sincronizam com headset:

- Permitir vários minutos para sincronização completar
- Reiniciar o headset para forçar atualização da conta
- Verificar conexão estável com internet em ambos dispositivos

Notas Importantes de Segurança

⚠ **Coordenação de Senha**: Nunca mude senhas sem coordenação WPS. Isso previne bloqueios de suporte técnico.

⚠ **Escolha do Método 2FA**: Se SMS ou WhatsApp foi selecionado como método 2FA, WPS não terá acesso a essas mensagens para assistir com login da conta, vinculação de dispositivos ou recuperação de conta.

⚠ **Compartilhamento de Dispositivo 2FA**: Múltipla equipe pode usar com segurança apps autenticadores para a mesma conta. Cada dispositivo recebe nome único.

⚠ **Sensibilidade ao Tempo**: Códigos 2FA expiram a cada 30 segundos. Observe temporizador de contagem regressiva no app autenticador.

Entendendo Segurança 2FA

Por que 2FA é necessário:

- Meta exige 2FA para a maioria das contas
- Protege contra acesso não autorizado

Como códigos funcionam:

- Apps geram códigos baseados em tempo
- Códigos sincronizam com servidores da Meta

Próximos Passos

Com acesso à conta Meta estabelecido:

- Testar conexão e pareamento do headset VR
- Verificar se informações do perfil aparecem corretamente no headset
- Documentar configuração 2FA para outros membros da equipe
- Estabelecer procedimentos de acesso de backup com WPS