Ativar autenticação em dois fatores (2FA)

1. O que é 2FA

A autenticação em dois fatores (2FA) adiciona uma camada extra de segurança.

Além da senha principal, você precisará de um segundo código para acessar sua conta.

Esse código muda constantemente e é gerado por um aplicativo no celular.

---

2. Aplicativos necessários

Você precisará de um app autenticador, como:

- Google Authenticator
- Microsoft Authenticator
- Authy

Esses apps geram códigos temporários de acesso.

---

3. Como ativar o 2FA no Vaultwarden

1. Acesse o Vaultwarden pelo navegador
2. Faça login normalmente
3. Vá em **Configurações da conta**
4. Procure a seção **Segurança / Two-Factor Authentication**
5. Escolha o método **Authenticator App (TOTP)**

---

4. Vinculando o aplicativo

1. O Vaultwarden mostrará um **QR Code**

2. Abra seu aplicativo autenticador no celular
3. Escaneie o QR Code
4. O app começará a gerar códigos de 6 dígitos

---

5. Confirmando a ativação

Após escanear:

1. Digite o código gerado pelo aplicativo
2. Confirme no Vaultwarden
3. O 2FA será ativado

---

6. Códigos de recuperação

O sistema vai gerar **códigos de backup**.

Esses códigos são muito importantes:

- Servem para recuperar acesso caso perca o celular
- Devem ser guardados em local seguro
- Não devem ser compartilhados

---

7. Boas práticas

- Nunca perca o acesso ao seu autenticador
- Salve os códigos de recuperação offline
- Não desative o 2FA depois de ativado
- Use 2FA em todas as contas importantes

Conclusão

Ativar o 2FA no Vaultwarden aumenta significativamente a segurança das suas credenciais. Mesmo que sua senha seja comprometida, o acesso à conta continua protegido por uma segunda camada de autenticação.

Revision #1
Created 30 April 2026 19:32:02 by Jefferson Carneiro
Updated 30 April 2026 19:32:25 by Jefferson Carneiro