Guia básico

- Como usar o Vaultwarden para gerenciar senhas com segurança
- Ativar autenticação em dois fatores (2FA)
- Como organizar suas senhas no Vaultwarden
- Como recuperar uma senha no Vaultwarden
- Como compartilhar senhas com segurança no Vaultwarden

Como usar o Vaultwarden para gerenciar senhas com segurança

Este guia apresenta o uso básico do Vaultwarden, uma solução de cofre de senhas para armazenar credenciais de forma segura em seu ambiente Cloud Server da Safearmor.

---

1. O que é o Vaultwarden

O Vaultwarden é um gerenciador de senhas compatível com Bitwarden, porém mais leve e focado em ambientes auto-hospedados.

Ele permite:

- Armazenar senhas de forma criptografada
- Organizar credenciais por categorias
- Compartilhar senhas com segurança
- Acessar via navegador, app ou extensão

---

2. Acessando o Vaultwarden

Você pode acessar o sistema pelo navegador:

- URL fornecida pela Safearmor (ex: https://vault.safearmor.com.br)
- Login com e-mail e senha principal da sua conta

---

3. Criando sua primeira senha

1. Clique em **“Novo item”**
2. Selecione o tipo (Login, cartão, nota segura etc.)
3. Preencha:

- Nome do serviço
- Usuário
- Senha
- URL (opcional)

4. Clique em **Salvar**

---

4. Gerando senhas seguras

O Vaultwarden possui um gerador interno:

- Clique em **Gerar senha**
- Defina:
  - Tamanho (recomendado: 16+ caracteres)
  - Uso de números e símbolos
- Copie e use a senha gerada

---

5. Organizando suas senhas

Para manter tudo organizado:

- Use **pastas ou coleções**
- Separe por cliente, sistema ou projeto
- Evite duplicar credenciais

---

6. Compartilhamento seguro

Você pode compartilhar senhas com equipe:

- Crie uma **coleção compartilhada**
- Adicione usuários autorizados
- Controle permissões de leitura ou edição

---

7. Boas práticas de segurança

- Nunca reutilize senhas entre sistemas
- Ative autenticação em dois fatores (2FA) quando possível
- Não compartilhe sua senha mestre
- Revise acessos periodicamente

Conclusão

O Vaultwarden é uma ferramenta essencial para centralizar e proteger credenciais em ambientes Cloud Server. Seu uso correto reduz riscos de vazamento e melhora a segurança operacional da infraestrutura.

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.

Como organizar suas senhas no Vaultwarden

Este guia explica como organizar corretamente suas credenciais no Vaultwarden para facilitar o uso no dia a dia e evitar confusão.

---

1. Por que organizar senhas

Quando você começa a usar o Vaultwarden, é comum acumular muitas senhas.

Sem organização, isso pode causar:

- Dificuldade para encontrar logins
- Erros ao acessar sistemas
- Confusão entre contas semelhantes

---

2. Usando pastas (ou coleções)

Você pode separar suas senhas por categorias:

Exemplos:

- Trabalho
- Clientes
- Sistemas internos
- E-mails
- Servidores

Para criar:

1. Vá em **Coleções / Pastas**
2. Clique em **Criar nova coleção**
3. Dê um nome claro
4. Salve

---

3. Nomeando corretamente os itens

Sempre use nomes claros e padronizados:

✔ Bom exemplo:

- “Nextcloud - Cliente A”
- “Painel VPS - Safearmor”
- “E-mail Gmail empresa”

 Evite:

- “login1”
- “senha teste”
- “acesso”

---

4. Usando tags (quando disponível)

Algumas versões permitem tags:

- produção
- teste
- cliente
- interno

Isso ajuda a filtrar rapidamente.

---

5. Separando por tipo de serviço

Uma boa prática é dividir por categoria:

- Logins de sistemas
- Acessos de servidores
- Contas de e-mail
- APIs e integrações

---

6. Evitando duplicação

Não crie várias senhas para o mesmo serviço.

Sempre atualize o item existente ao invés de duplicar.

---

7. Dica de organização profissional

Padrão recomendado:

[Serviço] - [Cliente/Sistema]

Exemplo:

- Nextcloud - Empresa X
- SSH - VPS Produção
- Dashboard - Interno

Conclusão

Uma boa organização no Vaultwarden melhora a produtividade e reduz erros de acesso. Em ambientes profissionais, isso é essencial para manter controle e segurança das credenciais.

Como recuperar uma senha no Vaultwarden

Este guia explica como localizar e recuperar senhas salvas no Vaultwarden de forma rápida e segura.

---

1. Acessando seu cofre

1. Abra o Vaultwarden pelo navegador
2. Faça login com sua conta
3. Aguarde carregar a lista de senhas

---

2. Buscando uma senha

Você pode encontrar uma senha de duas formas:

- Usando a barra de pesquisa no topo
- Navegando pelas pastas ou coleções

Digite o nome do serviço, por exemplo:

- “Nextcloud”
- “SSH”
- “Gmail”

---

3. Visualizando os dados

Ao clicar no item, você verá:

- Nome do serviço
- Usuário ou e-mail
- Senha (oculta por padrão)
- URL do sistema (se cadastrada)

4. Revelando a senha

Para ver a senha:

1. Clique no ícone de **olho (□□)**
2. O sistema pode solicitar sua senha principal novamente
3. A senha será exibida temporariamente

---

5. Copiando usuário e senha

Você pode copiar diretamente:

- Clique em **copiar usuário**
- Clique em **copiar senha**

Depois, cole no sistema onde deseja fazer login.

---

6. O que fazer se não encontrar a senha

Se não localizar o item:

- Verifique outras pastas
- Use termos diferentes na busca
- Confirme se a senha foi salva corretamente

---

7. Dica importante de segurança

- Evite deixar a senha visível após o uso
- Sempre feche a sessão em dispositivos compartilhados
- Não copie senhas em locais inseguros

Conclusão

O Vaultwarden permite recuperar senhas de forma rápida e organizada. O uso correto da busca e das pastas evita perda de tempo e melhora o acesso às credenciais no dia a dia.

Como compartilhar senhas com segurança no Vaultwarden

Este guia explica como compartilhar credenciais de forma controlada no Vaultwarden, sem expor sua senha principal.

---

1. Quando usar compartilhamento

O compartilhamento deve ser usado apenas quando necessário, por exemplo:

- Acesso de equipe a sistemas internos
- Credenciais de servidores ou serviços
- Integrações entre setores ou clientes

Evite compartilhar senhas por mensagens, e-mail ou anotações externas.

---

2. Usando coleções compartilhadas

O método correto é via **coleções (groups)**:

1. Acesse o Vaultwarden
2. Vá em **Coleções**
3. Crie ou selecione uma coleção existente
4. Adicione os itens (senhas) desejados
5. Defina quais usuários terão acesso

---

3. Definindo permissões

Você pode controlar o nível de acesso:

- **Leitura** → apenas visualizar e copiar
- **Edição** → alterar dados da senha
- **Admin (se disponível)** → gerenciar a coleção

Use sempre o menor nível necessário.

---

4. Compartilhamento seguro com equipe

Ao adicionar usuários:

1. Convide o usuário para o Vaultwarden
2. Atribua ele a uma coleção específica
3. Evite acesso global ao cofre completo

---

5. Boas práticas

- Nunca compartilhe sua senha principal
- Use coleções separadas por cliente ou projeto
- Revise acessos regularmente
- Remova usuários quando não forem mais necessários

---

6. Erros comuns

- Enviar senha por chat ou e-mail
- Dar acesso total ao cofre sem necessidade
- Não revogar acessos antigos
- Reutilizar a mesma senha em múltiplos usuários

Conclusão

O Vaultwarden permite compartilhamento seguro de senhas quando usado corretamente. O uso de coleções garante controle, rastreabilidade e redução de riscos em ambientes corporativos.