

# 보안강화

본 장은 앞서 생성된 관리자 계정만 접속을 허용하게 하는 단계입니다.

개인의 중요한 정보가 보관되는 프로그램으로 아래 단계의 진행을 권장 드립니다.

관리자 계정이 생성되었다면, Docker Container를 중지하고 환경 변수에 아래 두가지 값을 추가 합니다.

도메인주소는 Nginx Proxy Manager에서 등록한 `https://vault.dhcloud.me` 같은 값을 넣어주시면 됩니다.

✓ SIGNUPS\_ALLOWED=false  
DOMAIN=도메인주소

추가로 보안 강화를 위해 Admin 페이지에서 **"2단계 인증"**을 반드시 **활성화** 해줍니다.

ACCOUNT SETTINGS

내 계정

Security

설정

도메인 규칙

긴급 접근

Master password

2단계 인증

Keys

## 2단계 인증






로그인할 때 추가 단계를 요구하여 계정을 보호하십시오.

⚠ 경고

2단계 로그인을 활성화하면 Bitwarden 계정을 영원히 잠글 수 있습니다. 복구 코드를 사용하면 정상적인 2단계 로그인 제공자를 더 이상 사용할 수 없는 경우(예, 장치를 잃어버렸을 때) 계정에 액세스할 수 있습니다. 계정에 접근하지 못한다면 Bitwarden 지원팀은 어떤 도움도 줄 수 없습니다. 복구 코드를 기록하거나 출력하여 안전한 장소에 보관할 것을 권장합니다.

복구 코드

### 공급자

	인증 앱 ✓ 인증 앱(Authy, Google OTP 등)을 통하여 일회용 인증 코드를 생성합니다.	관리
	YubiKey OTP 보안 키 YubiKey를 사용하여 사용자의 계정에 접근합니다. YubiKey 4, 4 Nano, 4C 및 NEO 기기를 사용할 수 있습니다.	관리
	Duo Duo Mobile 앱, SMS, 전화 통화를 사용한 Duo Security 또는 U2F 보안 키를 사용하여 인증하세요.	관리
	FIDO2 WebAuthn WebAuthn이 활성화된 보안 키를 사용하여 계정에 접근하세요.	관리
	이메일 인증 코드가 담긴 이메일을 다시 보냅니다.	관리

## 인증 앱

인증 앱에서 6자리 인증 코드를 입력하세요.

☐ 기억하기

↩ 계속

취소

[다른 2단계 인증 사용](#)

Vaultwarden (unofficial Bitwarden® server)

버전 2023.3.0

🔗 버전 #6

★ 생성 24 6월 2023 03:46:20, DH Choi

✎ 수정 27 6월 2023 08:58:57, DH Choi