

MSP용 Umbrella에 대한 2단계 확인 활성화 및 관리

목차

[소개](#)

[2단계 검증 개요](#)

[2단계 확인 활성화](#)

[활성화 단계](#)

[방법 1: 문자 메시지 사용](#)

[방법 2: 모바일 앱 사용](#)

[2단계 확인으로 로그인](#)

[2단계 확인 사용 안 함](#)

[본실 전화](#)

소개

이 문서에서는 MSP용 Umbrella에 대한 2단계 검증을 활성화, 구성 및 비활성화하는 방법에 대해 설명합니다.

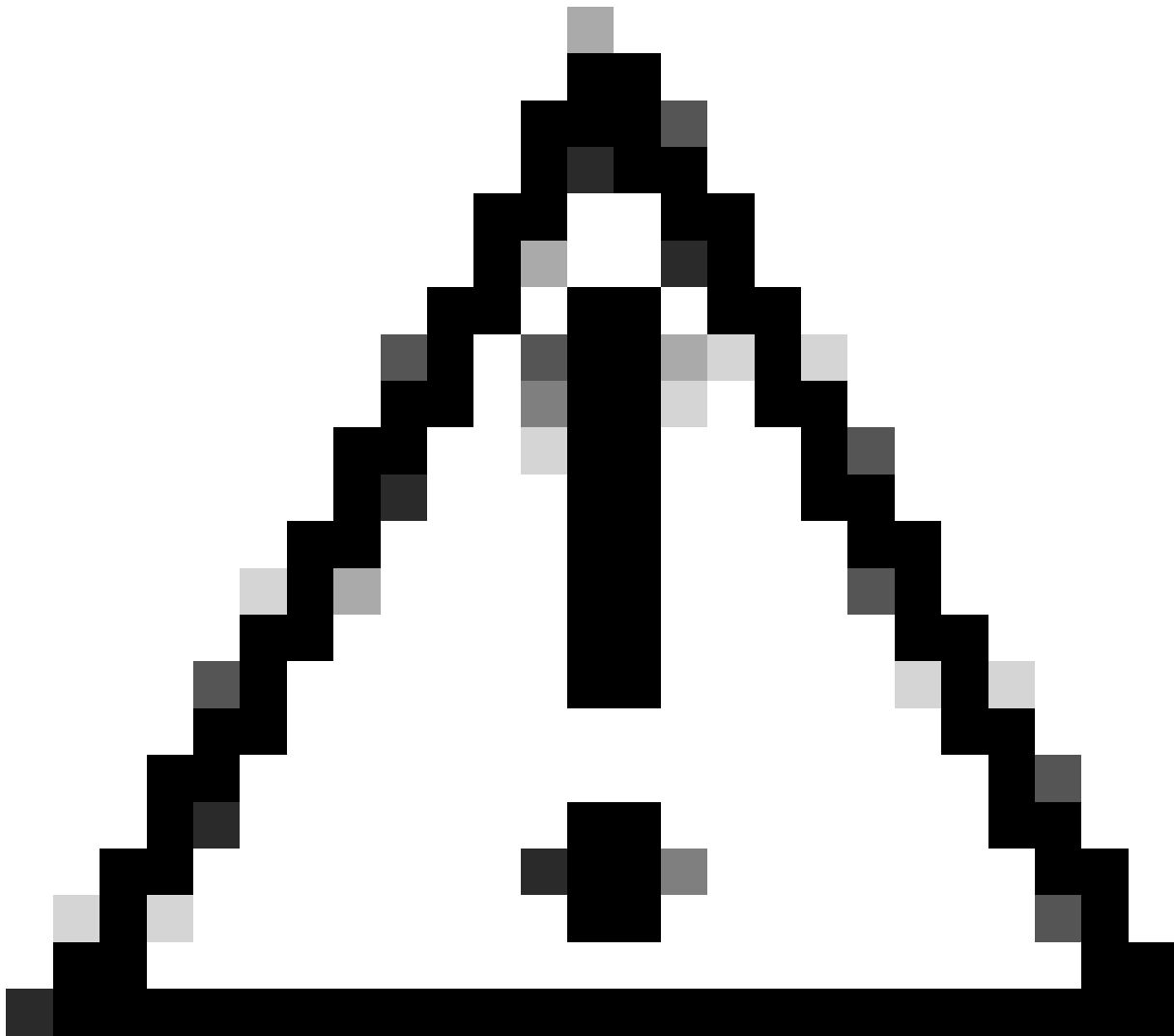
2단계 검증 개요

2단계 인증(2단계 인증이라고도 함)은 두 번째 인증 요소를 요구하여 MSP용 Umbrella 콘솔에 보안을 추가합니다. 사용자는 자신의 암호와 모바일 장치에서 생성된 보안 코드를 모두 입력해야 합니다. 이 프로세스는 무차별 대입 공격을 통해 무단 액세스를 차단하고 권한이 있는 사용자만 로그인할 수 있도록 합니다.

각 클라이언트의 대시보드 내에서 개별 클라이언트 로그인에 대해 2단계 확인도 활성화할 수 있습니다.

2단계 확인 활성화

시작하기 전에 기본적으로 2단계 인증이 비활성화되어 있고 현재 로그인한 계정에 대해 활성화해야 합니다.



주의: 현재 로그인한 어카운트에 대해서만 2단계 인증을 활성화할 수 있습니다. 다른 관리자의 계정에 대한 설정은 변경할 수 없지만 그 상태는 볼 수 있습니다.

활성화 단계

1. MSP Settings(MSP 설정) > Admins(관리자)로 이동합니다.
2. 계정 이름을 클릭하여 계정 항목을 확장합니다.
3. Enable(활성화)을 클릭합니다.

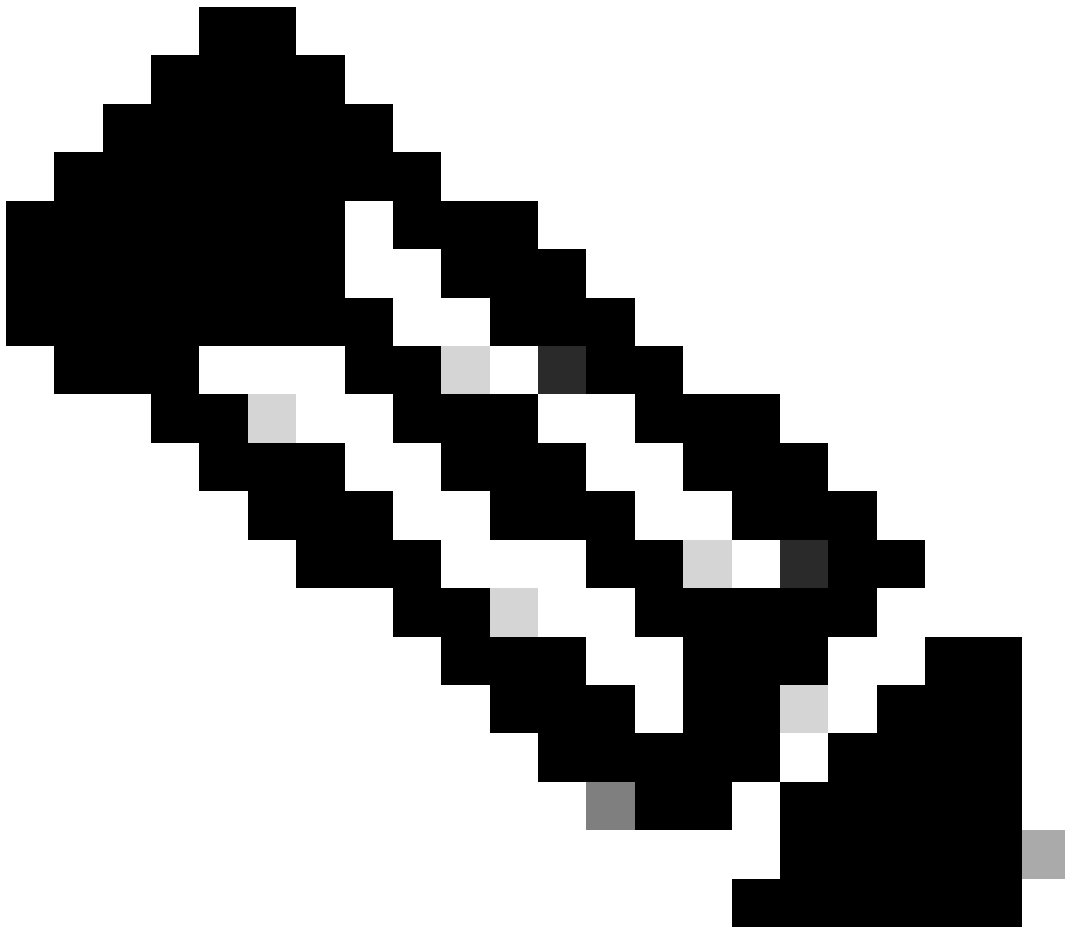
보안 코드를 받으려면 원하는 방법을 선택하고 확인해야 합니다.

- 문자 메시지(SMS)
- 모바일 앱([Google Authenticator](#)와 같은 [Authenticator 앱](#))

선택한 방법에 따라 단계를 진행합니다.

방법 1: 문자 메시지 사용

1. 텍스트 메시지 사용을 선택하고 계속을 누릅니다.
 2. 국가 및 지역 번호를 포함하여 전화 번호를 입력한 다음 계속을 클릭합니다.
 3. SMS를 통해 6자리 코드를 수신합니다.
 4. Umbrella for MSPs 비밀번호와 6자리 코드를 입력한 다음 Enable 2-step verification(2단계 검증 활성화)을 클릭합니다.
 5. 제공된 응급 복구 코드를 저장합니다. 모바일 디바이스 및 비밀번호와 별도로 안전하게 저장하십시오.
 6. 완료를 클릭합니다.
-



참고: 로그인할 때마다 문자 메시지 보안 코드가 수신됩니다. 보안 코드는 30초 후에 만료됩니다. 필요한 경우 로그인 화면에서 Resend Code(코드 재전송)를 사용합니다.

또한 누군가가 귀하의 Gmail 계정에 액세스 할 수 있는 경우, 공격자는 암호 재설정 기능을 사용하고 또한 1 회 암호를 수신 할 수 있기 때문에, 우리는 SMS를 위해 Google Voice를 사용하는 것을 제안 합니다.

방법 2: 모바일 앱 사용

1. 모바일 장치에 인증 앱(예: [Google Authenticator](#))을 다운로드하고 설치합니다.
2. 모바일 앱 사용을 선택하고 계속을 클릭합니다.
3. 인증 앱을 사용하여 QR 코드를 스캔합니다. 새 토큰을 추가하고 바코드를 스캔합니다. 그런 다음 QR 코드를 스캔하라는 메시지가 나타납니다.
4. 오른쪽 하단의 +를 클릭한 다음 Scan Barcode(바코드 스캔)를 클릭하여 새 토큰을 추가합니다.
5. 생성된 6자리 코드와 MSP용 Umbrella 비밀번호를 입력한 다음 Enable Two-Step Verification을 클릭합니다.
6. 제공된 응급 복구 코드를 저장합니다. 모바일 디바이스 및 비밀번호와 별도로 안전하게 저장하십시오. 보안은 비밀번호와 보안 코드가 별개인 경우에만 유효합니다.
7. 완료를 클릭합니다.

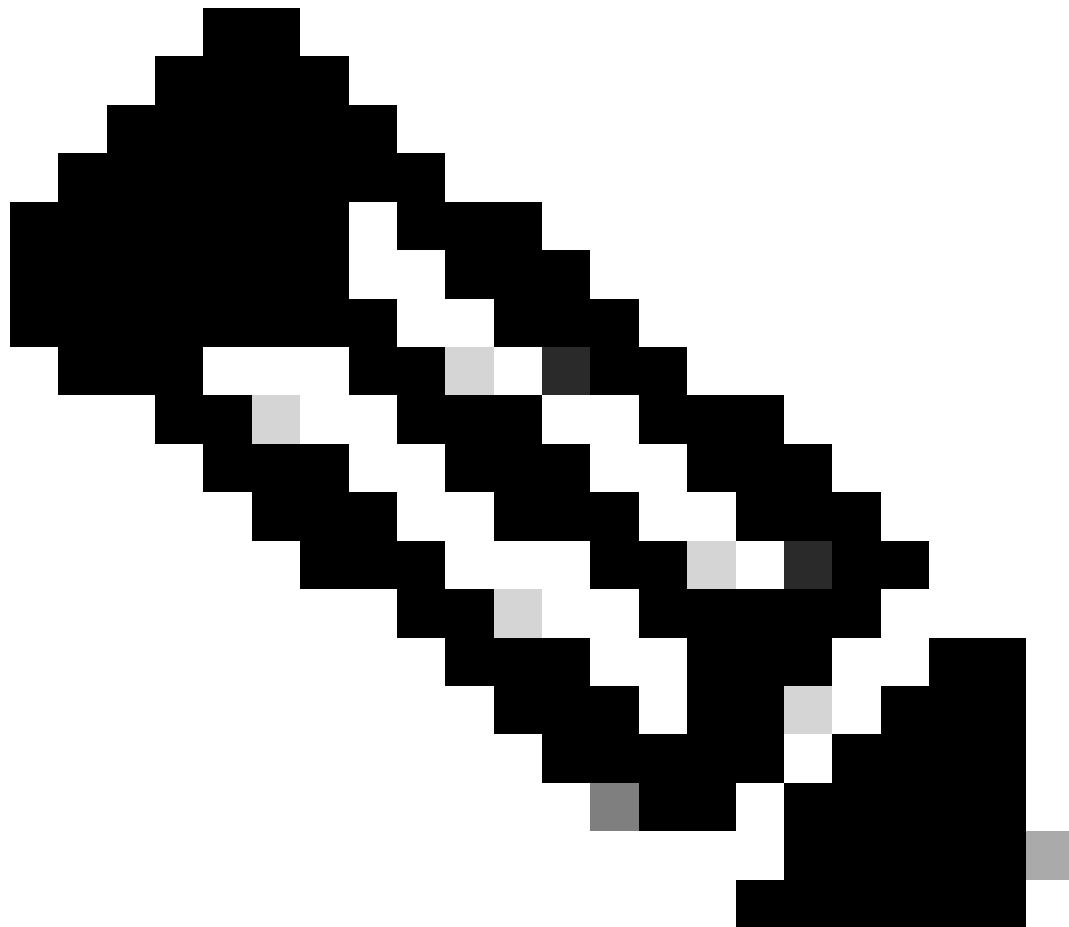
활성화되면 인증 앱은 30초마다 새 코드를 생성하여 로그인합니다.



경고: 모바일 장치가 시간 동기화되었는지 확인합니다. 잘못된 장치 시간으로 인해 코드 확인이 실패할 수 있습니다.

2단계 확인으로 로그인

비밀번호를 입력한 후 모바일 앱 또는 SMS를 통해 수신한 보안 코드를 입력합니다. 초기 로그인 후 확인 화면이 표시됩니다.



참고: SMS 코드를 받지 못한 경우 SMS 제공자(Twilio)에 문제가 발생할 수 있습니다. 업데이트에 대한 [Twilio](#) 상태를 확인합니다.

2단계 확인 사용 안 함

2단계 검증을 더 이상 사용하지 않으려면

1. Configuration(컨피그레이션) > System Settings(시스템 설정) > Accounts(계정)로 이동합니다.
2. 계정을 선택한 다음 2단계 인증에 대해 Disable(비활성화)을 클릭합니다.
3. 그런 다음 새 일회용 보안 코드를 보낸 다음 요청을 확인하기 위해 마지막으로 한 번 입력하라는 메시지가 표시됩니다.

분실 전화

휴대폰(또는 태블릿)을 분실했으며 더 이상 2단계 인증을 사용하지 않으려는 경우 Lost your phone?(휴대폰 분실)을 클릭합니다. 로그인합니다. 이렇게 하면 긴급 복구 코드를 입력하고 소프트웨어를 비활성화할 수 있는 영역으로 이동합니다. 다시 한 번 말씀드리지만, 응급 복구 코드는 SMS와 모바일 앱 모두에 대한 초기 설정 이후에 제공된 코드였습니다.

장치와 응급 복구 코드 모두를 분실한 경우 지원을 받으려면 계정 재설정에 도움이 되는 추가 정보가 필요합니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.