

# 보안 엔드포인트 콘솔에서 2단계 인증 구성

## 목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[액세스 제어](#)

[2단계 인증](#)

[구성](#)

[권한](#)

[2단계 인증](#)

## 소개

이 문서에서는 어카운트 유형 및 Cisco Secure Endpoint Console에서 2단계 인증을 구성하는 단계에 대해 설명합니다.

## 사전 요구 사항

### 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 보안 엔드포인트
- 보안 엔드포인트 콘솔 액세스

### 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Secure Endpoint Console v5.4.20211013

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

## 배경 정보

### 액세스 제어

Secure Endpoint Console에는 두 가지 유형의 어카운트가 있습니다. 관리자 및 권한이 없는 계정 또는 일반 계정입니다. 새 사용자 이름을 생성할 때 권한 레벨을 선택해야 하지만 언제든지 액세스 레벨을 변경할 수 있습니다.

관리자는 모든 권한을 가지며 조직의 모든 그룹 또는 컴퓨터에서 데이터를 보고 그룹, 정책, 목록 및 사용자 이름을 변경할 수 있습니다.

**참고:** 관리자는 다른 관리자를 일반 계정으로 강등시킬 수 있지만 자신의 상태를 내릴 수는 없습니다.

권한이 없거나 일반 사용자 계정은 액세스 권한이 부여된 그룹에 대한 정보만 볼 수 있습니다. 새 사용자 계정을 생성할 때 관리자 권한을 부여할지 여부를 선택할 수 있습니다. 이러한 권한을 부여하지 않으면 액세스할 수 있는 그룹, 정책 및 목록을 선택할 수 있습니다.

## 2단계 인증

Two-Factor Authentication은 Secure Endpoint Console 계정에 대한 무단 액세스 시도에 대한 추가 보안 레이어를 제공합니다.

## 구성

### 권한

관리자인 경우 권한을 변경하거나 관리자 권한을 부여하려면 Accounts > Users로 이동하여 사용자 계정을 선택하고 권한을 선택할 수 있습니다. 이 이미지를 참조하십시오.

**Privileges**

Grant Administrator Privileges Remove All Privileges Revert Changes Save Changes

Allow this user to fetch files (including Connector diagnostics) from the selected groups.

Allow this user to see command line data from the selected groups.

Allow this user to set Endpoint Isolation status for the selected groups.

Groups Clear Select Groups

None

For the selected groups: Auto-Select Policies Auto-Select Policies and Lists

Policies Clear Select Policies

None

관리자는 다른 관리자에게 관리자 권한을 취소할 수도 있습니다. 이렇게 하려면 관리자 계정으로 이동하여 이미지에 표시된 대로 옵션을 볼 수 있습니다.

## Privileges

Revoke Administrator Privileges

🔍 Administrator

👤 All Groups

⚙️ All Policies

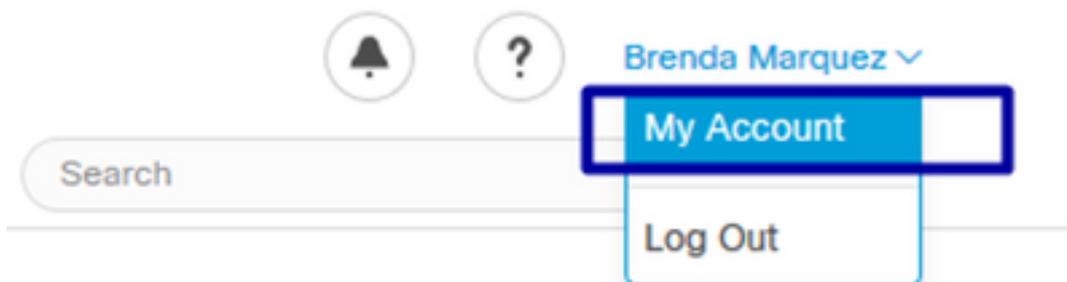
📄 All Outbreak Control Lists

**참고:** 사용자 권한이 변경되면 일부 데이터가 검색 결과에 캐시되므로 사용자가 그룹에 더 이상 액세스할 수 없더라도 일정 기간 동안 데이터를 볼 수 있습니다. 대부분의 경우 5분 후에 캐시가 새로 고쳐집니다.

## 2단계 인증

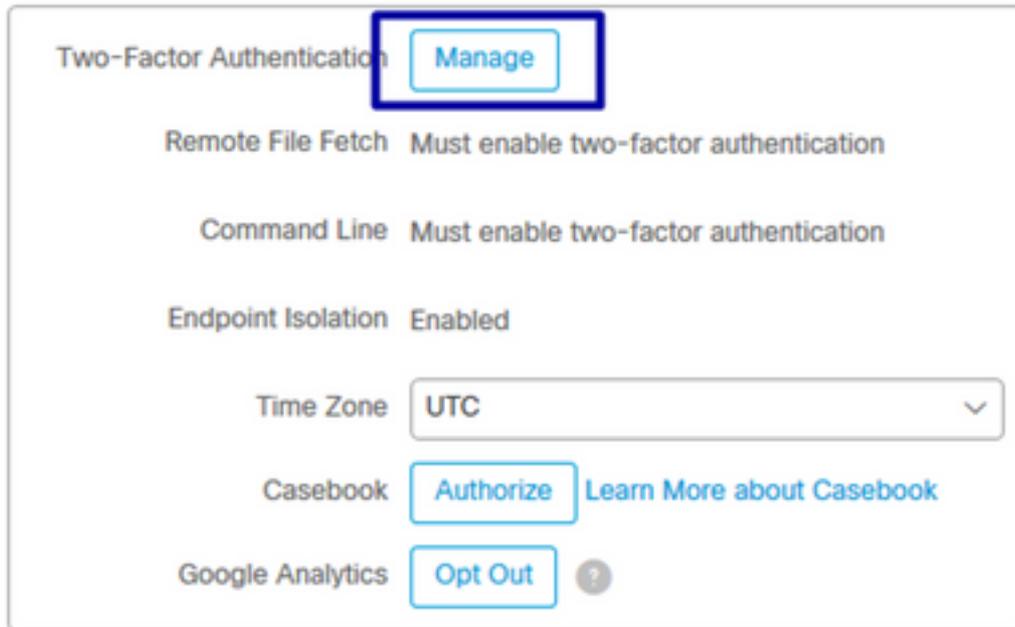
이 기능을 사용하면 외부 액세스 요청으로 인증을 적용할 수 있습니다. 이를 구성하려면 다음 절차를 수행합니다.

**1단계.** 이 이미지와 같이 보안 엔드포인트 콘솔 오른쪽 상단의 내 계정으로 이동합니다.



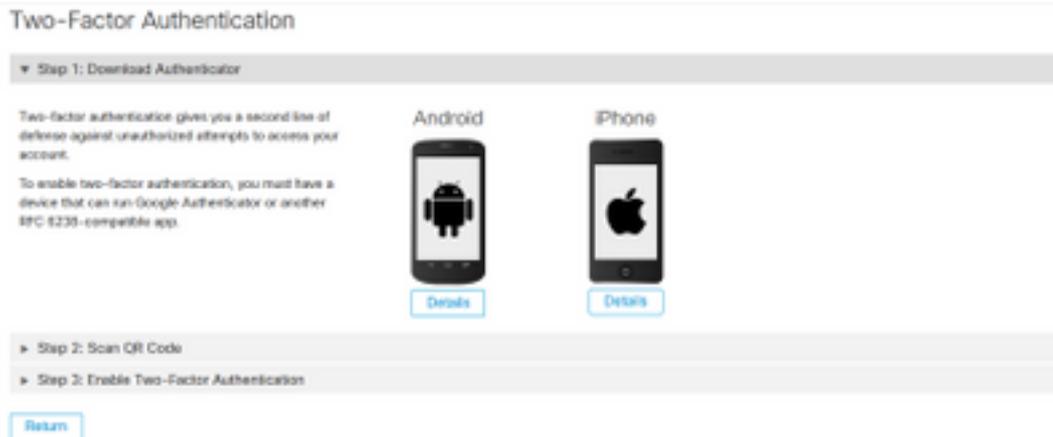
**2단계.** [설정] 섹션에서 [관리]를 선택하여 이미지에 표시된 대로 이 기능을 활성화하는 데 필요한 3단계 단계가 포함된 간단한 가이드를 확인합니다.

## Settings



3단계. 세 가지 빠른 단계가 있습니다.

a) Google Authenticator를 실행할 수 있는 Android 또는 iPhone용 인증자를 다운로드할 수 있습니다. 다운로드 페이지로 리디렉션하는 QR 코드를 생성하려면 모든 휴대폰에서 세부 정보를 선택합니다. 이 이미지를 참조하십시오.



b) QR 코드를 스캔하고 Generate QR code(QR 코드 생성)에서 이 이미지에 표시된 대로 Google Authenticator에서 스캔해야 하는 코드를 선택합니다.

## Two-Factor Authentication

▶ Step 1: Download Authenticator

▼ Step 2: Scan QR Code



Sample

Generate QR Code

**Warning:** This QR code is your **personal one-time code**. This should be kept secure. Generate the QR code only when you have some privacy and are ready.

Add this two-factor authentication account to your device

Click "Generate QR Code" and scan the generated QR code into Google Authenticator or another RFC 6238-compatible app.

If you cannot access your device

After completing Step 2, you will be given a set of backup codes. You can use a backup code to access your account and disable two-factor authentication until you can re-enable it with a new device. If you do not have access to any backup codes, contact Support.

**Note:** We do not recommend storing your Cisco Security password on the same device as your authenticator application. If your Cisco Security password is on the same device as your authenticator app and you lose your device, you should contact Support **immediately** to have your account password reset.

▶ Step 3: Enable Two-Factor Authentication

Return

c) Two-Factor Authenticator를 활성화하고, 휴대폰에서 인증자 애플리케이션을 열고 확인 코드를 입력합니다. 이미지에 표시된 대로 이 프로세스를 완료하려면 [사용]을 선택합니다.

## Two-Factor Authentication

▶ Step 1: Download Authenticator

▶ Step 2: Scan QR Code

▼ Step 3: Enable Two-Factor Authentication

1. Open your Authenticator app.
2. Enter the verification code from Authenticator.

Enter the verification code from Authenticator.

Please enter verification code

Enable

Return

4단계. 완료되면 일부 백업 코드가 제공됩니다. 저장하려면 클립보드에 복사를 선택하고 이미지를 예로 봅니다.

## Two-Factor Authentication

▶ Step 1: Download Authenticator

▶ Step 2: Scan QR Code

▼ Step 3: Enable Two-Factor Authentication

Two-Factor Authentication has been enabled. Here are your backup codes.

**Warning:** This is the only time that the backup codes are shown. If you do not make a note of them, you will need to generate a new set. Your backup codes need to be kept safe, as this will be the only way that you will be able to get into your account if you lose access to your device.

In case you cannot access your device we have generated a set of backup codes that you can use. Each backup code on the list can only be used once. You can regenerate a new list of backup codes from Two-Factor Authentication Details on the Users page. Once a new set has been generated, any backup code in the old set is no longer valid. We suggest printing this list out and keeping it somewhere safe.

### Backup Codes

- 5c9a4c84
- f20ea786
- 7f1aeb53
- a4f59f0c
- 21a32ced
- 1e3073b1
- 42e2e189
- f54f3fde
- 7424df5f
- 3dafab11

Copy to clipboard

**참고:** 각 백업 코드는 한 번만 사용할 수 있습니다. 모든 백업 코드를 사용한 후 새 코드를 생성하려면 이 페이지로 돌아가야 합니다.

자세한 내용은 Secure Endpoint [User Guide\(보안 엔드포인트 사용 설명서\)](#)를 참조하십시오.

또한 Accounts(어카운트)와 [Enable Two-Factor Authentication](#) 비디오를 볼 수 있습니다.