# Configuratie van twee factoren in de Secure Endpoint Console

## Inhoud

[Inleiding](#)
[Voorwaarden](#)
[Vereisten](#)
[Gebruikte componenten](#)
[Achtergrondinformatie](#)
[Toegangsbeheer](#)
[Twee-factoren verificatie](#)
[Configureren](#)
[Privileges](#)
[Twee-factoren verificatie](#)

## Inleiding

Dit document beschrijft het type rekeningen en de stappen om twee-factoren verificatie in de Cisco Secure Endpoint Console te configureren.

## Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Secure-endpoint
- Toegang tot de Secure Endpoint Console

### Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Secure-endpointconsole v5.4.2013

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

## Achtergrondinformatie

### Toegangsbeheer

Er zijn twee soorten rekeningen in de Secure Endpoint Console: administrateurs en niet-bevoorrechte of regelmatige rekeningen. Wanneer u een nieuwe gebruikersnaam maakt moet u hun voorkeursniveau selecteren, maar u kunt hun toegangsniveau op elk moment wijzigen.

De beheerders hebben volledige controle, kunnen gegevens van om het even welke groep of computer in de organisatie bekijken en veranderingen aanbrengen in groepen, beleid, lijsten en gebruikersnamen.

> **Opmerking:** Een beheerder kan een andere beheerder aan een regelmatige rekening aanwijzen maar kan zichzelf niet demonstreren.

Een bevoorrechte of regelmatige gebruikersaccount kan alleen informatie bekijken voor groepen tot wie ze toegang hebben gekregen. Wanneer u een nieuwe gebruikersaccount maakt, hebt u de keuze of u deze Administrator-rechten wilt geven. Als u hen niet deze privileges toekent, kunt u selecteren welke groepen, beleid en lijsten zij hebben.

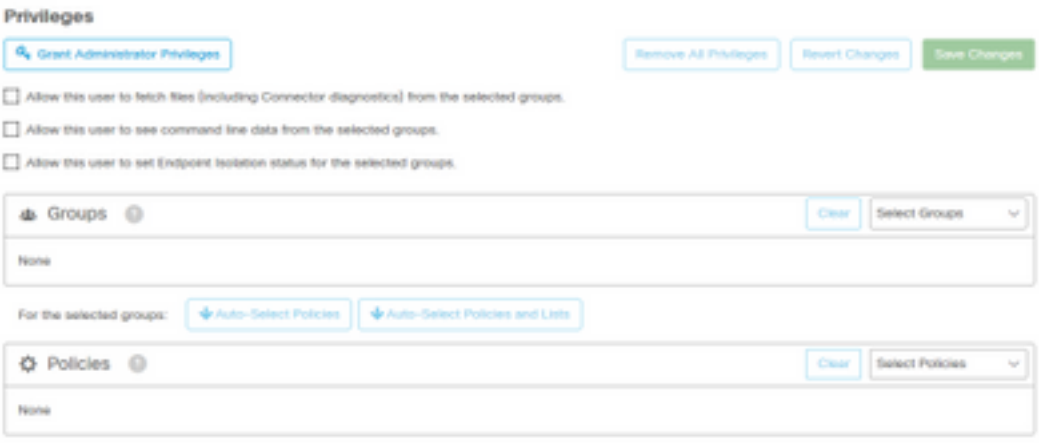
### Twee-factoren verificatie

Two-Factor Verificatie verstrekt een extra laag van veiligheid tegen onbevoegde pogingen om uw Secure Endpoint Console-account te benaderen.

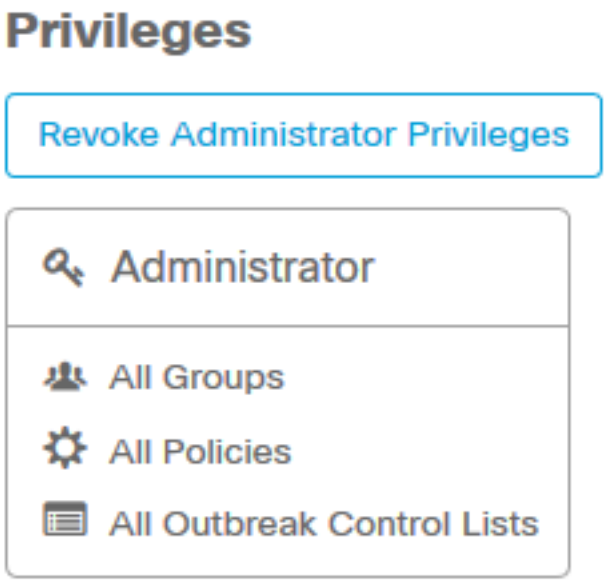
## Configureren

### Privileges

Als u een beheerder bent, kunt u om rechten te veranderen of beheerder rechten te verlenen door naar accounts > Gebruikers te navigeren om de gebruikersaccount te selecteren en de rechten te kiezen, zie deze afbeelding.




Een beheerder kan ook de administratorrechten aan een andere beheerder intrekken. U kunt dit doen door naar de Administrator-account te navigeren om de optie te zien, zoals in de afbeelding.

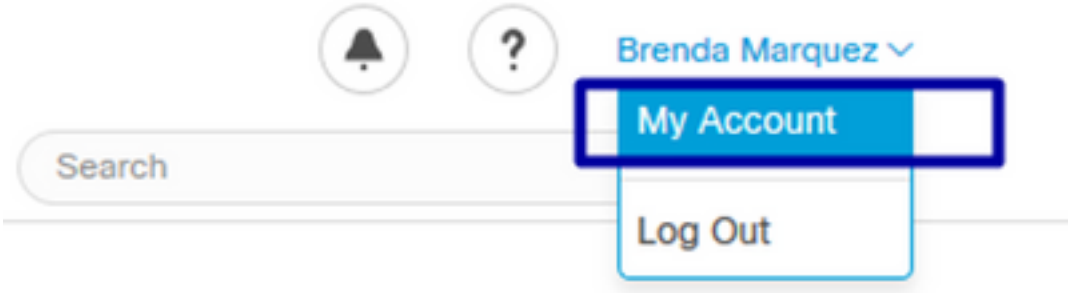



**Opmerking:** Wanneer gebruikersrechten veranderen worden sommige gegevens in de resultaten van het Zoeken gecached zodat een gebruiker het nog een periode kan zien zelfs alhoewel zij geen toegang meer tot een groep hebben. In de meeste gevallen wordt de cache na 5 minuten verfrist.

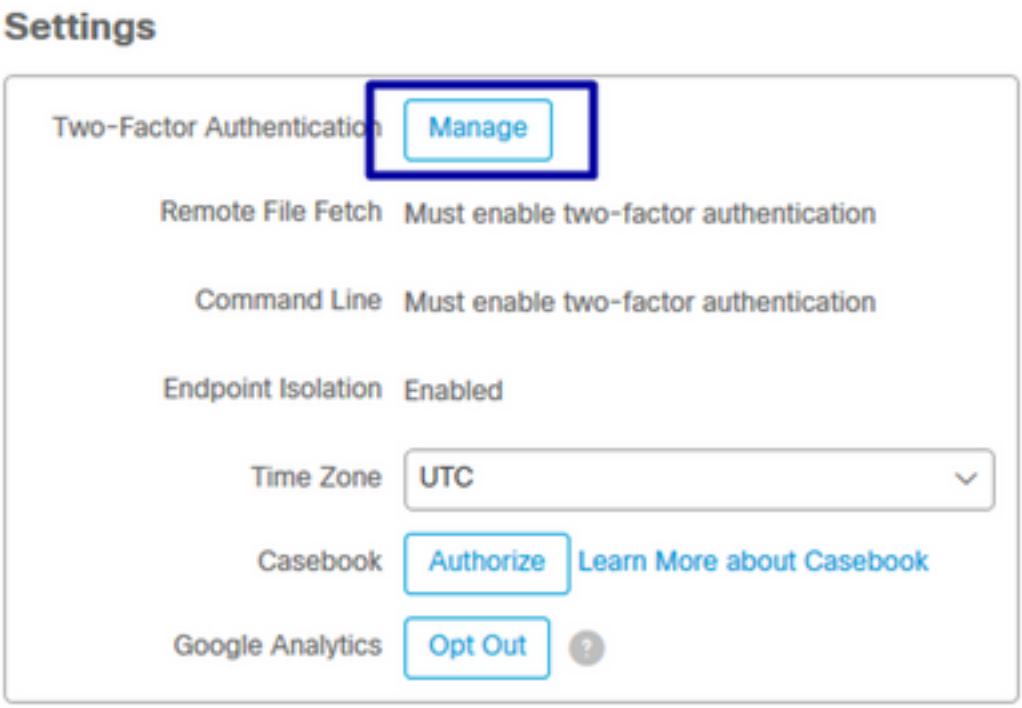
## Twee-factoren verificatie

Deze optie stelt u in staat de verificatie af te dwingen met een extern toegangsverzoek. Om dit te configureren volgt u deze procedure:

**Stap 1** . Navigeer naar Mijn account rechts boven in de Secure Endpoint Console zoals in deze afbeelding.

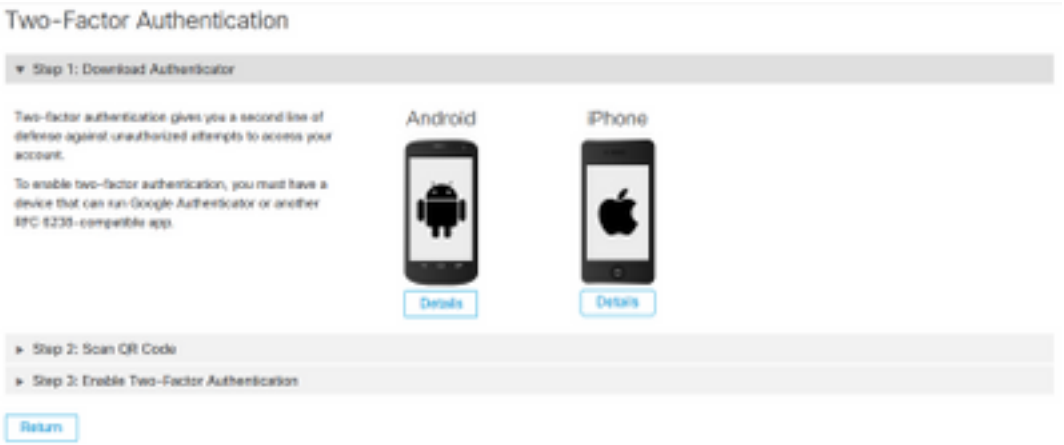



**Stap 2** . Selecteer in het gedeelte Instellingen de optie Bewerken, om een eenvoudige handleiding te kunnen zien met drie stappen die nodig zijn om deze functie in te schakelen, zoals in de afbeelding.

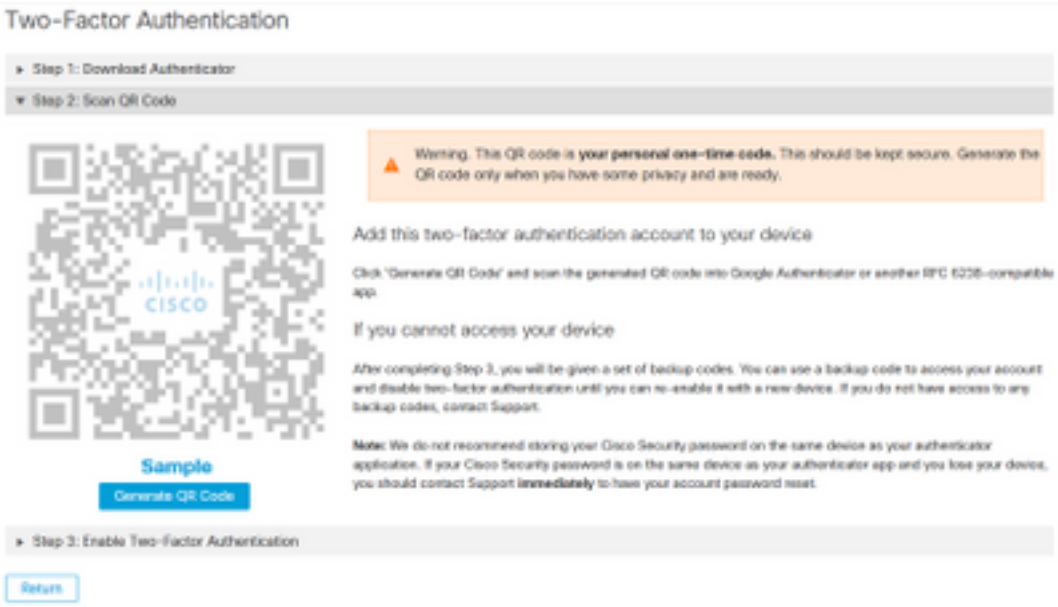



**Stap 3**. Er zijn drie snelle stappen:

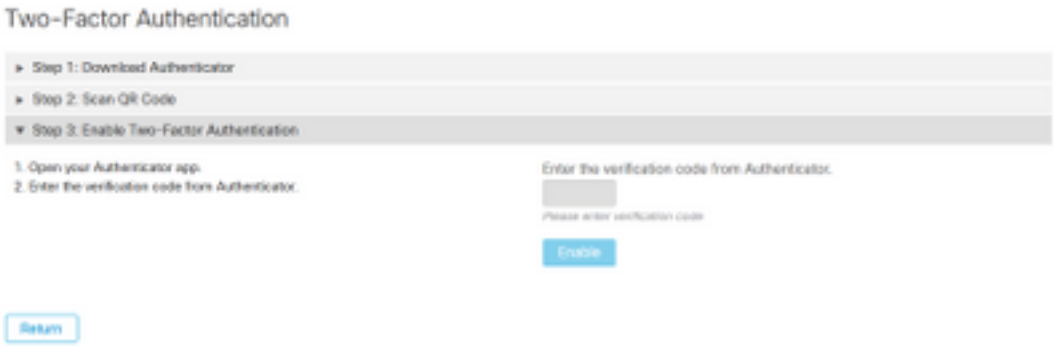
a) Download authenticator, wat u kunt verkrijgen voor Android of iPhone die Google Authenticator kan gebruiken. Selecteer Details in een van de mobiele telefoons om een QR-code te genereren die u omwijst naar de downloadpagina. Zie deze afbeelding.



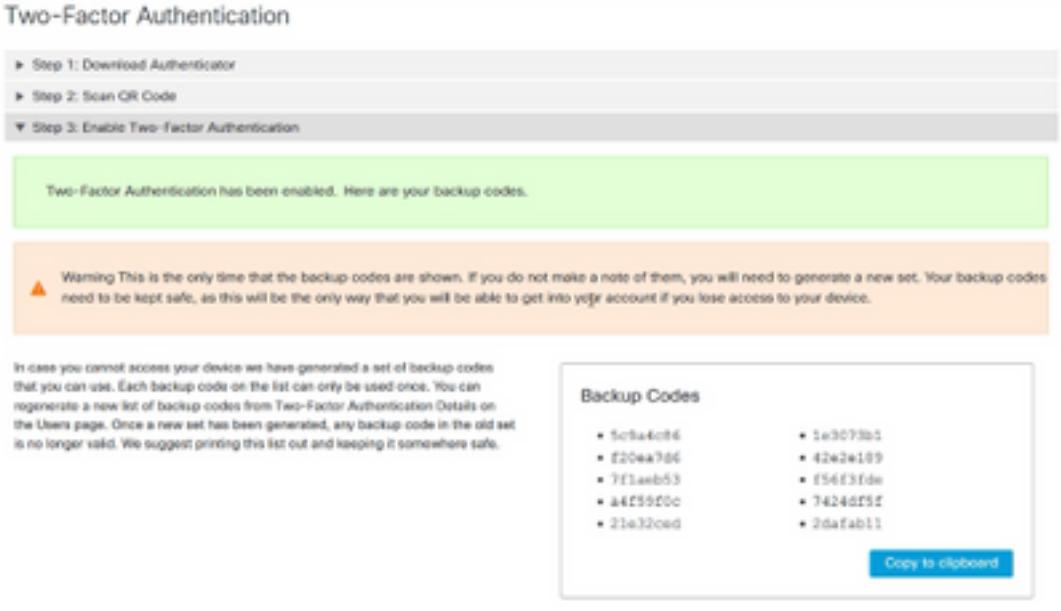

b) Scan QR-code, selecteer de Generate QR-code, die moet worden gescand door Google Authenticator zoals in deze afbeelding wordt getoond.




c) Schakel twee-factoren authenticator in, open uw authenticator-toepassing in uw mobiele telefoon en voer de verificatiecode in. Selecteer Inschakelen om dit proces te voltooien, zoals in de afbeelding.




**Stap 4** Zodra deze klaar is, geeft het een aantal reservecodes. Selecteer **Kopie** naar klembord om ze op te slaan, zie de afbeelding als voorbeeld.




**Opmerking:** Elke reservecode kan slechts één keer worden gebruikt. Nadat u al uw back-upcodes hebt gebruikt, moet u naar deze pagina terugkeren om nieuwe codes te genereren.

Raadpleeg de Secure Endpoint User Guide voor meer informatie.

Daarnaast kunt u de Account bekijken en de video Twee-factor Verificatie inschakelen.