

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.

The screenshot shows the 'Privileges' configuration page. At the top, there is a search bar with 'Grant Administrator Privileges' and three buttons: 'Remove All Privileges', 'Revert Changes', and 'Save Changes'. Below this are three checkboxes for permissions: '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.', and 'Allow this user to set Endpoint Isolation status for the selected groups.' There are two main sections for selecting groups and policies. The first section is labeled 'Groups' and has a 'Clear' button and a 'Select Groups' dropdown menu. The second section is labeled 'Policies' and has a 'Clear' button and a 'Select Policies' dropdown menu. Both sections currently show 'None' as the selected option.

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.

Privileges

Revoke Administrator Privileges

🔍 Administrator

👤 All Groups

⚙️ All Policies

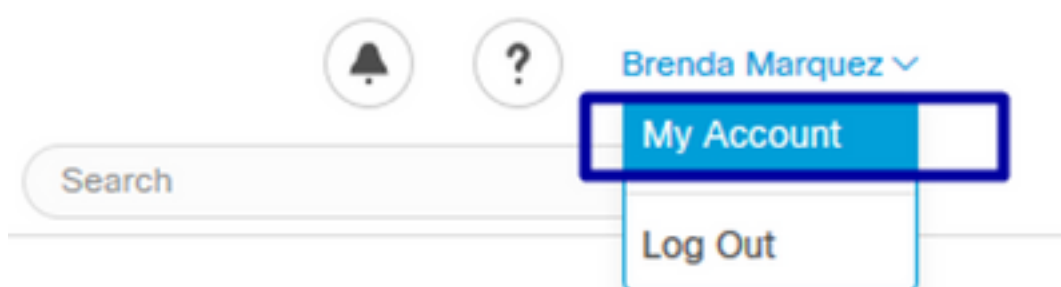
📄 All Outbreak Control Lists

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.

Settings

Two-Factor Authentication [Manage](#)

Remote File Fetch Must enable two-factor authentication

Command Line Must enable two-factor authentication

Endpoint Isolation Enabled

Time Zone

Casebook [Authorize](#) [Learn More about Casebook](#)

Google Analytics [Opt Out](#) [?](#)

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.

Two-Factor Authentication

▼ Step 1: Download Authenticator

Two-factor authentication gives you a second line of defense against unauthorized attempts to access your account.

To enable two-factor authentication, you must have a device that can run Google Authenticator or another RFC 6238-compatible app.

Android [Details](#)

iPhone [Details](#)

► Step 2: Scan QR Code

► Step 3: Enable Two-Factor Authentication


[Return](#)

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

Two-Factor Authentication

► Step 1: Download Authenticator

▼ Step 2: Scan 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.

Sample
Generate QR Code

► Step 3: Enable Two-Factor Authentication

Return

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.

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

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

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

- 5c9a4c086
- f20ea706
- 7f1aeb53
- a4f50f0c
- 21e32ced
- 1e307301
- 42e2e109
- f56f3fde
- 7424df5f
- 2dafab11

Copy to clipboard

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](#).