

# Poortbeveiliging op Cisco Business 220 Switches

## Doel

Dit artikel legt uw opties voor poortbeveiliging uit op uw Cisco Business 220 Series switch.

## Toepasselijke apparaten | Versie firmware

- CBS220-reeks ([Gegevensblad](#)) | 2.0.0.17

## Inleiding

De netwerkbeveiliging kan worden verhoogd door de toegang op een poort te beperken tot gebruikers met specifieke MAC-adressen. De MAC-adressen kunnen dynamisch of statisch worden geconfigureerd. Poortbeveiligingsmonitoren worden ontvangen en geleerd. Toegang tot afgesloten poorten is beperkt tot gebruikers met specifieke MAC-adressen.

Poortbeveiliging kan niet worden ingeschakeld voor poorten waarvoor 802.1X is ingeschakeld of voor poorten die worden gedefinieerd als SPAN-bestemming.

Poortbeveiliging heeft twee modi:

- **Classic Lock**-Alle geleerde adressen van MAC op de poort zijn vergrendeld en de poort leert geen nieuwe adressen van MAC. De aangeleerde adressen zijn niet onderworpen aan veroudering of publicatie.
- **Beperkt Dynamisch slot** - het apparaat leert MAC-adressen tot de geconfigureerde limiet van toegestane adressen. Nadat de grenswaarde wordt bereikt, leert het apparaat geen extra adressen. In deze modus zijn de adressen onderworpen aan veroudering en publicatie.

Wanneer een kader van een nieuw MAC-adres wordt gedetecteerd op een haven waar het niet is toegestaan (de haven is klassiek vergrendeld en er is een nieuw MAC-adres, of de haven is dynamisch vergrendeld en het maximum aantal toegestane adressen is overschreden), wordt het beschermingsmechanisme ingeroepen, en kan een van de volgende acties plaatsvinden:

- Frame wordt weggegooid.
- Het frame wordt doorgestuurd.
- Frame wordt verwijderd en er wordt een SYSLOG-bericht gegenereerd.
- De poort is gesloten.

Wanneer het beveiligde MAC-adres op een andere poort is gezien, wordt het frame doorgestuurd, maar het MAC-adres wordt niet geleerd op die poort.


Naast één van deze acties kunt u ook vallen genereren en hun frequentie en aantal beperken om overbelasting van de apparaten te voorkomen.

## Poortbeveiliging instellen

### Stap 1

Log in op de webgebruikersinterface (UI).

English ▾



### Cisco Business Dashboard

User Name\*

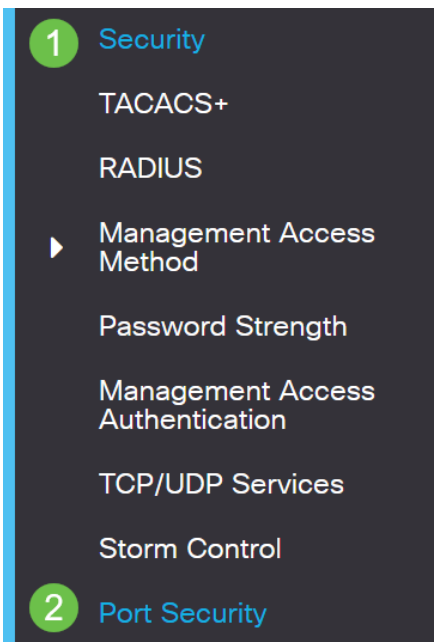
This field is required

Password\*

Login

### Stap 2

Selecteer in het menu links de optie **Beveiliging > Port Security**.



### Stap 3

Selecteer een aan te passen interface en klik vervolgens op het pictogram **Bewerken**.

#### Port Security Table

The screenshot shows a table with the following columns: Entry No., Port, Interface Status, Learning Mode, and Max No. of Address. The first row is highlighted in light blue and contains the values: 1, GE1, Disabled, Classic Lock, and 1. A green circle with the number '2' is positioned above a pencil icon in the top left corner of the table area, indicating the edit function.

Entry No.	Port	Interface Status	Learning Mode	Max No. of Address
1	GE1	Disabled	Classic Lock	1

### Stap 4

Voer de parameters in.

- **Interface** - Selecteer de interfacenaam.
- **Administratieve status**: selecteer deze optie om de poort te sluiten.
- **Leermodus**: selecteer het type poortvergrendeling. Om dit veld te configureren moet de interfacestatus worden ontgrendeld. Het veld Leermodus is alleen ingeschakeld als het veld Interfacestatus is vergrendeld. Om de leermodus te wijzigen, moet de interface voor vergrendelen worden gewist. Nadat de modus is gewijzigd, kan de interface voor vergrendeling worden hersteld. De opties zijn:
  - **Classic Lock** - hiermee wordt de poort onmiddellijk vergrendeld, ongeacht het aantal adressen dat al is geleerd.
  - **Beperkt Dynamisch Lock** - hiermee wordt de poort vergrendeld door de huidige dynamische MAC-adressen te verwijderen die aan de poort zijn gekoppeld. De haven leert tot de maximum adressen toegestaan op de haven. Zowel het loslaten als het verouderen van de MAC-adressen zijn ingeschakeld.
- **Max. aantal toegestane adressen**—Voer het maximale aantal MAC-adressen in dat op de poort kan worden geleerd als de beperkte Dynamic Lock learning-modus is

geselecteerd. Het getal 0 geeft aan dat alleen statische adressen op de interface worden ondersteund.

- **Handeling op schending** - Selecteer een actie die moet worden toegepast op pakketten die aankomen op een afgesloten haven. De opties zijn:
  - **VerWERP** - VerWERK pakketten van om het even welke onaangeleerd bron .
  - **voorwaarts**-door:sturen pakketten van een onbekende bron zonder het adres van MAC te leren
  - **Gooi de pakketten weg en loggen** - vernietigt de pakketten van een niet-aangeleerde bron, sluit de interface af, logt de gebeurtenissen af en stuurt vallen naar de gespecificeerde ontvangen van de val Shutdown - Hiermee worden de pakketten van een niet-aangeleerde bron verwijderd en wordt de poort afgesloten. De poort blijft gesloten totdat deze opnieuw wordt geactiveerd, of totdat het apparaat opnieuw wordt opgestart.
  - **Vangfrequentie**—Voer een minimale tijd in (in seconden) die tussen de vallen verstrijkt

Klik op **Apply** (Toepassen).

## Edit Port Settings



Interface: **1**  Port GE1 ▾

Administrative Status: **2**  Enable

Learning Mode: **3**  Classic Lock  
 Limited Dynamic Lock

✦ Max No. of Address Allowed: **4**  (Range: 1 - 256, Default: 1)

Action on Violation: **5**  Discard  
 Forward  
 Discard and Log  
 Shutdown

✦ Trap Frequency (sec): **6**  (Range: 1 - 1000000, Default: 1)

---

**7**

Als u een voorbeeld van het standaardgedrag voor poortbeveiliging op uw CBS220 wilt zien, controleer dan [poortsecurity gedrag](#).

Conclusie

Zo simpel is dat. Geniet van je veilige netwerk!

Raadpleeg voor meer configuraties de [Cisco Business 220 Series beheergids voor](#)

## Switches.

Als u andere artikelen wilt bekijken, raadpleegt u de [Cisco Business 220 Series ondersteuningspagina voor Switches.](#)