

# Configuratie 802.1x Verificatie op Cisco Business 220 Series Switches

## Doel

Het doel van dit artikel is om u te tonen hoe u 802.1x Verificatie op de Cisco Business 220 serie slimme switches kunt configureren.

## Toepasselijke apparaten | Versie firmware

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

## Inleiding

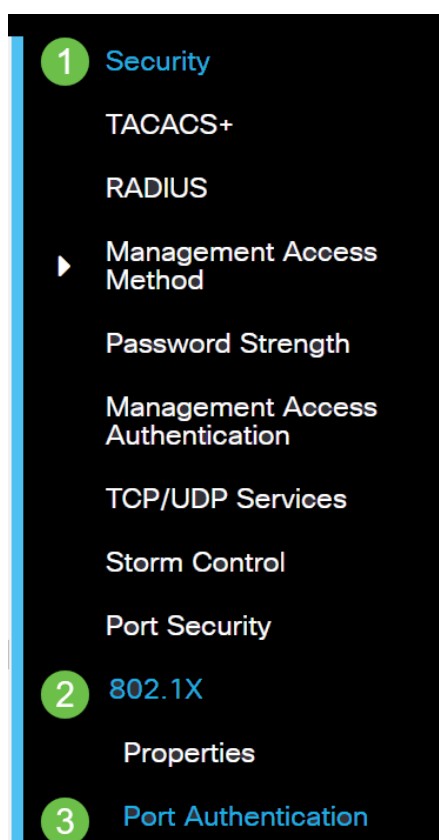
Poortverificatie maakt het mogelijk de parameters voor elke poort te configureren. Aangezien sommige van de configuratieveranderingen slechts mogelijk zijn terwijl de haven in een geautoriseerde staat van de Macht is, zoals de authenticatie van de gastheer, is het aanbevolen om de havencontrole te veranderen in Force Authorized alvorens veranderingen uit te voeren. Wanneer de configuratie is voltooid, moet u de poortcontrole terugbrengen naar de vorige status.

Een haven met 802.1x die op het kan geen lid van een LAG worden. 802.1x en Port Security kunnen niet tegelijkertijd op dezelfde poort worden ingeschakeld. Als u poortbeveiliging op een interface activeert, kan de Administratieve poortcontrole niet worden gewijzigd in Auto-modus.

## Poortverificatie configureren

### Stap 1

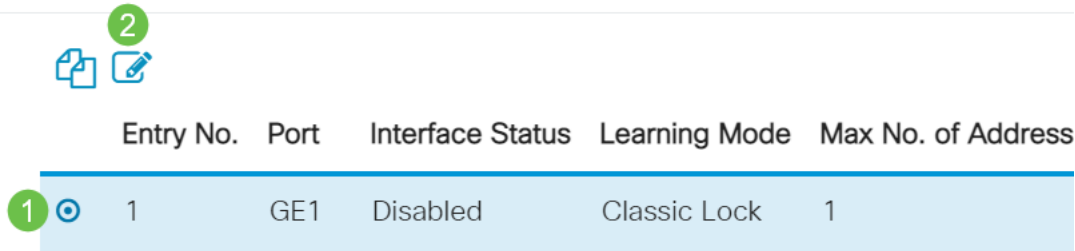
Meld u aan bij de switch Web User Interface (UI) en kiest u **Security > 802.1x > Port Authentication**.



## Stap 2

Klik op het radioknop voor de poort die u wilt configureren en klik vervolgens op het pictogram **Bewerken**.

### Port Security Table



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

## Stap 3

Het venster *Port-verificatie bewerken* verschijnt dan. Zorg ervoor dat de gespecificeerde poort in Stap 2 in de vervolgkeuzelijst Interface is geselecteerd. Anders klikt u op de vervolgkeuzelijst en kiest u de juiste poort.

### Edit Port Authentication

Interface:  Port GE1 ▾

## Stap 4

Kies een radioknop voor de administratieve poortcontrole. Dit zal bepalend zijn voor de staat van de havenvergunning. De opties zijn:

- **Uitgeschakeld** — schakelt 802.1x in. Dit is de standaard toestand.
- **Macht Onbevoegd** — ontkent de interfacetoegang door de interface naar de onbevoegde staat te verplaatsen. De switch verleent geen authenticatiediensten aan de cliënt via de interface.
- **Auto** — staat verificatie en autorisatie op basis van haven op de switch toe. De interface beweegt tussen een geautoriseerde of niet-geautoriseerde staat op basis van de authenticatie-uitwisseling tussen de switch en de cliënt.
- **Macht geautoriseerd** — machtigt de interface zonder authenticatie.

Interface:  Port GE1 ▾

Administrative Port Control:  Disabled  
 Force Authorized  
 Force Unauthorized  
 Auto

## Stap 5 (optioneel)

Kies een radioknop voor de RADIUS VLAN-toewijzing. Dit zal Dynamische VLAN-toewijzing op de gespecificeerde poort mogelijk maken. De opties zijn:

- **Uitgeschakeld** - Hiermee wordt het VLAN autorisatie resultaat genegeerd en wordt het oorspronkelijke VLAN van de host bewaard. Dit is de standaardactie.
- **Afwijzen** — Als de gespecificeerde poort een VLAN geautoriseerde informatie ontvangt, zal het de informatie gebruiken. Als er echter geen geautoriseerde informatie van VLAN is, zal deze de host verwerpen en onbevoegd maken.
- **Statisch** — Als de gespecificeerde poort VLAN geautoriseerde informatie ontvangt, zal het de informatie gebruiken. Als er echter geen geautoriseerde informatie van VLAN is, zal deze het oorspronkelijke VLAN van de host bewaren.

Als er VLAN-geautoriseerde informatie via RADIUS is, maar het VLAN wordt administratief niet gemaakt op Devices Onder Test (DUT), wordt het VLAN automatisch gemaakt.

RADIUS VLAN Assignment:  Disabled  
 Reject  
 Static

**Quick Tip:** Voor de functie Dynamische VLAN-toewijzing om te kunnen werken vereist de switch dat de volgende VLAN-eigenschappen door de RADIUS-server worden verzonden:

- [64] Tunnel-type = VLAN (type 13)
- [65] Tunnel-Medium-type = 802 (type 6)
- [81] Tunnel-Private-Group-ID = VLAN-id

### Stap 6 (optioneel)

Controleer het aanvinkvakje **Enable** for the Guest VLAN om een gast VLAN voor onbevoegde poorten te gebruiken.

Guest VLAN:  Enable

### Stap 7

Controleer het aanvinkvakje **Enable** for Periodic ReAuthentication (Periodieke verificatie). Dit zal pogingen tot herbevestiging van havens mogelijk maken na de gespecificeerde Reauthenticatieperiode.

Periodic Reauthentication:  Enable

### Stap 8

Voer een waarde in het veld *Verificatieperiode in*. Dit is de tijd in seconden om de poort opnieuw te bevestigen.

Reauthentication Period: 3600

### Stap 9 (optioneel)

Controleer het aanvinkvakje **Nu opnieuw bevestigen** om onmiddellijke port opnieuw te bevestigen.

Het veld Authenticator State geeft de huidige status van de authenticatie weer.

Reauthenticate Now:  Enable

Authenticator State: Initialize

Als de haven niet in werking is getreden, wordt de staat in de Auto Mode en de authenticator de staat van de lopende authenticatie weergegeven. Nadat de haven voor authentiek is verklaard, wordt de staat getoond zoals Verificeerd.

## Stap 10

In het veld *Max Hosts* voert u het maximale aantal gewaarmerkte hosts in dat op de specifieke poort is toegestaan. Deze waarde wordt alleen van kracht op de multi-sessiemodus.

(Range: 1 - 256, Default: 256)

## Stap 11

Voer in het veld *Quiet Period* het aantal seconden in dat de switch in de stille toestand blijft na een mislukte authenticatie-uitwisseling. Wanneer de switch zich in een rustige staat bevindt, betekent dit dat de switch niet luistert naar nieuwe authenticatieverzoeken van de cliënt.

sec (Range: 0 - 65535)

## Stap 12

Voer in het veld *Resending EAP* het aantal seconden in dat de switch wacht op een antwoord op een MAP-verzoek of identiteitskader van de aanvrager (cliënt) alvorens het verzoek in te dienen.

(Range: 1 - 65535, Default: 30)

## Stap 13

Voer in het veld *MAP MAP-aanvragen* het maximale aantal MAP-verzoeken in dat kan worden verstuurd. Indien na de vastgestelde periode geen reactie is ontvangen (leverende tijdslimiet), wordt het authenticatieproces hervat.

(Range: 1 - 10, Default: 2)

## Stap 14

Voer in het veld *Leverancier Time-out* het aantal seconden in dat vervalft voordat MAP-verzoeken aan de aanvrager worden gericht.

sec (Range: 1 - 65535, Default: 30)

## Stap 15

In het veld *Time-out voor server* specificeert u het aantal seconden dat vervalft voordat de switch een aanvraag doorstuurt naar de verificatieserver.

sec (Range: 1 - 65535, Default: 30)

## Stap 16

Klik op Apply (Toepassen).



U moet nu een 802.1x-verificatie op uw switch hebben uitgevoerd.

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

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