Configuratie 802.1X poortverificatie op Cisco SX220 Series Smart-switches

Doel

Het doel van dit artikel is om u te tonen hoe te om poortauthenticatie op de Sx220 Series slimme switches te configureren.

Met 802.1X Port-verificatie kunt u 802.1X-parameters configureren voor elke poort op uw apparaat. Een haven die om authenticatie verzoekt wordt de aanvrager genoemd. De authenticator is een schakelaar of een toegangspunt die als netwerkbeveiliging voor beambten fungeert. De authenticator stuurt authenticatieberichten naar de RADIUS-server zodat een poort kan worden geauthentiseerd en informatie kan verzenden en ontvangen.

Toepasselijke apparaten

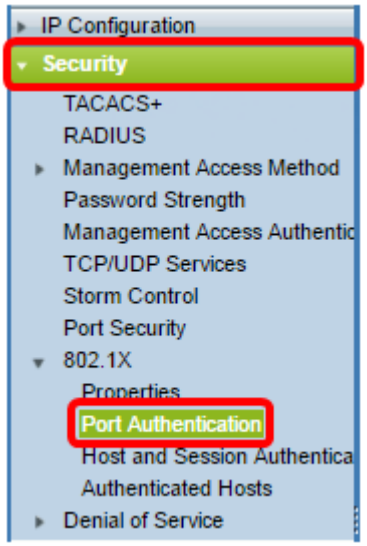
- SX220 Series-switches

Softwareversie

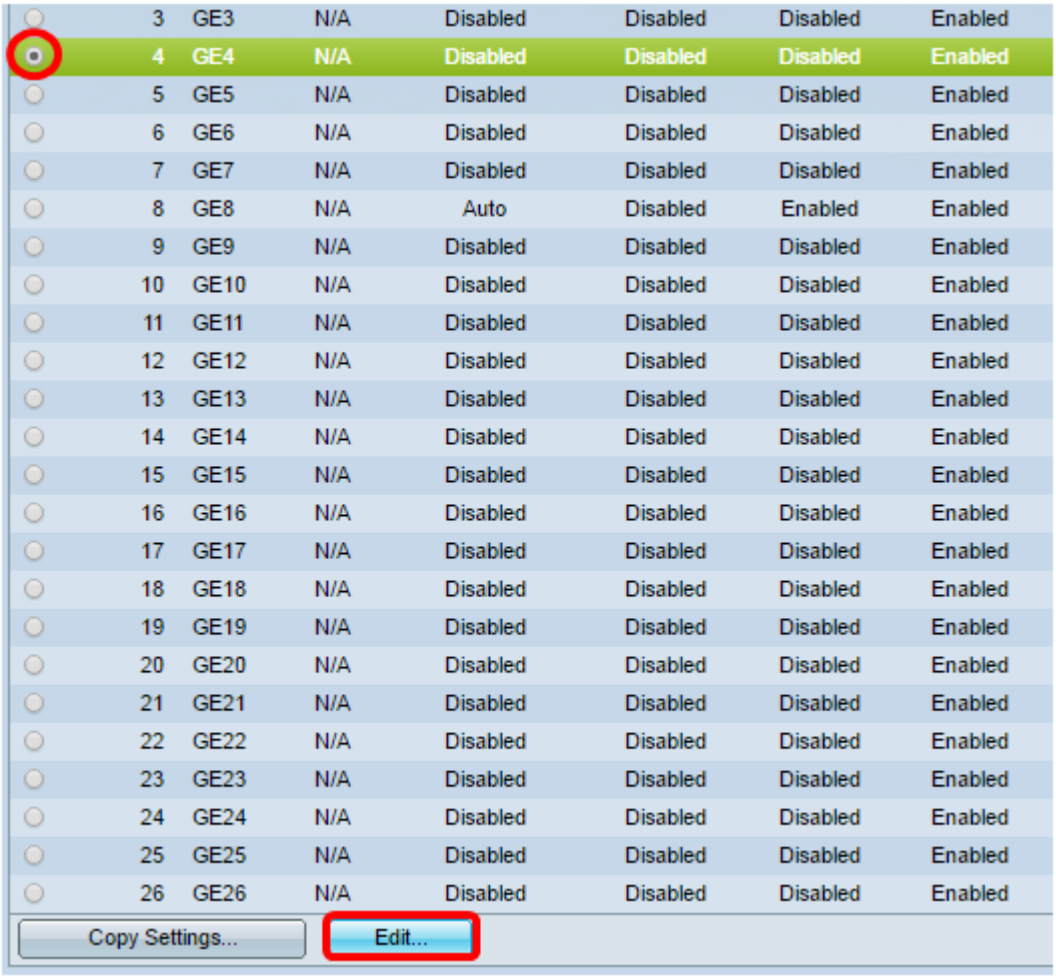
- 1.1.0.14

Poortverificatie configureren

Stap 1. Meld u aan bij het op het web gebaseerde wisselprogramma en kies **Security > 802.1X > Port-verificatie**.



Stap 2. Klik op het keuzerondje voor de poort die u wilt configureren en klik vervolgens op **Bewerken**.

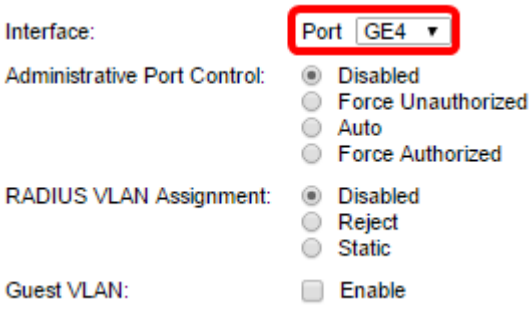


○	3	GE3	N/A	Disabled	Disabled	Disabled	Enabled
◉	4	GE4	N/A	Disabled	Disabled	Disabled	Enabled
○	5	GE5	N/A	Disabled	Disabled	Disabled	Enabled
○	6	GE6	N/A	Disabled	Disabled	Disabled	Enabled
○	7	GE7	N/A	Disabled	Disabled	Disabled	Enabled
○	8	GE8	N/A	Auto	Disabled	Enabled	Enabled
○	9	GE9	N/A	Disabled	Disabled	Disabled	Enabled
○	10	GE10	N/A	Disabled	Disabled	Disabled	Enabled
○	11	GE11	N/A	Disabled	Disabled	Disabled	Enabled
○	12	GE12	N/A	Disabled	Disabled	Disabled	Enabled
○	13	GE13	N/A	Disabled	Disabled	Disabled	Enabled
○	14	GE14	N/A	Disabled	Disabled	Disabled	Enabled
○	15	GE15	N/A	Disabled	Disabled	Disabled	Enabled
○	16	GE16	N/A	Disabled	Disabled	Disabled	Enabled
○	17	GE17	N/A	Disabled	Disabled	Disabled	Enabled
○	18	GE18	N/A	Disabled	Disabled	Disabled	Enabled
○	19	GE19	N/A	Disabled	Disabled	Disabled	Enabled
○	20	GE20	N/A	Disabled	Disabled	Disabled	Enabled
○	21	GE21	N/A	Disabled	Disabled	Disabled	Enabled
○	22	GE22	N/A	Disabled	Disabled	Disabled	Enabled
○	23	GE23	N/A	Disabled	Disabled	Disabled	Enabled
○	24	GE24	N/A	Disabled	Disabled	Disabled	Enabled
○	25	GE25	N/A	Disabled	Disabled	Disabled	Enabled
○	26	GE26	N/A	Disabled	Disabled	Disabled	Enabled

Copy Settings... Edit...

Opmerking: In dit voorbeeld wordt Port GE4 gekozen.

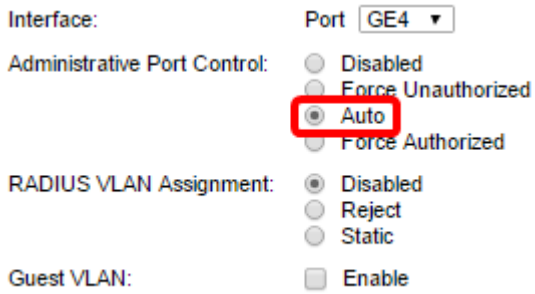
Stap 3. Het venster Port-verificatie bewerken verschijnt dan. Zorg ervoor dat de gespecificeerde poort in Stap 2 in de vervolgkeuzelijst Interface is geselecteerd. Anders klikt u op de vervolgkeuzelijst en kiest u de juiste poort.



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 biedt geen verificatiediensten aan de cliënt via de interface.
- Auto — schakelt poortgebaseerde verificatie en autorisatie in. De interface beweegt tussen een geautoriseerde of niet-geautoriseerde staat op basis van de authenticatie-uitwisseling tussen de switch en de client.

- Macht geautoriseerd — autoriseert de interface zonder authenticatie.

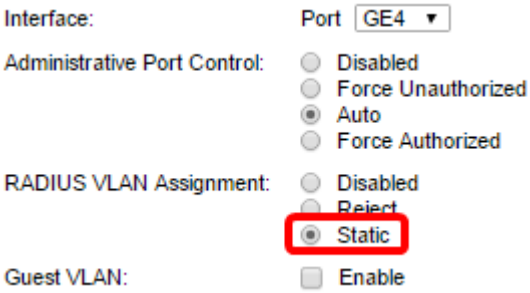


Opmerking: In dit voorbeeld wordt Auto geselecteerd.

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-autorisatieresultaat genegeerd en wordt origineel VLAN van 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 een 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.

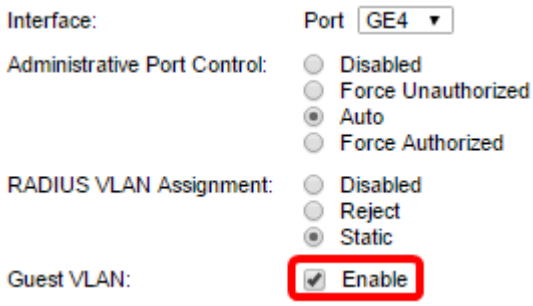
Opmerking: Als er een VLAN-geautoriseerde informatie via RADIUS is, maar het VLAN wordt administratief niet gemaakt op Devices Onder Test (DUT), wordt het VLAN automatisch gemaakt. In dit voorbeeld wordt Static geselecteerd.



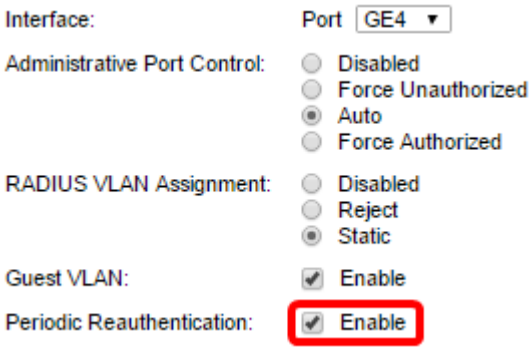
Quick Tip: Voor de functie Dynamische VLAN-toewijzing om te werken vereist de switch dat de volgende VLAN-eigenschappen door de RADIUS-server worden verzonden:

- [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 te gebruiken voor niet-geautoriseerde poorten.

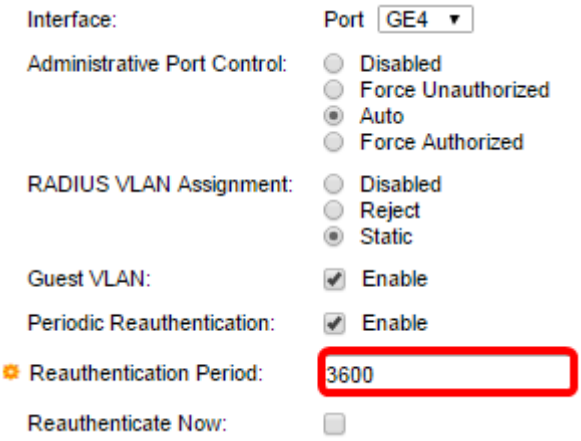


Stap 7. Controleer het vakje **Enable** check for Periodic ReAuthentication (Periodieke verificatie). Dit zal pogingen tot herbevestiging van havens mogelijk maken na de gespecificeerde Reauthenticatieperiode.



Opmerking: Deze optie is standaard ingeschakeld.

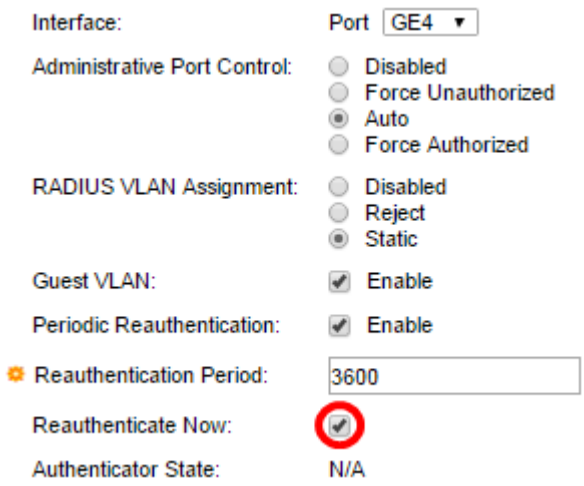
Stap 8. Voer een waarde in het veld *Verificatieperiode in*. Dit is de tijd in seconden om de poort opnieuw te bevestigen.



Opmerking: In dit voorbeeld wordt de standaardwaarde 3600 gebruikt.

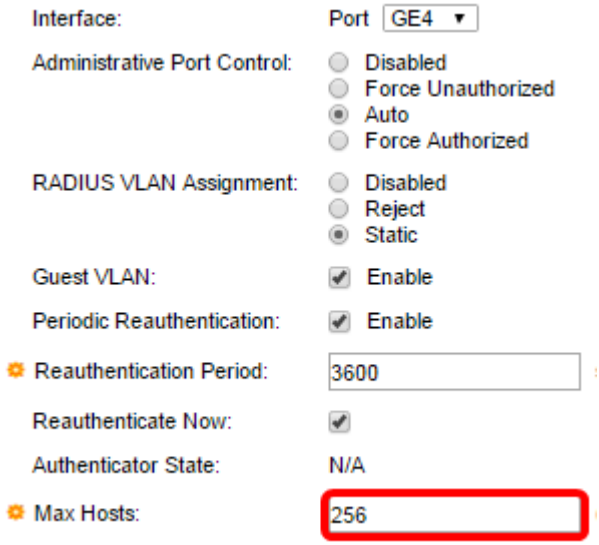
Stap 9. (Optioneel) Controleer het aanvinkvakje **Nu opnieuw** bevestigen om ervoor te zorgen dat de poort opnieuw wordt geauthentificeerd.

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



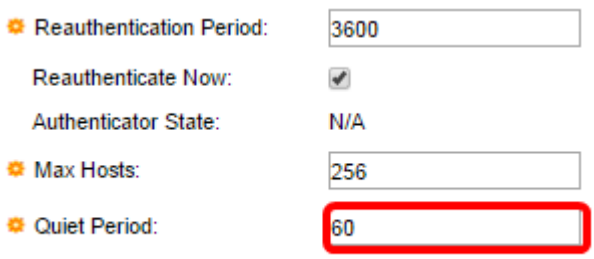
Opmerking: Als de haven niet in werking is getreden, wordt de staat in de Auto Mode en de authenticator de staat van de lopende authenticatie weergegeven. Nadat de haven voor authentiek is verklaard, wordt de staat getoond zoals Verificeerd.

Stap 10. In het veld *Max Hosts*, specificeert u het maximale aantal gewaarmerkte hosts dat op de specifieke poort is toegestaan. Deze waarde wordt alleen van kracht op multi-sessiemodus.



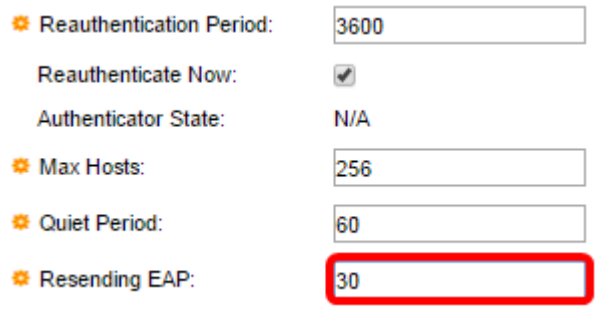
Opmerking: In dit voorbeeld wordt de standaardwaarde 256 gebruikt.

Stap 1. In het veld *Quiet Period* voert u het aantal seconden in dat de switch in de stille toestand blijft na een mislukte authenticatie-uitwisseling. Wanneer de schakelaar in rustige staat is, betekent het dat de schakelaar niet naar nieuwe authentificatieverzoeken van de cliënt luistert.



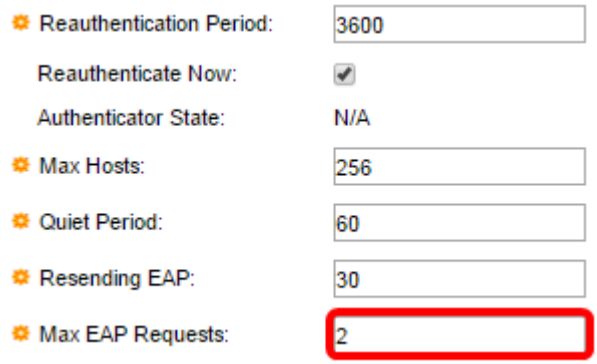
Opmerking: In dit voorbeeld wordt de standaardwaarde 60 gebruikt.

Stap 12. Voer in het veld *Resending EAP* het aantal seconden in dat de switch wacht op een reactie op een MAP-verzoek of een identiteitskader van de aanvrager (client) alvorens het verzoek in te dienen.



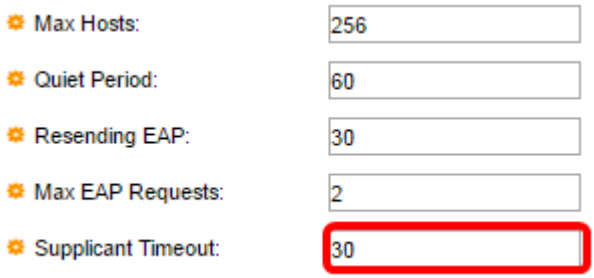
Opmerking: In dit voorbeeld wordt de standaardwaarde 30 gebruikt.

Stap 13. In het veld *MAP-aanvragen* vermeldt u het maximale aantal MAP-verzoeken dat kan worden verstuurd. Indien na de vastgestelde periode geen reactie is ontvangen (leverende tijdslimiet), wordt het authenticatieproces hervat.



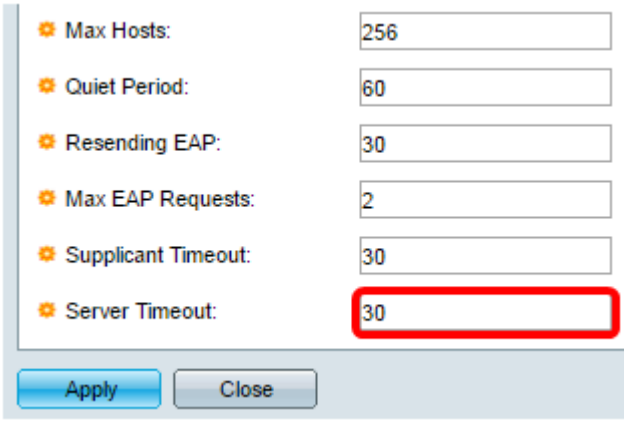
Opmerking: In dit voorbeeld wordt de standaardwaarde 2 gebruikt.

Stap 14. In het veld *Leverende Time-out* voert u het aantal seconden in dat vervalt voordat MAP-verzoeken aan de aanvrager worden gericht.



Opmerking: In dit voorbeeld wordt de standaardwaarde 30 gebruikt.

Stap 15. In het veld *Time-out voor servers* voert u het aantal seconden in dat vervalt voordat de switch een verzoek doorstuurt naar de verificatieserver.



Opmerking: In dit voorbeeld wordt de standaardwaarde 30 gebruikt.

Stap 16. Klik op **Toepassen**.

U had nu met succes Port Authentication op uw switch moeten configureren.