

802.1X host- en sessieverificatie-configuratie op 200/220/300 Series Switches

Doel

802.1X is een IEEE-standaard voor poortgebaseerde Network Access Control (PNAC) die een verificatiemethode biedt voor apparaten die zijn verbonden met poorten. De pagina Host- en Sessieverificatie in de beheerdersGUI van uw switch wordt gebruikt om te bepalen welk verificatietype per poort wordt gebruikt. Verificatie per poort is een functie waarmee een netwerkbeheerder de switch-poorten kan verdelen op basis van het gewenste type verificatie. De pagina Authenticated Hosts geeft informatie weer over hosts die zijn geverifieerd.

In dit artikel wordt uitgelegd hoe u host- en sessieverificatie per poort kunt configureren en hoe u de geverifieerde hosts kunt bekijken in 802.1X-beveiligingsinstellingen op de 200/220/300 Series beheerde Switches.

Toepasselijke apparaten

- SX200 Series
- SX220 Series
- Sx300 Series

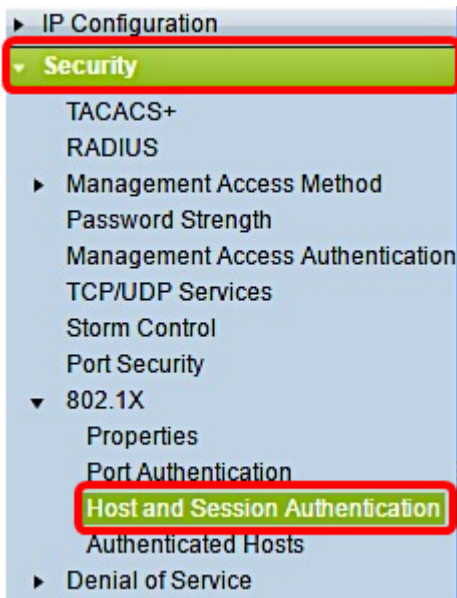
Softwareversie

- 1.4.5.02 — SX200 Series, SX300 Series
- 1.1.0.14 — SX220-serie

Host- en sessieverificatie

Stap 1. Meld u aan bij het webgebaseerde hulpprogramma en kies **Beveiliging > 802.1X > Host- en Sessieverificatie**.

Opmerking: de onderstaande afbeeldingen zijn afkomstig van de SG220-26P Smart switch.



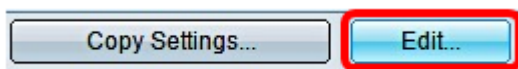
Stap 2. Klik op het keuzerondje van de poort die u wilt bewerken.

The screenshot shows the 'Host and Session Authentication' configuration page. It features a table titled 'Host and Session Authentication Table' with the following structure:

	Entry No.	Port	Host Authentication	Single Host			
				Action on Violation	Traps	Trap Frequency	Number of Violation
<input type="radio"/>	1	GE1	Multiple Host				
<input checked="" type="radio"/>	2	GE2	Multiple Host				
<input type="radio"/>	3	GE3	Multiple Host				
<input type="radio"/>	4	GE4	Multiple Host				
<input type="radio"/>	5	GE5	Multiple Host				
<input type="radio"/>	6	GE6	Multiple Host				
<input type="radio"/>	7	GE7	Multiple Host				

Opmerking: in dit voorbeeld is Port GE2 gekozen.

Stap 3. Klik op **Bewerken** om de verificatie van de host en de sessie voor de opgegeven poort te bewerken.



Stap 4. Het venster Poortverificatie bewerken wordt weergegeven. Zorg ervoor dat de opgegeven poort de poort is die u in Stap 2 hebt gekozen in de vervolgkeuzelijst Interface. Anders klikt u op het pijltje van de vervolgkeuzelijst en kiest u de juiste poort.

The screenshot shows the 'Port Verification Edit' dialog box. It has the following fields:

- Interface: Port GE2 (dropdown menu, highlighted with a red box)
- Host Authentication: Multiple Host, Single Host, Multiple Sessions

N.B.: Als u de 200 of 300 Series gebruikt, wordt het venster Host en Sessieverificatie bewerken weergegeven.

Stap 5. Klik op het keuzerondje dat overeenkomt met de gewenste verificatiemodus in het

veld *Hostverificatie*. De opties zijn:

- Eén host — De switch verleent slechts één gemachtigde host toegang tot de poort.
- Meervoudige host (802.1X) — Meervoudige hosts kunnen toegang verkrijgen tot de enkele poort. Dit is de standaardmodus. De switch vereist alleen dat de eerste host geautoriseerd is, daarna hebben alle andere clients die verbonden zijn met de poort toegang tot het netwerk. Indien de verificatie mislukt, wordt de eerste host en alle aangesloten clients de toegang tot het netwerk ontzegd.
- Meervoudige sessies — Meervoudige host kan toegang verkrijgen tot de enkele poort, maar elke host moet worden geauthenticeerd.

Opmerking: in dit voorbeeld wordt één host gekozen.

Interface: Port

Host Authentication: Single Host
 Multiple Host
 Multiple Sessions

Opmerking: als u meerdere host- of meerdere sessies hebt gekozen, gaat u naar [stap 9](#).

Stap 6. Klik in het gedeelte Single Host Violation Settings op het keuzerondje dat overeenkomt met de gewenste actie bij overtreding. Een schending komt voor als de pakketten van een gastheer aankomen die een adres heeft van MAC dat niet het adres van MAC van de originele bezoeker aanpast. Wanneer dit voorkomt, bepaalt de actie wat gebeurt met pakketten die van gastheren aankomen die niet als de originele bezoeker worden beschouwd. De opties zijn:

- Beschermen (Afdanken) — Laat de pakjes vallen. Dit is de standaardactie.
- Restrictie (Forward) — Geeft toegang tot de pakketten en stuurt ze door.
- Sluiten — Blokkeert de pakketten en sluit de poort. De poort blijft ingedrukt totdat deze opnieuw wordt geactiveerd of totdat de switch opnieuw wordt opgestart.

Opmerking: in dit voorbeeld is de optie Beperken (voorwaarts) geselecteerd.

Single Host Violation Settings:

Action on Violation: Protect (Discard)
 Restrict (Forward)
 Shutdown

Stap 7. (Optioneel) Controleer **of** in het veld *Traps Inschakelen* om traps in te schakelen. Traps zijn gegenereerde Simple Network Management Protocol (SNMP)-berichten die worden gebruikt om systeemgebeurtenissen te melden. Er wordt een trap naar de SNMP-beheerder van de switch gestuurd als er een overschrijding optreedt.

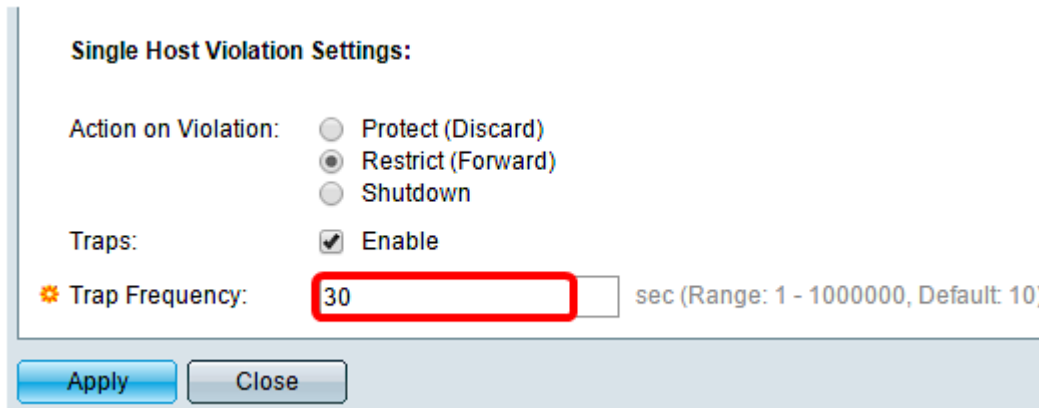
Single Host Violation Settings:

Action on Violation: Protect (Discard)
 Restrict (Forward)
 Shutdown

Traps: Enable

Stap 8. Voer in het veld *Trap Frequency* de gewenste tijd in die tussen de verzonden traps in seconden is toegestaan. Dit bepaalt hoe vaak vallen worden verzonden.

Opmerking: in dit voorbeeld wordt 30 seconden gebruikt.



Single Host Violation Settings:

Action on Violation: Protect (Discard)
 Restrict (Forward)
 Shutdown

Traps: Enable

Trap Frequency: sec (Range: 1 - 1000000, Default: 10)

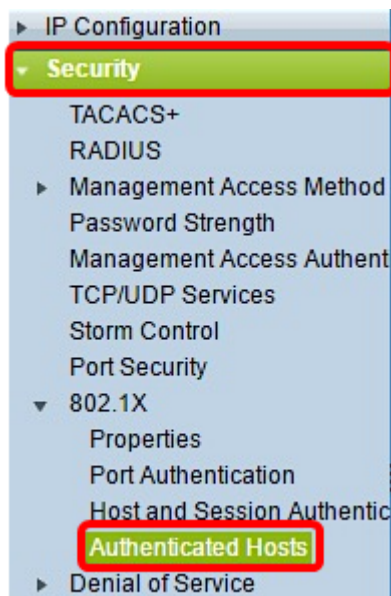
Apply Close

Stap 9. Klik op Apply (Toepassen).

U moet nu de host- en sessieverificatie op uw switch hebben geconfigureerd.

Geverifieerde hosts bekijken

Stap 1. Meld u aan bij het webgebaseerde hulpprogramma en kies **Security > 802.1X > Authenticated Host**.



De tabel Authenticated Hosts geeft de volgende informatie voor geverifieerde hosts weer.

Authenticated Hosts					
Authenticated Host Table					
User Name	Port	Session Time (DD:HH:MM:SS)	Authentication Method	MAC Address	VLAN ID
0 results found.					

- Gebruikersnaam — Specificeert de naam van de aanvrager die op de poort is geverifieerd.
- Port — Specificeert het poortnummer waarmee de aanvrager is verbonden.

- Sessietijd — Specificeert de gehele tijd dat de aanvrager is verbonden met de poort. Het formaat is DD:UU:MM:SS (Dag:Uur:minuut:seconde).
- Verificatiemethode — Specificeert de methode die wordt gebruikt voor het verifiëren. De mogelijke waarden zijn:
 - Geen — Geeft aan dat de aanvrager niet is geauthenticeerd.
 - Straal — Specificeert dat de aanvrager is geverifieerd door de RADIUS-server.
 - MAC-adres — Specificeert het MAC-adres van de aanvrager.
 - VLAN ID — Specificeert tot welk VLAN de host behoort. De kolom van VLAN-id is alleen beschikbaar in de 220 Series Smart Plus-Switches.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.