Management Access Connection Setup op SX500 Series Stackable-switches

Doel

De verificatiemethode helpt de netwerkbeheerders de toegang van het apparaat via verschillende methoden zoals SSH, telnet, HTTP enzovoort toe te staan of te ontkennen. RADIUS, TACACS+ en Local zijn de drie types van veiligheid die in de authenticatie instelling functie op de SG500x Series kunnen worden ingeschakeld. Er is ook een optie dat er geen beveiliging aanwezig is op de switch. RADIUS versleutelt alleen het wachtwoord in het toegangspakket dat van de client naar de server wordt overgebracht. TACACS+ versleutelt de gehele inhoud van het pakket. Er blijft echter een standaard TACACS+ header over. Local verifieert alleen gebruikersinformatie die op de switch is opgeslagen. Verificatie door de gebruiker vindt plaats in de volgorde dat de authenticatiemethoden worden geselecteerd. Als de eerste authenticatiemethode niet beschikbaar is, wordt de volgende geselecteerde methode gebruikt. Als een authenticatiemethode faalt of de gebruiker onvoldoende voorkeursniveau heeft, wordt de gebruiker toegang tot de schakelaar ontzegd.

Dit artikel legt uit hoe verificatiemethoden aan toegangsmodi zoals SSH, console, telnet, HTTP en HTTPS moeten worden toegewezen op de SG500x Series Stackable Switches.

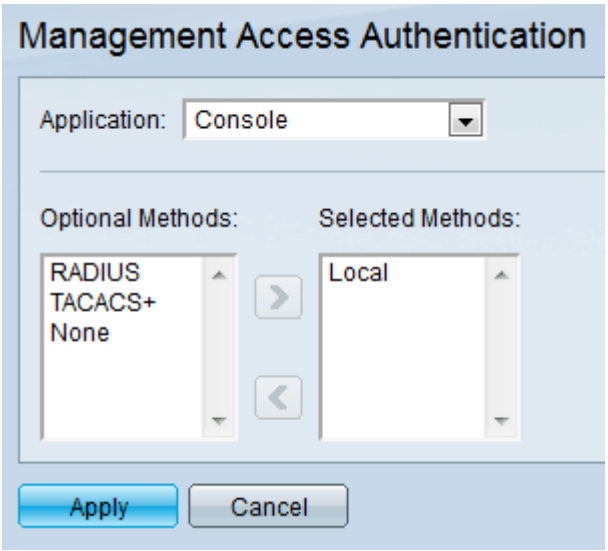
Toepasselijke apparaten

- SX500 Series Stackable-switches

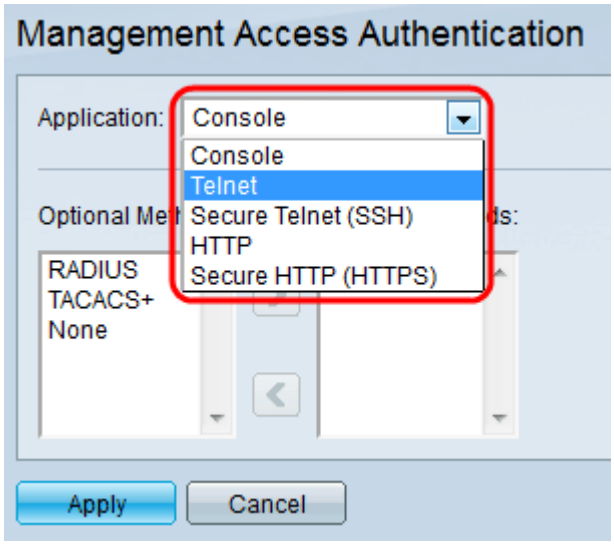
Softwareversie

•1.3.0.62

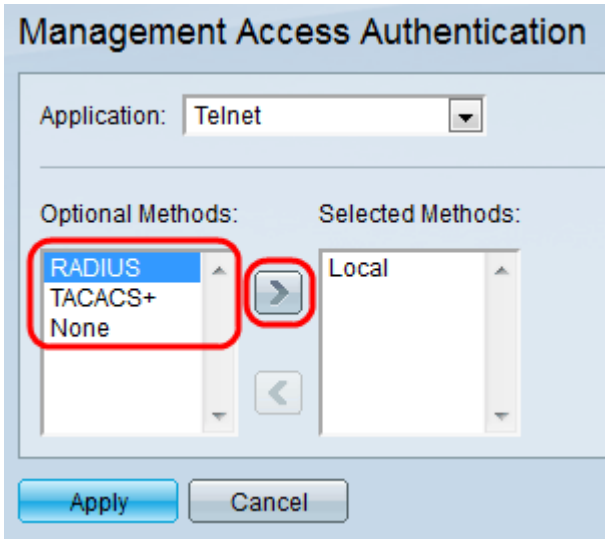
Instellen van beheertoegangsverificatie



Stap 1. Meld u aan bij het web-configuratieprogramma en kies **Security > Management Access Authentication**. De pagina *Management Access Authentication* wordt geopend:

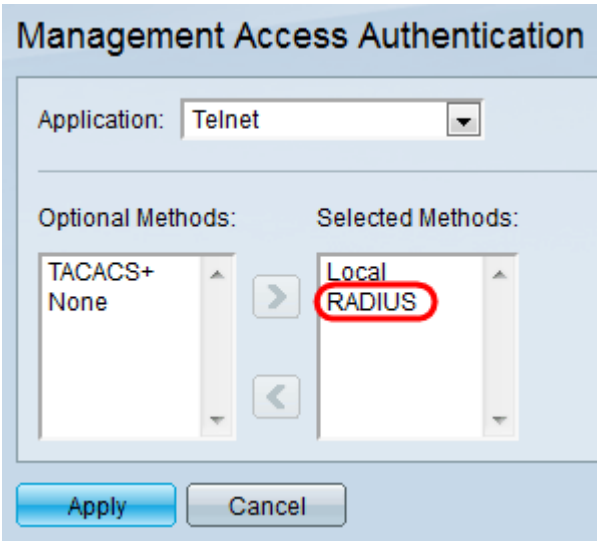


Stap 2. Kies het type toepassing waarin u verificatie wilt toewijzen in de vervolgkeuzelijst Toepassingsgebied.



Stap 3. Kies de methode van authenticatie in de lijst Optionele Methoden en klik op het pictogram **Rechts** om dit naar de lijst Geselecteerde Methoden te verplaatsen.

- RADIUS — Verificatie vindt plaats op een RADIUS-server. Een RADIUS-server moet worden geconfigureerd.
- TACACS+ — Verificatie is op een TACACS+ server uitgevoerd. Een TACACS+ server moet worden geconfigureerd.
- Lokaal — gebruikersinformatie wordt geverifieerd door informatie die op de schakelaar is opgeslagen.
- Geen — Verificatie is niet vereist voor toegang tot de schakelaar.



Stap 4. (Optioneel) Kies de methode uit de geselecteerde methoden en klik op het pictogram pijl-**links** om te verwijderen van de geselecteerde methoden en deze naar optionele methoden te verplaatsen.

Stap 5. Klik op **Toepassen** om de verificatie-instellingen op te slaan.