Secure Shell (SSH) serververificatie voor SSH-clients met SX500 Series Stackable-switches

Doel

Met de serverfunctie Secure Shell (SSH) kunt de gebruiker een SSH-sessie instellen met de SX500 Series Stackable-switches. Een SSH-sessie is net zoiets als een telnet-sessie, maar een SSH-sessie is veiliger. De beveiliging wordt door het apparaat behaald wanneer deze automatisch de openbare en privé toetsen genereert. Deze toetsen kunnen ook door de gebruiker worden gewijzigd. Een SSH-sessie kan worden geopend met behulp van de PuTTY-toepassing.

Dit artikel bevat informatie over de manier waarop SSH-serververificatie voor SSH-klanten mogelijk kan worden gemaakt en de vertrouwde servers op SX500 Series Stackable Switches kan worden gedefinieerd.

Toepasselijke apparaten

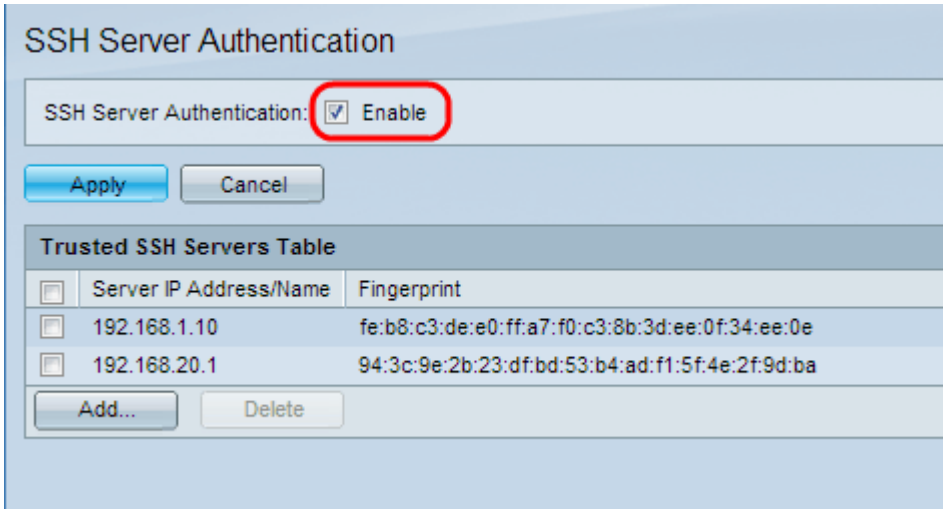
- SX500 Series Stackable-switches

Softwareversie

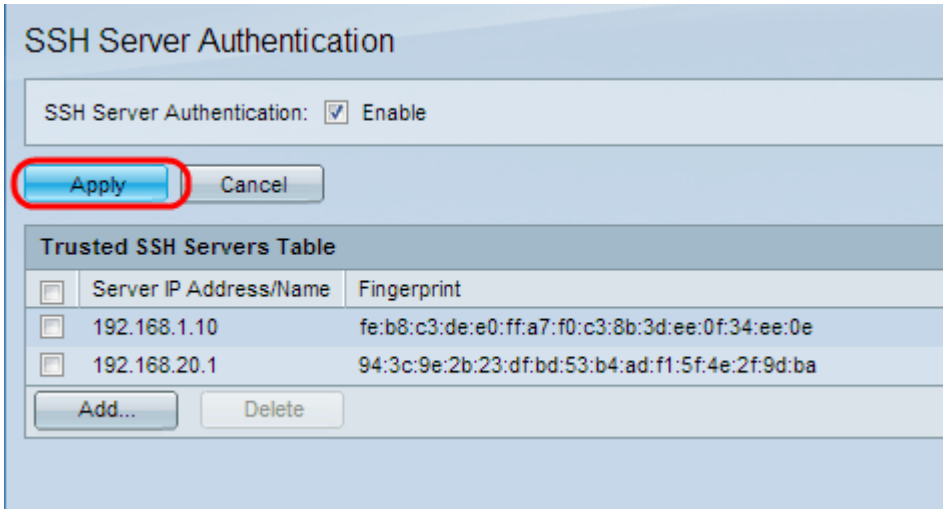
- v1.2.7.76

Configuratie van SSH-serververificatie

Stap 1. Meld u aan bij het web configuratieprogramma en kies **Security > SSH-client > SSH-serververificatie**. De pagina *SSH*-serververificatie wordt geopend:

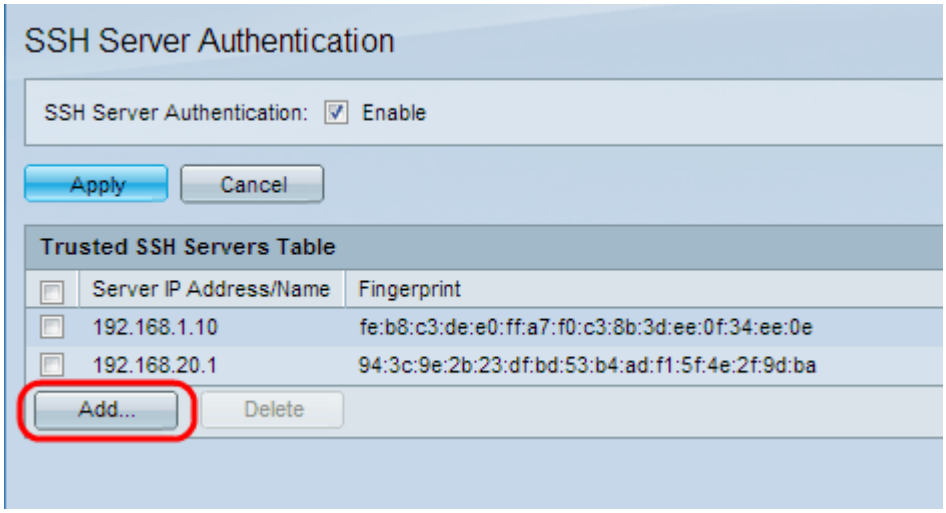


Stap 2. Controleer **Schakel** de SSH-serververificatie in.



Stap 3. Klik op **Toepassen** om de configuratie op te slaan.

Trusted SSH-server toevoegen



Stap 1. In de tabel Betrouwbare SSH-servers vindt u het IP-adres en de vingerafdruk van de SSH-server. Klik op **Add** om de vertrouwde SSH server toe te voegen. Het venster *Add Trusted SSH Server* verschijnt.

Stap 2. Klik op de knop **Door IP-adres** te selecteren om een IP-adres in het veld IP-adres/naam van de server in te voeren. Klik op het radioknop **By name** om de naam van de server in het veld IP Adres/naam van de server in te voeren.

Stap 3. Klik op de radioknop **Versie 4** of **Versie 6** om respectievelijk een IPv4 of IPv6 IP-adres in het veld IP-adres/naam van de server in te voeren. IP, versie 6, kan alleen worden

geselecteerd als er een IPv6-adres is ingesteld op het apparaat.

Stap 4. Voer een IPv4- of IPv6-adres in van de vertrouwde SSH-gebruiker in het veld IP-adres/naam van de server.

Stap 5. Voer 16 paren hexadecimale waarden in voor de vingerafdruk van de SSH-server in het veld Fingerprint. Om de vingerafdrukwaarde van de SSH-server te verkrijgen, navigeer naar **Security > SSH Server > SSH Server Verificatie.** Dit is een functie van SSH ter bescherming tegen een aanval waarbij een kwaadaardige gebruiker de client naar een andere server of computer leidt om de gebruikersnaam en het wachtwoord van de vertrouwde SSH-server te leren. De cliënt wordt geadviseerd om de vingerafdruk van de server te controleren en dan hun geloofsbrieven in te voeren.

Stap 6. Klik op **Toepassen** om de configuratie op te slaan.