Configuratie van Secure Shell (SSH) gebruikersverificatie-instellingen op een Cisco Business 350 Series Switch

Doel

Dit artikel bevat instructies hoe u de verificatie van clientgebruikers kunt configureren op Cisco Business 350 Series switches.

Inleiding

Secure Shell (SSH) is een protocol voor een beveiligde afstandsverbinding met specifieke netwerkapparaten. Deze verbinding biedt functionaliteit die vergelijkbaar is met een Telnet-verbinding, behalve dat het versleuteld is. SSH staat de beheerder toe om de switch door de interface van de opdrachtregel (CLI) met een programma van een derde te configureren.

In CLI-modus via SSH kan de beheerder meer geavanceerde configuraties uitvoeren in een beveiligde verbinding. SSH-verbindingen zijn handig om een netwerk op afstand op te lossen, in gevallen waarin de netwerkbeheerder niet fysiek aanwezig is op de netwerklocatie. De switch stelt de beheerder in staat om gebruikers voor authentiek te verklaren en te beheren om met het netwerk te verbinden via SSH. De authenticatie vindt plaats via een openbare toets die de gebruiker kan gebruiken om een SSH-verbinding naar een specifiek netwerk op te zetten.

De SSH client is een toepassing die over het SSH-protocol loopt om apparaatverificatie en -encryptie te leveren. Het stelt een apparaat in staat om een veilige en versleutelde verbinding te maken met een ander apparaat dat de SSH-server draait. Met verificatie en encryptie maakt de SSH-client een beveiligde communicatie via een onveilige Telnet-verbinding mogelijk.

Toepasselijke apparaten | Software versie

- CBS350 (Gegevensblad) | 3.0.0.69 (laatste download)
- CBS350-2X (Gegevensblad) | 3.0.0.69 (laatste download)
- CBS350-4X (Gegevensblad) | 3.0.0.69 (laatste download)

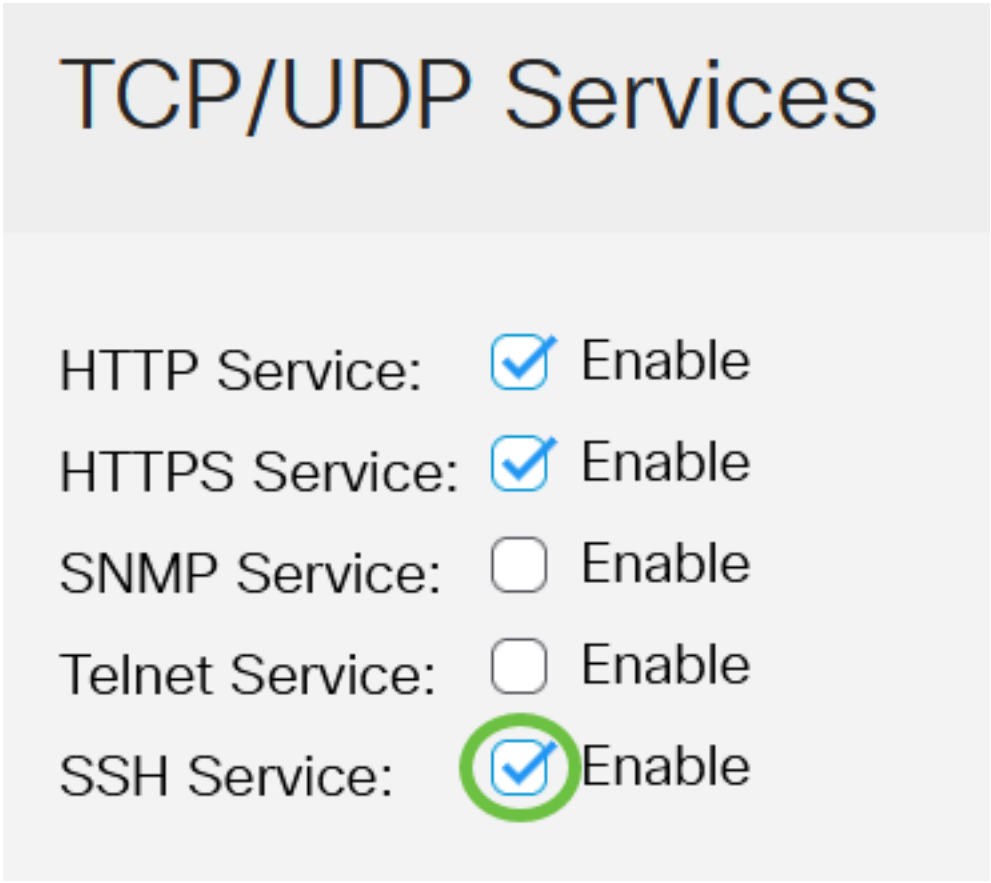
Instellingen SSH-clientverificatie

SSH-service inschakelen

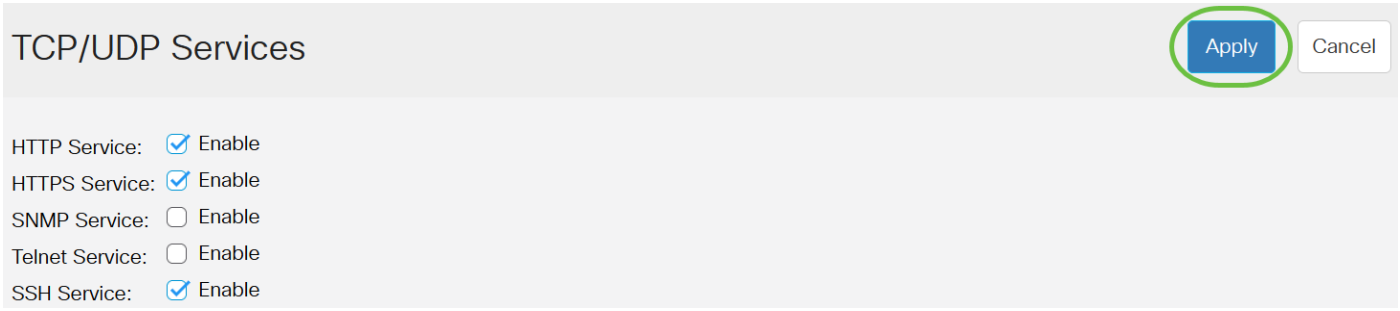
Om de automatische configuratie van een out-of-box apparaat te ondersteunen (apparaat met fabrieksstandaardconfiguratie), wordt de SSH-serververificatie standaard uitgeschakeld.

Stap 1. Meld u aan bij de webgebaseerde hulpprogramma's en kies **Beveiliging > TCP/UDP-services**

Stap 2. Controleer het aankruisvakje **SSH-service** om toegang tot de opdrachtmelding van switches via de SSH mogelijk te maken.



Stap 3. Klik op **Toepassen** om de SSH-service in te schakelen.

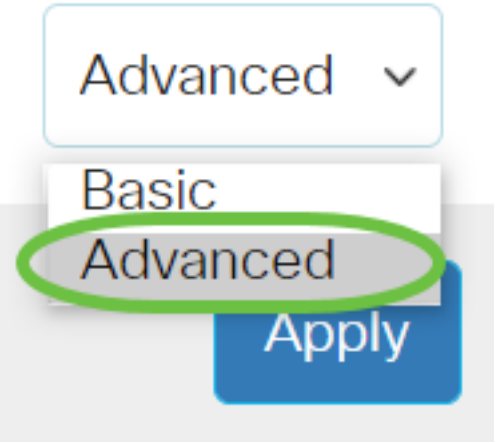


SSH-gebruikersverificatie-instellingen configureren

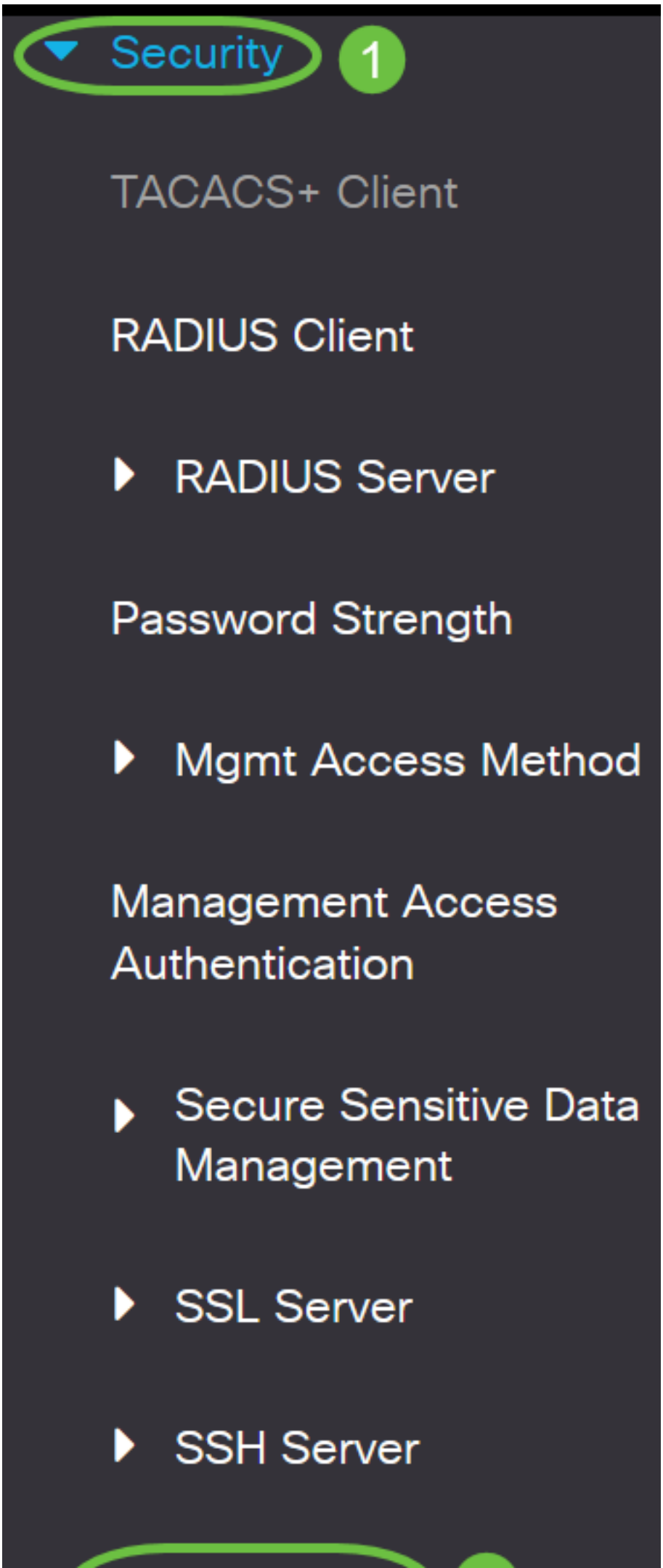
Gebruik deze pagina om een SSH-gebruikersverificatiemethode te kiezen. U kunt een gebruikersnaam en wachtwoord op het apparaat instellen als de wachtwoordmethode is gekozen. U kunt ook een Ron Rivest, Adi Shamir en Leonard Adleman (RSA) of Digital Signature Algorithm (DSA) toets genereren indien de openbare of particuliere methode is geselecteerd.

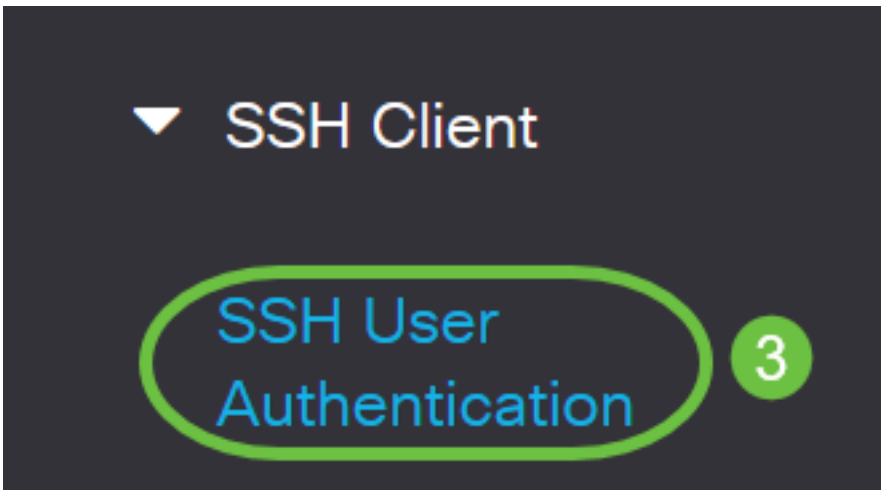
De standaardinstellingen van RSA en DSA worden gegenereerd voor het apparaat wanneer het wordt opgestart. Eén van deze toetsen wordt gebruikt om de gegevens te versleutelen die vanaf de SSH-server worden gedownload. De RSA-toets wordt standaard gebruikt. Als de gebruiker een of beide toetsen verwijdert, worden ze opnieuw gegenereerd.

Stap 1. Meld u aan bij het webgebaseerde hulpprogramma van uw switch en kies vervolgens Geavanceerd in de vervolgkeuzelijst Weergave-modus.

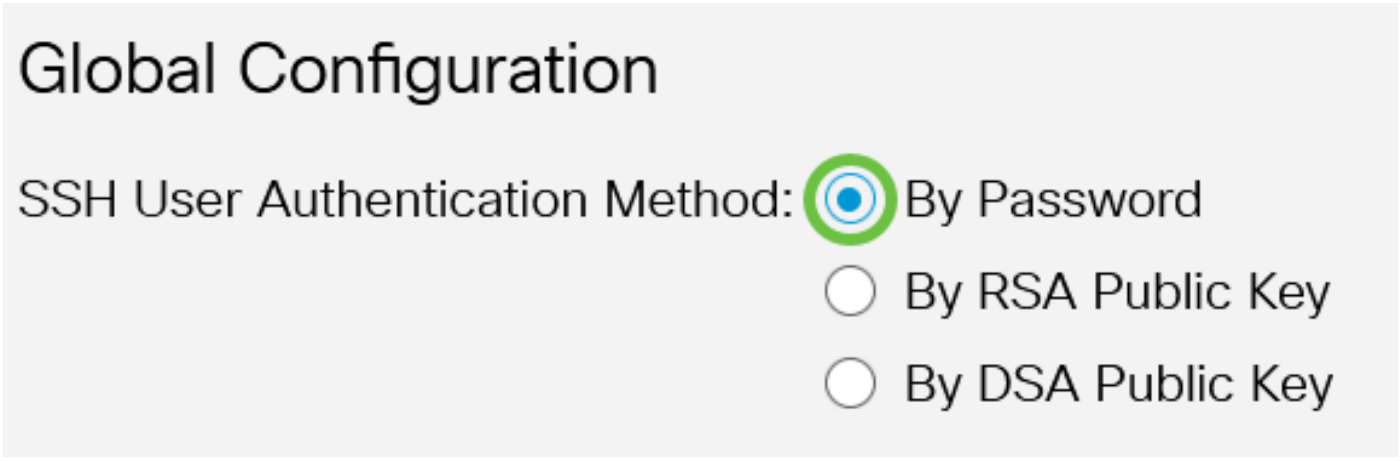


Stap 2. Kies **Security > SSH-client > SSH-gebruikersverificatie** in het menu.


Security
1
TACACS+ Client
RADIUS Client
RADIUS Server
Password Strength
Mgmt Access Method
Management Access Authentication
Secure Sensitive Data Management
SSL Server
SSH Server



Stap 3. Klik onder Global Configuration op de gewenste SSH-gebruikersverificatiemethode.



Wanneer een apparaat (SSH-client) probeert een SSH-sessie naar de SSH-server op te zetten, gebruikt de SSH-server een van de volgende methoden voor clientverificatie:

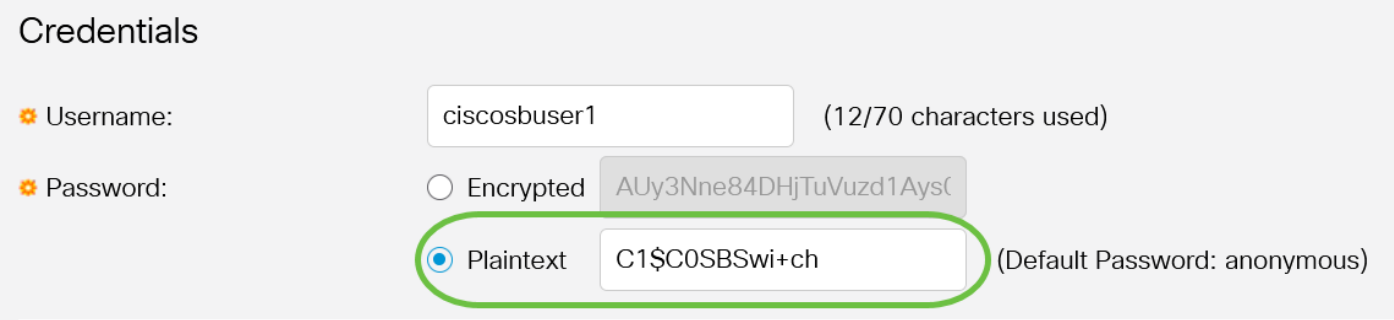
- Door wachtwoord - Met deze optie kunt u een wachtwoord voor de verificatie van gebruikers configureren. Dit is de standaardinstelling en het defaultwachtwoord is anoniem. Als deze optie geselecteerd is, zorg er dan voor dat de gebruikersnaam en de wachtwoordreferenties op de SSH-server zijn ingesteld.
- Door openbare RSA-toets - Met deze optie kunt u RSA-toets gebruiken voor gebruikersverificatie. Een RSA-toets is een gecodeerde sleutel gebaseerd op factorisatie van grote integers. Deze toets is het meest voorkomende type sleutel dat wordt gebruikt voor de authenticatie van SSH-gebruikers.
- Door openbare sleutel van DSA - Deze optie laat u een openbare sleutel van DSA voor gebruikersauthenticatie gebruiken. Een DSA-toets is een versleutelde sleutel gebaseerd op een discrete algoritme van ElGamal. Deze toets wordt niet algemeen gebruikt voor de authenticatie van SSH-gebruikers, aangezien het meer tijd vergt in het authenticatieproces.

In dit voorbeeld wordt met Wachtwoord gekozen.

Stap 4. Voer in het gebied Credentials de gebruikersnaam in het veld *Gebruikersnaam in*.

In dit voorbeeld wordt ciscosbuser1 gebruikt.

Stap 5. (Optioneel) Als u in Stap 2 voor Wachtwoord hebt gekozen, klikt u op de methode en vervolgens voert u het wachtwoord in het veld *Encrypted* of *Plaintext in*.

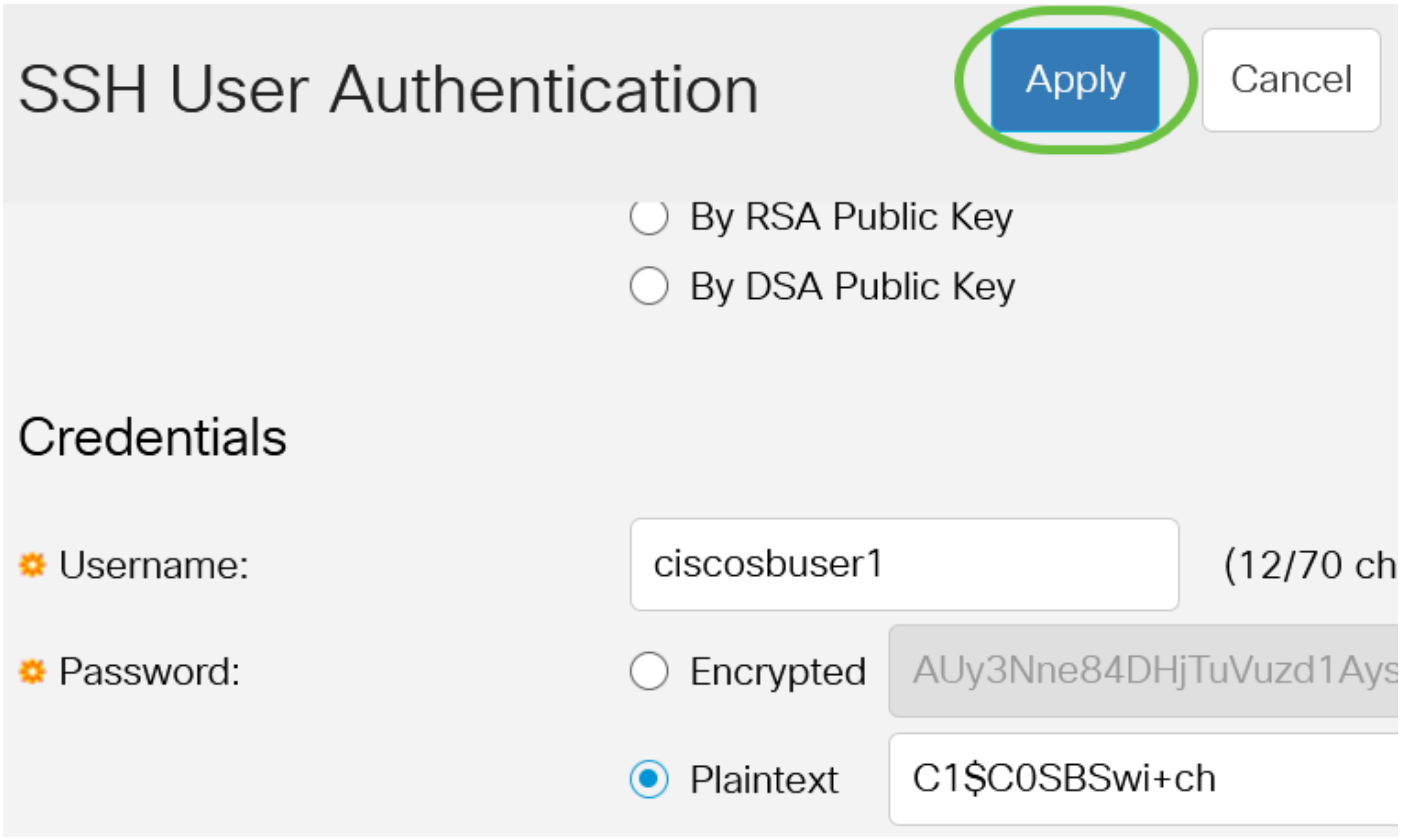


De opties zijn:

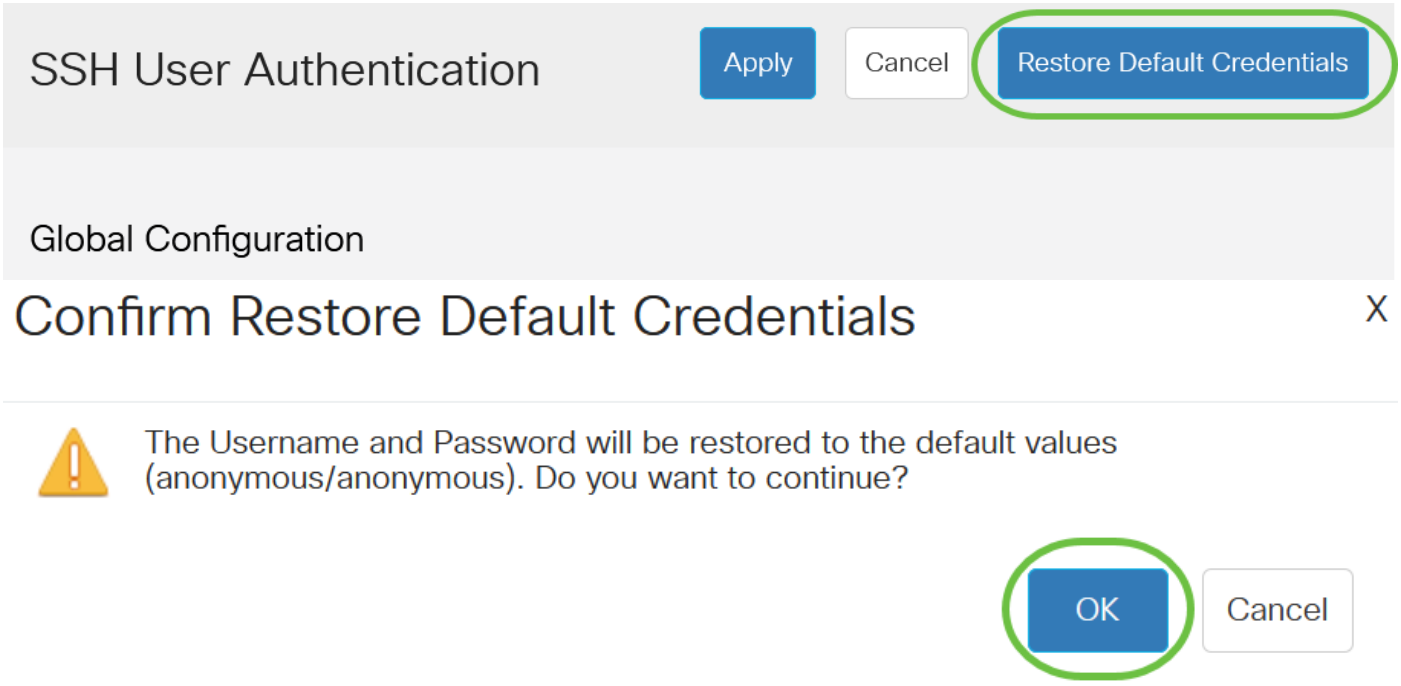
- Versleuteld - met deze optie kunt u een versleutelde versie van het wachtwoord invoeren.
- Plaintext - Met deze optie kunt u een duidelijk tekstwachtwoord invoeren.

In dit voorbeeld wordt de optie Plaintext geselecteerd en wordt een gewoon tekstwachtwoord ingevoerd.

Stap 6. Klik op **Toepassen** om uw verificatieconfiguratie op te slaan.

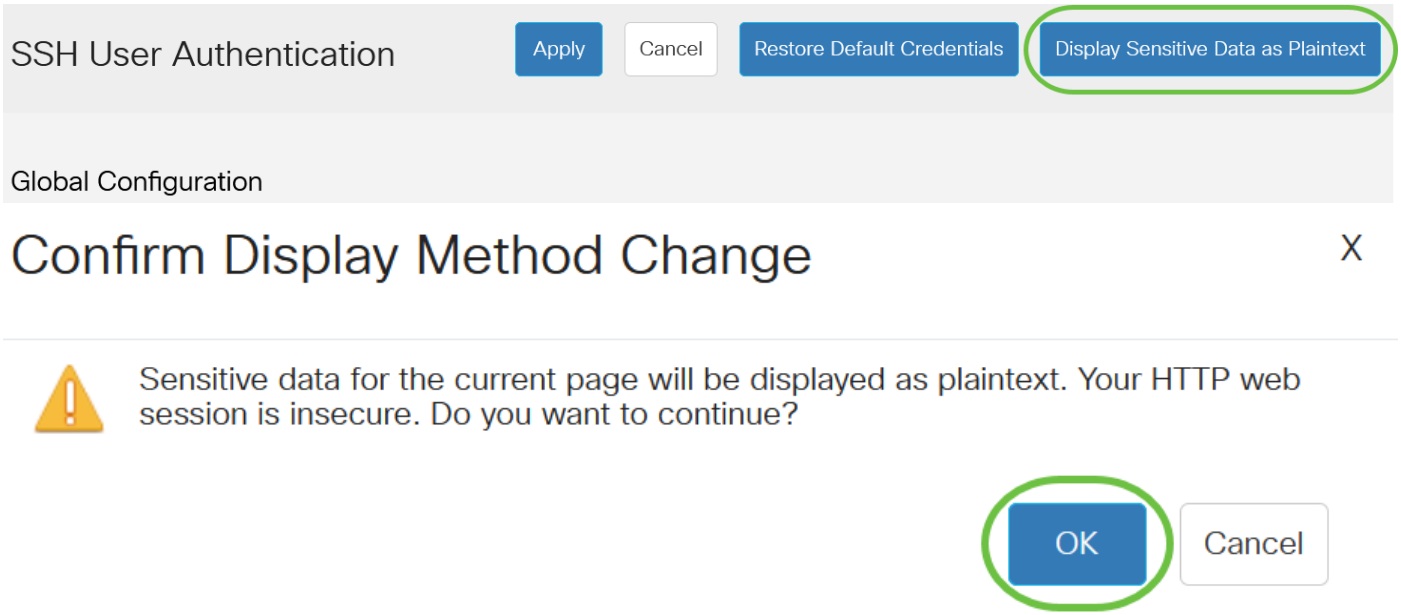


Stap 7. (Optioneel) Klik op **Standaardinstellingen herstellen** om de standaardnaam en het wachtwoord te herstellen en vervolgens op **OK** te klikken om verder te gaan.



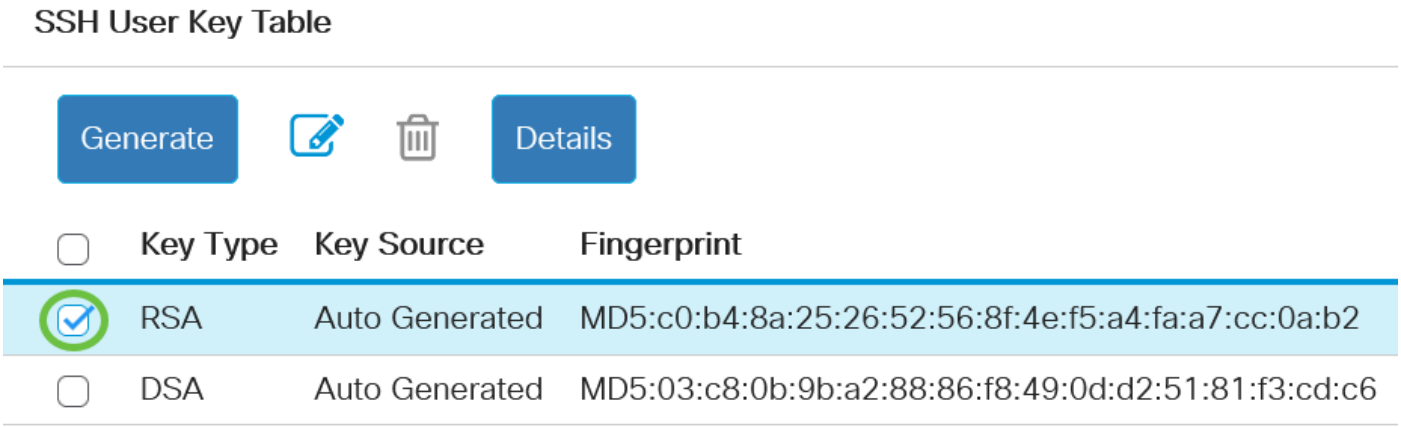
De standaardwaarden worden met de gebruikersnaam en het wachtwoord hersteld: anoniem/anoniem.

Stap 8. (Optioneel) Klik op **Weergave van gevoelige gegevens als spiltekst** om de gevoelige gegevens van de pagina in onbewerkte tekstindeling weer te geven en klik vervolgens op **OK** om verder te gaan.



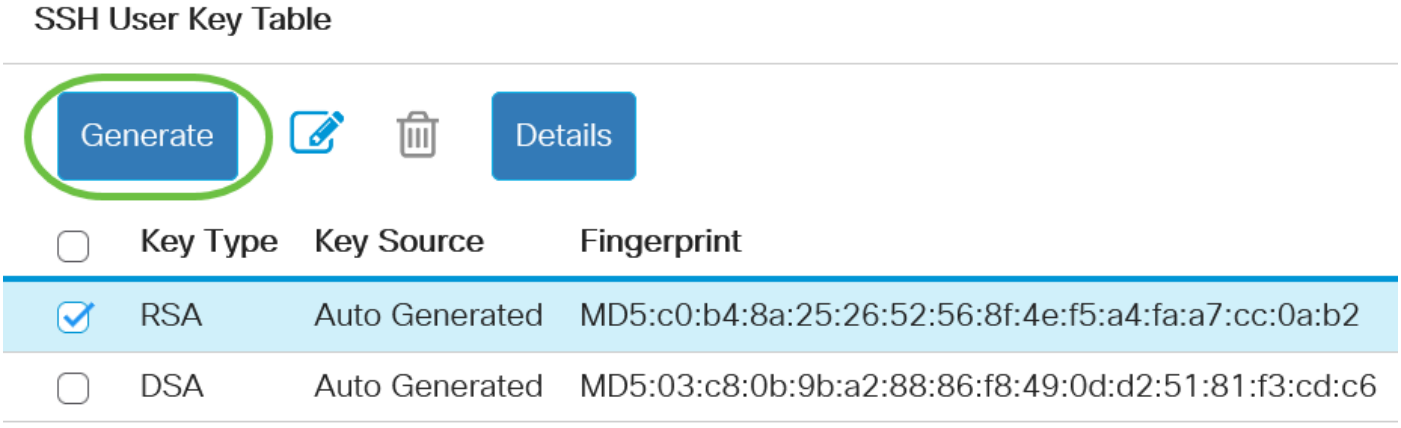
Tabel SSH-gebruiker instellen

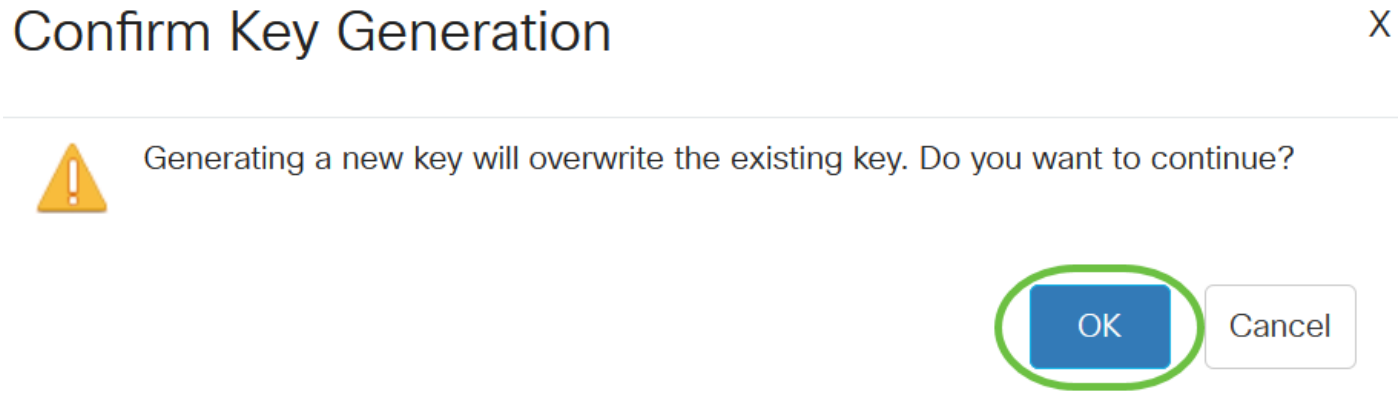
Stap 9. Controleer het aankruisvakje van de toets die u wilt beheren.



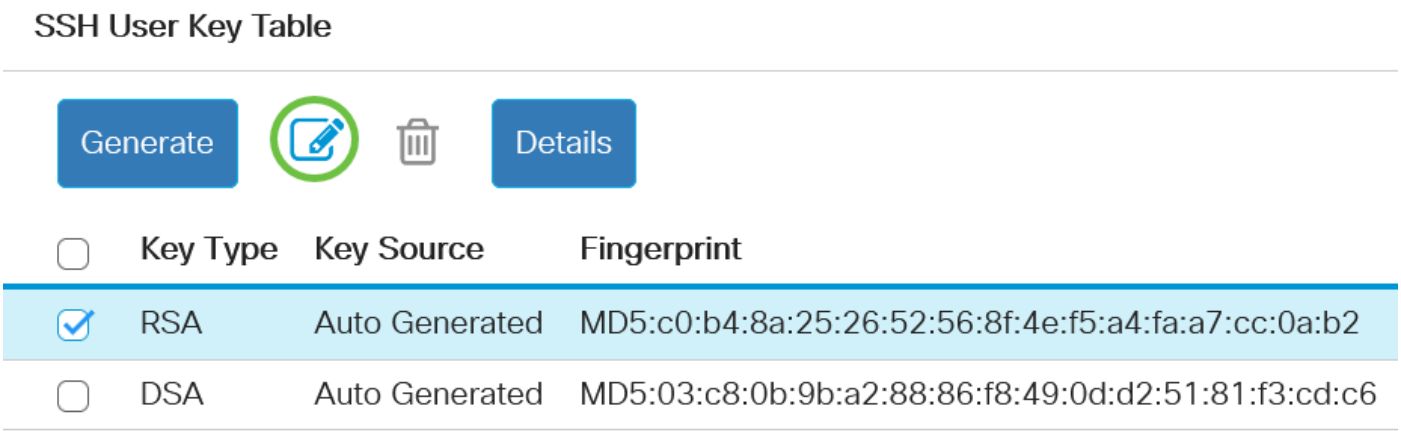
In dit voorbeeld wordt RSA gekozen.

Stap 10. (Optioneel) Klik op **Generate** om een nieuwe toets te genereren. De nieuwe toets negeert de afgevinkte toets en klikt vervolgens op **OK** om verder te gaan.

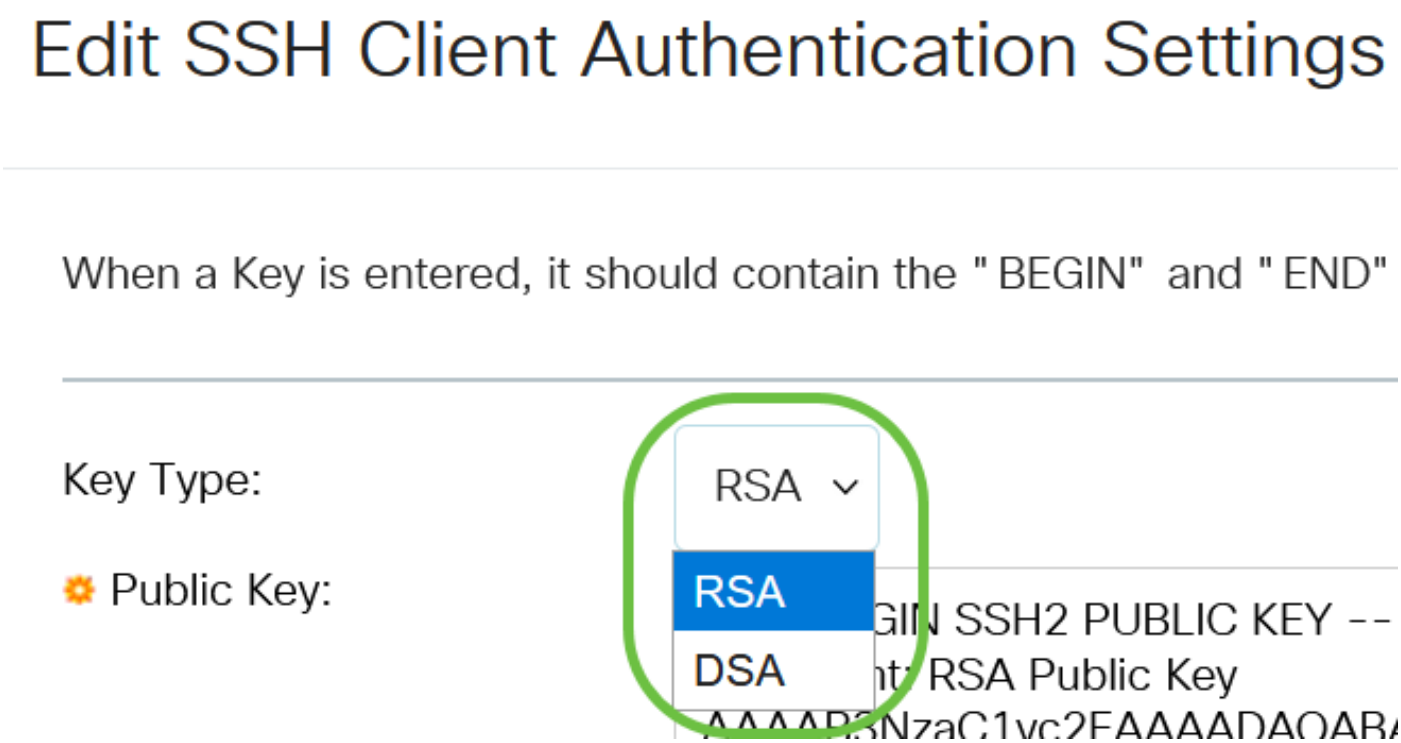




Stap 1. (Optioneel) Klik op **Bewerken** om een huidige toets te bewerken.

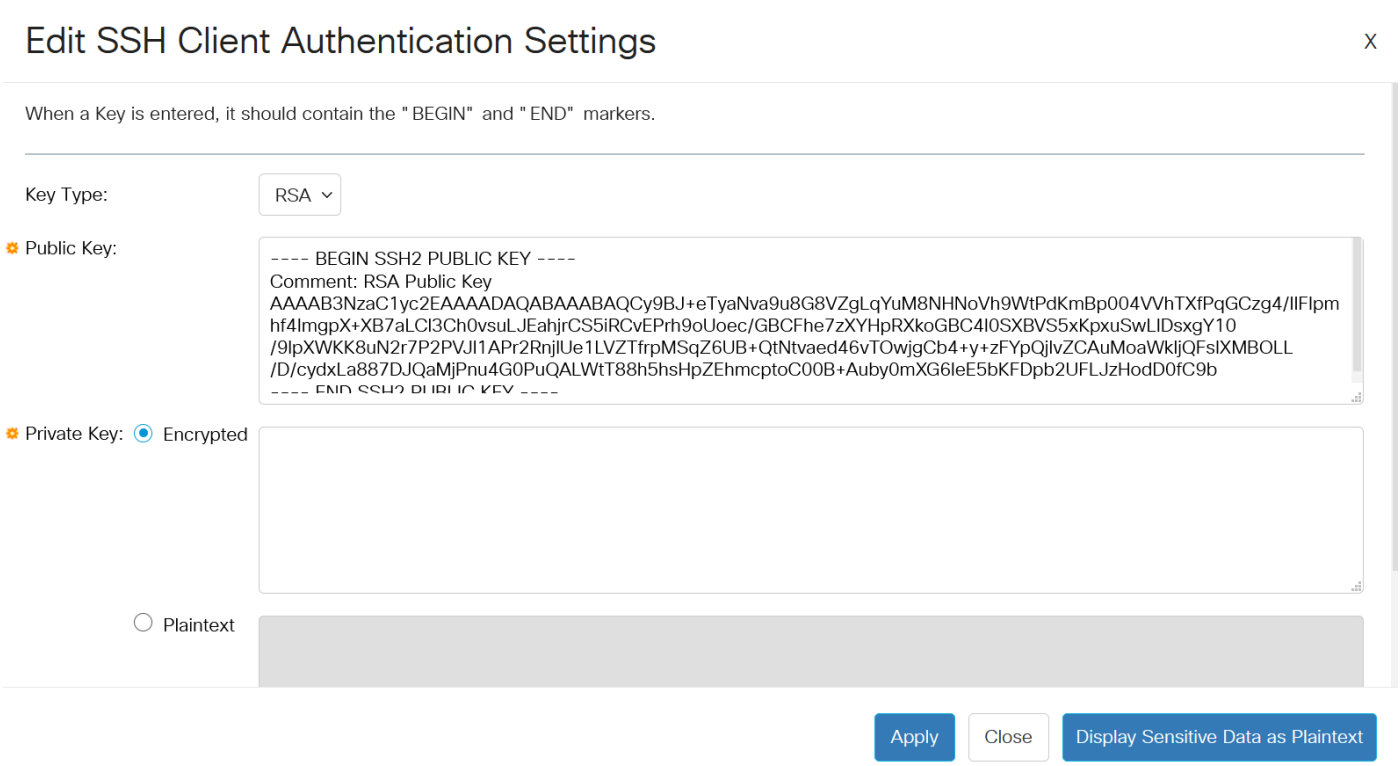


Stap 12. (Optioneel) Kies een sleuteltype uit de vervolgkeuzelijst Type toets.



In dit voorbeeld wordt RSA gekozen.

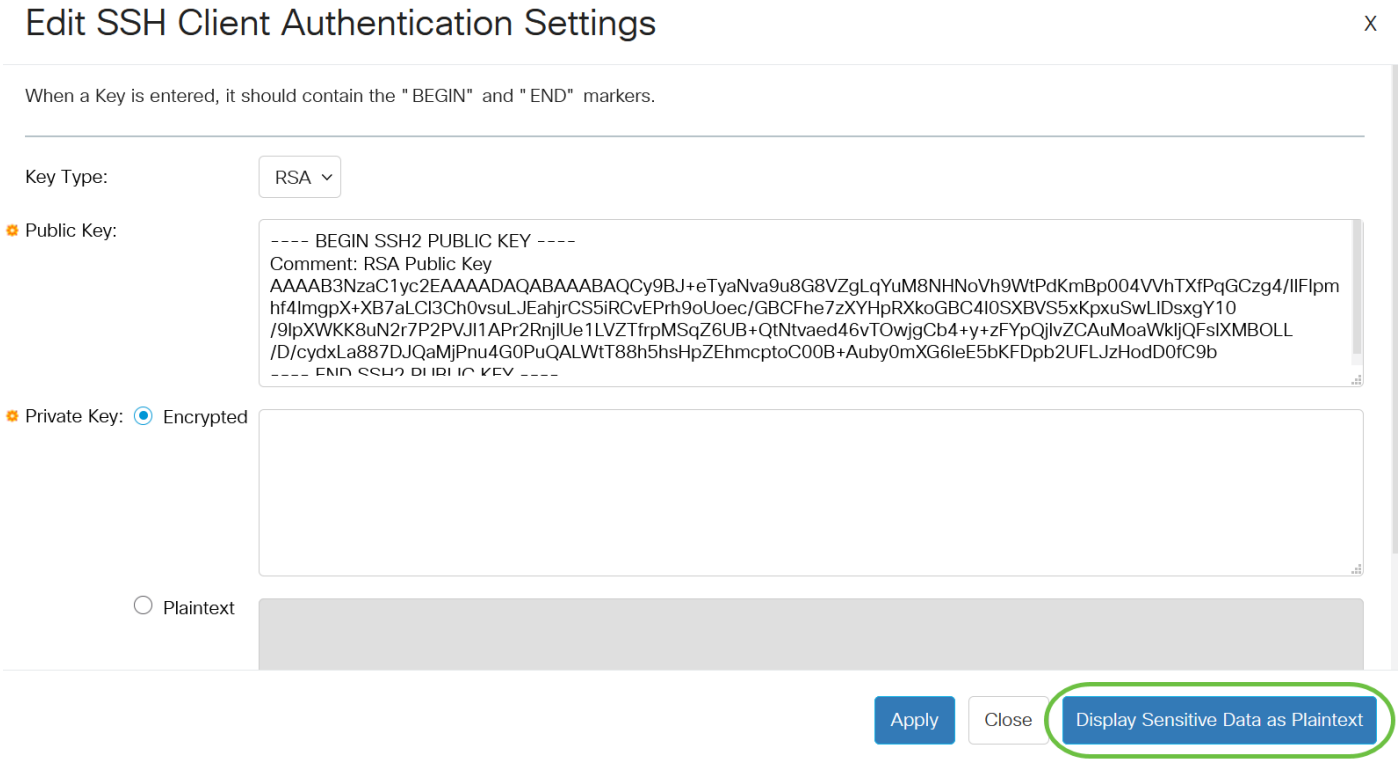
Stap 13. (Optioneel) Voer de nieuwe openbare sleutel in in het veld *Openbare sleutel*.

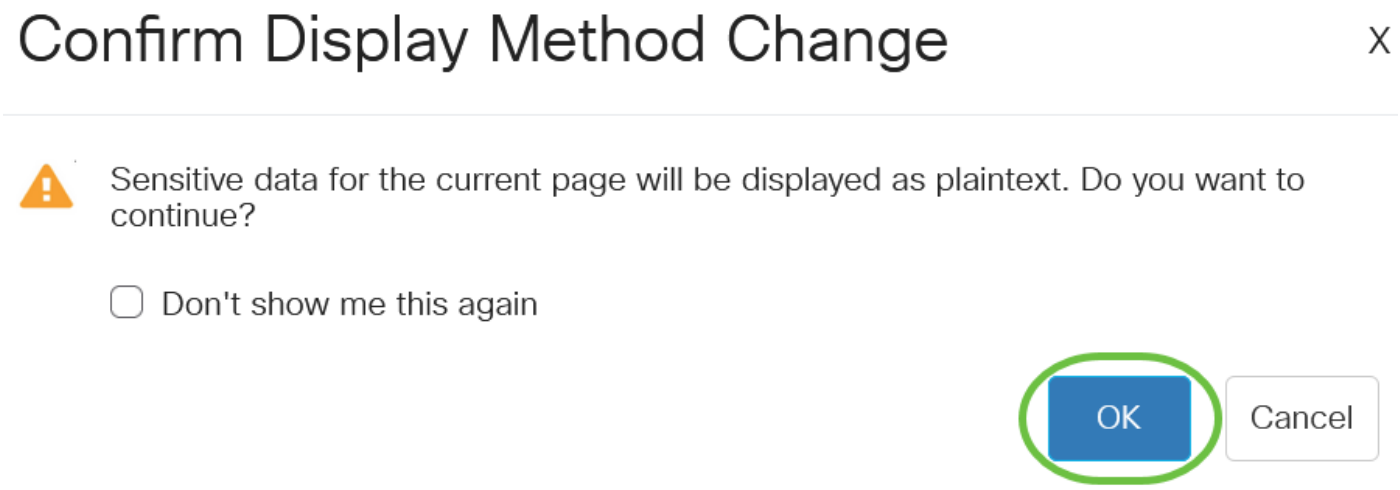


Stap 14. (Optioneel) Voer de nieuwe privé-toets in het veld *Private Key*.

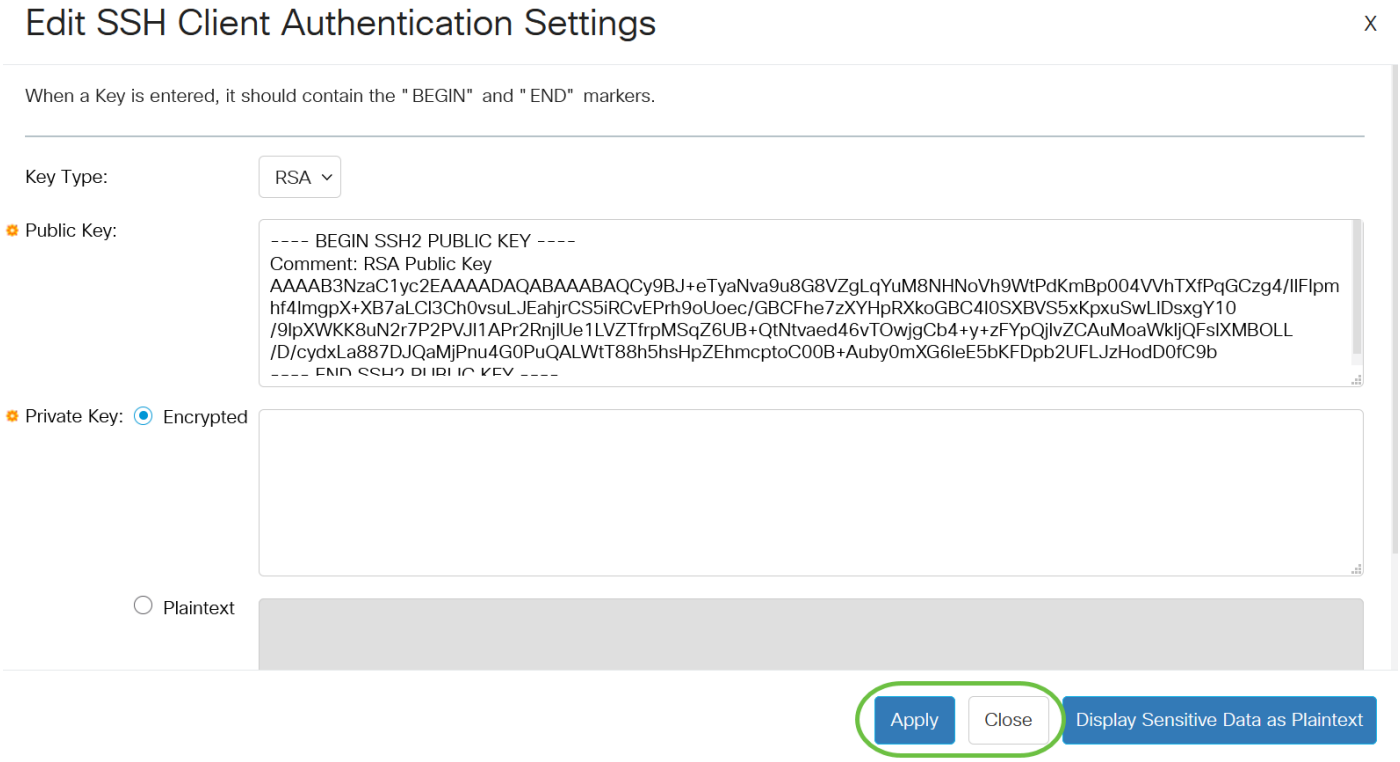
U kunt de privé-toets bewerken en u kunt op Versleuteld klikken om de huidige privé-toets als een gecodeerde tekst te zien, of Plaintext om de huidige privé-toets in onbewerkte tekst te zien.

Stap 15. (Optioneel) Klik op **Weergave van gevoelige gegevens als** spiltekst om de versleutelde gegevens van de pagina in onbewerkte tekstindeling weer te geven en klik vervolgens op **OK** om verder te gaan.

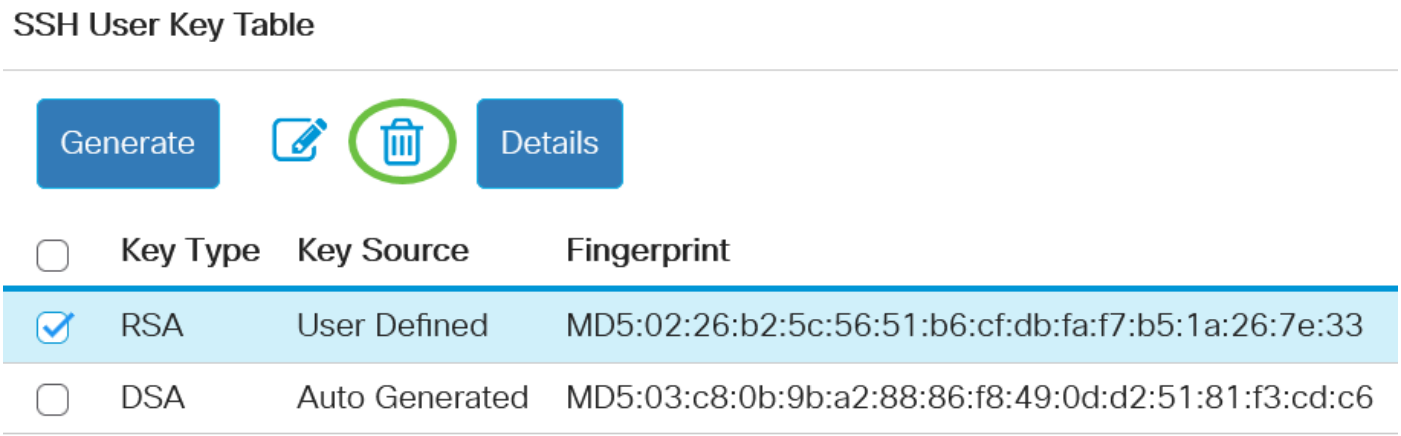




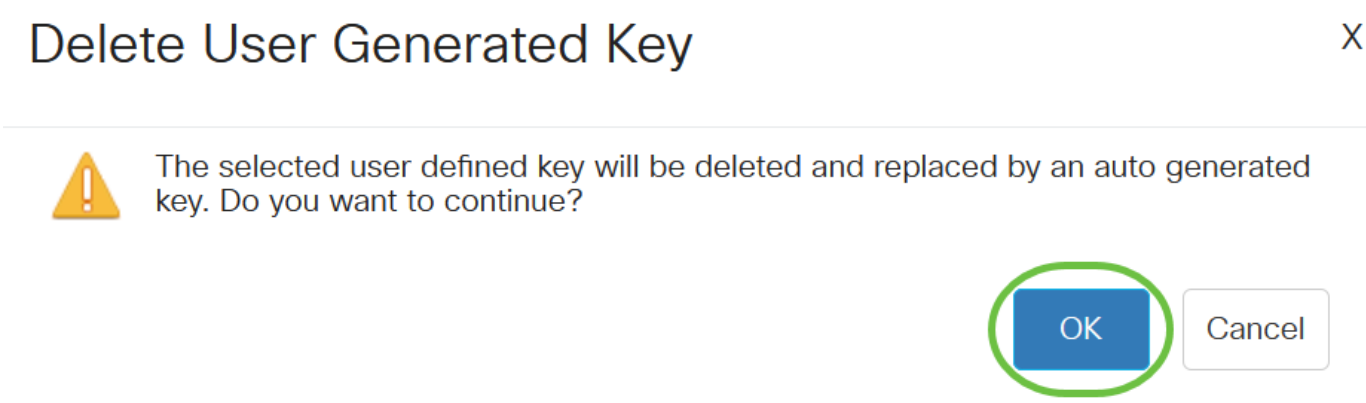
Stap 16. Klik op **Toepassen** om uw wijzigingen op te slaan en klik vervolgens op **Sluiten**.



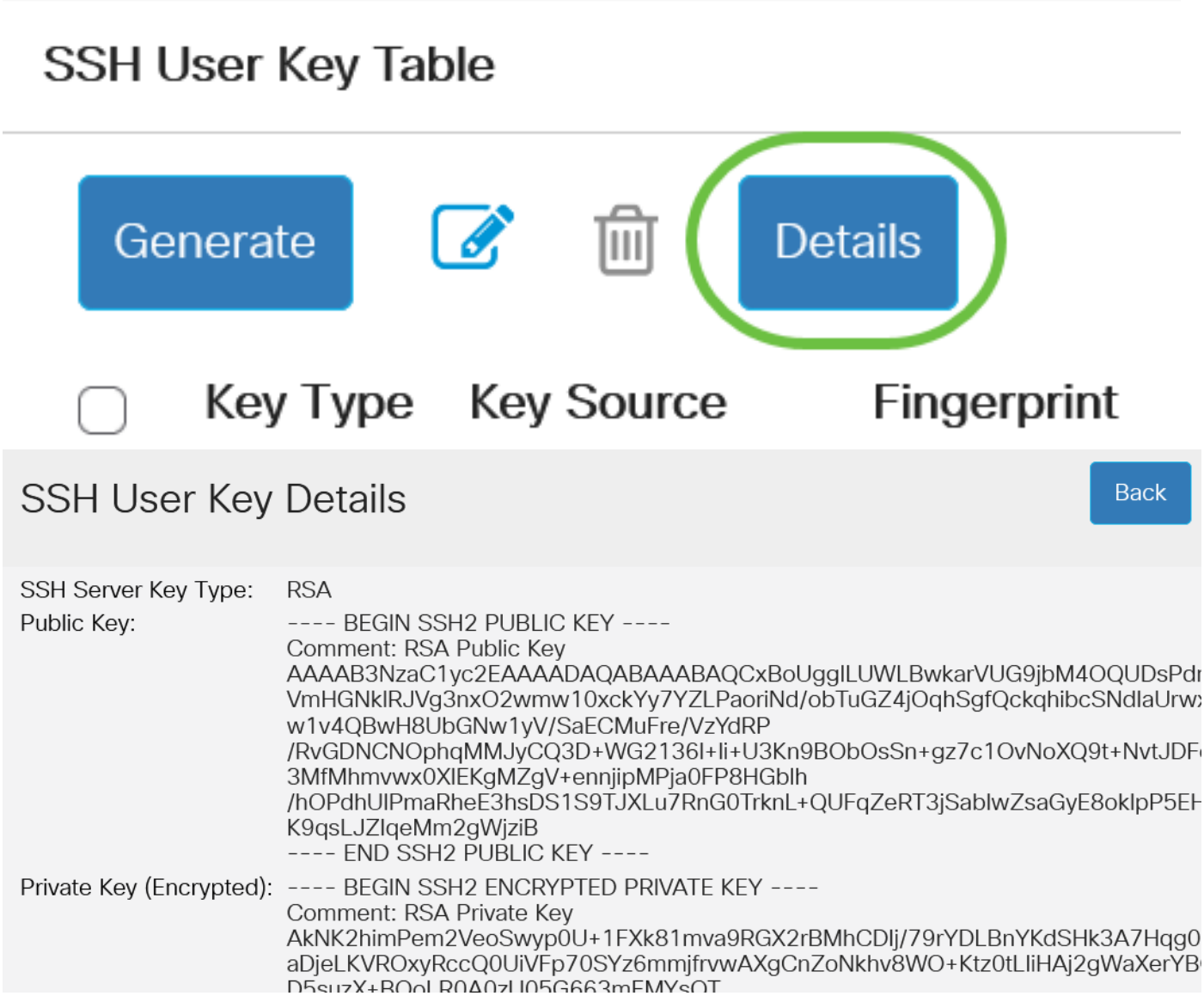
Stap 17. (Optioneel) Klik op **Verwijderen** om de gecontroleerde toets te verwijderen.



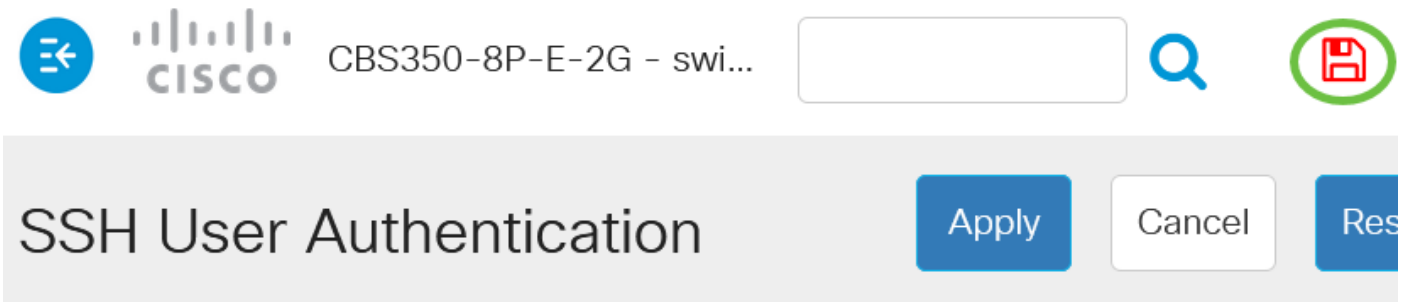
Stap 18. (Optioneel) Klik na een bevestigingsbericht zoals hieronder weergegeven op **OK** om de toets te verwijderen.



Stap 19. (Optioneel) Klik op **Details** om de details van de gecontroleerde toets te zien.



Stap 20. (Optioneel) Klik op de knop **Opslaan** boven op de pagina om de wijzigingen in het opstartconfiguratiebestand op te slaan.



U hebt nu de instellingen voor de gebruikersverificatie van de client ingesteld op uw Cisco Business 350 Series switch.