Instellingen voor SSH-gebruikersverificatie (Secure Shell) op een switch configureren

Doel

Secure Shell (SSH) is een protocol voor een beveiligde externe verbinding met specifieke netwerkapparaten. Deze verbinding biedt functionaliteit die vergelijkbaar is met een Telnet-verbinding, behalve dat deze is versleuteld. Met SSH kan de beheerder de switch configureren via de opdrachtregelinterface (CLI) met een programma van een derde partij.

In CLI-modus via SSH kan de beheerder meer geavanceerde configuraties uitvoeren in een beveiligde verbinding. SSH-verbindingen zijn nuttig bij het op afstand oplossen van problemen met een netwerk, in gevallen waarin de netwerkbeheerder niet fysiek aanwezig is op de netwerklocatie. De switch laat de beheerder gebruikers verifiëren en beheren om via SSH verbinding te maken met het netwerk. De verificatie vindt plaats via een openbare sleutel die de gebruiker kan gebruiken om een SSH-verbinding met een specifiek netwerk tot stand te brengen.

De SSH-clientfunctie is een toepassing die via het SSH-protocol wordt uitgevoerd voor apparaatverificatie en -codering. Het laat een apparaat toe om een veilige en gecodeerde verbinding aan een ander apparaat te maken dat de server van SSH in werking stelt. Met verificatie en codering maakt de SSH-client een beveiligde communicatie mogelijk via een onveilige Telnet-verbinding.

Dit artikel bevat instructies voor het configureren van gebruikersverificatie voor clients op een beheerde switch.

Toepasselijke apparaten

- SX200 Series
- Sx300 Series
- Sx350 Series
- SG350X Series
- Sx500 Series
- Sx550X Series

Softwareversie

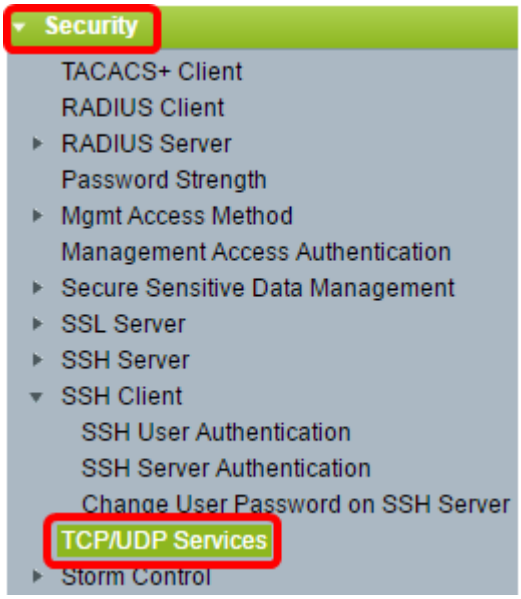
- 1.4.5.02 - SX200 Series, SX300 Series, SX500 Series
- 2.2.0.66 - SX350 Series, SG350X Series, SX550X Series

Instellingen voor SSH-clientgebruikersverificatie configureren

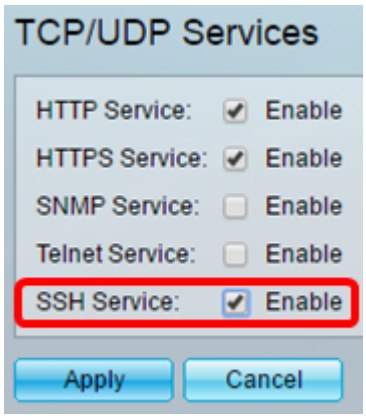
SSH-service inschakelen

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

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



Stap 2. Controleer het aanvinkvakje **SSH-service** om toegang van switches via SSH opdrachtprompt mogelijk te maken.



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

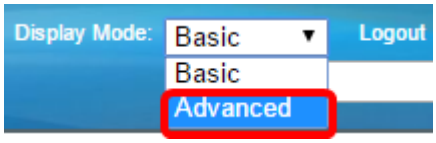
SSH-gebruikersverificatie-instellingen configureren

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 als de openbare of privé sleutel methode is geselecteerd.

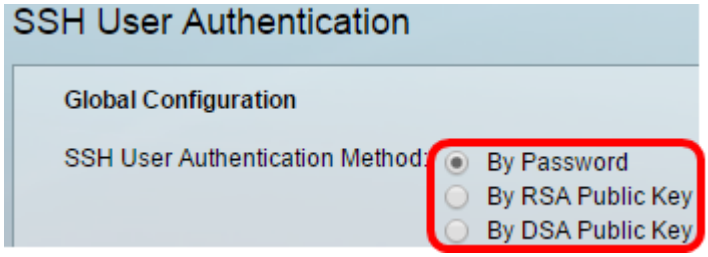
RSA- en DSA-standaardsleutelparen worden gegenereerd voor het apparaat wanneer dit wordt opgestart. Een van deze sleutels wordt gebruikt om de gegevens te versleutelen die worden gedownload van de SSH-server. De RSA-toets wordt standaard gebruikt. Als de gebruiker een of beide toetsen verwijdert, worden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

Stap 1. Meld u aan bij het webgebaseerde hulpprogramma en kies **Beveiliging > SSH-client > SSH-gebruikersverificatie**.

Opmerking: als u een SX350, SG300X of SX500X hebt, kiest u switch naar de geavanceerde modus door **Advanced** te kiezen uit de vervolgkeuzelijst Weergavemodus.



Stap 2. Klik onder Global Configuration op de gewenste SSH-gebruikersverificatiemethode.

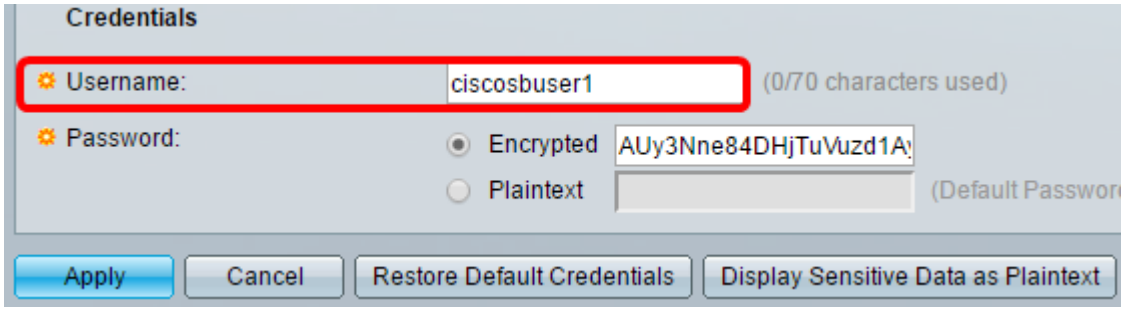


Opmerking: Wanneer een apparaat (SSH-client) probeert een SSH-sessie op te zetten naar de SSH-server, gebruikt de SSH-server een van de volgende methoden voor clientverificatie:

- Met Wachtwoord - Met deze optie kunt u een wachtwoord configureren voor gebruikersverificatie. Dit is de standaardinstelling en het standaardwachtwoord is anoniem. Als deze optie is gekozen, zorg er dan voor dat de gebruikersnaam en wachtwoordreferenties op de SSH-server zijn ingesteld.
- Door RSA Public Key — Met deze optie kunt u RSA Public Key gebruiken voor gebruikersverificatie. Een RSA-toets is een versleutelde sleutel op basis van factorisatie van grote gehele getallen. Deze sleutel is het meest gebruikelijke type sleutel dat wordt gebruikt voor SSH-gebruikersverificatie.
- Door DSA Public Key — Met deze optie kunt u een openbare DSA-sleutel voor gebruikersverificatie gebruiken. Een DSA-sleutel is een versleutelde sleutel op basis van een discrete algoritme van ElGamal. Deze toets wordt niet veel gebruikt voor SSH-gebruikersverificatie omdat dit meer tijd in het verificatieproces vergt.

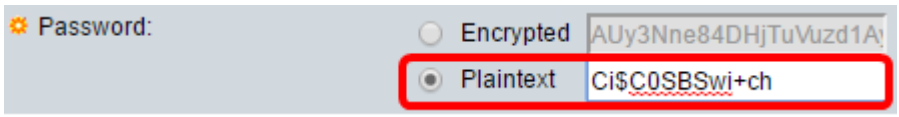
Opmerking: in dit voorbeeld is de optie Wachtwoord kiezen.

Stap 3. Voer in het gebied Credentials de gebruikersnaam in het veld *Gebruikersnaam in*.



Opmerking: in dit voorbeeld wordt ciscosbuser1 gebruikt.

Stap 4. (Optioneel) Als u in Stap 2 op Wachtwoord kiest, klikt u op de methode en vervolgens voert u het wachtwoord in het veld *Encrypted* of *Plaintext in*.



De opties zijn:

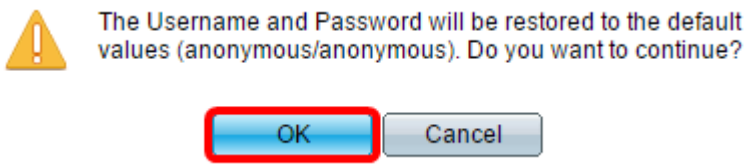
- Versleuteld — met deze optie kunt u een versleutelde versie van het wachtwoord invoeren.
- Platte tekst — met deze optie kunt u een wachtwoord voor onbewerkte tekst invoeren.

N.B.: In dit voorbeeld wordt Plaintext gekozen en wordt een wachtwoord voor onbewerkte tekst ingevoerd.

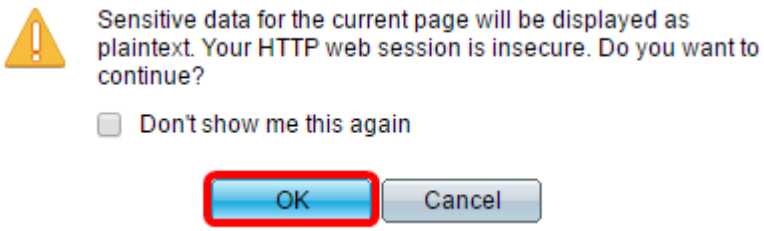
Stap 5. Klik op **Toepassen** om de verificatieconfiguratie op te slaan.

Stap 6. (Optioneel) Klik op **Standaardreferenties herstellen** om de standaardgebruikersnaam en het standaardwachtwoord te herstellen en klik vervolgens op **OK** om verder te gaan.

Opmerking: de standaardwaarden voor de gebruikersnaam en het wachtwoord worden hersteld: anoniem/anoniem.

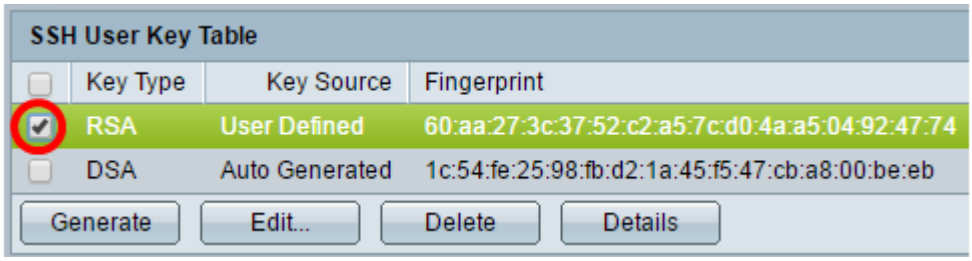


Stap 7. (Optioneel) Klik op **Gevoelige gegevens weergeven als onbewerkte tekst** om de gevoelige gegevens van de pagina in onbewerkte tekst weer te geven en klik vervolgens op **OK** om verder te gaan.



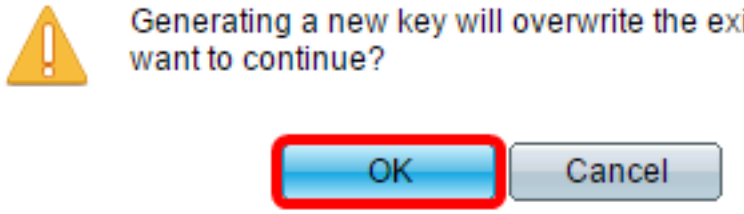
Toetstabel SSH-gebruiker configureren

Stap 8. Schakel het aankruisvakje in van de toets die u wilt beheren.

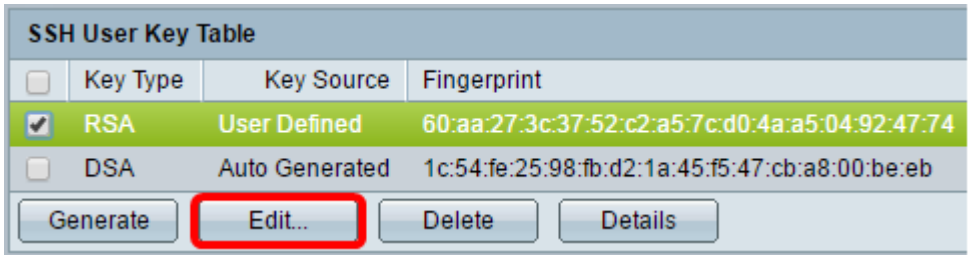


Opmerking: in dit voorbeeld is RSA gekozen.

Stap 9. (Optioneel) Klik op **Generate** om een nieuwe sleutel te genereren. De nieuwe sleutel overschrijft de aangevinkt toets en klikt vervolgens op **OK** om verder te gaan.



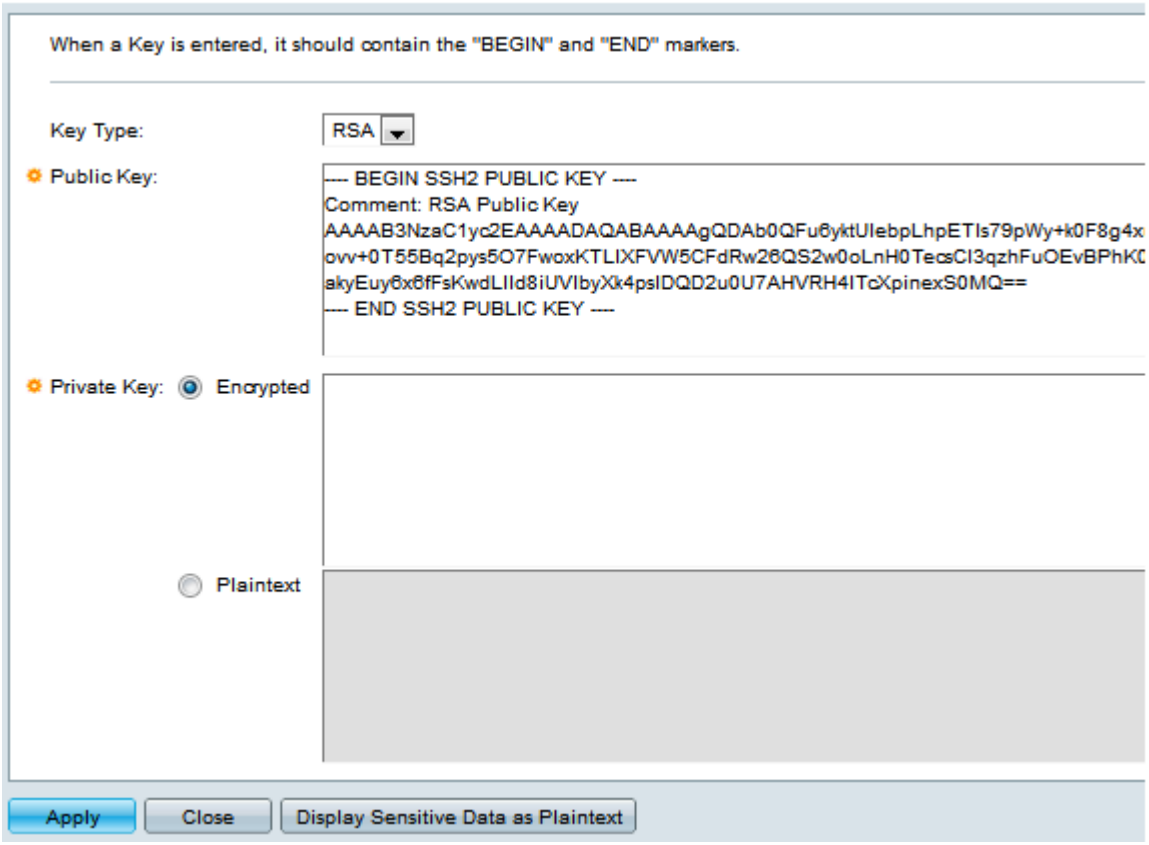
Stap 10. (Optioneel) Klik op **Bewerken** om een huidige toets te bewerken.



Stap 1. (Optioneel) Kies een type toets uit de vervolgkeuzelijst Type sleutel.

Opmerking: in dit voorbeeld is RSA gekozen.

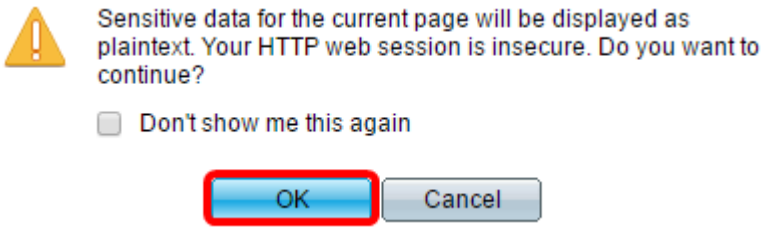
Stap 12. (Optioneel) Voer de nieuwe openbare sleutel in in het veld *Public Key*.



Stap 13. (Optioneel) Voer de nieuwe privé-sleutel in het veld *Private Key* in.

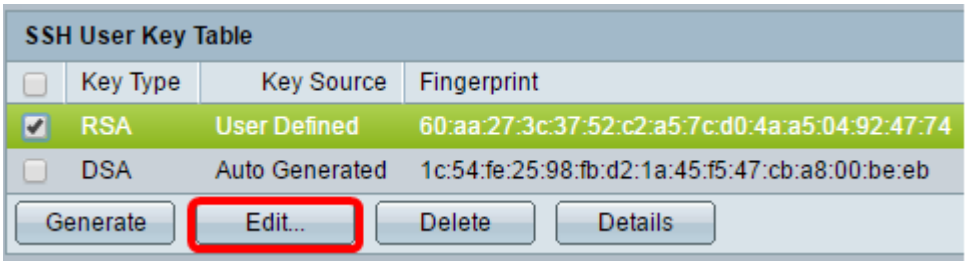
Opmerking: u kunt de privé-sleutel bewerken en u kunt op Versleuteld klikken om de huidige privé-sleutel als een versleutelde tekst te zien, of op Plaintext om de huidige privé-sleutel in onbewerkte tekst te zien.

Stap 14. (Optioneel) Klik op **Gevoelige gegevens weergeven als onbewerkte tekst** om de versleutelde gegevens van de pagina in onbewerkte tekst te tonen en klik vervolgens op **OK** om verder te gaan.

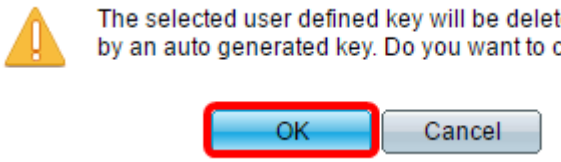


Stap 15. Klik op **Toepassen** om uw wijzigingen op te slaan en klik vervolgens op **Sluiten**.

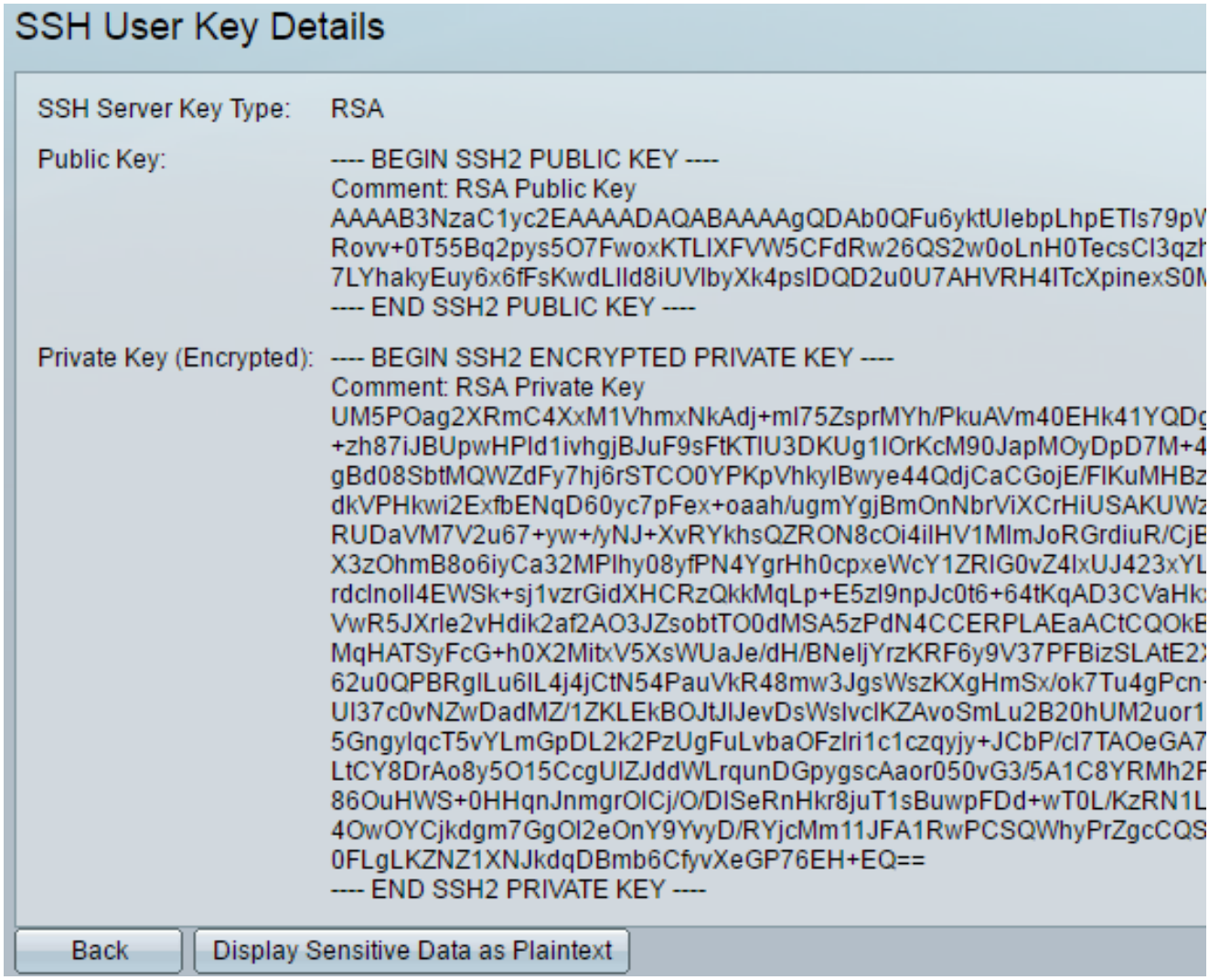
Stap 16. (Optioneel) Klik op **Verwijderen** om de geselecteerde toets te verwijderen.



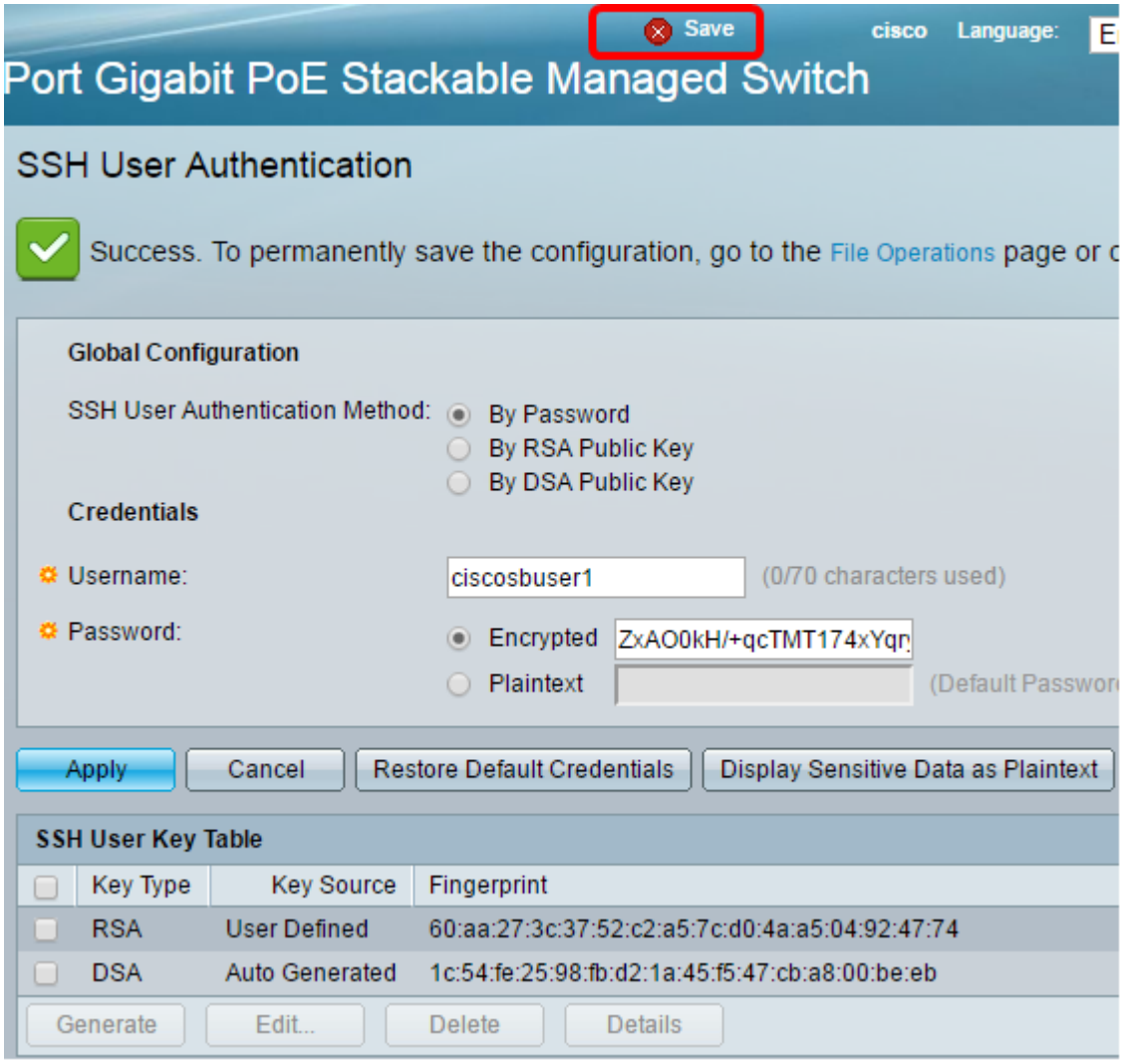
Stap 17. (Optioneel) Klik op **OK** om de toets te verwijderen nadat een bevestigingsbericht zoals hieronder wordt getoond.



Stap 18. (Optioneel) Klik op **Details** om de details van de geselecteerde toets te zien.



Stap 19. (Optioneel) Klik op de knop **Opslaan** bovenaan op de pagina om de wijzigingen in het opstartconfiguratiebestand op te slaan.



U moet nu de verificatie-instellingen voor de clientgebruiker op uw beheerde switch hebben geconfigureerd.

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.