Client Secure Shell (SSH)-gebruikersverificatie voor SG350XG en SG550XG-switches

Doel

Secure Shell (SSH) is een protocol voor een beveiligde afstandsverbinding met een specifiek apparaat. Met de 350XG en 550XG Series Managed-switches kunt u gebruikers authentiseren en beheren om verbinding te maken met het apparaat via SSH. De authenticatie vindt plaats via een openbare toets, zodat de gebruiker deze toets kan gebruiken om een SSH-verbinding met een specifiek apparaat te maken. SSH-verbindingen zijn handig om een netwerk extern op te lossen, in het geval dat de netwerkbeheerder niet op de netwerksite is.

Dit artikel legt uit hoe de gebruikersverificatie op de SG350XG en SG550XG Series Managed-switches te configureren.

Toepasselijke apparaten

- SG350XG router
- SG550XG router

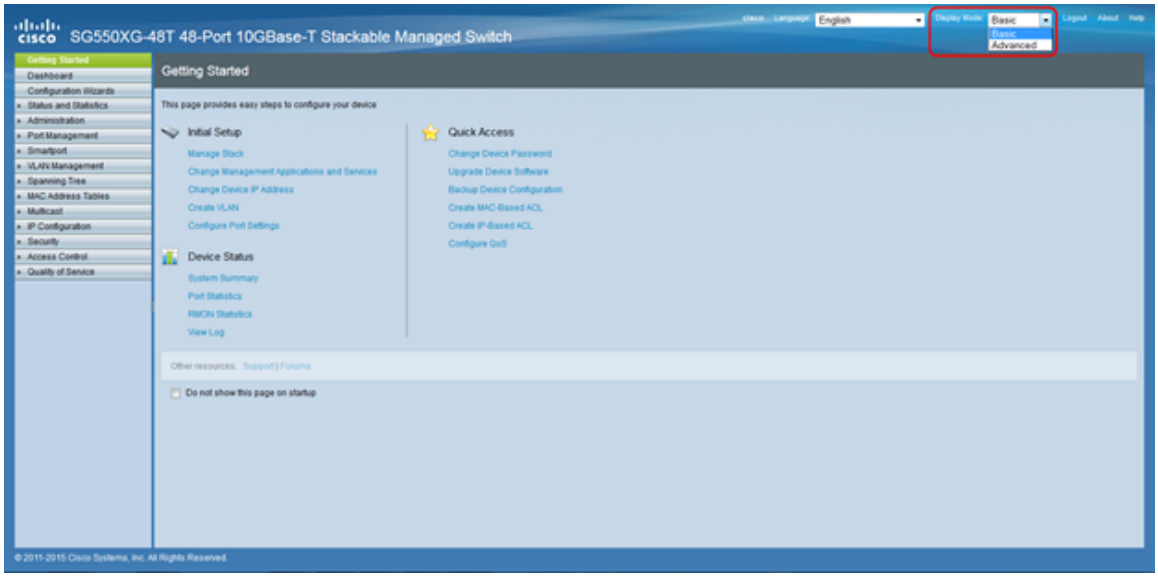
Softwareversie

- v2.0.0.73

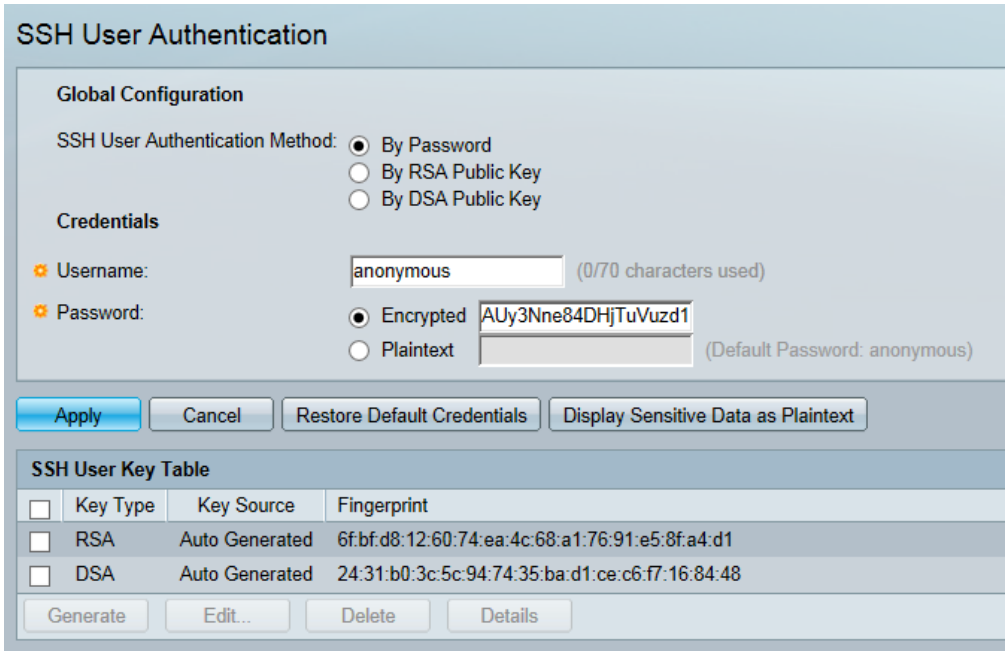
SSH configureren Clientclient Verificatie

Wereldwijde configuratie

Opmerking: De volgende screenshots worden weergegeven in het geavanceerde display. Dit kan worden gedraaid door op de vervolgkeuzelijst Weergavemodus te klikken rechtsboven op het scherm



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



Stap 2 . In het veld *SSH-gebruikersverificatiemethode* klikt u op de radioknop voor de gewenste wereldwijde verificatiemethode.

De beschikbare opties zijn:

- Door wachtwoord - Met deze optie kunt u een wachtwoord voor de verificatie van gebruikers configureren. Voer een wachtwoord in of bewaar de standaard "anoniem".
- Door RSA Public Key - Met deze optie kunt u een RSA-openbare sleutel voor gebruikersverificatie gebruiken. RSA wordt gebruikt voor encryptie en het ondertekenen. Als dit geselecteerd is, kunt u een openbare en particuliere RSA-toets in het SSH-sleuteltabelblok maken.
- Door openbare sleutel van DSA - Deze optie laat u een openbare sleutel van DSA voor gebruikersauthenticatie gebruiken. DSA wordt gebruikt voor het ondertekenen. Als dit geselecteerd is, kunt u een openbare/particuliere DSA-toets in het SSH User Key Table blok maken.

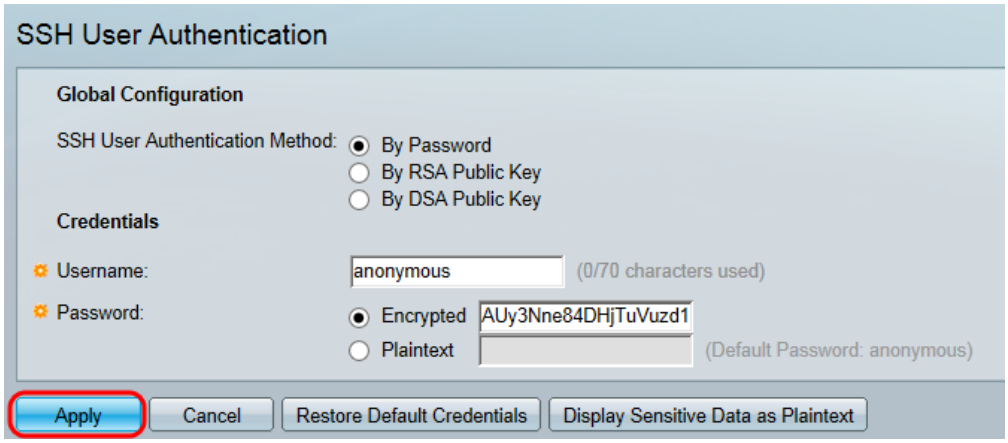
Stap 3. Zoek het gebied *Credentials*. Voer in het veld *Gebruikersnaam* de gebruikersnaam in.

Stap 4. Als **Wachtwoord** in Stap 2 is geselecteerd, klikt u op radioknop voor de gewenste wachtwoordmethode in het veld *Wachtwoord*. Het defaultwachtwoord is "anoniem".

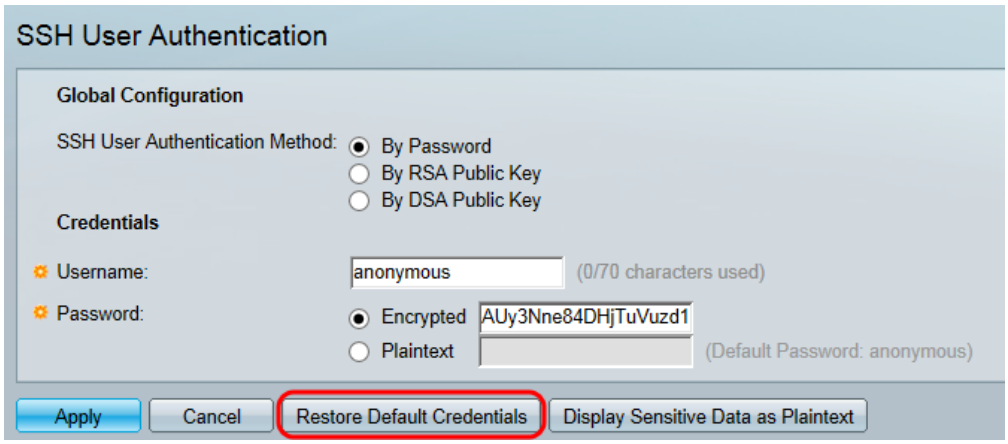
De beschikbare opties worden als volgt beschreven:

- Versleuteld - Voer een versleuteld wachtwoord in.
- Plaintext - Voer een wachtwoord in als onbewerkte tekst.

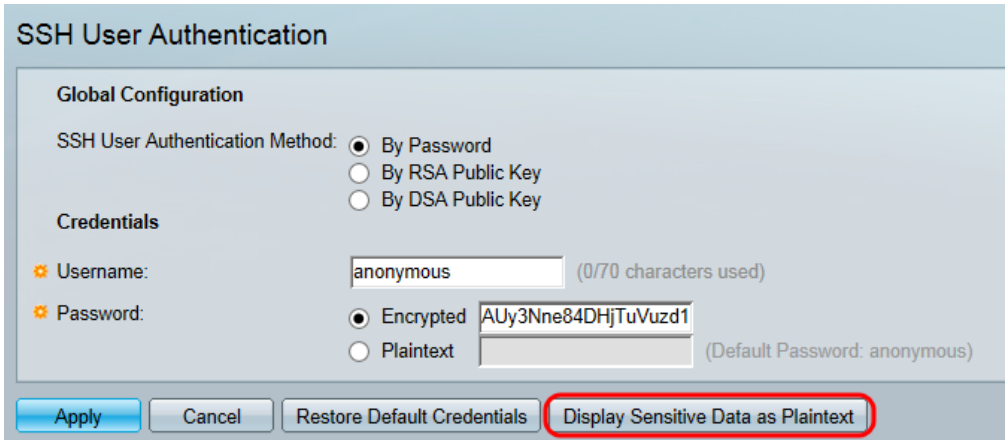
Stap 5. Klik op **Toepassen** om de authenticatieconfiguratie op te slaan.



Stap 6. (Optioneel) Klik om de standaardgebruikersnaam en -wachtwoord te herstellen op **Standaardwaarden herstellen**. Standaard is het wachtwoord "anoniem".



Stap 7. (optioneel) Klik om de gevoelige gegevens als tekst of als gecodeerde tekst te bekijken, op **Weergave van gevoelige gegevens als tekst/versleuteld.**

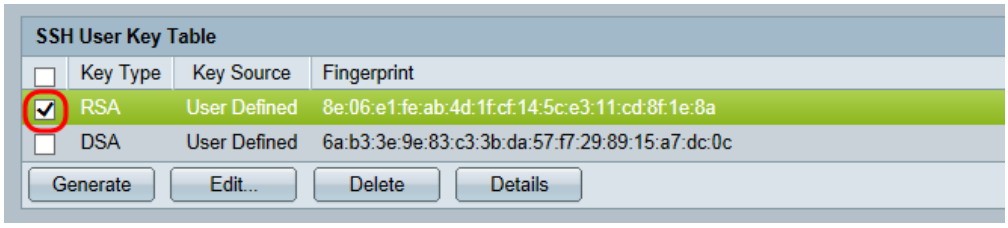


Opmerking: De naam van de knop verandert afhankelijk van de huidige instelling. De knop schakelt altijd de weergave van de gegevens in.

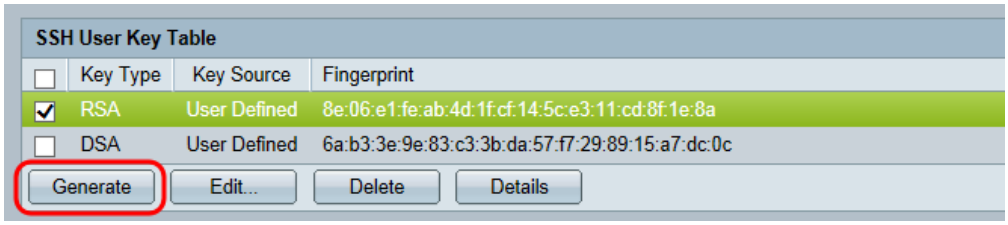
SSH-gebruikerstaal

In deze sectie wordt uitgelegd hoe u de SSH-gebruikerstaal wilt beheren.

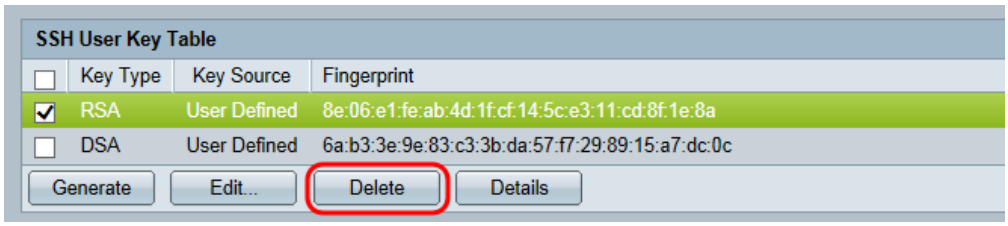
Stap 1. Navigeer naar de *SSH-gebruikerstaal*. Selecteer in de opgeroepen lijst het/de selectieteken die u wilt beheren.



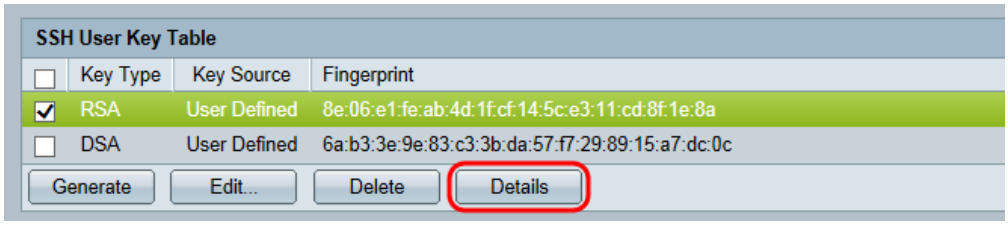
Stap 2. (Optioneel) Klik op **Generate** om een nieuwe toets te genereren. De nieuwe toets heeft voorrang op de geselecteerde toets. Er verschijnt een bevestigingsvenster. Klik op **OK** om verder te gaan.



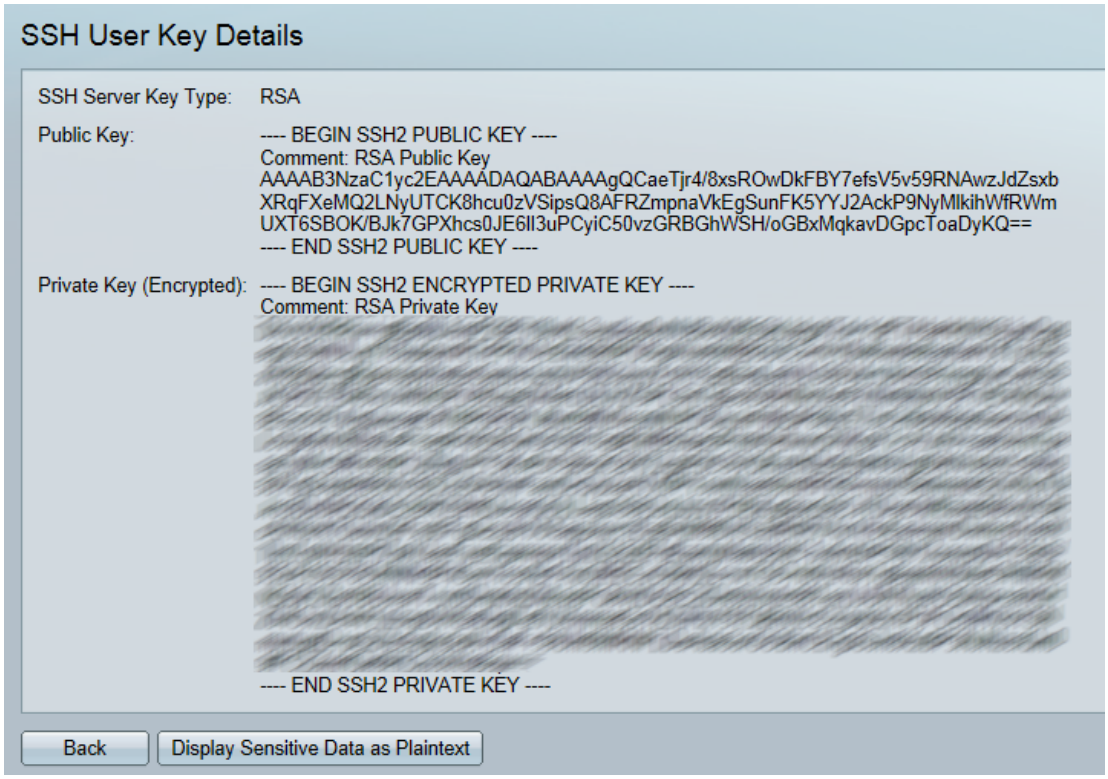
Stap 3. (Optioneel) Klik op **Verwijderen** om de geselecteerde toets te verwijderen. Er verschijnt een bevestigingsvenster. Klik op **OK** om verder te gaan.



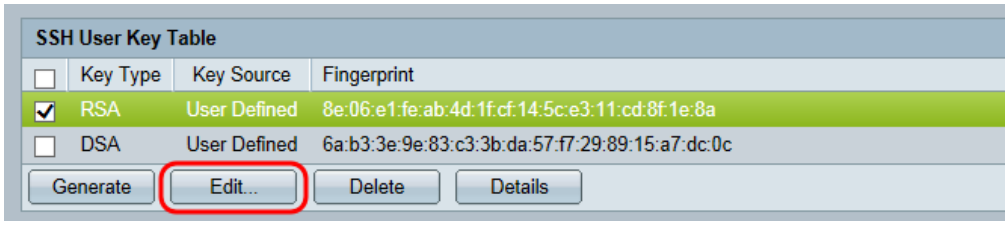
Stap 4. (Optioneel) Klik op **Details** om de details van de geselecteerde toets te bekijken.



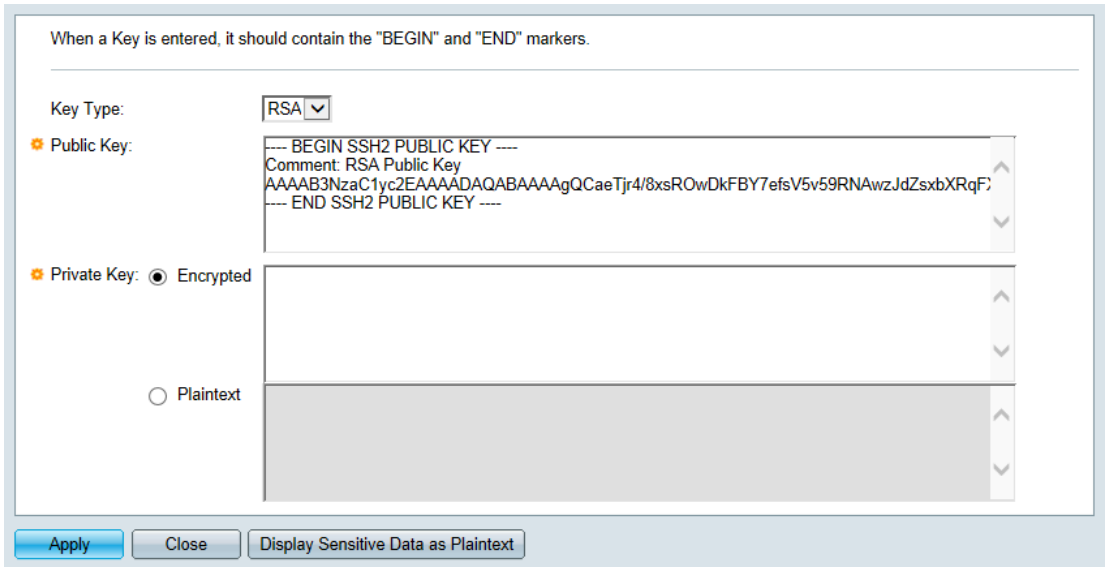
De pagina met SSH-gebruikershandleiding wordt weergegeven. Klik op **Terug** om terug te keren naar de SSH-gebruikerstaal.



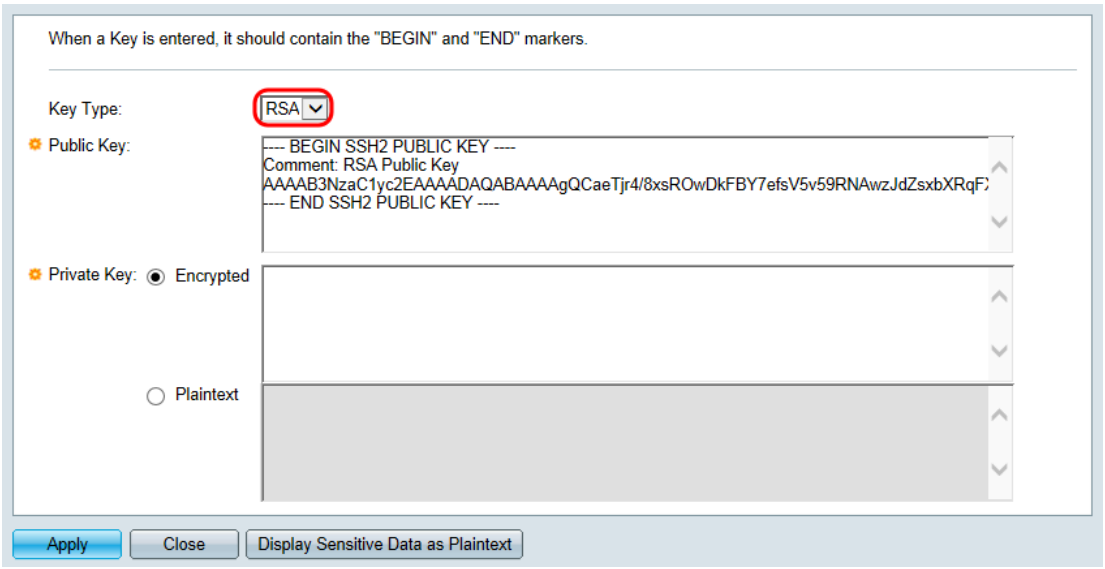
Stap 5. Klik op **Bewerken** om de gekozen toets te bewerken.



Het venster *Instellingen voor SSH-clientverificatie bewerken* wordt geopend:



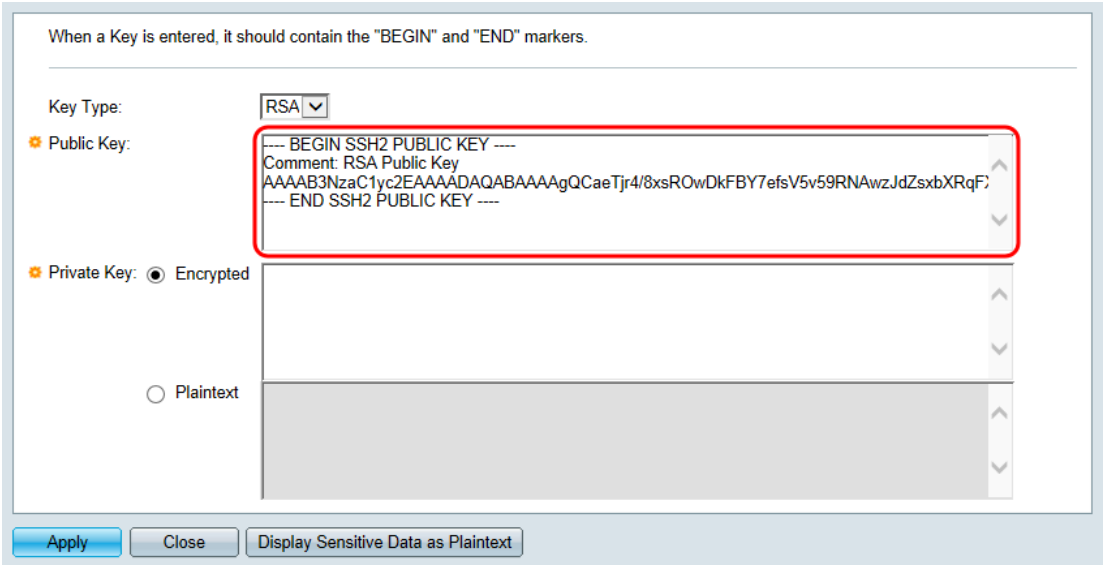
Stap 6. Selecteer het gewenste sleuteltype in de vervolgkeuzelijst *toetstype*.



De beschikbare opties zijn:

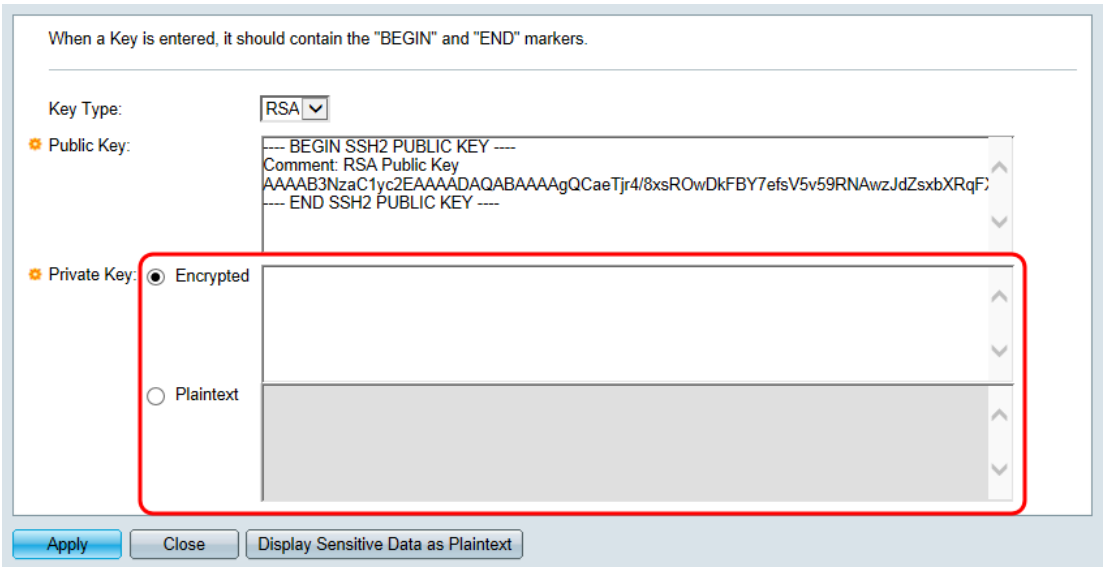
- RSA - RSA wordt gebruikt voor encryptie en het ondertekenen.
- DSA - DSA wordt uitsluitend gebruikt voor het ondertekenen.

Stap 7. In het veld *Openbare sleutel* kunt u de huidige openbare toets bewerken.



Stap 8. In het veld *Private Key*, kunt u de huidige privé-toets bewerken. Klik op het

Versleuteld radioknop om de huidige privé-sleutel te zien zoals versleuteld. Anders klikt u op het keuzerondje **Plaintext** om de huidige privé-toets als onbewerkte tekst te zien.



Stap 9. Klik op **Toepassen** om uw wijzigingen op te slaan.