Secure Shell (SSH)-clientverificatie op SX500 Series Stackable-switches

Doel

Met de SSH-serverfunctie (Secure Shell) kunt u een SSH-sessie instellen met de SX500 Series Stackable-switches. Een SSH-sessie is net zoiets als een telnet-sessie, maar 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 geopend worden door het gebruik van de PuTTY-toepassing.

Dit artikel bevat informatie over de wijze waarop de authenticatiemethode voor een SSH-client kan worden geselecteerd. Het legt ook uit hoe u een gebruikersnaam en wachtwoord voor de SSH-client kunt instellen op SX500 Series Stackable Switches.

Toepasselijke apparaten

- SX500 Series Stackable-switches

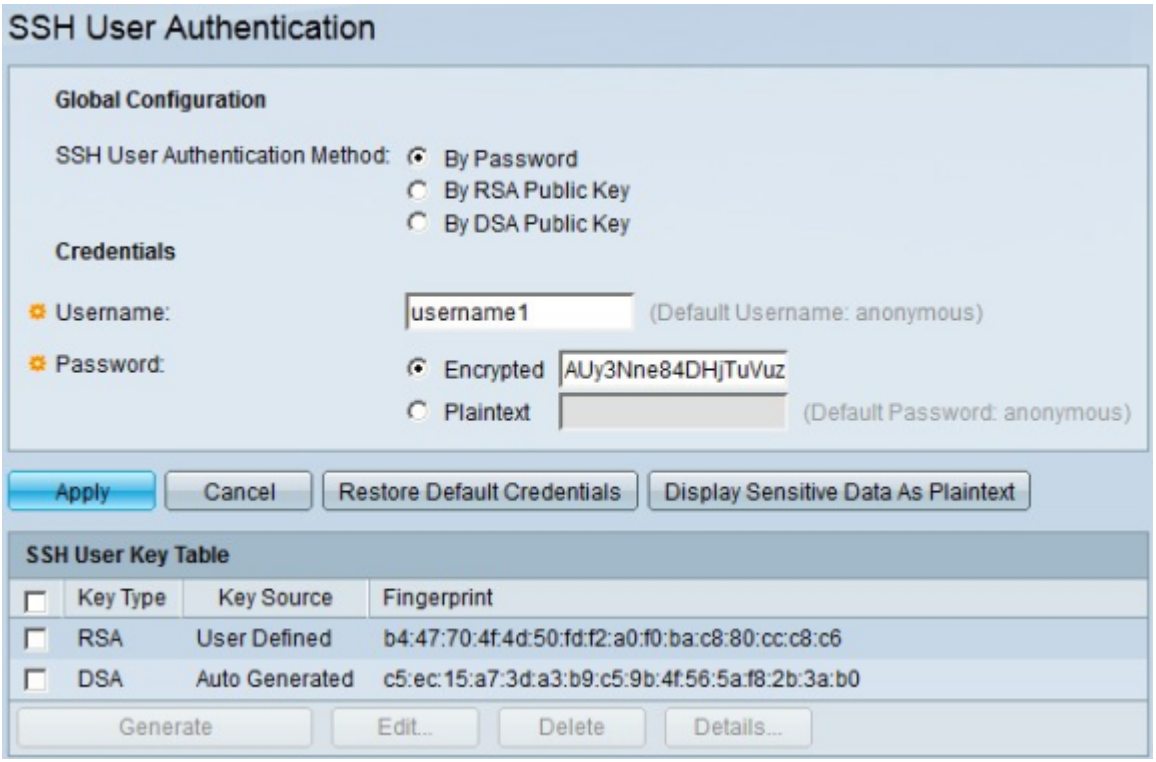
Softwareversie

•1.3.0.62

Configuratie van SSH-gebruikersverificatie

In dit gedeelte wordt uitgelegd hoe u gebruikersverificatie op de SX500 Series Stackable Switches kunt configureren.

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



Stap 2. Klik in het gebied Global Configuration op de radioknop voor de gewenste SSH-gebruikersverificatiemethode. De beschikbare opties zijn:

- Door Wachtwoord — Met deze optie kunt u een wachtwoord voor gebruikersverificatie configureren
- Door RSA Public Key — Met deze optie kunt u een RSA openbare sleutel voor gebruikersverificatie gebruiken. RSA wordt gebruikt voor encryptie en het ondertekenen.
- Door DSA Public Key — Met deze optie kunt u een DSA openbare sleutel voor gebruikersverificatie gebruiken. DSA is alleen voor ondertekening.

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

Stap 4. Als u in Stap 2 voor Wachtwoord hebt gekozen, klikt u in het veld Wachtwoord op de methode om het wachtwoord in te voeren. De beschikbare opties zijn:

- Versleuteld — Met deze optie kunt u een versleuteld wachtwoord invoeren.
- Plaintext — Met deze optie kunt u een duidelijk tekstwachtwoord invoeren. Plain tekst is ingevoerd, zodat u zich aan het apparaat kunt aanmelden en het wachtwoord kunt bekijken indien u het vergeet.

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

Stap 6. (Optioneel) Klik om de standaardgebruikersnaam en -wachtwoord te herstellen op **Standaardwaarden herstellen.**

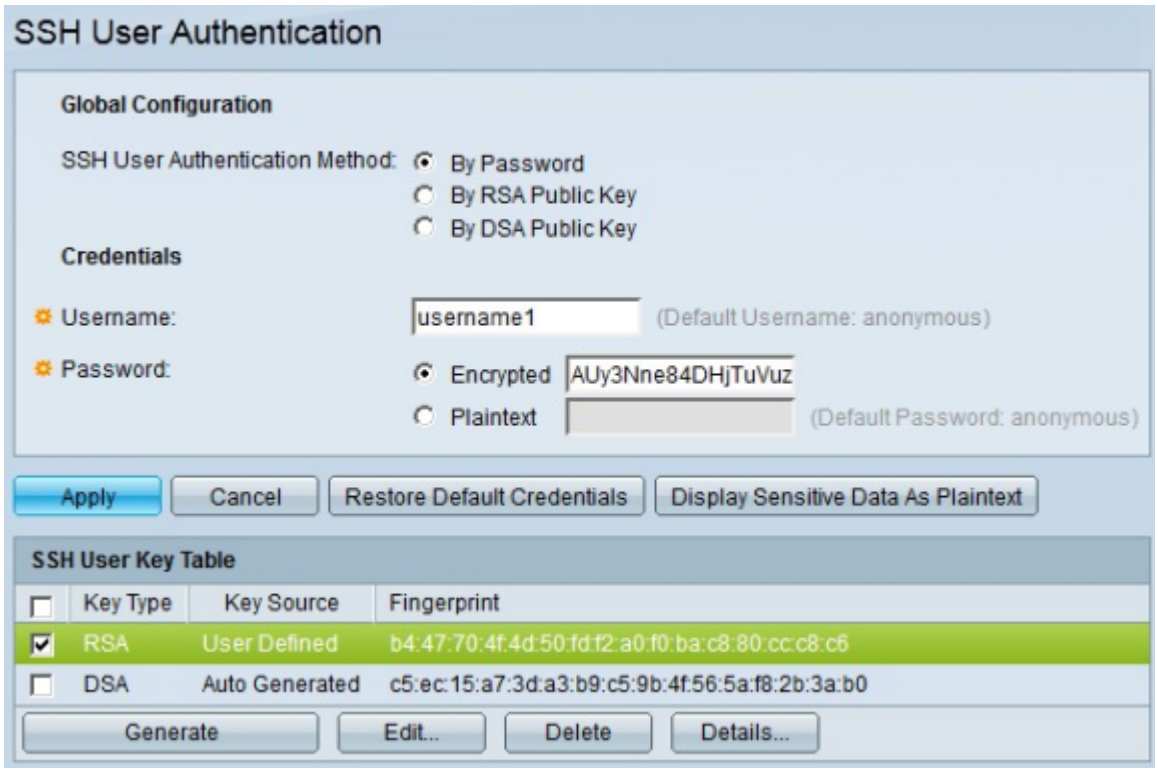
Stap 7. (Optioneel) Als u de gevoelige gegevens van de pagina in onbewerkte tekstindeling wilt weergeven, klikt u op **Gevoelige gegevens als spriettekst**.

SSH-gebruikerstaal

Deze sectie legt uit hoe u de SSH-gebruikerstaal kunt beheren op de SX500 Series

Stackable-switches.

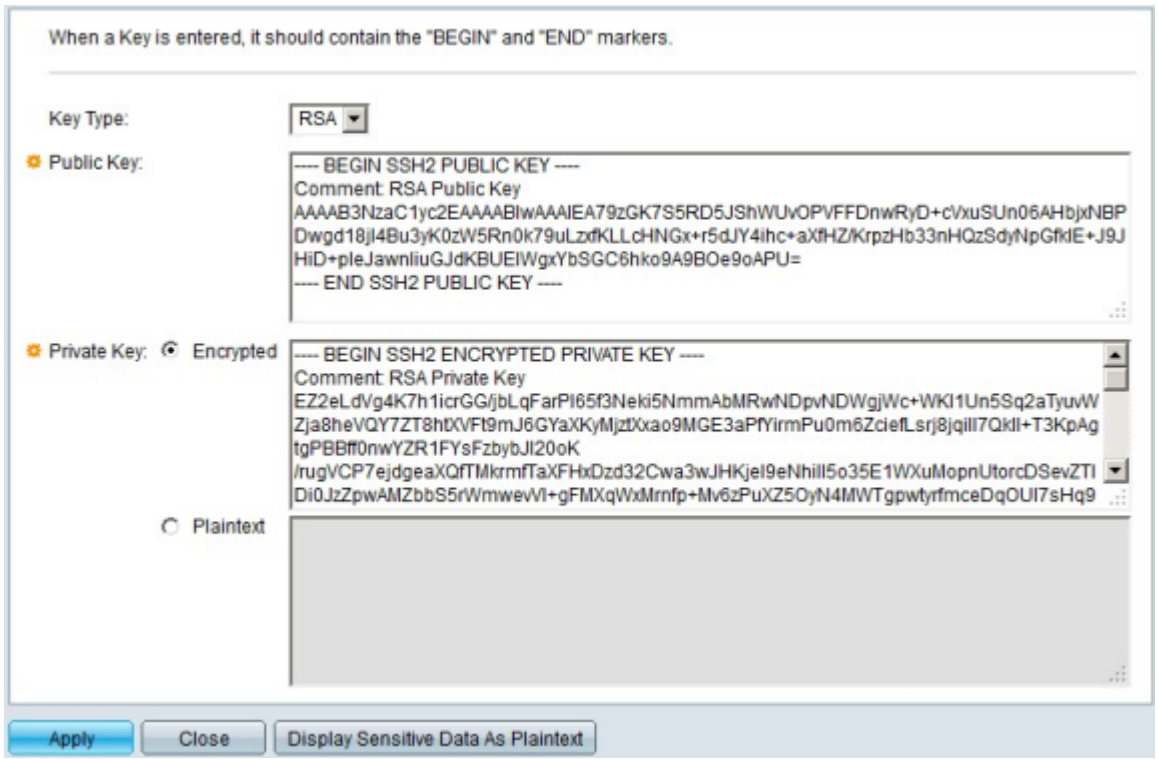
Stap 1. Meld u aan bij het web configuratieprogramma en kies **Security > SSH-client > SSH-gebruikersverificatie**. De pagina *SSH-gebruikersverificatie* wordt geopend:



Stap 2. Controleer het aanvinkvakje van de toets die u wilt beheren.

Stap 3. (Optioneel) Om een nieuwe toets te genereren, klikt u op **Generate**. De nieuwe toets heeft voorrang op de gecontroleerde toets.

Stap 4. (Optioneel) Klik op **Bewerken** om de huidige toets te bewerken. Het venster *Instellingen voor SSH-clientverificatie bewerken* verschijnt.



De opties die u kunt bewerken zijn:

- Type toets — Met deze optie kunt u uit de vervolgkeuzelijst Type toets het hoofdtype van uw voorkeur kiezen. U kunt RSA of DSA als belangrijkste type kiezen. RSA wordt gebruikt voor encryptie en het ondertekenen, terwijl DSA voor slechts het tekenen is.

- Openbare sleutel — In dit veld kunt u de huidige openbare sleutel bewerken.

- Private sleutel - In dit veld kunt u de privé-toets bewerken en u kunt op **Encrypt** klikken om de huidige privé-toets als een versleutelde tekst te zien, of **Plaintext** om de huidige privé-toets in onbewerkte tekst te zien.

Stap 5. Klik op **Toepassen** om uw wijzigingen op te slaan.

Stap 6. (Optioneel) Klik op **Verwijderen** om de gecontroleerde toets te verwijderen.

Stap 7. (optioneel) Klik op **Details** om de gegevens van de gecontroleerde toets te bekijken. Hieronder staat een afbeelding van de gegevens uit de gebruikerstalen.

SSH User Key Details

SSH Server Key Type:	RSA
Public Key:	---- BEGIN SSH2 PUBLIC KEY ---- Comment: RSA Public Key AAAAB3NzaC1yc2EAAAABIwAAAIEAzzGyPuoBcoaNa32Pk2ELNNt7UaGR5xFEPoH7 JdGj3Lto7UfkRAM9XIvai9Xua/B4pU1fCL /I2ZFjGVgTs7UUsNOjjuOtRSopHR8udhUGqgdzA4hHQycvCGy8OIuRYNIU0q6UHWW7 6NX+jnD4WphJxeYCKx2AIWzmsu14p6GQ2Ec= ---- END SSH2 PUBLIC KEY ----
Private Key (Encrypted):	---- BEGIN SSH2 ENCRYPTED PRIVATE KEY ---- Comment: RSA Private Key mF32KmMsoyqrru/46gXYvYHa8i4GpPchdIzh7fQDyx5+zAXxJ8skn3bAo /brrX7Nshm5zf0SPgbRGmdWXAfO3o0AZUaE/pHcPfpTE3Ilyu6Qtjfob64S /kJKYwfvZhRvU4g6hIBfZnCDXz0H1mgXvzoYBpkqxq8ZIdTdYOIRW+3W25z8+ez2r /LycEtNyEziv0RGhCfSZzat3PGCpNX9IH1DY9asfNAnIKDcRvqOnIO4hcBY+aCirtSs3wS xtYPS1m3rBUdhUB0X4m/bzH1qJJP6dLuxZAVsrNRY1XmK3WGjxsyNGsUgC /2dEmPZodIstKTv4xg13hux78rzd3u072ofCSRmEuO166S2JNNR1IRLcVOI /PKVv1pfuuZUDDm0qmegr8sDvWFXkDbeWPisOvRQXO3Yk2D94TiW1sFpW0B4zB9nN QMsO4/dQnI/Qa5ofk/ObzwVNmmaNhXdK /TYPXRQGJEz9McLc641VNYmKWpBELTqS /vujygonYqDpgUw2XJlxZ9nmhp1mYteqINTUNVv4QNnssc9no5YoffPdyNEuox9L0rmT LgNaIpdo5R6CP7hyN0Ao9wGgBMwnq6dz2fUSpIhu2vqNULmaRgUIKR2bVtmSBWuX S8CRtDFnt3qB3UMRLouMssWWEuGfCJaAA7zhDbeqDRuct /EiPWLgzYBqGbCvTB4EZtbbIQebmFphnqxc3X7CuxmU9klwUrkZTVhjoQb7rjySbCybP w47xpxi5/6u6A6kyhC+/wpWBId6C4UO2u/9C7zDJSnho5w+anL6 /1tl6p06lkwn+hCsqZJA9kphmaq5NjUscQadZqQtz4w5s8kVpjT3Ify5NZr2KB030Qi9ICsP O+ao1vhnfBSPfu8Rt/8fPXVQyfhXvYG /RI6aDIho3+pL7VUdqZ7u4CyYB+pnrZ5psX9I6qRuGfqiTDMSiZyWY /p+J6IhLfYwKfI3Lj2wpeggRwI4HUiZpGr+0S5O51ot8+1ItlkFhcqA1+Z3C9Sh7TvNyBGI gbLqLPsXxz2xAHIzH8 /NK7EquMs0Ob52DPJ79vNeJjtjfNAvPjwDkCunkEzjoo3LYxIiE3DtMCBAcVPUEGncKK hCA== ---- END SSH2 PRIVATE KEY ----

Back | Display Sensitive Data As Plaintext