

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 authenticeren 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

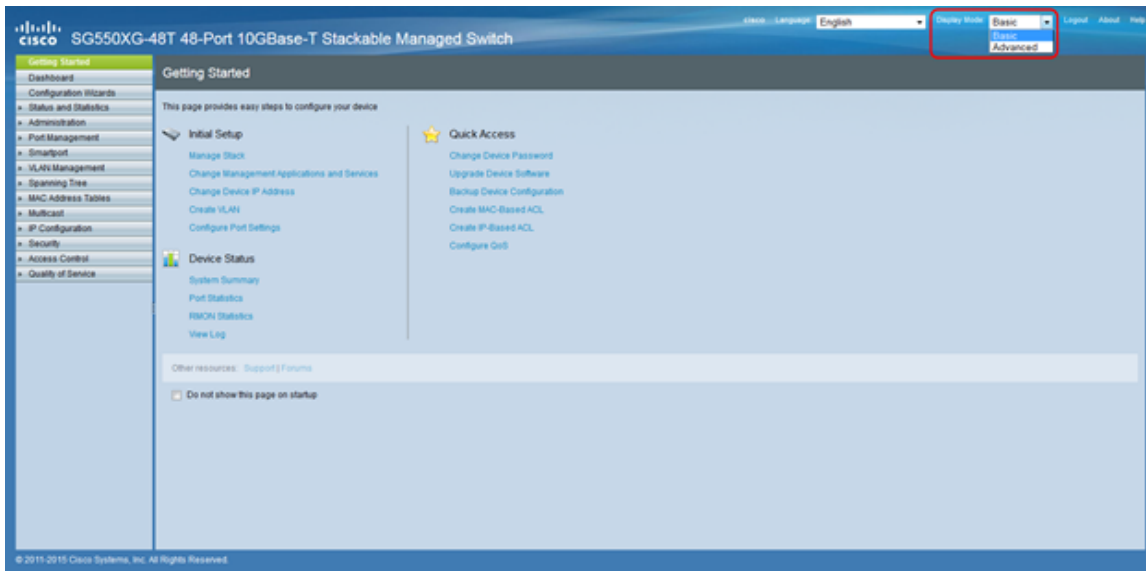
Softwareversie

- 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:

SSH User Authentication

Global Configuration

SSH User Authentication Method: By Password
 By RSA Public Key
 By DSA Public Key

Credentials

Username: (0/70 characters used)

Password: Encrypted
 Plaintext (Default Password: anonymous)

SSH User Key Table

| <input type="checkbox"/> | Key Type | Key Source | Fingerprint |
|--------------------------|----------|----------------|---|
| <input type="checkbox"/> | RSA | Auto Generated | 6f:bf:d8:12:60:74:ea:4c:68:a1:76:91:e5:8f:a4:d1 |
| <input type="checkbox"/> | DSA | Auto Generated | 24:31:b0:3c:5c:94:74:35:ba:d1:ce:c6:f7:16:84:48 |

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

SSH User Authentication

Global Configuration

SSH User Authentication Method: By Password
 By RSA Public Key
 By DSA Public Key

Credentials

Username: (0/70 characters used)

Password: Encrypted
 Plaintext (Default Password: anonymous)

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.

SSH User Authentication

Global Configuration

SSH User Authentication Method: By Password
 By RSA Public Key
 By DSA Public Key

Credentials

Username: (0/70 characters used)

Password: Encrypted
 Plaintext (Default Password: anonymous)

Apply Cancel Restore Default Credentials Display Sensitive Data as Plaintext

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".

SSH User Authentication

Global Configuration

SSH User Authentication Method: By Password
 By RSA Public Key
 By DSA Public Key

Credentials

Username: (0/70 characters used)

Password: Encrypted
 Plaintext (Default Password: anonymous)

Apply Cancel Restore Default Credentials Display Sensitive Data as Plaintext

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.

SSH User Authentication

Global Configuration

SSH User Authentication Method: By Password
 By RSA Public Key
 By DSA Public Key

Credentials

Username: (0/70 characters used)

Password: Encrypted
 Plaintext (Default Password: anonymous)

Apply Cancel Restore Default Credentials Display Sensitive Data as Plaintext

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

SSH User Authentication

Global Configuration

SSH User Authentication Method: By Password
 By RSA Public Key
 By DSA Public Key

Credentials

Username: (0/70 characters used)

Password: Encrypted
 Plaintext (Default Password: anonymous)

Apply Cancel **Restore Default Credentials** Display Sensitive Data as Plaintext

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

SSH User Authentication

Global Configuration

SSH User Authentication Method: By Password
 By RSA Public Key
 By DSA Public Key

Credentials

Username: (0/70 characters used)

Password: Encrypted
 Plaintext (Default Password: anonymous)

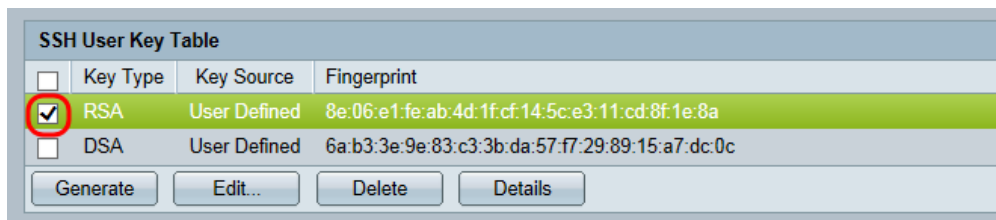
Apply Cancel Restore Default Credentials **Display Sensitive Data as Plaintext**

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

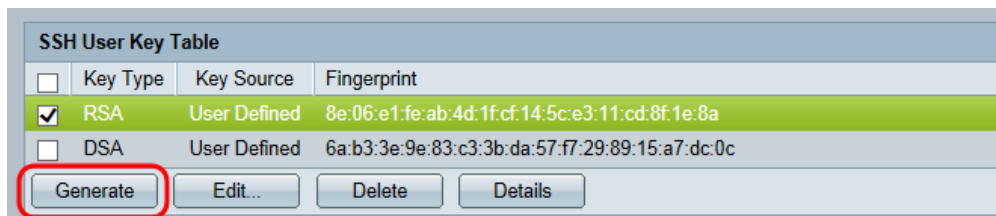
SSH-gebruikerstaal

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

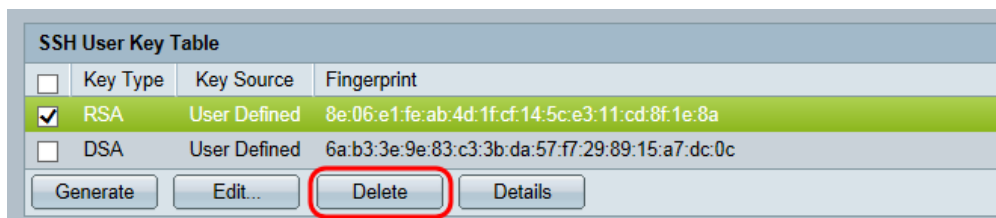
Stap 1. Navigeer naar de *SSH-gebruikerstaal*. Selecteer in de opgeroepen lijst het/de selectietekens die u wilt beheren.



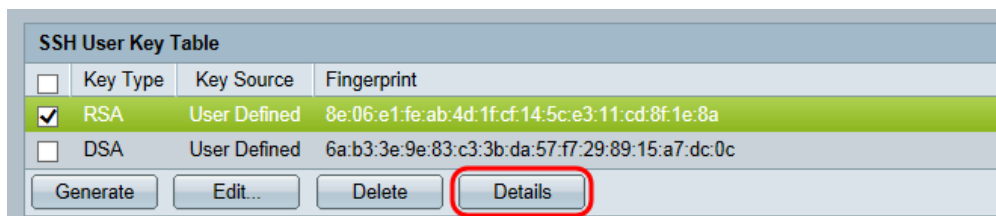
Stap 2. (Optioneel) Klik op **Generate** om een nieuwe toets te genereren. De nieuwe toets heeft voorrang op de geselecteerde toets. Er verschijnt een bevestigingsvenster. Klik op **OK** om verder te gaan.



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.

SSH User Key Details

SSH Server Key Type: RSA

Public Key: ---- BEGIN SSH2 PUBLIC KEY ----
Comment: RSA Public Key
AAAAB3NzaC1yc2EAAAADAQABAAQCAeTjr4/8xsROwDkFBY7efsV5v59RNAwzJdZsxb
XRqFXeMQ2LNyUTCK8hcu0zVSipsQ8AFRZmpnaVkEgSunFK5YYJ2AckP9NyMikihWfRWm
UXT6SBOK/BJk7GPXhcs0JE6I3uPCyiC50vzGRBGHWSH/oGBxMqkavDGpcToaDyKQ==
---- END SSH2 PUBLIC KEY ----

Private Key (Encrypted): ---- BEGIN SSH2 ENCRYPTED PRIVATE KEY ----
Comment: RSA Private Key

---- END SSH2 PRIVATE KEY ----

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

SSH User Key Table

| <input type="checkbox"/> | Key Type | Key Source | Fingerprint |
|-------------------------------------|----------|--------------|---|
| <input checked="" type="checkbox"/> | RSA | User Defined | 8e:06:e1:fe:ab:4d:1f:cf:14:5c:e3:11:cd:8f:1e:8a |
| <input type="checkbox"/> | DSA | User Defined | 6a:b3:3e:9e:83:c3:3b:da:57:f7:29:89:15:a7:dc:0c |

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

When a Key is entered, it should contain the "BEGIN" and "END" markers.

Key Type:

Public Key:

Private Key: Encrypted

Plaintext

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

When a Key is entered, it should contain the "BEGIN" and "END" markers.

Key Type: **RSA** ▼

Public Key:

```
-----BEGIN SSH2 PUBLIC KEY -----  
Comment: RSA Public Key  
AAAAB3NzaC1yc2EAAAADAQABAAQCAeTjr4/8xsROwDkFBY7efsV5v59RNAwzJdZsxbXRqF'  
-----END SSH2 PUBLIC KEY -----
```

Private Key: Encrypted

Plaintext

Apply Close Display Sensitive Data as Plaintext

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.

When a Key is entered, it should contain the "BEGIN" and "END" markers.

Key Type: **RSA** ▼

Public Key:

```
-----BEGIN SSH2 PUBLIC KEY -----  
Comment: RSA Public Key  
AAAAB3NzaC1yc2EAAAADAQABAAQCAeTjr4/8xsROwDkFBY7efsV5v59RNAwzJdZsxbXRqF'  
-----END SSH2 PUBLIC KEY -----
```

Private Key: Encrypted

Plaintext

Apply Close Display Sensitive Data as Plaintext

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.

When a Key is entered, it should contain the "BEGIN" and "END" markers.

Key Type:

Public Key:

```
-----BEGIN SSH2 PUBLIC KEY -----  
Comment: RSA Public Key  
AAAAB3NzaC1yc2EAAAADAQABAAQCAeTjr4/8xsROwDkFBY7efsV5v59RNAwzJdZsxbXRqF;  
-----END SSH2 PUBLIC KEY -----
```

Private Key: Encrypted Plaintext

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

When a Key is entered, it should contain the "BEGIN" and "END" markers.

Key Type:

Public Key:

```
-----BEGIN SSH2 PUBLIC KEY -----  
Comment: RSA Public Key  
AAAAB3NzaC1yc2EAAAADAQABAAQCAeTjr4/8xsROwDkFBY7efsV5v59RNAwzJdZsxbXRqF;  
-----END SSH2 PUBLIC KEY -----
```

Private Key: Encrypted Plaintext