# SSH-serververificatie-instellingen op een switch via de CLI configureren

## 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 stelt de beheerder in staat om de switch via de opdrachtregel interface (CLI) te configureren met een programma van een derde.

De switch fungeert als een SSH-client die SSH-functies biedt aan de gebruikers in het netwerk. De switch gebruikt een SSH-server om SSH-services te leveren. Wanneer de SSH-serververificatie uitgeschakeld is, neemt de switch elke SSH-server als betrouwbaar over, waardoor de beveiliging op uw netwerk afneemt. Als de SSH-service op de schakelaar is ingeschakeld, wordt de beveiliging verbeterd.

Dit artikel bevat instructies over het configureren van serververificatie op een beheerde switch via de CLI.

## Toepasselijke apparaten

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

## Softwareversie

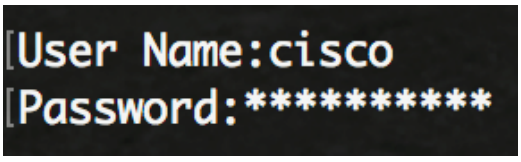
- 1.4.7.06 - SX300, SX500
- 2.2.8.04 - SX350, SG350X, SX550X

## SSH-serverinstellingen configureren

### SSH-serververificatie instellen

Stap 1. Meld u aan bij de switch-console. De standaardwaarden voor gebruikersnaam en wachtwoord zijn cisco/cisco. Als u een nieuwe gebruikersnaam of wachtwoord heeft geconfigureerd, moet u deze inloggegevens gebruiken.

Opmerking: Om te leren hoe te om tot een schakelaar CLI van Cisco van MKB door SSH of telnet toegang te hebben, klik hier.




Opmerking: Afhankelijk van het exacte model van de switch kunnen de opdrachten variëren. In dit

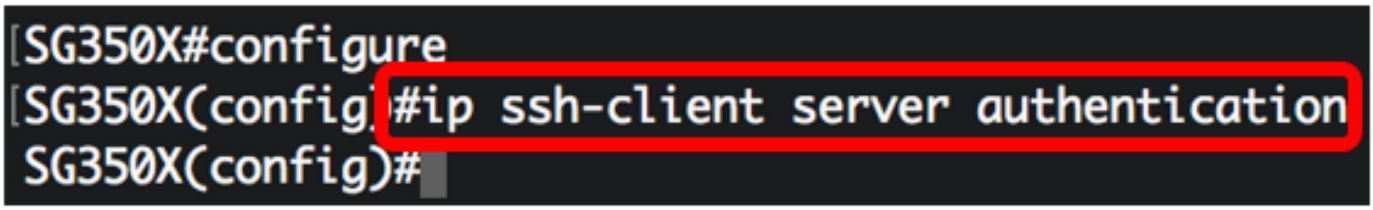
voorbeeld wordt de SG350X-switch benaderd via Telnet.

Stap 2. Voer in de bevoorrechte EXEC-modus van de switch de modus Global Configuration in door het volgende in te voeren:

```
SG350X#configuratie
```

Stap 3. Voer het volgende in om de externe SSH-serververificatie door de SSH-client mogelijk te maken:

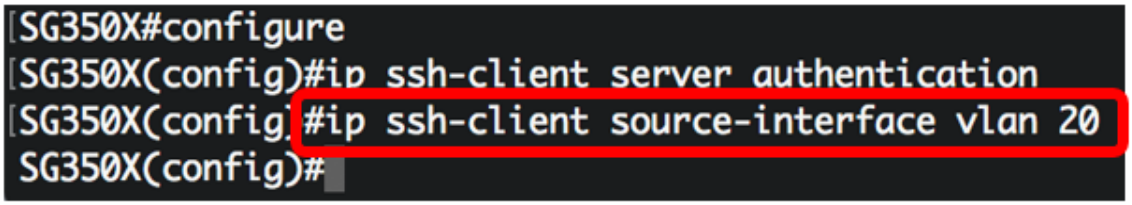
```
SG350X (configuratie)#ip ssh-client-serververificatie
```




Stap 4. Om de broninterface te specificeren die IPv4-adres zal worden gebruikt als het IPv4-adres van de bron voor communicatie met IPv4 SSH-servers, specificeert u het volgende:

```
SG350X (configuratie)#ip ssh-client-bron-interface [interface-id]
```

- interface-id - Specificeert de broninterface.




Opmerking: In dit voorbeeld is de broninterface VLAN 20.

Stap 5. (Optioneel) Om de broninterface te specificeren waarvan IPv6-adres zal worden gebruikt als het IPv6-adres van de bron voor communicatie met IPv6 SSH-servers, specificeert u het volgende:

```
SG350X (configuratie)#ipv6 ssh-client-bron-interface [interface-id]
```

- interface-id — Specificeert de broninterface.

Opmerking: In dit voorbeeld wordt het IPv6-adres van de bron niet ingesteld.

Stap 6. Voer het volgende in om een vertrouwde server aan de tabel met Trusted Remote SSH-server toe te voegen:

```
SG350X (configuratie)#ip ssh-client server vingerafdruk [host] | ip-adres] [vingerafdruk]
```

De parameters zijn:

- host - Domain Name Server (DNS)-naam van een SSH-server.
- ip-adres - Specificeert het adres van een SSH server. Het IP-adres kan een IPv4-, IPv6- of IPv6-adres zijn.
- vingerafdruk - vingerafdruk van de SSH-server (32 Hex-tekens).

```
SG350X#configure
SG350X(config)#ip ssh-client server authentication
SG350X(config)#ip ssh-client source-interface vlan 20
SG350X(config)#$00.1 76:0d:a0:12:7f:30:09:d3:18:04:df:77:c8:8e:51:a8
SG350X(config)#
```

Opmerking: In dit voorbeeld is het IP-adres van de server 192.168.100.1 en is de gebruikte vingerafdruk 76:0d:a0:12:7f:30:09:d3:18:04:df:77:c8:8e:51:a8.

Stap 7. Voer de opdracht **afsluiten** in om terug te gaan naar de modus Privileged EXEC:

`SG350X (configuratie)#**exit**`

```
SG350X#configure
SG350X(config)#ip ssh-client server authentication
SG350X(config)#ip ssh-client source-interface vlan 20
SG350X(config)#$00.1 76:0d:a0:12:7f:30:09:d3:18:04:df:77:c8:8e:51:a8
SG350X(config)#exit
SG350X#
```

Stap 8. Voer het volgende in om de instellingen voor SSH-serververificatie op de switch weer te geven:

`SG350X#**show ip ssh-client server [host] | ip-adres]**`

De parameters zijn:

- host - Domain Name Server (DNS)-naam van een SSH-server.
- ip-adres - Specificeert het adres van een SSH server. Het IP-adres kan een IPv4-, IPv6- of IPv6-adres zijn.

```
SG350X(config)#exit
SG350X#show ip ssh-client server 192.168.100.1
SSH Server Authentication is Enabled

Server address            : 192.168.100.1
  Server Key Fingerprint  : 76:0d:a0:12:7f:30:09:d3:18:04:df:77:c8:8e:51:a8


SG350X#
```

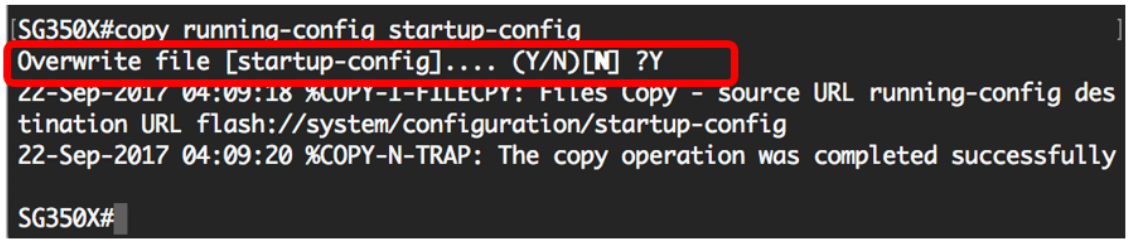
Opmerking: In dit voorbeeld wordt het IP-adres van de server 192.168.100.1 ingevoerd.

Stap 9. (Optioneel) In de bevoorrechte EXEC-modus van de switch, slaat u de geconfigureerde instellingen op in het opstartconfiguratiebestand door het volgende in te voeren:

`SG350X#copy running-config startup-config`

```
SG350X#copy running-config startup-config
Overwrite file [startup-config].... (Y/N)[N] ?
```

Stap 10. (Optioneel) Druk op **Y** for Yes of **N** for No op uw toetsenbord zodra het bestand overschrijven [startup-fig].... onmiddellijk verschijnt.




U hebt nu de stappen geleerd om serververificatie op een beheerde switch via de CLI te configureren.