Configure SSH Server Authentication Settings on a Switch through the CLI

Introduction

Secure Shell (SSH) is a protocol that provides a secure remote connection to specific network devices. This connection provides functionality that is similar to a Telnet connection, except that it is encrypted. SSH allows the administrator to configure the switch through the command line interface (CLI) with a third party program.

The switch acts as an SSH client that provides SSH capabilities to the users within the network. The switch uses an SSH server to provide SSH services. When SSH server authentication is disabled, the switch takes any SSH server as trusted, which decreases security on your network. If SSH service is enabled on the switch, security is enhanced.

This article provides instructions on how to configure server authentication on a managed switch through the CLI.

Applicable Devices

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

Software Version

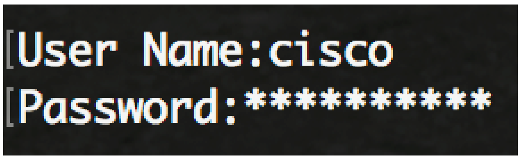
- 1.4.7.06 - Sx300, Sx500
- 2.2.8.04 - Sx350, SG350X, Sx550X

Configure SSH Server Settings

Configure SSH Server Authentication Settings

Step 1. Log in to the switch console. The default username and password is cisco/cisco. If you have configured a new username or password, enter the credentials instead.

Note: To learn how to access an SMB switch CLI through SSH or Telnet, click here.



```
[User Name:cisco
[Password:**********
```

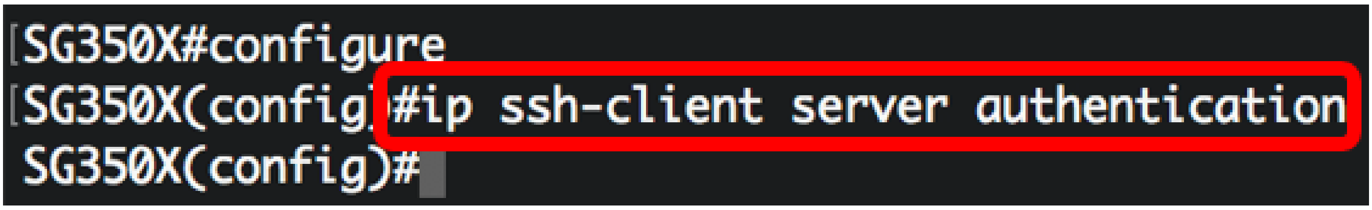
Note: The commands may vary depending on the exact model of your switch. In this example, the SG350X switch is accessed through Telnet.

Step 2. From the Privileged EXEC mode of the switch, enter the Global Configuration mode by entering the following:

```
SG350X#configure
```

Step 3. To enable remote SSH server authentication by the SSH client, enter the following:

```
SG350X(config)#ip ssh-client server authentication
```

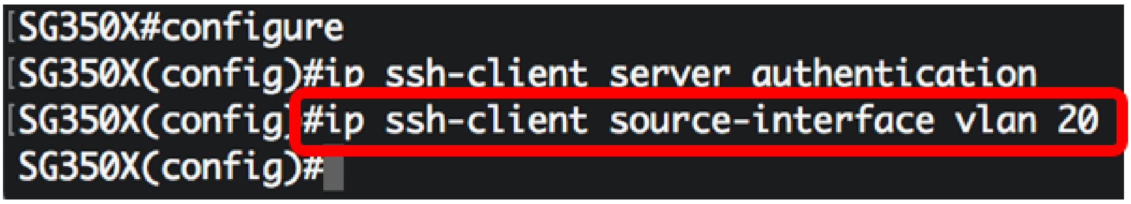


```
[SG350X#configure
[SG350X(config)#ip ssh-client server authentication
 SG350X(config)#
```

Step 4. To specify the source interface which IPv4 address will be used as the Source IPv4 address for communication with IPv4 SSH servers, enter the following:

```
SG350X(config)#ip ssh-client source-interface [interface-id]
```

- interface-id - Specifies the source interface.



```
[SG350X#configure
[SG350X(config)#ip ssh-client server authentication
[SG350X(config)#ip ssh-client source-interface vlan 20
 SG350X(config)#
```

Note: In this example, the source interface is VLAN 20.

Step 5. (Optional) To specify the source interface whose IPv6 address will be used as the Source IPv6 address for communication with IPv6 SSH servers, enter the following:

```
SG350X(config)#ipv6 ssh-client source-interface [interface-id]
```

- interface-id — Specifies the source interface.

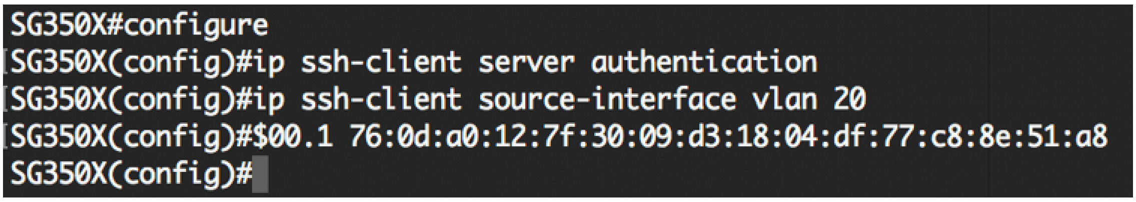
Note: In this example, source IPv6 address is not configured.

Step 6. To add a trusted server to the Trusted Remote SSH Server Table, enter the following:

```
SG350X(config)#ip ssh-client server fingerprint [host | ip-address] [fingerprint]
```

The parameters are:

- host - Domain Name Server (DNS) name of an SSH server.
- ip-address - Specifies the address of an SSH server. The IP address can be an IPv4, IPv6 or IPv6z address.
- fingerprint - Fingerprint of the SSH server public key (32 Hex characters).

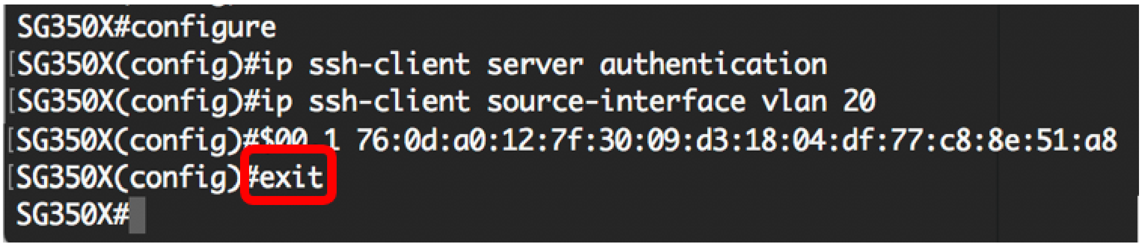


```
 SG350X#configure
[SG350X(config)#ip ssh-client server authentication
[SG350X(config)#ip ssh-client source-interface vlan 20
[SG350X(config)#$00.1 76:0d:a0:12:7f:30:09:d3:18:04:df:77:c8:8e:51:a8
 SG350X(config)#
```

Note: In this example, the server IP address is 192.168.100.1 and the fingerprint used is 76:0d:a0:12:7f:30:09:d3:18:04:df:77:c8:8e:51:a8.

Step 7. Enter the **exit** command to go back to the Privileged EXEC mode:

```
SG350X(config)#exit
```



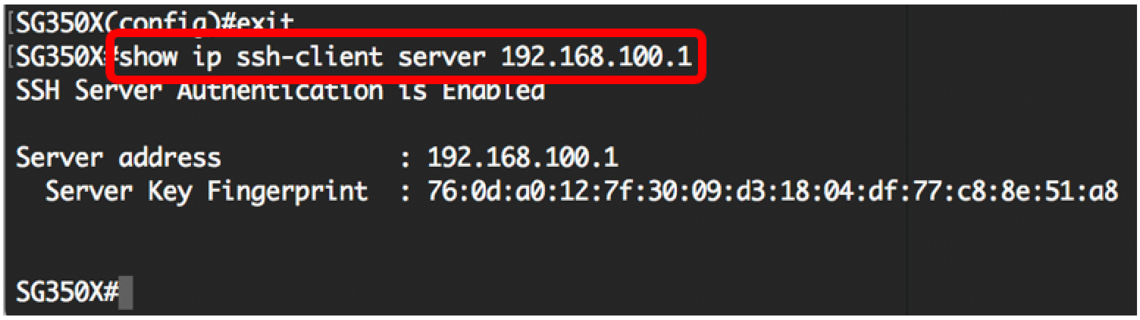
```
SG350X#configure
[SG350X(config)#ip ssh-client server authentication
[SG350X(config)#ip ssh-client source-interface vlan 20
[SG350X(config)#$00.1 76:0d:a0:12:7f:30:09:d3:18:04:df:77:c8:8e:51:a8
[SG350X(config)#exit
SG350X#
```

Step 8. To display the SSH server authentication settings on the switch, enter the following:

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

The parameters are:

- host - Domain Name Server (DNS) name of an SSH server.
- ip-address - Specifies the address of an SSH server. The IP address can be an IPv4, IPv6 or IPv6z address.

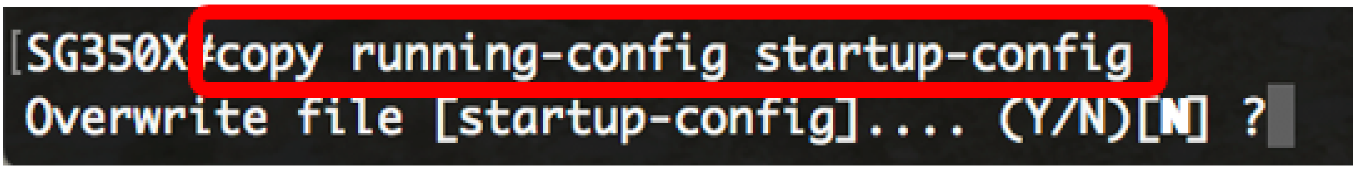


```
[SG350X(config)#exit
[SG350X#show ip ssh-client server 192.168.100.1
SSH Server Authentication is Enabled

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#
```

Note: In this example, the server IP address 192.168.100.1 is entered.

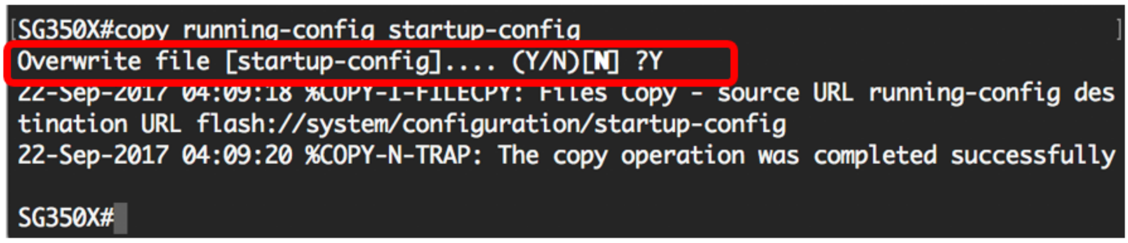
Step 9. (Optional) In the Privileged EXEC mode of the switch, save the configured settings to the startup configuration file by entering the following:

```
SG350X#copy running-config startup-config
```



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

Step 10. (Optional) Press **Y** for Yes or **N** for No on your keyboard once the Overwrite file [startup-config].... prompt appears.



```
[SG350X#copy running-config startup-config
Overwrite file [startup-config].... (Y/N)[N] ?Y
22-Sep-2017 04:09:18 %COPY-I-FILECPY: Files Copy - source URL running-config des
tination URL flash://system/configuration/startup-config
22-Sep-2017 04:09:20 %COPY-N-TRAP: The copy operation was completed successfully

SG350X#
```

You have now learned the steps to configure server authentication on a managed switch through the CLI.