Configure Simple Network Time Protocol (SNTP) Authentication Settings on a Switch through the Command Line Interface (CLI)

Objective

Simple Network Time Protocol (SNTP) is the simplified version of Network Time Protocol (NTP). NTP is the protocol that is used to synchronize the clock on a network. It provides time within 100 milliseconds of the accurate time, but does not authenticate traffic.

The SNTP authentication page of the switch allows the administrator to configure NTP authentication keys to verify a time source. SNTP authentication should be used only in situations where strong authentication is not required as it does not provide the complex filtering mechanisms of NTP.

This document explains how to define SNTP Authentication through the Command Line Interface (CLI) of a switch. You may also configure SNTP authentication settings through the web-based utility of the switch. For instructions, click [here](#).
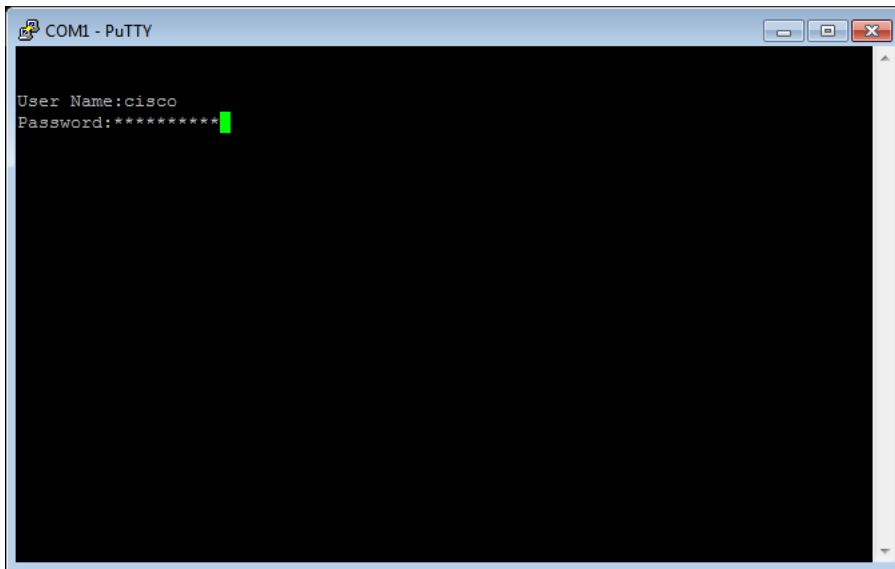
Applicable Devices

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

Software Version

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

## Configure SNMP Groups on a Switch

Step 1. Access the CLI of the switch.

Note: In this example, PuTTY is the application used to access the switch CLI. The default username and password is cisco/cisco. If you have customized your credentials, use your username and password.

Step 2. Switch to Global Configuration mode by entering the following command:

`SG350X#`**`configureterminal`**
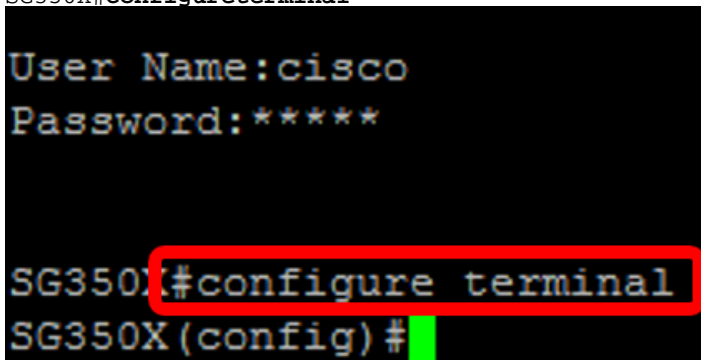
Step 3. Define an SNTP Authentication Key using one of the following syntax:

`SG350X(config)#`**`sntp authentication-key [key-number] md5 [key-value]`**

`SG350X(config)#`**`encrypted sntp authentication-key [key-number] md5 [encrypted key-value]`**
Where:

- key-number - This specifies the number of the key. It can be from 1 to 4294967295.
- key-value - This specifies the value of the key. It can be from one to eight characters long.
- Encrypted-key-value - This specifies the key value in encrypted format.

`SG350X(config)#`**`sntp authentication-key 121110 md5 cisco`**
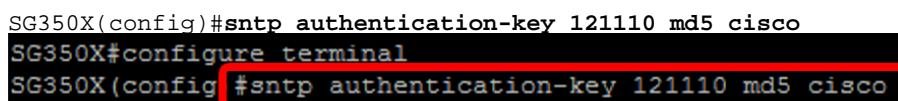
Note: In this example, sntp authentication-key 121110 md5 cisco is entered.

Step 4. Switch to Global Configuration mode by entering the following command:

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

```
SG350X(config)#sntp authentication-key 121110 md5 cisco
SG350X(config)#exit
```

Step 5. (Optional) Enter the following command in Privileged EXEC mode to save the configuration.

```
SG350X#copy running-config startup-config
```
```
Source IPv6 interface:
SG350X#copy running-config startup-config
Overwrite file [startup-config].... (Y/N)[N] ?Y
```

Step 6. (Optional) Press **Y** to save the settings in the startup configuration of the switch otherwise, press **N** to proceed without saving the configuration to the startup configuration of the switch.

```
SG350X#copy running-config startup-config
Overwrite file [startup-config].... (Y/N)[N] ?Y
24-May-2017 07:02:07 %COPY-I-FILECPY: Files Copy - source URL running-config de
tination URL flash://system/configuration/startup-config
24-May-2017 07:02:10 %COPY-N-TRAP: The copy operation was completed successfull

SG350X#
```

Note: In this example, Y is pressed.

Step 7. Verify the sntp authentication key with the following command:

```
SG350X#show sntp configuration
```
```
SG350X(config)#exit
SG350X#show sntp configuration
SNTP destination port : 123 .
Polling interval: 1024 seconds.
MD5 authentication keys.(Encrypted)
------------------------------------
121110      AR0EvVLMGAD24At8AbZCRXJgLKYwPRAx3qYDTZqk8Go=

Authentication is not required for synchronization.
No trusted keys.

Unicast Clients: Enabled
Unicast Clients Polling: Enabled

Server          : time-a.timefreq.bldrdoc.gov
  Polling       : Enabled
  Encryption Key : Disabled

Server          : time-b.timefreq.bldrdoc.gov
  Polling       : Enabled
  Encryption Key : Disabled

Server          : time-c.timefreq.bldrdoc.gov
  Polling       : Enabled
  Encryption Key : Disabled


Broadcast Clients: disabled
Anycast Clients: disabled
No Broadcast Interfaces.
Source IPv4 interface:
Source IPv6 interface:
```

Note: In this example, the MD5 Authentication keys are 121110 AR0EvVLMGAD24At8AbZCRXJgLKYwPRAx3qYDTZqk8Go=

You should now have configured an SNTP Authentication settings through the CLI of the switch.