

# Konfigurieren der Authentifizierungseinstellungen für das Simple Network Time Protocol (SNTP) auf einem Switch über die Befehlszeilenschnittstelle (CLI)

## Ziel

Simple Network Time Protocol (SNTP) ist die vereinfachte Version von Network Time Protocol (NTP). NTP ist das Protokoll, das zur Synchronisierung der Uhr in einem Netzwerk verwendet wird. Sie bietet eine Zeit innerhalb von 100 Millisekunden nach der genauen Uhrzeit, authentifiziert jedoch keinen Datenverkehr.

Auf der Seite für die SNTP-Authentifizierung des Switches kann der Administrator NTP-Authentifizierungsschlüssel konfigurieren, um eine Zeitquelle zu überprüfen. Die SNTP-Authentifizierung sollte nur in Situationen verwendet werden, in denen keine strenge Authentifizierung erforderlich ist, da sie die komplexen Filtermechanismen des NTP nicht bereitstellt.

In diesem Dokument wird erläutert, wie die SNTP-Authentifizierung über die Befehlszeilenschnittstelle (CLI) eines Switches definiert wird. Sie können die SNTP-Authentifizierungseinstellungen auch über das webbasierte Dienstprogramm des Switches konfigurieren. Anweisungen hierzu erhalten Sie [hier](#).

## Anwendbare Geräte

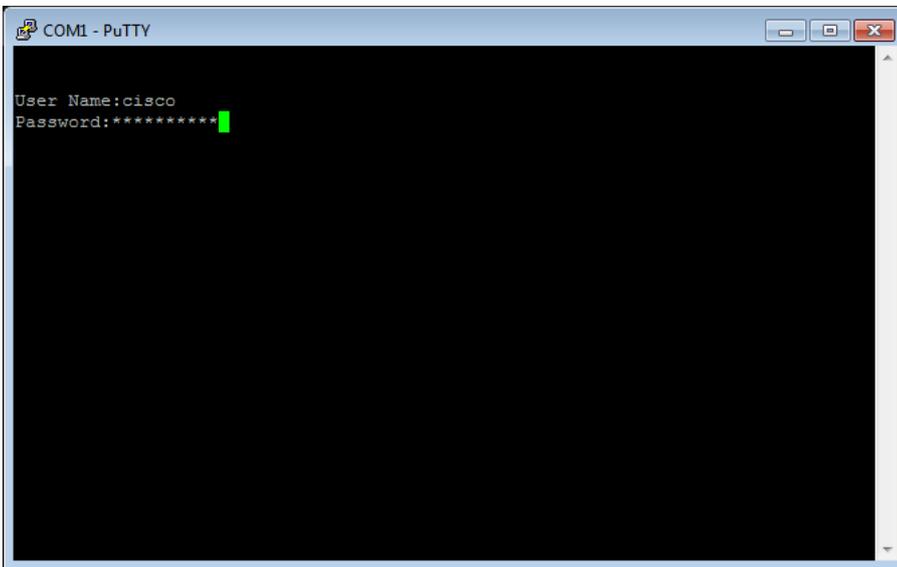
- Serie Sx300
- Serie Sx350
- SG350X-Serie
- Serie Sx500
- Serie Sx550X

## Softwareversion

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

## Konfigurieren von SNMP-Gruppen in einem Switch

Schritt 1: Zugriff auf die CLI des Switches



**Hinweis:** In diesem Beispiel wird PuTTY für den Zugriff auf die Switch-CLI verwendet. Der Standard-Benutzername und das Kennwort lautet cisco/cisco. Wenn Sie Ihre Anmeldeinformationen angepasst haben, verwenden Sie Ihren Benutzernamen und Ihr Kennwort.

Schritt 2: Wechseln Sie in den globalen Konfigurationsmodus, indem Sie den folgenden Befehl eingeben:

```
SG350X#ConfigurationTerminal
User Name:cisco
Password:*****
SG350X#configure terminal
SG350X(config)#
```

Schritt 3: Definieren Sie einen SNTP-Authentifizierungsschlüssel mithilfe einer der folgenden Syntax:

```
SG350X(config)#sntp authentication-key [Schlüsselnummer] md5 [Schlüsselwert]
```

```
SG350X(config)#verschlüsselter SNTP-Authentifizierungsschlüssel [Schlüsselnummer] md5
[verschlüsselter Schlüsselwert]
```

Wo:

- key-number - Gibt die Nummer des Schlüssels an. Sie kann zwischen 1 und 4294967295 liegen.
- key-value: Dieser Wert gibt den Wert des Schlüssels an. Es kann zwischen ein und acht Zeichen lang sein.
- Encrypted-key-value - Dieser Wert gibt den Schlüsselwert im verschlüsselten Format an.

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

**Hinweis:** In diesem Beispiel wird "sntp authentication-key 121110 md5 cisco" eingegeben.

Schritt 4: Wechseln Sie in den globalen Konfigurationsmodus, indem Sie den folgenden Befehl eingeben:

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

Schritt 5: (Optional) Geben Sie den folgenden Befehl im privilegierten EXEC-Modus ein, um die Konfiguration zu speichern.

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

Schritt 6: (Optional) Drücken Sie Y, um die Einstellungen in der Startkonfiguration des Switches zu speichern. Drücken Sie andernfalls N, um fortzufahren, ohne die Konfiguration in der Startkonfiguration des Switches zu speichern.

```
SG350X#copy running-config startup-config
Overwrite file [startup-config]... (Y/N) [N] ?Y
24-May-2017 07:02:07 %COPY-I-FILECOPY: 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#
```

**Hinweis:** In diesem Beispiel wird Y gedrückt.

Schritt 7: Überprüfen Sie den Authentifizierungsschlüssel sntp mit dem folgenden Befehl:

```
SG350X#show sntp-Konfiguration
```

```
SG350X(config)#exit
SG350X#show sntp configuration
SNTP destination port : 123 .
Polling interval: 1024 seconds.
MD5 authentication keys.(Encrypted)
-----
121110      AROEvVLMGAD24at8AbZCRXJgLKYwPRAx3qYDTZqk8Go=

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:
```

**Hinweis:** In diesem Beispiel sind die MD5-Authentifizierungsschlüssel 12110 AROEvVLMGAD24at8AbZCRXJgLKYwPRAx3qYDTZqk8Go=

Sie sollten jetzt über die CLI des Switches SNTP-Authentifizierungseinstellungen konfiguriert haben.

© 2018 Cisco Systems, Inc. Alle Rechte vorbehalten.