# NTP op draadloze LAN-controllers configureren

## Inhoud



## Inleiding

Dit document beschrijft hoe u AireOS draadloze LAN-controllers (WLC) kunt configureren om datum en tijd te synchroniseren met een Network Time Protocol (NTP)-server.

## Voorwaarden

### Vereisten

Voordat u deze configuratie uitvoert, moet aan de volgende vereisten worden voldaan:

- Basiskennis van de configuratie van Cisco WLC.
- Basiskennis van NTP.

### Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco WLC 3504 draait softwareversie 8.8.10.
- Cisco Catalyst 3560-CX Series L3-Switch waarop Cisco IOS®-softwarerelease 15.2(6)E2 wordt uitgevoerd.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

## Systeemdatum en -tijd beheren op de draadloze LAN-controller

Op een WLC, kunnen de systeemdatum en de tijd handmatig worden geconfigureerd vanuit de WLC of worden geconfigureerd om de datum en tijd te verkrijgen van een NTP-server.

De systeemdatum en -tijd kunnen handmatig worden geconfigureerd in de CLI-configuratiewizard of de WLC GUI/CLI.

Dit document biedt een configuratievoorbeeld om de WLC-systeemdatum en -tijd te synchroniseren via een NTP-server.

NTP is een netwerkprotocol voor kloksynchronisatie tussen computersystemen via datanetwerken met variabele latentie om de klokjes van computers op enige referentie te synchroniseren. De RFC 1305 en RFC 5905 bieden gedetailleerde informatie over respectievelijk NTPv3 en NTPv4-implementatie.

Een NTP-netwerk ontvangt zijn tijd meestal van een gezaghebbende tijdbron, zoals een radiokloktijd of een atoomklok die is gekoppeld aan een tijdserver. NTP verdeelt deze tijd vervolgens over het netwerk.

Een NTP-client maakt een transactie met de server via het poll interval, die dynamisch verandert in de tijd en afhankelijk is van de netwerkvoorwaarden tussen de NTP-server en de client.

NTP gebruikt het concept van een stratum om te beschrijven hoeveel NTP-hop weg een machine is van een gezaghebbende tijdbron. Bijvoorbeeld, een stratum 1 tijdserver heeft een radio of atoomklok direct aan het bevestigd. Het stuurt dan zijn tijd naar een stratum 2 tijdserver door NTP, enzovoort.

Raadpleeg Best Practices for Network Time Protocol voor meer informatie over de best practices voor NTP-implementatie.

In het voorbeeld in dit document wordt een Cisco Catalyst 3560-CX Series L3-Switch als NTP-server gebruikt. WLC wordt gevormd om zijn datum en tijd met deze server te synchroniseren NTP.

# Configureren

## Netwerkdiagram

WLC ---- 3560-CX L3 Switch ---- NTP-server

## Configuraties

### De L3-Switch configureren als een gezaghebbende NTP-server

Gebruik deze opdracht in globale configuratiemodus als u wilt dat het systeem een gezaghebbende NTP-server is, zelfs als het systeem niet gesynchroniseerd is met een externe tijdbron:

```
#ntp master  !--- Makes the system an authoritative NTP server
```

### NTP-verificatie configureren

Als u de associaties met andere systemen voor beveiligingsdoeleinden wilt verifiëren, gebruikt u de volgende opdrachten. De eerste opdracht maakt de NTP-verificatiefunctie mogelijk.

De tweede opdracht definieert elk van de verificatiesleutels. Elke toets heeft een sleutelnummer, een type en een waarde. Op dit moment is md5 het enige sleuteltype dat ondersteund wordt.

Ten derde wordt een lijst met vertrouwde verificatiesleutels gedefinieerd. Als een sleutel wordt vertrouwd op, is dit systeem klaar om aan een systeem te synchroniseren dat deze sleutel in zijn pakketten NTP gebruikt. Gebruik deze opdrachten in de globale configuratiemodus om NTP-verificatie te configureren:

```
#ntp authenticate

!--- Enables the NTP authentication feature

#ntp authentication-key number md5 value

!--- Defines the authentication keys

#ntp trusted-key key-number

!--- Defines trusted authentication keys
```

Hier is een voorbeeld NTP Server configuratie op de 3560-CX L3 Switch. De switch is NTP master, wat betekent dat de router fungeert als de gezaghebbende NTP server maar zelf krijgt de tijd van een andere NTP server **xxxx.xxx**.

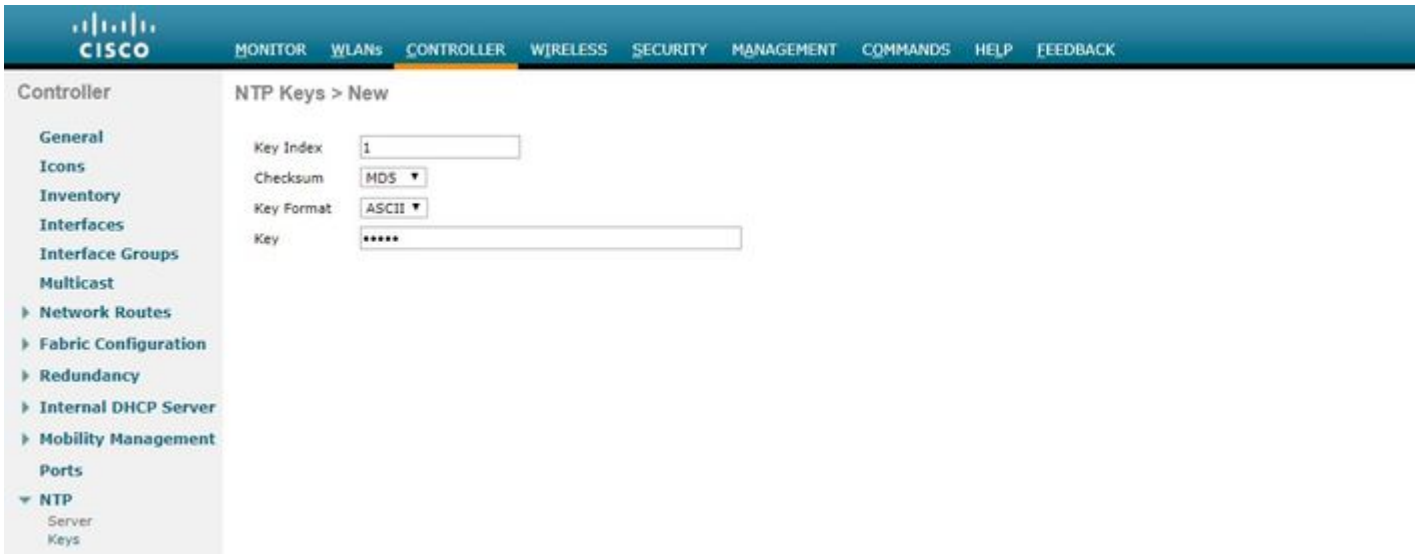
```
(config)#ntp authentication-key 1 md5 1511021F0725 7
(config)#ntp authenticate
(config)#ntp trusted-key 1
(config)#ntp master
(config)#ntp server xxxx.xxx
```

**Configureer de WLC voor de NTP-server**

Vanaf versie 8.6 kunt u NTPv4 inschakelen. U kunt ook een verificatiekanaal configureren tussen de controller en de NTP-server.

Voer de volgende stappen uit om NTP-verificatie in de controller GUI te configureren:

1. Kies **controller > NTP > toetsen**.
2. Klik op **Nieuw** om een toets te maken.
3. Voer de sleutelindex in in het tekstvak **sleutelindex in**.
4. Kies de **Key Checksum** (MD5 of SHA1) en de vervolgkeuzelijst **Key Format**.
5. Voer in het tekstvak **Sleutel de** sleutel in:

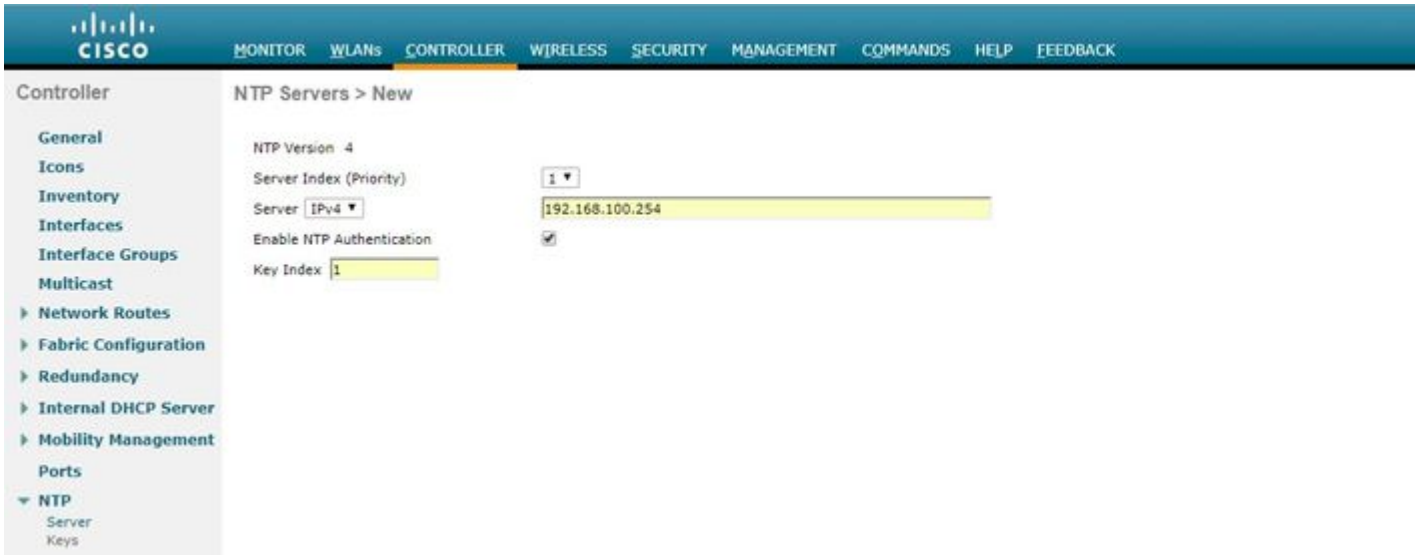



6. Kies **Controller > NTP > Servers** om de pagina NTP-servers te openen. Selecteer versie 3 of 4 en klik op **New** om een NTP-server toe te voegen. De **pagina NTP-servers > Nieuw** verschijnt.

7. Selecteer de **Server Index (prioriteit)**.

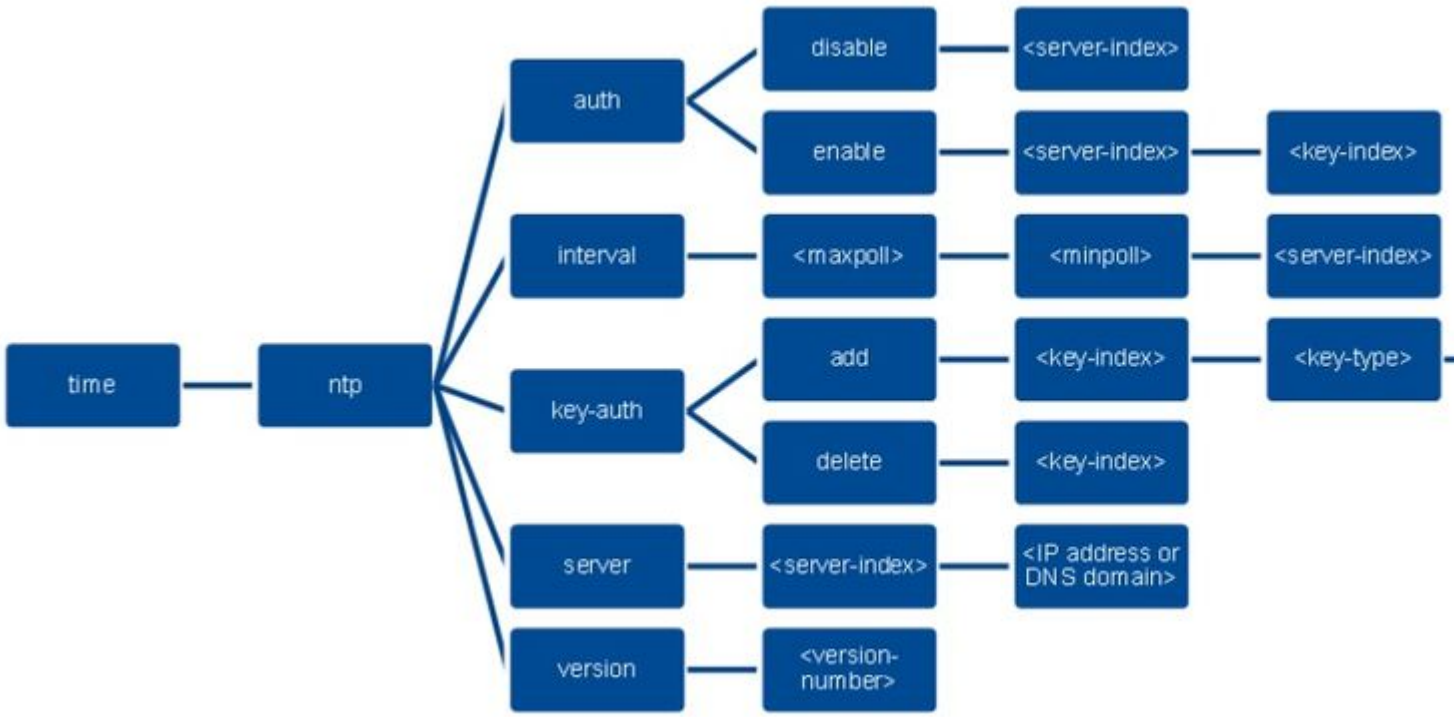
8. Voer het IP-adres van de NTP-server in het tekstvak **IP-adres van de server in**.

9. Schakel NTP-serververificatie in, selecteer het aanvinkvakje voor **NTP-serververificatie** en selecteer de eerder geconfigureerde **sleutelindex**.




10. Klik op Apply (Toepassen).

Om NTP-verificatie via de controller CLI te configureren, volgt u deze opdrachtstructuur:




```
>config time ntp version 4
>config time ntp key-auth add 1 md5 ascii cisco
>config time ntp server 1 192.168.100.254
>config time ntp auth enable 1 1
```

# Verifiëren

## Op de NTP-server

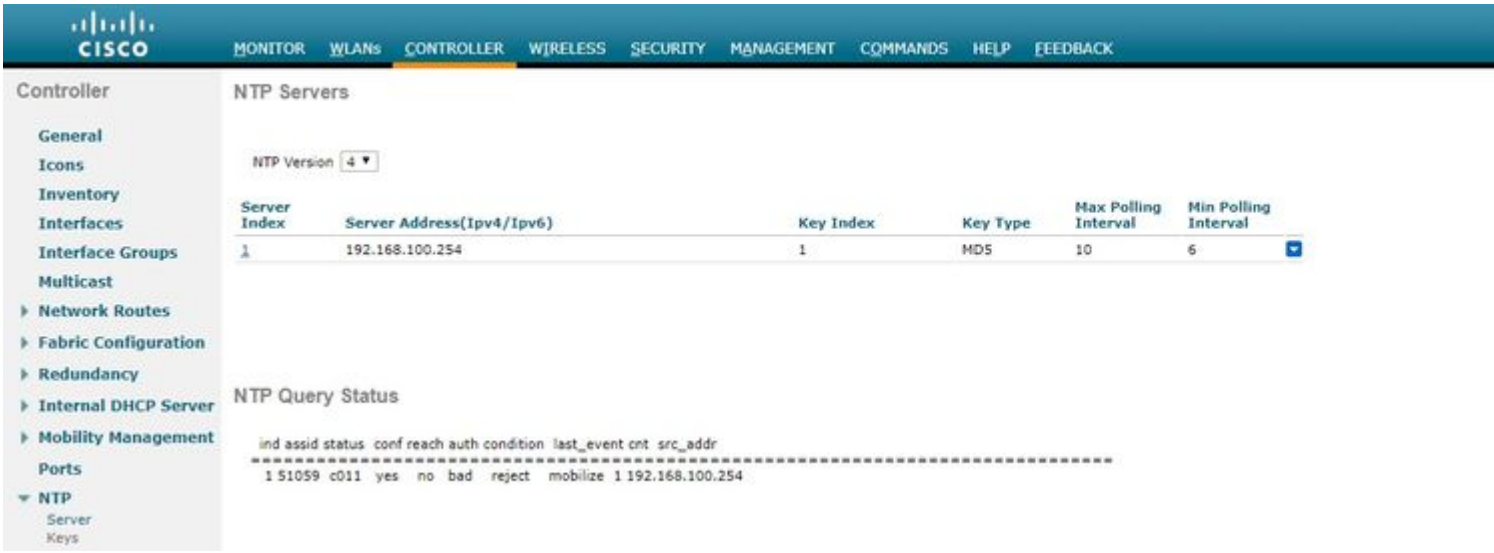
```
#show ntp status
Clock is synchronized, stratum 3, reference is x.x.x.x
nominal freq is 286.1023 Hz, actual freq is 286.0901 Hz, precision is 2**21
ntp uptime is 6591900 (1/100 of seconds), resolution is 3496
reference time is E007C909.80902653 (09:23:21.502 UTC Fri Feb 8 2019)
clock offset is 0.3406 msec, root delay is 59.97 msec
root dispersion is 25.98 msec, peer dispersion is 1.47 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000042509 s/s
system poll interval is 128, last update was 7 sec ago.

#show ntp associations

 address ref clock st when poll reach delay offset disp
*~x.x.x.x y.y.y.y 2 20 1024 17 13.634 0.024 1.626
 ~127.127.1.1 .LOCL. 7 9 16 377 0.000 0.000 0.232
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured

#show ntp information
Ntp Software Name : Cisco-ntpv4
Ntp Software Version : Cisco-ntpv4-1.0
Ntp Software Vendor : CISCO
```

```
Ntp System Type : Cisco IOS / APM86XXX
```

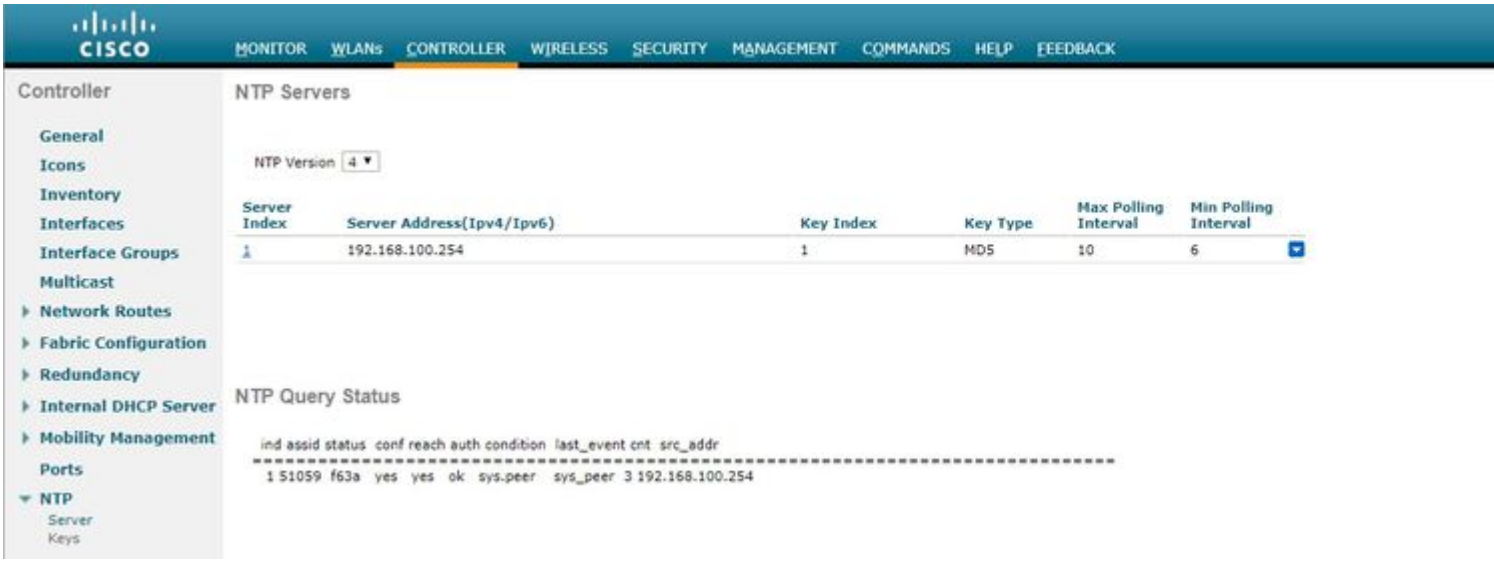
## Op de WLC

### In de GUI

Terwijl de WLC de communicatie tot stand brengt:




Nadat de verbinding is gemaakt:




### In de WLC CLI

```
(Cisco Controller) >show time

Time..................................... Fri Feb 8 10:14:47 2019

Timezone delta..................................... 0:0
Timezone location.................................
```

```
NTP Servers
 NTP Version.................................. 4

Index NTP Key NTP Server NTP Key Polling Intervals
 Index Type Max Min
 ------------------------------------------------------------
 1 1 192.168.100.254 MD5 10 6

NTPQ status list of NTP associations

assoc
 ind assid status conf reach auth condition last_event cnt src_addr
 ===========================================================================
 1 1385 f63a yes yes ok sys.peer sys_peer 3 192.168.100.254


(Cisco Controller) >
```

# Problemen oplossen

Aan de NTP-serverkant waarop Cisco IOS wordt uitgevoerd, kunt u debug ntp all enable opdracht:

```
#debug ntp all
NTP events debugging is on
NTP core messages debugging is on
NTP clock adjustments debugging is on
NTP reference clocks debugging is on
NTP packets debugging is on
#
(communication between SW and NTP server xxxx.xxx)
Feb 8 09:52:30.563: NTP message sent to x.x.x.x, from interface 'Vlan1' (192.168.1.81).
Feb 8 09:52:30.577: NTP message received from x.x.x.x on interface 'Vlan1' (192.168.1.81).
Feb 8 09:52:30.577: NTP Core(DEBUG): ntp_receive: message received
Feb 8 09:52:30.577: NTP Core(DEBUG): ntp_receive: peer is 0x0D284B34, next action is 1.

(communication between SW and WLC)
Feb 8 09:53:10.421: NTP message received from 192.168.100.253 on interface 'Vlan100' (192.168.100.254).
Feb 8 09:53:10.421: NTP Core(DEBUG): ntp_receive: message received
Feb 8 09:53:10.421: NTP Core(DEBUG): ntp_receive: peer is 0x00000000, next action is 3.
Feb 8 09:53:10.421: NTP message sent to 192.168.100.253, from interface 'Vlan100' (192.168.100.254).

(communication between SW and NTP server xxxx.xxx)
Feb 8 09:53:37.566: NTP message sent to x.x.x.x, from interface 'Vlan1' (192.168.1.81).
Feb 8 09:53:37.580: NTP message received from x.x.x.x on interface 'Vlan1' (192.168.1.81).
Feb 8 09:53:37.580: NTP Core(DEBUG): ntp_receive: message received
Feb 8 09:53:37.580: NTP Core(DEBUG): ntp_receive: peer is 0x0D284B34, next action is 1.

(communication between SW and WLC)
Feb 8 09:54:17.421: NTP message received from 192.168.100.253 on interface 'Vlan100' (192.168.100.254).
Feb 8 09:54:17.421: NTP Core(DEBUG): ntp_receive: message received
Feb 8 09:54:17.421: NTP Core(DEBUG): ntp_receive: peer is 0x00000000, next action is 3.
Feb 8 09:54:17.421: NTP message sent to 192.168.100.253, from interface 'Vlan100' (192.168.100.254).
```

Aan WLC-zijde:

```
 >debug ntp ?

detail Configures debug of detailed NTP messages.
low Configures debug of NTP messages.
packet Configures debug of NTP packets.
```

*(at the time of writte this doc there was Cisco bug ID CSCvo29660*
*on which the debugs of ntpv4 are not printed in the CLI. The below debugs are using NTPv3.)*

```
(Cisco Controller) >debug ntp detail enable
(Cisco Controller) >debug ntp packet enable
(Cisco Controller) >*emWeb: Feb 08 11:26:53.896: ntp Auth key Info = -1

*emWeb: Feb 08 11:26:58.143: ntp Auth key Info = -1

*emWeb: Feb 08 11:26:58.143: ntp Auth key Info = -1

*emWeb: Feb 08 11:26:58.143: Key Id = 1 found at Local Index = 0

*sntpReceiveTask: Feb 08 11:26:58.143: Initiating time sequence

*sntpReceiveTask: Feb 08 11:26:58.143: Fetching time from:192.168.100.254

*sntpReceiveTask: Feb 08 11:26:58.143: Started=3758614018.143350 2019 Feb 08 11:26:58.143

*sntpReceiveTask: Feb 08 11:26:58.143: hostname=192.168.100.254 hostIdx=1 hostNum=0
*sntpReceiveTask: Feb 08 11:26:58.143: Looking for the socket addresses

*sntpReceiveTask: Feb 08 11:26:58.143: NTP Polling cycle: accepts=0, count=5, attempts=1,
retriesPerHost=6. Outgoing packet on NTP Server on socket 0:

*sntpReceiveTask: Feb 08 11:26:58.143: sta=0 ver=3 mod=3 str=15 pol=8 dis=0.000000 ref=0.000000

*sntpReceiveTask: Feb 08 11:26:58.143: ori=0.000000 rec=0.000000
*sntpReceiveTask: Feb 08 11:26:58.143: tra=3758614018.143422 cur=3758614018.143422

*sntpReceiveTask: Feb 08 11:26:58.143: Host Supports NTP authentication with Key Id = 1

*sntpReceiveTask: Feb 08 11:26:58.143: NTP Auth Key Id = 1 Key Length = 5

*sntpReceiveTask: Feb 08 11:26:58.143: MD5 Hash and Key Id added in NTP Tx packet

*sntpReceiveTask: Feb 08 11:26:58.143: 00000000: 1b 0f 08 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
*sntpReceiveTask: Feb 08 11:26:58.143: 00000010: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
*sntpReceiveTask: Feb 08 11:26:58.143: 00000020: 00 00 00 00 00 00 00 00 e0 07 e6 02 24 b7 50 00 .....
*sntpReceiveTask: Feb 08 11:26:58.143: 00000030: 00 00 00 01 e4 35 f3 1a 89 f0 93 c5 51 c7 c5 23 .....5.
*sntpReceiveTask: Feb 08 11:26:58.143: 00000040: 01 dd 67 e0 ..g.
*sntpReceiveTask: Feb 08 11:26:58.143: Flushing outstanding packets

*sntpReceiveTask: Feb 08 11:26:58.143: Flushed 0 packets totalling 0 bytes

*sntpReceiveTask: Feb 08 11:26:58.143: Packet of length 68 sent to ::ffff:192.168.100.254 UDPport=123
*emWeb: Feb 08 11:26:58.143: ntp Auth key Info = 0

*emWeb: Feb 08 11:26:58.143: idx != 0 : ntp key Id = 1 Msg auth Status = 66

*sntpReceiveTask: Feb 08 11:26:58.146: Packet of length 68 received from ::ffff:192.168.100.254 UDPport=
*sntpReceiveTask: Feb 08 11:26:58.146: Incoming packet on socket 0: has Authentication Enabled
*sntpReceiveTask: Feb 08 11:26:58.146: 00000000: 1c 04 08 eb 00 00 0e a0 00 00 0b 2e c3 16 11 07 .....
*sntpReceiveTask: Feb 08 11:26:58.146: 00000010: e0 07 e5 f8 d3 21 bf 57 e0 07 e6 02 24 b7 50 00 .....!.
*sntpReceiveTask: Feb 08 11:26:58.146: 00000020: e0 07 e6 02 24 e5 e3 b4 e0 07 e6 02 24 f3 c7 5a ....$..
*sntpReceiveTask: Feb 08 11:26:58.146: 00000030: 00 00 00 01 32 e4 26 47 33 16 50 bd d1 37 63 b7 ....2.8
```

```
*sntpReceiveTask: Feb 08 11:26:58.146: KeyId In Recieved NTP Packet 1

*sntpReceiveTask: Feb 08 11:26:58.146: KeyId 1 found in recieved NTP packet exists as part of the truste

*sntpReceiveTask: Feb 08 11:26:58.146: The NTP trusted Key Id 1 length = 5

*sntpReceiveTask: Feb 08 11:26:58.146: NTP Message Authentication - SUCCESS

*sntpReceiveTask: Feb 08 11:26:58.146: sta=0 ver=3 mod=4 str=4 pol=8 dis=0.043671 ref=3758614008.824734

*sntpReceiveTask: Feb 08 11:26:58.146: ori=3758614018.143422 rec=3758614018.144133
*sntpReceiveTask: Feb 08 11:26:58.146: Offset=-0.000683+/-0.002787 disp=1.937698

*sntpReceiveTask: Feb 08 11:26:58.146: best=-0.000683+/-0.002787

*sntpReceiveTask: Feb 08 11:26:58.146: accepts=1 rejects=0 flushes=0

*sntpReceiveTask: Feb 08 11:26:58.146: Correction: -0.000683 +/- 0.002787 disp=1.937698

*sntpReceiveTask: Feb 08 11:26:58.146: Setting clock to 2019 Feb 08 11:26:58.145 + 0.001 +/- 1.940 secs
*sntpReceiveTask: Feb 08 11:26:58.146: correction -0.001 +/- 1.938+0.003 secs - ignored


(Cisco Controller) >
```

# Gerelateerde informatie

- **Cisco technische ondersteuning en downloads**

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.