# Problemen oplossen met Network Time Protocol (NTP) op FireSIGHT-systemen

## Inhoud



## Inleiding

Dit document beschrijft veel voorkomende problemen met tijdsynchronisatie op FireSIGHT-systemen en hoe u deze kunt oplossen.

## Voorwaarden

### Vereisten

Om de tijdsynchronisatie-instelling te kunnen configureren hebt u beheerdersniveau nodig op uw FireSIGHT Management Center.

### Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

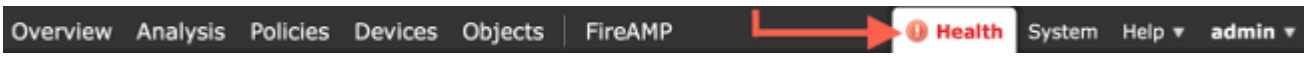
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

## Achtergrondinformatie

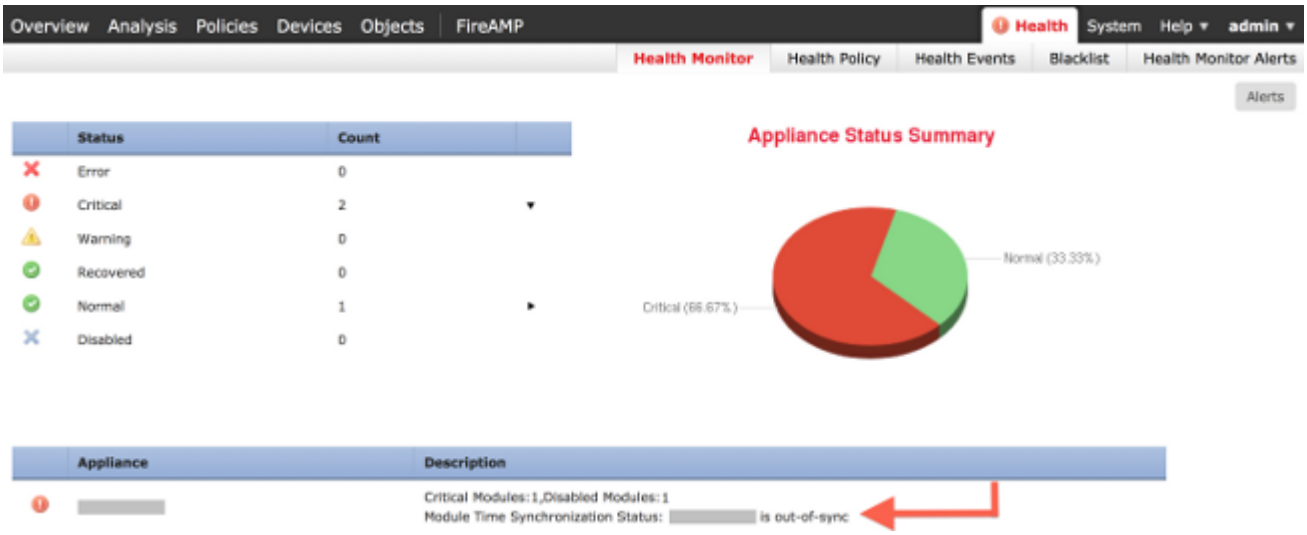
U kunt ervoor kiezen om de tijd tussen uw FireSIGHT-systemen op drie verschillende manieren te synchroniseren, zoals handmatig met externe Network Time Protocol (NTP)-servers, of met FireSIGHT Management Center dat fungeert als een NTP-server. U kunt een FireSIGHT Management Center configureren als een tijdserver met NTP en deze vervolgens gebruiken om de tijd tussen het FireSIGHT Management Center en beheerde apparaten te synchroniseren.

## Symptomen

- FireSIGHT Management Center geeft gezondheidswaarschuwingen op de browserinterface weer.




- De pagina **Health Monitor** toont een apparaat als kritisch, omdat de status van de Tijdsynchronisatiemodule niet synchroon is.




- Als de apparaten niet gesynchroniseerd blijven, kunt u af en toe gezondheidswaarschuwingen zien.
- Nadat een systeembeleid is toegepast, kunt u gezondheidswaarschuwingen zien, omdat een FireSIGHT Management Center en zijn beheerde apparaten tot 20 minuten kunnen duren om de synchronisatie te voltooien. Dit komt doordat een FireSIGHT Management Center eerst moet synchroniseren met de geconfigureerde NTP-server voordat het tijd kan dienen voor een beheerd apparaat.
- De tijd tussen een FireSIGHT Management Center en een beheerd apparaat komt niet overeen.
- Gebeurtenissen die op de sensor worden gegenereerd, kunnen enkele minuten of uren in beslag nemen om zichtbaar te worden op een FireSIGHT Management Center.
- Als u virtuele apparaten uitvoert en op de pagina **Health Monitor** wordt aangegeven dat de klokinstelling voor uw virtuele apparaat niet gesynchroniseerd is, controleert u de tijdsynchronisatie-instellingen van uw systeembeleid. Cisco raadt u aan uw virtuele apparaten te synchroniseren met een fysieke NTP-server. Synchroniseer uw beheerde apparaten (virtueel of fysiek) niet met een Virtual Defense Center.

# Problemen oplossen

## Stap 1: Controleer NTP-configuratie

### Hoe te om in Versies 5.4 en Vroeger te verifiëren

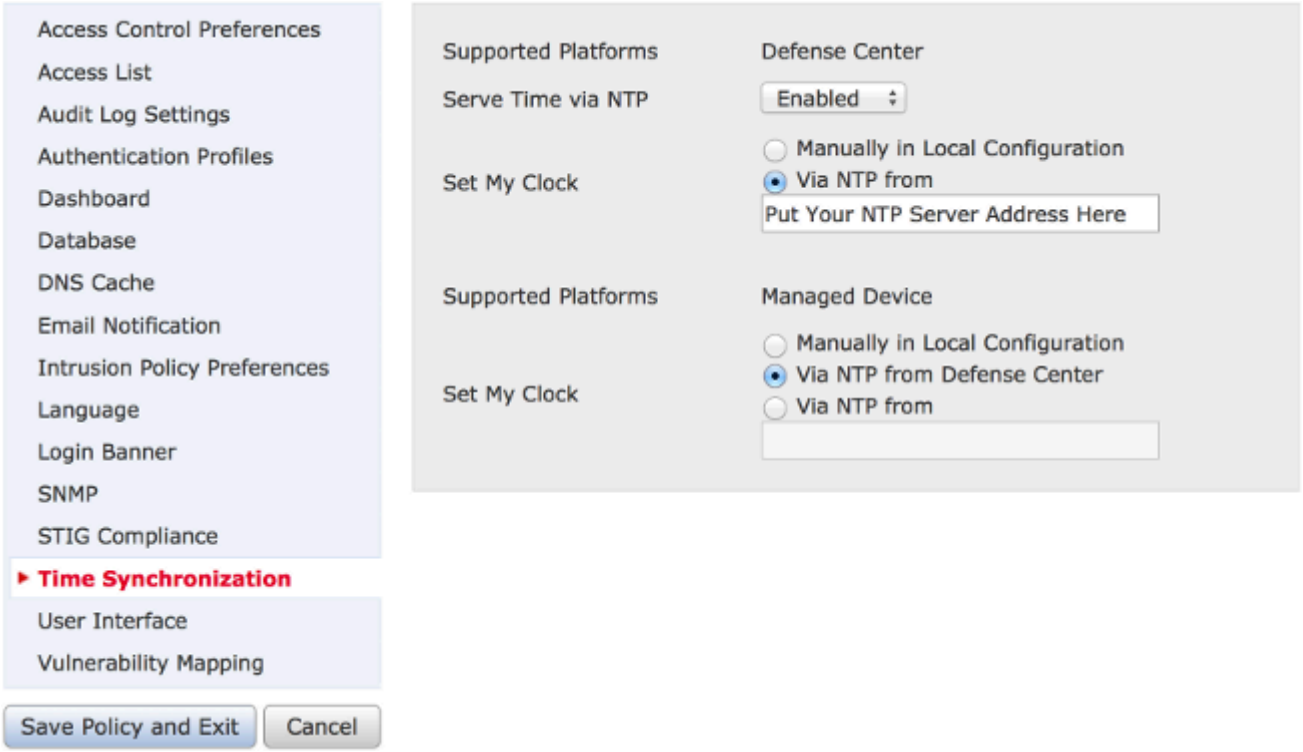
Controleer dat NTP is ingeschakeld op het systeembeleid dat op de FireSIGHT-systemen wordt toegepast. Voltooi de volgende stappen om te controleren of:

1. Kies **Systeem > Lokaal > Systeembeleid**.
2. Bewerk het systeembeleid dat op uw FireSIGHT Systems wordt toegepast.
3. Kies **Tijdsynchronisatie**.

Controleer of het FireSIGHT Management Center (ook bekend als Defense Center of DC) de klok heeft ingesteld op **Via NTP vanaf**, en of een adres van een NTP-server is opgegeven. Bevestig ook dat het

beheerde apparaat is ingesteld op **via NTP vanuit Defense Center**.

Als u een externe externe NTP-server opgeeft, moet uw apparaat netwerktoegang tot die server hebben. Specificeer geen onbetrouwbare NTP-server. Synchroniseer uw beheerde apparaten (virtueel of fysiek) niet met een Virtual FireSIGHT Management Center. Cisco raadt u aan uw virtuele apparaten te synchroniseren met een fysieke NTP-server.




**Hoe te om in Versies 6.0 en later te verifiëren**

In versies 6.0.0 en hoger worden de instellingen voor de tijdsynchronisatie op afzonderlijke plaatsen in het Firepower Management Center geconfigureerd, hoewel ze dezelfde logica overtrekken als de stappen voor 5.4.

De instellingen voor de tijdsynchronisatie voor het Firepower Management Center zelf staan onder **Systeem > Configuratie > Tijdsynchronisatie**.

De instellingen voor de tijdsynchronisatie van de beheerde apparaten vindt u onder **Apparaten > Platform-instellingen.** Klik op **bewerken** naast het beleid voor platforminstellingen dat op het apparaat is toegepast en kies vervolgens **Tijdsynchronisatie.**

Nadat u de configuratie voor tijdsynchronisatie hebt toegepast (ongeacht de versie), dient u ervoor te zorgen dat de tijd op uw Management Center en beheerde apparaten overeenkomt. Anders kunnen er onbedoelde gevolgen optreden wanneer de beheerde apparaten communiceren met het Management Center.

## Stap 2: Identificeer een Timeserver en de status ervan

- Om informatie te verzamelen over de verbinding met een tijdserver, voert u deze opdracht in op uw FireSIGHT Management Center:
  <#root>

  ```
  admin@FireSIGHT:~$
  ```

**ntpq -pn**

```
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*198.51.100.2   203.0.113.3      2 u  417 1024  377   76.814    3.458   1.992
```

Een asterisk '*' onder de afstandsbediening geeft de server aan waarop u momenteel gesynchroniseerd bent. Als een ingang met een asterisk niet beschikbaar is, is de klok momenteel niet gesynchroniseerd met zijn tijdbron.

Op een beheerd apparaat, kunt u deze opdracht op shell invoeren om het adres van uw NTP-server te bepalen:

<#root>

>

**show ntp**

```
NTP Server               : 127.0.0.2  (Cannot Resolve)
Status                   : Being Used
Offset                   : -8.344 (milliseconds)
Last Update              : 188 (seconds)
```

---

> **Opmerking**: Als een beheerd apparaat is geconfigureerd om tijd te ontvangen van een FireSIGHT Management Center, toont het apparaat een tijdbron met loopback-adres, zoals 127.0.0.2. Dit IP-adres is een tijdelijke proxy-vermelding en geeft aan dat het virtuele beheernetwerk wordt gebruikt om tijd te synchroniseren.

---

- Als een apparaat weergeeft dat het synchroniseert met 127.127.1.1, geeft dit aan dat het apparaat synchroniseert met de eigen klok. Het komt voor wanneer een tijdserver die op een systeembeleid wordt gevormd niet synchroniseerbaar is. Voorbeeld:
<#root>

admin@FirePOWER:~$

**ntpq -pn**

```
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
 192.0.2.200     .INIT.          16 u    - 1024    0    0.000    0.000   0.000
*127.127.1.1     .SFCL.          14 l    3   64  377    0.000    0.000   0.001
```

- Op de opdrachtoutput van ntpq, als u ziet dat de waarde van st (stratum) 16 is, geeft dit aan dat de tijdserver onbereikbaar is en dat het apparaat niet kan synchroniseren met die tijdserver.
- Op de ntpq opdrachtoutput toont reach een octale waarde die het succes of falen van het bereiken van de bron voor de meest recente acht opiniepeilingen aangeeft. Als je ziet dat de waarde 377 is, betekent dit dat de laatste 8 pogingen succesvol waren. Elke andere waarde kan aangeven dat een of meer van

de laatste acht pogingen niet succesvol waren.

## Stap 3: Controleer de connectiviteit

1. Controleer de basisverbinding met de tijdserver.
   <#root>

   ```
   admin@FireSIGHT:~$
   ```

   **ping**

2. Zorg ervoor dat poort 123 open is op uw FireSIGHT-systeem.
   <#root>

   ```
   admin@FireSIGHT:~$
   ```

   **netstat -an | grep 123**

3. Bevestig dat poort 123 is geopend op de firewall.
4. Controleer de hardwareklok:
   <#root>

   ```
   admin@FireSIGHT:~$
   ```

   **sudo hwclock**

   Als de hardwareklok te ver verouderd is, kan deze nooit met succes worden gesynchroniseerd. Voer deze opdracht in om handmatig te forceren dat de kloktijd wordt ingesteld met een tijdserver:

   <#root>

   ```
   admin@FireSIGHT:~$
   ```

   **sudo ntpdate -u**

   Vervolgens opnieuw starten ntpd:

   <#root>

   ```
   admin@FireSIGHT:~$
   ```

   **sudo pmtool restartbyid ntpd**

## Stap 4: Controleer de configuratiebestanden

1. Controleer of het bestand sfipproxy.conf correct is ingevuld. Dit bestand verstuurt NTP-verkeer via de sftunnel.

   Een voorbeeld van het bestand /etc/sf/sfipproxy.conf op een beheerd apparaat wordt hier weergegeven:

   <#root>

   ```
   admin@FirePOWER:~$
   ```

   **sudo cat /etc/sf/sfipproxy.conf**

   ```
   config
   {
       nodaemon 1;
   }
   peers
   {
       dbef067c-4d5b-11e4-a08b-b3f170684648
       {
           services
           {
               ntp
               {
                   listen_ip 127.0.0.2;
                   listen_port 123;
                   protocol udp;
                   timeout 20;
               }
           }
       }
   }
   ```

   Een voorbeeld van het /etc/sf/sfipproxy.conf-bestand op een FireSIGHT Management Center wordt hier weergegeven:

   <#root>

   ```
   admin@FireSIGHT:~$
   ```

   **sudo cat /etc/sf/sfipproxy.conf**

   ```
   config
   {
       nodaemon 1;
   ```

```
}
peers
{
    854178f4-4eec-11e4-99ed-8b16d263763e
    {
        services
        {
            ntp
            {
                protocol udp;
                server_ip 127.0.0.1;
                server_port 123;
                timeout 10;
            }
        }
    }
}
```

2. Zorg ervoor dat de Universally Unique Identifier (UUID) onder de peers sectie overeenkomt met het ims.conf bestand van de peer. Bijvoorbeeld, de UUID gevonden onder de peers sectie van het /etc/sf/sfipproxy.conf bestand op een FireSIGHT Management Center moet overeenkomen met de UUID gevonden op het /etc/ims.conf bestand van zijn beheerde apparaat. Op dezelfde manier moet de UUID die onder de peers sectie van het /etc/sf/sfipproxy.conf-bestand op een beheerd apparaat wordt gevonden overeenkomen met de UUID die in het /etc/ims.conf-bestand van het beheerapparaat wordt gevonden.

   U kunt de UUID van de apparaten met deze opdracht ophalen:

   <#root>

   admin@FireSIGHT:~$

   **sudo grep UUID /etc/sf/ims.conf**

   APPLIANCE_UUID=dbef067c-4d5b-11e4-a08b-b3f170684648

   Deze moeten normaliter automatisch worden ingevuld door het systeembeleid, maar er zijn gevallen geweest waarin deze stagnaties verloren zijn gegaan. Als ze moeten worden aangepast of gewijzigd moet u opnieuw starten sfipproxy en sftunnel zoals te zien in dit voorbeeld:

   <#root>

   admin@FireSIGHT:~$

   **sudo pmtool restartbyid sfipproxy**

   admin@FireSIGHT:~$

   **sudo pmtool restartbyid sftunnel**

3. Controleer of een ntp.conf bestand beschikbaar is in de map /etc.
   <#root>

```
admin@FireSIGHT:~$
ls /etc/ntp.conf*
```

Als er geen NTP-configuratiebestand beschikbaar is, kunt u een kopie maken van het back-upconfiguratiebestand. Voorbeeld:

```
<#root>
admin@FireSIGHT:~$
sudo cp /etc/ntp.conf.bak /etc/ntp.conf
```

4. Controleer of het /etc/ntp.conf bestand goed is ingevuld. Wanneer u een systeembeleid toepast, wordt het ntp.conf-bestand herschreven.

---

**Opmerking**: De uitvoer van een ntp.conf bestand toont de instellingen van de tijdserver die zijn ingesteld op een systeembeleid. De tijdstempel moet het tijdstip aangeven waarop het laatste systeembeleid op een apparaat is toegepast. De server moet het opgegeven adres van de tijdserver tonen.

---

```
<#root>
admin@FireSIGHT:~$
sudo cat /etc/ntp.conf

# automatically generated by /etc/sysconfig/configure-network ; do not edit
# Tue Oct 21 17:44:03 UTC 2014

restrict default noquery nomodify notrap nopeer
restrict 127.0.0.1
server 198.51.100.2
logfile /var/log/ntp.log
driftfile /etc/ntp.drift
```

Controleer NTP versies op twee apparaten en zorg dat het hetzelfde is.

Zie Best Practices for Network Time Protocol voor meer informatie over de basisprincipes van NTP.

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.