

# Probleemoplossing voor IoX-sensoren bij implementatie van Cyber Vision

## Inhoud

[Inleiding](#)

[Aansluiten op de sensor CLI](#)

[Belangrijke directory's](#)

[Config.yml](#)

[PCAP-opnamen](#)

[Bestanden ophalen uit de IoX-sensor](#)

[GUI voor Local Manager](#)

[Bestanden kopiëren via TFTP](#)

[Sensorstatus](#)

[Status](#)

[Verwerkingsstatus](#)

[Kritieke informatie in het diagrambestand](#)

## Inleiding

In dit document worden de basisgegevens beschreven die nodig zijn voor probleemoplossing bij het werken met de IoX Sensor op Cyber Vision-oplossing.

### Aansluiten op de sensor CLI

Sensortoepassingen zijn niet rechtstreeks toegankelijk. Eerst, moet met de switch door SSH verbinden. Dan, gebruik het showbevel om van de toepassing een lijst te maken die op het loopt.

```
Show app-hosting list
```

Valideren als de toepassing is geïnstalleerd en de naam ervan documenteren. Type (waar 'ccv\_sensor\_iox\_aarch64' de app naam is in dit voorbeeld)

```
app-hosting connect appid ccv_sensor_iox_aarch64 session
```

### Belangrijke directory's

#### Config.yml

Het is een belangrijk configuratiebestand dat de documentdoorstroming, het protocol en de instellingen voor poortinformatie documenteert. Het bestand is te vinden onder:

/iox\_data/etc/flow

## **PCAP-opnamen**

De opnamen die worden uitgevoerd en geactiveerd vanuit de GUI vallen onder

/iox\_data/var/flow/log/pcap

## **Bestanden ophalen uit de IoX-sensor**

### **GUI voor Local Manager**

Ga vanuit de GUI van de lokale beheerder naar de app en het tabblad 'App-DataDir' toont de bestanden in de map /iox\_data/appdata

Het tabblad 'Logs' onder de app toont de bestanden in /iox\_data/logs.

### **Bestanden kopiëren via TFTP**

Vanuit de CLI van de sensor kunnen bestanden worden gekopieerd naar een externe TFTP-server met behulp van de onderstaande opdracht:

```
tftp -p -l /iox_data/appdata/
```

-I

## **Sensorstatus**

Navigeer vanuit de Center GUI naar Beheer ' Sensoren ' Beheer om de Sensor details te bekijken. Dit zijn de connectie- en verwerkingsstatussen die beschikbaar zijn

## **Status**

- Nieuw
- Aanvraag in behandeling
- geautoriseerd
- Niet verbonden
- Verbonden -
- Onbekend
- SSH

## **Verwerkingsstatus**

- Niet ingeschreven
- Niet verbonden
- Wachten op gegevens
- Gegevens in behandeling
  
- Normaal verwerken

## **Kritieke informatie in het diagrambestand**

Datum - Rapporteer het tijdstip waarop de diagnostiek is uitgevoerd

IP\_addr - Rapporteer het IP-adres en de netwerkinformatie van alle geconfigureerde interfaces.

IP\_route - Rapporteer de geconfigureerde gateway

Journal\_error - meldt de diensten die niet zijn gestart

Journal\_sensorsyncd - rapporteert de TLC-verbindinginformatie

Geheugen - Geeft de hoeveelheid geheugen aan die in gebruik is

SBS-versie - Rapporteer de hoofdversie en de compilatiedatum

sensor-enroll.conf - Rapporteer het IP dat is geconfigureerd op het Inschrijfpakket

top - Rapporteer 4 "top"-opdrachten binnen 12 seconden, gesorteerd op CPU

## 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.