

Erläuterung der Anmeldung bei der Sensor-CLI für Cyber Vision

Inhalt

[Einleitung](#)

[Hardwaresensor - IC3000](#)

[Vor Cyber Vision Version 4.3.0](#)

[Cyber Vision 4.3.0 Version ab](#)

[Netzwerksensoren](#)

Einleitung

In diesem Dokument wird das Anmeldeverfahren der Sensor-CLI für Netzwerk- und Hardware Sensoren von Cisco Cyber Vision beschrieben.

Hardwaresensor - IC3000

Vor Cyber Vision Version 4.3.0



Hinweis: Vor der Einführung von Cyber Vision Version 4.3.0 wurde der IC3000-Sensor als virtuelles System im lokalen Manager von Cisco IOx (Cisco IOs + LinuxX) als End-to-End-Anwendungs-Framework bereitgestellt, das Funktionen zum Hosten von Anwendungen für verschiedene Anwendungstypen auf Cisco Netzwerkplattformen bereitstellt.

Melden Sie sich als Administrator-Benutzer bei der lokalen IC3000-Verwaltungsoberfläche (https://ip_address:8443) an, navigieren Sie zu den Anwendungen, und klicken Sie dann auf die Option Manage App (App verwalten).

Applications

App Groups

Remote Docker Workflow

Docker Layers

Cisco_Cyber_Vision

RUNNING

Cyber Vision Sensor Image for IC3000

TYPE
vm

VERSION
4.2.4+202308232047

PROFILE
custom

Memory *

90.0%

CPU *

100.0%

■ Stop

⚙ Manage

Wählen Sie das Menü App-info aus, und klicken Sie auf die Option Cisco_Cyber_Vision.pem, die im Abschnitt App Access (App-Zugriff) angezeigt wird:

Application information	
ID:	Cisco_Cyber_Vision
State:	RUNNING
Name:	Cisco Cyber Vision
Cartridge Required:	<ul style="list-style-type: none">• None
Version:	4.2.4+202308232047
Author:	Cisco
Author link:	
Application type:	vm
Description:	Cyber Vision Sensor Image for IC3000
Debug mode:	false

App Access	
Console Access	<code>ssh -p {SSH_PORT} -i Cisco_Cyber_Vision.pem appconsole@10.106.13.143</code>

Kopieren Sie den in der Datei `Cisco_Cyber_Vision.pem` vorhandenen Rivest-Shamir-Addleman (RSA)-Schlüssel.

Melden Sie sich jetzt bei der Cyber Vision Center-CLI an, und erstellen Sie eine neue Datei mit dem RSA-Schlüsselinhalt in der Datei.

Mit einem beliebigen Linux-Editor erstellt beispielsweise vi-Editor (visueller Editor) eine Datei und fügt den Inhalt der RSA-Schlüsseldatei in diese Datei ein (`Cisco_Cyber_Vision.pem` ist der Dateiname in diesem Beispiel).

```
cv-admin@Center-4:~$  
cv-admin@Center-4:~$ sudo su -  
root@Center-4:~#  
root@Center-4:~# vi Cisco_cyber_Vision.pem  
root@Center-4:~#  
root@Center-4:~# chmod 400 Cisco_cyber_Vision.pem  
root@Center-4:~#
```

Beschränken Sie die Berechtigungen für die Datei Cisco_Cyber_Vision.pem mit dem Befehl `chmod 400`.

Der Zugriff auf die IC3000 Sensorkonsole ist jetzt über folgende Funktionen möglich:

```
ssh -p {SSH_PORT} -i file_name appconsole@LocalManagerIP
```

Beispiel: Wenn der Secure Shell (SSH)-Port, der in der Konfiguration konfiguriert wurde, 22 ist, Cisco_Cyber_Vision.pem der Dateiname ist und Local Manager IP address (LMIP) die IP-Adresse von LocalManager, dann ist das Ergebnis `ssh -p 22 -i Cisco_Cyber_Vision.pem appconsole@LMIP`.



Hinweis: Das IC3000-Zertifikat ändert sich bei jedem Neustart des Switches. Daher muss dieser Vorgang wiederholt werden.

Cyber Vision 4.3.0 Version ab

Die Sensoranwendung Cisco Cyber Vision für das IC3000-Format wurde in Version 4.3.0 von VM in Docker geändert. Weitere Einzelheiten zu diesem Paket finden Sie unter [Cisco-Cyber-Vision Release-Notes-4-3-0.pdf](#).

Melden Sie sich als Administrator-Benutzer bei der lokalen IC3000-Verwaltungsoberfläche (https://ip_address:8443) an, navigieren Sie zu den Anwendungen, und klicken Sie dann auf die Option **Manage App** (App **verwalten**).

Applications App Groups Remote Docker Workflow Docker Layers

ccv_sensor_iox_activ... RUNNING

Cisco Cyber Vision sensor with Active Discovery for IC...

TYPE	VERSION	PROFILE
docker	4.3.0-202311161552	exclusive

Memory * 100.0%

CPU * 100.0%

■ Stop⚙ Manage

Navigieren Sie anschließend zur Registerkarte App-Console, um auf die Sensoranwendung zuzugreifen.

ns App Groups Remote Docker Workflow Docker Layers System Info System Setting System Troubleshoot

Resources **App-Console** App-Config App-info App-DataDir Logs

>_ Command Disconnect

```
sh-5.0#  
sh-5.0#  
sh-5.0#  
sh-5.0#  
sh-5.0#
```

Netzwerksensoren

Melden Sie sich bei der entsprechenden Switch-CLI an, und kopieren Sie die Sensor-Anwendungs-ID mithilfe des folgenden Befehls:

```
show app-hosting list
```

```
C9300L-24P-4G#sh app-hosting list
```

```
App id
```

```
State
```

```
-----  
ccv_sensor_iox_x86_64
```

```
RUNNING
```

Melden Sie sich bei der Sensoranwendung an, indem Sie:

```
app-hosting connect appid sensor_app_name session
```

In diesem Fall ist es zum Beispiel **app-hosting connect appid ccv_sensor_iox_x86_64 session**.

```
C9300L-24P-4G#app-hosting connect appid ccv_sensor_iox_x86_64 session
```

```
sh-5.0#
```

```
sh-5.0#
```

```
sh-5.0#
```

Die in der Screenshot-Funktion angezeigte Eingabeaufforderung bestätigt, dass die Anmeldung am Sensor erfolgreich war.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.