

# Entender o procedimento de login do sensor CLI para o Cyber Vision

## Contents

---

[Introdução](#)

[Sensor de hardware - IC3000](#)

[Antes do Cyber Vision Versão 4.3.0](#)

[Cyber Vision 4.3.0 Versão posterior](#)

[Sensores de rede](#)

---

## Introdução

Este documento descreve o procedimento de login do Sensor CLI para sensores de rede e de hardware do Cisco Cyber Vision.

## Sensor de hardware - IC3000

Antes do Cyber Vision Versão 4.3.0



Observação: antes do Cyber Vision versão 4.3.0, o sensor IC3000 era implantado como uma máquina virtual (VM) no Cisco IOx (Cisco IOSs + linux) é uma estrutura de aplicação completa que fornece recursos de hospedagem de aplicações para diferentes tipos de aplicações em plataformas de rede da Cisco) gerenciador local.

---

Faça login na interface do gerenciador local do IC3000 ([https://ip\\_address:8443](https://ip_address:8443)) como um usuário administrador, navegue para aplicativos e clique na opção gerenciar aplicativo.

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

Escolha o menu App-info e clique na opção Cisco\_Cyber\_Vision.pem presente na seção Acesso ao aplicativo como mostrado:

Application information	
ID:	Cisco_Cyber_Vision
State:	RUNNING
Name:	Cisco Cyber Vision
Cartridge Required:	<ul style="list-style-type: none"><li>None</li></ul>
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 <a href="#">Cisco_Cyber_Vision.pem</a> appconsole@10.106.13.143</code>

Copie a chave RSA (Rivest-Shamir-Addleman) presente no arquivo `Cisco_Cyber_Vision.pem`. Agora, faça login na CLI do Cyber Vision Center e crie um novo arquivo com o conteúdo-chave da RSA no arquivo.

Usando qualquer editor Linux, por exemplo, o editor vi (editor visual) cria um arquivo e cola o conteúdo do arquivo de chave RSA nesse arquivo (`Cisco_Cyber_Vision.pem` é o nome do arquivo neste exemplo).

```
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:~#
```

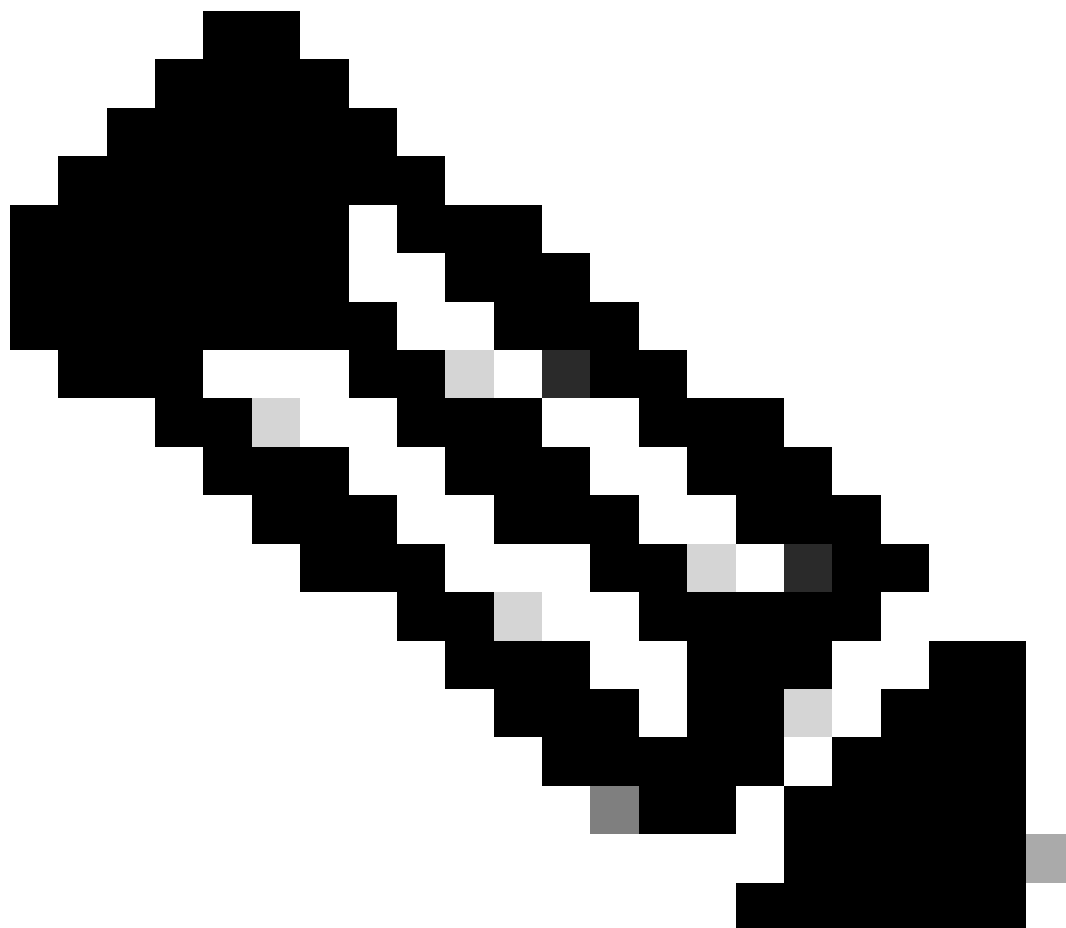
Restrinja as permissões para o arquivo Cisco\_Cyber\_Vision.pem, usando o comando chmod 400. Agora, o console do sensor IC3000 pode ser acessado usando:

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

Por exemplo, se a porta Secure Shell (SSH) configurada na configuração for 22, Cisco\_Cyber\_Vision.pem será o nome do arquivo e o endereço IP do Gerenciador Local (LMIP) será o endereço IP do LocalManager, então o resultado será `ssh -p 22 -`

```
i Cisco_Cyber_Vision.pem appconsole@LMIP.
```

---



**Observação:** o certificado IC3000 é alterado sempre que o switch é reinicializado e, portanto, esse procedimento precisa ser repetido.

---

Cyber Vision 4.3.0 Versão posterior

O aplicativo de sensor Cisco Cyber Vision para o formato IC3000 mudou de VM para Docker na versão 4.3.0. Para obter mais detalhes sobre o mesmo, consulte [Cisco-Cyber-Vision Release-Notes-4-3-0.pdf](#).

Faça login na interface do gerenciador local do IC3000 ([https://ip\\_address:8443](https://ip_address:8443)) como um usuário administrador, navegue para aplicativos e clique na opção **gerenciar** aplicativo.

**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

Em seguida, navegue até a guia App-Console para acessar o aplicativo sensor.

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#
```

Sensores de rede

Faça login no respectivo CLI do switch e copie o ID do aplicativo do sensor usando este comando:

```
show app-hosting list
```

```
C9300L-24P-4G#sh app-hosting list
App id                               State
-----
ccv_sensor_iox_x86_64                RUNNING
```

Faça login no aplicativo sensor usando:

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

Por exemplo, neste caso, é **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#
```

O prompt mostrado na captura de tela confirma que o login do sensor foi bem-sucedido.

## Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.