



Cyber Vision Center

- [Cyber Vision のサポート \(1 ページ\)](#)
- [LM GUI を使用した CVC センサーのインストール \(8 ページ\)](#)

Cyber Vision のサポート

Cisco Cyber Vision Center (CVC) は、制御ネットワークとデータネットワークをリアルタイムでモニタすることにより、産業用制御システム (ICS) 全体の産業用 IoT ネットワークの可視性を高めます。リリース 17.4 以降の IoT IOS-XE プラットフォームでは、IOX Cyber Vision センサーを展開することで CVC の統合がサポートされます。このセンサーを IoT ルータに展開すると、プラットフォームは IOX アプリケーションからのトラフィックを Cyber Vision Center に転送してリアルタイムでモニタし、キャプチャした PCAP ファイルを IOX アプリケーションから Vision Center に転送できます。

IOS-XE プラットフォームでの Cyber Vision Center (CVC) の展開

ステップ 1 次の場所から、シスコがサポートしている Cyber Vision IOX アプリケーションをダウンロードします。

<https://software.cisco.com/download/home/286325414/type/286325316/release/3.1.1?catid=268438162>

Cisco Cyber Vision Sensor IOx Application 3.1.1 for IE3400 and IR1101 を選択します。

ステップ 2 仮想マシンまたは任意のハイパーバイザに CVC バージョン 3.1.1 をインストールします。次の場所は、さまざまなバージョンの CVC のダウンロードリンクです。

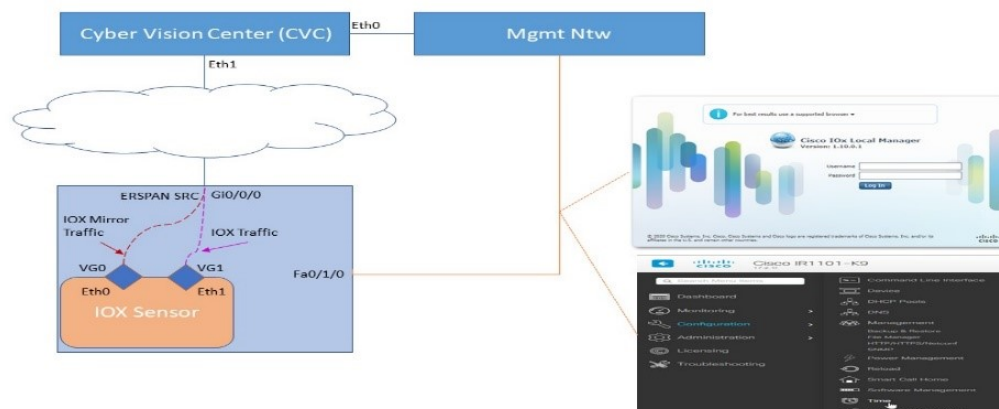
<https://software.cisco.com/download/home/286325414/type>

Cisco Cyber Vision リリース 3.1.1 のリリースノート :

https://www.cisco.com/c/dam/en/us/td/docs/security/cyber_vision/Cisco-Cyber-Vision_Release-Note-3-1-1.pdf

ステップ 3 CVC センサーには 2 つの VirtualPort Group インターフェイスが必要です。一つは IOx トラフィック用であり、もう一つは物理インターフェイス、SVI、トンネルインターフェイス等の ERSPAN ソースでミラーされたトラフィック用です。次の図を参照してください。

図 1: L3 インターフェイスを介した CVC



ステップ 4 CVC センサーの展開は、LMGUI または CLI からインストールできます。

L3 設定を介した ERSPAN と仮想ポートグループの設定例

物理ポートと仮想ポートの設定 :

```
interface virtualportgroup 0
ip address 169.254.1.1 255.255.255.252
interface virtualportgroup 1
ip nat inside
ip address 169.254.0.1 255.255.255.252
interface gi0/0/0
ip address 101.0.0.151 255.255.255.0
ip nat outside
no shut
```

ERSPAN 設定 :

```
monitor session 1 type erspan-source
source interface Gi0/0/0
no shutdown
destination
erspan-id 1
mtu 1464
ip address 169.254.1.2
origin ip address 169.254.1.1
```

アクセスリストを使用した NAT 設定 :

```
ip nat inside source list NAT_ACL interface Gi0/0/0 overload
ip access-list standard NAT_ACL
10 permit 169.254.0.0 0.0.0.3
```

CLIからのインストール

CLIを使用してアプリケーションをインストールするには、CVCセンサーをブートフラッシュ、USB、または mSATA にコピーします。次に、アプリケーションホスティング CLI を使用してアプリケーションをインストールし、Docker オプションを指定してからアプリケーションをアクティブ化します。

次に例を示します。

```
Router (config-if) #iox
Router# app-hosting install app-id <app-id> package {bootflash:|usbflash0:|msata:}
app-hosting appid <app-id>
app-vnic gateway0 virtualportgroup 0 guest-interface 0
  guest-ipaddress 169.254.1.2 netmask 255.255.255.252
app-vnic gateway1 virtualportgroup 1 guest-interface 1
  guest-ipaddress 169.254.0.2 netmask 255.255.255.252
app-default-gateway 169.254.0.1 guest-interface 1
app-resource docker
run-opts 1 "--rm --tmpfs /tmp:rw,size=128m"
Router# app-hosting {activate|start|stop|deactivate|uninstall} app-id <app-id>
```

LMGUIからのインストール

LMGUI に到達するには、次を設定します。

```
iox
ip http server
ip http secure-server
ip http authentication local
Username cisco privilege 15 password cisco
Login URL: http://<Mgmt_IP>/iox/login
```

その他の詳細については、次を参照してください。 [LM GUI を使用した CVC センサーのインストール \(8 ページ\)](#)

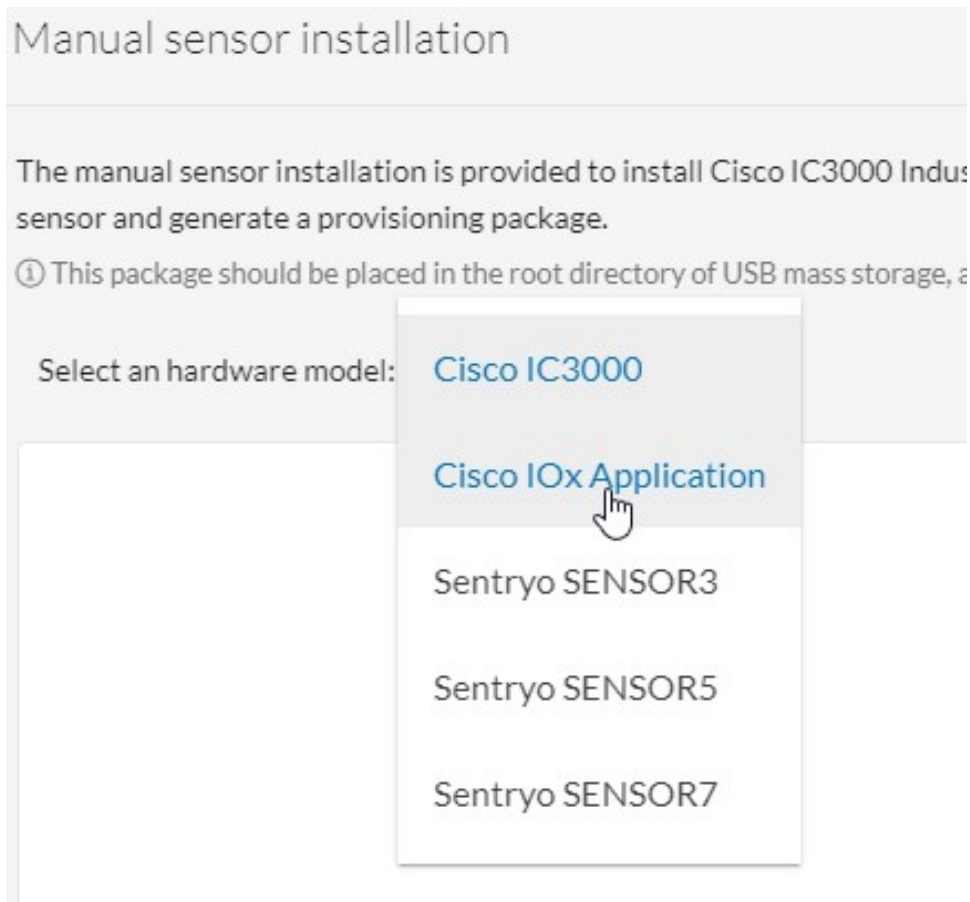
ルータ詳細の登録

ステップ 1 ログインして次の場所に移動し、CVC に IOS-XE ルータの詳細を登録します。

Admin > Sensors > Install Sensor Manually

次に、[Cisco IOx Application] をクリックします。次を参照してください。

図 2: センサーのインストール



ステップ 2 ルータのシリアル番号を入力します。 **show inventory** の出力と完全に一致する必要があります。次に [**Create Sensor**] をクリックします。次を参照してください。

図 3: ルータのシリアル番号

Manual sensor installation

The manual sensor installation is provided to install Cisco IC3000 Industrial Compute Gateway and sensors that are not allowed to access the Center's DHCP server for automatic configuration. Please fill the fields below to configure your sensor and generate a provisioning package.
 ⓐ This package should be placed in the root directory of USB mass storage, and plugged in the IC3000 / Sensor before powering it up.

Select an hardware model: Cisco IOx Application

Sensor configuration

Serial number: *
 Sensor's serial number as printed on the side panel
 FCW23500HDC

Center IP:
 Optional, leave blank to use current Center IP address

Gateway:
 Optional

Capture mode:
 Optional

All: analyze all the flows
 Optimal (Default): analyze the most relevant flows
 Industrial only: analyze industrial flows
 Custom: you set your filter using a packet filter in tcpdump-compatible syntax

Create Sensor Cancel

ステップ 3 [Get Provisioning File] をクリックして、CVC からプロビジョニングファイルを生成します。次を参照してください。

図 4: プロビジョニングファイルの生成

▼ FCW23500HDC	N/A	N/A	New	SSH
---------------	-----	-----	-----	-----

S/N: FCW23500HDC
 Name: FCW23500HDC ✎
 Status: New
 Processing status: Not enrolled
 Capture mode: All

ステップ 4 ローカルディレクトリにプロビジョニングファイルをダウンロードします。ファイルは次のようなファイル名の zip ファイルとして提供されます。

例 :

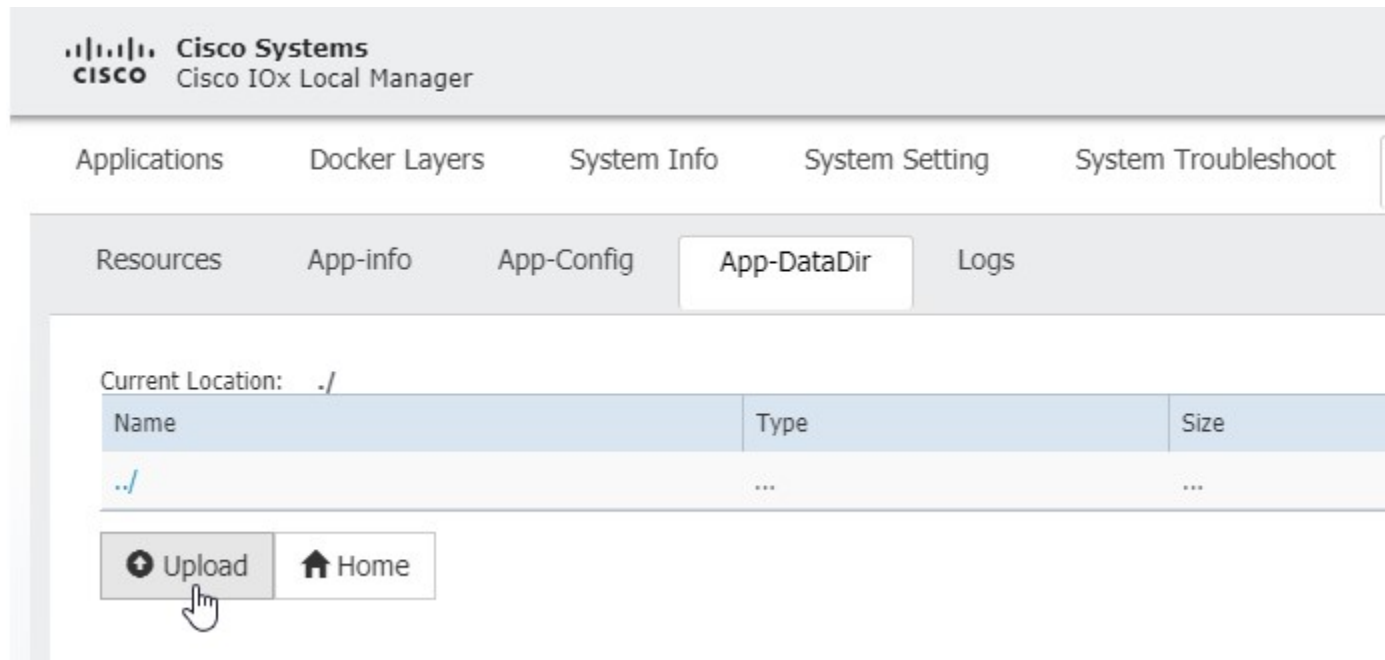
sbs-sensor-config-*<S/N of Router>*.zip

ステップ 5 LMGUI を使用して、プロビジョニングファイルをルータにインポートします。LMGUI アプリケーションから次の場所に移動します。

Applications > CVC App (Application Name) > Manage > App-DataDir

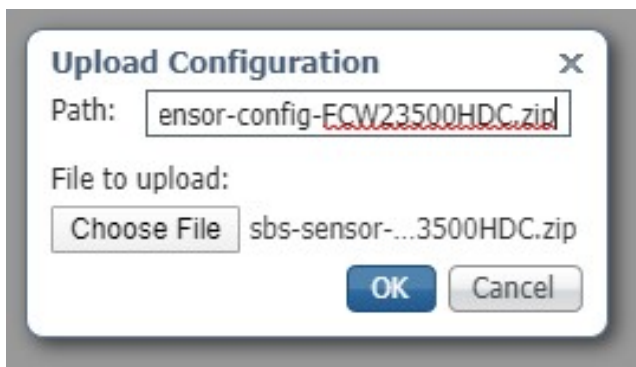
次を参照してください。

図 5: プロビジョニングファイルのアップロード



ステップ 6 [Upload] をクリックします。[Upload Configuration] ウィンドウが表示されます。ダウンロードしたプロビジョニング済みのファイルと同じ名前で CVC からアップロードします。次を参照してください。



図 6: アップロード設定



ステップ 7 CVC の認証を確認します。インストールされているセンサーのステータスが **Connected** または **Waiting for Data** に変更されたかどうかを検証します。次を参照してください。

図 7: Sensor Status

▼ FCW23500HDC	169.254.0.2	3.1.0+202004150634	Connected
---------------	-------------	--------------------	-----------

S/N: FCW23500HDC
 Name: FCW23500HDC 
 IP address: 169.254.0.2
 Version: 3.1.0+202004150634
 Status: Connected
 Processing status: Normally processing
 Uptime: 3h 3s
 Capture mode: All
 Start recording sensor
 Download (empty file)
 Go to statistics

ライブトラフィックのキャプチャ

ステップ 1 CVC とルータ間で日時を同期します。ライブトラフィックをキャプチャするには、ルータと CVC の間に正確なクロック同期が必要です。

ステップ 2 IOX トラフィックをシミュレートするか、またはキャプチャされた PCAP ファイルを再生します。ルータにインストールされている CVC センサーは Docker アプリです。アプリのコンソールにログインするには、次のコマンドを実行します。

例 :

```
app-hosting connect app-id <app-name> session
```

ステップ 3 LM-GUI から PCAP ファイルをアプリケーションにアップロードします。次のとおりに移動します。

Applications > CVC App (Application Name) > Manage > App-Dir

次のコマンドは、PCAP ファイルの再生方法を示しています。

例 :

```
Router# show app-hosting list
App id      State
-----
CVC Sensor  RUNNING
```

```

Router# app-hosting connect appid CVCsensor session
sh-5.0#
*Jul 14 08:45:05.603: %SELINUX-3-MISMATCH: R0/0: audispd: type=AVC msg=audit(15! in/busybox.nosuid"
  dev="overlay" ino=72930 scontext=system_u:system_r: polaris_bexecute_*
sh-5.0# flowctl read-capture-file /iox_data/appdata/t104
OK
sh-5.0#

```

ステップ 4 CVC のトラフィックをモニタします。次の場所に移動します。 **Explore > Essential Data > Activity List**
 次を参照してください。

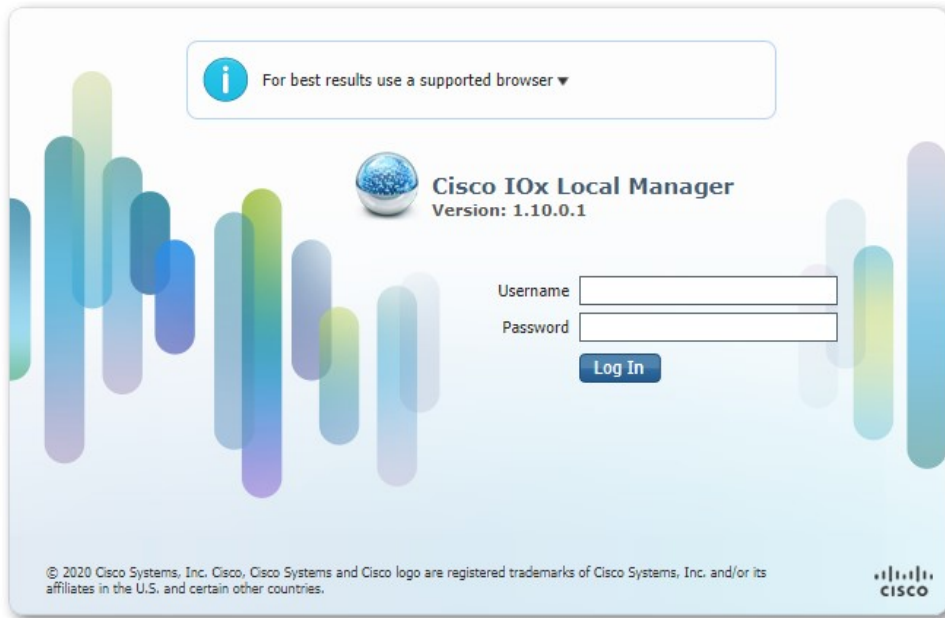
図 8: Activity List

Component	Component	First activity	Last activity	Tags
169.254.1.2	Cisco 169.254.1.1	Sep 12, 2020 3:00:29 PM	Sep 24, 2020 1:26:33 PM	Tunneling, ARP
105.0.0.1	101.0.0.151	Sep 14, 2020 7:44:21 AM	Sep 24, 2020 1:26:33 PM	Unestablished, Ping, Web, ARP
101.0.0.3	255.255.255.255	Jul 14, 2020 12:59:47 AM	Sep 24, 2020 1:25:51 PM	Time Management, Broadcast
SIT-DC	101.0.0.255	Jul 14, 2020 1:07:50 AM	Sep 24, 2020 1:22:02 PM	Insecure, Broadcast, Netbios, SMB

LM GUI を使用した CVC センサーのインストール

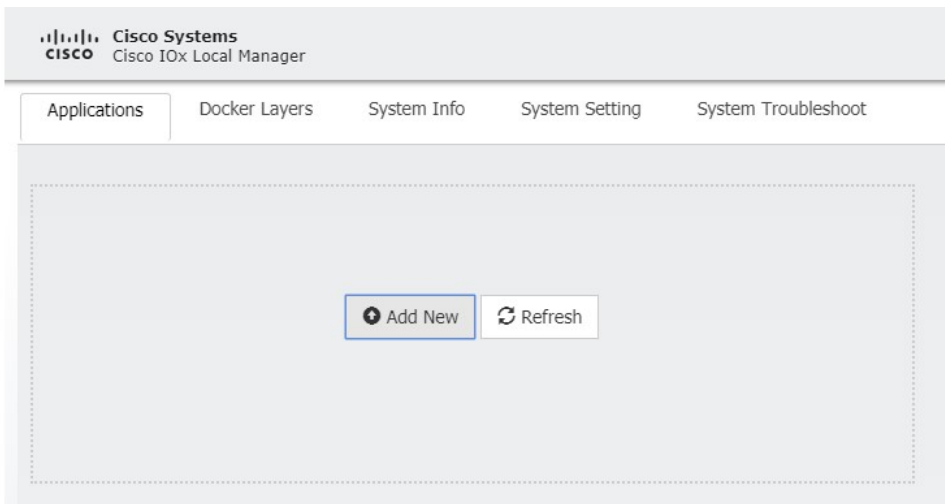
ステップ 1 ユーザアカウントとパスワードを使用してログインします。

図 9: ローカルマネージャのログイン



ステップ 2 センサー仮想アプリケーションをインストールします。ログインすると、次のメニューが表示されます。

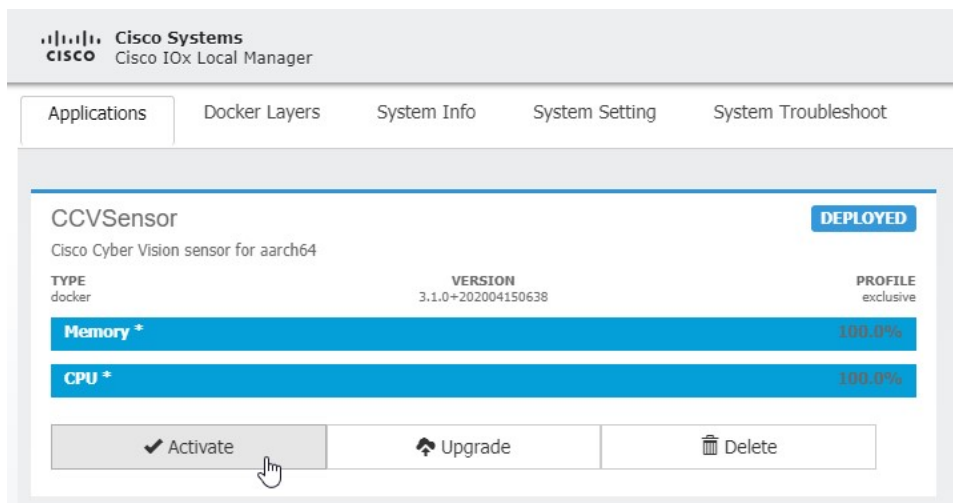
図 10: LM GUI アプリケーションのインストール



ステップ 3 [Add New] をクリックします。アプリケーションファイル（CiscoCyberVision-IOx-aarch64-xxx.tar など）に移動します。アプリケーションの名前（CCVSensor など）を追加します。

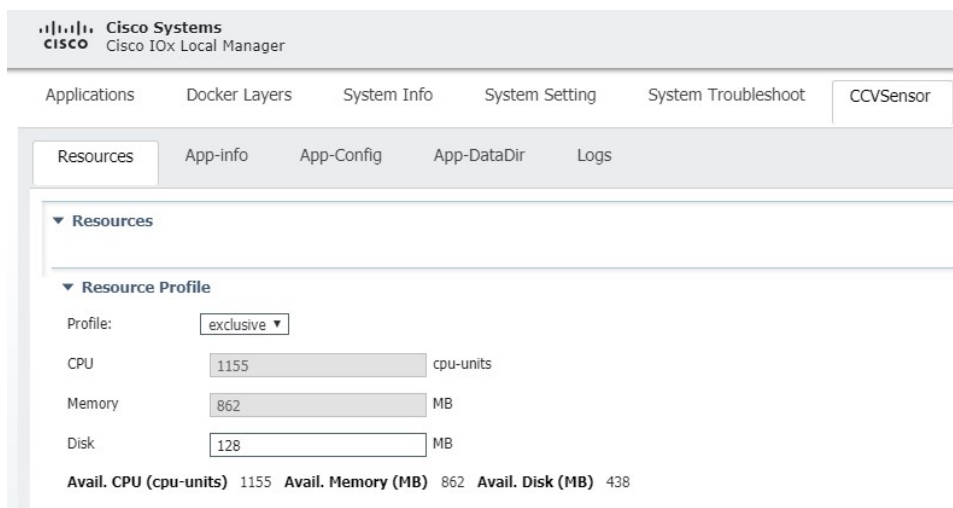
センサー仮想アプリケーションを設定します。次を参照してください。

図 11: CCVSensor のアクティブ化



ステップ 4 **Activate** をクリックして、センサーアプリケーションの設定を起動します。[CCVSensor] タブをクリックし、[Resources] をクリックします。次を参照してください。

図 12: センサー LM IOXAppDisk のセットアップ



ディスクサイズを 128 MB に変更します。

(注) それ以上の領域を使用しないでください。

ステップ 5 **Advanced Settings** にアクセスします。詳細オプションで、[Docked Options] の横にあるテキスト領域に次を追加して、tmpfs を設定します。

```
--tmpfs /tmp:rw,size=128m
```

図 13: Advanced Settings

▼ Resource Profile

Profile:

CPU: cpu-units

Memory: MB

Disk: MB

Avail. CPU (cpu-units) 1155 Avail. Memory (MB) 862 Avail. Disk (MB) 438

▼ Advanced Settings

Specify "docker run" options to be used while spawning the container. These will override activation settings above.

Docker Options:

Auto delete container instance

ステップ 6 Network Configuration セクション内のホスト上のインターフェイスにコンテナ内のインターフェイスをバインドします。

次のタスク

次のセクション（Binding eth0 と Binding eth1）に移動します。

eth0 のバインディング

eth0 を設定するには、次の手順を実行します。

ステップ 1 interface eth0 を選択し、[edit] をクリックします。

図 14: eth0

Name	Network Config	Description	Action
eth0	VPG0	none	edit
eth1	Not Configured	none	edit

ステップ 2 インターフェイス **VPG1** を選択します。

図 15: VPG1

▼ Network Configuration	
Name	Network Config
eth0	VPG0
eth1	Not Configured

eth0

Description (optional):

VPG1 VirtualPortGroup via intsv1 [Interface Setting](#)

VPG0 VirtualPortGroup via intsvc0

VPG1 VirtualPortGroup via intsvc1

✓ OK ✕ Cancel

ステップ 3 **[Interface Setting]** をクリックします。

図 16: インターフェイスの設定

▼ Network Configuration	
Name	Network Config
eth0	VPG0
eth1	Not Configured

eth0

VPG1 VirtualPortGroup via intsv1 [Interface Setting](#)

Description (optional):

✓ OK ✕ Cancel

ステップ 4 次の設定を適用します。

- **Static** オプションを選択します。
- IP/Mask で次を追加 **169.254.0.2 / 30**
- デフォルトゲートウェイの IP は **169.254.0.1**

次に **[OK]** をクリックします。

図 17: IPv4 設定

ステップ 5 もう一度 [OK] をクリックします。

Name	Network Config
eth0	VPG0
eth1	Not Configured

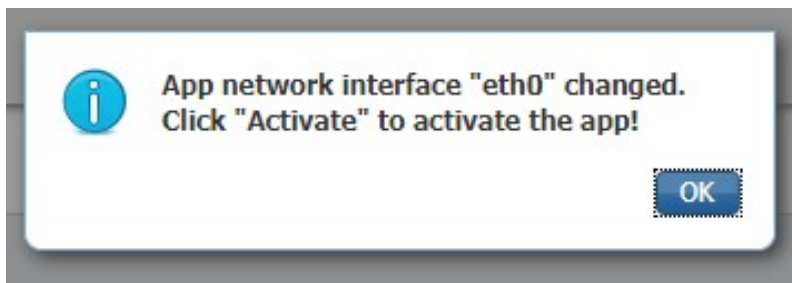
eth0 VPG0 VirtualPortGroup via intsr [Interface Setting](#)

Description (optional):

✓ OK ✗ Cancel

ステップ 6 [Activate (SIP MWI notification mechanism)] ウィンドウが表示されます。[OK] をクリックします。

図 18: ウィンドウのアクティブ化



eth1 のバインディング

eth1 インターフェイスを設定するには、次の手順を実行します。

ステップ1 VPG0 を選択します。

図 19: VPG0

The screenshot shows a 'Network Configuration' dialog box. It contains a table with the following data:

Name	Network Config
eth0	VPG1
eth1	Not Configured

Below the table, the 'eth1' interface is selected, and the 'VPG0 VirtualPortGroup via ints' dropdown menu is open. The 'Interface Setting' link is visible. Below this, there is a 'Description (optional):' text box. At the bottom, there are 'OK' and 'Cancel' buttons.

ステップ2 **Interface Setting** をクリックして、次の設定を適用します。

- **Static** オプションを選択します。
- IP/Mask で次を追加 **169.254.1.2 / 30**

図 20: IPv4 設定

Interface Setting

IPv4 Setting

Static Dynamic Disable

IP/Mask	169.254.1.2 / 30
DNS	
Default Gateway IP	

アプリケーションのアクティブ化

これで、センサーアプリケーションがアクティブになります。

ステップ 1 [Activate App] をクリックします。次を参照してください。

図 21: アプリケーションのアクティブ化

✓ Activate App

▼ Network Configuration

Name	Network Config	Description	Action
eth0	VPG1	none	edit
eth1	VPG0	none	edit

➡ Add App Network Interface

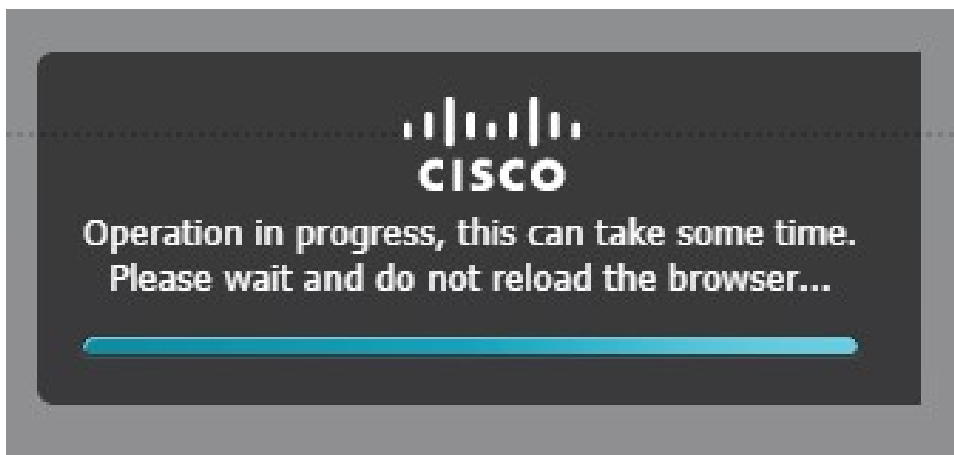
▼ Peripheral Configuration

Device Type	Name	Label	Status	Action
-------------	------	-------	--------	--------

➡ Add Peripheral

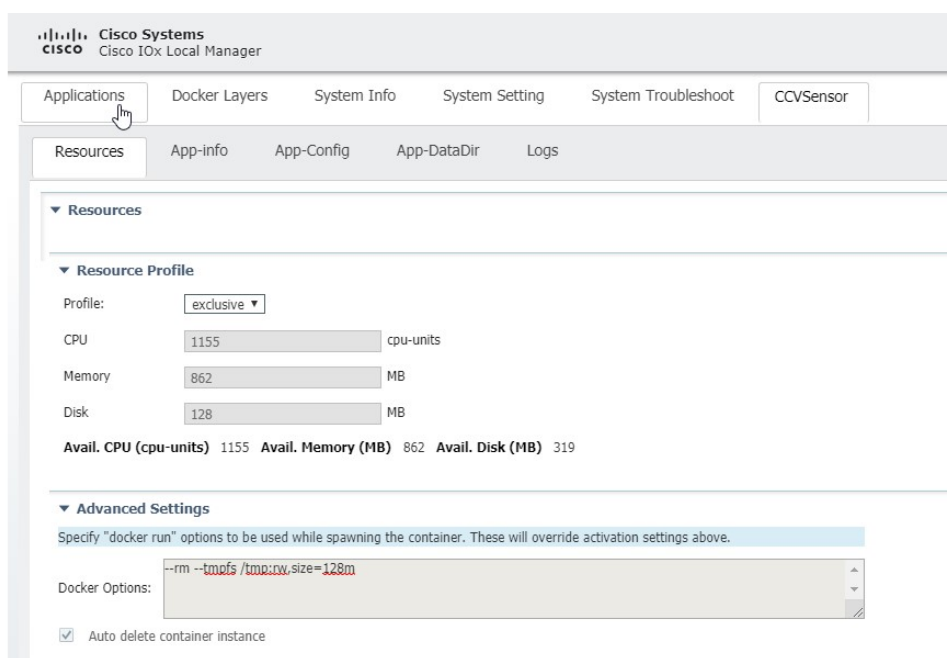
ステップ 2 進捗状況ウィンドウが表示されます。これが完了するまでに数秒かかる場合があります。

図 22: アクティブ化の進捗



ステップ 3 [Applications] をクリックしてアプリのステータスを表示します。次を参照してください。

図 23: アプリケーションのリソース

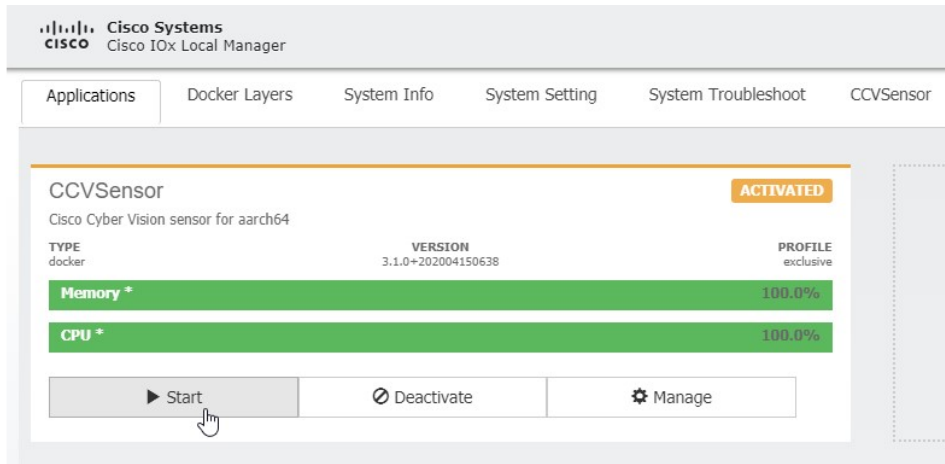


ステップ 4 アプリケーションがアクティブ化されており、起動する必要があります。

アプリケーションの起動

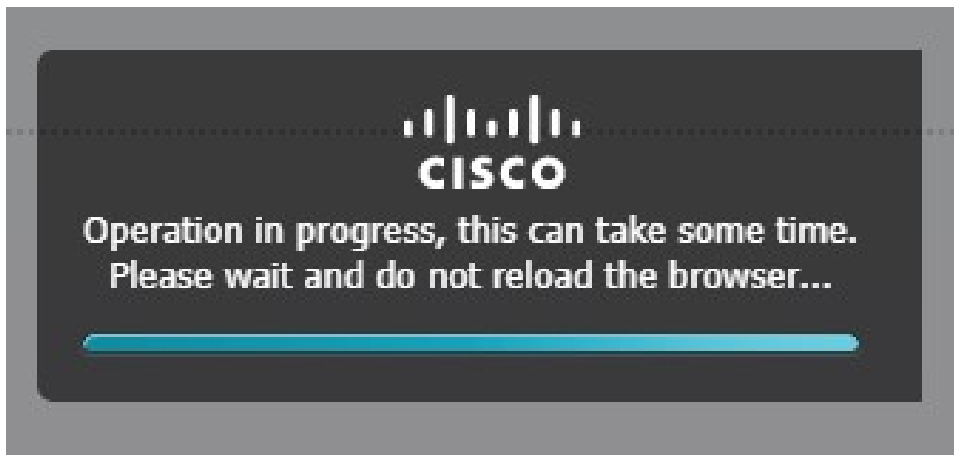
ステップ 1 [Start] をクリックします。次を参照してください。

図 24: アプリケーションの起動



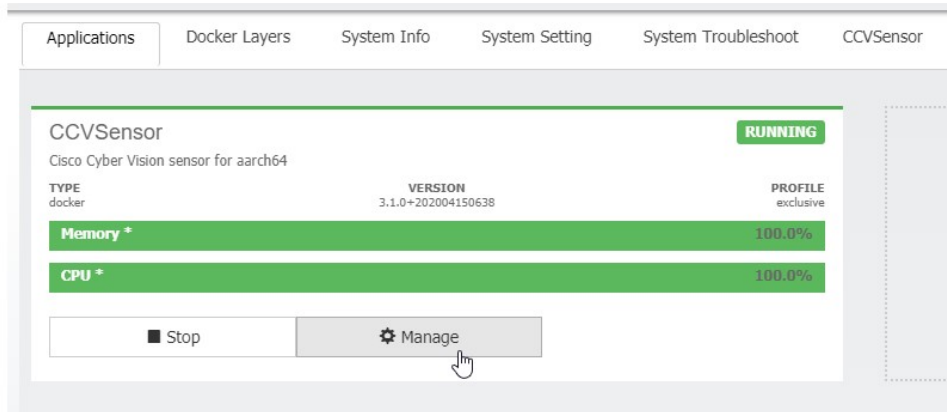
ステップ 2 進捗状況ウィンドウが表示されます。これが完了するまでに数秒かかる場合があります。

図 25: [Progress] ウィンドウ



ステップ 3 しばらくすると、アプリのステータスが実行中に変わります。

図 26: アプリケーション実行中



翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。