



産業用ルータの設定

- [産業用ルータの設定の前提条件](#) (1 ページ)
- [産業用ルータの設定](#) (2 ページ)
- [産業用ルータの準備](#) (2 ページ)
- [IOx の設定と有効化](#) (2 ページ)
- [IoT OD に接続するための IR デバイスの設定](#) (4 ページ)
- [デバイスでの設定の確認](#) (5 ページ)
- [Operations Dashboard でのデバイスステータスの確認](#) (6 ページ)

産業用ルータの設定の前提条件

IR1101 デバイス

IR1101 デバイスに IOx コンテナキーがプログラムされていることを確認します。

- 次のコマンドを実行します。

```
Router# show software authenticity keys | i Name
```

- 出力から、"Product Name: Cisco Services Containers" が含まれている行を探します。この行がある場合、デバイスには IOx コンテナキーがプログラムされています。
- この行がない場合は、次の手順を実行します。
 - 2020 年 1 月より前に出荷されたデバイス：署名の検証を無効にするか、デバイスをアップグレードします。
 - 2020 年 1 月 1 日以降に出荷されたデバイス：特に対処の必要はありません。デバイスにはデフォルトでコンテナキーがプログラムされているはずです。



(注) デバイスにコンテナキーがプログラムされておらず、署名の検証も有効になっていない場合、SEA のインストールは署名検証エラーで失敗します。

アプリケーション マネージャ サービス

IR ルータが Cisco IoT OD のアプリケーション マネージャ に追加されていることを確認します。

産業用ルータの設定

産業用ルータを設定して Cisco IoT OD との接続を確立するには、次の段階があります。

1. [デバイスの準備](#)
2. [IOx の設定と有効化 \(2 ページ\)](#)
3. [IoT OD に接続するための IR デバイスの設定 \(4 ページ\)](#)
4. [デバイスでの設定の確認 \(5 ページ\)](#)
5. [Operations Dashboard でのデバイスステータスの確認 \(6 ページ\)](#)

result

IoT OD と通信できるように、デバイスが正常に設定されました。

whats_next

リモートセッションの設定

産業用ルータの準備

この手順を使用して、SEA 設定用に産業用ルータを準備します。

手順

ステップ 1 必要なネットワークケーブルを接続します。

ステップ 2 デバイスの電源を入れます。

産業用ルータで SEA を設定できるようになりました。

IOx の設定と有効化

IOx アプリケーションが有効に動作するために必要な IP 接続とネットワーク設定があることを確認するには、このタスクを実行します。

IOx は、Cisco IOS XE で実行されるコンテナ ホスティング プラットフォームです。Cisco IoT Operations Dashboard が提供できる複数のサービス (Secure Equipment Access (SEA)、Cisco

Cyber Vision (CCV)、Edge Intelligence (EI) など) をインストールして実行するために使用されます。

手順

ステップ 1 IOx ネットワーク用のデバイスで VirtualPortGroup0 (VPG) インターフェイス、DHCP プール、および NAT ルールを設定します。

1. VPG インターフェイスを設定します。IOx アプリケーションを IOS XE に接続する仮想インターフェイスは、「VirtualPortGroup0」と呼ばれます。IOx アプリケーションには、仮想インターフェイスを介した IP 接続が必要です。これには、IP アドレスの受信が含まれます。次に設定例を示します。要件に合わせて IP アドレスを変更できます。ルータのコンソールで、コンフィギュレーションモードで次の設定コマンドを入力します。

```
! Example
conf t
interface VirtualPortGroup0
description IOx Interface
ip address 192.168.16.1 255.255.255.0
ip nat inside
ipv6 enable
end
```

2. DHCP プールを設定します。IOx アプリケーションは、起動すると、DHCP を介して IP アドレスを要求します。そのため、IOx アプリケーション用に DHCP プールを設定する必要があります。次に IP プールと DNS サーバーの設定例を示します。この設定は、要件に合わせてカスタマイズできます。デフォルトルータの IP アドレスが、VirtualPortGroup0 インターフェイスに設定済みの IP アドレスと同じであることを確認します。

```
! Example
conf t
ip dhcp pool ioxpool
network 192.168.16.0 255.255.255.0
default-router 192.168.16.1
dns-server 192.168.16.1 8.8.8.8
end
```

3. NAT を設定します。IOx アプリケーションは、DHCP から取得したプライベート IP アドレスを使用します。これらには、インターネットにアクセスするためのネットワークアドレス変換 (NAT) が必要です。DHCP プールの NAT ルールを追加して、IOx アプリケーション トラフィックがインターネットにアクセスできるようにします。

次の例では、インターネットへの接続が Cellular 0/1/0 を介して行われると想定しています。インターフェイスが Cellular 0/1/0 でない場合は、必ず変更または調整してください。たとえば、GigabitEthernet 0/0/0 や Cellular 0/3/0 などです。

```
! Example of a NAT rule for using Cellular0/1/0 as an uplink:
conf t
interface Cellular0/1/0
ip nat outside
ip access-list extended NAT_ACL
10 permit ip 192.168.16.0 0.0.0.255 any
route-map RM_WAN_ACL2 permit 10
match ip address NAT_ACL
match interface Cellular0/1/0
```

```
ip nat inside source route-map RM_WAN_ACL2 interface Cellular0/1/0 overload
end
```

ステップ2 IOx を有効化する。

```
conf t
iox
end
```

ステップ3 EXEC モードで次のコマンドを実行して、IOx が正しく動作していることを確認します。

```
show iox-service
! Example 1: When IOx is up and running, both the "IOx service (CAF)" and "dockerd" will be running.
Router#sh iox-service
IOx Infrastructure Summary:
-----
IOx service (CAF)           : Running
IOx service (HA)            : Not Supported
IOx service (IOxman)        : Running
IOx service (Sec storage)    : Running
Libvirtd 5.5.0              : Running
Dockerd v19.03.13-ce        : Running
```

IOx サービスがデバイスで実行されています。

IoT OD に接続するための IR デバイスの設定

Cisco IoT Operations Dashboard との接続を確立するには、デバイスの CLI で一連の IOS コマンドを実行する必要があります。IOx アプリケーションを管理するには、Cisco IoT Operations Dashboard で、IOS XE のスイッチでレベル 15 のログイン情報を使用して設定された有効なユーザーが必要です。

1. 次の設定を適用して、権限レベル 15 のユーザーを作成します。このログイン情報は、Cisco IoT Operations Dashboard の [デバイスプロファイル](#) で設定された値と一致している必要があります。

```
conf t
username <DEVICE PROFILE USERNAME> privilege 15 algorithm-type scrypt secret <DEVICE PROFILE PASSWORD>
end
```

2. 認証関連の設定と WSMA の設定を行います。

```
conf t
aaa new-model
aaa authentication login default local
aaa authorization exec default local
ip http server
ip http authentication local
ip http secure-server
wsma agent exec
profile exec
wsma profile listener exec
transport http path /wsma/exec
cna gzip
end
```

3. IDA トランスポートプロファイルを設定します。ポート TCP 443 で TLS を使用し、WebSocket を使用して Cisco IoT Operations Dashboard へのセキュア TLS 接続を有効にします。

US クラスタの場合：

```
conf t
ida transport-profile wst
  callhome-url wss://device-us.ciscoiot.com/wst/cgna
  active
end
```

EU クラスタの場合：

```
conf t
ida transport-profile wst
  callhome-url wss://device-eu.ciscoiot.com/wst/cgna
  active
end
```

4. CGNA 登録プロファイルを設定します。

```
conf t
cgna profile cg-nms-register
  transport-profile wst
  add-command show version | format flash:/managed/odm/cg-nms.odm
  add-command show inventory | format flash:/managed/odm/cg-nms.odm
  interval 3
  active
  url https://localhost/cgna/ios/registration
  gzip
end
```



(注) 設定が完了すると、デバイスは IoT OD に接続し、登録プロセスをトリガーします。

5. (オプション) DHCP サーバーを介して DNS をまだ取得していない場合は、ルータで DNS を有効にします。

これは、ルータが静的 IP と静的デフォルトゲートウェイを使用して設定され、DNS サーバーが明示的に指定されていない場合に重要です。この例では、Cisco DNS を使用します。任意の DNS サーバーを使用できます。

```
conf t
ip name-server 208.67.222.222
end
```

デバイスでの設定の確認

次のコマンドを使用して、デバイスが IoT OD に接続するために正しく設定されていることを確認します。

Router# **show ida transport-profile-state all**

```
! Verify that IDA status is connected for the "wst" transport profile
! Notice the line "IDA Status: Connected" in the show command output below for the "wst"
transport profile.
Router#sh ida transport-profile-state all
Transport Profile 1:
Profile Name: wst
Activated at: Fri Jun  7 07:26:42 2024
Reconnect Interval: 30 seconds
keepalive timer Interval: 50 seconds
Source interface: [not configured]
callhome-url: wss://device-us.ciscoiot.com/wst/cgna
Local TrustPoint: CISCO_IDEVID_SUDI
Remote TrustPoint: [not configured]
Execution-url: http://192.168.16.1
Proxy-Addr: [not configured]
IDA Status: Connected
State: Wait for activation
Last successful response at Fri Jun  7 08:25:29 2024
Last failed response:
Last failed reason:
```

Operations Dashboard でのデバイスステータスの確認

IoT OD が、デバイスからの登録要求を受信し、デバイスの設定を検証すると、デバイスが自動的に [Devices] > [Staged] ステータスから IoT OD 組織の [Registered] ステータスに移行します。

問題のトラブルシューティング

- IoT OD が登録試行を受信したものの何らかの問題（誤ったログイン情報など）が発生した場合、IoT OD が正しいログイン情報での登録試行を受信するまで、IR デバイスは [Devices] > [Staged] リストに [Configure Failure] ステータスで残ります。
- IoT OD が登録試行を受信しなかった場合、IR デバイスは [Devices] > [Staged] リストに残ります。

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。