



産業用ルータ向け **Cisco Secure Equipment Access** クイックスタートガイド

最終更新：2025 年 7 月 31 日

シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスコ コンタクトセンター

0120-092-255（フリーコール、携帯・PHS含む）

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>



目次

第 1 章	このガイドの目的 1 このガイドの目的 1
第 2 章	Secure Equipment Access サービスの有効化 3 Cisco Secure Equipment Access サービス 3 前提条件 3 SEA サービスの有効化 4
第 3 章	アプリケーション マネージャ サービスの設定 5 デバイスプロファイルの作成 5 アプリケーション マネージャ サービスへの IR デバイスの追加 6
第 4 章	産業用ルータの設定 7 産業用ルータの設定の前提条件 7 産業用ルータの設定 8 産業用ルータの準備 8 IOx の設定と有効化 8 IoT OD に接続するための IR デバイスの設定 10 デバイスでの設定の確認 11 Operations Dashboard でのデバイスステータスの確認 12
第 5 章	リモートセッションの設定 13 産業用ルータへの SEA エージェントのインストール 13 リモートセッションの設定 14

遠隔資産への接続	15
----------	----



第 1 章

このガイドの目的

- [このガイドの目的 \(1 ページ\)](#)

このガイドの目的

このガイドは、SEA 管理者が産業用ルータ（IR）で Secure Equipment Access（SEA）サービスを有効にする際に役立ちます。また、このガイドは、管理者が SEA サービスを介して最初のリモートセッションを設定する際にも役立ちます。

詳細と高度な概念については、[Cisco IoT Operations Dashboard のドキュメント](#)を参照してください。



第 2 章

Secure Equipment Access サービスの有効化

- [Cisco Secure Equipment Access サービス \(3 ページ\)](#)
- [前提条件 \(3 ページ\)](#)
- [SEA サービスの有効化 \(4 ページ\)](#)

Cisco Secure Equipment Access サービス

Cisco Secure Equipment Access (SEA) サービスは、Cisco IoT Operations Dashboard によって制御と管理が処理されるハイブリッドクラウドソリューションです。このオンプレミスコンポーネントは、対象の運用技術 (OT) 資産のあるリモートサイトに展開された、サポートされている産業用ネットワークデバイスで動作します。SEA サービスは、メンテナンス作業のために、特定の産業用 IoT リソースへのリモートアクセスをお客様とパートナーに提供することを目的としています。

前提条件

- 有効な IoT Operations Dashboard (IoT OD) 組織 (クラウドテナント) があることを確認します。ない場合は、<mailto:iotod-account-request@cisco.com> に要求を送信します。
- 組織内にアプリケーションマネージャと SEA システム管理者の両方のロールがあることを確認します。詳細については、[SEA のロールと権限に関する説明](#)を参照してください。
- IR ルータが Cisco IOS XE バージョン 17.15.1 以降を実行していることを確認します。
- IR ルータが、使用する IoT OD クラスタに応じて、us.ciscoiot.com または eu.ciscoiot.com へのアクティブなインターネット接続があることを確認します。

SEA サービスの有効化

process_workflow

産業用ルータで SEA サービスを有効にするための段階は次のとおりです。

1. [アプリケーション マネージャ サービスの設定](#) : IoT OD のアプリケーション マネージャ サービスを介して、必要な IR デバイスをオンボードします。
2. [IR ルータの設定](#) : アプリケーション管理のための IoT OD へのセキュアなトンネルを確立するように IR デバイスを設定します。
3. [リモートアクセスの設定](#) : IR デバイスに SEA エージェントをインストールし、SEA を介したターゲット OT 資産のリモートセッションを設定します。



第 3 章

アプリケーション マネージャ サービスの 設定

- [デバイスプロファイルの作成 \(5 ページ\)](#)
- [アプリケーション マネージャ サービスへの IR デバイスの追加 \(6 ページ\)](#)

デバイスプロファイルの作成

デバイスプロファイルは、デバイスにアクセスするためのユーザーログイン情報が含まれる設定ファイルです。デバイスプロファイルを使用して、複数のデバイスを Cisco IoT OD にオンボードします。Cisco IoT OD は、デバイスプロファイルで設定されたユーザーログイン情報を使用して複数のデバイスとの接続を確立します。

手順

ステップ 1 [Device Profiles] に移動し、[Create Device Profile] をクリックします。

[Create Device Profile] ページが表示されます。

ステップ 2 [Create Device Profile] ページで、[Device Profile Name] フィールドにプロファイル名を入力し、必要に応じて [Device Profile Description] フィールドに説明を入力します。

ステップ 3 [Configure credentials] エリアで、デバイスプロファイル設定用のユーザー名とパスワードをそれぞれのフィールドに入力します。

(注)

権限レベル 15 のユーザーログイン情報を使用してください。

ステップ 4 [Next] をクリックします。

デバイスプロファイルを確認する準備が整いました。

ステップ 5 デバイスプロファイルの詳細を確認したら、[Create Device Profile] をクリックします。

作成したデバイスプロファイルが、[Device Profiles] ページに一覧表示されます。

アプリケーションマネージャ サービスへの IR デバイスの追加

この手順の目的は、アプリケーションマネージャ サービスに IR ルータを追加できるようにすることです。

始める前に

次の状態を確認してください。

- IoT Operations Dashboard でデバイスプロファイルを作成している。
- IR ルータのシリアル番号と製品 ID をメモしている。

製品 ID とシリアル番号を表示するには、デバイスのコンソールで次のコマンドを使用します。

```
Router# show license udi
```

手順

ステップ 1 Cisco IoT Operations Dashboard で、[Application Manager] サービスに移動します。

ステップ 2 [Devices] > [Staged] タブの順に選択します。

ステップ 3 [Add Devices] をクリックします。

ステップ 4 [Select Add Device Method] ウィンドウで、[Single Device] を選択します。

ステップ 5 [Add Device] ページで、製品 ID、シリアル番号、および名前をそれぞれのフィールドに入力します。

ステップ 6 [Next] をクリックします。

ステップ 7 [Select Device Profile for Assignment] ページで、リストから [デバイスプロファイル](#) を選択し、[Next] をクリックします。

ステップ 8 [Review] ページで設定情報を確認し、[Add Device] をクリックします。

新しいデバイスが [Staged Devices] に表示され、このデバイスがまだ Cisco IoT Operations Dashboard に登録されていないことが示されます。

次のタスク

IR ルータの設定を行います。



第 4 章

産業用ルータの設定

- [産業用ルータの設定の前提条件](#) (7 ページ)
- [産業用ルータの設定](#) (8 ページ)
- [産業用ルータの準備](#) (8 ページ)
- [IOx の設定と有効化](#) (8 ページ)
- [IoT OD に接続するための IR デバイスの設定](#) (10 ページ)
- [デバイスでの設定の確認](#) (11 ページ)
- [Operations Dashboard でのデバイスステータスの確認](#) (12 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 \(8 ページ\)](#)
3. [IoT OD に接続するための IR デバイスの設定 \(10 ページ\)](#)
4. [デバイスでの設定の確認 \(11 ページ\)](#)
5. [Operations Dashboard でのデバイスステータスの確認 \(12 ページ\)](#)

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
cgn 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。



第 5 章

リモートセッションの設定

- [産業用ルータへの SEA エージェントのインストール \(13 ページ\)](#)
- [リモートセッションの設定 \(14 ページ\)](#)
- [遠隔資産への接続 \(15 ページ\)](#)

産業用ルータへの SEA エージェントのインストール

始める前に

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

手順

ステップ 1 [Secure Equipment Access] > [Quick Wizard] に移動します。

[Quick Wizard] ページが表示されます。

ステップ 2 [Install SEA Agent] で、[Start Configuration] をクリックします。

アプリケーション マネージャ サービスに追加されたすべてのネットワークデバイスが、[Select Network Device] エリアに一覧表示されます。

ステップ 3 SEA エージェントをインストールするデバイスを選択し、[Next] をクリックします。

[Advanced Configuration] ページが表示され、エージェントのインストールのデフォルト設定が示されます。デフォルトでは、SEA エージェントは、プロキシなしで DHCP を使用してネイティブ VLAN にインストールされます。

ステップ 4 (オプション) エージェントインストール設定をカスタマイズするには、[Advanced Configuration] ページで必要な設定の詳細情報を入力し、[Deploy] をクリックします。

SEA エージェントがネットワークデバイスにインストールされます。ステータスは、[System Management] ページの [SEA Agent Connection] 列で確認できます。5～10 分待ってからステータスを確認してください。

リモートセッションの設定

始める前に

管理する OT 資産に到達できる IR ルータに SEA エージェントがインストールされていることを確認します。

SEA ユーザーおよびアクセスグループ

SEA ユーザーには、特定のアクセスグループを介してアクセス権が付与されます。アクセスグループを作成し、ユーザーと設定されたリモートセッションの両方をグループに追加することをお勧めします。グループ内のユーザーのみが OT 資産にリモートでアクセスできます。

リモートセッションを設定する手順の概要

1. 資産に接続するネットワークデバイスを選択する
2. 資産を設定する
3. 資産にリモートでアクセスするためのアクセス方式を設定する
4. 資産とユーザーの両方が属するアクセス制御グループを選択する
5. 接続が機能していることを確認する

手順

ステップ 1 [Secure Equipment Access] > [Quick Wizard] に移動します。

右側に [Quick Wizard] ページが表示されます。

ステップ 2 [Connect to Asset] で、[Start Configuration] をクリックします。

アプリケーション マネージャ サービスに追加されたすべてのネットワークデバイスが、[Select Network Device] エリアに一覧表示されます。

ステップ 3 リストから IR ルータを選択し、[Next] をクリックします。

次の手順で設定する OT 資産は、このデバイスに関連付けられます。

ステップ 4 接続された資産を設定します。[Configure Connected Asset] エリアで、次の詳細情報を入力し、[Next] をクリックします。

- a) [Asset Name] : 追加する資産の名前。
- b) [IP Address] : 資産の IP アドレス。

- c) [Description] : 資産に関する簡単な説明。

ステップ 5 アクセス方式を設定します。

- a) [Choose Access Method] ドロップダウンリストからアクセス方式を選択します。

SEA ユーザーは、ここで選択したアクセス方式を使用して資産にアクセスします。選択可能なオプションは、[RDP]、[SSH]、[Telnet]、[VNC]、および [Web App] です。選択したアクセス方式に応じて、追加のフィールドが入力されます。

- b) [Assign to an Access Control Group] ドロップダウンリストからアクセス制御グループを選択し、[Finish] をクリックします。

アクセス制御グループに追加されたユーザーのみが、グループ内の資産にリモートでアクセスできます。

ステップ 6 [Test Access Method] をクリックしてリモート接続をテストします。

アセットへの接続を確認する新しいページが表示されます。

ステップ 7 [Done] をクリックします。

設定したリモートセッションが [Remote Sessions] ページに表示されます。SEA ユーザーは、Cisco IoT Operations Dashboard にログインしてセッションにアクセスできます。

遠隔資産への接続

リモートセッションを設定すると、SEA ユーザーは遠隔 OT 資産に接続できます。

1. Cisco IoT Operations Dashboard に SEA ユーザーとしてログインします。
2. [Secure Equipment Access] > [Remote Sessions] をクリックします。
使用可能なすべてのセッションが画面に表示されます。
3. 選択したセッションに移動し、[Connect] をクリックします。
SEA ユーザーは、以前に設定されたアクセス方式を使用して資産に接続します。



索引

I

IDA トランスポートプロファイルの設定 [10](#)
IoT Dashboard でのデバイス設定の確認 [12](#)

O

Operations Dashboard と通信するための IR スイッチの設定 [12](#)
Operations Dashboard と通信するための IR ルータの設定 [11](#)
Operations Dashboard のアプリケーション マネージャ サービス
への IR ルータの追加 [5](#)

S

SEA サービスの IR [3](#)
SEA サービスへの IR スイッチのオンボーディング [15](#)
SEA サービスへの IR ルータのオンボーディング [5](#)
SEA サービスへの産業用ルータのオンボーディング [3](#)
IR ルータを SEA にオンボーディングするための設定 [10](#)

W

WSMA の設定 [10](#)

さ

産業用ルータでの SEA の有効化 [3](#)

せ

IR ルータの設定 [10](#)
IR ルータ設定の確認 [11-12](#)

て

デバイス設定を確認するための CLI コマンド [11](#)
デバイスプロファイル [5](#)
デバイスプロファイルの作成 [5](#)
デバイスプロファイルの追加 [5](#)

り

リモートセッションの設定 [15](#)
リモートセッションへの接続 [15](#)

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。