



Cisco Secure Equipment Access への IE スイッチのオンボーディング クイックスタートガイド

最終更新：2025 年 1 月 24 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	新機能および変更された機能 1
	マニュアルの変更履歴 1
第 2 章	概要 3
	目的 3
	はじめに 3
	前提条件 4
第 3 章	デバイスプロファイルの作成とアプリケーション マネージャ サービスへの IE スイッチの追加 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 IE スイッチの追加 6
第 4 章	IE スイッチの設定と IoT Operations Dashboard との接続の開始 9
	IE スイッチの設定の前提条件 9
	設定手順 9
	IE デバイスの準備 10
	SD カードの設定と IOx の有効化 10
	IoT OD に接続するための IE3x00 スイッチの設定 11
	デバイスでの設定の確認 13
	IoT Operations Dashboard でのデバイスステータスの確認 14
第 5 章	Secure Equipment Access サービスへの IE スイッチの追加 15
	概要 15
	設定手順 15

第 6 章

リモートセッションの設定 19

概要 19

ネットワークデバイスへの OT 資産の追加 19

OT 資産のアクセス方式の設定 20

アクセスグループの作成とグループへのユーザーの割り当て 21

グループ内のユーザーへの資産の割り当て 23

リモートセッションへの接続 24



第 1 章

新機能および変更された機能

- [マニュアルの変更履歴](#) (1 ページ)

マニュアルの変更履歴

この表に、初版後このマニュアルに加えられた技術的な変更の履歴を示します。

表 1: マニュアルの変更履歴

日付	変更点
2024 年 7 月	このマニュアルの初回リリース



第 2 章

概要

- [目的 \(3 ページ\)](#)
- [はじめに \(3 ページ\)](#)
- [前提条件 \(4 ページ\)](#)

目的

このドキュメントの目的は、初めて Cisco IE ネットワークデバイスを Cisco IoT Operations Dashboard にオンボーディングし、Secure Equipment Access (SEA) サービスを介して初めてリモートセッションを設定する際に、新しいSEA管理者を支援することです。完了すると、SEA管理者はインターネット対応デバイスから必要な OT 資産へのリモートアクセスを実行できるようになります。

これは、目的を達成するための最短かつ最も効率的な経路を提供するように設計された、自己完結型のクイックスタートガイドです。

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

はじめに

Cisco Secure Equipment Access (SEA) サービスは、メンテナンス作業を実行するために、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。

IE スイッチでの SEA の有効化

IE スイッチで SEA を有効にし、接続された資産とのリモートセッションを実行するには、次の手順を実行します。

1. [デバイスプロファイルの作成とアプリケーション マネージャ サービスへの IE スイッチの追加 \(5 ページ\)](#)
2. [IE スイッチの設定と IoT Operations Dashboard との接続の開始 \(9 ページ\)](#)

3. [Secure Equipment Access サービスへの IE スイッチの追加](#) (15 ページ)
4. [リモートセッションの設定](#) (19 ページ)

前提条件

- 有効な IoT OD 組織（クラウドテナント）が必要です。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管理者ロールと SEA システム管理者ロールが必要です。
- IE スイッチに SD カードがある。
- IE スイッチには、最小バージョンで IOS-XE 17.14.1 が必要です。
- IE スイッチが、使用する IoTOD クラスタに応じて、インターネットサイト us.ciscoiot.com または eu.ciscoiot.com に接続できる。



第 3 章

デバイスプロファイルの作成とアプリケーションマネージャ サービスへの IE スイッチの追加

- [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 IE スイッチの追加 \(6 ページ\)](#)

デバイスプロファイルの作成

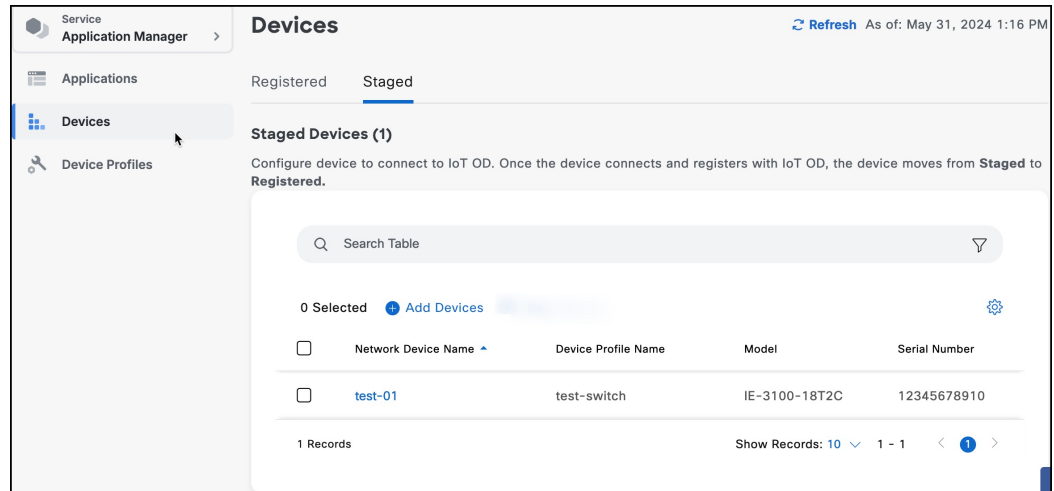
デバイスプロファイルには、ユーザーのログイン情報などの共通設定が含まれています。ユーザー名とパスワードのログイン情報を使用してプロファイルを作成し、これらのログイン情報を共有するすべてのデバイスにプロファイルをリンクすることができます。詳細については、[デバイスプロファイル](#)を参照してください。

1. Cisco IoT Operations Dashboard で、[Application Manager] サービスに移動します。
2. [Device Profiles] に移動し、[Create Device Profile] リンクをクリックします。[Create Device Profile] ページが表示されます。
3. このページで、名前と説明を入力し、[Next] をクリックします。
4. [Configure credentials] 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入力します。
5. [Next] をクリックします。作成したプロファイルが確認用に表示されます。
6. 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] の下に表示されます。

アプリケーション マネージャ サービスへの IE スイッチの追加

デバイスプロファイルを作成したら、アプリケーション マネージャ サービスに IE スイッチを追加できます。

1. Cisco IoT Operations Dashboard で、[Application Manager] サービスに移動します。
2. [Devices] > [Staged] タブをクリックします。
3. [Add Devices] をクリックします。
4. [Single Device] を選択して、[Add Device] ページを開きます。
5. [Devices] > [Staged] > [Add Devices] をクリックします。



6. [Select Add Device Method] ウィンドウで、[Single Device] をクリックします。
7. [Add Device] ページで、製品 ID、シリアル番号、名前などの詳細を入力します。

Add Device

1 Setup

2 Assign Device Profile

3 Review

Select your Devices

Product ID (PID)*

Serial Number*

Name

☐ I want to add my device using the Latitude, Longitude.

次のコマンドを使用して、デバイスの製品 ID とシリアル番号を表示します。

Switch# **show license udi**

シリアル番号と製品 ID は、デバイスの ID ステッカーと、デバイスが入っていた梱包箱にも記載されています。

8. [Next] をクリックします。
9. [Select Device Profile for Assignment] 画面で、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。
10. [Review] 画面で設定情報を確認します。

Add Device

✓ Setup

✓ Assign Device Profile

3 Review

Device Details

Product ID	IE-3105-18T2C
Device Type	ie3100
Name	Test Device
Serial Number(s)	
Longitude	-
Latitude	-

Device Profile Details

Device Profile Name	00test
Category	Switch
Description	-

11. [Add Device] をクリックします。

新しいデバイスが [Staged Devices] の下に表示されていることを確認できます。これは、このデバイスはアプリケーションマネージャを介して追加されましたが、IoTOD には登録されていないことを意味します。また、デバイスはまだ Cisco IoT Operations Dashboard に接続されていません。



第 4 章

IE スイッチの設定と IoT Operations Dashboard との接続の開始

- [IE スイッチの設定の前提条件](#) (9 ページ)
- [設定手順](#) (9 ページ)
- [IE デバイスの準備](#) (10 ページ)
- [SD カードの設定と IOx の有効化](#) (10 ページ)
- [IoT OD に接続するための IE3x00 スイッチの設定](#) (11 ページ)
- [デバイスでの設定の確認](#) (13 ページ)
- [IoT Operations Dashboard でのデバイスステータスの確認](#) (14 ページ)

IE スイッチの設定の前提条件

- IE スイッチが 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。詳細については、[デバイスプロファイルの作成とアプリケーションマネージャサービスへの IE スイッチの追加](#)を参照してください。

設定手順

1. [デバイスの準備](#)
2. [SD カードの設定と IOx の有効化](#)
3. [IoT OD に接続するための IE3x00 デバイスの設定](#)
4. [デバイスでの設定の確認](#)
5. [IoT OD でのデバイスステータスの確認](#)

IE デバイスの準備

1. 必要なネットワークケーブルを接続します。
2. デバイスの電源を入れます。

SD カードの設定と IOx の有効化

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あり、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。最初の手順として、IOx を設定して有効にします。

IOx アプリケーションを使用するには、IE3x00 に **ext4** 形式の SD カードが必要です。ただし、出荷の一部として注文される SD カードは FAT32 形式です。そのため、SD カードを **ext4** に再フォーマットする必要があります。

次のコマンドを使用します。

format sdflash: ext4

次の手順を実行します。

1. トランクモードで AppGigabitEthernet1/1 を設定します。このトランクは、スイッチのどこでも使用される可能性が低いネイティブ VLAN を使用して設定することを推奨します。また、必須ではありませんが、アプリケーションとインターネットまたは他の VLAN からの通信に必要な VLAN のみをこのトランクで許可することもできます。次の例のように 1004 より大きいネイティブ VLAN 番号を使用する場合は、スイッチが "vtp mode transparent" に設定されていることを確認して、この VLAN を作成できるようにします。この設定では、アプリケーション トラフィックをたどらせる任意の VLAN にアプリケーションが展開されます。

```
conf t
  vtp mode transparent
  vlan 4094
  name app-man-native-vlan
  interface AppGigabitEthernet1/1
    switchport trunk native vlan 4094
    switchport mode trunk
  end
```

2. IOx を有効化する。

```
conf t
  iox
end
```

3. IOx が正しく実行されていることを確認します。

次に例を示します。

IE-3400# **show iox-service**

デバイスに次のような出力が表示されます。

```
IOx Infrastructure Summary:
-----
IOx service (CAF)           : Running
IOx service (HA)           : Not Supported
IOx service (IOxman)       : Running
IOx service (Sec storage)   : Running
Libvirt                    : Running
Dockerd                    : Running
```

IoT OD に接続するための IE3x00 スイッチの設定

次に、デバイスの CLI で一連の IOS コマンドを実行して、Cisco IoT Operations Dashboard との接続を確立します。IoT Operations Dashboard の**デバイスプロファイル**は、IE スイッチなどのデバイスに関連付けられ、それらを管理するためのユーザー名/パスワードのセットも含まれます。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、特権レベル 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。



- (注) WSMA サービスの使用は http に依存するため、設定で "ip http server" を有効にする必要があります。アプリケーションを安全に展開するには、"ip http secure-server" も追加します。最初にデバイスで実行されている設定を確認します。一部の関連する設定は、すぐに使用できる場合があります。

```
conf t
aaa new-model
aaa authentication login default local
aaa authorization exec default local

ip http secure-server
ip http server
ip http authentication local

wsma agent exec
  profile exec
wsma profile listener exec
  transport http path /wsma/exec

cnga gzip
```

```
ntp server pool.ntp.org
end
```



- (注) "ip http server" コマンドは、デバイスで Web サーバーを開始します。この Web サーバーには、ポート 443 を使用してアクセスすることができます。企業のファイアウォールで保護されていないデバイスがインターネットにさらされている場合は、潜在的なセキュリティリスクを防ぐために、この Web サービスへのアクセスを制御することが重要です。この問題と解決方法の詳細については、「[Technote: Troubleshooting](#)」のヒントを参照してください。サポートが必要な場合は、Cisco TAC にお問い合わせください

3. 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 接続を有効にするように IDA トランスポートプロファイルを設定します。

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、スイッチで DNS を有効にします。



- (注) これは、スイッチが静的IPと静的デフォルトゲートウェイを使用して設定され、使用する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。確認するには、次のコマンドを実行します。

Switch# **ping us.ciscoiot.com**

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 35.84.105.79, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

ping は失敗します。これは予期されていることですが、ホスト名が IP アドレスに解決されていることを検証することが重要です。設定された DNS サーバーは、"show ip dns view" を使用して確認できます。DHCP サーバーが DNS を提供していない場合は、デバイスで DNS を明示的に設定する必要があります。次に例を示します。

```
conf t
ip name-server 208.67.222.222 208.67.220.220
end
```

デバイスでの設定の確認

設定手順が完了し、CLIからのテンプレートがスイッチにプッシュされていることを確認します。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。

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

デバイスに次のような出力が表示されます。IDA Status: Connected という行に注目してください。

```
Profile Name: wst
Activated at: Tue Mar 12 15:12:19 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://localhost:80
Proxy-Addr: [not configured]
IDA Status: Connected
State: Wait for activation
Last successful response at Tue Mar 12 15:13:19 2024
Last failed response at Tue Mar 12 15:12:15 2024
Last failed reason: Gracefully disconnected
```

IoT Operations Dashboard でのデバイスステータスの確認

デバイスが登録要求により接続されると、デバイス設定が IoT OD によって認識および検証され、デバイスが自動的に [Devices] > [Staged] ステータスから IoT OD 組織の登録済みステータスに移行します。

IoT OD が登録試行を受信しなかった場合、IE3x00 デバイスは [Devices] > [Staged] リストに残ります。デバイスで次のことを確認します。

- telnet コマンドを使用して、デバイスが適切な IoT OD クラスタ (US/EU) に接続されていることを確認します。

```
// Verify that opening a telnet session to the cluster is successful. The output should have "Open"
```

Example:

```
#telnet us.ciscoiot.com 443
Trying us.ciscoiot.com (10.105.58.227, 443)... Open
```

- 問題が発生した場合は、デバイスレベルの [Event Log] ページを使用して、接続およびアプリケーションマネージャ関連のイベントを確認します。デバッグには、デバイスの [Troubleshooting] ページにあるトラブルシューティング ツールを使用します。



第 5 章

Secure Equipment Access サービスへの IE スイッチの追加

- [概要](#) (15 ページ)
- [設定手順](#) (15 ページ)

概要

Cisco IoT Operations Dashboard と通信するために IE スイッチを設定したら、SEA サービスにデバイスを追加することができます。

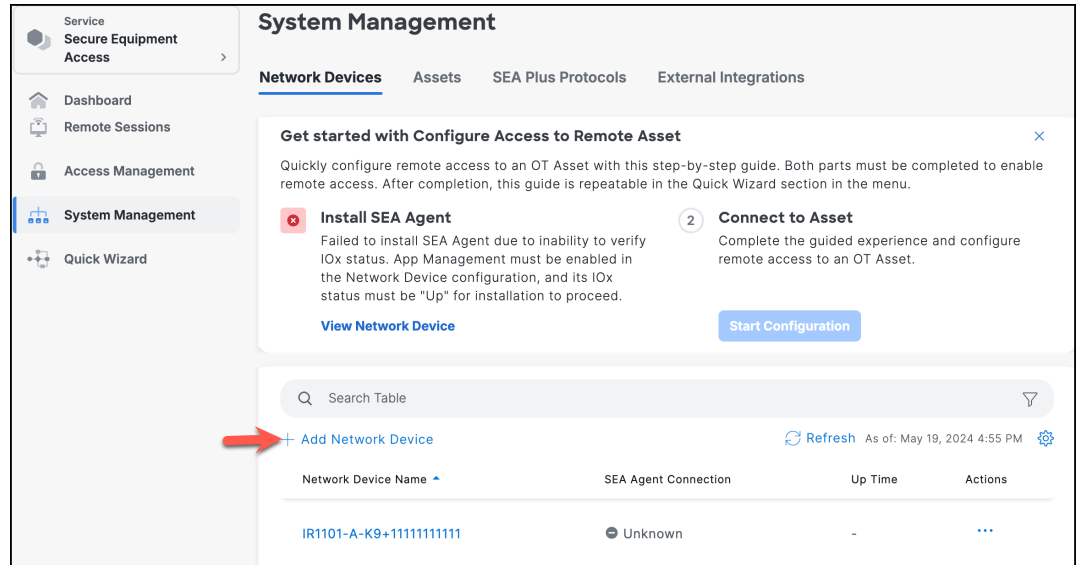


- (注)
- ネットワークデバイスまたは資産へのセキュアな遠隔通信を提供する [SEA Management] メニューオプションを開くことができるのは、SEA システム管理者ロールのみです。
 - また、初めての SEA システム管理者が遠隔 OT 資産に数ステップでアクセスできるように設計された、ガイド付きの新規ユーザーワークフローも用意されています。詳細については、「[SEA: New User Workflow](#)」を参照してください。
 - ネットワークデバイスまたは資産をより効率的にインストールおよび更新する方法については、「[SEA Quick Wizard](#)」を参照してください。

設定手順

1. [Services] パネルから、[Secure Equipment Access] > [System Management] を選択します。

2. [Network Devices] パネルで、[Add Network Device] をクリックします。



3. [Add Network Device] ページで、次の手順を実行します。

1. ネットワークデバイスをリストから選択するか、[Search] フィールドで検索します。
[Next] をクリックします。
2. ネットワークデバイスの説明、VLANID、およびIP割り当てを入力します。管理VLANとIP割り当ての設定の詳細については、「[Multi-VLAN and Static IP support](#)」を参照してください。
3. [Add Network Device] をクリックします。
SEA アプリケーションのインストールが開始されます。

4. [Next] をクリックします。確認ボックスが開きます。

5. ネットワークデバイスに関連付けられている SEA エージェントの展開の状態を確認します。

[SEA Agent] の展開状態が [Installed] に変わります。ステータスがインストール済みに変わらない場合は、ネットワークデバイスのリストに移動し、[Actions] 列の 3 つの点にカーソ

ルを合わせて、[Install SEA Agent] を選択します。

System Management

Network Devices

[Assets](#)[SEA Plus Protocols](#)[External Integrations](#)[+ Add Network Device](#)[Refresh](#)

As of: May 19, 2024 4:22 PM



Network Device Name ▲	SEA Agent Connection	Up Time	Actions
IR1101-A-K9+1111111111	Unknown	-	Install SEA Agent Delete
IR1101-K9+12345678901	Unknown		



第 6 章

リモートセッションの設定

- [概要 \(19 ページ\)](#)
- [ネットワークデバイスへの OT 資産の追加 \(19 ページ\)](#)
- [OT 資産のアクセス方式の設定 \(20 ページ\)](#)
- [アクセスグループの作成とグループへのユーザーの割り当て \(21 ページ\)](#)
- [グループ内のユーザーへの資産の割り当て \(23 ページ\)](#)
- [リモートセッションへの接続 \(24 ページ\)](#)

概要

SEA 管理者は、Secure Equipment Access (SEA) を使用して、OT 資産とネットワークデバイスを遠隔で管理および操作できます。

SEA 管理者はグループを作成してアクセスを管理し、SEA ユーザーは特定のアクセスグループを介してアクセス権を付与されます。グループの目的は、どの SEA ユーザーがどのアクセス方式にアクセスできるかを定義することです。SEA ユーザーは、アクセス権のあるデバイスのみを表示できるようになります。

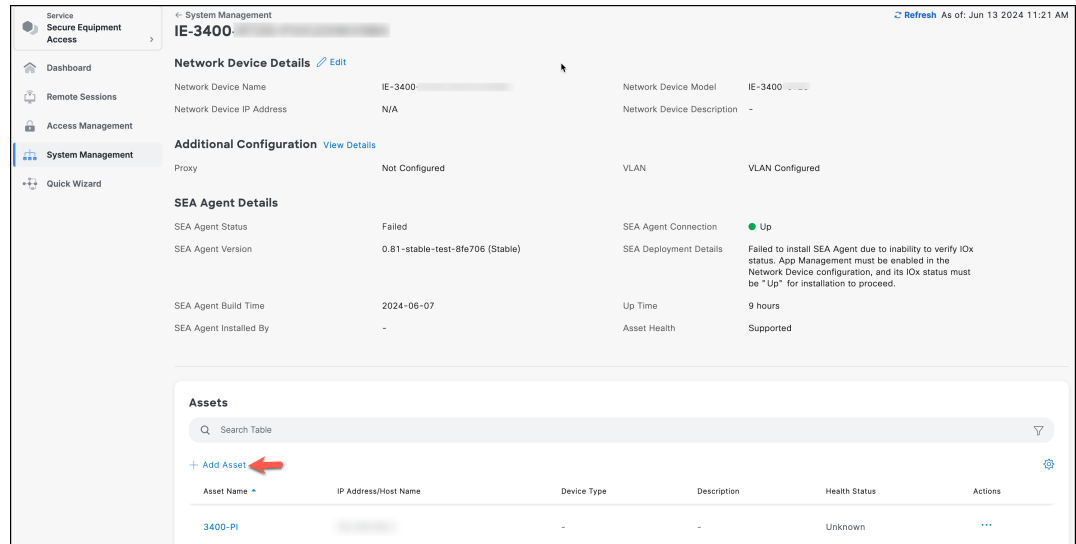
リモートセッションの設定には、次の手順が含まれます。

1. [ネットワークデバイスへの OT 資産の追加 \(19 ページ\)](#)
2. [OT 資産のアクセス方式の設定 \(20 ページ\)](#)
3. [アクセスグループの作成とグループへのユーザーの割り当て \(21 ページ\)](#)
4. [グループ内のユーザーへの資産の割り当て \(23 ページ\)](#)
5. [リモートセッションへの接続 \(24 ページ\)](#)

ネットワークデバイスへの OT 資産の追加

1. [System Management] 画面で、OT 資産を追加するネットワークデバイスを選択します。

2. [Network Device details] 画面で、[Add Asset] をクリックします。ページが表示され、[Network Device Details]、[SEA Agent Details]、および [Assets] が表示されます。
3. このページの [Assets] で、[Add Asset] をクリックします。[Add Asset] ページが表示されます。

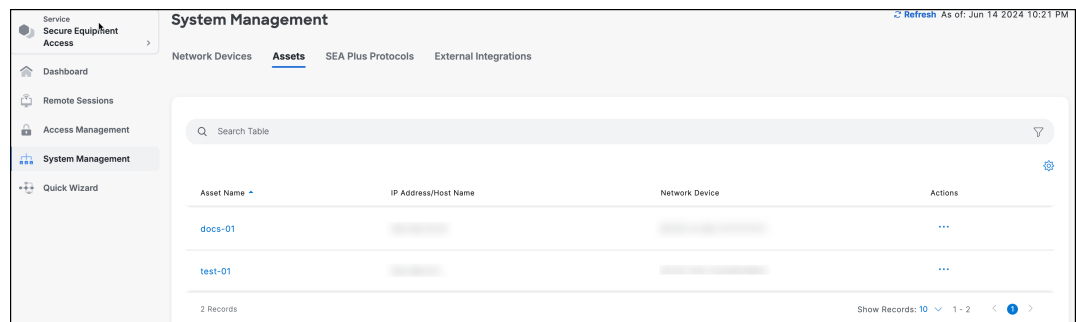


4. このページで、[Selection Method] から [Manual entry] を選択し、資産の名前と IP アドレス/ホスト名を入力します。
5. [Add] をクリックします。
新しく追加された資産が [Assets] セクションに表示されます。

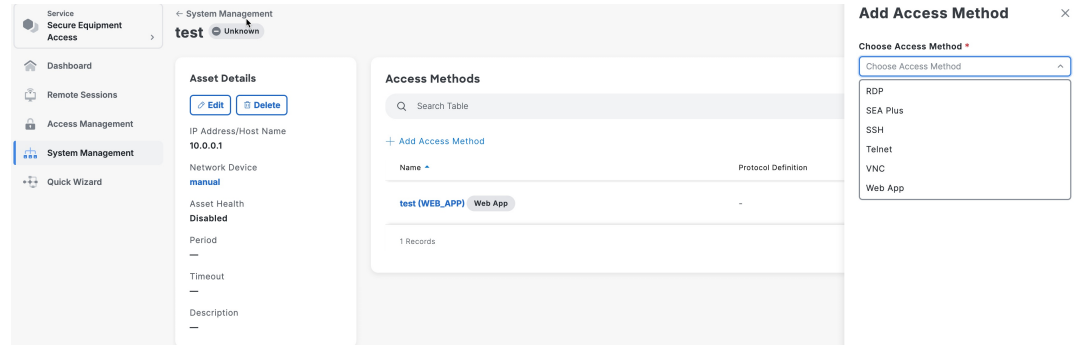
OT 資産のアクセス方式の設定

OT 資産を追加した後に、資産に接続するためのアクセス方式を設定できます。SEA には、SSH、RDP、VNC、Web アプリケーション、Telnet など、SEA に接続されたクライアントを設定するためのさまざまなアクセス方式があります。アクセス方式の詳細については、「[Access Methods](#)」を参照してください。

1. [Secure Equipment Access] > [System Management] > [Assets] に移動します。



2. アクセス方式を設定する資産の名前をクリックします。資産の詳細が表示されます。
3. [Access Methods] で、[Add Access Method] をクリックし、リストからアクセス方式を選択します。



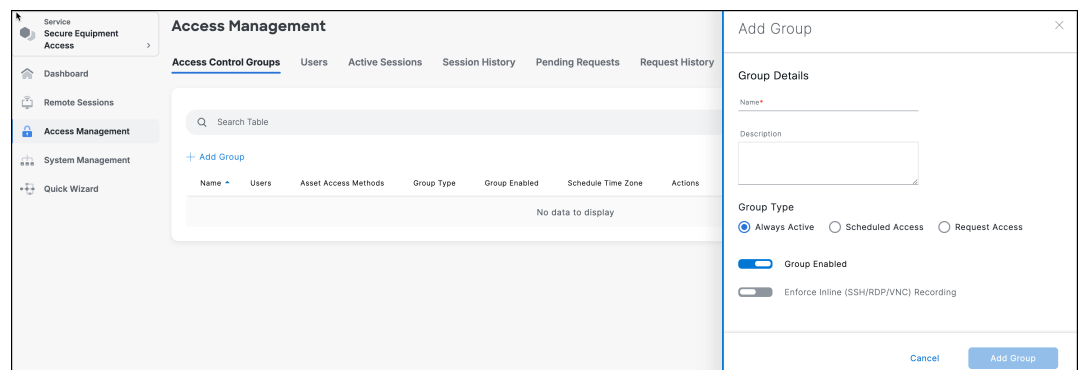
4. 選択したアクセス方式に関連する特定の詳細を入力し、[Add] をクリックします。
アクセス方式が [Access Methods] の下に表示されます。

アクセスグループの作成とグループへのユーザーの割り当て

アクセスグループは、グループ内の特定の OT 資産にアクセスする必要があるユーザーのコレクションです。アクセスグループには複数のユーザーと OT 資産を追加できます。

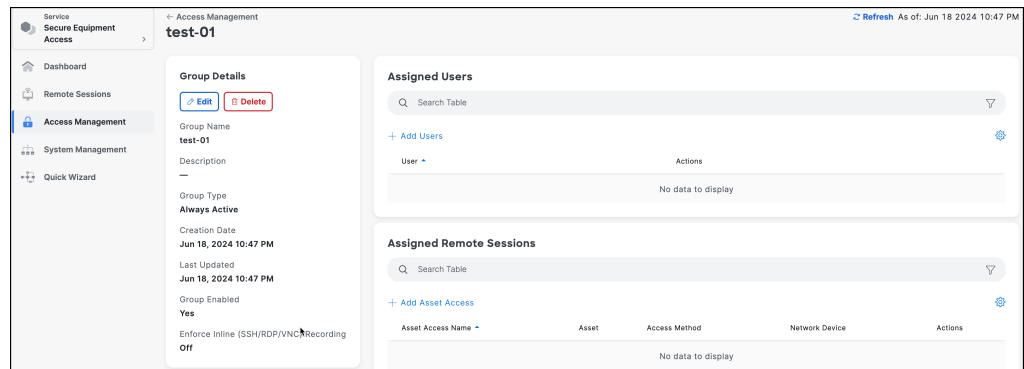
次の手順を実行してください。

1. [Secure Equipment Access] > [Access Management] 画面から、[Add Group] をクリックします。
[Add Group] ウィンドウが表示されます。

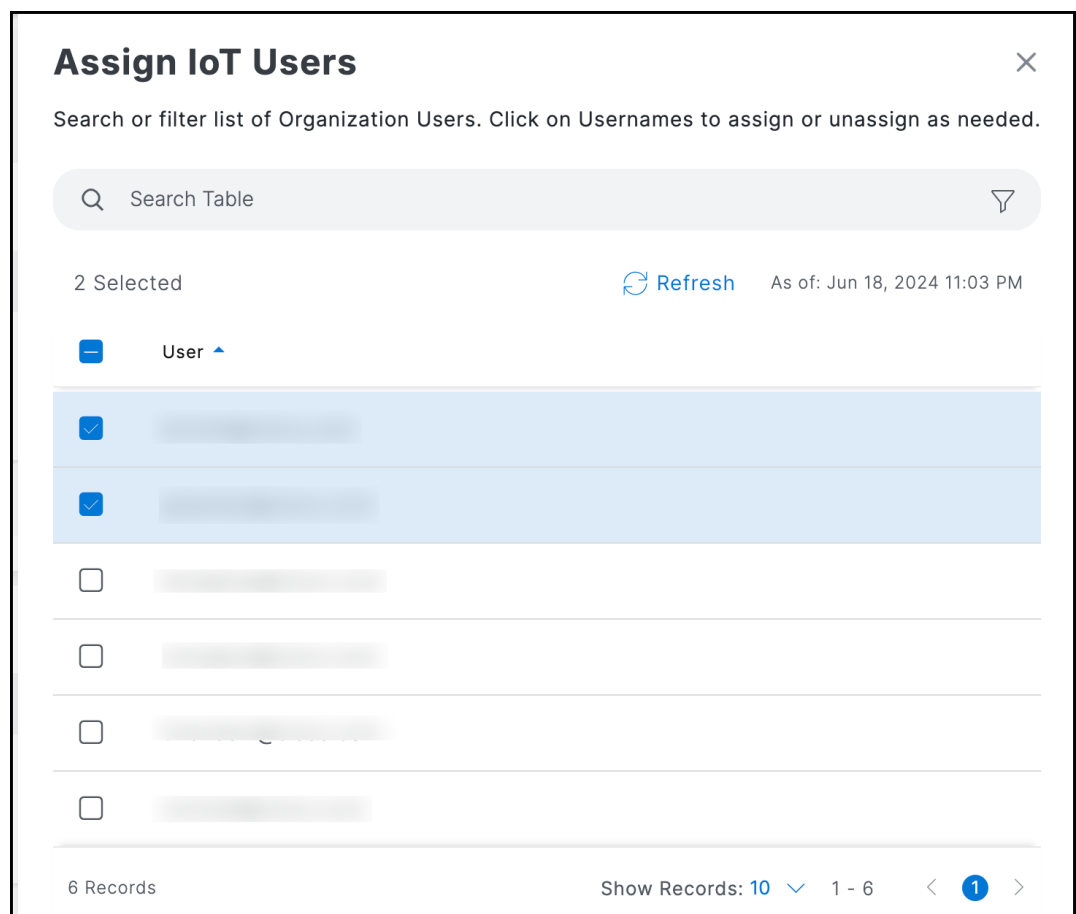


2. このウィンドウで、次の詳細を入力します。
 - 追加するグループの名前。
 - グループの説明
 - [Group Type] から [Always Active] を選択します。

- [Group Enabled] オプションは有効のままにします。
- [Add Group] をクリックします。追加したグループの詳細が表示されます。



3. [Assigned Users] で、[Add Users] をクリックします。[Assign IoT Users] ウィンドウが表示されます。
4. このウィンドウで、リストから 1 人以上のユーザーを選択し、[Save] をクリックします。



追加されたユーザーが、[Assigned Users] の下に表示されます

グループ内のユーザーへの資産の割り当て

SEA 管理者は、グループメンバーに資産を割り当てることができます。

1. [Secure Equipment Access] > [Access Management] をクリックします。
2. [Access Management] ページで、グループの名前をクリックします。
[Group Details] ページが表示されます。
3. [Group Details] ページの [Assigned Users & Asset Access] で、[Asset Access] をクリックします。
4. [Add Asset Access] をクリックします。[Assign Asset Access] ページが表示されます。

The screenshot displays the 'Access Management' page for a group named 'Test-01'. The left sidebar contains navigation links: Service Secure Equipment Access, Dashboard, Remote Sessions, Access Management (highlighted), System Management, and Quick Wizard. The main content area shows the 'Group Details' for 'Test-01', including fields for Group Name, Description, Group Type, Creation Date, Last Updated, Group Enabled, Enforce Full-Screen Monitoring & Recording, and Enforce Inline (SSH/RDP/VNC) Recording. Below this, the 'Assigned Users & Asset Access' section shows 'Users' and 'Asset Access' (highlighted) with counts of 0 each.

Access Management	
Test-01	
Group Details	
Group Name	Test-01
Description	Test
Group Type	Always Active
Creation Date	May 7, 2024 2:03 PM
Last Updated	May 10, 2024 1:23 PM
Group Enabled	Enabled
Enforce Full-Screen Monitoring & Recording	Off
Enforce Inline (SSH/RDP/VNC) Recording	Off
Assigned Users & Asset Access	
Users	0
Asset Access	0

5. [Assign Asset Access] ページで、リストから 1 つ以上の資産を選択します。

Assign Asset Access

Search or filter list of Assets and Access Methods. Click on Assets to assign or unassign as needed.

Search Table

2 Selected
[Refresh](#)
As of: May 12, 2024 3:51 PM

	Asset Access Name	Asset	Access Method	Network Device
☒	192.168.2.30 (SSH)	192.168.2.30	SSH	etychon-VIRTUAL-1
☒	Asset-1 (SSH)	Asset-1	SSH	Test-Switch-Girish
☐	AU-Telstra-LocalHost (SSH)	AU-Telstra-IR1831-LocalHost	SSH	AU-IOT-1831-TelstraNBN

6. [Save] をクリックします。

SEA ユーザーが IoT OD にログインすると、[Secure Equipment Access] > [Remote Sessions] の下にセッションが表示されます。

リモートセッションへの接続

SEA ユーザーは、SEA 管理者が SEA ユーザー用のセッションを設定した後に、リモートセッションに接続できます。

1. 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。
すべての自分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。

SSH

Vaudree (SSH)

Asset IP

Network Device LaVaudree

Serial Number

Connect



索引

記号

スイッチ用 QSG の目的 [3](#)
デバイスプロファイルの作成 [5-6](#)

C

Cisco Operations Dashboard の SEA サービスへの IE スイッチの追加 [15](#)

I

IDA トランスポートプロファイルの設定 [11](#)
IEx300 スイッチの設定 [11](#)
IE スイッチの設定 [9-10](#)
IE スイッチの設定の確認 [9, 13-14](#)
IE スイッチの設定の前提条件 [9](#)
IE スイッチの前提条件 [9](#)
IE スイッチへの OT 資産の追加 [19](#)
IE スイッチを SEA にオンボーディングするための設定 [9, 11](#)
IoT Dashboard でのデバイス設定の確認 [14](#)
IOx の有効化 [10](#)

O

Operations Dashboard と通信するための IE スイッチの設定 [9-10, 13-14](#)
Operations Dashboard のアプリケーション マネージャ サービスへの IE スイッチの追加 [5-6](#)
Operations Dashboard への IE スイッチの追加 [15](#)
OT 資産のアクセス方式の設定 [20](#)
OT 資産の作成 [19](#)

S

SD カードの設定 [9-10](#)
SEA サービスの IE スイッチ [3](#)
SEA サービスへの IE スイッチのオンボーディング [3, 5-6, 9-10, 15, 19-21, 23-24](#)
SEA への IE スイッチのオンボーディング、要件 [4](#)

SEA への IE スイッチのオンボーディングの前提条件 [4](#)
SEA への IE スイッチのオンボーディングの要件 [4](#)
Secure Equipment Access への IE スイッチの追加 [15](#)

W

WSMA の設定 [11](#)

あ

アクセスグループの作成 [21](#)
アクセスグループへのユーザーの割り当て [21](#)
アクセス方式の設定 [20](#)
アプリケーション マネージャ サービスへの IE スイッチの追加 [6](#)

く

グループへの資産の割り当て [23](#)

す

スイッチでの SEA の有効化 [3](#)
スイッチ用クイックスタートガイド、目的 [3](#)

て

デバイス設定を確認するための CLI コマンド [13](#)
デバイスプロファイル [5-6](#)
デバイスプロファイルの追加 [5](#)

ゆ

ユーザーへの資産の割り当て [23](#)

り

リモートセッションの作成 [19](#)
リモートセッションの設定 [20-21, 23-24](#)
リモートセッションへの接続 [24](#)

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。