Cisco Sensor Connect for IoT Services クイックスタートガイド

Cisco Sensor Connect for IoT Services の概要

Cisco Sensor Connect for IoT Services ソリューションにより、Cisco Catalyst ワイヤレス インフラストラクチャを介して高度な BLE 機能を提供できます。このソリューションの主要なコンポーネントは、Cisco IOx アプリケーションである IoT オーケストレータです。これは、ソフトウェアバージョン Cisco IOS-XE 17.15.3 以降を実行している既存の Cisco Catalyst 9800 ワイヤレス コントローラ プラットフォームに展開できます。Cisco Sensor Connect for IoT Services ソリューションにより、BLE デバイスを安全にオンボードおよび制御し、Message Queuing Telemetry Transport（MQTT）を使用してデータテレメトリを利用することができます。

IoT オーケストレータの前提条件

- AP が参加し、クライアントがネットワークに接続されている状態で、コントローラの初期設定を行う必要があります。
- コントローラは、Cisco IOS-XE バージョン 17.15.3 または 17.17.1 で実行される必要があります。
- 次のページに掲載されている IoT オーケストレータ（Spaces Orchestrator Software）イメージをダウンロードします。

  https://software.cisco.com/download/home/286323456/type

関連資料

- Cisco Sensor Connect for IoT Services Configuration Guide
- Cisco Sensor Connect for IoT Services Programmability Guide
- Cisco Sensor Connect for IoT Services Online Help
- Cisco Sensor Connect for IoT Services Release Notes

ライセンス

- Cisco Spaces Smart Operation
- Cisco Spaces ACT
- Cisco Spaces Unlimited
- Cisco Wireless Advantage

システム設定

サポート対象のシスコ ワイヤレス コントローラ プラットフォーム

- Cisco CW シリーズ 9800H1 および 9800H2 ワイヤレスコントローラ
- Cisco CW シリーズ 9800M ワイヤレスコントローラ
- Cisco Catalyst 9800-40 ワイヤレスコントローラ
- Cisco Catalyst 9800-80 ワイヤレスコントローラ
- Cisco Catalyst 9800-L ワイヤレスコントローラ

サポートされるアクセス ポイント

サポートされているアクセスポイントについては、『*Cisco Sensor Connect for IoT Services リリースノート、リリース 1.1*』を参照してください。

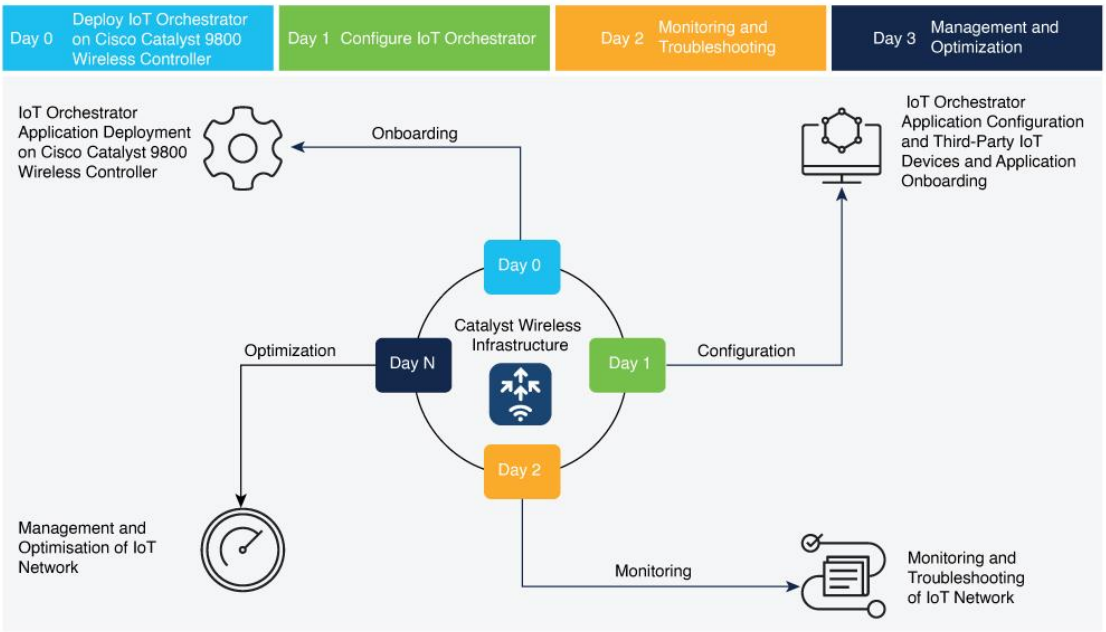


図 1.　　展開ワークフロー

Day-0 のアクティビティ

- Cisco Catalyst 9800 ワイヤレスコントローラでの IoT オーケストレータ アプリケーションの展開
- IoT オーケストレータの起動
- IoT オーケストレータ アプリケーション用 Day-0 WebUI ウィザード
- ユーザー名とパスワードの変更

Day-1 のアクティビティ

- IoT オーケストレータからの Cisco Catalyst 9800 ワイヤレスコントローラの設定
- サードパーティ アプリケーションの登録
- HTTP サーバーを開いて API をリッスンするための、証明書とキーのアップロード

- IoT オーケストレータ アプリケーションとデータをやり取りするための、パートナーアプリケーションの登録

Day-0：Cisco Catalyst 9800 ワイヤレスコントローラでの IoT オーケストレータ アプリケーションの展開

はじめる前に

- IoT オーケストレータをダウンロードし、コントローラ Web UI へのログインを行うシステムに保存します。

概要

IoT オーケストレータ アプリケーションを使用する場合は、Cisco Catalyst 9800 ワイヤレスコントローラに IoT オーケストレータ アプリケーションを展開する必要があります。

Cisco Catalyst 9800 ワイヤレスコントローラでの IoT オーケストレータ アプリケーションの展開

ステップ 1. Cisco Catalyst 9800 ワイヤレスコントローラ Web UI にログインします。

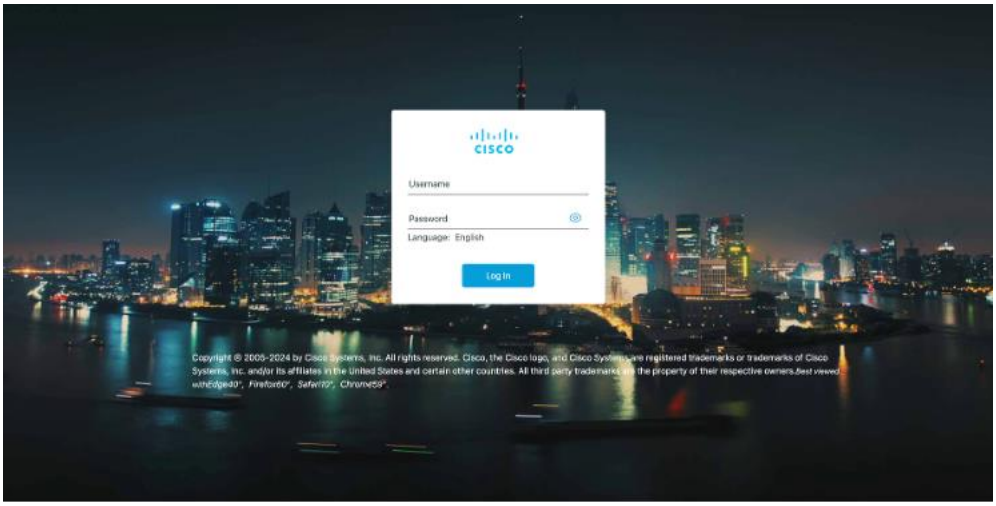


図 2.　Cisco Catalyst 9800 ワイヤレスコントローラ Web UI

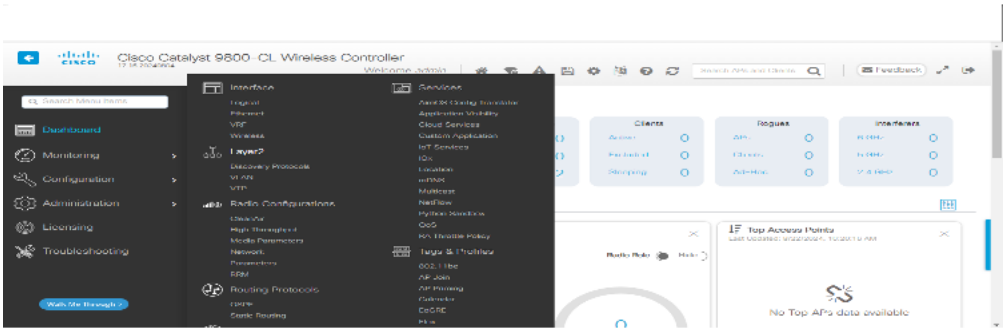
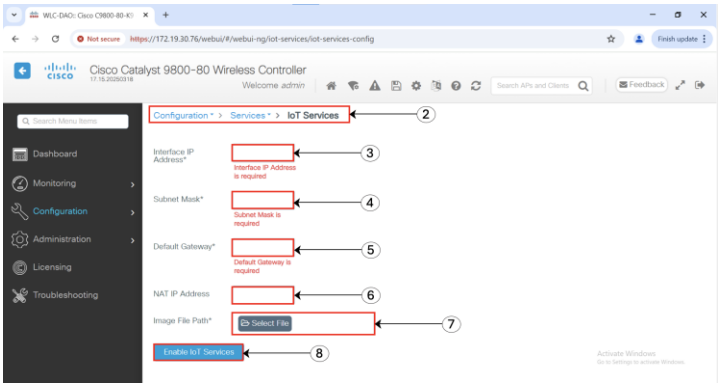


図 3.　[Configuration] > [Services] > [IoT Services]

ステップ 2. [Configuration] > [Services] > [IoT Services] の順に移動します。



ステップ 3. IoT オーケストレータの IP アドレスを入力します。

注： IP アドレスは一意で、Cisco Catalyst 9800 ワイヤレスコントローラで設定されている他の IP アドレスとは異なる必要があります。他のインターフェイスと重複する IP アドレスを設定すると、展開フローが失敗し、エラーメッセージが表示されます。たとえば、サブネット 192.168.1.0/30 では、192.168.1.1 を IoT オーケストレータの IP アドレスとして、192.168.1.2 をデフォルトゲートウェイの IP アドレスとして使用できます。

ステップ 4. IoT オーケストレータのサブネットマスクを入力します。

注： 推奨されるマスクサイズは /30 であり、このサイズでは 2 つの有効なホスト（IoT オーケストレータと Cisco Catalyst 9800 ワイヤレスコントローラの VirtualPortGroup インターフェイス）を使用できます。

ステップ 5. IoT オーケストレータのデフォルトゲートウェイの IP アドレスを入力します。

注： デフォルトゲートウェイの IP アドレスは、Cisco Catalyst 9800 コントローラの VirtualPortGroup インターフェイスの IP アドレスです。

ステップ 6. IoT オーケストレータに到達するためにシスコアクセスポイントが使用する NAT IP アドレスを入力します。

注： この設定は、Cisco Catalyst 9800 ワイヤレスコントローラがファイアウォールの背後にある場合、またはリモートデータセンターにある場合など、シスコアクセスポイントと IoT オーケストレータ間の直接接続が不可能な場合にのみ必要です。詳細については、『*Cisco Sensor Connect for IoT Services Configuration Guide*』の「NAT Configuration」の章を参照してください。

ステップ 7. [Image File Path] フィールドで、[Select File] をクリックして IoT オーケストレータイメージを選択し、[Open] をクリックします。

注： IoT オーケストレータイメージがローカルマシンにダウンロードされている必要があります。

ステップ 8. [Enable IoT Services] をクリックして、マシンから Cisco Catalyst 9800 コントローラにイメージをアップロードします。

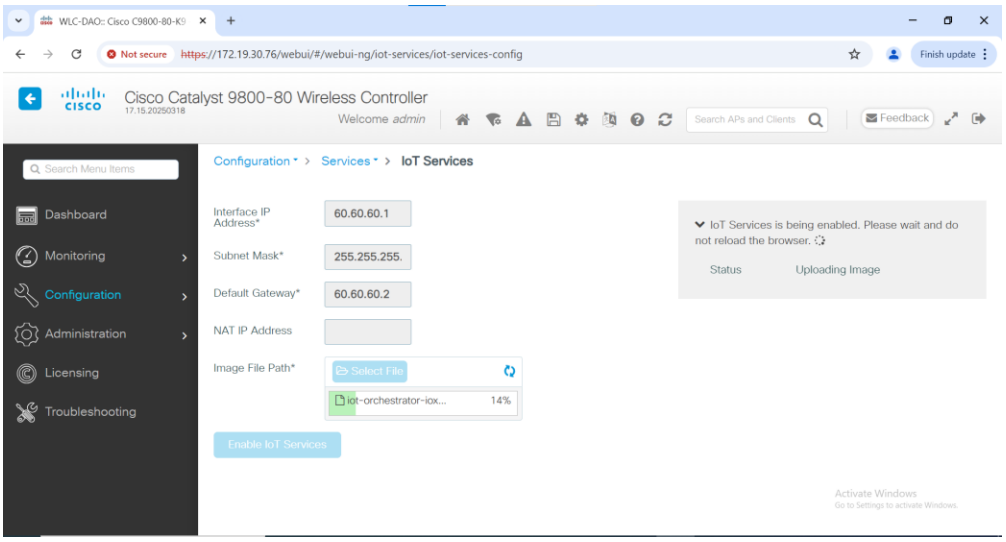


図 4.　　IoT サービスの有効化

次のステータスを示すバナーが表示されます。

- Installing
- Activating
- Starting
- Running

注：　Installing から Running に移行するまでに数分かかる場合があります。ステータスが Installing から Activating に移行する場合、これは、アプリケーションが Cisco IOS-XE インフラストラクチャによってインストールされていることを意味します。ステータスが Activating から Starting に移行する場合、これは、アプリケーションが Cisco IOS-XE インフラストラクチャによって起動されていることを意味します。ステータスが Starting から Running に移行する場合、これは、アプリケーションが実行状態になったことを意味します。

これで、IoT オーケストレータイメージがラップトップまたはコンピュータから Cisco Catalyst 9800 ワイヤレスコントローラにアップロードされます。

IoT オーケストレータ アプリケーションの展開が成功すると、アプリケーション名（デフォルトでは IoT Orchestrator）と IP アドレスが表示されます。

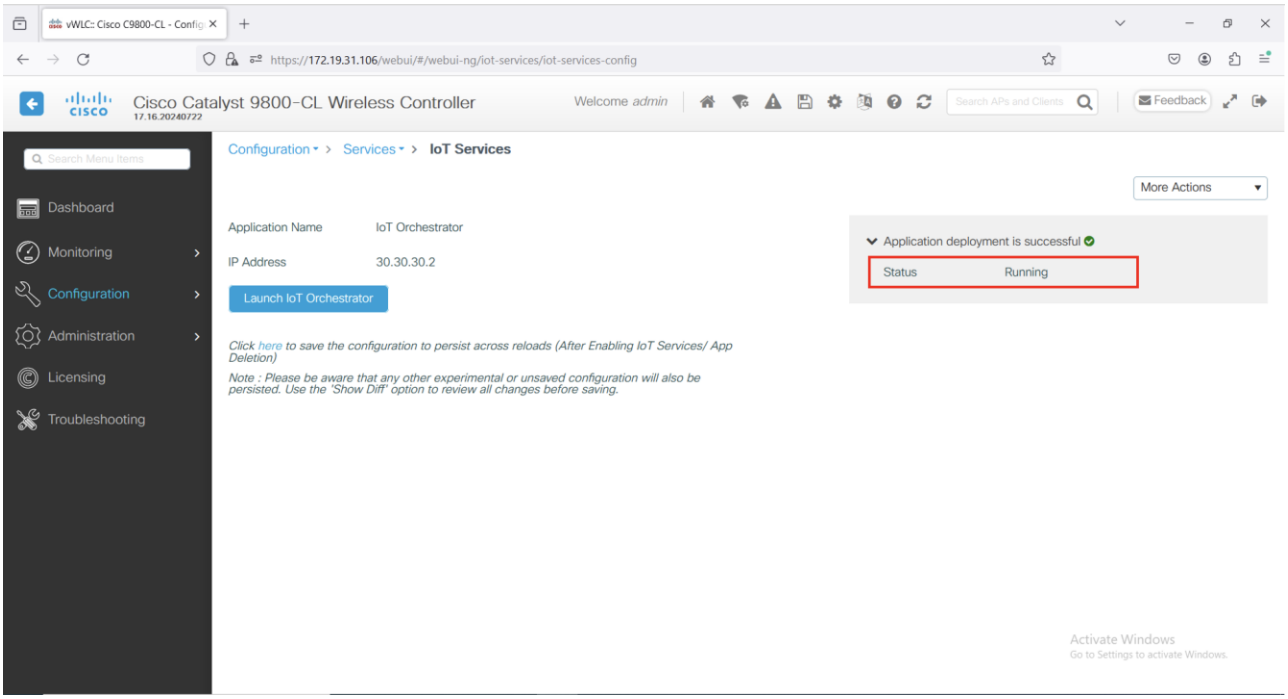


図 5.　　アプリケーション名と IP アドレスの表示

注：

- コンテナの展開と起動には、Cisco IOS-XE アプリケーション フレームワークが使用されます。アプリケーションは、Cisco Catalyst 9800 ワイヤレスコントローラで IOx コンテナとして実行されるようになりました。
- アプリケーション ホスティング コマンドを使用したインストール、アンインストール、アクティブ化、非アクティブ化、起動、または停止はサポートされておらず、IoT オーケストレータがエラー状態になる可能性があります。IOx Web インターフェイスを使用（[Configuration] > [Services] > [IOx] の順に選択）した、IoT オーケストレータでの操作の実行もサポートされていません。IoT オーケストレータの Day-0 および Day-1 管理操作については、IoT Services Web インターフェイスのみがサポートされています（[Configuration] > [Services] > [IoT Services] の順に選択）。

IoT オーケストレータの起動

始める前に：

- IoT オーケストレータのステータスが Running であることを確認します。
- IoT オーケストレータの IP アドレスが、コンピュータまたはラップトップから到達可能であることを確認します。
- IoT オーケストレータが Running の状態に到達してから、Cisco Catalyst 9800 ワイヤレスコントローラの高可用性（HA）機能を検出し、コントローラ間のすべてのデータベースを同期するまでに、最大 2 分かかることがあります。

概要

IoT オーケストレータ Web UI にアクセスする場合は、IoT オーケストレータ アプリケーションを起動する必要があります。

手順

[Configuration] > [Services] > [IoT Services] ページで、[Launch IoT Orchestrator] をクリックします。

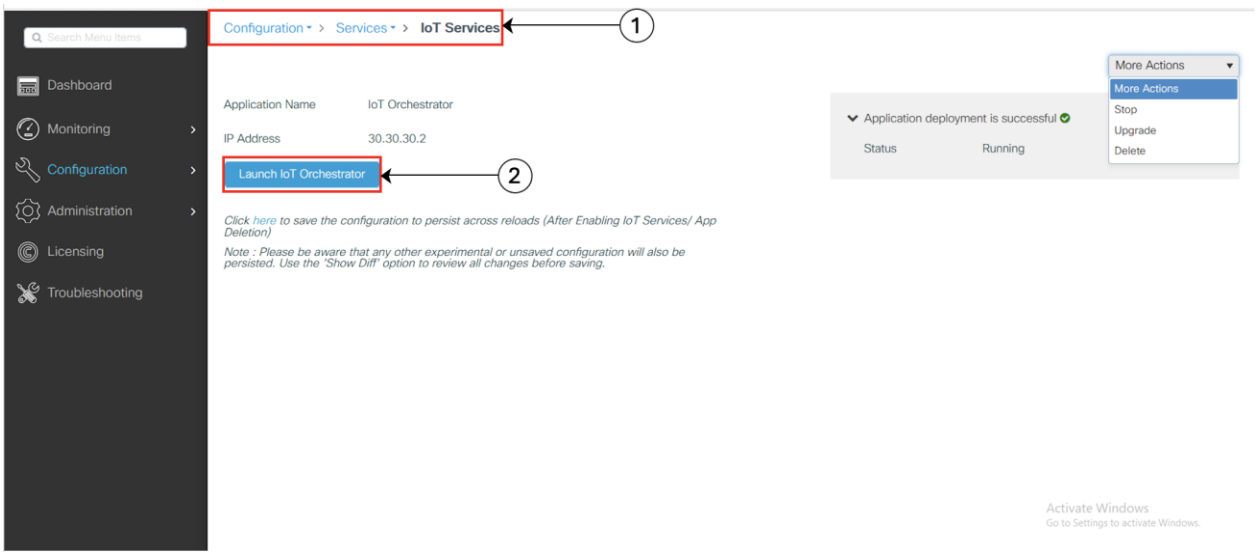


図 6.　　IoT オーケストレータの起動

注：　IP ネットワークが到達可能であることを確認するには、端末セッションを使用して IP アドレスの ping を実行する必要があります。

シスコアクセスポイントとワイヤレス IoT オーケストレータの間、またはワイヤレス IoT オーケストレータと外部のカスタムアプリケーションの間に、ファイアウォールや類似のデバイス（アクセス制御リスト（ACL）があるルータなど）が存在する場合は、適切な接続を可能にするルールを使用して、ファイアウォールまたは類似のデバイスを設定する必要があります。

シスコアクセスポイントとワイヤレス IoT オーケストレータ間の接続

次のポートを、シスコアクセスポイントからワイヤレス IoT オーケストレータまで開く必要があります。

表 1.　　プロトコル、ポート、および使用方法の詳細

プロトコル	ポート	使用方法
TCP	50221	AP のワイヤレス IoT オーケストレータとの初期 HTTP 接続
TCP	43626	ワイヤレス IoT オーケストレータとの接続を確立

外部アプリケーションとワイヤレス IoT オーケストレータ間の接続

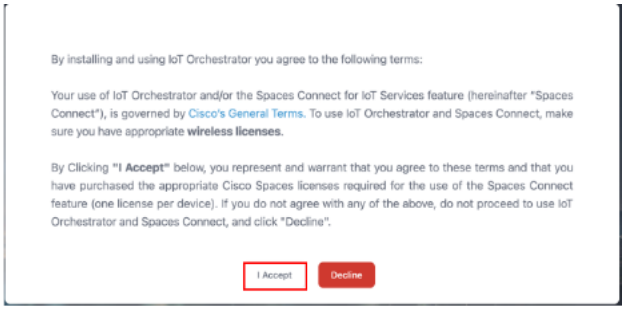
次のポートを、外部アプリケーションからワイヤレス IoT オーケストレータまで開く必要があります。

表 2.　　プロトコル、ポート、および使用方法の詳細

プロトコル	ポート	使用方法
TCP	8081	ワイヤレス IoT オーケストレータ REST API インターフェイス
TCP	41883	MQTT パブリッシャ リスニング ポート

IoT オーケストレータを使用するためのライセンスの詳細

利用規約を読み、[I Accept] をクリックします。



IoT オーケストレータのログインページが表示されます。

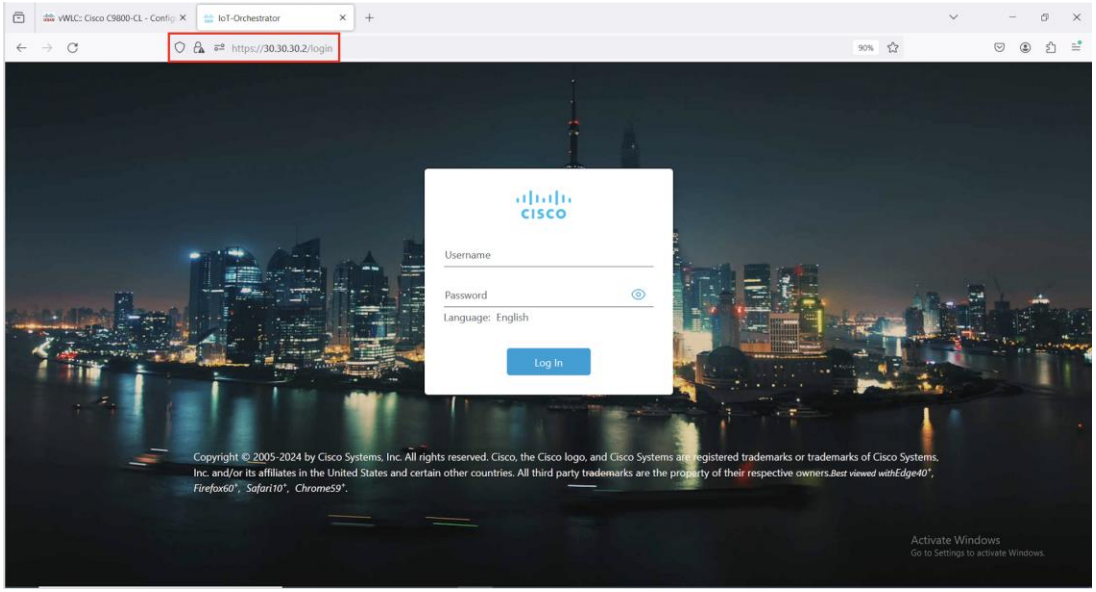


図 7.　　IoT オーケストレータのログインページ

IoT オーケストレータ アプリケーション用 Day-0 WebUI ウィザード

概要

Day-0 のために IoT オーケストレータ アプリケーションにログインするには、次の手順を実行する必要があります。

手順

ユーザー名に **admin** を、パスワードに **password** を入力します（デフォルトのログイン情報）。

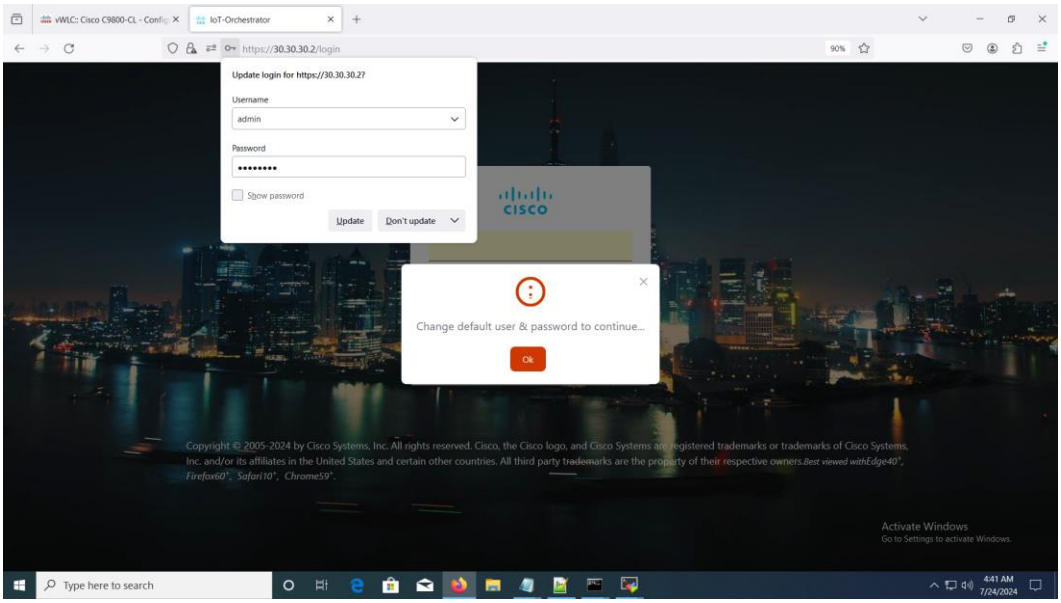


図 8.　　デフォルトログイン情報のログインページ

ユーザー名とパスワードの変更

概要

Day-0 ユーザープロファイルを作成するには、デフォルトのユーザー名とパスワードを変更する必要があります。

注：

- ログインページで、IoT オーケストレータのパスワードを入力する必要があります。
- このログインは、IoT オーケストレータのログイン情報であり、コントローラのログイン情報と同じではありません。

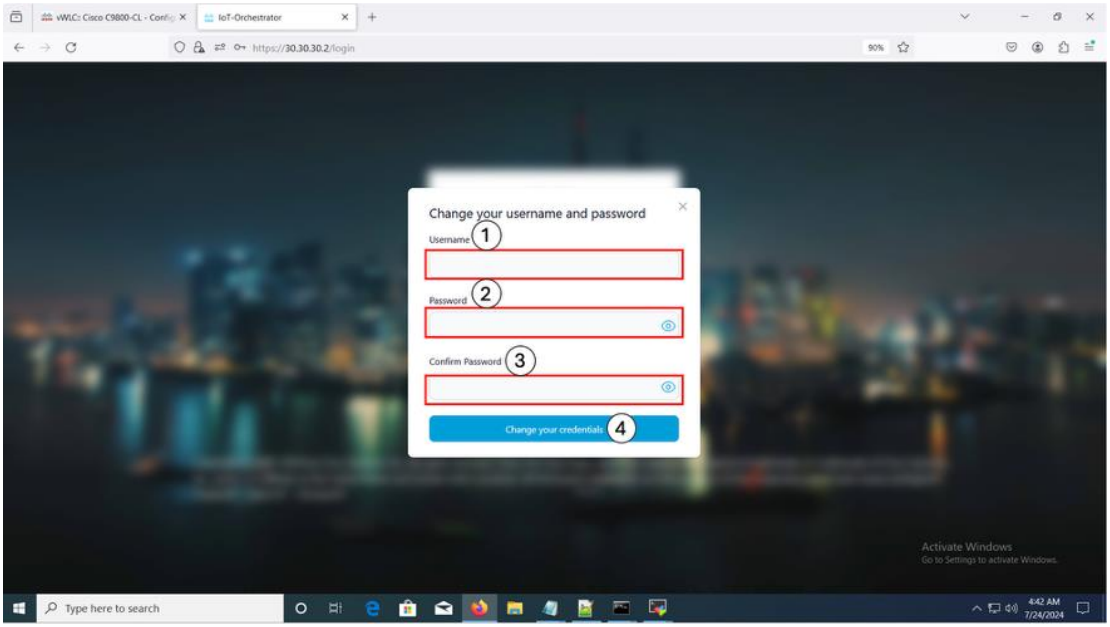


図 9.　　ユーザー名とパスワードの変更

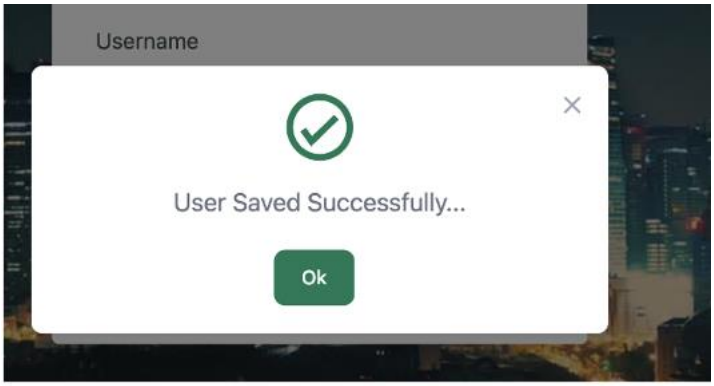


図 10.　　ユーザーの保存が成功したことを示すポップアップ

注：　管理者ログイン情報を覚えていない場合、パスワードの復旧手順を実行する必要があります。詳細については、ワイヤレス IoT オーケストレータ ドキュメントの「管理者パスワードの復旧」を参照してください。誤ったパスワードを 3 回連続して入力すると、ロックダウンタイマーが表示されます。タイマーの終了後に誤ったログインパスワードを再度入力すると、タイマーが更新され、最大 1 時間まで延長されます。

Day-1：IoT オーケストレータからの Cisco Catalyst 9800 ワイヤレスコントローラの設定

IoT オーケストレータ ダッシュボードで、[Administrator] > [9800 Wireless Controller configuration] ページを選択し、次の手順を実行します。

概要

AP（コントローラで使用可能）を IoT オーケストレータに接続するには、IoT オーケストレータを Cisco Catalyst 9800 ワイヤレスコントローラに接続し、コントローラにトークンと証明書をプッシュする必要があります。

IoT オーケストレータは、すべての AP 参加プロファイルでサポートされています。起動時に、アプリケーションによって default-ap-profile 上でのみ自動的に有効になります。no cisco-dna grpc コマンドを手動で使用することで、他の AP 参加プロファイルを設定できます。この設定により、そのプロファイルの AP が IoT オーケストレータとの gRPC チャネルを確立できるようになります。

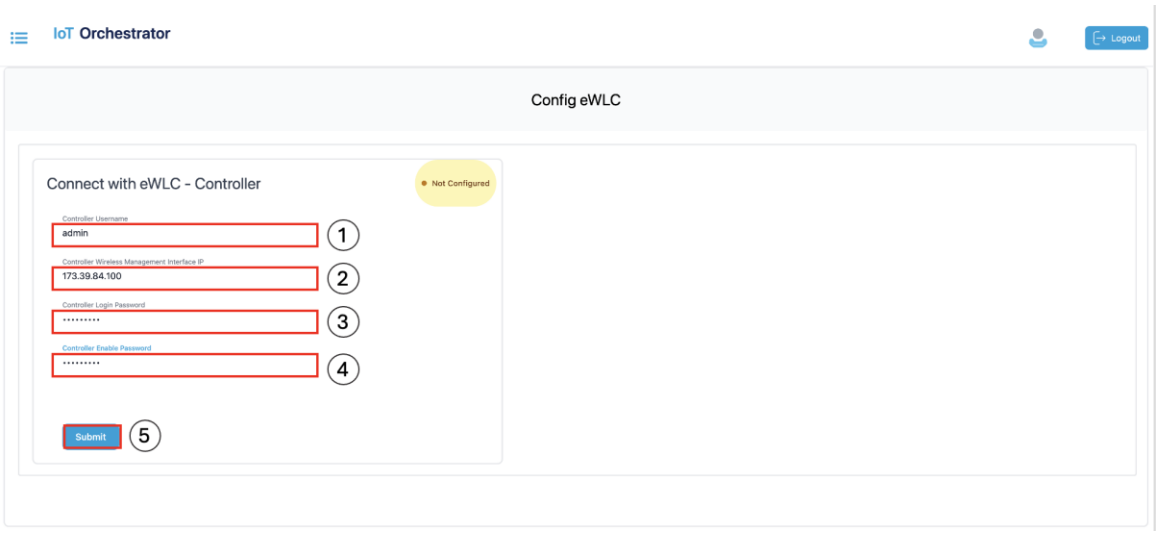


図 11.　　コントローラとの接続

次の内容を示すポップアップウィンドウが表示されます。

「コントローラとの接続が正常に確立されました。」

注：　コントローラに接続されているすべての AP が IoT オーケストレータに接続されているかどうかを確認するには、IoT オーケストレータ UI から [Inventory] > [Access Points] ページを確認します。

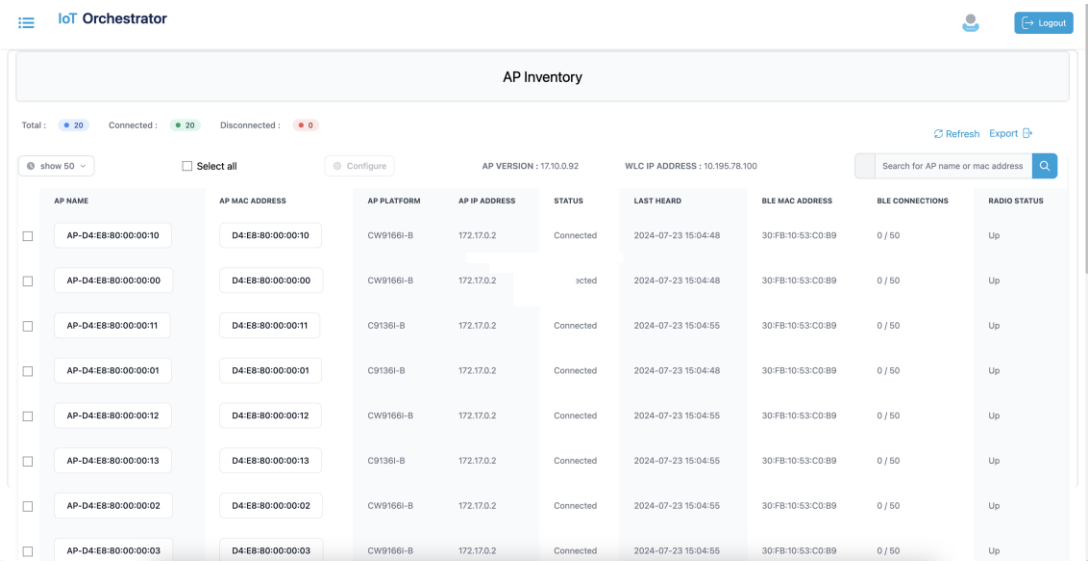


図 12.　[AP Inventory] ページ

AP BLE 送信設定（任意）

送信設定

手順

ステップ **1.** Cisco Catalyst 9800 ワイヤレスコントローラ Web UI にログインします。

ステップ **2.** メニューから、[Configuration] > [Transmit Configuration] を選択します。

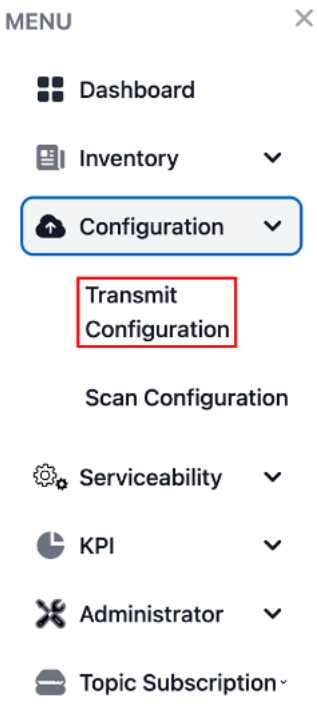


図 13.　IoT オーケストレータ ダッシュボード：[Configuration] -> [Transmit Configuration]

ステップ **3.** [Add] をクリックします。

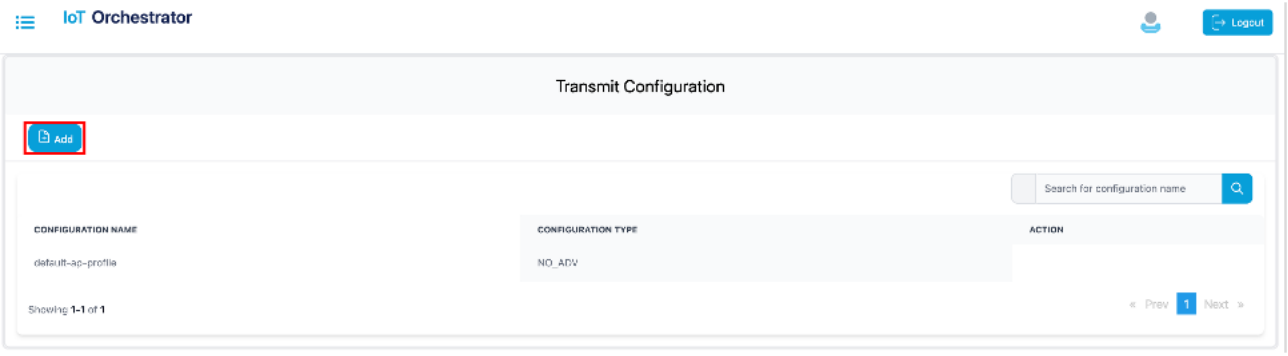


図 14.　[Transmit Configuration] ページ

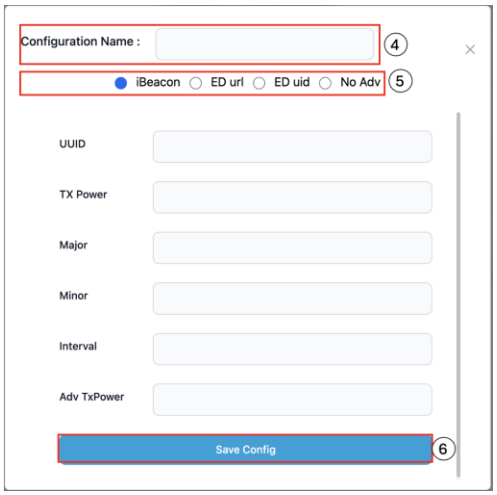


図 15.　[Transmit Configuration] : [Add] Page

ステップ 4. 送信設定の名前を入力します。

ステップ 5. 次の送信方法のいずれかを選択します。

- iBeacon：[UUID]、[TX power]、[major]、[minor]、[interval]、[Adv TxPower] の値を入力します。
- ED url：ED URL を入力します。

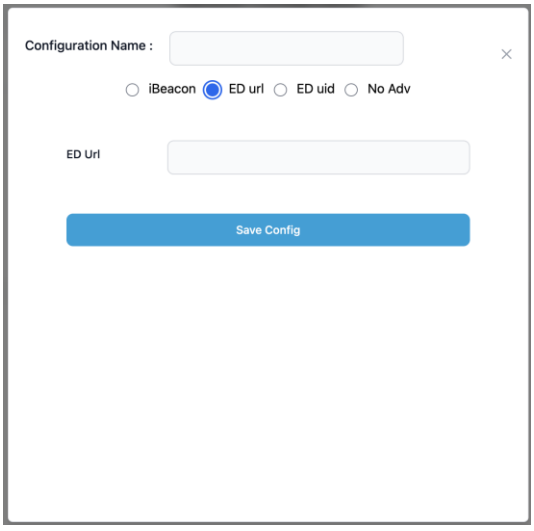


図 16.　ED URL の設定

- ED uid：[ED ns] および [ED instance] の値を入力します。

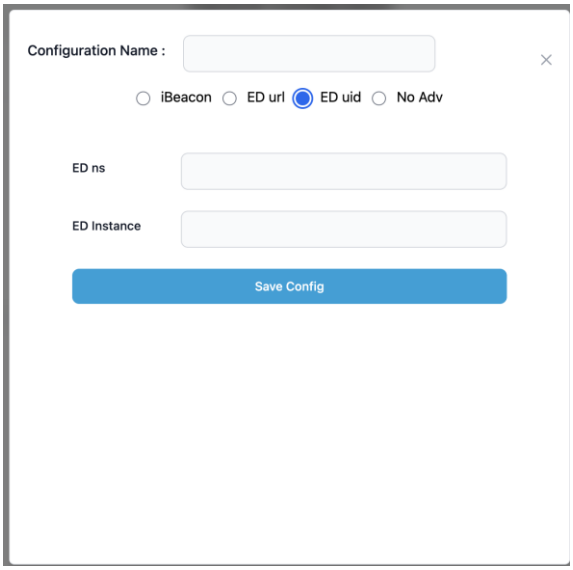


図 17.　　ED UID の設定

- アドバタイズなし：

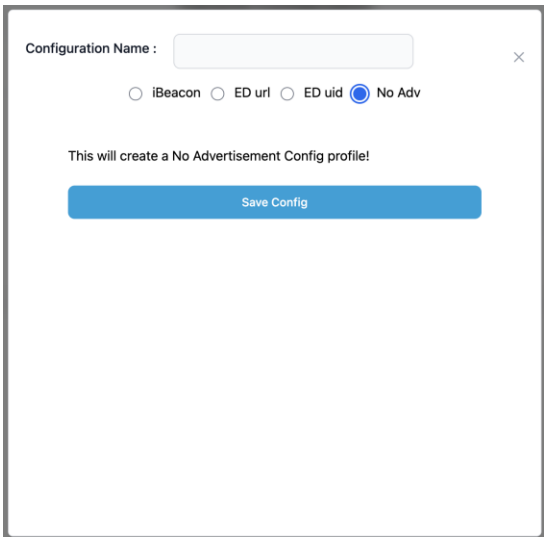


図 18.　　アドバタイズなしの設定

ステップ **6.** [Save Config] をクリックします。

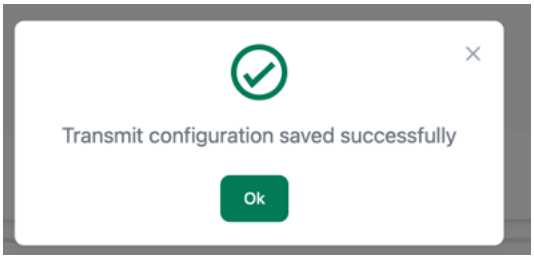


図 19.　　送信設定が成功したことを示すメッセージ

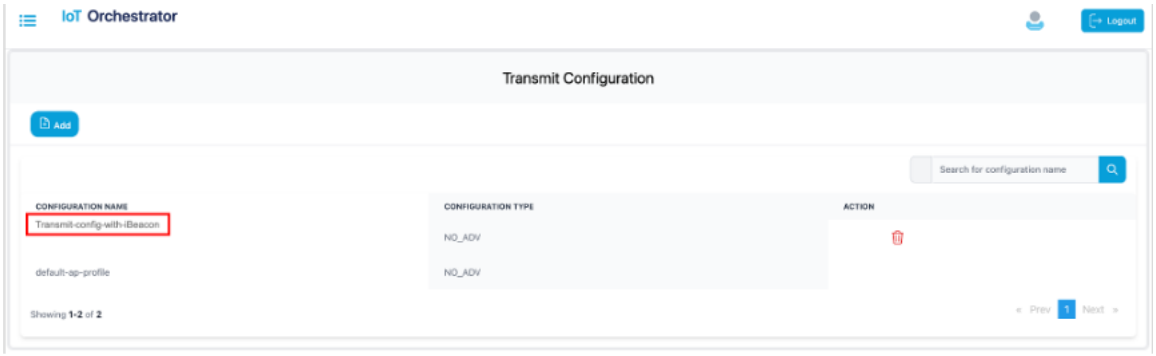


図 20.　　送信設定リスト

スキャン設定

ステップ **1.**　Cisco Catalyst 9800 ワイヤレスコントローラ Web UI にログインします。

ステップ **2.**　メニューから、[Configuration] > [Scan Configuration] を選択します。

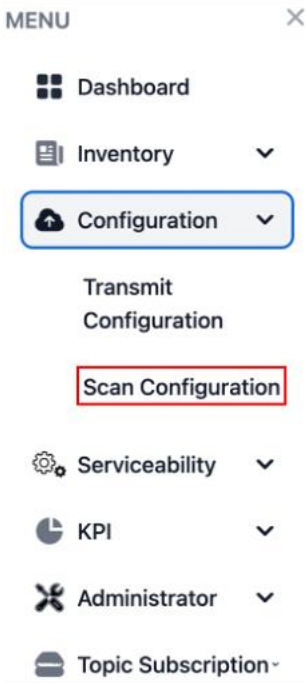


図 21.　　IoT オーケストレータ ダッシュボード：[Configuration] > [Scan Configuration]

ステップ **3.**　[Add] をクリックします。

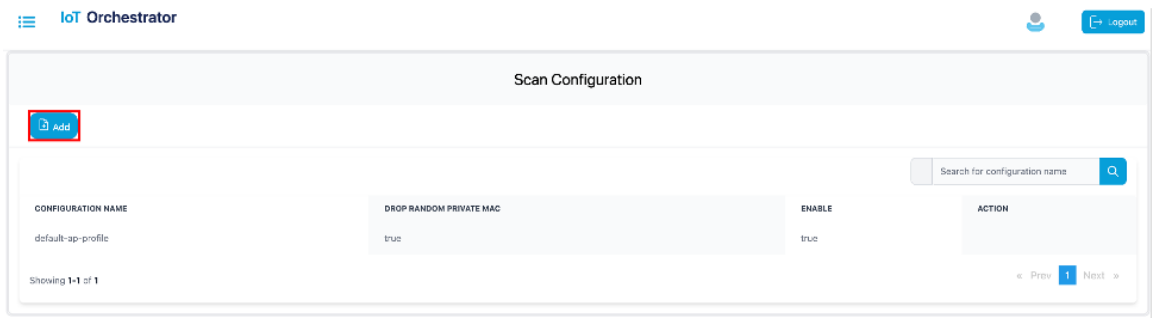


図 22.　[Scan Configuration] ページ

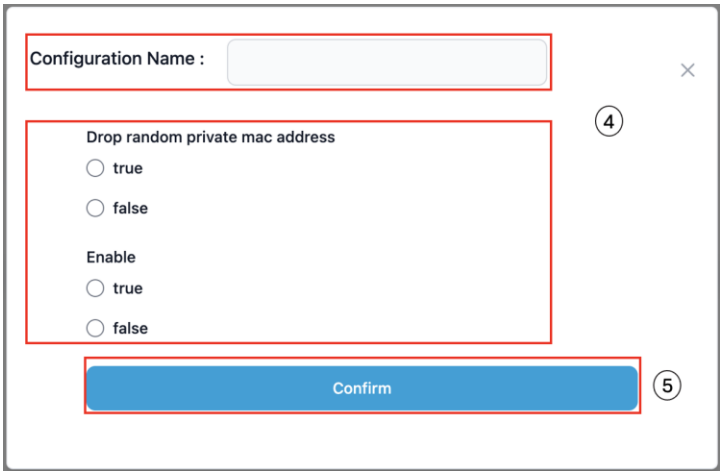


図 23.　[Configuration] ポップアップ

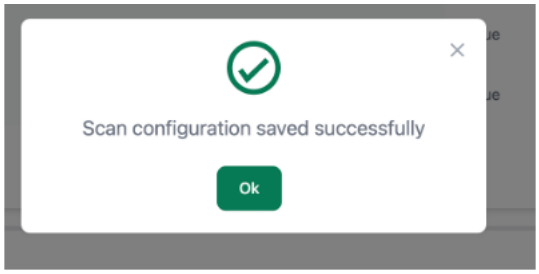


図 24.　スキャン設定が成功したことを示すメッセージ

値がスキャン設定リストに追加されます。

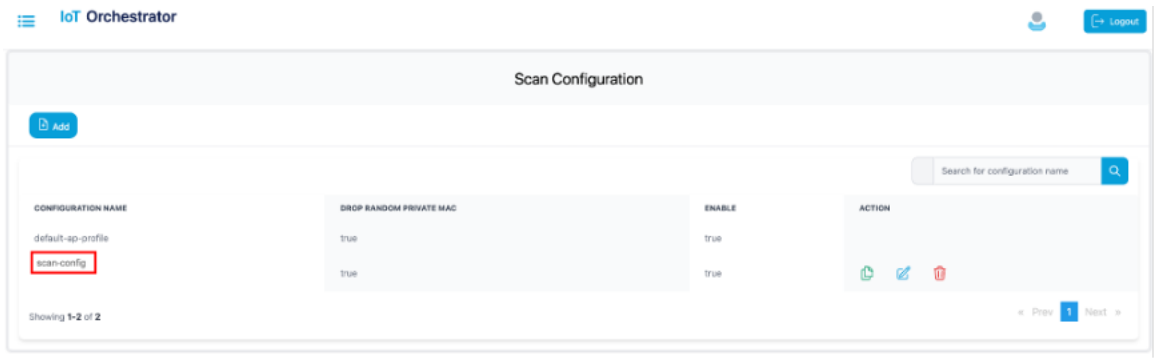


図 25.　スキャン設定リスト

サードパーティ アプリケーションの登録

概要

BLE デバイスにアクセスする場合は、IoT オーケストレータ アプリケーションにサードパーティ アプリケーションを登録する必要があります。

REST API 認証用のカスタム証明書のアップロード

デフォルトでは、IoT オーケストレータはポート 8081 で HTTPS 経由の API リクエストをリッスンします。API は、IoT オーケストレータによって生成された API キーを使用して認証され、HTTPS サーバーは、Day-0 フロー中に IoT オーケストレータによって自動的にプロビジョニングされた自己署名証明書を使用します。

デフォルトの証明書を上書きするには、次の手順を実行します。

ステップ 1. [Administrator] > [Certificate Management] ページを選択します。証明書を生成するには、「サーバー証明書の作成」セクションを参照してください。

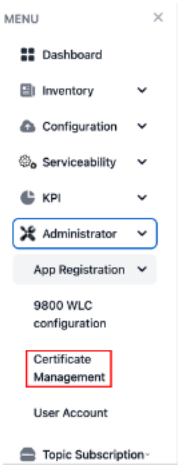


図 26.　[Administrator] > [Certificate Management Dashboard] ページ

[Upload Certificates] ページが表示されます。

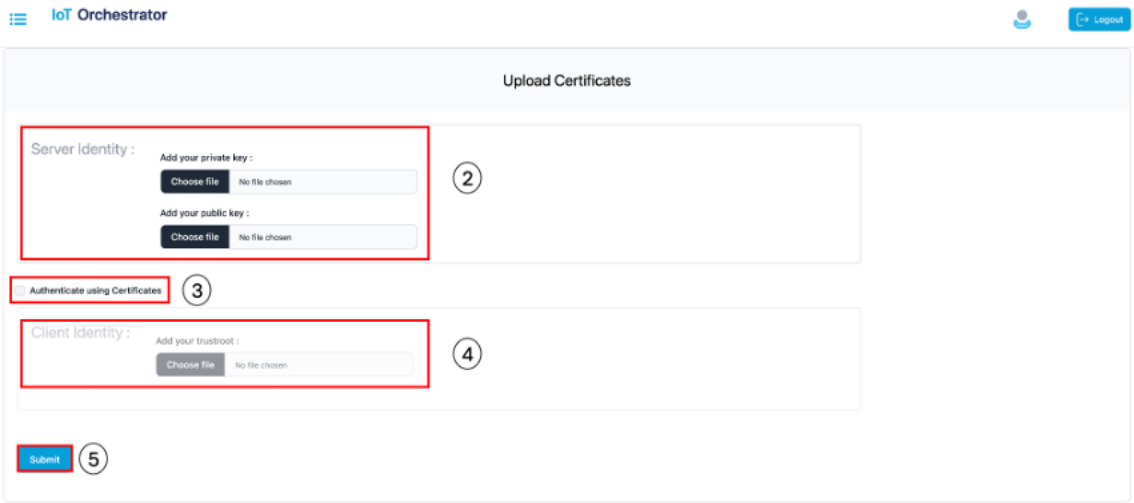


図 27.　[Upload Certificates] ページ

ステップ 2. [Server Identity] セクションで、秘密キーと公開キーを選択します。API キーを使用して RESTful API を認証する場合は、**ステップ 3** と**ステップ 4** をスキップします。

ステップ 3. 証明書を使用して REST API を認証するには、[Auth using Certificates] チェックボックスをオンにします。

ステップ 4. [Client Identity] セクションで、TLS ハンドシェイク中の証明書検証に用いるルート証明書を選択します。

ステップ 5. 証明書を検証するには、[Submit] をクリックします。

HTTPS サーバーが作成されたことを示すポップアップが表示されます。

サーバー証明書の作成

認証局（CA）によって生成された証明書を使用する場合は、次のプロセスが必要です。デフォルトでは、IoT オーケストレータは、データをオンボーディングまたは接続してストリーミングする準備ができており、REST API インターフェイスへの要求を保護するために、または TLS レイヤで MQTT ストリーミングを保護する際に、自己署名証明書を作成します。認証局（CA）によって署名された証明書が必要な場合は、証明書署名要求（CSR）が必須です。

次の手順で、この CSR を取得して IoT オーケストレータにアップロードする方法の詳細を説明します。

はじめる前に

- 端末で openssl を使用できる必要があります。

ステップ 1. 次のコマンドを実行して、秘密キーと証明書署名要求（CSR）を生成します。

```
openssl genrsa -out server.key 2048
openssl req -new -key server.key -out server.csr
```

プロンプトが表示されたら、次の情報を入力します。

- Country Name (2 letter code)
- State or Province Name（都道府県または州/郡の正式名）
- Locality Name（例：都市名）
- Organization Name（例：企業名）
- Organizational Unit Name（例：部署名）
- Common Name（IoT オーケストレータのドメイン名または IP アドレス）
- 電子メール アドレス

注： IoT オーケストレータ用の新しい証明書を生成するには、選択した認証局（CA）で生成された CSR ファイルを使用します。

ステップ 2. デジタル証明書サービスプロバイダーによって提供された **server.key** と証明書をアップロードします。

注：

- API キーを使用して RESTful API を認証する場合は、秘密キー（server.key）と、選択した認証局（CA）によって生成された証明書を添付する必要があります。前者は [Add your private key] セクション内で、後者は [Add your public key] セクション内で追加する必要があります。
- 証明書を使用して RESTful API を認証するには、秘密キー（server.key）と認証局（CA）によって生成された証明書に加えて、認証局（CA）の Web サイトからダウンロードできるルート証明書も必要です。ルート証明書は、[Client Identity] セクションの下にある [Add your trustroot] フィールドに追加する必要があります。

注：

- 秘密キーのファイル拡張子は **.key** である必要があります。
- 公開キーのファイル拡張子は **.crt** である必要があります。

IoT オーケストレータ アプリケーションとデータをやり取りするための、パートナーアプリケーションの登録

概要

IoT オーケストレータを使用して BLE デバイスにアクセスするには、パートナーアプリケーション（オンボードアプリケーション、制御アプリケーション、データ受信者アプリケーションなど）を登録する必要があります。

次のいずれかの方法を使用して、パートナーアプリケーションを登録できます。

- API キー（または）
- 証明書。詳細については、「HTTP サーバーを開いて API をリッスンするための、証明書とキーのアップロード」セクションの、「証明書を使用した認証」を参照してください。

承認方法

次の方法でキーを生成することで、アプリケーションを承認できます。

ステップ **1.** [Administrator] > [App Registration] > [Generate Keys] の順に選択します。

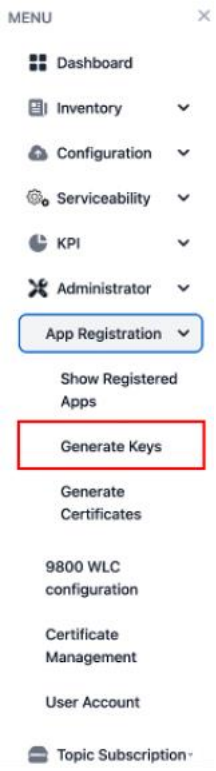


図 28. [Administrator] -> [App Registration] > [Generate Keys] ページ

[Generate Keys] ページが表示されます。

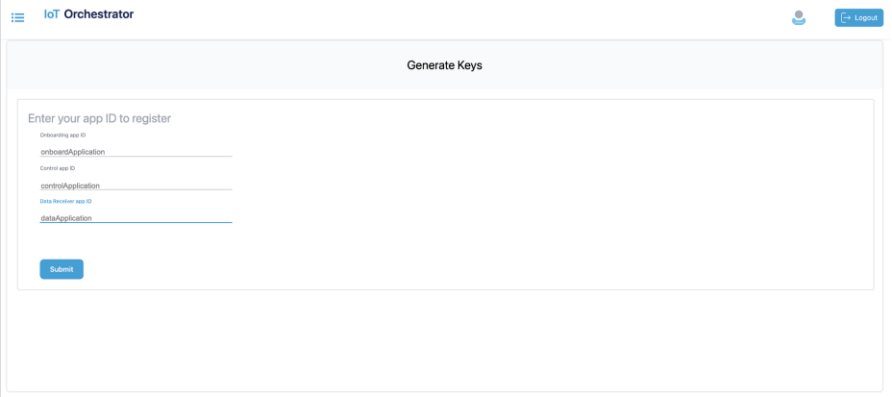


図 29.　　[Generate Keys]

ステップ 2. オンボードアプリケーション、制御アプリケーション、およびデータ受信者アプリケーションのアプリケーション ID を入力します。

注：

- アプリケーション ID は、キーを生成するために使用されます。
- アプリケーション ID には任意の文字列を使用できますが、コロン（「:」）文字はサポートされていないので、アプリケーション ID に使用しないでください。

ステップ 3. [Submit] をクリックします。

キーと秘密鍵が正常に生成されました。

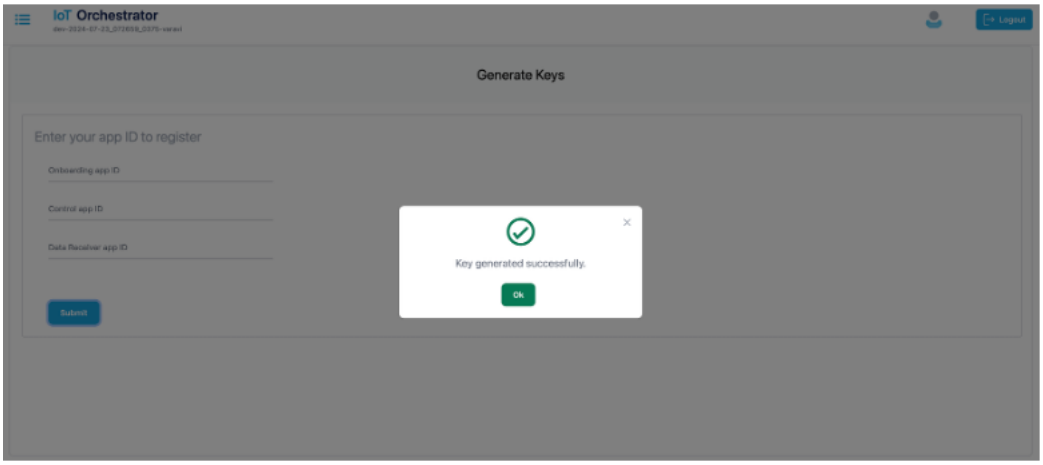


図 30.　　キーが生成されたことを示すメッセージのポップアップ

ステップ 4. メニューから、[Administrator] > [App Registration] > [Show Registered Apps] の順に選択します。

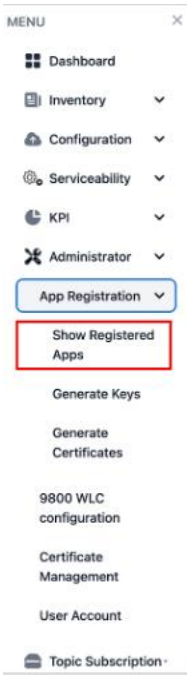


図 31.　[Administrator] > [App Registration] > [Show Registered Apps] ページ

[Registered Apps] ページが表示されます。アプリケーション用に生成されたキーまたは証明書を確認できます。

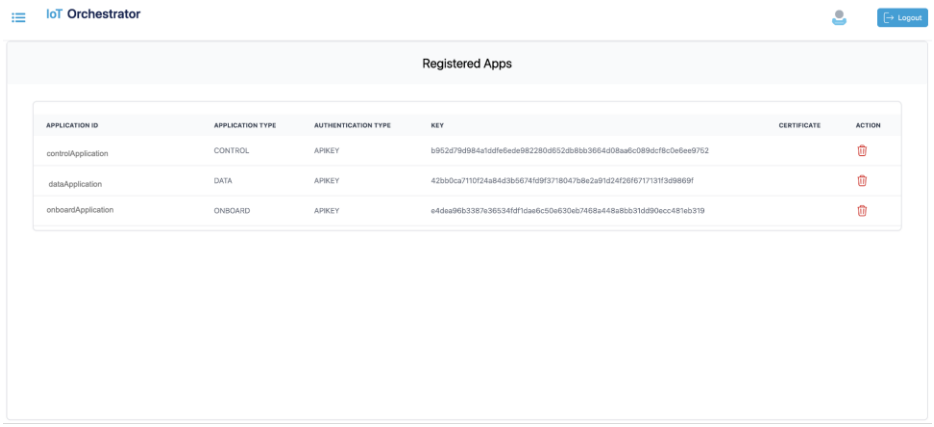


図 32.　アプリケーション用に生成されたキーまたは証明書

デバイスのオンボーディング

SCIM を使用した BLE デバイスのオンボーディングについては、『*Cisco Sensor Connect for IoT Services Programmability Guide*』の「Onboarding BLE Devices using SCIM」セクションを参照してください。

BLE インベントリ

概要

IoT オーケストレータでオンボードされた BLE デバイスの情報を確認できます。

オンボーディングされた BLE デバイスとそれぞれの状態が表示されます。

ステップ 1. メニューから、[Inventory] > [BLE Client] の順に選択します。

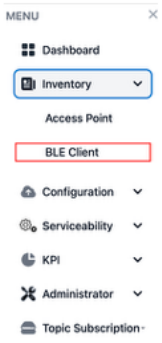


図 33. [Inventory] > [BLE Client] ページ

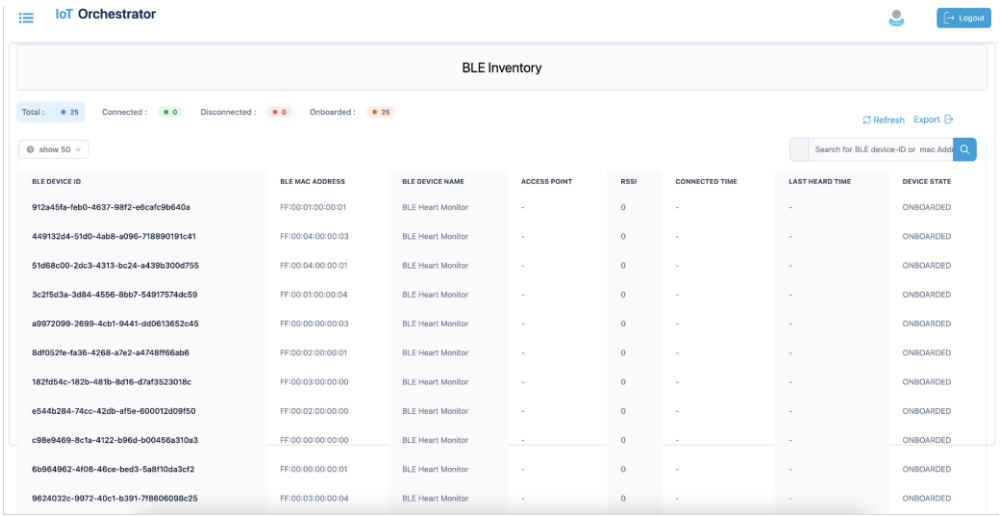


図 34. BLE インベントリ

デバイス制御とテレメトリ

データ受信者アプリケーションの登録

IoT オーケストレータからストリーミングメッセージを受信するには、データ受信者アプリケーションを登録する必要があります。

データアプリケーションの登録については、『*Cisco Sensor Connect for IoT Services Programmability Guide*』の「Registering the Data Receiver Application」セクションを参照してください。

トピックの登録

BLE デバイスからストリーミングメッセージを受信するには、トピックを登録する必要があります。

トピックの登録については、『Cisco Sensor Connect for IoT Services Programmability Guide』の「Registering a Topic」セクションを参照してください。

トピックへの登録

登録されたデータ受信者アプリケーションを使用して BLE デバイスからストリーミングメッセージを受信するには、トピックに登録する必要があります。

トピックへの登録については、『*Cisco Sensor Connect for IoT Services Programmability Guide*』の「Subscribing to Advertisements and Notifications」セクションを参照してください。

アセットトラッキングに関する **BLE** コネクションレスのユースケース

BLE コネクションレスのユースケースについては、オンボードされた BLE デバイスのアドバタイズメントをデータ受信者アプリケーションで受信する必要があります。『Cisco Sensor Connect for IoT Services Programmability Guide』の「Use Case 1: Asset Tracking」セクションを参照してください。

BLE 接続ベースのユースケース

BLE 接続ベースのユースケースについては、『Cisco Sensor Connect for IoT Services Programmability』の「Use Case 2: Remote Patient Health Monitoring (requiring BLE connection, reading, and writing)」セクションを参照してください。

GATT 通知を使用した **BLE** 接続ベースのユースケース

GATT 通知を使用した BLE 接続ベースのユースケースについては、『*Cisco Sensor Connect for IoT Services Programmability Guide*』の「Use Case 3: BLE Notification-based Use Cases」セクションを参照してください。

リリース表

このドキュメントは、Cisco Sensor Connect for IoT Services のクイックスタートガイドです。

日付	リリースバージョン
2025 年 4 月 1 日	リリース 1.1

通信、サービス、およびその他の情報

- シスコからタイムリーな関連情報を受け取るには、Cisco Profile Manager でサインアップしてください。
- 重要なテクノロジーを活用してビジネス成果を実現するには、シスコ サービスにアクセスしてください。
- サービスリクエストを送信するには、Cisco Support にアクセスしてください。
- 検証済みの安全なエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、Cisco DevNet にアクセスしてください。
- 一般的なネットワーク、トレーニング、認定関連の出版物を入手するには、Cisco Press にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、Cisco Warranty Finder にアクセスしてください。

シスコのバグ検索ツール

シスコのバグ検索ツール（BST）は、シスコ製品とソフトウェアの障害と脆弱性の包括的なリストを管理するシスコバグ追跡システムへのゲートウェイです。BST は、製品とソフトウェアに関する詳細な障害情報を提供します。

マニュアルに関するフィードバック

シスコの技術マニュアルに関するフィードバックを提供するには、それぞれのオンラインドキュメントの右側のペインにあるフィードバックフォームを使用してください。

米国本社
カリフォルニア州サンノゼ

アジア太平洋本社
シンガポール

ヨーロッパ本社
アムステルダム（オランダ）

シスコは世界各国に約 400 のオフィスを開設しています。オフィスの住所、電話番号、FAX 番号は当社の Web サイト（www.cisco.com/jp/go/offices）をご覧ください。

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。

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。