Cisco Spaces Connect for IoT Services Quick Start Guide

Release 1.0.0

Overview of Cisco Spaces Connect for IoT Services

Cisco Spaces Connect for IoT Services solution enables delivery of advanced BLE capabilities over Cisco Catalyst Wireless infrastructure. The key component of this solution is the IoT Orchestrator which is a Cisco IOx application that can be deployed on any existing Cisco Catalyst 9800 Wireless Controller platforms running software version Cisco IOS-XE 17.15.1 and later. With the Cisco Spaces Connect for IoT Services solution, you have capabilities to securely onboard and control BLE devices, and consume data telemetry using the Message Queuing Telemetry Transport (MQTT).

Prerequisites for IoT Orchestrator

- Controller must be configured for initial configuration with APs joined and clients connected to the network.
- Controller must run on version Cisco IOS-XE 17.15.1 and later.
- Download the IoT Orchestrator (**Spaces Orchestrator Software**) image that will be posted in the following page:

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

Note: The **Spaces Connect for IoT Services** is now in **Public Beta**.

For more information about the Spaces Connect for IoT Services, see the **Related Documentation**.

For further help, you can reach out to Cisco TAC or write to: c9800-spaces-connect-for-iot-services@external.cisco.com

Related Documentation

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

Licenses

- Spaces Smart Ops
- Spaces ACT
- Spaces Unlimited

System Configuration

Supported Cisco Wireless Controller Platforms

- Cisco Catalyst 9800-L Wireless Controller
- Cisco Catalyst 9800-CL Wireless Controller

Note:

- In newer C9800-CL platform deployment, choose one of the two new "**platform resource app-heavy**" templates to allocate additional resources for IoT Orchestrator. Once the C9800-CL node comes up, you must configure the "**platform resource app-heavy**" command in the configuration prompt mode before starting the IoT Orchestrator Day 0 deployment. To activate the template, you will need to save and reboot the controller.
- C9800-CL does not support Small template (low throughput and high throughput) for IoT Orchestrator deployment.
- C9800-CL Medium template (low throughout) supports 6 vCPUs and 16 GB RAM.

- Cisco Catalyst 9800-40 Wireless Controller
- Cisco Catalyst 9800-80 Wireless Controller
- Cisco Catalyst CW9800M Wireless Controller
- Cisco Catalyst CW9800H1 and CW9800H2 Wireless Controllers

Supported Access Points

- C9105AX
- C9115AX
- C9120AX
- C9130AX
- C9124AX
- C9136I
- CW9162I
- CW9164I
- CW9166I

Note: C9115AX APs support only scanning and advertising.

Deployment Workflow

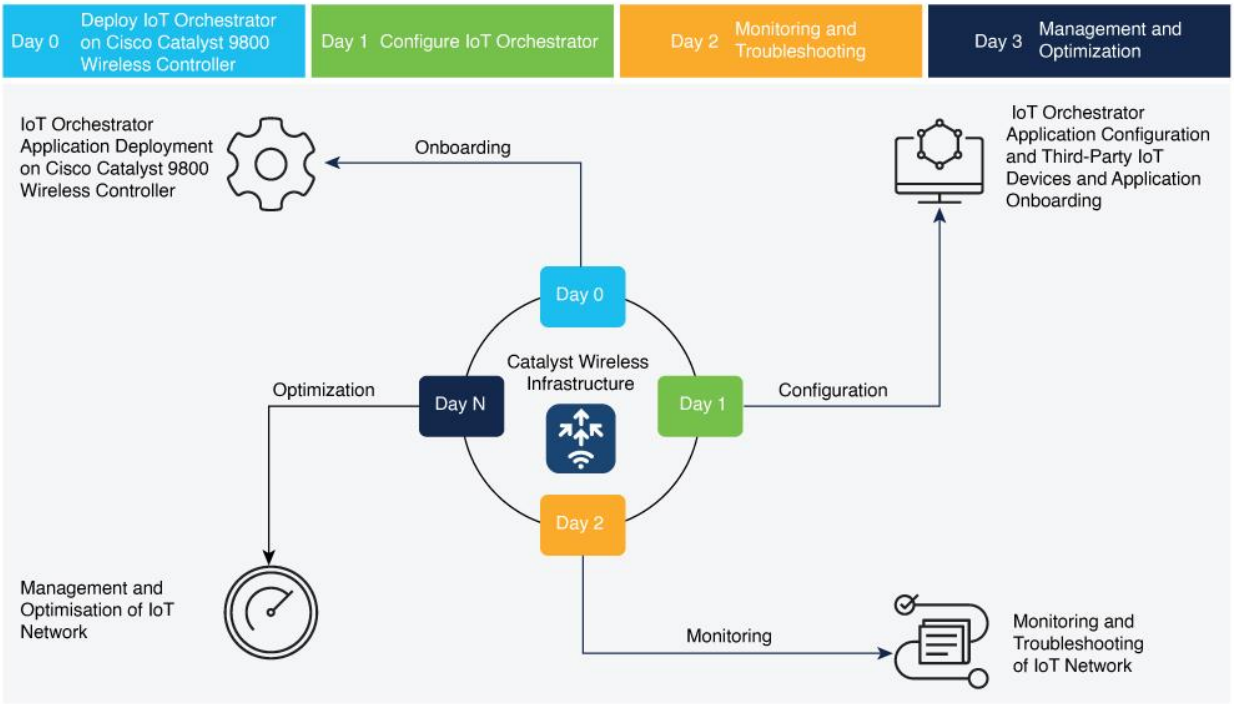


Figure 1.
Deployment Workflow

Day-0 Activities

- Deploying IoT Orchestrator Application on Cisco Catalyst 9800 Wireless Controller
- Launching IoT Orchestrator
- Day-0 WebUI Wizard for IoT Orchestrator Application
- Changing your Username and Password

Day-1 Activities

- Day-1: Configuring Cisco Catalyst 9800 Wireless Controller from IoT Orchestrator
- Register the Third-Party Applications
- Uploading Certificate and Key to Open HTTP Server and Listen for APIs
- Registering Partner Application to Interact with the IoT Orchestrator Application

Day-0: Deploying the IoT Orchestrator Application on Cisco Catalyst 9800 Wireless Controller

Before you begin

- Download IoT Orchestrator and save it on your system where you will login to the Controller Web UI.

Summary:

If you want to use the IoT Orchestrator application, you will need to deploy the IoT Orchestrator application on Cisco Catalyst 9800 Wireless Controller.

Deploying IoT Orchestrator Application on Cisco Catalyst 9800 Wireless Controller

Step 1. Log in to the Cisco Catalyst 9800 Wireless Controller Web UI.

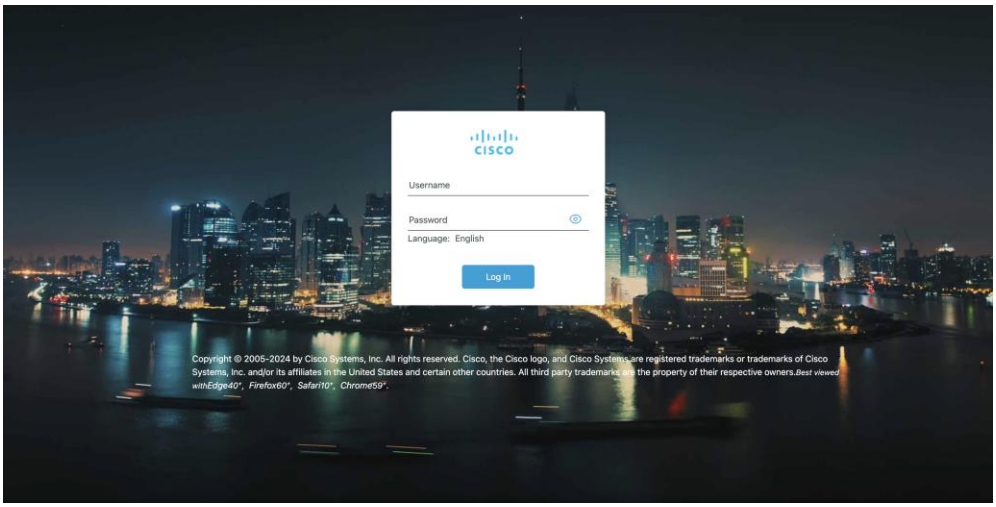
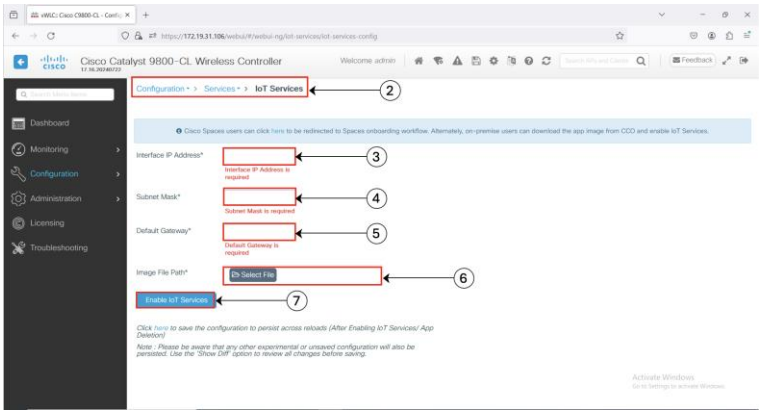


Figure 2.
Cisco Catalyst 9800 Wireless Controller Web UI

Step 2. Navigate to **Configuration > Services > IoT Services**.



Step 3. Enter the private IP address.

Note: The private IP address must be assigned to the IoT Orchestrator. The minimum size of the mask is /30 that allows two valid hosts (IoT Orchestrator and VirtualPortGroup Interface of Cisco Catalyst 9800 Controller).

Step 4. Enter the subnet mask IP address.

Note: The private and subnet mask IP addresses must be unique or different from other subnets configured in the controller. If you configure the private and subnet mask IP addresses that overlaps with other interfaces, you will get an error message.

Step 5. Enter the default gateway IP address.

Note: The default gateway IP address is the IP address of the VirtualPortGroup interface in Cisco Catalyst 9800 Controller.

Step 6. In the **Image File Path** field, click **Select File** to select the IoT Orchestrator image and click **Open**.

Note: You must have the IoT Orchestrator image downloaded on your local machine.

Step 7. Click **Enable IoT Services** to upload the image from your machine to the Cisco Catalyst 9800 controller.

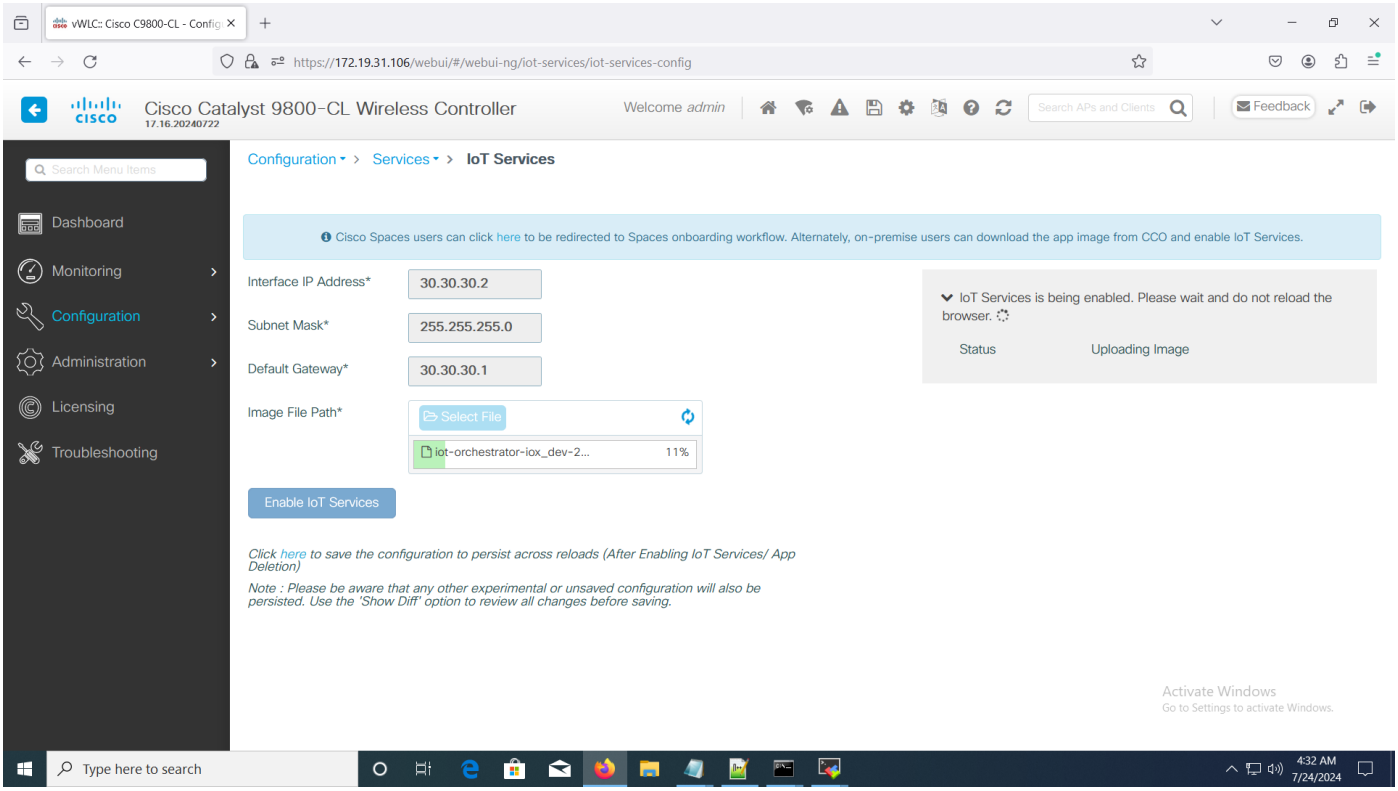


Figure 3.
Enabling IoT Services

You get to view a banner that displays the following status:

- Installing
- Activating

- Starting
- Running

Note: It might take few minutes to complete from Installation to Running.

Note:

- When the status moves from Installing to Activating, this implies that the application is installed by the Cisco IOS-XE infrastructure.
- When the status moves from Activating to Starting, this implies that the application is getting started by the Cisco IOS-XE infrastructure.
- When the status moves from Starting to Running, this implies that the application is in Running state.

Thus, the IoT Orchestrator image is uploaded from your device to the Cisco Catalyst 9800 Wireless Controller.

Once the IoT Orchestrator application deployment is successful, you get to view the application name (IoT Orchestrator by default) and IP address of the application.

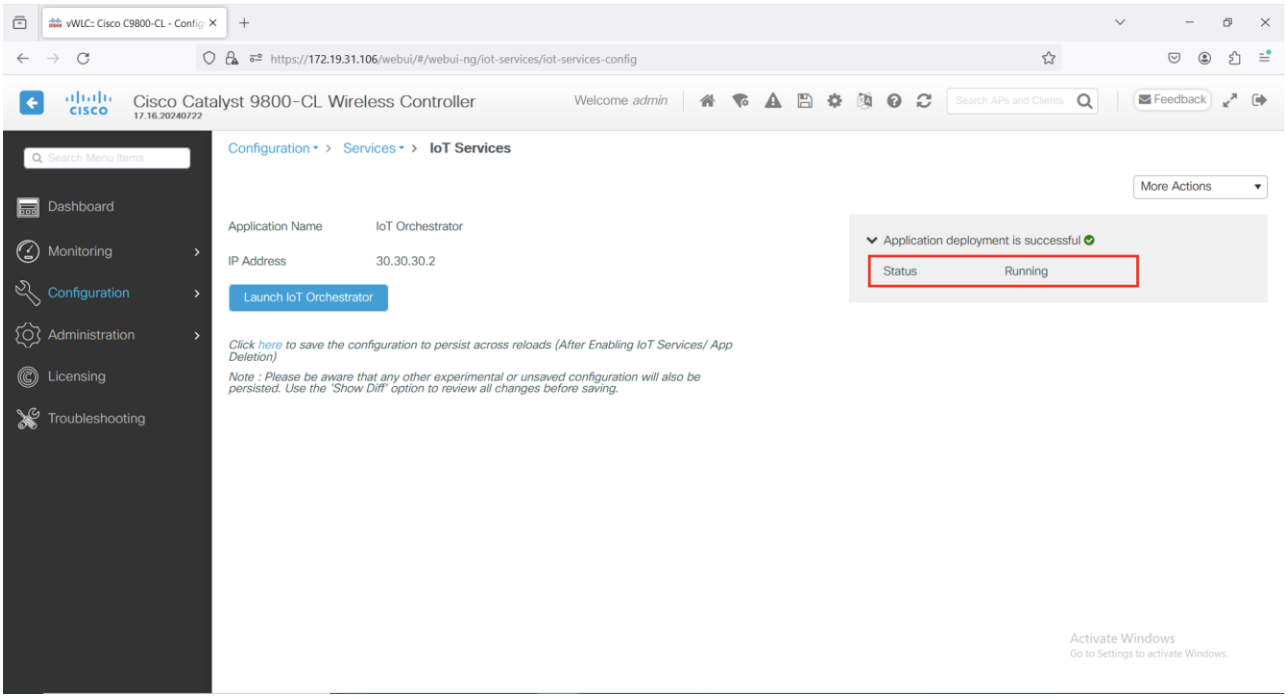


Figure 4.
Viewing Application Name and IP Address

NOTE: The Cisco IOS-XE application framework is used to deploy and start the containers. The application now runs as an IOx container in the Cisco Catalyst 9800 Wireless Controller.

Launching IoT Orchestrator

Before you begin

- Ensure that the IoT Orchestrator status is in Running state.

Summary:

If you want to access the IoT Orchestrator Web UI, you will need to launch the IoT Orchestrator application.

Procedure

On the **Configuration > Services > IoT Services** page, click **Launch IoT Orchestrator**.

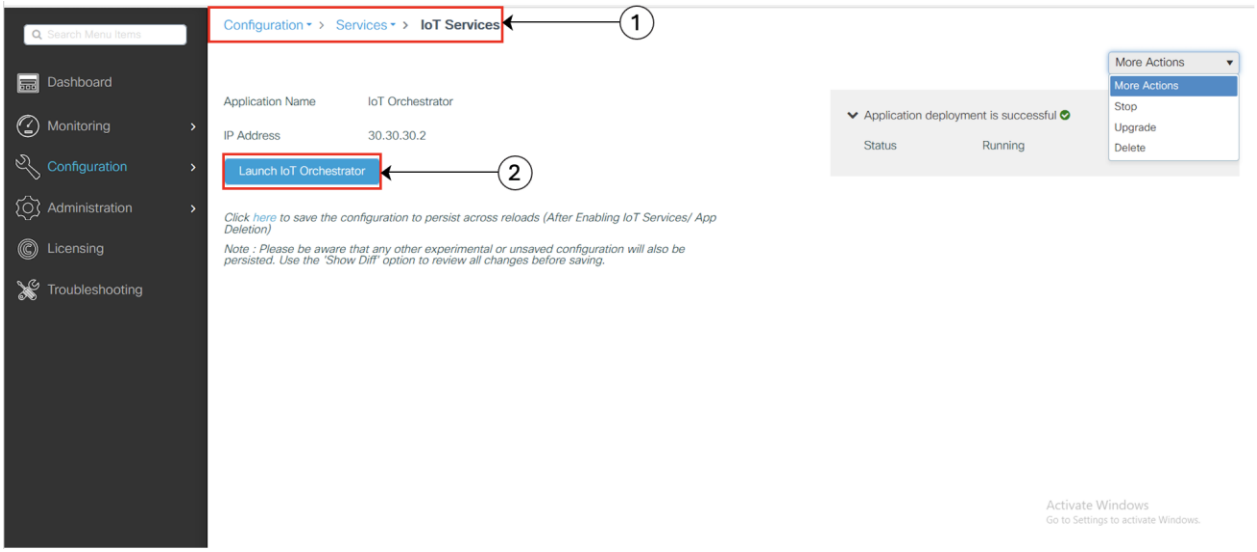
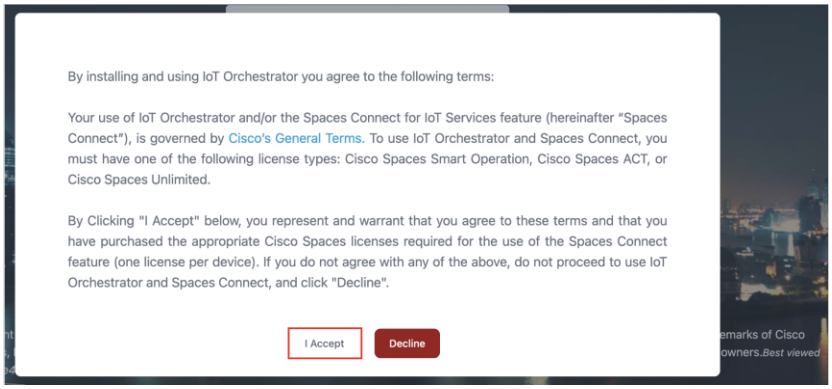


Figure 5.
Launching IoT Orchestrator

Note: To verify the IP network is reachable, you will need to ping the IP address using the terminal session.

Licensing Details to Use IoT Orchestrator

Read the terms and conditions and click **I Accept**.



The **IoT Orchestrator** login page is displayed.

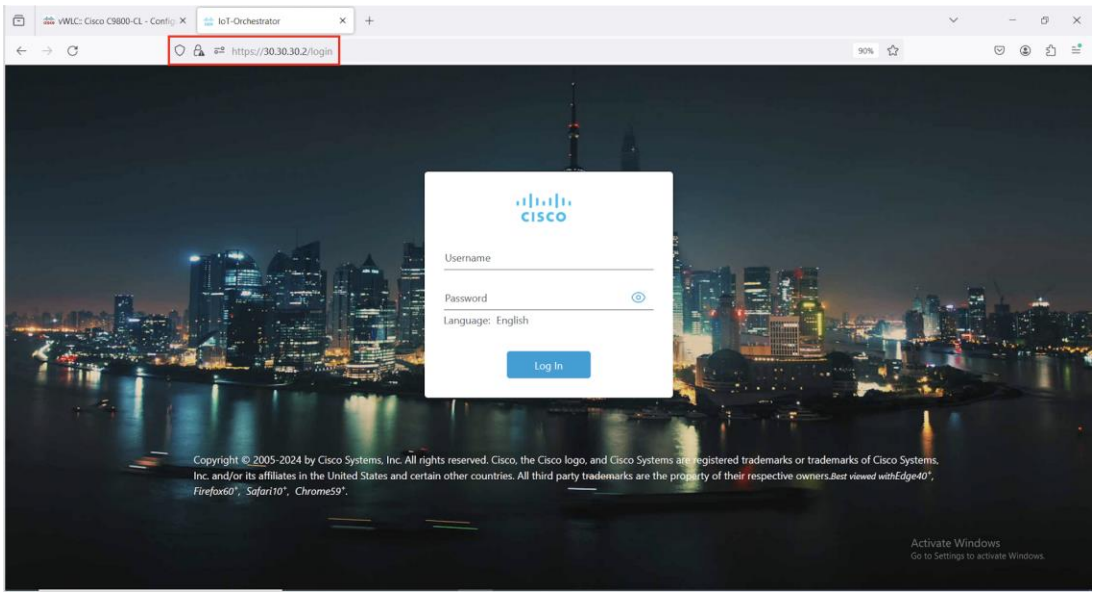


Figure 6.
IoT Orchestrator Login Page

Day-0 WebUI Wizard for IoT Orchestrator Application

Summary:

To login to the IoT Orchestrator application for Day-0, you will need to perform the following steps:

Procedure

Enter **admin** for username and **password** for password (default credentials).

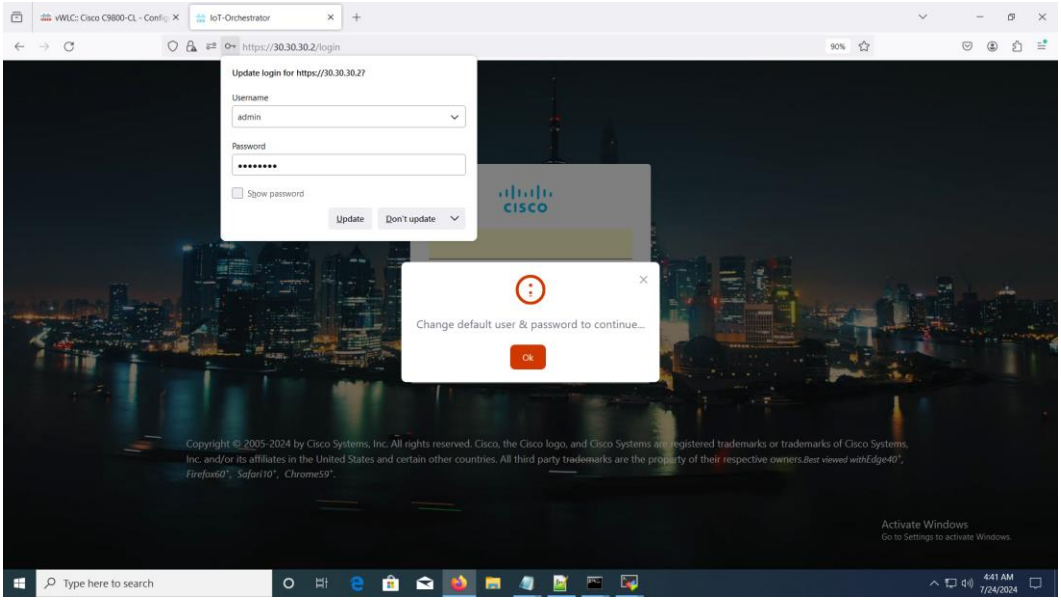


Figure 7.
Default Credentials Login Page

Changing your Username and Password

Summary:

To create a Day-0 user profile, you will need to change the default username and password.

Note:

- You will need to enter the IoT Orchestrator password in the Login Page.
- This login is the IoT Orchestrator login credentials and not the same as the controller login credentials.

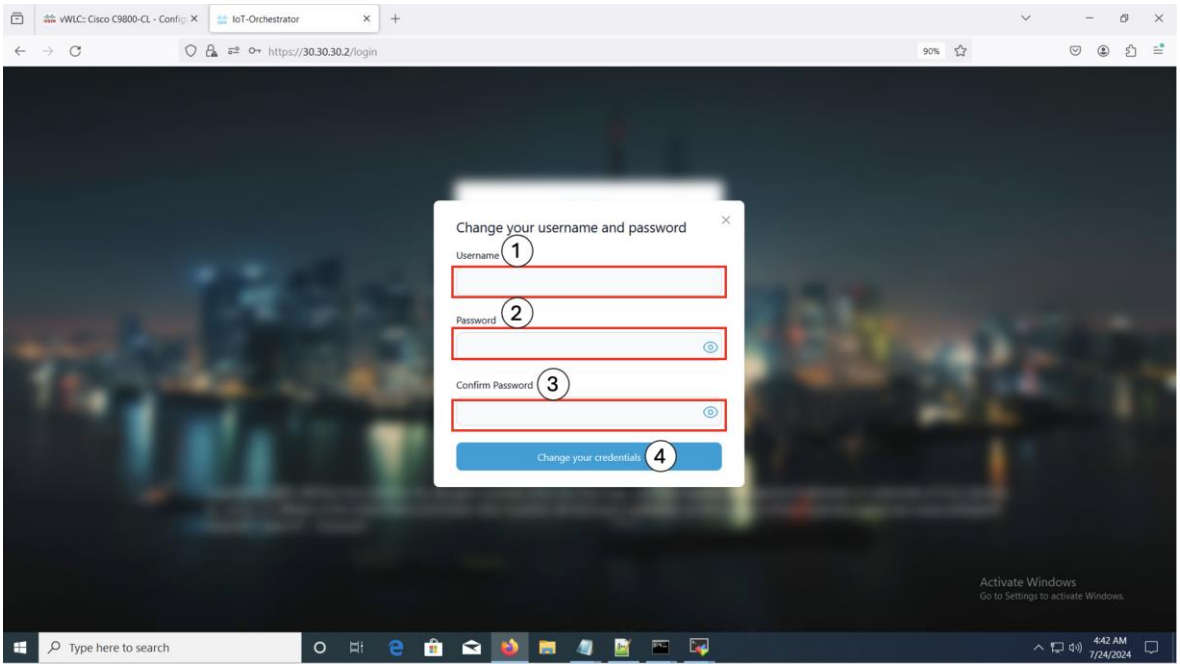


Figure 8.
Changing your Username and Password

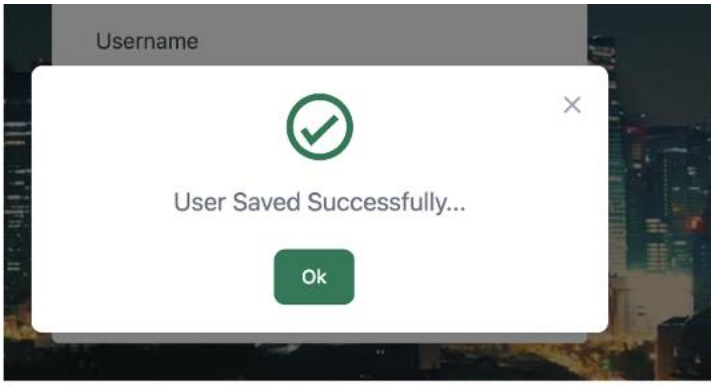


Figure 9.
User Saved Successful Pop-Up

Note: If you do not remember your admin credentials, you will need to trigger a Day 0 deployment (delete and redeploy the application).

Day-1: Configuring Cisco Catalyst 9800 Wireless Controller from IoT Orchestrator

In the IoT Orchestrator dashboard, choose the **Administrator > 9800 Wireless Controller configuration** page and perform the following:

Summary:

To connect the APs (available in the Controller) to the IoT Orchestrator, you will need to connect the IoT Orchestrator to the Cisco Catalyst 9800 Wireless Controller and push the token and certificate to the controller.

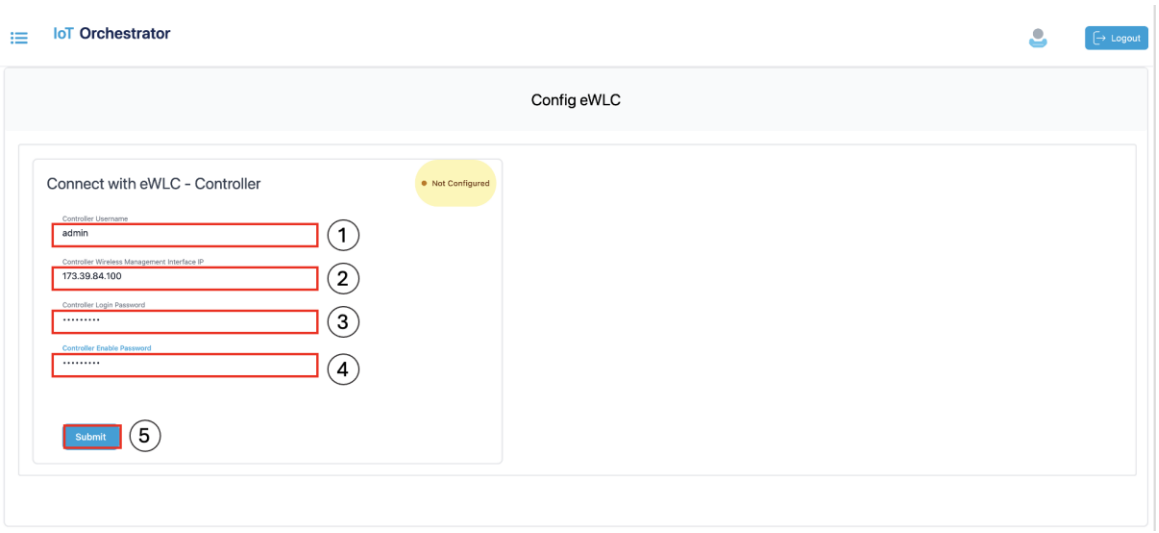


Figure 10.
Connect with the Controller

A pop-up window is displayed stating the following:

The connection establishment with the controller is successful.

Note: To verify if all the APs connected to the controller are connected to the IoT Orchestrator, check the **Inventory > Access Points** page from the IoT Orchestrator UI.

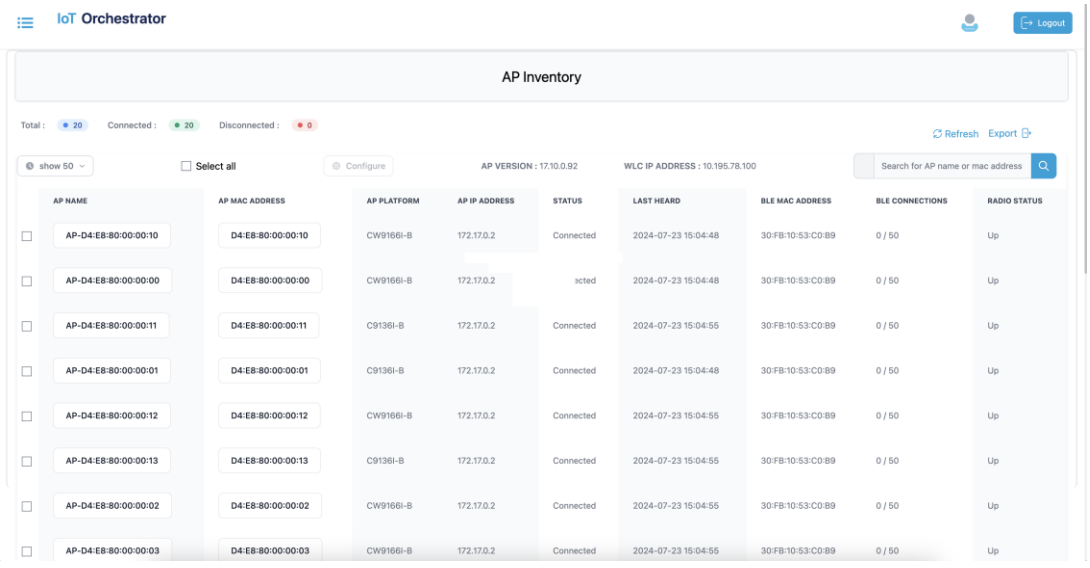


Figure 11.
AP Inventory Page

AP BLE Transmit Configuration (Optional)

Transmit Configuration

Procedure

Step 1. Log in to the Cisco Catalyst 9800 Wireless Controller Web UI.

Step 2. From the **MENU**, choose **Configuration > Transmit Configuration**.

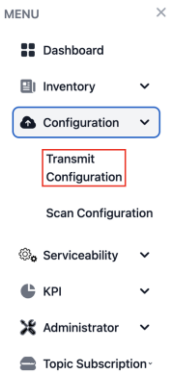


Figure 12.
IoT Orchestrator Dashboard – Configuration > Transmit Configuration

Step 3. Click **Add**.

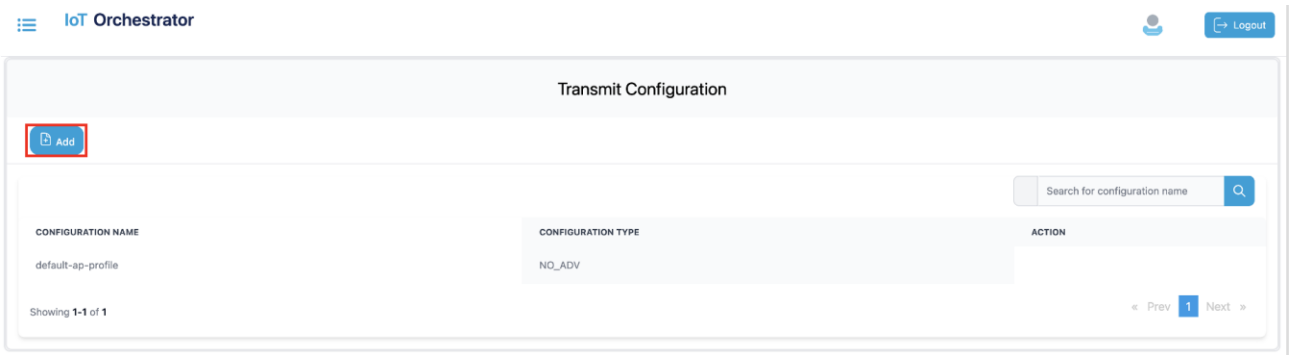


Figure 13.
Transmit Configuration Page

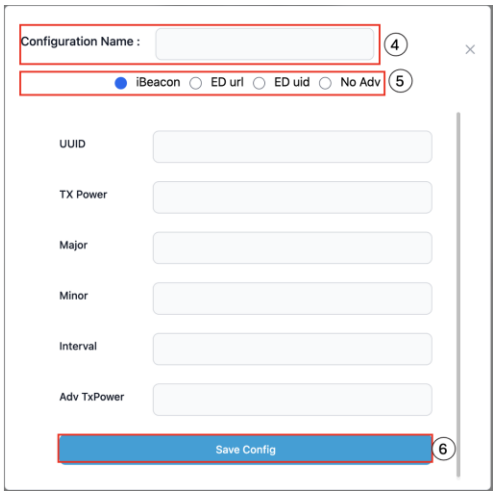


Figure 14.
Transmit Configuration – Add Page

Step 4. Enter a name for the transmit configuration.

Step 5. Choose one of the following transmission methods:

- **iBeacon**: Enter the UUID, TX power, major, minor, interval, and Adv TxPower values.
- **ED url**: Enter the ED url.

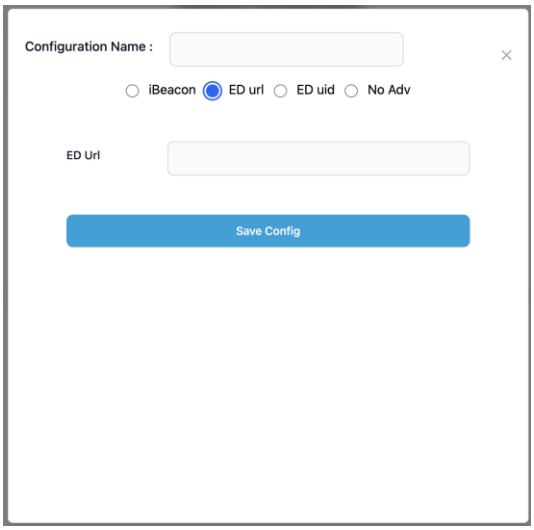


Figure 15.
ED url Configuration

- **ED uid**: Enter the ED ns and ED instance values.

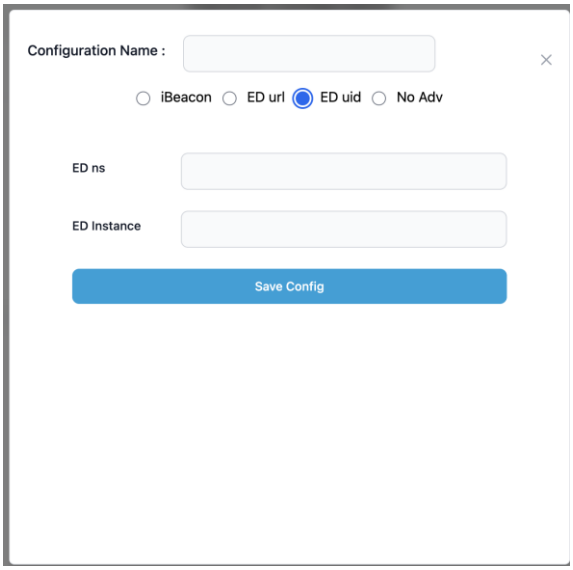


Figure 16.
ED uid Configuration

- **No Advertisement:**

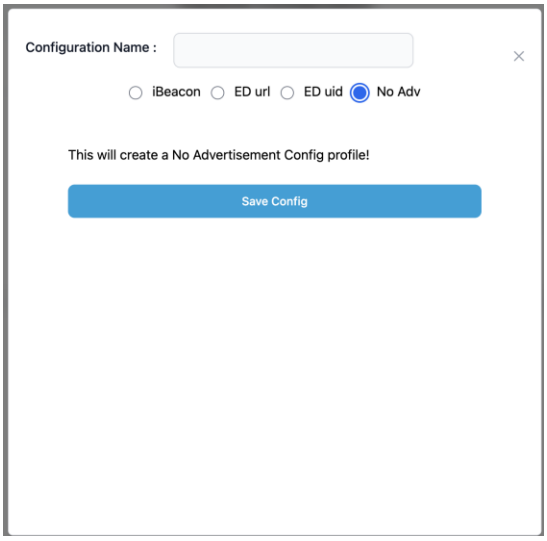


Figure 17.
No Adv Configuration

Step 6. Click **Save Config**.

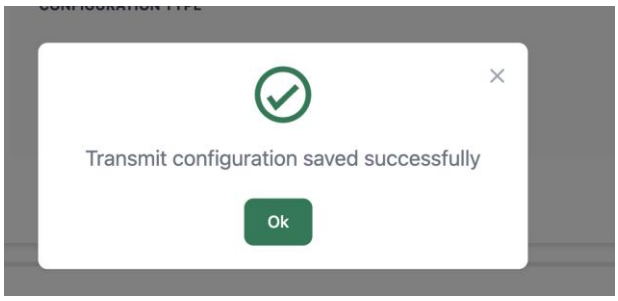


Figure 18.
Transmit Configuration Successful Message

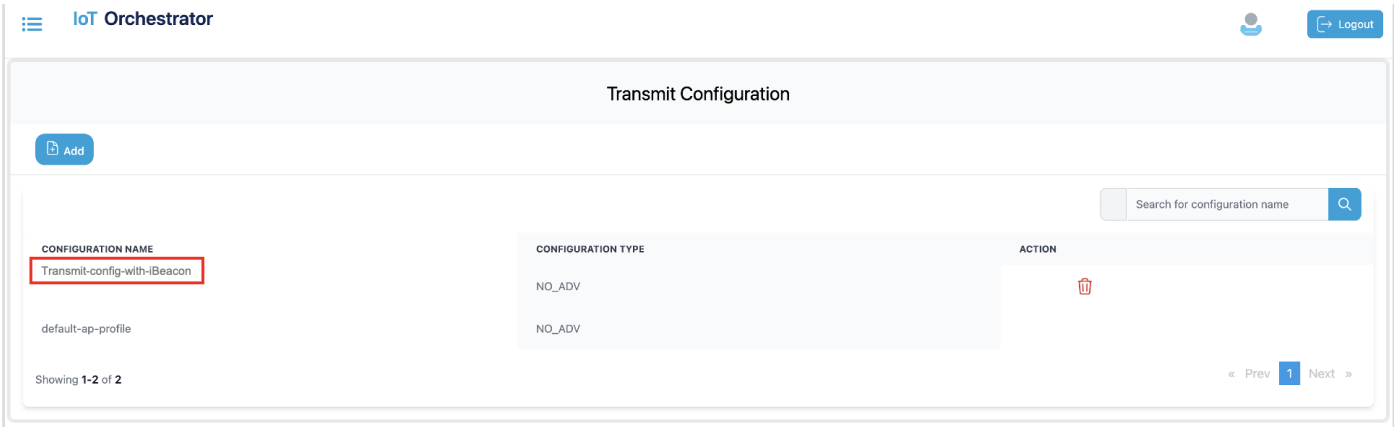


Figure 19.
Transmit Configuration List

Scan Configuration

Step 1. Log in to the Cisco Catalyst 9800 Wireless Controller Web UI.

Step 2. From the **MENU**, choose **Configuration > Scan Configuration**.

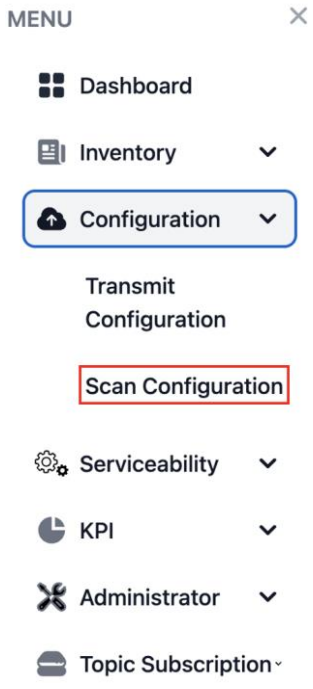


Figure 20.
IoT Orchestrator Dashboard – Configuration > Scan Configuration

Step 3. Click **Add**.

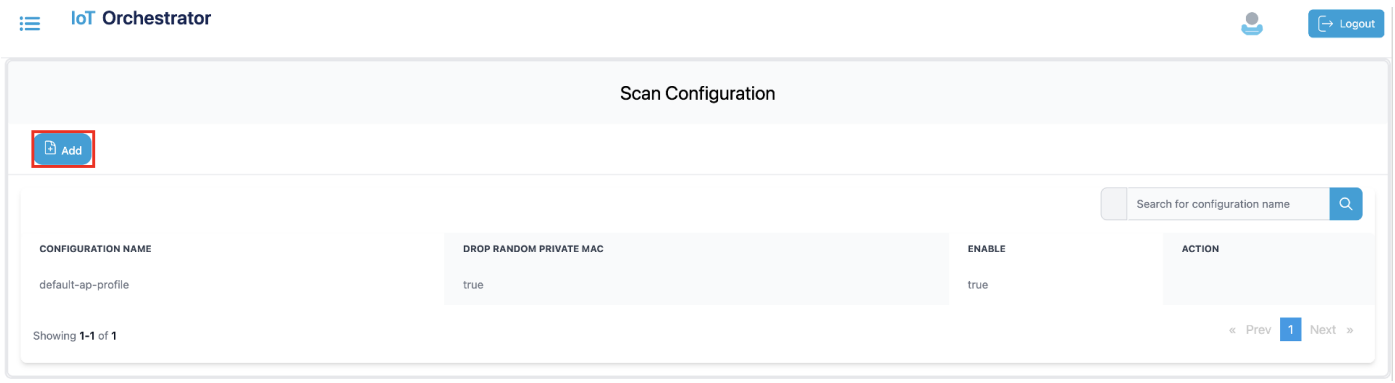


Figure 21.
Scan Configuration Page

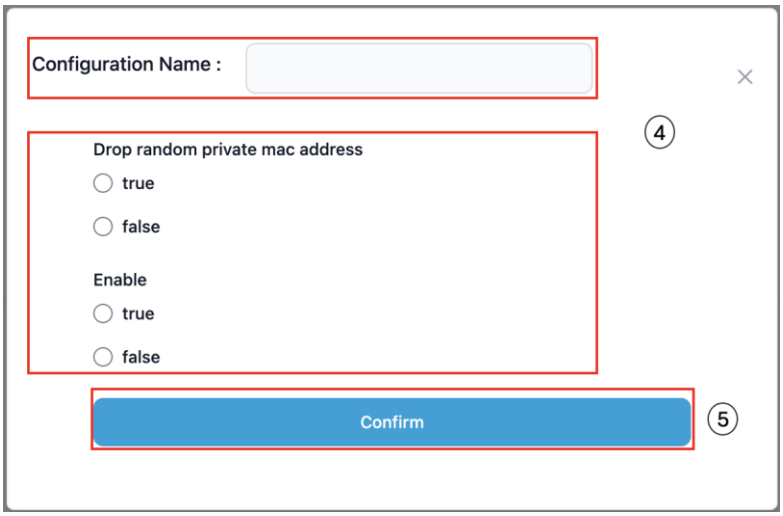


Figure 22.
Configuration pop-up

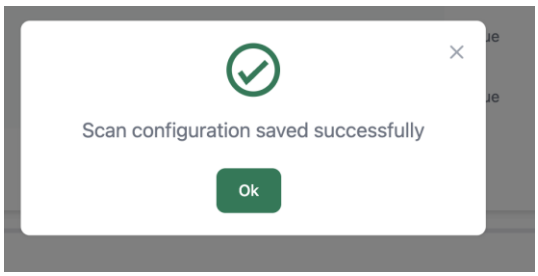


Figure 23.
Scan Configuration Successful Message

The value gets added to the scan configuration list.

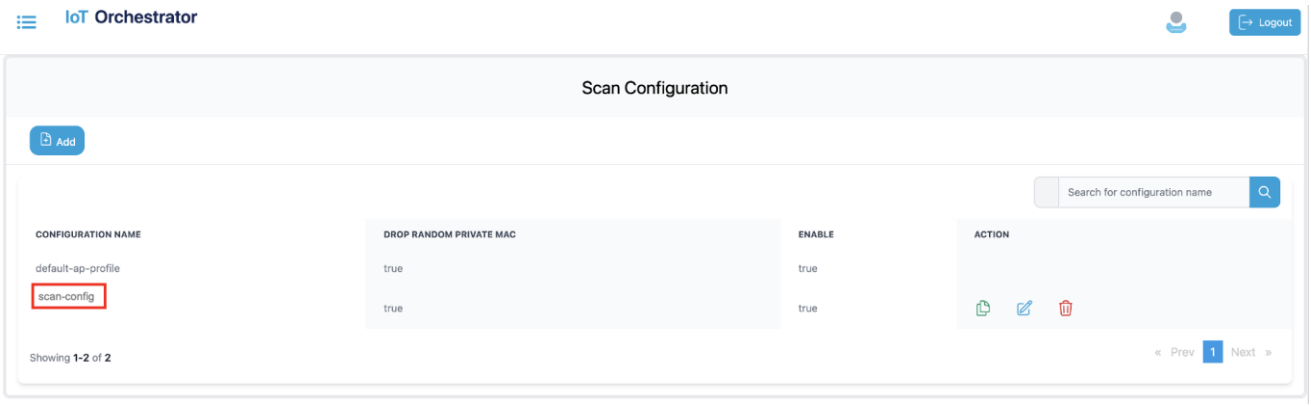


Figure 24.
Scan Configuration List

Register the Third-Party Applications

Summary:

If you want to access the BLE devices, you will need to register your third-party applications in the IoT Orchestrator application.

Uploading Certificate and Key to Open HTTP Server and Listen for APIs

Before you begin

By default, the IoT Orchestrator has the HTTP port open and APIs are authenticated using the API keys.

Summary:

If you want to use your certificates for authentication, you will need to attach your certificates in the IoT Orchestrator UI.

To overwrite the default certificates, perform the following:

Step 1. Choose the **Administrator > Certificate Management** page. To generate certificates, see **Creating a Server Certificate** section.

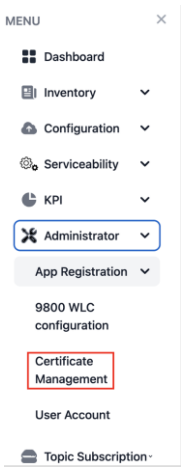


Figure 25.
Administrator > Certificate Management Dashboard Page

The **Upload Certificates** page is displayed.

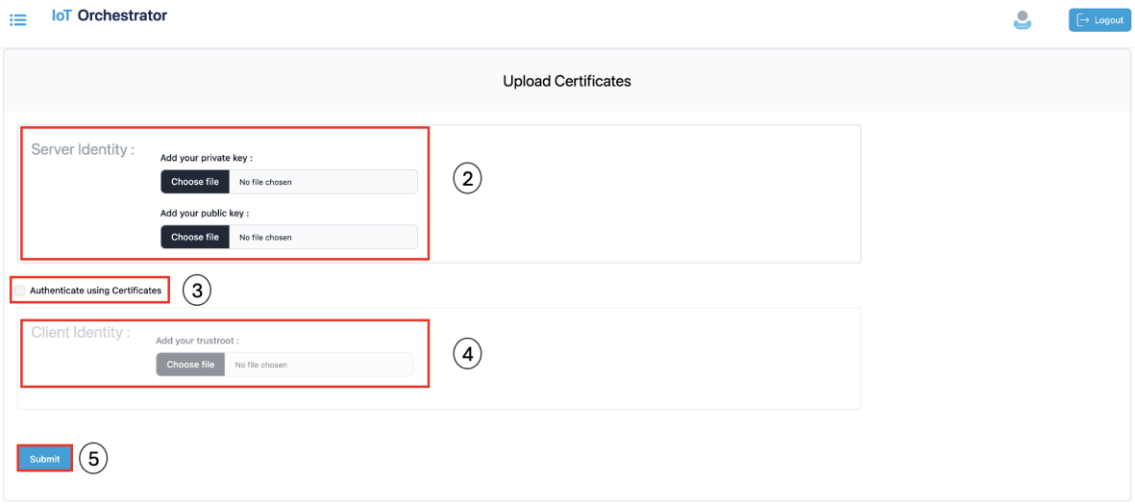


Figure 26.
Upload Certificates Page

Step 2. In the **Server Identity** section, select the private and public keys. To authenticate RESTful APIs using API keys, skip **Step 3** and **Step 4**.

Step 3. Select the **Auth using Certificates** check box to authenticate REST APIs with certificates.

Step 4. In the **Client Identity** section, select the certificate.

Step 5. Click **Submit** to validate the certificate and key.

A pop-up is displayed stating that the HTTPS server is created.

Creating a Server Certificate

Before you begin

- The **openssl** must be available in the terminal.

Summary:

If you want to create a server certificate with your organization details, you will need to perform the following:

To create a server certificate, perform the following:

Step 1. Generate a private key and create a self-signed Root Certificate Authority (CA) by executing the following commands:

```
openssl genrsa -out rootCA.key 2048
openssl req -x509 -new -nodes -key rootCA.key -sha256 -days 3650 -out rootCA.crt
```

Step 2. Generate a private key and Certificate Signing Request (CSR) for server by executing the following commands:

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

Step 3. Sign the server CSR with the root CA certificate to generate a server certificate using the following command:

```
openssl x509 -req -in server.csr -CA rootCA.crt -CAkey rootCA.key -CAcreateserial -out server.crt -days 365 -sha256
```

Step 4. Upload the **server.key** and **server.crt** files in the IoT Orchestrator GUI.

Note: The following six files are generated when you create a server certificate:

- rootCA.key
- rootCA.crt
- server.key
- server.csr
- rootCA.srl
- server.crt

- If you want to authenticate RESTful APIs using APIKeys, you must attach the **server.key** and **server.crt** in **Add your private key** and **Add your public key** sections respectively.
- If you want to authenticate RESTful APIs using certificates, you must attach the **server.key**, **server.crt**, and **rootCA.crt** in **Add your private key**, **Add your public key**, and **Add your trustroot** (Under **Client Identity**) sections respectively.

Note:

- The file extension for private key must be **.key**.
- The file extension for public key must be **.crt**.

Registering Partner Application to Interact with the IoT Orchestrator Application

Summary:

You need to register the partner applications (such as onboard application, control application, and data receiver application) to access BLE devices using the IoT Orchestrator.

You can register the partner applications using one of the following ways:

- API keys (or)
- Certificates. For information, see the **Auth using Certificates** in **Uploading Certificate and Key to Open HTTP Server and Listen for APIs** section.

How do you authorize:

You can authorize the applications by generating keys.

Procedure

Step 1. Choose the **Administrator > App Registration > Generate Keys**.

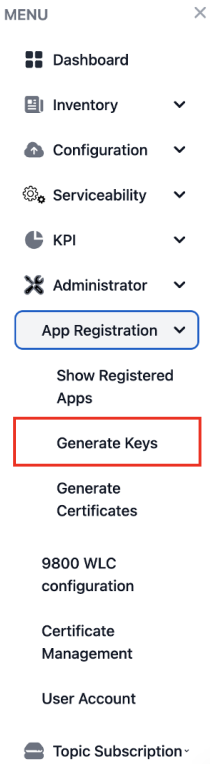


Figure 27.
Administrator > App Registration > Generate Keys Page

The **Generate Keys** page is displayed.

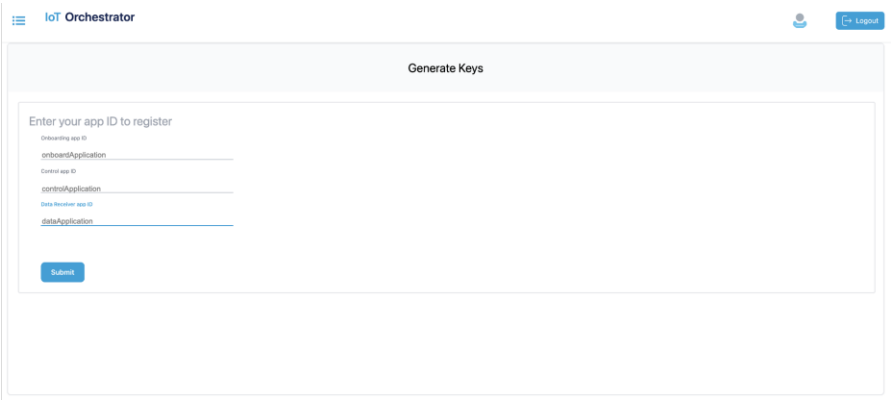


Figure 28.
Generate Keys

Step 2. Enter the application IDs for the onboard application, control application, and data receiver application.

Note: The application IDs are used to generate keys.

Step 3. Click **Submit**.

The keys are generated successfully.

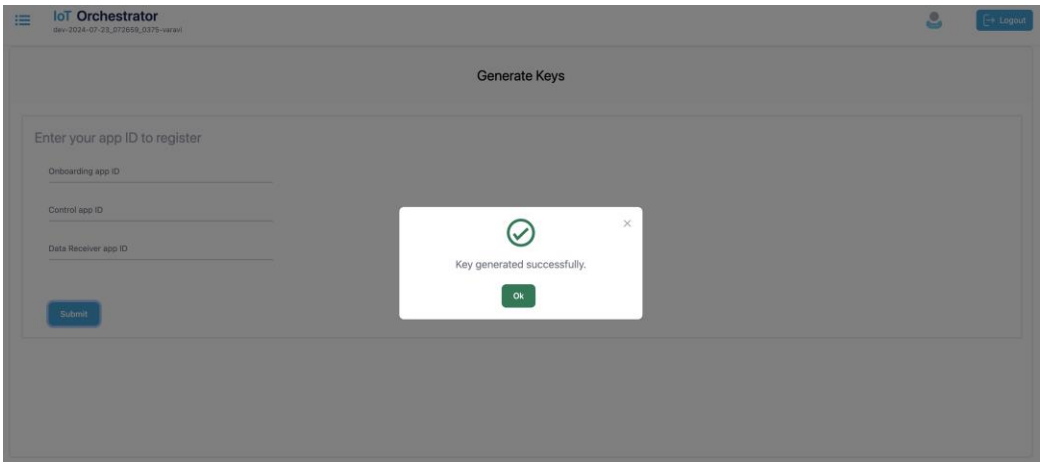


Figure 29.
Keys Generated Message Pop-Up

From MENU, choose the **Administrator > App Registration > Show Registered Apps**.

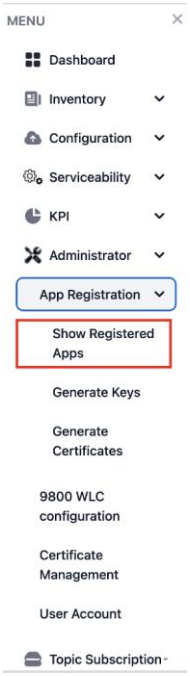


Figure 30.
Administrator > App Registration > Show Registered Apps Page

The **Registered Apps** page is displayed. You get to view the keys or certificates generated for the applications.

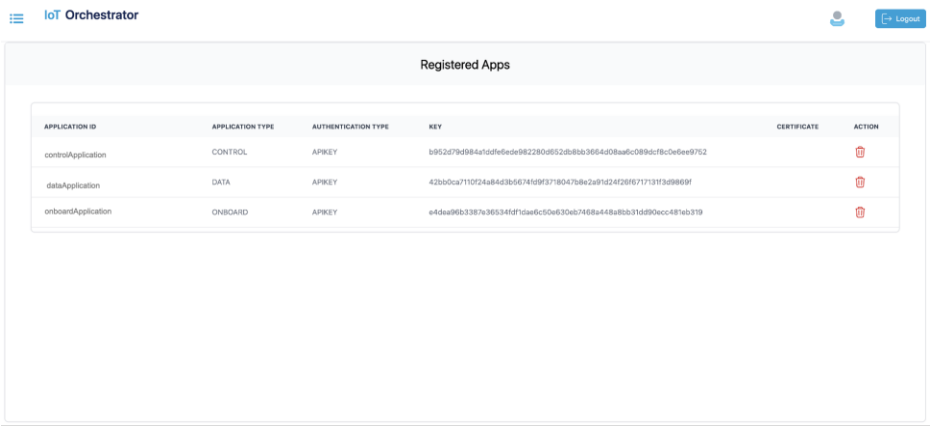


Figure 31.
Keys or Certificates Generated for Applications

Device Onboarding

For information on onboarding BLE devices using SCIM, see the Onboarding BLE Devices using SCIM section in *Cisco Spaces Connect for IoT Services Programmability Guide, Release 1.0.0*.

BLE Inventory

Summary:

You will be able to view the information of the BLE devices that are onboarded in the IoT Orchestrator.

Displays the BLE devices that are onboarded and the respective states.

Step 1. From the **MENU**, choose the **Inventory > BLE Client**.

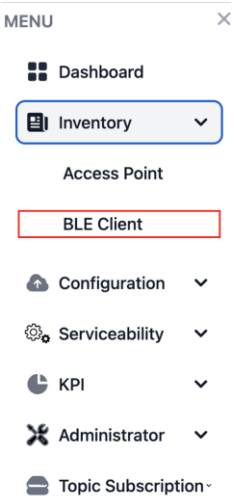


Figure 32.
Inventory > BLE Client Page

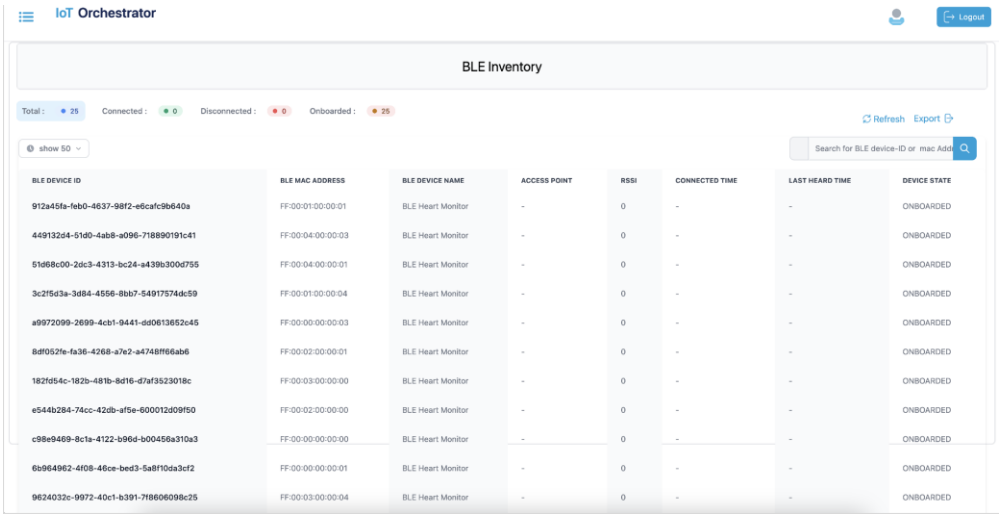


Figure 33.
BLE Inventory

Device Control & Telemetry

Registering Data Receiver Application

Summary:

You will need to register the data receiver application to receive the streaming messages from the IoT Orchestrator.

For information on registering data application, see the **Registering the Data Receiver Application** section in ***Cisco Spaces Connect for IoT Services Programmability Guide, Release 1.0.0***.

Registering a Topic

Summary:

You will need to register the topic to receive the streaming messages from the BLE devices.

For information on registering a topic, see the **Registering a Topic** section in **Cisco Spaces Connect for IoT Services Programmability Guide, Release 1.0.0**.

Subscribing to a Topic

Summary:

You will need to subscribe to a topic to receive the streaming messages from the BLE devices using the registered data receiver applications.

For information on subscribing to a topic, see the **Subscribing to Advertisements and Notifications** in **Cisco Spaces Connect for IoT Services Programmability Guide, Release 1.0.0**.

BLE Connectionless Use Case for Asset Tracking

For information on BLE connectionless use case, receive onboarded BLE device advertisements in Data Receiver application, see the **Use Case 1: Asset Tracking** section in **Cisco Spaces Connect for IoT Services Programmability Guide, Release 1.0.0**.

BLE Connection Based Use Case

For information on BLE connection-based use case, see the **Use Case 2: Remote Patient Health Monitoring (requiring BLE connection, reading, and writing)** section in **Cisco Spaces Connect for IoT Services Programmability Guide, Release 1.0.0**.

BLE Connection Based Use Case with GATT Notification

For information on BLE connection-based use case with GATT notification, see the **Use Case 3: BLE Notification-based Use Cases** in ***Cisco Spaces Connect for IoT Services Programmability Guide, Release 1.0.0***.

Release Table

This document is the quick start guide for Cisco Spaces Connect for IoT Services.

Date	Release Version
Aug 13, 2024	Release 1.0.0

Documentation Feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document. We appreciate your feedback.

Legal Information