Cisco Spaces Connect for IoT Services Configuration Guide, Release 1.0.0

First Published: 2024-08-26

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

Preface

This preface describes the conventions of this document and information on how to obtain other documentation. It also provides information on what's new in Cisco product documentation.

Document Conventions

This document uses the following conventions:

Convention	Description
^ or Ctrl	Both the ^ symbol and Ctrl represent the Control (Ctrl) key on a keyboard. For example, the key combination ^**D** or **Ctrl-D** means that you hold down the Control key while you press the D key. (Keys are indicated in capital letters but are not case sensitive.)
bold font	Commands and keywords and user-entered text appear in **bold** font.
Italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
[x]	Elements in square brackets are optional.

Reader Alert Conventions

This document may use the following conventions for reader alerts:

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Related Documentation

- *Cisco Spaces Connect for IoT Services Online Help* (Refer **Initial Configuration Workflow of IoT Orchestrator** section)

Communications, Services, and Additional Information

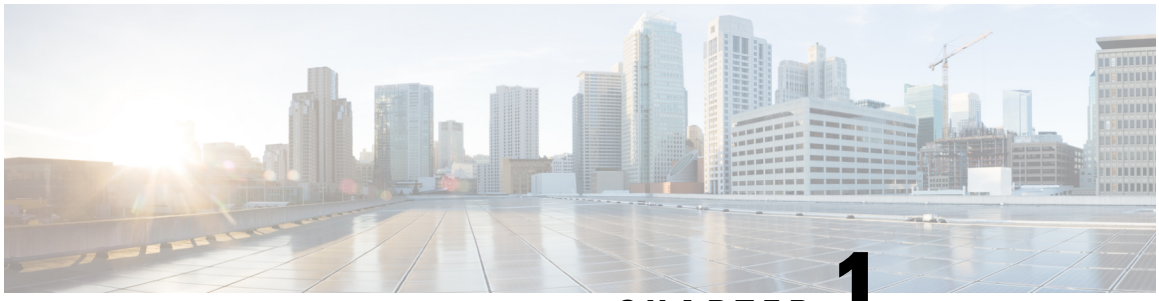
- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions, and services, visit Cisco DevNet.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a gateway to the Cisco bug-tracking system, which maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. The BST provides you with detailed defect information about your products and software.

Documentation Feedback

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



CHAPTER 1

Overview

Overview of Cisco Spaces Connect for IoT Services

Cisco Spaces Connect for IoT Services solution enables the 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. With the Cisco Spaces Connect for IoT Services solution, you can:

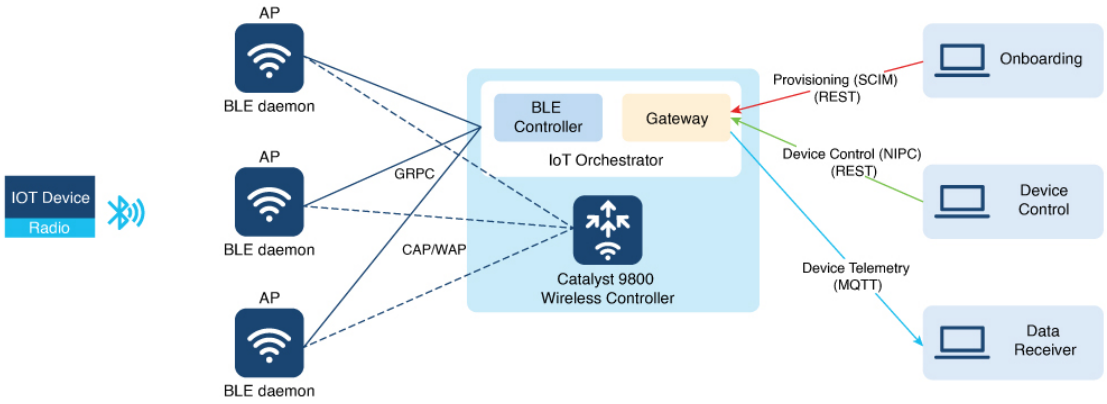
- Securely onboard and control BLE devices
- Consume data telemetry using the Message Queuing Telemetry Transport (MQTT)

Cisco's IoT Orchestrator is loaded on Cisco Catalyst 9800 Wireless Controllers and leveraged as an IoT gateway. This utilizes your existing network deployments and interfaces, reducing the need to deploy an entirely new infrastructure. Once loaded, you can use the IoT Orchestrator Manager in the Cisco Catalyst 9800 Wireless Controller to control the internal resources of the application. The IoT Orchestrator manages IoT devices to simplify the service deployment and ease of operation. The IoT Orchestrator provides a central area to control BLE devices and send BLE device data to appropriate recipients.

Cisco Spaces Connect Solution

The following diagram depicts the elements of the Cisco Spaces Connect solution.

Figure 1: Cisco Spaces Connect Solution (On-Premises Solution)



The BLE controller and gateway combined together is known as the IoT Orchestrator.

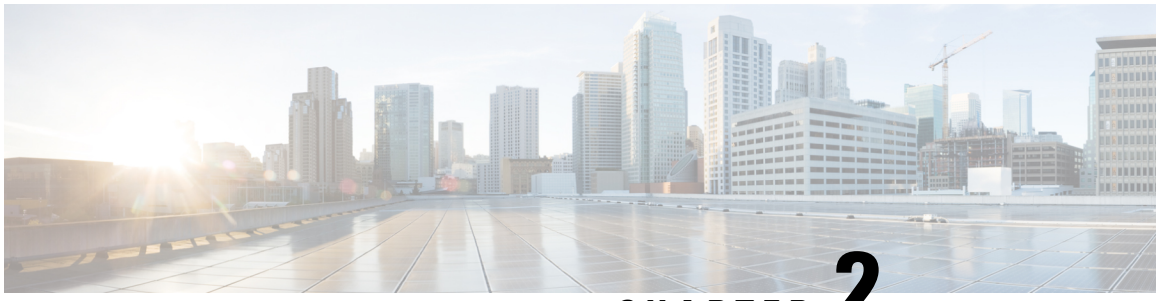
The IoT orchestrator is the new IOx application deployed on the Cisco Catalyst 9800 Wireless Controller as a Cisco IOx container that interacts with the AP using gRPC channels.

The AP uses its IoT radio to interact with the BLE device.

The IoT orchestrator provides APIs for the following:

- **Onboarding applications**: The onboarding applications leverage IETF SCIM for device models (https://datatracker.ietf.org/doc/draft-ietf-scim-device-model/). The SCIM allows an application to send a SCIM object to a SCIM server (gateway) to create, update, and delete devices in networks.
- **Device control applications**: The device control applications allow an application to connect to a non-IP device to exchange data with the device and register topics for streaming telemetry. The IETF draft used for this protocol is called the Non-IP Control (NIPC).
- **Data receiver applications**: The telemetry application receives the telemetry data from the IoT Orchestrator application.
- **Message Queuing Telemetry Transport (MQTT)**: Message Queuing Telemetry Transport (MQTT) is a lightweight messaging protocol commonly used for communication between devices in IoT applications. Subscriptions and notifications play crucial roles in enabling devices to receive and react to messages. In MQTT, the clients subscribe to topics for receiving messages published to those topics. A topic is a string that the MQTT broker uses to filter messages for each connected client. The notification for subscribed topic happens from the IoT Orchestrator application to the data receiver application.

Note All applications must be authenticated and authorized using certificate-based mechanism or API key-based mechanism. For example, if the API key-based mechanism is used, then all applications, such as onboarding, control, and data receiver applications must be registered on the IoT Orchestrator to generate the API key. Now when these applications interact with the IoT Orchestrator Application, they must present the API key in the issued API request. If you use the certificate-based mechanism, then you will need to present the certificate when issuing API requests to the IoT Orchestrator application.



CHAPTER 2

Prerequisites

Prerequisites for IoT Orchestrator

- Download the IoT Orchestrator Application (**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**.

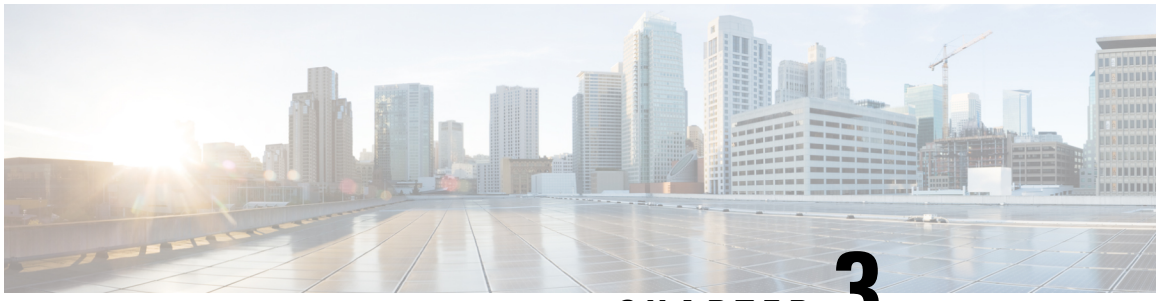
For more information about the Spaces Connect for IoT Services, see the following documentation:

- Cisco Spaces Connect for IoT Services Release Notes
- Cisco Spaces Connect for IoT Services Quick Start Guide
- Cisco Spaces Connect for IoT Services Programmability Guide
- Cisco Spaces Connect for IoT Services Online Help

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

- Controller must be configured for initial configuration with APs joined and clients connected to the network.
- The IP subnet assigned to the IoT Orchestrator must be unique and different from the other subnets configured in the controller. Also, the IP subnet must be reachable from all IP subnets belonging to access points.
- Controller must run on version Cisco IOS XE 17.15.1 and later.
- Ensure that the C9800-CL has at least the following resources before installing the IoT Orchestrator: 16 vCPU, 40 GB RAM, and 32 GB disk space, and the **app-heavy** template is configured.

Note This applies to Cisco Catalyst 9800-CL Wireless Controller.



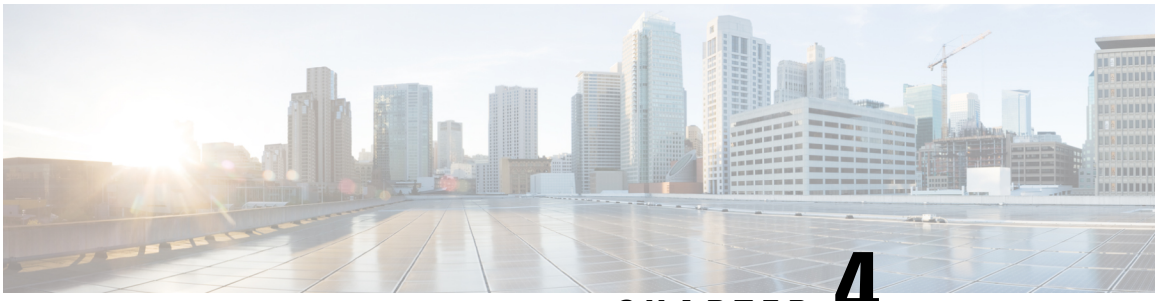
CHAPTER 3

License

License

- Spaces Smart Ops
- Spaces ACT
- Spaces Unlimited

License



CHAPTER 4

System Configuration

System Configuration

Supported Access Points

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

Note C9115AX APs support only scanning and advertising.

Supported Platforms

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

Note

- In newer C9800-CL platform deployment (Cisco IOS XE 17.15.1 release onwards), choose one of the two App Heavy deployment configurations 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.
- You cannot install IoT Orchestrator in C9800-CL running small or medium templates. You will need additional resources.
- Ensure that proper CPU allocation is in place before installing the IoT Orchestrator.

  To do so, perform the following:

  1. Ensure that the C9800-CL VM has the following resources 16 vCPU, 40 GB RAM, and 32 GB disk space.
  2. Verify the current CPU allocation using the following command:

```
Device# show platform software cpu alloc
CPU alloc information:

  Control plane cpu alloc: 0-7

  Data plane cpu alloc: 8-15

  Service plane cpu alloc: 0

  Platform plane cpu alloc: 0-7

  Slow control plane cpu alloc:
  Template used: None
```

  Based on the **Templated used** field, the following are the three different scenarios:

  a. If the **Templated used** is **CLI-app_heavy**, no action needs to be performed and C9800-CL is ready for IoT Orchestrator installation.

  b. If the **Templated used** is **None**, no template is allocated to C9800-CL. To configure the **app-heavy** template, issue the following commands:

```
Device# configure terminal
Enter configuration commands, one per line.  End with
CNTL/Z.
Device(config)# platform resource app-heavy
Please reboot to activate this template

Device(config)#
Device(config)# end
Device# write memory
Building configuration...
[OK]
Device# reload
Reload command is being issued on Active unit, this will
 reload the whole stack
```

```
Proceed with reload? [confirm]
```

Once the C9800-CL reboots, verify if the template is correctly applied or not using the following command:

```
Device# show platform software cpu alloc
CPU alloc information:

  Control plane cpu alloc: 0-7

  Data plane cpu alloc: 14-15

  Service plane cpu alloc: 8-13

  Platform plane cpu alloc: 0-7

  Slow control plane cpu alloc:
  Template used: CLI-app_heavy
```

c. If the **Templated used** is **Error**, this means that the specified template is configured and C9800-CL does not have the resources necessary to create the CPU allocation.

To resolve this after verifying that the resources are allocated to the virtual machine, perform the following:

- Unconfigure the template.

  In this example, the **CLI-app_heavy** template is errored.

```
Device# configure terminal
Enter configuration commands, one per line.  End with
 CNTL/Z.
Device(config)# no platform resource app-heavy
Please reboot to activate this template

Device(config)#
Device(config)# end
Device# write memory
Building configuration...
[OK]
Device# reload
Reload command is being issued on Active unit, this
 will reload the whole stack
Proceed with reload? [confirm]
```

- Once the C9800-CL reboots, verify that the template is deleted using the following command:

```
Device# show platform software cpu alloc
CPU alloc information:

  Control plane cpu alloc: 0-7

  Data plane cpu alloc: 8-15

  Service plane cpu alloc: 0

  Platform plane cpu alloc: 0-7

  Slow control plane cpu alloc:
  Template used: None
```

- Reconfigure the CPU allocation using the **app_heavy** template by issuing the following commands:

```
Device# configure terminal
Enter configuration commands, one per line.  End with
 CNTL/Z.
Device(config)# platform resource app-heavy
Please reboot to activate this template

Device(config)#
Device(config)# end
Device# write memory
Building configuration...
[OK]
Device# reload
Reload command is being issued on Active unit, this
 will reload the whole stack
```

```
Proceed with reload? [confirm]
```

- Verify if the template is correctly applied after the C9800-CL reboots using the following command:

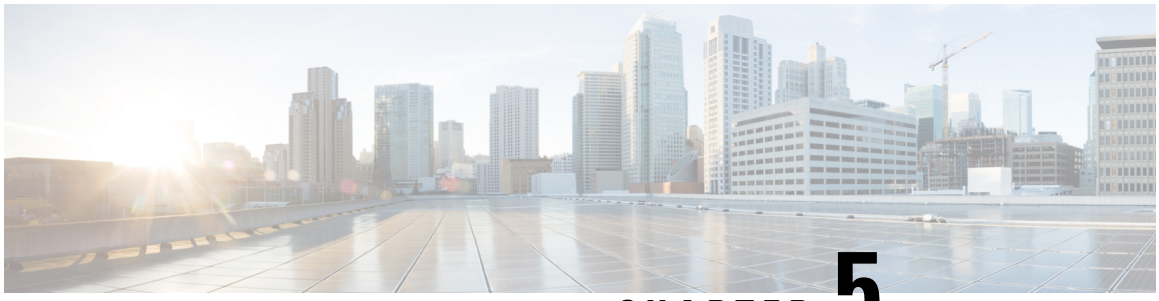
```
Device# show platform software cpu alloc
CPU alloc information:

  Control plane cpu alloc: 0-7

  Data plane cpu alloc: 14-15

  Service plane cpu alloc: 8-13

  Platform plane cpu alloc: 0-7

  Slow control plane cpu alloc:
  Template used: CLI-app_heavy
```

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

Scale Requirements

Table 1: Scale Requirements

Platform	Published Scale (Without IoT Orchestrator)	Target Scale (With IoT Orchestrator)
C9800-L	500 Aps, 10K WiFi clients	500 Aps, 10K clients (WiFi + BLE)
C9800-40	2K Aps, 32K WiFi clients	2K Aps, 32K clients (WiFi + BLE)
C9800-80	6K Aps, 64K WiFi clients	6K Aps, 64K clients (WiFi + BLE)
C9800-CL (Small)	1K Aps, 10K WiFi clients	1K Aps, 10K clients (WiFi + BLE)
C9800-CL (Medium)	3K Aps, 32K WiFi clients	3K Aps, 32K clients (WiFi + BLE)
C9800-CL (Large)	6K Aps, 64K WiFi clients	6K Aps, 64K clients (WiFi + BLE)
CW9800M	3K Aps, 32K WiFi clients	3K Aps, 32K clients (WiFi + BLE)
CW9800H1 and CW9800H2	6K Aps, 64K WiFi clients	6K Aps, 64K clients (WiFi + BLE)



CHAPTER 5

Deployment Workflow

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

Deploying 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.

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

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

Step 3 Enter the IP address.

Note The IP addresses must be unique and different from the other IP addresses configured in Cisco Catalyst 9800 Wireless Controller. If you configure an IP address that overlaps with other interfaces, you will get an error message.

Step 4 Enter the subnet mask.

Note The minimum size of the mask is /30 that allows two valid hosts (IoT Orchestrator and VirtualPortGroup Interface of Cisco Catalyst 9800 Wireless Controller).

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.

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.

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.

Upgrading an Existing IOT Orchestrator

You will be able to upgrade an existing IoT Orchestrator to a newer version when the application **status** is **Running** or **Stopped**.

From the **More Actions** drop-down list on the right-hand side of the **Configuration > Services > IoT Services** page, perform the following:

1. Choose **Upgrade**.

   A pop-up window is displayed stating if you want to upgrade the IoT Orchestrator or not.

2. Click **Yes**.
3. In the **Image File Path** field, click **Select File** to select the IoT Orchestrator image and click **Open**.
4. Click **Upgrade IoT Services**.

   The upgrade workflow starts. The status moves from Uploading image, triggering application upgrade, stopping, deactivating, deleting, and the new application deployment takes place with status as installing, activating, and starting.

Note If the upgrade workflow fails, the upgrade rolls back to the previous image or the system is cleaned.

High Availability

Restarting IoT Orchestrator Application

When you restart (stop or start) the IoT Orchestrator application, all databases restart except the BLE location repository. The BLE connections available before the restart are lost and the connections are re-established by the application. Once the IoT Orchestrator application restarts, the APs re-establish the gRPC connection to the IoT Orchestrator application.

Upgrading IoT Orchestrator Application

When you upgrade the IoT Orchestrator application, all databases upgrade except the BLE location repository. The BLE connections available before the upgrade are lost and the connections are re-established by the application. Once the IoT Orchestrator application upgrades, the APs re-establish the gRPC connection to the IoT Orchestrator application. For more information, see Upgrading an Existing IOT Orchestrator.

Reloading Cisco Catalyst 9800 Wireless Controller

When you restart the IoT Orchestrator application and Cisco Catalyst 9800 Wireless Controllers are reloaded, all the databases will be persisted across the controller reload workflow. The BLE connections available before the upgrade are lost and the connections are re- established by the application. Once the Controller reloads, the APs re-establish the gRPC connection to the IoT Orchestrator application.

Launching IoT Orchestrator Application

Before you begin

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

Procedure

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

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

You get to view a new tab with the IP address of the application provided in Deploying IoT Orchestrator Application on Cisco Catalyst 9800 Wireless Controller section.

Note When you click **Launch IoT Orchestrator**, a new tab opens up which might take upto a minute to be up and running. If the IoT Orchestrator login page does not load, you will need to check the reachability of your PC or laptop to the IoT Orchestrator IP.

Verifying IOT Orchestrator Version

Perform Day 0 WebUI Wizard for IoT Orchestrator Application and Changing your Username and Password.

Note You get to view the version of the installed IoT Orchestrator on the top left-hand side of the **IoT Orchestrator** GUI.

Reviewing Licensing Details to Use IoT Orchestrator

Step 1 Read the terms and conditions.

Step 2 Click **I Accept**.

The **Day 0 WebUI wizard** for IoT Orchestrator application is displayed.

Day 0 WebUI Wizard for IoT Orchestrator Application

Step 1 Enter *admin* for username and *password* for password.

Step 2 Click **Log In**.

Once you login with the default credentials, you get a pop-up to change the username and password.

Changing your Username and Password

Step 1 Enter the username.

Step 2 Enter the password.

Step 3 Enter the same password again to confirm.

Note

- The password must be minimum 8 characters and maximum 64 characters.
- The password supports all special characters including blank space.
- The password must be unique and not contain any repetitive, sequential, content-specific, and service-specific terms.

  The following are the content and service-specific terms:

  - cisco
  - 9800 controller
  - ewlc
  - iot orchestrator
  - password
  - service
  - secure
  - key
  - network

- The password must include at least one alphabetic character.

Step 4 Click **change your credentials**.

You get a pop-up that says *User Saved Successfully*.

Step 5 Click **Ok**.

Note You need to enter the changed credentials to login to the controller.

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

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 IoT Orchestrator Application

Pushing Token and Certificate from IoT Orchestrator to Cisco Catalyst 9800 Wireless Controller

Before you begin

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

Step 1 Enter the controller username.

Step 2 Enter the controller IP address.

Note The Wireless Management Interface of the controller is used as the IP address.

Step 3 Enter the controller login password.

Step 4 Enter the controller enable password.

Step 5 Click **Submit** to push the token and certificate to the controller.

The controller is now configured with a token and certificate required for APs to connect to the IoT Orchestrator.

Step 6 A pop-up window is displayed stating the following:

The connection establishment with the controller is successful.

Step 7 Click **Ok**.

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

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

Before you begin

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

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.

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.

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

Before you begin

You need to register the partner applications (such as onboard application, control application, and data receiver application) to authorize and interact with 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.

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

Note To view the keys or certificates generated for the applications, choose the **Administrator > App Registration > Show Registered Apps**.

Configuring Access Point BLE Transmission and Scanning

Transmit Configuration

Step 1 Log in to the IoT Orchestrator Web UI.

Step 2 Choose **Configuration > Transmit Configuration**.

Step 3 Click **Add**.

The configuration window pops-up.

Step 4 Choose one of the following transmission methods:

- iBeacon
- ED url
- ED uid
- No Advertisement

Step 5 Enter a name and required values for the transmit configuration.

Step 6 Click **Save Config**.

A success message is displayed.

Step 7 Click **Ok**.

The value gets added to the transmit configuration list.

Scan Configuration

Step 1 Log in to the IoT Orchestrator Web UI.

Step 2 Choose **Configuration > Scan Configuration**.

Step 3 Click **Add**.

The configuration window pops-up.

Step 4 Enter a name and required values for the scan configuration.

Step 5 Click **Save Config**.

A success message is displayed.

Step 6 Click **Ok**.

The value gets added to the scan configuration list.

Applying BLE Configuration to Access Point using GUI

Before you begin

- Ensure that the BLE scanning is enabled by default in all APs.

Step 1 Log in to the IoT Orchestrator Web UI.

Step 2 Click **AP Inventory** to view the list of APs.

Step 3 Select an AP MAC or AP Name and click **Configure**.

(Or)

Step 4 Select multiple APs using the checkbox and click **Configure**.

The BLE Config window pops-up.

Step 5 Click **Transmit Config** and select the saved configurations from the list.

Step 6 Click **Set Config**.

The Transmit Config is configured successfully.

Step 7 Click **Ok**.

Step 8 Click **Scan Config** and select the saved configurations from the list.

Step 9 Click **Set Config**.

The Scan Config is configured successfully.

Step 10 Click **Ok**.

Step 11 Select **On** or **Off** from the **IoT Radio** button.

Step 12 Click **Set** to apply the desired IoT Radio state.

The IoT Radio is configured successfully with the status displayed.

Step 13 Click **Ok**.

Onboarding IoT or BLE Devices

Use REST APIs to read data from the BLE device, write data on the BLE device, disconnect the BLE device.

For more information, see the *Cisco Spaces Connect for IoT Services Programmability Guide*.

Note Based on the BLE device operations, you will be able to view the current state of the device from the **Inventory** > **BLE Client** page:

Table 2: Device State

Device State
ONBOARDED
CONNECTED
DISCONNECTED

BLE Connection and Subscription

Before you begin

BLE connection and subscription is required for IoT Orchestrator to send the streaming data to the Partner application.

In the **IoT Orchestrator dashboard**, perform the following:

Step 1 Choose the **Topic Subscription** > **Device Topics** page to register the topic with the required BLE devices.

Note Topics are used to map the BLE devices to their respective user or group of interest.

Step 2 Choose the **Topic Subscription** > **Data App Topics** page to register the Data App to the Topic Data of interest.

Step 3 Choose the **Serviceability** page and select **notifications**.

Step 4 Click **Submit** to view notifications from the BLE device.

Day 2 - Monitoring and Troubleshooting the IoT Orchestrator

Metrics

Before you begin

In the **IoT Orchestrator dashboard**, perform the following:

Step 1 Choose **KPI > Orchestrator** to view the important metrics related to IoT application.

The Orchestrator Metrics page is displayed.

Step 2 Navigate through the different metrics in the left-hand navigation column.

Step 3 Choose **KPI > Access Points** to view the metrics related to AP and BLE processes.

Step 4 From the **AP Metrics** and **BLE Metrics** area, select an AP or BLE device.

Step 5 Click **Submit**.

Logs

Before you begin

You get to view three types of logs:

- Logs of the IoT Orchestrator application.
- AP logs from the IoT Orchestrator application.
- Radio active logs for a specific BLE device.

In the **IoT Orchestrator dashboard**, perform the following:

Step 1 Choose **Serviceability > Orchestrator Logs** to view the logs of the IoT Orchestrator application.

The **Orchestrator Logs** page is displayed.

Buttons	Description
Live Logs	Click **Live Logs** to view the live log details in a new page. You can perform the following actions: • **Clear**: Click **Clear** to clear the console. • **Download**: Click **Download** to get a copy of the live logs. • **Stop**: Click **Stop** to halt the live log.

Buttons	Description
View	Enter the number of latest offline logs to display and click **View**.
Clear	Enter the number of latest offline logs to display and click **Clear**.
Refresh	Click **Refresh** to refresh the page.
Download	Click **Download** to download the latest offline logs.
Download all	Click **Download all** to download all the logs.

Step 2 Choose **Serviceability > Access Point Logs** to view AP logs.

The **AP Logs** page is displayed.

a. From the **Connected AP's** area, search for the AP or choose the AP.

b. Click **Get Logs** to get all the logs (or) click **Set Log Level** to view logs based on the log level.

Note You can select one of the following log levels and click **Confirm**:

- ERROR
- WARN
- INFO
- DEBUG

c. From the **Saved Logs** area, search the AP and click **Show Logs**, **Download**, or **Download all** to view logs, download a specific AP log, or download all logs related to an AP.

Step 3 Choose **Serviceability > Radio Active Logs** to view BLE Device related logs.

The Radio Active Logs page is displayed.

a. From the **Available BLE's** area, search for the BLE.

b. Click **Add** to view the logs for that device.

Note
- You need to onboard the BLE devices to view logs.
- When devices are onboarded in the **Radio Active Logs** page and when you click **Action** as **Start**, the logs are captured in the IoT Orchestrator. You get to download and view the logs. This is applicable for 5 BLE devices at the same time.