IIIIII CISCO The bridge to possible

Cisco Spaces Connect for IoT Services Quick Start Guide

Release 1.0.0

Page 1 of 27 Cisco Confidential

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: <u>c9800-spaces-connect-for-iot-services@external.cisco.com</u>

Related Documentation

- <u>Cisco Spaces Connect for IoT Services Configuration Guide</u>
- Cisco Spaces Connect for IoT Services Programmability Guide
- Cisco Spaces Connect for IoT Services Online Help
- <u>Cisco Spaces Connect for IoT Services Release Notes</u>

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 appheavy" 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.
- 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

- Cisco Catalyst 9105AX Access Points
- Cisco Catalyst 9115AX Access Points
- Cisco Catalyst 9120AX Access Points
- Cisco Catalyst 9130AX Access Points
- Cisco Catalyst 9124AX Access Points
- Cisco Catalyst 9136 (I) Access Points
- Cisco Catalyst 9162 (I) Access Points
- Cisco Catalyst 9164 (I) Access Points
- Cisco Catalyst 9166 (I) Access Points
- Note: Cisco Catalyst 9115AX APs support only scanning and advertising.

Deployment Workflow

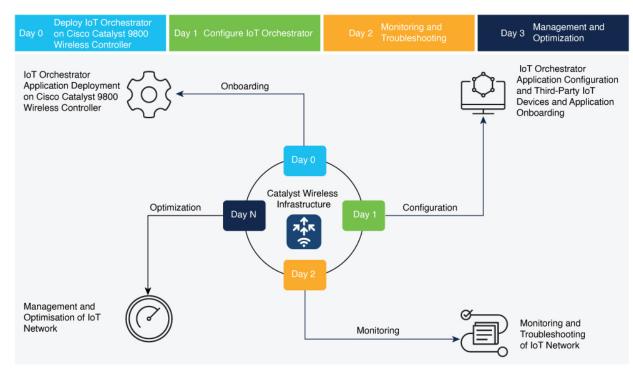


Figure 1.

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.

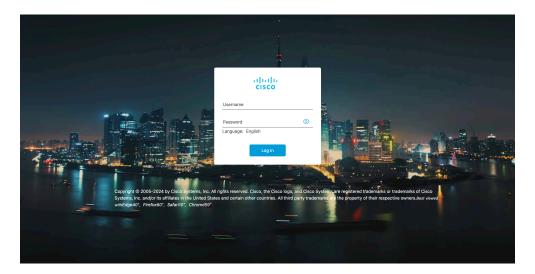


Figure 2.

Cisco Catalyst 9800 Wireless Controller Web UI

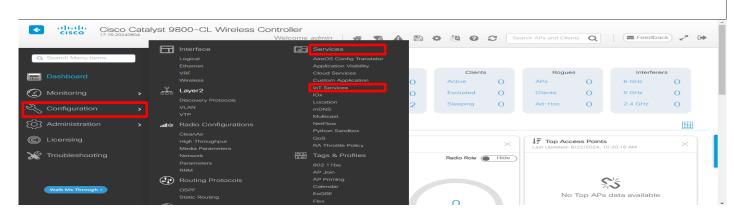
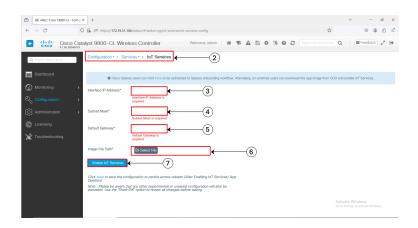


Figure 3. Configuration > Services > IoT Services

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.

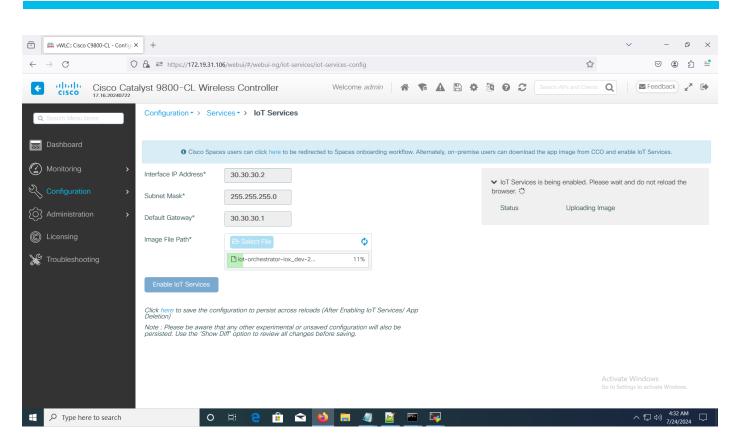


Figure 4.

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.

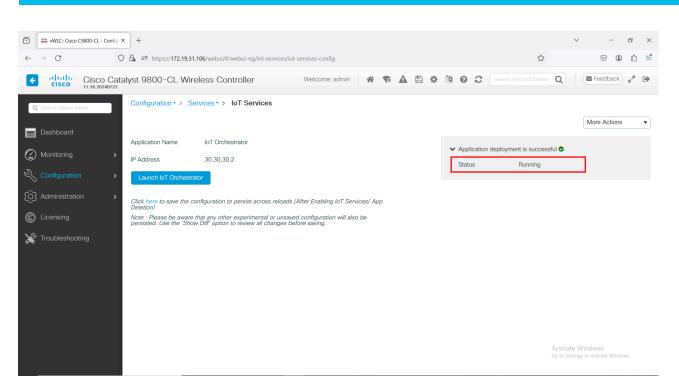


Figure 5.

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.

Q Search Menu Items	Configuration * > Services * > IoT Services			
Dashboard				More Actions More Actions
Monitoring >	Application Name IoT Orchestrator IP Address 30.30.30.2		iyment is successful 🛇	Stop Upgrade
Configuration	Launch IoT Orchestrator (2)	Status	Running	Delete
O Administration	Click here to save the configuration to persist across reloads (After Enabling IoT Services/ App			
C Licensing	Deletion) Note : Please be aware that any other experimental or unsaved configuration will also be persisted. Use the 'Show Diff' option to review all changes before saving.			
X Troubleshooting				
				Windows ings to activate Windows.

Figure 6. Launching IoT Orchestrator

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

When there is a firewall or similar device (such as a router with Access Control Lists (ACLs)), between Cisco Access Points and Wireless IoT Orchestrator or between Wireless IoT Orchestrator and external custom application, the firewall or similar device must be configured with rules that allow proper connectivity.

Connectivity Between Cisco Access Points and Wireless IoT Orchestrator

The following ports must be opened from Cisco Access Points to Wireless IoT Orchestrator:

Protocol	Port	Usage
TCP	8080	AP initial HTTP Connection with Wireless IoT Orchestrator
TCP	43626	Establish a gRPC connection with Wireless IoT Orchestrator

Table 1. Protocol, Port, and Usage Details

Connectivity Between External Applications and Wireless IoT Orchestrator

The following ports must be opened from external application to Wireless IoT Orchestrator:

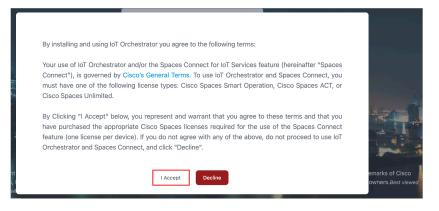
Table 2. Protocol, Port, and Usage Details

Protocol	Port	Usage

ТСР	8081	Wireless IoT Orchestrator REST API interface
ТСР	41883	MQTT Publisher listening port

Licensing Details to Use IoT Orchestrator

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



The IoT Orchestrator login page is displayed.

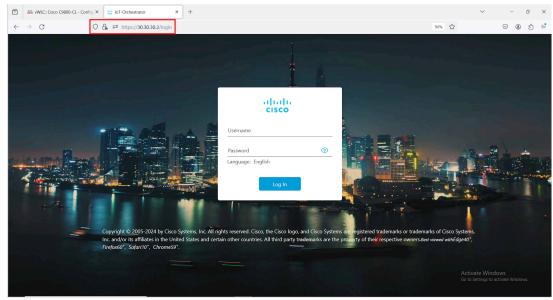


Figure 7. IoT Orchestrator Login Page

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).

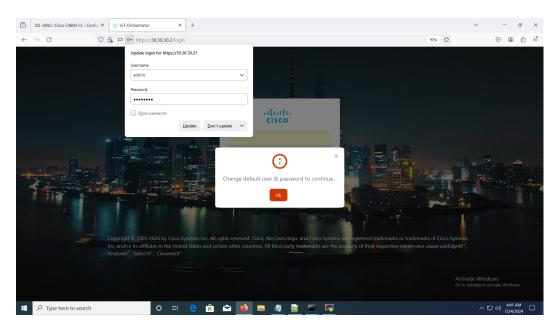


Figure 8. Default Credentials Login Page

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.

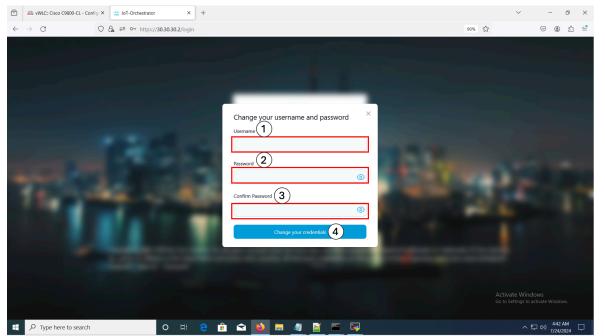


Figure 9.

Changing your Username and Password

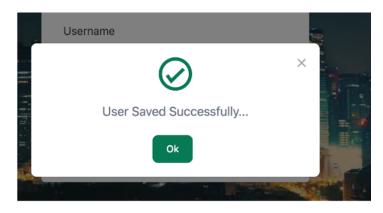


Figure 10.

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.

≔	IoT Orchestrator	2	[→ Logout
	Config eWLC		
	Connect with eWLC - Controller Image: Control Water Stars I		

Figure 11. 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.

=	IoT Orchestrator								
AP Inventory									
Total :	fotal: • 20 Connected: • 20 Disconnected: • 0								
© sł	100 50 v	Select all	Configure	AP VERSION	: 17.10.0.92	WLC IP ADDRESS : 10.195.78.	100	Search for AP name o	r mac address
	AP NAME	AP MAC ADDRESS	AP PLATFORM	AP IP ADDRESS	STATUS	LAST HEARD	BLE MAC ADDRESS	BLE CONNECTIONS	RADIO STATUS
	AP-D4:E8:80:00:00:10	D4:E8:80:00:00:10	CW9166I-B	172.17.0.2	Connected	2024-07-23 15:04:48	30:FB:10:53:C0:B9	0 / 50	Up
	AP-D4:E8:80:00:00:00	D4:E8:80:00:00:00	CW9166I-B	172.17.0.2	ected	2024-07-23 15:04:48	30:FB:10:53:C0:B9	0/50	Up
	AP-D4:E8:80:00:00:11	D4:E8:80:00:00:11	C9136I-B	172.17.0.2	Connected	2024-07-23 15:04:55	30:FB:10:53:C0:B9	0/50	Up
	AP-D4:E8:80:00:00:01	D4:E8:80:00:00:01	C9136I-B	172.17.0.2	Connected	2024-07-23 15:04:48	30:FB:10:53:C0:B9	0/50	Up
	AP-D4:E8:80:00:00:12	D4:E8:80:00:00:12	CW9166I-B	172.17.0.2	Connected	2024-07-23 15:04:55	30:FB:10:53:C0:B9	0/50	Up
	AP-D4:E8:80:00:00:13	D4:E8:80:00:00:13	C9136I-B	172.17.0.2	Connected	2024-07-23 15:04:55	30:FB:10:53:C0:B9	0/50	Up
	AP-D4:E8:80:00:00:02	D4:E8:80:00:00:02	CW9166I-B	172.17.0.2	Connected	2024-07-23 15:04:55	30:FB:10:53:C0:B9	0/50	Up
	AP-D4:E8:80:00:00:03	D4:E8:80:00:00:03	CW9166I-B	172.17.0.2	Connected	2024-07-23 15:04:55	30:FB:10:53:C0:B9	0/50	Up

Figure 12.

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 13. IoT Orchestrator Dashboard – Configuration > Transmit Configuration

Step 3. Click Add.

E IoT Orchestrator		2	[→ Logout
	Transmit Configuration		
🕒 Ada			
		Search for configuration name	Q
CONFIGURATION NAME	CONFIGURATION TYPE	ACTION	
default-ap-profile	NO_ADV		
Showing 1-1 of 1		« Prev 1	Next »

Figure 14.

Transmit Configuration Page

juration Name :		1
o i	Beacon 🔘 ED url 🔘 ED uid 🔘 No Adv (5)
UUID		
TX Power		
Major		
Minor		
Interval		
Adv TxPower		
	Save Config	

Figure 15.

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.

Transmit Configuration - Add Page

Configuration Name : iBeacon ED url ED uid No Adv	×
ED Url	
Save Config	

Figure 16.

ED url Configuration

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

Configuration Name :	×
🔿 iBeacon 🔿 ED url 🔘 ED uid 🔿 No Adv	
ED ns	
ED Instance	
Save Config	

Figure 17. ED uid Configuration

• No Advertisement:

Configuration Name : iBeacon O ED url O ED uid O No Adv	×
This will create a No Advertisement Config profile!	
Save Config	



Step 6. Click Save Config.

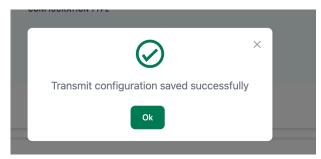


Figure 19.

Transmit Configuration Successful Message

i≡ IoT Orchestrator			٩	[→ Logout
	Transmit Configuration			
Add				
			Search for configuration name	Q
CONFIGURATION NAME	CONFIGURATION TYPE	ACTION		
Transmit-config-with-iBeacon	NO_ADV	⑪		
default-ap-profile	NQ_ADV			
Showing 1-2 of 2			« Prev 1	Next »

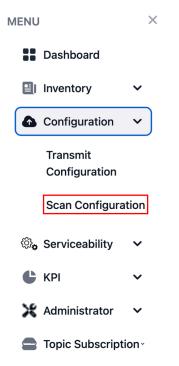
Figure 20.

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.





IoT Orchestrator Dashboard - Configuration > Scan Configuration

Step 3. Click Add.

			•	☐ Logout
	Scan Configuration			
Add				
		s	earch for configuration name	Q
CONFIGURATION NAME	DROP RANDOM PRIVATE MAC	ENABLE	ACTION	
default-ap-profile	true	true		
Showing 1-1 of 1			« Prev 1	Next »

Figure 22. Scan Configuration Page

Configuration Name :	×
Drop random private mac address	4
⊖ true	
⊖ false	
Enable	
⊖ true	
⊖ false	
Confirm	5

Figure 23.

Configuration pop-up

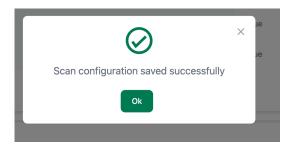


Figure 24.

Scan Configuration Successful Message

The value gets added to the scan configuration list.

E IoT Orchestrator			.	Logout
	Scan Configuration			
Add				
			Search for configuration name	٩
CONFIGURATION NAME	DROP RANDOM PRIVATE MAC	ENABLE	ACTION	
default-ap-profile	true	true		
scan-config	true	true	D 🗹 🛈	
Showing 1-2 of 2			« Prev 1 Next	t »

Figure 25.

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.

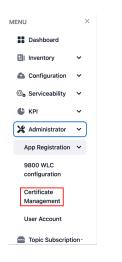


Figure 26.

Administrator > Certificate Management Dashboard Page

The Upload Certificates page is displayed.

E IoT Orchestrator		Logout →
	Upload Certificates	
Server Identity : Add your private key : Choose file No file chosen Add your public key : Choose file No file chosen	2	
Authenticate using Certificates 3		
Client Identity : Add your trustroot : Choose file No file chosen	4	

Page 19 of 27 Cisco Confidential **Figure 27.** 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 <u>Uploading Certificate and Key to</u> <u>Open HTTP Server and Listen for APIs</u> section.

How do you authorize:

You can authorize the applications by generating keys.

Procedure

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

М	ENU		2	×			
	::	Dashboard					
		Inventory	~				
	6	Configuration	~				
	© ,	Serviceability	~				
	¢	КРІ	~				
	ж	Administrator	~				
(4	pp Registration	~)			
		Show Registere Apps	d	_			
		Generate Keys					
		Generate Certificates					
	-	9800 WLC configuration					
		Certificate Nanagement					
	ι	Jser Account					
	8	Topic Subscripti	on×				

Figure 28.

Administrator > App Registration > Generate Keys Page

The **Generate Keys** page is displayed.

Figure 29.

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.

≔	IoT Orchestrator dee-3024-07-32_070568_0.076-search	2	[→ Logout
	Generate Keys		
E	nter your app ID to register		
	Onboarding app 10		
	Control lege ID		
	Data Receiver app ID Key generated successfully.		
	Submit		

Figure 30.

Keys Generated Message Pop-Up

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

м		
	ENU	×
	Dashboard	
	Inventory	~
	Configuration	~
	In the service of	~
	🕒 КРІ	~
	🔀 Administrator	~
(App Registration	~
- r		
	Show Registere	ed
	Apps	
	Generate Keys	
	-	
	Generate Keys Generate Certificates	
	Generate	
	Generate Certificates	
	Generate Certificates 9800 WLC	
	Generate Certificates 9800 WLC configuration	
	Generate Certificates 9800 WLC configuration Certificate	
	Generate Certificates 9800 WLC configuration Certificate Management	ion×

Figure 31.

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.

=	IoT Orchestrator					2	[→ Lo
				Registered Apps			
	APPLICATION ID	APPLICATION TYPE	AUTHENTICATION TYPE	KEY	CERTIFICATE	ACT	ION
	controlApplication	CONTROL	APIKEY	b952d79d984a1ddfe6ede982280d652db8bb3664d08aa6c089dcf8c0e6ee9752		Û	
	dataApplication	DATA	APIKEY	42bb0ca7110f24a84d3b5674fd9f3718047b8e2a91d24f26f6717131f3d9869f		Û	
	onboardApplication	ONBOARD	APIKEY	e4dea96b3387e36534fdf1dae6c50e630eb7468a448a8bb31dd90ecc481eb319		Û	

Figure 32.

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.

MENU ×	
Dashboard	
Inventory V	
Access Point	
BLE Client	
\land Configuration 🗸	
©₀ Serviceability ∨	
🕒 КРІ 🗸 🗸	
🔀 Administrator 🗸 🗸	
Topic Subscription	

Figure 33.

Inventory > BLE Client Page

BLE Inventory							
Total : • 25 Connected : • 0 Disconnected :	• 0 Onboarded : •	28				ទា	Refresh Export 🗗
Show 50 ~						Search for BLE d	evice-ID or mac Addi
BLE DEVICE ID	BLE MAC ADDRESS	BLE DEVICE NAME	ACCESS POINT	RSSI	CONNECTED TIME	LAST HEARD TIME	DEVICE STATE
912a45fa-feb0-4637-98f2-e6cafc9b640a	FF:00:01:00:00:01	BLE Heart Monitor		0		-	ONBOARDED
449132d4-51d0-4ab8-a096-718890191c41	FF:00:04:00:00:03	BLE Heart Monitor		0			ONBOARDED
51d68c00-2dc3-4313-bc24-a439b300d755	FF:00:04:00:00:01	BLE Heart Monitor		0			ONBOARDED
3c2f5d3a-3d84-4556-8bb7-54917574dc59	FF:00:01:00:00:04	BLE Heart Monitor		0			ONBOARDED
a9972099-2699-4cb1-9441-dd0613652c45	FF:00:00:00:00:03	BLE Heart Monitor		0			ONBOARDED
8df052fe-fa36-4268-a7e2-a4748ff66ab6	FF:00:02:00:00:01	BLE Heart Monitor		0		-	ONBOARDED
182fd54c-182b-481b-8d16-d7af3523018c	FF:00:03:00:00:00	BLE Heart Monitor		0		-	ONBOARDED
e544b284-74cc-42db-af5e-600012d09f50	FF:00:02:00:00:00	BLE Heart Monitor	-	0	-	-	ONBOARDED
c98e9469-8c1a-4122-b96d-b00456a310a3	FF:00:00:00:00:00	BLE Heart Monitor		0			ONBOARDED
6b964962-4f08-46ce-bed3-5a8f10da3cf2	FF:00:00:00:00:01	BLE Heart Monitor		0			ONBOARDED
9624032c-9972-40c1-b391-7f8606098c25	FF:00:03:00:00:04	BLE Heart Monitor		0			ONBOARDED

Figure 34.

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 26, 2024	Release 1.0.0

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 <u>Cisco Support</u>.
- To discover and browse secure, validated enterprise-class apps, products, solutions, and services, visit <u>Cisco DevNet</u>.
- 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

<u>Cisco Bug Search Tool</u> (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.

Copyright © 2024, Cisco Systems, Inc. All rights reserved.