Cisco Sensor Connect for IoT Services Configuration Guide

First Published: 2024-08-26

Last Modified: 2025-08-07

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

Communications, services, and additional information

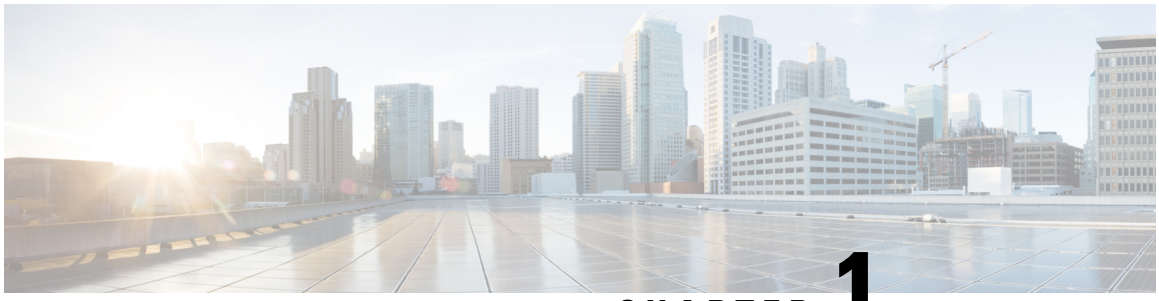
- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class 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 Sensor Connect for IoT Services

Cisco Sensor 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 Sensor Connect for IoT Services solution, you can:

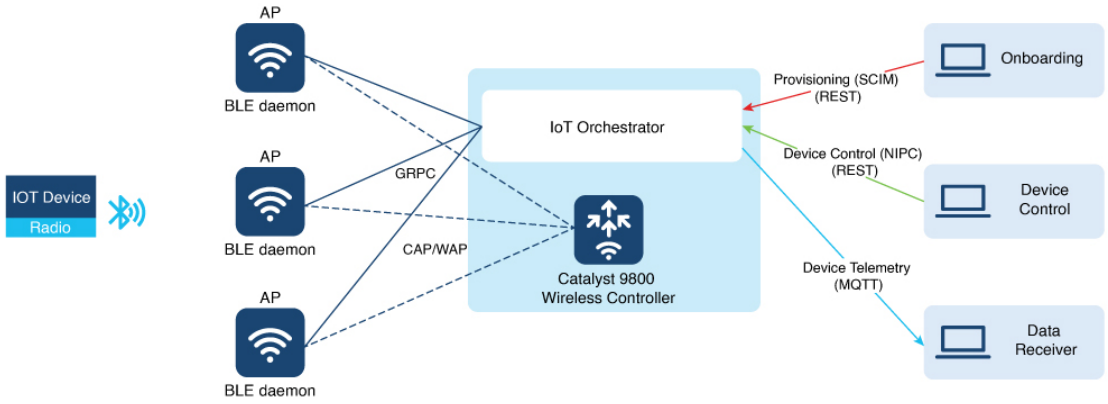
- Securely onboard and control BLE devices
- Consume data telemetry using the Message Queuing Telemetry Transport (MQTT)

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. 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 Sensor Connect Solution

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

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



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.

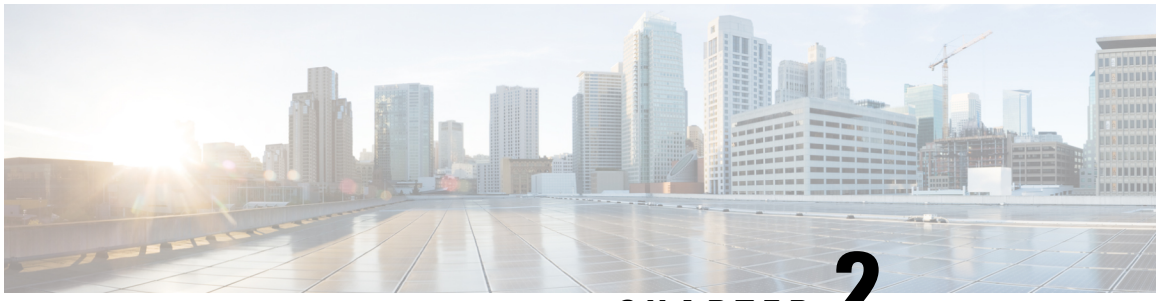
The AP uses its IoT radio to interact with the BLE device.

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

- The existing NIPC APIs were created when the standard was still evolving, leading to some aspects being implemented differently. Starting with IoT Orchestrator release 2.0, these APIs will be updated to align with the latest draft version of NIPC. Please note that backward compatibility with APIs from version 1.x will not be supported.
- Applications must be authenticated and authorized using either a certificate-based method or an API key-based method, but not both. If both methods are selected, the certificate-based approach is preferred. For API key-based authentication, applications such as onboarding, control, and data receiver must be registered with the IoT Orchestrator to obtain an API key. These applications must include the API key in their requests when interacting with the IoT Orchestrator. For certificate-based authentication, the certificate must be presented in API requests to the IoT Orchestrator.



CHAPTER 2

Prerequisites

Prerequisites for IoT Orchestrator

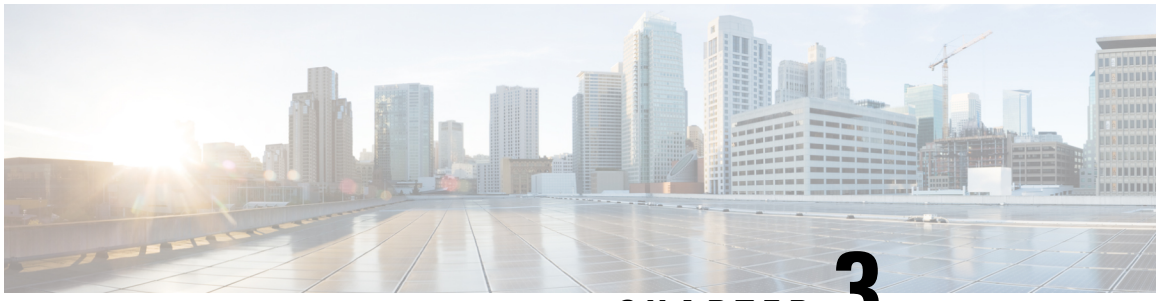
- Download the IoT Orchestrator Application (**Spaces Orchestrator Software**) image that will be posted in the following page:

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

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

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

- For the installation or configuration of Sensor Connect for IoT Services, ensure that SSH is enabled on the Cisco Catalyst 9800 Wireless Controller. Additionally, ensure that IoT Services are disabled on the Cisco Sensor Connector for the wireless controller intended for this purpose.
- 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 17.15.3 or 17.17.1.
- The Cisco Catalyst 9800 Wireless Controller communicates with the IoT Orchestrator using a VirtualPortGroup interface. This interface has its own subnet and will be configured automatically during the Day 0 installation process.



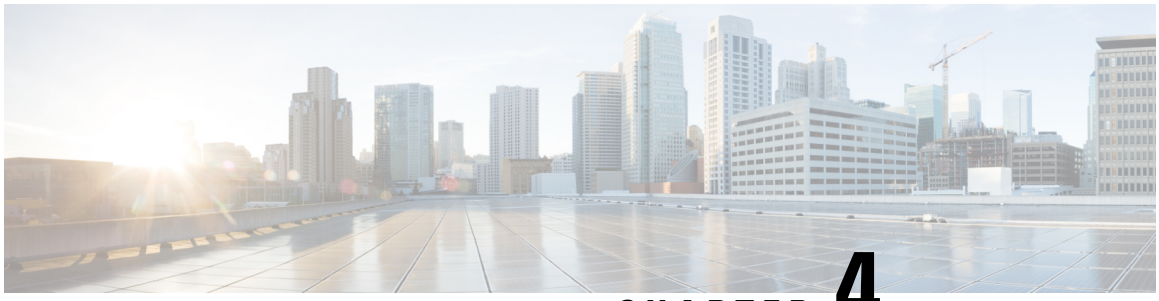
CHAPTER 3

License

License

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

License



CHAPTER 4

System Configuration

System Configuration

Supported Access Points

- C9105AX
- C9115AX
- C9120AX
- C9130AX
- C9124AX
- C9136I
- CW9162I
- CW9164I
- CW9166I
- CW9172H
- CW9172I
- CW9176
- CW9178

Note C9115AX APs support only scanning and advertising.

Supported Platforms

- Cisco Catalyst 9800-L Wireless Controller

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

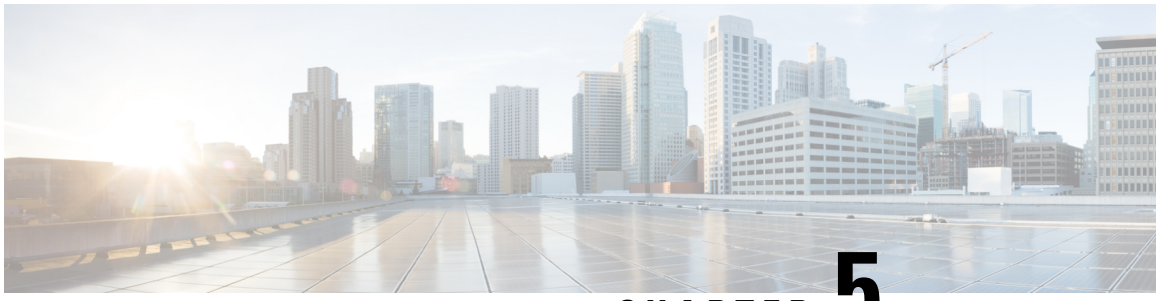
Scale Summary

Table 1: Scale Summary

KPIs	C9800-L	C9800-
Maximum BLE devices that can be onboarded (including connected)	1000, 2000 (with Performance license)	6400
Maximum BLE devices connected	1000, 2000 (with Performance license)	6400
Maximum number of APs to be onboarded to IoT Orchestrator	250/500	2000
Maximum BLE advertisements handling	Subscribed: 8K/sec Total Advertisements: 22K/sec	Subscri Total A
Maximum channel throughput	6 Mbps	20 Mbp
Maximum and average latency	Maximum: 3 seconds Average: 1.5 seconds	Maxim Averag
High Availability Failover Time	360 seconds	300 sec
Any impact to existing Wi-Fi capabilities	Maximum WiFi clients reduced: From 5000 to 4000, From 10000 to 8000 (with Performance license)	Maxim 32000 t

Note

- Key Performance Indicators (KPIs): KPIs are collected in ideal lab conditions with negligible network latency. The above table represents only ideal conditions. In production, numbers may vary from environment to environment.
- Latency: The delay between BLE events initiated from AP to when they are received from the MQTT application (third-party application).
- Maximum MQTT Throughput: The throughput of the MQTT channel between IoT Orchestrator and third-party application.
- Maximum GRPC Events or Messages: The maximum number of events or messages the IoT Orchestrator can handle from AP.
- Maximum BLE Advertisements Handling - The maximum BLE advertisements the IoT Orchestrator can process or handle.
- Total Advertisements: Covers both subscribed advertisements and advertisements received from non-onboarded or connected devices.
- High Availability Failover Time: The time taken for IoT Orchestrator to resume operations after active controller goes down.



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.

Procedure

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 of the IoT Orchestrator.

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 as the deployment flow will fail.

For example, in the subnet 192.168.1.0/30, 192.168.1.1 can be used as the IP address of the IoT Orchestrator, and 192.168.1.2 can be used as the IP address of the default gateway.

Step 4 Enter the subnet mask of the IoT Orchestrator.

Note

The recommended 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 IP address of the default gateway for the IoT Orchestrator.

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

Step 6 Enter the NAT IP address used by Cisco Access Points to reach the IoT Orchestrator.

Note
This configuration is necessary only when a direct connection between Cisco Access Points and the IoT Orchestrator is not possible, such as when a Cisco Catalyst 9800 Wireless Controller is behind a firewall or in a remote data center. For more information, see the NAT Configuration.

Step 7 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 8 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 laptop or computer 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.
- The use of app-hosting commands to install, uninstall, activate, deactivate, start, or stop is not supported and may lead to an error state of the IoT Orchestrator. The use of the IOx web interface (from **Configuration > Services > IOx**) is also not supported for performing any operations on the IoT Orchestrator. Only the IoT Services web interface

(from **Configuration > Services > IoT Services**) is supported for Day-0 and Day-1 management operations for the IoT Orchestrator.

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.
- Upgrading from any version in the 1.0.x series to version 1.1.0 is not supported. If the IoT Orchestrator is operating on a pre-release (Public Beta) version, you must uninstall the existing software and perform a fresh installation using the official release version 1.1.0.

Container Data Persistency and 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 must be 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 must be 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.

Stateful-Switchover (SSO)

When the Cisco Catalyst 9800 Wireless Controller is configured with SSO, the active controller will handle syncing the VirtualPortGroup interface configuration, the IOx container application, and the IoT Orchestrator databases.

Note The IOx process, responsible for managing container applications in the Cisco Catalyst 9800 Wireless Controller, starts in the standby controller only after it takes over due to a stateful switchover (SSO) maneuver. The average time for this process to start is between 2 and 3 minutes. Only after the IOx process starts in the old standby or new active controller, the IoT Orchestrator will be able to respawn with the configuration saved from the old active or new standby controller.

N+1 (Active/Active High Availability)

When the Cisco Catalyst 9800 Wireless Controller is configured in N+1 mode, the IoT Orchestrator inside each of the N+1 members acts as a standalone IoT controller and gateway, each with its own IP address, API keys, and registered AP or BLE clients.

Note The third-party application is responsible for handling and managing each of the IoT Orchestrators in the N+1 deployment. To facilitate management of this deployment model, a new subscription for critical application events has been introduced. For more information, see the *Cisco Sensor Connect for IoT Services Programmability Guide*.

Launching IoT Orchestrator Application

Before you begin

- Ensure that the IoT Orchestrator status is in Running state.
- Ensure that the IP address of the IoT Orchestrator is reachable from your computer or laptop.
- The IoT Orchestrator may take up to an additional 2 minutes after reaching the Running state to discover HA capabilities in the Cisco Catalyst 9800 Wireless Controller and to synchronize all databases between the controllers.

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 Wireless Controller section.

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

Procedure

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

Procedure

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

Procedure

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 perform a password recovery procedure. For more information, see the Password Recovery for IoT Orchestrator.
- If the incorrect password is entered three times consecutively, a back-off timer will be activated. Each subsequent incorrect attempt will extend the waiting period further, with the timer reaching up to one hour.

Day 1 - Configuring IoT Orchestrator Application

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

Before you begin

Cisco Access Points must be configured with a token and the IoT Orchestrator's root certificate to reach and authenticate with the IoT Orchestrator. The token is generated by the IoT Orchestrator and pushed to the Cisco Catalyst 9800 Wireless Controller via SSH. Additionally, the IoT Orchestrator will enable gRPC on the default-ap-profile. If an AP profile other than the default-ap-profile is used, you must manually enable gRPC on the AP profile by issuing the command `cisco-dna grpc` on each AP profile where gRPC is required.

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

Procedure

Step 1 Enter the controller username.

Note
You must have sufficient privileges to connect through SSH to the wireless controller and perform configuration updates.

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 listens on port 8081 for API requests over HTTPS. APIs are authenticated using API keys generated by the IoT Orchestrator, and the HTTPS server uses a self-signed certificate automatically provisioned by the IoT Orchestrator during the Day-0 flow.

To overwrite the default certificate, follow these steps:

Procedure

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

The following process is required when using a certificate generated by a Certificate Authority (CA). By default, the IoT Orchestrator is ready to onboard or connect and stream data, creating self-signed certificates to secure requests to the REST API interface or when protecting MQTT streaming with a TLS layer. If a certificate signed by a Certificate Authority (CA) is needed, then a certificate signing request (CSR) is required.

The following procedure details how to obtain this CSR and upload it to the IoT Orchestrator:

Before you begin

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

Procedure

Step 1 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
```

You will be prompted to enter the following information:

- Country Name (2 letter code)

- State or Province Name (full name)
- Locality Name (e.g., city)
- Organization Name (e.g., company)
- Organizational Unit Name (e.g., department)
- Common Name (domain name or IP address of IoT Orchestrator)
- Email Address

Note
Use the CSR file generated with the Certificate Authority (CA) of your choice to generate a new certificate for the IoT Orchestrator.

Step 2 Upload the **server.key** file and the certificate provided by your Certificate Authority (CA).

If you want to authenticate RESTful APIs using APIKeys, you must attach the private key (**server.key**) and the certificate generated by the Certificate Authority (CA) of your choice. The former should be added within the **Add your private key** section and the later within the **Add your public key** section.

To authenticate RESTful APIs using certificates, in addition to the private key (**server.key**) and the certificate generated by the Certificate Authority (CA), you will also need the Root Certificate, which can be downloaded from the Certificate Authority (CA) website. The Root Certificate should be added in the **Add your trustroot** field under the **Client Identity** section.

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.

Procedure

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.
- The application IDs can be any string, but do not use the colon (':') character in the application ID, as it is not supported.

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

Procedure

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

Note From release 1.1.1, scanning mode is disabled by default.

Procedure

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.

Configure a filter policy

Create an allow-list filter policy for BLE MAC addresses in IoT Orchestrator.

Procedure

Step 1 Log in to the IoT Orchestrator Web UI.

Step 2 Choose **Configuration** > **Filter Configuration**.

Step 3 Click **Add**.
The configuration window is displayed.

Step 4 Enter the name of the policy in the **Policy Name** field.

Step 5 Check the **Allow-List Prefixes** check box.

Step 6 In the **Configured MAC Prefixes (0 of 64)** field, enter up to 64 MAC address prefixes between 2 and 12 bytes.

Step 7 Click **Save Policy**.

Note If you enable the allow-list filter, APs forward only devices with BLE MAC addresses that match the configured prefixes to the IoT Orchestrator.

Applying BLE Configuration to Access Point using GUI

Before you begin

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

Procedure

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:

Procedure

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:

Procedure

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:

Procedure

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.
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**.

Buttons	Description
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.

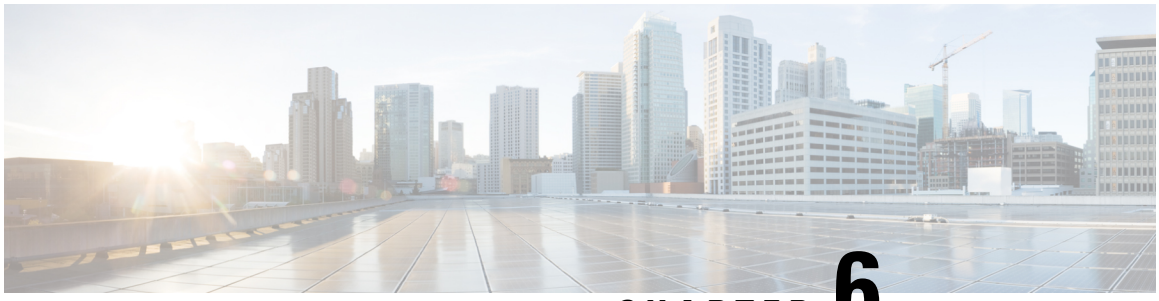
Step 3 Choose **Serviceability** > **Radio Active Logs** to view BLE Device related logs.

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.



CHAPTER 6

NAT Configuration

Overview of NAT Configuration

The Cisco Sensor Connect for IoT Services (Wireless IoT Orchestrator) requires Cisco Access Points to establish a TLS connection using GRPC. The default destination target IP address is the Wireless IoT Orchestrator IP address. This IP address is embedded in a JWT token that is passed to APs using AP profile configuration.

In cloud deployments, the IP address configured on Cisco Access Points differs from the IP address configured in the Wireless IoT Orchestrator. This deployment involves NAT to provide reachability over the internet. The NAT IP address field indicates to the Wireless IoT Orchestrator container which destination IP address the Cisco APs can use for GRPC connection.

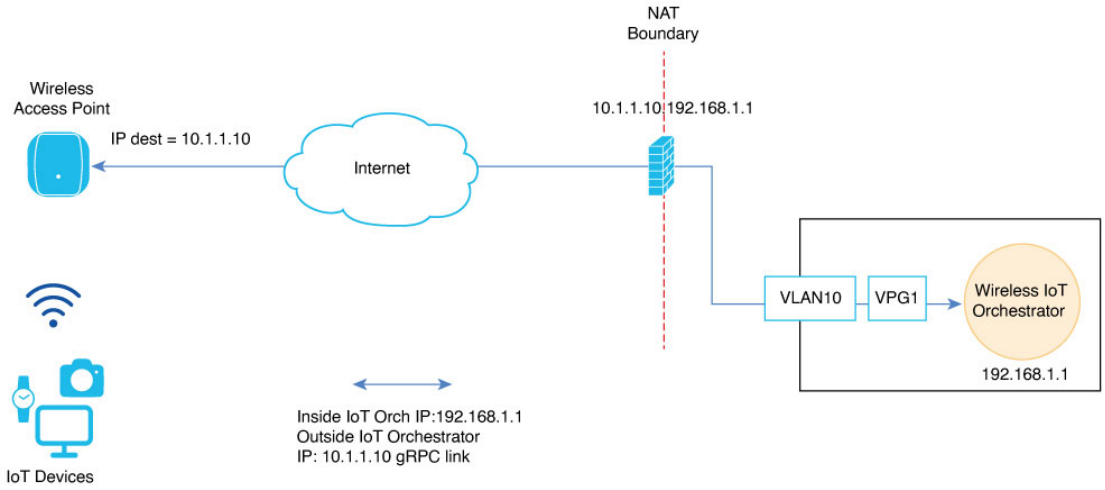
The NAT IP address field is necessary when the Cisco Catalyst 9800 Wireless Controller is configured to use CAPWAP discovery with a public IP. For more information on CAPWAP discovery with a public IP, see the Wireless Management Interface documentation.

This chapter describes how to use the NAT IP address field in the Cisco Catalyst 9800 Wireless Controller Web UI (**Configuration > Services > IoT Services**) and configure NAT on the Cisco Catalyst 9800 Wireless Controller for IoT Orchestrator use cases.

Supported Scenarios

The following scenarios are supported for the NAT IP address field in the Wireless IoT Orchestrator:

Figure 2: Schema for NAT Configured External to the Cisco Catalyst 9800 Wireless Controller (Example: In a Perimetral Firewall)



In Figure 1, the external network device (for instance, a perimetral firewall or router) performs NAT or PAT for the Wireless IoT Orchestrator.

Therefore, add the corresponding NAT IP address of the Wireless IoT Orchestrator to the NAT IP Address field.

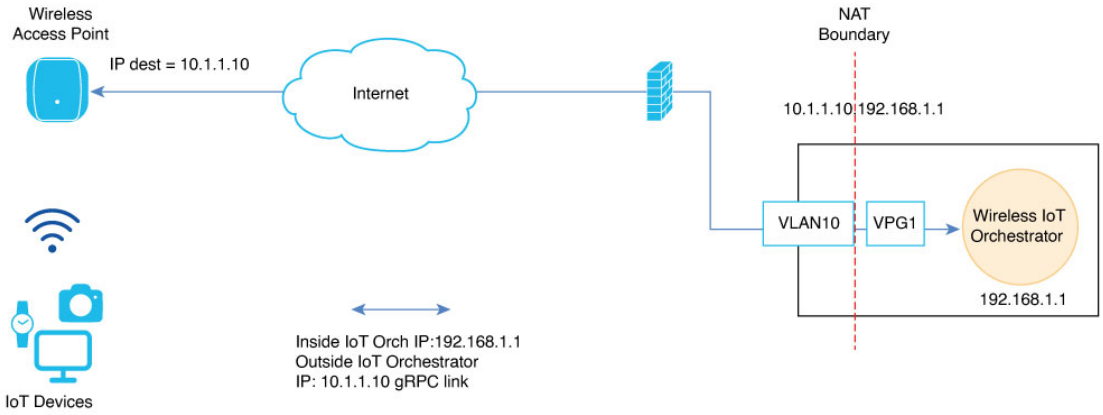
To add the corresponding NAT IP address for the Wireless IoT Orchestrator, perform the following steps:

1. Log in to the Cisco Catalyst 9800 Wireless Controller Web UI.
2. Navigate to **Configuration > Services > IoT Services**.
3. Enter the NAT IP address.

Note The NAT IP address determines the destination IP address used by Cisco APs for the GRPC connection.

4. Click **Enable IoT Services**.

Figure 3: Schema for NAT Configured on Cisco Catalyst 9800 Wireless Controller



Restrictions

- Out-of-band management interfaces of the Cisco Catalyst 9800 Wireless Controller hardware appliances (interface configured under vrf Mgmt-intf) cannot be used as an outside interface for NAT.
- The use of VRFs with NAT configuration for IoT Orchestrator is not supported.
- Static and dynamic NAT or PAT are supported on all Layer 3 interfaces, including SVIs and physical interfaces configured with the **no switchport** command.
- The IP address used as the global address must be an IP address of an interface on the Wireless IoT Orchestrator. For more information, see CSCwn12646.
- As a best practice, NAT should not be used on the same physical port as the Wireless Management Interface (WMI) when APs are deployed in large-scale local mode, or when the uplink port of the Cisco Catalyst 9800 Wireless Controller has limited bandwidth.
- When APs are deployed in FlexConnect mode, there is no restriction on the NAT interface being the same as the WMI. For more information on the AP mode deployments, see the Catalyst 9800 Wireless Controller Configuration Model.

  Once the NAT is configured on the Cisco Catalyst 9800 Wireless Controller, the IP address selected as the NAT outside IP address of the Wireless IoT Orchestrator must be configured in the **NAT IP Address** field as shown in Figure 2.

Examples of NAT Configuration on Cisco Catalyst 9800 Wireless Controller

Prerequisites

- Before mapping any TCP port, ensure that it is not already in use by the Cisco Catalyst 9800 Wireless Controller. To verify, execute the following commands to ensure that each port is available before you attempt to map it:

```
Device# show tcp brief | include <tcp port>
Device# show platform software tcpudpport | include <tcp port>
```

Configuration

The following are the types of configurations:

- Static NAT – Used for AP GRPC connections to the Wireless IoT Orchestrator or for accessing the Wireless IoT Orchestrator GUI.
- Dynamic NAT – Used when the Wireless IoT Orchestrator requires an internet connection, leveraging one of the Cisco Catalyst 9800 Wireless Controller interfaces.

Example: Static NAT Configuration

This example demonstrates how to expose ports 50221 and 43626 on a Cisco Catalyst 9800 Wireless Controller. The configuration was performed on a C9800-CL wireless controller running the 17.15.3 image. GigabitEthernet1 is configured as the Wireless Management Interface, and APs are deployed in FlexConnect mode.

Configuration Details:

- Wireless IoT Orchestrator IP address: 192.168.1.1/30
- Default Gateway for IoT Orchestrator: 192.168.1.2
- GigabitEthernet1 IP address: 10.1.1.10/24

To configure static NAT, issue the following commands on the controller:

```
Device (config)# interface GigabitEthernet1
Device (config-if)# no switchport
Device (config-if)# ip address 10.1.1.10 255.255.255.0
Device (config-if)# ip nat outside
Device (config-if)# exit
Device (config-if)#interface VirtualPortGroup1
Device (config-if)# ip address 192.168.1.2 255.255.255.252
Device (config-if)# ip nat inside
Device (config-if)# exit
Device (config)# ip nat inside source static tcp 192.168.1.1 43626 interface GigabitEthernet1
 43626
Device (config)# ip nat inside source static tcp 192.168.1.1 50221 interface GigabitEthernet1
 50221
Device (config)# exit
```

To verify the static NAT configuration details, use the following command:

```
Device# show platform software nat chassis active F0 translation
Pro  Inside global         Inside local          Outside local         Outside global
tcp  10.1.1.10:43626       192.168.1.1:43626     ---                   ---
tcp  10.1.1.10:50221       192.168.1.1:50221      ---                   ---
Total number of translations: 2
```

Example: Dynamic NAT Configuration

This example demonstrates how to overload all traffic from the Wireless IoT Orchestrator towards the internet through interface Vlan 180, except for traffic destined for access points. Assume an AP deployment in local mode, adhering to all NAT restrictions and recommendations in this document.

Configuration Details:

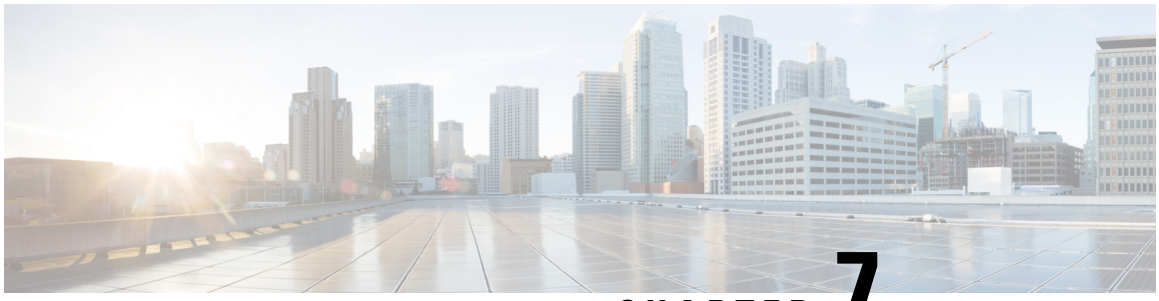
- Wireless IoT Orchestrator IP address: 192.168.1.1/30
- Default Gateway for IoT Orchestrator: 192.168.1.2
- Vlan 180 IP address: 172.16.200.100/24
- IP subnets for access points: 192.168.15.0/24 and 10.10.10.0/24

To configure dynamic NAT, issue the following commands on the controller:

```
Device(config)# interface Vlan 180
Device (config-if)# ip address 172.16.200.100 255.255.255.0
Device (config-if)# ip nat outside
Device (config-if)# exit
Device (config-if)#interface VirtualPortGroup1
Device (config-if)# ip address 192.168.1.2 255.255.255.252
 WLC(config-if)# ip nat inside
Device (config-if)# exit
Device (config)# ip access-list extended NAT_IOT_ACL
Device (config-ext-nacl)# 10 deny ip host 192.168.1.1 192.168.15.0 0.0.0.255
Device (config-ext-nacl)# 20 deny ip host 192.168.1.1 10.10.10.0 0.0.0.255
Device (config-ext-nacl)# 30 permit ip host 192.168.1.1 any
Device (config)# exit
Device (config)# ip nat inside source list NAT_IOT_ACL interface Vlan 180 overload
Device (config)# exit
```

To verify the dynamic NAT configuration details, use the following command:

```
Device# show platform software nat chassis active F0 translation
Pro  Inside global         Inside local          Outside local         Outside global
icmp 172.18.29.7:8743      192.168.1.1:8743      8.8.8.8:8743          8.8.8.8:8743
tcp  172.18.29.7:5062      192.168.1.1:45156     173.37.145.84:443     173.37.145.84:443
Total number of translations: 2
```



CHAPTER 7

Common Issues or Troubleshooting

Access Points cannot join the Wireless IoT Orchestrator

Here are the common reasons Access Points may not join the IoT Orchestrator after onboarding the Cisco Catalyst 9800 Wireless Controller:

1. **Reachability**: The access point's subnet cannot reach the IoT Orchestrator's subnet. Use the following steps to troubleshoot:
   - Verify ping connectivity between the Access Point and IoT Orchestrator.
   - Ensure no filtering rules exist in routing devices between Access Points and IoT Orchestrator. Open TCP ports 50221 and 43626 for discovery and communication in firewalls between Access Points and IoT Orchestrator.
2. **AP Profiles**: The IoT Orchestrator automatically enables GRPC only in the default-ap-profile. Access Points using a profile other than the default-ap-profile must manually configure GRPC on those profiles. Add the configuration line **cisco-dna grpc** to each ap-profile.
3. **Spaces Connector interaction with Wireless IoT Orchestrator**: Cisco Spaces Connector cannot be configured at the same time as IoT Orchestrator. You must disable IoT Services on the Cisco Spaces Connector before deploying IoT Orchestrator. Follow these steps if this was not done:
   a. Disable IoT Services within Cisco Spaces Connector.
   b. In IoT Orchestrator, go to the **Administrator** section, then select **9800 Wireless Controller configuration**. Redeploy the username and password to ensure the correct JWT token is pushed to the Cisco Catalyst 9800 Wireless Controller, prompting APs to re-join the IoT Orchestrator.

Wireless IoT Orchestrator UI cannot be accessed from a laptop or computer

Here are the common reasons why the wireless IoT Orchestrator UI cannot be accessed from a laptop or computer:

1. **Initial Wait Time**: After installing IoT Orchestrator, wait until it reaches the **Running** state in the **Configuration > Services > IoT Services** page on the Cisco Catalyst 9800 Wireless Controller UI. The system will take 1-2 minutes to detect the deployment type (standalone or SSO). If needed, it will sync databases with the standby controller. During this period, the access to the IoT Orchestrator UI will be unavailable.
2. **Reachability**: Use the **ping** command to verify that the IoT Orchestrator can be reached from your laptop or computer. If necessary, adjust the routing configuration in your network to ensure your PC or laptop can reach the IoT Orchestrator. If routing changes are not possible, consider configuring NAT. For information, see the NAT Configuration.

NAT configuration on the Cisco Catalyst 9800 Wireless Controller is not functioning properly

Follow these steps to troubleshoot connectivity issues related to NAT configuration on the Cisco Catalyst 9800 Wireless Controller.

1. Ensure that the ports on your outside interface are not currently in use by another application on the Cisco Catalyst 9800 Wireless Controller.
   a. Remove the NAT configuration from the outside interface on the Cisco Catalyst 9800 Wireless Controller.
   b. Run the following commands to verify that each TCP port used for NAT is not in conflict:

```
Device# show tcp brief | include <tcp port>
Device# show platform software tcpudpport | include <tcp port>
```

Note Ensure these commands return no conflicts for the ports configured for NAT.

2. Examine the NAT entries in the NAT table to ensure the inside IP address matches the IP address of the IoT Orchestrator. Also, confirm that the TCP ports listed are correct.

```
Device# show platform software nat chassis active F0 translation
Pro  Inside global         Inside local          Outside local         Outside global
tcp  172.18.29.7:9433      192.168.1.1:443       ---                   ---
tcp  192.168.2:50221       192.168.1.1:50221     ---                   ---
tcp  192.168.2:43626       192.168.1.1:43626     ---                   ---
Total number of translations: 3
```

3. Verify that the IP addresses used for NAT are among those configured in the Cisco Catalyst 9800 Wireless Controller. These must be identical, as different IP addresses within the same subnet are not supported. For more information, refer to CSCwn12646.

Password Recovery for IoT Orchestrator

If the admin user's password is lost, follow the Password Recovery process outlined below:

1. Log in to the Cisco Catalyst 9800 Wireless Controller using the **ssh** connection.
2. Log in to the IoT Orchestrator shell:

```
Device# app-hosting connect appid IoT_Orchestrator session bash
root@96e268c7acb8:/#
```

3. Touch the following file in shell:

```
root@96e268c7acb8:/#touch /iox_data/recovery/passwordRecovery
```

4. Open a new browser window and open a connection to the IoT Orchestrator GUI.

   The Day 0 banner is displayed. Read the terms and conditions and click **I Accept**.

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

5. Enter **admin** for username and **password** for password (default credentials).
6. Log in with the new username.

Note This process deletes all users created in IoT Orchestrator (Spaces Orchestrator Software) database and returns the login to the Day 0 credentials.

Prerequisites

- This feature is supported from Cisco Spaces Connect for IoT Services, 1.0.3 release.
- Ensure that an ssh connection is established to the Cisco Catalyst 9800 Wireless Controllers with privilege access to the **app-hosting** commands.

Common Problems During IoT Orchestrator Installation

Here are the common issues encountered during the installation of IoT Orchestrator:

1. **Application Configuration Failed**: During Day 0 installation, there is some configuration that is done on the Cisco Catalyst 9800 Wireless Controller. This means the IP addresses chosen for IoT Orchestrator were incorrect, as they were already used by the Cisco Catalyst 9800 Wireless Controller. Ensure that you use a unique IP subnet for the IoT Orchestrator.
2. **Installation of IoT Orchestrator failed**: After the failure, syslog messages are displayed on the Cisco Catalyst 9800 Wireless Controller console, such as:

```
%IOXCAF-6-INSTALL_MSG: Chassis 2 R0/0: wncloudm: app-hosting: Failed to install
IoT_Orchestrator: app-hosting infrastructure is busy! Try again later
```

If IoT Orchestrator fails to install for any reason, it will automatically revert any changes made to the configuration (for instance, VirtualPortGroup configuration) and return to the Day 0 page. The fields for entering the IP address, subnet mask, default gateway, and NAT IP address are prepopulated with previous values. Some of the most common causes include:

a. The IP address selected for IoT Orchestrator and default gateway are not in the same subnet (according to the subnet mask provided).

b. If the tar file is extracted, modified, and repacked, the IoT Orchestrator image signed by Cisco root CA is verified during installation by the Cisco Catalyst 9800 Wireless Controller. If you modify the tar file, the installation fails.

c. Another IOx application is installed on the Cisco Catalyst 9800 Wireless Controller. IoT Orchestrator must run as the only IOx application on the C9800 Wireless Controller. If another application, such as GuestShell, is running, the installation will fail, reporting that not enough resources are available. For more information, see the CSCwo66172.

Using App-Hosting Control Commands with IoT Orchestrator

Using app-hosting control commands with IoT Orchestrator is not supported, and this could cause the IoT Services webpage to become unresponsive. If the IoT Orchestrator application has been altered using an app-hosting command, apply the appropriate app-hosting CLI to revert the changes.

Command used in IoT Orchestrator	Command to revert to valid state
app-hosting stop appid IoT_Orchestrator	**app-hosting start appid IoT_Orchestrator**
app-hosting deactivate appid IoT_Orchestrator	To reactivate the IoT Orchestrator, use the command **app-hosting activate appid IoT_Orchestrator** followed by **start** if the **app-hosting stop** command was used.
app-hosting uninstall appid IoT_Orchestrator	Please follow the actions listed below, if the IoT Services UI page remains unresponsive.

If the IoT Services UI page remains unresponsive, you can perform the following actions:

- Restart HTTP server on Cisco Catalyst 9800 Wireless Controller, by executing the following commands from its console:

```
Device(config)#no ip http server
Device(config)#ip http server
```

- Reload the Cisco Catalyst 9800 Wireless Controller during a maintenance window.
- Open a case with Cisco TAC.