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 1: 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.