Device OnBoarding And Connection to the Dosatsu Platform

Introduction

In the document of Platform API, we have describe the APIs how to interact with the services in the Dosatsu platform. All the data managed by the Dosatsu are posted by the APIs, such as equipment and relevant data. To ensure that the APIs are used legitimately and its data transmission is secure, we need to onboard the device and secure its connection to the Dosatsu platform. The Dosatsu platform allows two connection methods to onboard device and secure connection:

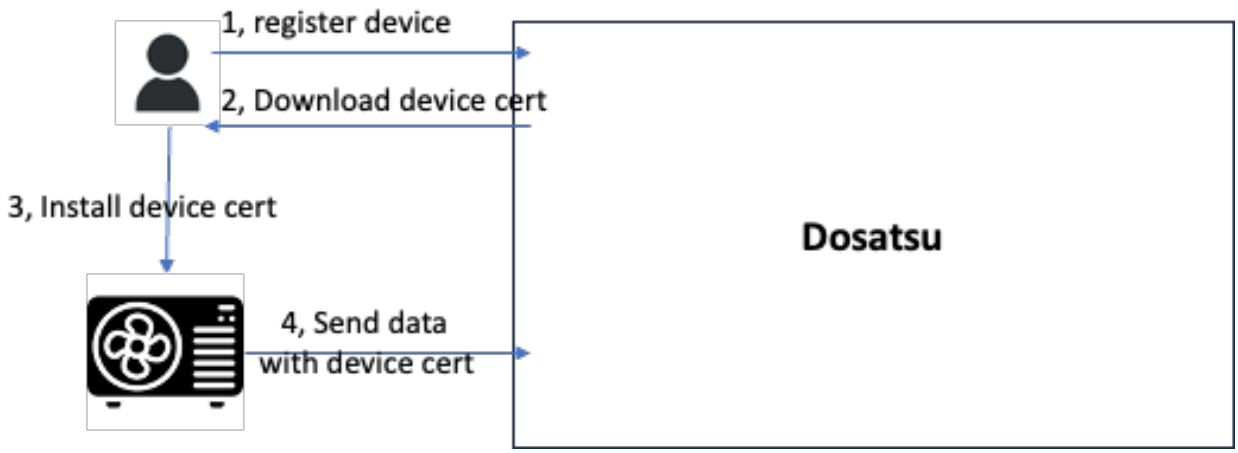
- MQTTS: For an individual device, register the device to get certificates and key for secure connection, install certificates and key on device and service, use certificate to secure a MQTTS connection with the Dosatsu platform and call the API to send data to the Dosatsu platform.
- HTTPS: For multiple equipments which share the same secure connection mechanism, typically multiple equipments managed by a same edge, register the IOConnection to get certificates and key for secure connection, install certificates and key on device and service, use certificate to secure a HTTPS connection with the Dosatsu platform to get access token for the device, and use access token to secure a HTTPS connection with the Dosatsu platform and call the API to send data to the Dosatsu platform.

In the later sections, we will explain the details of the above two connections so that the users can onboard device and secure connection to send data to the Dosatsu platform. As for sending different types of data, please refer the document of Platform API.

In this document, we use cp-stage.daikinlab.com as the base URL of the Dosatsu Platform.

Connection Methods

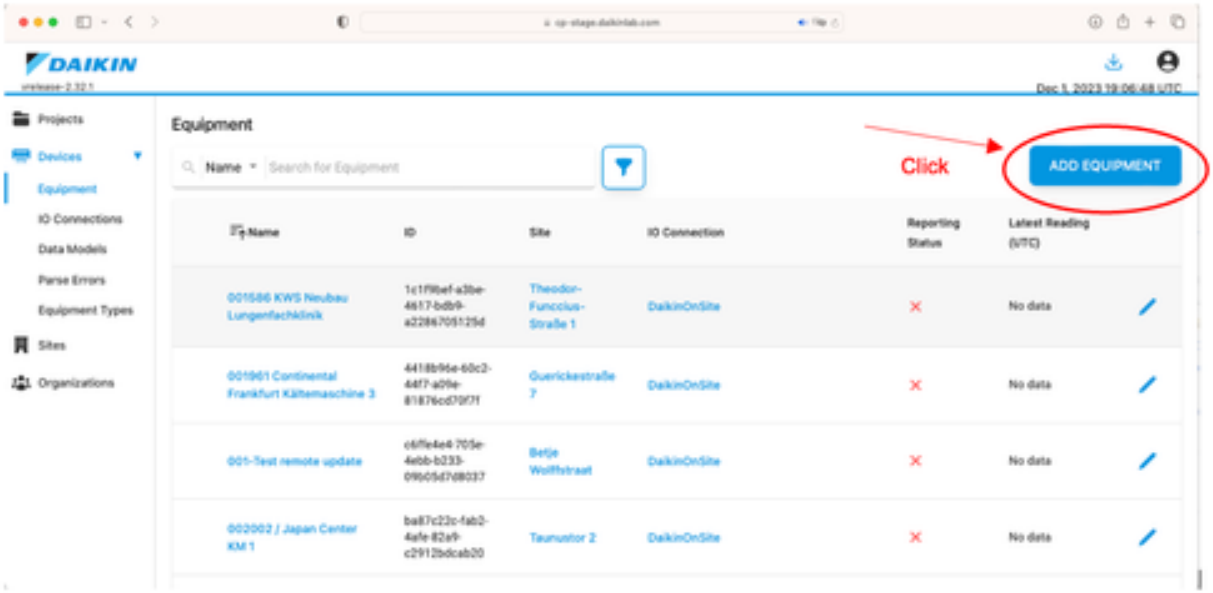
MQTTS



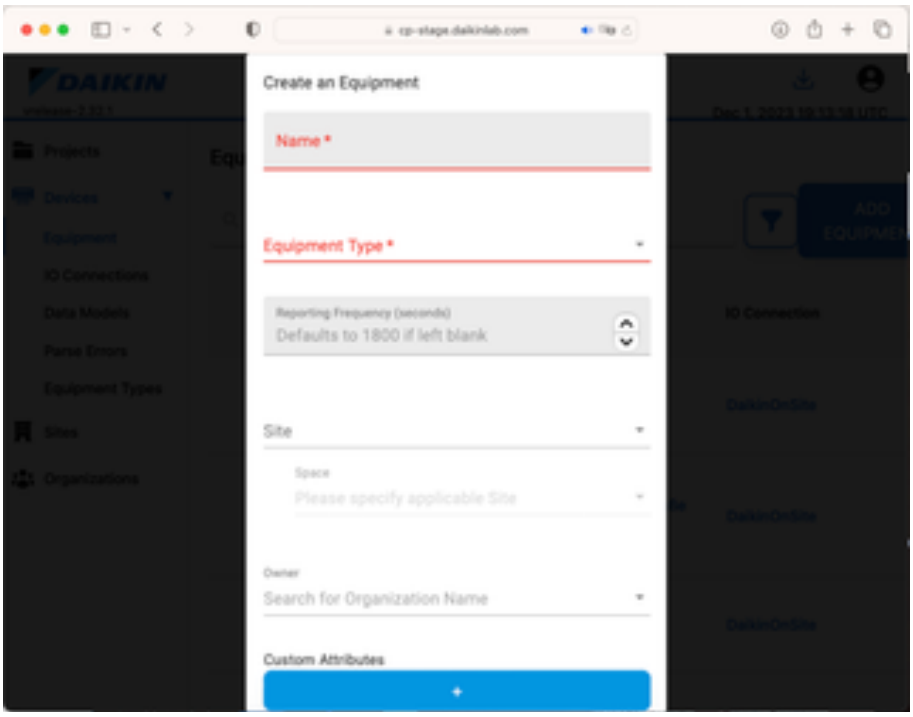
The steps in the above picture are detailed below.

Step#1 Equipment Registration

An equipment/device that would connect to the common platform, needs to be first registered at http://cp-stage.daikinlab.com/app/equipment

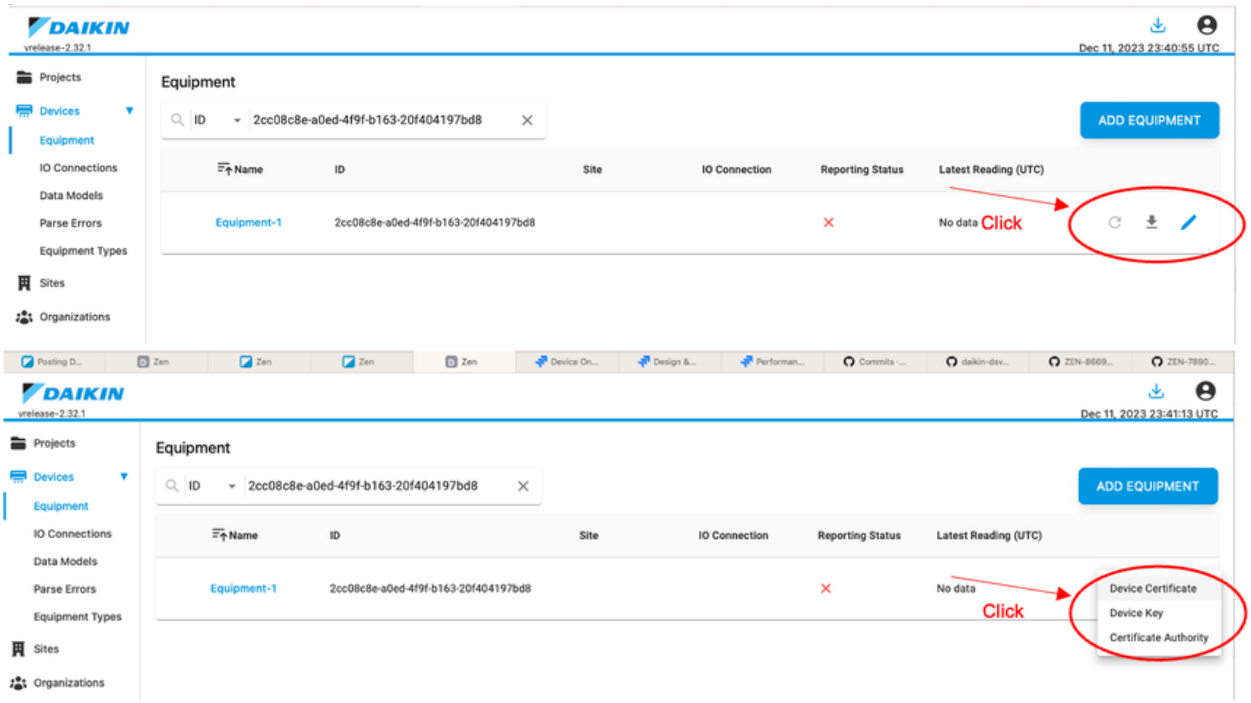


Create an equipment clicking on the blue button “ADD EQUIPMENT”.



Step#2 Download device certificates

Download the device certificate(s) by clicking the download icon. It will prompt you to save the certificates (device cert, device cert key, root ca) to your disk.



The download file names would by default be:

- Device certificate – <deviceid>.crt
- Device certificate key – <deviceid>-key.crt
- Root CA (Certificate Authority) – cp-stage-daikinlab-com.crt

Step#3 Install certificate

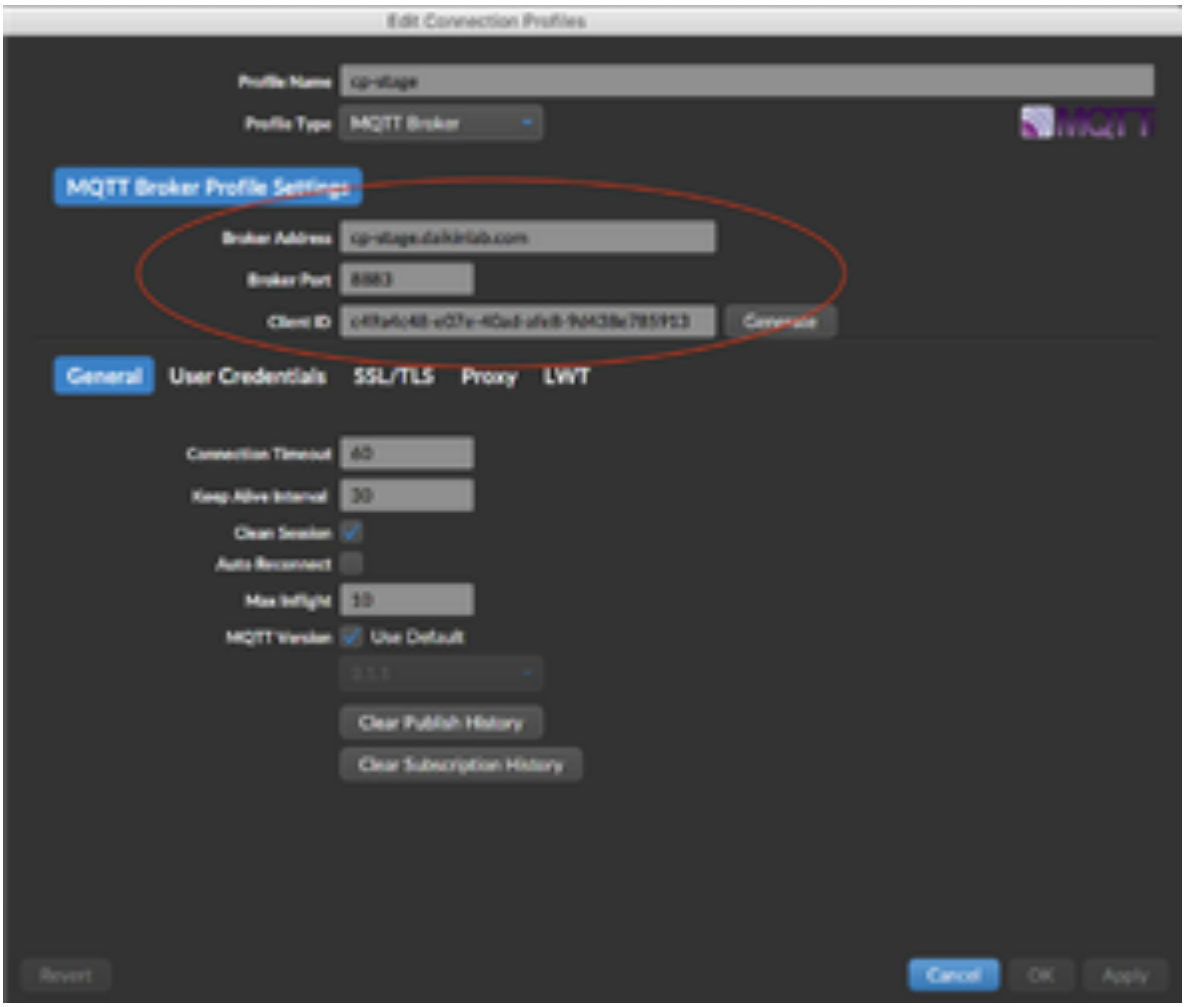
On an edge device, the certificate should be stored securely. Preferably on a hardware security module (HSM). For this test, download to a safe place on your computer.

Step#4 Equipment Connection

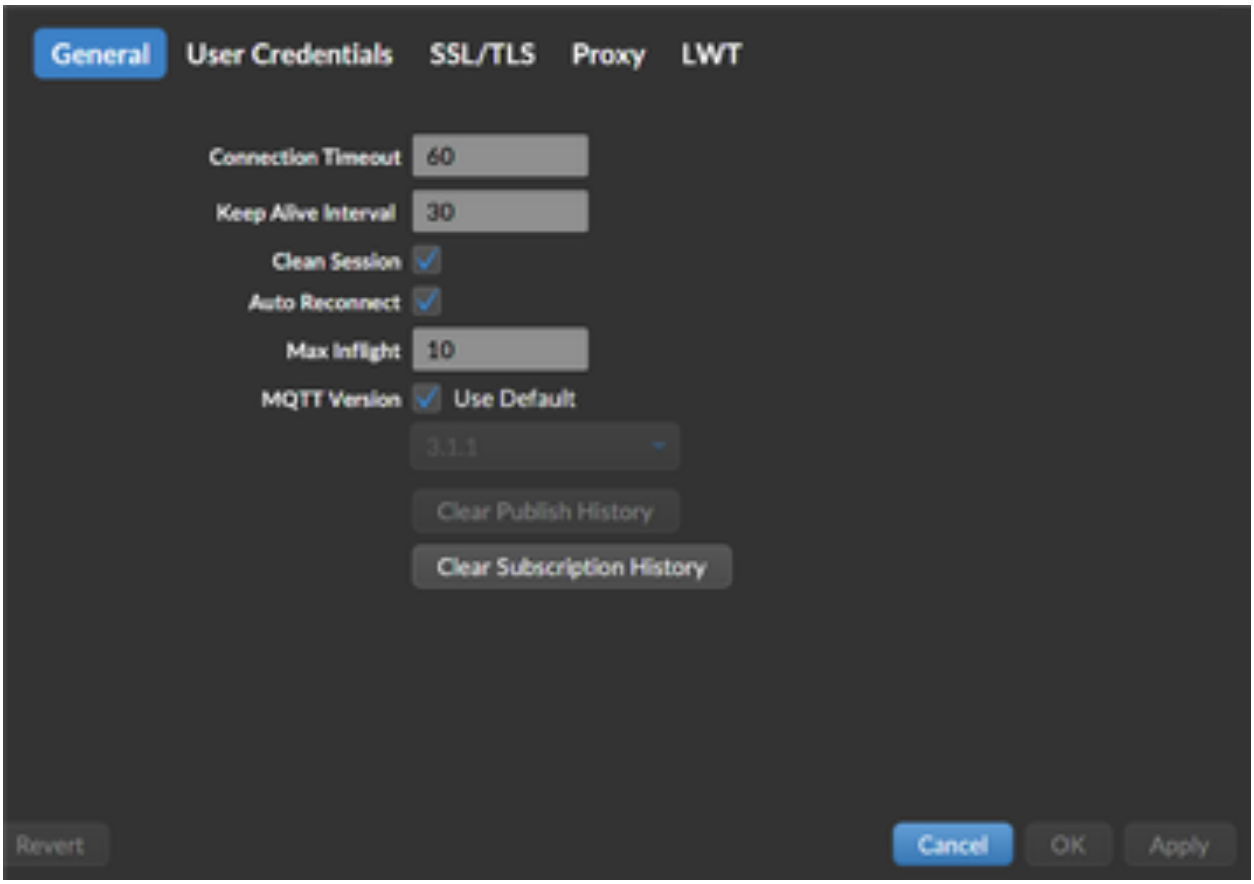
Collect Equipment ID and certificates from the previous steps before proceeding to the next step for device connections.

Use them to connect the Dosatsu platform over MQTTS. For example if you are using MQTT.fx to test connection or simulate a device, follow these instructions:

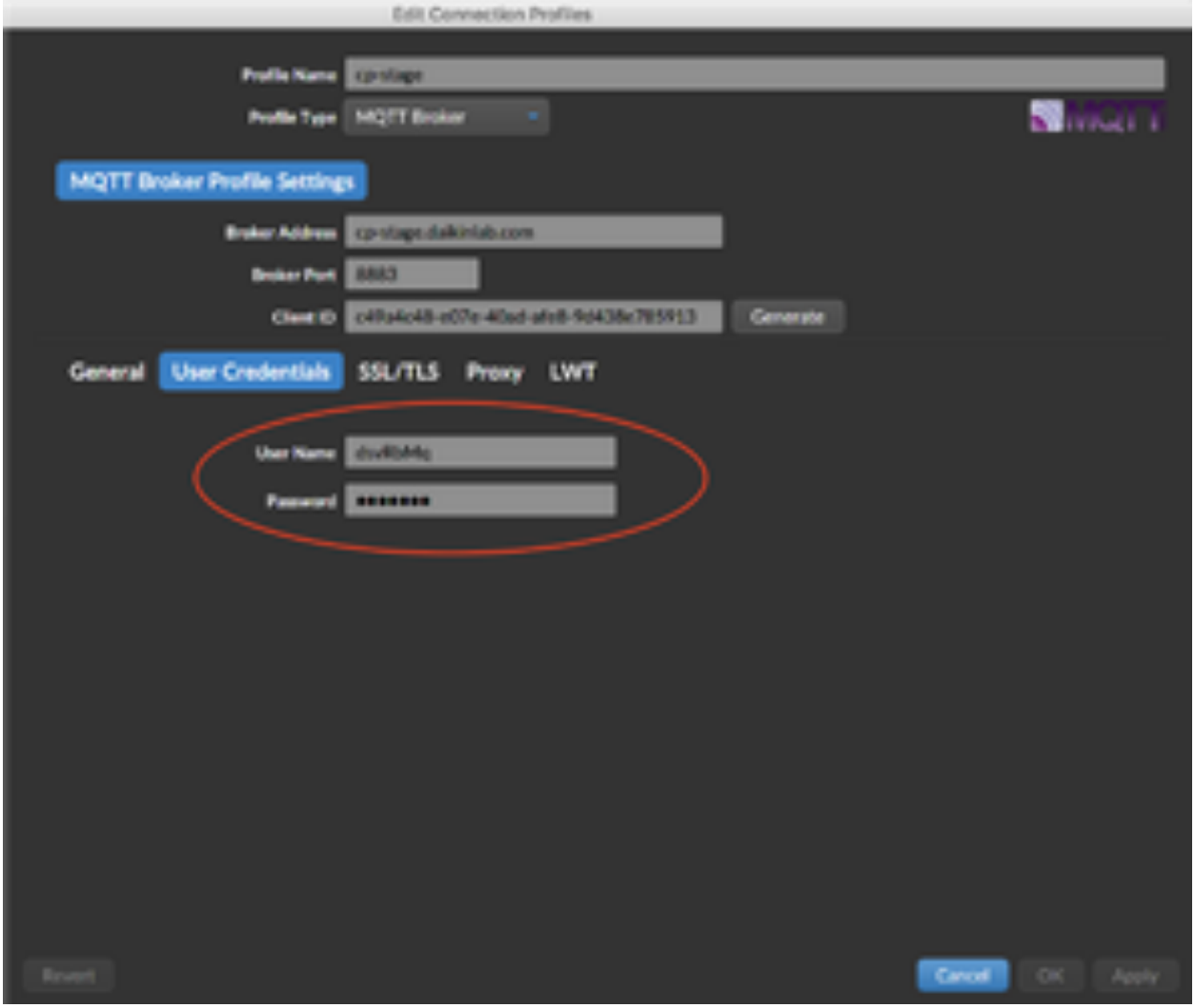
Configure MQTT.fx tool broker settings (address: http://cp-stage.daikinlab.com , Port: 8883) and enter Equipment ID from the Dosatsu platform into “Client ID” text field



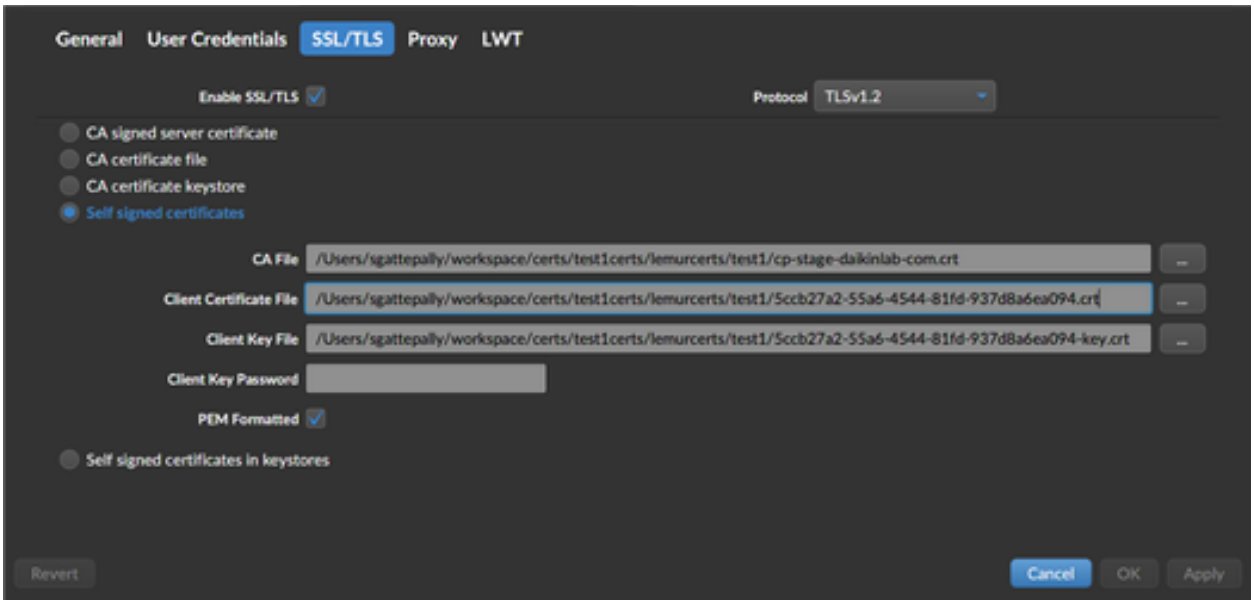
General setting tab enter the following numbers for longer connection window



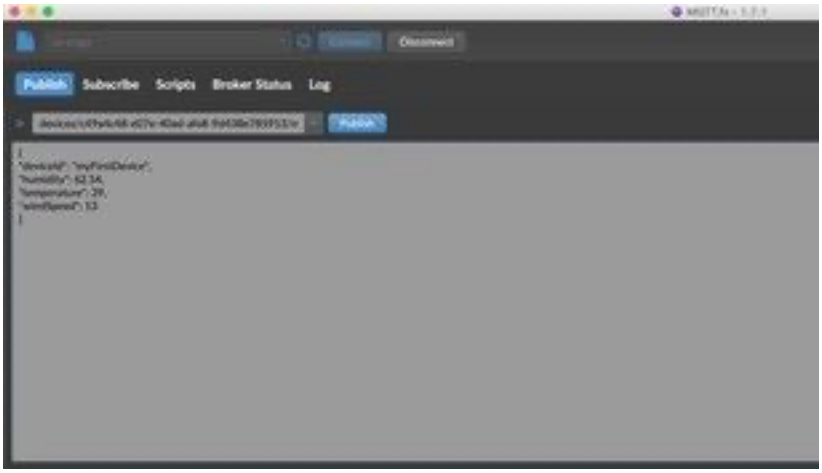
Enter dsvRbMq/<password> in the “User Credentials” tab. Get password from Support



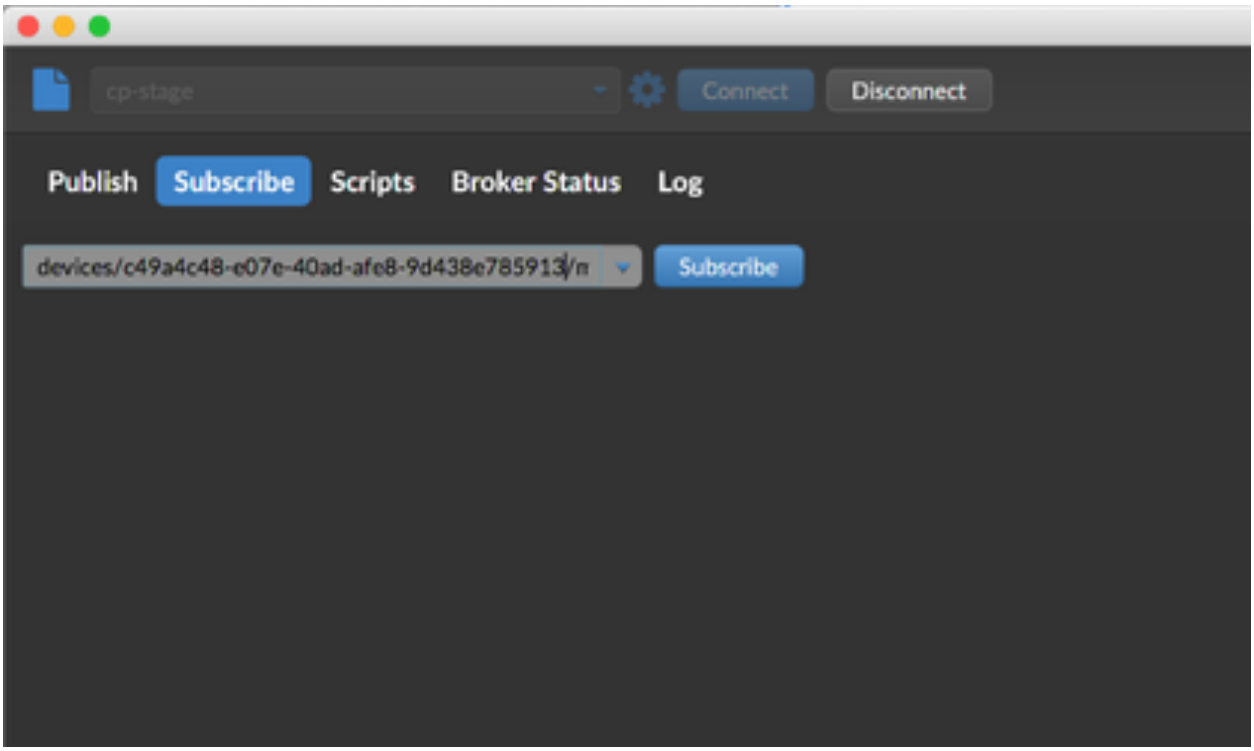
1. SSL/TLS: Select the cert files for SSL/TLS settings as shown in the picture. Earlier on this page in “Step#2 Download device certificate”, certificates were downloaded. We need to use them here.
    1. For CA File choose “cp-stage-daikinlab-com.crt” file.
    2. For Client Certificate File choose the Device certificate – <deviceid>.crt
    3. For Client Key File chooe Device certificate key – <deviceid>-key.crt
    4. For Client Key Password: Keep it empty.



1. Apply and click connect on the main window.
2. To post readings to the Dosatsu platform, enter “devices/<deviceid>/messages/events” in the publish topic name and enter payload and “publish”.



To receive settings from the Dosatsu platform, enter “devices/<deviceid>/messages/devicebound” in the subscribe window and press “subscribe”.

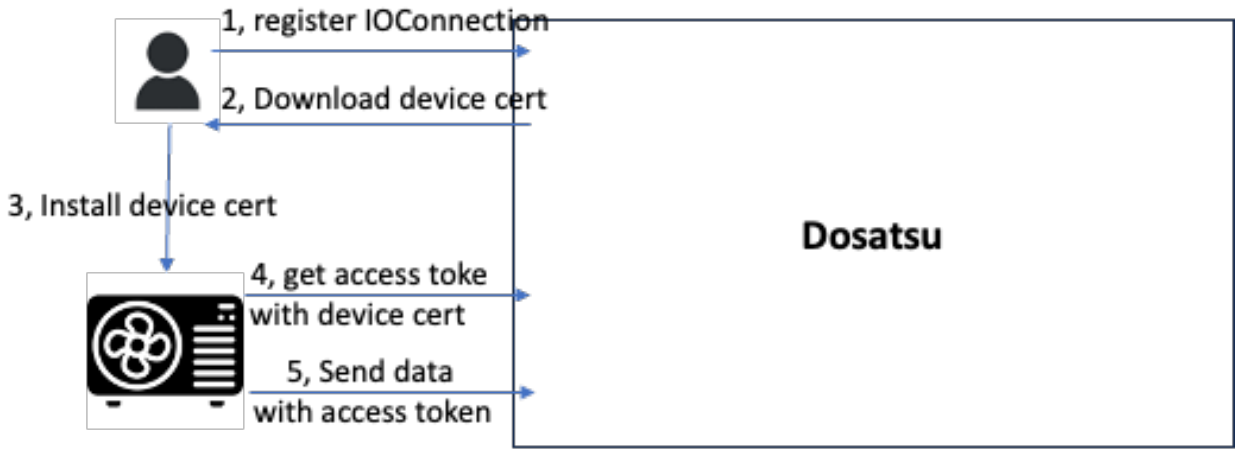


Equipment Blocking:

An administrator can block connections of a device by performing these steps:

1. Revoking certificate.
2. Change device status to ‘disabled’.

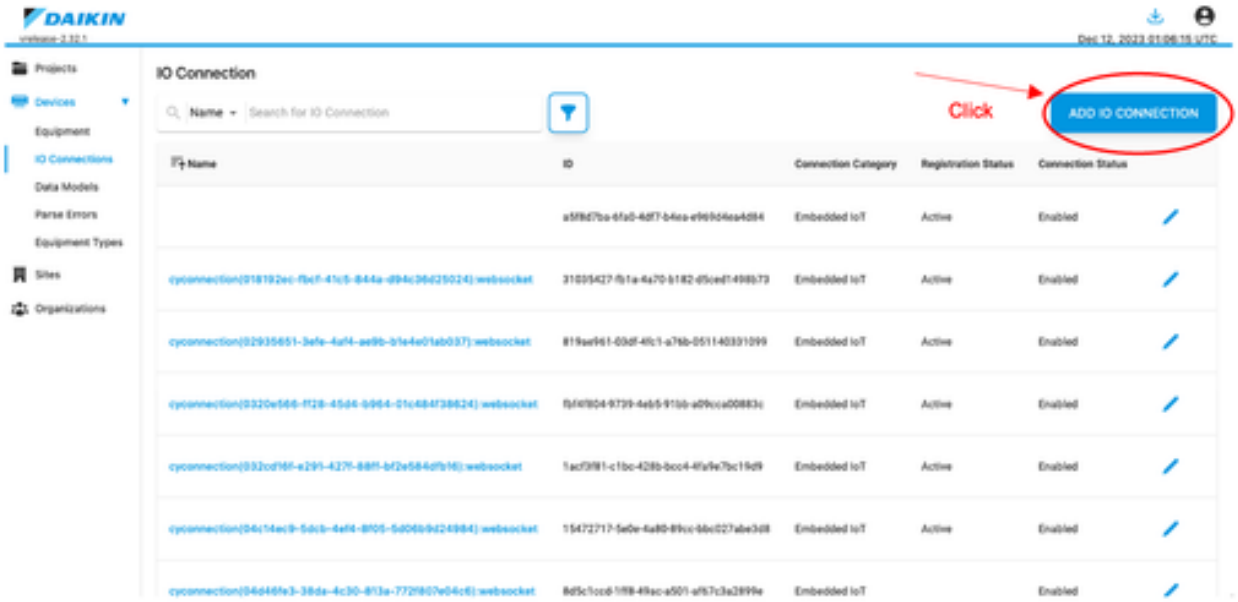
HTTPS



The steps in the above picture are detailed below.

Step#1 IoConnection Registration

For an ioconnection to connect to the common platform, it needs to be first registered at http://cp-stage.daikinlab.com/app/ioconnection

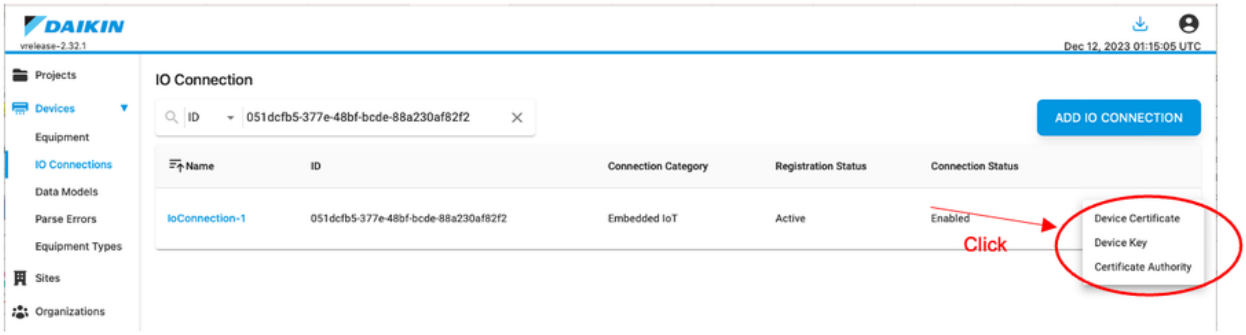


Create an ioconnection clicking on the blue button “ADD IO CONNECTION”.

To generate certificates for a new IoConnection, it is required to mark the checkbox “Request Certificates”.

Step#2 Download IoConnection Certificates

Download the device certificate(s) by clicking the download icon. It will prompt you to save the certificates (device cert, device cert key, root ca) to your disk.



Step#3 Use IoConnection Certificates

In any edge cloud which aggregates equipment data in a region and use an IOConnection to send the equipment data to our cloud, the certificate should be stored securely in the edge cloud. The certificates are used as below:

- Device certificate – <deviceid>.crt: The certificate for the IOConnection.
- Device certificate key – <deviceid>-key.crt: The certificate key for the IOConnection.
- Root CA (Certificate Authority) – cp-stage-daikinlab-com.crt: The certificate to establish HTTPS connection to the HTTP service in our cloud.

Equipment Connection

The connection requires two steps:

1. Get access token

```
1. POST https://sso.daikinlab.com/auth/realms/daikin/protocol/openid-
   connect/token
2. Request Headers:
3. Content-Type:application/x-www-form-urlencoded
4. Request Body:
5. grant_type:client_credentials
6. client_id:cpiot
7. client_secret:<CLIENT_SECRET>
8. Response:
9. {
10.      "access_token": "<ACCESS_TOKEN>",
11.      "expires_in": 300,
12.      "token_type": "bearer",
13.      "not-before-policy": 1582439696,
14.      "session_state": "5873b3b2-868c-4516-9b99-ec03cc472d11",
15.      "scope": "profile email"
16.  }
```

2. Post Data: Ex:

```
1. POST https://cp-stage.daikinlab.com/data
2. Headers:
3. ioconnectionref:<IOCONNECTION_ID>
4. Authorization:Bearer <ACCESS_TOKEN>
5. Body:
6. {
7.   "category_name": "Allergen Count",
8.   "category_color": "blue",
9.   "parameter_name": "Alternaria Mold",
10.    "log_value": 24,
11.    "particle_category": "1",
12.    "env_index": "4",
13.    "log_unit": "particles",
14.    "log_intensity": "Moderate",
15.    "t": "2019-06-11T00:00",
16.    "networkRef": "111-000-111"
17.  }
```

Equipment Blocking

An administrator can block connections of a device by performing these steps:

1. Change device status to ‘disabled’.

Trouble shooting

HTTP Status 401

HTTP Status 401 and HTTP Response “Unauthorized” indicates an expired or invalid JWT token.

If the access token expires, get a fresh access token:

```
POST https://sso.daikinlab.com/auth/realms/daikin/protocol/openid-
connect/token
Request Headers:
Content-Type:application/x-www-form-urlencoded
Request Body:
grant_type:client_credentials
client_id:cpiot
client_secret:<CLIENT_SECRET>
Response:
{
    "access_token": "<ACCESS_TOKEN>"
    "expires_in": 300,
    "token_type": "bearer",
    "not-before-policy": 1582439696,
    "session_state": "5873b3b2-868c-4516-9b99-ec03cc472d11",
    "scope": "profile email"
}
```

HTTP Status 400

HTTP Status 400 indicates an invalid/disabled equipment ID or invalid json body.

HTTP Status 200

HTTP Status 200 indicates a successful connection & Response