D70 - Getting Started Guide for AWS IoT Core

Glossary

- *Thing*: Device in AWS IoT Core
- AWS: Amazon Web Services
- DQP: Device Qualification Program (AWS program)
- Webview: Embedded web server for configuration and monitoring

1 - Document information

This document provides instructions for connecting the SOCOMEC DIRIS Digiware M/D gateway to AWS IoT Core :

- Register and configure your *Thing* in AWS IoT Core
- Provision your device
- Configure AWS IoT Core connectivity on the device

Prerequisites:

- IP address
- DNS
- Outgoing port 8883 open
- SNTP Configured configured

2 - Overview

The DIRIS Digiware D-50 (and D-70) display is a master on the Digiware bus and acts as a gateway interface to communicate measurements over RS485 and Ethernet.

DIRIS Digiware M-50 and M-70 act as the Digiware system interface and communication gateway centralizing measurements from DIRIS Digiware modules and communicating data over Ethernet.

3 - Hardware Description

Product user manual and datasheet can be found here:

- For D50/D70: https://www.socomec.us/en-us/reference/48290203
- For M50/M70: https://www.socomec.us/en-us/reference/48290204

4 - Set up your Development Environment

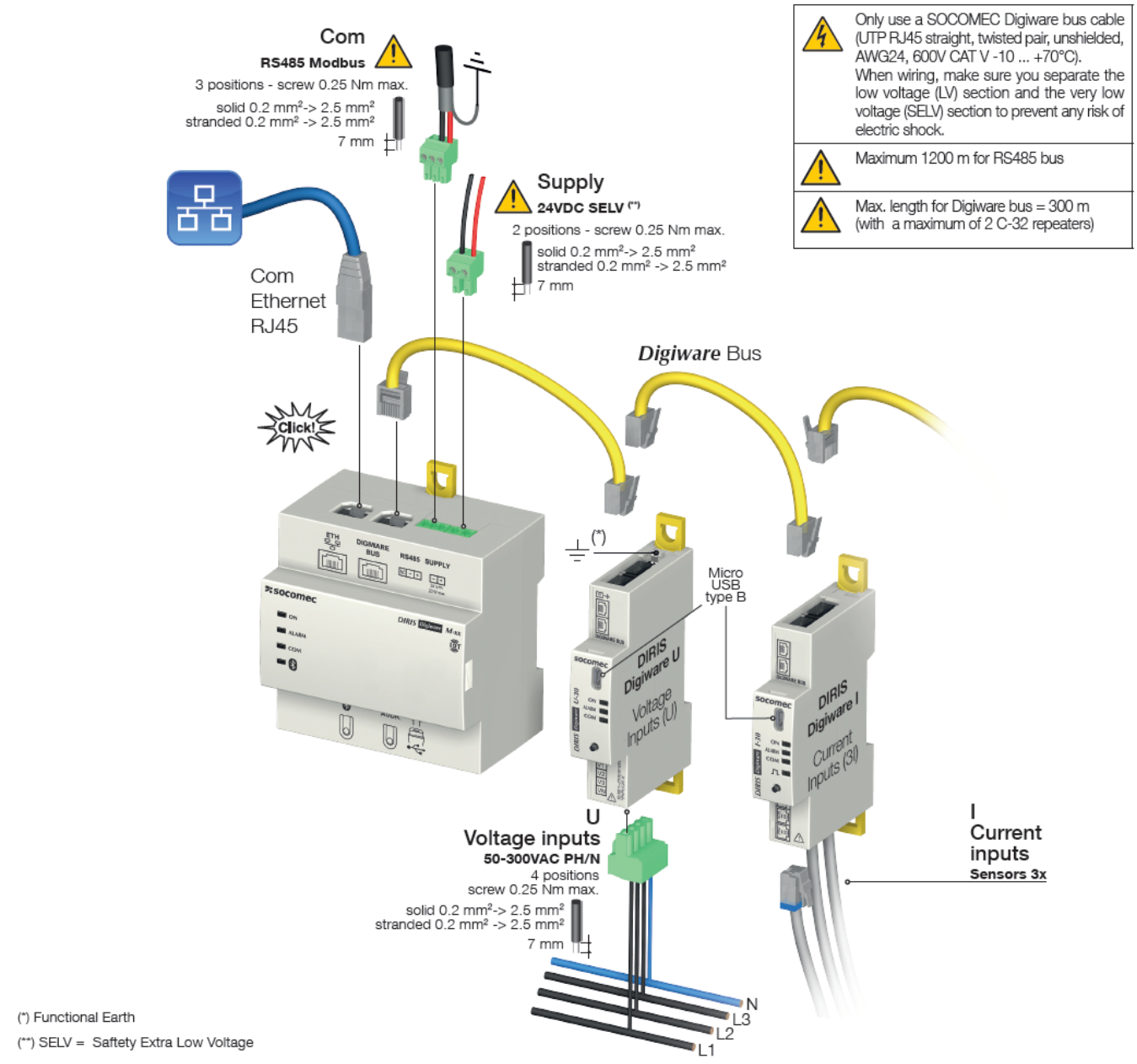
The DIRIS Digiware M/D gateways come with firmware natively compatible with AWS connectivity. No need to compile source code or libraries, as configuration is easily done through the integrated web server.

5 - Set up your hardware

Prior connecting your gateway to AWS, you will need to install the gateway in your installation. Following resources will help you in this task:

- User manual of your device, which can be found at socomec.com

Before enabling the AWS platform in your gateway, make sure all devices are properly connected and configured. You can verify this using the diagnostic page of the integrated web server.



6 - Setup your AWS account and Permissions

Refer to the instructions at Set up your AWS Account. Follow the steps outlined in these sections to create your account and a user and get started:

- Sign up for an AWS account
- Create an user and grant permissions.
- Open the AWS IoT console

7 - Connect your gateway

In order to connect your gateway to AWS, you will have to configure the AWS connection using the embedded webserver "Webview".

Please refer to the product datasheet in order to configure your "Cybersecurity" Webview account.

There are 3 ways to provision certificates in your gateway.

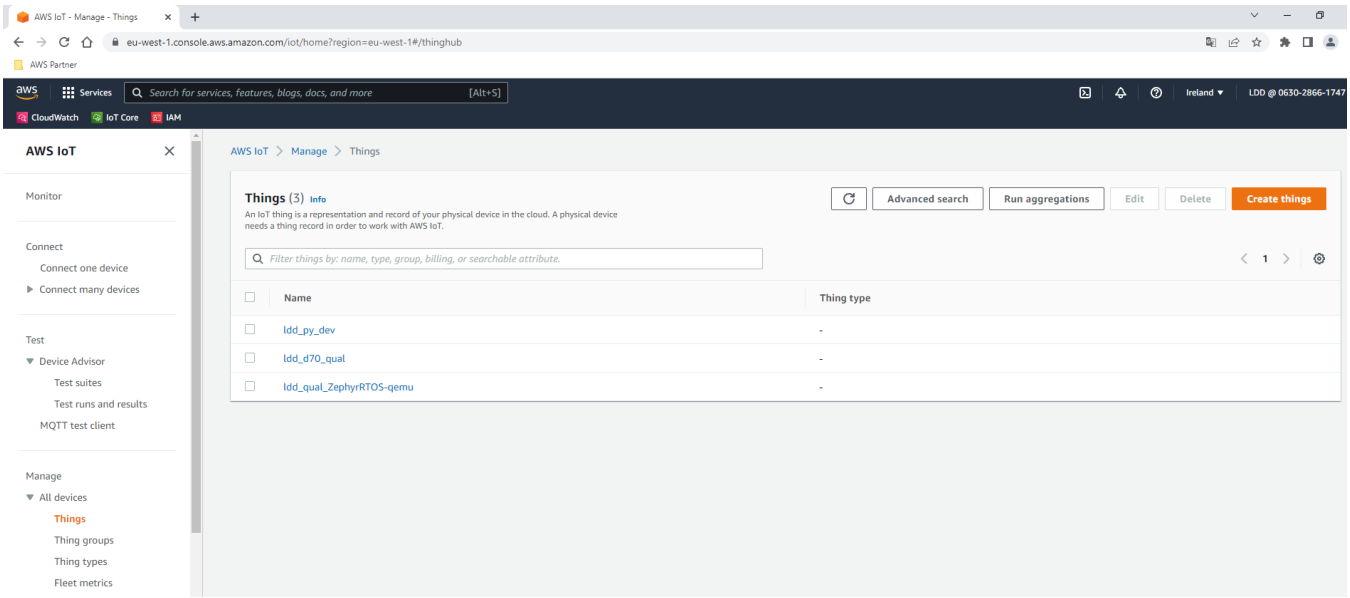
- Allow AWS to generate a private key and a public certificate, then upload these credentials to the gateway (recommended and described below).
- Allow the gateway to generate a private key and a public certificate, then download the public certificate and upload it to AWS when creating your *Thing*.
- Download a generated CSR from the gateway, sign it using AWS CA, and upload the public certificate back to the device. This method has the advantage of keeping the private key protected by not exposing it.

The CSR method also allows you to use a custom CA instead of the default AWS CA. This custom CA should be registered in AWS IoT Core (refer to this guide). To provision your gateway, download the CSR generated by the gateway, sign the certificate, and upload this certificate back to the gateway. This method offers two advantages:

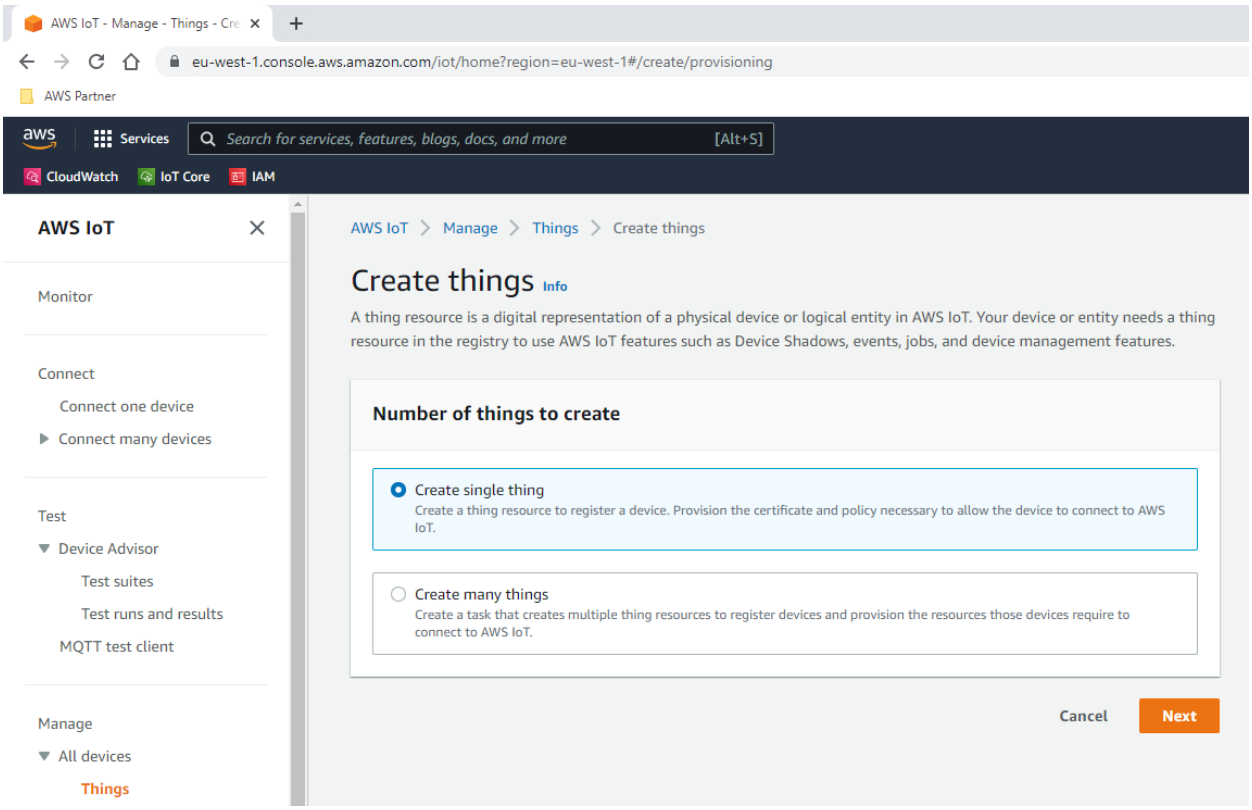
  - The private key remains protected in the gateway's persistent storage and is never exposed
  - Using a CA with AWS enables Just In Time Provisioning (JITP), which eliminates the need to manually create your Thing.

Follow the steps outlined in these sections to provision resources for your device, or you can also refer to the official documentation at Create AWS IoT Resources.

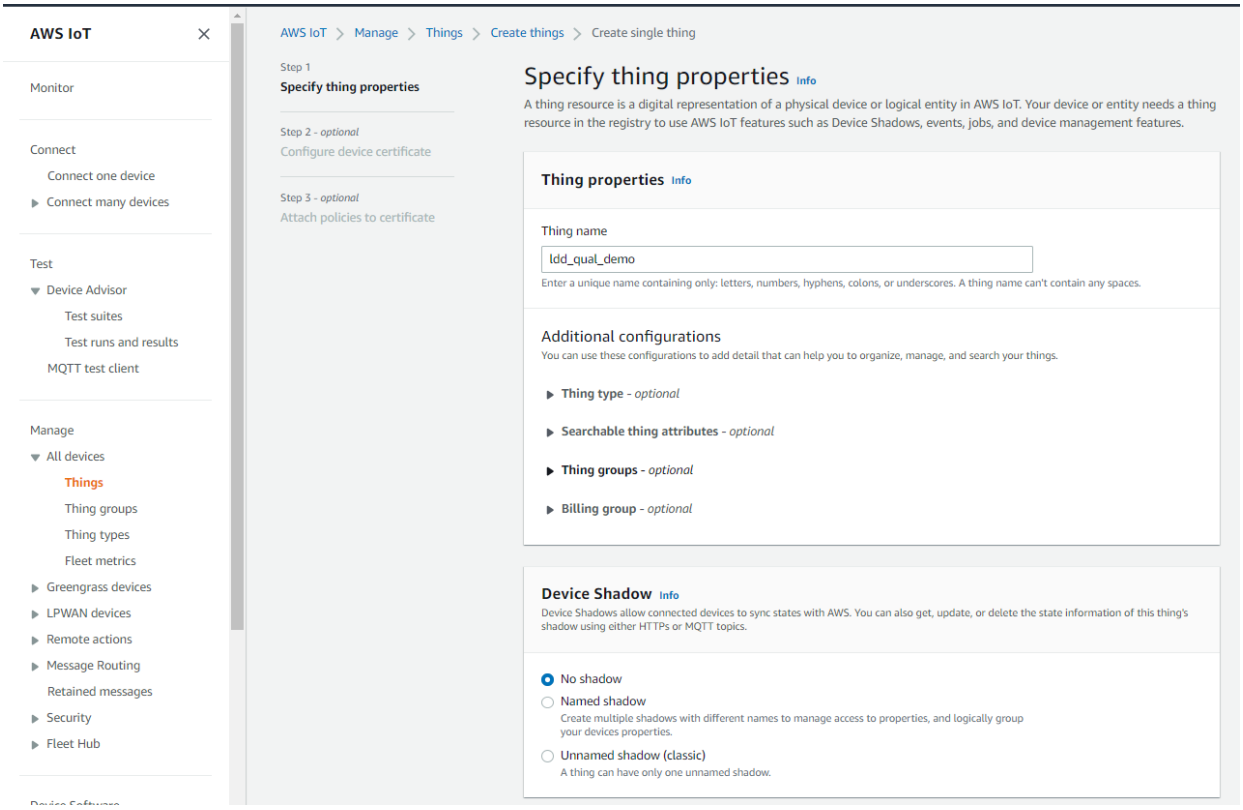
1. Select *Thing* tab
2. Click "Create *Things*"



3. Select "Create single *Thing*"

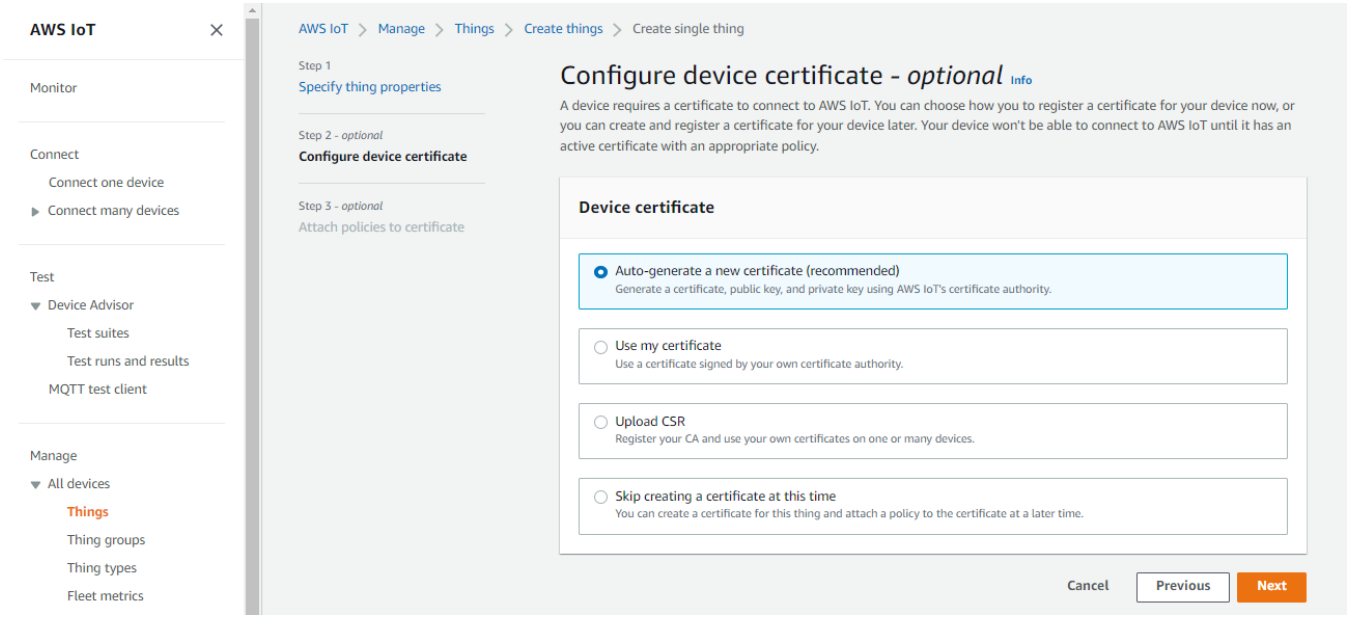


4. Choose the *Thing* name, this name cannot be change and will identify the *Thing*.



5. Select "Auto-generate a new certificate (recommended)". Other possibilities to select a certificate are discussed bellow.

> This step differ depending on the method you choose to provision your gateway



6. Click on "Create policy" and choose a name for the policy

Create a tailored, minimal policy that perfectly meets the Thing's requirements (connect and publish/subscribe to specific topics).

The policy should match the topics the gateway operates on. An incorrect policy may prevent the gateway from connecting to the broker or from publishing/ subscribing.

It is recommended to use the following policy document:

- In "policy document" section click "JSON"
- Paste the following policy document (JSON format)
- Change the region "eu-west-1" with your current AWS region
- Change the account ID "000000000000" with your current account ID

Gateway policy document

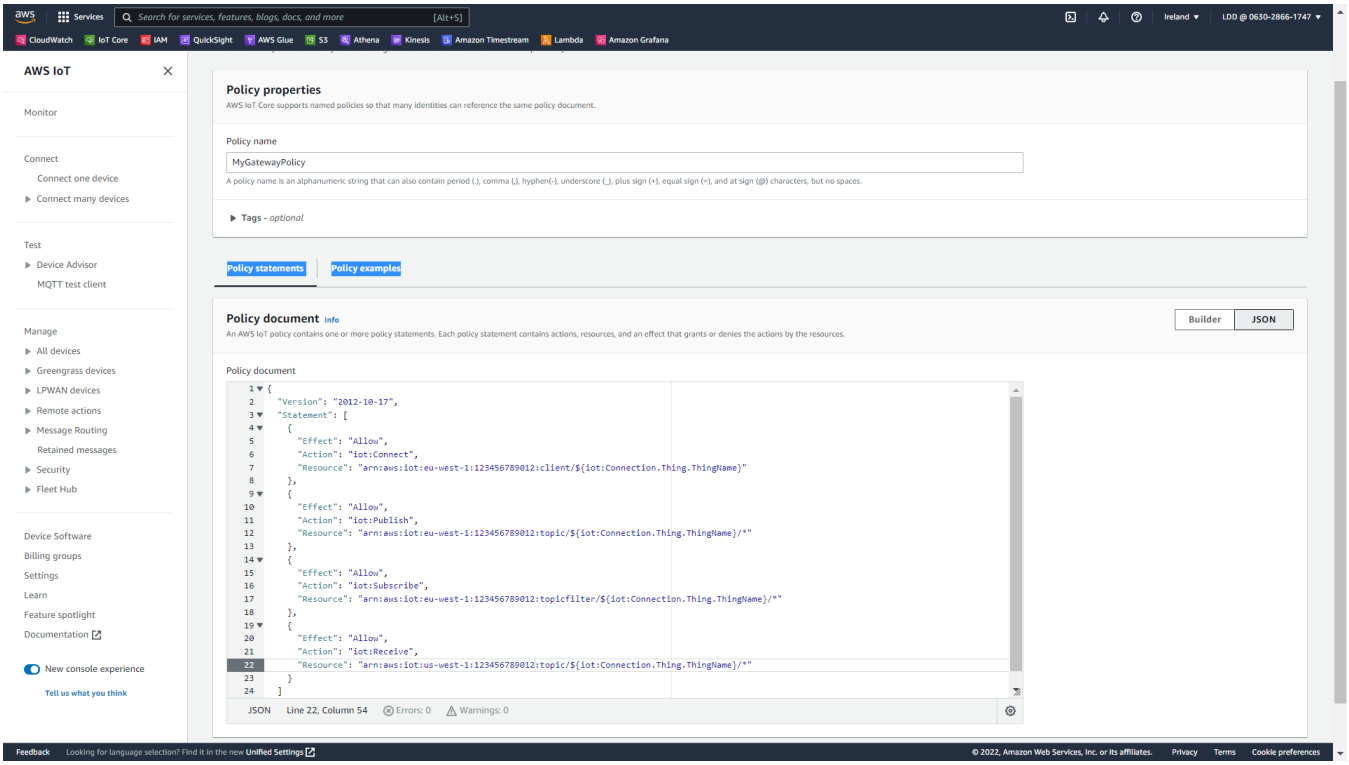
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "iot:Connect",
            "Resource": "arn:aws:iot:eu-west-1:000000000000:client/${iot:Connection.Thing.ThingName}"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iot:Publish",
                "iot:Receive"
            ],
            "Resource": "arn:aws:iot:eu-west-1:000000000000:topic/${iot:Connection.Thing.ThingName}/*"
        },
        {
            "Effect": "Allow",
            "Action": "iot:Subscribe",
            "Resource": "arn:aws:iot:eu-west-1:000000000000:topicfilter/${iot:Connection.Thing.ThingName}/*"
        }
    ]
}
```

This minimal policy enables the *Thing* to:

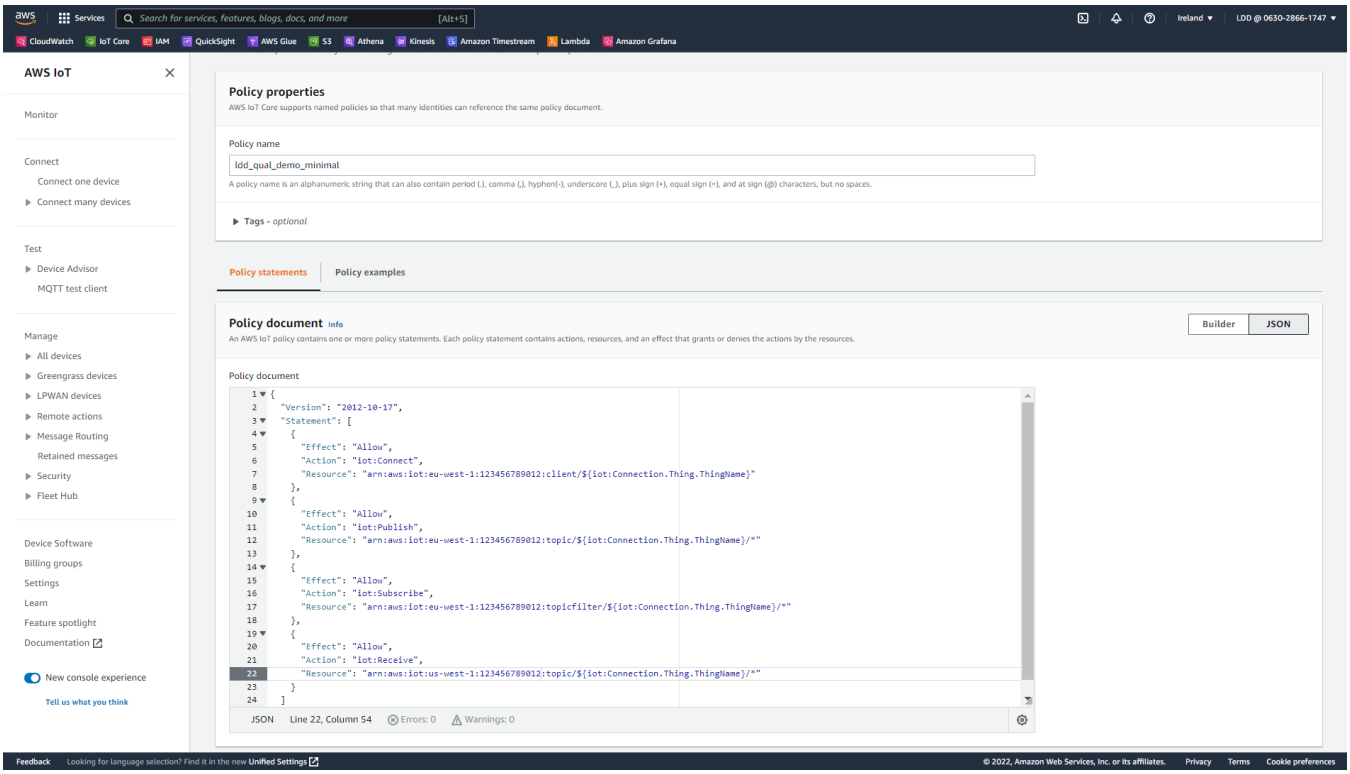
- Connect to the broker
- Publish to topics matching the pattern "{ThingName}/*"

- Subscribe to topics matching the pattern "{ThingName}/*"
- Receive published messages on subscribed topics matching the pattern "{ThingName}/*"

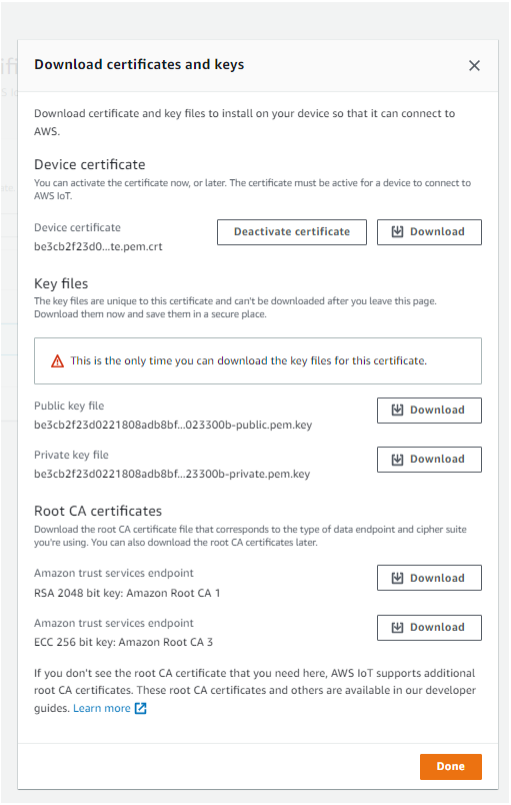
> **NOTE**
>
> The examples in this document are intended only for development environments. All devices in your production fleet must have credentials with privileges that authorize only intended actions on specific resources. The specific permission policies can vary for your use case. Identify the permission policies that best meet your business and security requirements. For more information, refer to Example policies (https://docs.aws.amazon.com/iot/latest/developerguide/example-iot-policies.html) and Security Best practices (https://docs.aws.amazon.com/iot/latest/developerguide/security-best-practices.html).



7. Select the newly created policy for your certificate and click "Create thing".



8. Download your *Thing* private key and certificate.

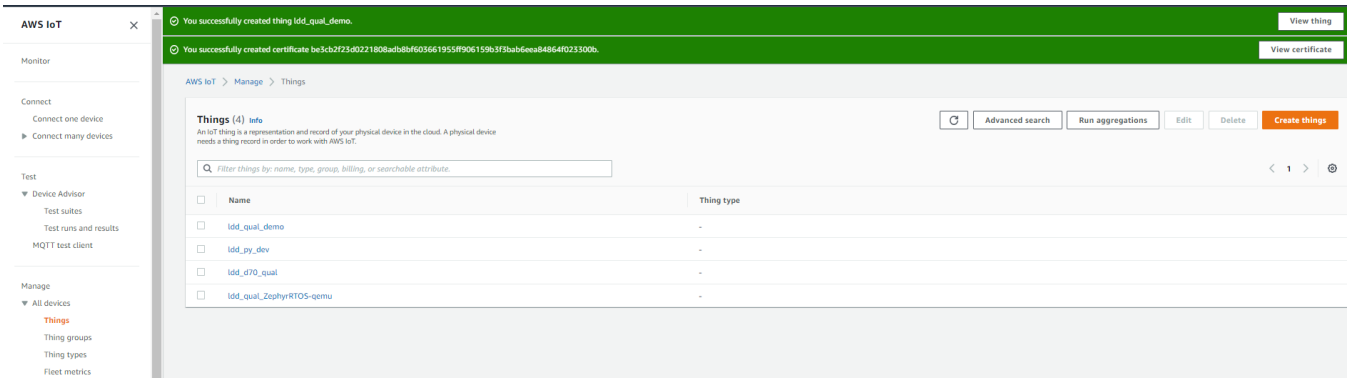


This page is your only chance to download the private key file for your certificate.

You don't need to manually upload the AWS CA certificate as it is already embedded.

9. Click "done".

At this point you have created the *Thing* and attached to it a certificate. You will find your *Thing* in the list :

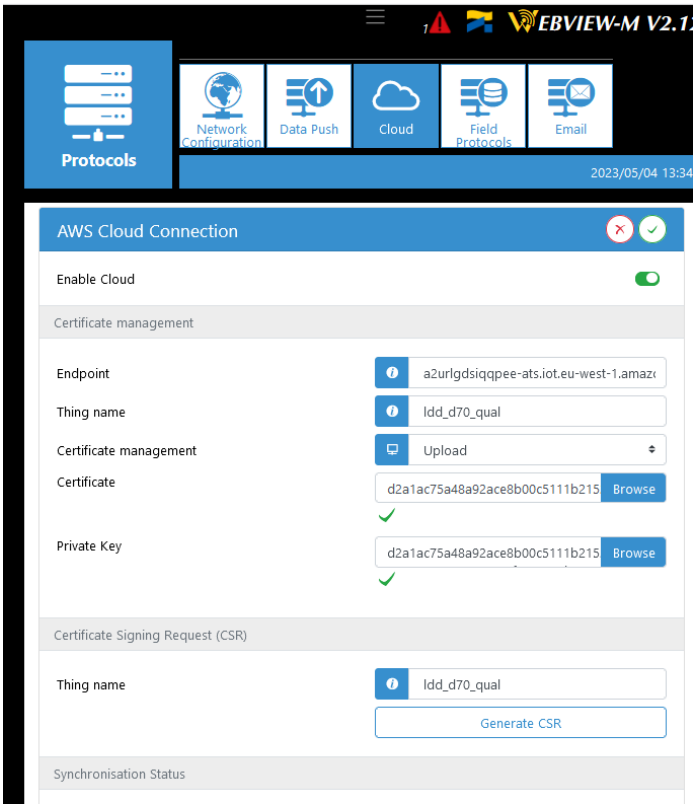


8 - Provision your gateway

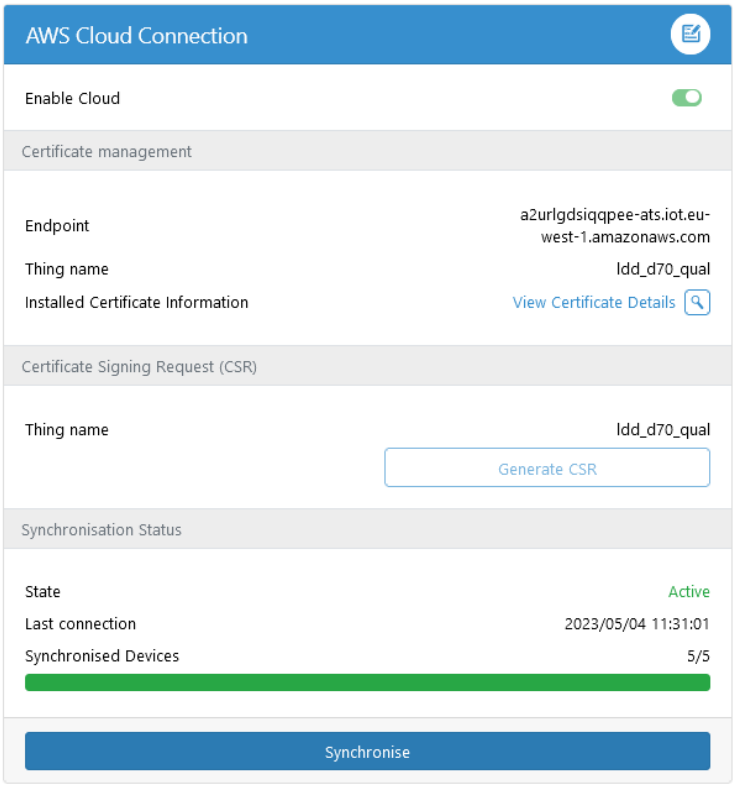
Once you have a Webview account with necessary privilege and you created the *Thing* and you downloaded the device public certificate and private key. You will need to provision the gateway with these credentials.

To do so, you will need to:

- Connect to Webview application with either Admin or Cyber account.
- Navigate to "Protocol" section, "Cloud" tab
- Enable AWS IoT Core cloud platform
- Fill following information in the form:
    - AWS Endpoint (Endpoint can be found in AWS IoT Core > Settings page)
    - *Thing* name
    - Select "Upload method" in the list
        - Upload the x509 certificate generated by AWS
        - Upload the private key generated by AWS
- Validate your changes



- Click synchronize



After few seconds, the gateway should connects to AWS and synchronize devices. You should be able to see uplinked MQTT messages in the AWS MQTT Test Client.

```
{
  "name": "Atys P",
  "productId": 2300,
  "netId": "29E021",
  "serialNumber": "99999999999",
  "uuid": "bb9b5f10-4215-11cc-9ac5-393939393939"
}
```

> Additional provisioning methods involving x509 certificates are described in the annex.

You should be able to view the JSON payloads pushed by the gateway in the *MQTT* test client when subscribing to the topic starting with your *Thing Name*.

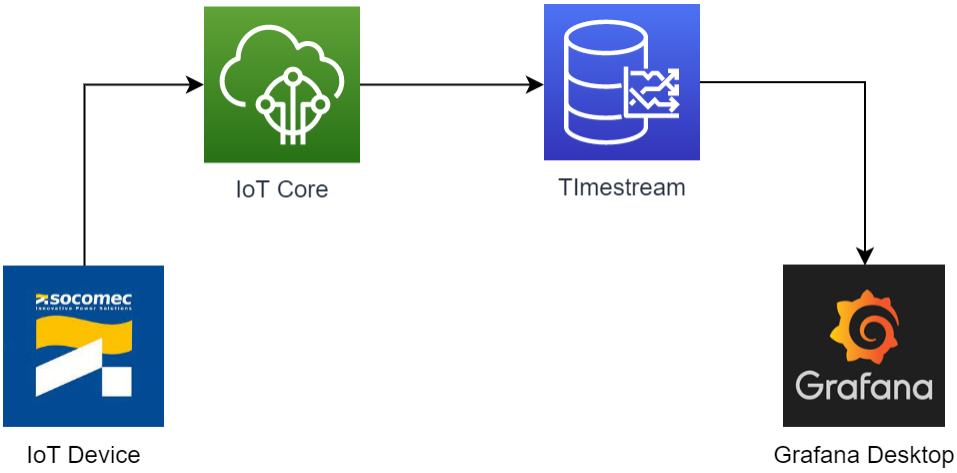
Congratulations, you have successfully connected your gateway to AWS IoT Core, and you can now process pushed data as needed.

> The Socomec's gateway send the message in JSON format. The complete description is available in the annex bellow.

9 - Exploit your Socomec data

Once IoT Core receives the data published by the gateway you might want to exploit them.

To do this, we will present a simple and straightforward architecture for storing the data in a timeseries database (Timestream) and displaying it in Grafana:

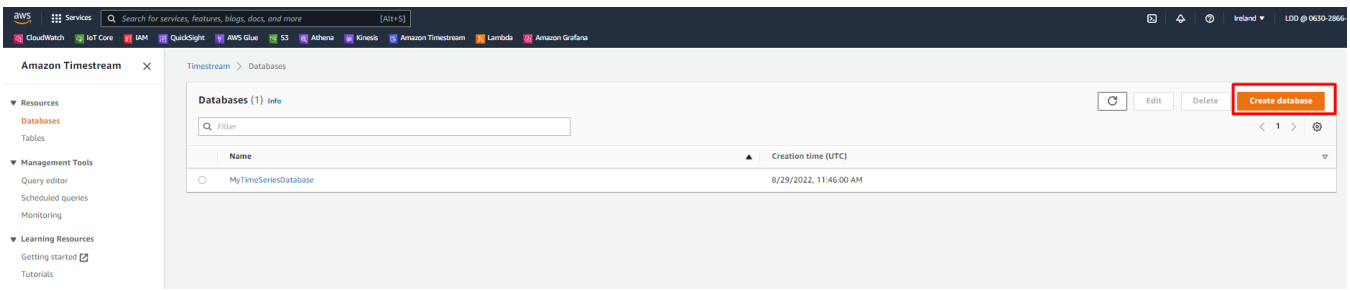


a. Create the AWS Timestream database and table

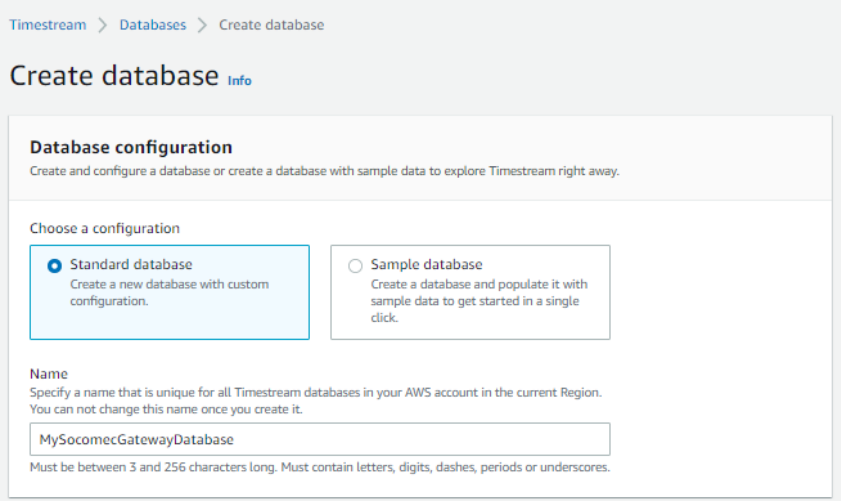
General documentation about Timestream is available here: What is Amazon Timestream?

To create a Timestream database:

- Select your region
- Go to the Timestream service console
- Click "Create database"

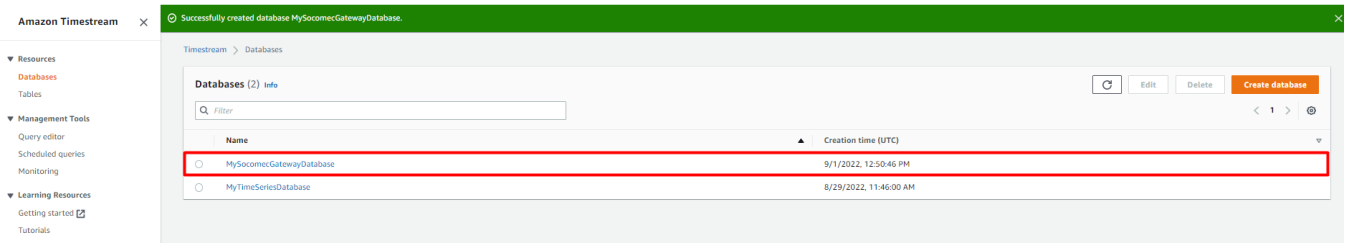


- Select "Standard database"
- Choose a name for your database



- Keep the rest of the configuration unchanged
- Click "Create database"

Your created database should appear in the list:

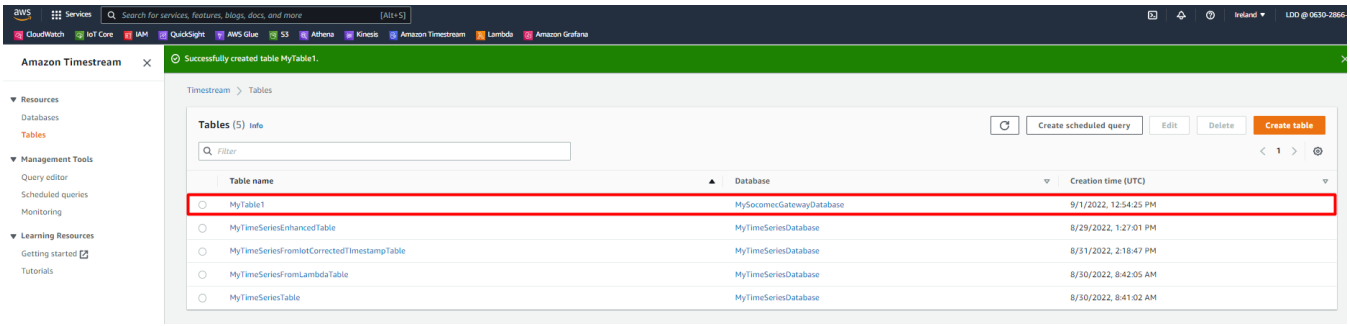


Now we will create a table in this database:

- Go to "Tables" panel
- Click "Create Table"
- Choose from the databases list the one previously created
- Choose a name for your table
- Configure data retention, I will choose
    - 1 Day of "Memory store retention"
    - 1 Week of "Magnetic store retention"

- Keep the rest of the configuration unchanged
- Finally click "Create table"

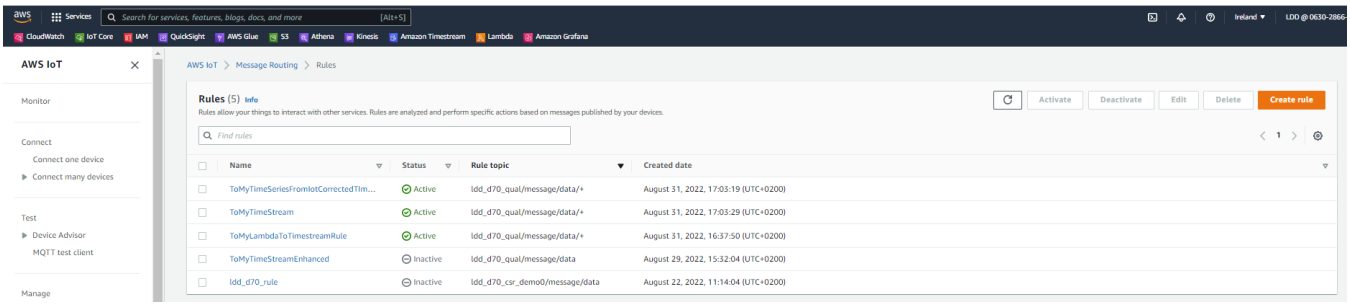
Your table should appear in the list of tables



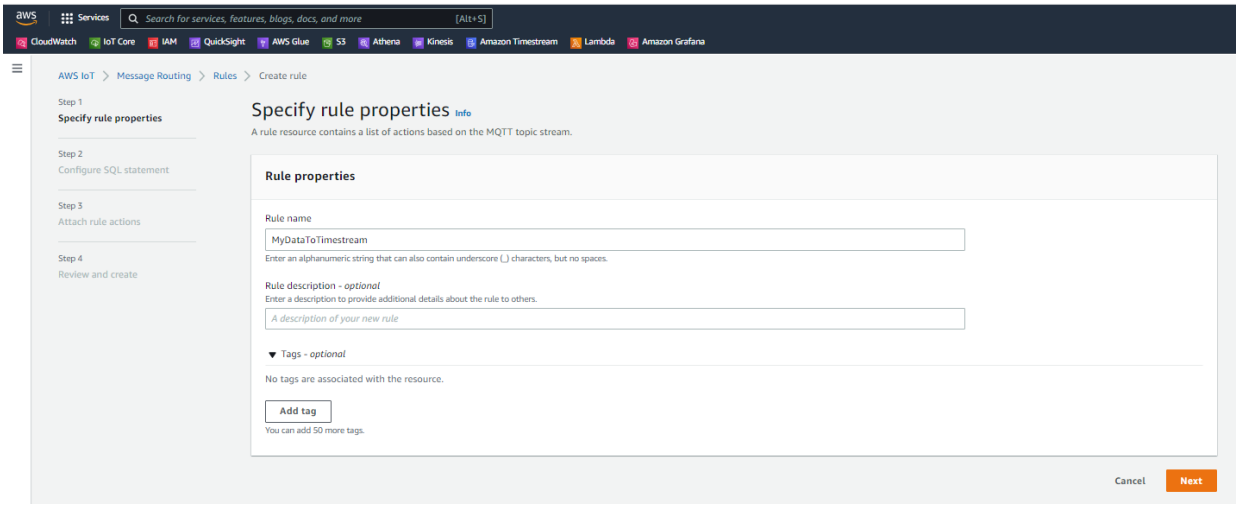
b. Forward your data from IoT Core to the Timestream database

Now we will create a IoT Core rule to forward data collected by IoT Core to the Timestream database, documented here: Working with other services : AWS IoT Core

- Go to IoT Core
- Go to "Message Routing > Rules" panel
- Click "Create rule"



- Choose a name for your rule
- Click "Next"



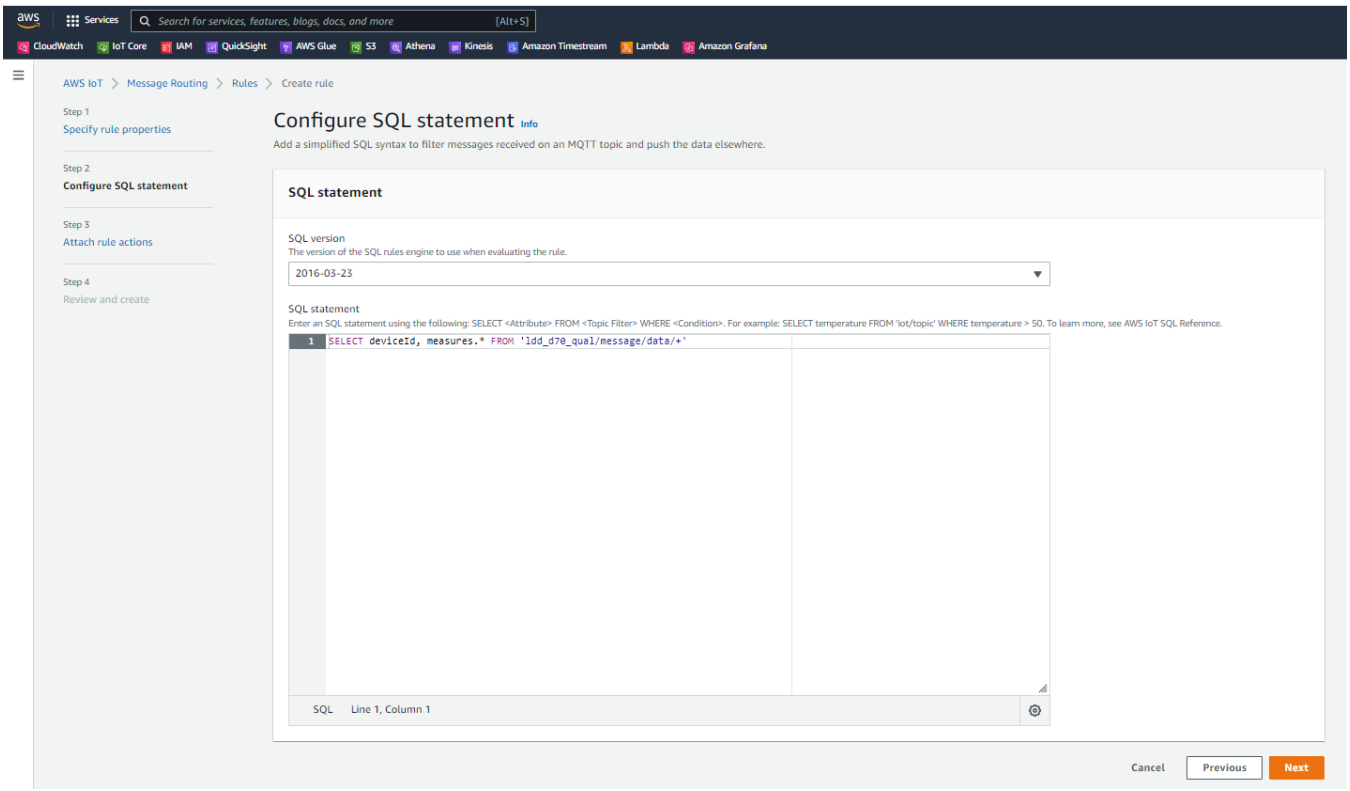
- Select SQL version "2015-10-08"

> The reason why using an older version of SQL, is because with SQL version "2016-03-23", fractional part of float numbers is wiped out if equals 0. Whereas with the older version, it is kept. This fractional part is required for inserting the measure into the proper (double/bigint) column in the table.

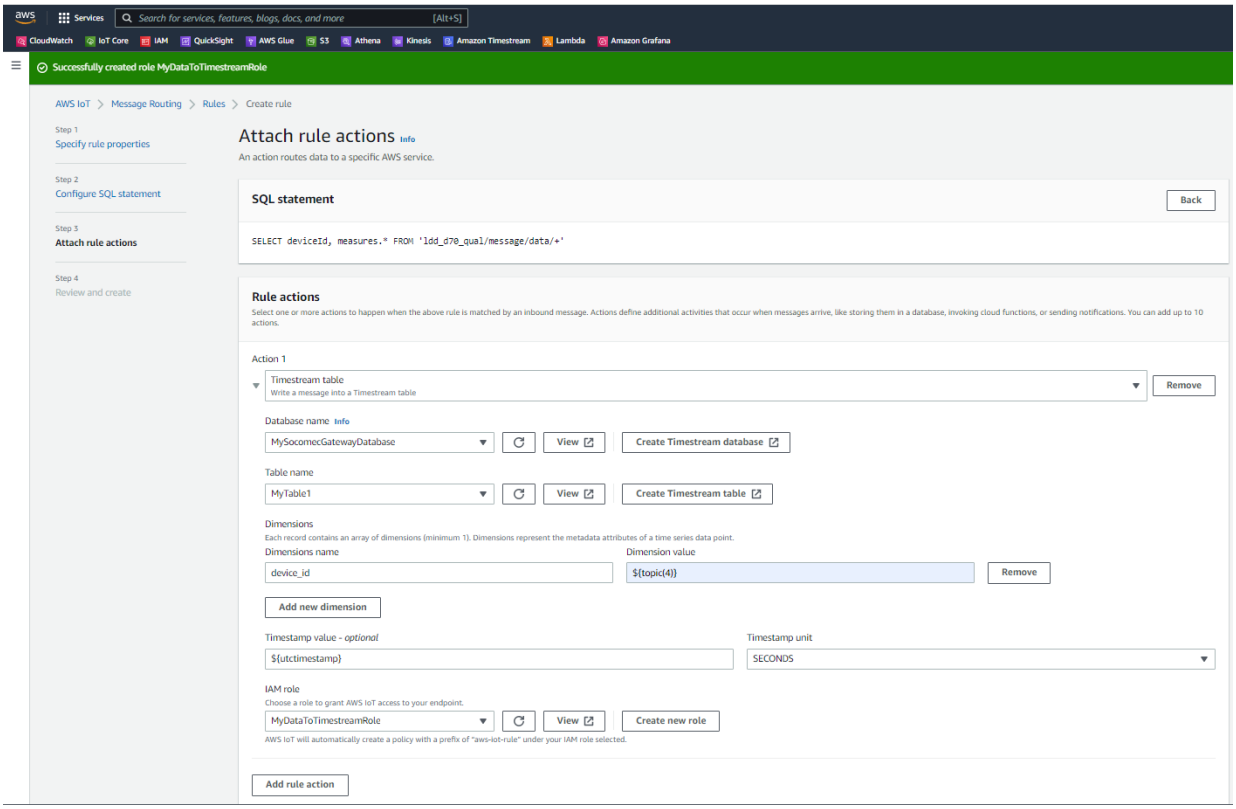
- Copy the following SQL statement

```
SELECT measures.* FROM 'ldd_d70_qual/message/data/+'
```

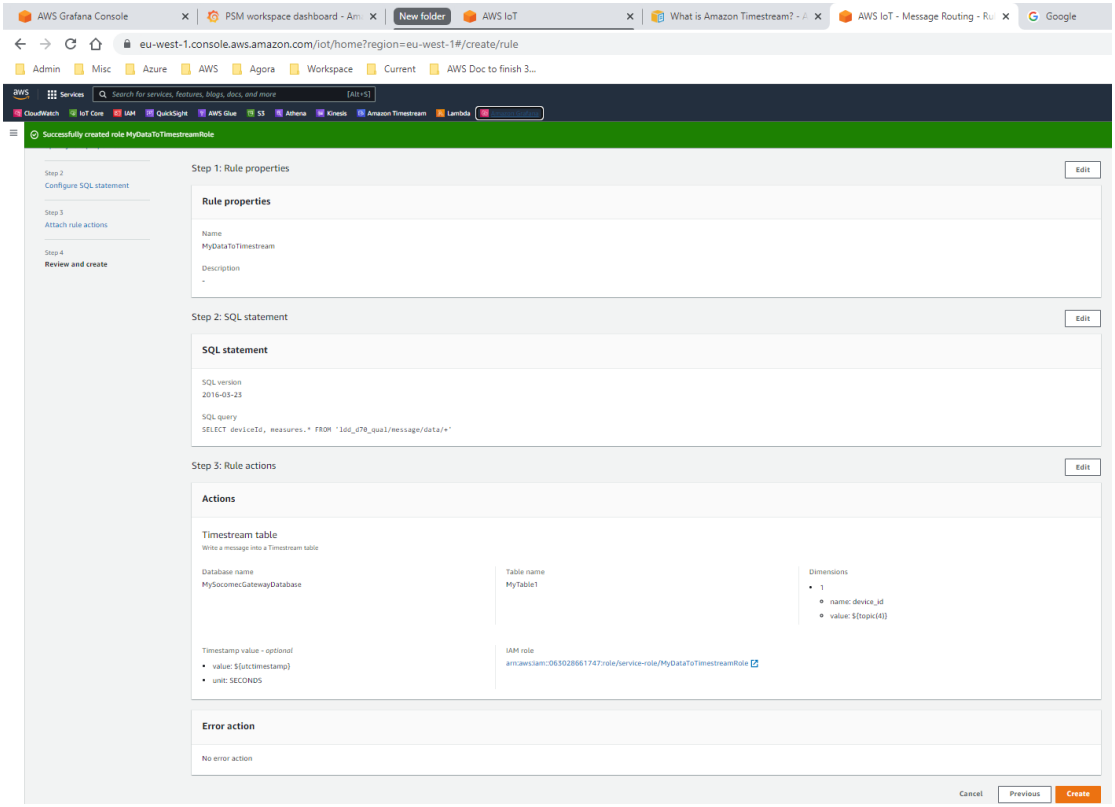
- Click Next



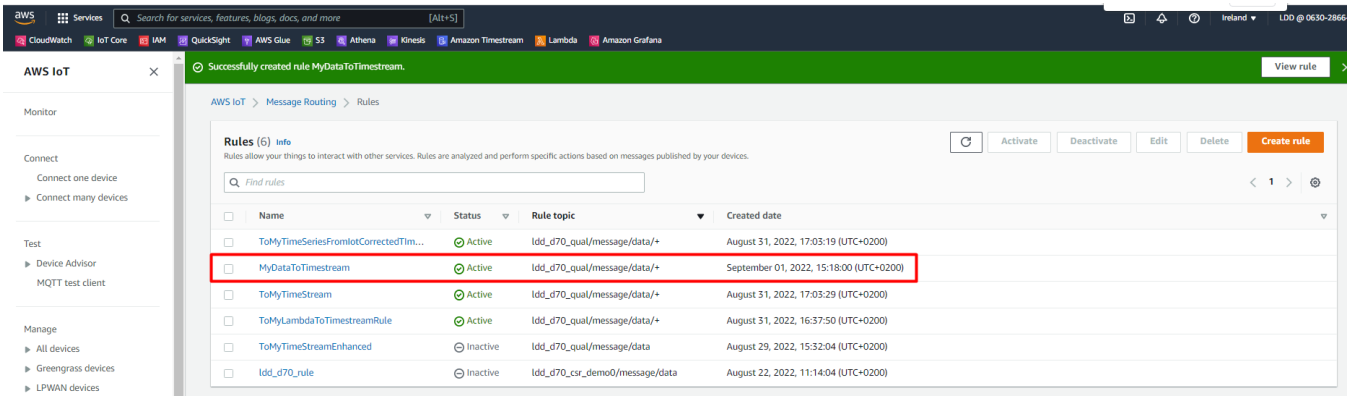
- Select "Timestream table "as Action 1
- Select your Timestream database from the list
- Select your Timestream table from the list
- Add a first dimension, with following configuration
    - Dimension name: "device_id"
    - Dimension value "${topic(4)}"
- Configure the timestamp source
    - Timestamp value: "${utctimestamp}"
    - Select "SECONDS" as timestamp unit
- Configure the IAM role:
    - Click "Create new role"
    - Choose a name for your role
    - Click "Create"



- Keep the rest of the configuration unchanged and click "Next
- Review your rule configuration
- Then click "Create"



Your rule should be listed in the following table:



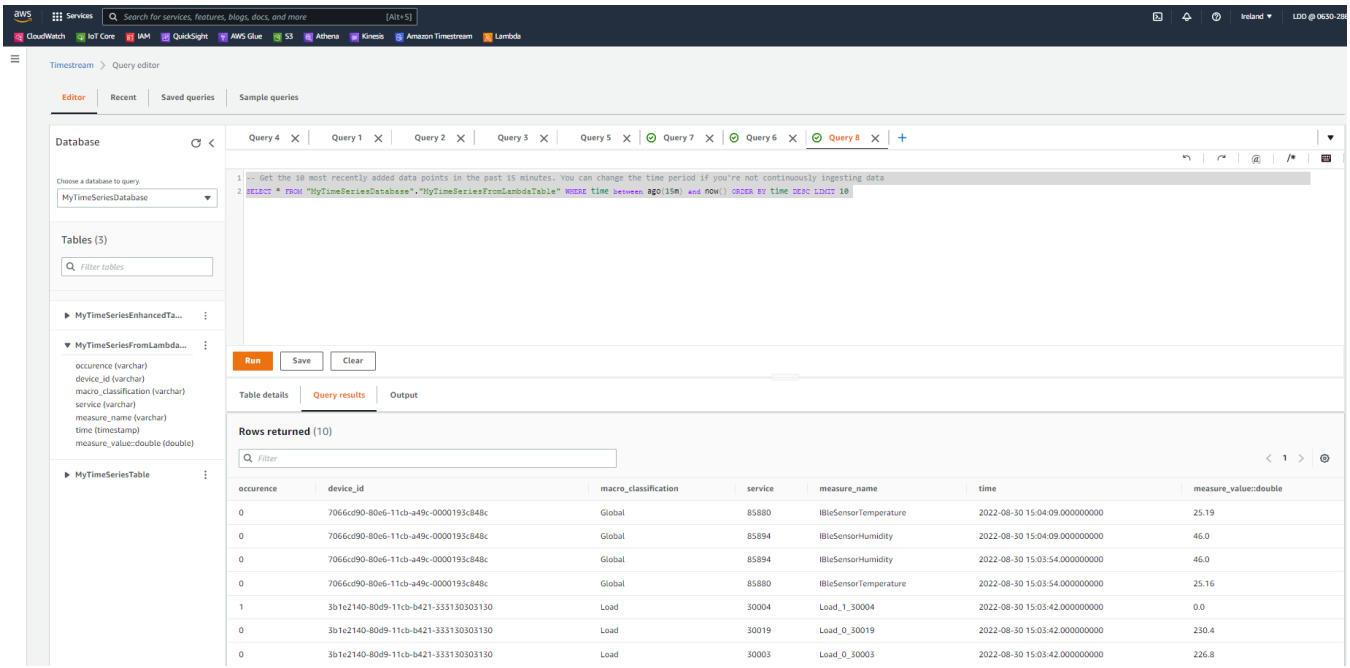
c. Check your configuration

Once your create the Timestream table and the IoT Core rule. If your gateway is connected to AWS, you should see your table being filled with the data.

Go to the Timestream Query editor

- Select your database
- Select your Table
- Click the three dots
- Click "Preview data"
- Run query

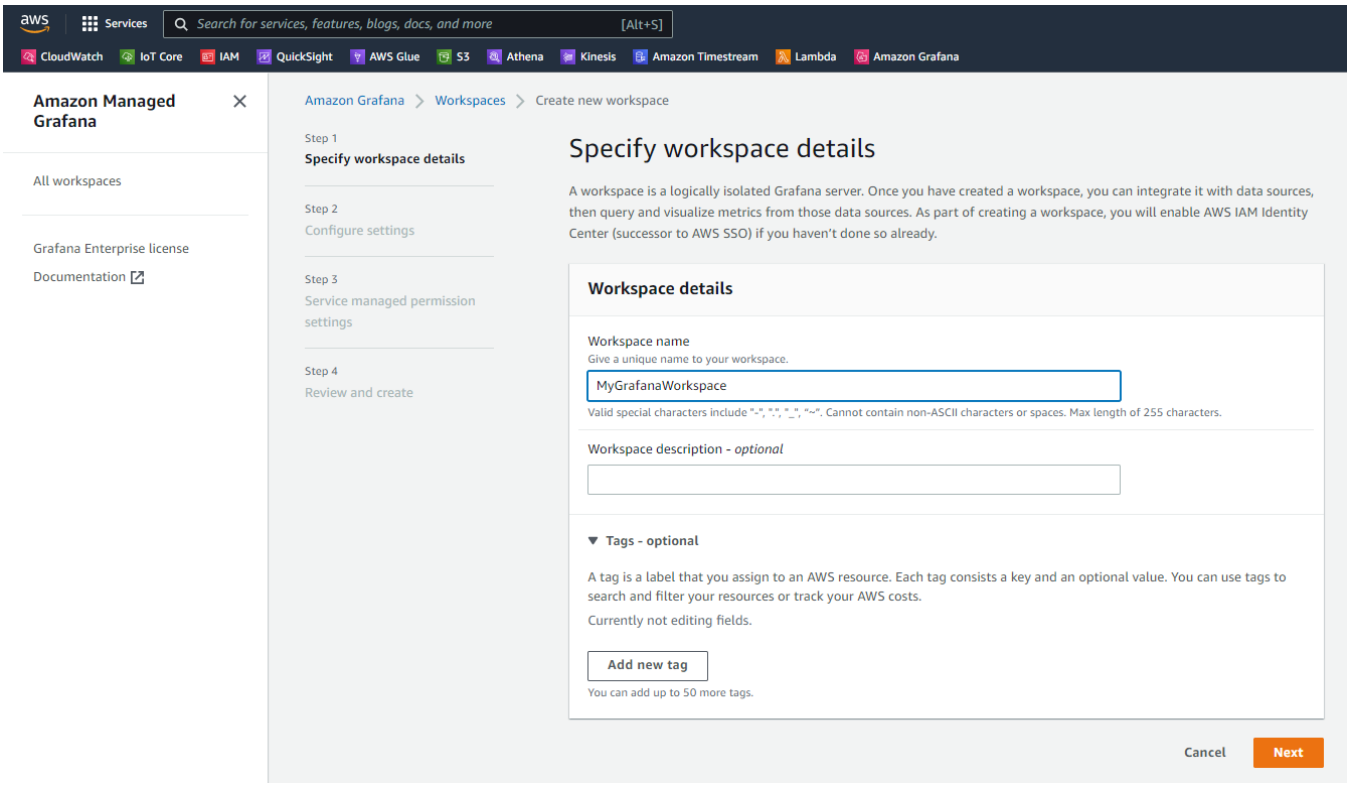
You should get something like this:



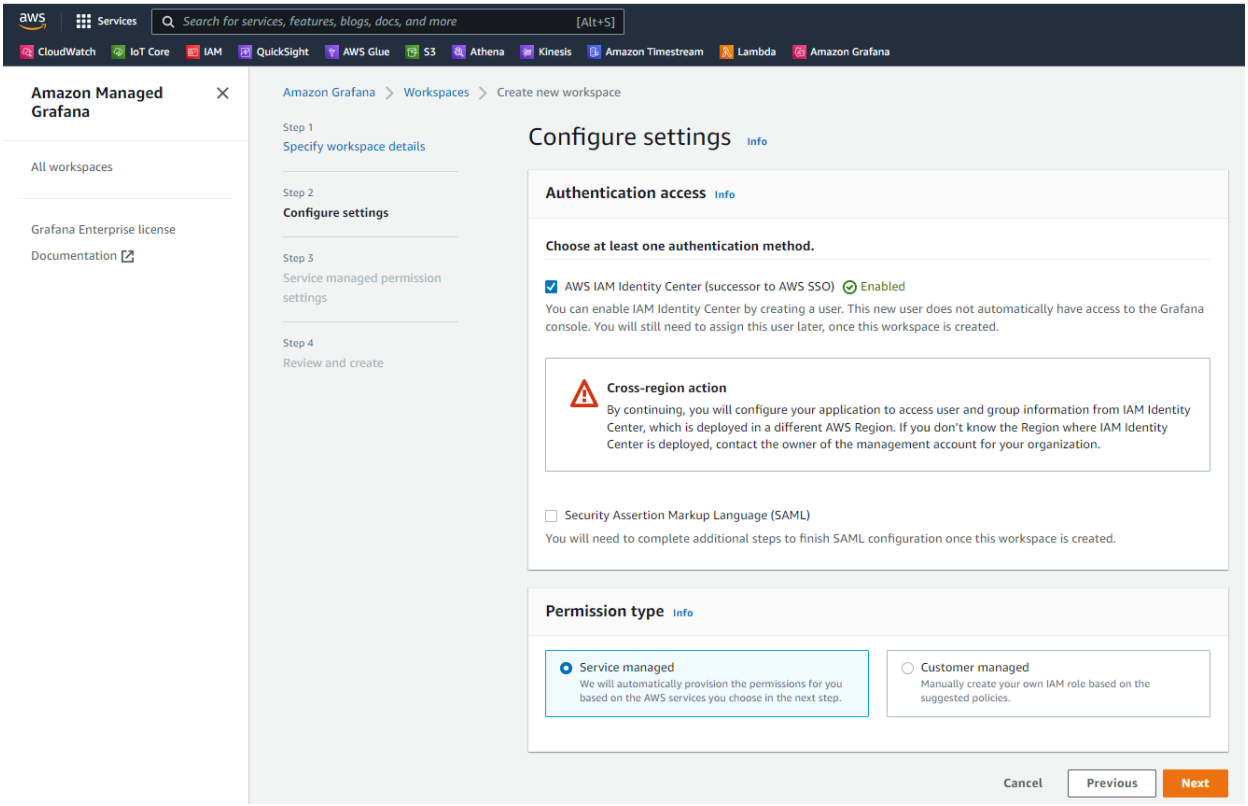
d. Install Grafana (hosted)

In the following steps, we will use AWS Amazon Grafana service, which is a simple and convenient way to create dashboards accessible worldwide. But you are free to use the desktop version of Grafana or another dashboard tool .

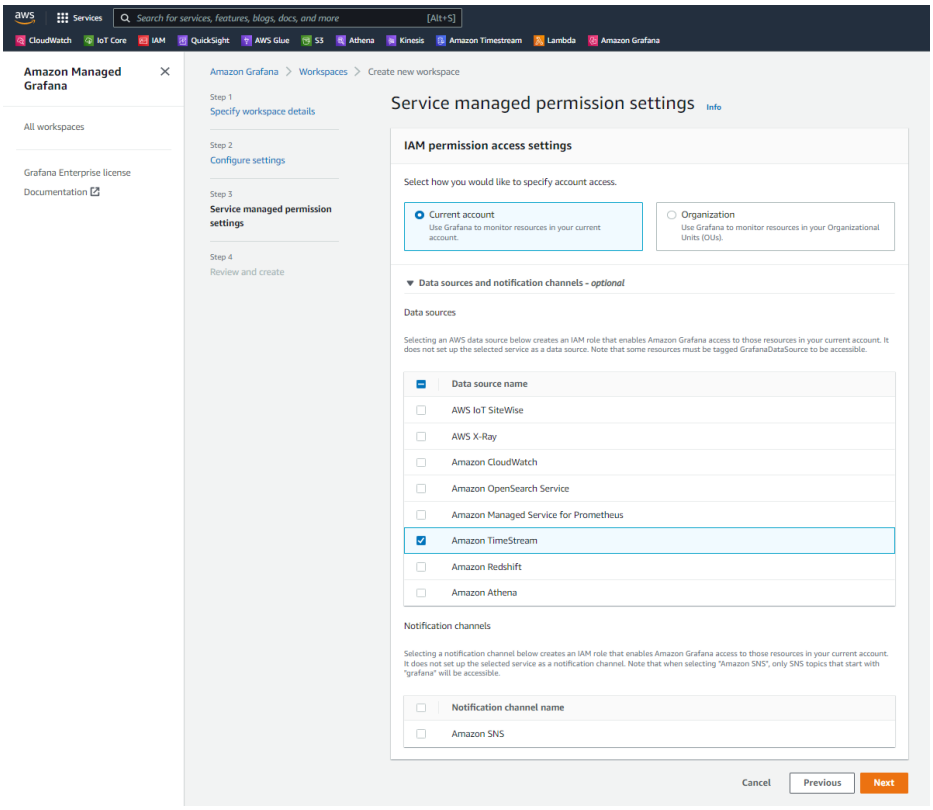
- Goto to AWS Grafana Console
- Click "Create Workspace"
- Choose a name
- Click "Next"



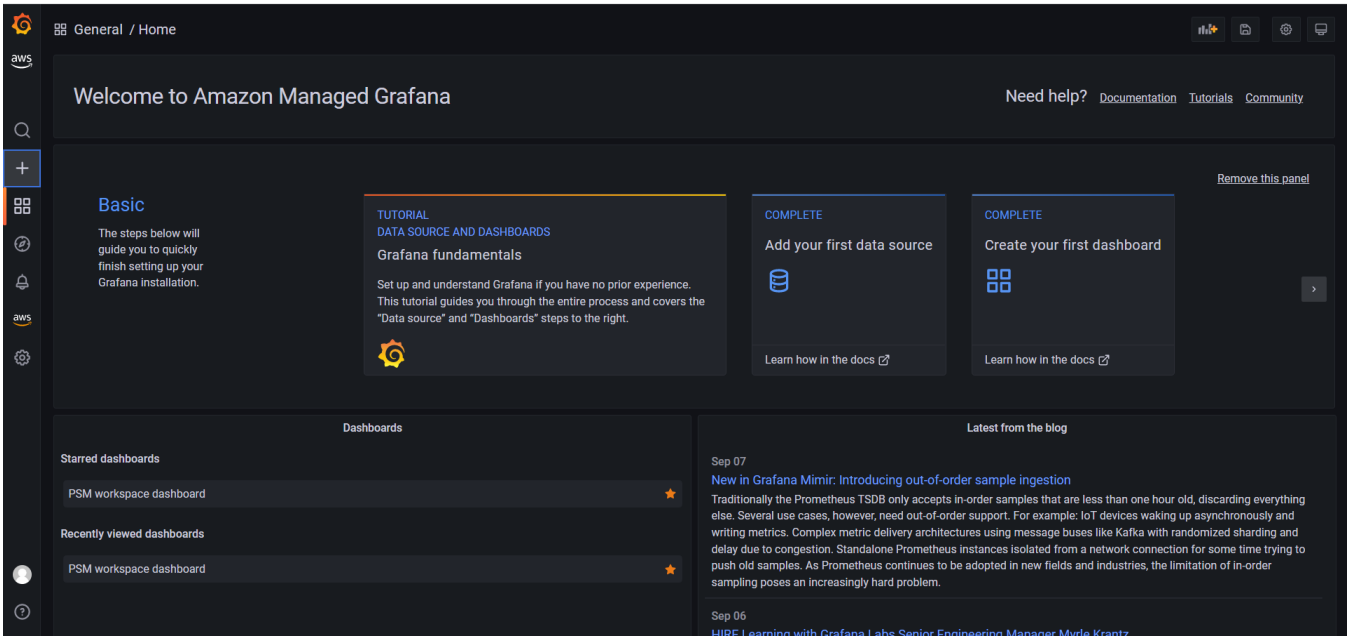
- Choose the authentication access, we will use "AWS IAM Identity Center (successor to AWS SSO)"



- Select your account
- Select a single or multiple data source name(s)
- Click next



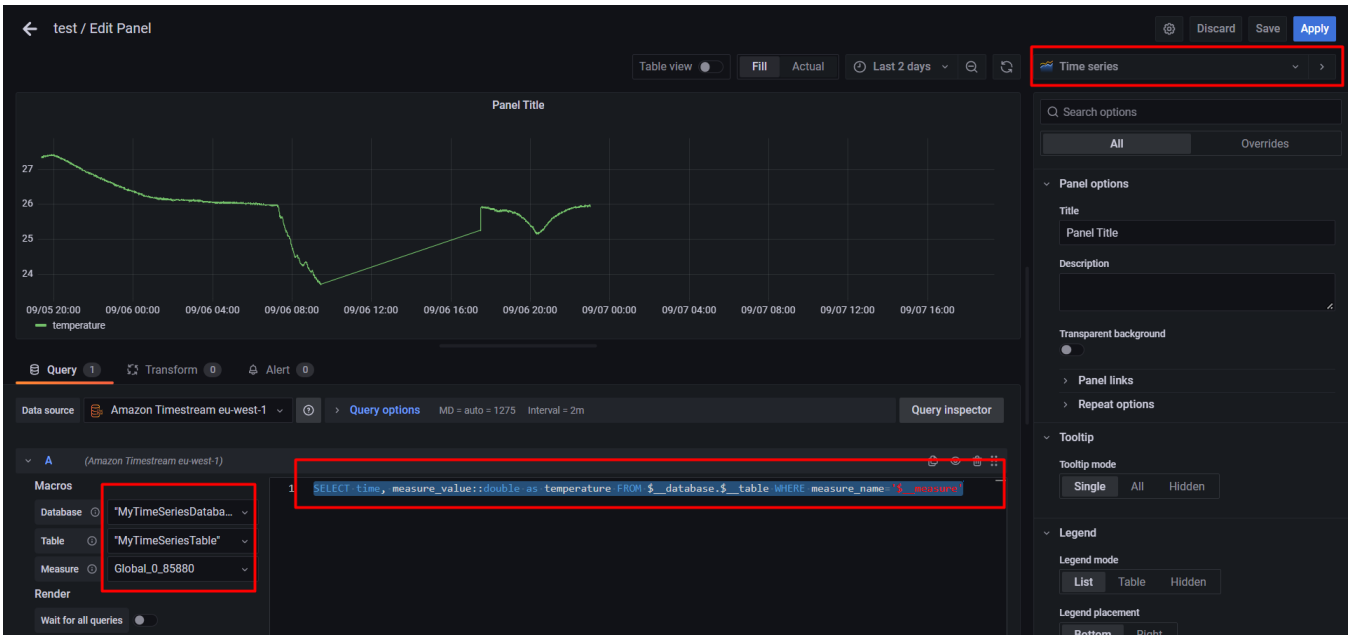
- Review your Grafana workspace
- Then click "Create"
- You workspace should have in the home list
- From there click on the Grafana workspace URL
- You will have to sign in



- Once you have access to the Grafana dashboard, click on the plus "+" symbol, then "Create a dashboard"
- Click "Add panel"
- Select time series
- Copy the following SQL request

```
SELECT time, measure_value::double as temperature FROM $__database.$__table WHERE measure_name='$__measure'
```

- Select your AWS Timestream data source
- Select the database
- Select the table
- Select the measure



- Click Apply
- Exit and save your dashboard

Grafana SQL commands samples

- Data source: "Amazon Timestream"
- Select your database and table for "$__database" and "$__table".

Plot temperature for all BLE temperature sensors found

Select measure ("$__measure") : "Global_0_85880":

```
SELECT device_id, CREATE_TIME_SERIES(time, measure_value::double) as temperature
FROM $__database.$__table
WHERE $__timeFilter AND measure_name='$__measure'
GROUP BY device_id
ORDER BY device_id
```

Plot distribution of received messages count per device

```
SELECT device_id, COUNT(*) as message_counts
FROM $__database.$__table
WHERE $__timeFilter
GROUP BY device_id
ORDER BY device_id
```

Plot BLE magnetic sensor counter value:

Select measure "Global_0_85895":

```
SELECT time, measure_value::bigint
FROM $__database.$__table
WHERE measure_name='$__measure' AND $__timeFilter
```

Plot measured voltage 1 from U30 device:

Select measure "Global_0_110228"

```
SELECT device_id, CREATE_TIME_SERIES(time, measure_value::double) as "V1"
FROM $__database.$__table
WHERE $__timeFilter
AND measure_name='$__measure'
AND $__timeFilter
GROUP BY device_id
ORDER BY device_id
```

10 - Troubleshooting

- If you're experiencing any issues or need further assistance, reach us at https://www.socomec.co.uk/en-gb/technical-support.
- AWS Policy: More documentation about Policies at AWS IoT Core policies
- Certificates: More information about x509 certificate at https://docs.aws.amazon.com/iot/latest/developerguide/x509-client-certs.html

Annex

1 - Dashboard demo

2 - Socomec data types description

Socomec data (called "*service*") are labelled depending on their multiplicity and type. Following table describe all services that are send to AWS.

Devices which uses a given service are listed in the "products" column. If a *service* is not related to specific product, the cell is empty.

Service	Products	Unit	Name / Description
Global_0_5204	ATS Loose controller ATyS C65 IEC [2402] Atys p [2300]	-	Alarm/Fault Code
Global_0_9000		-	ILoadAvgMeasurementCplx

Global_0_9001		-	ILoadEnergyMeasurementCplx
Load_0_10179 Load_1_10179 Load_2_10179	Diris Digiware I-35 DC [4118]	A	IDCIrmsAvg IDCIrmsAvg IDCIrmsAvg
Load_0_10180 Load_1_10180 Load_2_10180	Diris Digiware I-35 DC [4118]	A	IDCIdcAvg IDCIdcAvg IDCIdcAvg
Load_0_10181 Load_1_10181 Load_2_10181	Diris Digiware I-35 DC [4118]	A	IDCIacAvg IDCIacAvg IDCIacAvg
Load_0_10220 Load_1_10220 Load_2_10220	DIRIS PMD US Medium level RJ12 [50] DIRIS PMD US Medium level 333mV [51]	-	Crest factor : I1 Crest factor : I1 Crest factor : I1
Load_0_10221 Load_1_10221 Load_2_10221	DIRIS PMD US Medium level RJ12 [50] DIRIS PMD US Medium level 333mV [51]	-	Crest factor : I2 Crest factor : I2 Crest factor : I2
Load_0_10222 Load_1_10222 Load_2_10222	DIRIS PMD US Medium level RJ12 [50] DIRIS PMD US Medium level 333mV [51]	-	Crest factor : I3 Crest factor : I3 Crest factor : I3
Load_0_10223 Load_1_10223 Load_2_10223	DIRIS PMD US Medium level RJ12 [50] DIRIS PMD US Medium level 333mV [51]	-	Crest factor : In Crest factor : In Crest factor : In
Global_0_30276	DIRIS PMD US Medium level RJ12 [50] DIRIS PMD US Medium level 333mV [51]	-	IEnergiesTotalCplx
Global_0_45136	DIRIS PMD US Medium level RJ12 [50] DIRIS PMD US Medium level 333mV [51]	-	ILoadMetroAvgVUCplx
Global_0_45137	DIRIS PMD US Medium level RJ12 [50] DIRIS PMD US Medium level 333mV [51]	-	ILoadMetroAvgIPQSCplx
Multi_Fluid_0_65014 Multi_Fluid_1_65014 Multi_Fluid_2_65014	Diris Digiware IO-10 [4114]	-	MFF 1 Total MFF 2 Total MFF 3 Total
Multi_Fluid_0_65015 Multi_Fluid_1_65015 Multi_Fluid_2_65015	Diris Digiware IO-10 [4114]	-	MFF 1 Partial MFF 2 Partial MFF 3 Partial
Load_0_80031 Load_1_80031 Load_2_80031	Diris Digiware I-35 DC [4118]	W	P tot Load 1 P tot Load 2 P tot Load 3
Global_0_85880	Environmental sensor : ELA RHT [30000]	°C	Temperature
Global_0_85894	Environmental sensor : ELA RHT [30000]	%	Humidity
Global_0_85895	Environmental sensor : ELA MAG [30001]	-	IBleSensorMagCount
Global_0_85896	Environmental sensor : ELA MAG [30001]	-	IBleSensorMagPresent
Load_0_100000 Load_1_100000 Load_2_100000	DIRIS PMD US Medium level RJ12 [50] DIRIS PMD US Medium level 333mV [51]	%	Ph-N Voltage total harmonic distortion : THD V1 Ph-N Voltage total harmonic distortion : THD V1 Ph-N Voltage total harmonic distortion : THD V1
Load_0_100001 Load_1_100001 Load_2_100001	DIRIS PMD US Medium level RJ12 [50] DIRIS PMD US Medium level 333mV [51]	%	Ph-N Voltage total harmonic distortion : THD V2 Ph-N Voltage total harmonic distortion : THD V2 Ph-N Voltage total harmonic distortion : THD V2
Load_0_100002 Load_1_100002 Load_2_100002	DIRIS PMD US Medium level RJ12 [50] DIRIS PMD US Medium level 333mV [51]	%	Ph-N Voltage total harmonic distortion : THD V3 Ph-N Voltage total harmonic distortion : THD V3 Ph-N Voltage total harmonic distortion : THD V3
Load_0_100003 Load_1_100003 Load_2_100003	DIRIS PMD US Medium level RJ12 [50] DIRIS PMD US Medium level 333mV [51]	%	Ph-Ph Voltage total harmonic distortion : THD U12 Ph-Ph Voltage total harmonic distortion : THD U12 Ph-Ph Voltage total harmonic distortion : THD U12
Load_0_100004 Load_1_100004 Load_2_100004	DIRIS PMD US Medium level RJ12 [50] DIRIS PMD US Medium level 333mV [51]	%	Ph-Ph Voltage total harmonic distortion : THD U23 Ph-Ph Voltage total harmonic distortion : THD U23 Ph-Ph Voltage total harmonic distortion : THD U23
Load_0_100005 Load_1_100005 Load_2_100005	DIRIS PMD US Medium level RJ12 [50] DIRIS PMD US Medium level 333mV [51]	%	Ph-Ph Voltage total harmonic distortion : THD U31 Ph-Ph Voltage total harmonic distortion : THD U31 Ph-Ph Voltage total harmonic distortion : THD U31
Load_0_100006 Load_1_100006 Load_2_100006	DIRIS PMD US Medium level RJ12 [50] DIRIS PMD US Medium level 333mV [51]	%	Curent total harmonic distortion : THD I1 Curent total harmonic distortion : THD I1 Curent total harmonic distortion : THD I1
Load_0_100007 Load_1_100007 Load_2_100007	DIRIS PMD US Medium level RJ12 [50] DIRIS PMD US Medium level 333mV [51]	%	Curent total harmonic distortion : THD I2 Curent total harmonic distortion : THD I2 Curent total harmonic distortion : THD I2

Load_0_100008 Load_1_100008 Load_2_100008	DIRIS PMD US Medium level RJ12 [50] DIRIS PMD US Medium level 333mV [51]	%	Curent total harmonic distortion : THD I3 Curent total harmonic distortion : THD I3 Curent total harmonic distortion : THD I3
Load_0_100009 Load_1_100009 Load_2_100009	DIRIS PMD US Medium level RJ12 [50] DIRIS PMD US Medium level 333mV [51]	%	Curent total harmonic distortion : THD In Curent total harmonic distortion : THD In Curent total harmonic distortion : THD In
Load_0_100056 Load_1_100056 Load_2_100056	DIRIS PMD US Medium level RJ12 [50] DIRIS PMD US Medium level 333mV [51]	-	K-Factor I1 K-Factor I1 K-Factor I1
Load_0_100057 Load_1_100057 Load_2_100057	DIRIS PMD US Medium level RJ12 [50] DIRIS PMD US Medium level 333mV [51]	-	K-Factor I2 K-Factor I2 K-Factor I2
Load_0_100058 Load_1_100058 Load_2_100058	DIRIS PMD US Medium level RJ12 [50] DIRIS PMD US Medium level 333mV [51]	-	K-Factor I3 K-Factor I3 K-Factor I3
Load_0_100059 Load_1_100059 Load_2_100059	DIRIS PMD US Medium level RJ12 [50] DIRIS PMD US Medium level 333mV [51]	-	K-Factor In K-Factor In K-Factor In
Load_0_100060 Load_1_100060 Load_2_100060	DIRIS PMD US Medium level RJ12 [50] DIRIS PMD US Medium level 333mV [51]	%	System THD V System THD V System THD V
Load_0_100061 Load_1_100061 Load_2_100061	DIRIS PMD US Medium level RJ12 [50] DIRIS PMD US Medium level 333mV [51]	%	System THD U System THD U System THD U
Load_0_100062 Load_1_100062 Load_2_100062	DIRIS PMD US Medium level RJ12 [50] DIRIS PMD US Medium level 333mV [51]	%	System THD I System THD I System THD I
Global_0_100120	DIRIS PMD US Medium level RJ12 [50] DIRIS PMD US Medium level 333mV [51]	%	Total demand distortion : TDD I1
Global_0_100121	DIRIS PMD US Medium level RJ12 [50] DIRIS PMD US Medium level 333mV [51]	%	Total demand distortion : TDD I2
Global_0_100122	DIRIS PMD US Medium level RJ12 [50] DIRIS PMD US Medium level 333mV [51]	%	Total demand distortion : TDD I3
Global_0_100123	DIRIS PMD US Medium level RJ12 [50] DIRIS PMD US Medium level 333mV [51]	%	Total demand distortion : TDD In
Global_0_100124	DIRIS PMD US Medium level RJ12 [50] DIRIS PMD US Medium level 333mV [51]	%	System TDD I
Global_0_110343	Diris Digiware I-35 DC [4118]	V	ILoadDCVrmsAvg
Global_0_110344	Diris Digiware I-35 DC [4118]	V	ILoadDCVdcAvg
Global_0_110345	Diris Digiware I-35 DC [4118]	V	ILoadDCVacAvg
Global_0_135000	ATS3 Socomec pM [1000] ATS Loose controller ATyS C65 IEC [2402] Atys p [2300]	-	Priority
Global_0_135001	ATS3 Socomec pM [1000]	-	Alarm/Fault Code
Global_0_135030	Atys Bypass single line [2600] Atys Bypass dual line [2601]	-	Type of Application
Global_0_135038	ATS Loose controller ATyS C65 IEC [2402] ATS3 Socomec pM [1000] Atys Bypass dual line [2601] Atys Bypass single line [2600] Atys p [2300]	-	Operating Mode
Global_0_135039	ATS Loose controller ATyS C65 IEC [2402] ATS3 Socomec pM [1000] Atys Bypass dual line [2601] Atys Bypass single line [2600] Atys p [2300]	-	Switch Position
Global_0_135041	ATS Loose controller ATyS C65 IEC [2402]	-	Source 1 Start Generator relay State
Global_0_135042	ATS Loose controller ATyS C65 IEC [2402] Atys p [2300]	-	Source 2 Start Generator relay State
Global_0_135044	ATS Loose controller ATyS C65 IEC [2402] ATS3 Socomec pM [1000] Atys Bypass dual line [2601] Atys Bypass single line [2600] Atys p [2300]	-	Source 1 State

Global_0_135045	ATS Loose controller ATyS C65 IEC [2402] ATS3 Socomec pM [1000] Atys Bypass dual line [2601] Atys Bypass single line [2600] Atys p [2300]	-	Source 2 State
Global_0_135046	ATS Loose controller ATyS C65 IEC [2402] ATS3 Socomec pM [1000] Atys Bypass dual line [2601] Atys Bypass single line [2600] Atys p [2300]	-	Test in progress
Global_0_135048	ATS3 Socomec pM [1000]	-	Cycle Counter
Global_0_135049	ATS3 Socomec pM [1000]	-	Position 1 Manoeuvre counter
Global_0_135050	ATS3 Socomec pM [1000]	-	Position 2 Manoeuvre counter
Global_0_135052	ATS Loose controller ATyS C65 IEC [2402] ATS3 Socomec pM [1000] Atys Bypass dual line [2601] Atys Bypass single line [2600] Atys p [2300]	-	Alarm/Fault summary
Global_0_148015	PMS (Power Management System) [8272]	-	S012: General Alarm
Global_0_148021	PMS (Power Management System) [8272]	-	S005: Inverter ready
Global_0_160007	PMS (Power Management System) [8272]	%	Bank SOC
Global_0_160164	PMS (Power Management System) [8272]	Wh	Nominal energy for 1 string
Global_0_160253	PMS (Power Management System) [8272]	°C	External temperature
Global_0_160606	PMS (Power Management System) [8272]	-	Application - Generic alarm 11
Global_0_160914	PMS (Power Management System) [8272]	W	M016: Grid Active Power (signed)
Global_0_160916	PMS (Power Management System) [8272]	W	M018: ESS Active Power (signed)
Global_0_160920	PMS (Power Management System) [8272]	V	M025: DC voltage on ESS
Global_0_160922	PMS (Power Management System) [8272]	%	M027: Battery State-Of-Charge
Global_0_160923	PMS (Power Management System) [8272]	%	M028: Battery State-Of-Health
Global_0_160924	PMS (Power Management System) [8272]	-	M029: Number of battery racks connected
Global_0_160931	PMS (Power Management System) [8272]	W	Power wind turbines
Global_0_160932	PMS (Power Management System) [8272]	W	Power PV
Global_0_160933	PMS (Power Management System) [8272]	W	Power Genset
Global_0_160944	PMS (Power Management System) [8272]	-	Counter balancing
Global_0_160945	PMS (Power Management System) [8272]	Wh	Battery energy discharged
Global_0_160950	PMS (Power Management System) [8272]	-	Number of Source
Global_0_160951	PMS (Power Management System) [8272]	-	Output type
Global_0_160952	PMS (Power Management System) [8272]	W	Output power
Item_0_160953	PMS (Power Management System) [8272]	-	Type of source
Item_0_160954	PMS (Power Management System) [8272]	-	Status of the contact
Item_0_160955	PMS (Power Management System) [8272]	W	Source nominal power
Item_0_160956	PMS (Power Management System) [8272]	W	Source measured power
Item_0_160957	PMS (Power Management System) [8272]	-	Measured power is available
Global_0_160960	PMS (Power Management System) [8272]	-	Counter System in alarm
Global_0_160961	PMS (Power Management System) [8272]	-	Counter System ON
Global_0_160962	PMS (Power Management System) [8272]	-	Counter PV On
Global_0_160963	PMS (Power Management System) [8272]	-	Counter Genset On
Global_0_160964	PMS (Power Management System) [8272]	%	Deep of Discharge of batteries set
Global_0_160965	PMS (Power Management System) [8272]	-	Counter Wind turbine on
Global_0_165000	PMS (Power Management System) [8272]	s	Delta Counter System in alarm
Global_0_165001	PMS (Power Management System) [8272]	s	Delta Counter System ON
Global_0_165002	PMS (Power Management System) [8272]	s	Delta Counter PV On
Global_0_165003	PMS (Power Management System) [8272]	s	Delta Counter Genset On

Global_0_165004	PMS (Power Management System) [8272]	s	Delta Counter Wind Turbine On
Global_0_165005	PMS (Power Management System) [8272]	s	Delta Counter balancing
Global_0_165006	PMS (Power Management System) [8272]	Wh	Delta Battery energy discharged
Global_0_165010	PMS (Power Management System) [8272]	%	ESS System availability
Global_0_165011	PMS (Power Management System) [8272]	-	Battery cycle number per day
Global_0_165012	PMS (Power Management System) [8272]	%	Battery load rate
Global_0_400013	Atys Bypass single line [2600] Atys Bypass dual line [2601]	-	Bypass internal temperature
Global_0_400015	Atys Bypass single line [2600] Atys Bypass dual line [2601]	-	Bypass internal humidity
Global_0_400016	Atys Bypass single line [2600] Atys Bypass dual line [2601]	-	Bypass source 1 state
Global_0_400017	Atys Bypass single line [2600] Atys Bypass dual line [2601]	-	Bypass isolated state
Global_0_400018	Atys Bypass single line [2600] Atys Bypass dual line [2601]	-	Bypass source 2 state
Global_0_400101	Atys Bypass single line [2600] Atys Bypass dual line [2601]	-	Switch operating factor alarm
Global_0_400102	Atys Bypass single line [2600] Atys Bypass dual line [2601]	-	Switch neutral alarm
Global_0_400103	Atys Bypass single line [2600] Atys Bypass dual line [2601]	-	Switch fault 1 alarm
Global_0_400104	Atys Bypass single line [2600] Atys Bypass dual line [2601]	-	Switch fault 2 alarm
Global_0_400105	Atys Bypass single line [2600] Atys Bypass dual line [2601]	-	Switch alarm 1 alarm
Global_0_400106	Atys Bypass single line [2600] Atys Bypass dual line [2601]	-	Switch alarm 2 alarm
Global_0_400107	Atys Bypass single line [2600] Atys Bypass dual line [2601]	-	Switch phase rotation 1 alarm
Global_0_400108	Atys Bypass single line [2600] Atys Bypass dual line [2601]	-	Switch phase rotation 2 alarm
Global_0_400109	Atys Bypass single line [2600] Atys Bypass dual line [2601]	-	Switch capa 1 alarm
Global_0_400110	Atys Bypass single line [2600] Atys Bypass dual line [2601]	-	Switch capa 2 alarm
Global_0_400111	Atys Bypass single line [2600] Atys Bypass dual line [2601]	-	Switch power 1 alarm
Global_0_400112	Atys Bypass single line [2600] Atys Bypass dual line [2601]	-	Switch power 2 alarm
Global_0_400113	Atys Bypass single line [2600] Atys Bypass dual line [2601]	-	Switch position 1 alarm
Global_0_400114	Atys Bypass single line [2600] Atys Bypass dual line [2601]	-	Switch position 2 alarm
Global_0_400115	Atys Bypass single line [2600] Atys Bypass dual line [2601]	-	Switch position 0 alarm
Global_0_400116	Atys Bypass single line [2600] Atys Bypass dual line [2601]	-	Switch fault 0 alarm
Global_0_400117	Atys Bypass single line [2600] Atys Bypass dual line [2601]	-	Switch unbalanced 1 alarm
Global_0_400118	Atys Bypass single line [2600] Atys Bypass dual line [2601]	-	Switch unbalanced 2 alarm
Global_0_400119	Atys Bypass single line [2600] Atys Bypass dual line [2601]	-	Switch mainfault alarm
Global_0_400120	Atys Bypass single line [2600] Atys Bypass dual line [2601]	-	Switch motor fault alarm
Global_0_400121	Atys Bypass single line [2600] Atys Bypass dual line [2601]	-	Switch autoconf failed alarm
Global_0_400122	Atys Bypass single line [2600] Atys Bypass dual line [2601]	-	Switch unexpected transfer alarm

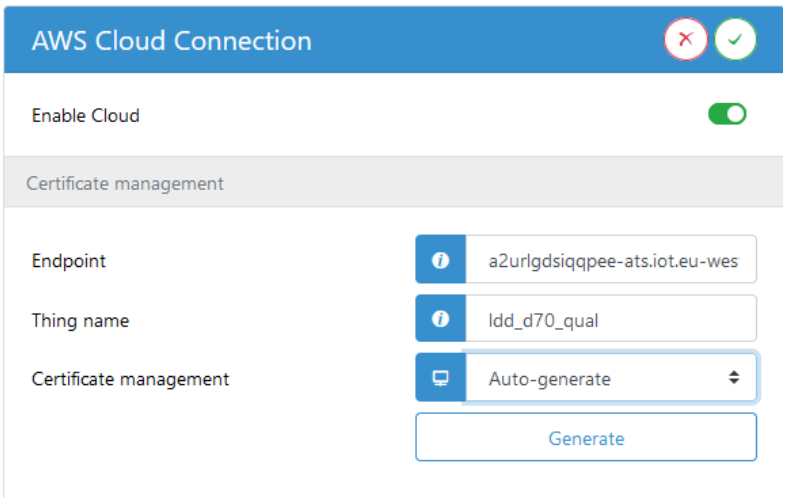
Global_0_400123	Atys Bypass single line [2600] Atys Bypass dual line [2601]	-	Switch fail to transfer alarm
Global_0_400125	Atys Bypass single line [2600] Atys Bypass dual line [2601]	-	Switch max power attempts alarm
Global_0_400126	Atys Bypass single line [2600] Atys Bypass dual line [2601]	-	Switch genset failed to start alarm
Global_0_400127	Atys Bypass single line [2600] Atys Bypass dual line [2601]	-	Switch external fault alarm
Global_0_400128	Atys Bypass single line [2600] Atys Bypass dual line [2601]	-	Switch unknown position alarm
Global_0_400120	Atys Bypass single line [2600] Atys Bypass dual line [2601]	-	Switch motor fault alarm
Global_0_400121	Atys Bypass single line [2600] Atys Bypass dual line [2601]	-	Switch autoconf failed alarm
Global_0_400122	Atys Bypass single line [2600] Atys Bypass dual line [2601]	-	Switch unexpected transfer alarm
Global_0_400123	Atys Bypass single line [2600] Atys Bypass dual line [2601]	-	Switch fail to transfer alarm
Global_0_400125	Atys Bypass single line [2600] Atys Bypass dual line [2601]	-	Switch max power attempts alarm
Global_0_400126	Atys Bypass single line [2600] Atys Bypass dual line [2601]	-	Switch genset failed to start alarm
Global_0_400127	Atys Bypass single line [2600] Atys Bypass dual line [2601]	-	Switch external fault alarm
Global_0_400128	Atys Bypass single line [2600] Atys Bypass dual line [2601]	-	

3 - Alternate provisioning methods

a) Gateway generatess certificate

If you decide to use the x509 certificate generated by the gateway. Instead of uploading credentials in webview, you shall rather :

- Fill the thing name
- Fill the AWS endpoint
- Select "Auto-generate"
- Click on the "Generate" button



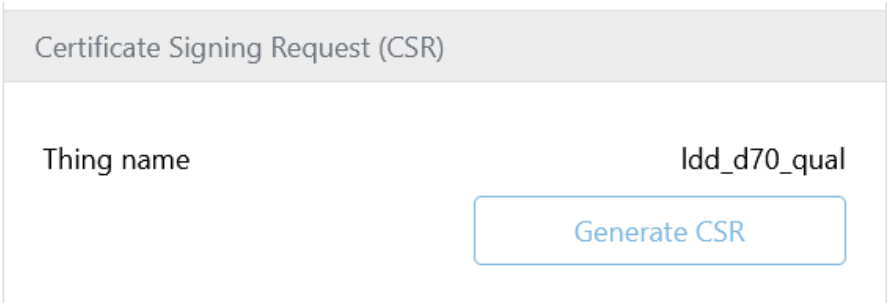
- Download the generated public certificate
- Register the public certificate to AWS and attach it to your thing (with the proper policy)

b) Gateway generates CSR, signed by AWS

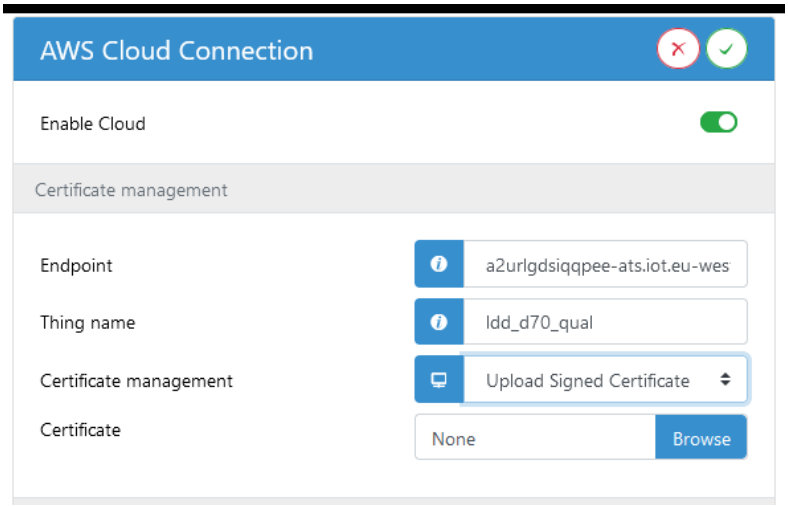
If you decide to use the CSR generated by the gateway:

- Fill the thing name

- Fill the AWS endpoint
- Click the button to generate a CSR, and download it.



- Give the CSR to AWS, so that it can sign and generate a certificate for your device.
- Download the signed public certificate from AWS
- Upload the certificate to the gateway



c) Gateway generates CSR, custom CA signs the certificate

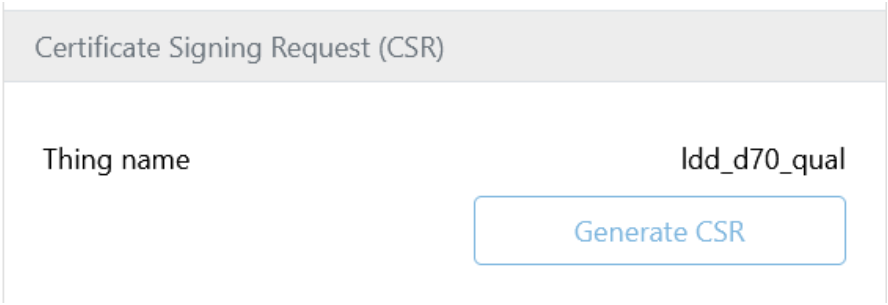
If you desire to use your own CA to sign the CSR, please refer to following documentation, main steps are:

CA:

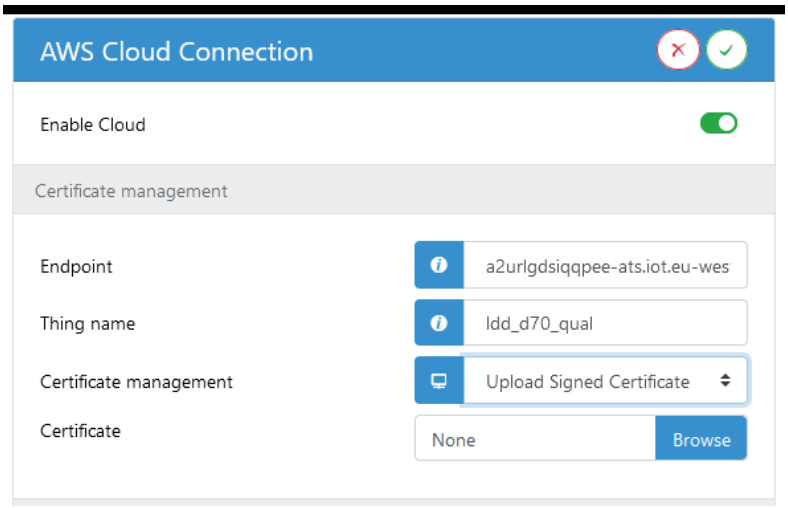
- Generate a CA
- Register your CA in AWS

Device (Webview) :

- Fill the thing name
- Fill the AWS endpoint
- Click the button to generate a CSR, and download it.



- Sign the CSR with your CA
- Upload the signed certificate to the gateway



Furthermore, following guide demonstrates how to create a custom CA certificate and register it to AWS to enable JITP : Set up JITP with AWS IoT Core (amazon.com)

In case you generate a certificate or a CSR from the gateway, make sure you have filled the thing name before clicking the button in Webview. Certificate and CSR use the thing name as common name, which is required to authenticate the device from AWS.

When generating a x509 certificate by yourself, subject name is limited in size and should not exceed 128 bytes.