D70 - Getting Started Guide for AWS IoT Core

- 1 Document information
- 2 Overview
- 3 Hardware Description
- 4 Set up your Development Environment
- 5 Set up your hardware
- 6 Setup your AWS account and Permissions
- 7 Connect your gateway
- 8 Provision your gateway
- 9 Exploit your Socomec data
 - a. Create the AWS Timestream database and table
 - $^{\rm o}~$ b. Forward your data from IoT Core to the Timestream database
 - c. Check your configuration
 - d. Install Grafana (hosted)
 - Grafana SQL commands samples
 - Plot temperature for all BLE temperature sensors found
 - Plot distribution of received messages count per device
 - Plot BLE magnetic sensor counter value:
- 10 TroubleshootingAnnex
 - 1 Dashboard demo
 - 2 Socomec data types description
 - 3 Alternate provisioning methods
 - a) Gateway generatess certificate
 - b) Gateway generates CSR, signed by AWS
 - c) Gateway generates CSR, custom CA signs the certificate

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
- IP addi
 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"

🔒 AWS loT - Manage - Things 🗙 🕂		✓ − Ø
← → C ☆ 🔒 eu-west-1.console.av	vs.amazon.com/iot/home?region=eu-west-1#/thinghub	Bi @ ☆ ★ D 😩
AWS Partner		
aws Services Q Search for servi	ces, features, blogs, docs, and more [Alt+S]	נו בא גער פאר גער גער גער גער גער גער גער גער גער גע
🔄 CloudWatch 🖓 IoT Core 🔟 IAM		
AWS IoT ×	AWS IoT > Manage > Things	
Monitor	Things (3) Info An IoT thing is a representation and record of your physical device in the cloud. A physical device	C Advanced search Run aggregations Edit Delete Create things
Connect Connect one device	needs a thing record in order to work with AWS IoT. Q. Filter things by: name, type, group, billing, or searchable attribute.	< 1 > ⊚
Connect many devices	Name	Thing type
Test	ldd_py_dev	• · · · · · · · · · · · · · · · · · · ·
 Device Advisor 	ldd_d70_qual	
Test suites	Ldd_qual_ZephyrRTOS-qemu	
Test runs and results MQTT test client		
Manage		
 All devices 		
Things		
Thing groups		
Thing to page		

3. Select "Create single Thing"

Fleet metrics



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

AWS IoT \times	AWS IoT > Manage > Things >	Create things > Create single thing
Monitor	Step 1 Specify thing properties	Configure device certificate - optional Info A device requires a certificate to connect to AWS IoT. You can choose how you to register a certificate for your device now, or
Connect	Step 2 - optional Configure device certificate	you can create and register a certificate for your device later. Your device won't be able to connect to AWS IoT until it has an active certificate with an appropriate policy.
 Connect many devices 	Step 3 - optional Attach policies to certificate	Device certificate
Test		• Auto-generate a new certificate (recommended) Generate a certificate, public key, and private key using AWS IoT's certificate authority.
Test suites Test runs and results MOTT test client		Use my certificate Use a certificate signed by your own certificate authority.
Manage		O Upload CSR Register your CA and use your own certificates on one or many devices.
 All devices Things Thing groups 		 Skip creating a certificate at this time You can create a certificate for this thing and attach a policy to the certificate at a later time.
Thing types Fleet metrics		Cancel Previous Next

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

(1)

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 "00000000000" with your current account ID

```
Gateway policy document
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "iot:Connect",
            "Resource": "arn:aws:iot:eu-west-1:00000000000:client/${iot:Connection.Thing.ThingName}"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iot:Publish",
                "iot:Receive"
            ],
            "Resource": "arn:aws:iot:eu-west-1:0000000000:topic/${iot:Connection.Thing.ThingName}/*"
        },
        {
            "Effect": "Allow",
            "Action": "iot:Subscribe",
            "Resource": "arn:aws:iot:eu-west-1:00000000000: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).

aws Services Q Search for service	es, features, blogs, docs, and more (Alt+S)	D	\$	⑦ Ireland •	LDD @ 0630-2866-1747 🔻 🔶
🔯 CloudWatch 🚳 IoT Core 🗧 IAM 🛃 Qu	edSight 🕎 AWS Glue 🤨 53 💐 Athena 👿 Kinesis 👿 Anazon Timestream 🌉 Lambda 🦉 Anazon Grafana				
AWS InT X					
	Policy properties				
Monitor	AWS IoT Core supports named polities so that many identifies can reference the same policy document.				
Connect	Poury maile				
Connect one device	my concentry only A policy many is an alphanumeric string that can also contain period (.), comma (.), hyphen(-), underscore (.), plus sign (+), equal sign (-), and at sign (@) characters, but no spaces.				
Connect many devices					
	► Tags - optional				
Test					
Device Advisor	Policy statements Policy examples				
MQTT test client					
	Policy document into			Bi	uilder JSON
Manage	An AWS IoT policy contains one or more policy statements. Each policy statement contains actions, resources, and an effect that grants or denies the actions by the resources.				
All devices					
Greengrass devices	Policy document				
LPWAN devices	2 "Version": "2012-10-17",				
Message Routing	3 * "Statement": [4 * (
Retained messages	5 "Effect": "Allow", 6 "Coting" "introduced"				
Security	7 Resource': "arn:aws:iot:eu-west-1:123456789012:client/\$(iot:Connection.Thing.ThingHame)"				
Fleet Hub	8 }, 9* {				
	10 "Effect": "Allow", 11 Technol : "introbalist"				
Device Software	12 "Resource": "arr:aws:lot:eu-west-1:123456789012:topic/\${lot:Connection.Thing.ThingName}/*"				
Billing groups	13 }, 14 \varphi {				
Settings	15 "Effect": "Allow", 16 "Action" 'Introducedon"				
Learn	<pre>17 "Resource": "arn:awsiot:eu-west-1:123456789012:topicfilter/\$(iot:Connection.Thing.ThingName)/*"</pre>				
Feature spotlight	18 }, 19 ¥ {				
Documentation 🔼	20 "Effect": "Allow", 11 "Action" 'Interfactur"				
New console experience	22 "Resource': "arn:wesilotus-west-1:123456789012:topic/\${iot:Connection.Thing.ThingWame}/*"				
Tell us what you think	23 } 24]				
	JSON Line 22, Column 54 🛞 Errors: 0 🛕 Warnings: 0				
Feedback Looking for language selection? Find it	© 2022, Amizon	Web Services,	Inc. or its af	filiates. Privacy	Terms Cookie preferences

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

Services Q Search for se	kces, features, blogs, docs, and more [Alt+5]	▶ 🔶 ⑦ Ireland ▼ LDD @ 0630-2
atch 🚳 IoT Core 🛅 IAM 🛛	QuickSight 📱 AWS Glue 🧕 S3 💐 Athena 📓 Kinesis 🕃 Amazon Timestream 🧏 Lambda 🐻 Amazon Grafana	
loT ×		
	Policy properties	
	AWS IoT Core supports named policies so that many identities can reference the same policy document.	
	Policy name	
	ldd gual demo.minimat	
ect one device	A policy name is an alphanumeric string that can also contain period (1, comma (), hyphen(-), underscore (), plus sign (+), equal sign (-), and at sign (@) characters, but no spaces.	
ect many devices		
	▶ Tags - optional	
ice Advisor	Policy statements Policy examples	
IT test client		
e	Policy document info an all's to notice rotation one or more policy statements. Each policy statement rotations are services and an effect that grants or deales the articles by the resources	Builder JSON
devices		
engrass devices	Policy document	
/AN devices	1•{	
note actions	2 "Version": "2012-10-17", 3 * "Statement": [
sage Routing	4 - (
ained messages	5 "Effect: "Allow", 6 "Action: "iot:Connect".	
urity	7 "Resource": "arn:aws:iot:eu-west-1:123456789012:client/\${iot:Connection.Thing.ThingName}"	
et Hub	8 3) 9 \ {	
	10 "Effect": "Allow",	
Software	<pre>11 Action : iot:Fublish , 12 "Resource": "armisws/iot:eu-west-1:123456789012:topic/\${iot:Connection.Thing.ThingName}/*"</pre>	
groups	13 },	
s	1" 1 15 Effect": "Allow",	
	16 "Action': "iotiSubscribe", 17 "Becoment" image sup: (otraumestal:123456780012:ton/ffltar/f/(ot/Conpartion Thing ThingName)/*"	
spotlight	18 },	
ientation [2]	19 ¥ { 20 "Effect": "Allow",	
	21 "Action": "iot:Receive",	
ew console experience	22 "Resource": "anniaws:lotius-west-1:123456789012:topic/\${iot:Connection.Thing.ThingName}/*" 23 }	
ell us what you think	24] 73	
	JSON Line 22, Column 54 (R) Errors: 0 A Warnings: 0	

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

Download certificate and key files to AWS.	o install on your device so tha	at it can connect to
Device certificate You can activate the certificate now, or la AWS IoT.	ter. The certificate must be active	for a device to connect
Device certificate be3cb2f23d0te.pem.crt	Deactivate certificate	🕑 Download
The key nices are unique to this certificate Download them now and save them in a s	and can't be downloaded after yo secure place. download the key files for th	u leave this page. his certificate.
Public key file	00k nuklis nem keu	🕑 Download
Private key file	oob-public.pent.key	(1) December 2
be3cb2f23d0221808adb8bf2330	0b-private.pem.key	W Download
Root CA certificates Download the root CA certificate file that you're using. You can also download the r	corresponds to the type of data e oot CA certificates later.	ndpoint and cipher suit
Amazon trust services endpoint		🕑 Download
RSA 2048 bit key: Amazon Root CA	1	
Amazon trust services endpoint		Download
ECC 256 bit key: Amazon Root CA 3		
If you don't see the root CA certifica root CA certificates. These root CA c guides. Learn more 🗹	ate that you need here, AWS I certificates and others are ava	oT supports addition ilable in our develop

(i) 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 :

AWS IoT \times	O You successfully created thing idd_quai_demo.	View thing
Monitor	⊘ You successfully created certificate be3cb2f23d0221808adb8bf603661955ff906159b3f3bab6eea84864f023300b.	View certificate
Monitor	AWS IoT > Manage > Things	
Connect Connect one device Connect many devices	Things (4) into An UT thing is a representation and record of your physical divice in the claud. A physical divice reads a thing reard in order to work with MASUST. Q. Fitter things by name, type, group, Milling, or searchable attribute.	Ø Advanced search Run aggregations Edit Delete Create things < 1 > Ø
Test ▼ Device Advisor Test suites	Name	Thing type
Test runs and results	Idd_qual_demo	· · · · · · · · · · · · · · · · · · ·
MQTT test client	Lidd_py_dev	
	Lidd_d70_qual	
 All devices 	Ltdqual_ZephyrRTOS-qemu	•
Things Thing groups Thing types Fleet metrics		

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

	= 👔 🔁 🕅 EBVIEW-M V2
Retwork Configuration	Cloud Field Protocols
Protocols	2023/05/04 1
AWS Cloud Connection	×
Enable Cloud	
Certificate management	
Endpoint	a2urlgdsiqqpee-ats.iot.eu-west-1.amazc
Thing name	0 Idd_d70_qual
Certificate management	₽ Upload ♦
Certificate	d2a1ac75a48a92ace8b00c5111b215 Browse
Private Key	d2a1ac75a48a92ace8b00c5111b215 Browse
Certificate Signing Request (CSR)	
Thing name	0 Idd_d70_qual
	Generate CSR
Synchronisation Status	

Click synchronize

AWS Cloud Connection	
Enable Cloud	
Certificate management	
Endpoint Thing name Installed Certificate Information	a2urlgdsiqqpee-ats.iot.eu- west-1.amazonaws.com ldd_d70_qual View Certificate Details (
Certificate Signing Request (CSR)	
Thing name	Idd_d70_qual Generate CSR
Synchronisation Status	
State Last connection Synchronised Devices	Active 2023/05/04 11:31:01 5/5
Synchi	ronise

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": "9999999999",
    "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.

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

9 - Exploit your Socomec data

(i)

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"

aws Services Q Search for se	rvices, features, blogs, docs, and more [Alt+S]		▶ ♦ Ø Ireland ▼ LDD @ 0630-2866
🔯 CloudWatch 🦉 IoT Core 🥫 IAM 🔢	QuickSight 📑 AWS Glue 🥳 53 🐧 Athena 🥫 Kinesis 🦉 Amazon Timestream 🌉 Lambda 👸 Amazon Grafana		
Amazon Timestream $~~ imes$	Timestream > Databases		
▼ Resources	Databases (1) Info		C Edit Delete Create database
Databases Tables	Q, Filter		< 1 > @
▼ Management Tools	Name	 Creation time (UTC) 	▽
Query editor	O MyTimeSeriesDatabase	8/29/2022, 11:46:00 AM	
Scheduled queries Monitoring			
Learning Resources			
Getting started 🔀			
Tutorials			

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

Timestream $>$ Databases $>$ Create database		
Create database Info		
Database configuration Create and configure a database or create a database	e with sample data to explore Timestream right awa	у.
Choose a configuration Standard database Create a new database with custom create an environmention	Sample database Create a database and populate it with	
Name	click.	
Specify a name that is unique for all Timestream dat You can not change this name once you create it.	abases in your AWS account in the current Region.	
MysocomecGatewayDatabase Must be between 3 and 256 characters long. Must co	ntain letters, digits, dashes, periods or underscores.	

- Keep the rest of the configuration unchangedClick "Create database"

Your created database should appear in the list:

Amazon Timestream $~~ imes$	⊘	Successfully created database MySocomecGatewayDatabase.		×
▼ Resources		Timestream > Databases		
Databases Tables		Databases (2) Info		C Edit Delete Create database
▼ Management Tools		Q, Filter		< 1 > @
Query editor		Name	Creation time (UTC)	Ψ
Scheduled queries Monitoring		O MySocomecGatewayDatabase	9/1/2022, 12:50:46 PM	
▼ Learning Resources		O MyTimeSeriesDatabase	8/29/2022, 11:46:00 AM	
Getting started 🔀				
Tutorials				

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"

and the second s		
reate table տ		
Table details		
Database name Crosse the detabase where this table	le will be created.	
MySocomecGatewayDatabase		*
Table name Specify a table name that is unique	within this database. You can not change th	is name once you create H.
MyTable1		
Hast be between 3 and 256 characti	ers long. Must contain letters, digits, dashes,	periods or anderscores.
Data retention into Specify how long your data is retain exceeds the magnetic stress retention	ed in each storage tier. Data moves from the mwill be deleted.	memory store to the magnetic store as it ages. Data that
Memory store retention Seech new loss data will be stored	f in the memory store before it is request to -	magnetic store.
Memory store retention Specify how long data will be stored	I in the memory store before it is moved to r Day(s)	magnetic store.
Memory store retention Specify how long data will be stored 1 The value must be a number. Mean number of another. Magnetic store retention	E in the memory store before it is moved to- Dap(s) we 1 hear,	napelii dun.
Memory shore retention Specify how long data will be stored 1 The value must be a number. However, maximum 12 months. Magnetic store retention Specify how long data will be stored	I in the memory store before it is moved to- Day(s) ares 1 hour, in the magnetic stars before it is distored.	rapeli dan.

- Keep the rest of the configuration unchangedFinally click "Create table"

Your table should appear in the list of tables

aws iii Services Q. Search for su Image: CloudWatch Image: Low Core Image: Low Core Image: Low Core	ervices, features, blogs, docs, and more [Alt+S] @ QuickSight: 197 AWS Glue: 195 53. 100, Athens: 1976 Amazon Timestream 1976 Lambda: 100, Amazon Grafiana		[♣] ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓
Amazon Timestream $~~ imes$	⊘ Successfully created table MyTable1.		
▼ Resources	Timestream > Tables		
Databases Tables Management Tools	Tables (5) toto Q. Filter		Create scheduled query Edit Delete Create table < 1 > ⊗
Query editor	Table name	Database	v Creation time (UTC) v
Scheduled queries	O MyTable1	MySocomecGatewayDatabase	9/1/2022, 12:54:25 PM
▼ Learning Resources	MyTimeSeriesEnhancedTable MyTimeSeriesFromIotCorrectedTimestampTable	MyTimeSeriesDatabase MyTimeSeriesDatabase	8/29/2022, 1:27.01 PM 8/31/2022, 2:18:47 PM
Tutorials	MyTimeSeriesFromLambdaTable	MyTimeSeriesDatabase	8/30/2022, 8:42:05 AM
	O MyTimeSeriesTable	MyTimeSeriesDatabase	8/30/2022, 8:41:02 AM

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"

aWS Services Q. Search for	r services, features, blogs, docs, and more [Alt+5] 20 QuádSight 📲 Alk5 Glue 🦷 53 🔳 Anteon 🗑 Kinesk 📓 Anazon Timetaram 関 Landob 📓 Anazon Garlina	☑ 🎝 Ø Ireland ▼ LDD @ 0530-2866
AWS IoT ×	AWS IoT > Message Routing > Rules	
Monitor	Rules (5) Info Rules allow your things to interact with other services. Rules are analyzed and perform specific actions based on messages published by your devices.	C Activate Deactivate Edit Delete Create rule
Connect	Q. Find rules	< 1 > 0
Connect one device	□ Name v Status v Rule topic v Created date	v
Connect many devices	□ ToMyTimeSeriesFromIotCorrectedTim ② Active Idd_d70_qual/message/data/* August 31, 2022, 17:03:19 (UTC+0200)	
Test	ToMyTimeStream Q Active Idd_d70_qual/message/data/+ August 31, 2022, 17:03:29 (UTC+0200)	
Device Advisor	□ ToMyLambdaToTimestreamRule	
MQTT test client	□ ToMyTimeStreamEnhanced ⓒ Inactive Idd_d70_qual/message/data August 29, 2022, 15:32:04 (UTC+0200)	
Manane	Idd_d70_rule	

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

aws	Q Search for services, fe	atures, blogs, docs, and more (Alt+5)
🛛 Clou	dWatch 🛛 IoT Core 📅 IAM 👿 QuickSig	nt 📷 AMS Glue 🤠 53 🗮 Athena 📺 Kinesis 🕎 Anazon Tinestream 📜 Lambda 📷 Anazon Grafana
=	AWS IoT > Message Routing > Rules	> Create rule
	Step 1 Specify rule properties	Specify rule properties Info A rule resource contains a list of actions based on the MQTT topic stream.
	Step 2 Configure SQL statement	Rule properties
	Step 3 Attach rule actions	Rule name MultataToTimestroam
	Step 4 Review and create	There an alghanumeric string that can also contain undencore () characters, but no spaces. Rule description - optional Enter a description to provide additional details about the rule to others.
		A description of your new rule Tags - optional
		No tags are associated with the resource.
		You can add 50 more tags.
		Cancel 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"

aws Services Q Search for services	features, blogs, docs, and more [Alt+5]
Coolswatch @ for Core @ two @ Quece	sgent 🝸 na suute 🛐 ss 🐧 numeta 📷 numesa 📷 annacon meserean 🔌 Lunicola 🧐 numera unanan estemanRole
AWS IoT > Message Routing > Ru	ies > Create rule
Step 1 Specify rule properties	Attach rule actions Info An action routes data to a specific AWS service.
Step 2 Configure SQL statement	SQL statement Back
Step 3 Attach rule actions	SELECT deviceId, measures.* FROM 'ldd_070_qual/message/data/+'
Step 4 Review and create	Rule actions Select one or more actions to happen when the above rule is matched by an inbound message. Actions define additional activities that occur when messages anive, like storing them in a database, invoking cloud functions, or sending notifications. You can add up to 10 activities
	Action 1 Timestream table Remove <l< th=""></l<>
	Database name infe MySconrecGatewayDatabase View C View C Create Timestream database C
	MyTable1 View [2] Create Timestream table [2]
	Dimensions Each record contains an array of dimensions (minimum 1). Dimensions represent the metadata attributes of a time series data point. Dimension ranne Dimension value
	device_jd \$(topic(4)) Remove
	Add new dimension
	Timestamp value - optional Timestamp unit
	S(utrimestamp) SECONDS V
	IAM role Choose a role to grant. AWS IoT access to your endpoint. MyDataToTimestreamRole Wile Commentation MyDataToTimestreamRole Wile Commentation MyDataToTimestreamRole MyDataToTime
	Add rule action

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

🍅 AWS Grafana Console	🗙 🛛 🧑 PSM workspace dashboard - Ami 🗙 🛛 New folder 🛛 🥚	AWS IoT × 👔 What is Amazon Timestream	? - A 🗙 🥚 AWS IoT - Message Routing - Rul 🗙	G Google
← → C ①	west-1.console.aws.amazon.com/iot/home?region=eu-west-1#/cre	ate/rule		
📕 Admin 📕 Misc 📕 Az	ure 📃 AWS 📃 Agora 📙 Workspace 📙 Current 📒 AWS Do	c to finish 3		
aws Services Q Search for se	vices, features, blogs, docs, and more [Alt+S]			
CloudWatch 😨 IoT Core 🔯 IAM 题	QuickSight 📱 AWS Glue 🦉 53 🔳 Athena 🗮 Kinesis 🔃 Amazon Timestream 📗 Lambda 🤇	anaran Galana		
Successfully created role MyData1	oTimestreamRole			
Step 2 Configure SQL statement	Step 1: Rule properties			Edit
Step 3	Rule properties			
Attach rule actions Step 4	Name MyDataToTimestream			
Review and create	Description -			
	Step 2: SQL statement			Edit
	SQL statement			
	SQL version 2016-03-23			
	SQLquery SELECT deviceId, measures.* FROM 'ldd_d70_qual/message/data/*'			
	Step 3: Rule actions			Edit
	Actions			
	Timestream table White a message into a Timestream table			
	Database name MySocomerGatewayDatabase	Table name MyTable1	Dimensions 1 name: device, jd • value: \${topic(4)}	
	Timestang value - optional • value 5(sittimestang) • unit 5CCND5	LAR role amaanstam: 063028661747;role/service-role/MyDataToTimestreamRole 🔀		
	Error action			
	No error action			
			Cancel	Previous Create

Your rule should be listed in the following table:

aws Services Q Search for services	s, features, blogs, docs, and more [.	Alt+S]			L. E)	⑦ Ireland	- LDD @ 0630-286
🔯 CloudWatch 🛛 IoT Core 📴 IAM 💹 Quick	kSight 🕎 AWS Glue 👦 S3 💐 Athena 📝 Kinesis	🛐 Amazon Timestream 🛛 🔣 Lamb	ida 🛛 🥂 Amazon Grafana					
AWS IOT × 🔍 🛇 S	Successfully created rule MyDataToTimestream.							View rule
Monitor	AWS IoT > Message Routing > Rules							
Connect	Rules (6) Info Rules allow your things to interact with other services. Rule	s are analyzed and perform specific act	tions based on messages published by your	devices.	C Activate Deactivate	Edit	Delete	Create rule
Connect one device	Q. Find rules					< 1 > ⊚		
Connect many devices	□ Name マ	Status v Rule top	ic 🔻	Created date				~
Test	ToMyTimeSeriesFromIotCorrectedTIm	⊘ Active Idd_d70_	_qual/message/data/+	August 31, 2022, 17:03:19 (UTC+0200)				
Device Advisor	MyDataToTimestream	⊘ Active Idd_d70_	_qual/message/data/+	September 01, 2022, 15:18:00 (UTC+0200)				
MQI I test client	ToMyTimeStream	⊘ Active Idd_d70_	_qual/message/data/+	August 31, 2022, 17:03:29 (UTC+0200)				
Manage	ToMyLambdaToTimestreamRule	⊘ Active Idd_d70_	_qual/message/data/+	August 31, 2022, 16:37:50 (UTC+0200)				
All devices	ToMyTimeStreamEnhanced	⊖ Inactive Idd_d70_	_qual/message/data	August 29, 2022, 15:32:04 (UTC+0200)				
Greengrass devices	ldd_d70_rule	⊖ Inactive Idd_d70_	_csr_demo0/message/data	August 22, 2022, 11:14:04 (UTC+0200)				

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

You should get something like this:

aws	Services	Q Search for services, feature	es, blogs, docs, and more	[Alt+S]					D & 0	ireland 🔻	LDD @ 0630-286
🔯 Clou	dWatch 🦉 IoT	l Core 🥫 IAM 🔃 QuickSight	🍸 AWS Glue 🛛 👸 S3 🛛	Athena 📷 Kinesis 👸 Amazon Timestream 👩 Lambda							
=	Timestream	> Query editor									
	Eultor	Recent Saved queries	Sample queries								
	Database		Query 4 X	Query 1 X Query 2 X Query 3 X	Query 5 X 🛛 Query 7 X	Ø Query 6 X	⊘ Query 8 × +				•
									5 6	<u>(a)</u> /	• 🔳
	Choose a data	abase to query.	1 Get the 10 m	most recently added data points in the past 15 minutes. You	can change the time period if y	ou're not continuou	usly ingesting data				
	MyTimeSi	eriesDatabase 🔻	2 BELECT * FROM "F	wylimeberlesbatapase", "nylimeberlessrombampdalapie" www	SKE (INC between dgo(ISM) and now	() OKDER BY CIME DE	SC LIMIT 10				
	Tables ((3)									
	Q Filter	r tables									
	▶ MyTin	meSeriesEnhancedTa									
	▼ MyTin	neSeriesFromLambda									
	occure	ence (varchar)	Run Save	Clear							
	device macro	e_id (varchar) o_classification (varchar)	Table details	Query results Output							
	service measu	e (varchar) ure_name (varchar)									
	time ((timestamp) ure value::double (double)	Rows returned	(10)							
			Q, Filter							< 1	> ©
	▶ MyTin	neSeriesTable	occurence	device_id	macro_classification	service	measure_name	time	measure_val	ue::double	
			0	7066cd90-80e6-11cb-a49c-0000193c848c	Global	85880	IBleSensorTemperature	2022-08-30 15:04:09.000000000	25.19		
			0	7066cd90-80e6-11cb-a49c-0000193c848c	Global	85894	IBleSensorHumidity	2022-08-30 15:04:09.000000000	46.0		
			0	7066cd90-80e6-11cb-a49c-0000193c848c	Global	85894	IBleSensorHumidity	2022-08-30 15:03:54.000000000	46.0		
			0	7066cd90-80e6-11cb-a49c-0000193c848c	Global	85880	IBleSensorTemperature	2022-08-30 15:03:54.000000000	25.16		
			1	3b1e2140-80d9-11cb-b421-333130303130	Load	30004	Load_1_30004	2022-08-30 15:03:42.000000000	0.0		
			0	3b1e2140-80d9-11cb-b421-333130303130	Load	30019	Load_0_30019	2022-08-30 15:03:42.000000000	230.4		
			0	3b1e2140-80d9-11cb-b421-333130303130	Load	30003	Load_0_30003	2022-08-30 15:03:42.000000000	226.8		

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"

aws Services Q Search fo	r services, features, blogs, docs, and more	[Alt+S]
점 CloudWatch 🛛 IoT Core 🔤 IAM	🕜 QuickSight 🛛 🛛 AWS Glue 📴 S3 🔍 Athena	😿 Kinesis 🥫 Amazon Timestream 🛛 🐹 Lambda 🛛 🔞 Amazon Grafana
Amazon Managed X Grafana	Amazon Grafana > Workspaces > Ci Step 1	reate new workspace
All workspaces	Specify workspace details Step 2	A workspace is a logically isolated Grafana server. Once you have created a workspace, you can integrate it with data sources, then query and visualize metrics from those data sources. As part of creating a workspace, you will enable AWS IAM Identity
Grafana Enterprise license	Configure settings	Center (successor to AWS SSO) if you haven't done so already.
Documentation 🖸	Step 3 Service managed permission	Workspace details
	Step 4	Workspace name Give a unique name to your workspace.
	Review and create	MyGrafanaWorkspace
		Workspace description - optional
		 Tags - optional A tag is a label that you assign to an AWS resource. Each tag consists a key and an optional value. You can use tags to search and filter your resources or track your AWS costs. Currently not editing fields. Add new tag You can add up to 50 more tags.
		Cancel 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

Step 2 Configure settings Step 3 Service managed permission settings Step 4 Review and create	IAM permission access settings Select how you would like to specify account access.
Configure settings Step 5 Service managed permission settings Step 4 Review and create	Select how you would like to specify account access.
Service managed permission settings Step 4 Review and create	Current account Use Grafana to monitor resources in your current Use Grafana to monitor resources in your Organizational Data sources Selecting an AUS data source below creates an IAM role that non-lose Annapor Grafana access to those resources in your corrent account. It desen not set up the selected envice as a data source. Note that source measures must be tagged Grafana@utaGaure to be accessible.
step 4 Review and create	Data sources and notification channels - optional Data sources Selecting on AMS data source below creates an IAM role that enables Amazon Grafina access to those resources in your current account. It does not act up the selected service as a data source. Note that some resources must be tagged GrafinaDataSource to be accessible.
	Data sources Selecting an AVS-data source below creates an IAM role that enables Amazon Grafima access to there resources in your current account. It does not as tay the selected service as a data source. Note that some resources must be tagged Grafinathadhardhore to be accessible.
	Data source name
	AWS IoT SiteWise
	AWS X-Ray
	Amazon CloudWatch
	Amazon OpenSearch Service
	Amazon Managed Service for Prometheus
	Amazon TimeStream
	Amazon Redshift
	Amazon Athena
	Notification channels
	Selecting a notification channel below creates an IAM role that enables Amazon Grafana access to those resources in your current account. It does not set up the selected services as a notification channel. Note that when selecting Yamazon 5455, only SRS topics that start with "grafitm" will be executed.
	Notification channel name
	Amazon SNS

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

Ø	器 General / Home					114 B 🐵 🖵
as) ⊘	Welcome to Amazon Managed	d Grafana			Need help? Documentation	Tutorials Community
+ III () () () () () () () () () () () () ()	Basic The steps below will guide you to quickly finish setting up your Grafana installation.	TUTORIAL DATA SOURCE AND DASHBOARDS Grafana fundamentals Set up and understand Grafana if you have no prior experience. This tutorial guides you through the entire process and covers th "Data source" and "Dashboards" steps to the right.	e	COMPLETE Add your first data source	COMPLETE Create your first dashboard	Remove this panel
•	Das Starred dashboards PSM workspace dashboard Recently viewed dashboards PSM workspace dashboard	shiboards *	Sep 07 New in Traditio else. Se writing i delay du push ole samplin	Grafana Mimir: Introducing out-of-ord nally the Prometheus TSDB only accepts in veral use cases, however, need out-of-ord metrics. Complex metric delivery architect te lo congestion. Standalone Prometheus d samples. As Prometheus continues to be g poses an increasingly hard problem.	Latest from the blog ler sample ingestion •order samples that are less than one hour r support. For example: IoT devices waking ures using message buses like Kafka with r instances isolated from a network connect e adopted in new fields and industries, the li	old, discarding everything up asynchronously and andomized sharding and on for some time trying to mitation of in-order
(?)			Sep 06	earning with Grafana Labe Senior Eng	ineering Manager Myrle Krantz	

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

	арріу
Table view • Fill Actual ⑦ Last 2 days ~ ♀ २ 2 2 Time series ~	>
Panel Title Q. Search options	
All Overrides	
27 V Panel options	
26 Tritle Panel Title	
23 24 Description	
temperature Transparent background	
€ Query 1 \$3 Transform 0	
Deta source 🔓 Amazon Timestream eu-west-1 🗸 🕐 > Query options MD = auto = 1275 Interval = 2m Query inspector Participations	
✓ Tooltip	
A (Amazon Timestream cu-west-1) C C T Tooltip mode Tooltip mode	
Macros 1 SELECT time, measure_value::double as temperature FROM \$_database.\$_table MIERE measure_name*1 missions Single All Hidden	
Ustabase 0 wy importenzataba v	
Table O Wy Imperents laber v	
Render	
Wait for all queries	

- 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	IDClacAvg IDClacAvg IDClacAvg
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 : 11 Crest factor : 11 Crest factor : 11
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 : 12 Crest factor : 12 Crest factor : 12
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 : 13 Crest factor : 13 Crest factor : 13
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
ltem_0_160953	PMS (Power Management System) [8272]	-	Type of source
ltem_0_160954	PMS (Power Management System) [8272]	-	Status of the contact
ltem_0_160955	PMS (Power Management System) [8272]	W	Source nominal power
ltem_0_160956	PMS (Power Management System) [8272]	W	Source measured power
ltem_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 nameFill the AWS endpoint
- Select "Auto-generate"
 Click on the "Generate" button

AWS Cloud Connection		×
Enable Cloud		
Certificate management		
Endpoint	(i)	a2urlgdsiqqpee-ats.iot.eu-wes
Thing name	•	ldd_d/0_qual
Certificate management	₽	Auto-generate 🗢
		Generate

- 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.

Thing name	ldd_d70_qual
	Generate CSR

Upload the certificate to the gateway

AWS Cloud Connection	×
Enable Cloud	
Certificate management	
Endpoint	a2urlgdsiqqpee-ats.iot.eu-wes
Thing name	ldd_d70_qual
Certificate management	□ Upload Signed Certificate ◆
Certificate	None Browse

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

Certificate Signing Request (CSR)	
Thing name	ldd_d70_qual
	Generate CSR

- Sign the CSR with your CAUpload the signed certificate to the gateway

AWS Cloud Connection	8 🗸
Enable Cloud	
Certificate management	
Endpoint	a2urlgdsiqqpee-ats.iot.eu-wes
Thing name	ldd_d70_qual
Certificate management	☐ Upload Signed Certificate
Certificate	None Browse

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.

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