Azure connectivity: Get started document

platform	device	language
Proprietary	DIRIS Digiware M-xx DIRIS Digiware D-xx	Not required

Introduction

About this document

This document describes how to connect the SOCOMEC DIRIS Digiware M/D gateways with Azure IoT. This multi-step process includes:

- Configuring Azure IoT Hub
- Registering your IoT device
- Provisioning your devices on Device Provisioning service (DPS)
- Configuring Azure IoT connectivity on device

Step 1: Prerequisites

You should have the following items ready before beginning the process:

- Setup your IoT hub
- Provision your device over DPS

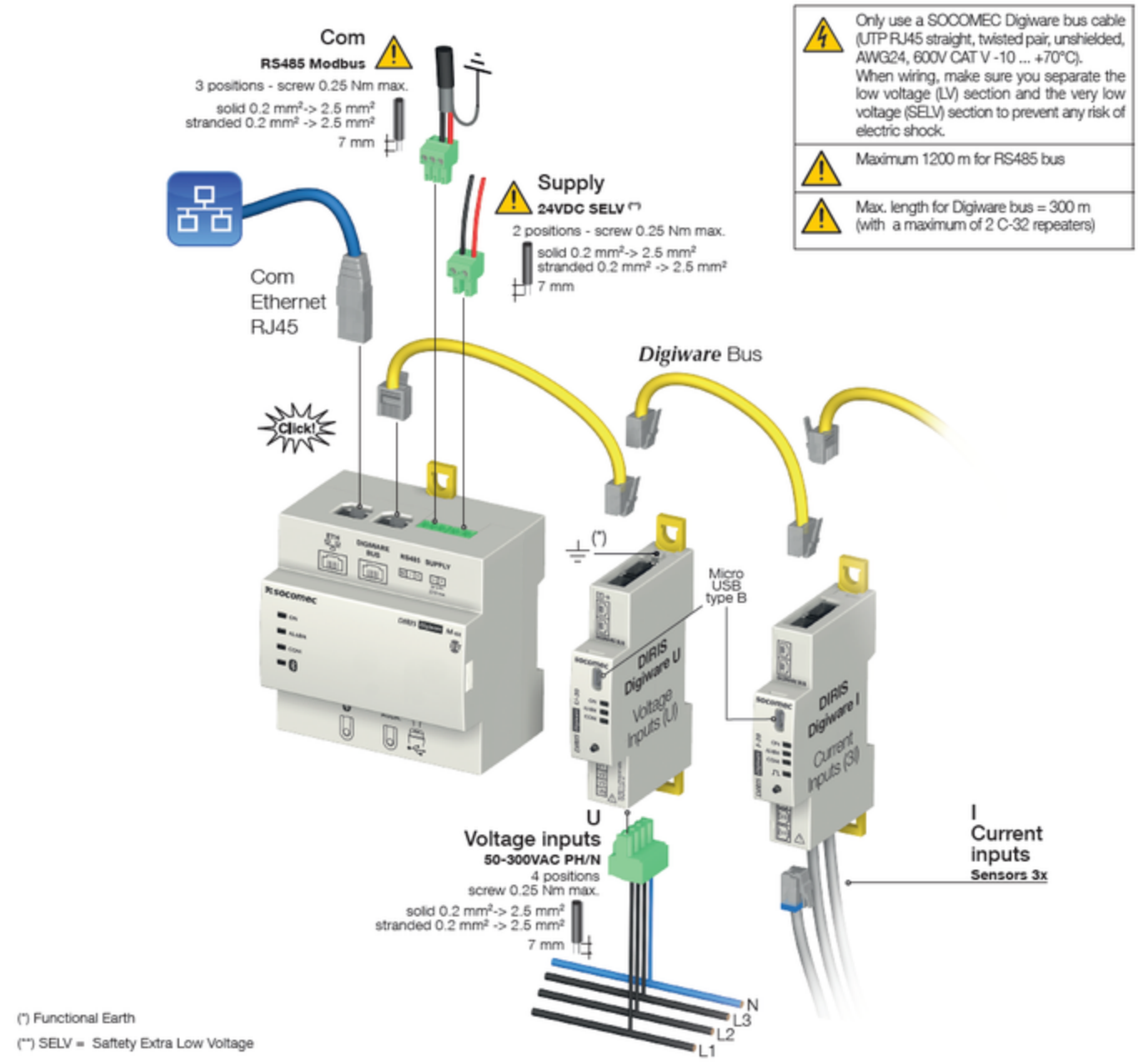
The DIRIS Digiware M/D gateways integrate a firmware natively compatible with Azure connectivity. There is no need to compile source code or libraries, and configuration can be done easily through the integrated web server.

Step 2: Prepare your DIRIS Digiware M/D gateway

System wiring

Please refers to the user manual of the device to get all the details of commissioning. You can also look at Configure your DIRIS Digiware system video.

Before enabling the Azure connectivity from your gateway, please verify that all devices are correctly connected and configured (you can check it with the diagnostic page of the integrated web server).



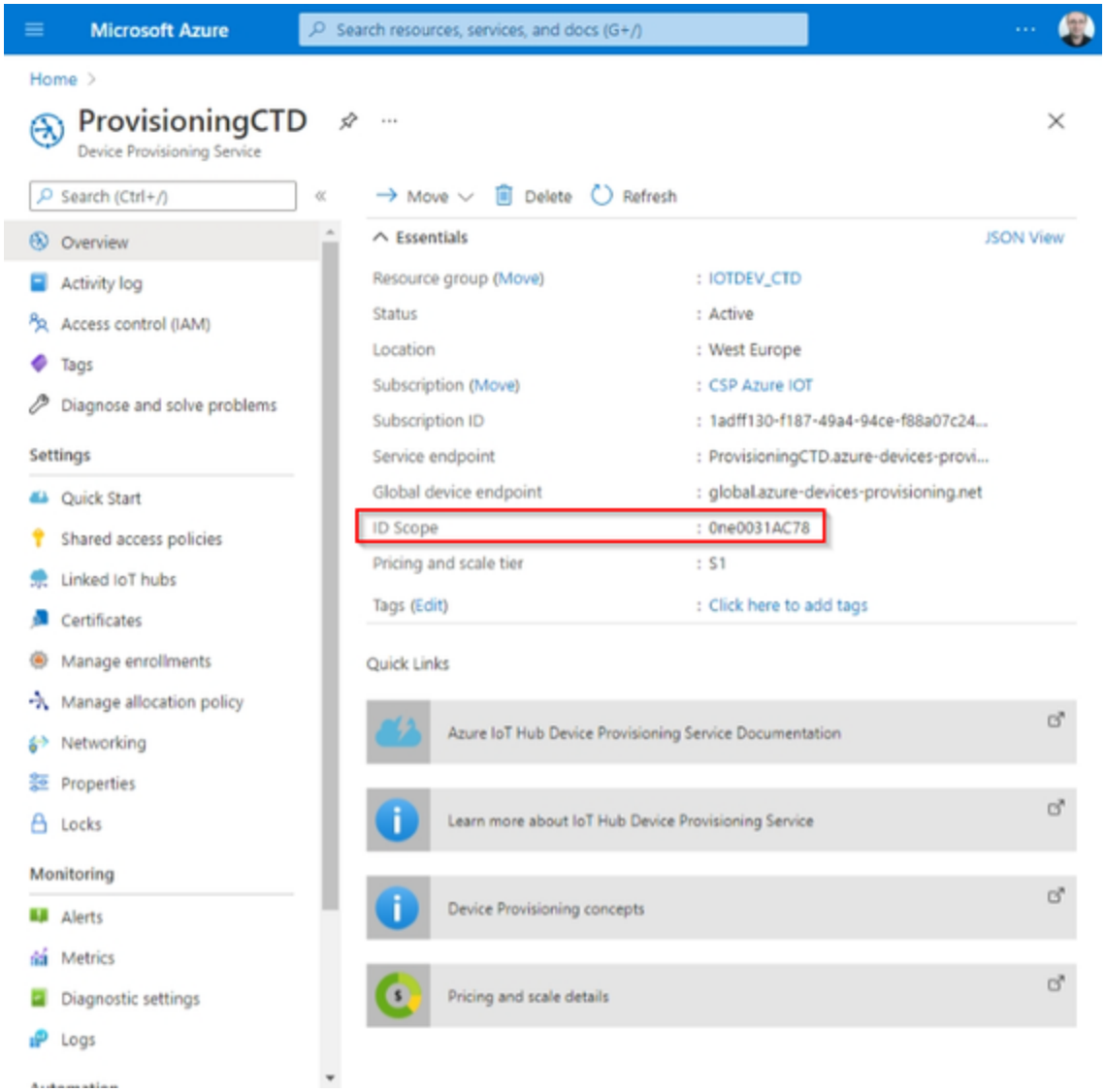
Configuration with DPS (Device Provisioning Service)

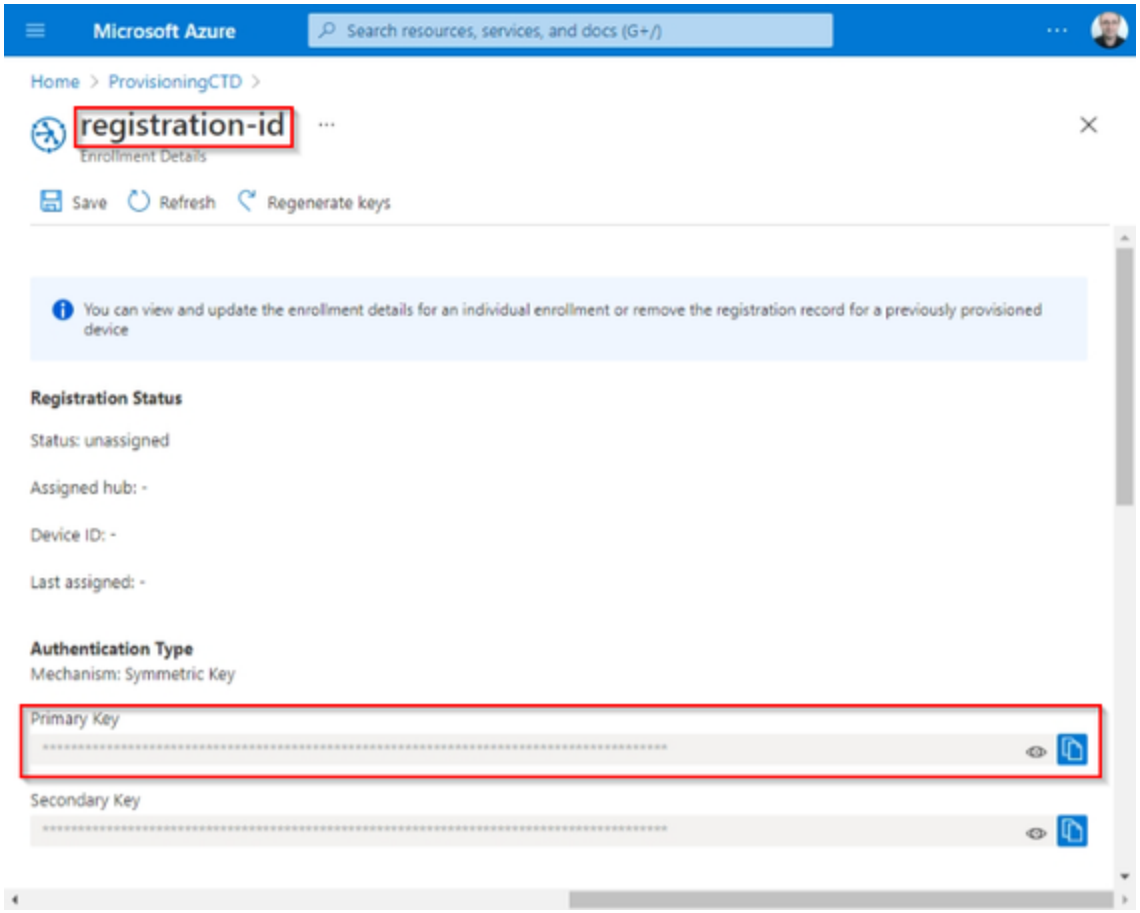
> The configuration through DPS is provided in the Socomec gateways to ensure the complete compatibility with Azure platform.
>
> The gateways can also be declared directly in the Azure IOTHub without need of DPS. In that case the provisioning mode “Manual” should be selected in the integrated web server (see below).

DPS with SAS Token authentication

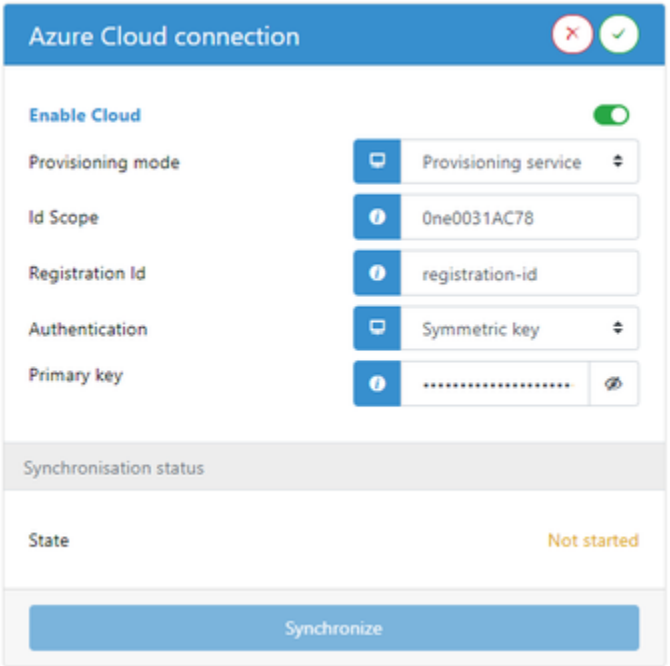
First step is to retrieve the parameters from your DPS instance.

- **ID Scope** of the DPS
- **Registration ID** of the enrollment
- **Primary key** of the enrollment


Microsoft Azure
Search resources, services, and docs (G+/)
Home
ProvisioningCTD
Device Provisioning Service
Search (Ctrl+/)
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Quick Start
Shared access policies
Linked IoT hubs
Certificates
Manage enrollments
Manage allocation policy
Networking
Properties
Locks
Monitoring
Alerts
Metrics
Diagnostic settings
Logs
Move
Delete
Refresh
Essentials
JSON View
Resource group (Move) : IOTDEV_CTD
Status : Active
Location : West Europe
Subscription (Move) : CSP Azure IOT
Subscription ID : 1adff130-f187-49a4-94ce-f88a07c24...
Service endpoint : ProvisioningCTD.azure-devices-provi...
Global device endpoint : global.azure-devices-provisioning.net
ID Scope : 0ne0031AC78
Pricing and scale tier : S1
Tags (Edit) : Click here to add tags
Quick Links
Azure IoT Hub Device Provisioning Service Documentation
Learn more about IoT Hub Device Provisioning Service
Device Provisioning concepts
Pricing and scale details



Then you can go into the integrated web server of the Socomec's gateway to enter the settings accordingly. Log in the page with profile "**Adminis trator**" or "**Cyber**", then go in ***Settings>Protocols>Data Push***.



Validate settings and click on "**Synchronize**" to start the synchronisation process with the DPS.

The push of telemetry data into the Azure IoT Hub will start automatically, according to the devices capabilities (energy meters, power measurements, …).

DPS with X.509 certificate authentication

The configuration is similar than SAS Token authentication. Get the parameters from your DPS and set the Socomec's device parameters.

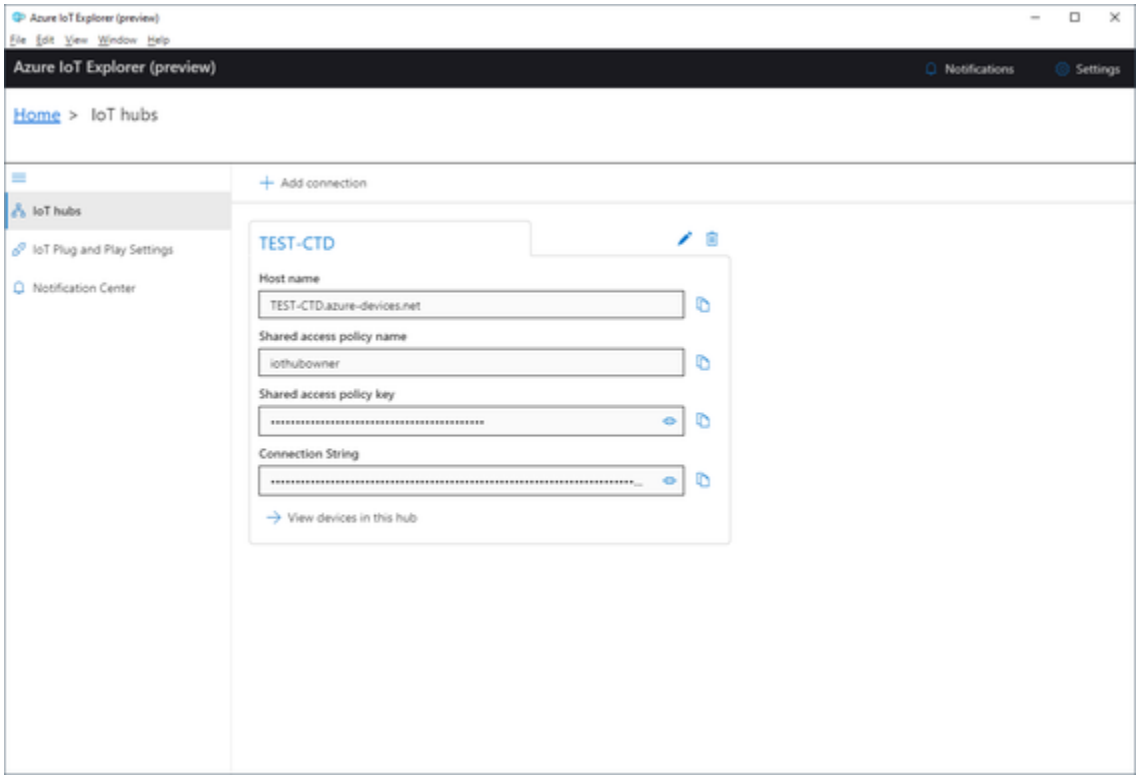
- **ID Scope** of the DPS
- **Registration ID** of the enrollment
- **Certificate** and **private key** generated from the certificate/key of the enrollment

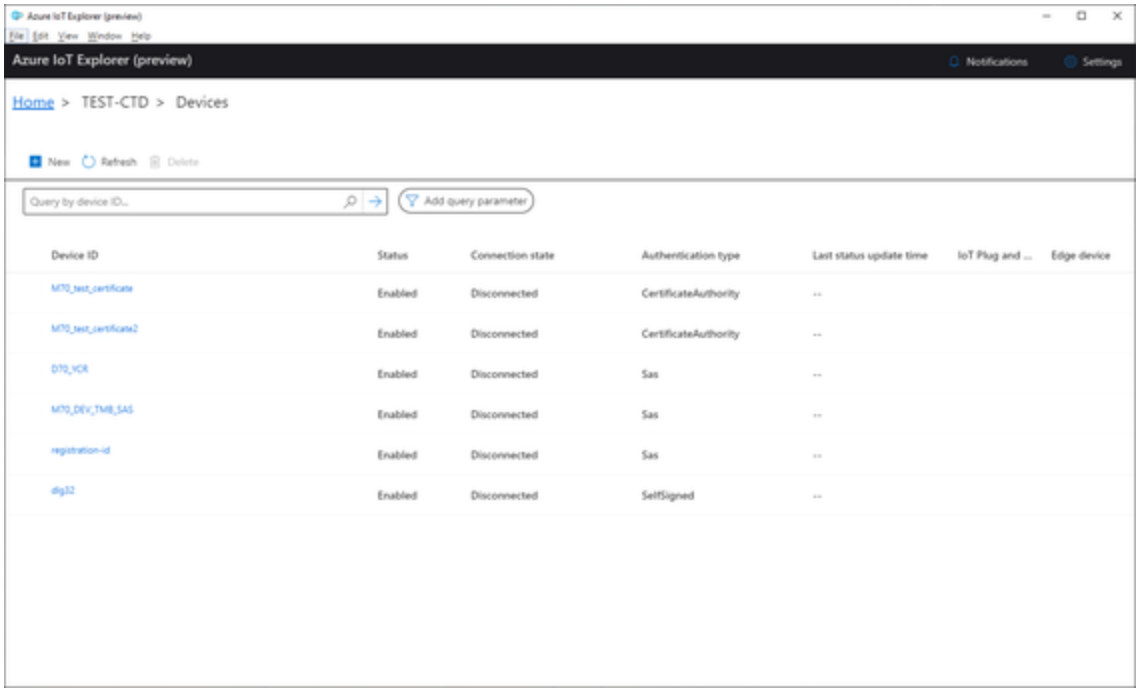
Step 3: Integration with Azure IoT Explorer

The Socomec gateways are compatible with Azure IoT Explorer. However, there is no "Direct method" or "Cloud to Device" capabilities on these gateways.

Please refers to Azure IoT Explorer documentation to get all details about this software.

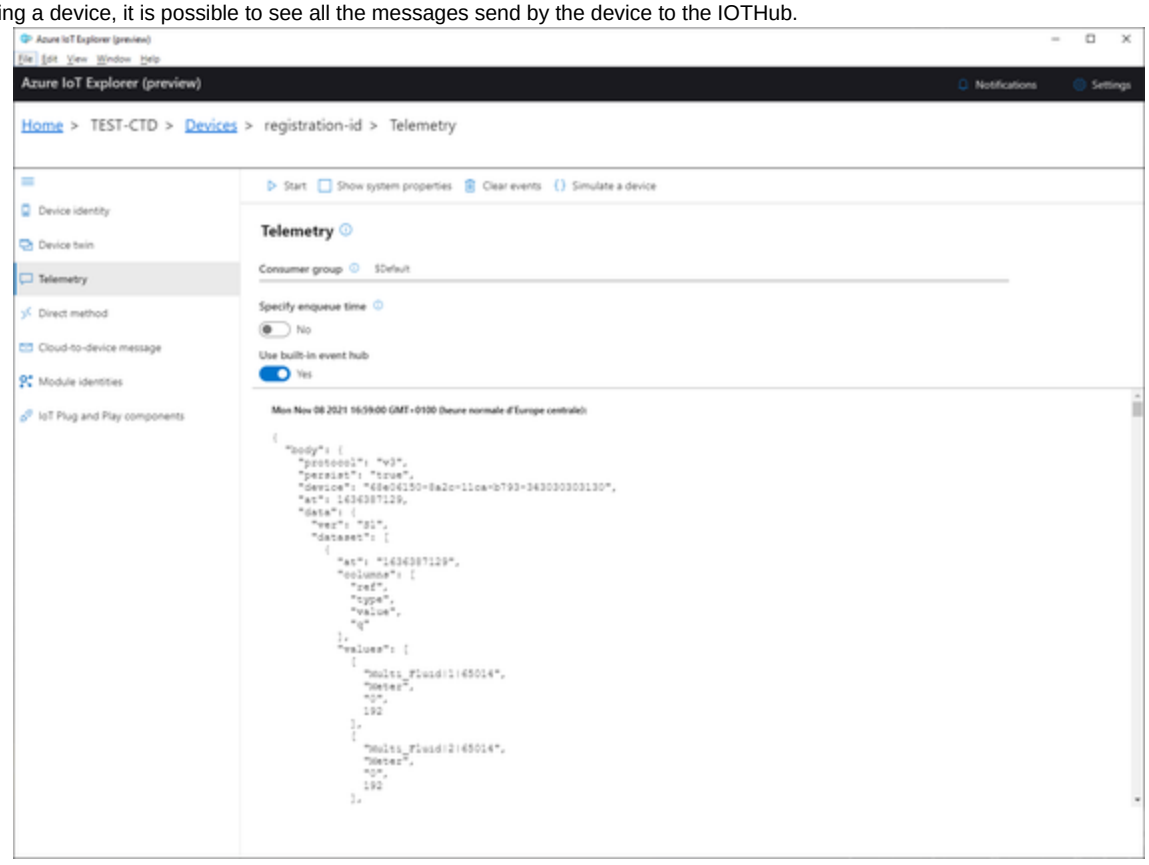
Connect Azure IoT Explorer to the Azure IOTHub





View telemetry messages

After selecting a device, it is possible to see all the messages send by the device to the IOTHub.

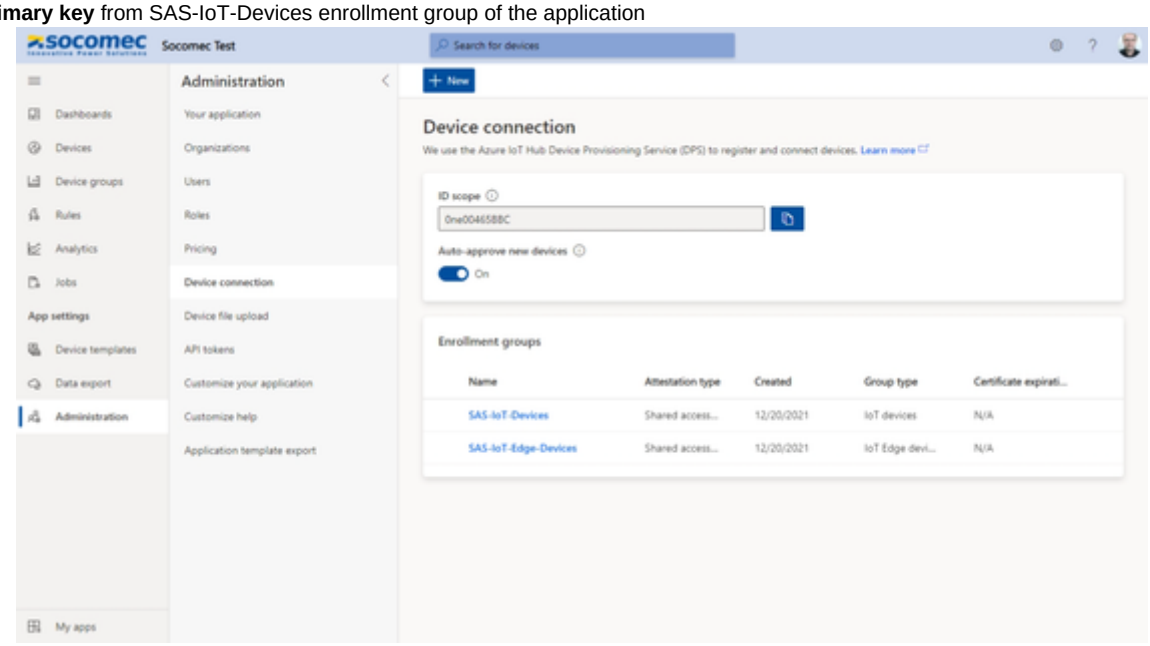


Step 4: Connect to Azure IoT Central

The Socomec gateways are fully compatible with Azure IoT Central.

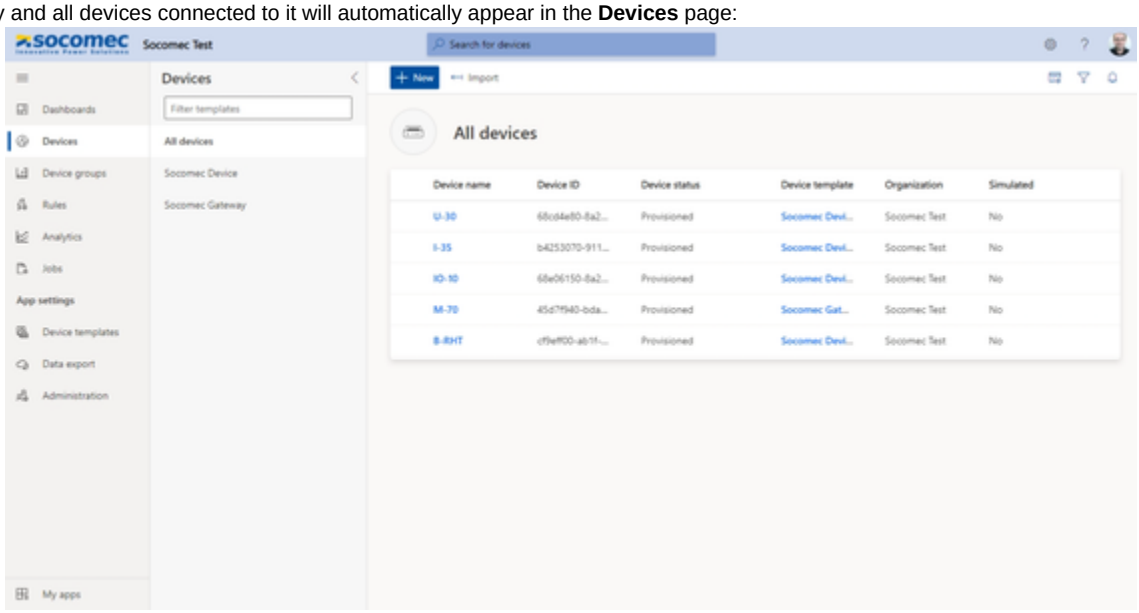
After creating an application into Azure IOT Central, get the connection parameters from **Administration**>**Device connection**:

- **ID Scope** of the application
- **Primary key** from SAS-IoT-Devices enrollment group of the application

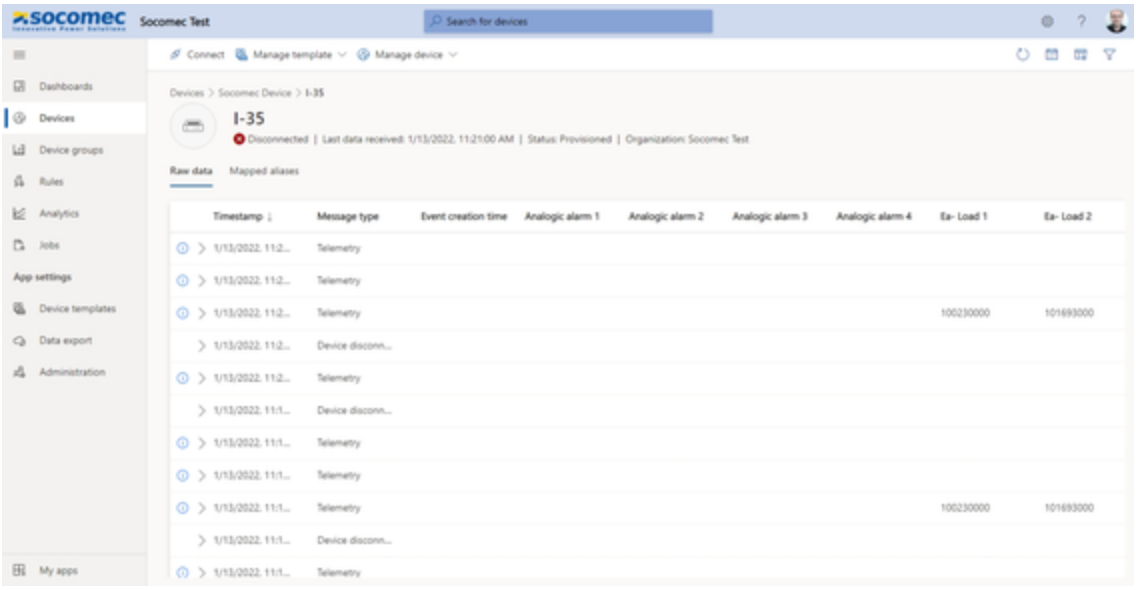


Then you can go into the integrated web server of the Socomec's gateway to enter the settings accordingly. Validate settings and click on "**Synch ronize**" to start the synchronisation process with the application DPS.

The gateway and all devices connected to it will automatically appear in the **Devices** page:



The push of **telemetry** and **property** data into the Azure IoT Hub will start automatically, according to the devices capabilities (energy meters, power measurements, …). The **device templates** are retrieved from the public space, so the data will be automatically decoded by Azure IOT Central application.



You can now customize the application with dashboards, analytics, etc…

Step 5: Additional Information

The Socomec's gateway send the message in JSON format. The complete description is available on demand, for any information please contact Socomec's support team.

Step 6 : Additional Links

Please refer to the below link for additional information for Plug and Play

- Manage cloud device messaging with Azure-IoT-Explorer
- Configure to connect to IoT Hub
- How to use IoT Explorer to interact with the device