AWS IOT CUSTOM (MQTT) AND DEVICE CONFIGURATION

GUIDE

**Contents**

[1. General information 1](#_Toc144133001)

[2. Create IoT Hub 3](#_Toc144133002)

[2.1. Basics 4](#_Toc144133003)

[3. Add device 6](#_Toc144133004)

[4. Primary and secondary keys 10](#_Toc144133005)

[5. Configuration 12](#_Toc144133006)

[6. Certificate creation and upload 14](#_Toc144133007)

[6.1. Converting certificate to .pem format 14](#_Toc144133008)

[6.2. Upload certificate to device 19](#_Toc144133009)

[7. Certificate key saving to device 20](#_Toc144133010)

[7.1. Data sending 21](#_Toc144133011)

[8. Checking received data in Azure IoT Explorer 23](#_Toc144133012)

[8.1. Downloading Azure IoT Explorer 23](#_Toc144133013)

# General information

Firmware version: 03.28.06.Rev.280

Hardware revision: 288

Configurator: 1.7.45\_B.3.28\_R.11

Notes: This guide does not contain any information how to store received MQTT packets in the Azure.

# Create IoT Hub

Login to <https://portal.azure.com/>

Press  and select – **create new resource**

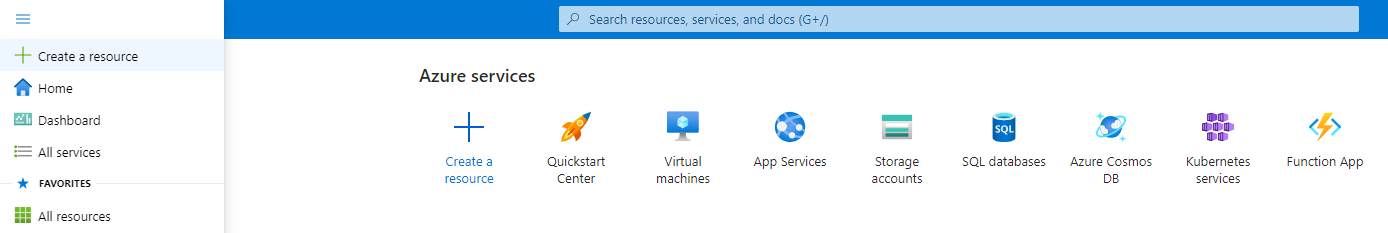


Figure 1 Create new resource

Select **Internet of things** in the Categories on the left

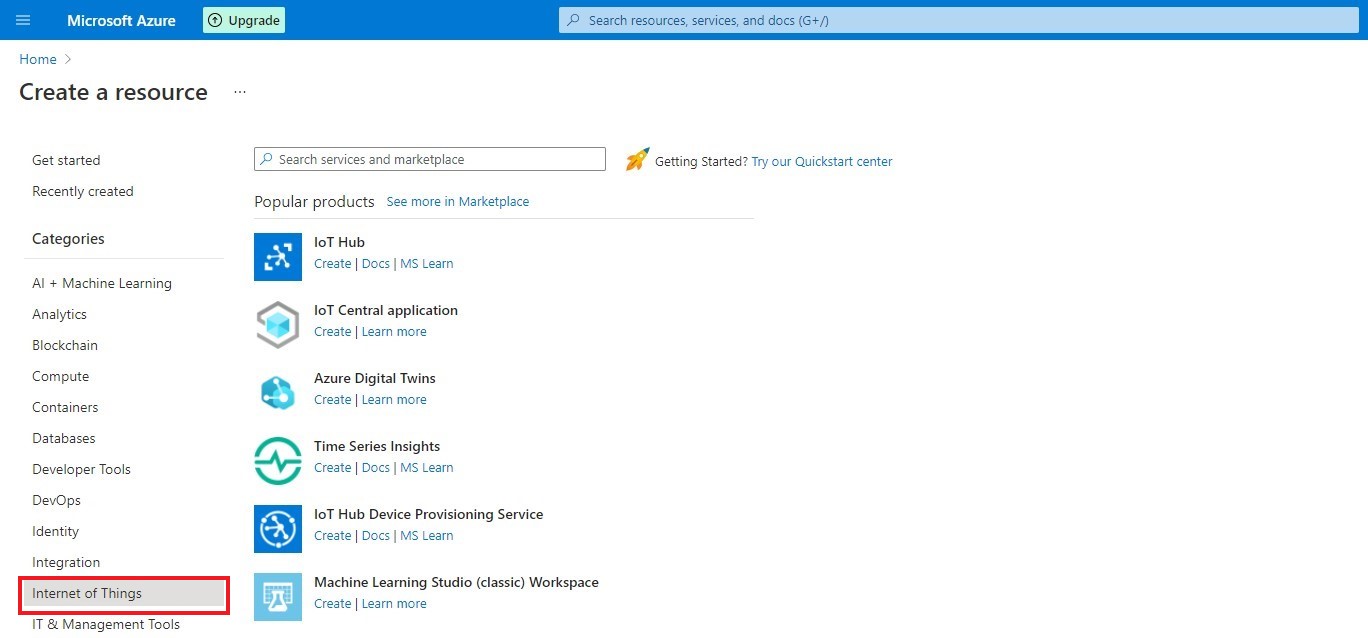


Figure 2 Selecting IoT

Press **Create** near the icon.

## Basics

In the **Basics** tab choose your **subscription**. Create a new **Resource group**. Enter **IoT hub name** (Can be any created name). Select **Region** that is closest to you.

Choose the wanted **Tier, Free** **tier** should be used for testing purpose, alternatively use **standard**. (You can find all the necessary information about tiers when you click **Comapare tiers** below option box).

Then choose your **Daily message limit** according to your needs (You can find all the necessary information about **Daily message limit** when you click **See all options** below option box).

Press: **Review + create**

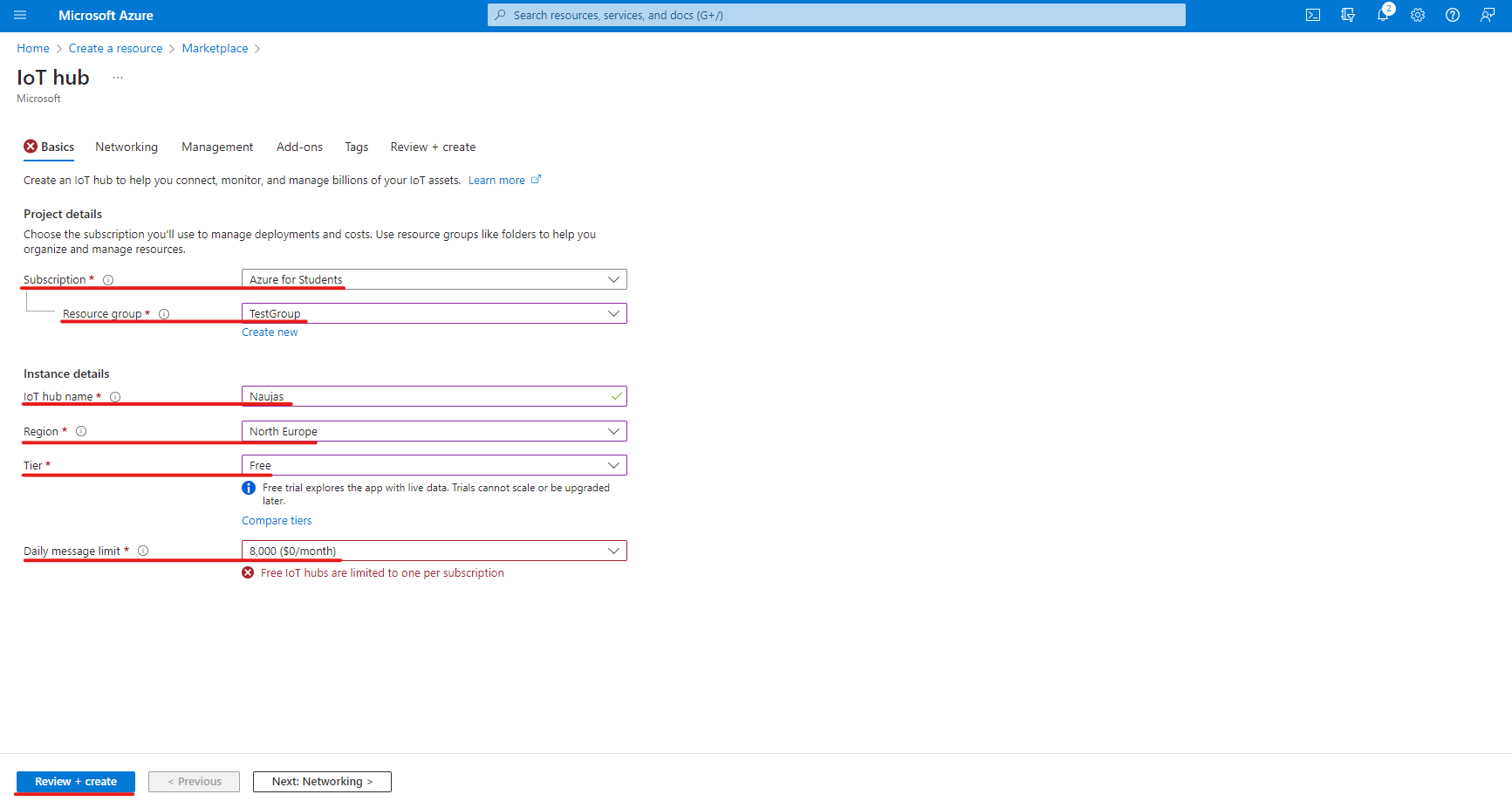


Figure 3 Basics parameters

Check if all the parameters are as you intended and click **Create.**

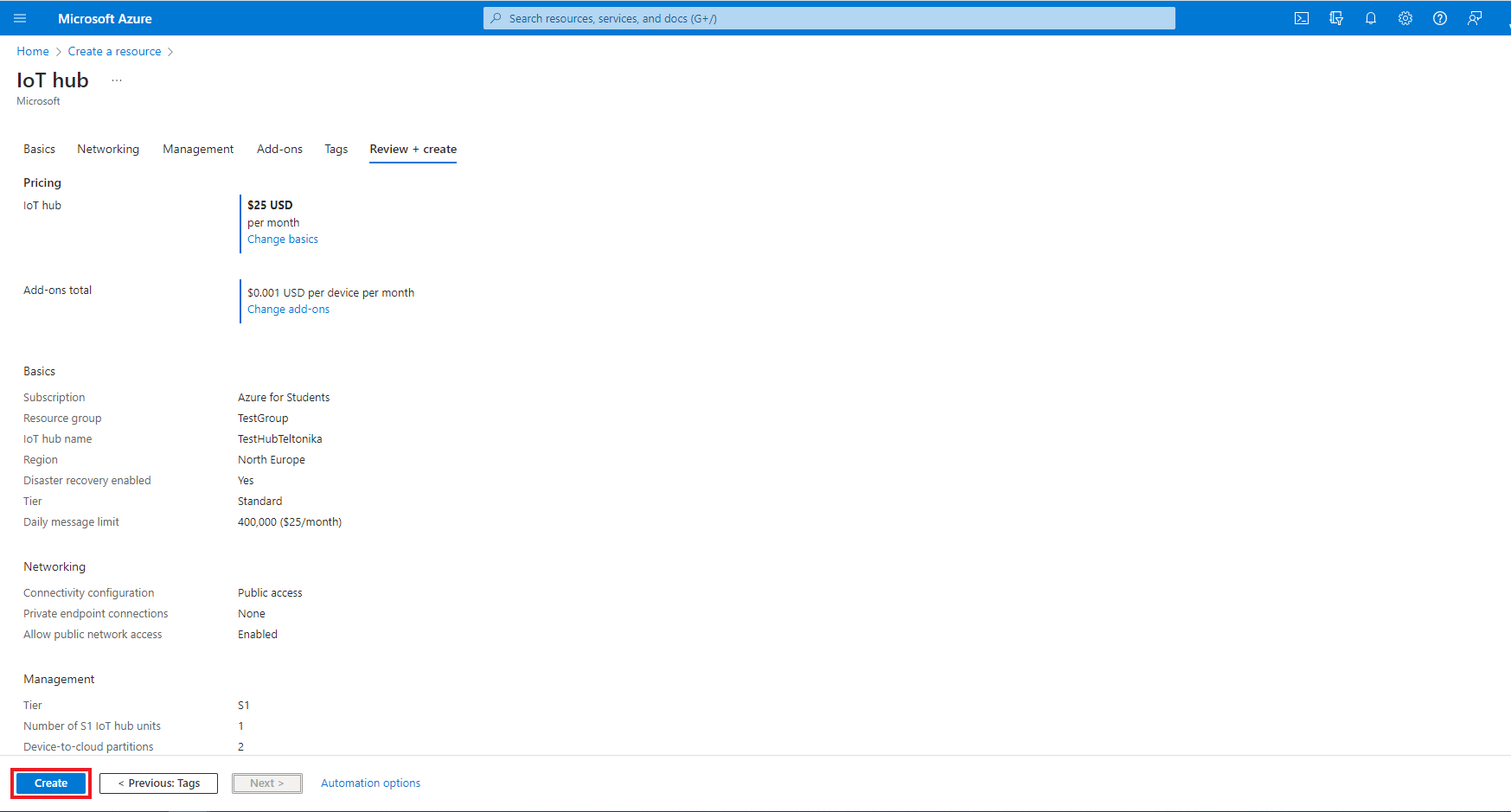


Figure 4 Creating IoT hub

# Add device

Press  , **Home** and click on your created IoT Hub.

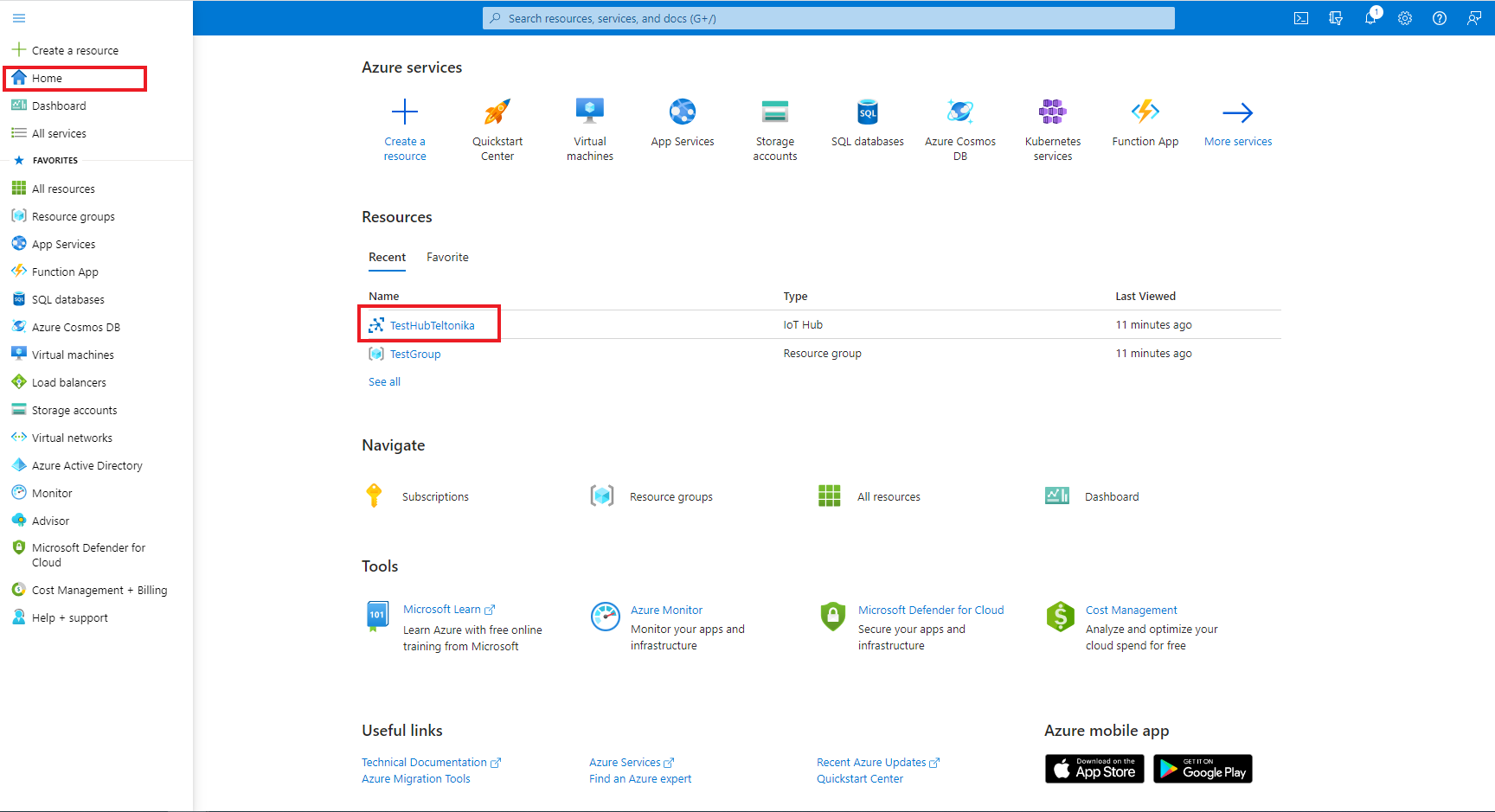


Figure 5 Selecting IoT Hub

Copy hostname and press **devices** In the left menu.

|  |  |
| --- | --- |
|  | **If you see a warning:** |
|  | * This resource uses a certificate on the Baltimore CyberTrust Root which will expire in 2025 and must be migrated to the DigiCert Global G2 root.   Go to: **Migrate to DigiCert Global G2** section at the bottom of this tutorial. |

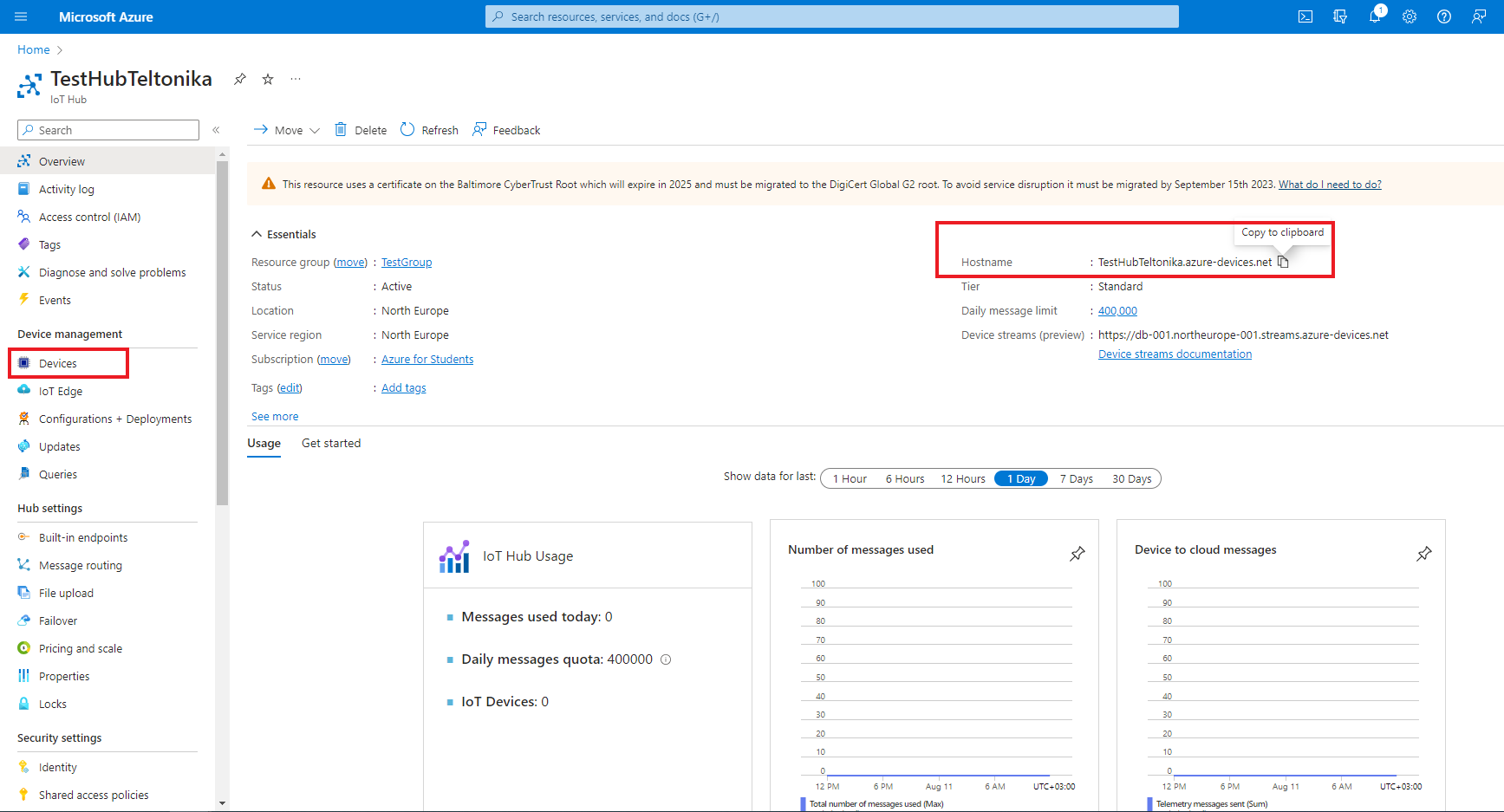


Figure 6 Domain and devices

Select **Add Device** in **Devices** tab.

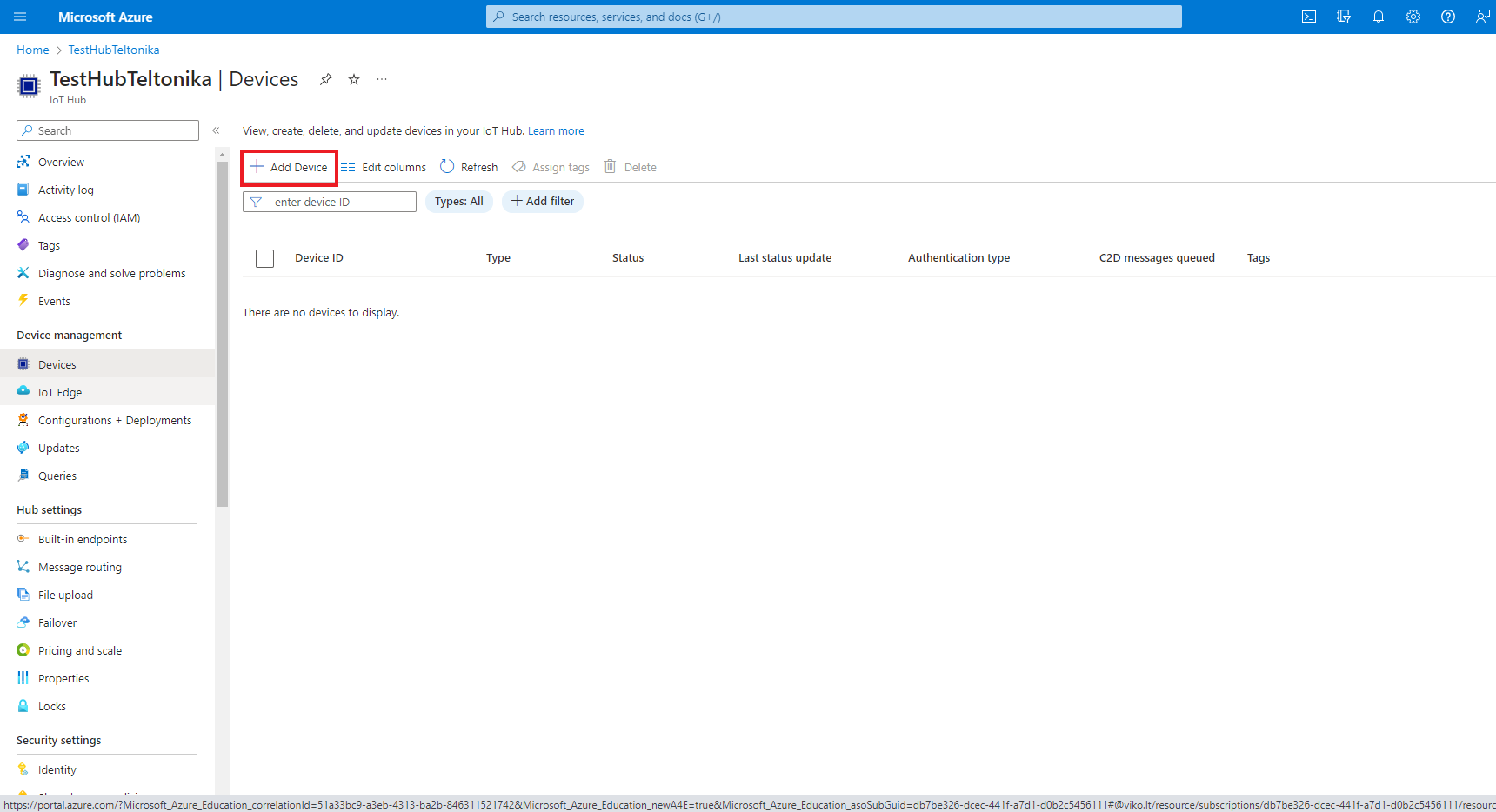


Figure 7 Add Device

Once you are inside **Create a device** tab:

Enter your device IMEI in the **device ID** field.

Other fields here should be left default

Authentication type: Symmetric key Connection this device to an Iot Hub: Enabled

Press **save**.

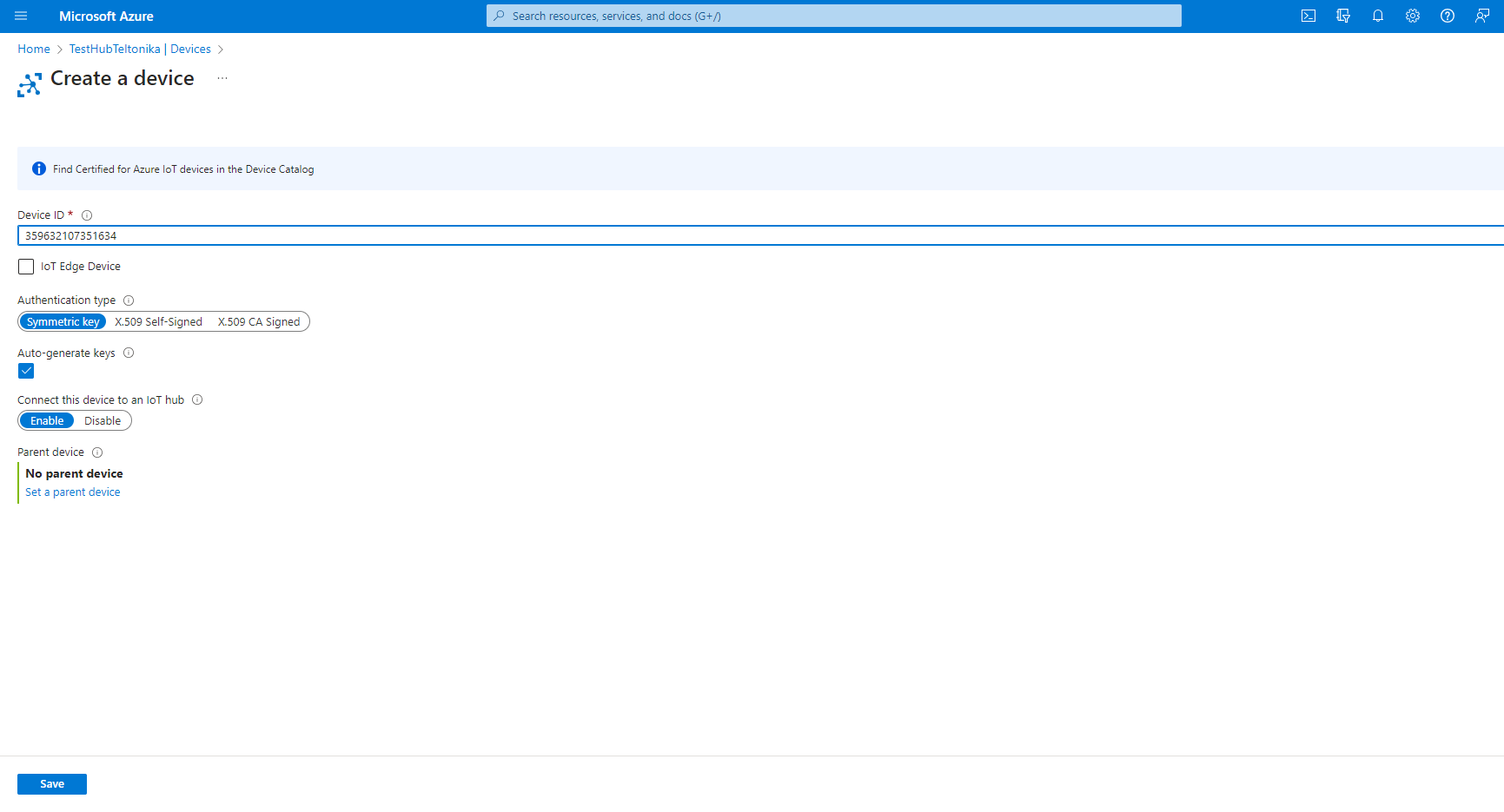


Figure 8 Creating a device

# Share access policies

To get your primary and secondary keys go to **Shared access policies,** change **Connect using shared access policies** to **Allow** and click on **iothubowner**.

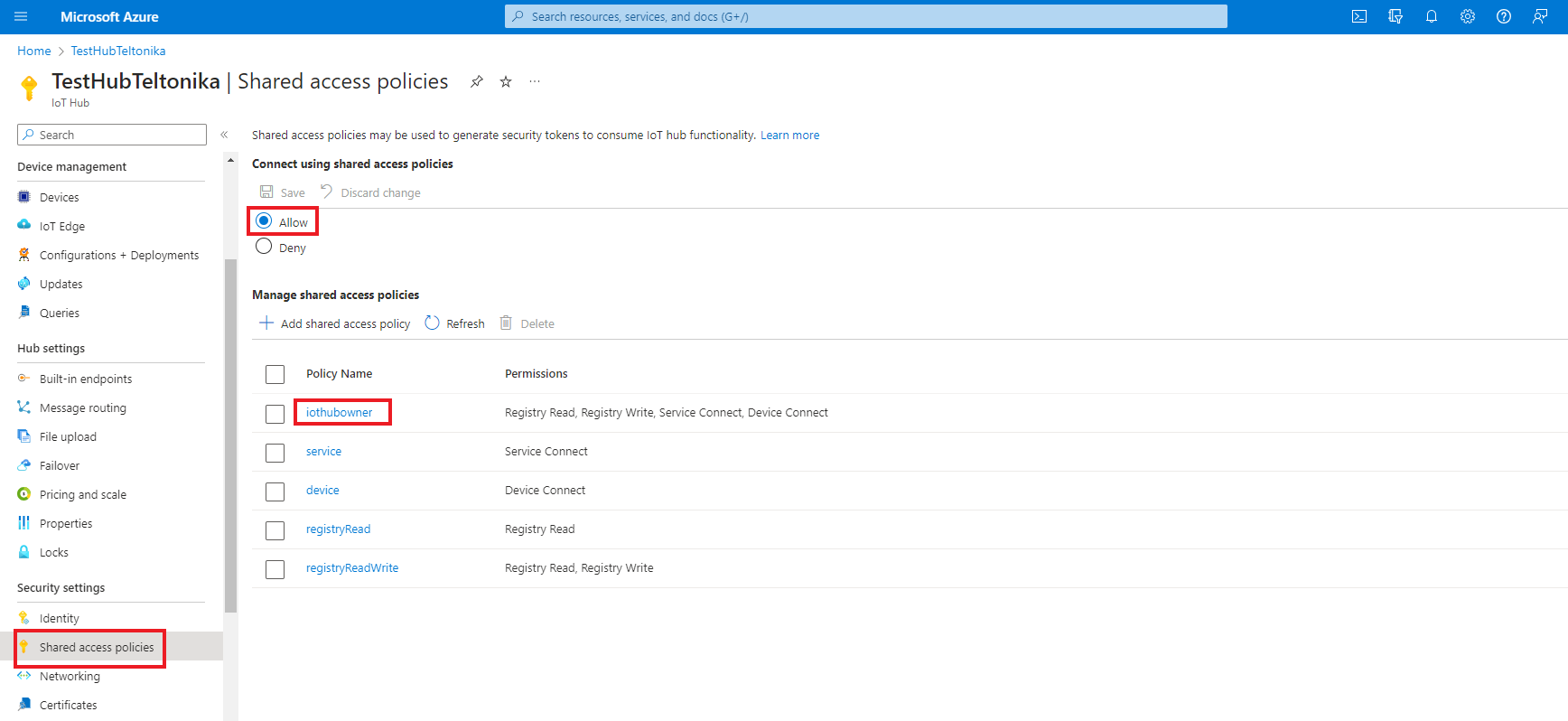


Figure 9 Shared access policies

An **iothubowner** tab will pop out on the right.

Copy:

1. Primary key
2. Secondary key
3. “iothubowner”

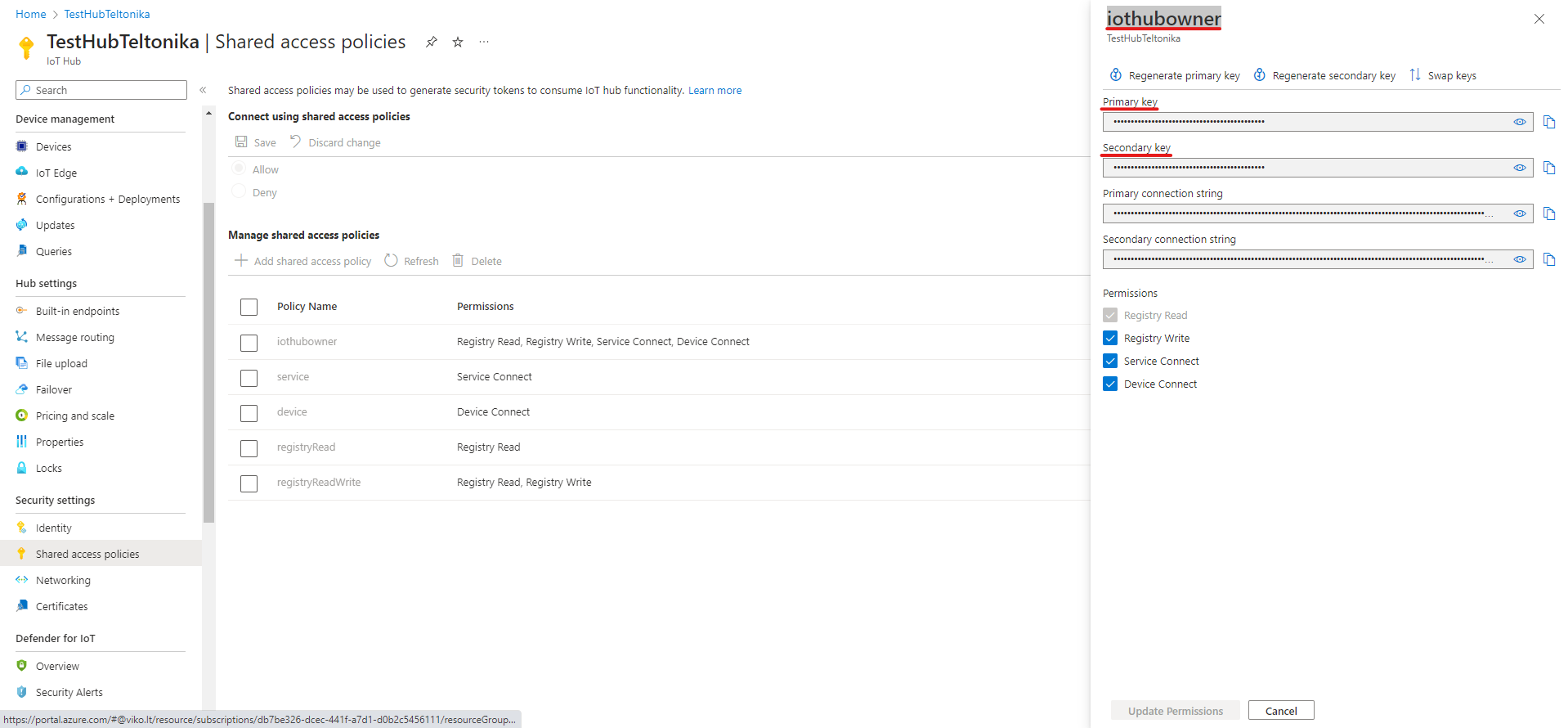


Figure 10 Saving keys

# Configuration

In the ***GPRS tab****,* under ***Server Settings***select:

1. Domain – **Hostname** (copy here the host name from your Iot Hub overview window in Azure)
2. Port: ***8883***
3. Protocol – ***MQTT***
4. TLS Encryption – ***TLS/DTLS***

In the ***GPRS tab****,* under ***MQTT Settings***select:

1. MQTT Client type – **Azure IoT**
2. Device ID: ***IMEI***
3. Primary SAS key – ***Primary key*** *from* ***‘iothubowner’*** *shared access policy*
4. Secondary SAS key – **Secondary *key*** *from* ***‘iothubowner’*** *shared access policy*
5. SAS Policy Name – ***iothubowner***

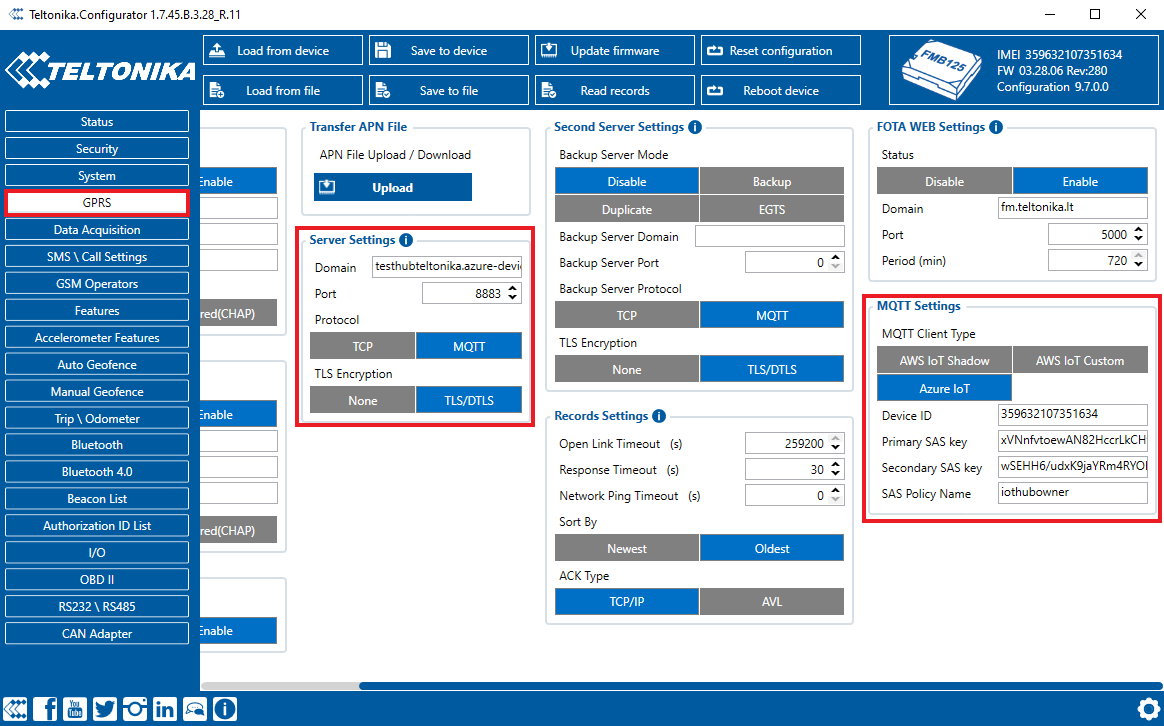


Figure 11 Device configuration

# Certificate creation and upload

## Converting certificate to .pem format

Download **DigiCert Global Root G2** and put it inside a new folder: [Download DER/CRT](https://cacerts.digicert.com/DigiCertGlobalRootG2.crt)

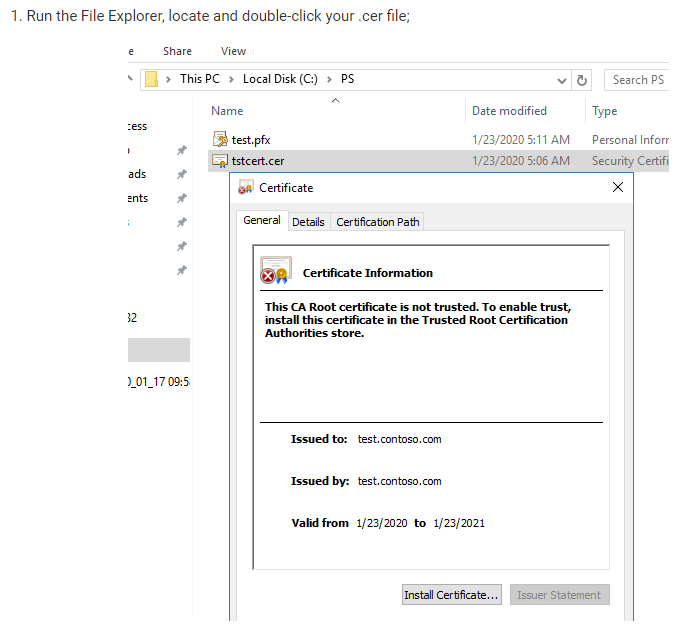


Figure 12 Certificate creation 1

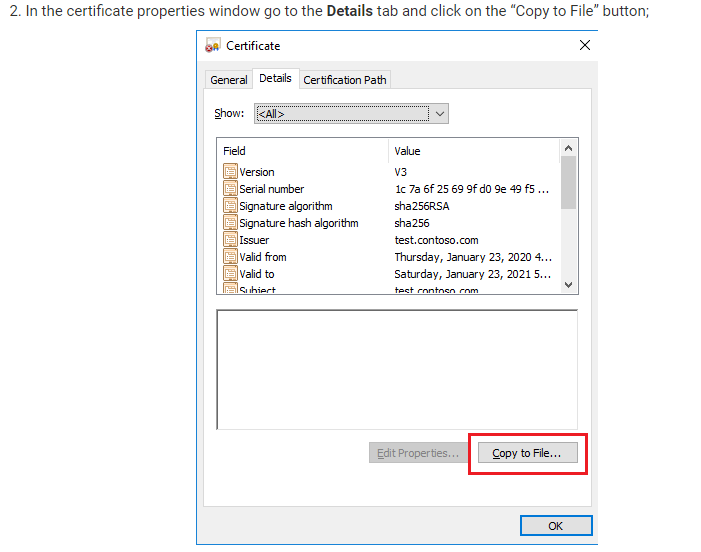


Figure 13 Certificate creation 2

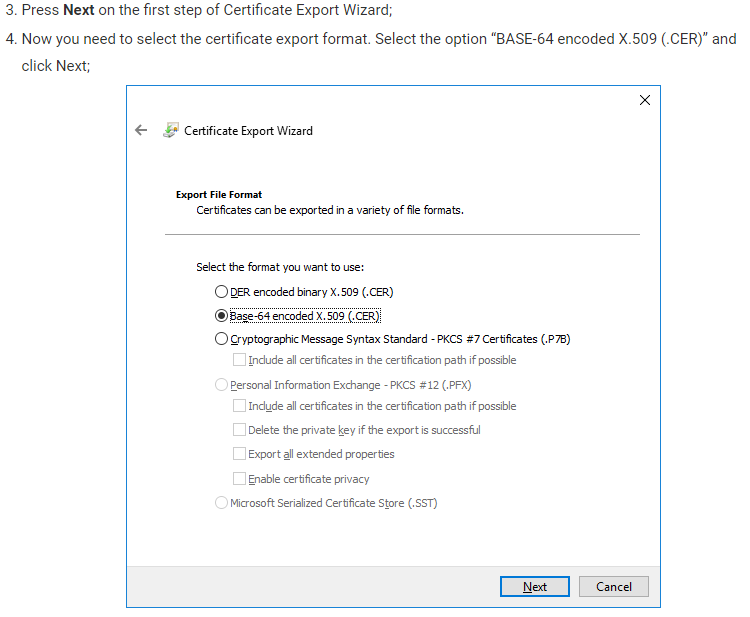


Figure 14 Certificate creation 3

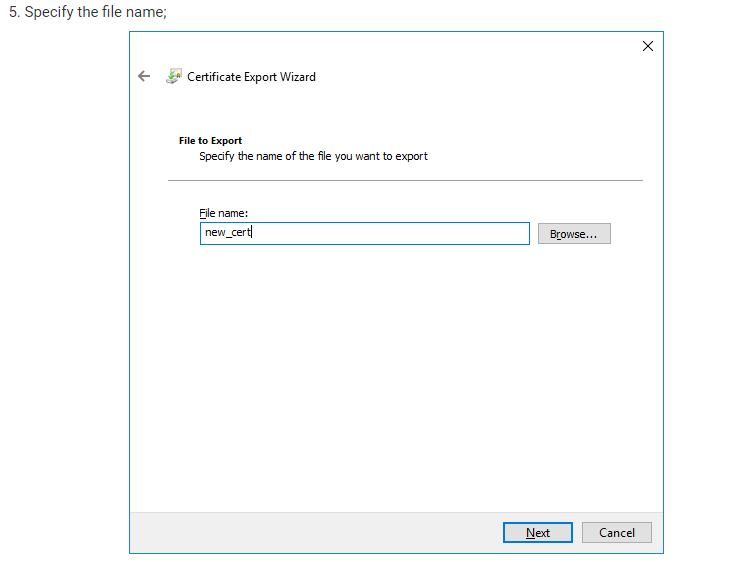


Figure 15 Certificate creation 4

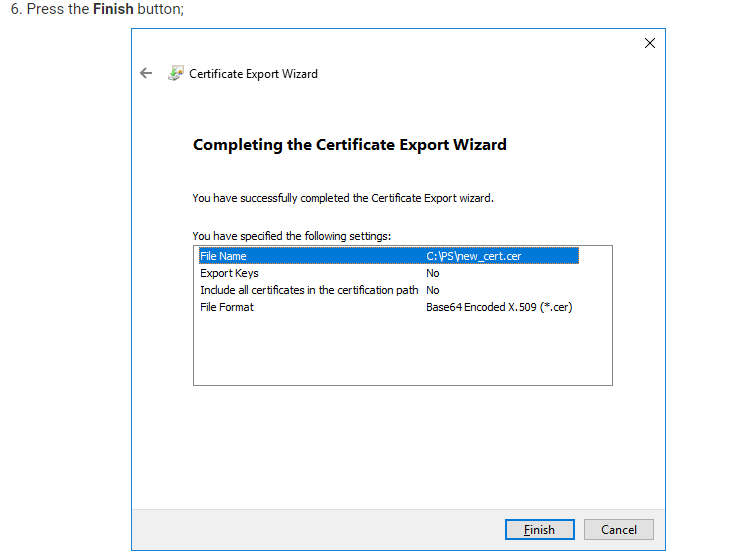
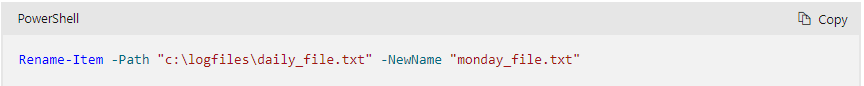


Figure 16 Certificate creation 5



Certificate.pem will be created.

Upload the file you have created to the device using configurator > Security > Certificate > upload

## Upload certificate to device

# Data sending

# Trigger a high priority event so that device would start to send data to the server.

In the device configurator screen check for the Status > GSM Info > Records Sent records count.

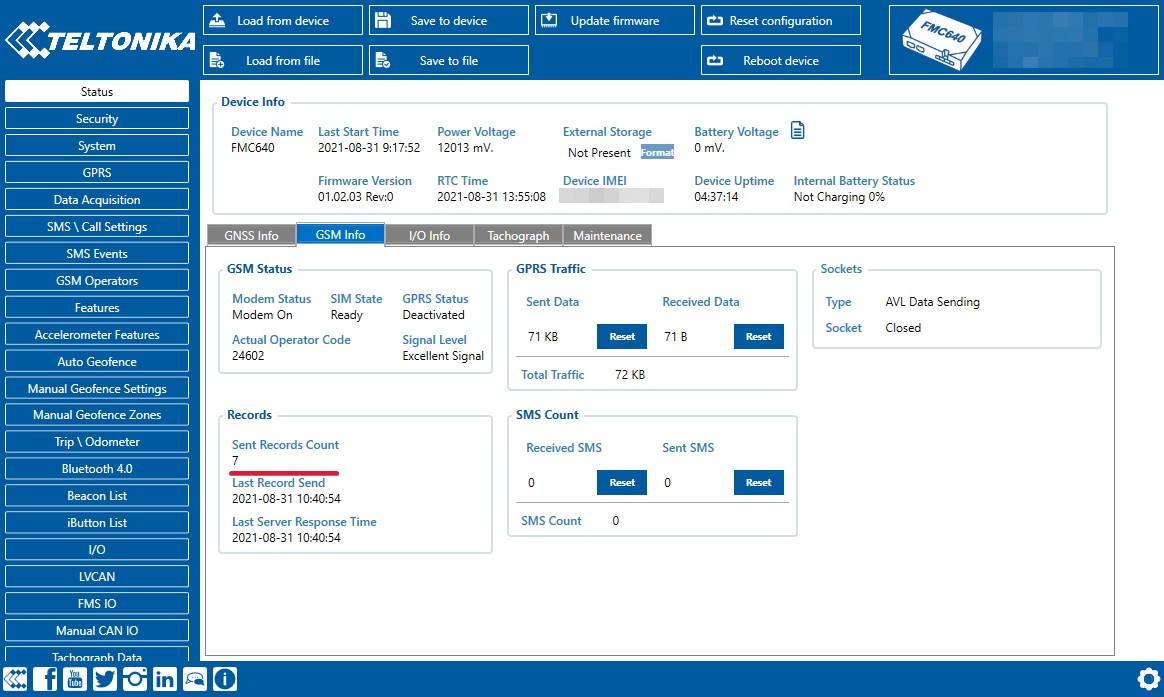


Figure 17 Sent records count

On the Azure service > IOT hub > Overview there is a Device to cloud chart that will show the records received. Be aware - this window has noticeable delay.

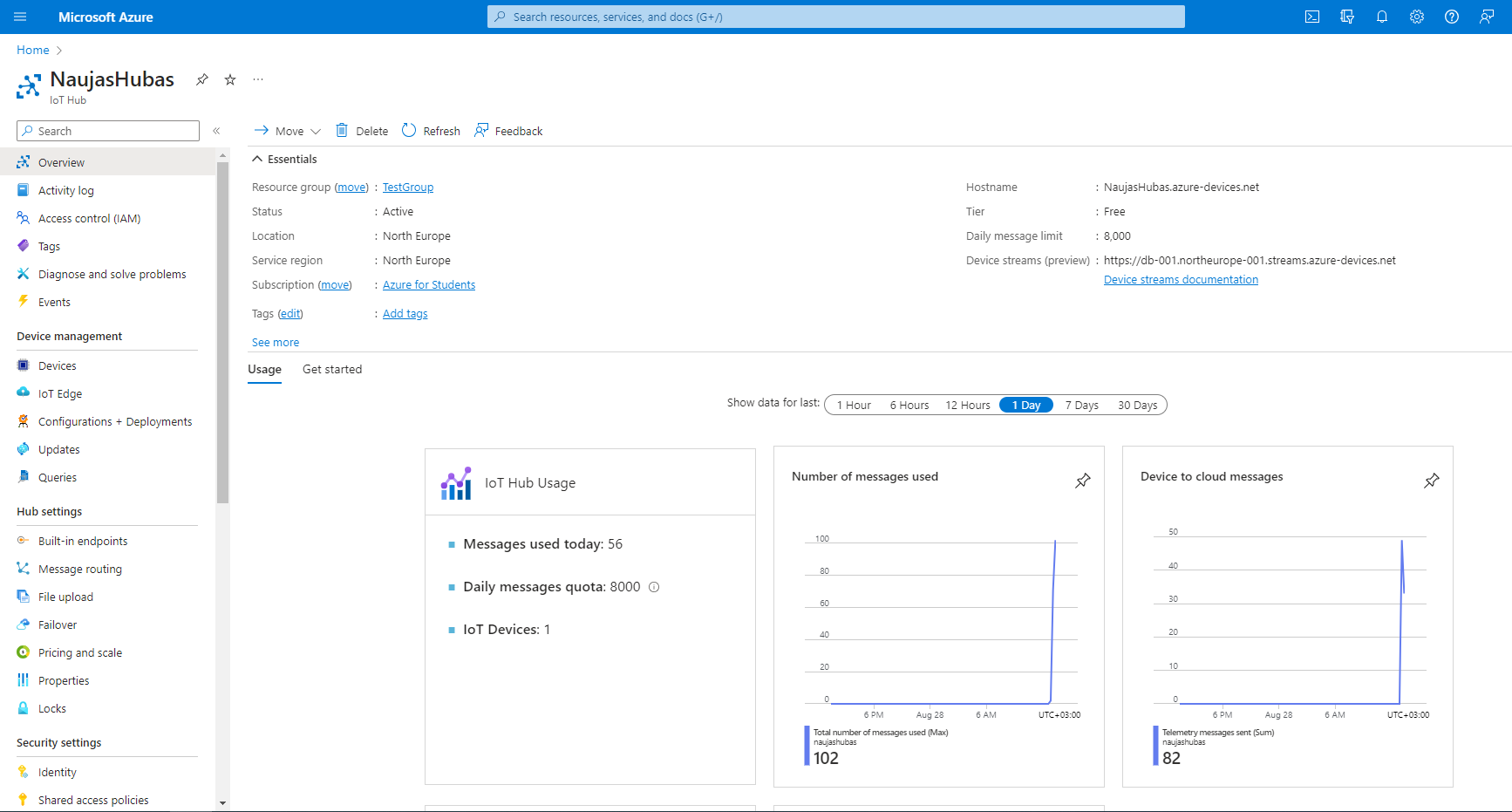


Figure 18 IoT hub overview

# Checking received data in Azure IoT Explorer

## Downloading Azure IoT Explorer

The data received from the device can be found in the **Azure IoT Explorer**

Go to: <https://github.com/Azure/azure-iot-explorer/releases>  
Find the latest version and download the file with .msi header:

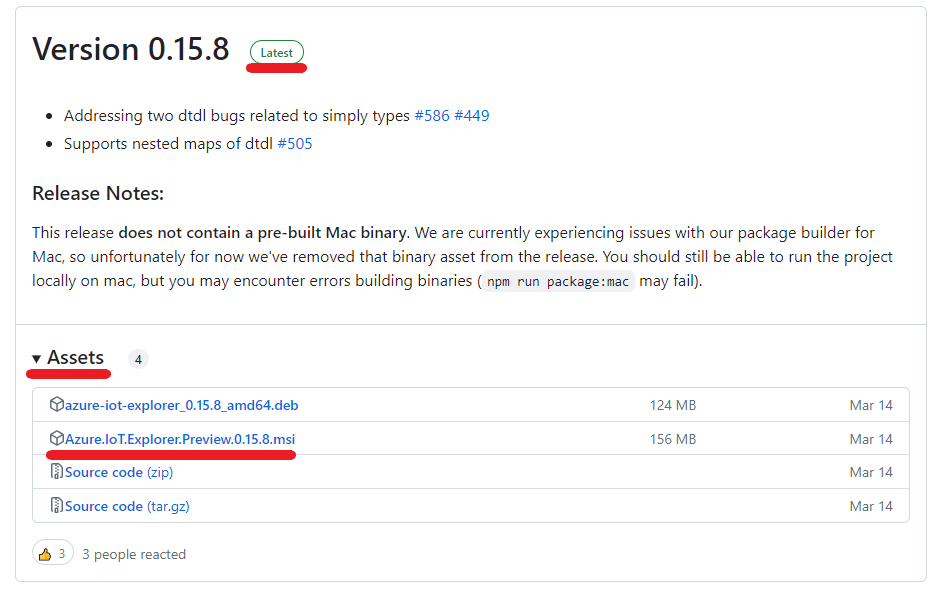


Figure 19 Azure IoT explorer 1

After opening Azure explorer click:

1. **IoThubs**
2. **Add connection**

In the pop-up bar enter **primary connection string** which you can get from **Shared access policies** which was explored in section 4.

Click **save** after completion.

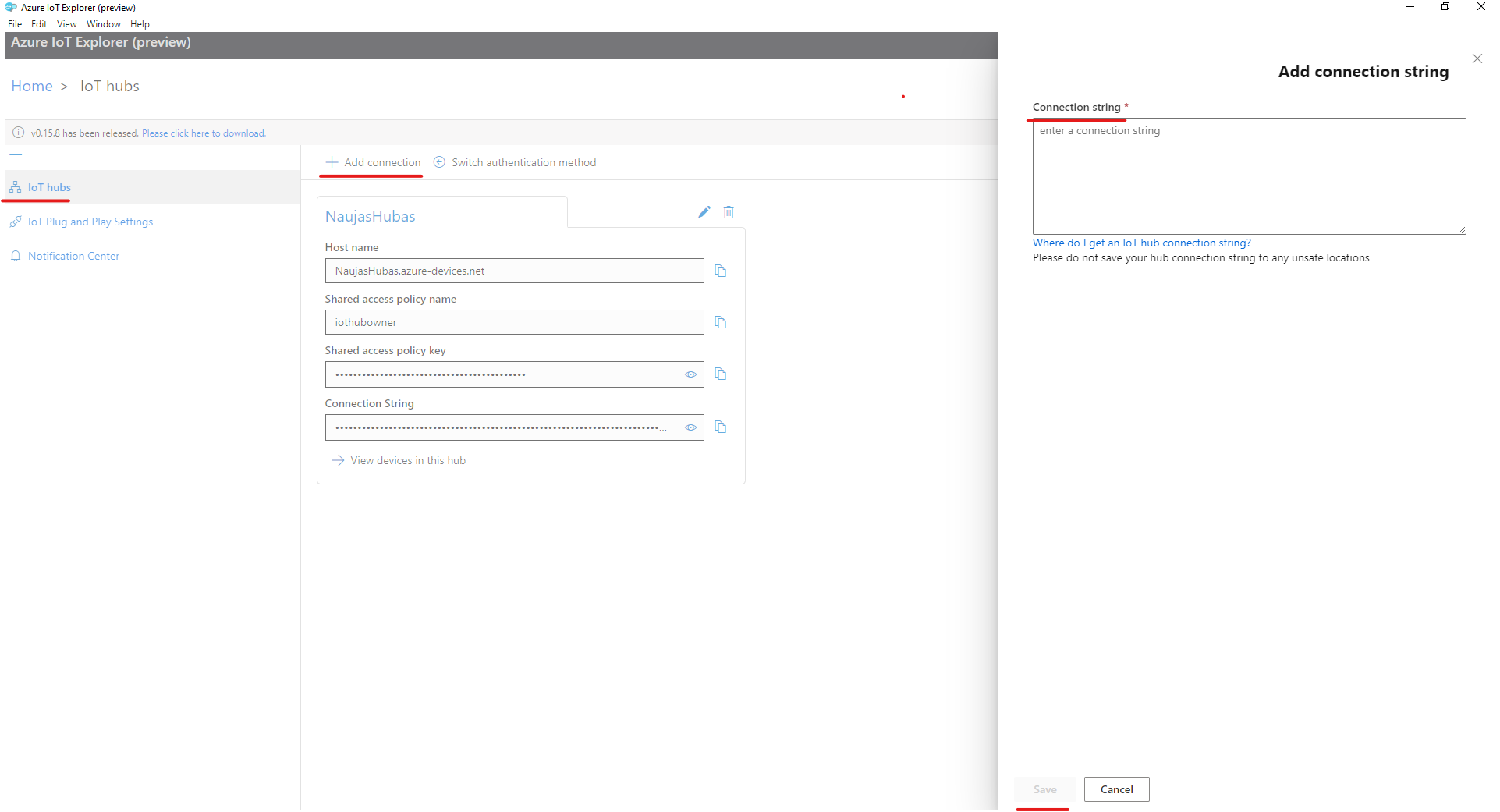


Figure 20 Azure IoT explorer 2

Click the Name of your hub which will be in blue color.

Select the device that you want to explore by **clicking** on it’s **IMEI.**

On the following window click **Telemetry** and the **Start.**

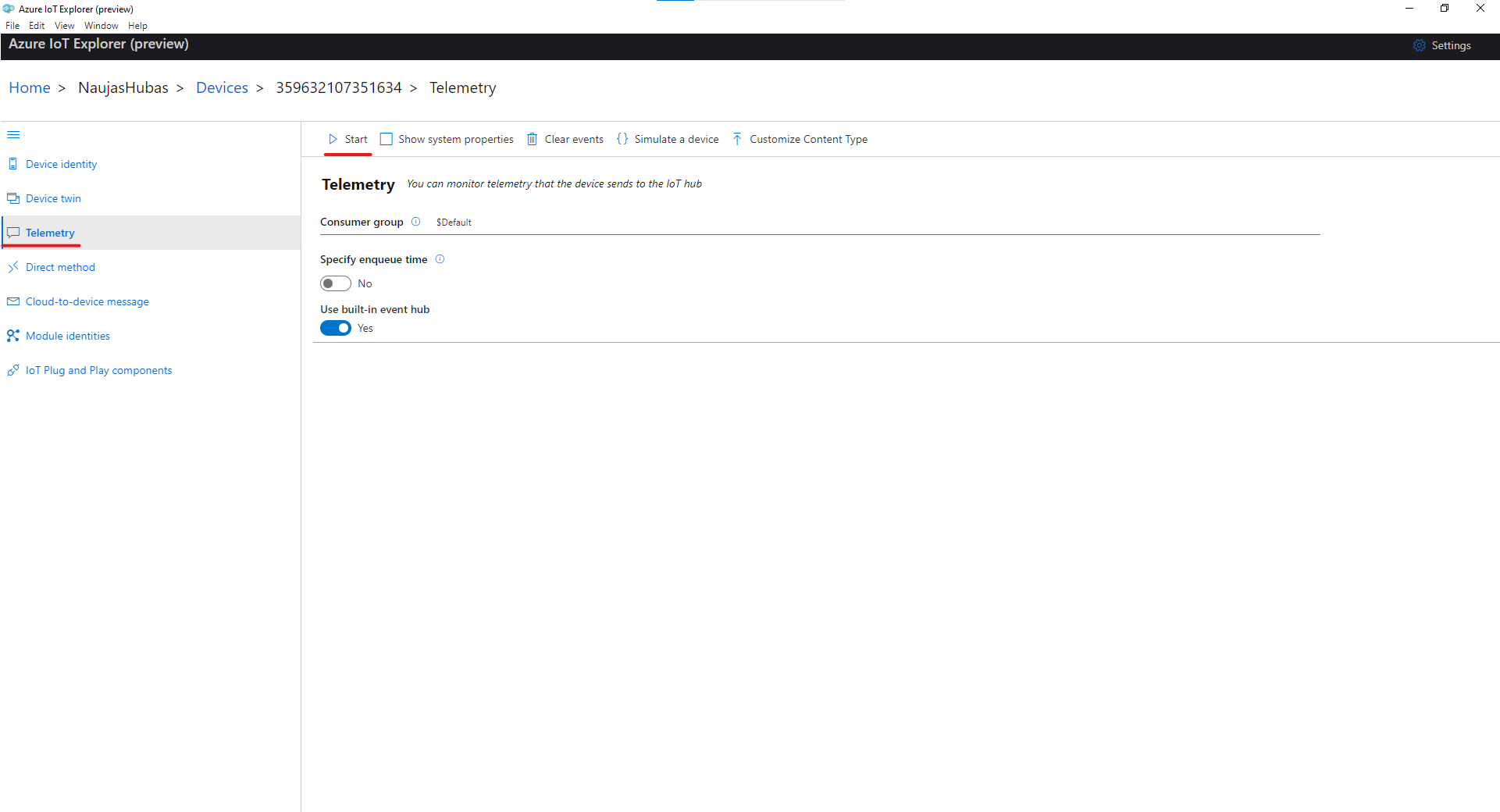


Figure 21 Azure IoT explorer 3

Example of data sent in JSON format:

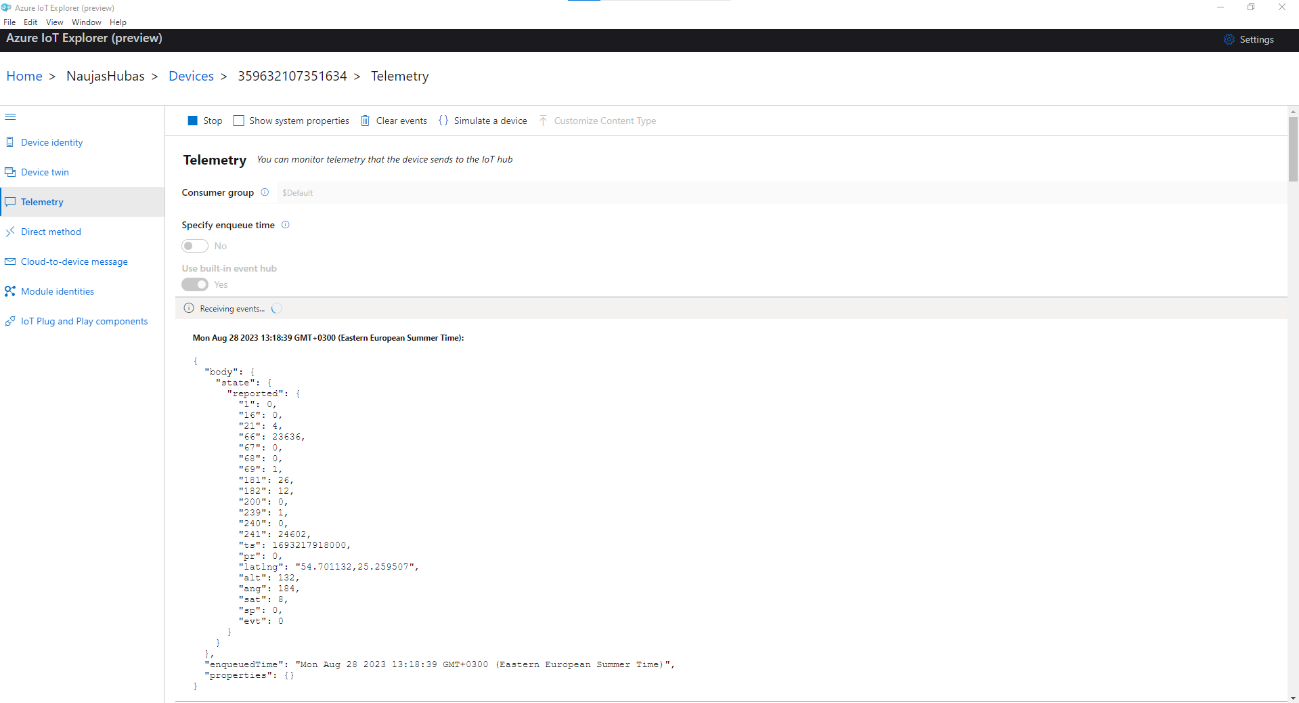


Figure 22 Records JSON

Example of data sent in Codec 8 format:

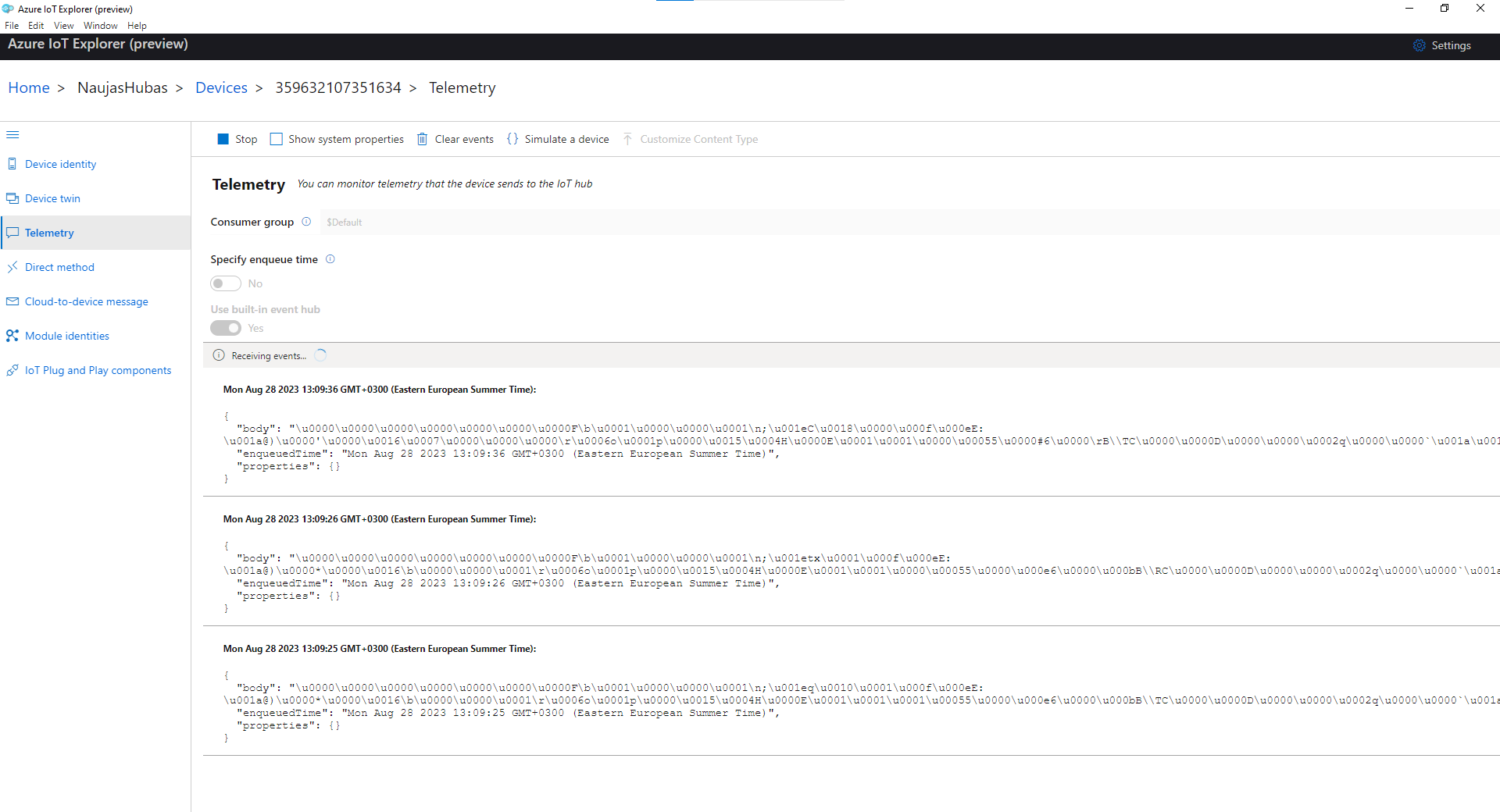
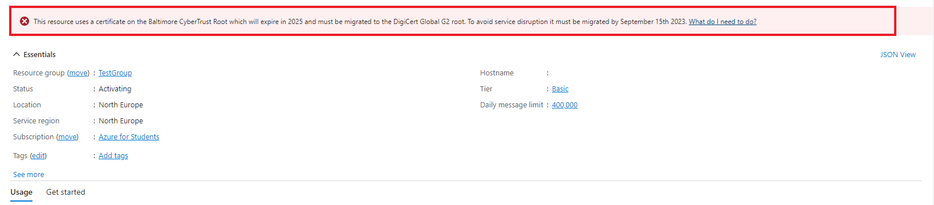


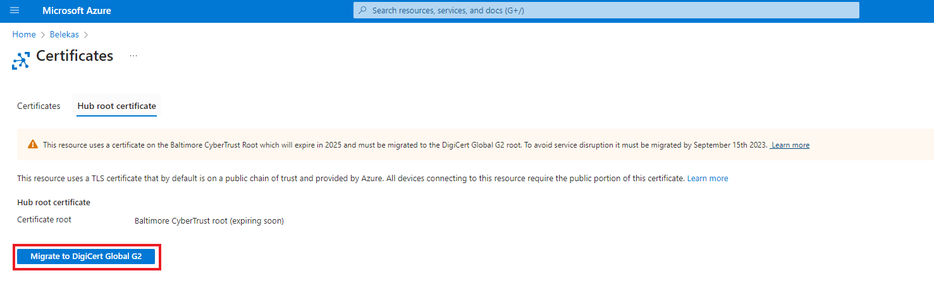
Figure 23 Records Codec 8

# Migrate to DigiCert Global G2 (If you saw a warning in overview)

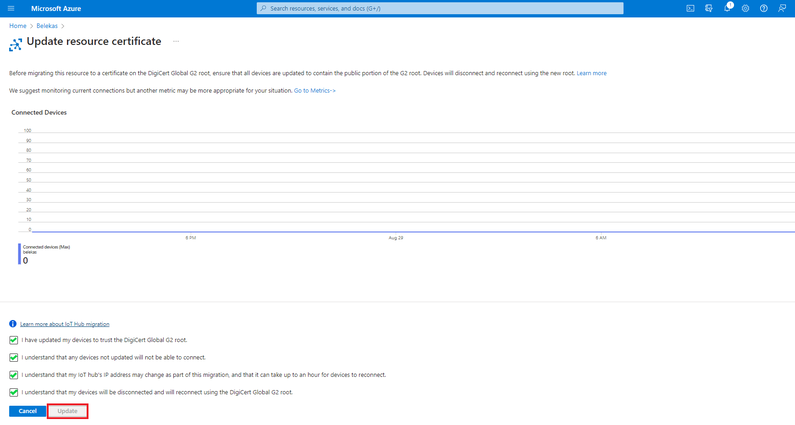
# In overview window click on the red error message



# In the following window click Migrate to DigiCert Global G2



On the next window check all the boxes and click **Update**



Migration may take up to a minute. You can now continue with the instructions from where you left off.