

# AWS IOT CUSTOM (MQTT) AND DEVICE CONFIGURATION GUIDE

## Contents


1.	General information .....	2
2.	Create IoT Hub .....	3
2.1.	Basics .....	4
3.	Add device .....	6
4.	Share access policies .....	10
5.	Configuration .....	12
6.	Certificate creation and upload .....	13
6.1.	Converting certificate to .pem format .....	13
6.2.	Upload certificate to device .....	18
7.	Data sending .....	19
8.	Checking received data in Azure IoT Explorer .....	21
8.1.	Downloading Azure IoT Explorer .....	21
9.	Migrate to DigiCert Global G2 (If you saw a warning in overview) .....	25
	In overview window click on the red error message .....	25
	In the following window click Migrate to DigiCert Global G2 .....	25

## 1. General information

Firmware version:	03.28.06.Rev.280
Hardware revision:	280
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.

## 2. Create IoT Hub

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

Press  and select – **create new resource**

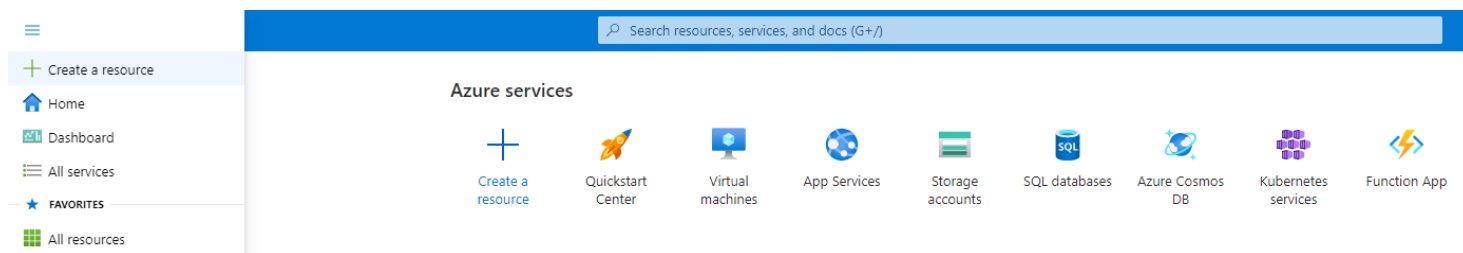


Figure 1 Create new resource

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

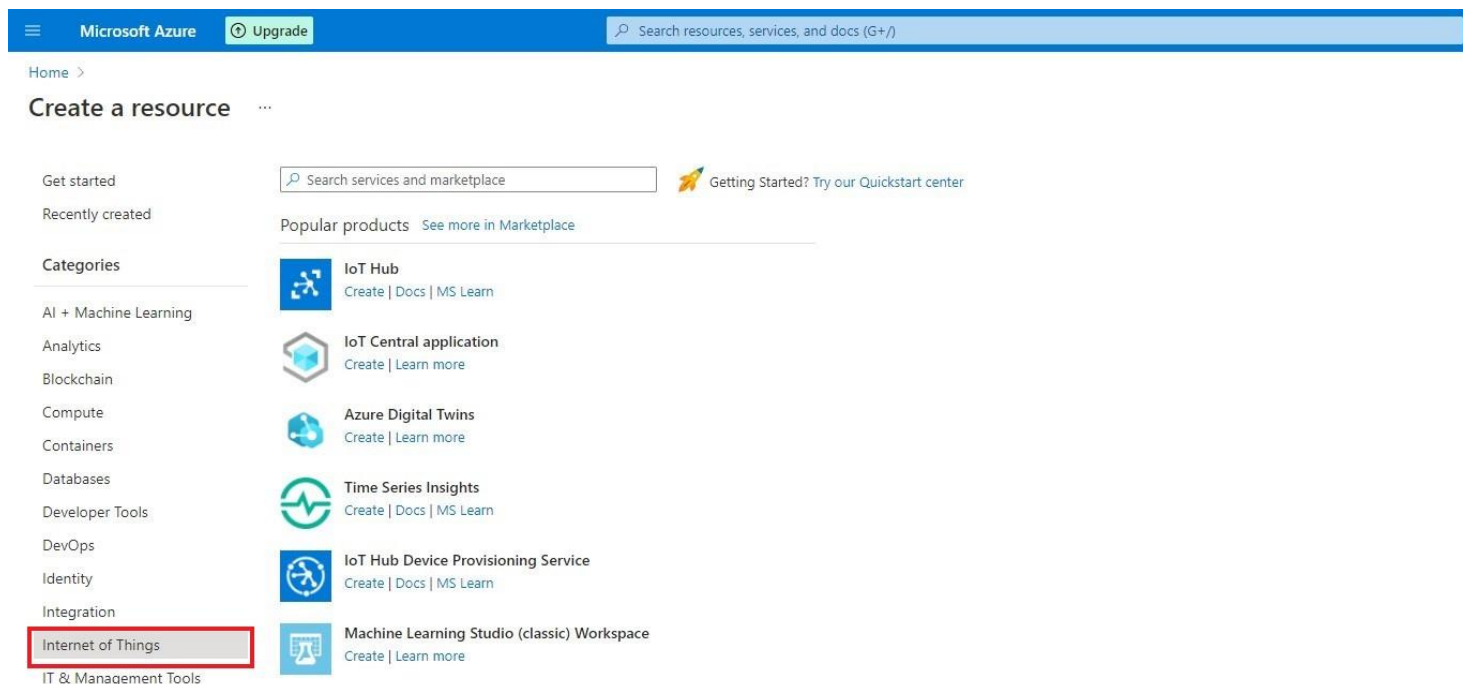



Figure 2 Selecting IoT

Press **Create** near the  icon.

## 2.1. 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 **Compare tiers** below option box).

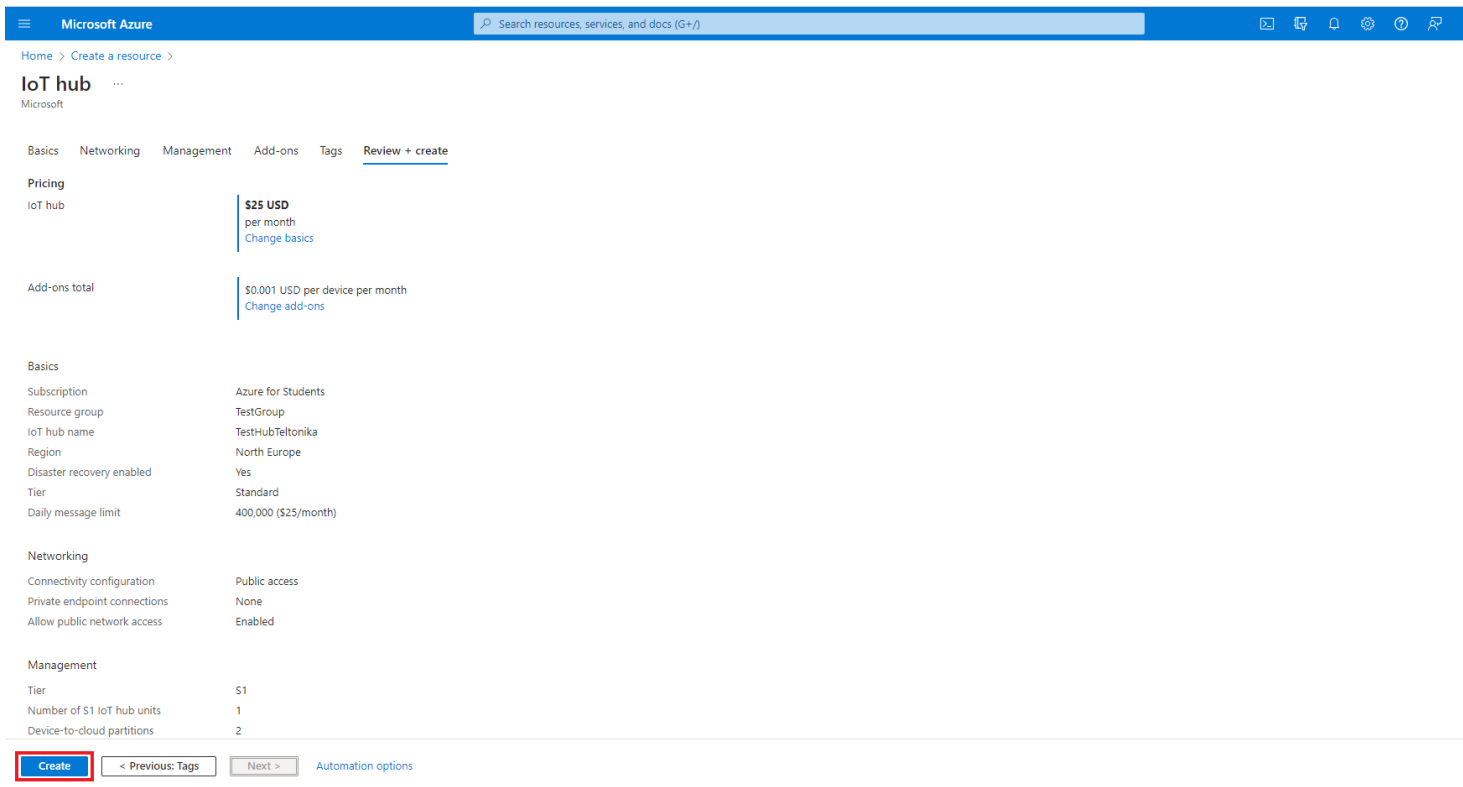
Then choose your **Daily message limit** according to your needs (You can find all the necessary information about **Daily message limit** when you click **See all options** below option box).

Press: **Review + create**

The screenshot shows the 'Basics' configuration page for an IoT Hub in Microsoft Azure. The page is divided into sections: 'Project details' and 'Instance details'. In the 'Project details' section, the 'Subscription' is set to 'Azure for Students' and the 'Resource group' is 'TestGroup'. In the 'Instance details' section, the 'IoT hub name' is 'Naujas', the 'Region' is 'North Europe', and the 'Tier' is 'Free'. The 'Daily message limit' is set to '8,000 (\$0/month)'. A 'Review + create' button is located at the bottom left of the page.

Figure 3 Basics parameters

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



The screenshot shows the Microsoft Azure portal interface for creating an IoT Hub. The top navigation bar includes the Microsoft Azure logo, a search bar, and utility icons. The breadcrumb trail is 'Home > Create a resource > IoT hub'. The page title is 'IoT hub' with a Microsoft logo. The 'Review + create' tab is selected. The pricing section shows a cost of \$25 USD per month for the IoT hub and \$0.001 USD per device per month for add-ons. The 'Basics' section lists configuration details: Subscription (Azure for Students), Resource group (TestGroup), IoT hub name (TestHubTeltonika), Region (North Europe), Disaster recovery enabled (Yes), Tier (Standard), and Daily message limit (400,000). The 'Networking' section shows Connectivity configuration (Public access), Private endpoint connections (None), and Allow public network access (Enabled). The 'Management' section shows Tier (S1), Number of S1 IoT hub units (1), and Device-to-cloud partitions (2). At the bottom, there are buttons for 'Create', '< Previous: Tags', 'Next >', and 'Automation options'. The 'Create' button is highlighted with a red box.

Figure 4 Creating IoT hub

UAB TELTONIKA TELEMATICS  
Saltoniskiu st. 9B-1, LT-08105 Vilnius,  
Lithuania


Registration code 305578349 VAT number LT100013240611

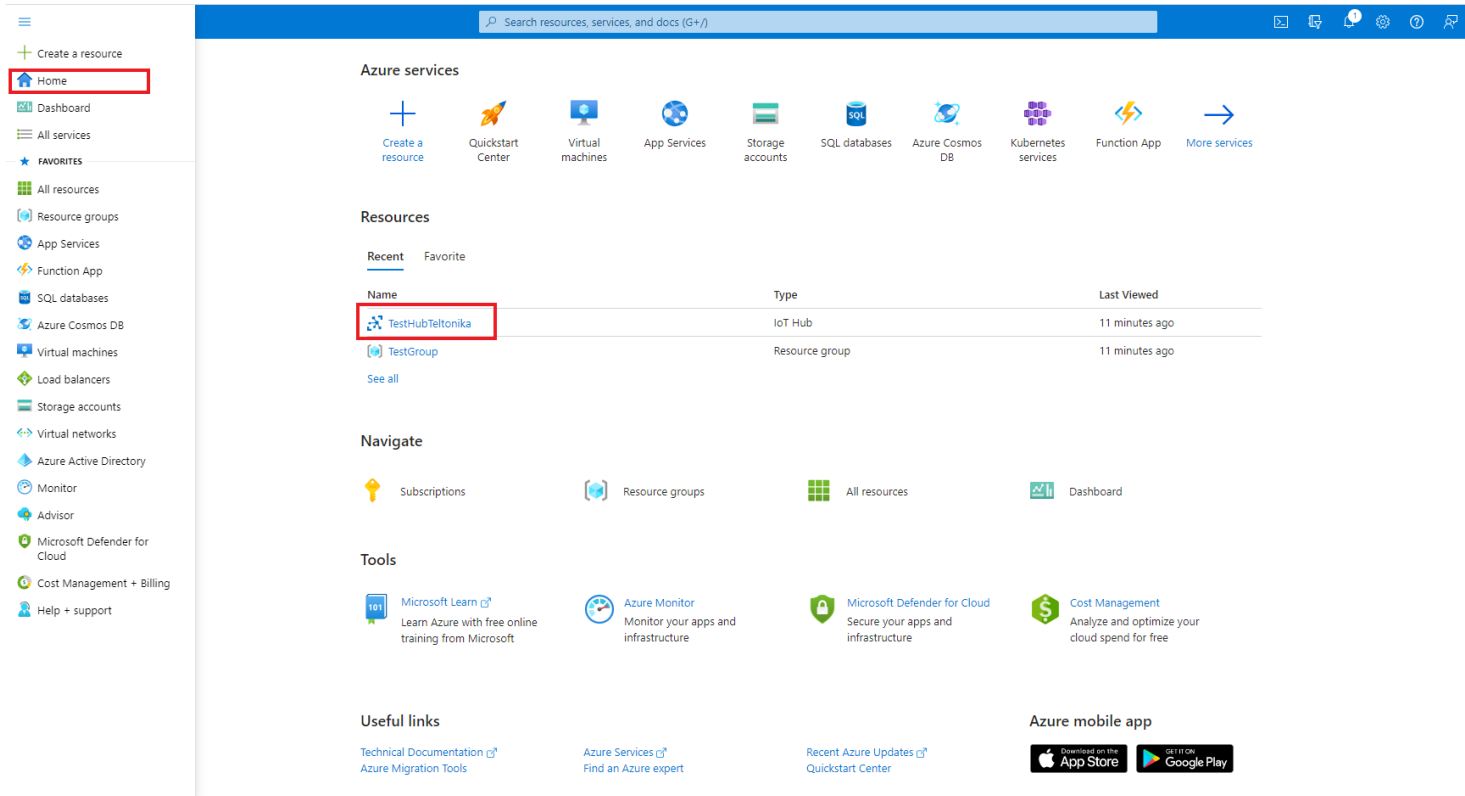
Swedbank AB  
LT71 7300 0101 6274 0043 S.W.I.F.T. HABALT22

Data on the company is collected and stored in the Register of Legal Entities of the Republic of Lithuania.



### 3. Add device

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



The screenshot shows the Azure portal interface. On the left is a navigation sidebar with 'Home' highlighted in a red box. The main content area is titled 'Azure services' and includes a 'Resources' section. In the 'Resources' section, a table lists recent resources, with 'TestHubTeltonika' (IoT Hub) highlighted in a red box. Below the table are sections for 'Navigate', 'Tools', and 'Useful links'.

Name	Type	Last Viewed
TestHubTeltonika	IoT Hub	11 minutes ago
TestGroup	Resource group	11 minutes ago

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.

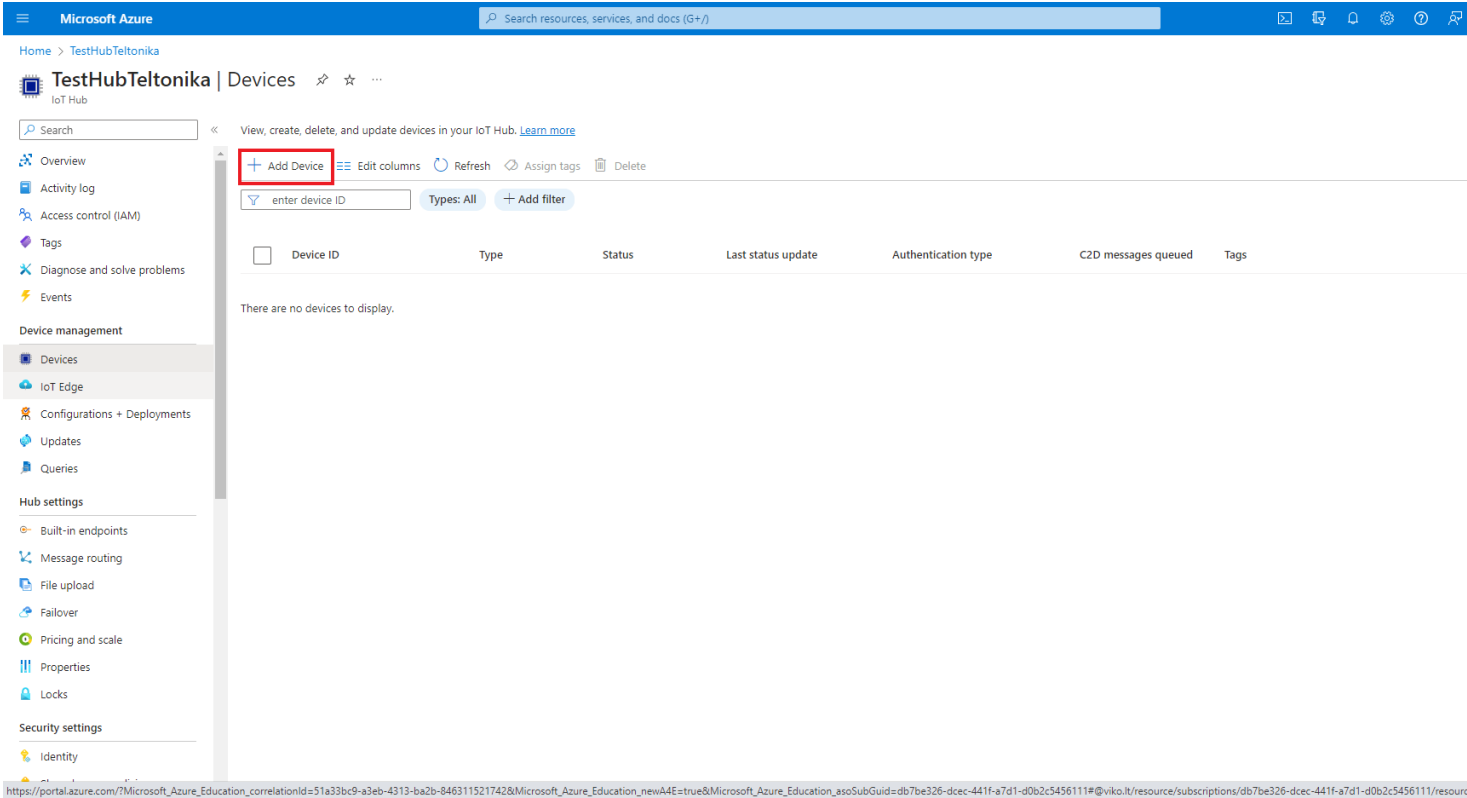


Figure 7 Add Device

UAB TELTONIKA TELEMATICS  
Saltoniskiu st. 9B-1, LT-08105 Vilnius,  
Lithuania

Registration code 305578349 VAT number LT100013240611

Swedbank AB  
LT71 7300 0101 6274 0043 S.W.I.F.T. HABALT22

Data on the company is collected and stored in the Register of Legal Entities of the Republic of Lithuania.





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

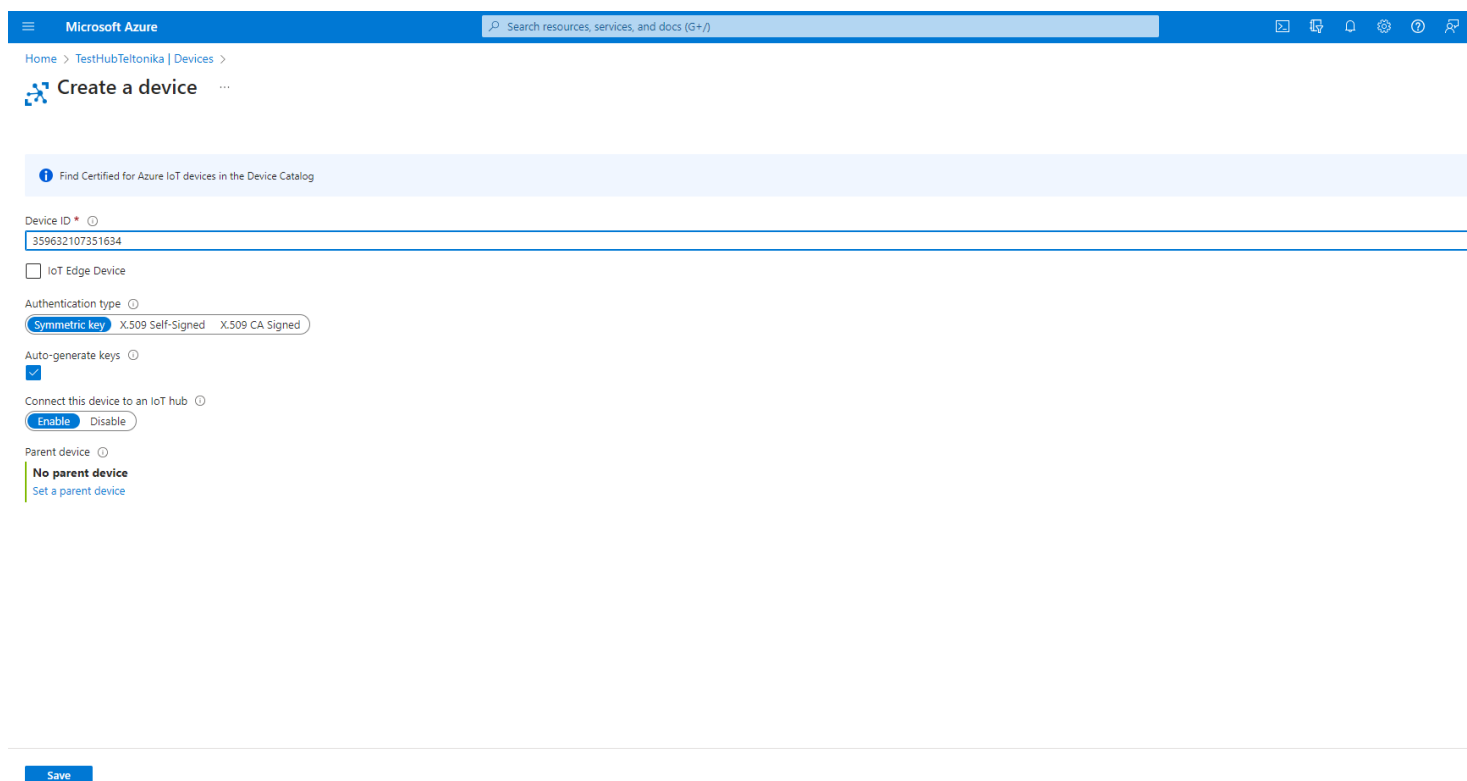
Enter your device IMEI in the **device ID** field.

Other fields here should be left default

Authentication type: Symmetric key Connection this

device to an IoT Hub: Enabled

Press **save**.



Microsoft Azure | Search resources, services, and docs (G+)

Home > TestHubTeltonika | Devices >

### Create a device

Find Certified for Azure IoT devices in the Device Catalog

Device ID \*

IoT Edge Device

Authentication type  Symmetric key  X.509 Self-Signed  X.509 CA Signed

Auto-generate keys

Connect this device to an IoT hub  Enable  Disable

Parent device  No parent device [Set a parent device](#)

[Save](#)

Figure 8 Creating a device

## 4. 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**.

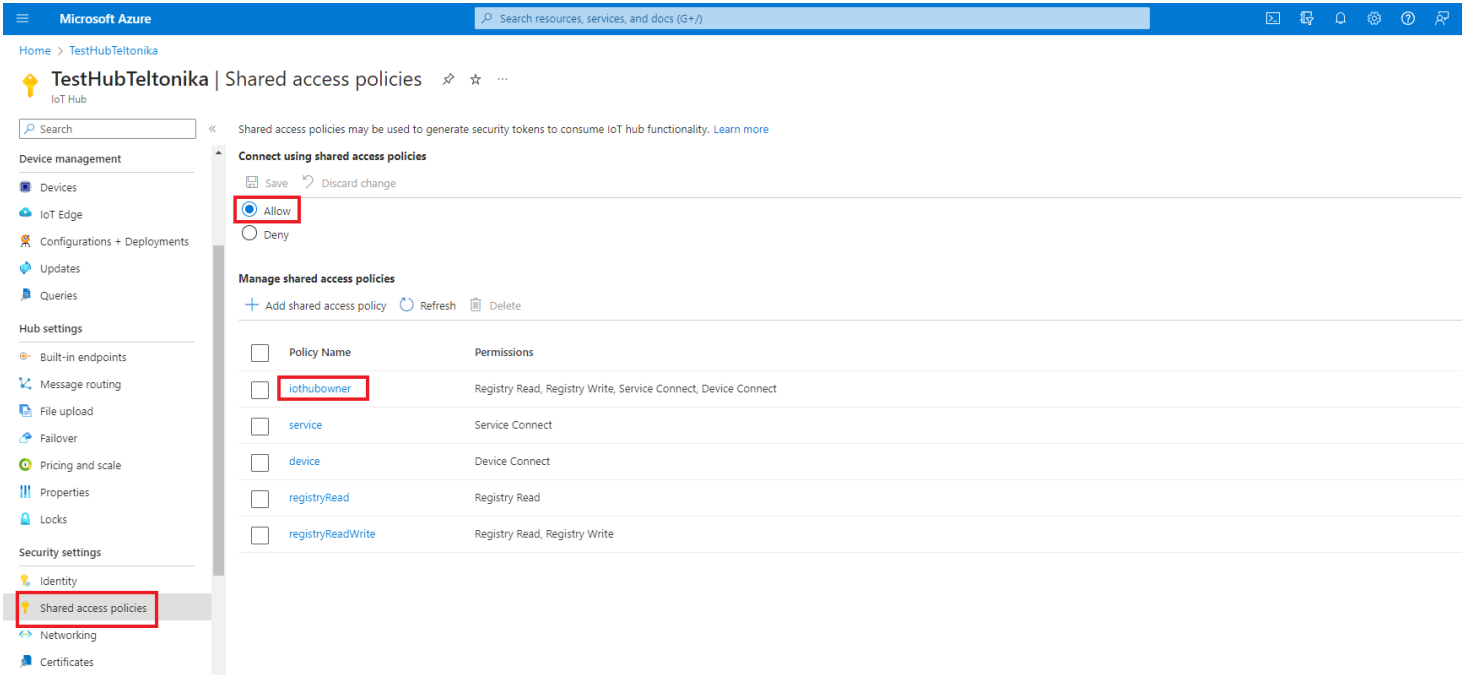


Figure 9 Shared access policies

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

Copy:

1. Primary key
2. Secondary key
3. "iothubowner"

Shared access policies may be used to generate security tokens to consume IoT hub functionality. [Learn more](#)

Connect using shared access policies

Save Discard change

Allow  
Deny

Manage shared access policies

+ Add shared access policy Refresh Delete

Policy Name	Permissions
<input type="checkbox"/> iothubowner	Registry Read, Registry Write, Service Connect, Device Connect
<input type="checkbox"/> service	Service Connect
<input type="checkbox"/> device	Device Connect
<input type="checkbox"/> registryRead	Registry Read
<input type="checkbox"/> registryReadWrite	Registry Read, Registry Write

iothubowner

Regenerate primary key Regenerate secondary key Swap keys

Primary key

Secondary key

Primary connection string

Secondary connection string

Permissions

Registry Read

Registry Write

Service Connect

Device Connect

Update Permissions Cancel

Figure 10 Saving keys

## 5. Configuration

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

1. Domain – **Hostname** (copy here the host name from your lot 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**

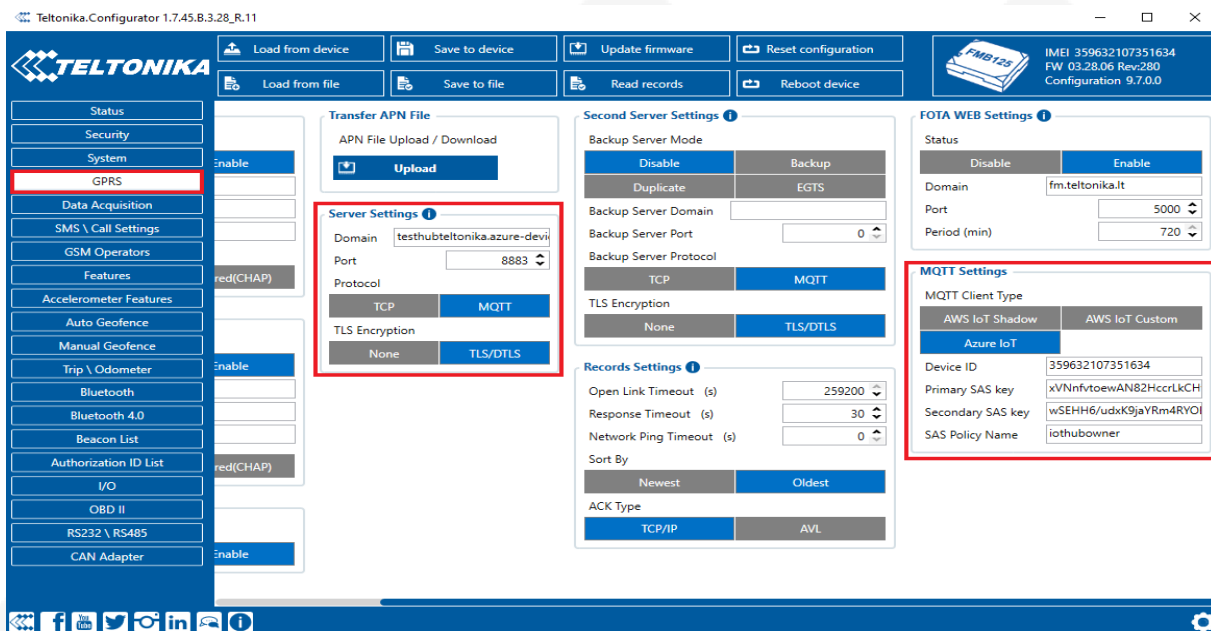


Figure 11 Device configuration

## 6. Certificate creation and upload

### 6.1. Converting certificate to .pem format

Download **DigiCert Global Root G2** and put it inside a new folder: [Download DER/CRT](#)

1. Run the File Explorer, locate and double-click your .cer file;

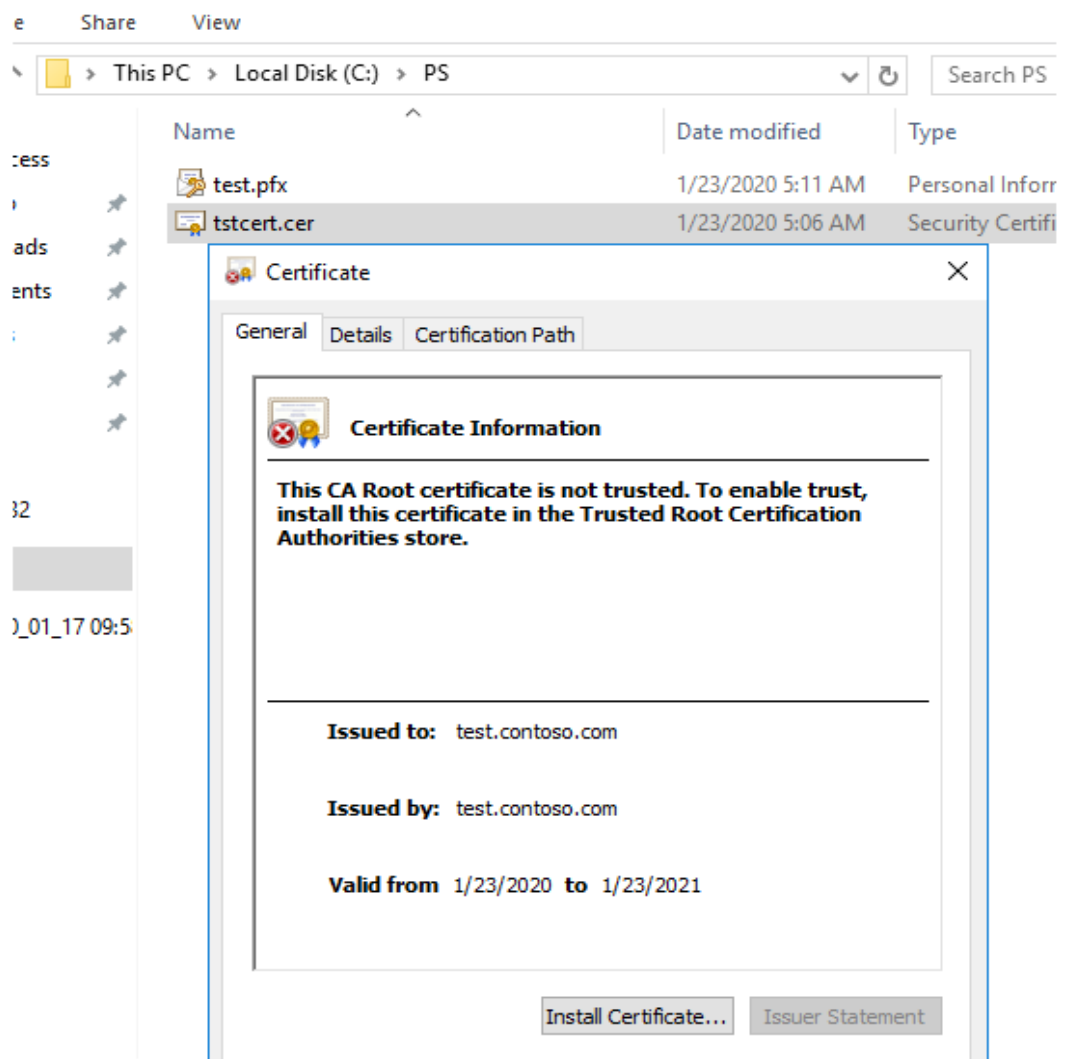


Figure 12 Certificate creation 1

2. In the certificate properties window go to the **Details** tab and click on the “Copy to File” button;

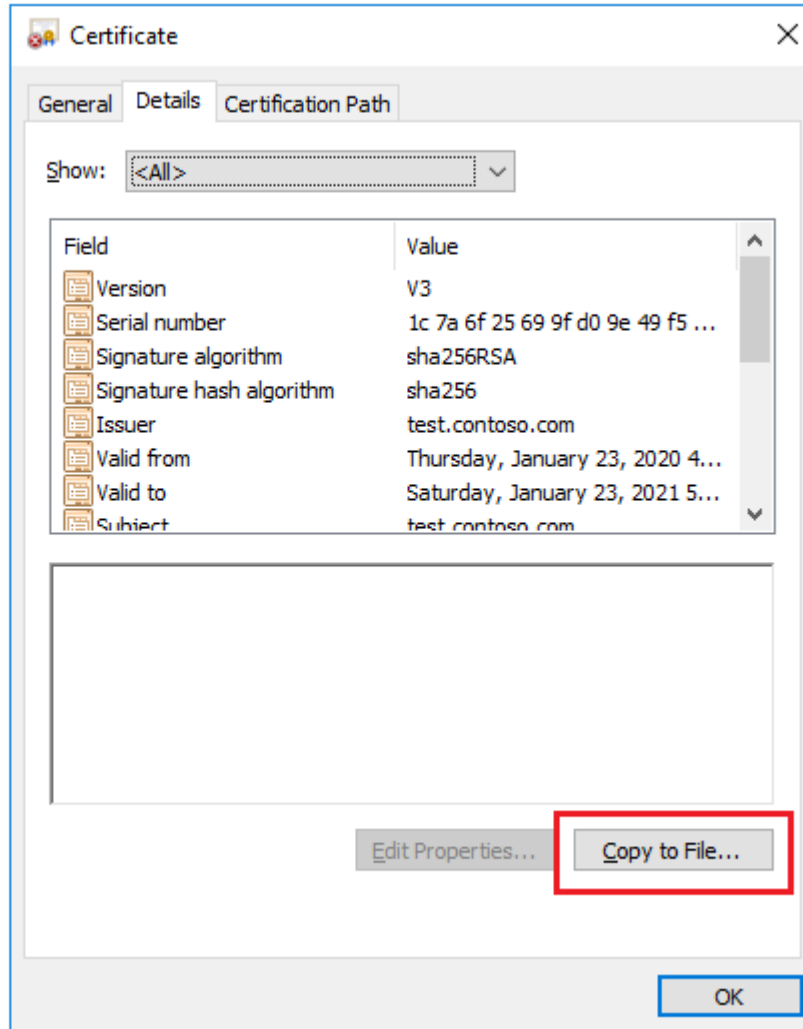


Figure 13 Certificate creation 2

3. Press **Next** on the first step of Certificate Export Wizard;

4. Now you need to select the certificate export format. Select the option "BASE-64 encoded X.509 (.CER)" and click Next;

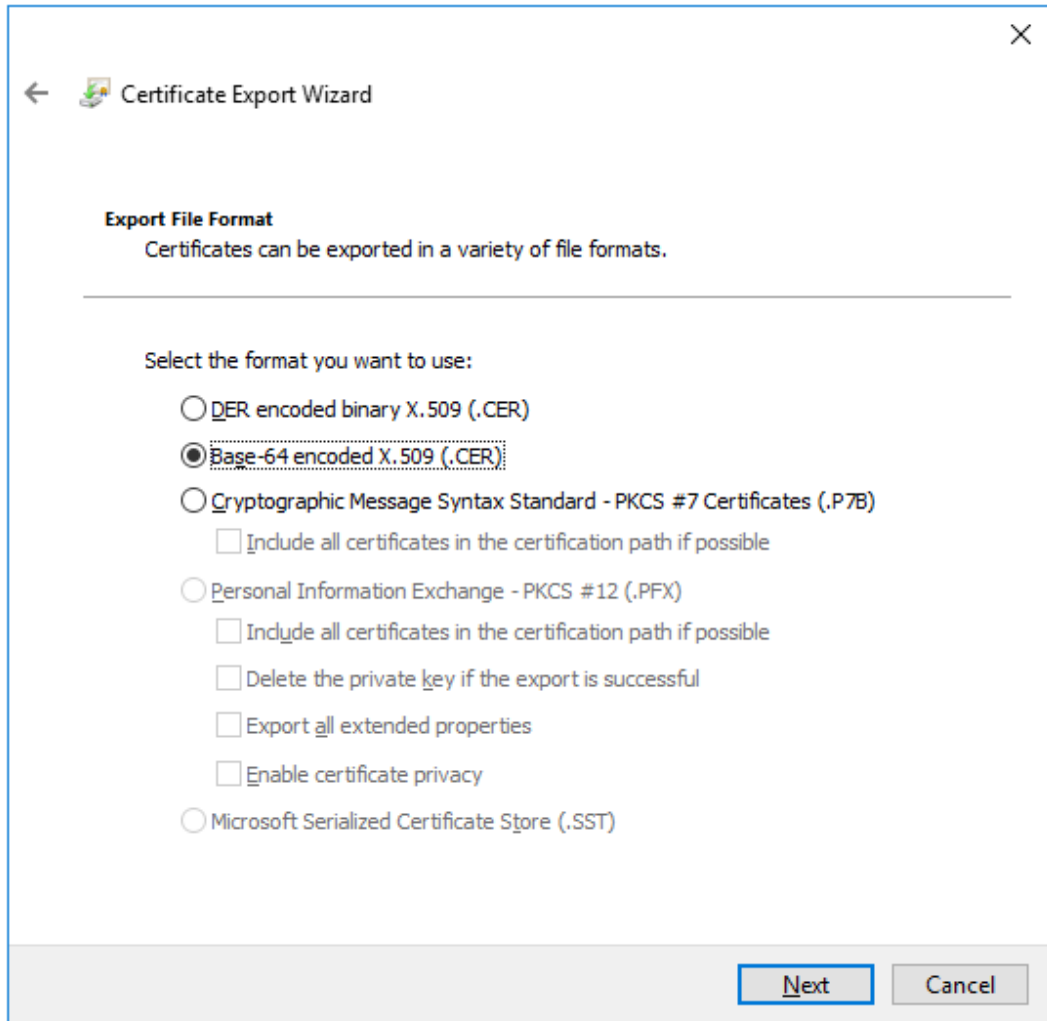
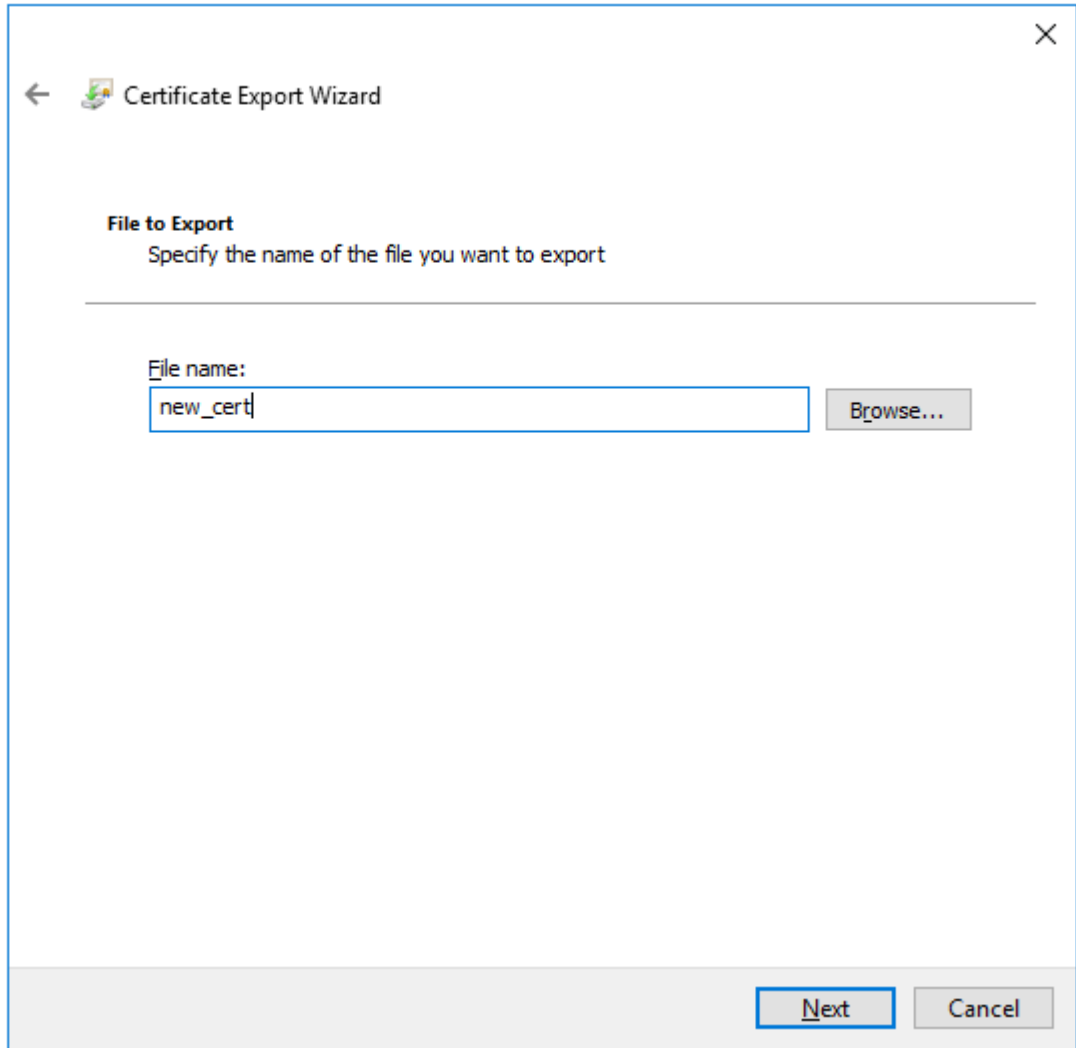



Figure 14 Certificate creation 3

5. Specify the file name;



←  Certificate Export Wizard

**File to Export**  
Specify the name of the file you want to export

---

File name:

Figure 15 Certificate creation 4



6. Press the **Finish** button;

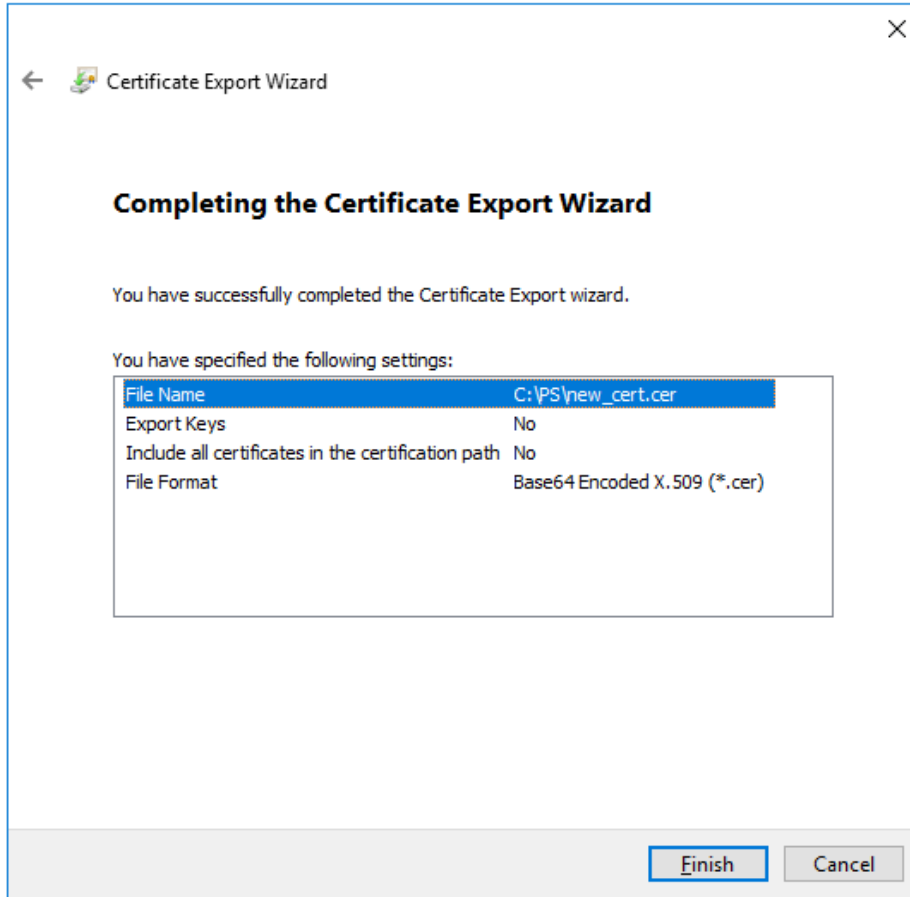


Figure 16 Certificate creation 5

```
PowerShell Copy  
  
Rename-Item -Path "c:\logfiles\daily_file.txt" -NewName "monday_file.txt"
```

7. Now you can change your certificate file extension from .cer to .pem. You can use the following PowerShell command:

Certificate.pem will be created.

## 6.2. Upload certificate to device

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

UAB TELTONIKA TELEMATICS  
Saltoniskiu st. 9B-1, LT-08105 Vilnius,  
Lithuania

Registration code 305578349 VAT number LT100013240611

Swedbank AB  
LT71 7300 0101 6274 0043 S.W.I.F.T. HABALT22

Data on the company is collected and stored in the Register of Legal Entities of the Republic of Lithuania.



## 7. 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.

The screenshot shows the Teltonika device configurator interface. On the left is a navigation menu with options like Status, Security, System, GPRS, Data Acquisition, SMS \ Call Settings, SMS Events, GSM Operators, Features, Accelerometer Features, Auto Geofence, Manual Geofence Settings, Manual Geofence Zones, Trip \ Odometer, Bluetooth 4.0, Beacon List, iButton List, I/O, LVCAN, FMS IO, Manual CAN IO, and Tachograph Data. The main content area is titled 'Device Info' and includes fields for Device Name (FMC640), Last Start Time (2021-08-31 9:17:52), Power Voltage (12013 mV), External Storage (Not Present), and Battery Voltage (0 mV). Below this, there are tabs for GNSS Info, GSM Info (selected), I/O Info, Tachograph, and Maintenance. The GSM Info section contains 'GSM Status' (Modem On, SIM Ready, GPRS Deactivated), 'GPRS Traffic' (Sent Data 71 KB, Received Data 71 B, Total Traffic 72 KB), and 'Records' (Sent Records Count 7, Last Record Send 2021-08-31 10:40:54, Last Server Response Time 2021-08-31 10:40:54). There are also 'Sockets' and 'SMS Count' sections.

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.

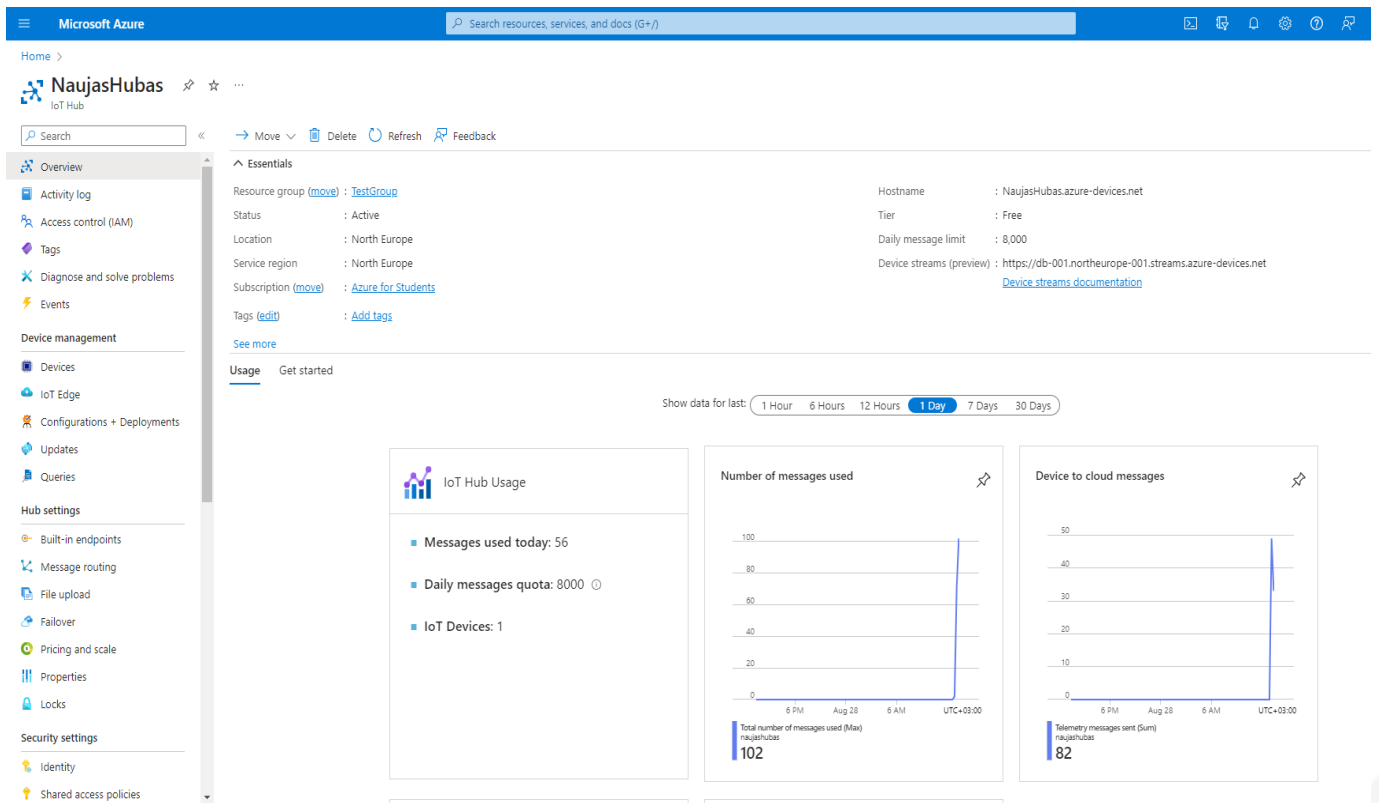


Figure 18 IoT hub overview

## 8. Checking received data in Azure IoT Explorer

### 8.1. 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:

## Version 0.15.8 Latest





- Addressing two dtidl bugs related to simply types [#586](#) [#449](#)
- Supports nested maps of dtidl [#505](#)

**Release Notes:**

This release **does not contain a pre-built Mac binary**. We are currently experiencing issues with our package builder for Mac, so unfortunately for now we've removed that binary asset from the release. You should still be able to run the project locally on mac, but you may encounter errors building binaries ( `npm run package:mac` may fail).

---

**Assets** 4

 <a href="#">azure-iot-explorer_0.15.8_amd64.deb</a>	124 MB	Mar 14
 <a href="#">Azure.IoT.Explorer.Preview.0.15.8.msi</a>	156 MB	Mar 14
 <a href="#">Source code (zip)</a>		Mar 14
 <a href="#">Source code (tar.gz)</a>		Mar 14


 3 3 people reacted

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.

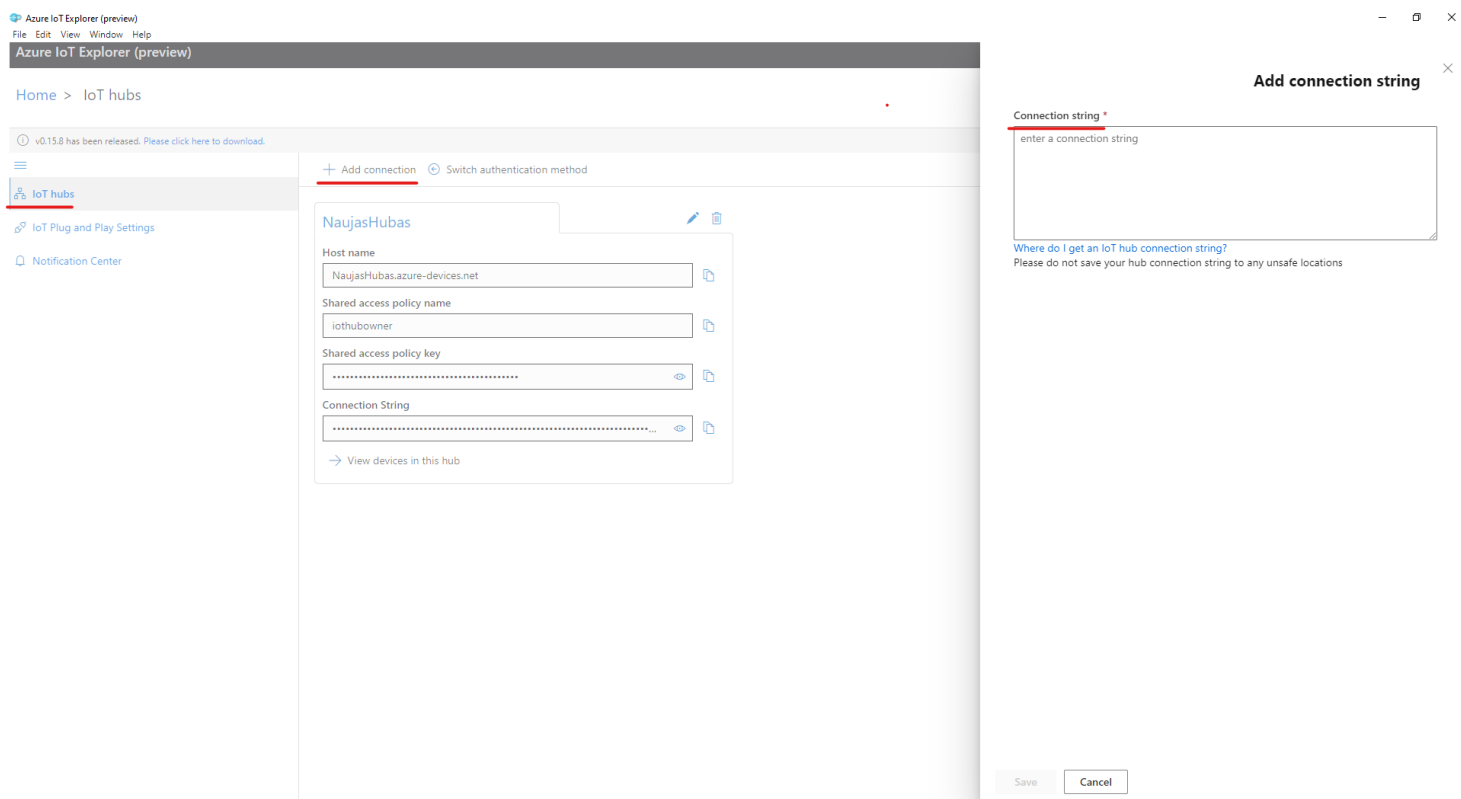


Figure 20 Azure IoT explorer 2

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**.

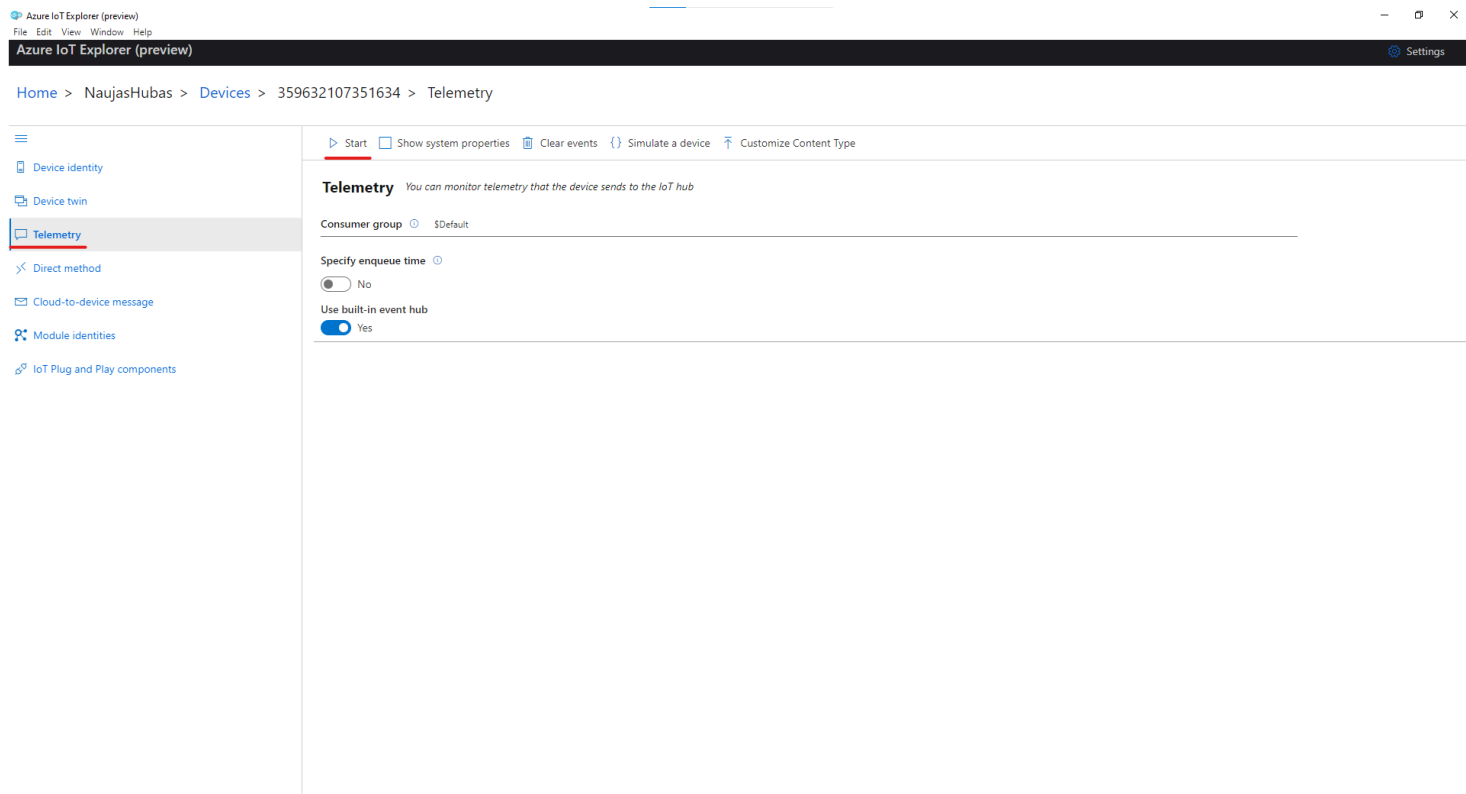


Figure 21 Azure IoT explorer 3

UAB TELTONIKA TELEMATICS  
Saltoniskiu st. 9B-1, LT-08105 Vilnius,  
Lithuania

Registration code 305578349 VAT number LT100013240611

Swedbank AB  
LT71 7300 0101 6274 0043 S.W.I.F.T. HABALT22

Data on the company is collected and stored in the Register of Legal Entities of the Republic of Lithuania.

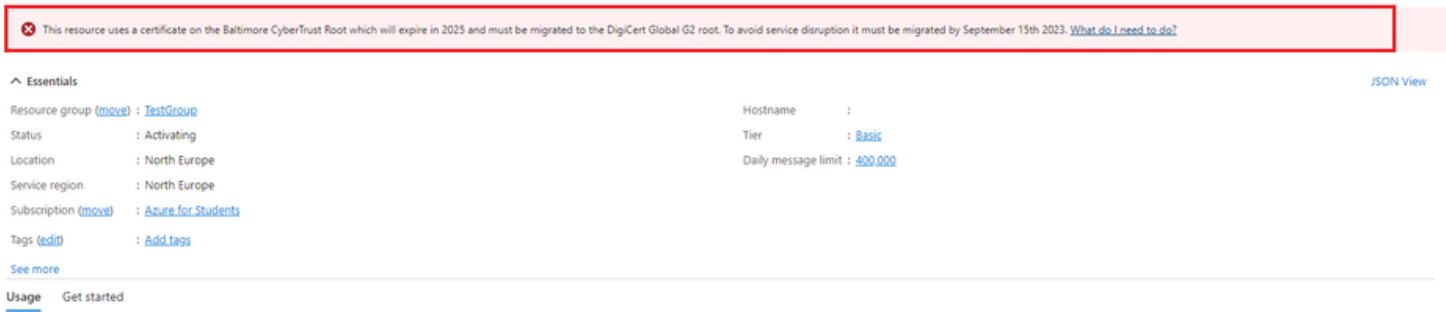






## 9. Migrate to DigiCert Global G2 (If you saw a warning in overview)

In **overview** window click on the red error message



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. To avoid service disruption it must be migrated by September 15th 2023. [What do I need to do?](#)

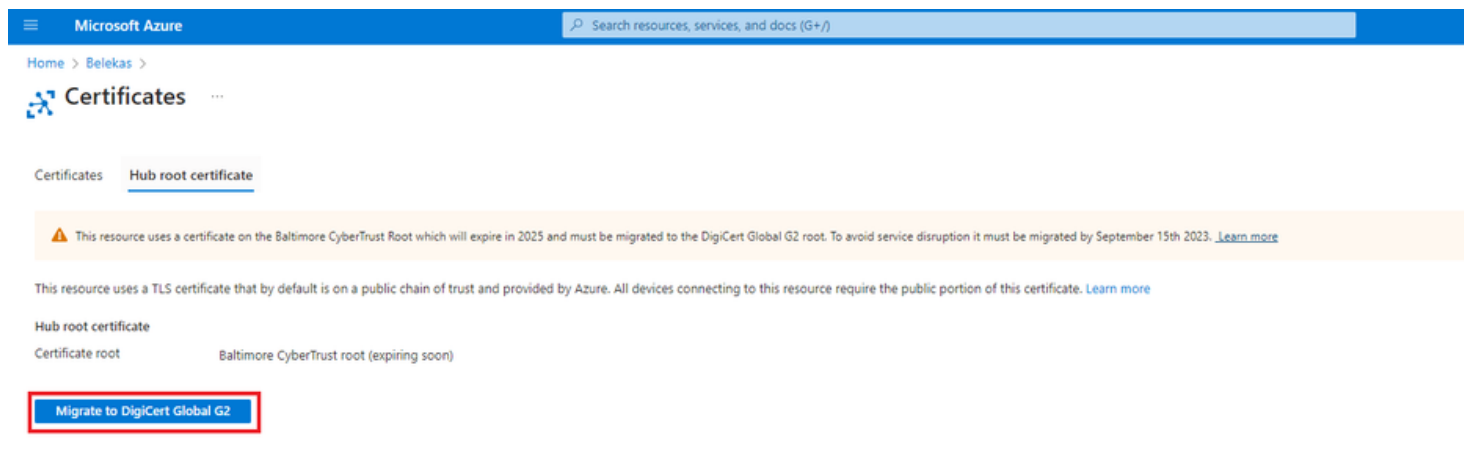
Essentials JSON View

Resource group (move) : <a href="#">TestGroup</a>	Hostname :
Status : Activating	Tier : <a href="#">Basic</a>
Location : North Europe	Daily message limit : <a href="#">600,000</a>
Service region : North Europe	
Subscription (move) : <a href="#">Azure for Students</a>	
Tags (edit) : <a href="#">Add tags</a>	

[See more](#)

Usage [Get started](#)

In the following window click **Migrate to DigiCert Global G2**




Microsoft Azure Search resources, services, and docs (G+)

Home > Belekas >

### Certificates

Certificates **Hub root certificate**

 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. To avoid service disruption it must be migrated by September 15th 2023. [Learn more](#)

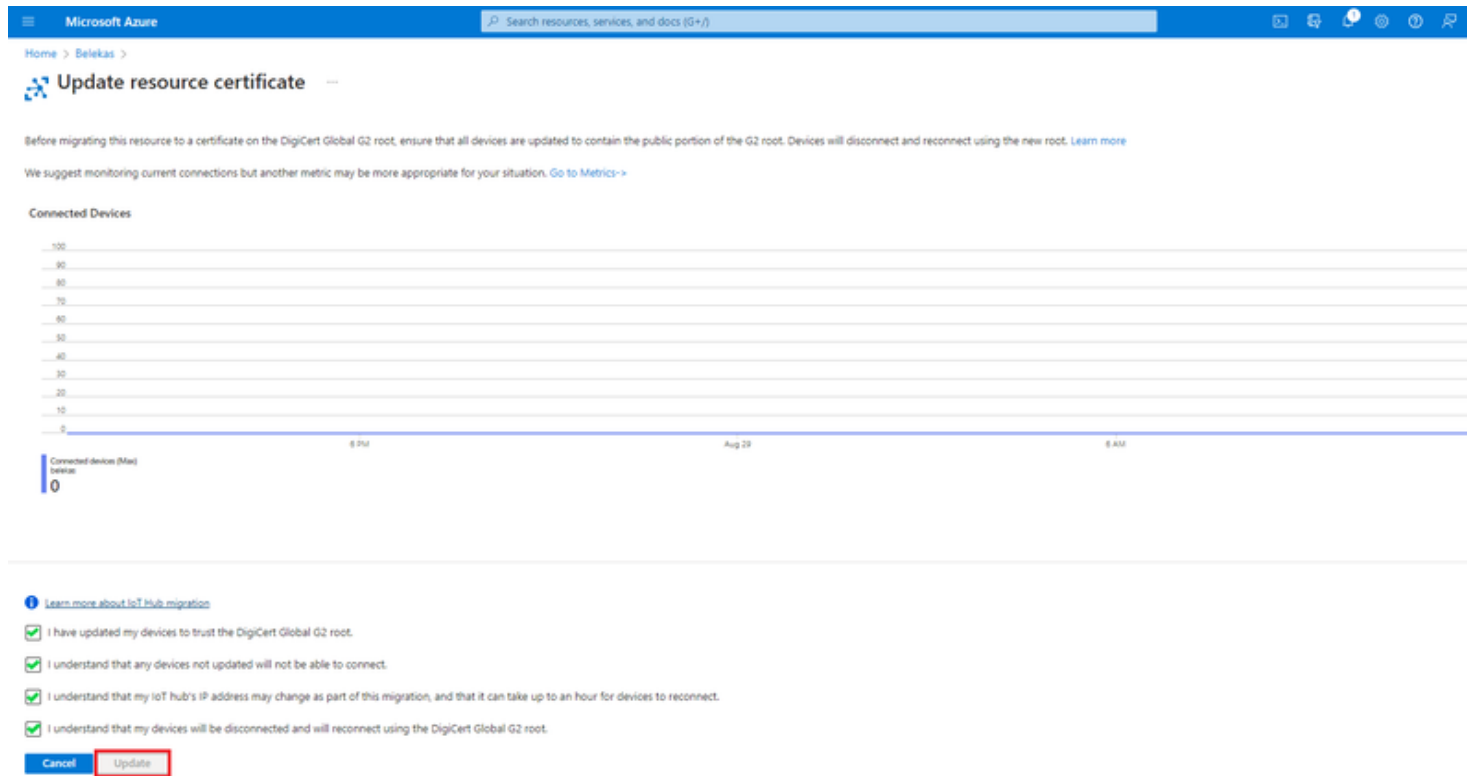
This resource uses a TLS certificate that by default is on a public chain of trust and provided by Azure. All devices connecting to this resource require the public portion of this certificate. [Learn more](#)

Hub root certificate

Certificate root Baltimore CyberTrust root (expiring soon)

**Migrate to DigiCert Global G2**

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



Microsoft Azure

Home > Belekas >

### Update resource certificate

Before migrating this resource to a certificate on the DigiCert Global G2 root, ensure that all devices are updated to contain the public portion of the G2 root. Devices will disconnect and reconnect using the new root. [Learn more](#)

We suggest monitoring current connections but another metric may be more appropriate for your situation. [Go to Metrics->](#)

Connected Devices

Connected devices (Max) below: 0

[Learn more about IoT Hub migration](#)

- I have updated my devices to trust the DigiCert Global G2 root.
- I understand that any devices not updated will not be able to connect.
- I understand that my IoT hub's IP address may change as part of this migration, and that it can take up to an hour for devices to reconnect.
- I understand that my devices will be disconnected and will reconnect using the DigiCert Global G2 root.

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

UAB TELTONIKA TELEMATICS  
Saltoniskiu st. 9B-1, LT-08105 Vilnius,  
Lithuania

Registration code 305578349 VAT number LT100013240611

Swedbank AB  
LT71 7300 0101 6274 0043 S.W.I.F.T. HABALT22

Data on the company is collected and stored in the Register of Legal Entities of the Republic of Lithuania.

