MQTT

Connecting to Microsoft Azure

Vers. 1.0 – Jul 2021

1. Introduction

All of Infinite's devices that support the MQTT protocol, are capable to connect to any local or remote MQTT Broker. Microsoft Azure, commonly referred to as Azure, is a cloud computing service created by Microsoft for building, testing deploying, and managing applications and services through Microsoft-managed centers.

This document is a brief how-to guide for all device communications between Infinite's devices and Microsoft Azure.

2. Generating Self-Signed Device Certificate and Key

Azure requires TLS communications so we will have to create our own self-signed certificate and key for our device. We do that with the commercial-grade TLS toolkit openssl. The easiest way to do that is to simply install git on your computer and locate the openssl.exe file in this directory: `C:\Program Files\Git\usr\bin\openssl.exe`.

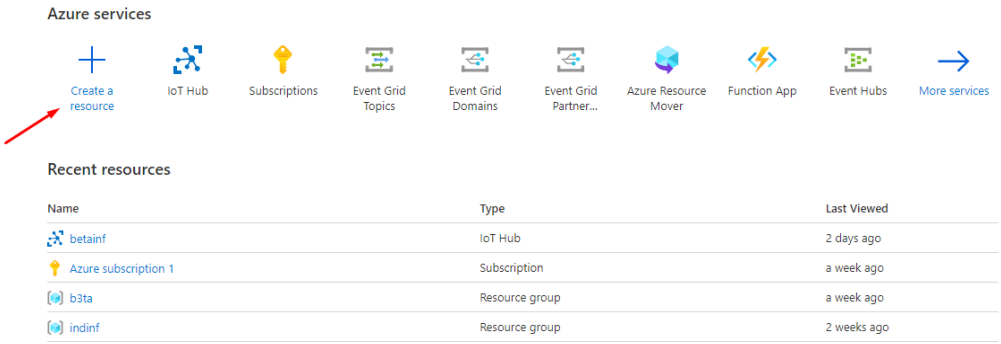
Open a Command Prompt or PowerShell window in the above directory and type the following commands to create the device certificate and key:

req -x509 -nodes -sha256 -days 365 -newkey rsa:2048 -keyout device.key -out device.crt - creates device certificate and private key

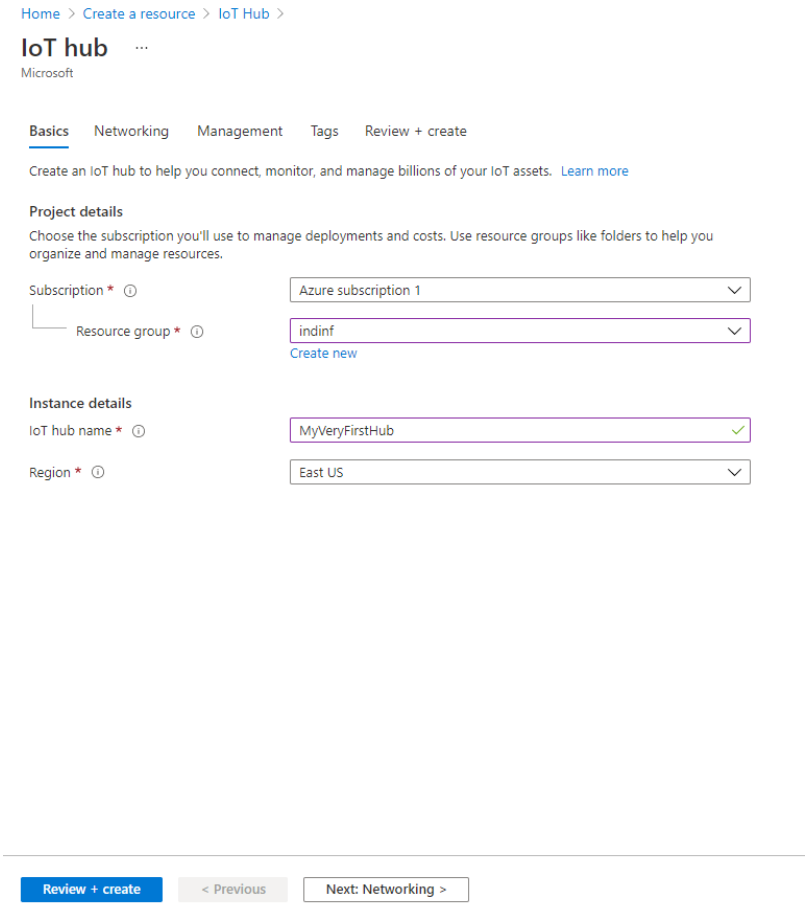
(These commands are for testing purposes and should be adjusted for different requirements.)

3. Creating an IoT Hub

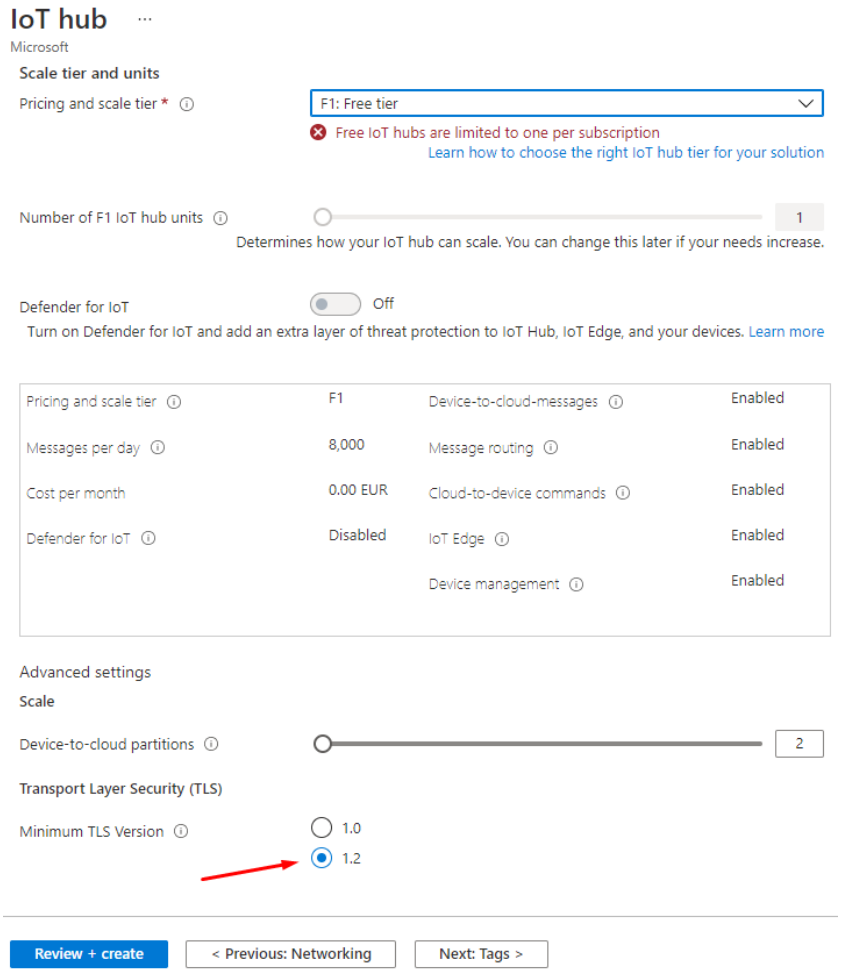
After creating a Microsoft Account, the first step of this procedure is to create an IoT Hub. On the homepage of Microsoft Azure, click Create a resource and then search for IoT Hub.



Create an IoT Hub by filling out the project details and creating a new Resource group. You must choose East US as your region for the time being as Microsoft is working on enabling TLS1.2 on all regions.

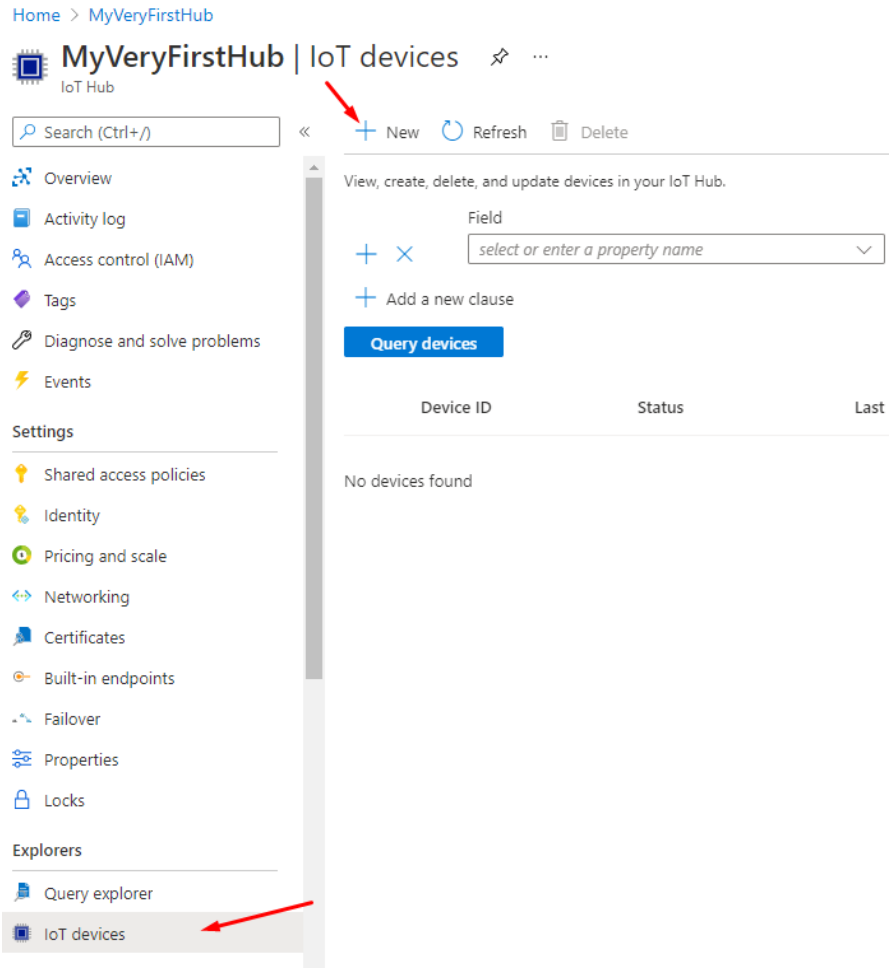


Make sure that you configure the minimum TLS version as well.

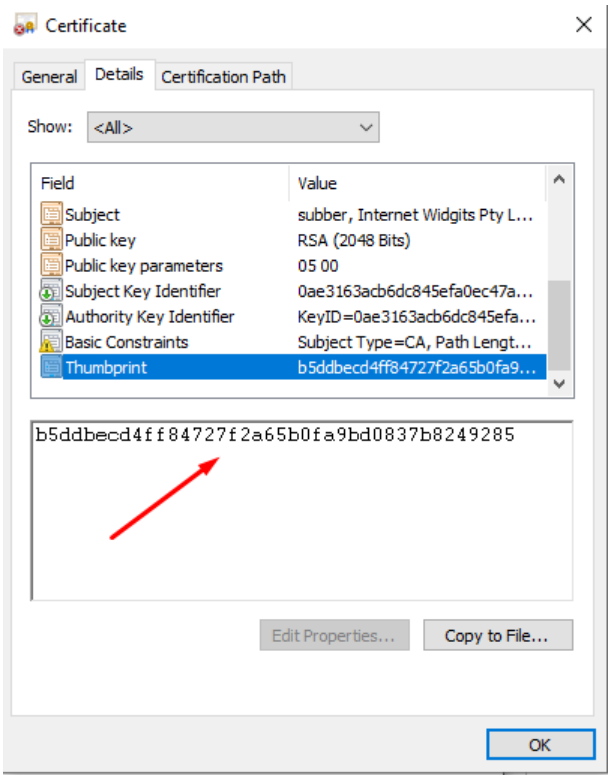


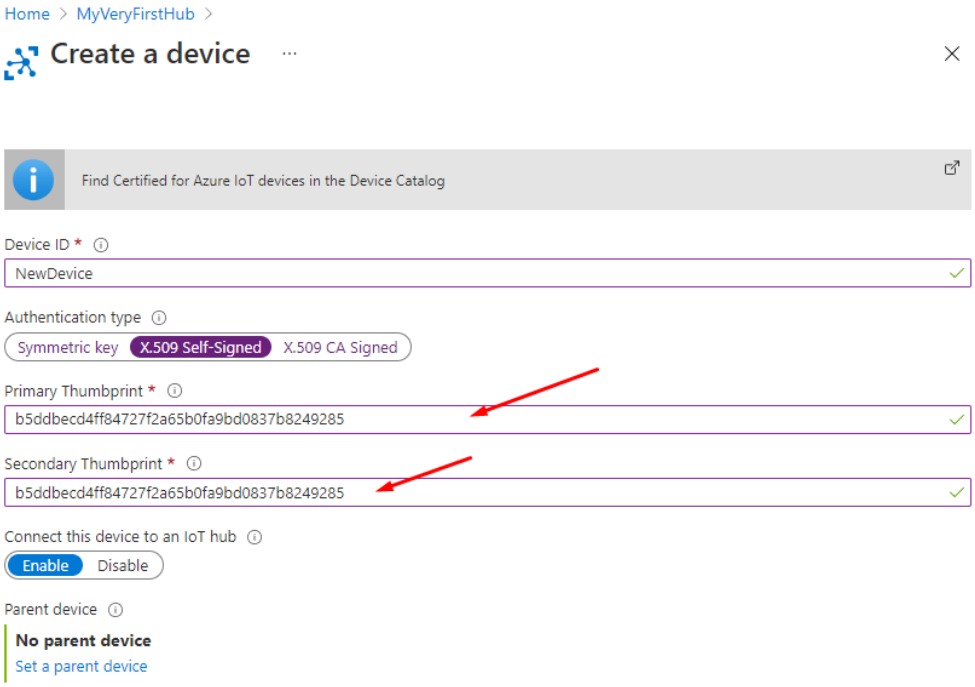
3.1 Creating a device

While you are on your IoT Hub page, enter the IoT devices tab and click New to create an IoT device.



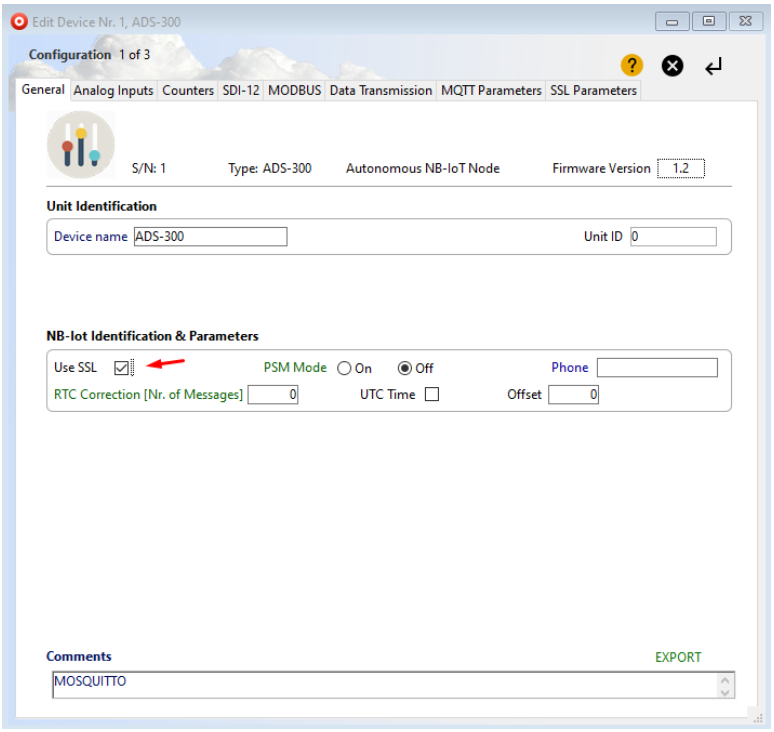
On the next page name your device, choose X.509 Self-Signed as the authentication type and enter your certificates Primary Thumbprint. You can find this thumbprint by opening the device.crt file we created earlier.


Certificate
General
Details
Certification Path
Show:
<All>
Field
Value
Subject
subber, Internet Widgits Pty L...
Public key
RSA (2048 Bits)
Public key parameters
05 00
Subject Key Identifier
0ae3163acb6dc845efa0ec47a...
Authority Key Identifier
KeyID=0ae3163acb6dc845efa...
Basic Constraints
Subject Type=CA, Path Lengt...
Thumbprint
b5ddbecd4ff84727f2a65b0fa9...
b5ddbecd4ff84727f2a65b0fa9bd0837b8249285
Edit Properties...
Copy to File...
OK


Home
MyVeryFirstHub
Create a device
Find Certified for Azure IoT devices in the Device Catalog
Device ID *
NewDevice
Authentication type
Symmetric key
X.509 Self-Signed
X.509 CA Signed
Primary Thumbprint *
b5ddbecd4ff84727f2a65b0fa9bd0837b8249285
Secondary Thumbprint *
b5ddbecd4ff84727f2a65b0fa9bd0837b8249285
Connect this device to an IoT hub
Enable
Disable
Parent device
No parent device
Set a parent device

4. Device Configuration with WA Manager

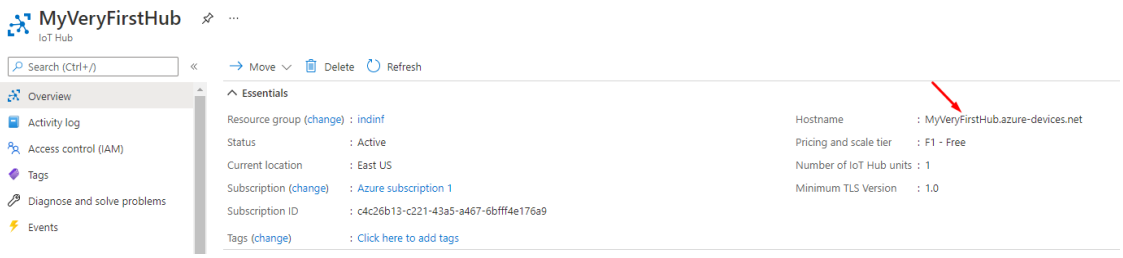
In the Edit Device window in WA Manager, tick the Use SSL box.



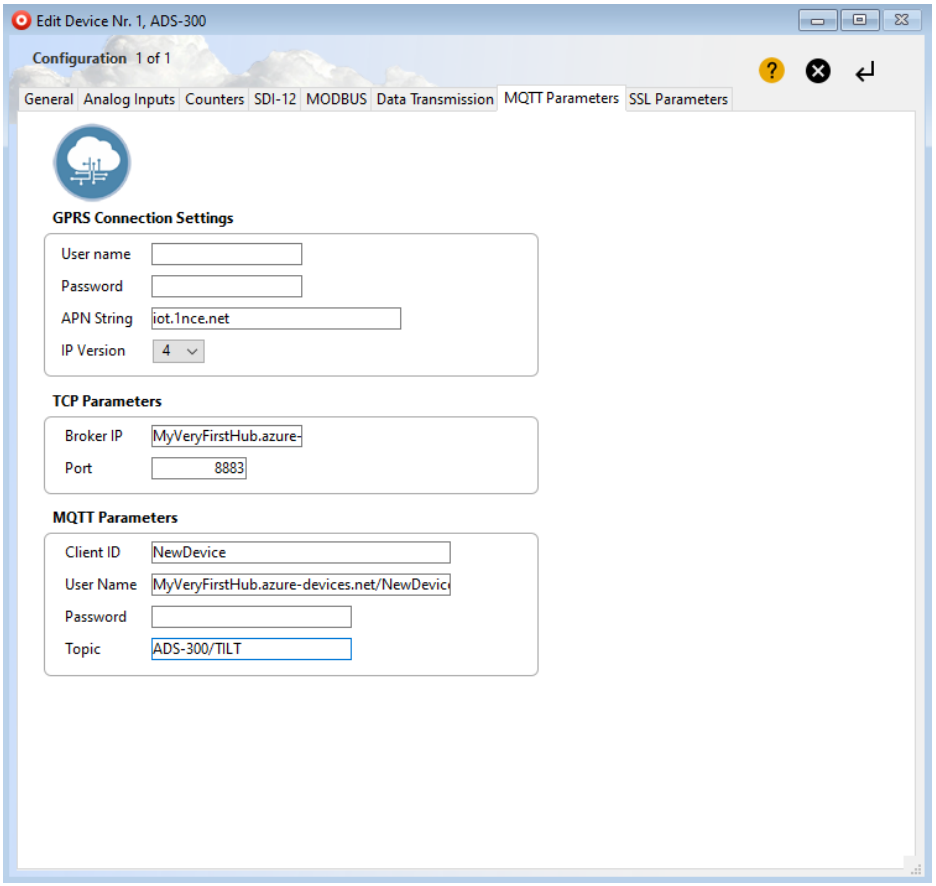
Next, we configure the MQTT parameters.

Although Azure supports MQTT connectivity, it is not a pure MQTT Broker and so it has some limitations regarding its MQTT paramaters.

For the Broker IP, the IoT Hub endpoint must be used that can be found in the IoT Hub page.

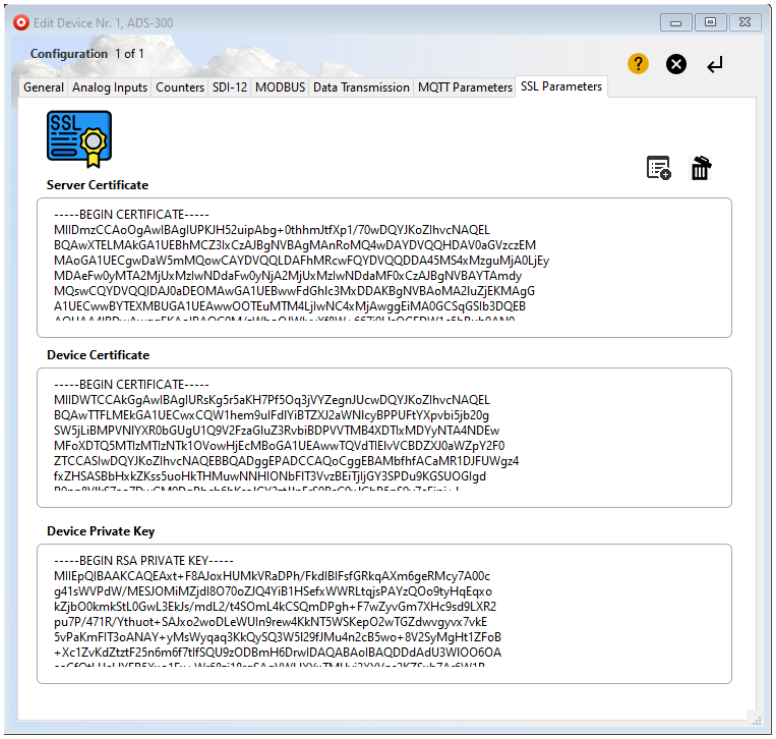


For the Client ID, the Device ID must be used that we used to create our device.



The username must be of this format based on the name of our DeviceID and IoT Hub name: MyVeryFirstHub.azure-devices.net/NewDevice/?api-version=2018-06-30

Lastly, in the SSL Parameters tab, we copy and paste the three files needed for the TLS communication: Server Certificate (CA), Device Certificate and Device Private Key.



The Server Certificate is [this](#) Digicert CA, the Device Certificate is the device.crt file and the Device Private Key is the device.key file. These files should be first opened with Notepad++ and their contents should be copy and pasted in the above tab. All files must be PEM formatted.

Your device can now connect Azure and send your encrypted data safely.

Disclaimer:

Azure is a registered trademark of Microsoft Corporation, USA. All products and software mentioned in this document for educational and demonstration purposes.

Revision: 1.0

© 2021, Infinite Informatics Ltd

Infinite Informatics, Ltd
1, Valaoritou Street
GR-54626 Thessaloniki, Greece
Phone: +30-2310-553545
E: info@indinf.gr
W: www.infinite.com.gr