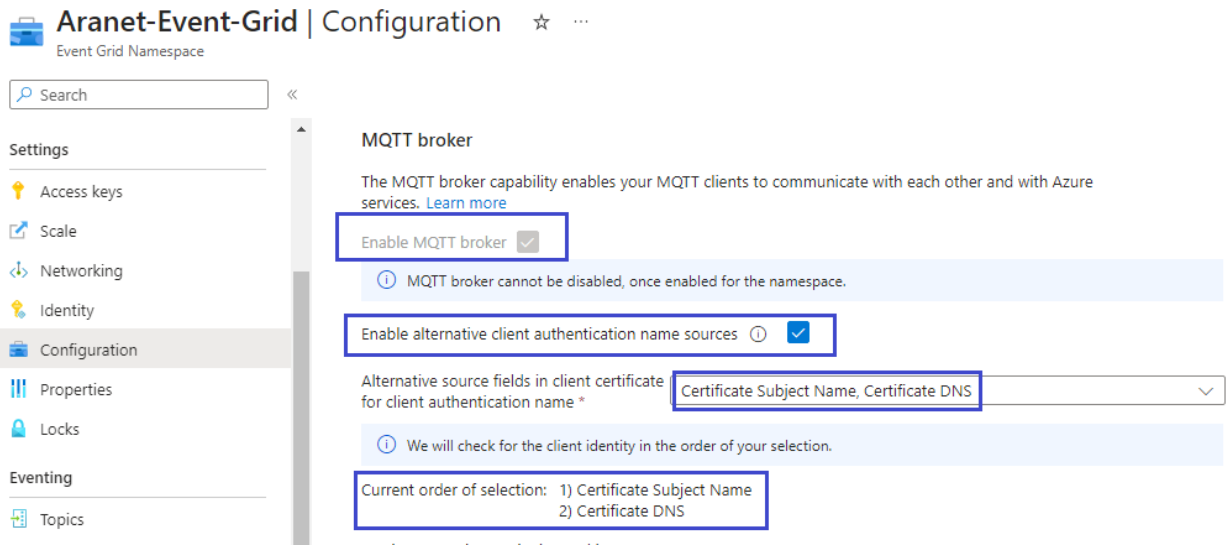
How to Connect Aranet PRO to Azure Event Grid MQTT broker

This example will describe Event Grid Namespace MQTT broker and Aranet PRO base station MQTT configuration details for Client authentication using self-signed CA certificate chain.

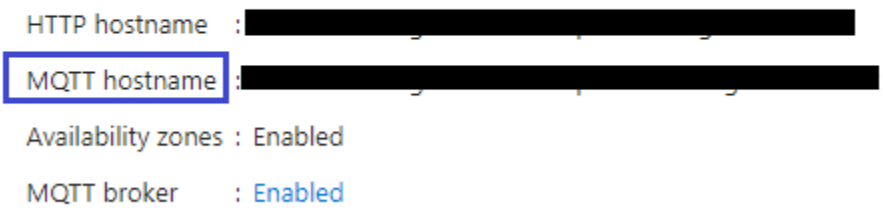
Before configuration, make sure you have access to **Event Grid** Namespace and it has **MQTT broker enabled**, **alternative client authentication name sources enabled** and for client authentication **Alternative source fields in client certificate** set in following order:

1) Certificate Subject Name
2) Certificate DNS

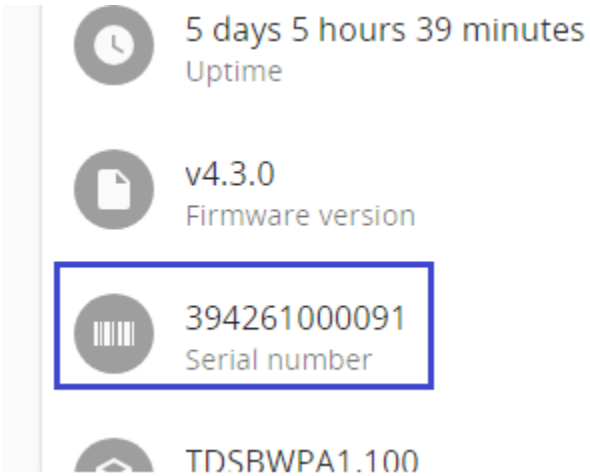


In this example will be used a self-signed CA certificate file, Client certificate file and Client key file.

For **CA certificate's** Common Name **MQTT hostname** of your Event Grid Namespace will be used.



For **Client certificate's** Common Name the Aranet base station **serial number** will be used. It will be also used later in Event Grid **"Clients"** configuration as **Client Authentication Name**.



Generate certificate and key files

In order to generate certificate and key files OpenSSL utilities will be used. In this example **OpenSSL v3.0.2** is being used.

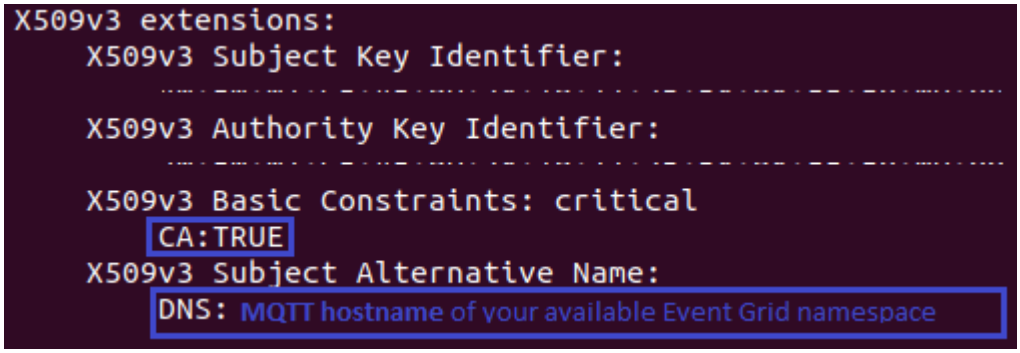
Additional configuration in OpenSSL configuration file ***openssl.cnf*** is required:

Configuration section	Section variable and value pairs
[**v3_ca**]	basicConstraints = critical,**CA:TRUE** subjectAltName = @**alt_names**
[**req**]	x509_extensions = **v3_ca**,**v3_req** req_extensions = **v3_req**
[**alt_names**]	**DNS.1** = <Event Grid Namespace **MQTT hostname**>

Steps of generating the files

1) Generate CA key:
```
openssl genrsa -aes256 -out ca.key 4096
```
2) Generate CA certificate file using previously created CA key file (for the **Common Name** use the **MQTT hostname** of your available Event Grid Namespace):
```
openssl req -new -x509 -sha256 -days 2525 -key ca.key -out ca.crt -
extensions v3_ca
```

3) Verify that created CA certificate file contains necessary X509v3 extension key - value pairs:
`openssl x509 -in ca.crt -text`



4) Generate client key file:
`openssl genrsa -out client.key 4096`

5) Generate client certificate signing request file for signing the client certificate file (for the **Common Name** use the **serial number** of Aranet PRO base station):
`openssl req -new -sha256 -out client.csr -key client.key -extensions v3_req`

6) Generate client certificate file using previously generated CSR file and CA certificate and key files:
`openssl x509 -req -sha256 -in client.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out client.crt -days 2525`

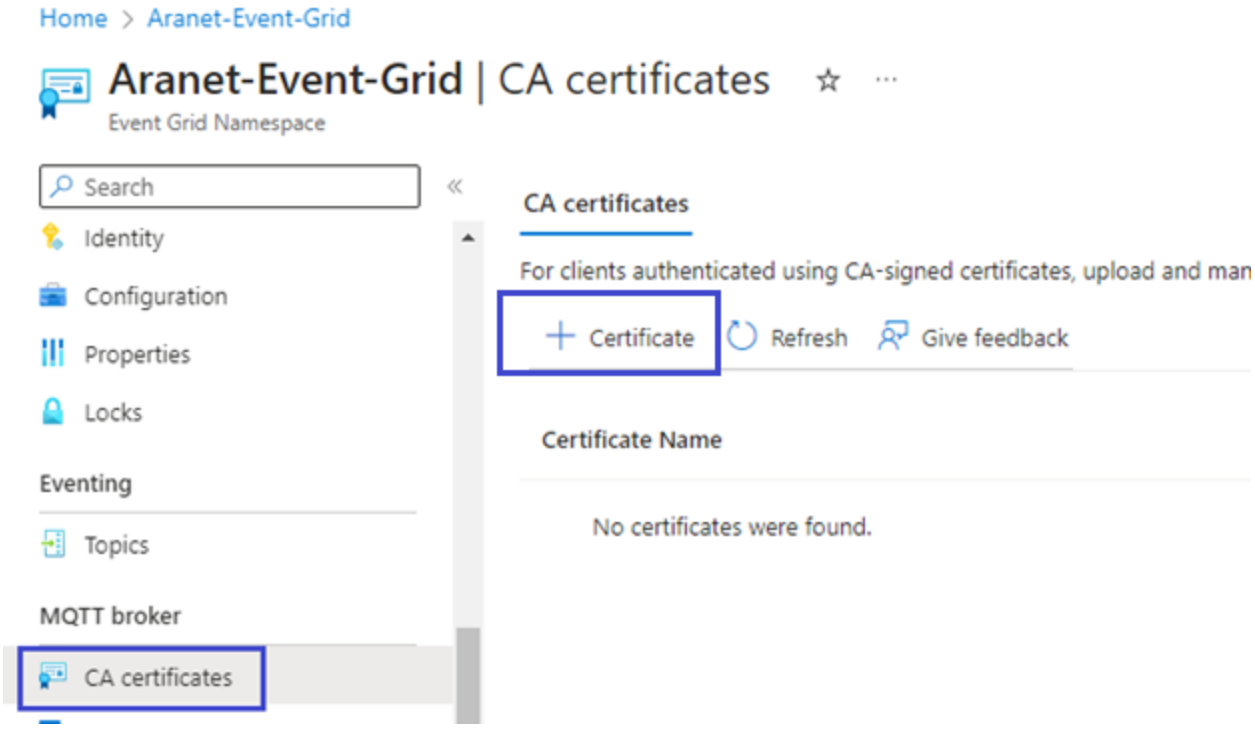
7) Self-signed CA and client certificate and key files are now created. List of files:
   a. **ca.crt** – root CA certificate which was used to sign client certificate file (will be used in Event Grid "**CA certificate**" configuration);
   b. **ca.key** – CA privatye key file;
   c. **client.crt** – client certificate file signed with CA certificate (will be used in Aranet PRO base station MQTT configuration);
   d. **client.key** – client private key (will be used in Aranet PRO base station MQTT configuration);
   e. **client.csr** – can be removed (will not be used).

NOTE: if more than one pair of client key and certificate files are needed (in case if two or more Aranet PRO base stations are planned to be connected) then the same pair of CA certificate and key files can be used to sign other pairs of client certificate and key files as long as these clients are planned to be connected to the same Event Grid Namespace using the same MQTT hostname set in the CA certificate's **Common Name**.

Proceed with Event Grid configuration steps.

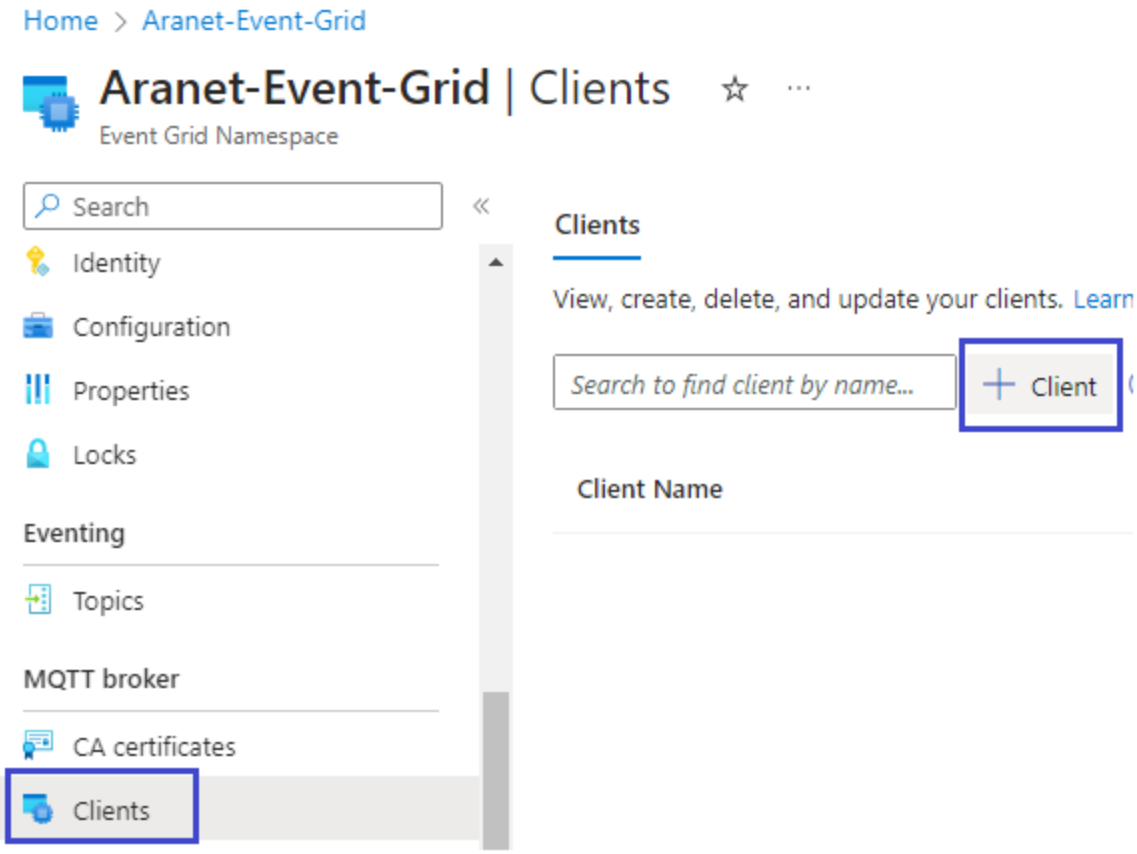
Event Grid configuration – add CA certificate

In Event Grid Namespace section "**MQTT broker**" open "CA certificates" and upload **ca.crt** file. Set name as **CertificateCA**.



Event Grid configuration – create MQTT broker client

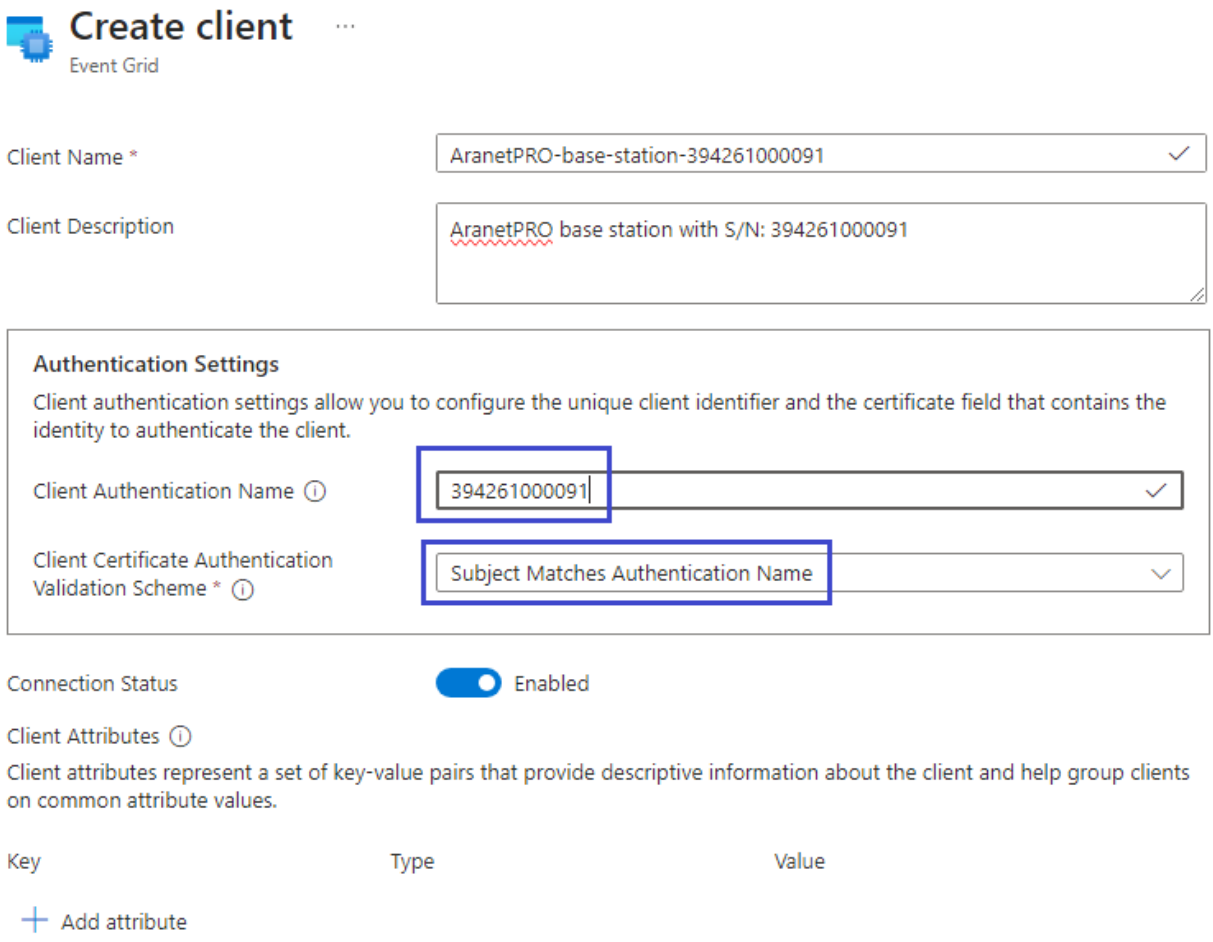
In the same Event Grid Namespace navigate to the MQTT broker section "**Clients**" and press on "+" to add a new Client.



For the client following important **Authentication Settings** must be set:

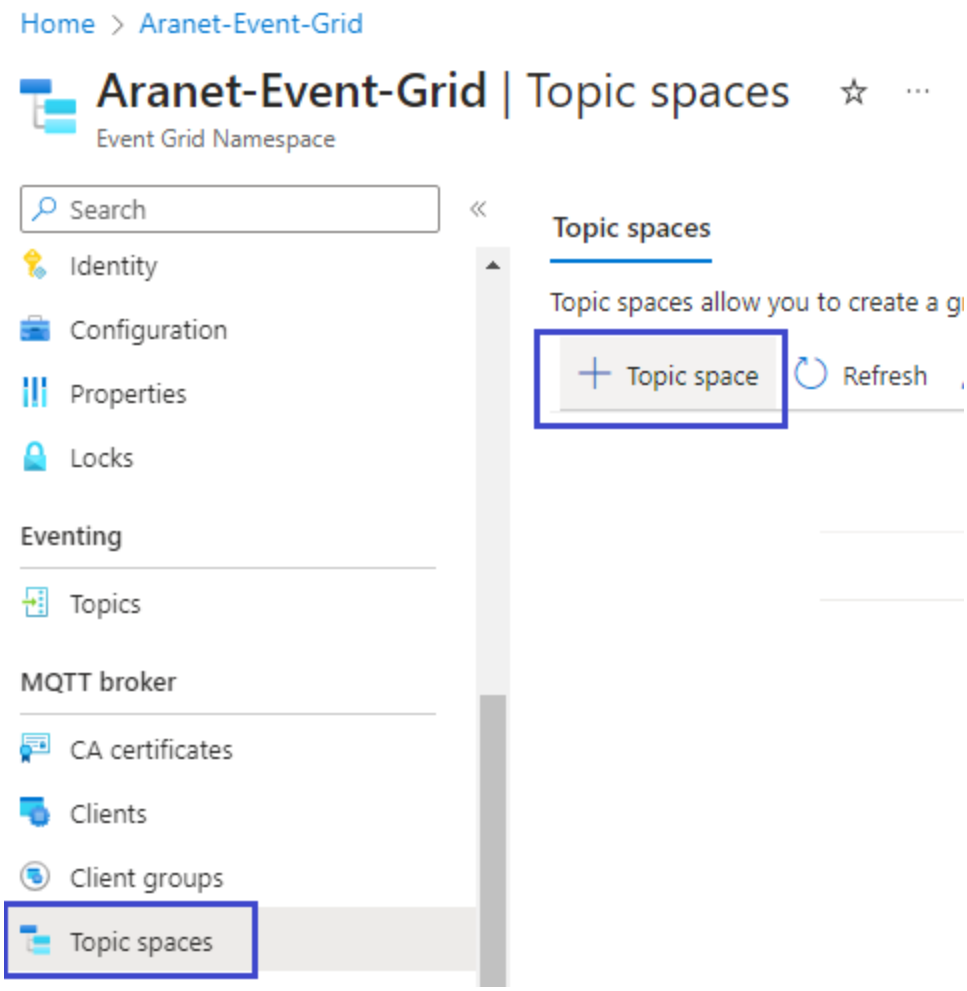
- Client Authentication Name: <Aranet base station **serial number**>
- Client Certificate Authentication Validation Scheme: **Subject Matches Authentication Name**

Set **Connection Status** to **Enabled** and press "**Create**" to add the new client for the Event Grid Namespace MQTT broker.

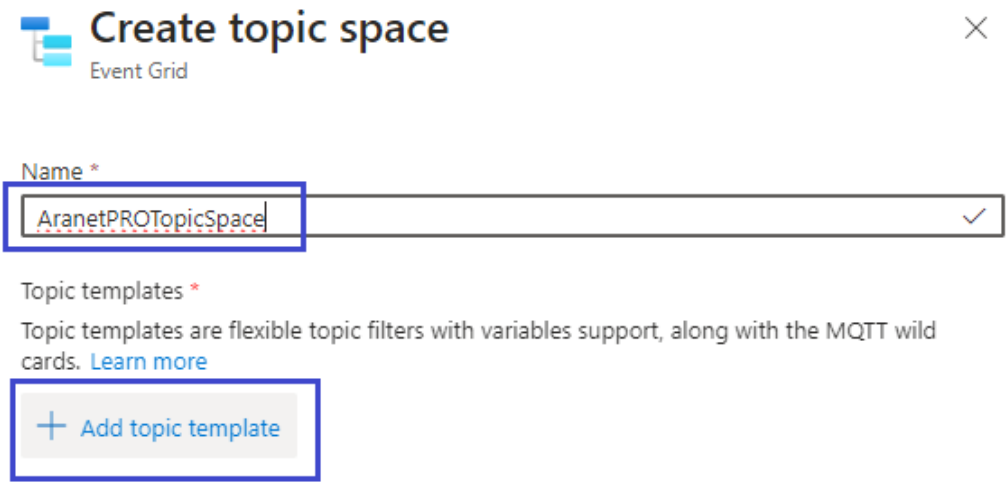


Create root topic for the Event Grid Namespace MQTT broker

In order to publish and subscribe on MQTT messages additional configuration step – creation of topic must be performed. For this proceed to the Event Grid Namespace MQTT broker section "**Topic spaces**" and create a new **Topic space** by pressing "+".

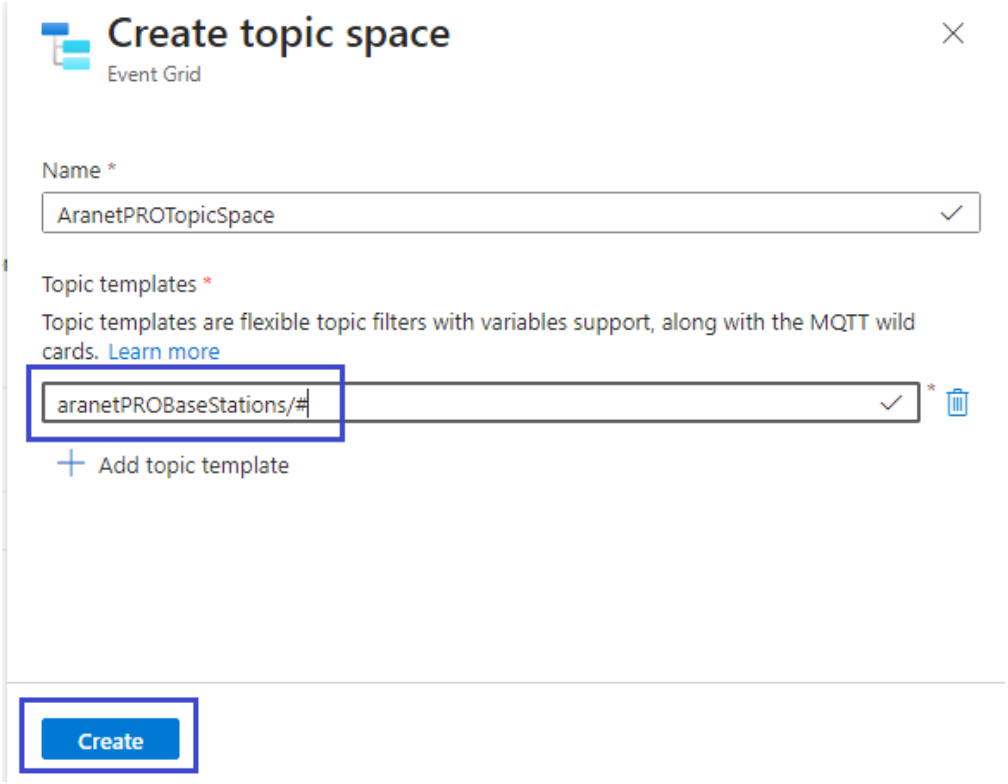


Give a **Name** for the Topic space. This name will be used later in the **Permission bindings** (publish and subscribe access rights) configuration. Press "**Add topic template**" to add a new topic template for this Topic space.



For the Topic template set the topic: **`aranetPROBaseStations/#`**

IMPORTANT: **`aranetPROBaseStations`** can be replaced with any other name. Topic template string must end with '**/#**'.



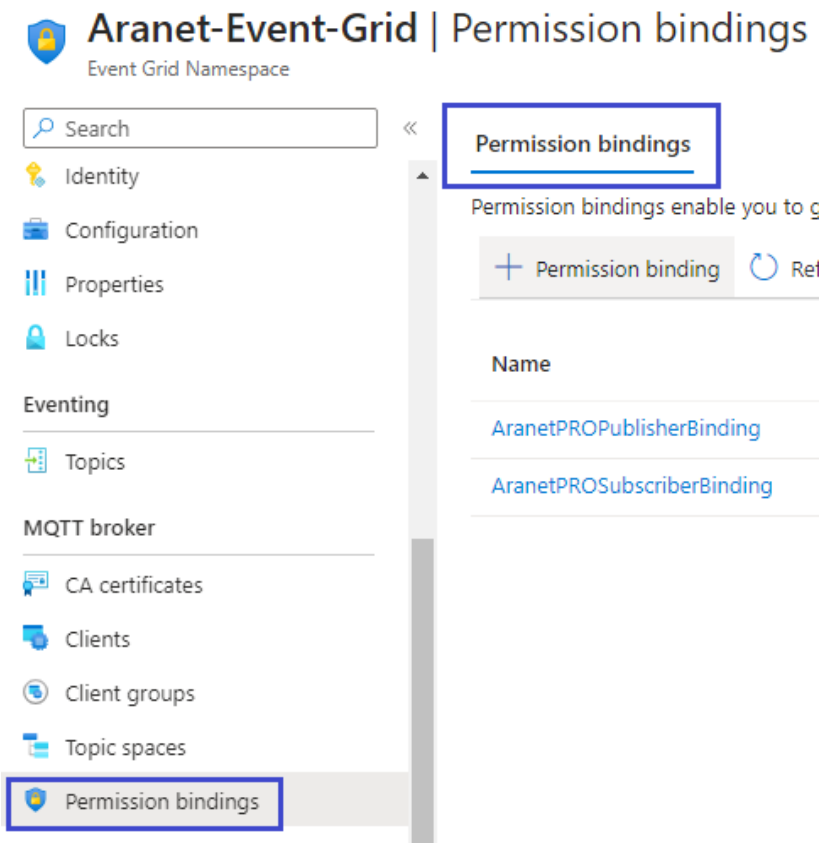
Later in this configuration example manual the topic template **`aranetPROBaseStations`** will be used in Aranet PRO MQTT configuration as the "**Root topic**" string.

Finally press "**Create**" button to add a new topic template.

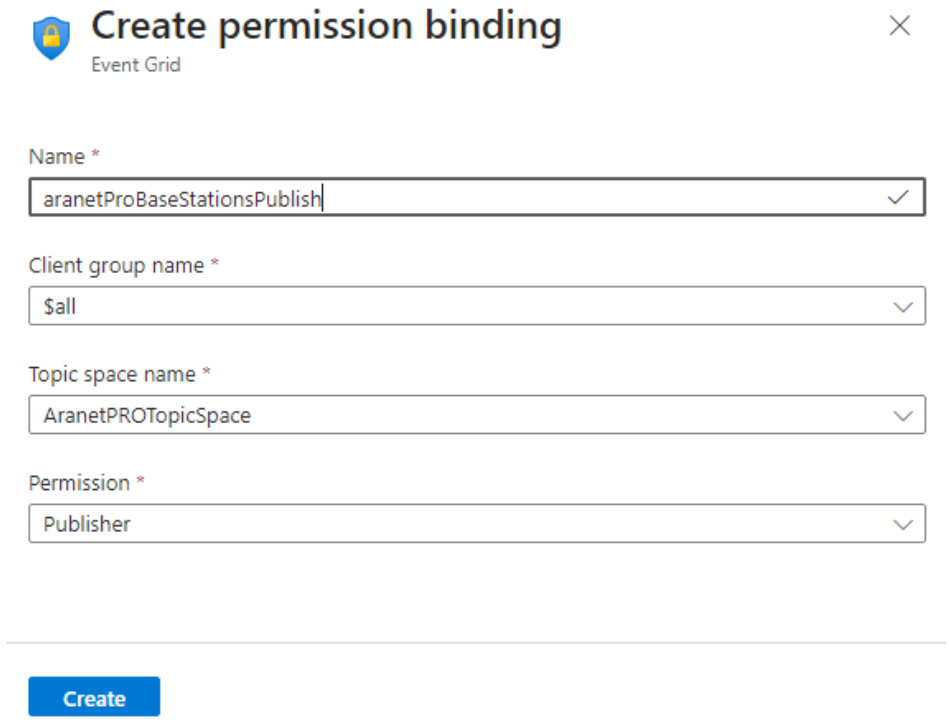
NOTE: in the scenario where multiple base stations are connected to the same MQTT broker hostname, the same topic template can be used across all base stations for publishing and subscribing to MQTT messages.

Setup topic Permission bindings for the Event Grid Namespace MQTT broker

Proceed to the Event Grid Namespace MQTT broker section "**Permission bindings**". Press on "+" to create a new "Permission binding" for MQTT message **publishing** permission.

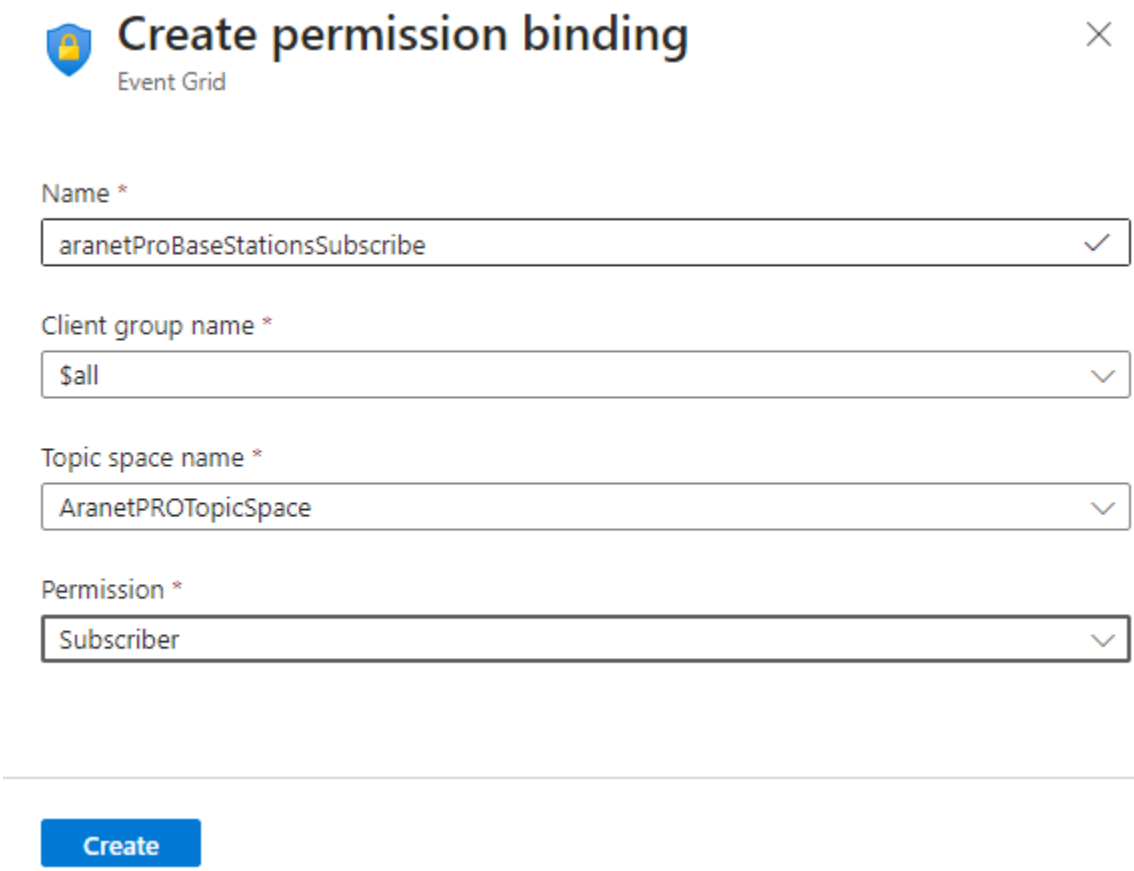


Create permission for the **Publisher** with following settings:



Press “**Create**”. Permission for **Publisher** has been created.

Now press on “+” to create a new “Permission binding” for MQTT message **subscribe** permission. Create permission for the **Subscriber** with following settings:

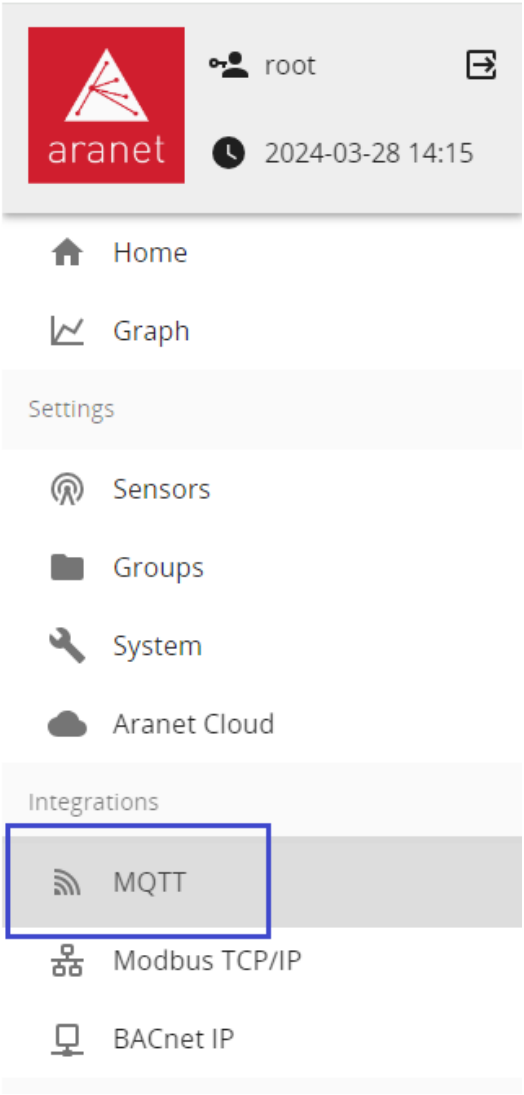


Press “**Create**” to add permission for the **Subscriber**.

Now Event Grid Namespace MQTT broker configuration is completed. Proceed to Aranet PRO base station to configure MQTT client settings in order to connect to Event Grid Namespace MQTT broker.

Setup Aranet PRO connection with Event Grid Namespace MQTT broker

Open web GUI of your Aranet PRO base station and proceed to **Integrations**: **MQTT** section.



Aranet PRO MQTT Connection settings

- Enable: ON
- Host address: **MQTT hostname** of your available Event Grid Namespace
- Port: **8883**
- Protocol version: **MQTT v5**
- keepAlive: 30 seconds
- Authentication: OFF
- QoS level: **0** or **2** (connection is being dropped by using QoS: 1)
- Root topic: **`aranetPROBaseStations`**
- Sensor measurement format: **raw** or **JSON**
- Encryption: **TLSv1.2**

- Validate host certificate: OFF
- Supply client certificate: ON
- Client private key: upload **client.key** file
- Client certificate: upload **client.crt** file

Connection successful
Status (2024-03-28 15:39)

Enable

Host address *
[redacted]
54 / 255

Port *
8883

Protocol version
MQTT v5

keepAlive *
30

Authentication

QoS level
0

Root topic *
aranetPROBaseStations
13 / 100

Sensor measurement format
raw

Encryption
TLSv1.2

Validate host certificate

Supply client certificate

Client private key
1024/2048 bit PEM encoded

Signature:
[redacted]

MQTT_CLIENT.KEY REGENERATE

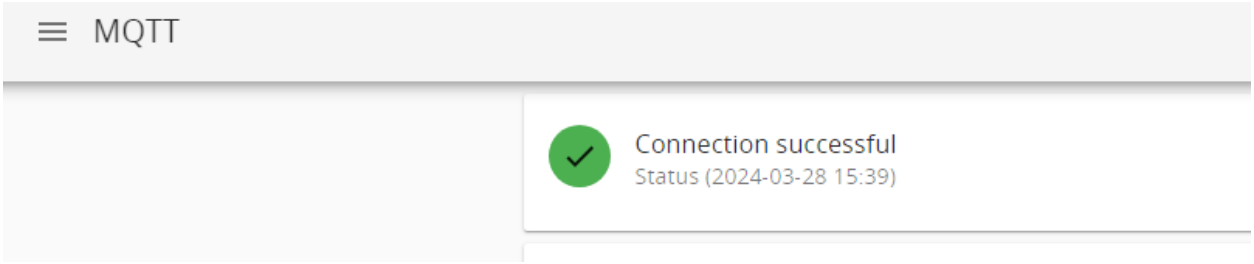
mqttClient.csr

Client certificate
1024/2048 bit PEM encoded

Signature:
[redacted]

MQTT_CLIENT.CRT

Press  to save the configuration. If all the steps were performed correctly Aranet PRO MQTT base station MQTT client process will report status “**Connection successful**”.



Now messages of the Arent PRO base station MQTT client are being published to the Event Grid Namespace MQTT broker.