1.0.0

Operating instructions manual

netFIELD App OPC UA to MQTT Converter

DOC210305OI1.0.0EN | Revision 1.0.0 | English | Released | Public

empowering communication

Table of Contents

1 About this document

1.1 Description of the contents

This document describes the **netFIELD App OPC UA to MQTT Converter** application container. The converter will also be referred to as "OPC UA to MQTT Converter" or "the converter".

Here you will find instructions on how to deploy and configure the application container.

1.2 List of revisions

Index	Date	Author	Revision
1.0.0	2024-07-05	NAM	Document created

Table 1. List of revisions

1.3 Conventions in this document

The terms *Edge Device* and *Edge Gateway* in this document refer to all devices and virtual machines running the *netFIELD Operating System (netFIELD OS)*, including the *netFIELD OS Datacenter* on virtualization platforms.

Admonitions

Notes, operation instructions and results of operation steps are marked as follows:

TIP | This is a tip with additional information.

NOTE | This is a note that explains something about the text.

IMPORTANT | This is a more important version of a note.

CAUTION | This is less severe than a warning but more important than a note. Not adhering to this could lead to undesired effects.

WARNING | This is a warning. Not adhering to this could lead to data loss or other more severe effects.

User instructions

User instructions in documents will look like this:

→ Goal

a. Step 1
b. Step 2
c. Step n

⇒ Result

2 Introduction

2.1 Brief description

The **netFIELD App OPC UA to MQTT Converter** acts as an OPC UA client, aggregating configurable data objects from one or more OPC UA servers, and publishing them to an MQTT broker (like e.g. *mosquitto*) through its MQTT client.

Key features

- Capable of aggregating data from multiple OPA UA servers at a time
- Capable of consolidating all aggregated data in a single MQTT broker
- It can be seamlessly integrated into any existing message network that supports an MQTT Broker
- Works with any TCP/IP based messaging network and over standard physical Ethernet ports
- Is the quickest method to support OPC UA messages next to MQTT messages
- Requires no alteration in the OPC UA servers to pass the data to the MQTT broker
- Secure-by-design by supporting common authentication methods and ensuring data confidentiality through encrypted transmissions
- Keeping data sovereignty at any time of the communication chain

Like all netFIELD application containers, the OPC UA to MQTT Converter runs in the **IoT Edge Docker** of a netFIELD Edge Gateway (or netFIELD OS Datacenter) and can be deployed via the netFIELD Portal or on any OCI compliant container engine. The app can be configured either via Remote Control from the netFIELD Portal or via local Ethernet access (see section Configuration for more information).

2.2 General Requirements

Requirements

- netFIELD Edge Gateway or netFIELD OS for virtual machines
- MQTT Broker (on the same device or reachable network)
- MQTT Client for monitoring the resulting topics

2.2.1 Memory

The RAM needed by the container depends on the amount of data that you intend to capture and process in your application. We recommend you to provide at least **1 GByte of free RAM** on your Edge Device (ideally 2 GByte or more). In use cases with a stable amount of little data processing, less than 1 GByte RAM might be sufficient.

2.2.2 MQTT broker

The *netFIELD App OPC UA to MQTT Converter* container publishes or retrieves the acquired data via MQTT and thus requires an MQTT broker for operation. The MQTT broker can run on the same host or on a different host machine in your local IT network.

2.2.3 Limitations

- OPC UA write operations are not supported by the app
- Connecting to OPC UA Servers via HTTPS is not supported by the app

3 Use cases

In the use case depicted below, the netFIELD App OPC UA to MQTT Converter runs in the **IoT Edge Docker** of the **netFIELD OS** of an **OnPremise** Edge Gateway. The gateway is connected to an Ethernet network that contains multiple OPC UA servers and an MQTT Broker. The embedded OPC UA client of the converter subscribes to the configured OPC UA servers, monitors the selected nodes and converts them into MQTT topics. The topics are published at the configured intervals to the configured MQTT Broker:

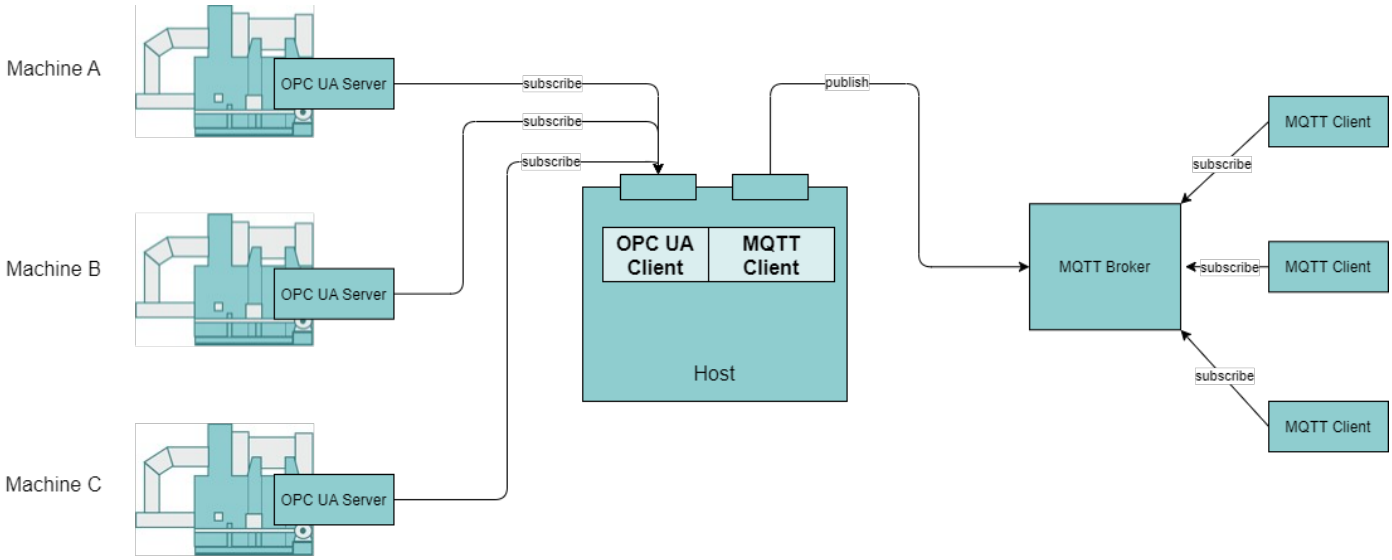


Figure 1. netFIELD App MQTT to OPC UA Converter with MQTT to OPC UA Converter example

Note that the MQTT to OPC UA Converter and/or the MQTT broker could also be running in a different Docker instance or even on a different device, if connected to the OnPremise device via Ethernet.

4 Start parameters of the container

NOTE The application container will be offered with a suitable configuration. Changing the start parameters and configuration is optional.

PortBindings

`"5003:5001"`

Port for the internal REST Server. Only needed for environment `RUNTIME_TARGET=datacenter`

Binds

Bind	Description
`netfield-app-opc-ua-to-mqtt-converter-data:/app/appData`	Volume for Application data
`/etc/gateway/mqtt-config.json:/mqtt-config.json:ro`	Optional file which contains the default MQTT config, the application will create a default config and you can change it via the UI. **Snippet 1. Format** `{ "schemaVersion": 1, "connectTimeout": 300, "serverURIs": [ "tcp://localhost:1883", "tcp://mosquitto:1883" ], "mqttVersion": 3 }`
`/usr/share/ca-certificates/:/usr/share/ca-certificates/`	CA certificates from the host system.
`/etc/shadow:/etc/shadow:ro`	User definition and hashed password from the host system.
`/etc/hostname:/etc_host/hostname:ro`	Hostname of the host system. Used in the application certificate and endpoint.
`/usr/local/:/host`	Path where the UI is copied on our systems and this path is also used to store the PKI of the application.

Table 2. Binds

Environment variables

Variable	Description
`LOGLEVEL`	Specify which severity you want to see in the logs. Possible values: - fatal - error - warn (Default) - info - debug - verbose
`RUNTIME_TARGET`	Specifies if the operation mode of the container. Possible values: - datacenter - netfield - iotedge
`MAXSTRINGLENGTH`	Specifies the maximum length of string which can be forwarded (MQTT payload size). Default: `102400`.
`ENCRYPTIONKEY`	Defines a "portable" encryption key for the built-in OPC UA Client (see below)

Table 3. Environment variables

OPC UA Encryption Key Environment Variable

The encryption key is used by the OPC UA Client app to generate a security hash tag for server access credentials when you add a new OPC UA Server (that requires a certificate or user name and password) to your local configuration.

This ensures that the credentials in the configuration of your OPC UA Client instance become “portable”; i.e. that they can be used by other instances of the OPC UA Client app (e.g. running on other netFIELD Edge Devices or Datacenters), when the configuration is exported and imported accordingly.

Note that every other instance of the OPC UA Client that shall use an imported configuration must have the same `encryptionkey` in its environment variables. Note also that you can use the given `PleaseChangeThisencryption` key as default key if you do not want to define your own “personal” key. However, we highly recommend changing this key.

5 Configuration

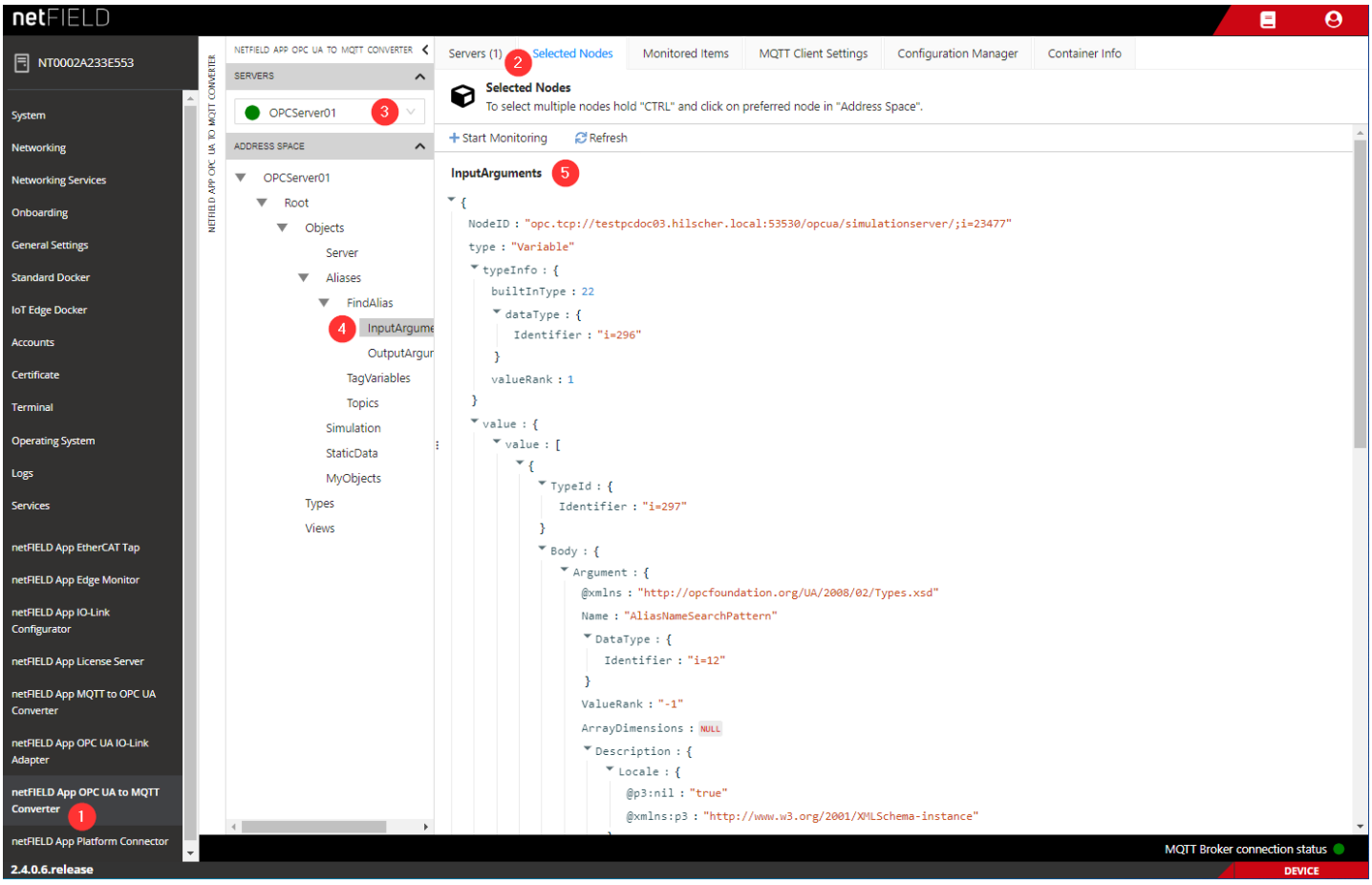
Once the container is deployed, you need to configure which OPC UA nodes will be converted and configure the MQTT settings for the individual topics.

Optionally you can configure the MQTT Broker if you do not wish to use the default settings.

5.1 Overview

The netFIELD App OPC UA to MQTT Converter container provides a configuration GUI in the Local Device Manager of the netFIELD OS. This configuration GUI is automatically plugged-in when the container is deployed. After having established a connection to the Local Device Manager (e.g. by Remote Control from the netFIELD Portal, see section *Remote Control* in the *netFIELD Portal* manual, DOC190701OIxxEN), the configuration GUI can be selected in the navigation panel **(1)** of the Local Device Manager.

NOTE Note that it might take a few minutes after deployment before the netFIELD App OPC UA to MQTT Converter entry becomes visible in the navigation panel. You may also have to reload the web page in your browser by pressing F5 on your keyboard.

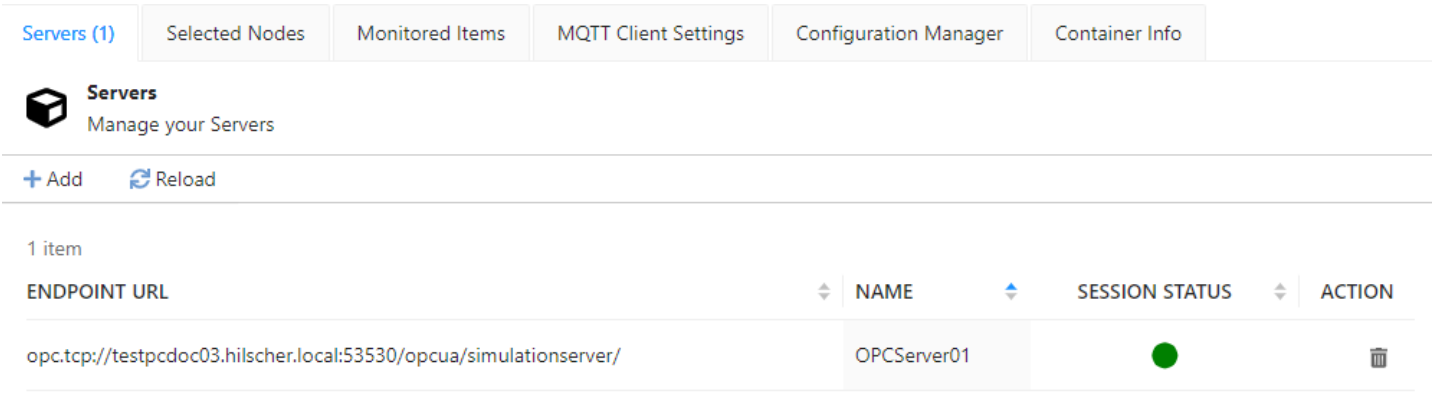


The tabs in the header of the screen **(2)** allow you to navigate through the configuration and management options of the netFIELD App OPC UA to MQTT Converter.

The "SERVERS" **(3)** and "ADDRESS SPACE" **(4)** menus on the left allow you to pick OPC UA data nodes from the selected server.

Once a node is selected, the "Selected Nodes" tab will open and show the JSON data **(5)** for the node.

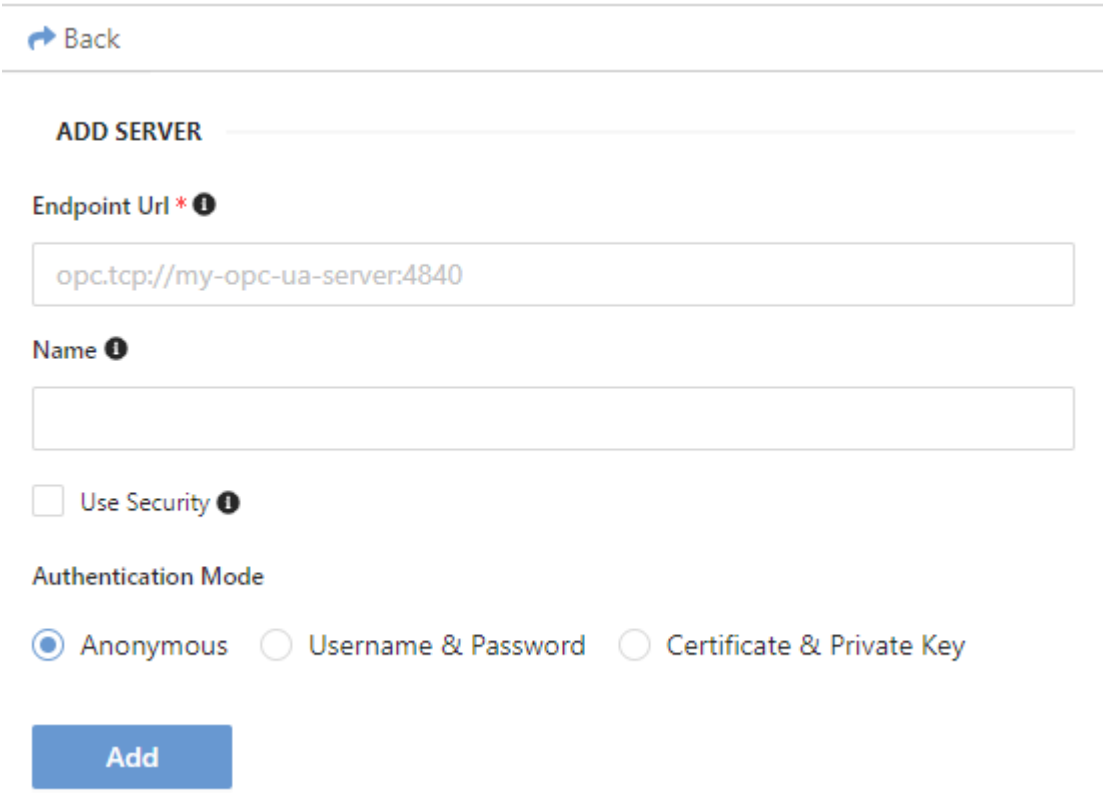
5.2 Servers



In this tab you can manage the OPC UA servers that the converter will conntect to. Click the + Add button to open the Add Server dialog.

Once added and connected, the configured servers will become available in the "SERVERS" dropdown menu on the left.

5.2.1 Add Server



Option	Description
Endpoint URL	The qualified URL for the OPC UA server endpoint
Name	A name for this entry
Use Security	Tick this box to enable authentication against the OPC UA server endpoint

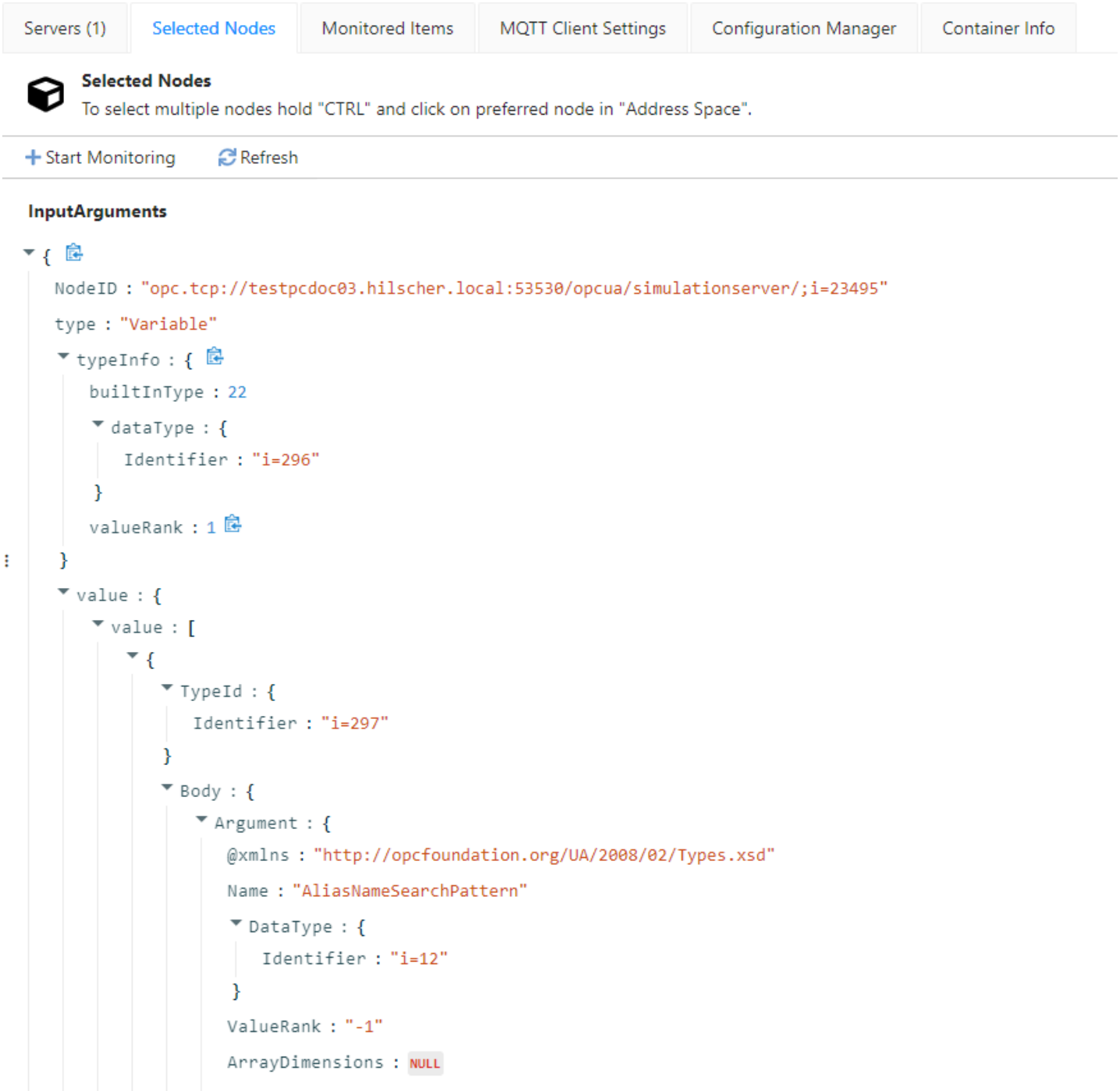
Option	Description

Authentication Mode	Set the type of authentication mode used:
	`Anonymous`
	Provide no authentication details (not recommended)
	`Username & Password`
	Provide a user name and password
	`Certifcate & Private Key`
	Provide the unencrypted contents of the certificate and private key for accessing the OPC UA server. Must be in PEM format.

Table 4. Add Server Dialog Options

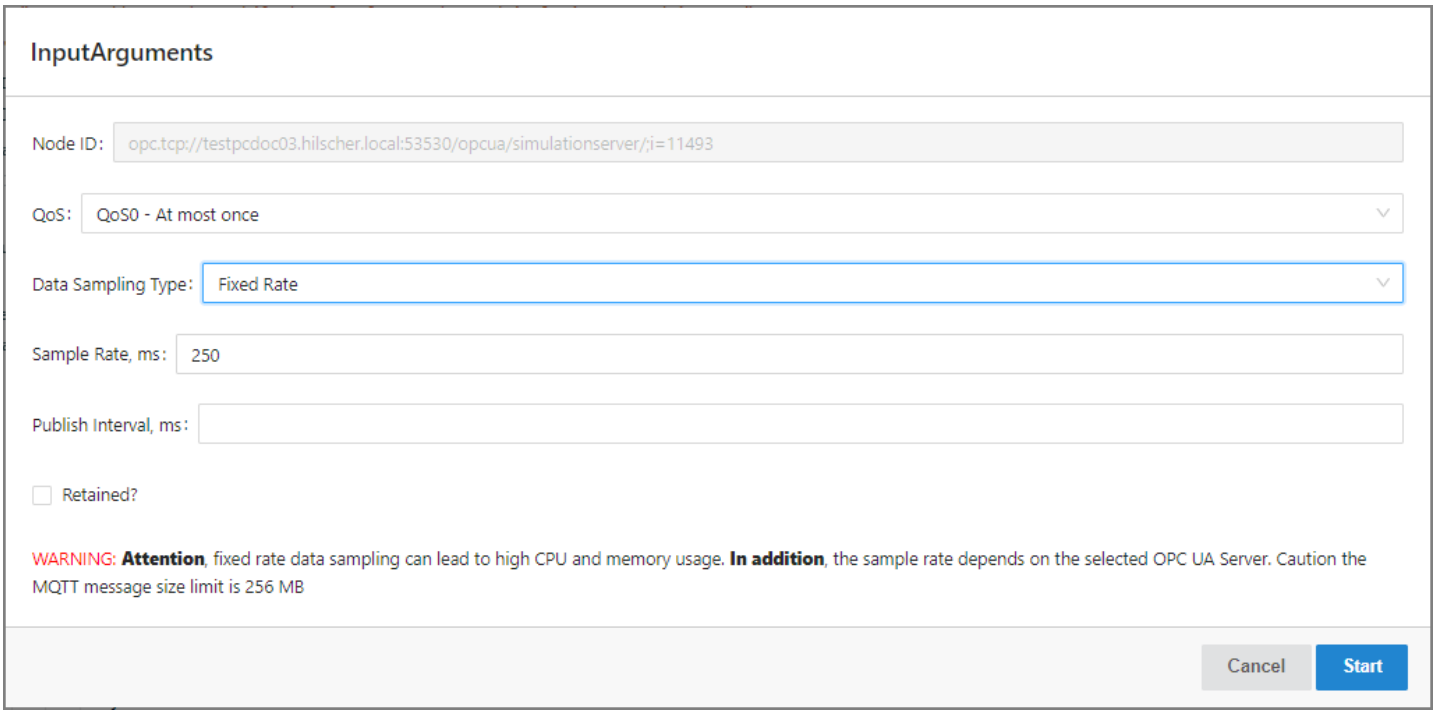
5.3 Selected Nodes

The "Selected Nodes" tab will automatically be activated when clicking on any of the OPC UA objects in the "ADDRESS SPACE" browser. If no current selection is active in the object browser, the last enabled object will be displayed.



The servers' available data node objects can be selected with the "ADDRESS SPACE" list menu. Click on the server name and then on **ROOT › Objects**. The data objects can be expandeds in a similar way. When you select a node the "Selected Nodes" tab will open and show the JSON representation of the OPC UA data.

When a node has an associated value, the button + Start Monitoring will appear at the top of the tab above the JSON view. A click on this button will display the configuration dialog for the MQTT topic settings of the selected node.



Option	Description
Server	Select the server from the dropdown menu

QoS	MQTT Quality of Service
	`QoS0`
	At most once
	`QoS1`
	At least once
	`QoS2`
	Exactly once

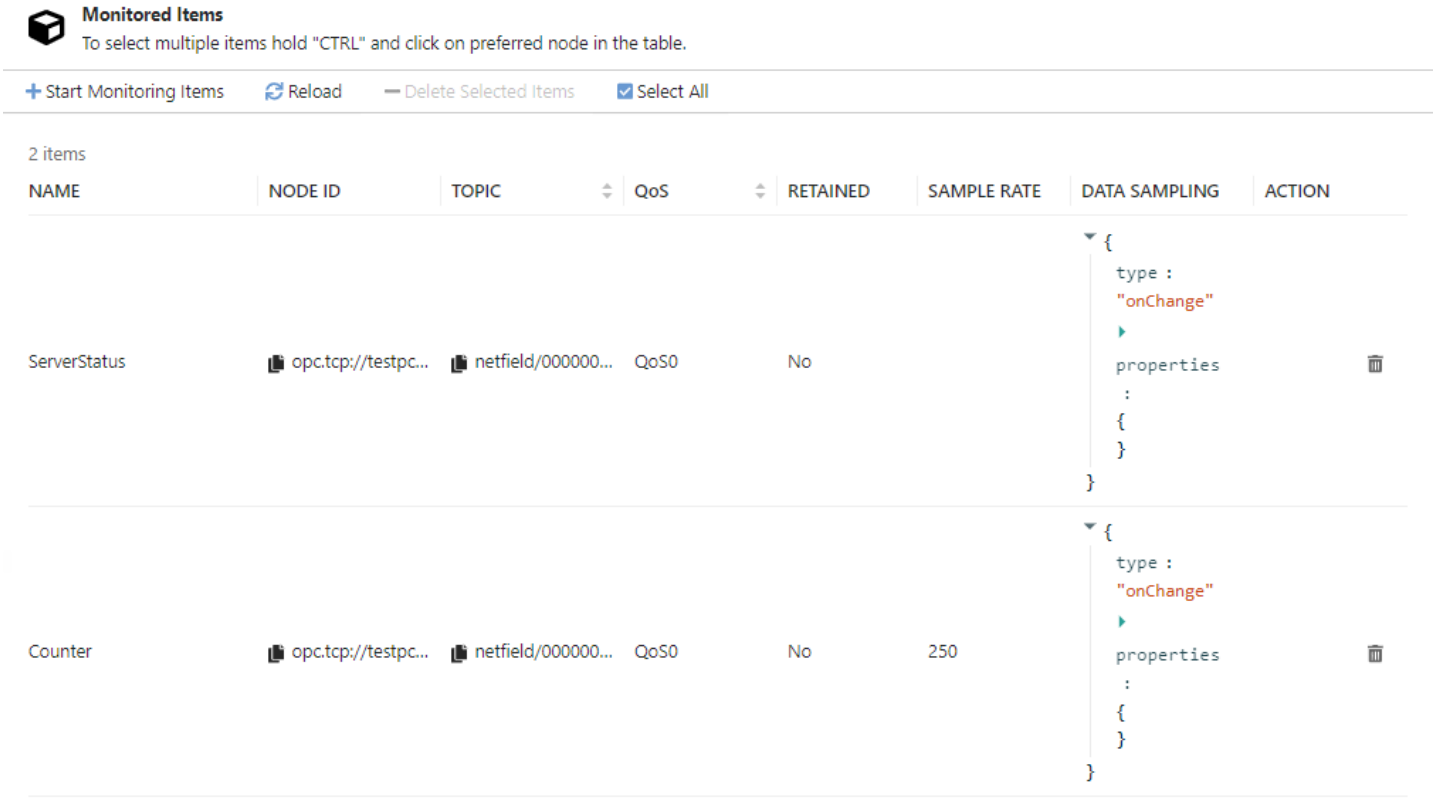
Data Sampling Type	Select how often the data should be sampled from the OPC UA server.
	`On Change`
	Data will be refreshed according to the configured sample rate and published when there was a change.
	`Fixed Rate`
	Data will be refreshed at the configured sample rate, collected as multiple values and published in the configured publish interval. **Note**: Please note the limitations of a fixed rate sampling approach.

Sample Rate, ms	Interval between data refresh from the OPC UA server (in milliseconds).
Publish Rate, ms	(Only with Fixed Rate Sampling) Publishing interval of the data set.
Retained?	Enable MQTT message retention for this topic.

Table 5. Node Monitoring Options

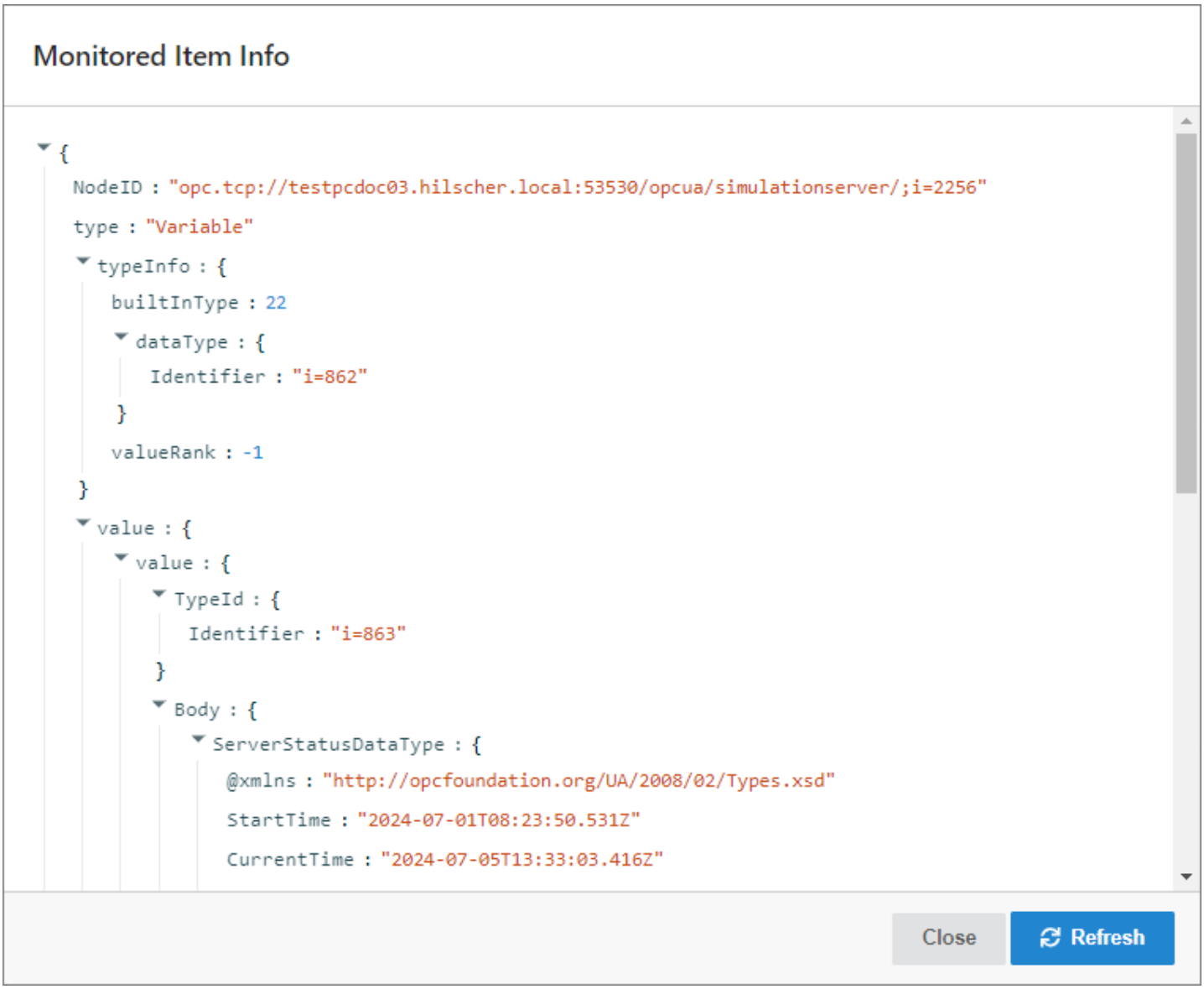
5.4 Monitored Items

The items selected for monitoring in the Selected Nodes tab will be listed here.



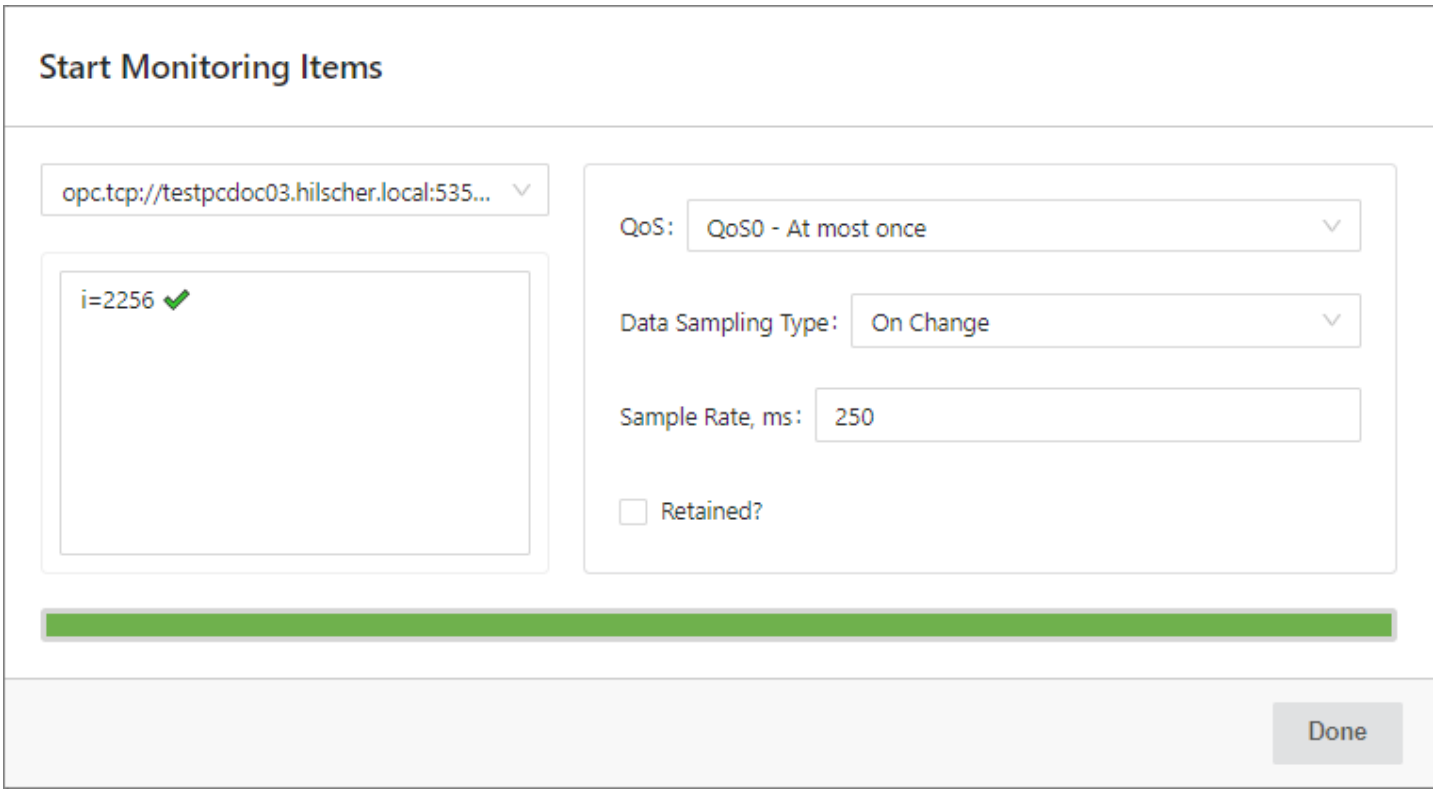
You can remove single or multiple items by holding down the "CTRL"-Key and clicking on the items to select them. The rows will change to a darker color to indicate their selected status. Then click on — Delete Selected Items.

A click on the row of an item will reveal the JSON data for the selected item. A click on "Refresh" will update the view to the latest data. You can close the dialog with "Close".



Adding items by OPC UA ID

You can add OPC UA data objets via their ID by clicking on + Start Monitoring Items. Then enter the ID in the field on the left and set the MQTT options on the right. Then click "Start" to monitor. If the settings are correct, you will see a green tick mark and can confirm the dialog with "Done".



5.5 MQTT Client Settings

In the **MQTT Client Settings** tab, you can configure the settings of the embedded MQTT client of the OPC UA to MQTT Converter app. By default, the app uses the standard MQTT client settings of the netFIELD OS. According to these default settings, the app first tries to connect to any MQTT broker under the URI `tcp://localhost:1883`, then (if connecting to the first URI fails) tries to connect to a *mosquitto* broker under the URI `tcp://mosquitto:1883`.

If you cannot use these standard MQTT client settings for your OPC UA to MQTT Converter app – because you want to connect it to a different broker (under a different URI and/or with different parameters/credentials) – you must uncheck the **Use general settings** option and enter your new MQTT settings in the configuration fields that are now displayed:

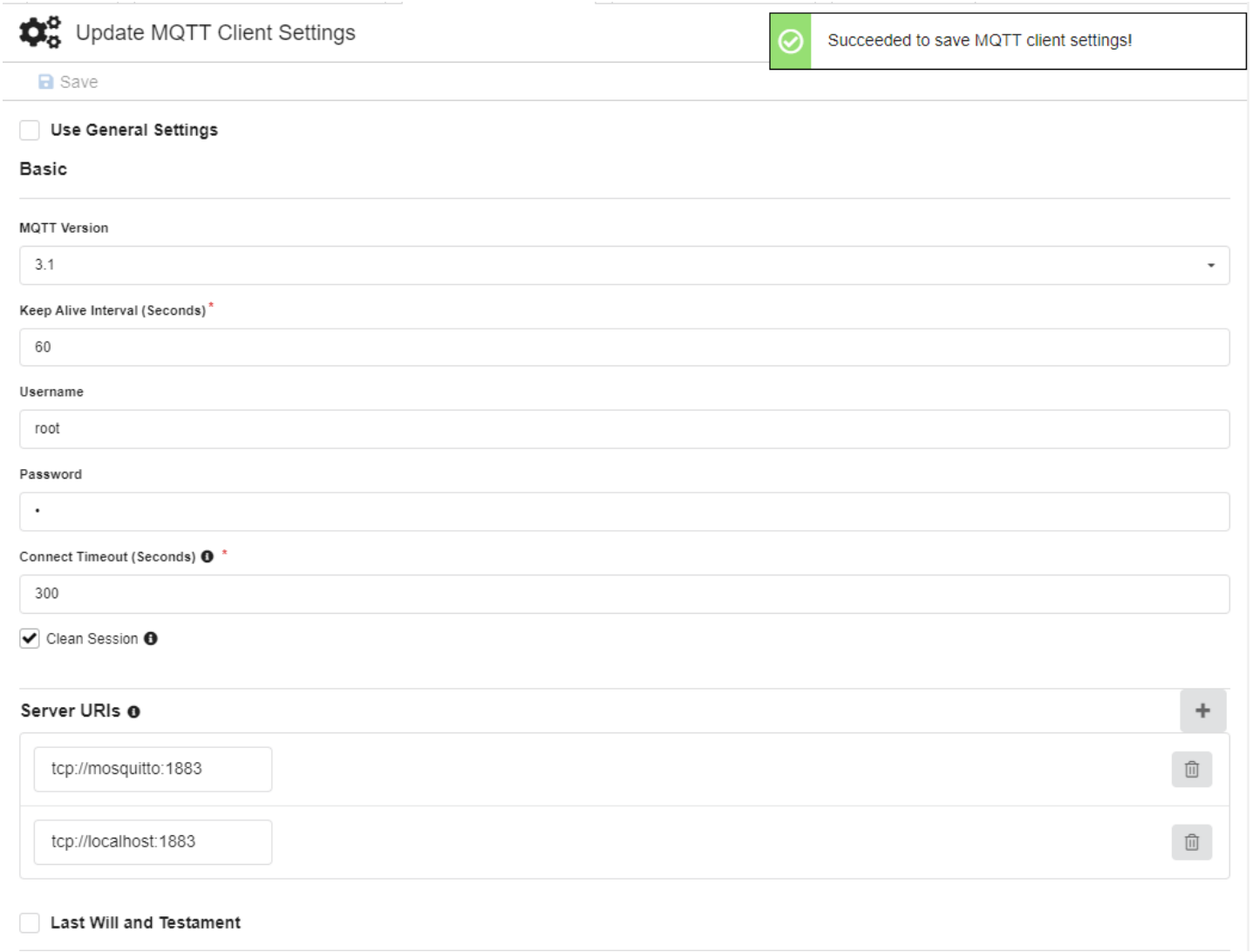


Figure 2. MQTT Client Settings

NOTE Changes to the MQTT Client Settings that you make here for your OPC UA to MQTT Converter app will not affect the standard "global" MQTT Settings of your netFIELD OS.

The standard "global" MQTT client settings of the netFIELD OS can be viewed (and changed if necessary) in the Local Device Manager under **General Settings › Default MQTT Client Settings**.

Element	Description
MQTT version	MQTT version to be used (depending on the MQTT broker).
Keep alive interval (Seconds)	Defines the maximum length of time in seconds that the broker and client may not communicate with each other.
User name	User name for authentication at the broker (if implemented and required by the broker). Note that the *mosquitto* broker deployed from the netFIELD Portal does not require login authentication.
Password	Password for authentication at the broker (if implemented and required by the broker). Note that the *mosquitto* broker deployed from the netFIELD Portal does not require login authentication.
Connect timeout (Seconds)	Defines the maximum length of time in seconds that is allowed for completing the connection process.
Clean session	If **Clean session** is selected, the client does not want a persistent session (meaning that if the client disconnects for any reason, all information and messages that are queued from a previous persistent session are lost). If **Clean session** is unchecked, the broker creates a persistent session for the client.
Server URIs	Server URI of the MQTT broker. **Note**: When multiple server URIs are specified, the client will try to connect to each server one after the other, starting with the first server in the list. If a server connection is successfully established, only this connection will be used. The client will not open multiple connections to multiple servers simultaneously.

Last Will and Testament	Select this option if you want to use the "last will and testament" (LWT) feature of MQTT. (I.e. to notify other clients about an unexpected loss of connection to the broker)
	
	`Topic name`
	Topic name of LWT message
	
	`Retained`
	LWT will be retained on Broker even if a client has already received it.
	
	`Quality of Service`
	QoS of LWT message
	
	`Message`
	Message text, e.g. "unexpected loss of connection"

SSL / TLS	Select this option if you want to use SSL/TLS encryption for creating a secure connection to the MQTT broker.
	
	`File name and path to private key in PEM format`
	Path to the private key on the device; e.g.: `/etc/ssl/private/client-key.pem`
	
	`File name and path to certificate chains in PEM format`
	Path to the certificate chains on the device; e.g.: `/etc/ssl/services/client-cert.pem`
	
	`Override the trusted CA certificates in PEM format`
	Path to override the trusted CA certificates on the device; e.g.: `/etc/ssl/services/ca-cert.pem`
	
	`Enable verification of the server certificate`
	If this option is disabled, the OPC UA to MQTT Converter app will also accept invalid certificates from the broker (not recommended).
	
	Note: This option is for expert users only! In the standard use case, in which the *mosquitto* broker and the OPC UA Converter app are running on the same device, a secure SSL/TLS connection is not necessary (because the connection is "internal" and the overhead of the secure connection can thus be avoided). If you want to use SSL/TLS encryption anyway, see section Using SSL/TLS encryption (optional) for further information.

Table 6. MQTT Client Settings

a. Click Save button to save your new MQTT Client Settings.

⇒ The **Succeeded to save MQTT client settings** message appears.

b. Check the **MQTT Broker connection status indicator** in the footer to see if the connection to the new server has been successfully established:

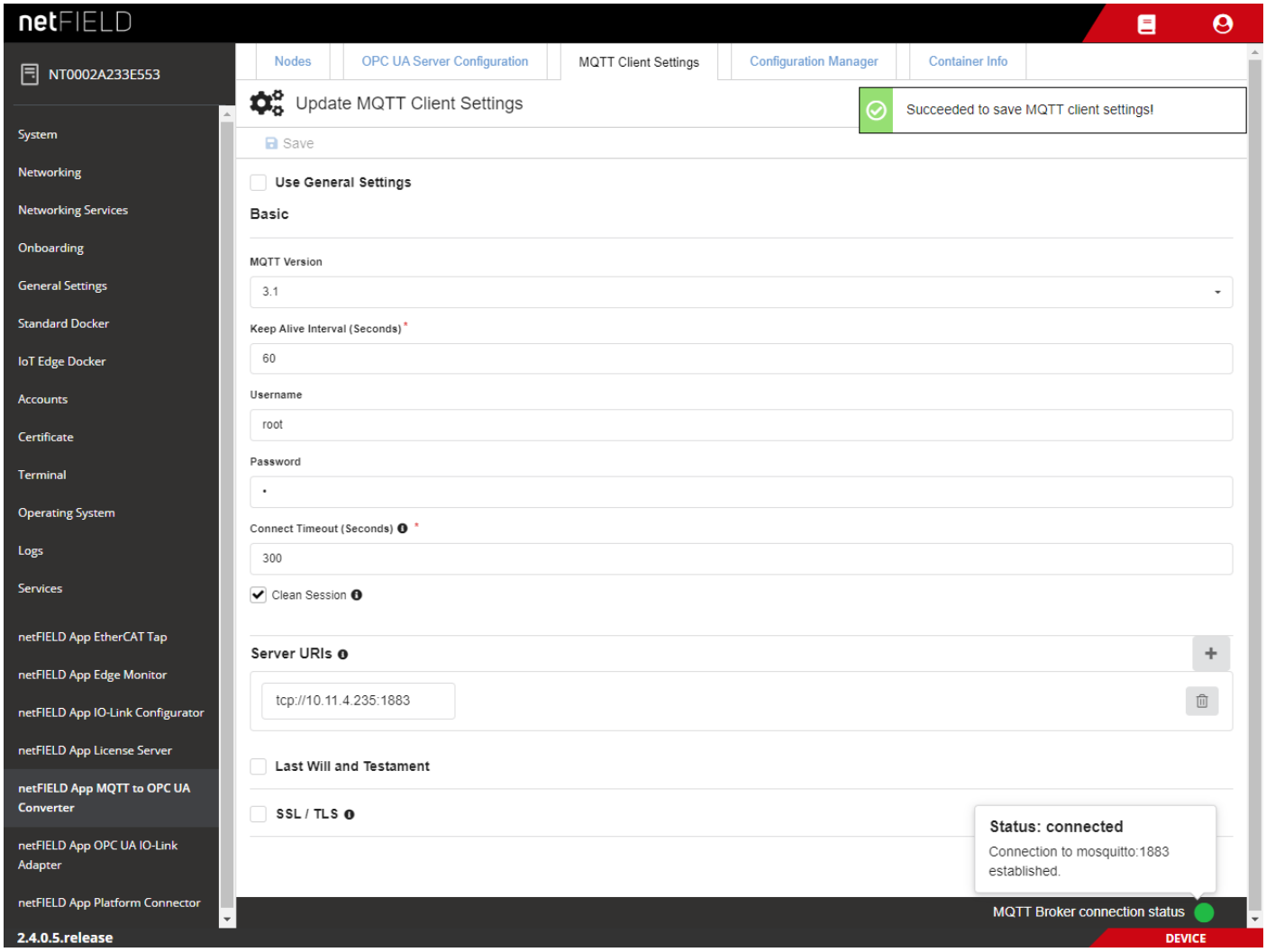


Figure 3. MQTT server connection status indicator in footer

5.6 Configuration Manager

In the **Configuration Manager** tab, you can save the OPC UA to MQTT Converter app configuration settings to your local PC. You can also restore a formerly saved configuration by uploading the configuration file. The download/upload function allows you to practically "clone" your configuration and use it in other OPC UA to MQTT Converter instances (e.g. running on other netFIELD Edge Devices or netFIELD OS Datacenters).

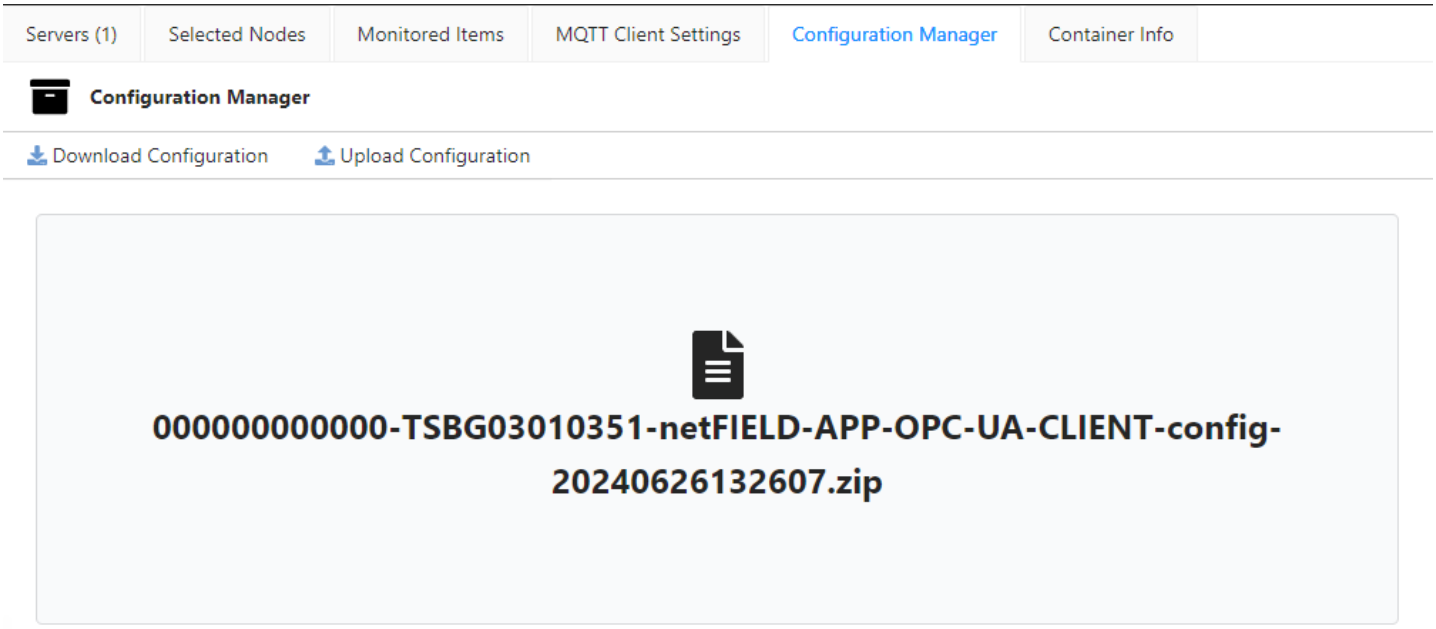


Figure 4. Configuration Backup

Save configuration

1. To save your current configuration, click **[Download Configuration]** button.

   ⇒ The configuration settings are saved to your local PC as ZIP file. The name of the ZIP file is made up by the gateway prefix, app name and date/time of the download. The download path depends on the settings of your web browser.

   NOTE The "gateway prefix" is by default the device ID of the Edge Device on which the OPC UA to MQTT Converter app is deployed. If you are using the app as "standalone" app - i.e. if the app has not been deployed in the IoT Edge Docker via netFIELD Portal -, the "gateway prefix" is the host name of the device.

Restore/import configuration

To restore a formerly saved configuration (or import it into other instances), you must first select the configuration ZIP file by dragging and dropping it from your desktop onto the grey field (as an alternative, you can open the standard Windows file selection dialog by clicking into the grey field).

After having selected the file, the **[Upload Configuration]** button is enabled, and you can now "load" the configuration by clicking the button.

IMPORTANT The Upload Configuration function will overwrite the current configuration settings. We recommend you to save your current configuration before using this function.

Figure 5. Upload Configuration

5.7 Container Info

The Container Info tab shows general information about the container.

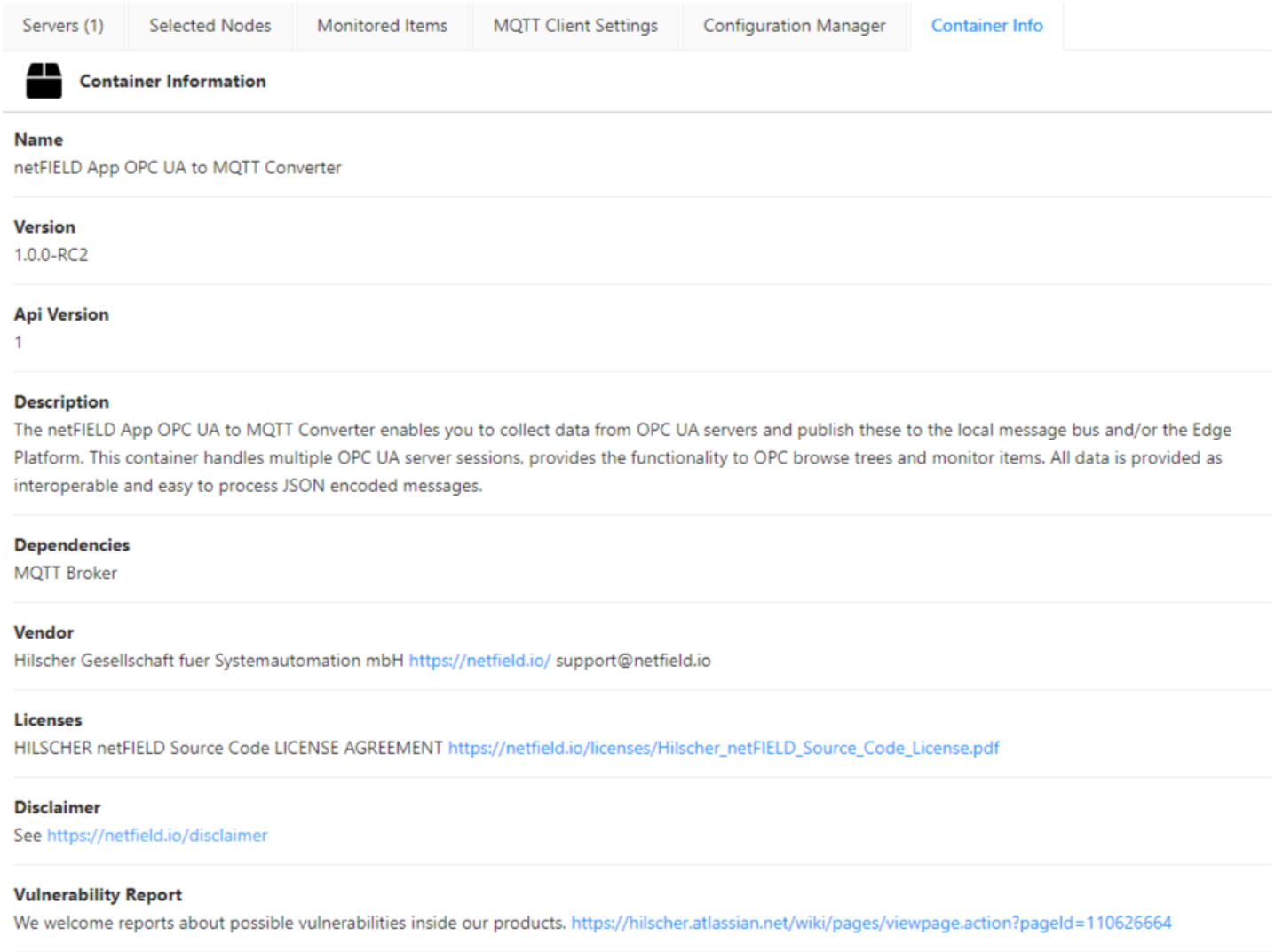


Figure 6. Container Info

Category	Description
Name	Container name
Version	Container software version
API Version	REST API version of the container
Description	Brief description of the function of the container
Dependencies	Other containers or components required for proper operation of the container
Vendor	Vendor of container
Licenses	Name of the software license(s), under which the container was published
Disclaimer	Path/link to the software license(s)
Vulnerability Report	Path/link to the Hilscher Vulnerability Handling & Management web page

Table 7. Container Info tab

6 Good to Know

6.1 Using SSL/TLS encryption (optional)

Please note the following if you intend to use SSL/TLS encryption:

The certificates and key files that the embedded MQTT client of the netFIELD App MQTT to OPC UA Converter container needs for establishing a secure SSL/TLS connection to the MQTT broker are not managed by the OPC UA Server container app itself. Instead, they are to be stored on the Edge Device and mapped into the container from the netFIELD OS. For this mapping, the following standard directories are mapped into the container when you use the default Create Options in the netFIELD Portal:

`/etc/ssl/`

`/usr/share/ca-certificates/`

NOTE If you require different directories for your use case, you may change the mapping of these "bind mounts" in the default Create Options of the container in the netFIELD Portal (see section Create Options).

As a user, you can store your required keys and certificates in these directories. By selecting the SSL / TLS option on the MQTT Client Settings page (see section MQTT Client Settings), you can allow the embedded MQTT client of the OPC UA Server app container to use these files for establishing its secure SSL/TLS connection.

Note that these keys and certificates must be stored in PEM format (a specific file format for storing this kind of data) and that you have to specify the full path to the appropriate PEM file in the corresponding fields of the MQTT Client Settings page. For example:

File name and path to private key in PEM format: `/etc/ssl/private/client-key.pem`

File name and path to certificate chains in PEM format: `/etc/ssl/services/client-cert.pem`

Override the trusted CA certificates in PEM format: `/etc/ssl/services/ca-cert.pem`

IMPORTANT If you intend to use more than one "secure" MQTT broker (as listed in the Server URIs field), and thus require several different certificates, you have to store them *in one single* PEM file. This is because it is not possible to specify a list of multiple paths to separate PEM files for individual brokers.

6.2 Container configuration data storage

The configuration data of the container is stored in the `netfield-app-mqtt-to-opc-ua-converter-data` Docker volume.

Your whole application configuration data - such as your MQTT configuration, activated publishers etc. - is stored here independently of the run state or the version of your netFIELD App OPC UA to MQTT Converter container. When you stop and restart the container, the configuration will be loaded from this volume again.

IMPORTANT **Automatic Upgrading**

The configuration data in this volume will be automatically migrated to the latest version when you deploy a newer version of the netFIELD App OPC UA to MQTT Converter.

CAUTION **No backwards compatibility**

Only upgrading towards *higher* versions is possible. If you try to start a lower container version with a newer configuration volume, the configuration will not be loaded, but will be cleared instead.

7 Appendix

7.1 Technical data

Product name	netFIELD App OPC UA to MQTT Converter
Item number	1917.059
Product type	Container As A Single Service (CAASS)
Download	Container accessible exclusively to netFIELD Cloud subscribers
Accounting model	Available to all netFIELD Cloud subscribers

Table 8. General

Processor	AMD64 or ARM64
Required RAM	min 200 MB
Container size	400 MB, decompressed
Aggregration interface	at least 1x Standard Ethernet Port if communication to external systems is required

Table 9. Hardware requirements

Operating system	Linux
Container engine	Yes, OCI compliant
External data sink/sources	MQTT Broker, OPC UA Server(s)

Table 10. Software requirements

Data inbound protocol	OPC UA (as a client)
Data inbound protocol	On change or at fixed rate >=100msec
Data outbound protocol	MQTT (as a client)
MQTT publishing interval	In accordance with the inbound protocol data rate

Table 11. Runtime properties

Container protection	Unprotected, but accessible to netFIELD Cloud subscribers only

Table 12. Licensing

Appendix A: Content listing

7.A.1 List of tables

7.A.2 List of figures

Appendix B: Legal Notes

Copyright

Important notes

Utmost care was/is given in the preparation of the documentation at hand consisting of a user's manual, operating manual and any other document type and accompanying texts. However, errors cannot be ruled out. Therefore, we cannot assume any guarantee or legal responsibility for erroneous information or liability of any kind. You are hereby made aware that descriptions found in the user's manual, the accompanying texts and the documentation neither represent a guarantee nor any indication on proper use as stipulated in the agreement or a promised attribute. It cannot be ruled out that the user's manual, the accompanying texts and the documentation do not completely match the described attributes, standards or any other data for the delivered product. A warranty or guarantee with respect to the correctness or accuracy of the information is not assumed.

We reserve the right to modify our products and the specifications for such as well as the corresponding documentation in the form of a user's manual, operating manual and/or any other document types and accompanying texts at any time and without notice without being required to notify of said modification. Changes shall be taken into account in future manuals and do not represent an obligation of any kind, in particular there shall be no right to have delivered documents revised. The manual delivered with the product shall apply.

Under no circumstances shall Hilscher Gesellschaft für Systemautomation mbH be liable for direct, indirect, ancillary or subsequent damage, or for any loss of income, which may arise after use of the information contained herein.

Liability disclaimer

The hardware and/or software was created and tested by Hilscher Gesellschaft für Systemautomation mbH with utmost care and is made available as is. No warranty can be assumed for the performance or flawlessness of the hardware and/or software under all application conditions and scenarios and the work results achieved by the user when using the hardware and/or software. Liability for any damage that may have occurred as a result of using the hardware and/or software or the corresponding documents shall be limited to an event involving willful intent or a grossly negligent violation of a fundamental contractual obligation. However, the right to assert damages due to a violation of a fundamental contractual obligation shall be limited to contract-typical foreseeable damage.

It is hereby expressly agreed upon in particular that any use or utilization of the hardware and/or software in connection with

- Flight control systems in aviation and aerospace;
- Nuclear fission processes in nuclear power plants;
- Medical devices used for life support and
- Vehicle control systems used in passenger transport

shall be excluded. Use of the hardware and/or software in any of the following areas is strictly prohibited:

- For military purposes or in weaponry;
- For designing, engineering, maintaining or operating nuclear systems;
- In flight safety systems, aviation and flight telecommunications systems;
- In life-support systems;
- In systems in which any malfunction in the hardware and/or software may result in physical injuries or fatalities.

You are hereby made aware that the hardware and/or software was not created for use in hazardous environments, which require fail-safe control mechanisms. Use of the hardware and/or software in this kind of environment shall be at your own risk; any liability for damage or loss due to impermissible use shall be excluded.

Warranty

Hilscher Gesellschaft für Systemautomation mbH hereby guarantees that the software shall run without errors in accordance with the requirements listed in the specifications and that there were no defects on the date of acceptance. The warranty period shall be 12 months commencing as of the date of acceptance or purchase (with express declaration or implied, by customer's conclusive behavior, e.g. putting into operation permanently).

The warranty obligation for equipment (hardware) we produce is 36 months, calculated as of the date of delivery ex works. The aforementioned provisions shall not apply if longer warranty periods are mandatory by law pursuant to Section 438 (1.2) BGB, Section 479 (1) BGB and Section 634a (1) BGB [Bürgerliches Gesetzbuch; German Civil Code] If, despite of all due care taken, the delivered product should have a defect, which already existed at the time of the transfer of risk, it shall be at our discretion to either repair the product or to deliver a replacement product, subject to timely notification of defect.

The warranty obligation shall not apply if the notification of defect is not asserted promptly, if the purchaser or third party has tampered with the products, if the defect is the result of natural wear, was caused by unfavorable operating conditions or is due to violations against our operating regulations or against rules of good electrical engineering practice, or if our request to return the defective object is not promptly complied with.

Costs of support, maintenance, customization and product care

Please be advised that any subsequent improvement shall only be free of charge if a defect is found. Any form of technical support, maintenance and customization is not a warranty service, but instead shall be charged extra.

Additional guarantees

Although the hardware and software was developed and tested in-depth with greatest care, Hilscher Gesellschaft für Systemautomation mbH shall not assume any guarantee for the suitability thereof for any purpose that was not confirmed in writing. No guarantee can be granted whereby the hardware and software satisfies your requirements, or the use of the hardware and/or software is uninterruptable or the hardware and/or software is fault-free.

It cannot be guaranteed that patents and/or ownership privileges have not been infringed upon or violated or that the products are free from third-party influence. No additional guarantees or promises shall be made as to whether the product is market current, free from deficiency in title, or can be integrated or is usable for specific purposes, unless such guarantees or promises are required under existing law and cannot be restricted.

Confidentiality

The customer hereby expressly acknowledges that this document contains trade secrets, information protected by copyright and other patent and ownership privileges as well as any related rights of Hilscher Gesellschaft für Systemautomation mbH. The customer agrees to treat as confidential all of the information made available to customer by Hilscher Gesellschaft für Systemautomation mbH and rights, which were disclosed by Hilscher Gesellschaft für Systemautomation mbH and that were made accessible as well as the terms and conditions of this agreement itself.

The parties hereby agree to one another that the information that each party receives from the other party respectively is and shall remain the intellectual property of said other party, unless provided for otherwise in a contractual agreement.

The customer must not allow any third party to become knowledgeable of this expertise and shall only provide knowledge thereof to authorized users as appropriate and necessary. Companies associated with the customer shall not be deemed third parties. The customer must obligate authorized users to confidentiality. The customer should only use the confidential information in connection with the performances specified in this agreement.

The customer must not use this confidential information to his own advantage or for his own purposes or rather to the advantage or for the purpose of a third party, nor must it be used for commercial purposes and this confidential information must only be used to the extent provided for in this agreement or otherwise to the extent as expressly authorized by the disclosing party in written form. The customer has the right, subject to the obligation to confidentiality, to disclose the terms and conditions of this agreement directly to his legal and financial consultants as would be required for the customer's normal business operation.

Export provisions

The delivered product (including technical data) is subject to the legal export and/or import laws as well as any associated regulations of various countries, especially such laws applicable in Germany and in the United States. The products / hardware / software must not be exported into such countries for which export is prohibited under US American export control laws and its supplementary provisions. You hereby agree to strictly follow the regulations and to yourself be responsible for observing them. You are hereby made aware that you may be required to obtain governmental approval to export, reexport or import the product.

Appendix C: Contacts

Germany
Hilscher Gesellschaft für Systemautomation mbH
Rheinstrasse 15
65795 Hattersheim
Phone: +49 (0) 6190 9907-0
Fax: +49 (0) 6190 9907-50
E-Mail: info@hilscher.com

Support
Phone: +49 (0) 6190 9907-990
E-Mail: de.support@hilscher.com

China
Hilscher Systemautomation (Shanghai) Co. Ltd.
200010 Shanghai
Phone: +86 (0) 21-6355-5161
E-Mail: info@hilscher.cn

Support
Phone: +86 (0) 21-6355-5161
E-Mail: cn.support@hilscher.com

France
Hilscher France S.a.r.l.
69800 Saint Priest
Phone: +33 (0) 4 72 37 98 40
E-Mail: info@hilscher.fr

Support
Phone: +33 (0) 4 72 37 98 40
E-Mail: fr.support@hilscher.com

India
Hilscher India Pvt. Ltd.
Pune, Delhi, Mumbai, Bangalore
Phone: +91 8888 750 777
E-Mail: info@hilscher.in

Support
Phone: +91 8108884011
E-Mail: info@hilscher.in

Austria
Hilscher Austria GmbH
4020 Linz
Phone: +43 732 931 675-0
E-Mail: sales.at@hilscher.com

Support
Phone: +43 732 931 675-0
E-Mail: at.support@hilscher.com

USA
Hilscher North America, Inc.
Lisle, IL 60532
Phone: +1 630-505-5301
E-Mail: info@hilscher.us

Support
Phone: +1 630-505-5301
E-Mail: us.support@hilscher.com

Japan
Hilscher Japan KK
Tokyo, 160-0022
Phone: +81 (0) 3-5362-0521
E-Mail: info@hilscher.jp

Support
Phone: +81 (0) 3-5362-0521
E-Mail: jp.support@hilscher.com

Republic of Korea
Hilscher Korea Inc.
13494, Seongnam, Gyeonggi
Phone: +82 (0) 31-739-8361
E-Mail: info@hilscher.kr

Support
Phone: +82 (0) 31-739-8363
E-Mail: kr.support@hilscher.com

Switzerland
Hilscher Swiss GmbH
4500 Solothurn
Phone: +41 (0) 32 623 6633
E-Mail: info@hilscher.ch

Support
Phone: +41 (0) 32 623 6633
E-Mail: ch.support@hilscher.com

Italy
Hilscher Italia S.r.l.
20090 Vimodrone (MI)
Phone: +39 02 25007068
E-Mail: info@hilscher.it

Support
Phone: +39 02 25007068
E-Mail: it.support@hilscher.com