APPLICATION NOTE: **AN-0385**

AC500 MQTT & MOSQUITTO

FIRST STEPS AND CONFIGURATION

Contents

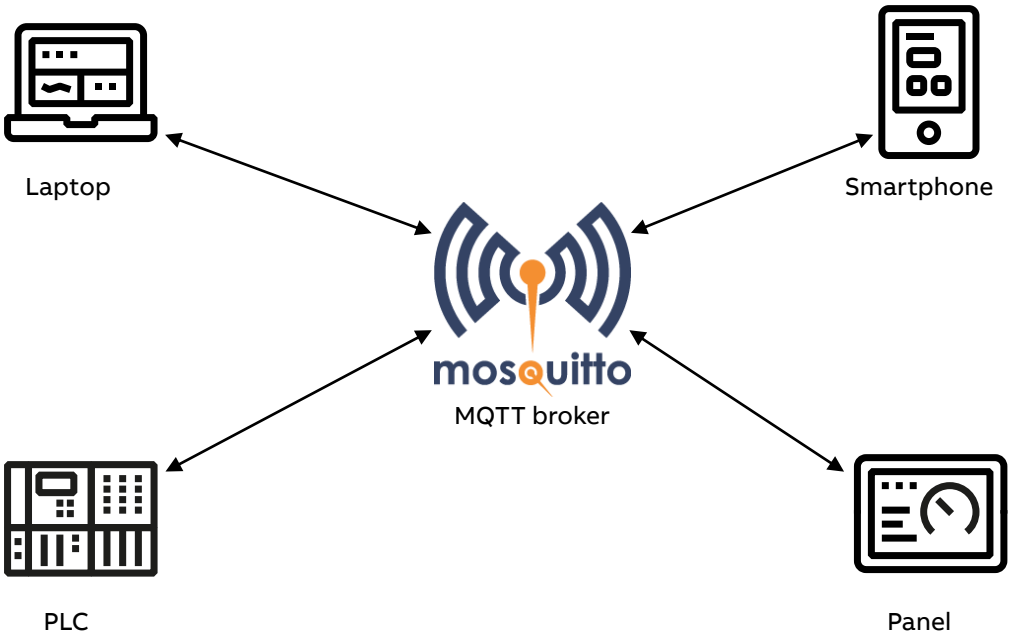
1 Introduction

1.1 Scope of the document

This manual gives a first introduction into Mosquitto as MQTT broker. This document contains information how to work with a public server hosted online and how to set up a local server running local.

Further information about MQTT can be found in the application example: AC500 – MQTT library.

1.2 Overview



2 Mosquitto online

Easiest solution to test some MQTT features is to use a free broker which is running online. test.mosquitto.org is hosted public and offers many possibilities.

A detailed documentation about ports, services and certificates can be found on the website test.mosquitto.org.

CAUTION!

This broker is hosted public. Please don't publish any sensitive information. Anybody could be listening.

3 Local Mosquitto broker

Download and install the required software here: https://mosquitto.org/download

The setup will lead you through the installation. There is no need to change any default setting.

3.1 Mosquitto broker without encryption

1. Navigate to the installation folder: C:\Program Files\mosquitto
2. Open the file mosquitto.conf with any text editor like notepad++
3. In the section **Listeners** add a listener on port **1883**
4. In the section **Security**. Uncomment **allow_anonymous** and set it to **true**
5. Save the file (admin rights required)

```
209 # ================================================================
210 # Listeners
211 # ================================================================
212
213 # Listen on a port/ip address combination. By using this variable
214 # multiple times, mosquitto can listen on more than one port. If
215 # this variable is used and neither bind_address nor port given,
216 # then the default listener will not be started.
217 # The port number to listen on must be given. Optionally, an ip
218 # address or host name may be supplied as a second argument. In
219 # this case, mosquitto will attempt to bind the listener to that
220 # address and so restrict access to the associated network and
221 # interface. By default, mosquitto will listen on all interfaces.
222 # Note that for a websockets listener it is not possible to bind to a host
223 # name.
224 #
225 # On systems that support Unix Domain Sockets, it is also possible
226 # to create a # Unix socket rather than opening a TCP socket. In
227 # this case, the port number should be set to 0 and a unix socket
228 # path must be provided, e.g.
229 # listener 0 /tmp/mosquitto.sock
230 #
231 # listener port number [ip address/host name/unix socket path]
232 listener 1883
233
234 # By default, a listener will attempt to listen on all supported IP protocol
235 # versions. If you do not have an IPv4 or IPv6 interface you may wish to
236 # disable support for either of those protocol versions. In particular, note
237 # that due to the limitations of the websockets library, it will only ever
```

```
508
509
510  # ================================================================
511  # Security
512  # ================================================================
513
514  # If set, only clients that have a matching prefix on their
515  # clientid will be allowed to connect to the broker. By default,
516  # all clients may connect.
517  # For example, setting "secure-" here would mean a client "secure-
518  # client" could connect but another with clientid "mqtt" couldn't.
519  #clientid_prefixes
520
521  # Boolean value that determines whether clients that connect
522  # without providing a username are allowed to connect. If set to
523  # false then a password file should be created (see the
524  # password_file option) to control authenticated client access.
525  #
526  # Defaults to false, unless there are no listeners defined in the configuration
527  # file, in which case it is set to true, but connections are only allowed from
528  # the local machine.
529  allow_anonymous true
530
```

6. To start the broker manually open a command prompt (**CMD**).

No Encryption path:

Navigate to: `cd C:\Program Files\mosquitto`
Call: `mosquitto.exe -c mosquitto.conf -v`

	Note: The parameter -c mosquitto.conf links to the right configuration file The parameter -v is optional and is activating the logging

```
Microsoft Windows [Version 10.0.19044.1586]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Test>cd c:/program files/mosquitto

c:\Program Files\mosquitto>mosquitto.exe -c "mosquitto.conf" -v
1647951796: mosquitto version 2.0.14 starting
1647951796: Config loaded from mosquitto.conf.
1647951796: Opening ipv6 listen socket on port 1883.
1647951796: Opening ipv4 listen socket on port 1883.
1647951796: mosquitto version 2.0.14 running
```

The commands above can also be included inside a batch file which can be used to start the Mosquitto broker without encryption. The content of the batch can be copied from below.

```
run cmd.exe
cd "C:\Program Files\Mosquitto"
mosquitto.exe -c mosquitto.conf -v
pause
```

3.2 Mosquitto broker with encryption

3.2.1 Create self-signed certificates

CAUTION!

Self-signed certificates like created and used in this chapter, can be used for test purposes. It's not recommended to use such certificates in a real plant. There certificates signed from an official CA should be used.

Further details about cyber security can be found in our:

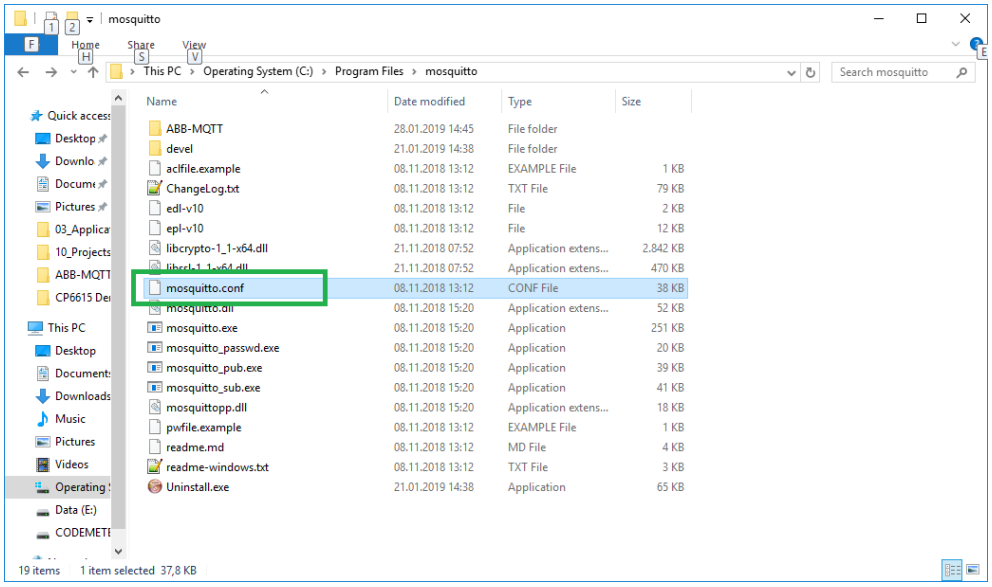
- Whitepaper: Cyber Security in the AC500 PLC
- AC500 Cyber Security FAQs
- AC500 V3 certificates & encryption

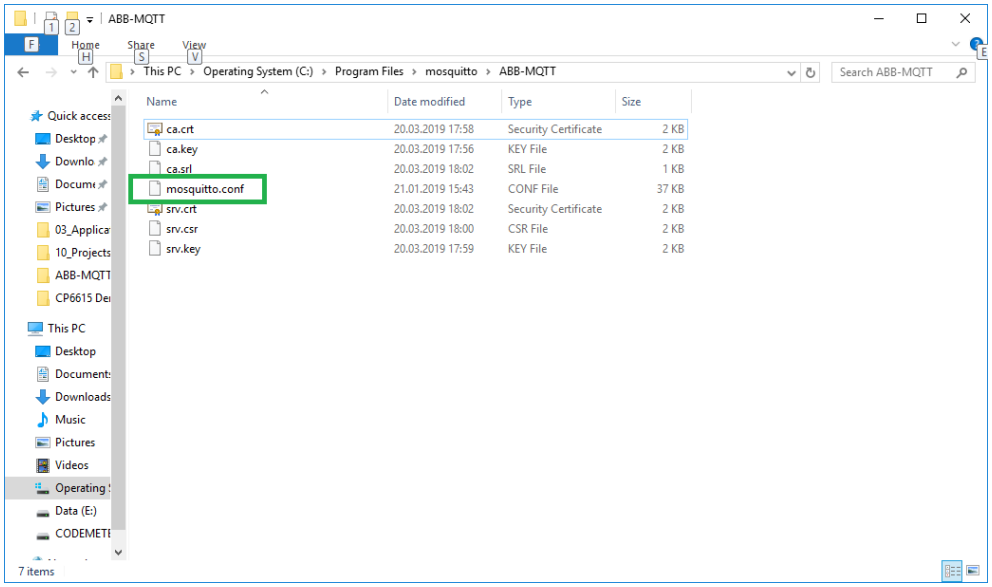
How self-signed certificates can be created using open ssl is explained in the mosquitto documentation.

The created certificates are stored in the folder C:\Program Files\mosquitto\ABB-MQTT

3.2.2 Adapt mosquitto configuration

1. Create a copy of the **mosquitto.conf** and paste it to the **ABB-MQTT** folder:
   This has the advantage that two different configurations for the mosquitto broker are existing. One configuration for a not encrypted and one for an encrypted communication. In case both configurations should be possible in parallel the changes described here needs to be added to the existing mosquitto.conf.





2. Adapt the **mosquitto.conf** file inside the **ABB-MQTT** directory. The following lines must be adapted:

   The Security setting allow anonymous was already changed in the last chapter it

   - needs to be set to **true**. See chapter 3.1

   Listening port

   - needs to be changed from 1883 to **8883**. For details see chapter 3.1

   Path to the PEM encoded server certificate

   - certfile C:\Program Files\mosquitto\ABB-MQTT\srv.crt

   Path to the PEM encoded keyfile.

   - keyfile C:\Program Files\mosquitto\ABB-MQTT\srv.key

   Path to the ca.crt file

   - cafile C:\Program Files\mosquitto\ABB-MQTT\ca.crt

```
310
311  # Both of certfile and keyfile must be defined to enable certificate based
312  # TLS encryption.
313
314  # Path to the PEM encoded server certificate.
315  certfile C:\Program Files\mosquitto\ABB-MQTT\srv.crt
316
317  # Path to the PEM encoded keyfile.
318  keyfile C:\Program Files\mosquitto\ABB-MQTT\srv.key
319
```

```
351  # cafile and capath define methods of accessing the PEM encoded
352  # Certificate Authority certificates that will be considered trusted when
353  # checking incoming client certificates.
354  # cafile defines the path to a file containing the CA certificates.
355  # capath defines a directory that will be searched for files
356  # containing the CA certificates. For capath to work correctly, the
357  # certificate files must have ".crt" as the file ending and you must run
358  # "openssl rehash <path to capath>" each time you add/remove a certificate.
359  cafile C:\Program Files\mosquitto\ABB-MQTT\ca.crt
360  #capath
```

3.2.3 Start Mosquitto broker

Configuration is done. Now we can start the broker. To start the broker manually open a command prompt (**CMD**).

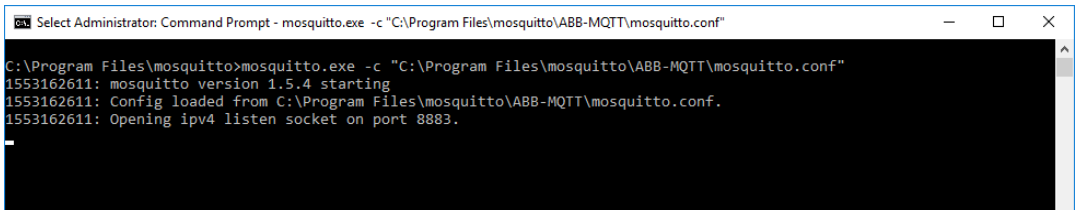
With Encryption path:

Navigate to: `cd C:\Program Files\mosquitto`
Call: `mosquitto.exe -c "C:\Program Files\mosquitto\ABB-MQTT\mosquitto.conf" -v`

Note:

The parameter -c "C:\Program Files\mosquitto\ABB-MQTT\mosquitto.conf" links to the right configuration file

The parameter -v is optional and is activating the logging



The commands above can also be included inside a batch file which can be used to start the Mosquitto broker with encryption. The content of the batch can be copied from below.

```
run cmd.exe
cd "C:\Program Files\Mosquitto"
mosquitto.exe -c "C:\Program Files\Mosquitto\ABB-MQTT\mosquitto.conf" -v
pause
```

ABB AG

Contact:
https://access.motion.abb.com/contact/contact

Homepage:
www.abb.com/plc