

FAQ - Application server TLS connection using username /password

Introduction

On this page we would like to show some connection examples using username/password. Secure TLS communication will be established but only Nx70 device cert will be validated on customer side.

As this connection is not the most secure, we have disabled it by default and it can be enabled by provisioning.

Set-up:

- Nx70 software 2.47 or higher
- DECT handset R700H software release 11
- Secure with username and password using port **8886**

Configuration:

1. The Application server must be enabled [FAQ - Application servers](#)
2. Messaging and Location enabled for the handset [FAQ - Messaging and Location how to enable/disable per handset](#)
3. Contact Gigaset to get the GigasetCA.pem that is needed on the server where mosquitto is executed
for Novalink the GigasetCA.pem is NOT needed: Zur Authentifizierung des Gigaset Multizellen Systems gegenüber novaalert muss der Thumbprint / Hash des Zertifikates in novaalert hinterlegt werden. Der Thumbprint wird beim Start von novaalert in den novaalert Aktivitäten ausgegeben./The thumbprint / hash of the certificate must be stored in novaalert for authentication of the Gigaset multi-cell system against novaalert. The thumbprint is output in the novaalert activities when novaalert is started.
4. Add device to the known hosts [FAQ - Add device to the known hosts](#)
5. Enable this TLS connection via provisioning

```
<?xml version="1.0" encoding="UTF-8"?>
<settings version="1.0" productID="e2">

  <oper name="set_uci">
    <param name="mosquitto.listener.enabled" value="1" />
  </oper>

</settings>
```

MQTT example using Windows PC

Windows: mosquitto version 2.0.14

Nx70: Software 2.47.0

```
.\mosquitto_pub --cafile GigasetCA.pem -p 8886 -h 589ec62904f3 -u as1 -P 123456789012345678901234567890ab -t 'as1/msg/xxl/msgsrv/req
/setMsg' -m '{\"msgId\": \"1\", \"payload\": {\"amsgId\": \"23643\", \"sipId\": \"1021\", \"msg\": {\"server_msg_status\": \"new\", \"prio\": \"1\", \"title\": {\"text\": \"
Message prio1\", \"color\": \"04\"},
\"status_icon\": \"0D\", \"status_text\": \"accept\",
\"ttl\": \"600\",
\"alert_info\": \"msg_melody_low\",
\"override_silencing\": \"no\",
\"vibration\": \"no\",
\"ringtone_volume\": \"50\",
\"presentation_time\": \"30\",
\"deletable\": \"yes\",
\"local_ignore\": \"yes\",
\"presentation_time\": \"30\",
\"body_starter\": \"Body starter\",
\"msg_icon\": {\"value\": \"28\",
\"body\": {\"msg_icon\": {\"value\": \"4E\", \"color\": \"04\"}},
{\"paragraph\": {\"text\": \"Prio 1 message: some longer test to check how long the message can be\", \"blink\": \"no\", \"underline\": \"yes\", \"bold\": \"
yes\", \"align\": \"left\", \"color\": \"00\"}},
{\"paragraph\": {\"text\": \"This text is only shown in detailed view\", \"blink\": \"no\", \"underline\": \"no\", \"bold\": \"no\", \"align\": \"left\"}},
\"reply_options\": {\"option_id\": \"1\", \"reply\": {\"text\": \"Msg1SK1\"}}, {\"option_id\": \"2\", \"reply\": {\"text\": \"Msg1SK2\"}}, {\"option_id\": \"3\", \"
make_call\": {\"text\": \"Call\", \"to\": \"1021\"}}}}}' -i as1
```

where:

- cafile GigasetCA.pem root CA received from Gigaset
- -p 8886 dedicated port for this communication option
- -h 589ec62904f3 host name corresponding to certificate Common Name.
- -u as1 application server previously added via webUI or provisioning
- -P 123456789012345678901234567890cc password previously added via webUI or provisioning