

FAQ Nx70 - Client certificates

Introduction

The N870 has default from the factory Client certificates installed on the device.

The Factory installed Client certificates can be found here:

```
/config/ssl/gigaset_factory_cert.pem  
/config/ssl/gigaset_factory_key.pem
```

Valid for:

N670

N870

Web-interface

The Client certificates can be uploaded from the web-interface, go to: **SETTINGS - Telephony - VoIP**.

The screenshot shows the Gigaset N870 IP PRO web interface. The left sidebar contains a menu with 'Telephony' expanded to show 'VoIP'. The main content area is titled 'SIP' and contains several configuration fields: SIP port (5060), Secure SIP port (5061), SIP timer T1 (500 ms), SIP session timer (1800 s), Failed registration retry timer (300 s), and Subscription timer (1800 s). There is an unchecked checkbox for 'PRACK'. The 'SIP security certificate' field shows 'File not uploaded' and a 'Delete' button. Below this are two sections: 'Certificate' with a 'Browse...' button, and 'Private key' with a 'Browse...' button.

Auto-provisioning

```
<?xml version="1.0" encoding="UTF-8"?>  
<provisioning version="1.1" productID="e2">  
  <firmware>  
  </firmware>  
  <nvm>  
  </nvm>  
  <custom>  
    <step type="certificate" url="<URL to certificate>" key="<URL to Private key>" flags="CLIENT_CERT" />  
  </custom>  
</provisioning>
```

How to generate Client certificates

You can generate your own Client certificates on the N870 CLI if you have no access to a Linux machine.

To create self-signed client certificate you have to follow the instructions below. If you have own CA you can skip the first step.

1. Generate CA certificate and key:

```
openssl genrsa -des3 -out ca.key 4096
openssl req -new -x509 -days 365 -key ca.key -out ca.crt
```

and follow the on-screen instructions.

2. Generate Client Key, Certificate Signing Request, and Signed Client Certificate:

```
openssl genrsa -des3 -out N870.key 4096
openssl req -new -key N870.key -out N870.csr
openssl x509 -req -days 365 -in N870.csr -CA ca.crt -CAkey ca.key -set_serial 01 -out N870.crt
openssl rsa -in N870.key -out N870_key.pem
```

As Common Name you can put the MAC address of the device (with capital letters).

You can download the **N870.crt** and **N870.pem** file using WinSCP.

In the WebUI you have to upload **N870.crt** and **N870.pem** files.