Certificates

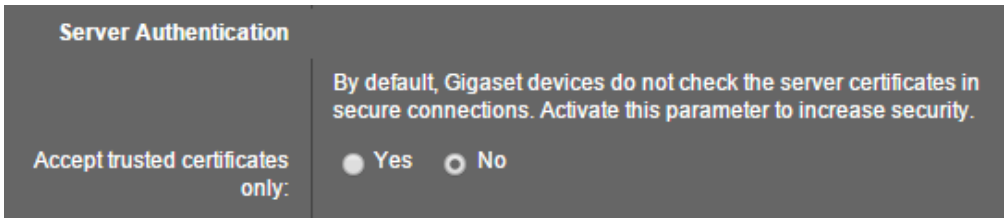
Introduction

By default the Gigaset devices will accept all certificates if they are provided by the HTTP(S) server.

N510 IP PRO

Web-interface

Open the web-interface and go to: **Settings - Network - Security**



> **Important N510**
>
> After the device downloads the certificate, you need to wait 2 minutes before the xml config file is downloaded. This is only for the first time the device comes online.

If needed, the certificate can also be downloaded by the device (Only N510), see the info below.

Download TLS-Certificates via link in Profile

Only Gigaset N510 IP PRO.

A new tag in plain xml profiles is supported. This tag enables e.g. a provider to force a download of a Certificate without user interaction.
The certificate tag will be supported only in plain xml profiles. The name of the XML tag is "CERTIFICATE". The given URL which refers to the certificate file must be complete (Host + Filename) like the example below:

<CERTIFICATE class="string" value="http://profile.gigaset.net/device/certificate.bin"/>

Only one certificate tag is allowed per profile. Redirection to another location is supported!

The certificate can be downloaded only via a http server.

Here is an example how to do this with an Gigaset N510 IP PRO

1. First we have placed the certificate on our web-server.

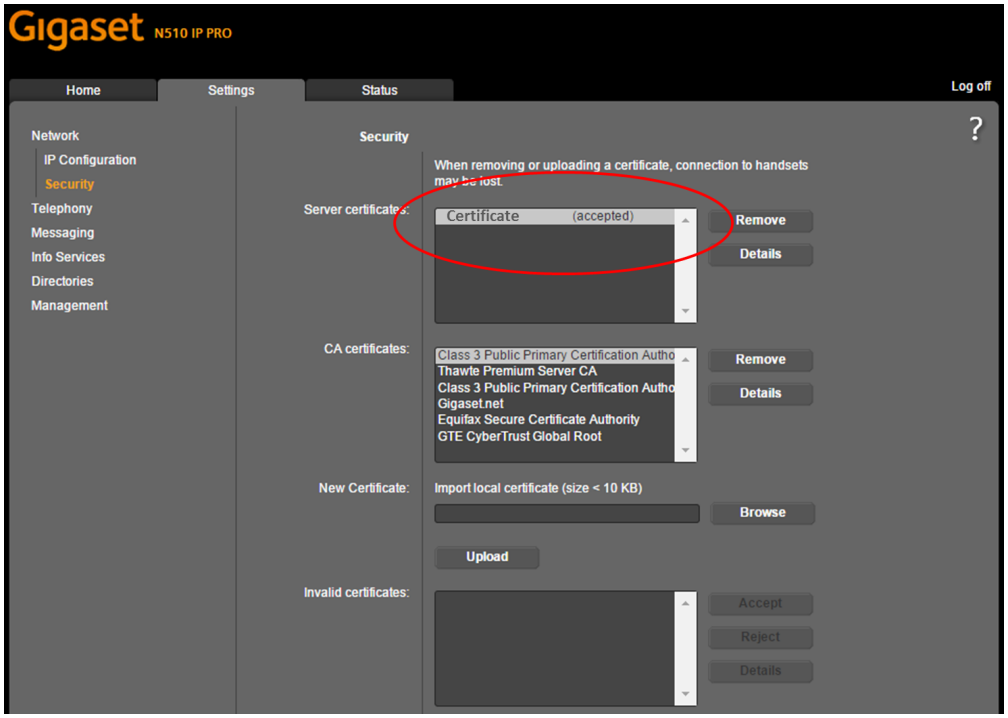
2. Second we created an XML configuration file where we added the parameter to download the certificate

XML file

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<ProviderFrame xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:noNamespaceSchemaLocation="profile.xsd">
<Provider>
<!-- Please enter the correct MAC Address example: 3E2F800E1234
Please enter a Profile name
If not correct, no setting will be done
-->
<MAC_ADDRESS value="7C2F805A0895"/>
<PROFILE_NAME class="string" value="N510"/>

<!-- VoIP account 1, example config -->
<SYMB_ITEM ID="BS_IP_Data1.aucS_SIP_ACCOUNT_NAME_1" class="symb_item" value="'Gigaset'"/>
<SYMB_ITEM ID="BS_IP_Data1.aucS_SIP_DISPLAYNAME" class="symb_item" value="'Test24'"/>
<SYMB_ITEM ID="BS_IP_Data3.aucS_SIP_LOGIN_ID" class="symb_item" value="'249'"/>
<SYMB_ITEM ID="BS_IP_Data1.aucS_SIP_PASSWORD" class="symb_item" value="'Test'"/>
<SYMB_ITEM ID="BS_IP_Data1.aucS_SIP_USER_ID" class="symb_item" value="'249'"/>
<SYMB_ITEM ID="BS_IP_Data1.aucS_SIP_DOMAIN" class="symb_item" value="'192.168.178.120'"/>
<SYMB_ITEM ID="BS_IP_Data1.aucS_SIP_SERVER" class="symb_item" value="'192.168.178.120'"/>
<SYMB_ITEM ID="BS_IP_Data1.aucS_SIP_REGISTRAR" class="symb_item" value="'192.168.178.120'"/>
<SYMB_ITEM ID="BS_IP_Data1.aucS_STUN_SERVER" class="symb_item" value="''"/>
<SYMB_ITEM ID="BS_IP_Data1.aucS_OUTBOUND_PROXY" class="symb_item" value="''"/>
<SYMB_ITEM ID="BS_IP_Data1.aucS_SIP_PROVIDER_NAME" class="symb_item" value="'GigasetPRO'"/>
<SYMB_ITEM ID="BS_IP_Data1.uiI_SIP_SERVER_PORT" class="symb_item" value="0x13c4"/>
<SYMB_ITEM ID="BS_IP_Data1.uiI_SIP_REGISTRAR_PORT" class="symb_item" value="0x13c4"/>
<SYMB_ITEM ID="BS_IP_Data1.ucB_SIP_USE_STUN" class="symb_item" value="0x0"/>
<SYMB_ITEM ID="BS_IP_Data1.uiI_STUN_SERVER_PORT" class="symb_item" value="0xd96"/>
<SYMB_ITEM ID="BS_IP_Data1.ucI_OUTBOUND_PROXY_MODE" class="symb_item" value="0x1"/>
<SYMB_ITEM ID="BS_IP_Data1.uiI_OUTBOUND_PROXY_PORT" class="symb_item" value="0x13c4"/>
<SYMB_ITEM ID="BS_IP_Data1.uiI_RE_REGISTRATION_TIMER" class="symb_item" value="0xb4"/>
<SYMB_ITEM ID="BS_IP_Data1.uiI_RE_STUN_TIMER" class="symb_item" value="0xf0"/>

<!-- WEB UI: Settings - Telephony - Connections - Active
Enable the SIP account -->
<SYMB_ITEM ID="BS_IP_Data1.ucB_SIP_ACCOUNT_IS_ACTIVE_1" class="symb_item" value="0x1"/>

<!-- Download certificate -->
<CERTIFICATE class="string" value="http://<Server URL>/gigaset.cer"/>

</Provider>
</ProviderFrame>
```

3. When the device reboots and downloads this xml file, the device directly downloads the certificate.

4. In the web-interface you can see that the certificate is in the device.


Gigaset N510 IP PRO
Home
Settings
Status
Log off
Network
IP Configuration
Security
Telephony
Messaging
Info Services
Directories
Management
Security
When removing or uploading a certificate, connection to handsets may be lost.
Server certificates:
Certificate (accepted)
Remove
Details
CA certificates:
Class 3 Public Primary Certification Autho
Thawte Premium Server CA
Class 3 Public Primary Certification Autho
Gigaset.net
Equifax Secure Certificate Authority
GTE CyberTrust Global Root
Remove
Details
New Certificate:
Import local certificate (size < 10 KB)
Browse
Upload
Invalid certificates:
Accept
Reject
Details