FAQ - System Security

Valid for:	N610	N670	N870	N870E	Embedded Integrator	Virtual Integrator

Security

The page allows you to organize the certificates used for secure internet communication and to define the credentials for HTTP authentication.

Certificates

The phone system supports the establishment of secure data connections on the Internet with the TLS security protocol (Transport Layer Security). With TLS, the client (the phone) uses certificates to identify the server. These certificates must be stored on the base stations.

Accept all certificates

Mark the Yes radio button, if you want to accept all certificates.

Server certificates / CA certificates

The lists contain the server certificates or CA certificates that have been certified by a certification authority (CA). The certificates in both lists have already been implemented by default or have been downloaded via the Web configurator and are classed as valid, i.e., have been accepted.

If one of the certificates becomes invalid, e.g., because it has expired, it is transferred to the Invalid certificates list.

Invalid certificates

The list contains the certificates that have been received from servers but have not passed the certificate check, and certificates from the Server certificates / CA certificates lists that have become invalid.

Accepting / rejecting invalid certificates

Accepting a certificate:

- Select the certificate and click on the **Accept** button . . . depending on its type, the certificate is transferred to one of the Server certificates / CA certificates lists (even if it has already expired). If a server responds again with this certificate, this connection is accepted immediately.

Reject a certificate:

Select the certificate and click on the **Reject** button . . . the certificate is transferred to the Server certificates list with the label Rejected. If a server responds again with this certificate, this connection is rejected immediately.

Checking information about a certificate

Select the certificate and click on the **Details** button. . . . a new web page appears, displaying the properties of the certificate.

Deleting a certificate from one of the lists

Select the certificate and click on the **Remove** button. The certificate is deleted from the list immediately.

Import local certificate

You can make available further certificates to your phone system. The certificates must have been downloaded to your computer before.

Click **Browse...** and select the local certificate file from your computer's file system click on **Upload . . .** the selected certificate file is loaded and, depending on its type, added to one of the certificate lists.

HTTP authentication

Define the credentials (user name and password) for HTTP authentication. The credentials are used for HTTP digest authentication of the provisioning client with the provisioning server.

HTTP digest username

Enter the user name for HTTP authentication. Value: max. 74 characters

HTTP digest password

Enter the password for HTTP authentication. Value: max. 74 characters

HTTP Authentication

HTTP digest username ❓	7C2F80C6E5C2
HTTP digest password ❓	••••••••

Auto-provisioning

Parameter	Description
SystemSettings.global.Security_Certificates_AcceptAllCertificates	Yes, If you want to accept all certificates. 0 = No 1 = Yes
Security.global.HTTPAuthUsername	Enter the user name for HTTP authentication.
Security.global.HTTPAuthPassword	Enter the password for HTTP authentication