Interoperability report

Ascom i62, sw 5.5.5

Lancom Systems L(N)-8xx, sw 10.12Rel

Lancom Systems LN-17xx, sw 10.12Rel

Lancom Systems WLC-4006+, 4025+, 4100, 10.12Rel

Introduction

This document describes necessary steps and guidelines to optimally configure the Lancom Systems solutions WLAN platform with Ascom i62 VoWiFi handset. The guide should be used in conjunction with both Lancom Systems and Ascoms configuration guide(s).

About Ascom

Ascom is a global solutions provider focused on healthcare ICT and mobile workflow solutions. The vision of Ascom is to close digital information gaps allowing for the best possible decisions – anytime and anywhere. Ascom's mission is to provide mission-critical, real-time solutions for highly mobile, ad hoc, and time-sensitive environments. Ascom uses its unique product and solutions portfolio and software architecture capabilities to devise integration and mobilization solutions that provide truly smooth, complete and efficient workflows for healthcare as well as for industry, security and retail sectors.

Ascom is headquartered in Baar (Switzerland), has subsidiaries in 15 countries and employs around 1,300 people worldwide. Ascom registered shares (ASCN) are listed on the SIX Swiss Exchange in Zurich.

About Lancom Systems

LANCOM Systems is the first choice for secure, reliable and future-proof network solutions "Made in Germany". We are the only German manufacturer of networking solutions for the public and commercial sectors. This is a market that is strongly influenced by American and Asian companies. With our two business units—Network Connectivity (VPN networking, switching) and Wireless LAN—we offer professional users secure, flexible infrastructure solutions for local-area and multi-site networks. The LANCOM core portfolio is developed, manufactured and quality assured by us in Germany in keeping with highest standards of security, privacy and quality. We also offer VPN solutions as certified by the BSI (German Federal Office for Information Security), which are especially designed to protect confidential networks and critical infrastructures against cyber attack. Another special feature is our policy of free updates that keeps our customers' networks up to date over many years.

Site information

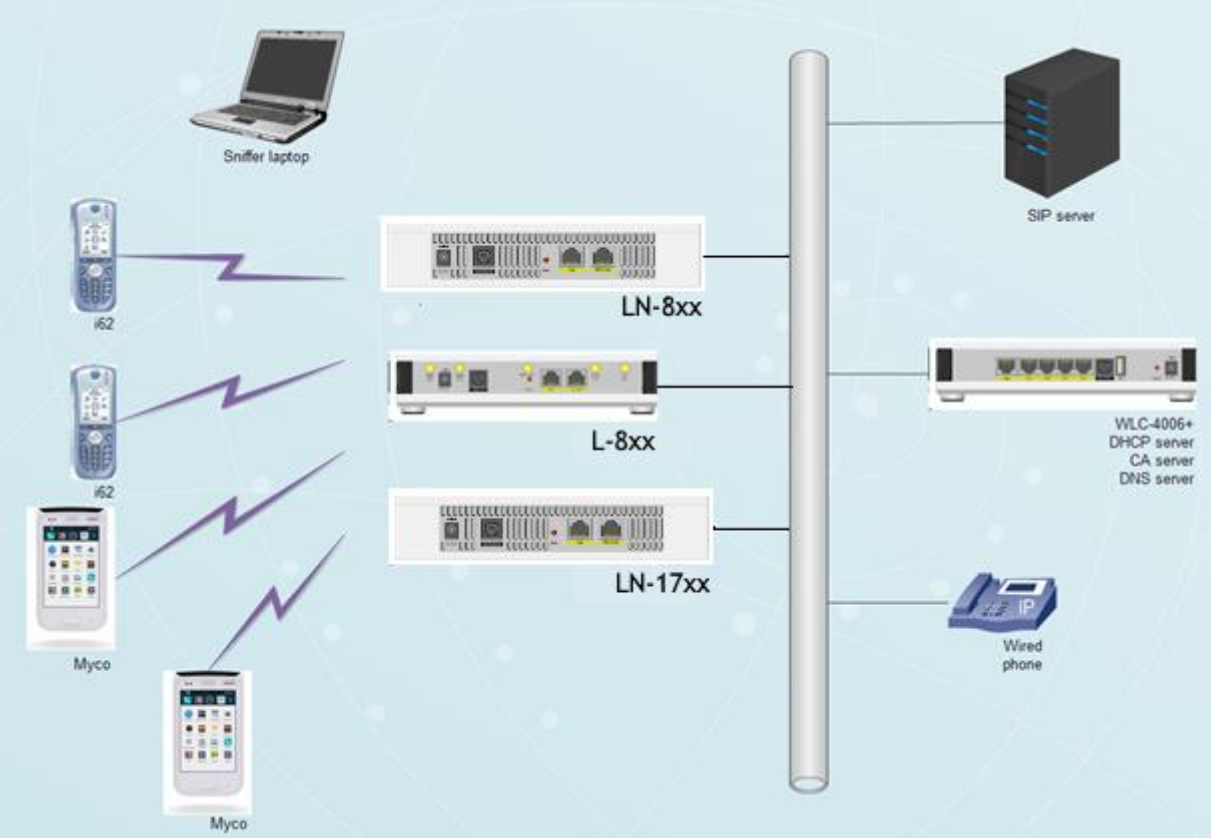
Test site

Lumiad
Veldzigt 24
3454PW De Meern
The Netherlands

Participants

N. Crijns, Lumiad

TEST TOPOLOGY



Summary

Please refer to Appendix B for detailed results for respective access point.

ASSOCIATION / AUTHENTICATION	**Test Description**	**Result**
#101	Association with open authentication, no encryption	PASS
#104	Association with WPA-PSK authentication, TKIP encryption	PASS
#105	Association with WPA-PSK authentication, AES-CCMP encryption	PASS
#106	Association with WPA2-PSK authentication, TKIP encryption	PASS
#107	Association with WPA2-PSK authentication, AES-CCMP encryption	PASS
#110	Association with PEAP-MSCHAPv2 auth, AES-CCMP encryption	PASS
#111	Association with EAP-FAST authentication	PASS
#115	Association with multiple ESSIDs on AP	PASS
#118	Association with Group key rotation (regression)	PASS
POWER-SAVE AND QOS		
#150	802.11 Power-save mode	PASS
#151	Beacon period and DTIM interval	PASS
#152	802.11e U-APSD	PASS
#202	WMM prioritization	PASS
ROAMING AND HANDOVER TIMES		
#401	Handover with open authentication and no encryption	PASS
#403	Handover with WPA-PSK authentication and TKIP encryption	PASS
#404	Handover with WPA2-PSK auth and AES-CCMP encryption	PASS
#408	Handover with PEAP-MSCHAPv2 authentication and AES-CCMP encryption	PASS
#409	Handover with EAP-FAST authentication with CCKM	PASS
#410	Handover using PMKSA caching	PASS
#411	Handover using PMKSA and opportunistic/proactive key caching	PASS
#412	Preauthentication	PASS

BATTERY LIFETIME		
#501	Battery lifetime in idle	76 hours to 92 hours
#502	Battery lifetime in call with no power save	1.5 to 2.5 hours
#504	Battery lifetime in call with power save mode U-APSD	13 hours to 17 hours
STABILITY		
#601	Duration of call – Active mode	PASS
#602	Duration of call – U-APSD mode	PASS
802.11n		
#801	Frame aggregation A-MSDU	PASS
#802	Frame aggregation A-MPDU	PASS
#804	40Mhz channels	PASS
#805	802.11n rates	PASS

General conclusion

The result of the verified test areas, such as authentication, association, handover and call stability test, produced very good results. The roaming times, both PSK and 802.1x MS-CHAPv2 were excellent by ranging in the interval 25ms to 50ms.

A number of settings are required to set in the Lancom Controller/Access point in order to get the best performance out of the handset.

QoS is strongly recommended for the most optimal speech when in call.

U-APSD/WMM is required for the most optimal battery usage. Without this setting the battery will drain rapidly!

The recommended setting for DTIM is 5. The tested battery lifetime on standby is around 80 hours with the active call time around 14 hours. Keeping the DTIM to 1 (system default) will half the active standby and active call time.

Note that the age of the battery in the handset has a great impact on battery life expectancy. An older battery will have less battery lifetime then a new one.

It is recommended to follow the best practice of Ascom in regards to channel planning and channel bonding, as shown below:

"General guidelines when deploying Ascom i62 handsets in 802.11a/n/ac environments:

1. ***Enabling more than 8 channels will degrade roaming performance. Ascom recommends against going above this limit.***

2. ***Using 40 MHz channels (or "channel-bonding") will reduce the number of non-DFS* channels to two in ETSI regions (Europe). In FCC regions (North America), 40 MHz is a more viable option because of the availability of additional non-DFS channels. The handset can co-exist with 40 MHz stations in the same ESS.***

3. ***Ascom do support and can coexist in 80MHz channel bonding environments. The recommendations is however to avoid 80MHz channel bonding as it severely reduces the number of available non overlapping channels.***

4. ***Make sure that all non-DFS channel are taken before resorting to DFS channels. The handset can cope in mixed non-DFS and DFS environments; however, due to "unpredictability" introduced by radar detection protocols, voice quality may become distorted and roaming delayed. Hence Ascom recommends if possible avoiding the use of DFS channels in VoWIFI deployments.***

***) Dynamic Frequency Selection (radar detection)"**

It is highly recommended to deploy the VoWLAN network to the 5 GHz frequency whenever possible. If 2.4 GHz does have to be used then it is recommended that 802.11b is turned off.

The performance testscases #301-310 have not been done, as the required amount of devices for the test (12+ handsets) were not available during the testing period.

Known Issues

When not enabling the U-APSD/WMM the handset's battery lifetime will last 1.5 to 2 hours (talk time). It is there for required that this is activated at any given time.

The phone doesn't support 80 MHz channels. When configured with 80 MHz it is possible that the phone doesn't receive the returning packets. This will result in poor voice quality or one way speech scenarios. While the phone does function fine with on a 802.11a/n/ac setting it is required to turn off 80 MHz and only use 20 MHz or 40 MHz.

Test Configuration

Ascom WLAN Infrastructure Verification

Software versions:

- Lancom Systems L(N)-8xx, firmware 10.12Rel
- Lancom Systems LN-17xx, firmware 10.12Rel
- Lancom Systems WLC4006+, firmware 10.12Rel
- Ascom i62, version 5.5.5
- SNOM 300, version 8.7.34

Signalling Protocol

- Yaestar MyPBX

Configuration of WLAN System:

- Beacon Interval: 100ms
- DTIM Period: 5
- 802.11g/n
- 802.11a/n/ac
- WMM/ U-APSD Enabled (See appendix A for QoS profiles)
- 802.11d Regulatory Domain: World mode

Ascom i62 Configuration:

- World Mode Regulatory Domain set to World mode
  (Devices deployed in the USA must be set Regulatory domain to "US")
- IP DSCP for Voice: 0x30 (48) – Class selector 6
- IP DSCP for Signaling: 0x1A (26) – Assured Forwarding 31

Ensure that Ascom i62 unsupported features: 802.11r (fast roaming) & 802.11w (protected management frames) are disabled.

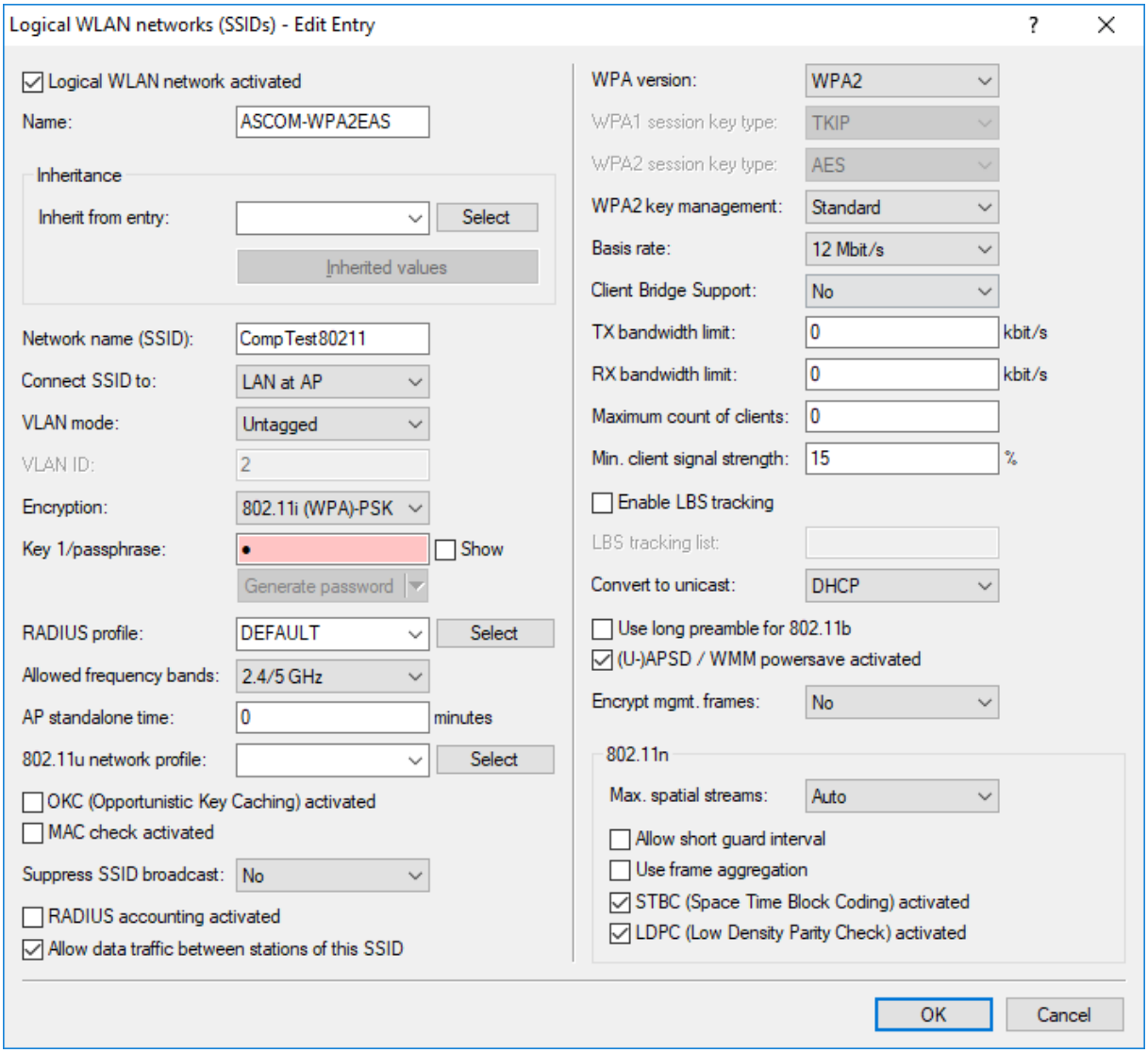
Keep in mind that security options and power save modes were adjusted according to requirements in individual test cases. Please refer to appendix A for information regarding device configuration.

Appendix A: Test configurations

Lancom Systems WLC4006+ and L(N)-8xx and LN-17xx access points.

In the following chapter you will find screenshots and explanations of basic settings in order to get the Lancom Systems solution operational with Ascom i62. Please note that security settings were modified according to requirements in individual test cases.

Logical networks (ESS)



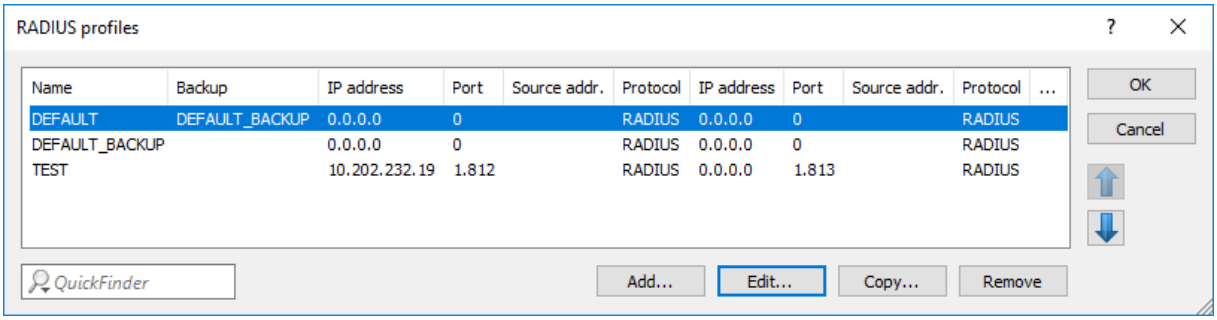
Logical WLAN Profiles can be set under WLAN Controller -> Profiles -> Logical WLAN networks (SSIDs)

- Enter a name the profile
- Enter a network name. This is the broadcasted SSID.
- Select the desired encryption.
- Enter a key in the passphrase.
- Set the Allowed frequency bands to the band that will be used for deployment
- Set AP standalone time to 9999. This setting will allow the access points to broadcast the SSID standalone if the controller show fail

- Enable U-APSD
- Disable OKC when using WPA2-PSK
- Disable Use long preamble for 802.11b
- In high density networks it is recommended to disable Allow short guard interval
- NB. When using WPA2-Enterprise enable OKC

If 802.1x is used, select 802.1i(WPA)-802.1x under the encryption option in the Logical SSID. When selecting this encryption having a RADIUS server is required. Lancom Systems supports both the internal RADIUS in the WLC, access point, routers of Lancom Systems or a third party external one, such as Microsoft NPS or FreeRADIUS.

Configure the wanted external RADIUS under WLAN Controller -> Profiles -> RADIUS Profiles.



- Create a new entry or edit the existing one.
- Input the RADIUS that is to be used. For the internal RADIUS this should 127.0.0.1
- Set the port to be used to 1812 (RADIUS standard)
- Input the shared secret

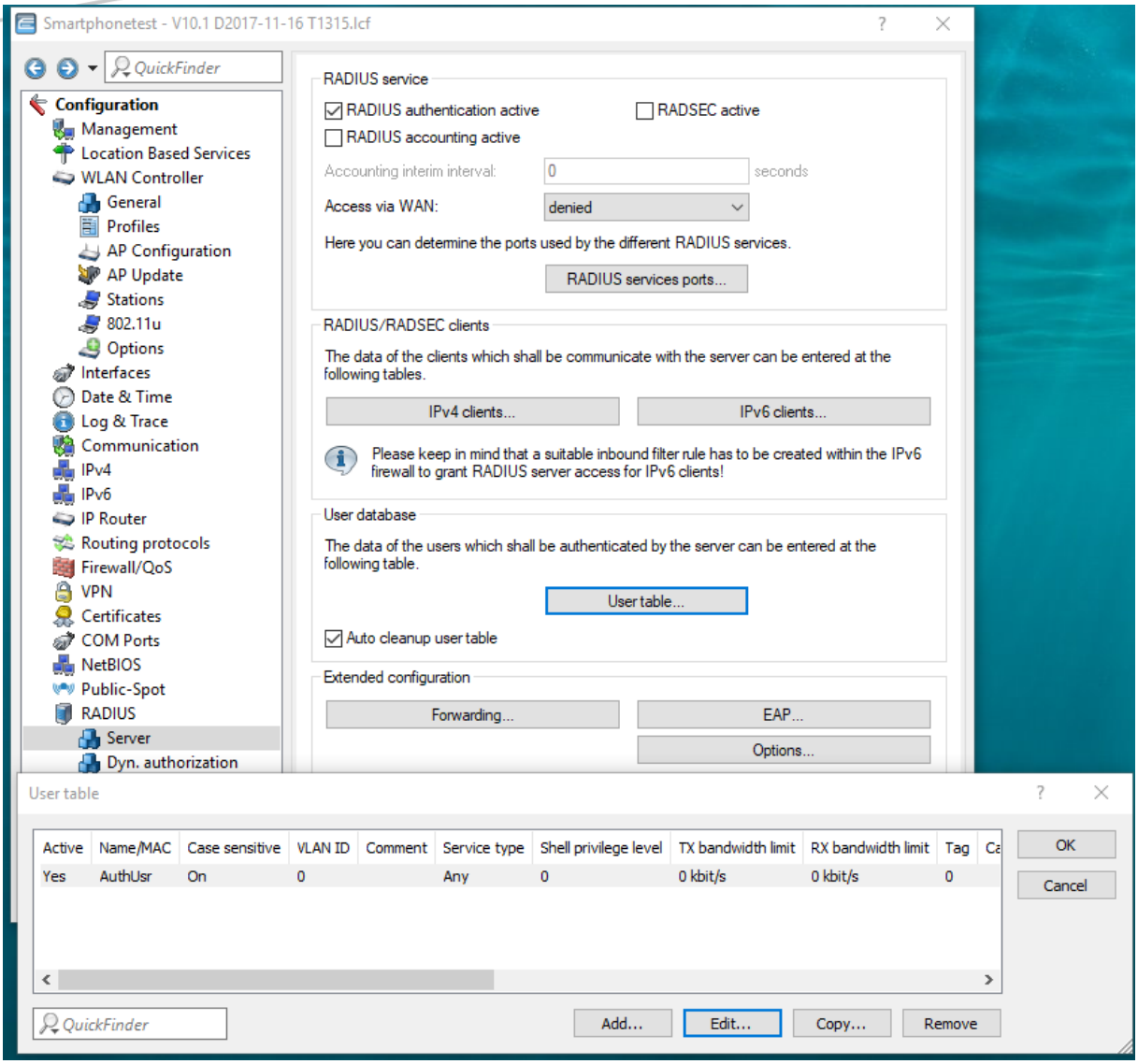
If an accounting server is used, fill out the second block as well.

- Input the RADIUS accounting server that is to be used. For the internal RADIUS this should 127.0.0.1
- Set the port to be used to 1813 (RADIUS standard)
- Input the shared secret

NB. When using a RADIUS server in the Logical SSID profile, this will cause all access points to individually send RADIUS requests to the configured RADIUS server.

NB. It is possible to use the WLC as RADIUS proxy to an external RADIUS server, however this is not the recommended solution.

If the internal RADIUS server of the WLC is to be used, please configure this under RADIUS Server -> General.



- Select RADIUS authentication active
- Add users to the User table as desired

To deploy 802.1x with EAP-TLS with certificates on the controller side please refer to the video explanation to be found at:

https://www.youtube.com/watch?v=q9a1kChF_4w

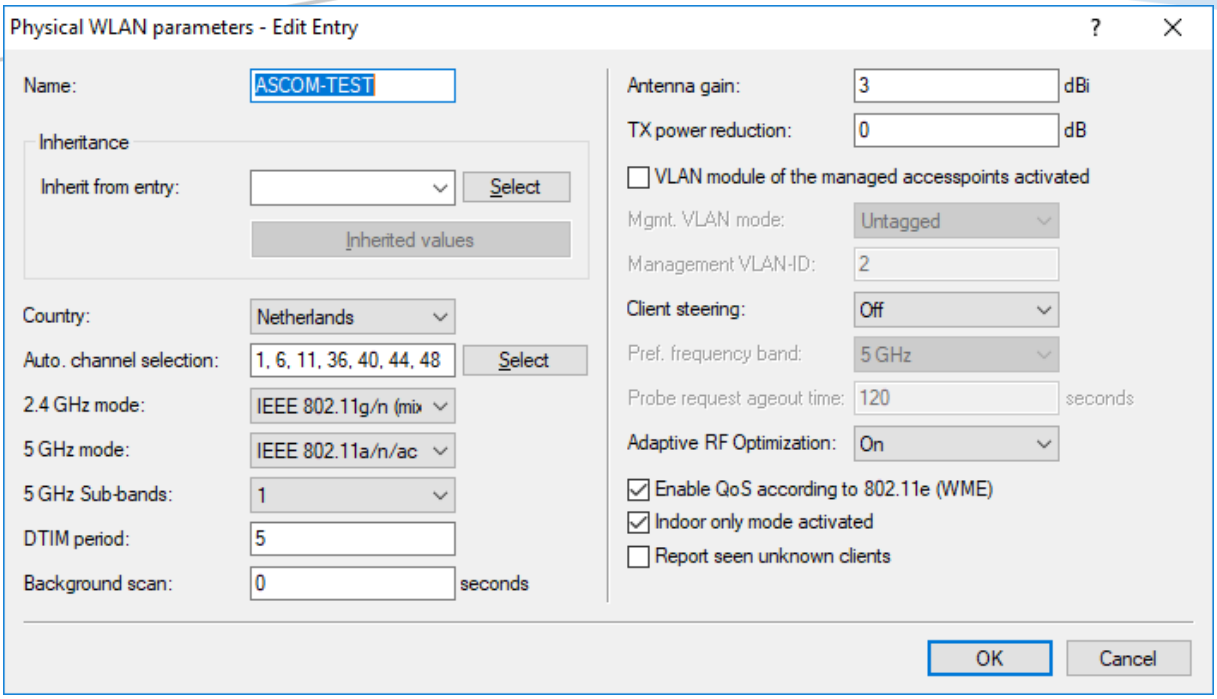
Or the support knowledgebase article:

https://www2.lancom.de/kb.nsf/1276/27223FFC04685925C125805000489A79?OpenDocument

To create the accompanying certificates, please refer to:

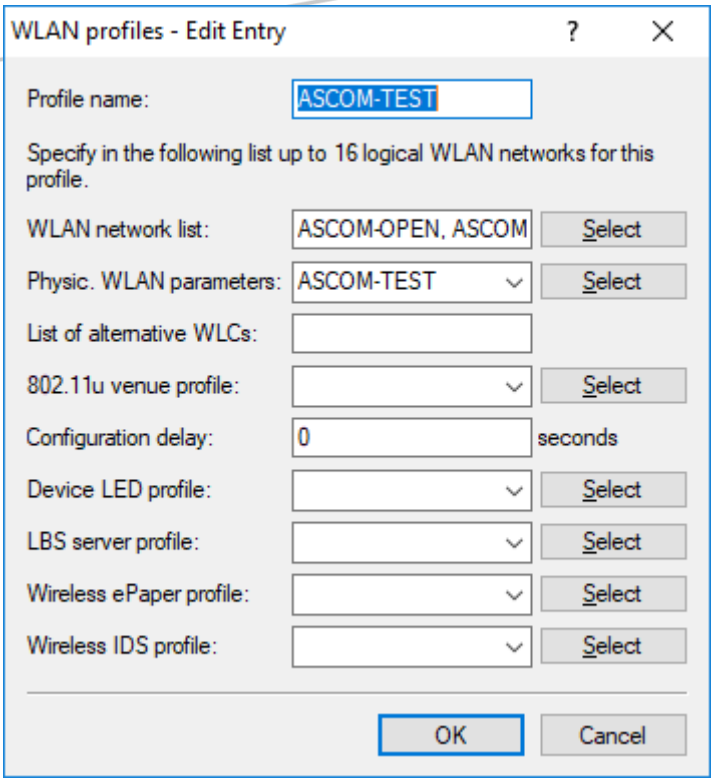
https://www2.lancom.de/kb.nsf/474f6c68bad2df5ac1257f3800526796/d5af67ed27c636dbc1257e9d004836f9?OpenDocument

Physical settings (PHY radio configuration):



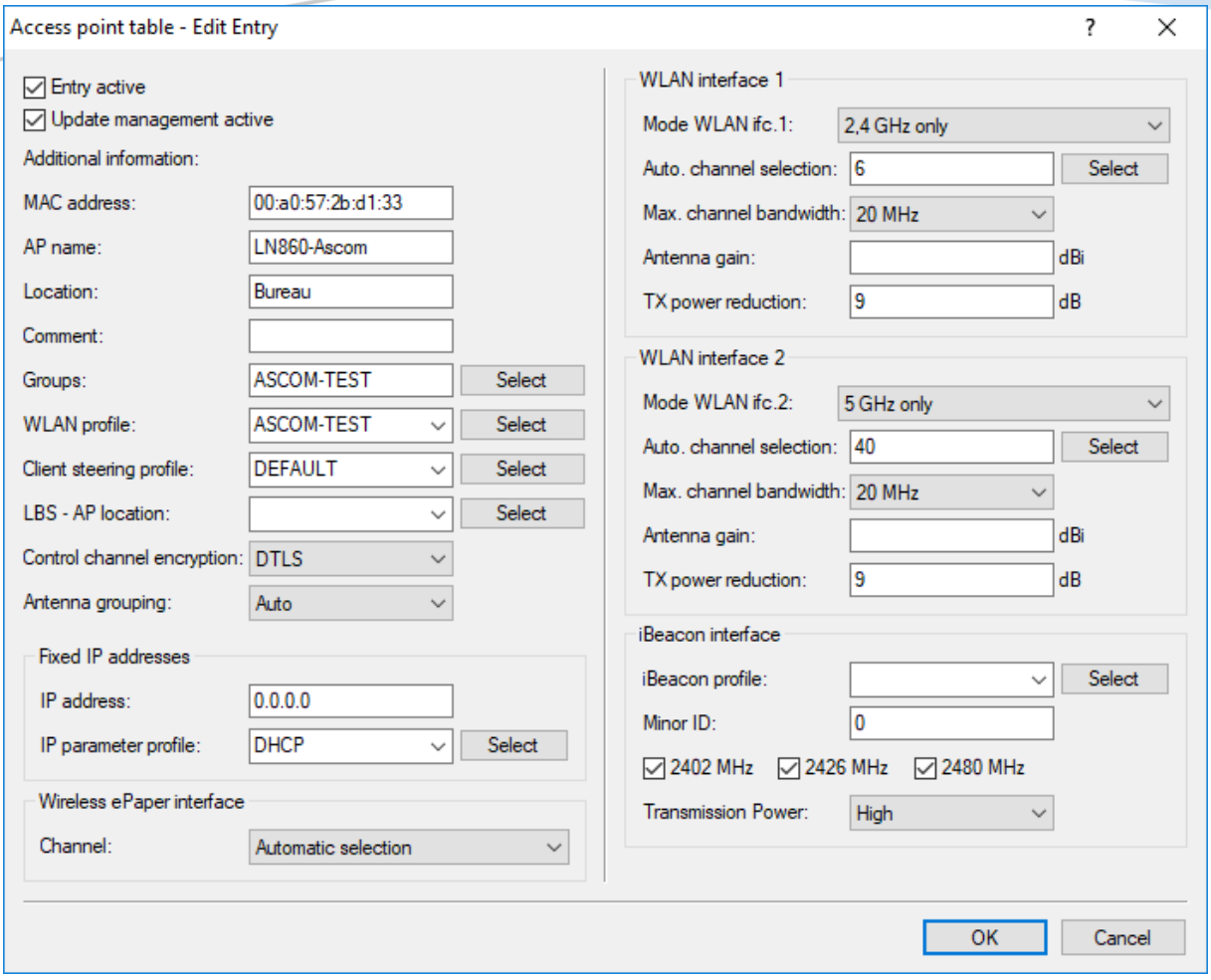
- Enter a profile name
- Select channels for 2.4 and 5 at Auto. Channel selection if you which to have the system do an auto channel distribution
- For 2.4 GHz the recommended channels are 1, 6 and 11
- For 5 GHz the recommended channels are 36, 40, 44 and 48
- Set DTIM to 5 (highly recommended)
- Enable QoS
- Activate Indoor only mode. Activating this setting will enable the system to set UNII-1 channels and prevent the system to use any DFS channels
- Client Steering is recommended to use, but not required
- Adaptive RF Optimization is recommended to use, but not required
- NB. When using VLANs enable the VLAN module of the managed access points

WLAN profile:



- Enter a profile name
- Select the Logical WLAN networks that should be transmitted
- Select the desired PHY Profile

Access point configuration

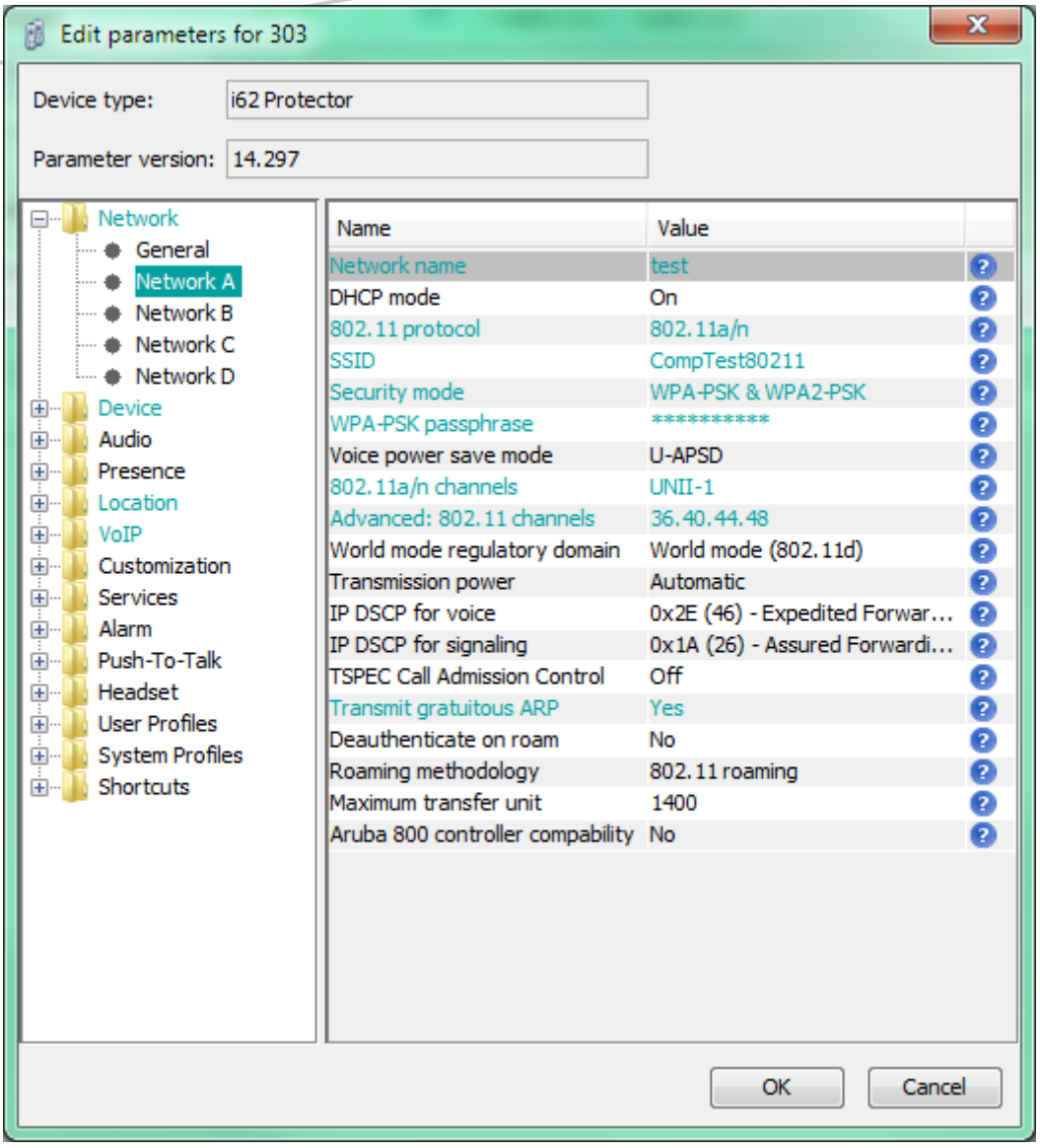


- Select the correct WLAN profile for the access point
- If client steering is used, select the profile here
- The Auto. Channel selection in this screen will overwrite the PHY parameter setting!
- Set Max. Channel bandwidth to 20 MHz. 40 and 80 are supported, but not recommended for VoWLAN deployments.

Please see attached file Smartphonetest - V10.1 D2017-11-16 T1315 for the configuration

Smartphonetest - V10.1 D2017-11-16 T

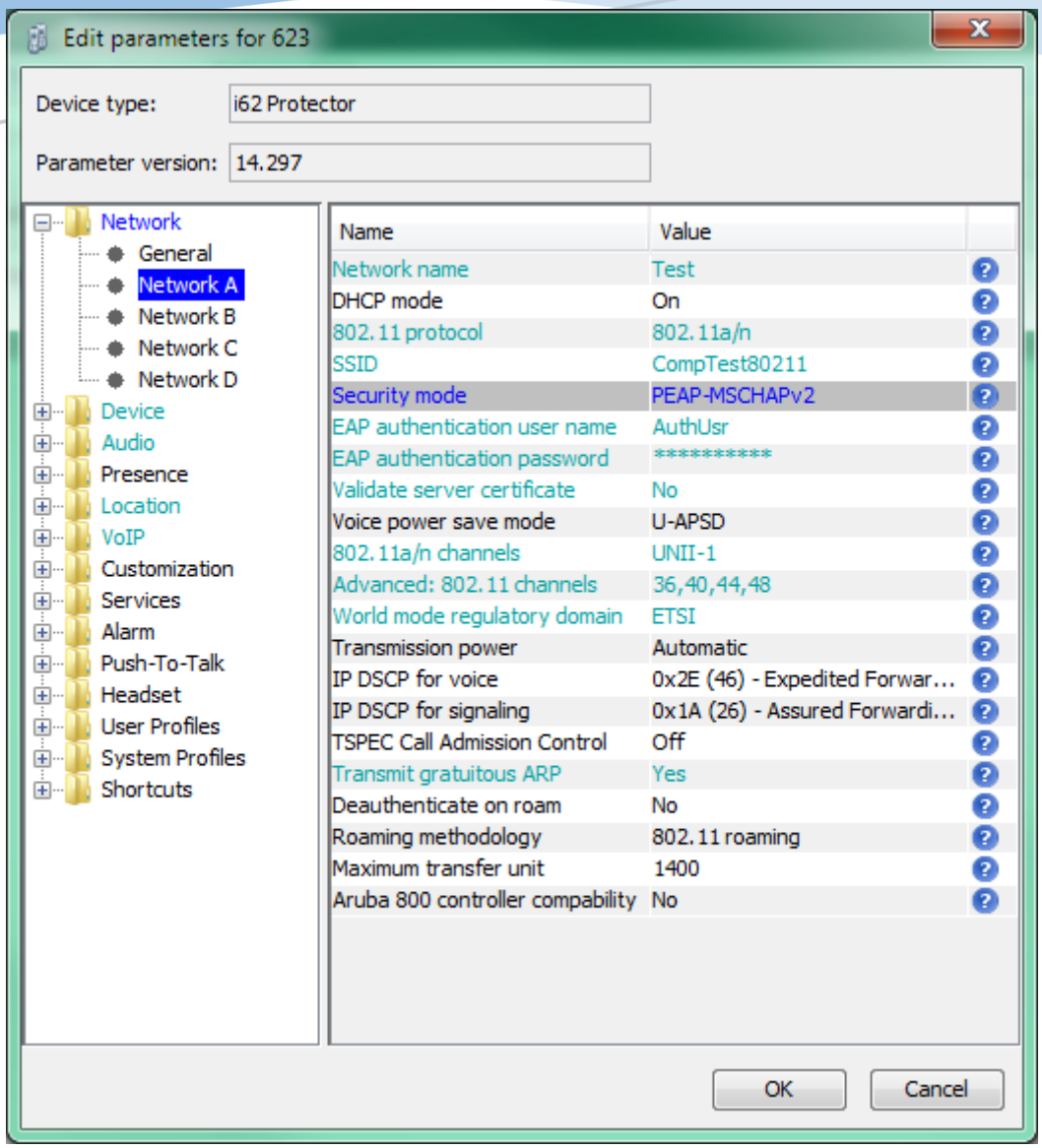
Network settings Ascom i62



I62 networks settings for WPA2

In the 802.11a/n channels select either UNII-1 or advanced and fill out the recommended channels in the box below. The Advanced: 802.11 channels.

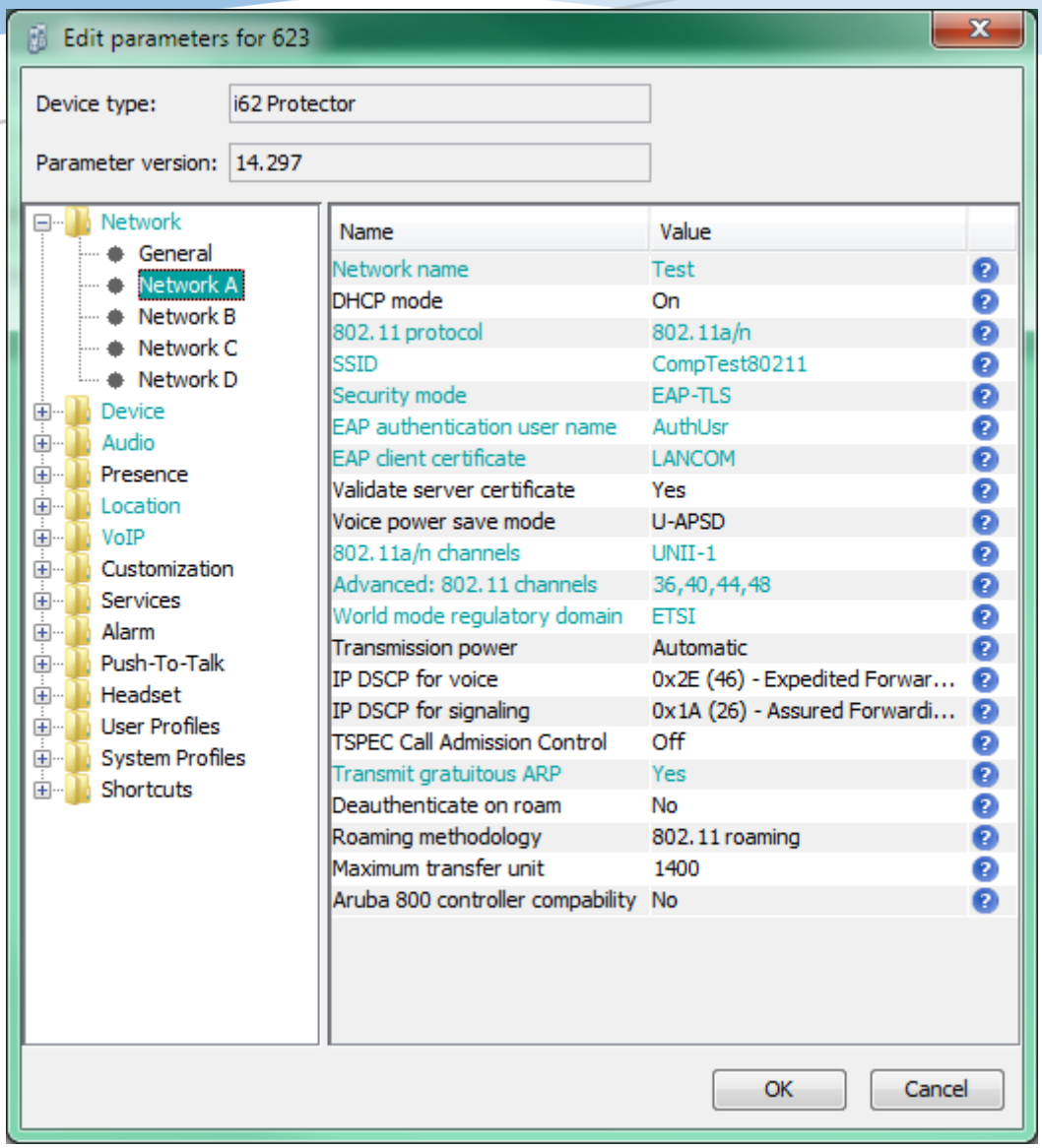
Transmit gratuitous ARP is advised to enable for the switched infrastructure behind the access points.



I62 network settings for 802.1X authentication (PEAP-MSCHAPv2)

- Set Security mode to PEAP-MSCHAPv2
- Input the user credentials under EAP authentication user name
- Input the password under EAP authentication password
- Set Validate server certificate to No

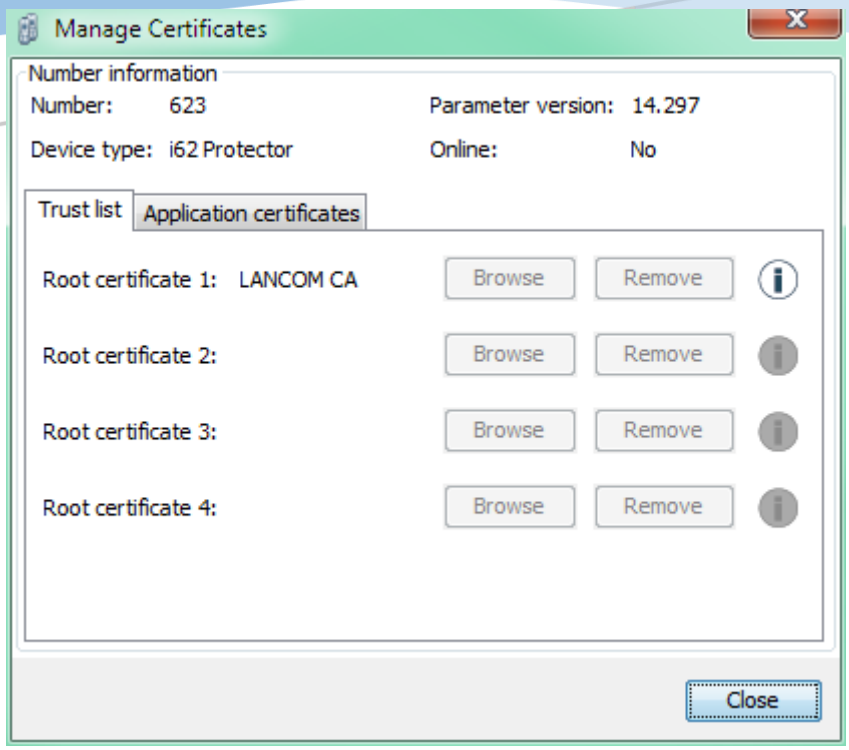
NB. The credentials can differ per i62 handset if required, depending on if the RADIUS server allows multiple devices to authenticate to the network on the same user account.



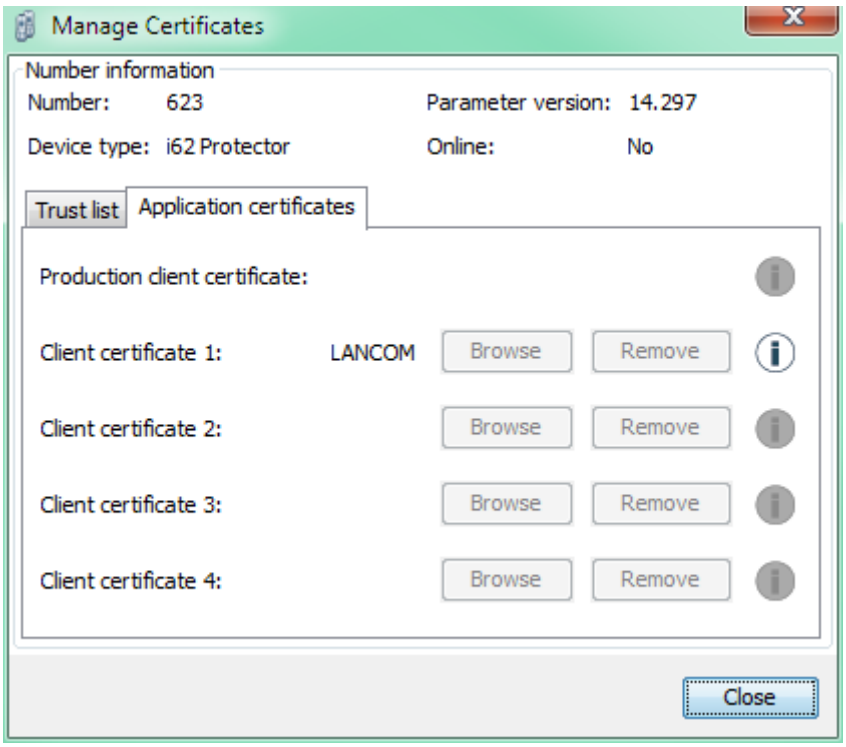
I62 network settings for 802.1X authentication (TLS)

- Set Security mode to PEAP-TLS
- Input the user credentials under EAP authentication user name. This is the same name to which the certificate is generated
- Select the certificate under EAP client certificate
- Set Validate server certificate to No

NB. The credentials can differ per i62 handset if required, depending on if the RADIUS server allows multiple devices to authenticate to the network on the same user account.



Upload a Root Certificate to the phone



Upload a Client Certificate to the phone

Appendix B: Detailed Test Records:

The tables below describes all tests that have been performed with the i62 VoWiFi handset and the different models access points. There is one column per model access point and one table per frequency.

Per access point all tests have been performed twice. Once for 2.4 GHz and once for 5 GHz.

Test for 2.4 GHz	**L(N)-8xx**	**LN-17xx**
Pass	30	30
Fail	0	0
Untested	6	6
Total	*36*	*36*

Test for 5 GHz	**L(N)-8xx**	**LN-17xx**
Pass	30	30
Fail	0	0
Untested	6	6
Total	*36*	*36*

Please refer to the attached xlsx documents for detailed information regarding the tests. There is one excel file per access point model.

WLANinteroperabilityTestReport_Rev D

WLANinteroperabilityTestReport_Rev D - i62-handset – L(N)-8xx.xls

WLANinteroperabilityTestReport_Rev D

WLANinteroperabilityTestReport_Rev D - i62-handset - LN-17xx.xls

Document history

Revision	Date	Author	Description
001	16-11-2017	N Crijns	Initial draft
002	20.11.2017	N Crijns	Feedback from Lancom