

Interoperability report

Ascom Myco 6.5.0

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 VoWiFi handsets and Ascom Myco handsets. 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

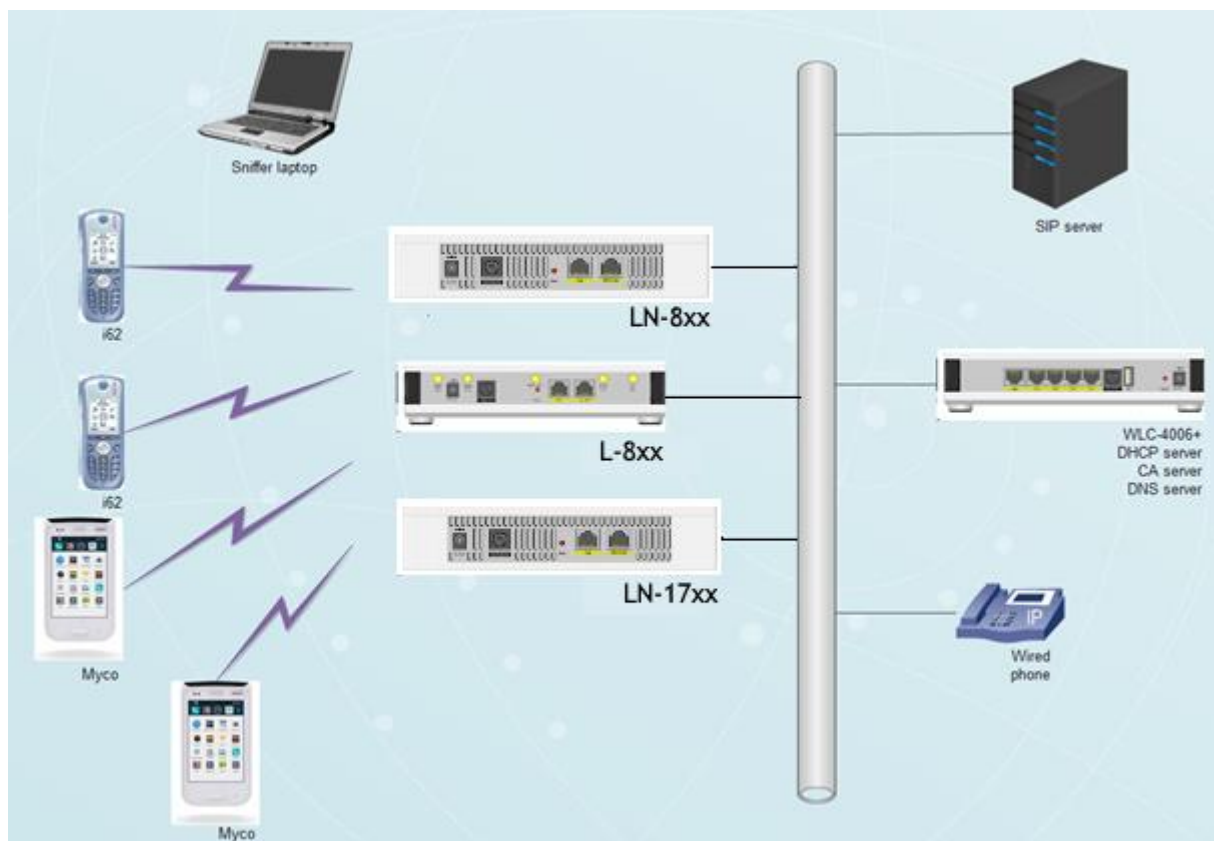
Test site

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.

<u>ASSOCIATION</u>	Test Description	Result
<u>/ AUTHENTICATION</u>		
#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
<u>POWER-SAVE AND QOS</u>		
#150	802.11 Power-save mode	PASS
#151	Beacon period and DTIM interval	PASS
#152	802.11e U-APSD	PASS
#202	WMM prioritization	PASS
<u>ROAMING AND</u>		
<u>HANDOVER TIMES</u>		
#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

<u>BATTERY LIFETIME</u>		
#501	Battery lifetime in idle	72 hours to 93 hours
#502	Battery lifetime in call with no power save	7 hours to 10 hours
#504	Battery lifetime in call with power save mode U-APSD	8 hours to 11 hours
<u>STABILITY</u>		
#601	Duration of call – Active mode	PASS
#602	Duration of call – U-APSD mode	PASS
<u>802.11n</u>		
#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 and TLS 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.

The recommended setting for DTIM is 5. The tested battery lifetime on standby is around 80 hours with the active call time around 10 hours. Keeping the DTIM to 1 (system default) will negatively affect 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 than 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 Myco 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

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 Myco, build number 6.5.0, android 4.4.2
- SNOM 300, version 8.7.34

Signalling Protocol

- Yeastar 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
(Devices deployed in the USA must be set Regulatory domain to “US”)

Ensure that Ascom Myco 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 Myco handsets. Please note that security settings were modified according to requirements in individual test cases.

Logical networks (ESS)

Logical WLAN networks (SSIDs) - Edit Entry

Logical WLAN network activated

Name: ASCOM-WPA2EAS

Inheritance

Inherit from entry: [] Select

Inherited values

Network name (SSID): CompTest80211

Connect SSID to: LAN at AP

VLAN mode: Untagged

VLAN ID: 2

Encryption: 802.11i (WPA)-PSK

Key 1/passphrase: [] Show

Generate password

RADIUS profile: DEFAULT Select

Allowed frequency bands: 2.4/5 GHz

AP standalone time: 0 minutes

802.11u network profile: [] Select

OKC (Opportunistic Key Caching) activated

MAC check activated

Suppress SSID broadcast: No

RADIUS accounting activated

Allow data traffic between stations of this SSID

WPA version: WPA2

WPA1 session key type: TKIP

WPA2 session key type: AES

WPA2 key management: Standard

Basis rate: 12 Mbit/s

Client Bridge Support: No

TX bandwidth limit: 0 kbit/s

RX bandwidth limit: 0 kbit/s

Maximum count of clients: 0

Min. client signal strength: 15 %

Enable LBS tracking

LBS tracking list: []

Convert to unicast: DHCP

Use long preamble for 802.11b

(U-)APSD / WMM powersave activated

Encrypt mgmt. frames: No

802.11n

Max. spatial streams: Auto

Allow short guard interval

Use frame aggregation

STBC (Space Time Block Coding) activated

LDPC (Low Density Parity Check) activated

OK Cancel

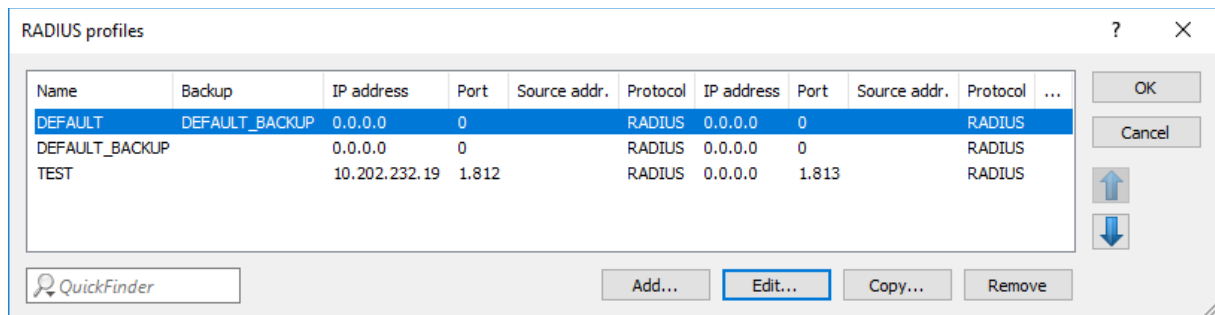
Logical WLAN Profiles can be set under WLAN Controller -> Profiles -> Logical WLAN networks (SSIDs)

- 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 OKC and U-APSD
- Disable Use long preamble for 802.11b
- In high density networks it is recommended to disable Allow short guard interval

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

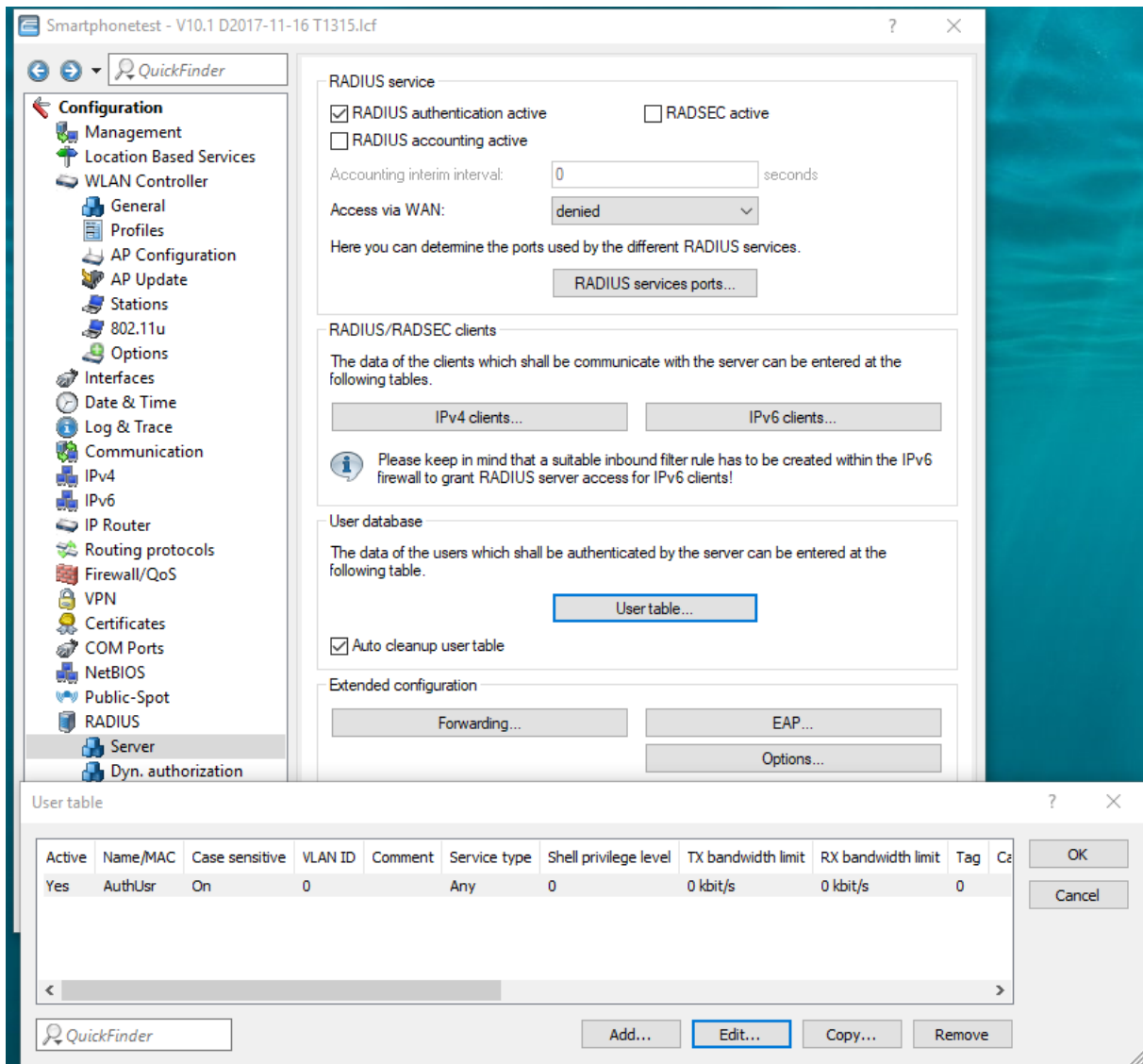
If an accounting server is used, fill out the second block aswell.

- 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/675ae5e6532c992a41256a100049e9e3/b75b51c219a60b14c1257e90002665bd?OpenDocument>

For an extensive description beyond the scope of this article.

Physical settings (PHY radio configuration):

Physical WLAN parameters - Edit Entry

Name:

Inheritance

Inherit from entry:

Country:

Auto. channel selection:

2.4 GHz mode:

5 GHz mode:

5 GHz Sub-bands:

DTIM period:

Background scan: seconds

Antenna gain: dBi

TX power reduction: dB

VLAN module of the managed accesspoints activated

Mgmt. VLAN mode:

Management VLAN-ID:

Client steering:

Pref. frequency band:

Probe request ageout time: seconds

Adaptive RF Optimization:

Enable QoS according to 802.11e (WME)

Indoor only mode activated

Report seen unknown clients

- Enter a profile name
- Select channels for 2.4 and 5 at Auto. Channel selection if you wish 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:

WLAN profiles - Edit Entry

Profile name:

Specify in the following list up to 16 logical WLAN networks for this profile.

WLAN network list:

Physic. WLAN parameters:

List of alternative WLCs:

802.11u venue profile:

Configuration delay: seconds

Device LED profile:

LBS server profile:

Wireless ePaper profile:

Wireless IDS profile:

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

Access point configuration

Access point table - Edit Entry

Entry active
 Update management active

Additional information:

MAC address: 00:a0:57:2b:d1:33
AP name: LN860-Ascom
Location: Bureau
Comment:
Groups: ASCOM-TEST Select
WLAN profile: ASCOM-TEST Select
Client steering profile: DEFAULT Select
LBS - AP location: Select
Control channel encryption: DTLS
Antenna grouping: Auto

Fixed IP addresses

IP address: 0.0.0.0
IP parameter profile: DHCP Select

Wireless ePaper interface

Channel: Automatic selection

WLAN interface 1

Mode WLAN ifc.1: 2,4 GHz only
Auto. channel selection: 6 Select
Max. channel bandwidth: 20 MHz
Antenna gain: dBi
TX power reduction: 9 dB

WLAN interface 2

Mode WLAN ifc.2: 5 GHz only
Auto. channel selection: 40 Select
Max. channel bandwidth: 20 MHz
Antenna gain: dBi
TX power reduction: 9 dB

iBeacon interface

iBeacon profile: Select
Minor ID: 0
 2402 MHz 2426 MHz 2480 MHz
Transmission Power: High

OK Cancel

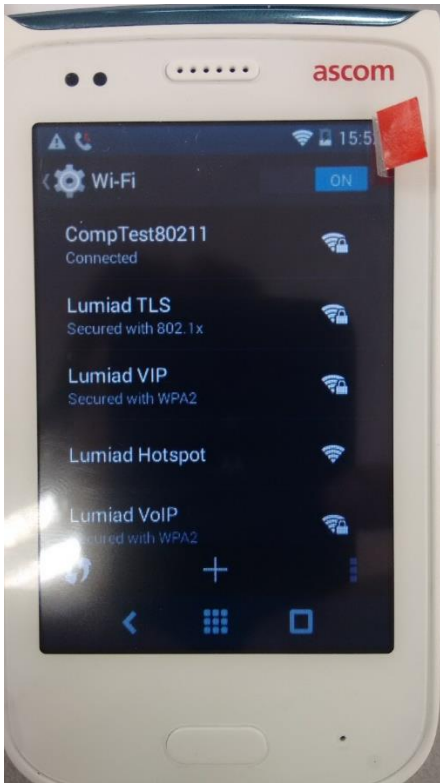
- Select the correct WLAN profile for the access point
- If client steering is used, select the profile here
- The Auto. Channel selection in this screen will overwrite the PHY parameter setting!
- Set Max. Channel bandwidth to 20 MHz. 40 and 80 are supported, but not recommended for VoWLAN deployments.

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



Smartphonetest -
V10.1 D2017-11-16 T

Network settings Ascom Myco



Myco WPA2-PSK network settings

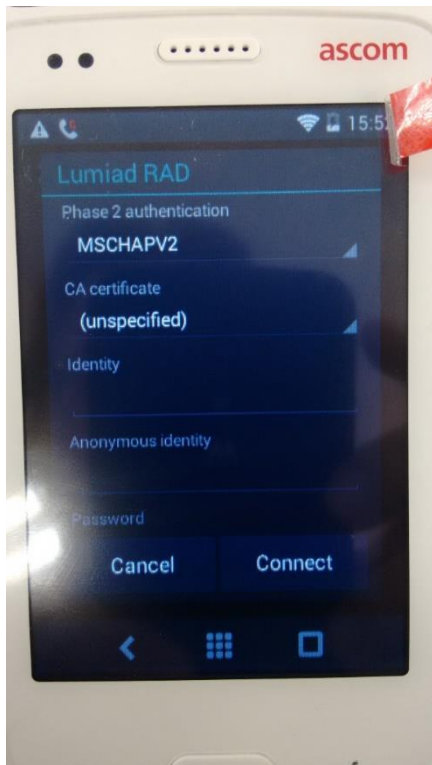
- Go to the menu and press the settings icon
- In the settings menu, select Admin settings
- You will be prompted for a password. Default this is 40022
- Press on the Wi-Fi menu

- Press on the column symbol in the right bottom corner to call up the menu
- Press on Advanced
- Deselect the network notification box
- Verify that Keep Wi-Fi on during sleep is on Always
- Change the Wi-Fi Frequency band to your frequency
- Press on Wi-Fi channels
- Select the channels used by your deployment.

- Return to the previous menu
- Select the desire SSID
- Input the key
- Press on Connect

The handset should now connect to the wireless network

NB. For recommended channels please refer to a previous chapter for the Ascom recommended channel deployment



Myco WPA2-Enterprise (PEAP-MS-CHAP-v2) network settings

- Go to the menu and press the settings icon
- In the settings menu, select Admin settings
- You will be prompted for a password. Default this is 40022

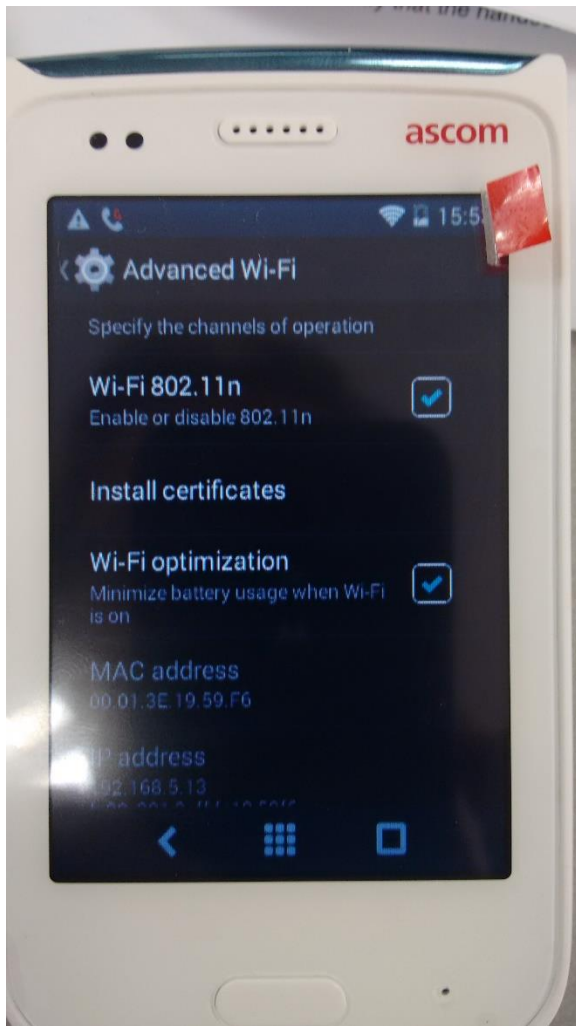
- Press on the Wi-Fi menu
- Press on the column symbol in the right bottom corner to call up the menu
- Press on Advanced
- Deselect the network notification box
- Verify that Keep Wi-Fi on during sleep is on Always
- Change the Wi-Fi Frequency band to your frequency
- Press on Wi-Fi channels
- Select the channels used by your deployment.

- Select the desire SSID
- Select EAP method -> PEAP
- Select Phase 2 authentication -> MSCHAPv2
- Input the identity
- Input the password
- Press on Connect

The handset should now connect to the wireless network

NB. An Anonymous identity is not required.

NB. For recommended channels please refer to a previous chapter for the Ascom recommended channel deployment



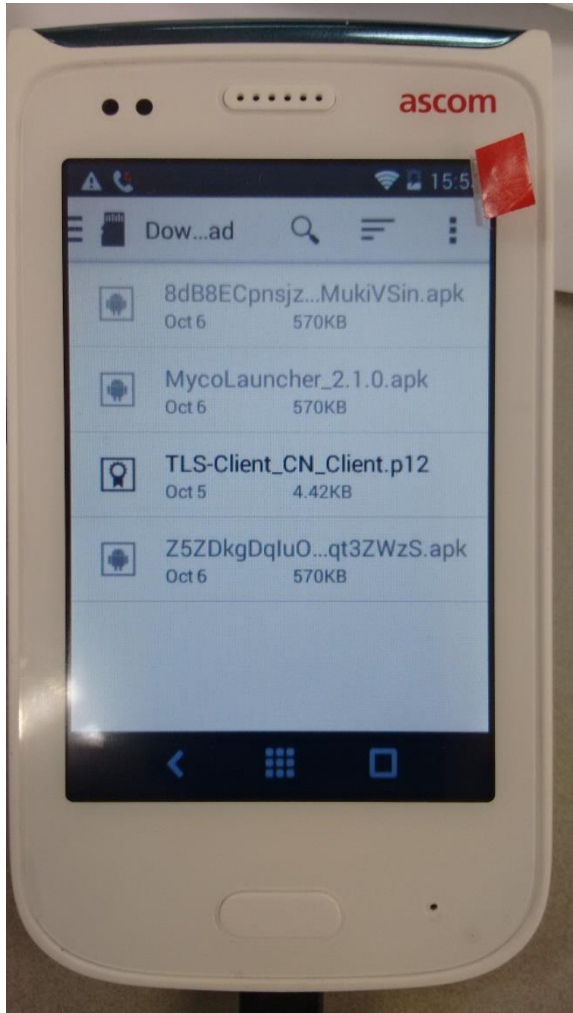
Myco WPA2-Enterprise (TLS) network settings

- Connect the handset to a PC or laptop
- Upload the CA certificate and Client certificate to the handset download map
- Disconnect the handset from the PC or Laptop

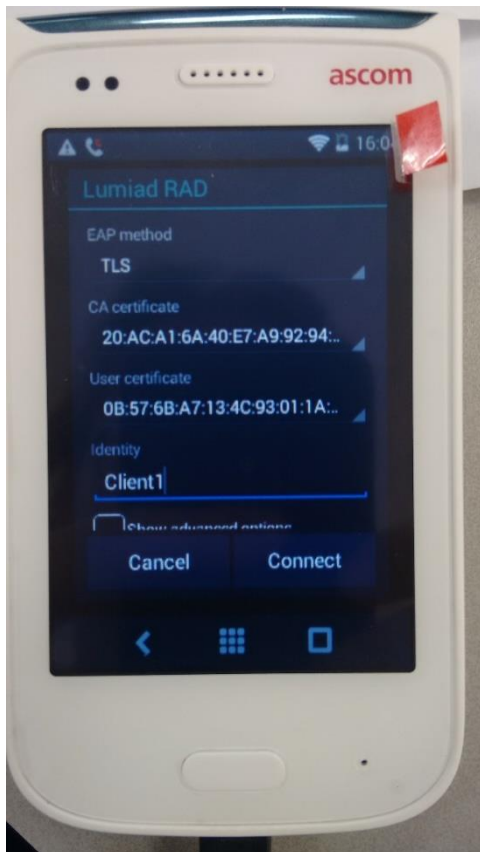
- Go to the menu and press the settings icon
- In the settings menu, select Admin settings
- You will be prompted for a password. Default this is 40022
- Press on the Wi-Fi menu

- Press on the column symbol in the right bottom corner to call up the menu
- Press on Advanced
- Deselect the network notification box
- Verify that Keep Wi-Fi on during sleep is on Always
- Change the Wi-Fi Frequency band to your frequency
- Press on Wi-Fi channels

- Select the channels used by your deployment. For recommended channels please refer to a previous chapter for the Ascom recommended channel deployment.
- Press install certificates



- Select the desired certificate for installation that is uploaded from the PC or laptop previously



- Return to the WI-Fi menu
- Select the desired SSID
- Select EAP method TLS
- Select the desired CA certificate
- Select the desired User certificate
- Input the Identity used in the client certificate
- Press on Connect

The handset should now connect to the network

NB. Take care with selecting the right certificate. The common names with which they uploaded are not shown. Instead the identifier string of the certificate is used. This may cause confusion and allow for switching the CA and client certificate around.

Ascom Myco can also be configured “over the air” through Ascom’s centralized management. Please refer to Ascom’s documentation for further information.

Appendix B: Detailed Test Records:

The tables below describes all tests that have been performed with the Myco 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
<i>Pass</i>	30	30
<i>Fail</i>	0	0
<i>Untested</i>	6	6
<i>Total</i>	36	36

Test for 5 GHz	L(N)-8xx	LN-17xx
<i>Pass</i>	30	30
<i>Fail</i>	0	0
<i>Untested</i>	6	6
<i>Total</i>	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 - MyCo-handset – L(N)-8xx.xls



WLANinteroperabilityTestReport_Rev D

WLANinteroperabilityTestReport_Rev D - MyCo-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