Technology Solution Guide

Deploying Ascom i62 with Aruba Networks' Secure Mobility Solution

Ascom i62 Handset and OEM derivatives
Software version 5.5.0

Aruba iAP
103/205/215
AOS version 6.4.2.6-4.1.3.0

June 30th 2016

WARRANTY DISCLAIMER

THE FOLLOWING DOCUMENT, AND THE INFORMATION CONTAINED HEREIN IS PROVIDED ON AN "AS IS" BASIS. ARUBA MAKES NO REPRESENTATIONS, WARRANTIES, CONDITIONS OR GUARANTEES AS TO THE USEFULNESS, QUALITY, SUITABILITY, TRUTH, ACCURACY OR COMPLETENESS OF THISDOCUMENT AND THE INFORMATION CONTAINED IN THIS DOCUMENT.

DISCLAIMER OF LIABILITY

Aruba Networks, Inc. disclaims liability for any personal injury, property or other damages of any nature whatsoever, whether special, indirect, consequential or compensatory, directly or indirectly resulting from the certification program or the acts or omissions of any company or technology that has been certified by Aruba Networks.

Certification does not mean that the company is a subcontractor or under the technical control or direction of Aruba Networks. In conducting the certification program Aruba Networks is not undertaking to render professional or other services for or on behalf of any person or entity.

Table of Contents

Introduction

This document describes the steps and guidelines necessary to configure Aruba's wireless LAN (AOS version. 6.4.2.6-4.1.3.0) infrastructure to work interoperable with Ascom's i62 handsets.

The guide is intended to be used in conjunction with Aruba and Ascom configuration guides. Please contact the respective company's sales engineering or support groups should additional information be required.

Solution Verified: Ascom Phones

Aruba Product: Aruba Campus WLAN Solution OS version 6.4.2.6-4.1.3.0

Partner Solution Tested: Ascom i62 Handset; Software version 5.5.0

Solution Components

Aruba Campus WLAN Solution

Secure and reliable mobility is the responsibility of the enterprise network, which must support a wide range of converged clients over wireless, wired, and remote access networks. Laptops and smartphones are capable of simultaneously running voice, data, and now video applications, an operating model that breaks traditional dedicated VLAN and SSID architectures. Delivering the quality of service (QoS), bandwidth, and management tools necessary to accommodate these devices on a grand scale – within a campus environment, to users on the road, and in branch offices – requires a specially tailored system design.

Aruba's unique application and device fingerprinting enable the system to detect the types of traffic flows, and the devices from which they originate. The network can then be dynamically conditioned to deliver QoS - on an application-by-application, device-by-device basis - as needed to ensure highly reliable application delivery. Aruba's integrated policy enforcement firewall isolates applications from one another to essentially create multiple dedicated virtual networks, and then allocates the necessary bandwidth for each user and application.

To ensure reliable application delivery in changing RF environments, Aruba's Adaptive Radio Management (ARM) technology forces client devices to shift away from the noisy 2.4GHz band to the quieter 5GHz band, adjusts radio power levels to blanket coverage areas, load balance by shifting clients between access points, and even allocates airtime based on the capabilities of each client device. The result is a superb user experience without any user involvement.

These services are complemented by security systems that ensure the integrity of the network. Rogue detection, wireless intrusion and prevention, access control, remote site VPN, content security scanning, end-to-end data encryption, and other services protect the network and users at all times.

Aruba's extensive portfolio of campus, branch/teleworker, and mobile solutions simplify operations and secure access to unified communications applications and services - regardless of the user's device, location, or network. This dramatically improves productivity, lowering capital and operational costs while providing a superior uninterrupted user experience.

Ascom Solution

The Ascom i62 offers a sophisticated telephony, messaging and alarm solution for enterprise business based on Wi-Fi technology. By offering Voice over Wi-Fi, only one network needs to be installed and maintained for all applications including Internet access, e-mail, voice and other business related applications.

The latest 802.11n and 802.11ac standards provide the benefits of higher throughput and longer range, increasing the ability to integrate with other systems and build efficient applications. With the new generation networks and handsets the capacity and versatility outperforms any other on-site wireless technology.

The Ascom i62 offers a unique management tool with central management concept enabling remote management and SW upgrades of the handsets over the air.

Certified Product Summary

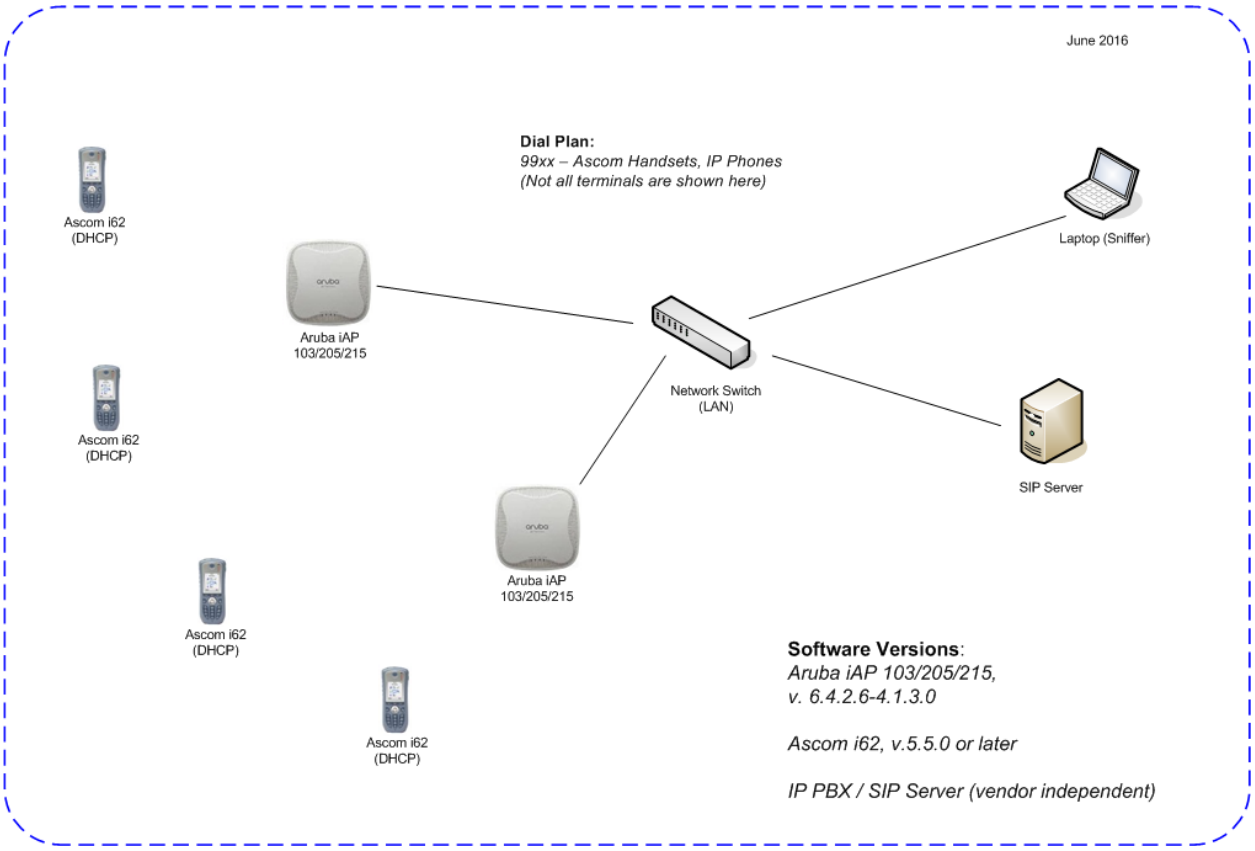
Manufacturer	Ascom Wireless Solutions
Products Certified	Ascom i62 and OEM derivatives
• Hardware Model Numbers	WH1-xxxx
• Software Version Numbers	5.5.0
RF Features Tested	
• Radio Supported	802.11a/b/g/n
QoS Features Supported / Tested	WMM
• Powersave Features Tested	U-APSD
• Encryption Supported	WPA2-PSK, PEAP-MSCHAPv2, EAP-TLS
• Encryption Tested	WPA2-PSK, PEAP-MSCHAPv2, EAP-TLS
• 802.11h Supported	Yes
• Key Caching Support for Optimized Roaming	OKC and PMK
Voice Specific Features	
• Protocols Supported	SIP-UDP, SIP-TCP, SIP-TLS, H.323
• Control Traffic Pattern	Handset to Server and vice versa
• Voice Traffic Pattern	Peer-to-peer (between handsets)
• # of Calls per AP Tested	12 calls (not AP-capacity limited)

ArubaEdge Solution Qualification

Qualification Objective

Validate the interoperability of the Ascom i62 with the Aruba's wireless LAN infrastructure (version 6.4.2.6-4.1.3.0).

Network Topology



Settings on the Aruba WLAN

The following Aruba Instant Access Point configuration settings are recommended for use with Ascom i62 handsets:

- RF Recommended Settings for Ascom
  - Beacon Interval: 100ms
  - DTIM Period: 5
  - WMM/ U-APSD Enabled
    802.11d Regulatory Domain: Country specific
    Note: Exception for the FCC region
- Encryption and Authentication
  - The handset and the WLAN infrastructure support and were tested with WPA/WPA2 enterprise and PSK. Please refer the Aruba configuration guide for additional information on how the SSIDs and encryption/authentication methods should be configured.
- Adaptive Radio Management
  - Enable ARM, voice aware scanning, WMM / UAPSD, and band steering.

Ascom Settings

The following Ascom i62 Handset configuration settings are recommended for use with Aruba Instant Access Point.

Ascom i62 Configuration:

- World Mode Regulatory Domain set to World mode
  Note: In the FCC region, set to USA
- IP DSCP for Voice: 0x2E (46) – Expedited Forwarding
- IP DSCP for Signaling: 0x1A (26) – Assured Forwarding 31
- Transmit Gratuitous ARP: Enable

Refer to Appendix A for additional details.

Test Methodology

Summary Test Results

The features and functions listed below were assessed during interoperability testing. The test results are presented in the right-most column

WLAN Features

High Level Functionality	Result
Association, Open with No Encryption	OK
Association, WPA2-PSK, AES Encryption	OK
Association, PEAP-MSCHAPv2 Auth., AES Encryption	OK
Association, EAP-TLS	OK
Association, Multiple ESSIDs	OK
Beacon Interval and DTIM Period	NOK*
Pre-authentication	N/A
PMKSA Caching	OK
WPA2-Opportunistic/Proactive Key Caching	OK
WMM Prioritization	OK
802.11 Power-Save Mode	N/A**
802.11e U-APSD	OK
802.11e U-APSD (load test)	OK

*) iAP205/215 will advertise a DTIM interval of 1 irrespective of configuration. Refer to the section "Known Limitations" in this report.

**) Ascom strongly recommends that U-APSD is enabled in the WLAN.

Roaming

High Level Functionality	Result
Roaming, Open with No Encryption	OK (typical avg. 30-35ms)
Roaming, WPA2-PSK, AES Encryption	OK (typical avg. 40-50ms)
Roaming, PEAP-MSCHAPv2 Auth, AES Encryption	OK (typical avg. 40-50ms)*

*) Results observed with Opportunistic Key Caching enabled.

Known Limitations

- Ascom i62 does not handle 802.11K info correctly which affects the roaming negatively. It is therefore highly recommended to configure the Aruba system not to advertise the 802.11K capabilities for the Ascom i62 SSID.

- During testing, it was occasionally noted that an Ascom i62 associated to a WLAN on the 5GHz band couldn't immediately switch to 2.4GHz. As a workaround, "Band Steering Mode" was changed from "Prefer 5GHz" to "Disabled" (refer to the screenshot on p.21 or Aruba's documentation regarding band steering).

- 802.11ac-capable iAP205/215 advertises a DTIM interval of 1 irrespective of configuration (5), which marginally increases the battery consumption of the Ascom i62 in idle mode (observed standby time: approx. 66-68 hours).

  This issue in AOS version 6.4.2.6-4.1.3.0 does not affect 802.11n-only iAP103.

Conclusion

The verification, including association, authentication, roaming, and load test produced very good results overall. Roaming times were in general good with roaming times of around 40-50ms both when using WPA2-PSK/AES and PEAP-MSCHAPv2 (WPA2/AES).

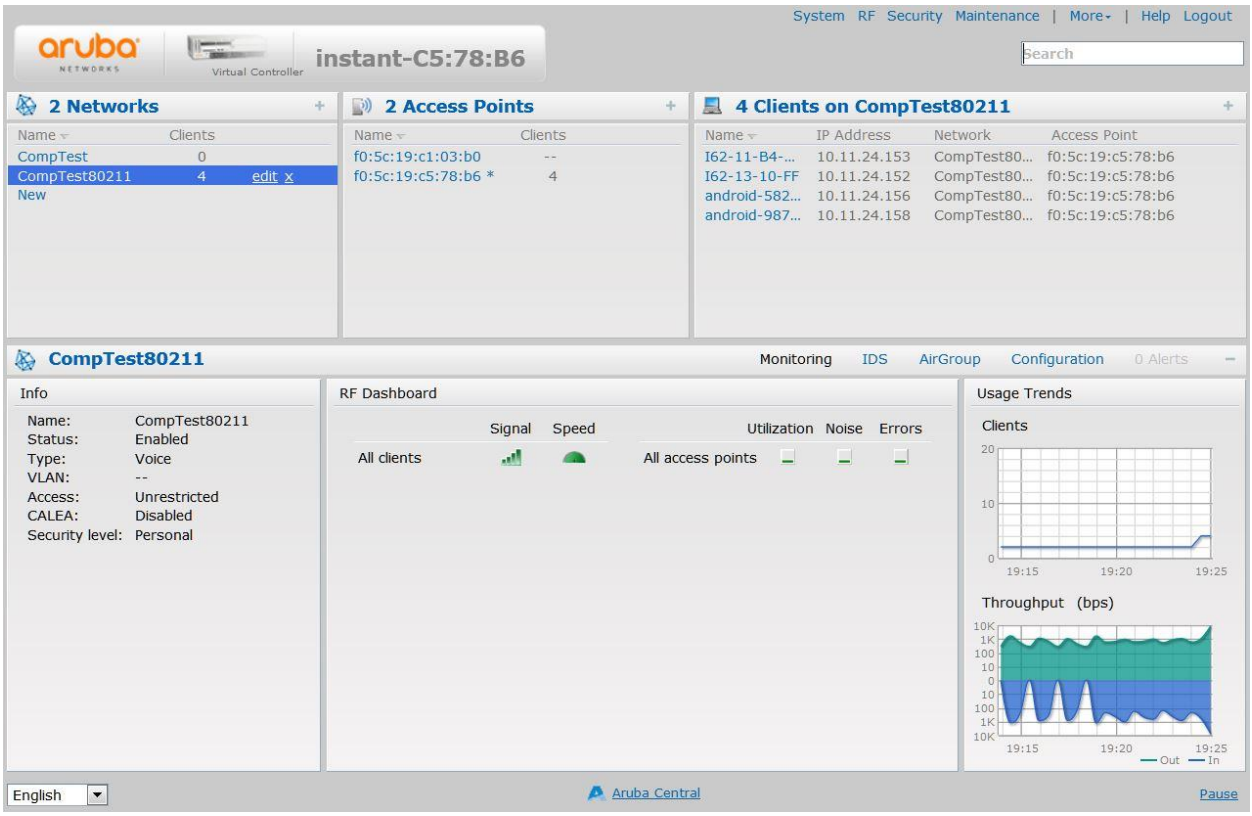
Load testing showed that more than 12 Ascom i62 Handsets could maintain a call via a single Aruba access point when tested in U-APSD mode. Note that 12 was the maximum number of devices tested and not the capacity limit.

Appendix A

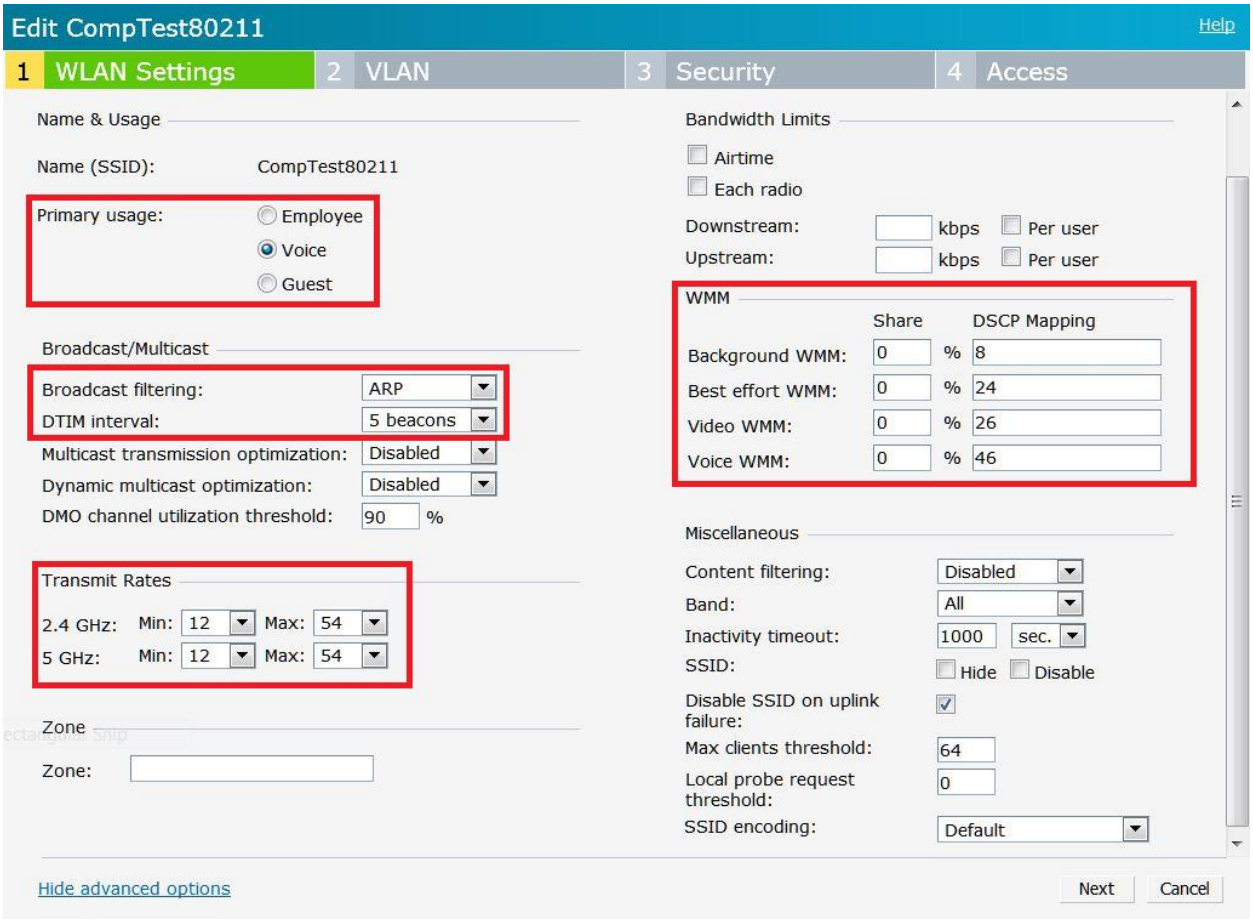
This section includes screenshots and explanations of basic settings required to use Ascom i62 Handsets with Aruba Instant Access Points. Please note the security settings of each test case, as they were modified according to needs of the test cases.

The configuration file is found at the end of Appendix B.

General settings (SSID, Authentication, Radio and QoS)

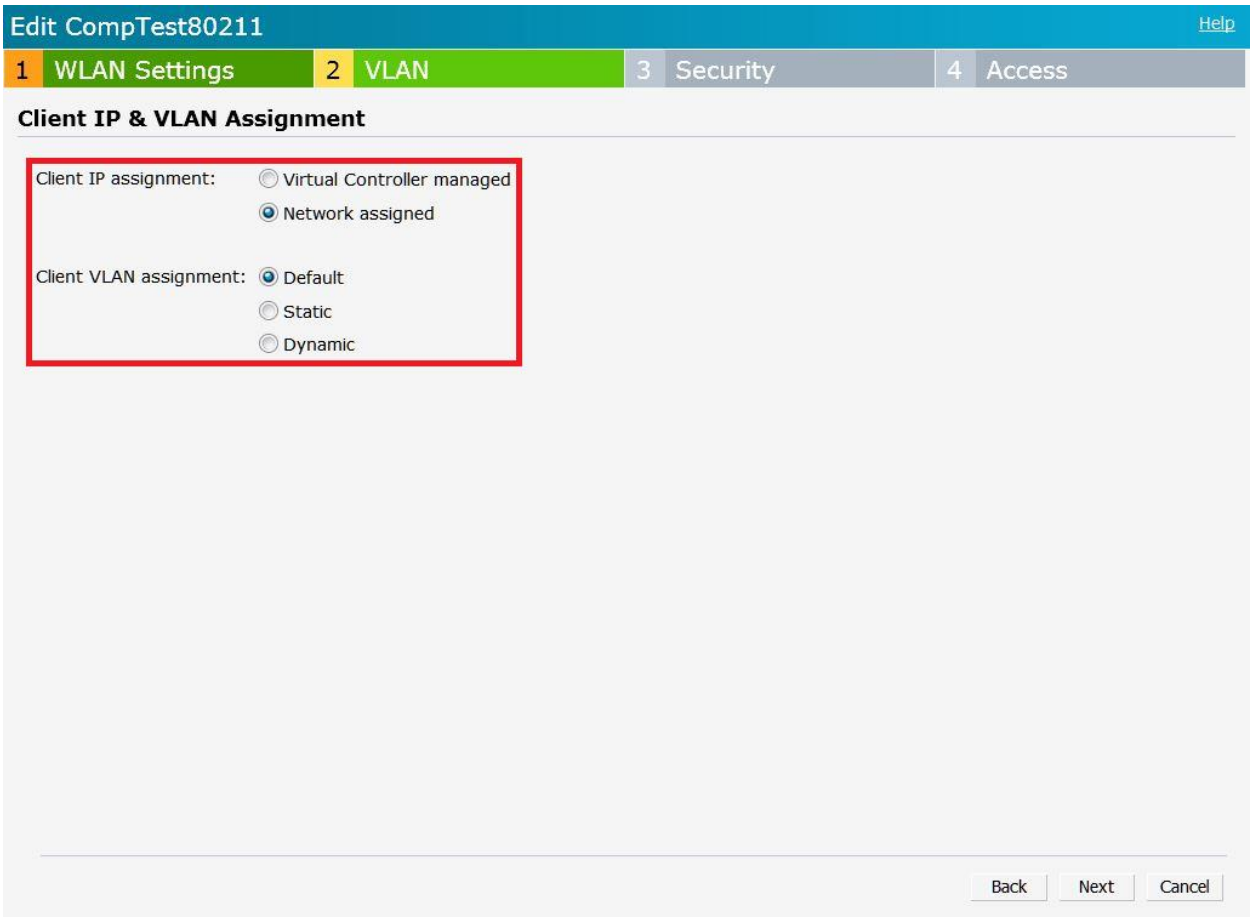


General Overview



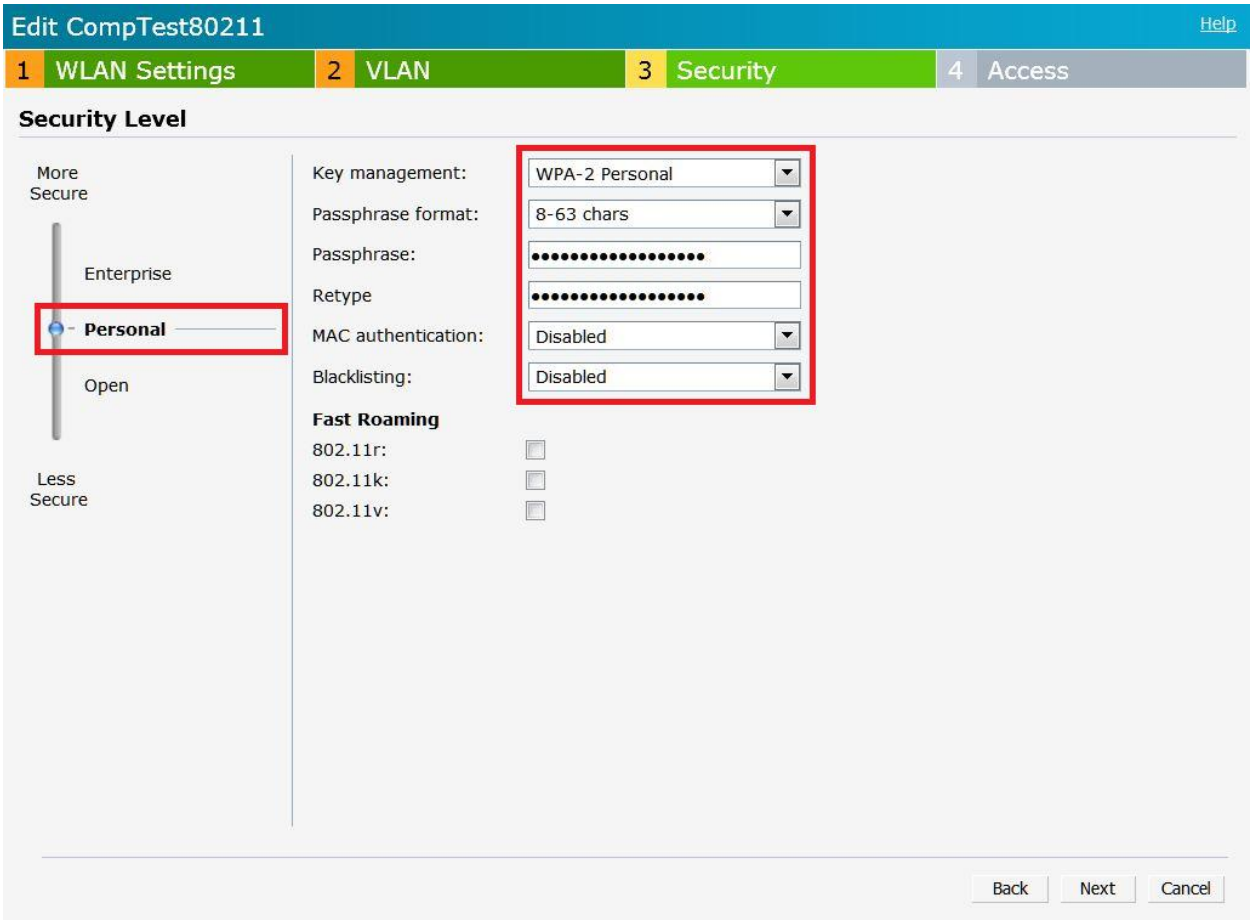
Network configuration -> WLAN settings

- Select Voice as primary usage
- Set broadcast filtering to ARP. This implies that access points drop all broadcast and multicast frames, except ARP and DHCP. In addition, ARP requests will be converted to unicast and sent to the associated station.
- Set DTIM Interval to 5. This value is recommended for maximum battery conservation without impacting call quality. A lower value is possible but will decrease the battery life slightly.
- Ascom recommends disabling the lowest transmit rates and recommends that 12mbits is the lowest basic rate.
- To match the default values for the i62 ensure to use DSCP 46 for Voice, 26 for video and 0 for best effort. Ensure that WMM and U-APSD are enabled (default).



Network configuration -> VLAN settings

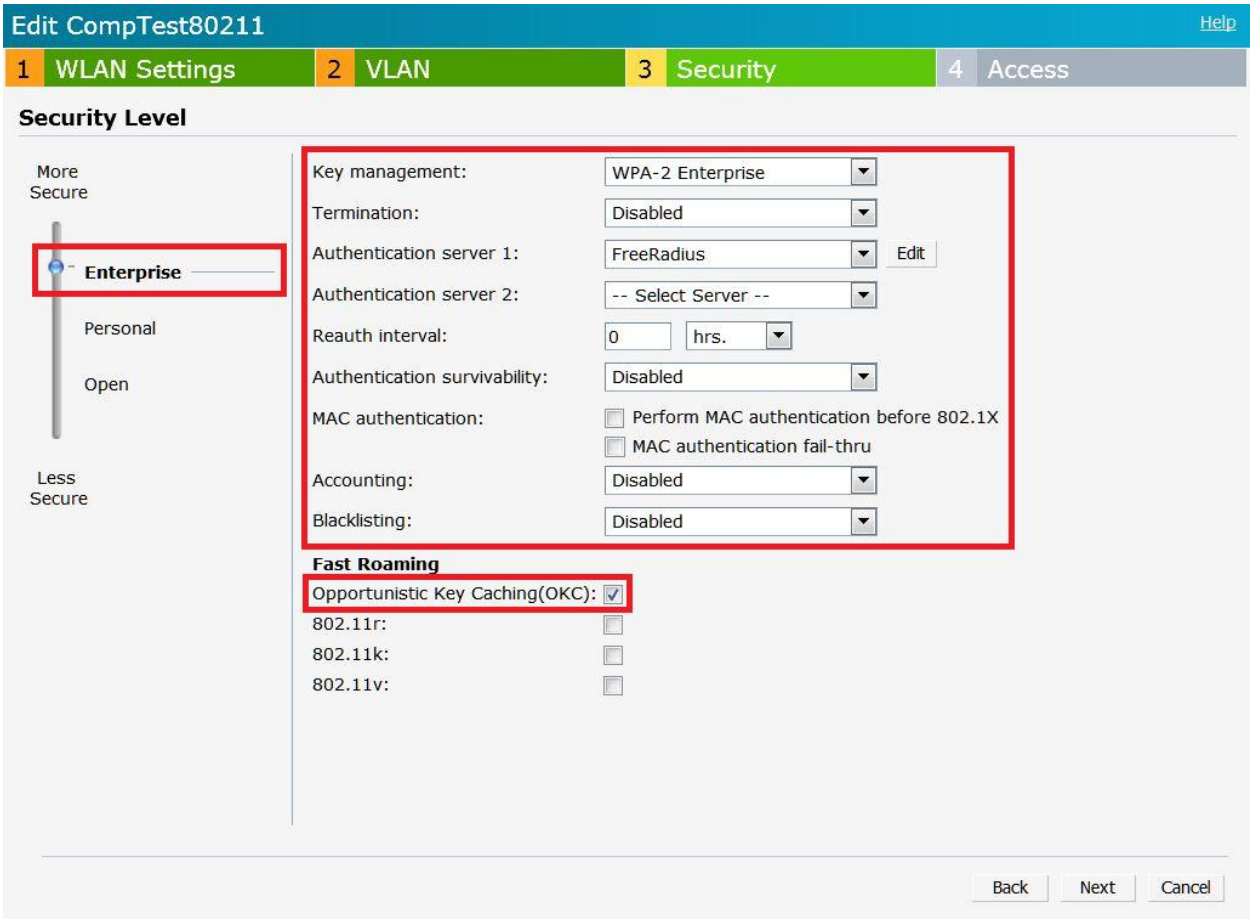
- Client IP assignment is handled by the network in the test setup.
- VLAN assignment set to Default.



Network configuration -> Security (Personal – WPA2-PSK)

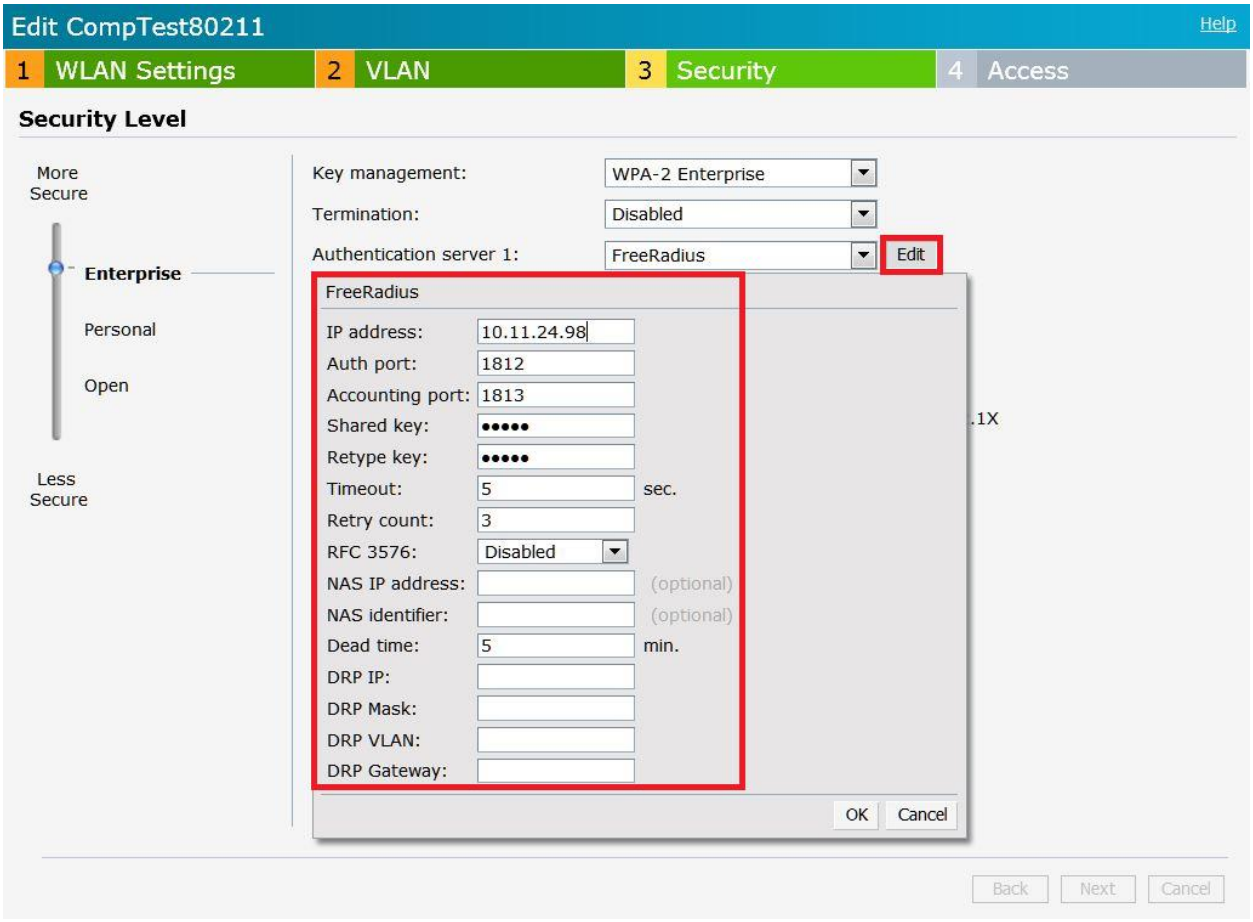
- Key Management set to WPA2. WPA2 also implies that AES/CCMP encryption will be used, while WPA implies TKIP encryption. The latter is not recommended.

Note: The Ascom i62 does not support fast roaming.



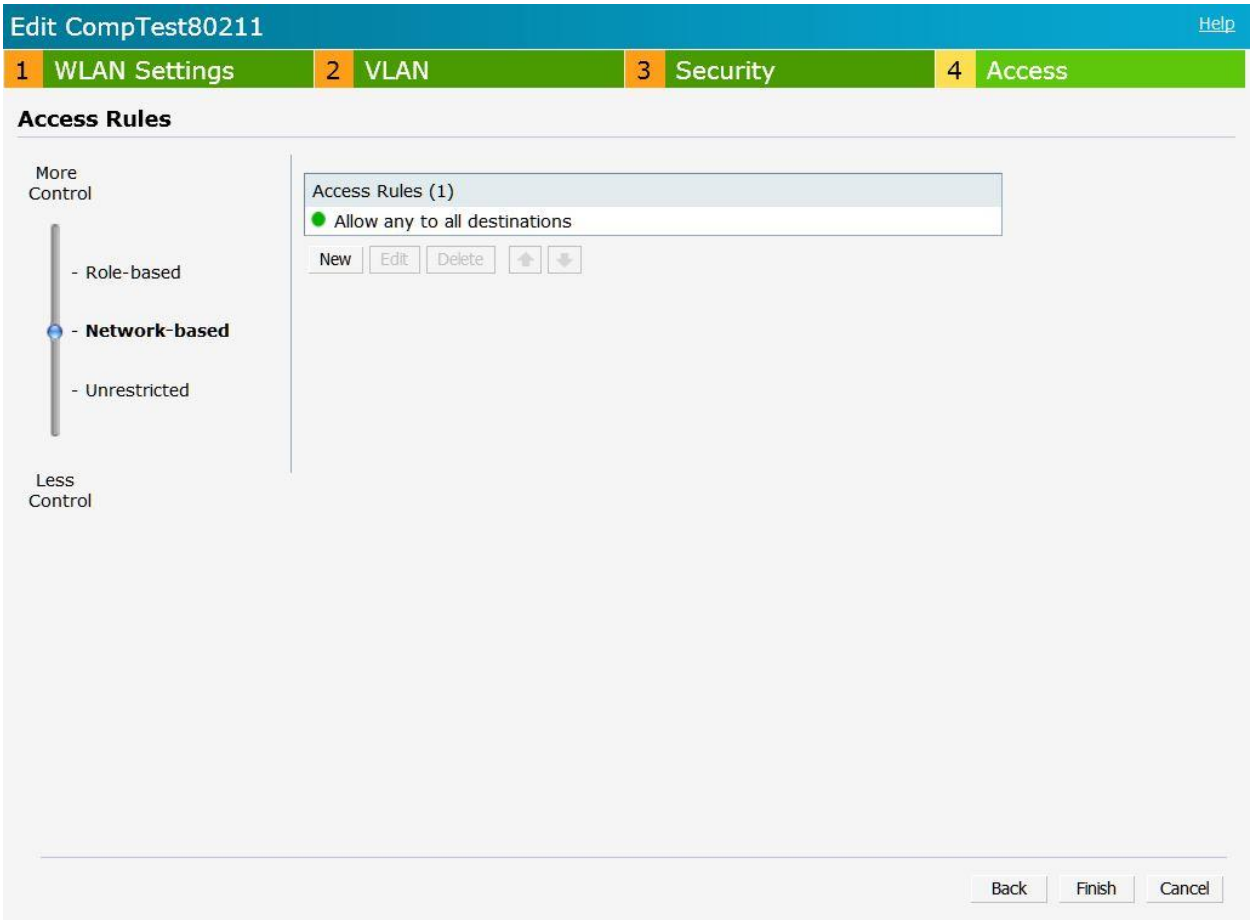
Network configuration -> Security (Enterprise/.1X)

- Set Key management to WPA-2 Enterprise
- Ensure that Opportunistic Key Caching is enabled.
- Configure Authentication server 1. See next picture.



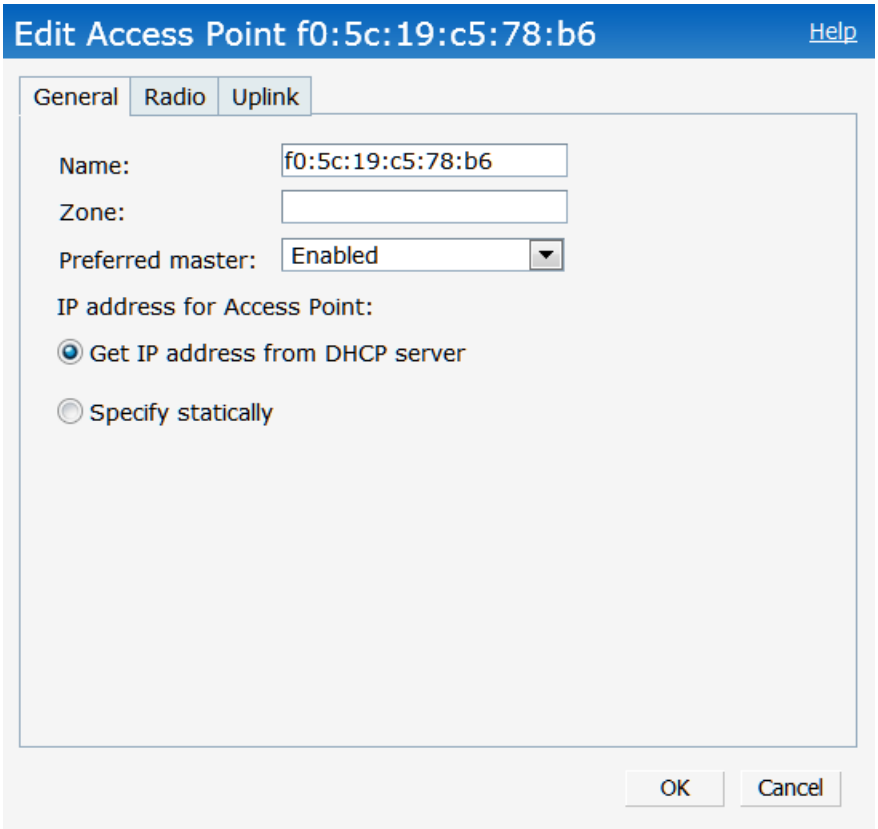
Network configuration -> Security (Enterprise/.1X)

- The IP address and the secret must correspond to the IP address and the credential used by the Radius server.



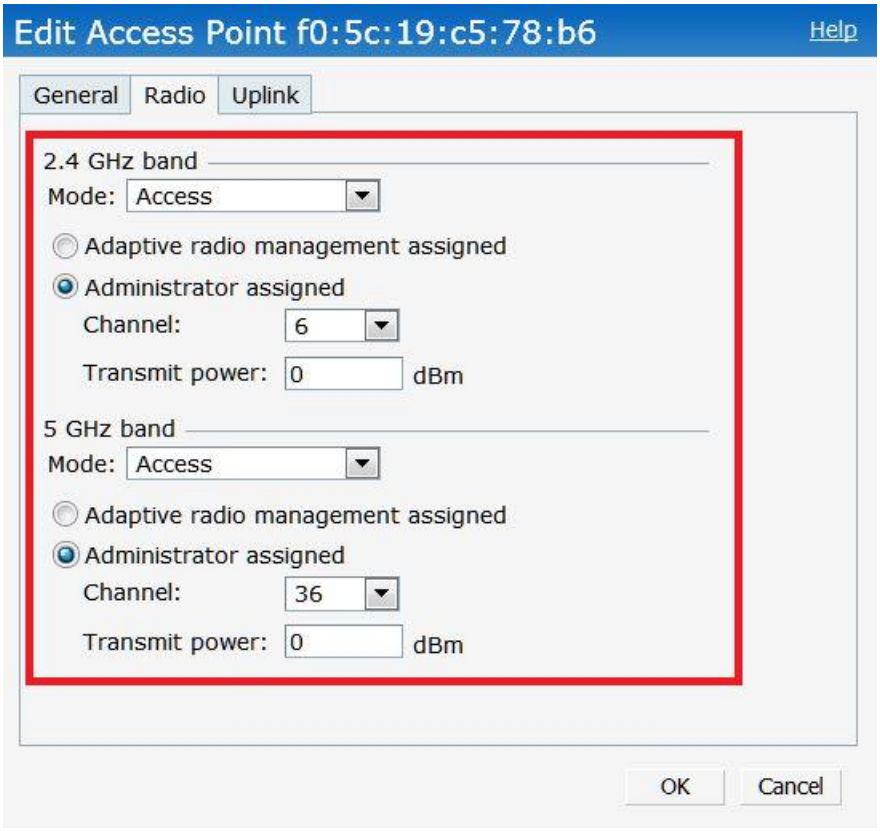
Network configuration -> Access

- Access rules set to default (Network-based)



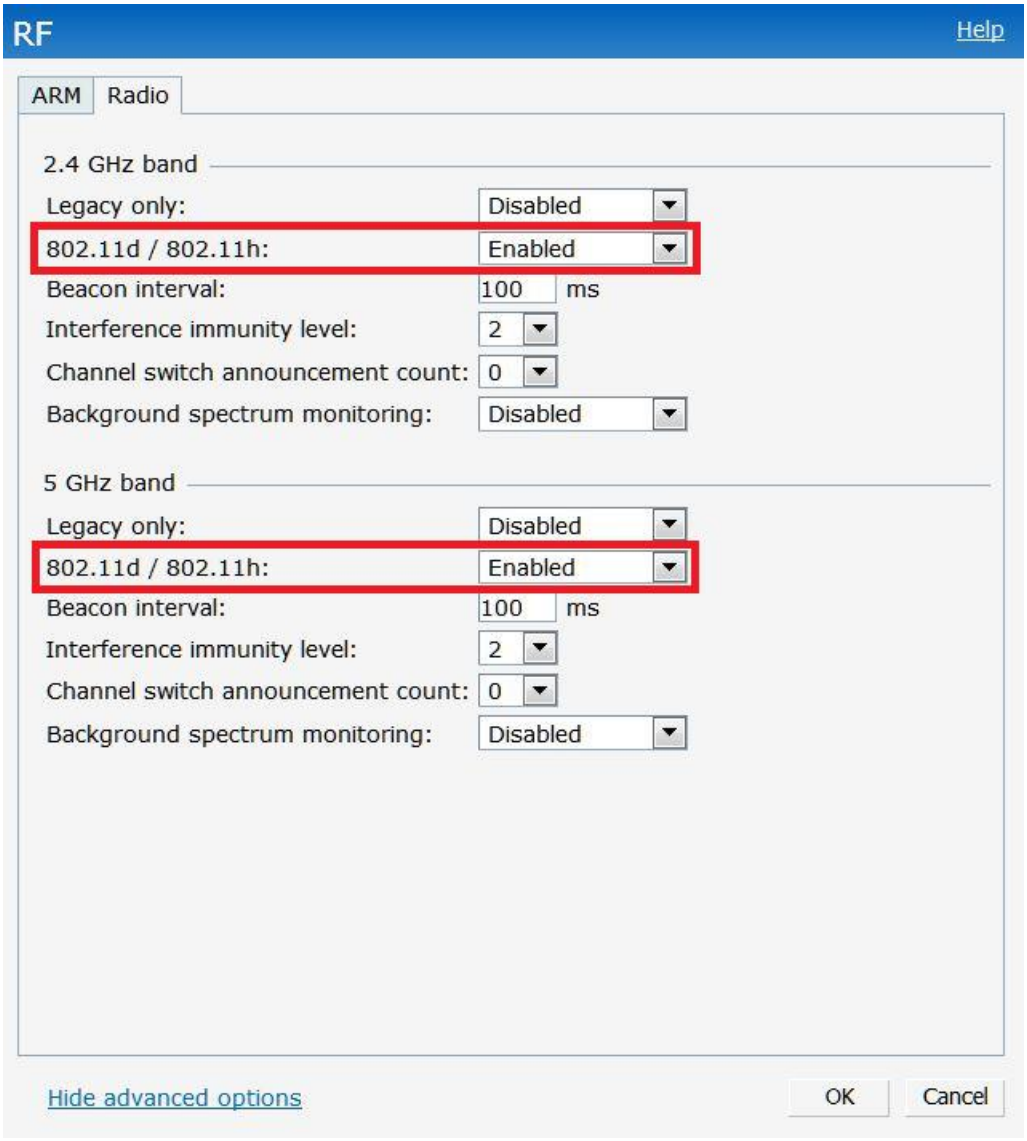
Configuration of Access Points -> General

- The access points will get their IP address assigned by a DHCP server.



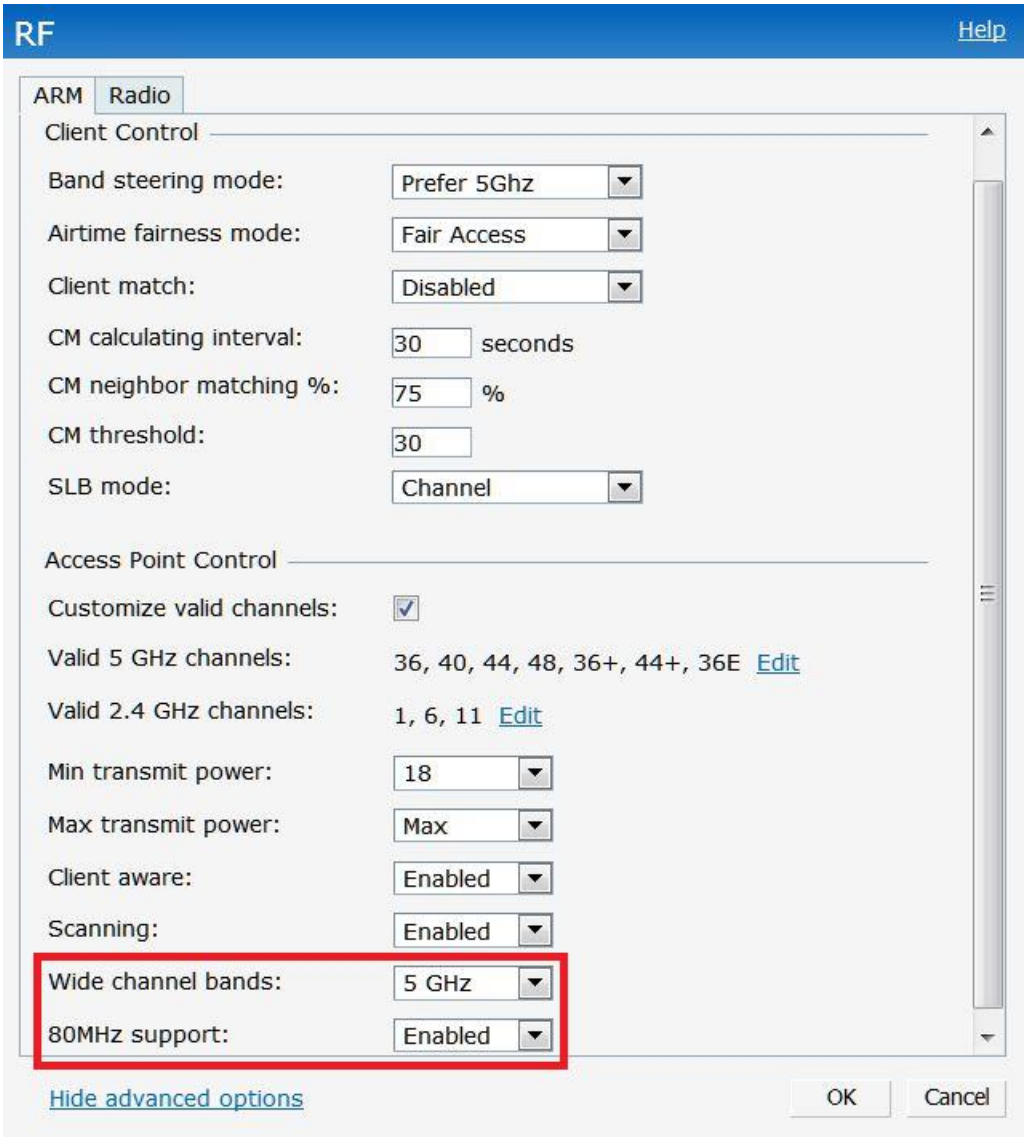
Configuration of Access Points -> Radio

- For testing purposes, the channel and transmit power were assigned manually.



RF settings -> Radio

- 802.11d/802.11h has to be enabled if regulatory domain is set to “world mode” on the Ascom i62



RF settings -> ARM

- For testing purposes, available channels and wide channel support were set statically

Note: Ascom recommends a Beacon Interval of 100ms and advertising 802.11d/h capabilities. Recommended settings for 802.11b/g/n are to use only channel 1, 6 and 11. For 802.11a/n/ac use channels according to the infrastructure manufacturer, country regulations and per guidelines 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), 40MHz is a more viable option because of the availability of additional non-DFS channels. The handset can co-exist with 40MHz stations in the same ESS.***

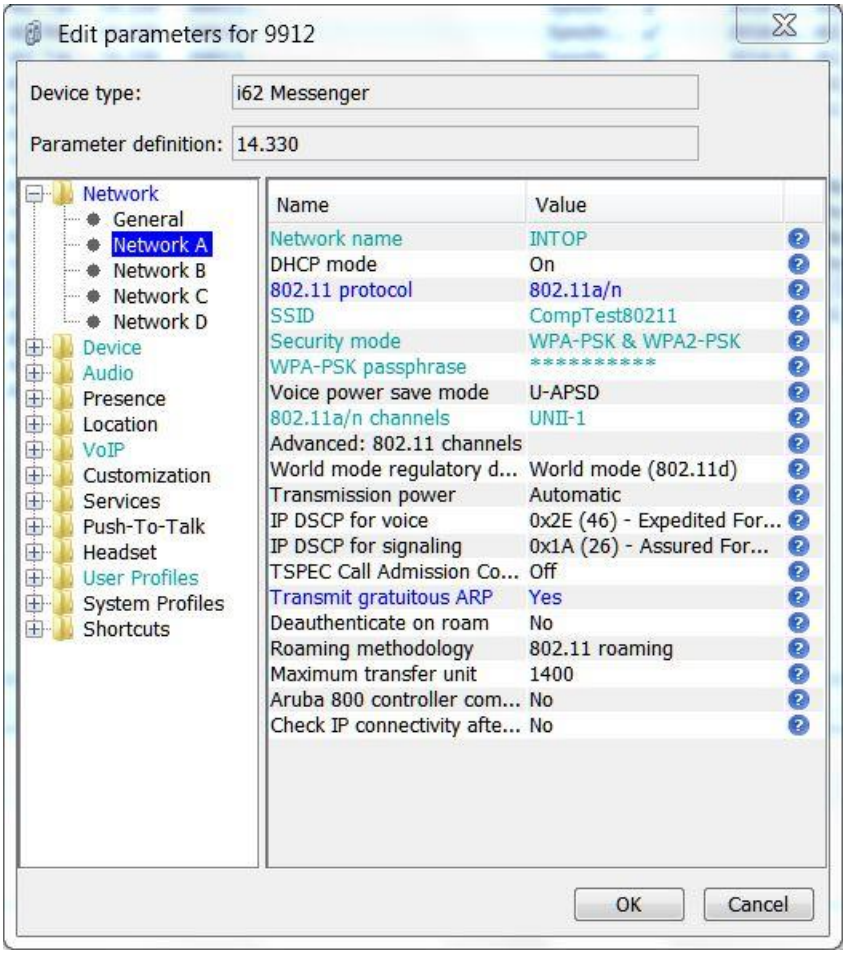
3. ***Ascom do support and can coexist in 80MHz channel bonding environments. The recommendations is however to avoid 80MHz channel bonding as it severely reduces the number of available non overlapping channels.***

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)**

See Appendix B for the controller configuration used for the certification process.

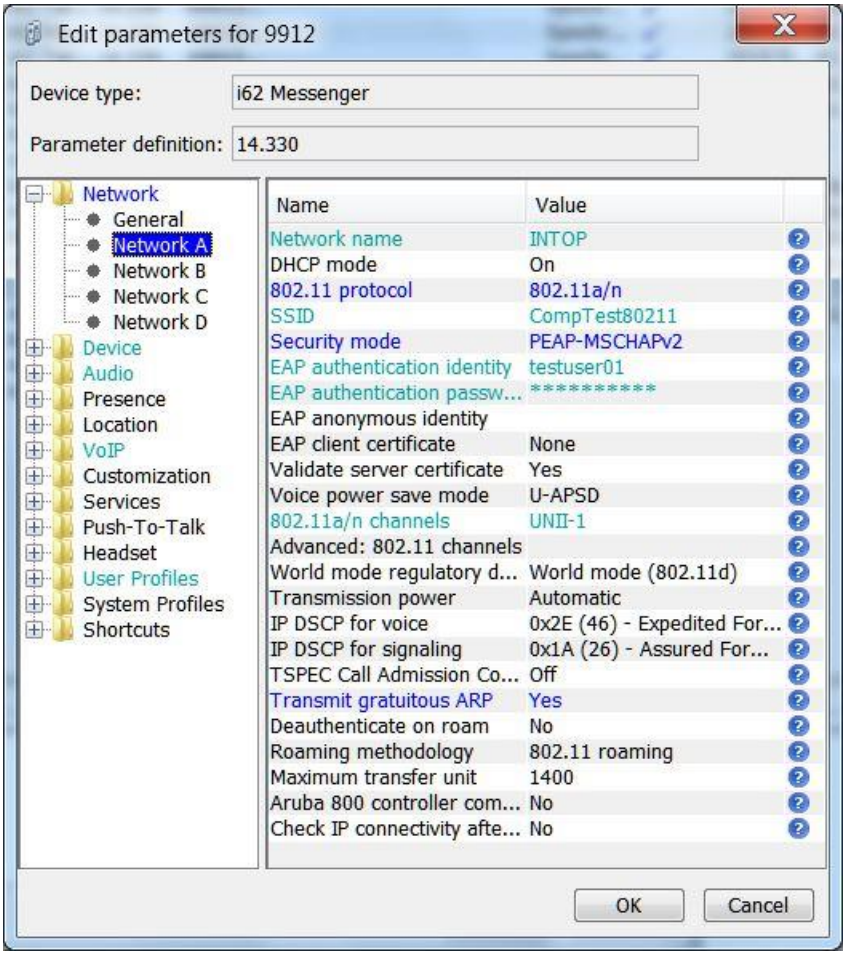
Ascom i62 Setting Summary



Network settings for WPA2-PSK

- Select frequency band according to system setup (here 802.11a/n)
- Select only the channels used in the system. In this example UNII1 (Non DFS)

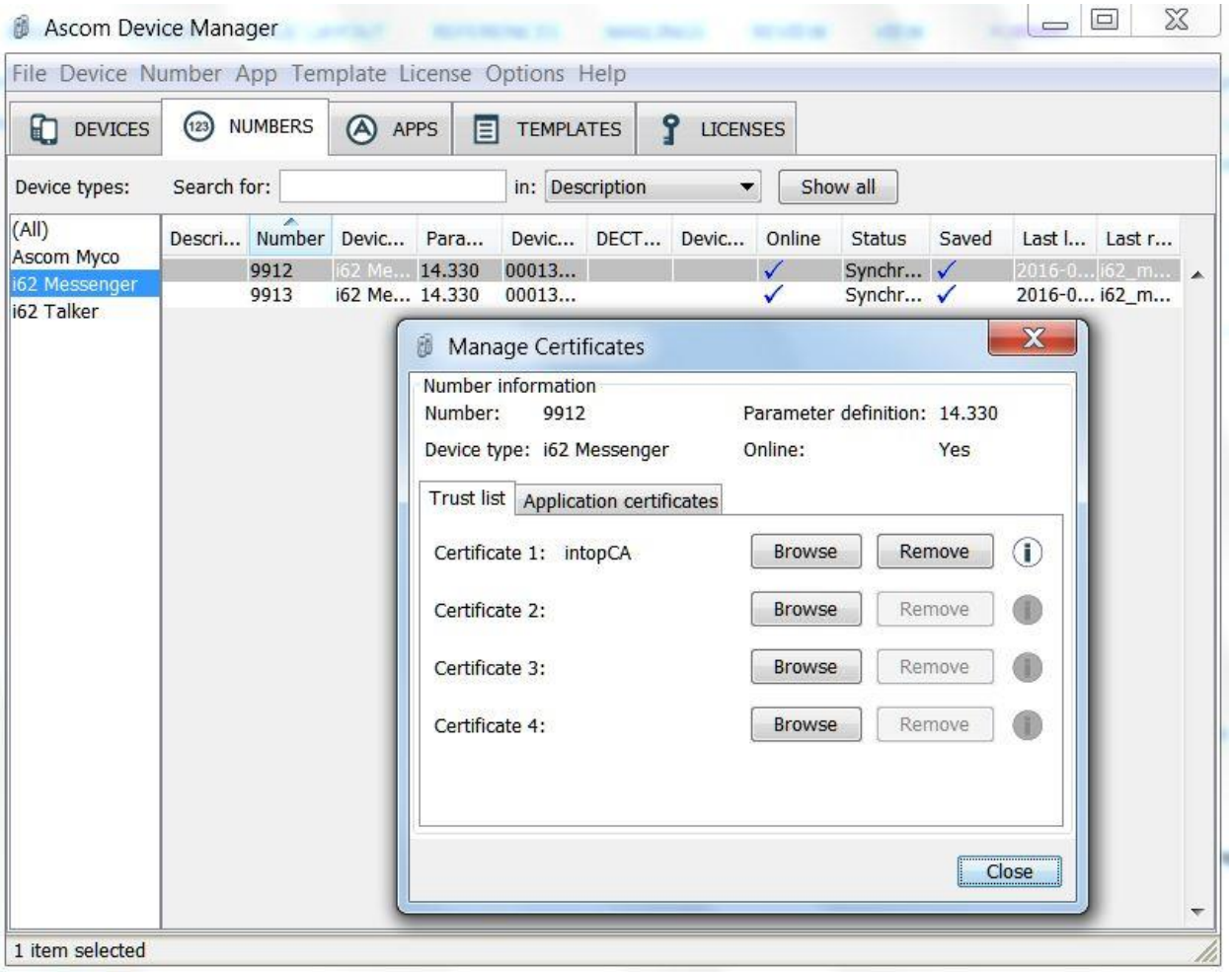
Note: FCC is no longer allowing 802.11d to determine regulatory domain. Devices deployed in the USA must set Regulatory domain to "USA".



Network settings for .1X authentication (PEAP-MSCHAPv2)

- Select frequency band according to system setup (here 802.11a/n)
- Select only the channels used in the system. In this example UNII1 (Non DFS)

Note: FCC is no longer allowing 802.11d to determine regulatory domain. Devices deployed in the USA must set Regulatory domain to "USA".



Ascom Device Manager (or Ascom Portable Device Manager)

- 802.1X Authentication requires a CA certificate to be uploaded to the device. This is done under the "Numbers" tab by "right clicking" the device and selecting "Manage Certificates".

- Upload the required CA certificate under Trust list.

Note that both a root and a client certificate are needed for TLS. Otherwise only a CA certificate is needed. Server certificate validation can be overridden in version 4.1.12 and above per handset setting (Validate server certificate under Network settings).

Appendix B

Test Summary

Please see attached Excel file for detailed test results.

Aruba Test Configuration

```
version 6.4.2.0-4.1.3
virtual-controller-country SE
virtual-controller-key 473d214b0129b787eb61c537eb1cc5a846f060f960ba6dcdca
name instant-C5:78:B6
terminal-access
clock timezone none 00 00
rf-band all

allow-new-aps
allowed-ap f0:5c:19:c5:78:b6
allowed-ap f0:5c:19:c8:2a:c4
allowed-ap f0:5c:19:c1:03:b0

arm
wide-bands none
a-channels 36,40,44,48,36+,44+,36E
g-channels 1,6,11
min-tx-power 18
max-tx-power 127
band-steering-mode disable
air-time-fairness-mode fair-access
client-aware
scanning

rf dot11g-radio-profile
dot11h

rf dot11a-radio-profile
dot11h

syslog-level warn ap-debug
syslog-level warn network
syslog-level warn security
syslog-level warn system
syslog-level warn user
syslog-level warn user-debug
syslog-level warn wireless

extended-ssid

mgmt-user admin 0b94834ab66a32436197776d9e611640

wlan access-rule default_wired_port_profile
index 0
rule any any match any any any permit

wlan access-rule wired-instant
index 1
rule masterip 0.0.0.0 match tcp 80 80 permit
rule masterip 0.0.0.0 match tcp 4343 4343 permit
rule any any match udp 67 68 permit
rule any any match udp 53 53 permit
```

```
wlan access-rule CompTest80211
index 2
rule any any match any any any permit

wlan access-rule CompTest
index 3
rule any any match any any any permit

wlan ssid-profile CompTest80211
enable
index 0
type voice
essid CompTest80211
wpa-passphrase
15cbb11337a83dff3aae1150a2edaff823f0721d3797584044fadcd321082057
opmode wpa2-psk-aes
max-authentication-failures 0
auth-server FreeRadius
rf-band all
captive-portal disable
l2-auth-failthrough
dtim-period 5
inactivity-timeout 1000
broadcast-filter arp
g-min-tx-rate 12
a-min-tx-rate 12
dmo-channel-utilization-threshold 90
local-probe-req-thresh 0
max-clients-threshold 64
wmm-background-dscp "8"
wmm-best-effort-dscp "24"
wmm-video-dscp "26"
wmm-voice-dscp "46"

wlan ssid-profile CompTest
enable
index 1
type voice
essid CompTest
wpa-passphrase
1be82f4c9be1d34374c2b63ca3299126614bc969d5a101f68641252078b147f2
opmode wpa2-psk-aes
max-authentication-failures 0
auth-server InternalServer
rf-band all
captive-portal disable
dtim-period 5
inactivity-timeout 1000
broadcast-filter arp
dmo-channel-utilization-threshold 90
local-probe-req-thresh 0
max-clients-threshold 64

auth-survivability cache-time-out 24

wlan auth-server FreeRadius
ip 10.11.24.98
port 1812
```

```
acctport 1813
key 8b58b860192c587a3ca5282b32be0fbe

wlan external-captive-portal
server localhost
port 80
url "/"
auth-text "Authenticated"
auto-whitelist-disable
https

blacklist-time 3600
auth-failure-blacklist-time 3600

ids
wireless-containment none

wired-port-profile wired-instant
switchport-mode access
allowed-vlan all
native-vlan guest
no shutdown
access-rule-name wired-instant
speed auto
duplex auto
no poe
type guest
captive-portal disable
no dot1x
inactivity-timeout 1000

wired-port-profile default_wired_port_profile
switchport-mode trunk
allowed-vlan all
native-vlan 1
shutdown
access-rule-name default_wired_port_profile
speed auto
duplex full
no poe
type employee
captive-portal disable
no dot1x
inactivity-timeout 1000

enet0-port-profile default_wired_port_profile

uplink
preemption
enforce none
failover-internet-pkt-lost-cnt 10
failover-internet-pkt-send-freq 30
failover-vpn-timeout 180

airgroup
disable
```

```
airgroupservice airplay
disable
description AirPlay

airgroupservice airprint
disable
description AirPrint
```